

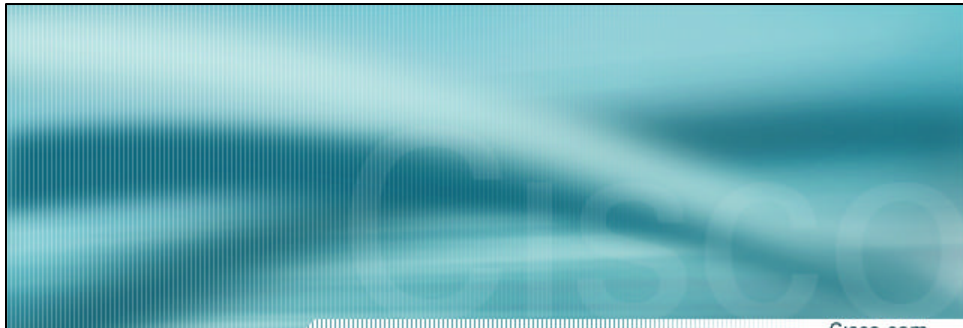


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

1

CISCO SYSTEMS





Cisco.com

MPLS–Technology Options and Applications

Session PS-542

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 3

Power Session Agenda

Cisco.com

- Introduction and MPLS Standardization
- MPLS VPNs
- Management of MPLS
- MPLS Traffic Engineering
- MPLS VPN Services
- OCP Strategy and Roadmaps

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 4



Cisco.com

Introduction

MPLS—Technology and Services

Section 1

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 5

Agenda

Cisco.com

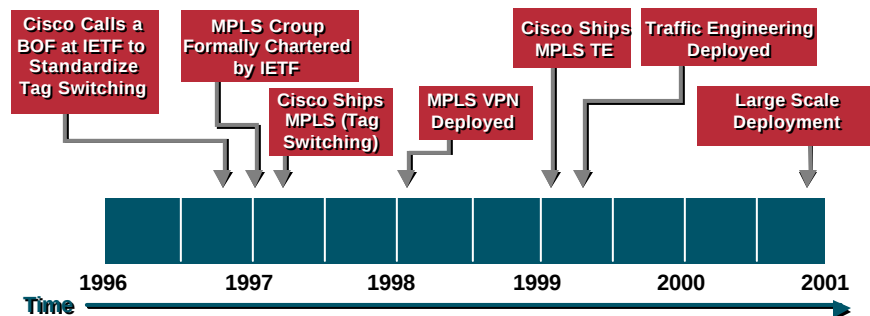
- **Evolution and Key Drivers**
- **Technology Basics**
 - What Is MPLS? Where Is It Used?
- **Label Distribution in MPLS Networks**
 - LDP, RSVP, BGP
- **Building MPLS-Based Services**
 - VPNs
 - Traffic Engineering (FRR and Protection)
 - AToM
- **IETF Update**
- **Summary**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 6

Evolution of MPLS

Cisco.com

- From tag switching
- Proposed in IETF—Later combined with other proposals from IBM (ARIS), Toshiba (CSR)

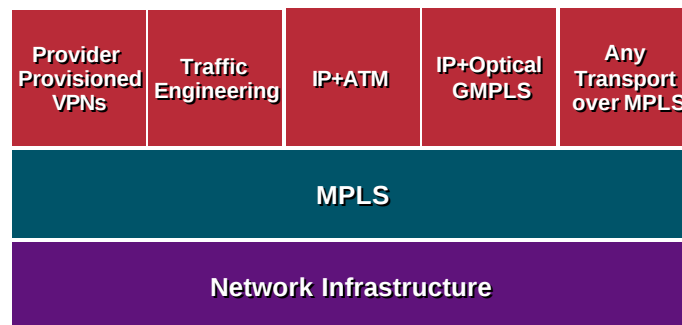


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

7

MPLS as a Foundation for Value-Added Services

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

8



Cisco.com

Technology Specifics

PS-542
3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

9



Cisco.com

Encapsulations

ATM Cell Header

GFC	VPI	VCI	PTI	CLP	HEC	DATA
-----	-----	-----	-----	-----	-----	------

Label

**PPP Header
(Packet over SONET/SDH)**

PPP Header	Label Header	Layer 3 Header
------------	--------------	----------------

LAN MAC Label Header

MAC Header	Label Header	Layer 3 Header
------------	--------------	----------------

PS-542
3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

10

MPLS Operation—Re-Cap

Cisco.com

1a. Existing Routing Protocols (E.G. OSPF, ISIS)
Establish Reachability to Destination Networks

1b. Label Distribution Protocol (LDP)
Establishes Label to Destination
Network Mappings

4. Edge LSR at Egress
Removes Label and
Delivers Packet

2. Ingress Edge LSR Receives Packet,
Performs Layer 3 Value-Added
Services, and "Labels" Packets

3. LSR Switches Packets
Using Label Swapping

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

11

Label Distribution in MPLS Networks

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

12

Label Distribution Protocol

Cisco.com

- **Defined in RFC 3036 and 3037**
- **Used to distribute labels in a MPLS network**
- **Forwarding equivalence class**
How packets are mapped to LSPs
(Label Switched Paths)
- **Advertise labels per FEC**
Reach destination a.b.c.d with label x
- **Neighbor discovery**
Basic and extended discovery

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

13

Label Distribution Protocol

Cisco.com

- **Label merge**
Done by default for packet
networks—Unique label advertised
per FEC
Requires VC merge for ATM networks

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

14

TDP and LDP

Cisco.com

- **Tag Distribution Protocol**
 - Pre-cursor to LDP
 - Used for Cisco tag switching
- **TDP and LDP supported on the same box**
 - Per neighbor/link basis
 - Per target basis

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

15

TDP and LDP

Cisco.com

- **Similarities and differences**
 - Same label format
 - Different message format
- **LDP features that are not part of TDP:**
 - Extension mechanism for vendor-private and experimental features
 - Backoff procedures for session establishment failures
 - Abort mechanism for LSP setup
 - Optional use of TCP MD5 signature option for (more) secure operation
 - Optional path-vector based loop detection mechanism to prevent setup of looping LSPs
 - More combinations of modes of operation

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

16

RSVP and Label Distribution

Cisco.com

- **Used in MPLS traffic engineering**
- **Additions to RSVP signaling protocol**
- **Leverage the admission control mechanism of RSVP**
- **Label requests are sent in PATH messages and binding is done with RESV messages**
- **EXPLICIT-ROUTE object defines the path over which setup messages should be routed**
- **Using RSVP has several advantages**
 - Traffic engineering, shared explicit, FRR**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

17

BGP-Based Label Distribution

Cisco.com

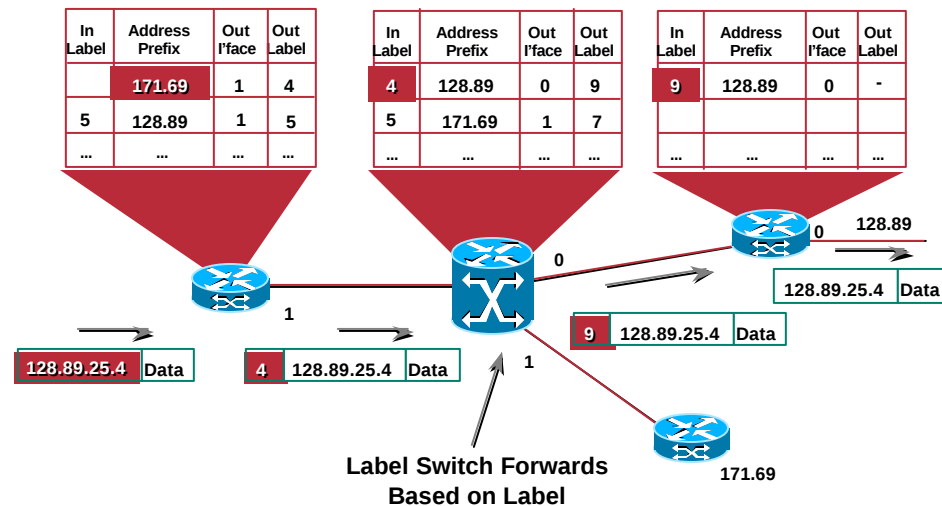
- **Used in the context of MPLS VPNs**
- **Need multi-protocol extensions to BGP**
- **Routers need to be BGP peers**
- **Label mapping info carried as part of NLRI (Network Layer Reachability Information)**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

18

MPLS Example: Forwarding Packets

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

19

Label Stacking

Cisco.com

- IGP labels—Used for routing packets
- BGP labels—Used for assigning end users/communities
- RSVP labels—Used for TE tunnels
- If more than one service is used
Then multiple labels are required—TE and FRR
In some cases a single service requires the use of multiple labels—VPNs

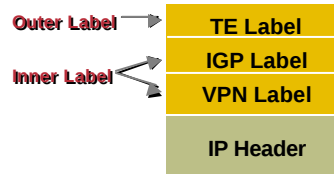
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

20

Label Stacking—How?

Cisco.com

- Arrange labels in a stack
- Inner labels can be used to designate services/FECs, etc.
E.g VPNs, fast re-route
- Outer label used to route/switch the MPLS packets in the network
- Allows building services such as
 - MPLS VPNs—Basic and advanced—CSC
 - Traffic engineering and fast re-route
 - VPNs over traffic engineered core
 - Any transport over MPLS



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

21

MPLS-Based Services

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

22

Provider Provisioned VPNs

Categories

- **BGP MPLS VPNs—RFC 2547**
Supported by Cisco
- **Virtual routers**
Alternative proposal—Relies on logical partitioning of the physical box
Requires the use of multicast/broadcast for better convergence

What Is a VPN?

Cisco.com

- VPN is a **set of sites** which are allowed to **communicate** with each other
- VPN is defined by a **set of administrative policies**

Policies determine both connectivity and QoS among sites

Policies **established by VPN customers**

Policies could be **implemented** completely by **VPN service providers**

Using **BGP/MPLS VPN** mechanisms

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

25

What Is a VPN? (Cont.)

Cisco.com

- **Flexible inter-site connectivity**
Ranging from complete to partial mesh
- **Sites may be either within the same or in different organizations**
VPN can be either Intranet or Extranet
- **Site may be in more than one VPN**
VPNs may overlap
- **Not all sites have to be connected to the same service provider**
VPN can span multiple providers

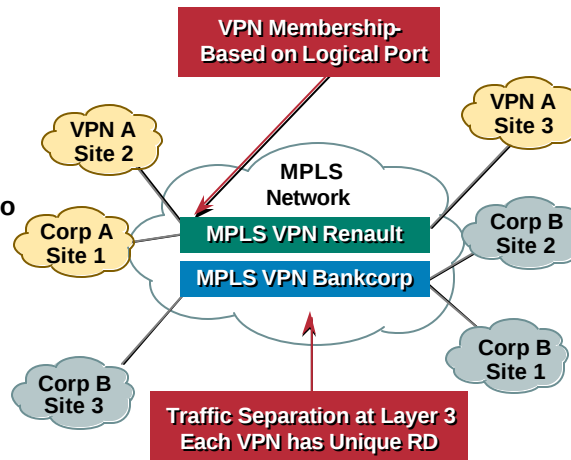
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

26

MPLS-Based IP-VPN Architecture

Cisco.com

- Scalable VPNs
- IP QoS and traffic engineering
- Easy to manage and no VC provisioning required
- Provides a level of Security equivalent to Frame Relay and ATM
- Supports the deployment of new value-added applications
- Customer IP address freedom

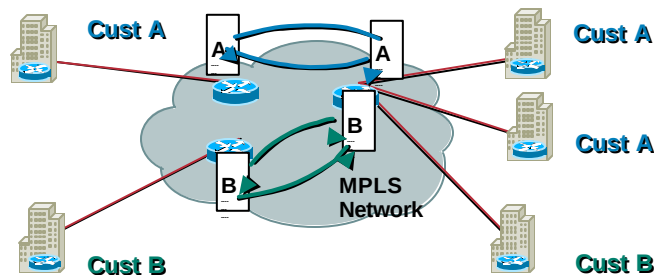


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

27

Using Labels to Build an IP VPN

Cisco.com



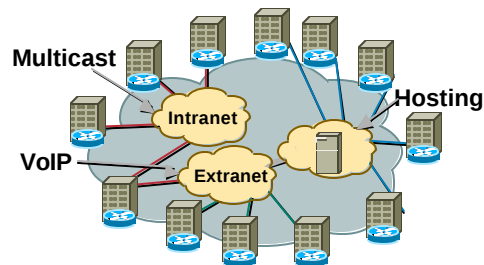
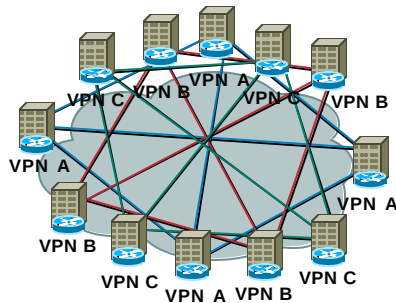
- The network distributes labels to each VPN
- Only labels for other VPN members are distributed
Each VPN is provisioned automatically by IP routing
- Privacy and QoS of ATM without tunnels or encryption
Each network is as secure as a Frame Relay connection
- One mechanism (labels) for QoS and VPNs—No tradeoffs

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

28

Service Provider Benefits of MPLS-Based VPNs

Cisco.com



- **Overlay VPN**

Pushes content **outside** the network
 Costs scale exponentially
 Transport dependent
 Groups endpoints, not groups
 Complex overlay with QoS, tunnels, IP

- **MPLS-based VPNs**

Enables content hosting **inside** the network
 "Flat" cost curve
 Transport independent
 Easy grouping of users and services
 Enables QoS inside the VPNs

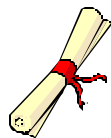
PS-542
 3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

29

MPLS-Based IP-VPN Security

Cisco.com

Miercom



**"Cisco MPLS-Based VPNs:
 Equivalent to the Security of
 Frame Relay and ATM."**

Miercom, March 30, 2001

<http://www.mier.com/reports/cisco/MPLS-VPNs.pdf>



PS-542
 3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

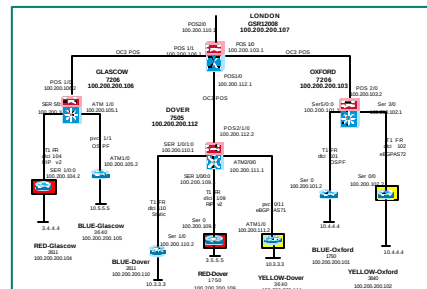
30

Validating Cisco MPLS-Based IP-VPN as a Secure Network

Cisco.com

Miercom Independent Testing Confirmed Cisco MPLS VPN Is Secure

- Customers network topology is not revealed to the outside world
- Customers can maintain own addressing plans and the freedom to use either public or private address space
- Attackers cannot gain access into VPNs or service provider's network
- Impossible for attacker to insert "spoofed" label into a Cisco MPLS network and thus gain access to a VPN or the MPLS core



Test Network Topology

Security



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

31

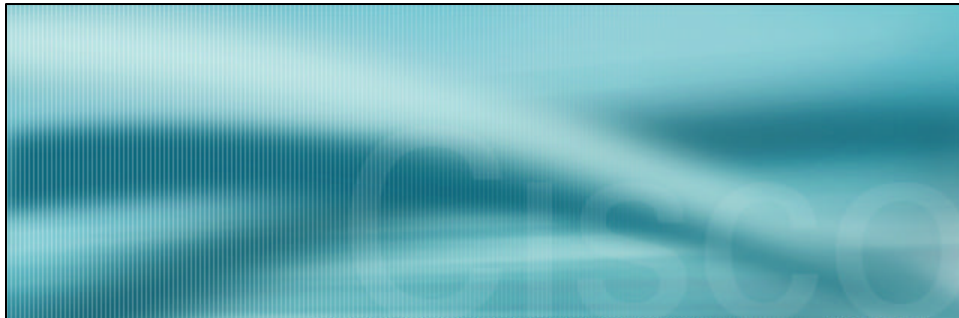
BGP/MPLS VPN—Summary

Cisco.com

- Supports large scale VPN service
- Increases value add by the VPN service provider
- Decreases service provider cost of providing VPN services
- Mechanisms are general enough to enable VPN service provider to support a wide range of VPN customers

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

32



Cisco.com

MPLS Traffic Engineering

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 33

Why Traffic Engineering?

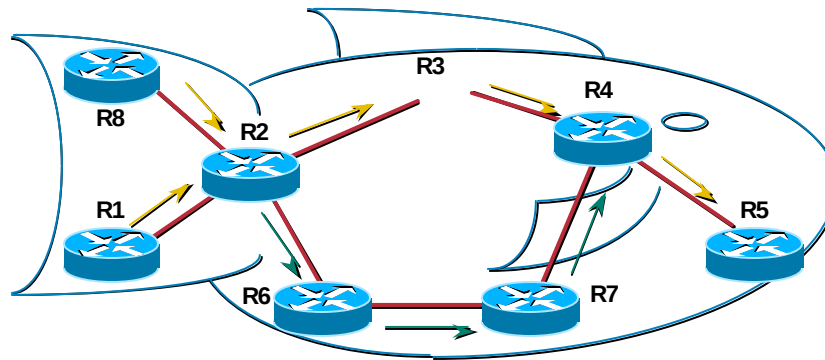
Cisco.com

- **Congestion in the network due to changing traffic patterns**
Election news, online trading, major sports events
- **Better utilization of available bandwidth**
Route on the non-shortest path
- **Route around failed links/nodes**
Fast rerouting around failures, transparently to users
Like SONET APS (Automatic Protection Switching)
- **Build new services—Virtual leased line services**
VoIP toll-bypass applications, point-to-point bandwidth guarantees
- **Capacity planning**
TE improves aggregate availability of the network

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 34

IP Routing and the Fish

Cisco.com



IP (Mostly) Uses Destination-Based Least-Cost Routing
Flows from R8 and R1 Merge at R2 and Become Indistinguishable
from R2, Traffic to R3, R4, R5 Use Upper Route

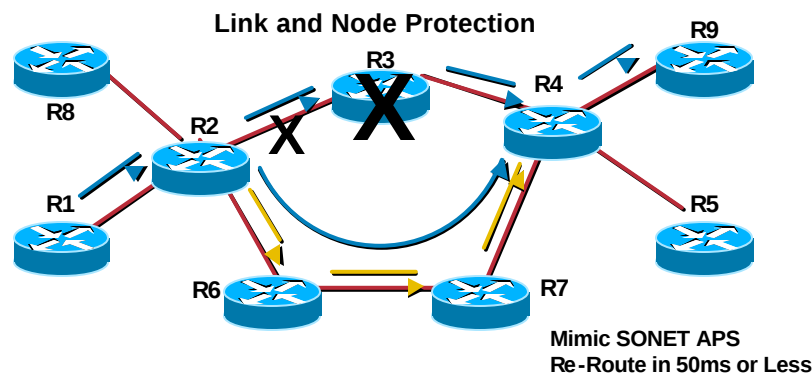
Alternate Path Under-Utilized

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

35

Applications of MPLS TE

Cisco.com



- Multiple hops can be by-passed; R2 swaps the label which R4 expects before pushing the label for R6
- R2 locally patches traffic onto the link with R6

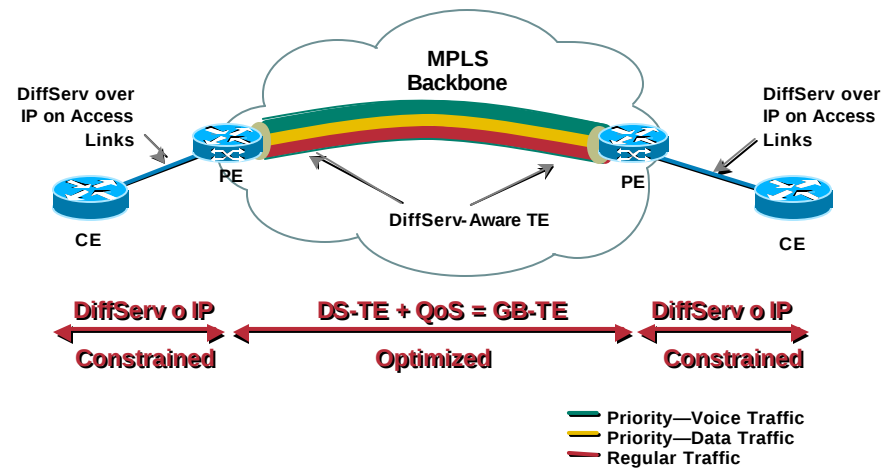
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

36

MPLS Traffic Engineering for a QoS-Optimized Backbone

Cisco.com

DiffServ-Aware TE and QoS!

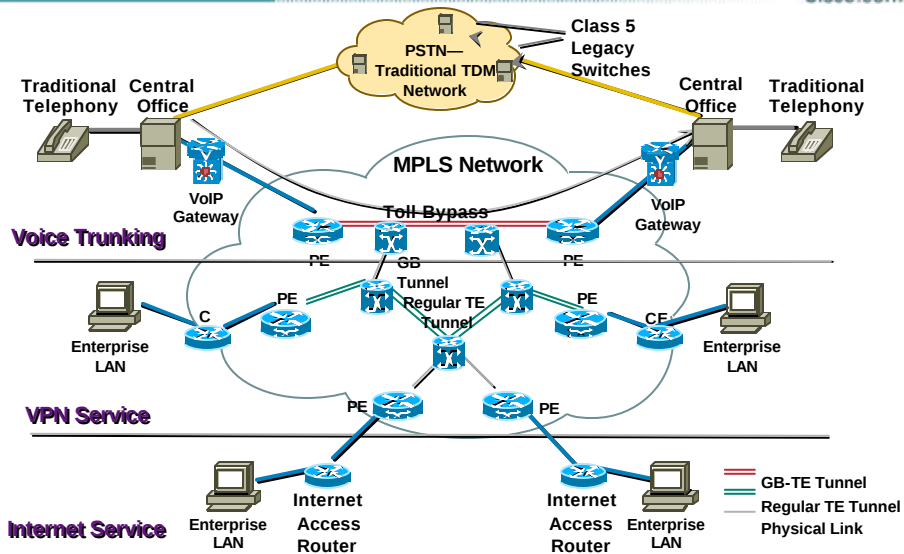


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

37

DiffServ Aware TE Virtual Leased line

Cisco.com



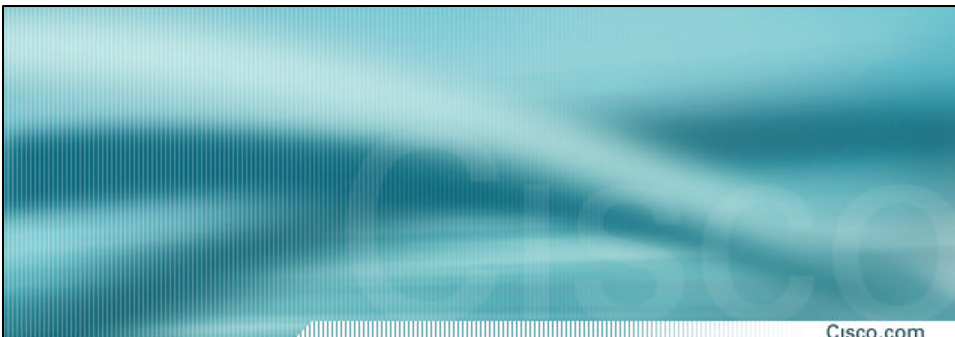
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

38

MPLS TE Summary

Cisco.com

- **Useful for re-routing traffic in congested environments**
- **Build innovative services like virtual leased line**
- **Build protection solutions using MPLS FRR**



Cisco.com

Any Transport over MPLS

Any Transport over MPLS

Cisco.com

- **Trunking Layer 2 over an MPLS Network**
 - Ethernet**
 - Frame Relay**
 - ATM—AAL5, cell mode**
 - PPP**
 - Cisco HDLC**
 - SONET**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

41

Motivation for AToM

Cisco.com

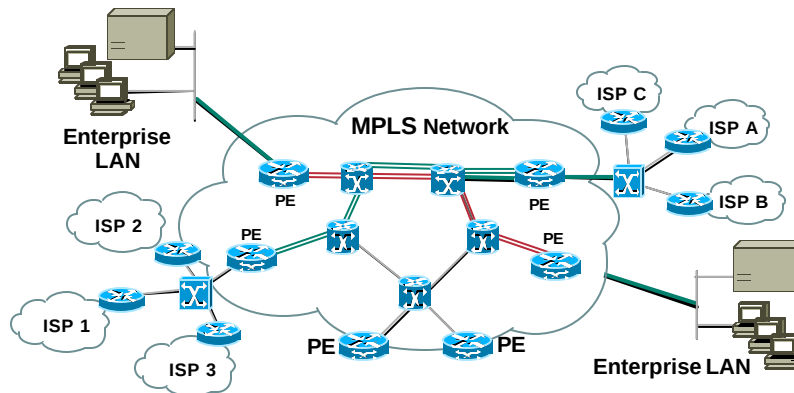
- **Leverage the existing installed gear**
- **Provide circuit-based services in addition to packet/IP based services**
- **Transparent trunking of customer IGP**
- **Provide any-to any connectivity**
- **Similar to existing circuit switched environment**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

42

Ethernet over MPLS

Cisco.com

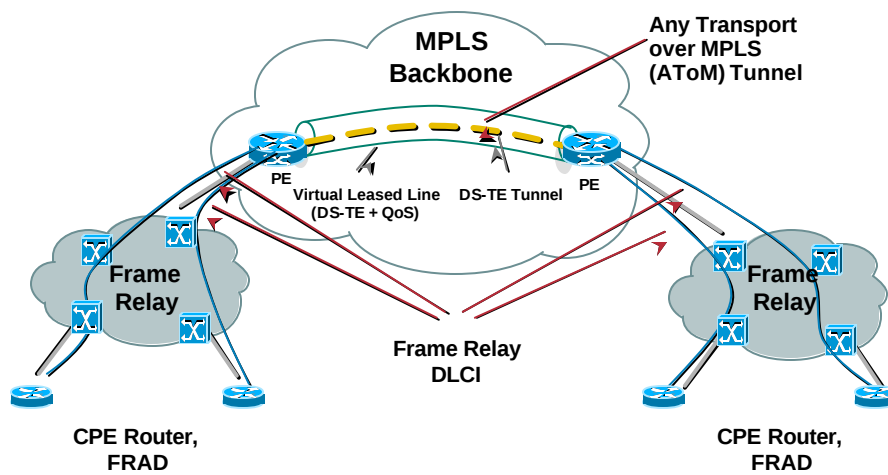


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

43

Frame Relay over MPLS

Cisco.com

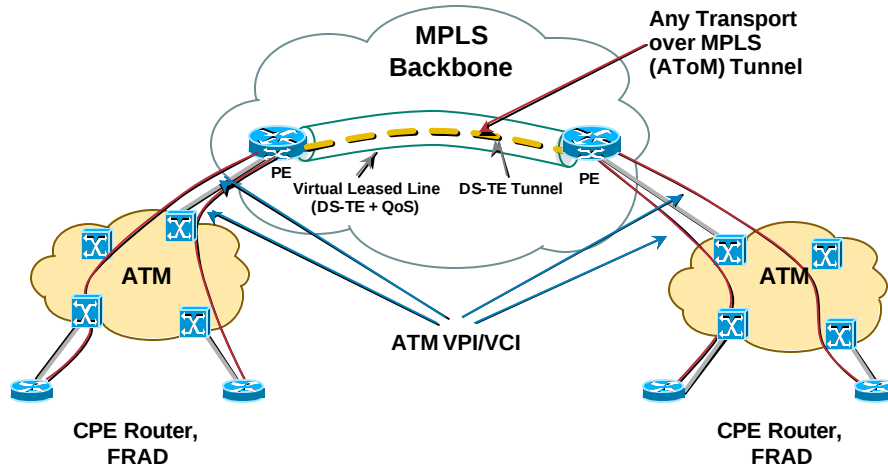


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

44

ATM over MPLS

Cisco.com

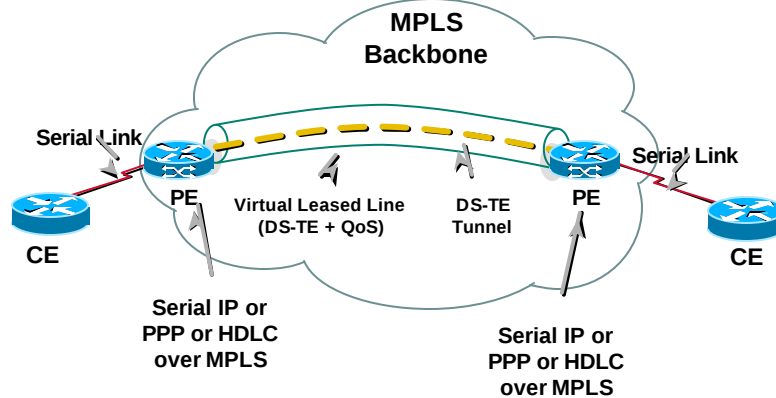


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

45

PPP, Cisco HDLC over MPLS

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

46



Cisco.com

MPLS QoS

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 47

Coloring MPLS Frames

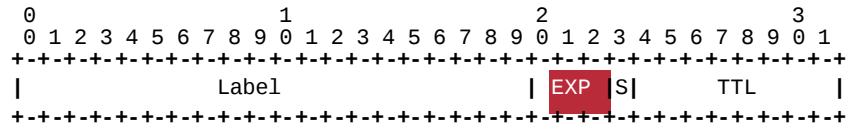
Cisco.com

- **Two methods are possible**
 - Using the EXP bits in the MPLS header and mapping DSCP to EXP**
 - Convenient for frame-based interface**
 - Mapping a label per-CoS per-FEC**
 - Convenient for ATM-based interface**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 48

Using the EXP Bits

Cisco.com



- Copy of precedence into EXP
- Mapping of DSCP into EXP

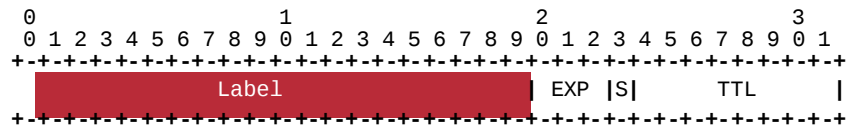


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

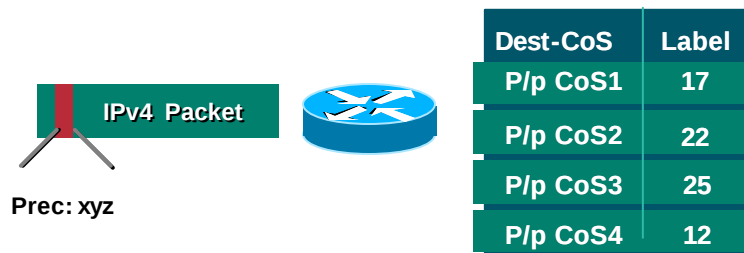
49

Label-Inferred CoS

Cisco.com



- DSCP/precedence to label mapping



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

50

MPLS QoS Summary

Cisco.com

- Use the same underlying IP QoS mechanisms
 - Queuing—LLQ, CBWFQ
 - Policing
 - WRED
- Classification and marking done on EXP bits in the label header
- Label header marking can be different from the IP header DSCP providing a transparency

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

51

IETF Update

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

52

IETF Update

Cisco.com

- **MPLS workgroup status**
- **IETF/MPLS reorganization**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

53

MPLS WG

Cisco.com

- **Base MPLS technology specifications are complete**
- **11 MPLS WG RFCs**
- **10 more drafts awaiting publication**
- **Available at:**
<http://www.ietf.org/html.charters/mpls-charter.html>
- **RFC2547—MPLS/BGP VPNs (informational)**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

54

MPLS RFCs

Cisco.com

- Requirements for **Traffic Engineering** over MPLS (RFC 2702)
- Multiprotocol Label Switching **Architecture** (RFC 3031)
- MPLS **Label Stack** Encoding (RFC 3032)
- Use of Label Switching on Frame Relay Networks Specification (RFC 3034)
- MPLS using LDP and **ATM** VC Switching (RFC 3035)
- **LDP** Specification (RFC 3036)
- LDP Applicability (RFC 3037)
- VCID Notification over ATM link for LDP (RFC 3038)
- The Assignment of the Information Field and Protocol Identifier in the Q.2941 Generic Identifier and Q.2957 User-to-User Signaling for the Internet Protocol (RFC 3033)
- MPLS Loop Prevention Mechanism (RFC 3063)
- Carrying Label Information in **BGP-4** (RFC 3107)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

55

Near RFC Publication

Cisco.com

- **RSVP-TE**: Extensions to RSVP for LSP Tunnels
- Applicability Statement for Extensions to RSVP for LSP-Tunnels
- **Constraint-Based LSP** Setup using LDP
- LSP Modification Using CR-LDP
- Applicability Statement for CR-LDP
- LDP State Machine
- Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)
- MPLS Support of **Differentiated Services**
- Framework for IP Multicast in MPLS
- MPLS Label Switch Router Management Information Base Using SMIv2

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

56

Reorganization of MPLS

Cisco.com

- Original charter is complete
- Focus has moved in two directions
 - Applications—VPNs, DS-TE, L2 transport
 - Generalization of the MPLS-TE control plane to optical and circuit technologies

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

57

Generalized MPLS

Cisco.com

- Really a generalization of the traffic engineering application of MPLS
- Originally applied to setting up light-paths and called MPLambdaS
- Now includes SDH, port switching
- Renamed to G-MPLS

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

58

New Workgroups

Cisco.com

- **Traffic engineering involves MPLS signaling (RSVP or CR-LDP) and link-state routing (OSPF or IS-IS)**
- **Since the technology involves more than MPLS it was decided to form a separate work-group**
- **CCAMP—Common Control and Measurement Protocols**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

59

New Workgroups

Cisco.com

- **Pseudo-Wire Emulation Edge-to-Edge (PWE3)**
Layer 2 transport of AAL5 frames, ATM cells, Frame Relay, SONET
- **Provider Provisioned Virtual Private Networks (PPVPN)**
MPLS-BGP VPN: RFC2457, I2vpn with use of PWE3 technology, virtual routers, IPSEC

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

60

Traffic Engineering Workgroup

Cisco.com

- Formed—2 yrs ago
- Originally had an operational focus
- With re-org, now has a role in defining requirements
- DS-TE will first be addressed here

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

61

Sup-IP Area

Cisco.com

- Area director(s):
 - Scott Bradner <sob@harvard.edu>
 - Bert Wijnen <bwijnen@lucent.com>
- Working groups:
 - Common Control and Measurement Plane (CCAMP)
 - General Switch Management Protocol (GSMP)
 - IP over Optical (IPO)
 - IP over Resilient Packet Rings (IPORPR)
 - Internet Traffic Engineering (TEWG)
 - Multiprotocol Label Switching (MPLS)
 - Provider Provisioned Virtual Private Networks (PPVPN)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

62



Cisco.com

Summary

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 63

What **Isn't** MPLS?

Cisco.com

- MPLS is not just integration of IP and ATM, **but**
- Integration of IP and ATM is just one of the applications of MPLS

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 64

What **Isn't** MPLS?

Cisco.com

- MPLS is not a way to make routers (much) faster, **but**
- MPLS forwarding algorithm is simpler than IP forwarding algorithm, **and** it enables more functionality than could be provided with the IP forwarding algorithm

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

65

MPLS and the OSI Reference Model (OSIRM)

Cisco.com

- **MPLS is not a network layer**
Doesn't have routing and addressing on its own—uses IP addressing + IP routing (with extensions)
- **MPLS is not a link layer**
Because MPLS works over various Link Layer technologies (e.g., SONET, Ethernet, ATM, etc...)
- **MPLS is not a layer in the OSIRM sense**
Doesn't have a single format for transport of the data from the layer above
“shim” on SONET, VCI/VPI on ATM, lambda on OXC, etc...

