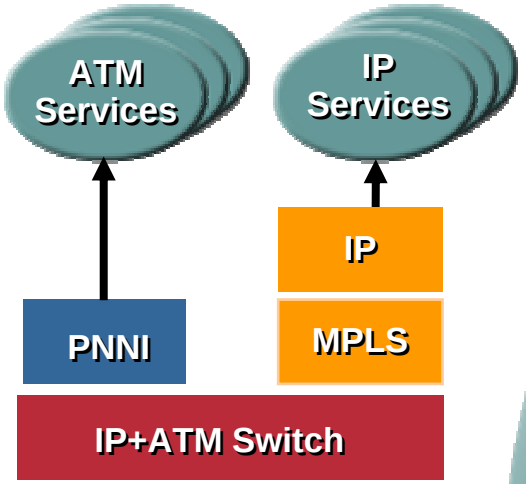
Cisco MPLS - Traffic Engineering for VPNs

Amrit Hanspal
Sr. Product Manager – MPLS & QoS
Internet Technologies Division

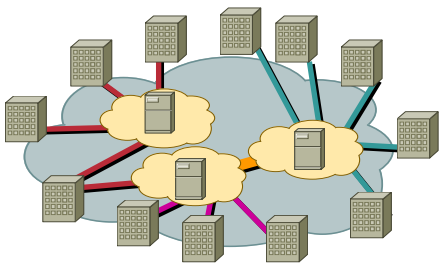
Agenda

- MPLS Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering for VPNs
- Summary

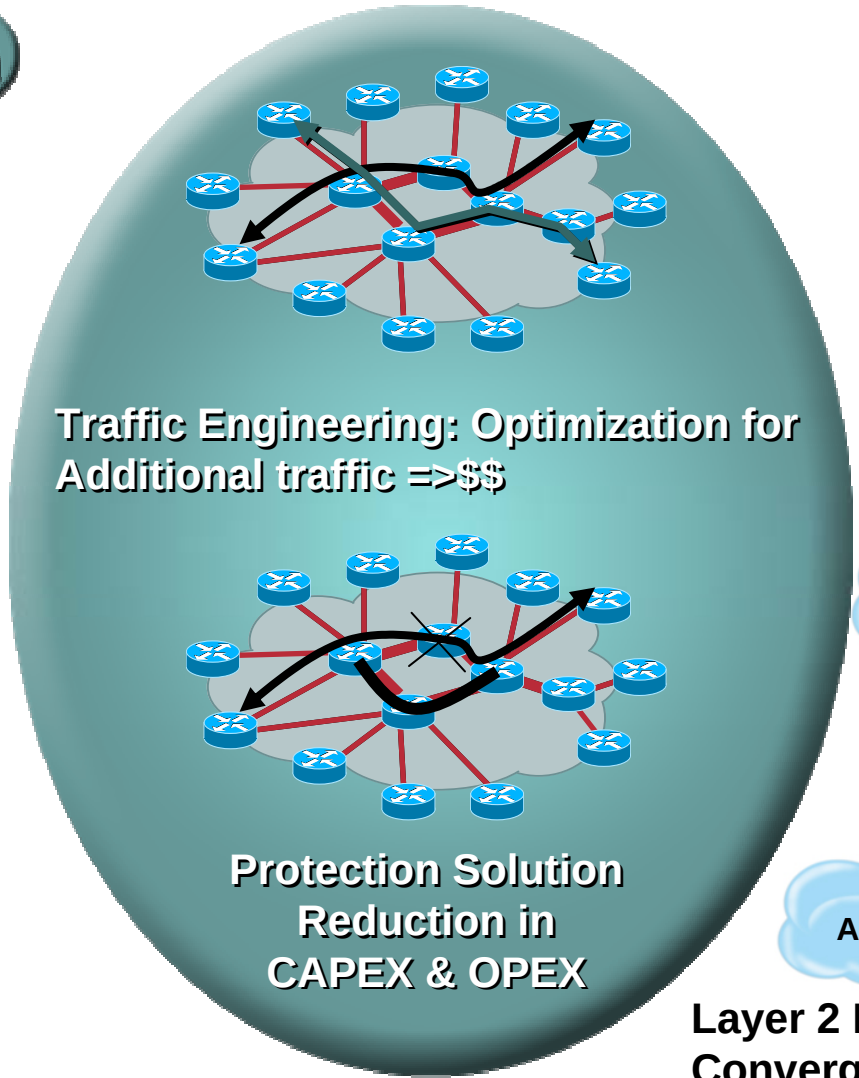
MPLS Is Key technology for Delivery of Layer 2 & Layer 3 Services

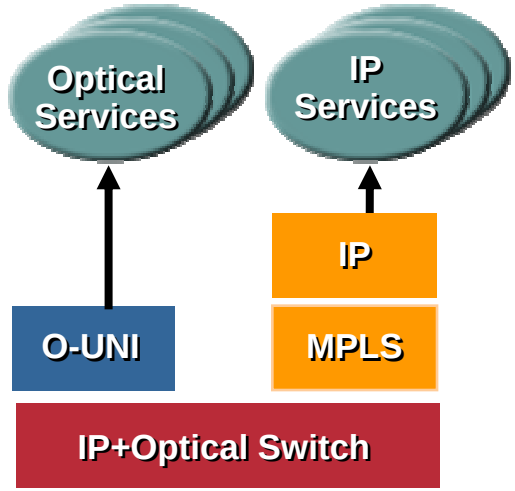


IP+ATM Integration

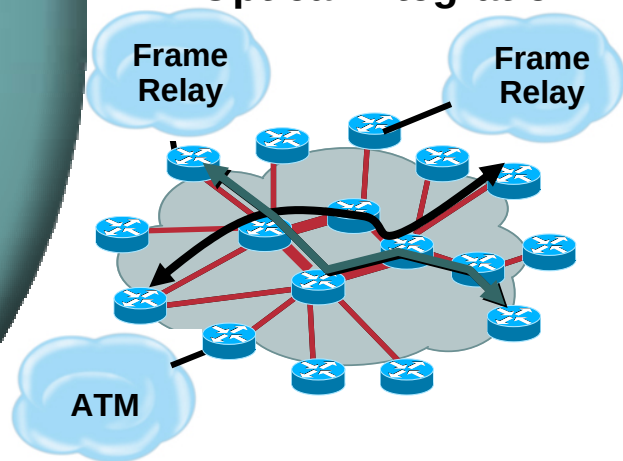


MPLS VPNs: Build Once / Sell Many Network Based VPNs





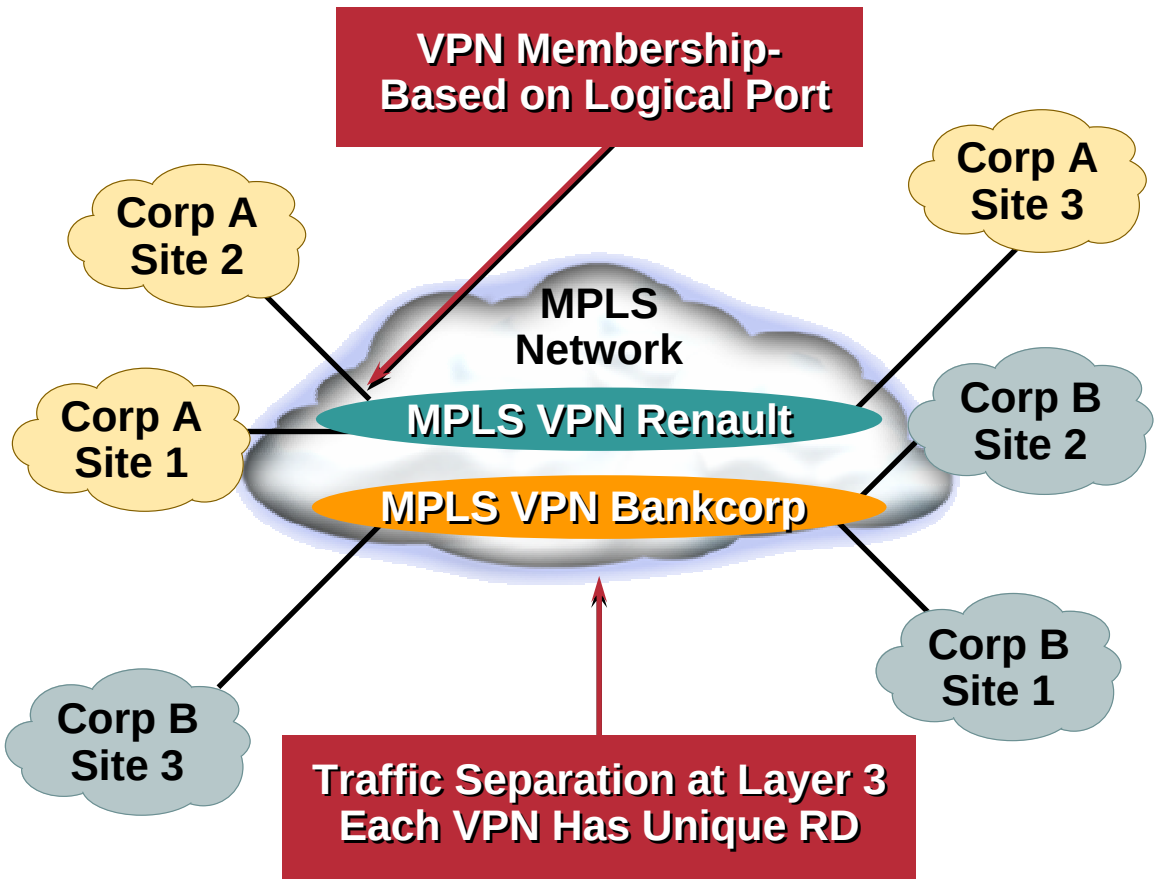
IP+Optical Integration



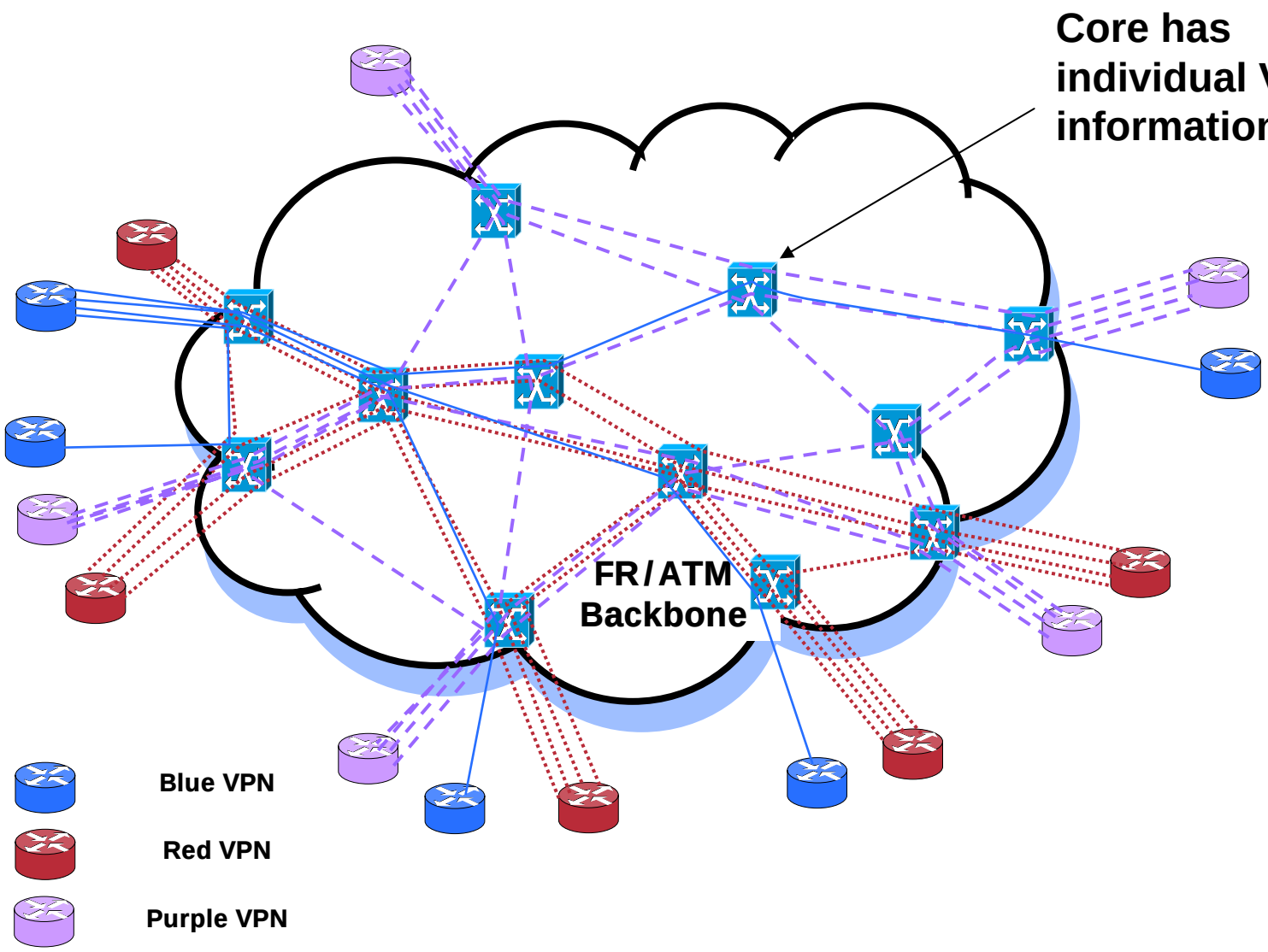
Layer 2 Integration for a Single Converged Network Infrastructure

