Cisco Systems

Cisco.com

# Cisco MPLS Traffic Engineering and Bandwidth Protection

**Amrit Hanspal**

**Sr. Product Manager – MPLS & QoS**

**Internet Technologies Division**

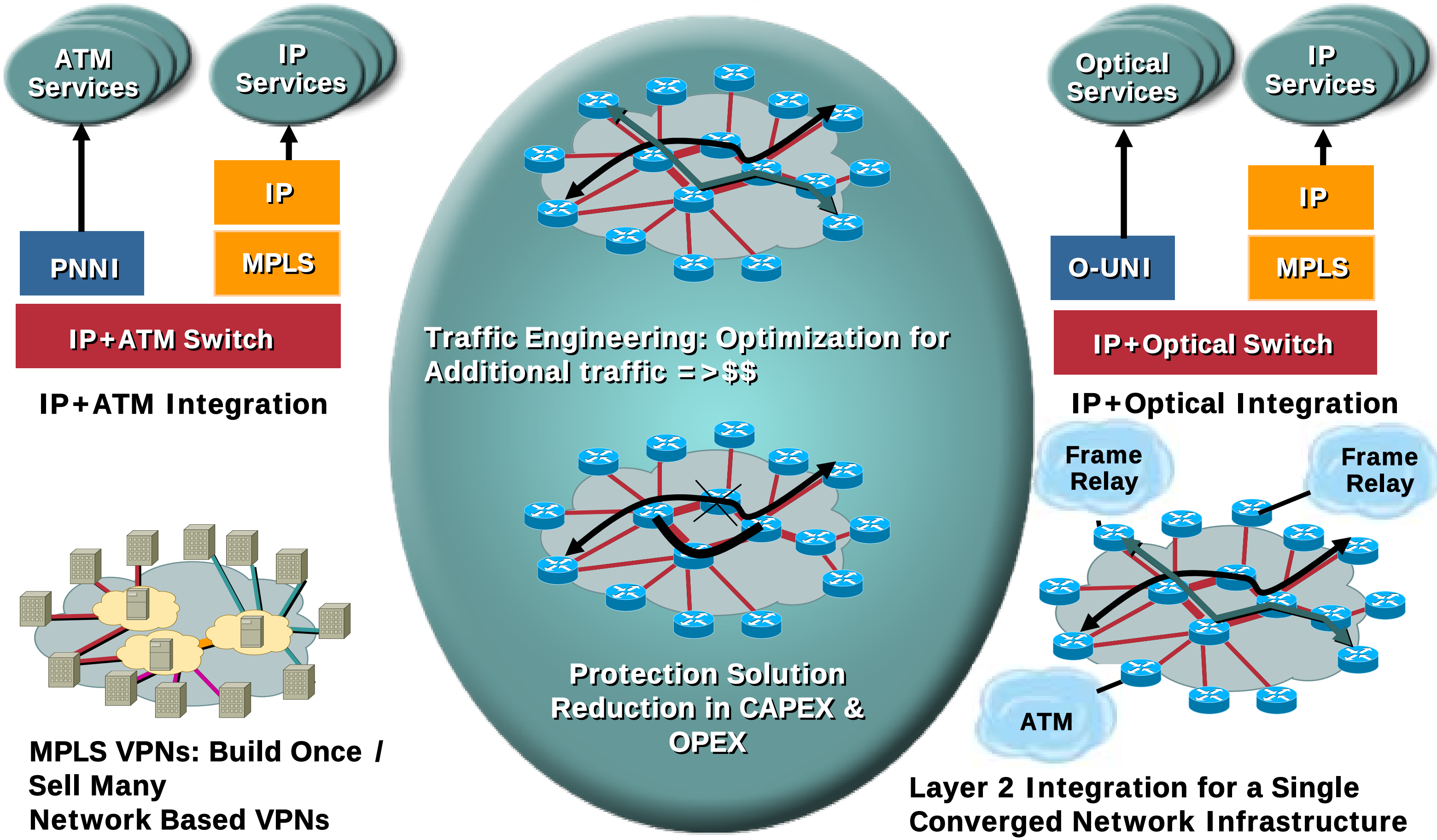
# Agenda



- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

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