MPLS Does Not Fit Into the OSI Reference Model

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

66

MPLS—Key Benefits

Cisco.com

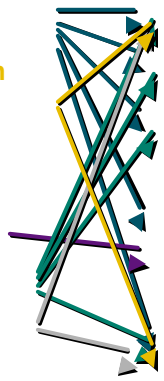
- **New value-added services**
 - BGP MPLS VPNS—RFC 2547**
 - Traffic engineering**
 - L2 VPNS**
 - Protection solutions**
 - Link and node protection**
 - Bandwidth protection—Future**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

67

MPLS and Its Applications

Cisco.com

- **Separate forwarding information (label) from the content of IP header**
 - **Single forwarding paradigm (label swapping)—multiple routing paradigms**
 - **Multiple link-specific realizations of the label swapping forwarding paradigm**
 - **Flexibility of forming FECs**
 - **Forwarding hierarchy via label stacking**
- 
- **Traffic engineering**
 - **Fast re-route**
 - **“Hard” QoS support**
 - **Integration with optical cross connects**
 - **Scalable VPN**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

68

MPLS—Deployment

Cisco.com

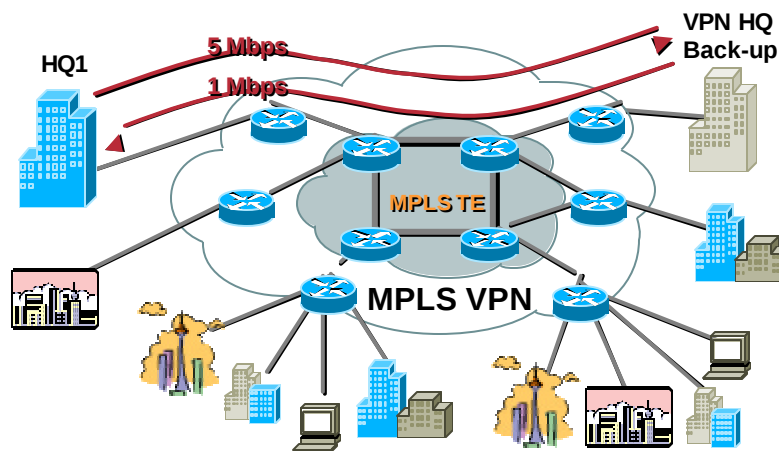
- Supported on
GSR, 7500, 7200, 3600, 2600, MGX, BPX, 6400,
uBR7200, 10K
- Production deployed by many service providers
- Key to providing innovative services

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

69

End-to-End Solution

Cisco.com



**VPN and Traffic Engineering Combined
to Provide End-to-End Services**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

70

Questions?

MPLS VPN Architecture Scaling

Section 2

Agenda

Cisco.com

- **MPLS VPN Single Backbone Architecture**
- **MPLS VPN Scalability Elements**
- **Sizing Provider Edge (PE) Routers**
- **Memory Sizing Design Guidelines**
- **PE Router Throughput Considerations**
- **Internal and External Routing Protocol Sizing**
- **MPLS VPN Convergence Tuning**
- **Summary**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

73

MPLS VPN

Single Backbone Architecture

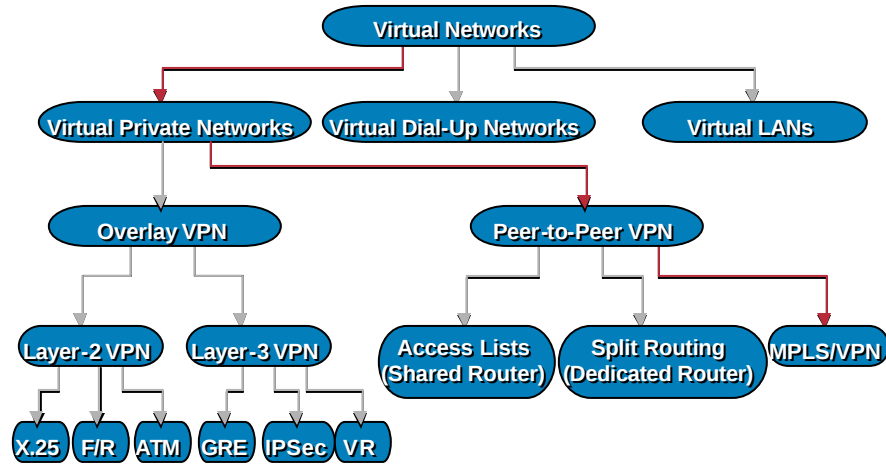
Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

74

Virtual Network Models

Cisco.com

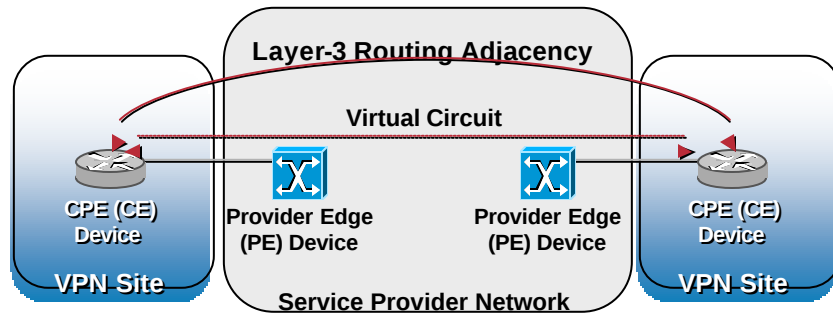


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

75

Overlay VPN Model

Cisco.com



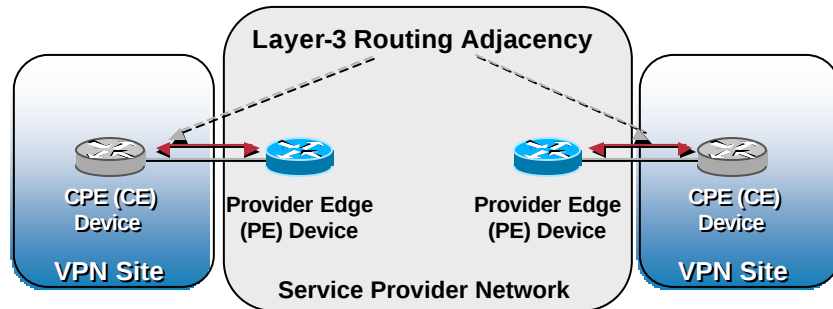
- ✗ How to Size Inter-Site Circuit Capacity?
- ✗ Duplicate IP Addressing Capability
- ✗ Full Circuit Mesh Requirement for Optimal Routing
- ✗ Complete Isolation Between Customers
- ✗ Layer-3 CPE Routing Adjacencies between Sites
- ✗ Secure VPN Service

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

76

Peer-to-Peer VPN Model

Cisco.com



~~✗~~ All VPN Routes Carried in SP IGP

~~✗~~ Duplicate IP Addressing Is **Not** an Option

~~✗~~ Complex Filters or Dedicated Devices

~~✗~~ Routing between Sites Is Optimal

~~✗~~ Circuit Sizing between Sites No Longer Such an Issue

~~✗~~ Simple Routing Scheme for Customers—No Overlay Mesh

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

77

VPN—MPLS/VPN Model

Cisco.com

- **Combine benefits of overlay and peer-to-peer models**
 - Overlay (security and isolation between customers)
 - Peer-to-peer (simplified customer routing)
- **PE routers only hold routes for attached VPNs**
 - Reduces size of PE routing information
 - Proportional to number of VPNs attached
- **MPLS used to forward packets (not routing)**
 - Full routing within backbone no longer required

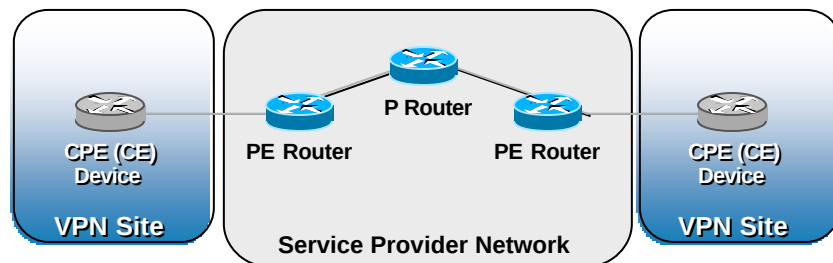
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

78

MPLS/VPN Model

Cisco.com

Combined Benefits of Overlay and Peer-to-Peer VPN Models



Routing between Sites Is Optimal

Duplicate IP Addressing Capability

Secure Service

PE Routers Hold **Only** Relevant VPN Routes

Complete Isolation between Customers

No Complex Filters or Dedicated Routers

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

79

VPN Routing and Forwarding Instance (VRF)

Cisco.com

- PE routers maintain separate routing tables

Global routing table

Contains all PE and P routes (perhaps BGP)

Populated by the VPN backbone IGP

VRF (VPN routing and forwarding)

Routing and forwarding table associated with one or more directly connected sites (CE routers)

VRF is associated with any type of interface, whether logical or physical (e.g. sub/virtual/tunnel)

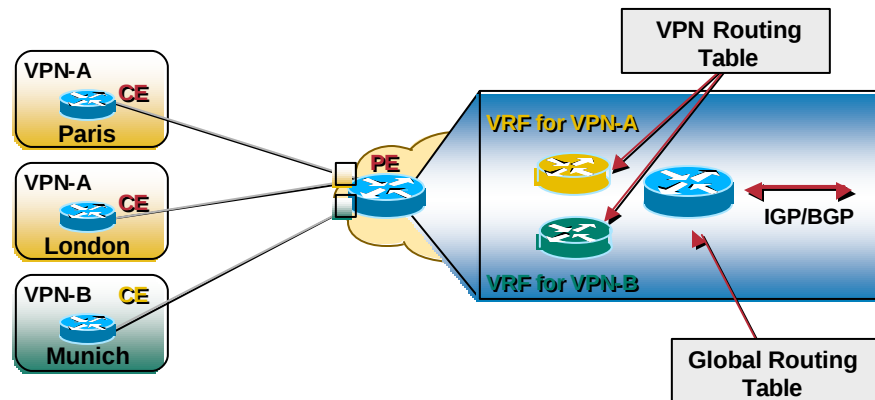
Interfaces may share the same VRF if the connected sites share the same routing information

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

80

VPN Routing and Forwarding Instance (VRF)

Cisco.com



**Multiple Routing and Forwarding Instances (VRFs)
Provide the Separation**

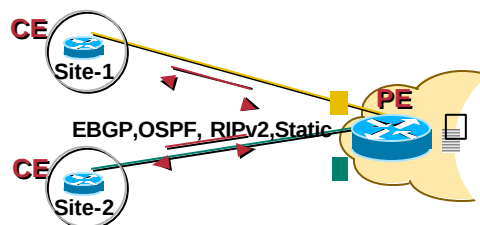
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

81

VRF Route Population

Cisco.com

- VRF is populated **locally** through PE and CE routing protocol exchange
 - RIP version 2, OSPF, BGP-4 and static routing
- Separate routing context for each VRF
 - Routing protocol context (BGP-4 and RIP v2)
 - Separate process (OSPF)



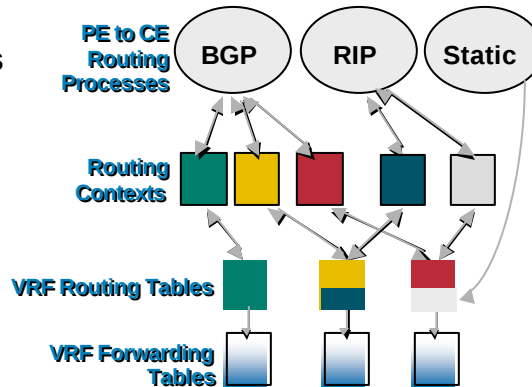
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

82

VRF and Multiple Routing Instances

Cisco.com

- Routing processes run within specific routing contexts
- Populate specific VPN routing table and FIBs (VRF)
- Interfaces are assigned to VRFs

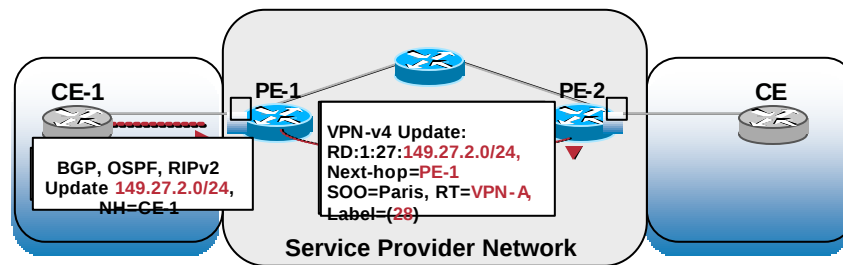


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

83

VRF Population of MP-BGP

Cisco.com

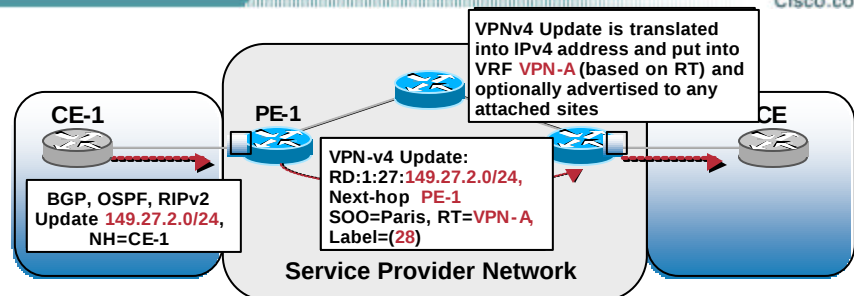


- PE routers translate into VPN-V4 route
 - Assigns an RD, SOO, and RT based on configuration
 - Re-writes next-hop attribute (to PE loop back)
 - Assigns a label based on VRF and/or interface
 - Sends MP-BGP update to all PE neighbors

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

84

VRF Population of MP-BGP

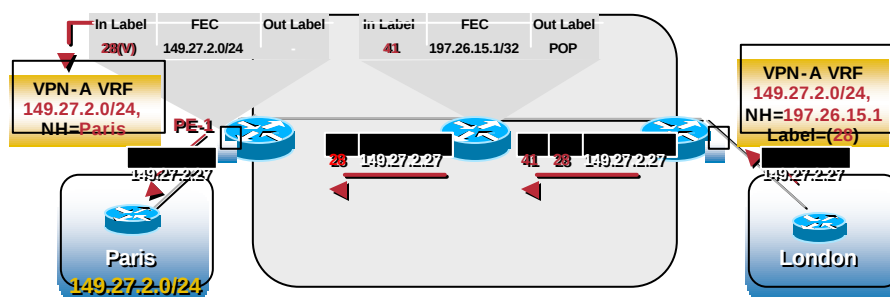


- Receiving PE routers translate to IPv4
Insert the route into the VRF identified by the RT attribute (based on PE configuration)
- The label associated to the VPN-V4 address will be set on packets forwarded towards the destination

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

85

MPLS/VPN Packet Forwarding



Packet Forwarding Based on Stack of Labels

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

86



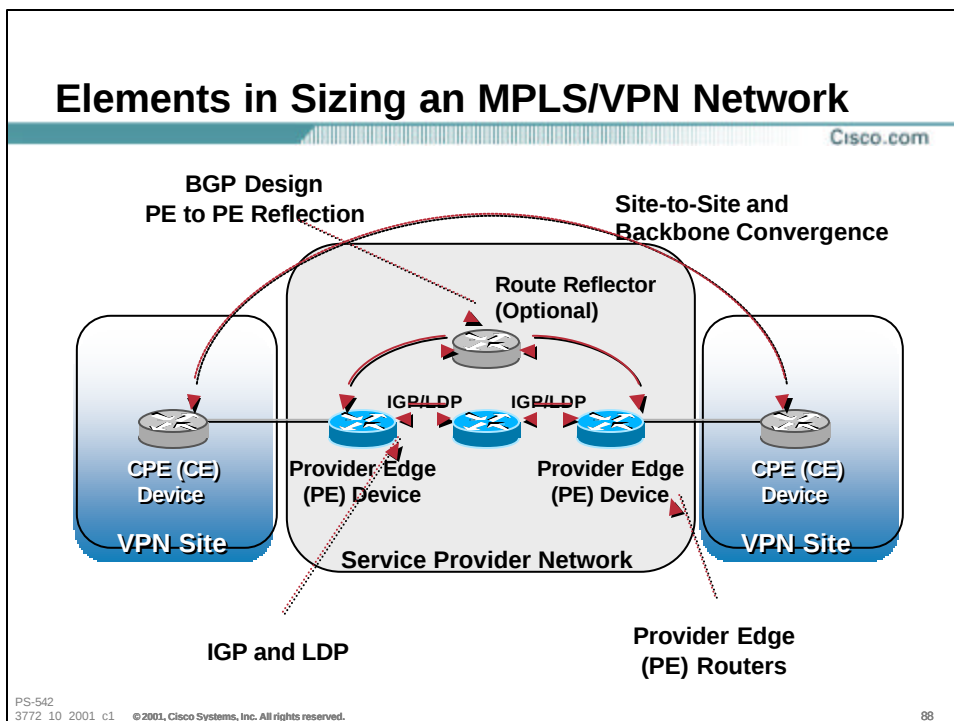
Cisco.com

MPLS VPN

Scalability Elements

PS-542
 3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

87



Elements in Sizing an MPLS/VPN Network

Cisco.com

- **Provider Edge (PE) routers**

How many do I need, how many can I have, what will affect these numbers, when should I add more?

- **Interior gateway and label distribution protocols**

How do they interact, how large can they grow, what factors will increase the network deployment size?

- **iBGP**

How many sessions can I have, do I need RRs, Should I confederate?

- **Convergence**

How quickly can I detect failure, how quickly can I detect new routes?

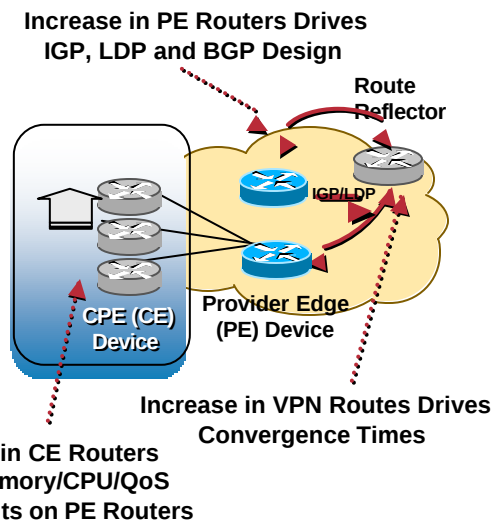
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

89

Elements in Sizing an MPLS/VPN Network

Cisco.com

- CPU, memory, and QoS requirements drives number of PEs
- Number of PEs helps determine IGP and BGP design



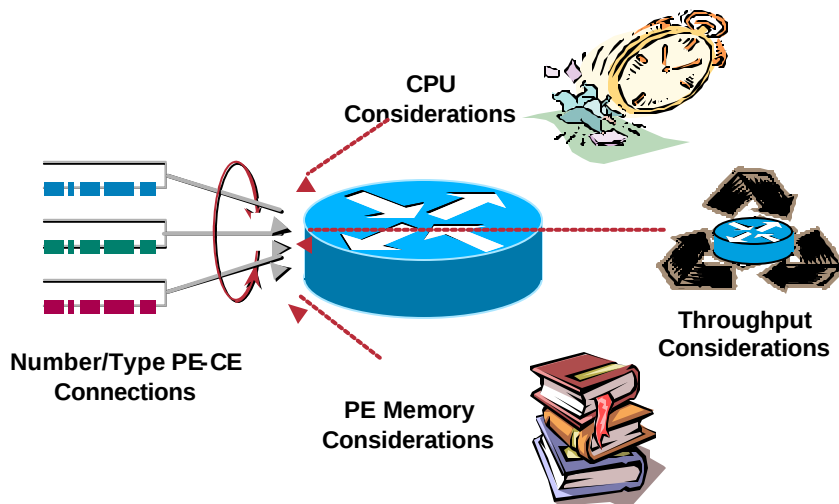
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

90

MPLS VPN

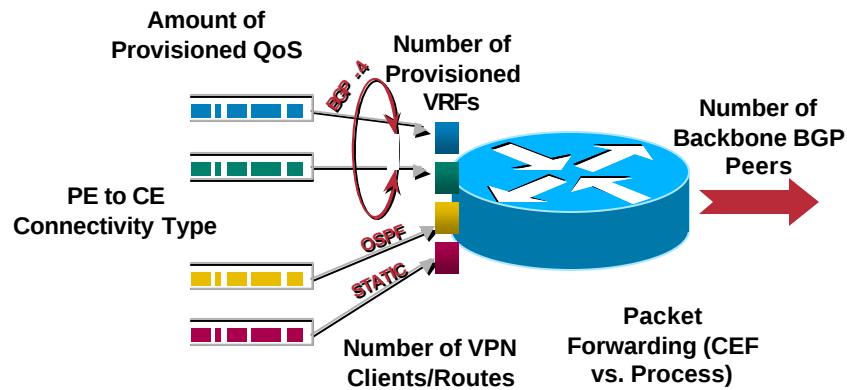
Sizing Provider Edge (PE) Routers

Sizing Provider Edge (PE) Routers



Sizing Provider Edge (PE) CPU Considerations

Cisco.com



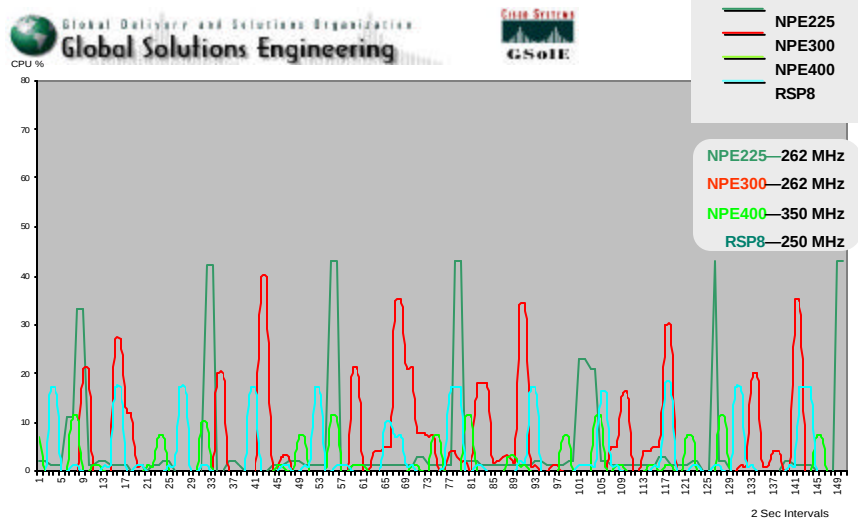
Several Factors Determine CPU Usage

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

93

Baseline CPU Comparison

Cisco.com

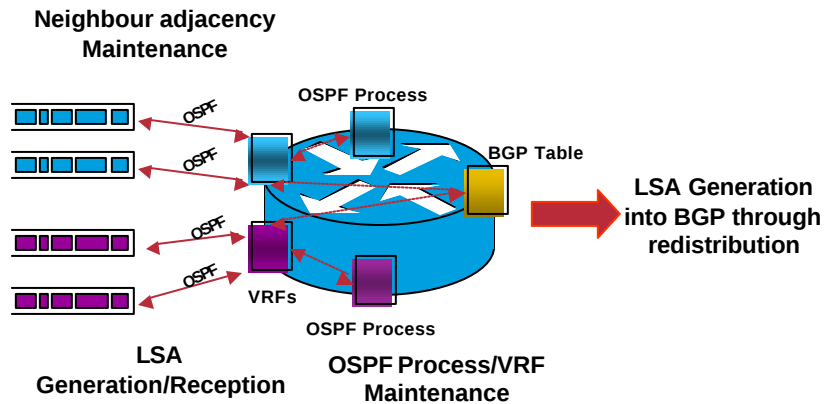


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

94

Sizing Provider Edge (PE) OSPF Considerations

Cisco.com

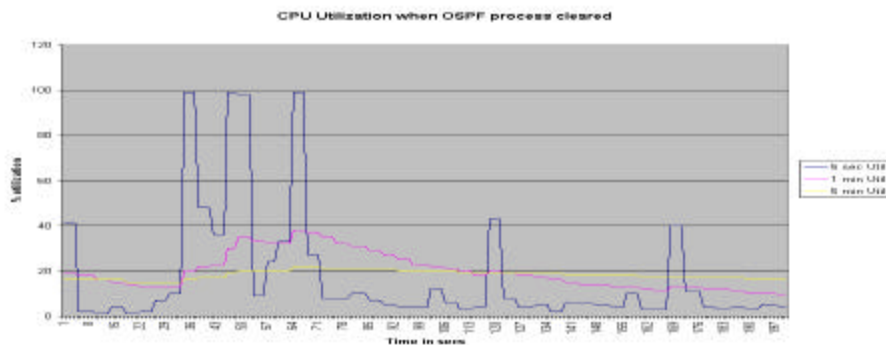


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

95

CPU Usage with OSPF

Cisco.com



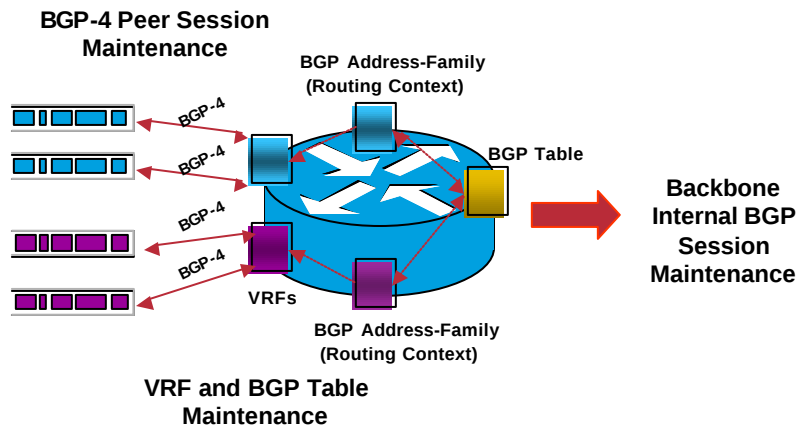
	Number of Routes Per VRF	Total Number of Routes
OSPF Processes 1 – 11	2000	22,000
OSPF Processes 12 – 23	5000	60,000
OSPF Processes 24 – 28	2000	10,000
TOTAL		92,000 VPN routes

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

96

Sizing Provider Edge (PE) BGP-4 Considerations

Cisco.com

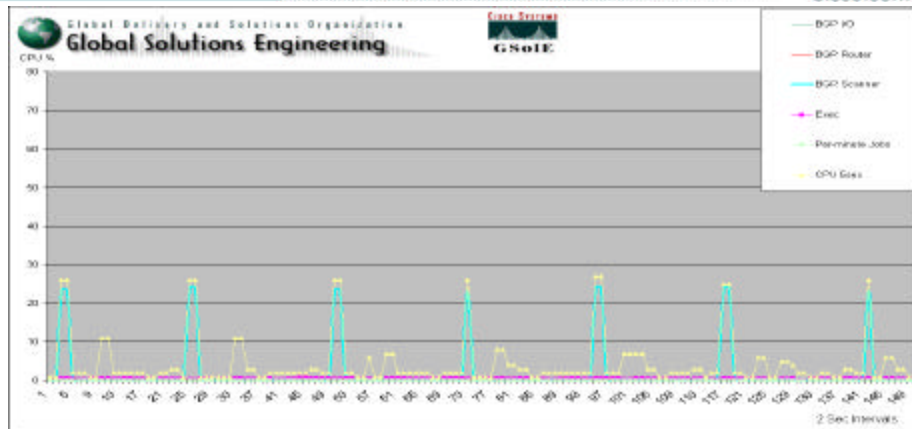


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

97

CPU Usage with BGP-4

Cisco.com



	Number of Routes Per VRF	Total Number of Routes
BGP Routing Context 1 - 499	500	250,000
TOTAL		250,000 VPN routes

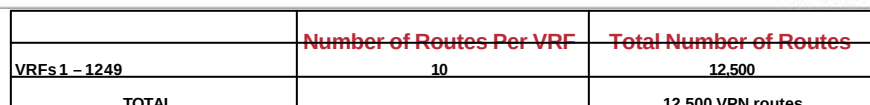
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

98

Cisco.com

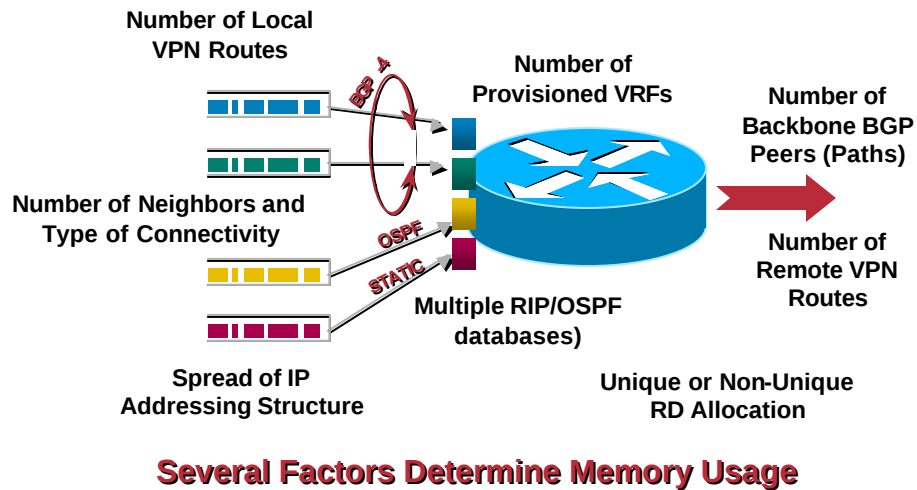


Cisco.com



Sizing Provider Edge (PE) Memory Considerations

Cisco.com

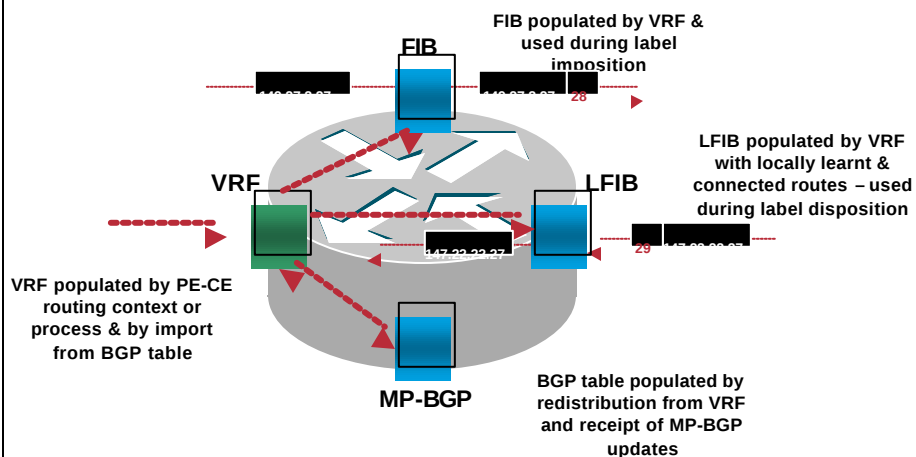


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

101

Sizing Provider Edge (PE) Table Population

Cisco.com

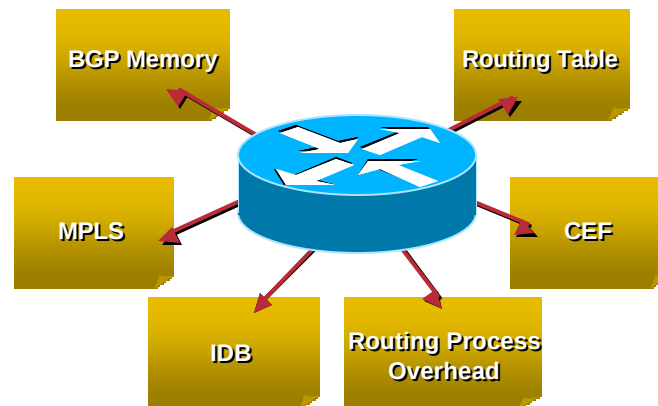


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

102

Sizing Provider Edge (PE) Memory Considerations

Cisco.com



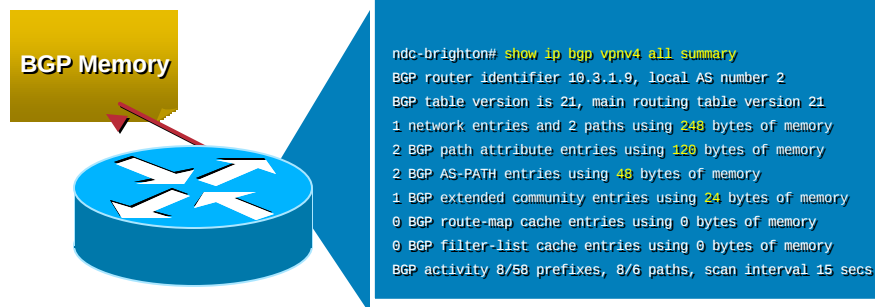
Several Areas of Memory Usage

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

103

Sizing Provider Edge (PE) BGP Memory

Cisco.com



$$Mp = (N*128) + (Np*60) + (P*60) + (Pa * 24) + (Ec * 24)$$

Mp = Total memory used for BGP table by PE in Bytes

N = Number of BGP network entries

Np = Number of BGP path entries

P = Number of path attribute entries

Pa = Number of AS_PATH entries

Ec = Number of Extended Community entries

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

104

Sizing Provider Edge (PE) Routing Table Memory

Cisco.com

Routing Table Memory



```
ndc-brighton# show memory summary | include IP: Control Block
0x60567BB0      33184      101      3351584      IP: Control Block

ndc-brighton# show ip route vrf testing summary
IP routing table name is testing(1)
Source      Networks      Subnets      Overhead      Memory (bytes)
connected   0              1              64             144
  External: 0 Internal: 0 Local: 0
internal    1              1              64             1164
Total       1              1              64             130
```

Each VRF Consumes :

1 IP control block -> 33,184 Bytes

1 Network Descriptor Block (NDB) Per Route (64 Bytes)

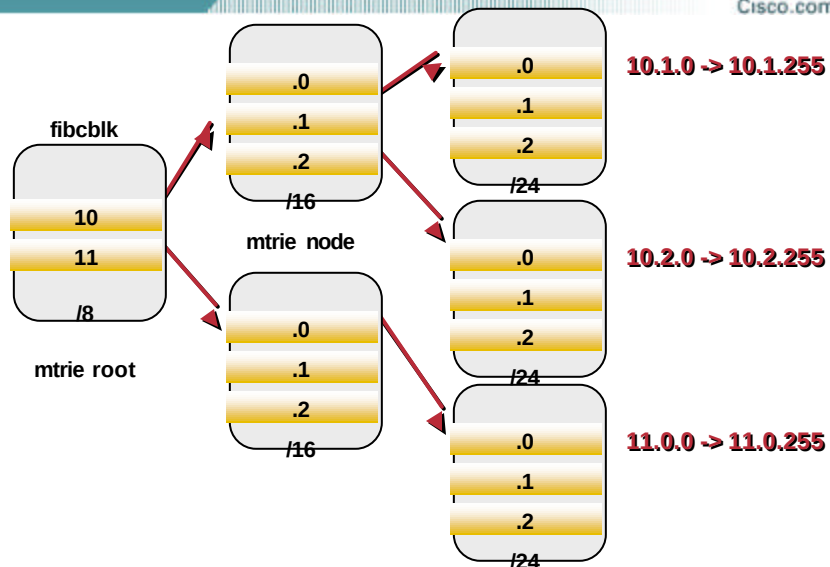
1 Routing Descriptor Block (RDB) Per Path (144 Bytes)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

105

Sizing Provider Edge (PE) CEF Memory

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

106

Sizing Provider Edge (PE) CEF Memory

Cisco.com

It Is Difficult to Predict Exactly How Much Memory Will Be Consumed by the FIB As It Depends on How Scattered the Prefix Information Is