MPLS Layer 3 VPNs

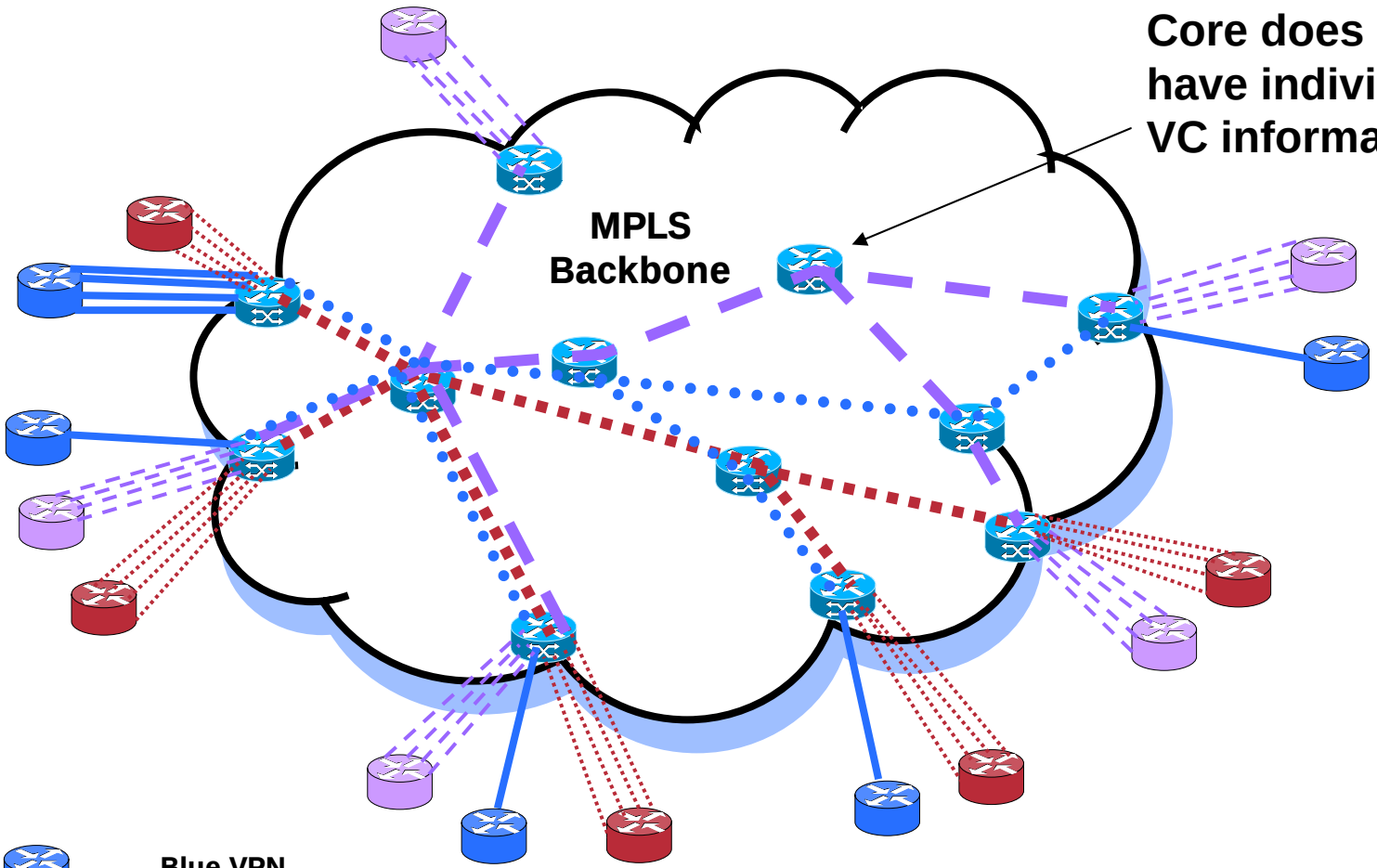
- Scalable VPNs
- IP QoS and Traffic Engineering
- Easy to manage and No VC provisioning required
- Hub/Spoke or Mesh Topologies can easily be deployed
- Provides a level of Security equivalent to Frame-relay and ATM
- Supports the deployment of new value-added applications
- Customer IP address freedom



Current Layer 2 VPNs – With FR & ATM



MPLS Layer 2 VPNs – Any Transport over MPLS (AToM)

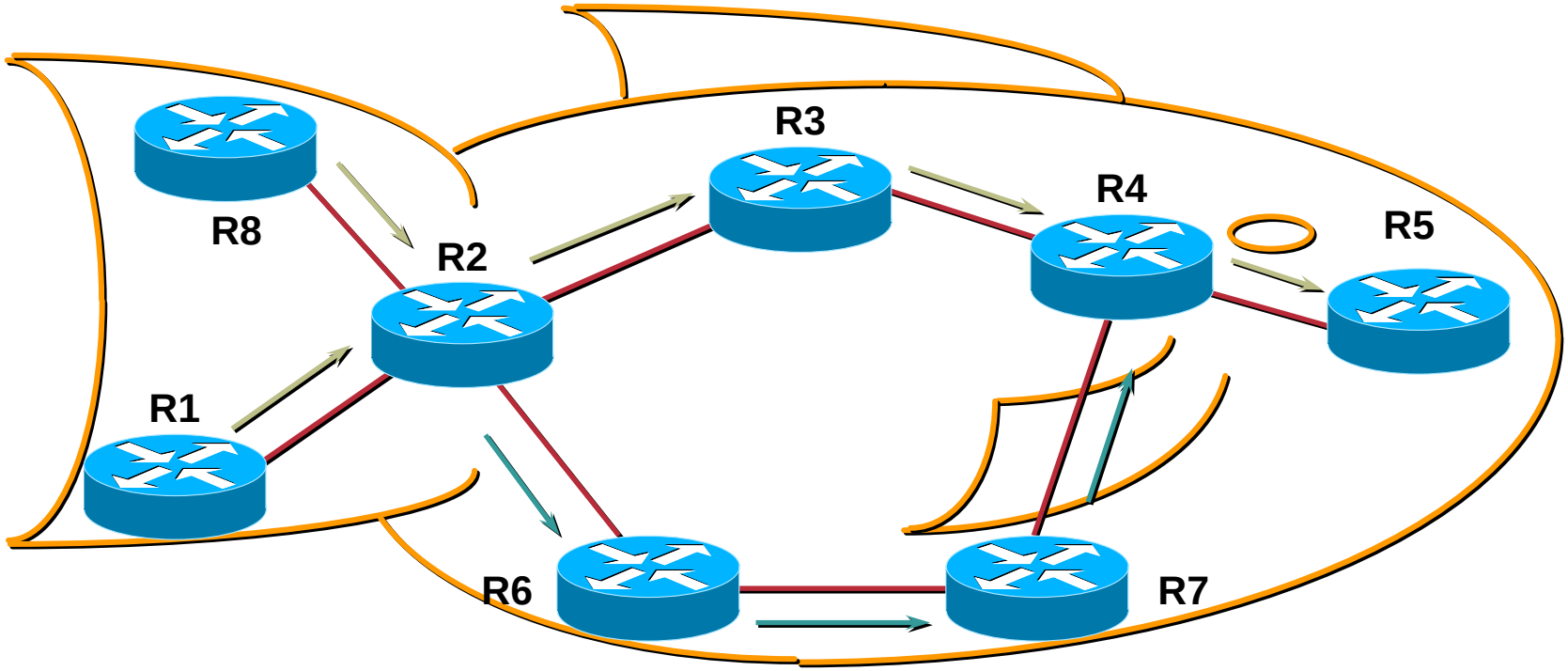


Idea is to do the same as ATM & FR
Transport layer 2 frames in MPLS packet
Create mapping of layer 2 circuits to LSPs
Scale better by using label stacking

Agenda

- MPLS Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering for VPNs
- Summary

IP Routing and the Fish Problem



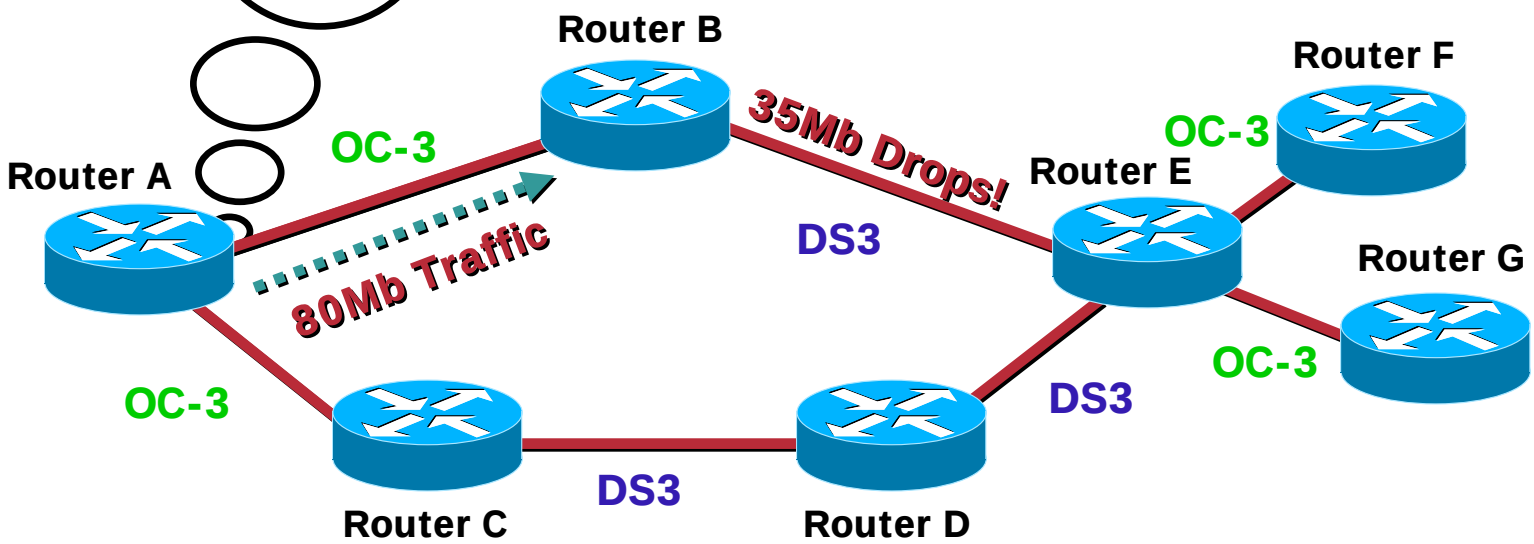
IP (Mostly) Uses Destination-Based Least-Cost Routing
Flows from R8 and R1 Merge at R2 and Become Indistinguishable
From R2, Traffic to R3, R4, R5 Use Upper Route