Cisco.com



# Defining Convergence

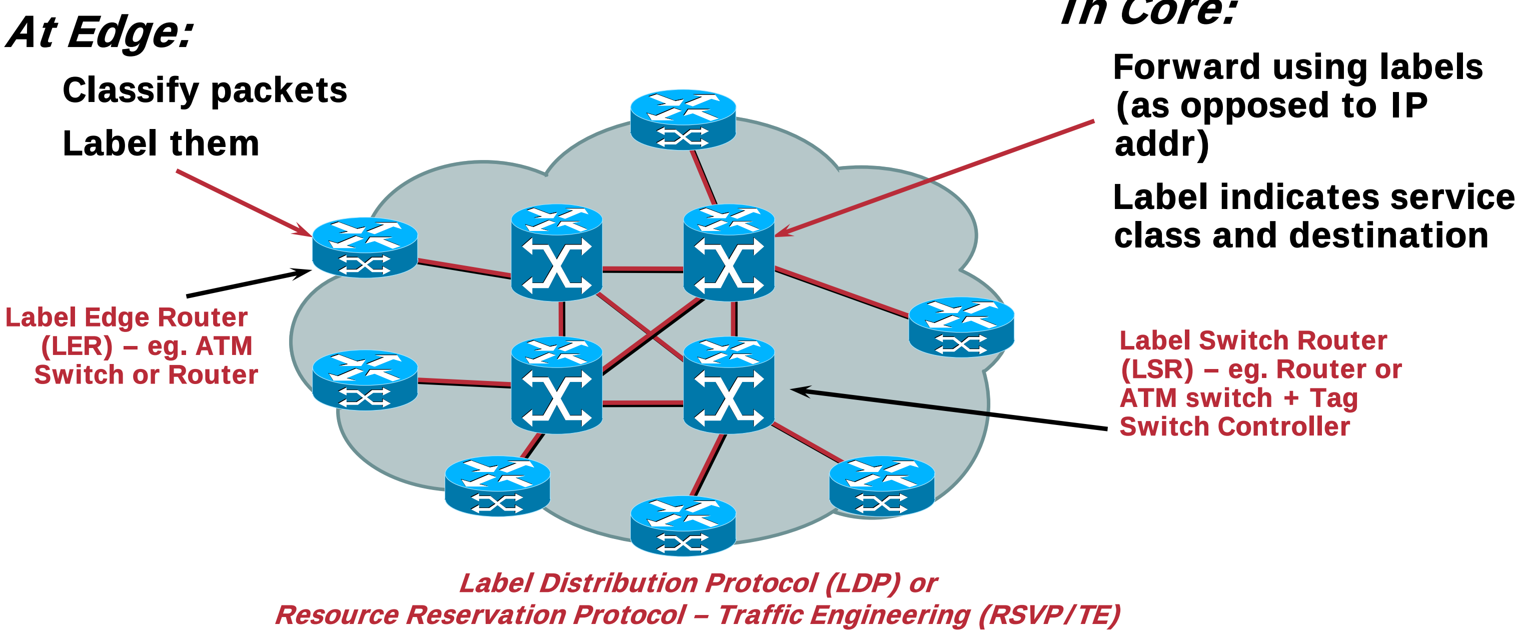


- **Convergence: Many Aspects, Same Objective**
- **Traffic Types: Voice, Video, Data**
- **Service Delivery: Internet, VPN, Extranets**
- **Transport Mechanism: ATM, Ethernet, Frame Relay, PPP, HDLC, etc.**