Example: Calculation for **10.1/16, 10.2/16, 10.1.1/24 and 11.1/16.**

DECISION FLOW

1k for the Root (First Byte)
 1k More If the Route Is a /16 (and No Other Route Shares the Same First Byte)
 1k More for a /24 (If No Other Route Shares the First Two Bytes)
 1k More If > /24

CALCULATION

1k Root Plus 10.1/16, 10.2/16: 1k for 2nd Level Entry for 10
 10.1.1/24: 1k for 3rd Level Entry 10.1
 11.1/16: 1k for 2nd Level Entry for 11

Total of Approximately 4k for These Routes

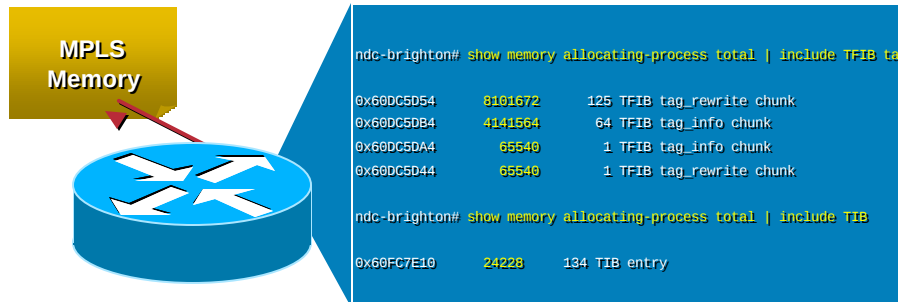
PS-542

3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

107

Sizing Provider Edge (PE) MPLS Memory

Cisco.com



MPLS Forwarding Memory (LFIB) consumes one 'taginfo' (64 Bytes) per route, plus one Forwarding Entry (104 Bytes) for each path

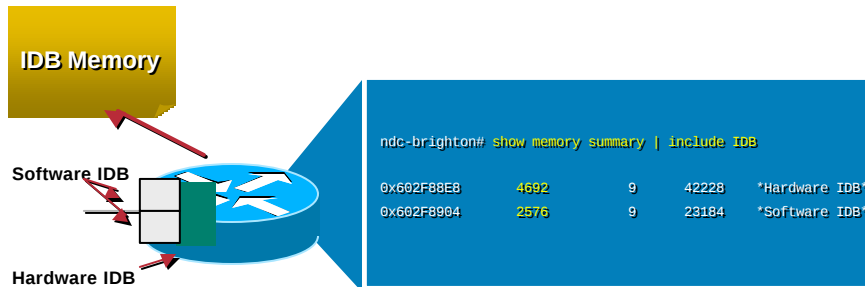
PS-542

3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

108

Sizing Provider Edge (PE) IDB Memory

Cisco.com



Interface Description Block

Hardware IDB: 4692 Bytes (One Per Physical Interface)

Software IDB: 2576 Bytes (One Per Interface and Per Sub-Interface)

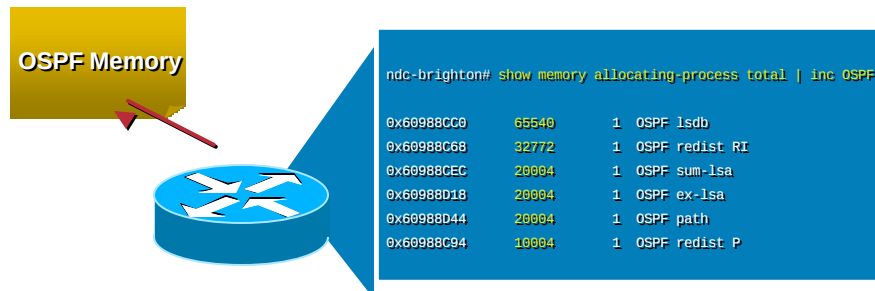
Note: The amount of memory required will differ from platform to platform

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

109

Sizing Provider Edge (PE) OSPF Protocol Memory

Cisco.com



OSPF Protocol Memory

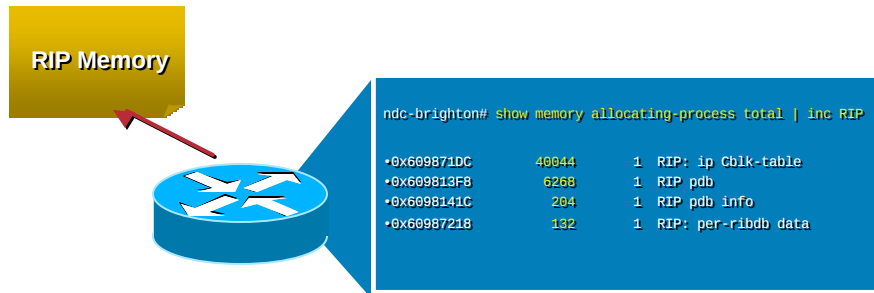
~ 168K per process (additional memory requirements for database population)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

110

Sizing Provider Edge (PE) RIP Protocol Memory

Cisco.com



RIP Protocol Memory

~ 47K for the RIP process plus ~250 bytes per ndb/rdb combination and
~400 bytes per routing context (address-family)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

111

MPLS VPN

Memory Sizing Design Guidelines

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

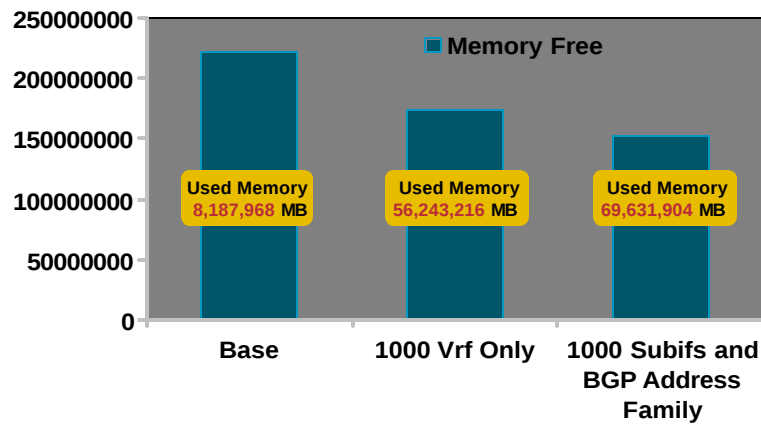
112

PE VRF Memory Sizing

No VPN Routes

Cisco.com

Base Memory Free



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

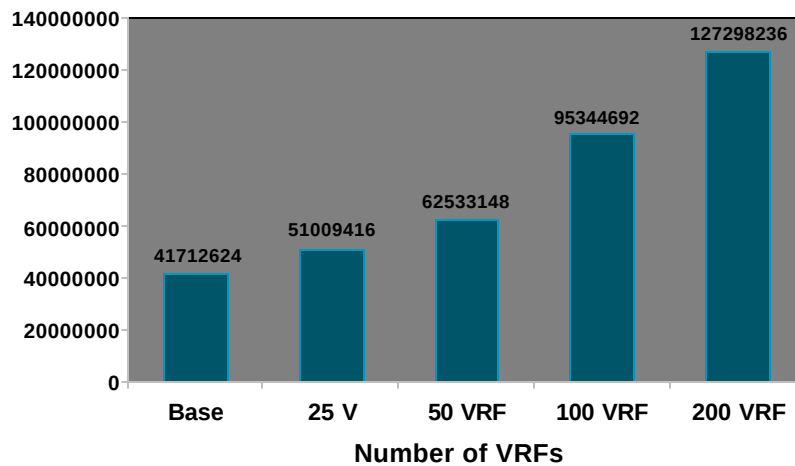
113

VPN Memory Comparison

Cisco.com

Memory Used

Memory Comparison (12.1(5)T)
500 Routes Per VRF, 2 iBGP Paths



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

114

PE Memory Sizing Design Rules

Cisco.com

- ~60–70K per VRF
32K for base VRF control block, other memory such as CEF, TFIB overhead, IDBs and so on
- ~800–900 bytes per route
(Includes CEF, TFIB, and RIB memory in BGP)
- Remember Cisco IOS® uses memory
- Remember Routing Protocol memory
- Remember Internet routes!
- Remember to leave transient memory
Recommended to leave ~20MB free

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

115

PE Memory Sizing Design Observations

Cisco.com

- 128 Mb platforms are limited
(NPE 225, 3640 may **NOT** be suitable for full Internet table and VPNs!!!)
- 256 Mb minimum recommended on PE devices (if possible)
- Limit the number of Route Distinguishers per VRF in the same VPN
Unless you require iBGP load balancing with RRs

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

116

VRF and Route Limits Summary

Cisco.com

- VRF limits

- Constrained mainly by CPU

- Between 500 and 1000 VRFs for static routing (depending on platform—10 routes per VRF)

- Between 250 and 500 VRFs if using EBGp or RIPv2 (depending on platform—500 routes per VRF)

- VPN and global route limits

- Constrained mainly by available memory

- With 256 Mb, 200,000 routes total (IPv4 and VPNv4)

- If Internet table is present, this reduces the memory available for VPNs (current calculations are near 65 Mb for 100K Internet routes—with tightly packed attributes)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

117

MPLS VPN

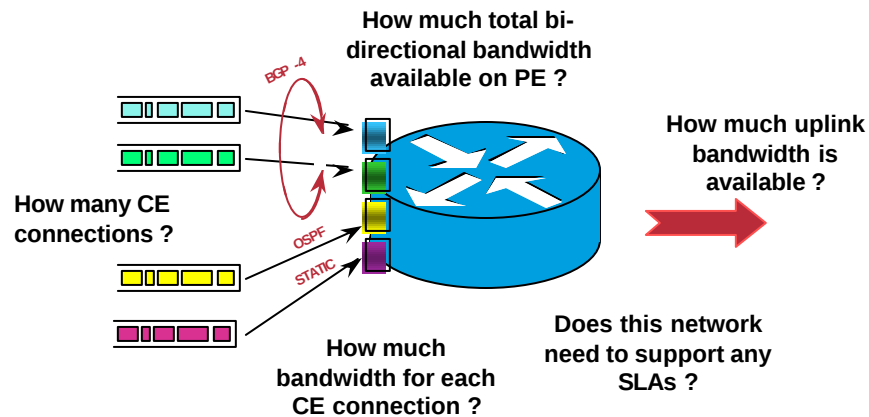
PE Router Throughput Considerations

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

118

PE Router Throughput Considerations

Cisco.com



Several Factors Determine PE Router Throughput

PS-542

3772_10_2001_c1

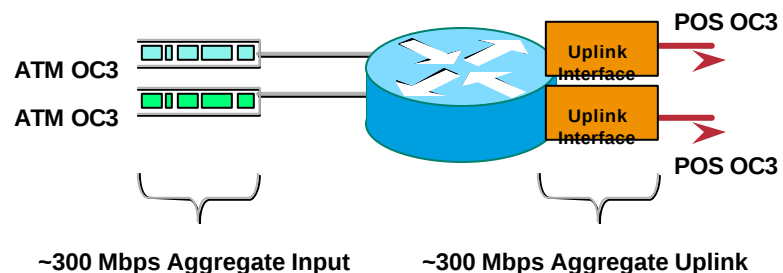
© 2001, Cisco Systems, Inc. All rights reserved.

119

Basic Throughput Analysis: 7200VXR

Cisco.com

- We know 7200 VXR is capable of 300 Megabits bi-directional throughput
- With 2 OC-3 uplinks in use, that leaves us with ~290 Mbps ($600 - (2 * OC-3)$) left for CE connections (assuming no I/O FE)
- Average CE connection speeds can be computed by taking $290 \text{ Mbps} / \# \text{ CE connections}$



PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

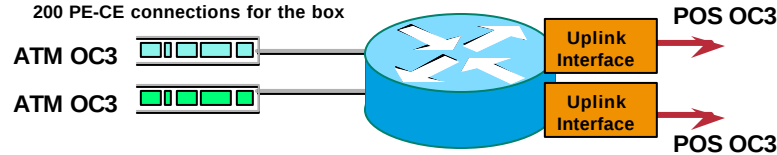
120

Basic Throughput Analysis: 7200VXR

Cisco.com

- Typically, there will be several customers with differing bandwidth requirements
- In this example, on average, this works out to 100 CE connections across ATM OC-3 interface at T1 rates

~100 customers per ATM interface -> total
200 PE-CE connections for the box



Conclusions: Easily within the VRF limits. The same throughput analysis can be repeated for sizing any platform

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

121

Considerations when designing for Quality of Service

Cisco.com

- Failure of an uplink may cause bus congestion or over-subscription of the backup uplink interface
Non-distributed load balancing may also provide a variance in uplink bandwidth usage
- SLA requirements (gold/silver/bronze classes of service) obviate the need for Qos
- Applying Qos on the PE addresses SLA requirements, but may limit the overall throughput, *depending on the features and platforms configured*

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

122

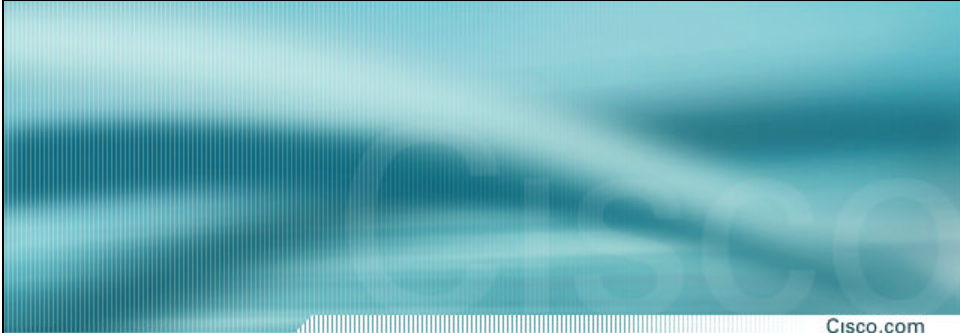
Considerations when designing for Quality of Service

Cisco.com

- Performance testing of customer specific Qos feature sets is highly desirable!
- Can the Qos function be pushed to the CE router ?
Such as CAR marking & traffic shaping
- Remember that in general Qos “kicks in” only when there is congestion present
CBWFQ for scheduling on uplinks

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

123



Internal and External Routing Protocol Sizing

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

124

IGP Scaling Evolution

Cisco.com

Flat Topology

- Link flaps are topology wide
- Full SPF (OSPF), partial IS-IS (if only prefix/metric change—PE loop back will ALWAYS be full SPF!)
- Good for TE—Good if stable links

Area Topology

- Link flaps restricted to area
- Change in type-3 (or type-5) -> partial SPF for all type-3's which announce the prefix
- Requires area filtering (OSPF) or route leaking (IS-IS) for /32 loop backs
- More complex for TE

Confederated AS

- Different IGP per sub-region
- PE addresses restricted to sub-region
- Next-hop re-written at sub-region boundary

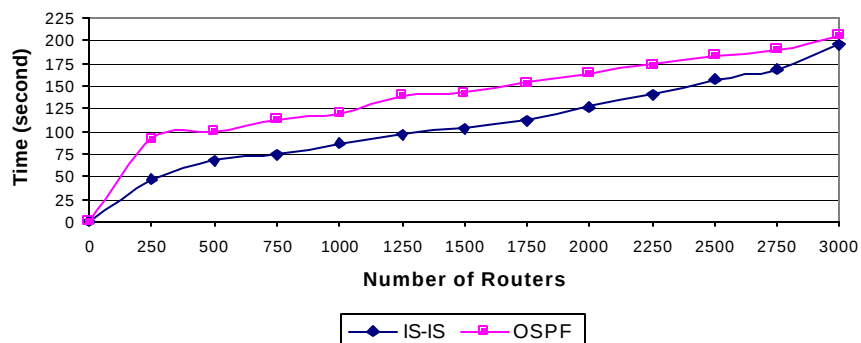
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

125

OSPF Vs. IS-IS Convergence

Cisco.com

Average Network Convergence for IS-IS & OSPF



**Convergence Time = First Adjacency to
Last SPF Execution**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

126

IGP Scalability Task

Cisco.com

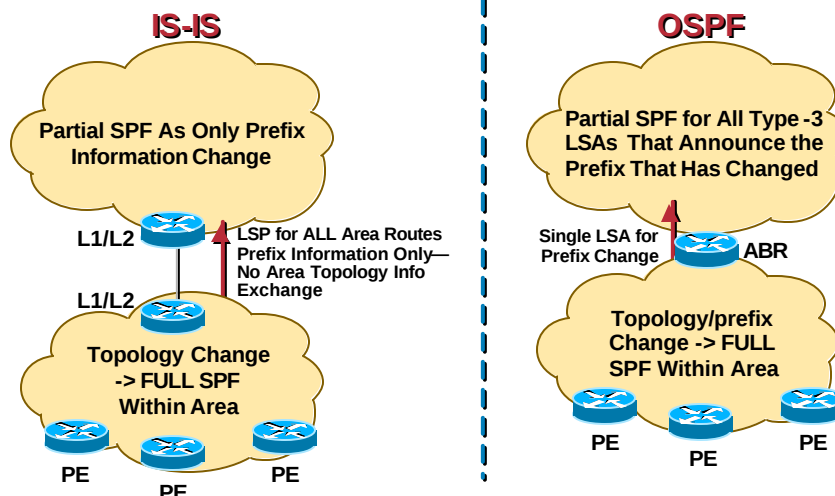
- **Convergence is not the ONLY consideration**
Flooding, CPU usage, link flapping and so on
- **Task: Design an IGP backbone to support one million VPN sites**
- **Quick math:**
2000 PE devices * 500 VRF forwarding interfaces
This breaks the (theoretical) IGP rules for number of routers in a single area
Assumes multiple areas or even confederations

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

127

Area Topology Considerations

Cisco.com



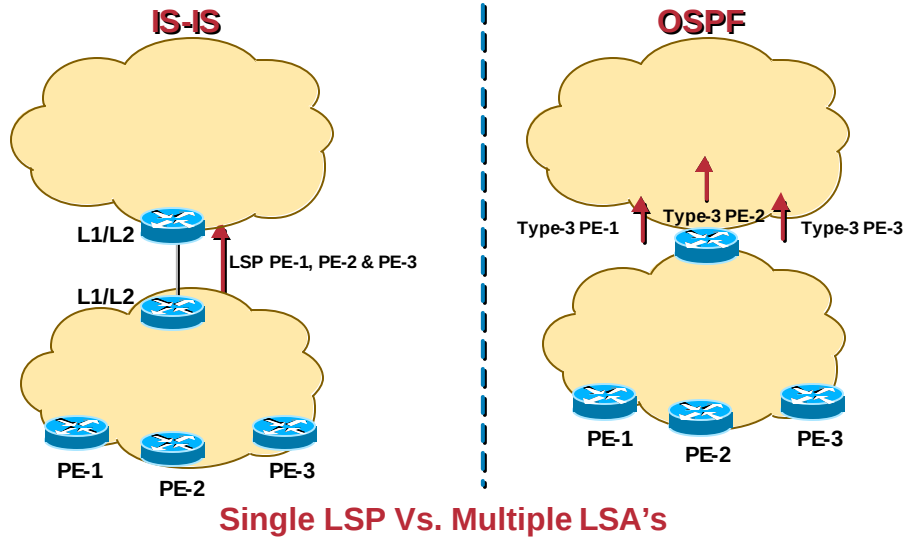
Area Topology Provides Separation and Stability

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

128

Area Topology Considerations

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

129

Sizing the IGP Area Topology

Cisco.com

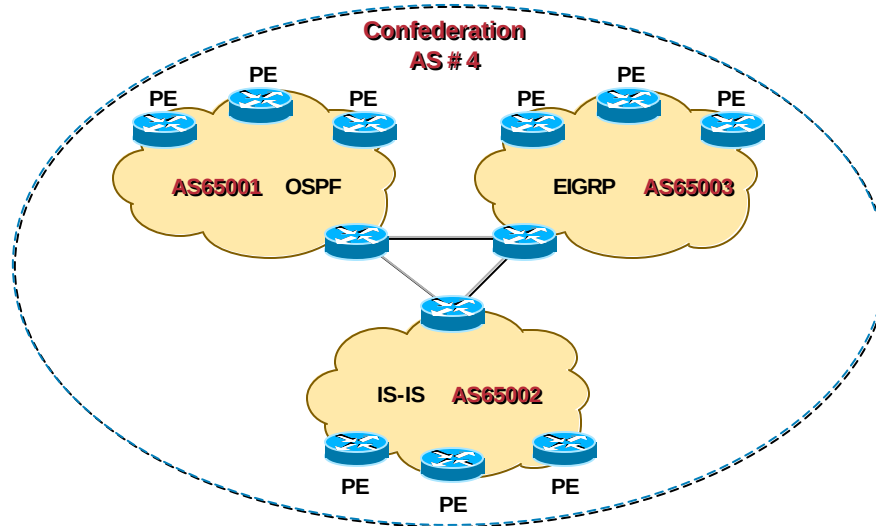
- **Backbone area sizing issues**
 - Number of routers
 - Number of links and topology
 - Leaking of PE loop back addresses
 - Large MPLS networks = lots of PEs potentially!
- **Maximum allocated labels**
 - Defaults to 100K labels—including IGP and VPN
 - Can be changed 'mpls label range' command

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

130

IGP Scaling Using Confederations

Cisco.com

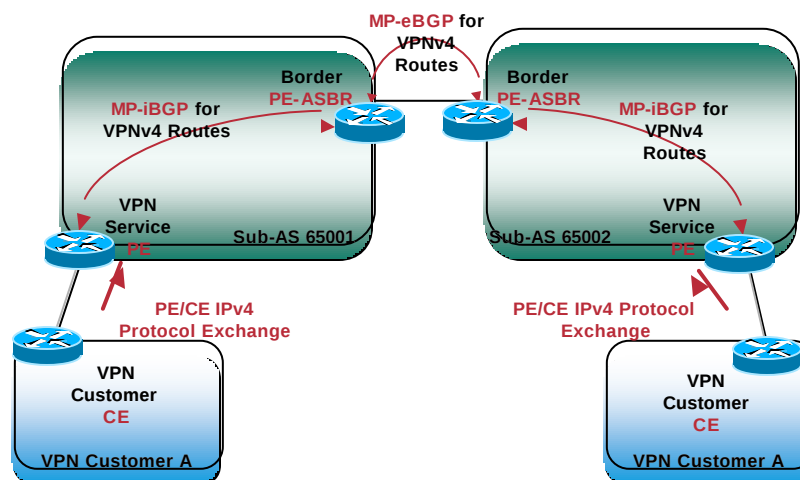


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

131

Confederated MPLS VPN Operation

Cisco.com

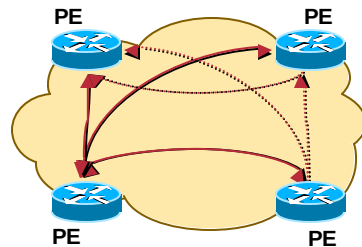


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

132

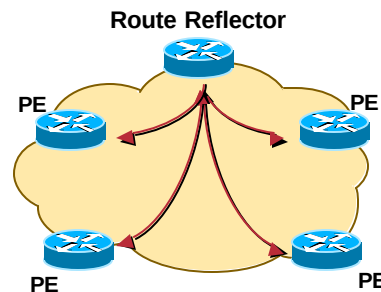
MP-BGP Deployment Requirements

Cisco.com



- **Remember—PE only needs routes for attached VPNs**
- No full mesh requirement—one session to each route reflector
- Could partition to break up the topology and reduce processing overhead on PE routers

- Full iBGP mesh requirement between PEs that require same VPN information
- Could partition to break up the mesh—**mini iBGP cluster**



MP-BGP Used to Distribute VPN Prefix Information

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

133

Peer-Group Concepts for RR Clients

Cisco.com

- Same set of updates sent to group of neighbors using peer-group concept
- Results in lower CPU and I/O memory consumption
- Dramatic improvement observed in convergence using peer-group over non-peer group
- 250K prefixes with 500K paths—100 core and 32 PE clients

With peer-group -> 12 minutes, 29 seconds

Without peer-group -> 56 minutes, 6 seconds

Use Redundant Route Reflectors WITH Peer-Groups

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

134

RR Tuning and Recommendations

Cisco.com

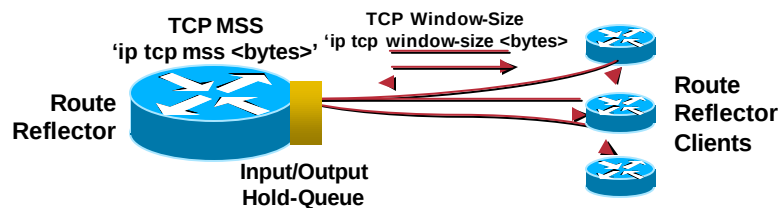
- **Keep RRs separate for IPv4 and VPNv4**
 - Better stability, faster convergence
 - Meets SLA requirements (with high number of routes)
- **Use route reflector server model**
 - Dedicated for RR function—not in forwarding path
 - Conserve CPU and memory for faster convergence
- **Recommended RR for VPN is NPE-400**
 - Highest CPU power
 - Availability of large DRAM memory—512 MB

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

1355

RR Tuning and Recommendations

Cisco.com



- **On RR, increase input hold-queue and window-size**
 - $\text{Window size}/(\text{MSS}) * \text{number of peers} = \text{hold-queue size}$
 - hold-queue <packets> in
 - ip tcp window-size <bytes>
 - Prevent input drops -> decrease convergence times
- **Use ip tcp path-mtu-discovery**
 - The packet rate will drop substantially;
 - default MSS size is 536 bytes

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

136

RR Core Design Option 1

Cisco.com

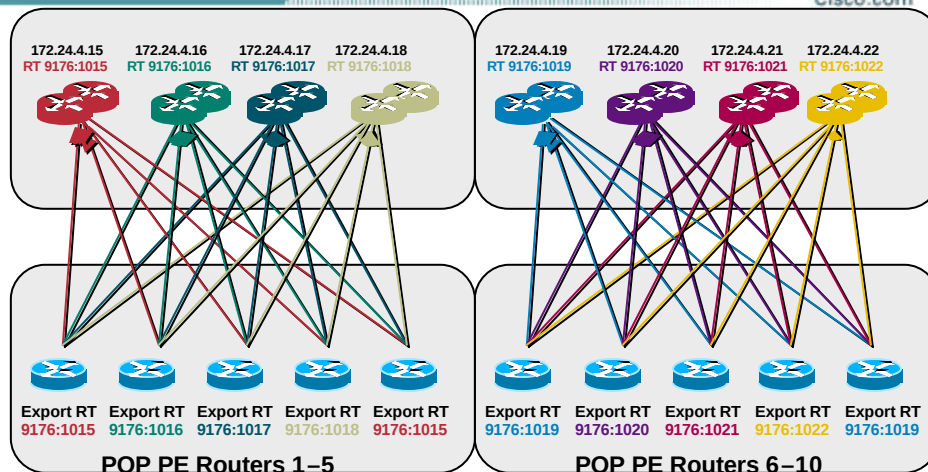
- Scale for 250 thousand VPN sites
- 500 VRF interfaces per PE device
500 PE routers in total
- 50 POP topology
10 PE routers per POP
- Centralized route reflection topology
Split PE routers into groups and use specific route reflector RT values

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

137

RR-Group Route Reflector Partitioning

Cisco.com



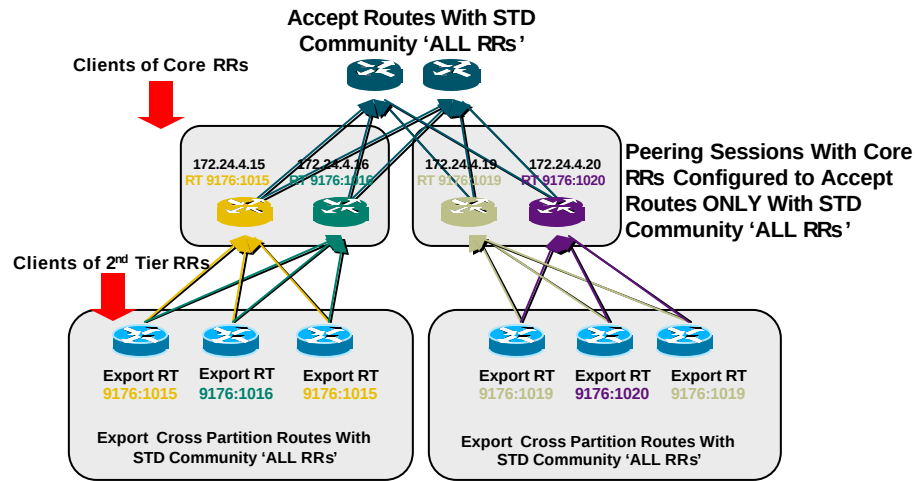
RR-Group Based on Route Reflector RT Value

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

138

RR-Group Route Reflector Partitioning

Cisco.com



Cross Partition Pollination Via 2nd Tier RRs

PS-542

3772_10_2001_c1

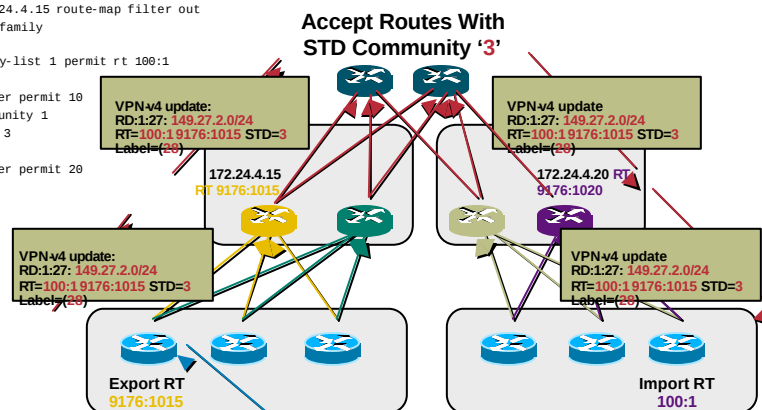
© 2001, Cisco Systems, Inc. All rights reserved.

139

RR-Group Route Reflector Partitioning

Cisco.com

```
address-family vpnv4
  neighbor 172.24.4.15 activate
  neighbor 172.24.4.15 send-community both
  neighbor 172.24.4.15 route-map filter out
  exit-address-family
!
ip extcommunity-list 1 permit rt 100:1
!
route-map filter permit 10
  match extcommunity 1
  set community 3
!
route-map filter permit 20
```



'Clear ip bgp 172.24.4.15 vpnv4 unicast out'

PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

140

RR Core Design Option 2

Cisco.com

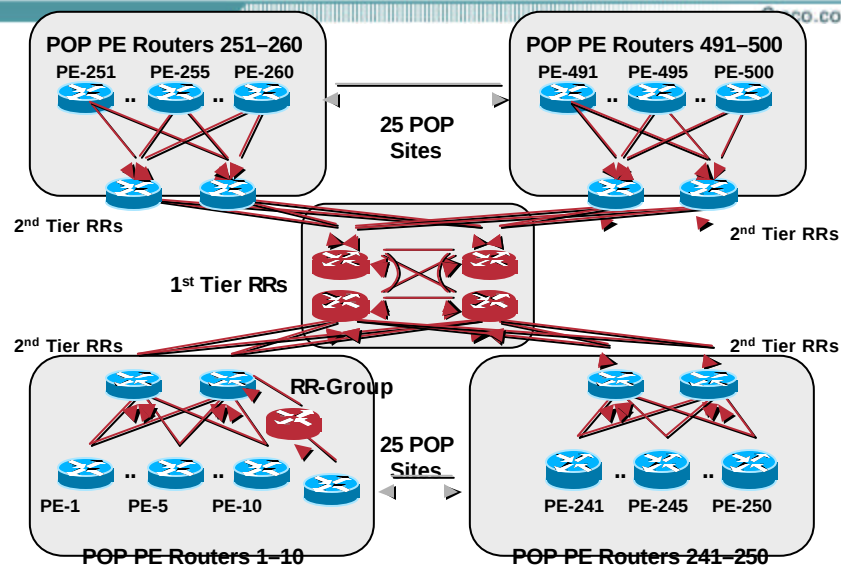
- Scale for 250 thousand VPN sites
- 500 VRF interfaces per PE device
500 PE routers in total
- 50 POP topology
10 PE routers per POP
- Distributed route reflection topology
‘All knowing’ distributed route reflectors
Core RRs fully meshed—PE clients

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

141

Distributed Route Reflection

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

142



Cisco.com

MPLS VPN Convergence Tuning

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 143

Routing Convergence

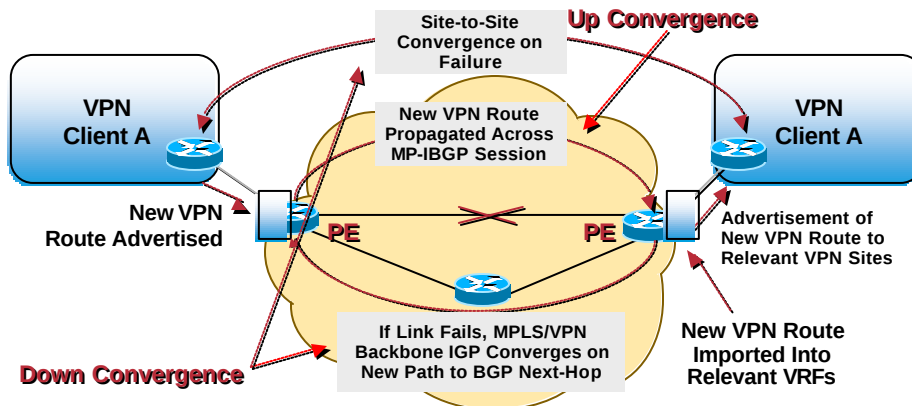
Cisco.com

- **Convergence needs to be assessed in two main areas**
 - Convergence within the MPLS/VPN backbone
 - Convergence between VPN client sites
- **And with two separate scenarios...**
 - Convergence on platform/network failure—**'down convergence'**
 - Convergence on new routing information—**'up convergence'**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 144

End-to-End Routing Convergence

Cisco.com



Site-to-Site and MPLS/VPN Backbone IGP Convergence Are Independent

PS-542

3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

145

Convergence across Backbone

Cisco.com

- **Convergence of MPLS/VPN backbone IGP will not affect client-to-client route convergence**
Unless BGP next-hop becomes unavailable;
but will affect client-to-client traffic while backbone converges
- **Backbone may be router-only based or based on ATM switches**
Convergence will be different for the MPLS forwarding plane—cell-mode or frame-mode implementation?