Alternate Path Under-Utilized

The Problem with Shortest-Path

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

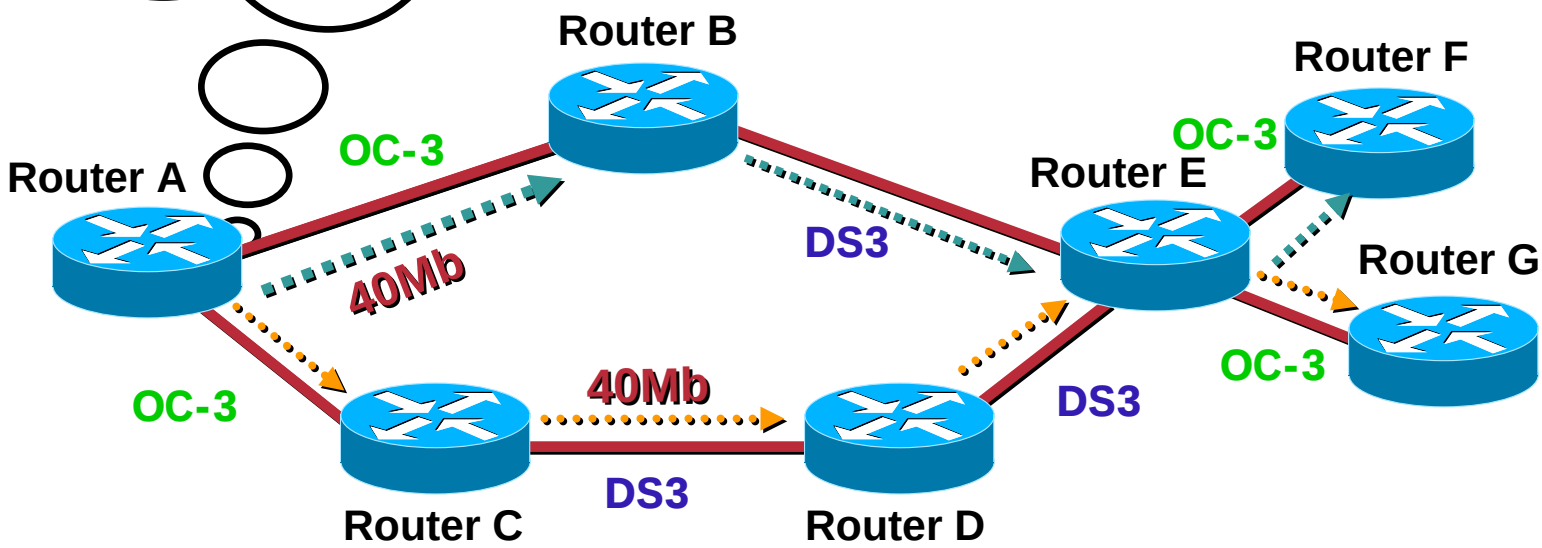
- Some links are DS3, some are OC-3
- Router A has 40Mb of traffic for Route F, 40Mb of traffic for Router G
- Massive (44%) packet loss at Router B->Router E!
  - Changing to A->C->D->E won't help



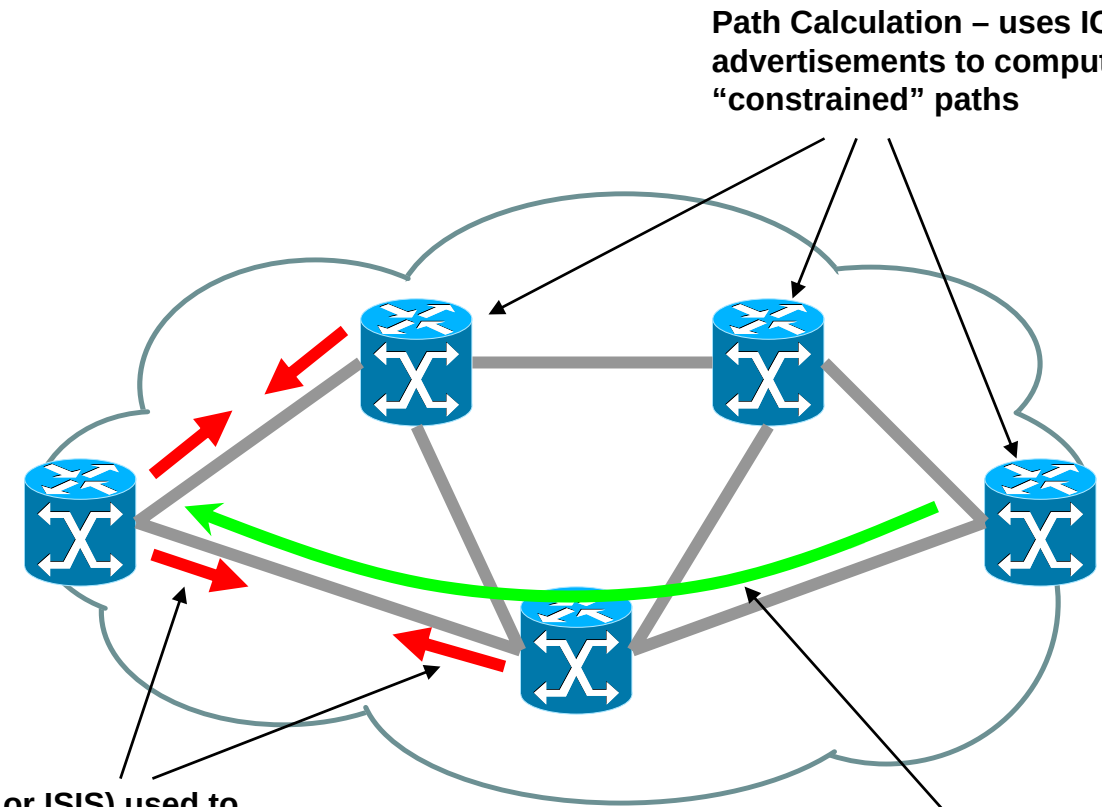
How MPLS TE Solves the problem

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	Tunnel 0	30
G	Tunnel 1	30

- Router A sees all links
- Router A computes paths on properties other than just shortest cost
- No link oversubscribed!



TE Fundamentals – “Building Blocks”



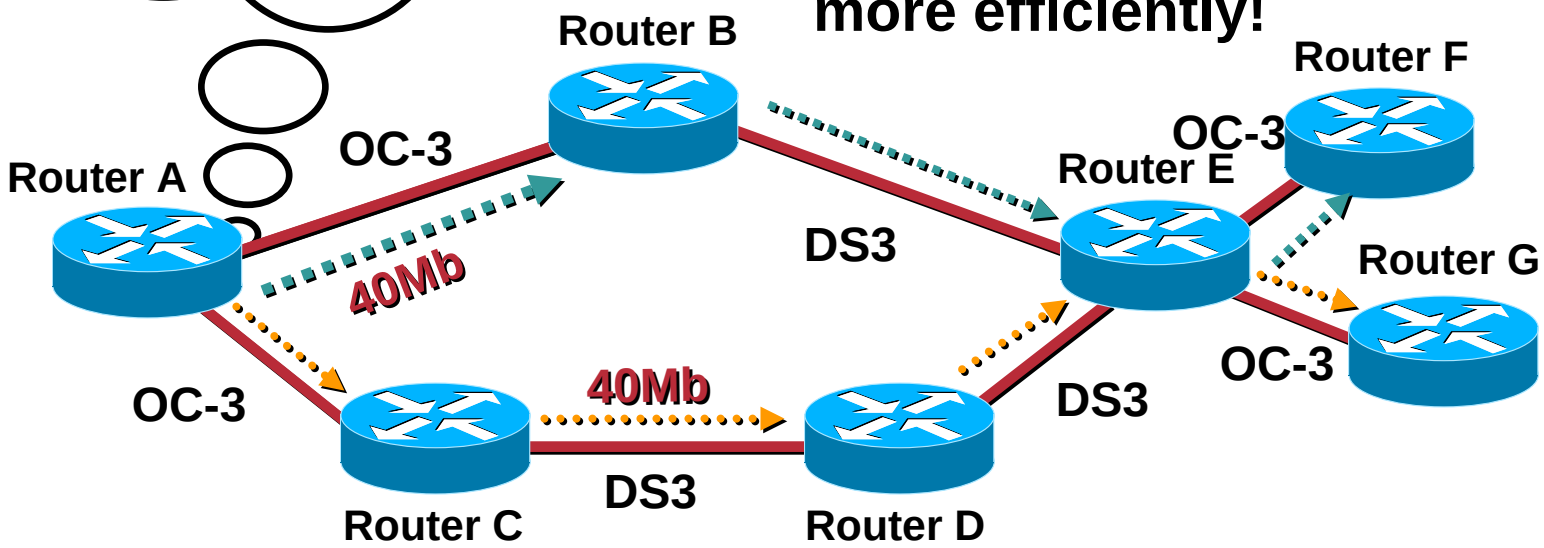
Information Distribution

- 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!
- Why do I need a link-state protocol?
  - To make sure info gets flooded
  - To build a picture of the entire network
- Information flooded includes Link, Bandwidth, Attributes, etc.

Path Calculation (PCALC)

Node	Next-Hop	Cost
B	B	10
C	C	10
D	C	20
E	B	20
F	Tunnel 0	30
G	Tunnel 1	30

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

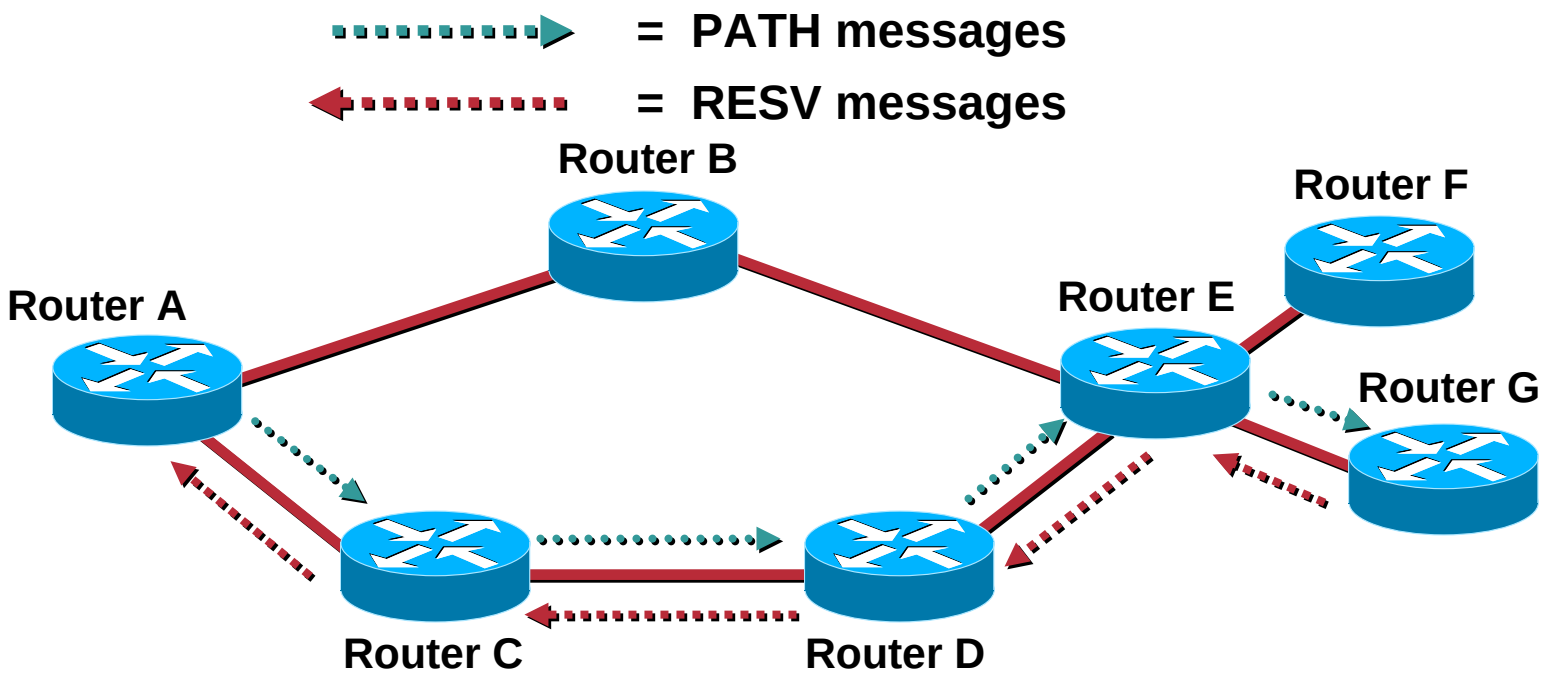


Path Calculation

- 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
  1. Pick the path with the highest minimum available bandwidth along the path
  2. Then pick the path with the lowest hop count (not IGP cost, but hop count)
  3. Then just pick one path at random