***"Have a single infrastructure to handle multiple services"***

# MPLS Architecture

Cisco.com

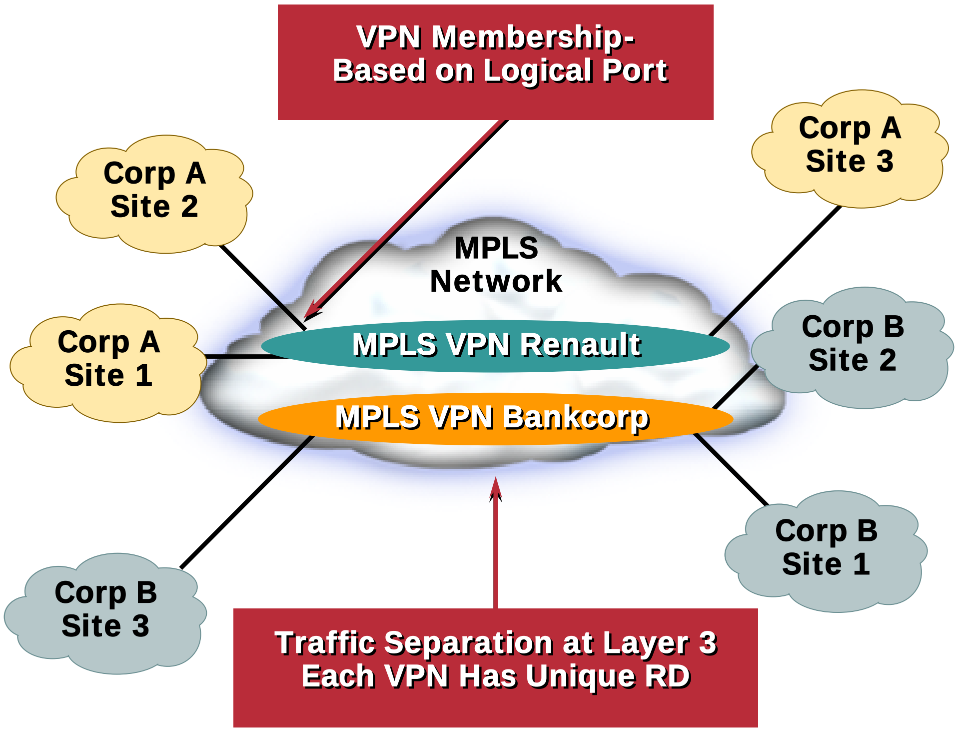



- **Control Plane builds Forwarding Table**
- **Data Plane forwards packets based on Forwarding Table**
- **Connection-oriented which leverages IP Routing (OSPF, ISIS, etc.)**