PS-542

3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

146

Convergence—Router-Based Backbone

Cisco.com

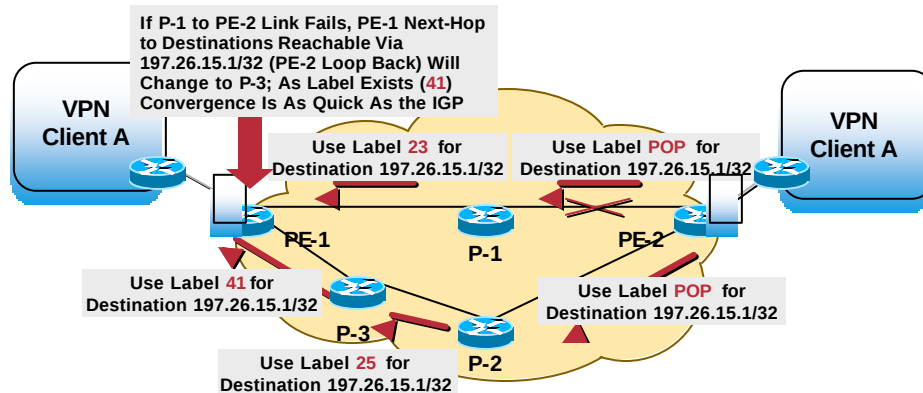
- **Unsolicited downstream**
Bindings advertised as soon as route within the routing table
- **Liberal label retention**
If multiple neighbors, next-hop change causes new label to be used for forwarding
- **Immediate notification of routing table change**
Whenever a route changes (addition/deletion) MPLS process informed immediately

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

147

Convergence—Router Based Backbone

Cisco.com



MPLS and IGP Backbone Convergence Equivalent

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

148

Convergence—ATM Backbone

Cisco.com

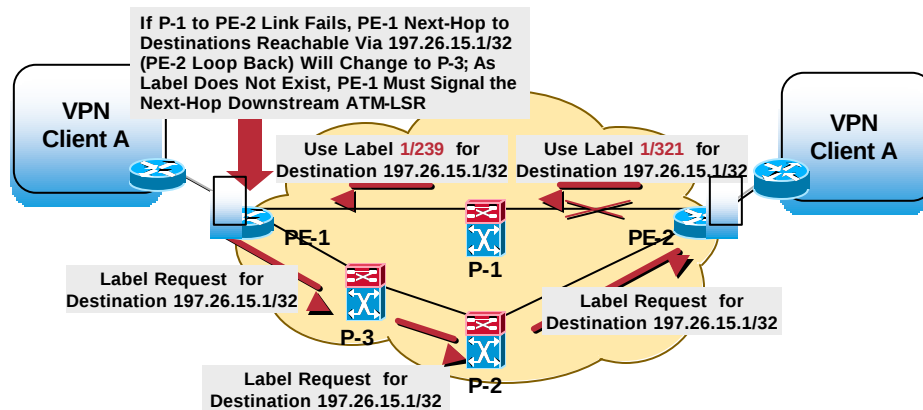
- **Downstream-on-demand**
Convergence affecting, as LSR must signal for downstream label binding
- **Conservative label retention**
Convergence affecting, as LSR must signal for downstream label binding if one does not exist
Next-hop change will cause label request
- **Two stage convergence:**
IGP: Converge around topology changes
MPLS: Re-establish label mappings

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

149

Convergence—ATM-Based Backbone

Cisco.com



MPLS LSR Must Re-Converge on IGP Change AND Re-Signal for Label Mapping to Downstream Next-Hop

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

150

Site-to-Site Convergence

Cisco.com

- Four main convergence areas

Advertisement of routes from CE to PE and placement into VRF (**T1** and **T2**)

Propagation of routes across the MPLS/VPN backbone (**T3** and **T4**)

Import process of these routes into relevant VRFs (**T5**)

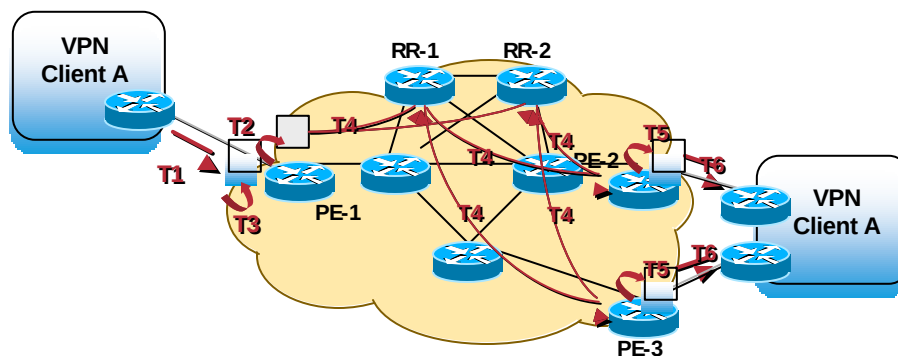
Advertisement of VRF routes to attached VPN sites (**T6**)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

151

Site-to-Site Convergence

Cisco.com



Site-to-Site Convergence Points

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

152

Backbone Route Propagation

Cisco.com

- Change are not propagated to other BGP speakers immediately

Batched together and sent at **advertisement-interval**

Default is every 5 seconds for iBGP, 30 for eBGP

- Can be tweaked using the **neighbor advertisement-interval** command

Needs to be changed for both backbone and CE routers if BGP between PE and CE

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

153

Scanner Process

Cisco.com

- **Scanner** process will also have an affect on convergence

Used to check next-hop reachability and to process any network commands within the BGP process

Invoked every 60 seconds by default for IPv4 and VPNv4 prefixes

Can be tuned with **BGP scan-time** command

Large BGP table and small scan-time can be **very** CPU intensive—beware!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

154

Import Process

Cisco.com

- Import process uses a separate invocation of the scanner process
 - Every 15 seconds by default
 - Can be tuned using the **BGP scan-time import** command
- Could take up to 15 seconds for a route to be placed into a receiving VRF
 - And then potentially a further 30 seconds to be advertised to CE if eBGP is in operation!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

155

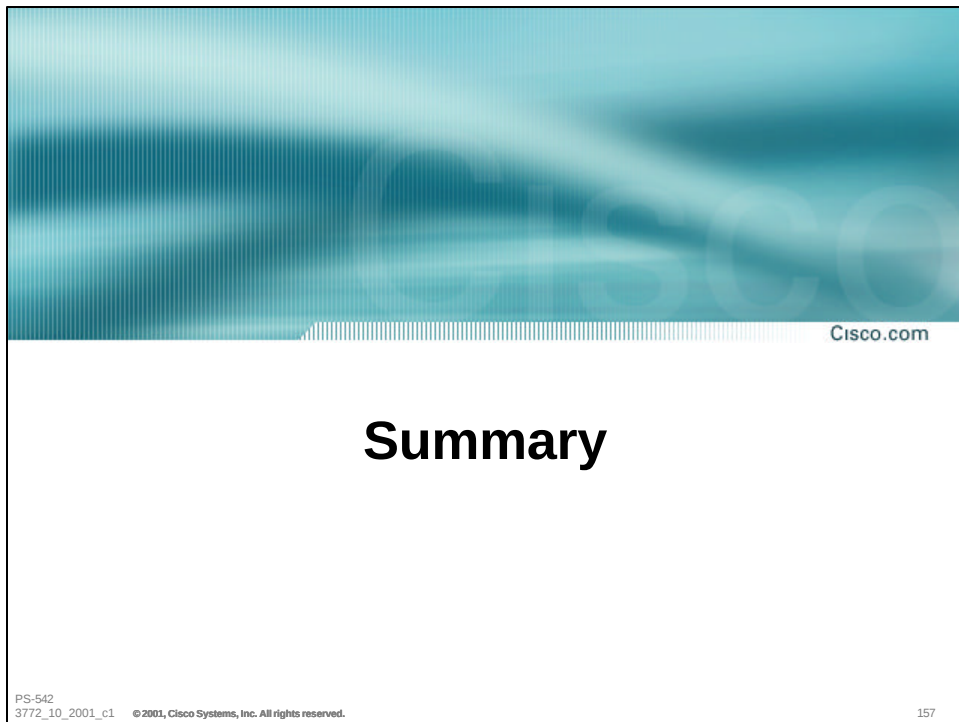
Site-to-Site Theoretical Maximum UP Convergence

Cisco.com

	BGP-4	RIP V2	OSPF
T1_max	30 (Default Adv Int)	30 (0 with Triggered)	Variable (Time for LSA Propagation)
T2_max	0	0	0
T3_max	0	0	0
T4_max	10 ((n+1) * Adv Int)	10 ((n+1) * Adv Int)	10 ((n+1) * Adv Int)
T5_max	0	0	0
T6_max	30 (Default Adv Int)	30 (0 with Triggered)	Variable (Time for LSA Propagation)
Total	~70 Seconds	~85 Seconds or ~25 Seconds (with Triggered)	~25 Seconds

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

156



Summary

Cisco.com

- **MPLS/VPN—best of both worlds**
Advantages of peer-to-peer and overlay models but without the previous scaling issues
- **Optimal routing between sites**
- **PE routes hold only relevant routing information**
- **No complex filters or dedicated routers**

But We Still Have to Scale This Architecture

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 158

Summary

Cisco.com

- **MPLS/VPN backbone scalability elements**
BGP, IGP/LDP, PE routers
- **PE router sizing**
QoS, memory, CPU
- **Border Gateway Protocol (BGP) sizing**
Route reflection design
TCP tuning
- **IGP/LDP sizing**
Flat or area topology

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

159

Operations Management for MPLS Networks and Services

Section 3

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

160

Generic Service Provider Management Functions

Cisco.com

Performance
Monitoring and
Assurance

Accounting
And Billing

Network
and Service
Provisioning

Network
Planning and
Engineering

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

161

Recent Viewpoint Change Importance of Management

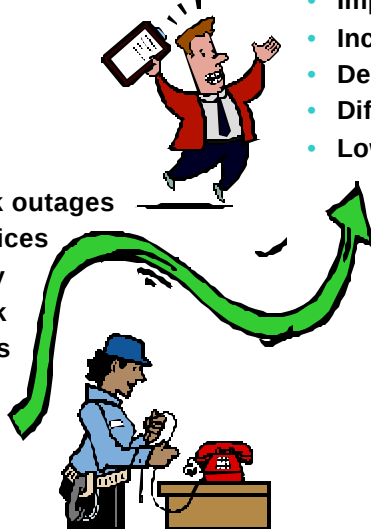
Cisco.com

- Repair network outages
- Provision services
- Track inventory
- Design network
- Bill for services

Utility

- Improve customer service
- Increase service profit
- Decrease time-to-revenue
- Differentiate product
- Lower ownership costs

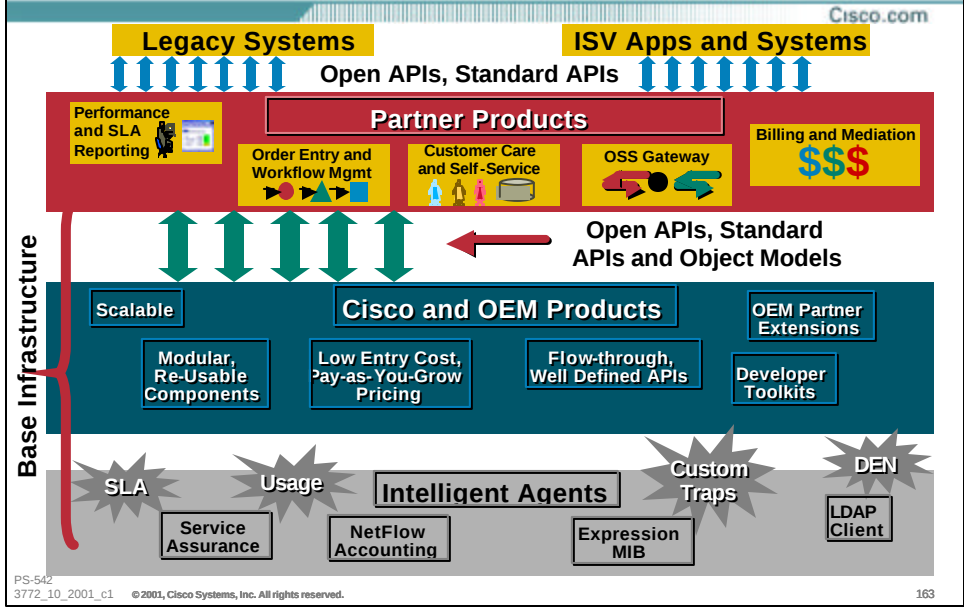
Strategic



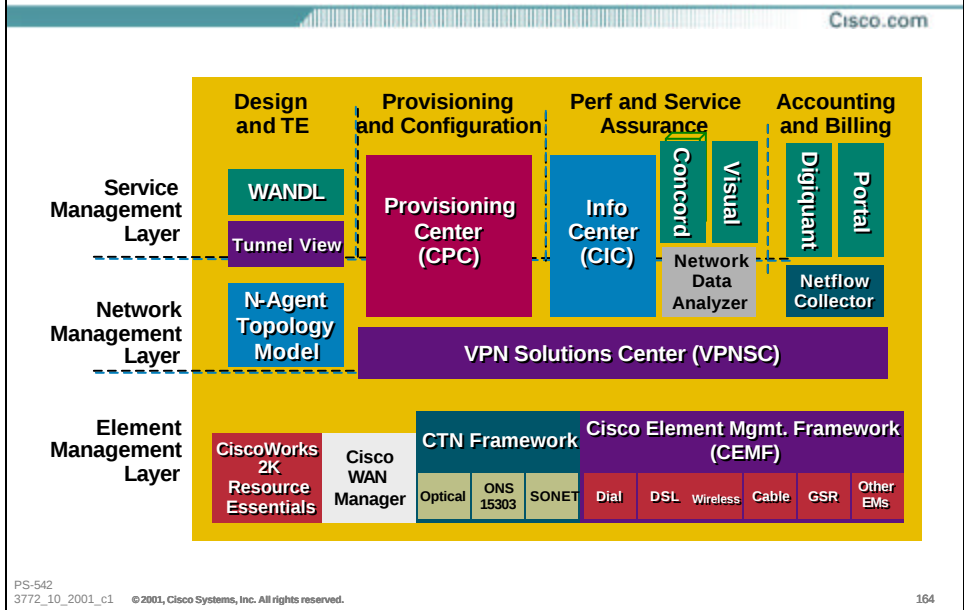
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

162

Cisco's Solution Toolbox

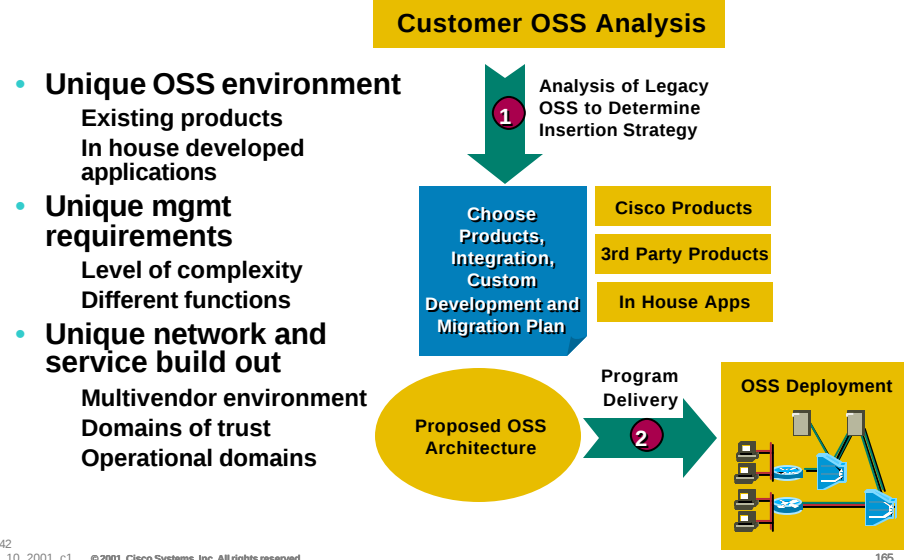


Cisco Service Management Products for MPLS Networks



Mgmt Solutions One Size Doesn't Fit All

Cisco.com



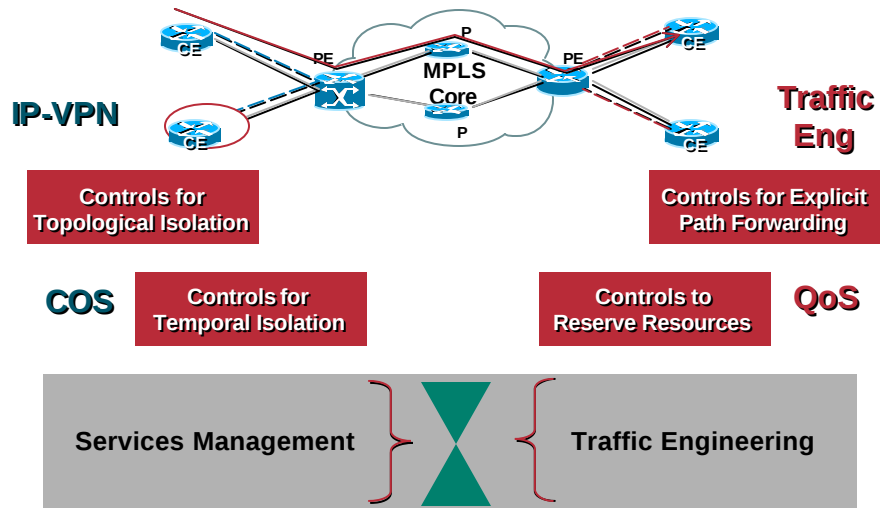
Agenda

Cisco.com

- **What Does MPLS Mean to Network Management?**
- **What Are the Specific Functions Required to Support MPLS Networks and Services?**
- **What Are the Technologies and Applications Needed for Each Function?**
- **How Does a Provider Bring These Tools Together Within the Larger Context of an Existing OSS/BSS?**

What Does MPLS Mean to Network and Operations Management?

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

167

IP VPN Service Provisioning

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

168

IP VPN Service Provisioning

Cisco.com

- Define VPN service and service attributes
- Determine changes required
- Activate service by implementing changes
- Perform tests to ensure delivery success
- Schedule and track service activation



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

169

Craft Provisioning

Cisco.com

- VPN services can be manually configured through CLI commands
- Home grown scripts also can be developed using telnet/tftp to routers
- Manual and script-based provisioning becomes quickly unmanageable automated provisioning tools

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

170

Benefits of Provisioning Tools

Cisco.com

- Deploy “first time right”
- Require fewer and less skilled workers
- Reduce inter-service dependency failures
- Faster delivery of new services
- Easier access to service inventory data

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

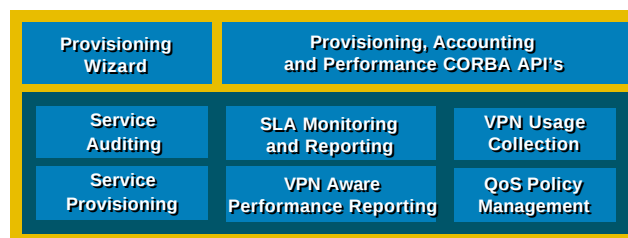
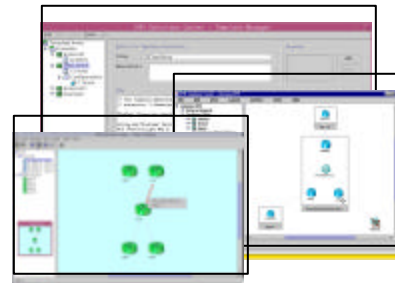
171

Baseline Tool for VPN Management: VPN Solution Center (VPNSC)

Cisco.com

- Cisco's service mgmt platform for IP VPN services

Managed MPLS VPN
Managed IPsec VPN
Access VPN
IPSec to MPLS VPN

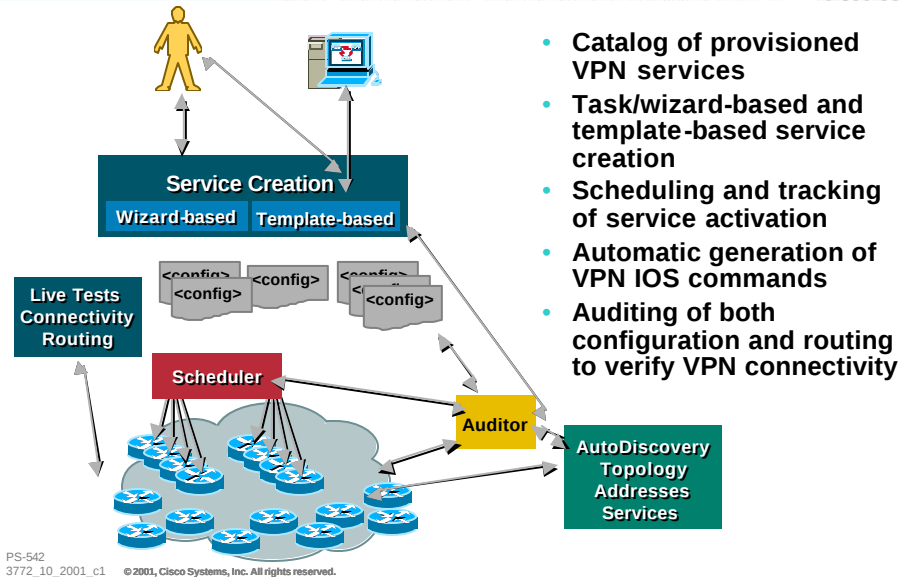


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

172

VPNSC Provisioning

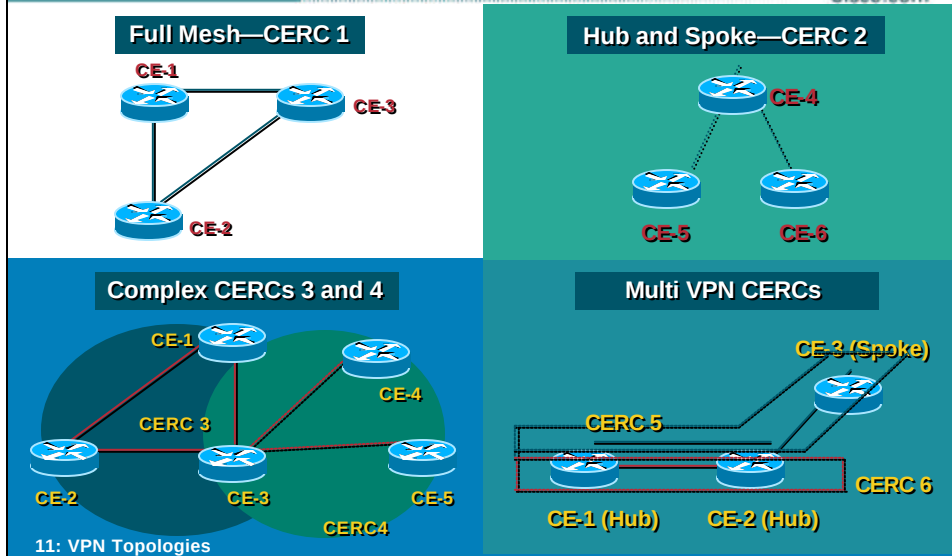
Cisco.com



173

MPLS/VPN Topology Building Blocks CE Routing Communities

Cisco.com



174

Provisioning of Service Redundancy

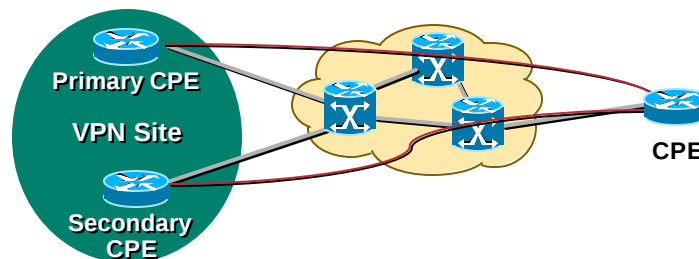
Cisco.com

- **Redundancy support**

Provision a secondary redundant device in a VPN site

The secondary CPE may use a floating static route for fail over to other VPN peers

The dual homed connection for the secondary CPE may be used to load balance to the VPN site

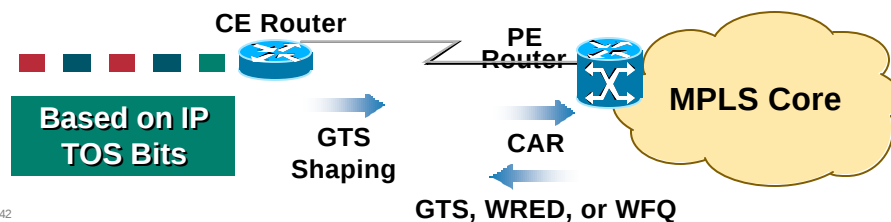
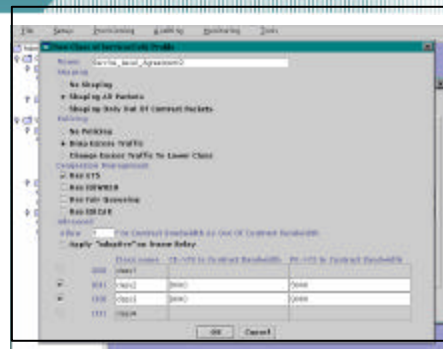


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

175

CoS Provisioning

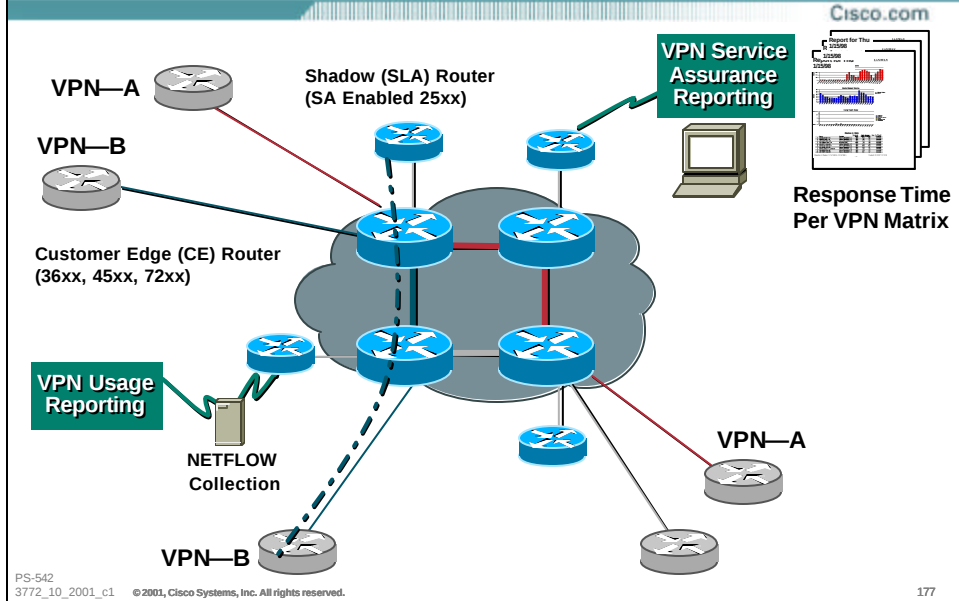
Cisco.com



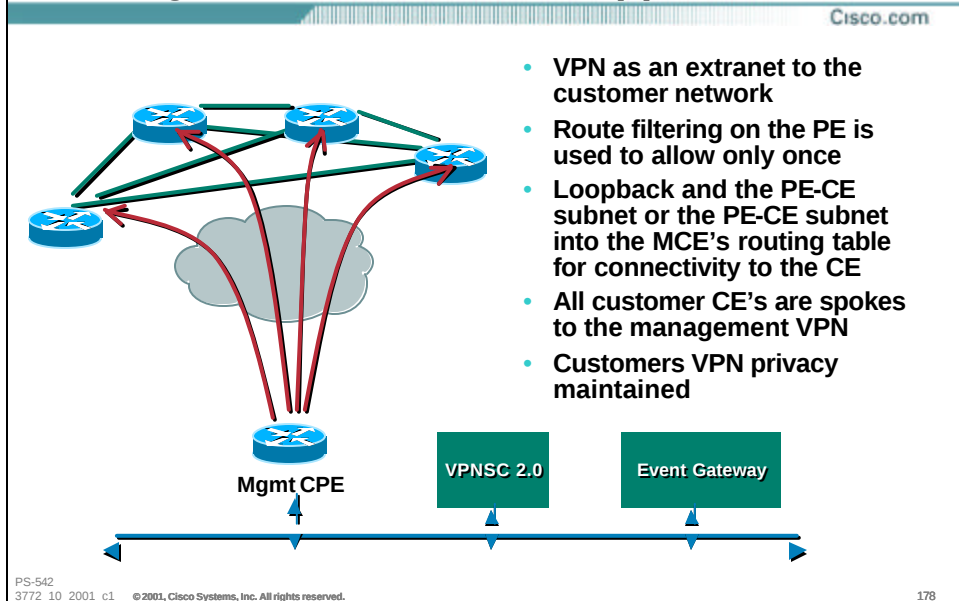
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

176

Provisioning of Performance Monitoring



Managed Customer VPN Support



Cisco.com

- ## API support

179

Cisco.com

-

180

Service Auditing

Cisco.com

- Validation of service request configuration
- Network wide scheduled service audits ensures health of the VPN services
- Audit of routing information
- Excellent tool for trouble shooting failed configuration
- Per customer and per VPN reporting



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

181

VPNSC OSS Interfaces

Cisco.com

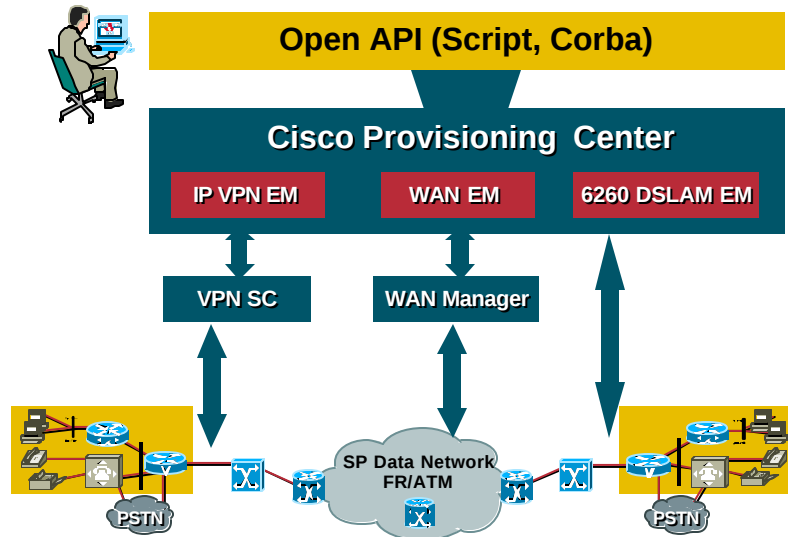
- Complete Corba API's for IPsec and MPLS/VPN
 - Provisioning
 - VPN aware SLA data
 - Accounting API's (MPLS only)
 - Task manager (scheduling)
 - Events API
- Corba event gateway and Tibco bus events
- SLA, Mib data available in XML format
- XML interface for easy import and export of data to VPNSC repository

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

182

CPC VPN Provisioning

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

183

Cisco Provisioning Center (CPC) Overview

Cisco.com

- Comprehensive service creation and service activation via a single step
- Perform a change request (across multiple network elements) in a single transaction
- Single provisioning interface to create/activate services across multiple technologies and multiple products

Service Administration



Service Creation

Flow-Through Interface and GUI



Service Activation



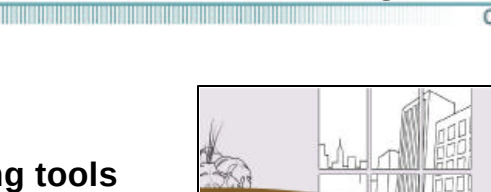
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

184



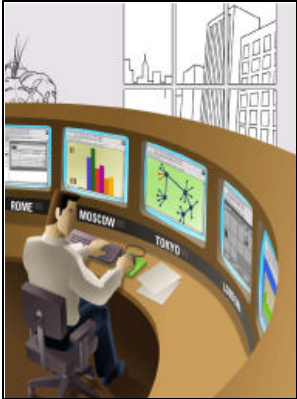
Network Performance and Fault Monitoring

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 185



Performance and Fault Monitoring

- Troubleshooting tools
- Exception monitoring
- Device health monitoring
- Fault management



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 186

Why Do We Need Management Information?

Cisco.com

- **To monitor**

Network faults are detected and restored ASAP

Network has the capacity to handle traffic demand

Network is secure from intrusion and tampering

Network maintains proper configuration

Network faults can be isolated to speed time to repair

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

187

MPLS MIBS

Cisco.com

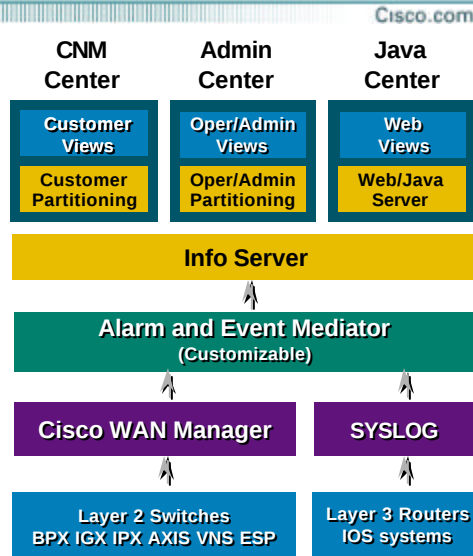
- **mpls-lsr-mib -- label switch router (NHLFE)**
 - mpls-ldp-mib -- ldp**
 - mpls-te-mib -- THE traffic engineering MIB for MPLS**
 - mpls-ftp-mib -- fec-nhlfe**
 - mpls-vpn-mib -- mpls/bgp vpn**
 - mpls-ds-te-mib -- diffserv-aware te**
- **We are also defining several proprietary MIBs to go with the above:**
 - cisco-te-topo-mib -- CDP output for traffic engineering**
 - cisco-te-mib -- proprietary extensions to MPLS-TE-MIB**
 - cisco-ldp-mib -- ldp/tdp**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

188

Cisco Info Center (CIC) Overview

- Event consolidation, correlation, de-duplication and filtering
- Collect and consolidate events from multiple sources on the network
- VPN, CNM, and resource partitioning support
- Scalable and robust product components
- Powerful administrative desktop GUI
- Distributable mgmt. of service and network affecting faults

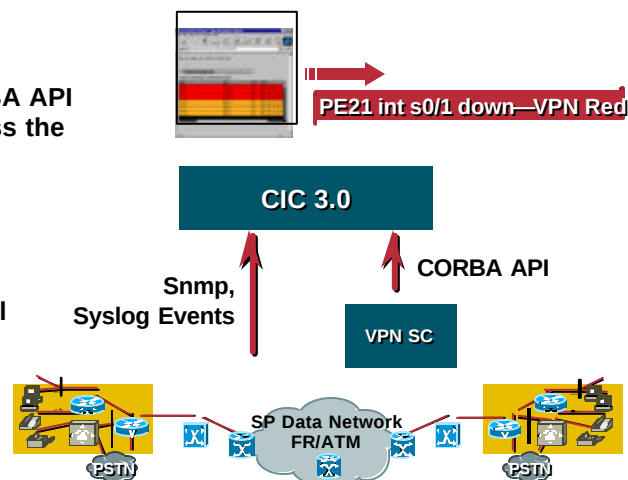


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

189

Cisco Info Center: IP VPN Fault

- CIC 3.0: use CORBA API of VPNSC to access the repository
- Map interfaces to VPNs
- Provide events at a VPN service level
- Correlate sites, VPNs affected by fault



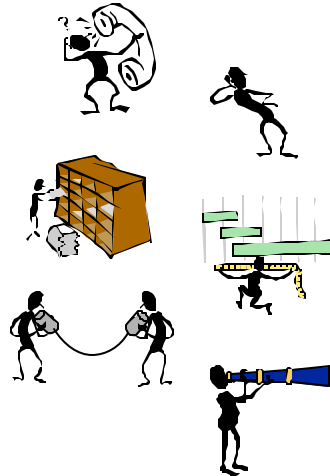
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

190

CIC Enables Service Assurance

Cisco.com

- Customer is **NOT** the alarm system
- Rapid fault detection and forwarding
- Performance data collection, storage and analysis
- Pro-active maintenance
- Remote diagnosis



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

191

Service Quality Assurance

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

192

SLA Management

Cisco.com

- Using Cisco **Service Assurance Agent (SAA)**
- SAA creates application-aware synthetic transactions to closely emulate applications' performance on network
 - ICMP, UDP, TCP, DNS, FTP, HTTP, DHCP...
 - TOS or DSCP byte setting
 - RTD, OWD, jitter, packet loss, availability...
- **Allows end-to-end Service Level Agreements (SLA) monitoring/reporting per class of service**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

193

Application Performance Metrics

Cisco.com

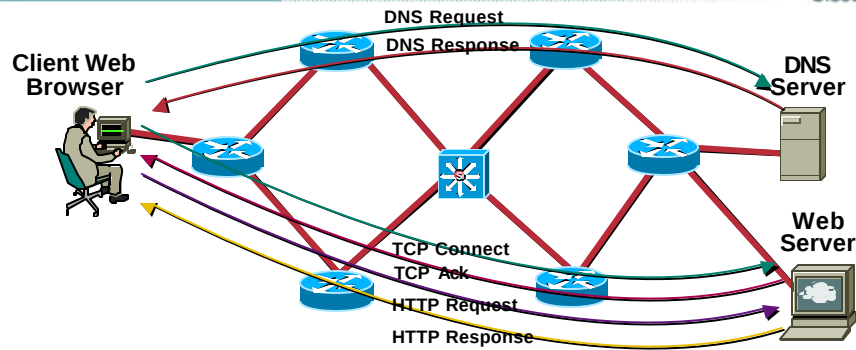
- Responsiveness
- Availability
- Throughput
- Utilization
- Jitter

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

194

Responsiveness

Cisco.com



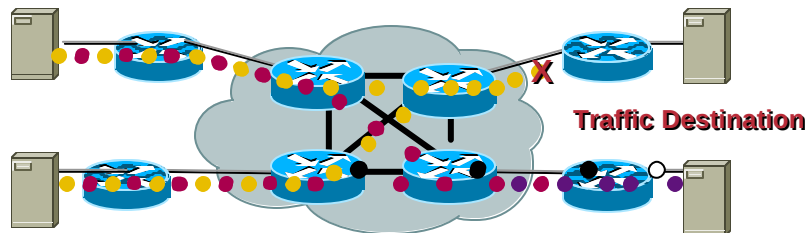
- The response time to fulfill a request for service
- Measurement based on the start of fulfillment
 - When the server responds with requested data
 - Not all services requested are the same effort

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

195

Availability

Cisco.com



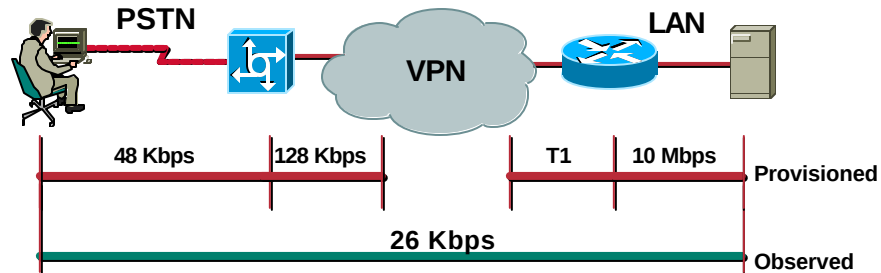
- As a percentage of time the service is actually provided
 - Network service is not busy
 - Network service is not down
 - Network service does not introduce errors
- As a function of MTBF and MTTR

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

196

Throughput

Cisco.com



- Transmission rate of observed data transport measured in:
Bits/bytes per second
Packets per second
- Differences between “provisioned” and “observed” due to:
Oversubscription of circuit
Router utilization
Server congestion

PS-542

3772_10_2001_c1

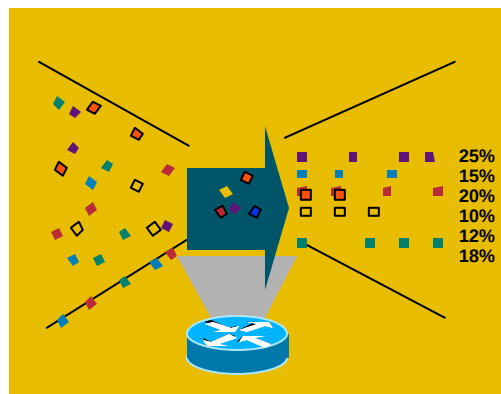
© 2001, Cisco Systems, Inc. All rights reserved.