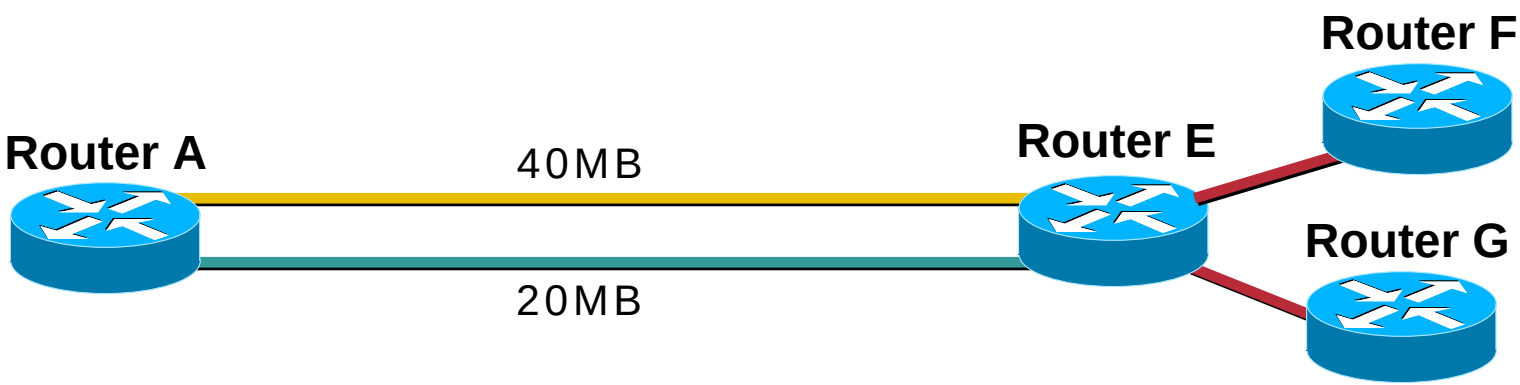
Path Setup

- PATH message: “Can I have 40Mb along this path?”
- RESV message: “Yes, and here’s the label to use”
- Labels are installed along each hop



Unequal Cost Load Balancing

- IP routing has equal-cost load balancing, but not unequal cost*
- Unequal cost load balancing difficult to do while guaranteeing a loop-free topology
- Since MPLS doesn't forward based on IP header, permanent routing loops don't happen
- 16 hash buckets for next-hop, shared in rough (11:5 for case below) proportion to configured tunnel bandwidth or load-share value



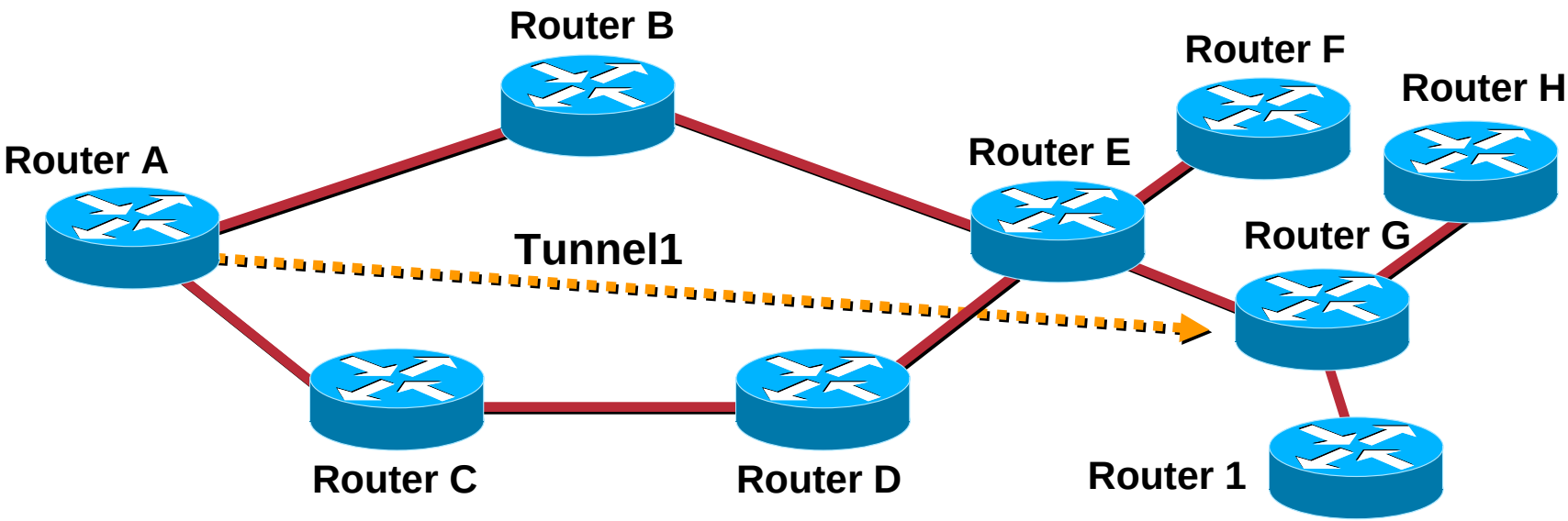
*EIGRP Has 'Variance', but That's Not As Flexible

Auto-Route

Routing Table

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**

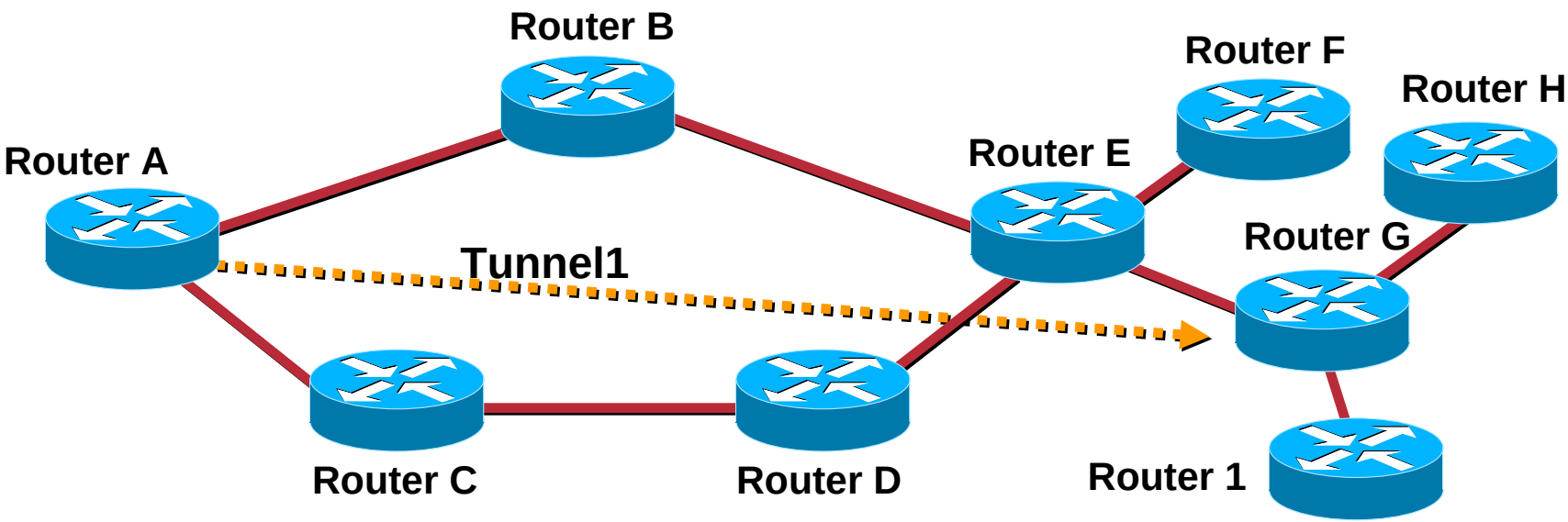


Static Routing

Routing Table

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!

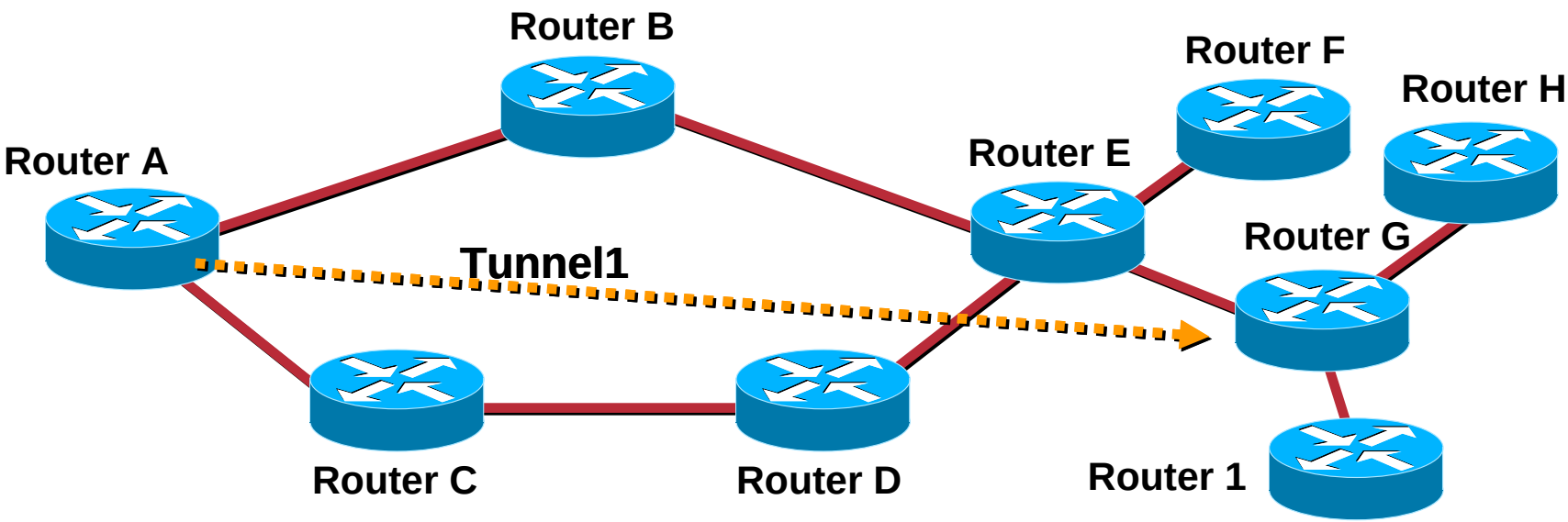


Policy Routing

Routing Table

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

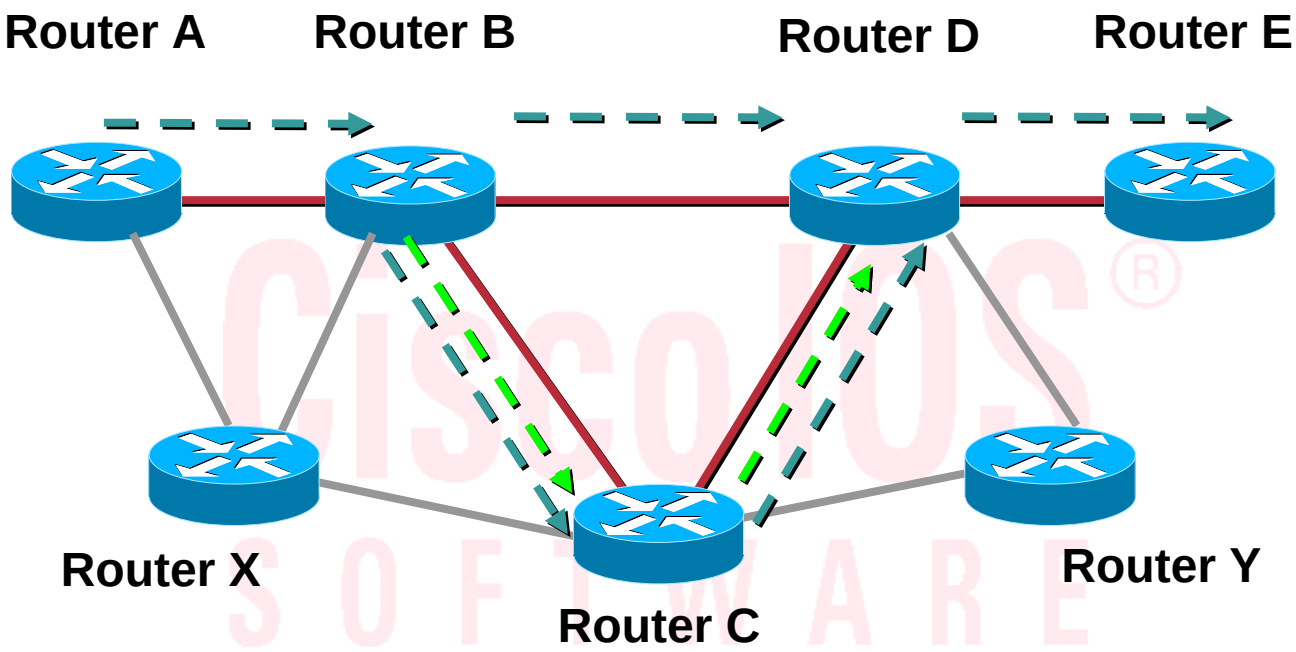
- **Routing table isn't affected by policy routing**
- **Require 'set interface tunnel' within PBR to work**