# MPLS Layer 3 VPNs

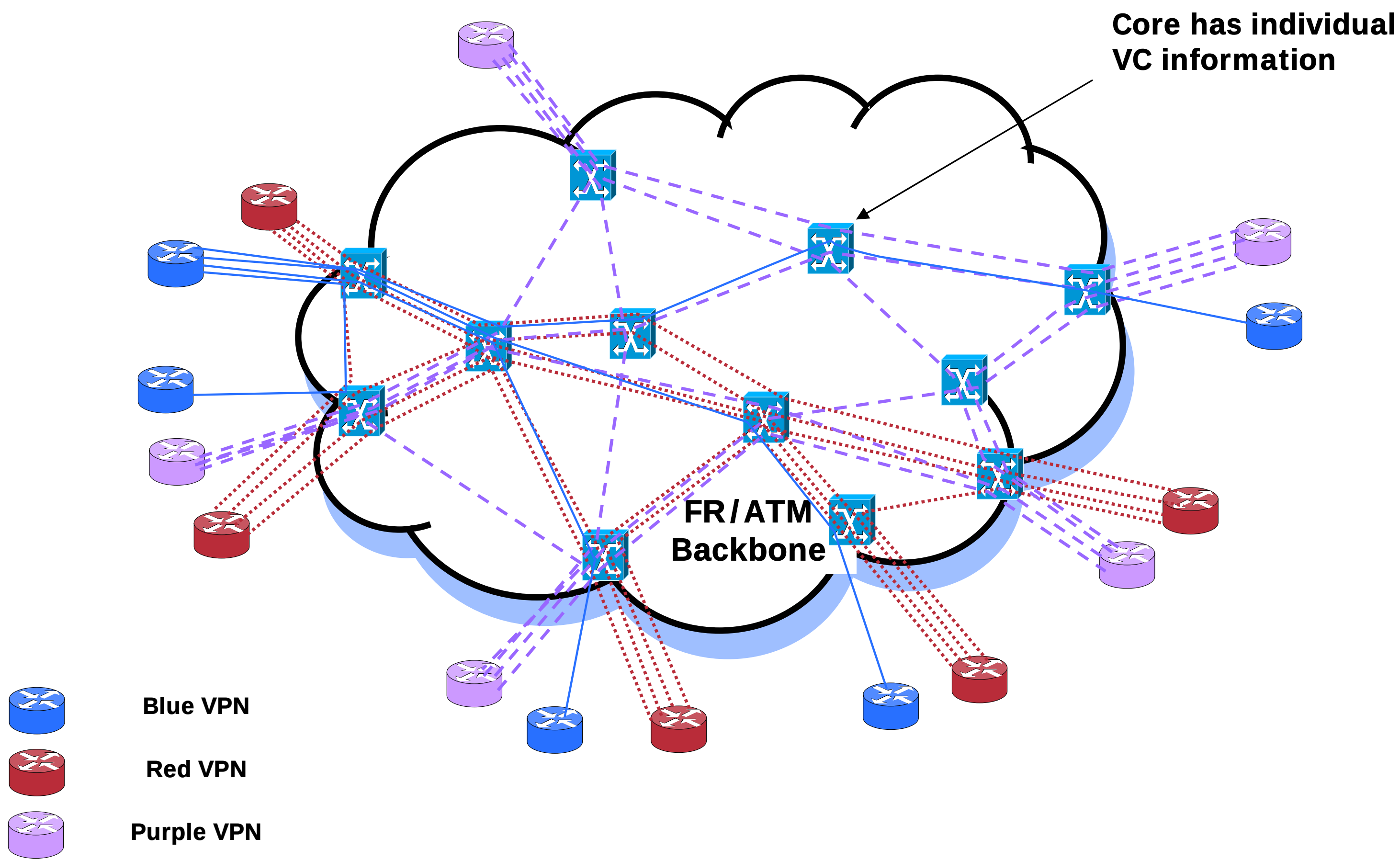
Cisco.com

- 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



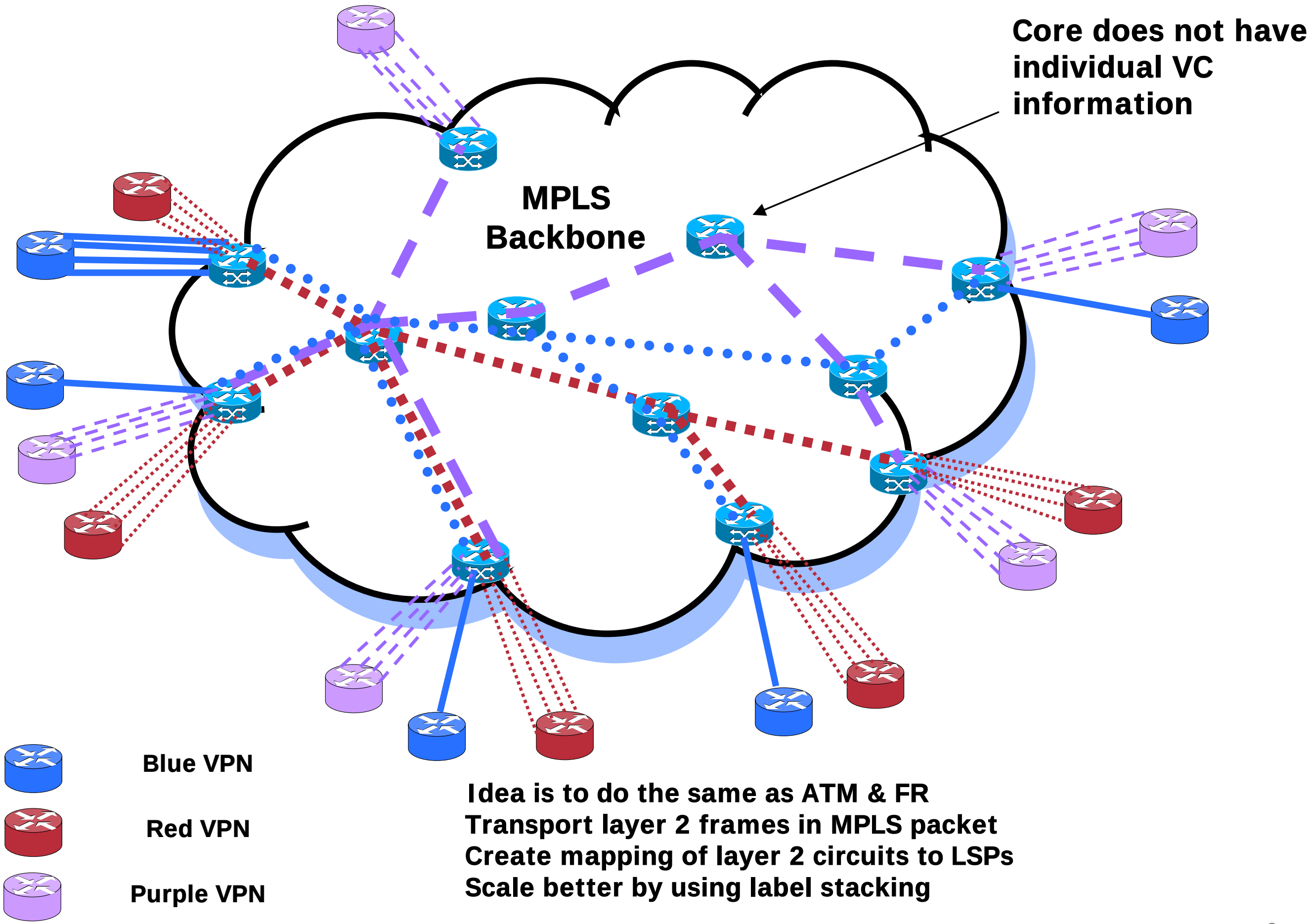
# Current Layer 2 VPNs – With FR & ATM





# 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

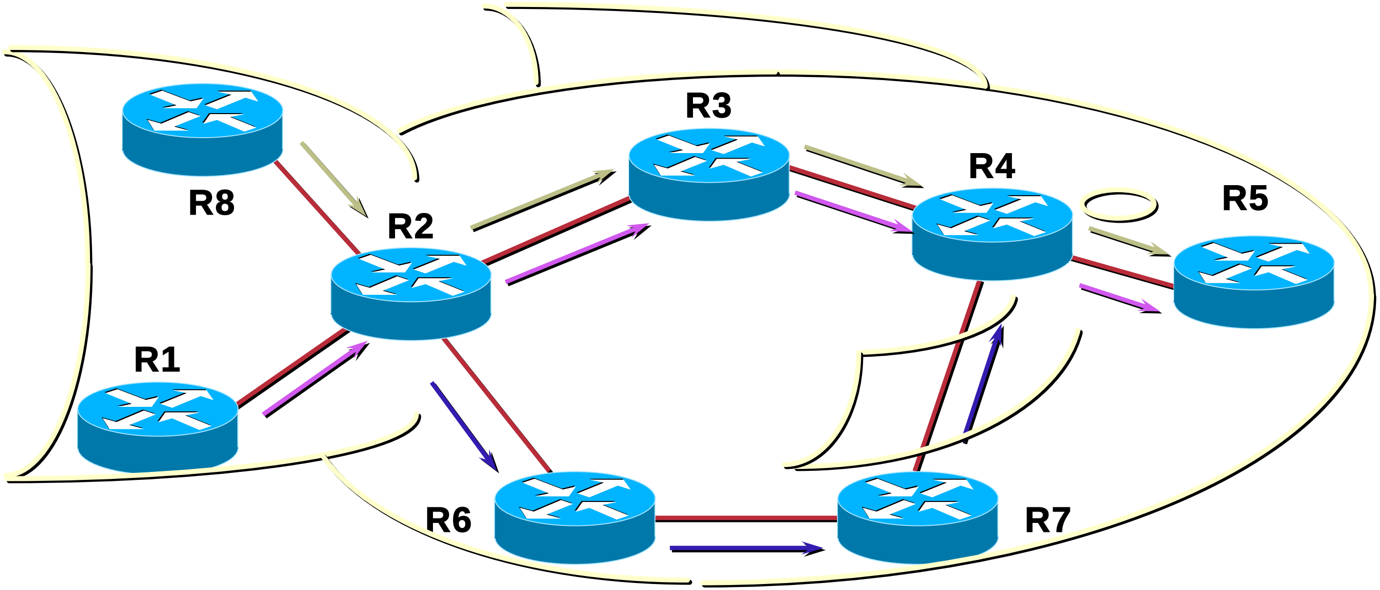
# Agenda

Cisco.com

- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

# IP Routing and the Fish Problem

Cisco.com

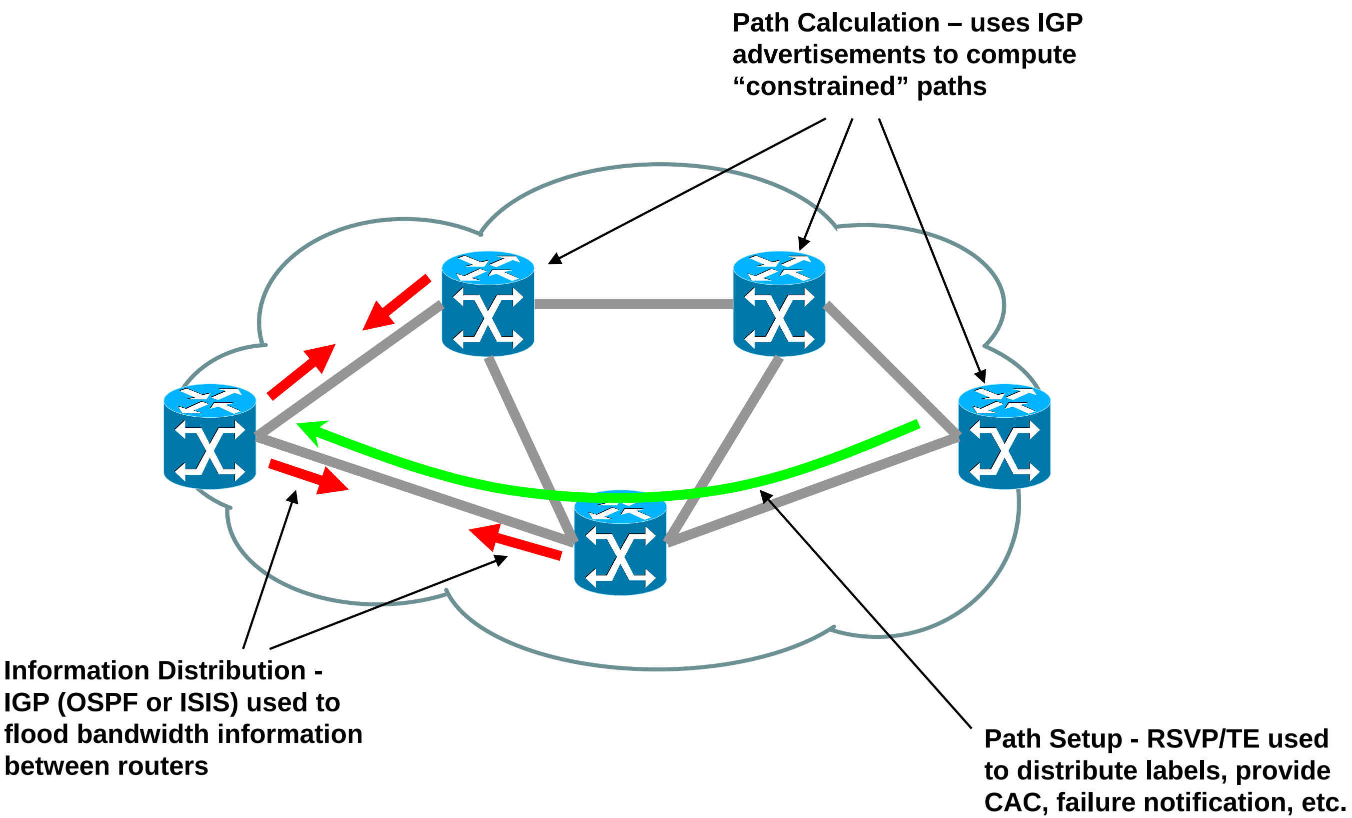



**IP (Mostly) Uses Destination-Based Least-Cost Routing**
**Flows from R8 and R1 Merge at R2 and Become Indistinguishable**
**From R2, Traffic to R3, R4, R5 Use Upper Route**

**Alternate Path Under-Utilized**

# TE Fundamentals – “Building Blocks”





# Information Distribution

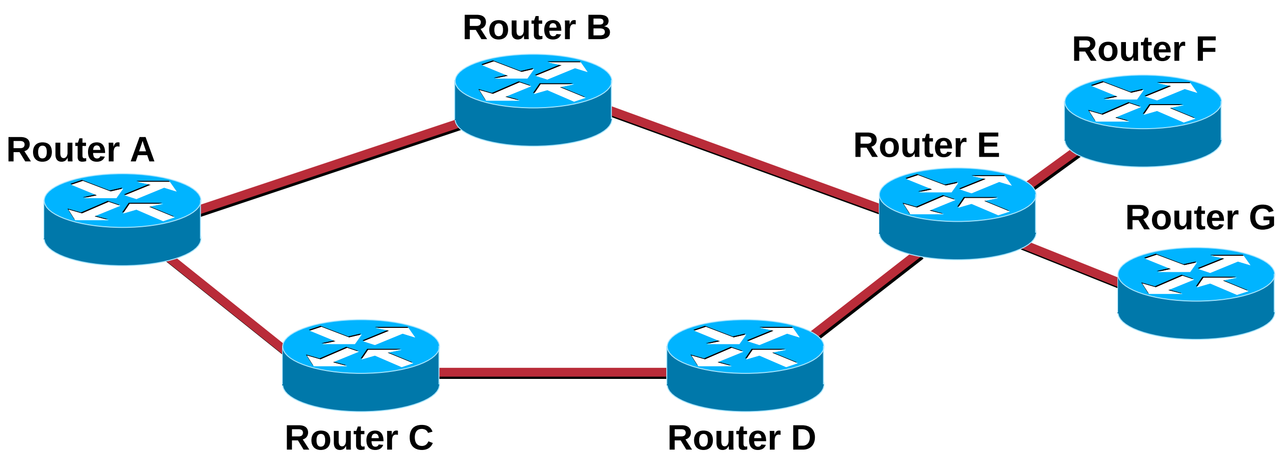


- You need a link-state protocol as your IGP
  - IS-IS or OSPF
- Link-state requirement is only for MPLS-TE!
  - Not a requirement for VPNs, etc!
- Why do I need a link-state protocol?
  - To make sure info gets flooded
  - To build a picture of the entire network