197

Utilization

Cisco.com

- Percent of total bandwidth consumed
 - Per interface
 - Per interface by traffic class
 - Per interface by application or protocol



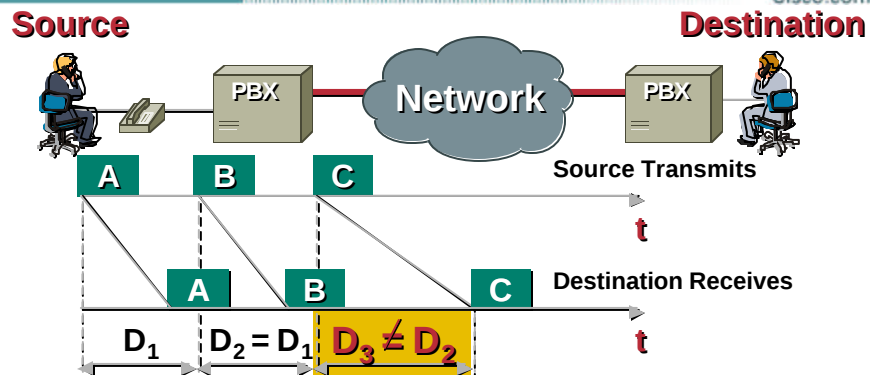
PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

198

Delay Variation—"Jitter"



- The change in packet interval for sequential packets

Source transmits with constant inter-packet interval
 During network transit, inter-packet interval is affected
 At destination, variation of inter-packet interval is jitter

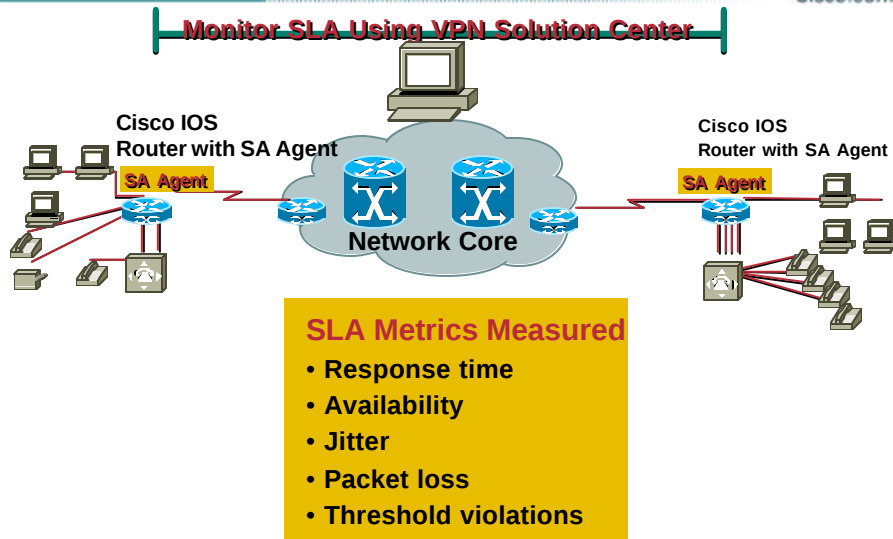
PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

199

SLA Monitoring



PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

200

VPNSC SLA Network Statistics

Cisco.com

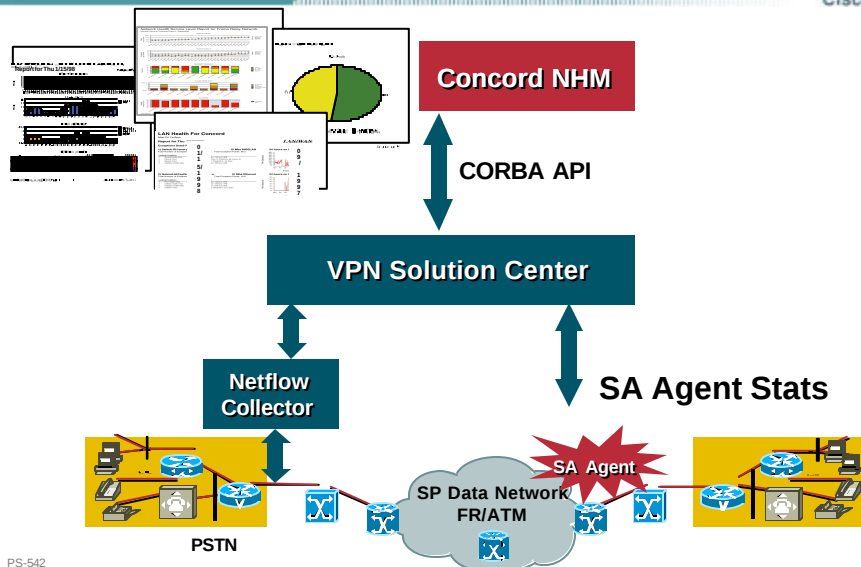
- **Customer statistics**
 - Monitor customer is within SLA for packet delay
 - Monitor customer is within SLA for packet loss
- **Monitor PE to PE statistics**
 - Monitor core is within SLA for packet delay
 - Monitor core is within SLA for packet loss
- **Provision SAA probes to produce traps**
 - Timeout trap
 - Connectivity loss trap
 - Threshold trap
- **Setup SAA history bucket for 15 minutes on router—collection and correlation hourly**
- **Mib2 interface statistics collection**
- **Car Mib stats collection**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

201

Concord's Network Health IP VPN Reporting

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

202

Accounting and Billing

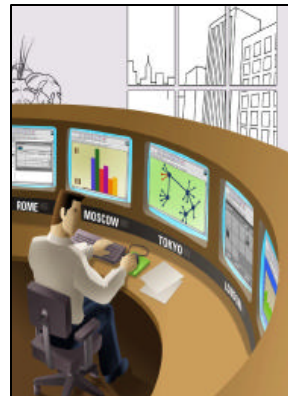
Traffic Accounting and Billing

Network Layer

- Monitor performance and operational status of network elements and services
- Diagnose and repair network faults

Services Layer

- Ensure quality of service and that SLA are met



NetFlow Cache Tracks Flows

Cisco.com

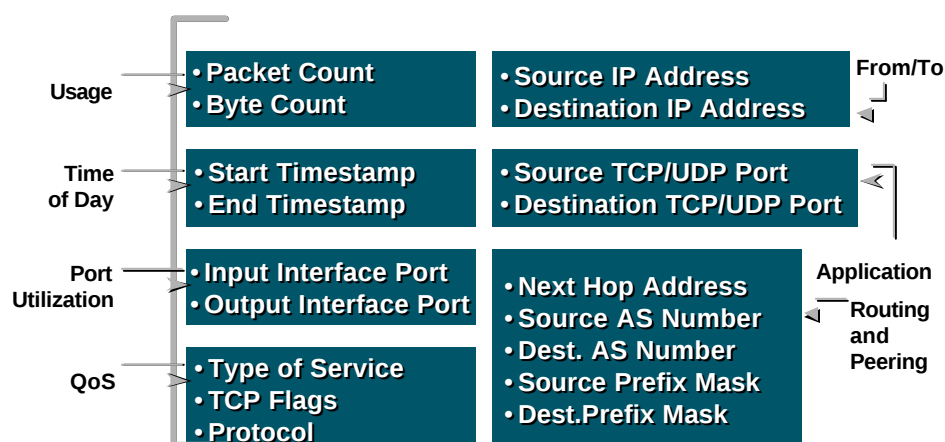
- A “flow” is defined by **seven characteristics**:
 - Source/destination IP address pair
 - Source/destination application port pair
 - IP protocol
 - Input physical interface index
 - IP Type of Service (ToS) byte
- Flows are unidirectional
- NetFlow is enabled on a per input-interface basis

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

205

NetFlow Data Record

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

206

VPN Accounting

Cisco.com

- **Populate the IP address to I/F mapping**
Use I/F Mib collection
- **Collect from the collectors**
Gather the flow data
- **Collect router VPN info**
Gathers VPN data
- **Create the VPN traffic matrix**
Correlates the flow data to VPNs

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

207

VPNSC Accounting

Cisco.com

- **VPNSC can produce VPN aware accounting reports using Netflow collector**
- **VPNSC has repository of VPN information and correlates using Netflow data**
- **VPNSC has accounting API's for partners or an OSS to retrieve the data**
- **VPNSC data can be used by billing partners for usage based billing or capacity planning**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

208

Traffic Accounting

Cisco.com

- CE to CE traffic volume bytes, packets
- PE to PE traffic volume bytes, packets
- PE to CE traffic volume bytes, packets
- Traffic per COS
- PE to PE reports for all customers
- CE to CE reports for each customer
- Customer site to customer site report
- Traffic breakdown by application type and type of service
- Charting also available

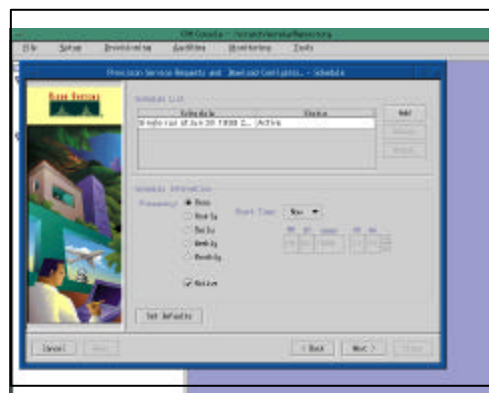
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

209

Performance Monitoring and Reporting

Cisco.com

- SLA report statistics
- Per PE performance reports
- Per VPN performance reports
- Per customer performance reports
- XML



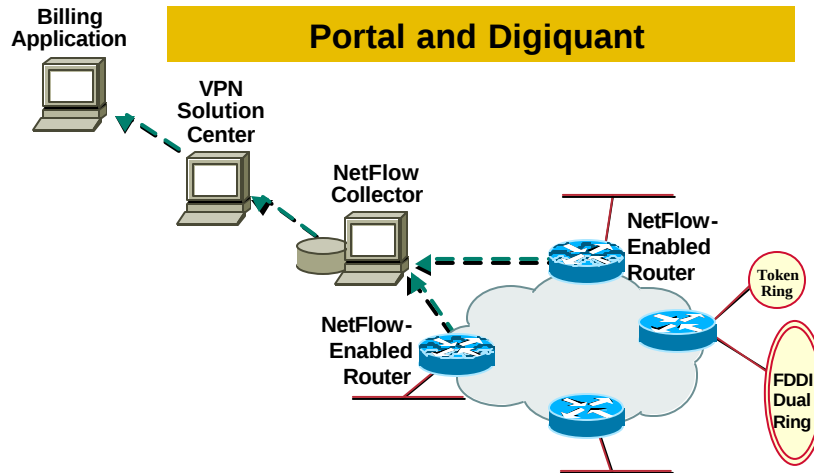
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

210

Usage Collection and Billing

Cisco.com

NetFlow



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

211

IP Services: Traffic Accounting and Billing

Cisco.com



Account/Billing Statistics for:

Time of Day	On or Off Network
Application	Distance Based
QoS/CoS	Bandwidth Usage
Transit or Peer	Data Transferred



NetFlow/BGP Data Exported to
3rd-party Billing Applications



Accounting and Billing Partners:

IP Mediation

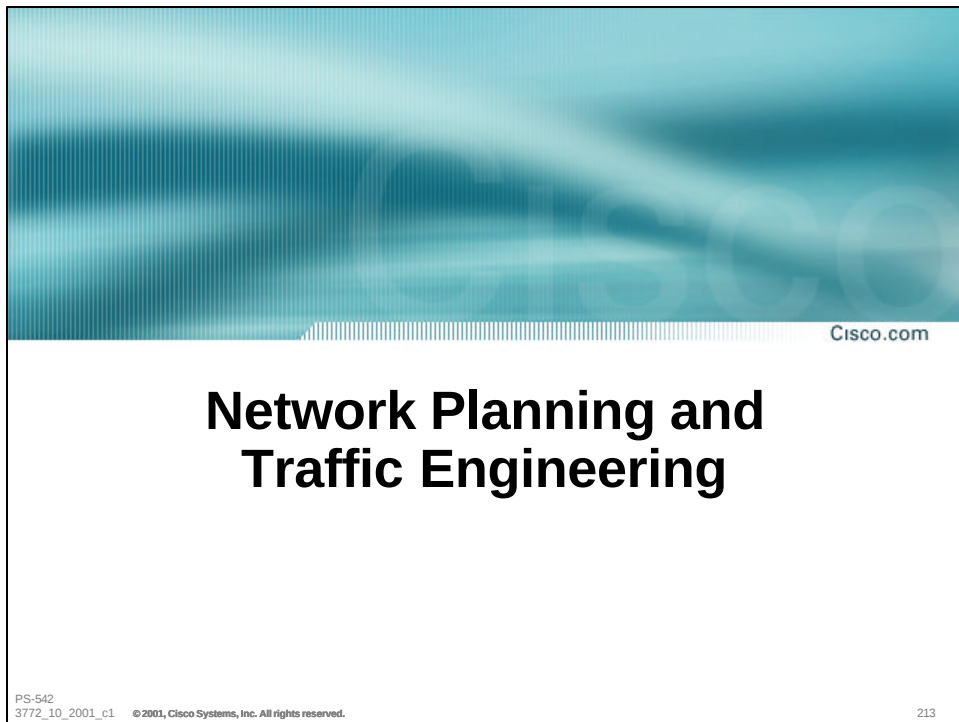


Traffic Analysis or Billing



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

212



Planning and Design

- Is my network ready?
 - Inventory
 - Bandwidth
 - Network quality
 - Availability

The illustration shows a network engineer sitting at a desk, working on a laptop. There are two thought bubbles above the engineer. The top bubble contains several blue Cisco routers. The bottom bubble contains two yellow documents with charts and a small clock icon. The Cisco.com logo is in the top right corner. At the bottom left, there is small text: "PS-542 3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved." and the number "214" is at the bottom right.

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 214

Solutions for Planning MPLS Networks

Cisco.com

- How are LSP tunnels routed in the network?
- How they affect the layer 3 traffic flows in the network?
- During a network failure, how are LSP tunnels rerouted; what's the effect on layer 3 traffic?
- If a tunnel fail to route, what are the bottlenecks?
- What is the trunk utilization during any of these scenarios?
- Where should new trunks or tunnels be added to the network?

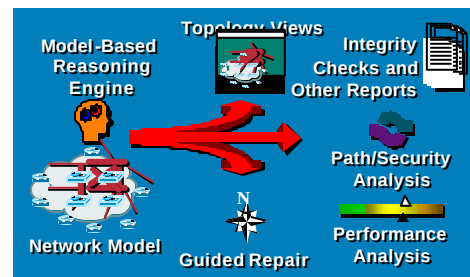
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

215

WANDL Network Design and TE Tools

Cisco.com

- Design and simulate IP/MPLS networks
- Config file parsing and integrity checking
- Planning for traffic growth
- Play “what-if” scenarios to ensure reliability of your network under stress
- MPLS TE provisioning



Periodic Upload of
Topology and Traffic
Statistics

Modified/Repaired
Design Scenario

**Infrastructure
and Control**



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

216

Variety of Tools Depending on Need

Cisco.com

- [1] NPAT "Network Planning and Analysis Tools"
- With three main capabilities:
 - 1-Path Placement (Optimum Routing of Traffic)
 - 2-Exhaustive Failure Simulation
 - 3-Automatic Basic Design and Diversity Design
- [2] NPAT for MPLS Traffic Engineering
- [3] MPLS View "MPLS Traffic Engineering, Management and Provisioning Tools"
- [4] IPAT "IP Analysis Tools" is the Netsys migration/replacement product

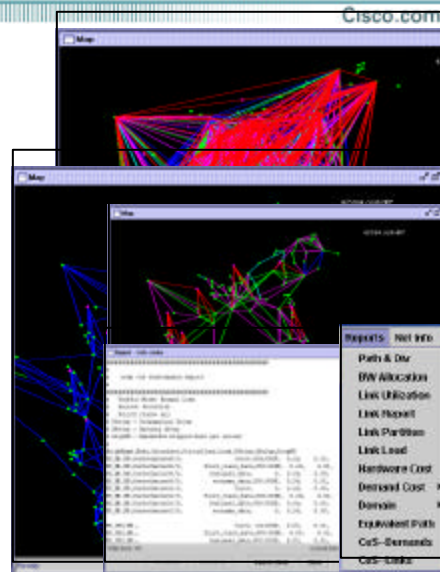


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

217

MPLS View

- LSP tunnel config data and traffic collection
- Config file parsing, topology extraction, integrity checking
- IOS delta configuration for MPLS TE provisioning
- Integrated set of monitoring, modeling, and design capabilities
 - Multi-layer simulation with equipment details
 - Multi-period traffic load analysis
 - LSP tunnel path placements and provisioning
 - What-if (fiber cut, for example) simulation
 - Primary/backup LSP path computation



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

218

WANDL MPLS Network Models

Cisco.com

Nodes	Cisco 7500, GSR12000, GSR12400 Series	Constraint Based Routing
Links	T3/E3, OC3, OC12, OC48, OC192 32 Bits Resource or Media Attributes Routing Metrics	
LSP Tunnels	Source, Destination Bandwidth and RSVP Reservable Bandwidth Affinity, Mask Priority/Holding Priority Guaranteed Bandwidth or Diff Serv TE Routing Method: Dynamic Route Explicit Route Backup Routes	
Layer 3 Traffic	OSPF, ISIS, BGP4 Forwarding Equivalence Classes Influence of LSP Tunnels	

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

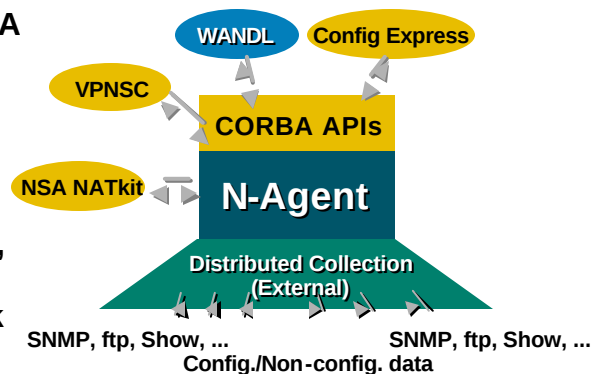
219

N-Agent

Cisco.com

Overview

- Server with CORBA APIs that can be integrated with OSS solutions to perform complex functions such as network modeling, analysis, and validating network integrity



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

220

Agenda

Cisco.com

- What Does MPLS Mean to Network Management?
- What Are the Specific Functions Required to Support MPLS Networks and Services?
- What Are the Technologies and Applications Needed for Each Function?
- **How Does a Provider Bring These Tools Together Within the Larger Context of an Existing OSS/BSS?**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

221

Carrier Class Platform—RAS

Cisco.com

- Support multiple administrators
- Provision backup redundant routers for load balancing or fail over support
- Scalable secure management
- Multiple transport gateways
- Multi-threaded programming
- Scalable SLA management
- Self healing
- Auto inventory population

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

222

VPNSC OSS Interfaces

Cisco.com

Flow-through Provisioning

- Tibco bus events
- XML
- Corba event gateway
- Complete Corba API's
 - Provisioning
 - VPN aware SLA data
 - Accounting API's
 - Task manager (scheduling)
 - Events API
 - Template API

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

223

Internet OSS: End-to-End Solutions— Telemanagement Forum

Cisco.com

New Generation Plug-and-Play “TMF” Catalyst Program

Addresses:

- Data, voice, and video services
- Fulfillment, assurance and billing
- Commercially availability
- Reference architectures

Enabled by:

- Workflow
- Bus/messaging architecture
- Common data/directory
- UML process documentation

TeleManagement World—Chicago

Systems Integrators

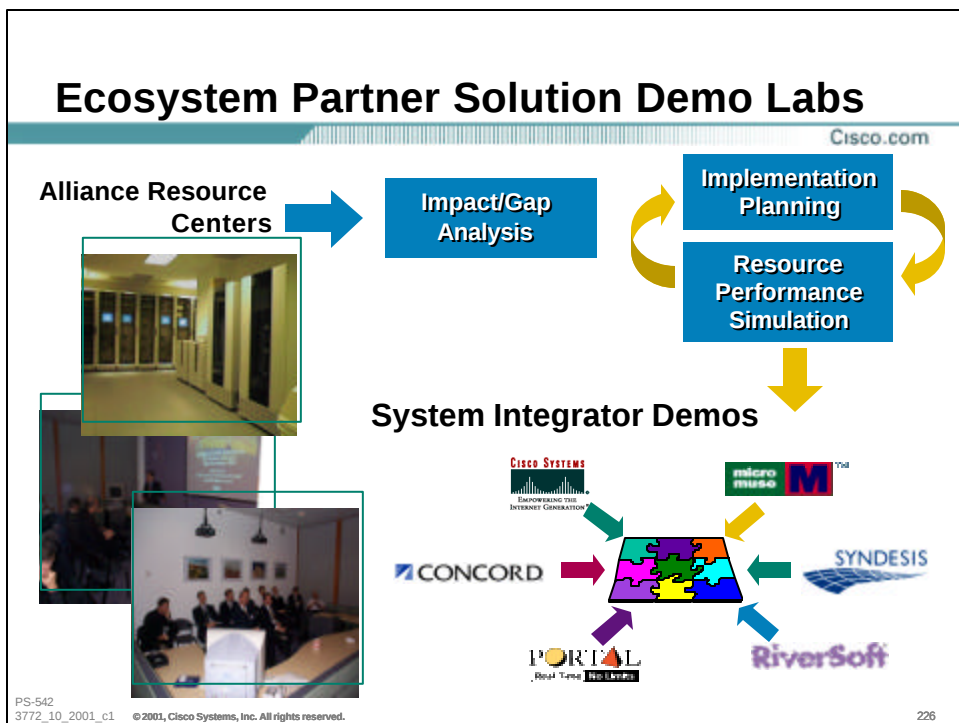
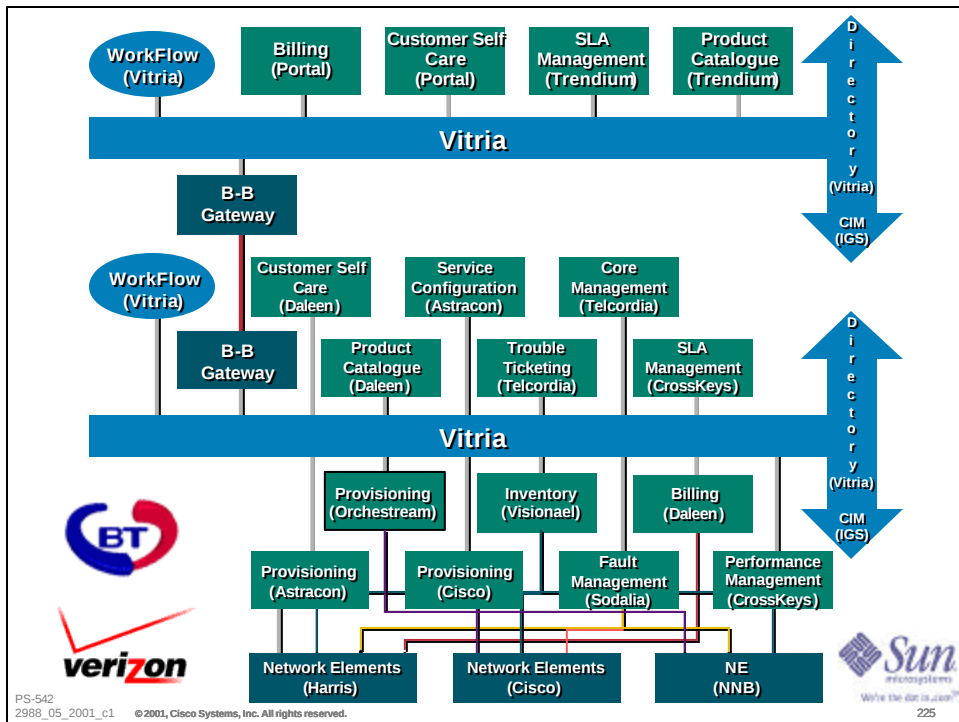
HP—Self Service Over Multiple Networks
PWC—DSL Customer Management Services
PWC—Mobile IP (Nice 2001)
E&Y—Broadband Cable Service Mgmt
—IP Service Management
Dimension Data—IP/VPN Service Mgmt

ISVs

Active, Alcatel, Metasolv, Astracon, Micromuse, Siebel, Cygent, IGS, Syndesis, Cambio, Portal, Tibco, Sun, MDSI, Trendium, TCSI, Microsoft, Nokia, ADC, Sodalia, Orchestream, Vertel, CommTech, CrossKeys, Riversoft, Vitria, EHPT, Cramer, Daleen, OSI

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

224





Cisco.com

MPLS Traffic Engineering

Section 4

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 227



Cisco.com

Basics, Advanced Concepts, and Deployment Strategies

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 228

Agenda

Cisco.com

- **How MPLS-TE Works**
- **Advanced Concepts**
- **Deploying and Designing**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

229

How MPLS-TE Works

Cisco.com

- **How MPLS-TE works**
 - What good is MPLS-TE?**
 - Information distribution**
 - Path calculation**
 - Path setup**
 - Forwarding traffic down a tunnel**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

230

What Good Is MPLS-TE?

Cisco.com

- There are three kinds of networks
 1. Those that have plenty of bandwidth everywhere
 2. Those with congestion in some places, but not in others
 3. Those with constant congestion everywhere
- The first kind always evolves into the second kind!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

231

What Good Is MPLS-TE?

Cisco.com

- MPLS-TE introduces a 4th kind:
 1. Those that have plenty of bandwidth everywhere
 2. Those with congestion in some places, but not in others
 3. Those with constant congestion everywhere
 4. Those that use all of their bandwidth to its maximum efficiency, regardless of shortest-path routing!
- MPLS-TE can help turn #2 into #4
 - If you have #1, you probably don't need MPLS-TE—yet
 - If you have #3, you're stuck—you need more bandwidth (or less traffic)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

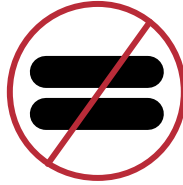
232

What Good Is MPLS-TE?

Cisco.com

What Is MPLS-TE?

- Multi Protocol Label Switching—Traffic Engineering



What Is It Not?

- Magic Problem Solving Labor Substitute which is Totally Effortless

This Stuff Takes **Work**, but It's **Worth It!!!**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

233

Information Distribution

Cisco.com

- You need a link-state protocol as your IGP
IS-IS or OSPF
- Link-state requirement is **only** for MPLS-TE!
Not a requirement for VPNs, etc!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

234

Need for a Link-State Protocol

Cisco.com

- **Why do I need a link-state protocol?**
 - To make sure info gets flooded
 - To build a picture of the entire network

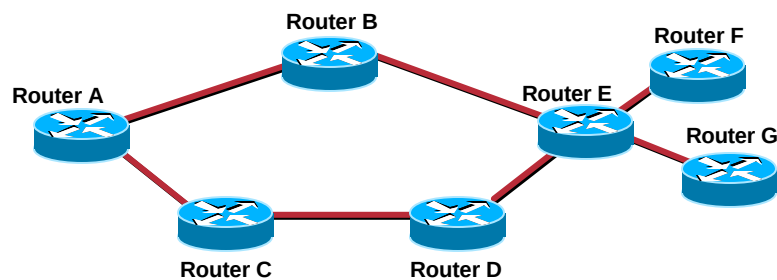
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

235

Need for a Link-State Protocol

Cisco.com

- **Consider the following network:**
 - All links have a cost of 10
 - Router A's path to Router E is A->B->E, cost 20
 - All traffic from A to {E,F,G} goes A->B->E

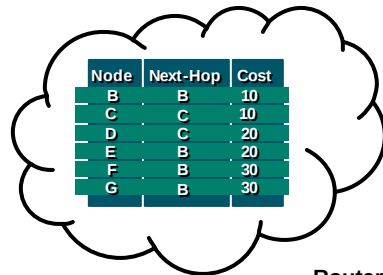


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

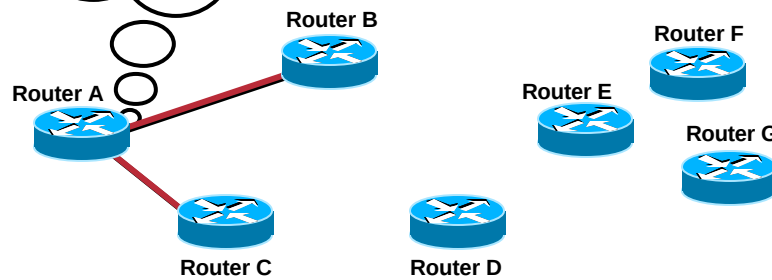
236

What a DV Protocol Sees

Cisco.com



- Router A doesn't see all the links
- Router A only knows about the shortest path
- This is by design

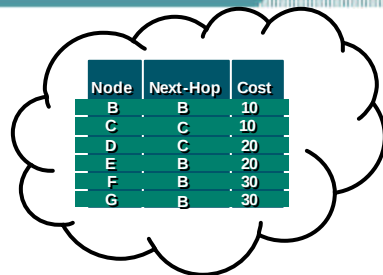


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

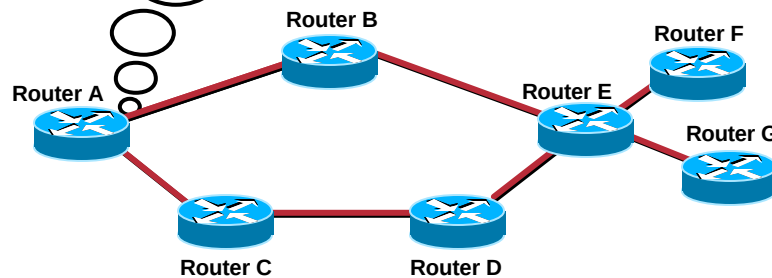
237

What a LS Protocol Sees

Cisco.com



- Router A sees all links
- Router A only **computes** the shortest path
- Routing table doesn't change

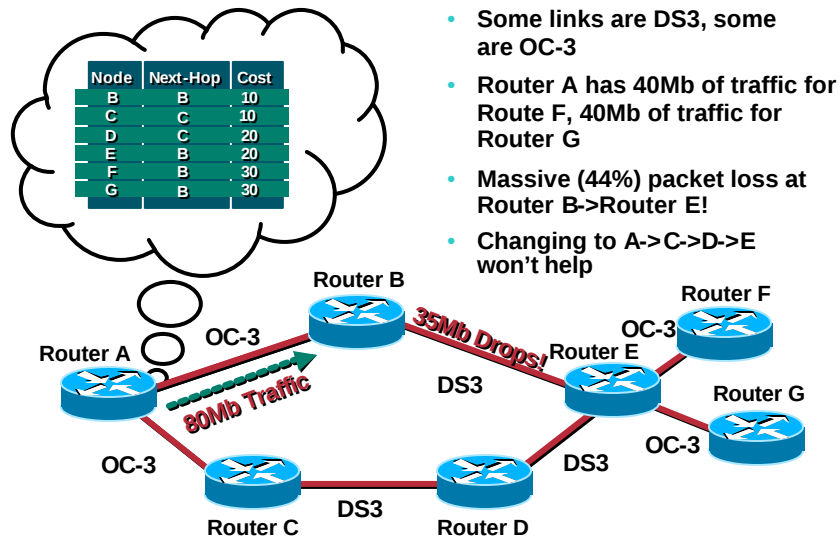


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

238

The Problem with Shortest-Path

Cisco.com

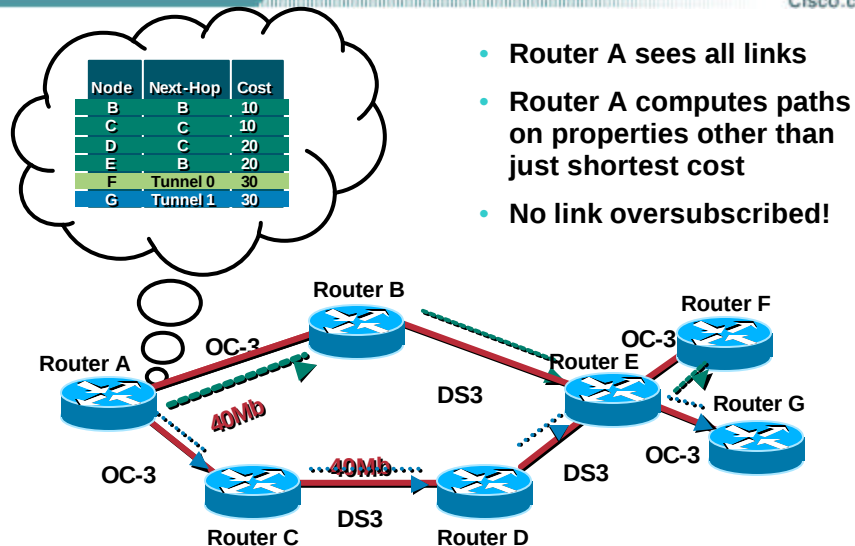


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

239

What MPLS-TE Address

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

240

How MPLS-TE Works

Cisco.com

- **How MPLS-TE works**

What good is MPLS-TE?