Agenda

- MPLS Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering for VPNs
- Summary

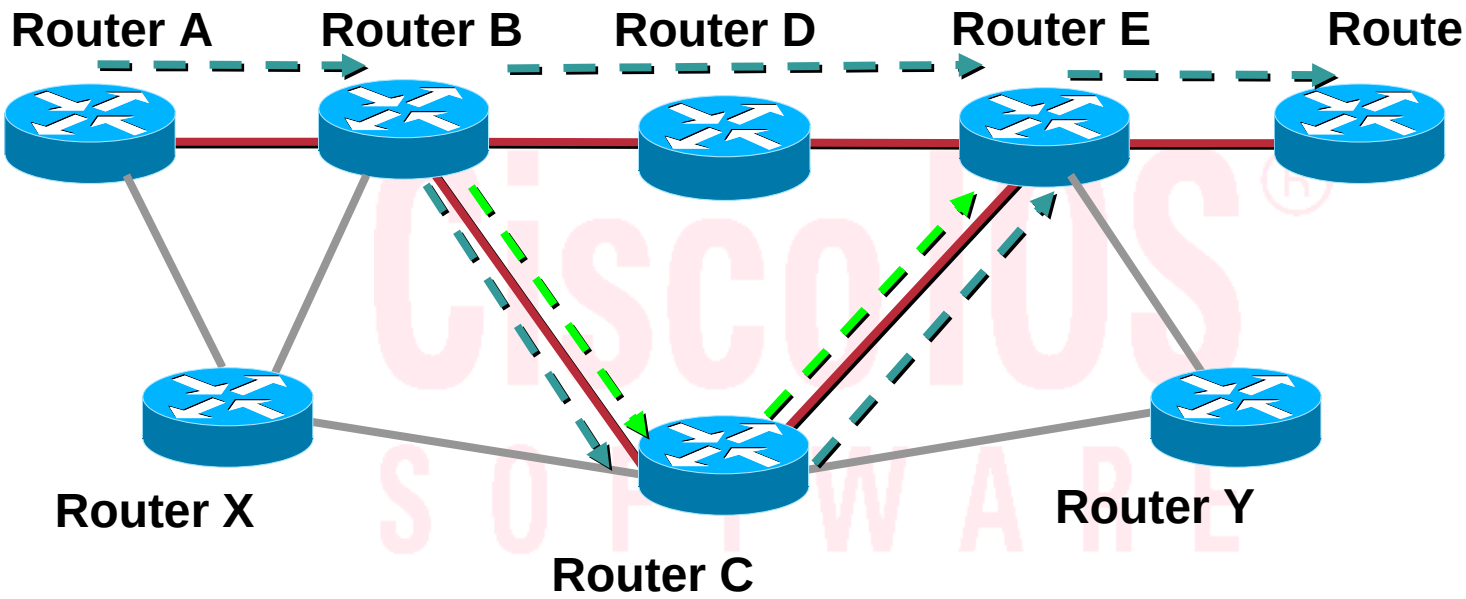
Link Protection



- Primary Tunnel: A -> B -> D -> E
- BackUp Tunnel: B -> C -> D (Pre-provisioned)
- Recovery = ~50ms

*Actual time varies – well below 50ms in lab tests, can also be higher

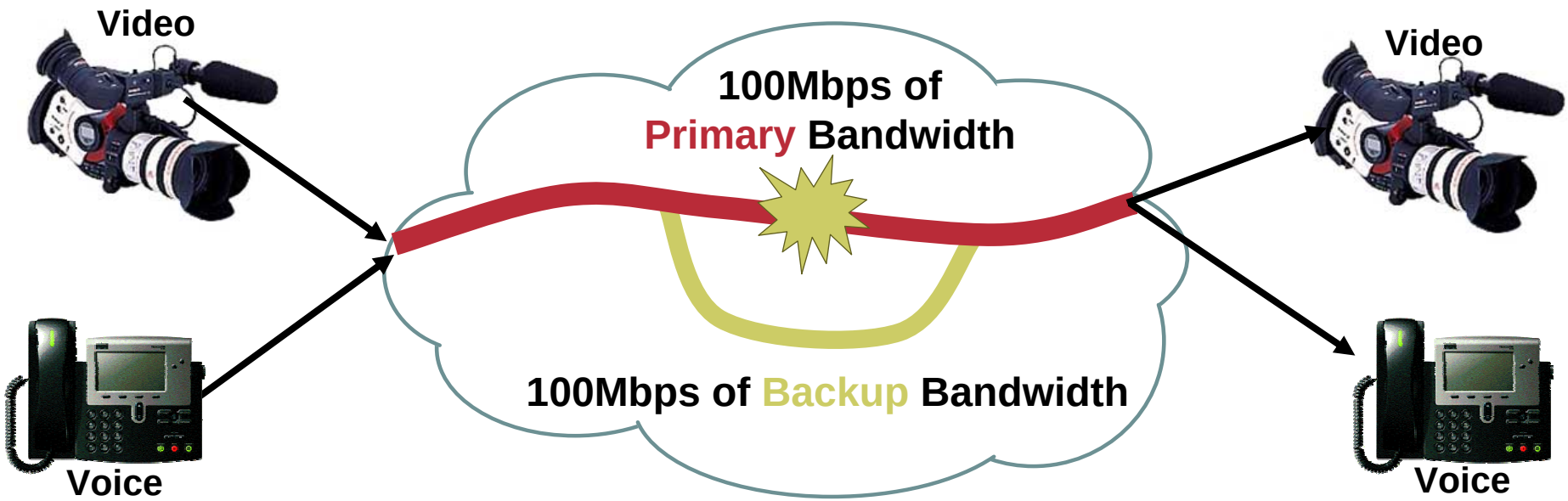
Node Protection



- Primary Tunnel: A -> B -> D -> E -> F
- BackUp Tunnel: B -> C -> E (Pre-provisioned)
- Recovery = ~100ms

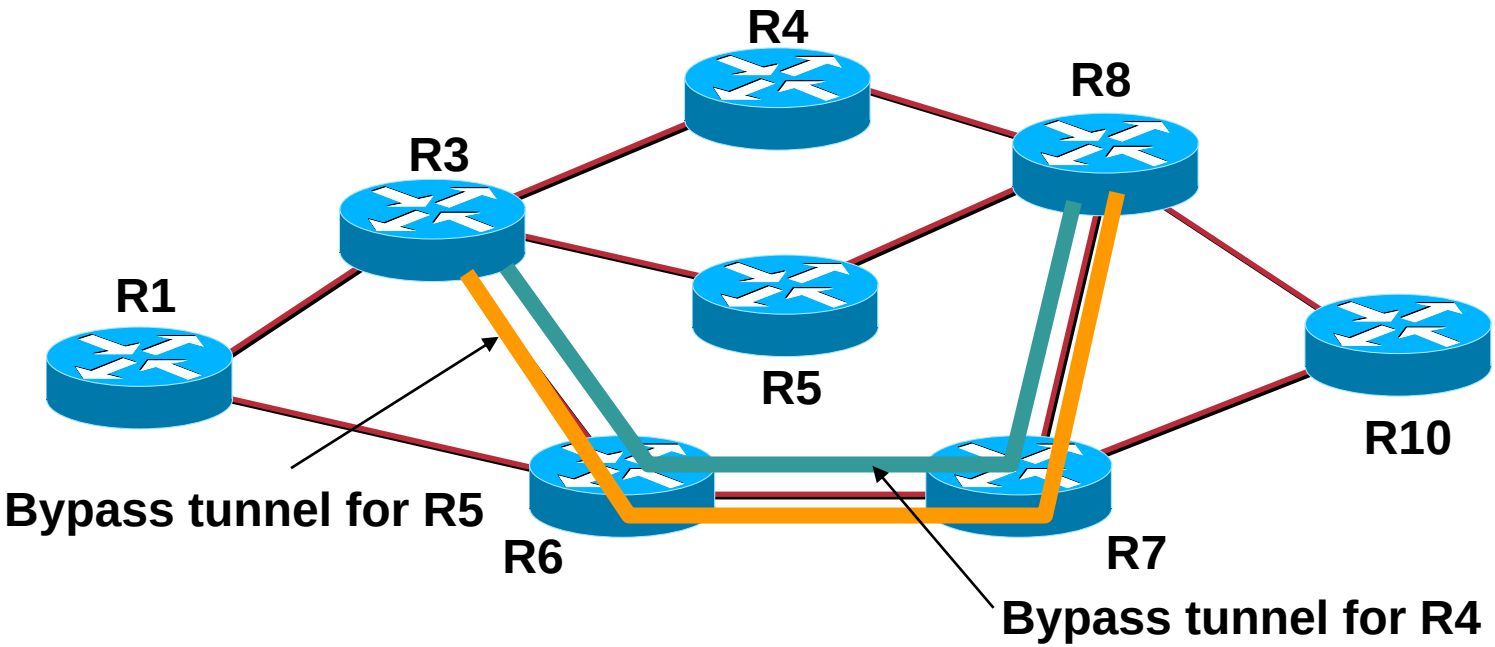
What is Bandwidth Protection?

Subscribers want bandwidth & services from point A to B for Voice & Video traffic. They don't care what happens in the network – HOW it is offered by a Service Provider is secondary.