# Need for a Link-State Protocol



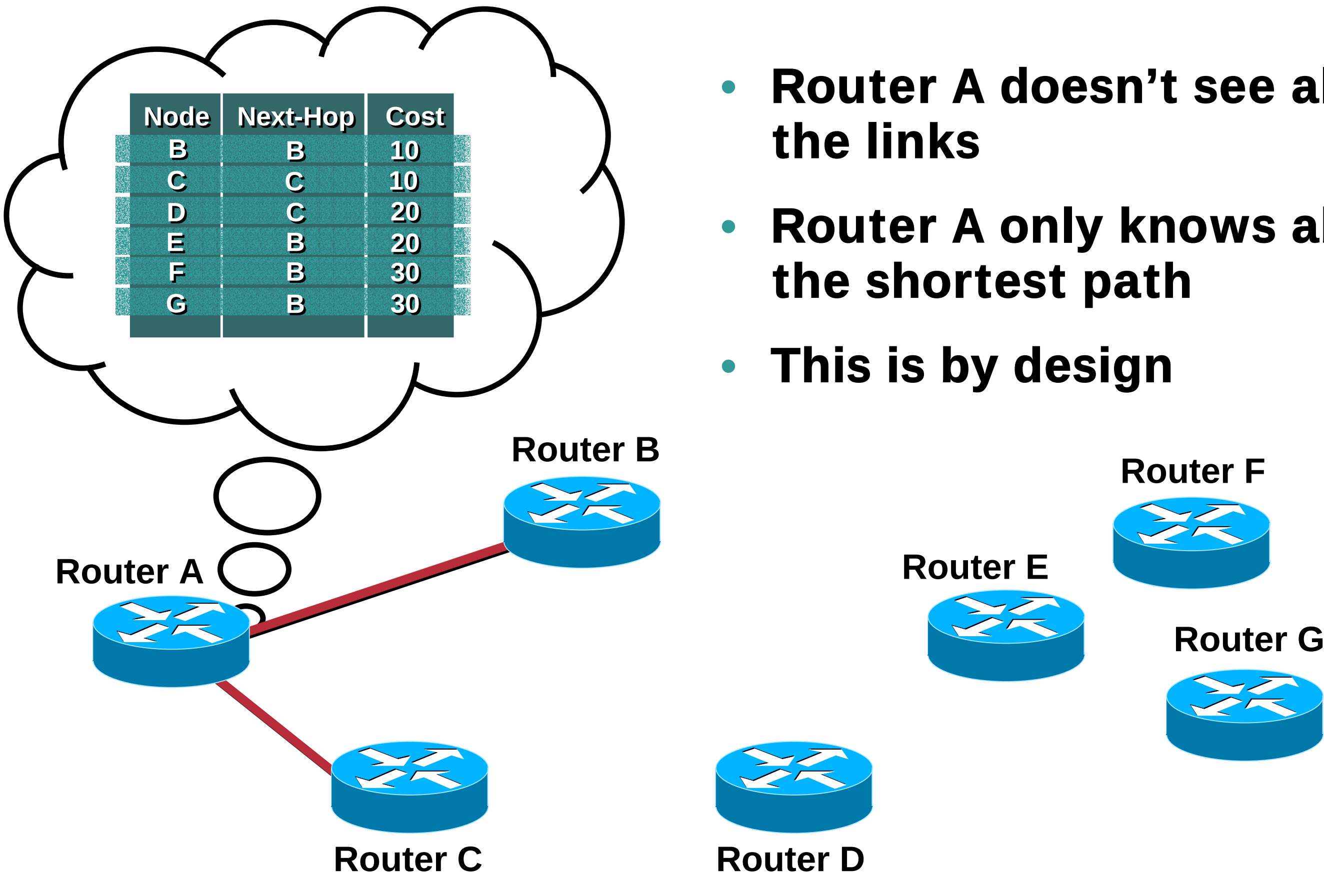
- Consider the following network:
    - All links have a cost of 10
    - Router A's path to Router E is A->B->E, cost 20
    - All traffic from A to {E,F,G} goes A->B->E