Information distribution

Path calculation

Path setup

Forwarding traffic down a tunnel

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

241

Information Distribution

Cisco.com

- **OSPF**

Uses type 10 (opaque area—local) ISAs

See draft-katz-yeung-ospf-traffic

See also the Networkers 2001 OSPF
Deployment session

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

242

Information Distribution

Cisco.com

- **IS-IS**

Uses Type 22 TLVs

See draft-ietf-isis-traffic

**See also the Networkers 2001 IS-IS
Deployment session**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

243

Information Distribution

Cisco.com

- **IS-IS and OSPF propagate the same
information!**

Link identification

TE metric

**Bandwidth information (maximum physical,
maximum reserveable, available per-class)**

Attribute flags

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

244

Information Distribution

Cisco.com

- TE flooding is local to a single {area|level}
- Inter-{area|level} TE harder, but possible (think PNNI)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

245

How MPLS-TE Works

Cisco.com

- **How MPLS-TE works**
 - What good is MPLS-TE?
 - Information distribution
 - Path calculation**
 - Path setup
 - Forwarding traffic down a tunnel

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

246

Path Calculation

Cisco.com

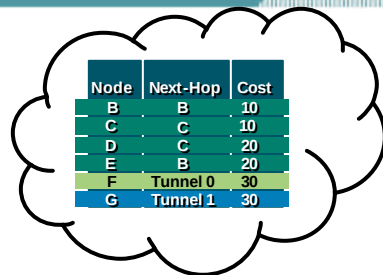
- Modified Dijkstra at tunnel head-end
- Often referred to as CSPF
Constrained SPF
- ...or PCALC (path calculation)

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

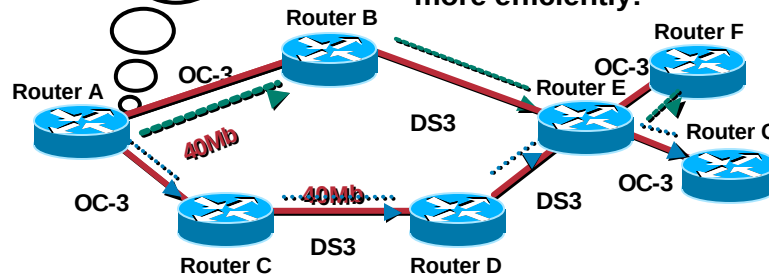
247

Path Calculation

Cisco.com



- PCALC takes bandwidth, other constraints into account
- Paths calculated, resources reserved if necessary
- End result: Bandwidth used more efficiently!



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

248

Path Calculation

Cisco.com

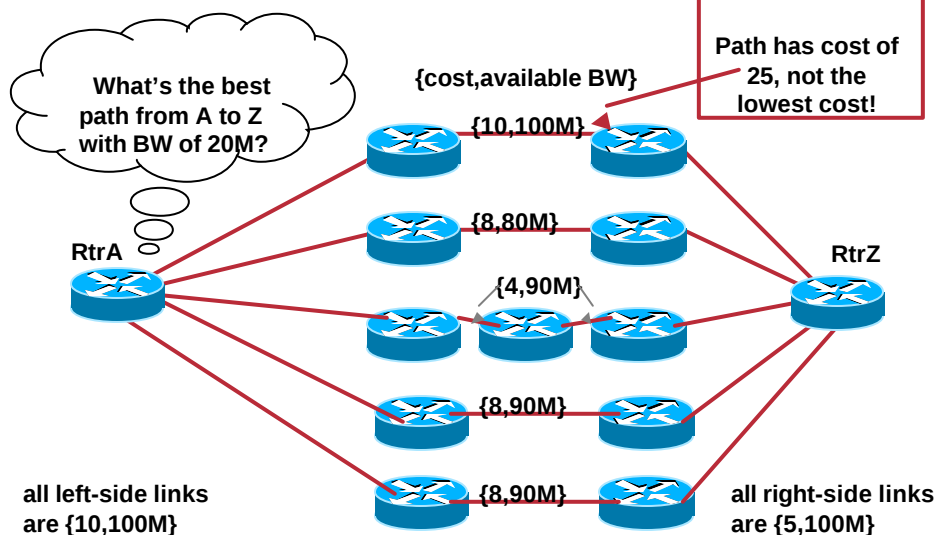
- What if there's more than one path that meets the minimum requirements (bandwidth, etc.)?
- PCALC algorithm:
 - Find all paths with the lowest IGP cost
 - Then pick the path with the highest minimum bandwidth along the path
 - Then pick the path with the lowest hop count (not IGP cost, but hop count)
 - Then just pick one path at random

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

249

Path Calculation

Cisco.com

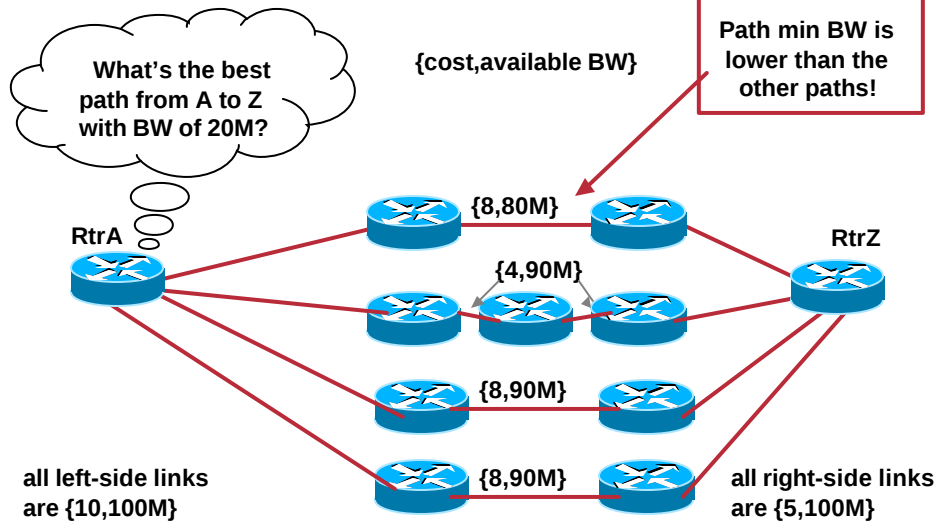


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

250

Path Calculation

Cisco.com

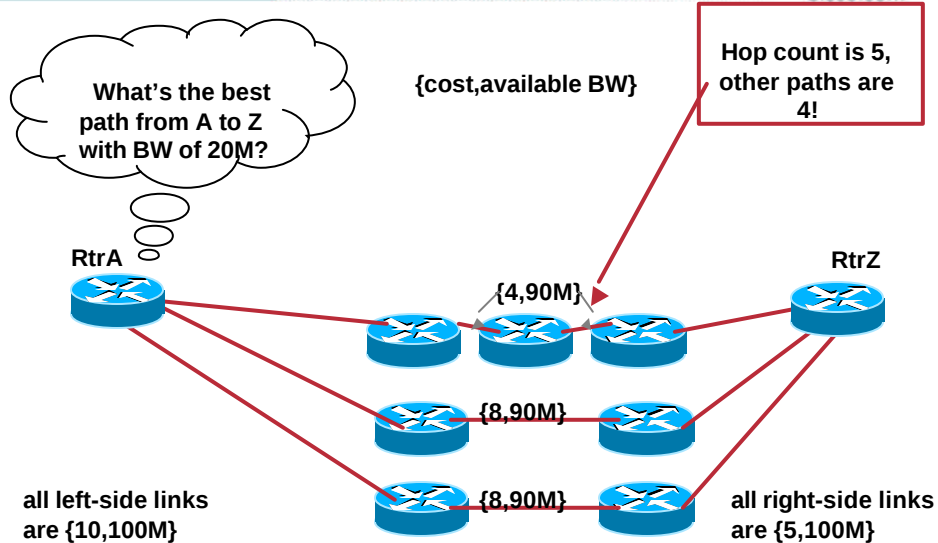


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

251

Path Calculation

Cisco.com

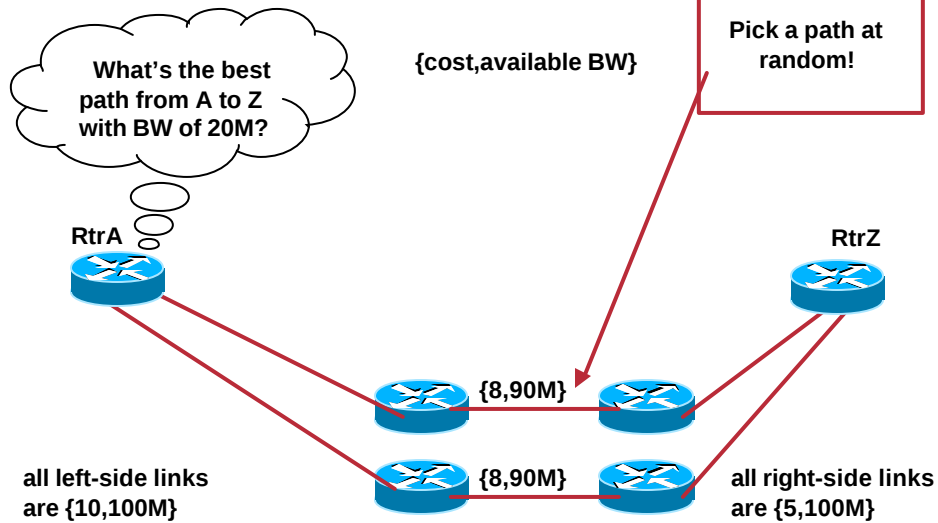


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

252

Path Calculation

Cisco.com

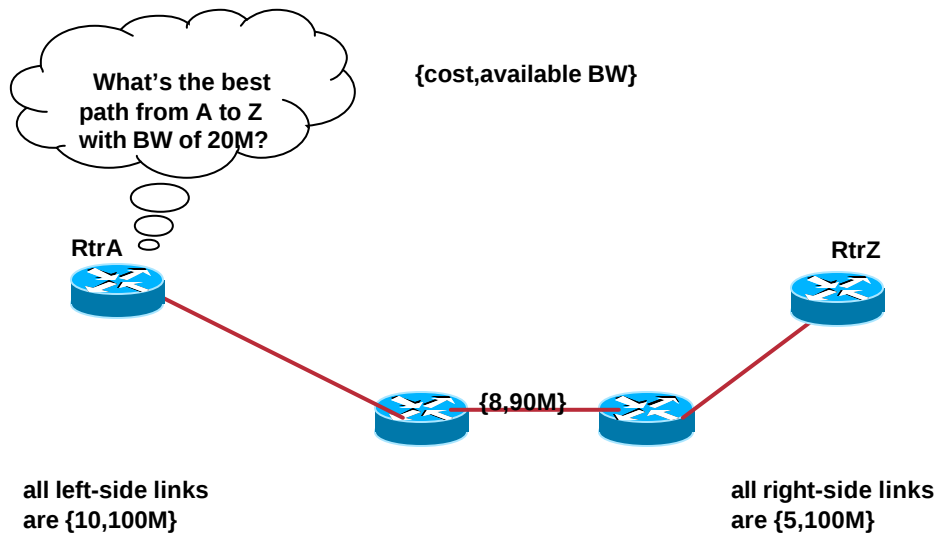


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

253

Path Calculation

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

254

How MPLS-TE Works

Cisco.com

- **How MPLS-TE works**

What good is MPLS-TE?

Information distribution

Path calculation

Path setup

Forwarding traffic down a tunnel

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

255

Path Setup

Cisco.com

- Cisco MPLS-TE uses RSVP
- RFC2205, plus
draft-ietf-mpls-rsvp-lsp-tunnel

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

256

Path Setup

Cisco.com

- Once the path is calculated, it is handed to RSVP
- RSVP uses PATH and RESV messages to request an LSP along the calculated path

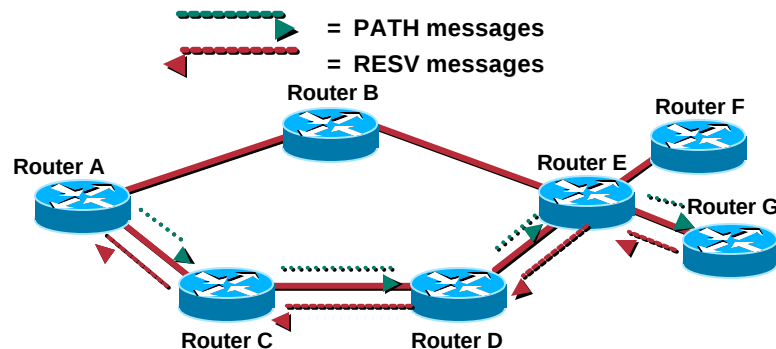
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

257

Path Setup

Cisco.com

- PATH message: "Can I have 40Mb along this path?"
- RESV message: "Yes, and here's the label to use"
- LFIB is set up along each hop



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

258

Path Setup

Cisco.com

- Errors along the way will trigger RSVP errors
- May also trigger re-flooding of TE information if appropriate

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

259

How MPLS-TE Works

Cisco.com

- **How MPLS-TE works**
 - What good is MPLS-TE?
 - Information distribution
 - Path calculation
 - Path setup
 - Forwarding traffic down a tunnel**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

260

Forwarding Traffic Down a Tunnel

Cisco.com

- There are three ways traffic can be forwarded down a TE tunnel
 - Autoroute
 - Static routes
 - Policy routing
- With the first two, MPLS-TE gets you unequal cost load balancing

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

261

Autoroute

Cisco.com

- Autoroute = “Use the tunnel as a directly connected link for SPF purposes”
- This is **not** the CSPF (for path determination), but the regular IGP SPF (route determination)
- Behavior is intuitive, operation can be confusing

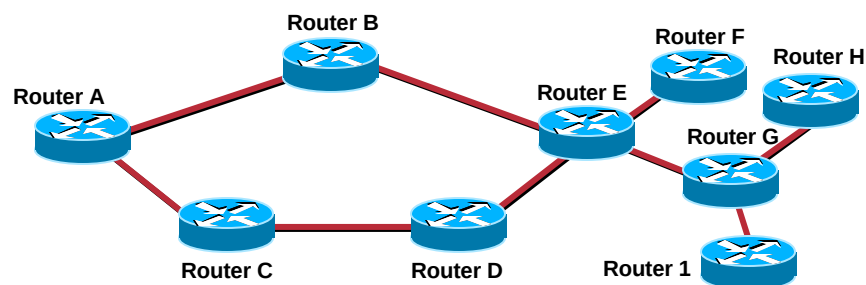
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

262

Autoroute

Cisco.com

This Is the Physical Topology



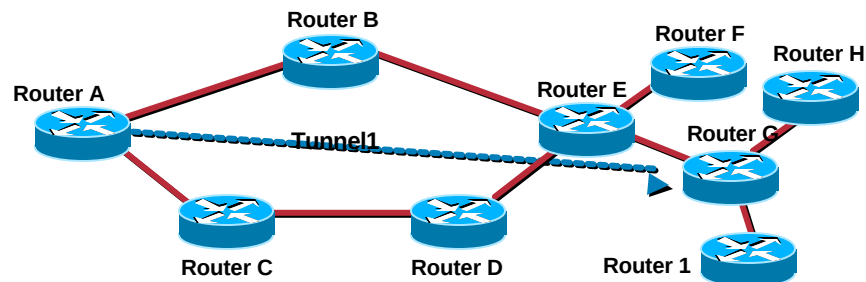
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

263

Autoroute

Cisco.com

- This is Router A's logical topology
- By default, other routers don't see the tunnel!



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

264

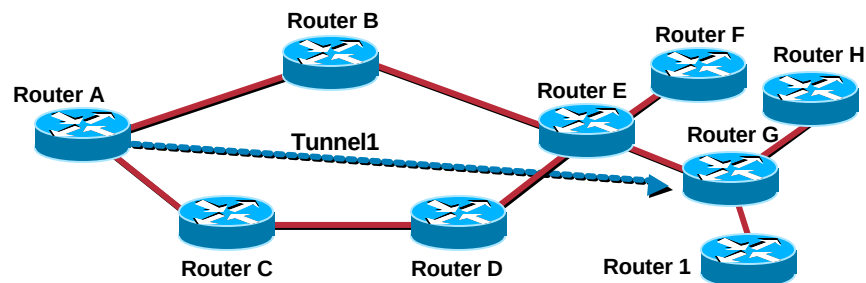
Autoroute

Cisco.com

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	B	30
G	Tunnel 1	30
H	Tunnel 1	40
I	Tunnel 1	40

- Router A's routing table, built via auto-route

- Everything "behind" the tunnel is routed via the tunnel



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

265

Unequal Cost Load Balancing

Cisco.com

- IP routing has equal-cost load balancing, but not unequal cost*
- Unequal cost load balancing difficult to do while guaranteeing a loop-free topology

*EIGRP Has 'Variance', but That's Not As Flexible

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

266

Unequal Cost Load Balancing

Cisco.com

- Since MPLS doesn't forward based on IP header, permanent routing loops don't happen
- 16 hash buckets for next-hop, shared in **rough** proportion to configured tunnel bandwidth or load-share value

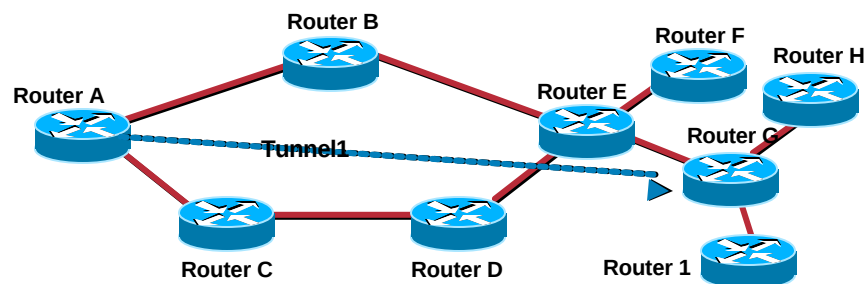
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

267

Static Routing

Cisco.com

```
RtrA(config)#ip route H.H.H.H  
255.255.255.255 Tunnel1
```



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

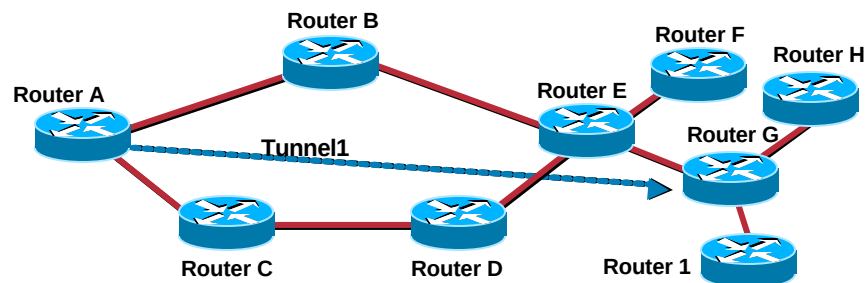
268

Static Routing

Cisco.com

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	B	30
G	B	30
H	Tunnel 1	40
I	B	40

- Router H is known via the tunnel
- Router G is **not** routed to over the tunnel, even though it's the tunnel tail!



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

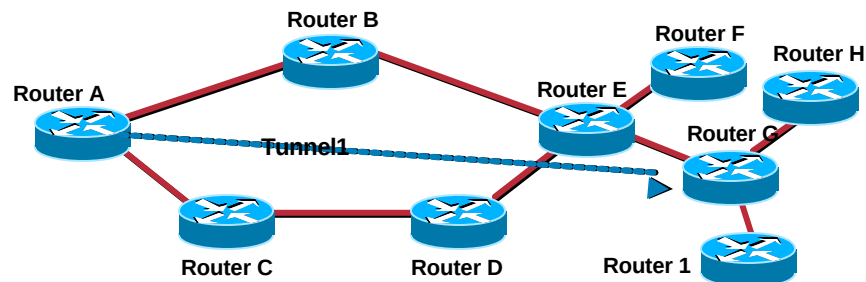
269

Policy Routing

Cisco.com

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	B	30
G	B	30
H	B	40
I	B	40

- Routing table isn't affected by policy routing
- Need (12.0(16)ST or 12.2T) or higher for 'set interface tunnel' to work (CSCdp54178)



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

270

Forwarding Traffic down a Tunnel

Cisco.com

- You can use any combination of auto-route, static routes, or PBR
- ...But simple is better unless you have a good reason
- Recommendation: Either auto-route or statics to BGP next-hops, depending on your needs

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

271

Agenda

Cisco.com

- How MPLS-TE Works
- **Advanced Concepts**
 - Fast ReRoute**
 - Diffserv-Aware Traffic Engineering
- Deploying and Designing

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

272

Fast Reroute

Cisco.com

- In an IP network, a link failure causes several seconds of outage

Thing	Dependency	Time
Link Failure Detection	Media- and Platform-specific	~usecs (POS + APS)
Information Propaganda	IGP Timers, Network Size, Collective Router Load	~5–30sec
Route Recalculation	LSDB Size, CPU Load	~1–3sec

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

273

Fast Reroute

Cisco.com

- In an MPLS network, there's more work to be done, so a (slightly) longer outage happens

Thing	Dependency	Time
Link Failure Detection	Media- and Platform-specific	~Usecs (POS + APS)
Information Propaganda	IGP Timers, Network Size, Collective Router Load	~5–30sec
Route Recalculation	LSDB Size, CPU Load	~1–3sec
New LSP Setup	Network Size, CPU Load	~5–10sec

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

274

Three Kinds of Fast Reroute

Cisco.com

- **Link protection**
The only scheme implemented today
- **Node protection**
On the way
- **Path protection**
On development radar

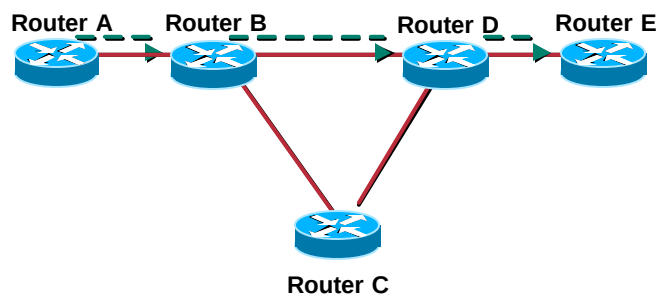
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

275

Link Protection

Cisco.com

- **TE Tunnel A -> B -> D -> E**



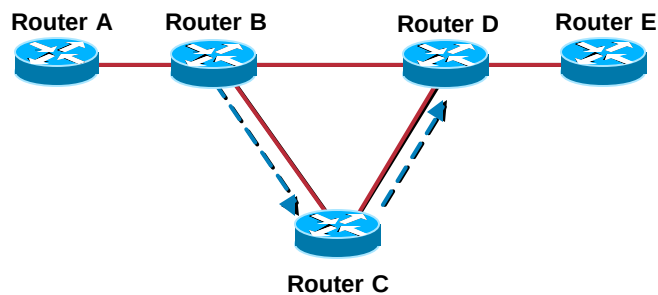
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

276

Link Protection

Cisco.com

- B has a pre-provisioned backup tunnel to the other end of the protected link (Router D)
- B relies on the fact that D is using global label space



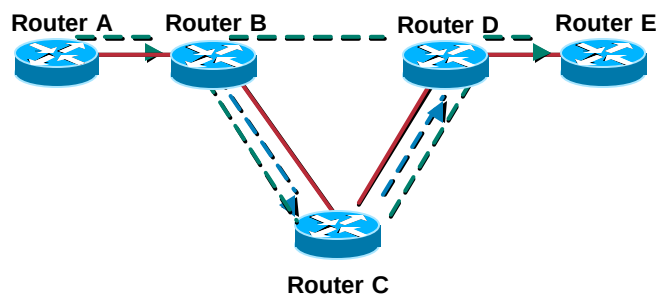
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

277

Link Protection

Cisco.com

- B -> D link fails, A -> E tunnel is encapsulated in B -> D tunnel
- Backup tunnel is used until A can re-compute tunnel path as A -> B -> C -> D -> E (10–30 seconds or so)



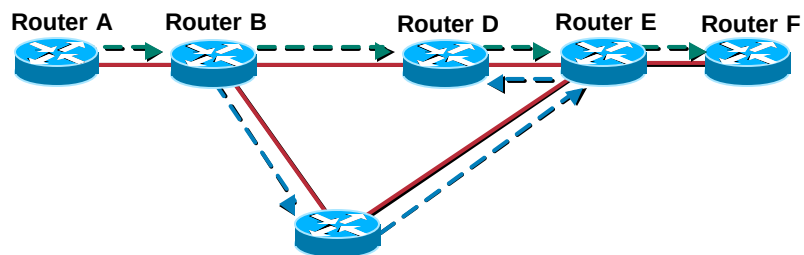
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

278

Node Protection

Cisco.com

- Router A has a tunnel A -> B -> D -> E -> F
- Router B has a protect tunnel B -> C -> E -> D



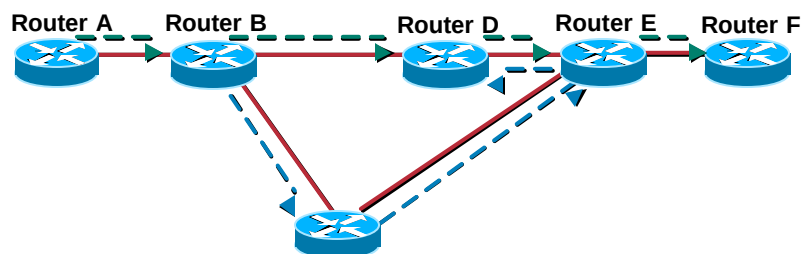
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

279

Node Protection

Cisco.com

- Link protection is OK if the B -> D link goes down
- What if Router D goes away?



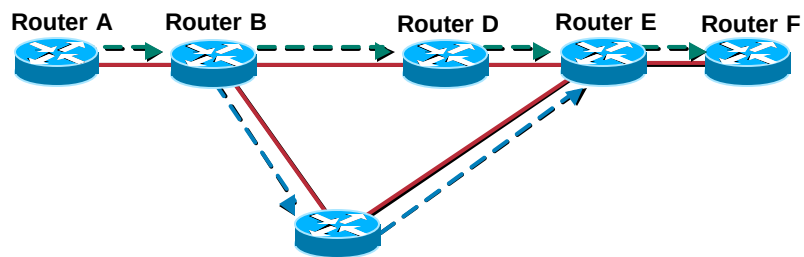
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

280

Node Protection

Cisco.com

- Solution: protect tunnel to the hop **past** the protected link



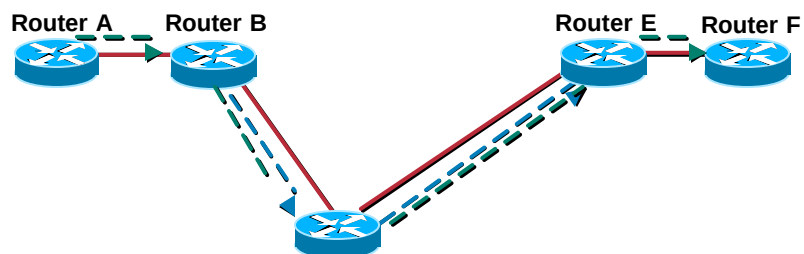
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

281

Node Protection

Cisco.com

- Solution: protect tunnel to the hop **past** the protected link



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

282

Node Protection

Cisco.com

- Node protection still has the same convergence properties as link protection
- Deciding where to place your backup tunnels is a much harder to problem to solve large-scale
 - ...Turns out it's an NP-complete problem
- For small-scale protection, link may be better
- Cisco is developing tools to solve these hard problems for you (see TunnelVision, later)

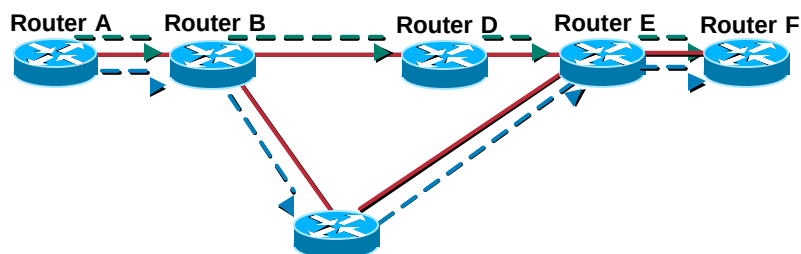
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

283

Path Protection

Cisco.com

- Path protection: Multiple tunnels from TE head to tail, across diverse paths



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

284

Path Protection

Cisco.com

- **Path protection: Least scalable, most resource-consuming, slowest convergence of all 3 protection schemes**
- **Path protection is useful in two places:**
 1. When you have more links than tunnels
 2. When you need to protect links not using global label space

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

285

Path vs. Local Protection

Cisco.com

Local (Link/Node) Protection

Thing	Dependency	Time
Link Failure Detection	Media- and Platform-specific	~Usecs (POS + APS)
Local Switch-over to Protect Tunnel	RP-> Communication Time	~Few msec or less

Path Protection

Thing	Dependency	Time
Link Failure Detection	Media- and Platform-specific	~Usecs (POS + APS)
Information Propagation	IGP Timers, Network Size, Collective Router Load	~Few sec+
Head-end Switch-over to Protect LSP	Network Size, CPU Load	~Msec

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

286

Agenda

Cisco.com

- Prerequisites
- How MPLS-TE Works
- **Advanced Concepts**
 - Fast ReRoute
 - Diffserv-Aware Traffic Engineering**
- Deploying and Designing

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

287

DiffServ-Aware Traffic Engineering

Cisco.com

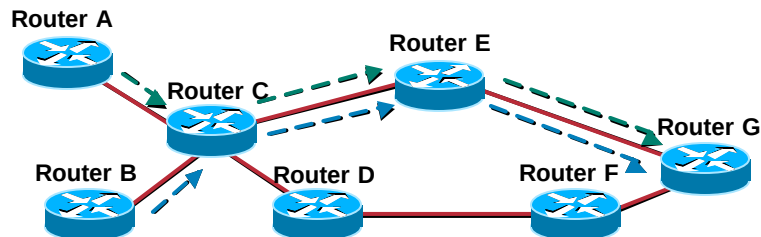
- MPLS can advertise and reserve bandwidth on a link
- Works great, but what if you send a mix of LLQ and BE traffic down a TE tunnel?
- Need some way to differentiate and reserve LLQ bandwidth on a link

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

288

DiffServ-Aware Traffic Engineering

Cisco.com



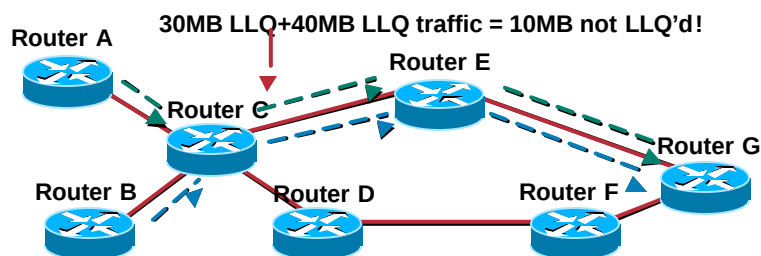
- 2 tunnels across C->E link
- 40MB each tunnel
- 150MB reservable on C->E, with a 30MB LLQ
- What happens as when both tunnels send 20MB of VoIP traffic?

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

289

DiffServ-Aware Traffic Engineering

Cisco.com



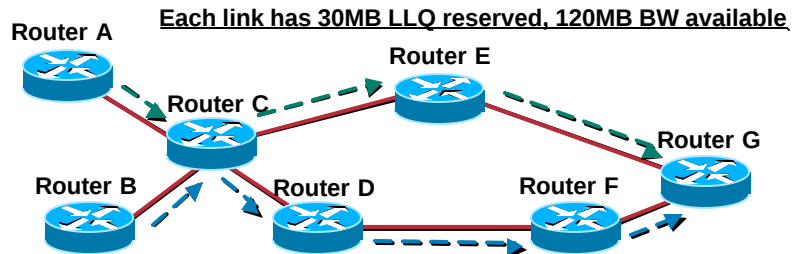
- Problem: Only one bandwidth pool on an interface, no way to differentiate what types of traffic are carried.
- Solution: Advertise more than one pool!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

290

DiffServ-Aware Traffic Engineering

Cisco.com



- Configure each link with 150MB reservable, 30MB of which is LLQ'd
- Tunnels for VoIP can reserve from the sub-pool
- Much less chance of queue oversubscription
- Minimal bandwidth waste – VoIP and data traffic follow the best path they can find.

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

291

DiffServ-Aware Traffic Engineering

Cisco.com

- Coming soon to a router near you: Delay-Sensitive Metric!