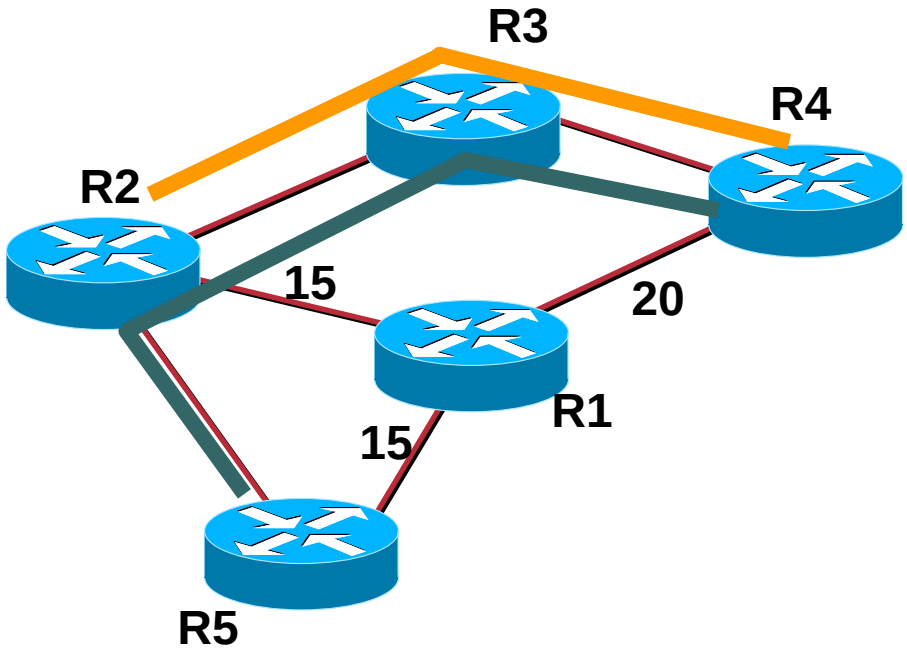
Bandwidth Protection is NOT a new problem – but using MPLS we have a new paradigm to provide a solution

Scenario 1: Backup Bandwidth Sharing



- **Only need to allocate enough BW on R3-R6-R7-R8 to protect for a single node failure – "N:1" protection**

Scenario 2: Backup Bandwidth Sharing



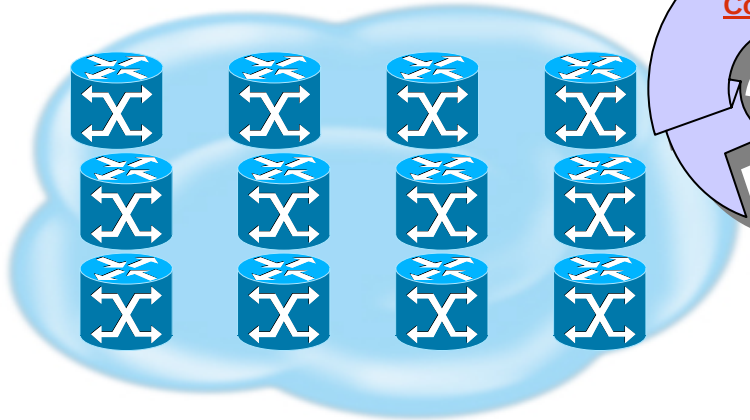
- **Backup tunnels R5-R2-R3-R4 and R2-R3-R4 protect R1**
- **Naïve approach – each tunnel needs capacity 15**
- **Shared approach – allocate 20Mbps on R2-R3 and R3-R4; 15 Mbps on R5-R2**

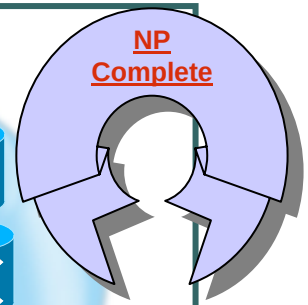
Bandwidth Protection – The Complexity

2 Router Network

Size of problem =
1 x 2
Time to compute solution =
2 seconds

16 Router Network





Size of problem =
1 x 2 x 3 x 4 x 5 .... x 16
Time to compute solution =
663,000 YEARS!!!

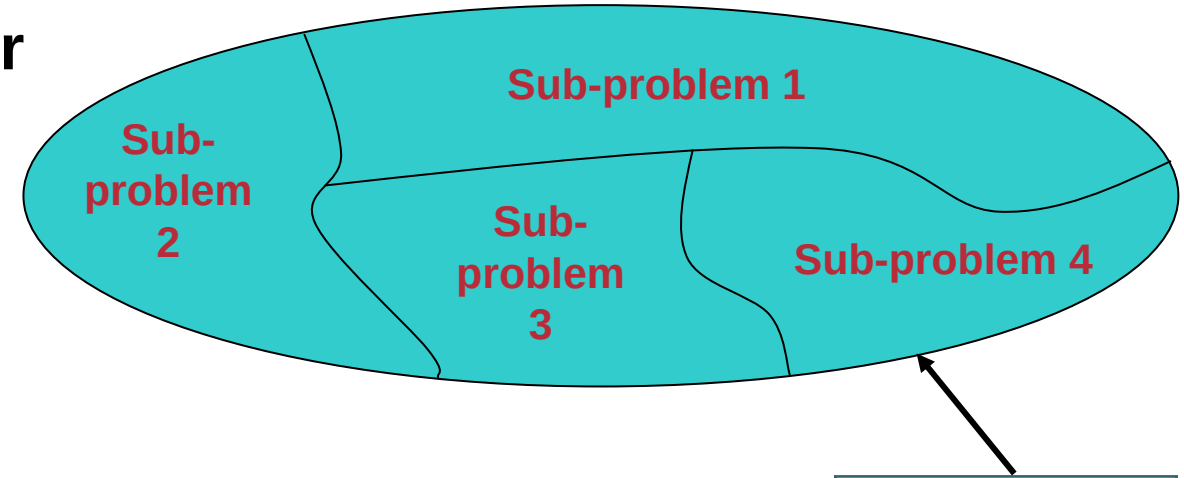
Bandwidth Protection implies computing backup tunnels for each node/ router such that an end to end bandwidth bound can be provided

Classified as "NP-complete" problem – very hard to solve

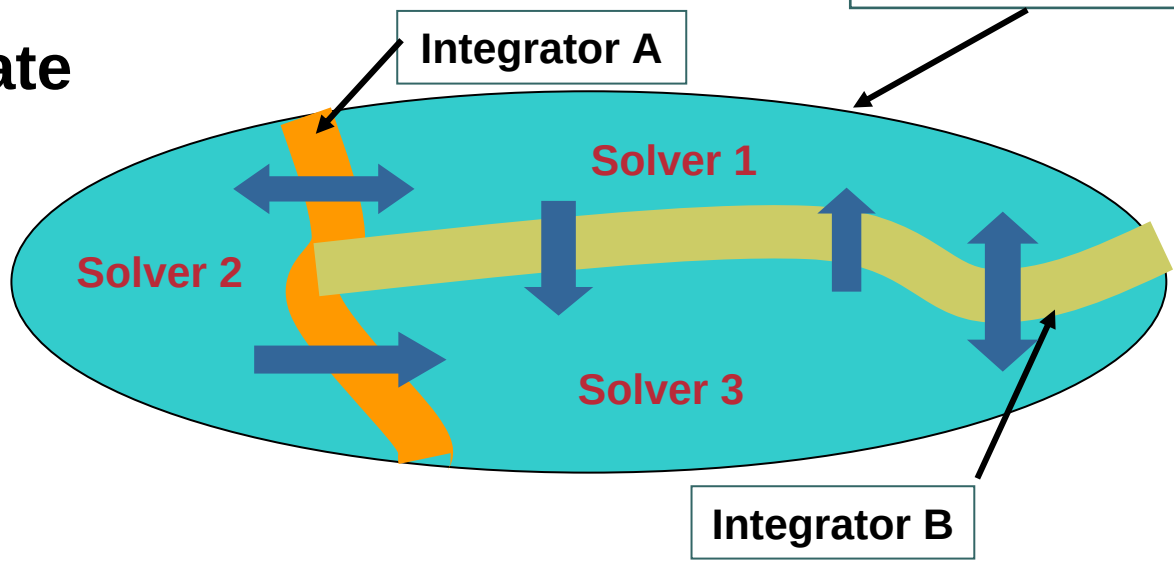
A sophisticated mathematical algorithm is needed !!

Hybrid Optimization Algorithms at Work

1. Divide and Conquer



2. Search and Integrate

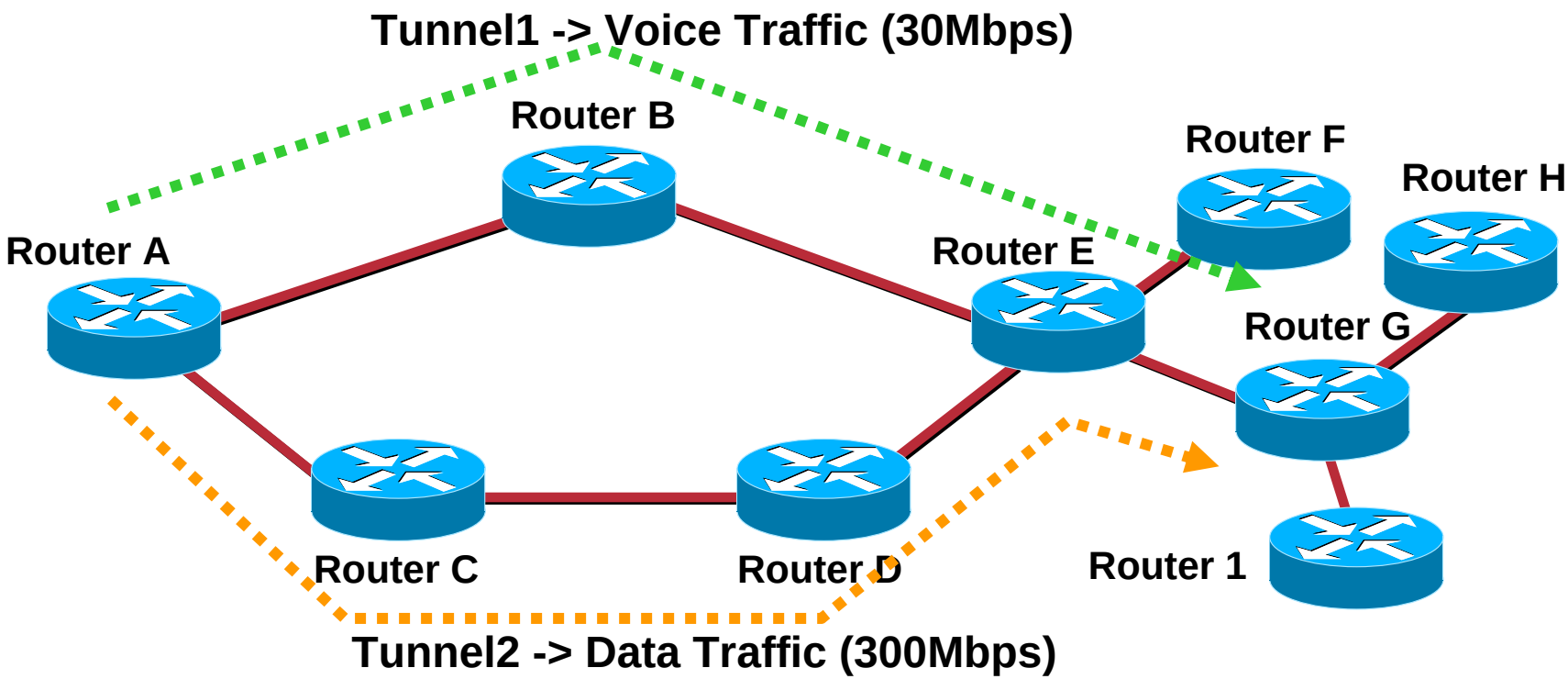


Agenda

- MPLS Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering for VPNs
- Summary

What is DiffServ aware Traffic Engineering?

- Used when there exist multiple diverse links
- Create TE tunnels on a Per-Class basis
- One TE Tunnel for Voice, another for Data



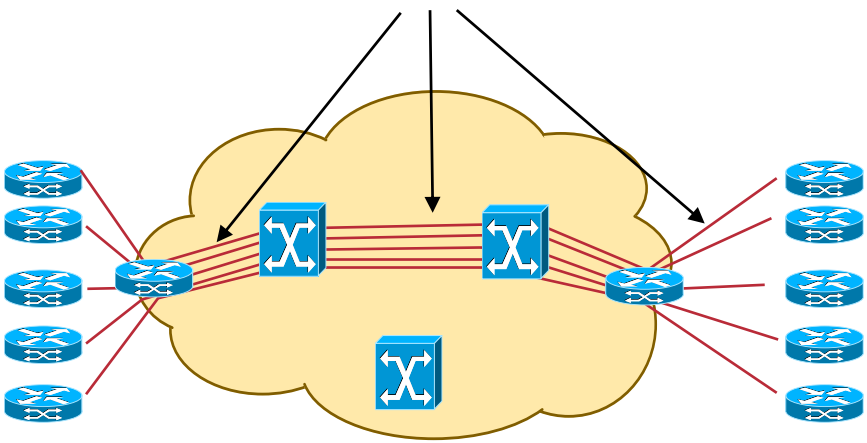
MPLS TE / DS-TE – the same as ATM QoS??