An OC3 satellite link and an OC3 land line have the same bandwidth, same IGP metric, but vastly different delay characteristics

Configure TE administrative-weight as one-way propagation delay

Tell VoIP tunnels to use the delay metric as their link cost in CSPF

Combine this with bandwidth utilization, and your VoIP trunks can find paths that match both bandwidth and delay needs!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

292

Agenda

Cisco.com

- Prerequisites
- How MPLS-TE Works
- Advanced Concepts
- **Deploying and Designing**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

293

Deploying and Designing

Cisco.com

- **Deployment methodologies**
- Scalability
- Management
- Security

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

294

Deployment Methodologies

Cisco.com

- **Two ways to deploy MPLS-TE**
 - As needed to clear up congestion
 - Full mesh between a set of routers
- **Both methods are valid, both have their pros and cons**

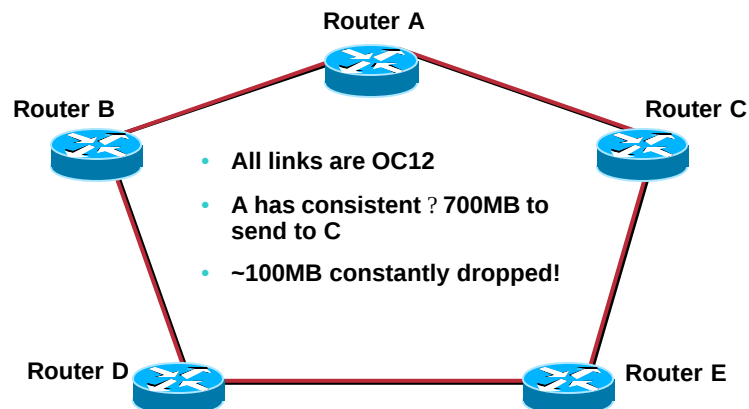
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

295

As Needed

Cisco.com

Case Study: A Large US ISP



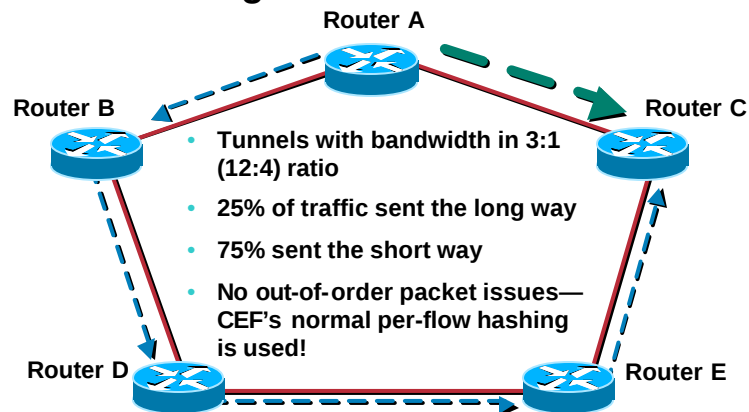
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

296

As Needed

Cisco.com

- **Solution: Multiple tunnels, unequal cost load sharing!**



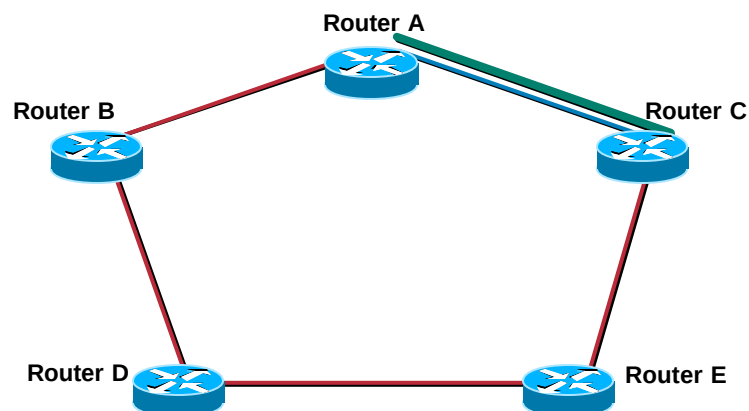
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

297

As Needed

Cisco.com

- **From Router A's perspective, topology is:**



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

298

As Needed

Cisco.com

- **As needed**—Easy, quick, but hard to track over time
- **Easy to forget why a tunnel is in place**
- **Inter-node BW requirements may change, tunnels may be working around issues that no longer exist**
- **Link protection pretty straightforward, node protection much harder to track**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

299

Full Mesh

Cisco.com

- **Put a full mesh of TE tunnels between routers**
- **Initially deploy tunnels with 0 bandwidth**
Or according to a traffic matrix (Netflow, etc.)
- **Watch tunnel interface statistics, see how much bandwidth you are using between router pairs**
Tunnels are interfaces—use IF-MIB!
Make sure that ? tunnel BW <= ? network BW

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

300

Full Mesh

Cisco.com

- Some folks deploy full mesh just to get router-to-router (pop-to-pop) traffic matrix
- Largest TE network ~80 routers full mesh (~6400 tunnels)
- As tunnel bandwidth is changed, tunnels will find the best path across your network

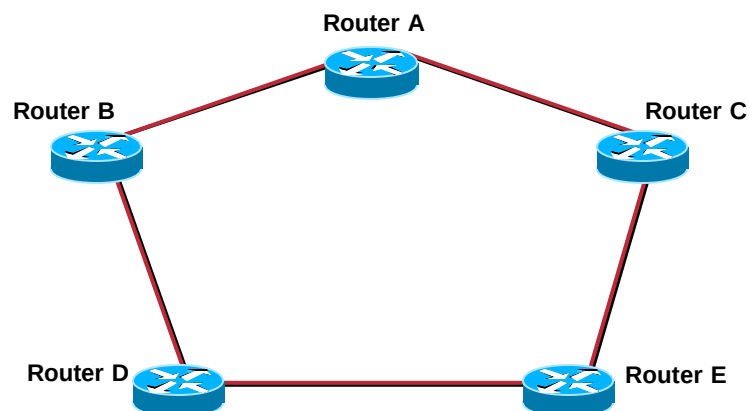
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

301

Full Mesh

Cisco.com

- Physical topology is:



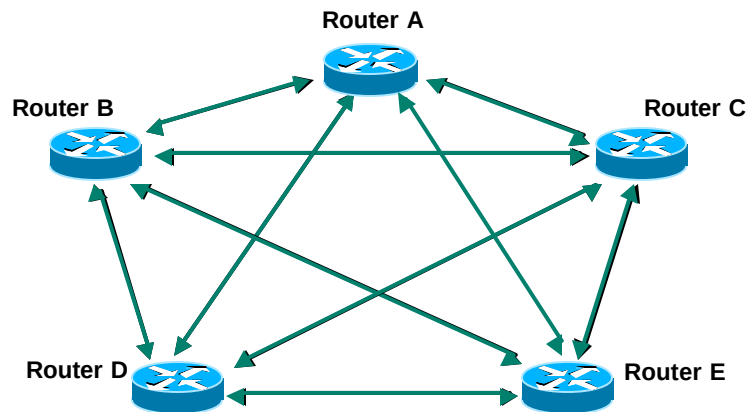
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

302

Full Mesh

Cisco.com

- Logical topology is*
*Each link is actually 2 unidirectional tunnels
- Total of 20 tunnels in this network



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

303

Full Mesh

Cisco.com

- Things to remember with full mesh
 - N routers, $N*(N-1)$ tunnels
 - Routing protocols are **not** run over TE tunnels—
unlike an ATM/FR full mesh!
 - Tunnels are **unidirectional**—this is a
good thing
 - ...Can have different bandwidth reservations in two
different directions

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

304

Full Mesh

Cisco.com

- **Best practices for full mesh:**
 - Periodically re-optimize tunnels based on need (just like an ATM network)**
 - Use a combination of online (router-based) and offline (topology calculation) tools**
 - Node protection more practical in a full-mesh, offline-generated TE topology**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

305

Full Mesh

Cisco.com

- **What tools are available to help me?**
 - Cisco's upcoming TunnelVision (see later), along with the Bandwidth Protection Tool to calculate backup paths**
 - WANDL, OpNet, other modeling tools support MPLS-TE**
 - Adapt your existing ATM design tools to MPLS-TE**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

306

Deploying and Designing

Cisco.com

- Deployment methodologies
- **Scalability**
- Management
- Security

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

307

Scalability

Cisco.com

How Many Tunnels on a Router?

Code	Number of Head-End Tunnels	Number of Mid-Points	Number of Tails
12.OST	600	10,000	5,000

- Tests were done on a GSR
- RSP4, RSP8, VXR300, VXR400 will be similar

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

308

Scalability

Cisco.com

- Largest TE network today = 80 routers, ~6400 tunnels full mesh
- 12.0ST—600 head-ends, 360,000 tunnels full mesh with 10,000 tunnels per midpoint
- $600 = 80 * 7.50$
Or $(360,000 = 6400 * 56)$ if you're in marketing
- Bottom line: MPLS-TE is not a gating factor in scaling your network!

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

309

Scalability

Cisco.com

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st14/scalable.htm>

- Or just search CCO for “Scalability Enhancements for MPLS Traffic Engineering”

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

310

Deploying and Designing

Cisco.com

- Deployment methodologies
- Combining VPN+TE
- Scalability
- **Management**
- Security

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

311

Traffic Engineering MIBs

Cisco.com

- Interfaces MIB
- MPLS-TE-MIB
- CISCO-TE-MIB
- MPLS-DS-TE-MIB

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

312

MPLS-TE-MIB

Cisco.com

- **Goal: Exposes MPLS TE tunnels**
 - Configured tunnel heads and path(s)**
 - Active path(s)**
 - Back-up/stand-by path(s)**
 - Traps**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

313

MPLS-DS-TE-MIB

Cisco.com

- **Goal: Exposes DiffServ-Aware traffic engineering parameters**
- **Extends the MPLS-TE-MIB and MPLS-LSR-MIBs**
- **Work still in progress: Presented version 00 in Minneapolis IETF meeting (March 2001)**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

314

Cisco-TE-MIB

Cisco.com

- Exposes non-standardized TE features such as additional CSPF extensions, auto-bandwidth tunnels, link/node protection, path options, etc., etc...
- Other vendors have similar proprietary MIBs

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

315

TunnelVision

Cisco.com

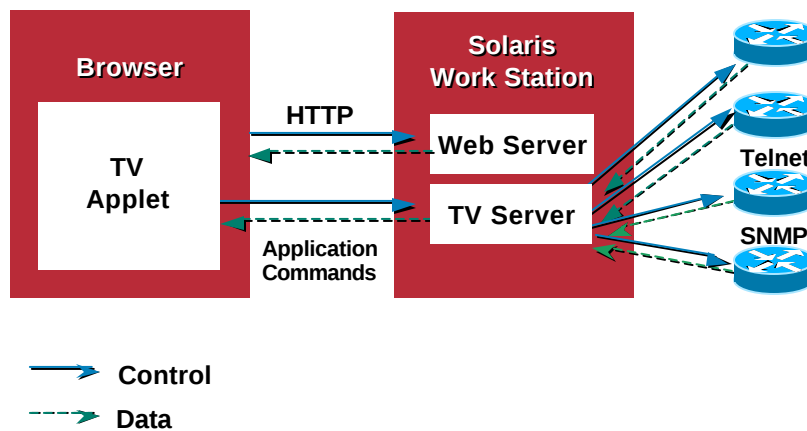
- Need a tool to help manage TE LSPs?
- TunnelVision (server and client component, will run on Solaris and Windows 2000)
- Not a network modeling tool!
Use WANDL, Orchestream, MakeSys, Opnet, and others

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

316

TunnelVision Architecture

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

317

TunnelVision + BPT

Cisco.com

- **Bandwidth Protection Tool**—to calculate placement of link/node protection tunnels
- Cisco is working with an external partner with world-class algorithm experience to build an efficient topology generation tool
- Goal is 10,000 routers, 32-degree connectivity, 16 parallel links, protection topology generated in minutes

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

318

TunnelVision + BPT

Cisco.com

- TunnelVision is the designated front-end for the Bandwidth Protection Tool
- TV determines the topology, BPT builds backup paths

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

319

Deploying and Designing

Cisco.com

- Deployment methodologies
- Scalability
- Management
- **Security**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

320

Security

Cisco.com

- **MPLS-TE is not enabled on externally facing interfaces**
- **Biggest security risk is spoofed RSVP**
 - Hacker would have to know a lot about your topography to do anything
 - RSVP authentication exists (rfc2747), not yet implemented, on the radar
- **If you're concerned about spoofed RSVP, then add RSVP to the ACLs you probably already use to stop spoofed BGP, OSPF, etc.**
- **uRPF also helps here**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

321

Conclusion

Cisco.com

- **TE is cool**
- **You should use lots of it**
- **It will make you popular**
- **It also cures leprosy, rickets, and tennis elbow!**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

322



Cisco.com

MPLS VPN Services

Section 5

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 323



Cisco.com

Making the Case for MPLS VPN Services

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 324

Agenda

Cisco.com

- **Introduction: What Do I Do with This Technology?**
- **Service Opportunities**
- **Site-to-Site**
- **Redundancy**
- **Extranet**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

325

Agenda

Cisco.com

- **Central Service**
- **Internet Access**
- **Remote Access**
- **Inter-AS vs Carrier Supporting Carriers**
- **Differentiated Service**
- **SLA Management**
- **Network Management and Provisioning**
- **Security**
- **Summary**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

326



Cisco.com

What Do I Do With This Technology?

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 327

What Do I Do With This Technology?

Cisco.com

- **Service Provider Perspective**
 - Scalability
 - Reduce complexity
 - Price point
- **End customer perspective**
 - Site to site
 - Bandwidth
 - Quality of service
 - Security
 - Service at an attractive price

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 328



Cisco.com

Service Opportunities

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 329

Service Opportunities

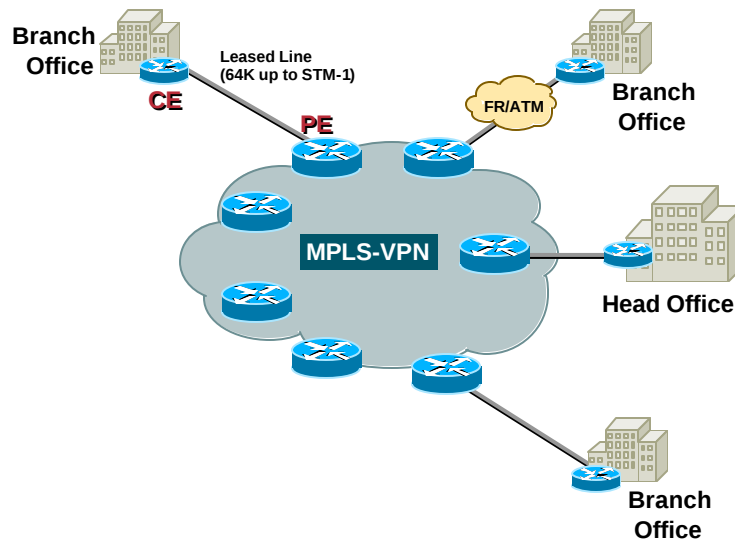
Cisco.com

- **Topological Considerations**
 - Site-to-site
 - Redundancy
 - Extranet
 - Central service
 - Internet access
 - Remote access
 - Inter-AS vs CsC

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 330

Basic Site-to-Site Intranet VPN

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

331

Site-to-Site Intranet VPN Summary

Cisco.com

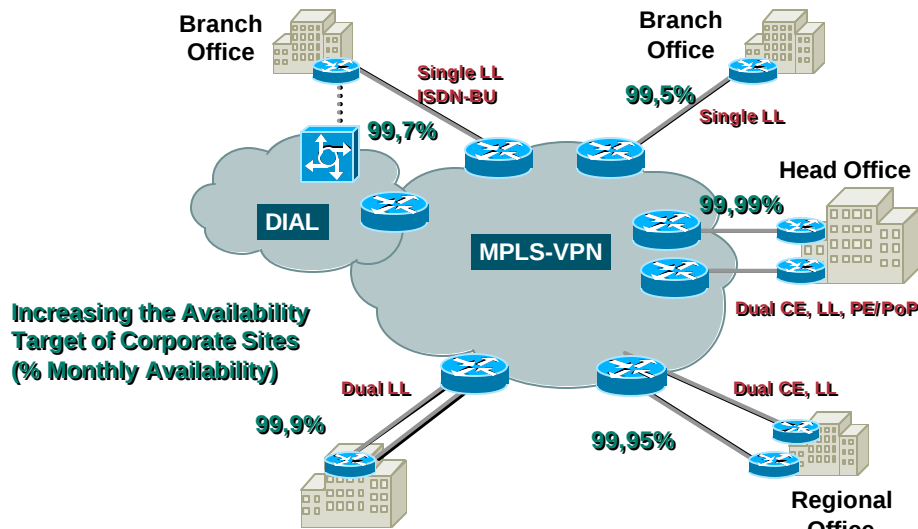
- Managed CPE (often but does not have to be)
- Positioning with LAN-I/FR
- Dimension VPNs: small/medium/large
- IGP—either IS-IS or OSPF
- Routing protocol between PE-CE either BGP-4, RIPv2, static or OSPF
- Route distinguisher—unique per VPN
- Address overlapping (non-unique VPNs)
- Basic QoS CE-PE

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

332

Redundancy

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

333

Redundancy Summary

Cisco.com

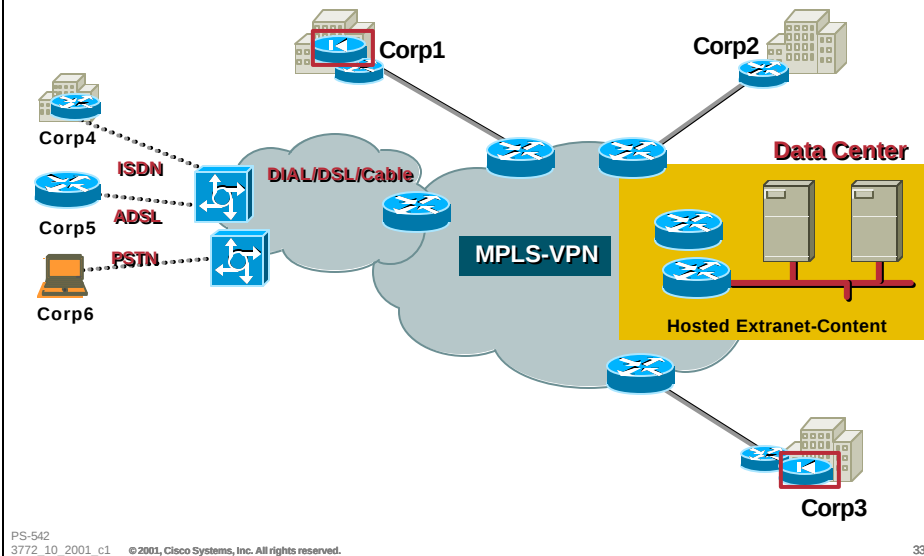
- Drivers—customer wants resilience options from Service Provider
- Typically regional—HQ
- Dual access lines
- Dual access lines and dual CE
- Dual access lines in dual CE connecting to dual PoPs
- Unique RD per VRF for iBGP load-balancing

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

334

Managed Extranet (Single-Provider)

Cisco.com



MPLS/VPN Extranet Support

Cisco.com

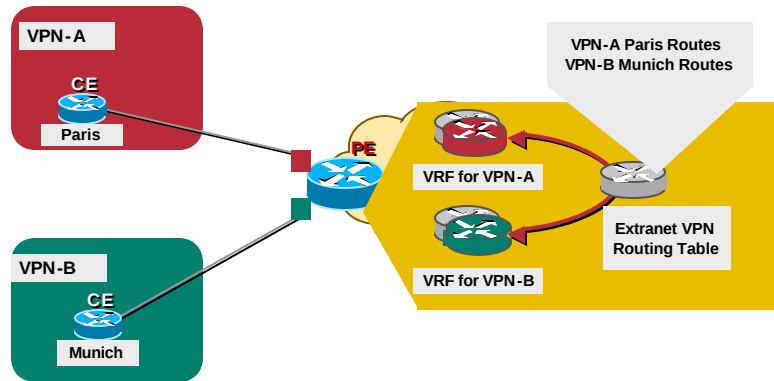
- Extranet support is simply the import of routes from one VRF into another VRF which services a different VPN
- Controlled through the use of route target
If we import the route, we have access
- Various topologies are viable using this technique

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

336

MPLS/VPN Extranet Support

Cisco.com



Sharing of VPN Information between VRFs Provides Extranet Support

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

337

Extranet Summary

Cisco.com

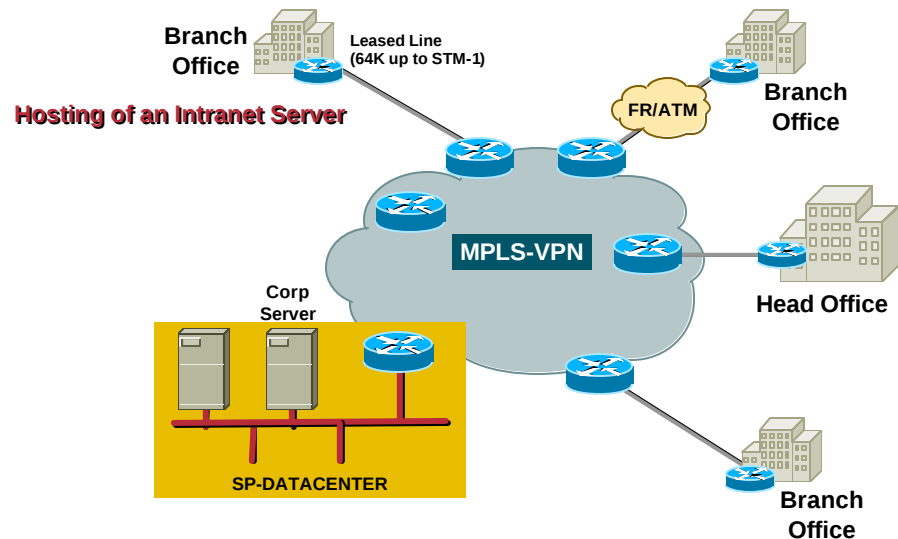
- **Service Provider motivation**
 - All sites from various companies participating in Extranet to be connected to Service Provider network**
 - Manage end-to-end service level agreement**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

338

Central Services

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

339

Central Services Model

Cisco.com

- **Common topology is central services VPN**
Client sites may access central services but may not communicate directly with other client sites

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

340

Central Services Summary

Cisco.com

- **Service Provider Opportunity**

Offer end customers the possibility to host some of their servers in a Service Provider data center

Server may be dedicated or shared

Lower cost hosted services for the service provider

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

341

Internet Access

Cisco.com

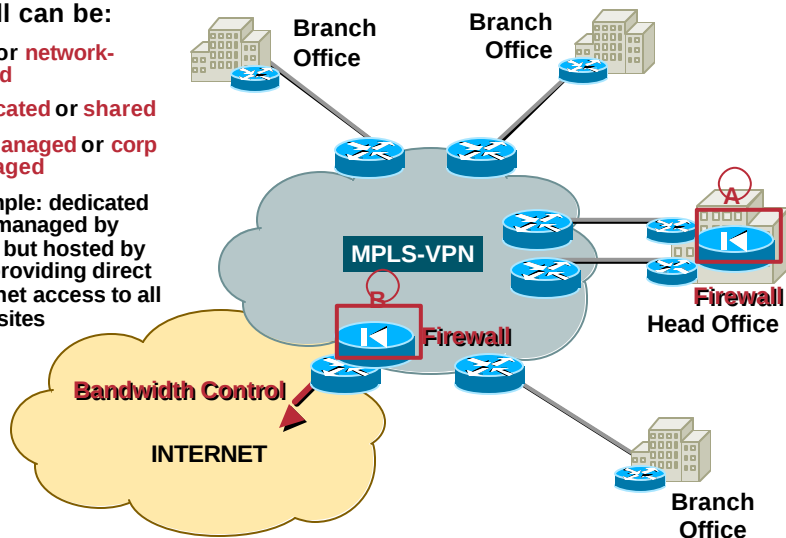
- **Firewall can be:**

CPE or network-based

Dedicated or shared

SP managed or corp managed

Example: dedicated FW, managed by Corp but hosted by SP, providing direct Internet access to all VPN sites



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

342

Internet Access Concepts

Cisco.com

- **Factors for service provider to consider**
 - Customer with no NAT/no Firewall requirements
 - Customer with NAT, but no Firewall requirements
 - Customer with Firewall, but no NAT requirements
 - Customer with NAT and Firewall requirements
 - Central vs distributed—who is responsible for these?
 - End customer expects a service offering
 - Note: Security requirements between Intranet and Internet

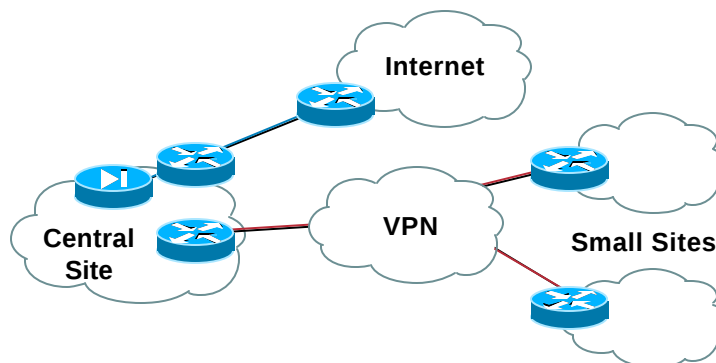
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

343

Internet Access Existing Customer Requirements

Cisco.com

- **What do customers have at the moment?**
 - A secure private network via VPNs or leased lines
 - One or more secure connections to the Internet



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

344

Internet Access: Possible Implementation Scenarios

Cisco.com

- Simple solution
- VPN to Internet via subinterfaces
- Single Router and managed firewall gateway

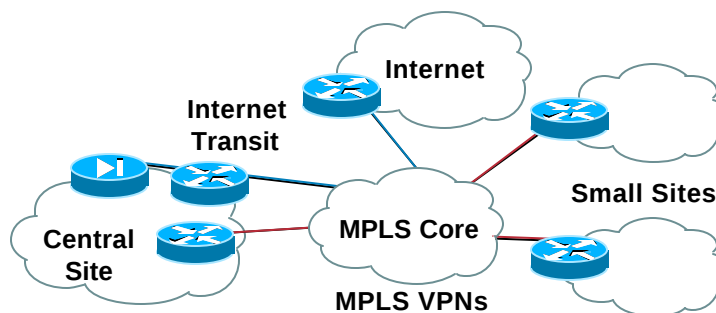
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

345

Internet Access: Simple Solution

Cisco.com

- Advantages of the simple solution

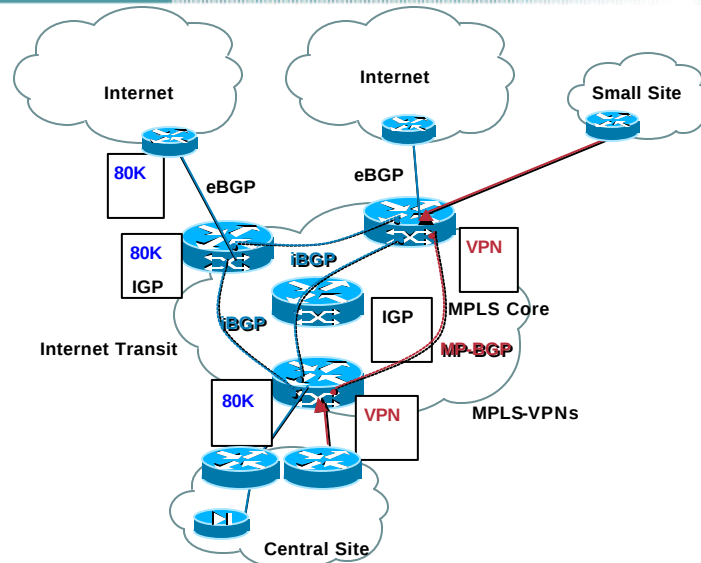


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

346

Internet Access: Simple Solution

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

347

Internet Access: VPN to Internet Via Subinterfaces

Cisco.com

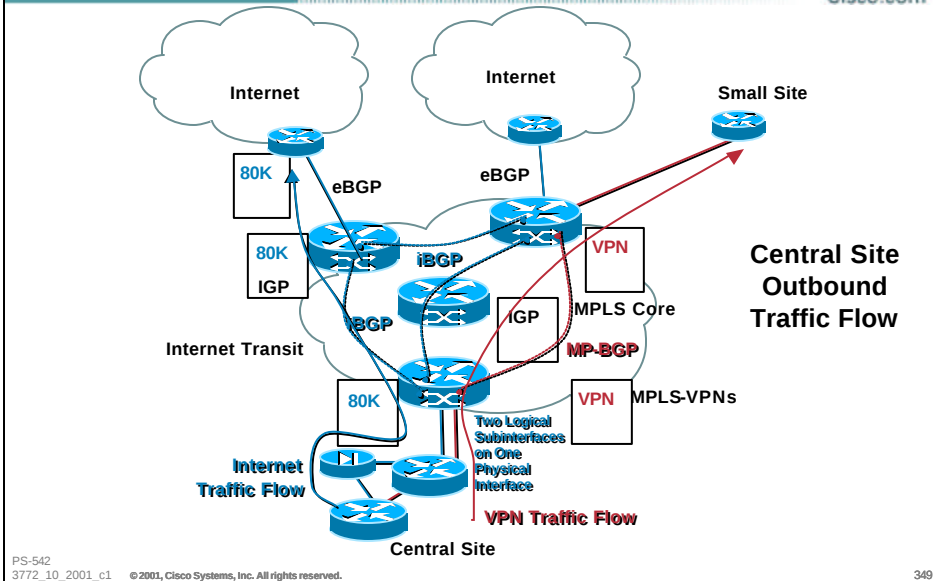
- Sub optimal routing in Service Provider core network
- Full Internet routing table available at central Site CE
- Two logical subinterfaces which might incur additional costs
- Central site needs to differentiate between Internet and VPN traffic

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

348

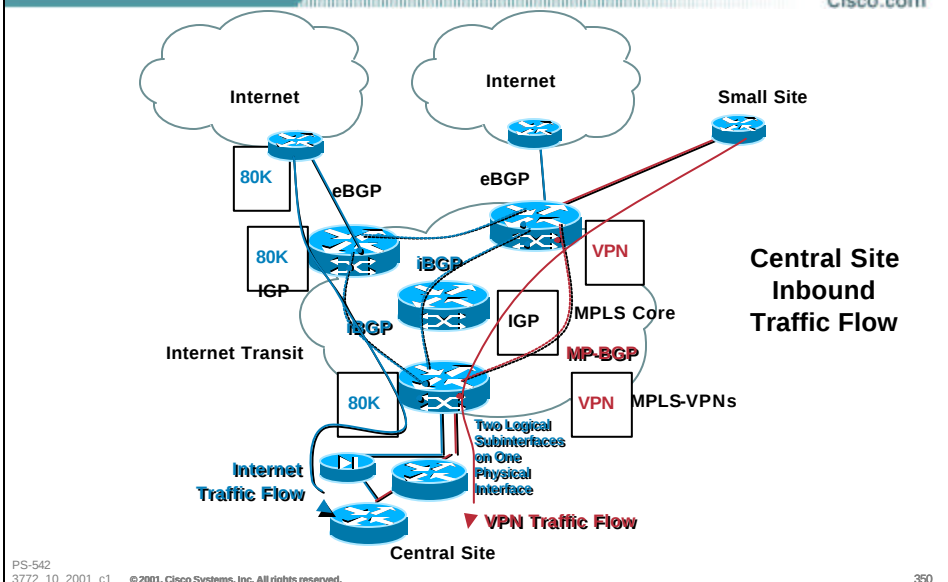
Internet Access: VPN to Internet Via Subinterfaces

Cisco.com



Internet Access: VPN to Internet via Subinterfaces

Cisco.com



Internet Access: Single Router and Managed Firewall Gateway

Cisco.com

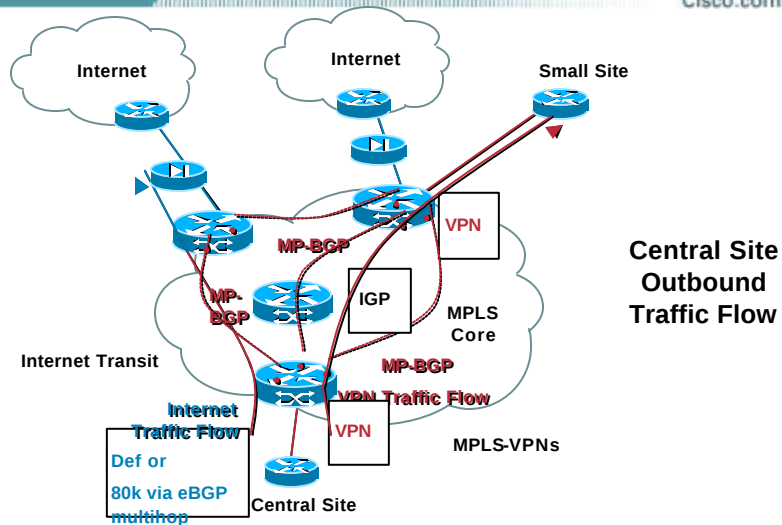
- Service Provider supplies managed firewall service
- Only single VPN connection between each customer site and Service Provider network required
- Provides a gateway from the VPN to the global routing table so the first non-VPN router can be any PE router in the MPLS core
- Full Internet routing table available to customers using eBGP multihop peering to external Internet PE router
- Allows for optimal routing with minimum hops through MPLS core

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

351

Internet Access: Single Router and Managed Firewall Gateway

Cisco.com

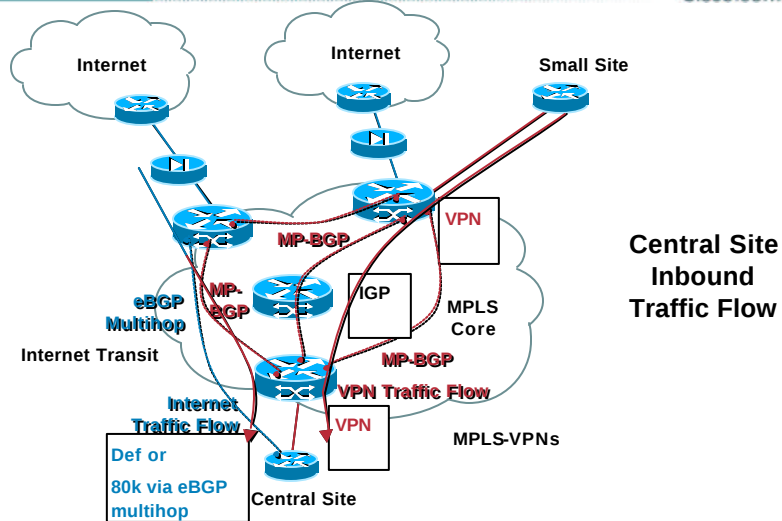


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

352

Internet Access: Single Router and Managed Firewall Gateway

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

353

Internet Access: Scenario Review

Cisco.com

- Simple Solution
Recommend
- VPN to Internet via Subinterfaces
Recommend
- Single Router Managed Firewall Gateway
Recommend
- Different Solutions Appropriate for the individual requirement

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

354

Internet Access Summary

Cisco.com

- **Service Provider opportunity**

Provide end customer option to buy Internet connectivity for corporate VPN

CPE-based Firewall all VPN sites send traffic to a specific customer site where centralized customer or service provider managed firewall is located

Network based Firewall all corporate VPNs have direct Internet access via network-based firewall (could be dedicated)

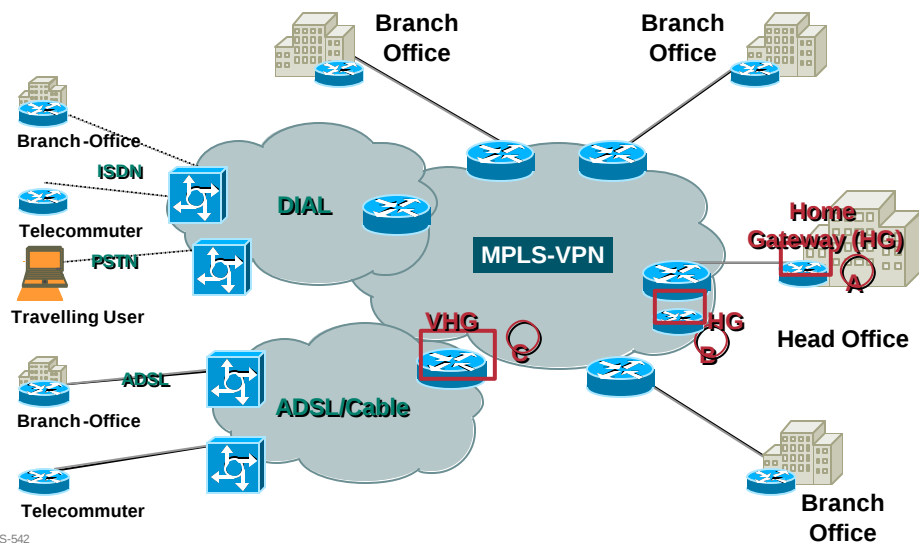
Extend value-add for “basic” site-to-site services

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

355

Remote Access PSTN, ISDN, Cable...