Cisco.com

MPLS TE or DS-TE is NOT DiffServ or ATM QoS
However, End result is the same in a more scalable environment

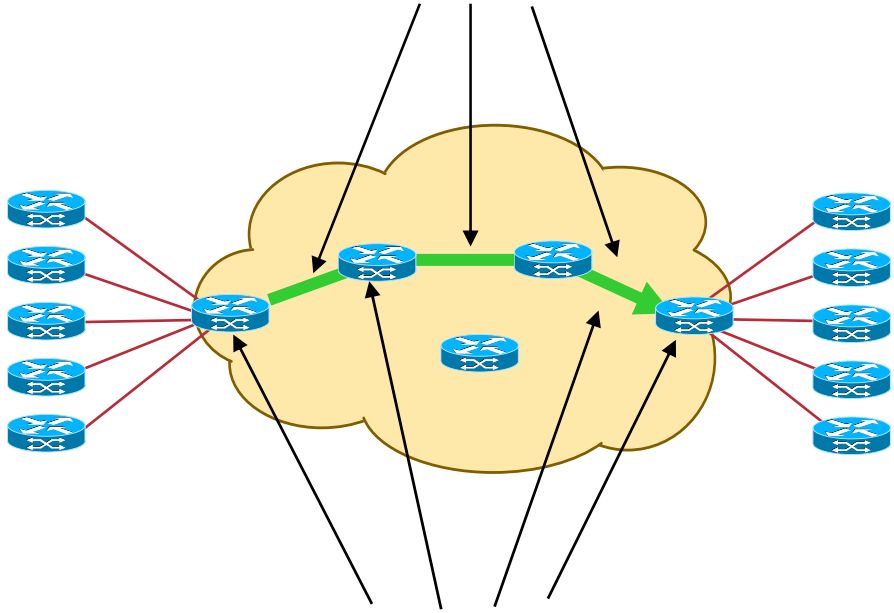
ATM QoS

ATM QoS – creates a PVC per subscriber



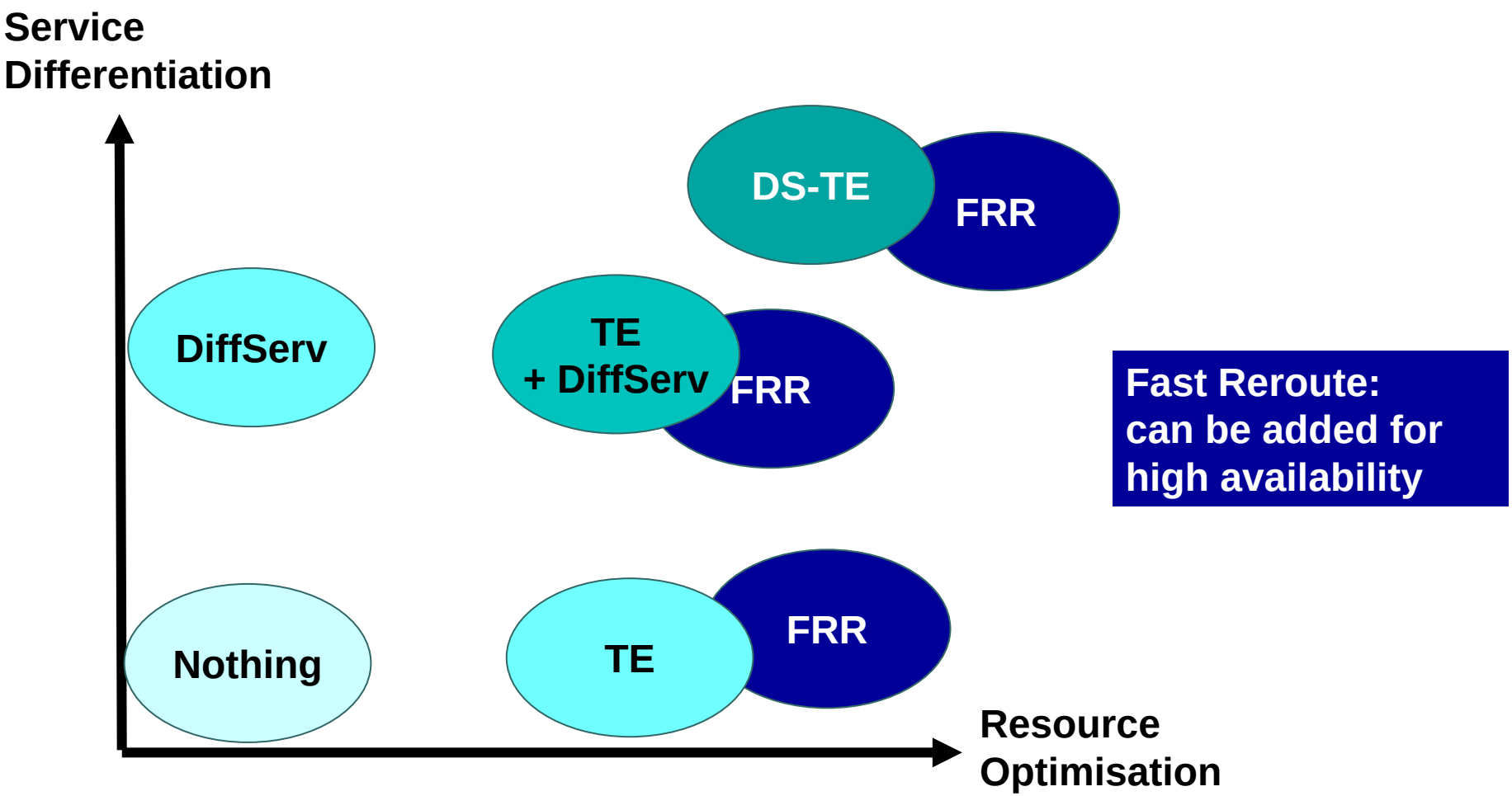
MPLS TE (DS-TE) with DiffServ

MPLS TE is used as an “aggregated bandwidth trunk”



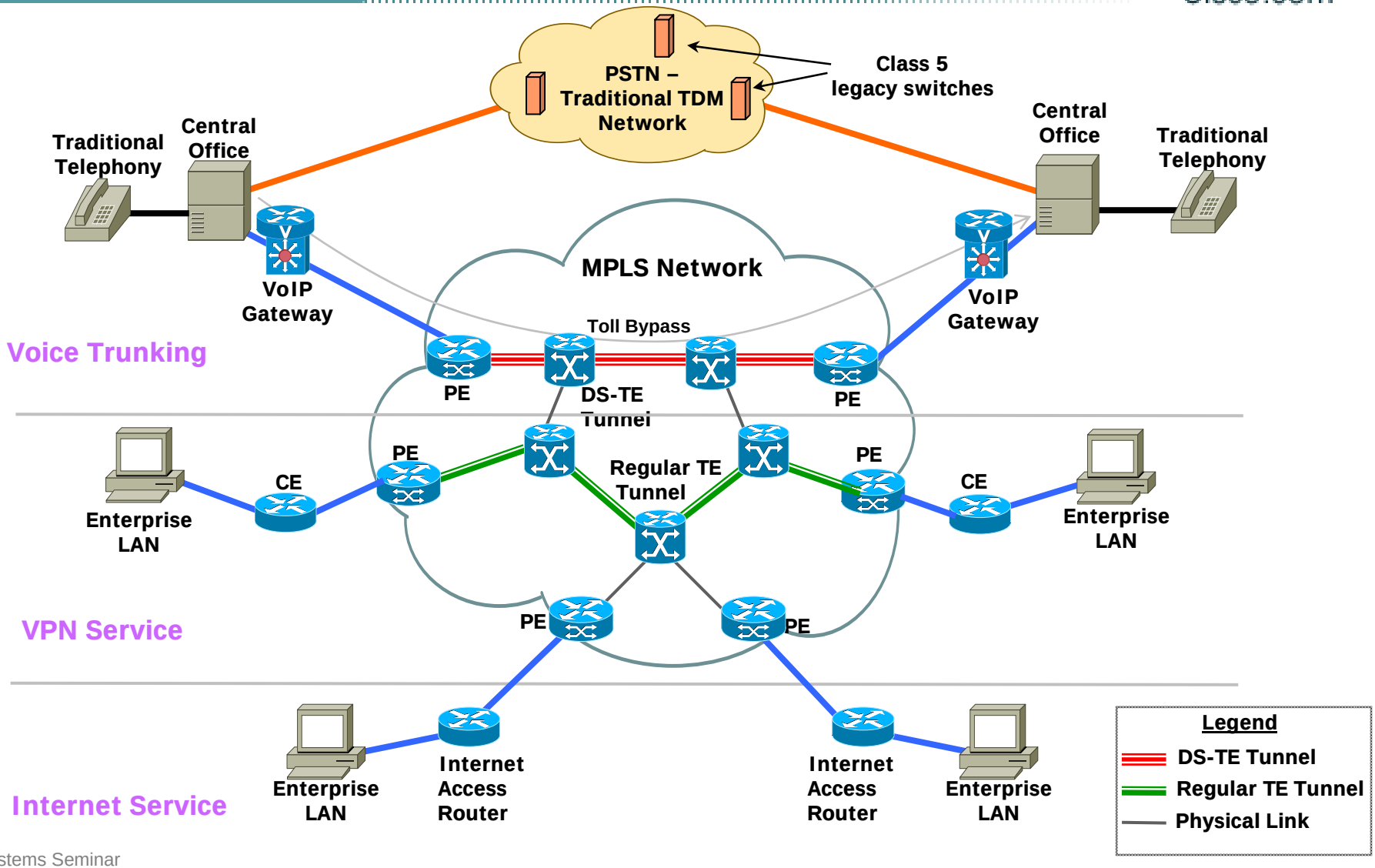
DiffServ is used to enforce “offered load” at edges. Core Interfaces maybe configured with QoS

Do I need DS-TE in my network?



Fast Reroute: can be added for high availability

Voice Trunking - Summary

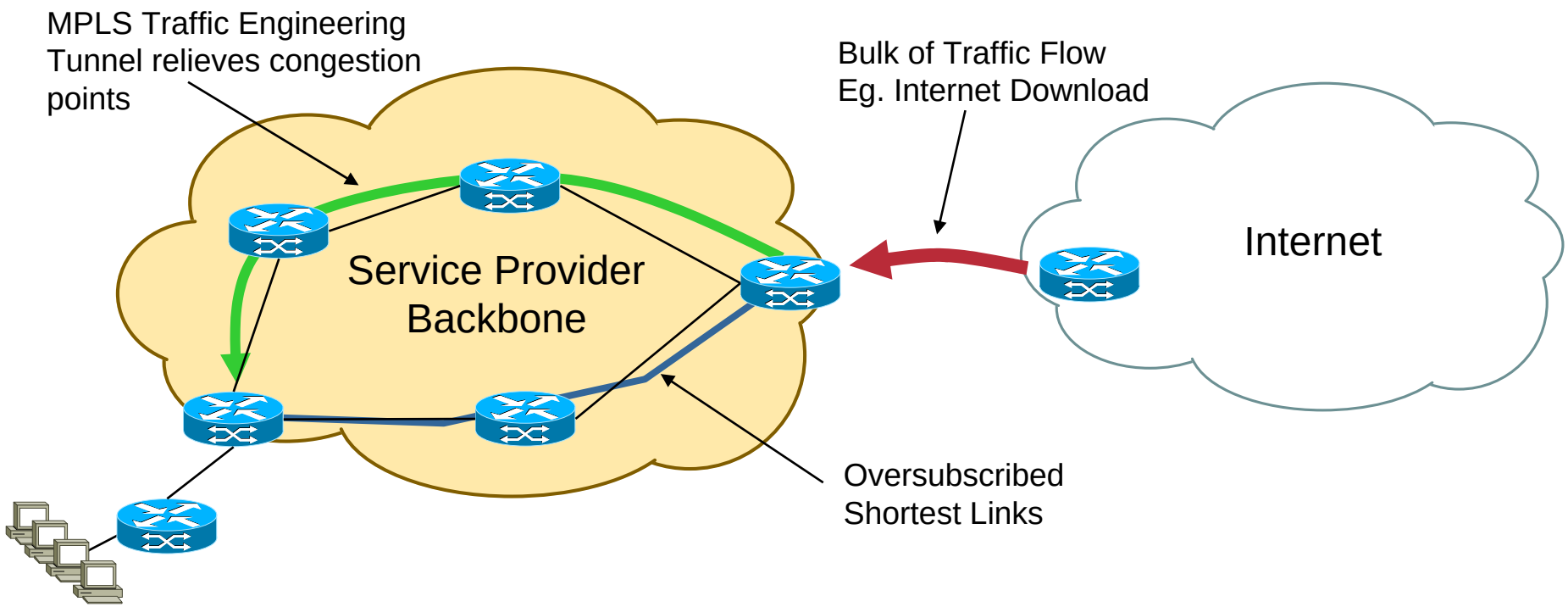


Agenda

- MPLS Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering for VPNs
- Summary