Cisco.com

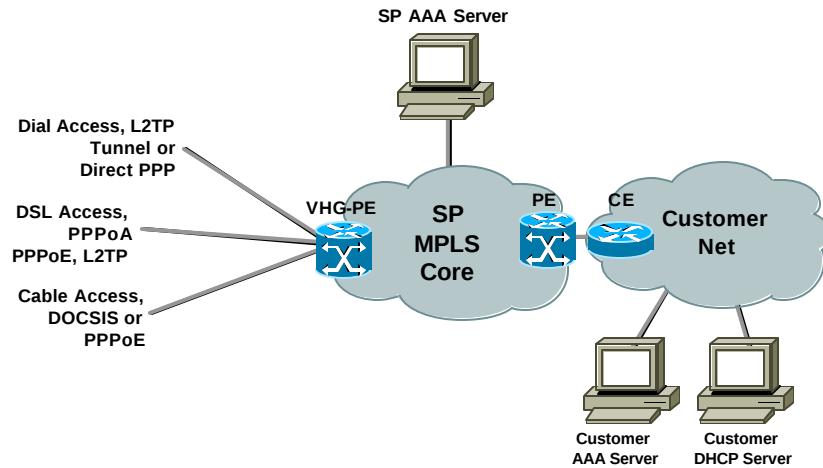


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

356

Remote Access

Cisco.com

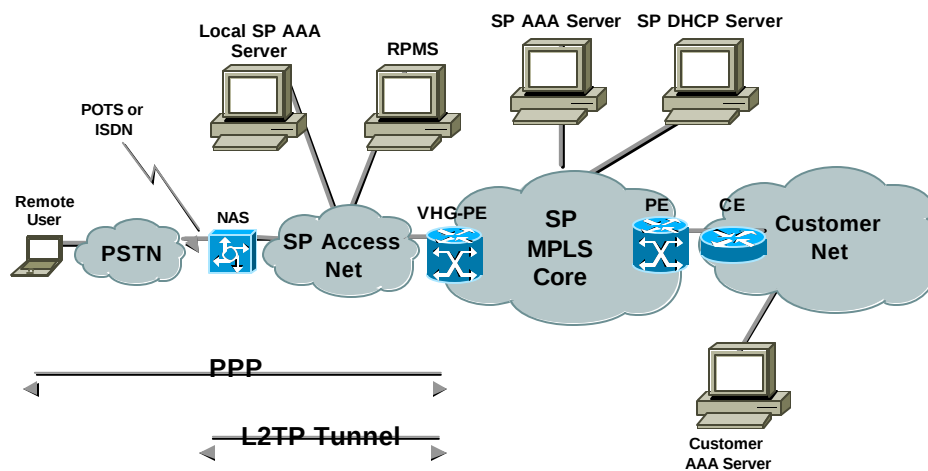


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

357

Remote Access: L2TP to MPLS VPN Integration

Cisco.com

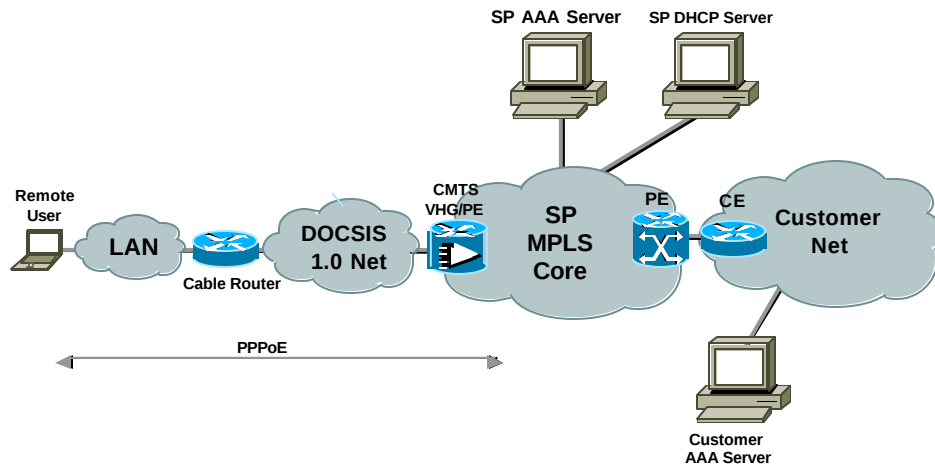


PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

358

Cable: PPPoE to MPLS VPN Integration

Cisco.com



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

359

Remote Access Summary

Cisco.com

- **Service Provider opportunity**
 - Provide customer alternative access methods as not all customers can afford a dedicated VPN connection
 - Small sites (LAN-based) via ISDN/ADSL/Cable
 - Solution for small sites, traveling users and telecommuters

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

360

Inter-AS vs CsC

Cisco.com

- **Methods of extending MPLS-VPN services across geographical boundaries as well as providing scalable VPN services**
- **Providers want to build VPNs with other providers, “VPN-Peering” (Inter-AS)**
- **Service Provider wants to develop international VPN service with its subsidiaries (Inter-AS)**
- **Service Providers may want to deliver services to ISPs who do not run MPLS, but these ISPs want to provide VPN services to its end customers (CsC—Hierarchical VPNs)**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

361

Inter-AS vs CsC

Cisco.com

Fact is that MPLS-VPN works with a single Autonomous System Number (ASN) only

- **Peer-to-peer topologies**
 - MPLS VPN spanning several autonomous systems (Inter-AS VPN)**
 - MPLS VPN in a BGP confederation**
- **Client-server topologies**
 - ISP or MPLS VPN provider is a customer of another MPLS VPN provider (Carrier’s Carrier model—Carriers Supporting Carriers—CsC)**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

362

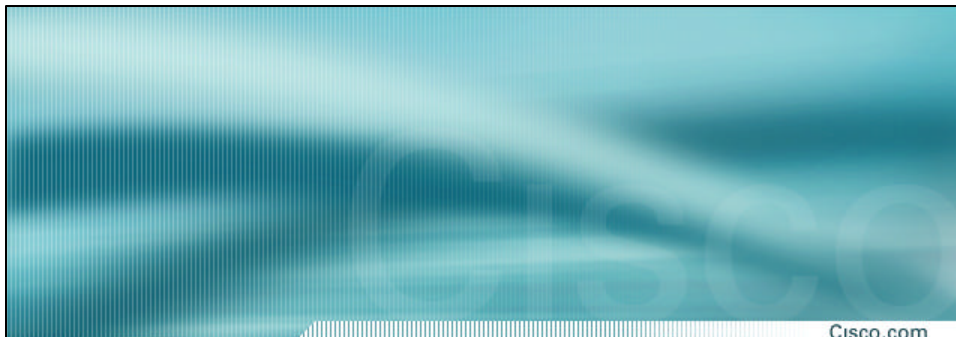
Inter-AS vs CsC Summary

Cisco.com

- **Service provider can build an international MPLS-VPN service with its subsidiaries**
- **Service Providers may have VPN peering agreements**
- **Mechanism to deliver services to other customer ISPs who wish to offer VPN services to its end customers**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

363



Cisco.com

Differentiated Services

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

364

Differentiated Services

Cisco.com

- Requirement to provide application aware service, e.g. Multiple Class of Services (CoS)—delay and loss tolerance factors
- Example types: “Business Class”
 - Gold : Real-time applications like Voice over IP
 - Silver: Mission critical data, e.g. SNA/SAP
 - Bronze: “Best-effort,” e.g., E-mail
- End customer specifies to Service Provider Ingress Committed Rate (ICR) as well as Egress Committed Rate (ECR) per site and per service class

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

365

Differentiated Services

Cisco.com

- Service Provider: Uses end-to-end QoS mechanisms to guarantee performance of customers' vpn applications
- Combination of DiffServ and traffic engineering capabilities in core
- Ability to offer SLAs per application
- Solutions:
 - Traffic engineering helps manage SP BW
 - CoS (DiffServ) helps SP to offer differentiated services in the backbone
 - TE+ CoS = Guaranteed bandwidth
 - Guaranteed bandwidth can help SP to offer delay as a QoS

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

366

SLA Management

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

367

SLA Management

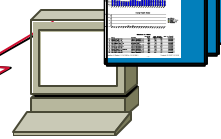
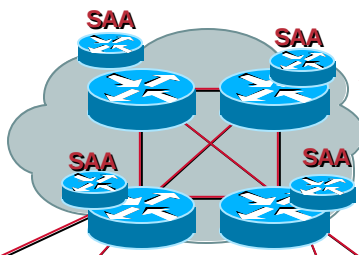
- SAA Benefits**

Standardly available
in Cisco IOS

Leverages large
installed base of
Cisco routers

Measures delay,
jitter, packet loss
and availability per
Class of Service

CPE



Response Time
Matrix Per VPN

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

368

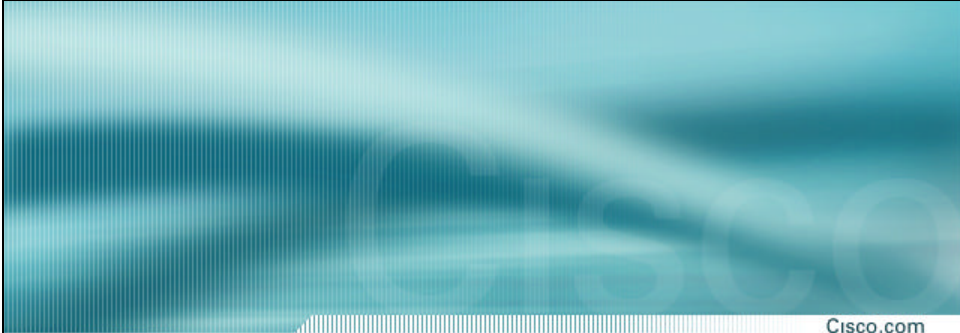
SLA Management Summary

Cisco.com

- End customers want to know guarantees in Service Levels
- As the Service Provider charge model advocates differentiated services, a method for managing these service levels is required
- Failure to meet service levels results in penalty payments to the end customer
- “Intelligent—Real-Time” SLA management is required by the end customer

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

369



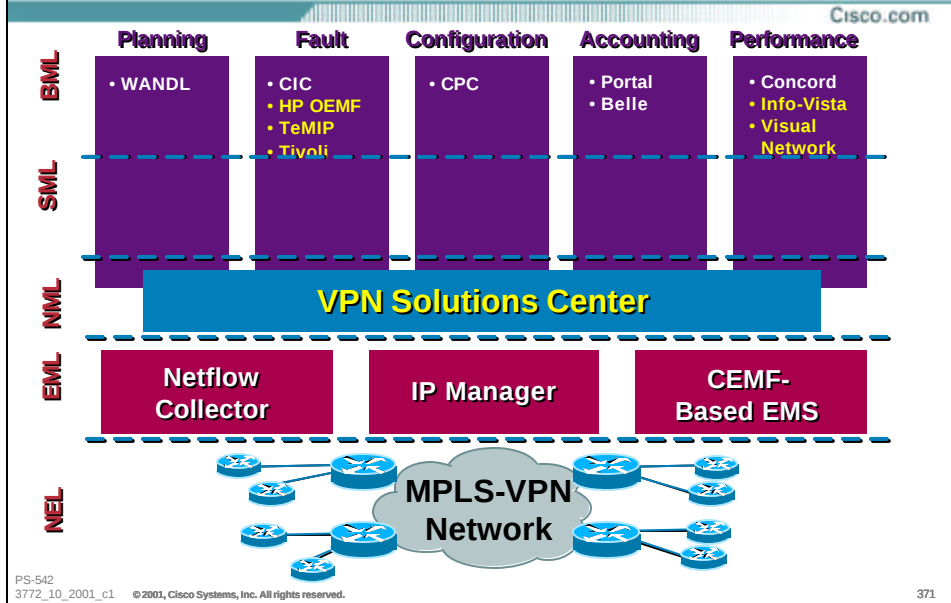
Network Management and Provisioning

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

370

Network Management and Provisioning



Network Management and Provisioning VPN SC

- Automatic generation of VPN Cisco IOS commands
- Just in time provisioning
- Manages IP addresses, RD and RT values and VRF's
- Auditing of both configuration and routing to verify VPN connectivity
- Managed and unmanaged VPN support
- Automatic management VPN provisioning

Network Management and Provisioning VPN SC

Cisco.com

- **Formation of routing communities for VPN connectivity**
- **Allows provisioning of arbitrary mesh without knowledge of BGP**
- **Auto picks values for route targets once communities are specified**
- **Hub and spoke and full mesh topology support**
- **Extranet provisioning**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

373

Network Management and Provisioning

Cisco.com

- **VPN SC automatically provisions the management VPN as an extranet to the customer network**
- **Route filtering on the PE is used to allow only one loopback and the PE-CE subnet or the PE-CE subnet into the MCE's routing table for connectivity to the CE**
- **All customer CE's are spokes to the management VPN**
- **Customers VPN privacy maintained**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

374

Network Management and Provisioning

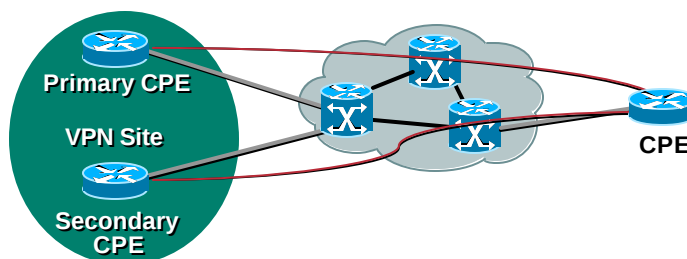
Cisco.com

- **Redundancy support**

Provision a secondary redundant device in a VPN Site

The secondary CPE may use a floating static route for fail over to other VPN peers

The dual homed connection for the secondary CPE may be used to load balance to the VPN site



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

375

Network Management and Provisioning

Cisco.com

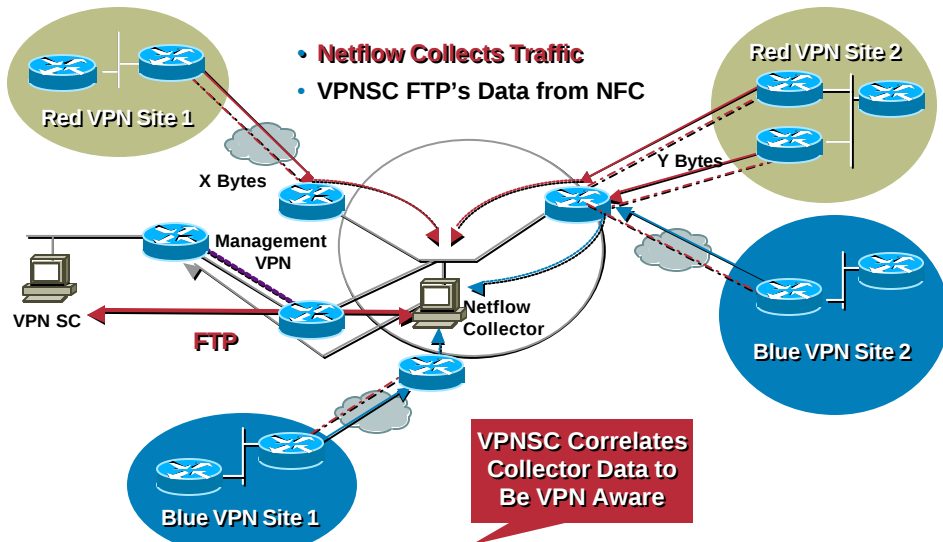
- **VPNSC can produce VPN aware accounting reports using Netflow collector**
- **VPNSC has repository of VPN information and correlates using Netflow data**
- **VPNSC has accounting API's for partners or an OSS to retrieve the data**
- **VPNSC data can be used by billing partners for usage based billing or capacity planning**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

376

Network Management and Provisioning

Cisco.com



PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

377

Network Management and Provisioning

Cisco.com

- **Populate the IP address to I/F mapping**
Use I/F Mib collection
- **Collect from the collectors**
Gather the flow data
- **Collect router VPN info**
Gathers VPN data
- **Create the VPN traffic matrix**
Correlates the flow data to VPN's

PS-542

3772_10_2001_c1

© 2001, Cisco Systems, Inc. All rights reserved.

378

Network Management and Provisioning

Cisco.com

- CE to CE traffic volume bytes, packets
- PE to PE traffic volume bytes, packets
- PE to CE traffic volume bytes, packets
- Traffic per COS
- PE to PE reports for all customers
- CE to CE reports for each customer
- Customer site to customer site report
- Traffic breakdown by application type and type of service
- Charting also available

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

379

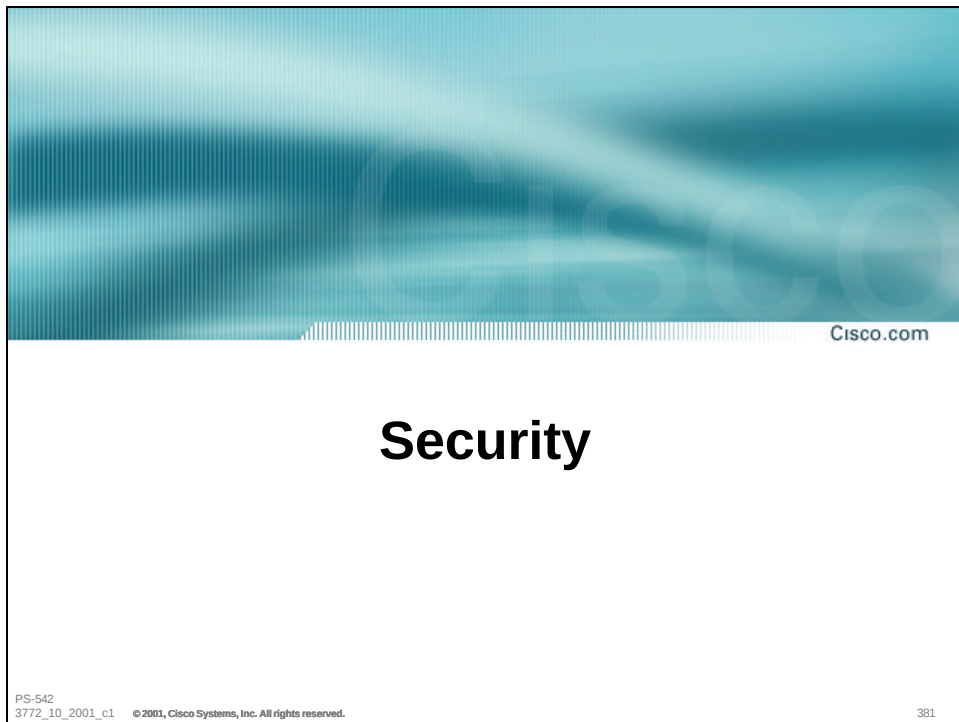
Network Management and Provisioning Summary

Cisco.com

- Most significant application for the service provider is the ability to manage and provision its service
- This capability must be scalable, e.g., carrier class model
- The network management and provisioning architecture permits the management and provisioning of MPLS-VPN services

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

380



Security

- **MPLS provides full address and traffic separation as in traditional layer-2 VPN services**
- **It hides addressing structures of the core and other VPNs**
- **It is also not possible to intrude into the MPLS core if this is properly secured**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 382

Security

Cisco.com

- **MPLS itself does not provide encryption, integrity or authentication services**
- **If these are required IPsec should be used over the MPLS infrastructure**
- **The same applies to ATM and Frame Relay**
- **Also here IPsec can provide these missing services**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

383

Security

Cisco.com

- **What MPLS doesn't provide**
 - Protection against mis-configurations of the core and attacks "within" the core**
 - The security mechanisms discussed here assume correct configuration of the involved network elements on the MPLS core network (PE and P routers)**
 - Deliberate or inadvertent misconfigurations from SP staff may result in undesired behavior including severe security leaks**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

384

Security Summary

Cisco.com

- **To avoid the risk of mis-configurations**
 - Configuration tools
 - Well-trained Staff
- **To avoid the risk of "internal" attacks the MPLS core network must be properly secured**
- **This includes**
 - Network element security
 - Management security
 - Physical security of the service provider infrastructure
 - Access control to service provider installations
 - Other standard SP security mechanisms

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

385

Summary

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

386

Summary End-user Benefits

Cisco.com

- **Any-to-Any Connectivity within the VPN**
- **End-to-End Application-level Quality of Service and SLA's**
- **Support for any access speed to support small, medium and large sites**
- **Security and Privacy equivalent to FR/ATM**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

387

Summary End-user Benefits

Cisco.com

- **Support for corporate private IP addressing**
- **Leverage the Price/Performance ratio of modern IP Networks**
- **Fully managed Service allowing the corporate to focus on his core business**
- **Integration of Intranet VPN, Access VPN, Extranet VPN and Internet Access**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

388

Summary Service Provider Benefits

Cisco.com

- Scalable architecture that supports thousands of VPN's with thousands of Sites allowing the SP to capture the huge revenue potential of IP-VPN Services
- Low cost, Any-to-Any Connectivity
- Ability to offer strong, application level SLAs
- Supports any access technology and any access speed
- Build Once, Sell many through single routing image for all VPN's

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

389

Summary Service Provider Benefits

Cisco.com

- Easy adds, moves and changes
- Software only upgrade on most Cisco platforms
- Simple, low cost CPE resulting from network based architecture
- Security and privacy equivalent to FR/ATM without requiring expensive and complex encryption

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

390

Summary Service Provider Benefits

Cisco.com

- **Ideal Platform for Value-Added Services through the use of a simple Route Import/Export mechanism per VPN**
- **Centralized Provisioning through VPNSC**
- **Compatibility and Synergies with other VPN Technologies (IPSec)**
- **Standards based Solution allowing VPN Services to cross Service Provider boundaries through Private Peering**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

391

OCP Strategy

Section 6

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

392

Vision

Cisco.com

- **Unified control plane across all platforms and technologies**
- **More intelligent use of bandwidth**
- **Unified network management**
- **Integrated/coordinated recovery across multiple levels**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

393

Vision

Cisco.com

- **Optical cross connects**
- **SONET / SDH Muxes**
- **Routers**
- **Blended products**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

394

A Generalized Control Plane

Cisco.com

- Enable one control plane to handle
 - Label switching
 - ATM VC/VP switching
 - SONET / SDH
 - Lambda switching
 - Waveband switching
 - Port switching

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

395

What We Already Did with IP+ATM

Cisco.com

- Original rational—integrate:
 - Layer 3 routing—scalability and flexibility
 - Layer 2 switching—high-performance and traffic management



- Now architecture for new services...

* LSR . . . Label Switch Router

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

396

Why Extend the Control Plane?

Cisco.com

- **Unified procedures for deploying facilities**
- **New / standardized capabilities for layer 2 technologies**
- **Example: Optical Cross Connect**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

397

Standardization Activities

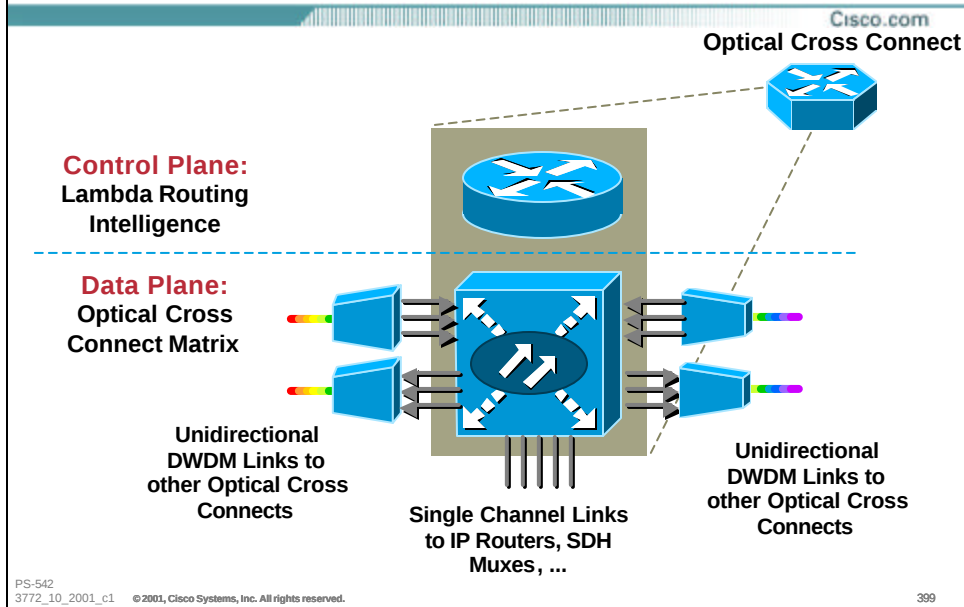
Cisco.com

- **ITU and ANSI T1X1**
G.ason “Automatically Switched Optical Channel Networks (ASON)”
- **OIF Signalling Working Group**
Proposal for Photonic MPLS Network
- **IETF**
Proposal for Generalized Multi-Protocol Label Switching (GMPLS)
OSPF, IS-IS, RSVP, LDP extensions

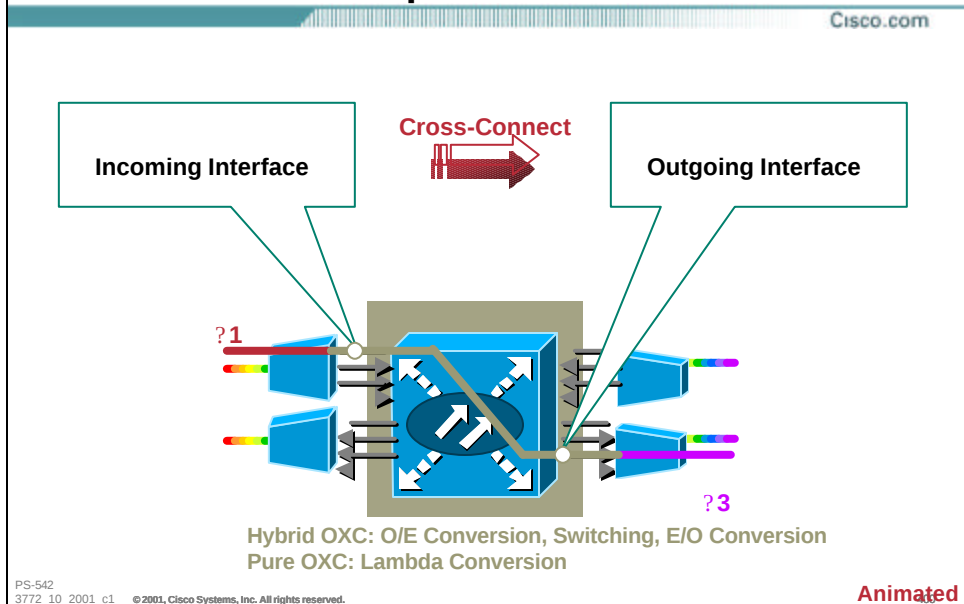
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

398

The Key Element is the Optical Cross Connect

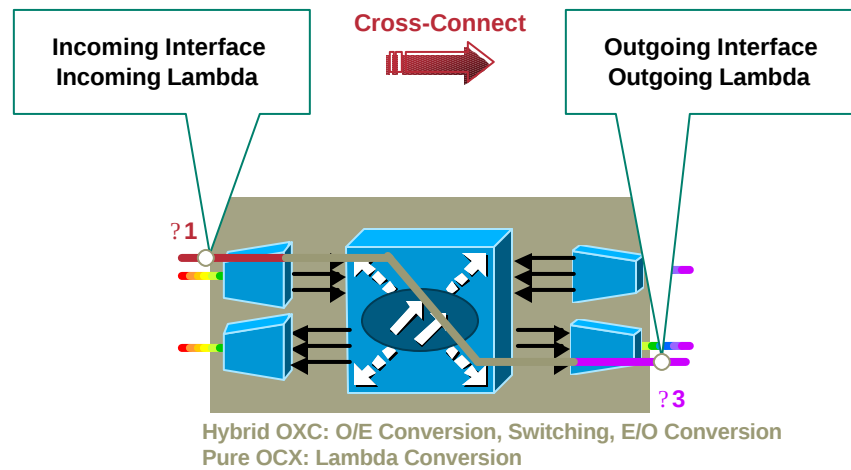


Data Plane First Generation Optical Cross Connect



Data Plane Optical Cross Connect with integrated DWDM

Cisco.com



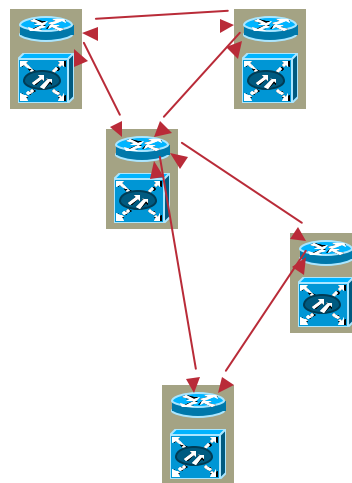
PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

Animated

Control Plane Lambda Routing Intelligence

Cisco.com

- Resource Discovery
- Topology State Maintenance
 - Reliable broadcast
- Path Selection
 - Constraint-based Routing
- Optical Channel Management
 - Path placement
 - Path maintenance
 - Path revocation



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

402

LSR and OXC Similarities

Cisco.com

- **Data vs. Control planes**
they both clearly distinguish these planes
- **Data plane driven by a switching matrix**
LSR: (i_if, ingress **label**) => (o_if, egress **label**)
OXC: (i_if, ingress **?**) => (o_if, egress **?**)
- **Switching is independent of switching unit payload**
LSR/OXC only switch based on Label or Lambda

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

403

Traits common across all circuit types

Cisco.com

- **Explicitly Routed according to constraints**
Bandwidth, priority, pre-emption, policy color, re-optimization
- **Point-to-point**
- **Payload transparency**
- **Survivability properties on a per LSP/ Optical trail basis**
Protection and restoration

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

404

Traits Unique to Certain Circuit Types

Cisco.com

- Bi-directional
- Multicast
- Label range restrictions
- Label encodings
- Restoration capabilities

SONET BLSR

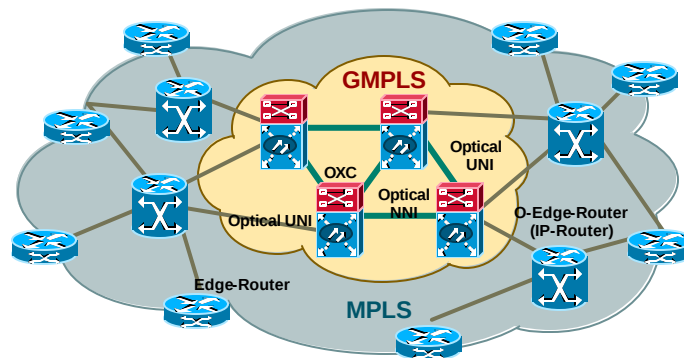
MPLS LSP in LSP

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

405

GMPLS Architecture

Cisco.com

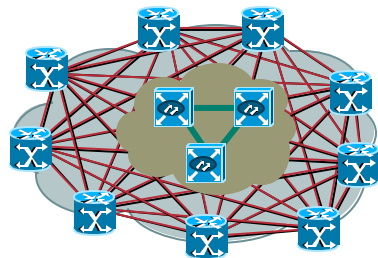


- A unified, open, standard control plane for packets, cells and circuits
- Benefits much more than just transport

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

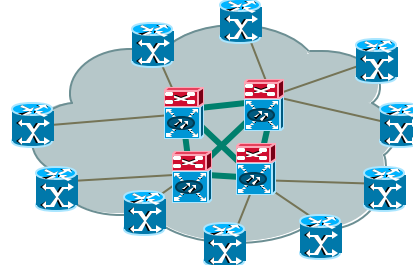
406

Control Domains



Separate control plane instances

Routers
Optical Switches
SDH Muxes (not pictured)



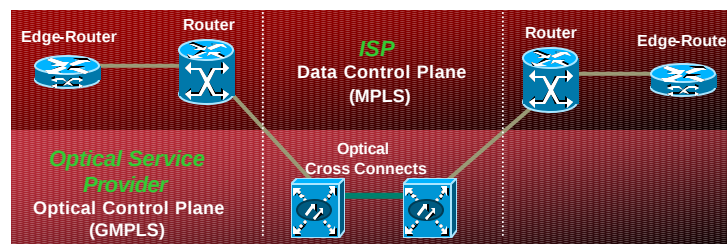
Single control plane inst

Routers
Optical Switches

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

407

Overlay Model



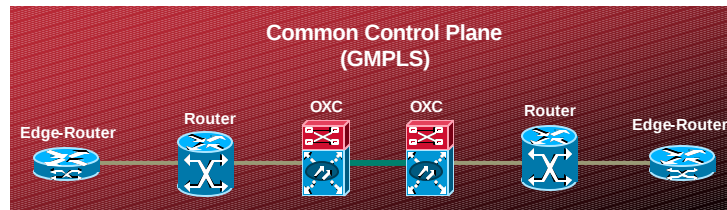
- **Two Administrative Domains**
 - Optical Transport Network
 - Internet Service Provider
- **ISP requests circuits via a UNI interface**
- **OTN uses its own Control Plane for Provisioning**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

408

Peer Model

Cisco.com



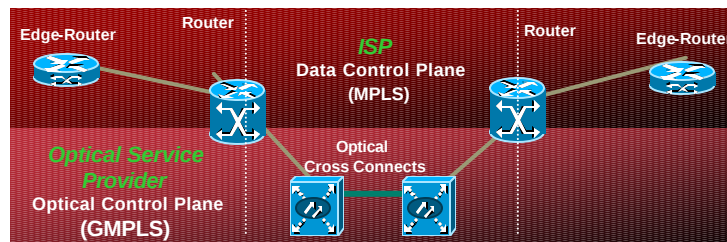
- One Administrative Domain
- Routers and OXCs are Peers
- Common Control Plane for both IP and Optical Transport Networks

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

409

Border Model

Cisco.com



- Two Administrative Domains
 - Optical Transport Network
 - Internet Service Provider
- Border router participates in both

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

410

Communication between layers

Cisco.com

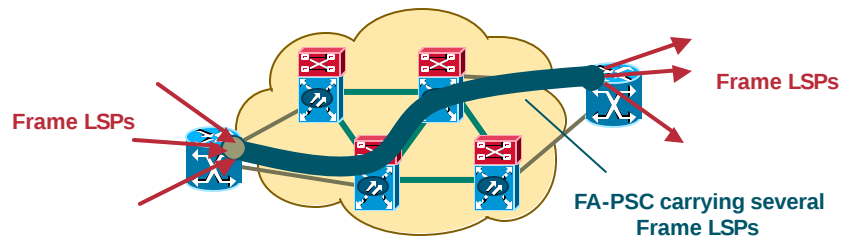
- **Forwarding Adjacency**

Circuit created at one layer is advertised into the IGP of the next higher layer

Note that this may be the same instance of the IGP

At the IP level no routing adjacency is formed

Much more scalable



PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

Animated

Flexible Spectrum

Cisco.com

- **Overlay, Border, Peer models are points along a spectrum**
- **Real issue is how much information and control can cross the interface**
- **Intermediate options exist and have practical value to large providers**

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

412

Summary

Cisco.com

- **Unified Control Plane**
Integrated
Flexible
Standard

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

413

Summary

Cisco.com

- **Integrated**
One control plane across diverse products
Integrated / Coordinated recovery
Potential for truly Integrated Network Management

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

414

Summary

Cisco.com

- **Flexible**

Peer, Overlay, and Border models

Provide organizational choices for

**How various domains share information
and control**

Blended products

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

415



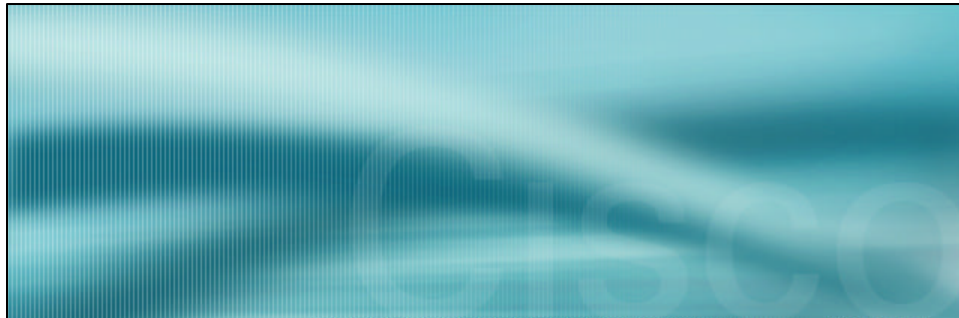
MPLS-Technology Options and Applications

Session PS-542

Cisco.com

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved.

416



Cisco.com

Please Complete Your Evaluation Form

Session PS-542

PS-542
3772_10_2001_c1 © 2001, Cisco Systems, Inc. All rights reserved. 417



CISCO SYSTEMS

EMPOWERING THE
INTERNET GENERATIONSM

PS-542
3186_06_2001_c1_X © 2001, Cisco Systems, Inc. All rights reserved. 418