Tactical TE Deployment

Requirement: Need to handle scattered congestion points in the Network
Solution: Deploy MPLS TE on only those nodes that face congestion

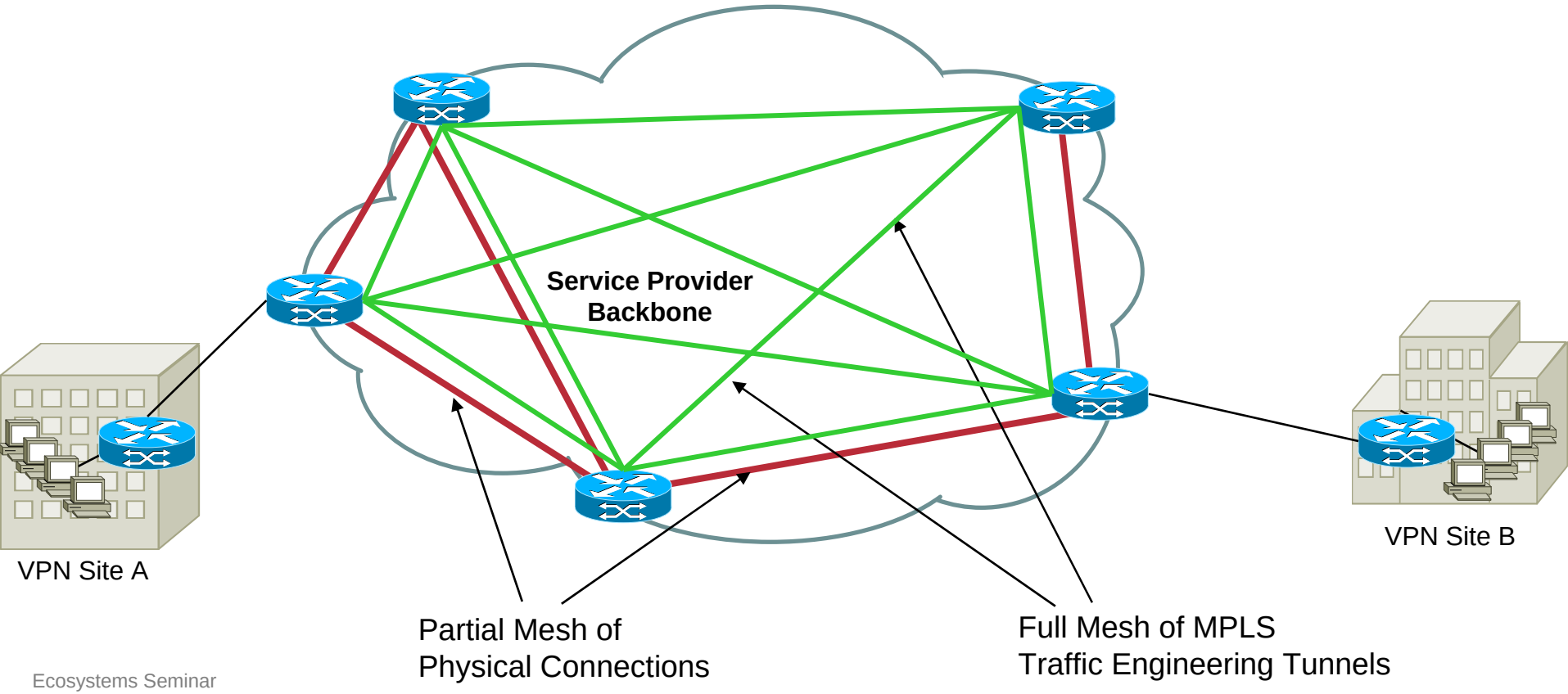


Full Mesh TE Deployment

Cisco.com

Requirement: Need to increase “bandwidth inventory” across the network

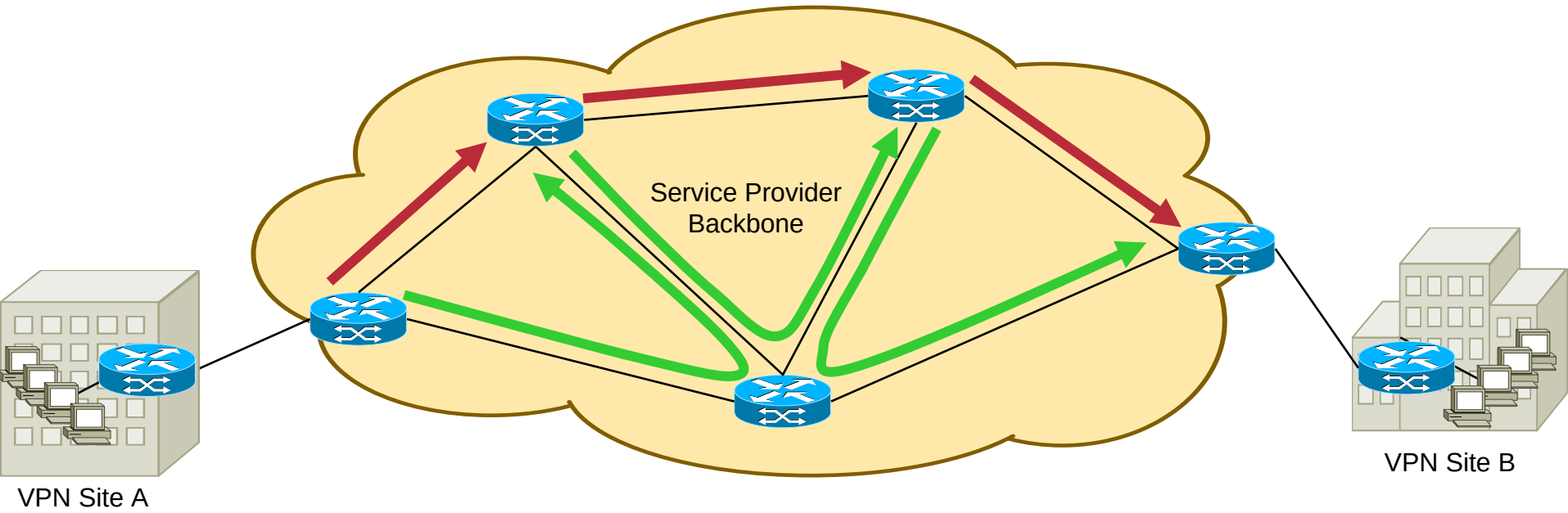
Solution: Deploy MPLS TE with a full logical mesh over a partial physical mesh and use Offline Capacity Planning Tool



1-Hop TE Deployment

Requirement: Need protection only – minimize packet loss. Lots of Bandwidth in the core

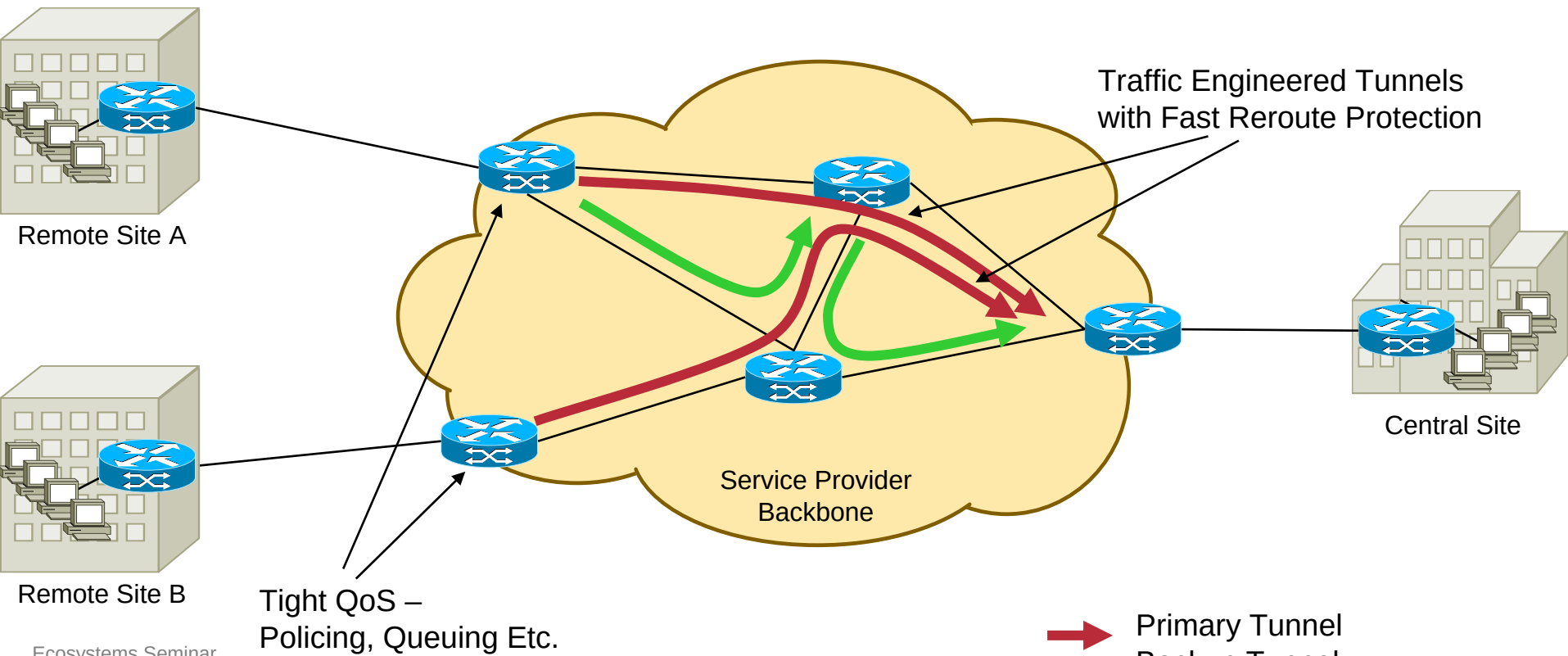
Solution: Deploy MPLS Fast Reroute for less than 50ms failover time with 1-Hop Primary TE Tunnels and Backup Tunnel for each



Virtual Leased Line Deployment

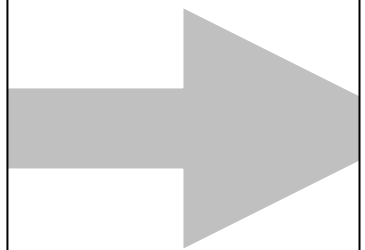
Requirement: Need to create dedicated point-to-point circuits with bandwidth guarantees – Virtual Leased Line (VLL)

Solution: Deploy MPLS TE (or DS-TE) with QoS. Forward traffic from L3 VPN or L2 VPN into a TE Tunnel. Unlike ATM PVCs, use 1 TE Tunnel for multiple VPNs creating a scalable architecture



Eventually – MPLS TE / RSVP for "Tight SLAs"

Hey Mr. Customer - here is 4 Classes of service that I can offer
- *Voice*
- *Mission Critical traffic*
- *Interactive traffic*
- *Best Effort Traffic*



Hey Mr. Customer - here is 4 Classes of service that I can offer
- **Voice**
- **Mission Critical traffic**
- **Interactive traffic**
- **Best Effort Traffic**

PLUS
- **Packet loss, of say no more than 0.001% of traffic (with FRR)**
- **Guaranteed delay of 50ms (using TE)**
- **Admission control for, say 200 Voice calls & 200 Video calls**

Benefits provided by MPLS Traffic Engineering

Benefits provided by future MPLS Traffic Engineering Capabilities

The Cisco IOS® Advantage

Cisco.com

- Shipped MPLS in Cisco IOS software release 11.1CT - July 1998
- First to deploy MPLS in a production network
- First to deploy MPLS Traffic Engineering
- First to deploy MPLS VPNs
- First to deploy QoS-enhanced MPLS TE
- First to ship MPLS TE Fast Reroute
- First to ship MPLS Managed Shared Services
- Broadest platform support
- Interoperable solution based in standards

First to ship MPLS Bandwidth Protection