# What a DV Protocol Sees



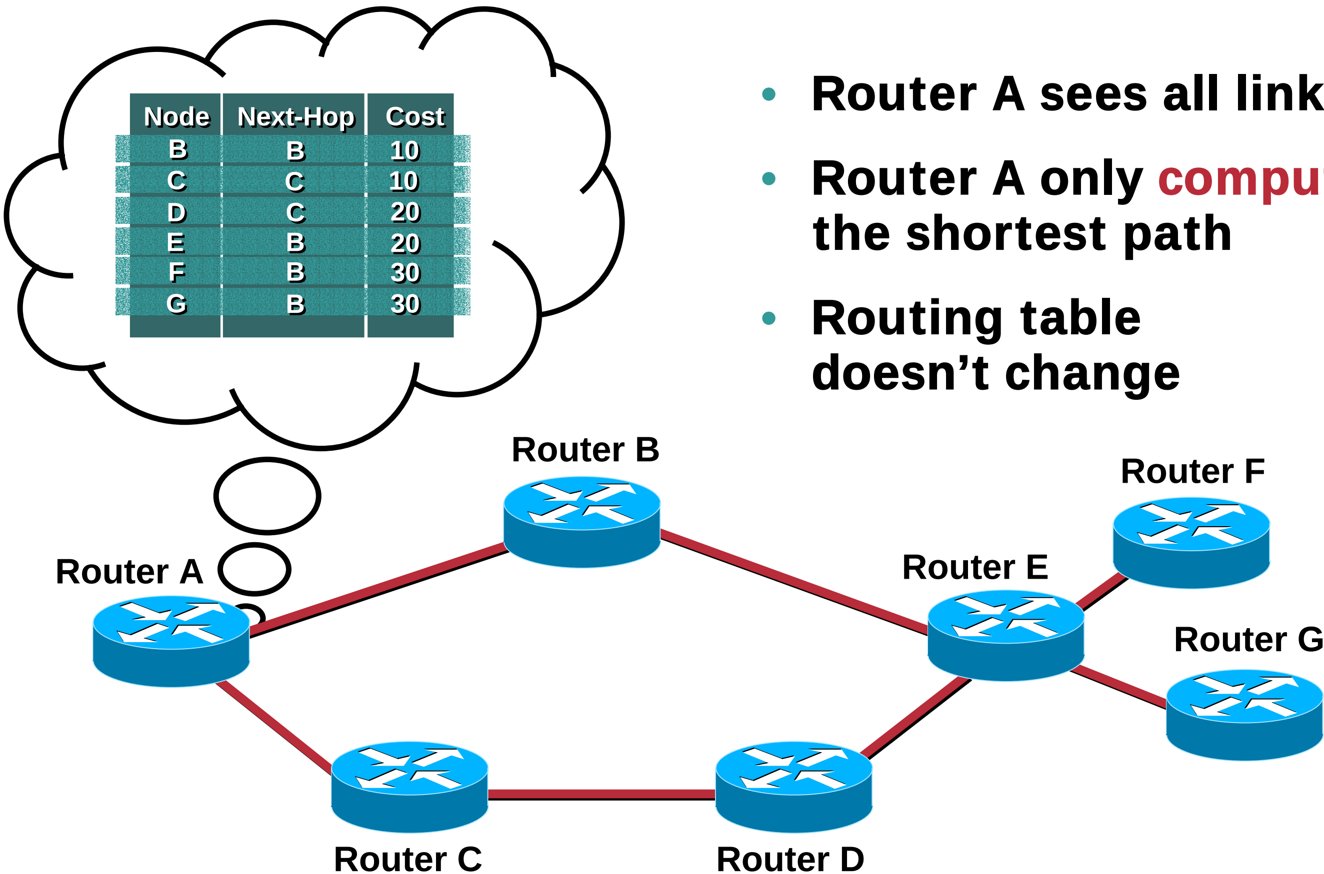
| Node | Next-Hop | Cost |
|---|---|---|
| B | B | 10 |
| C | C | 10 |
| D | C | 20 |
| E | B | 20 |
| F | B | 30 |
| G | B | 30 |




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

# What a LS Protocol Sees






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

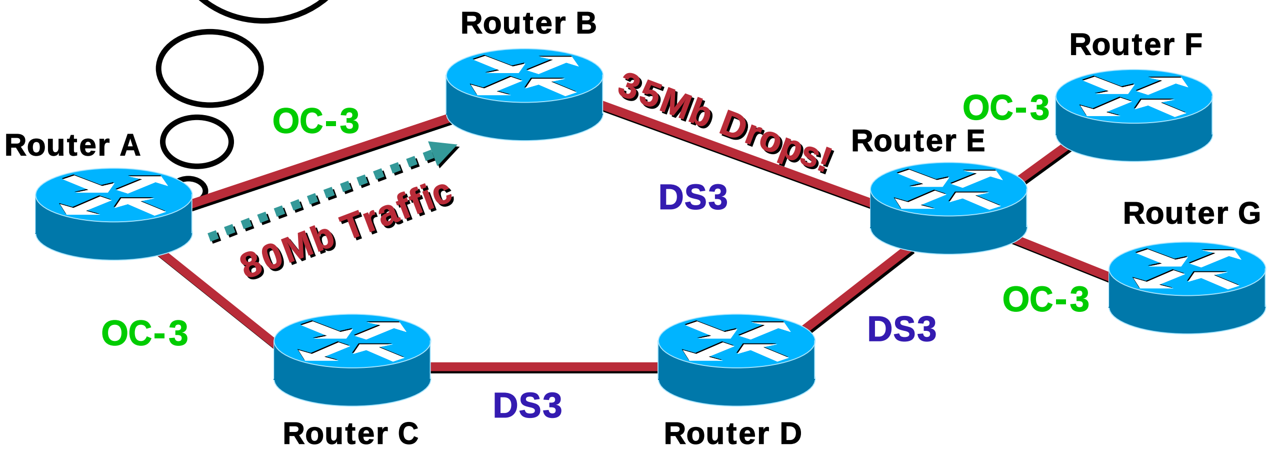
- **Router A sees all links**
- **Router A only computes the shortest path**
- **Routing table doesn't change**

# The Problem with Shortest-Path

Cisco.com

| 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

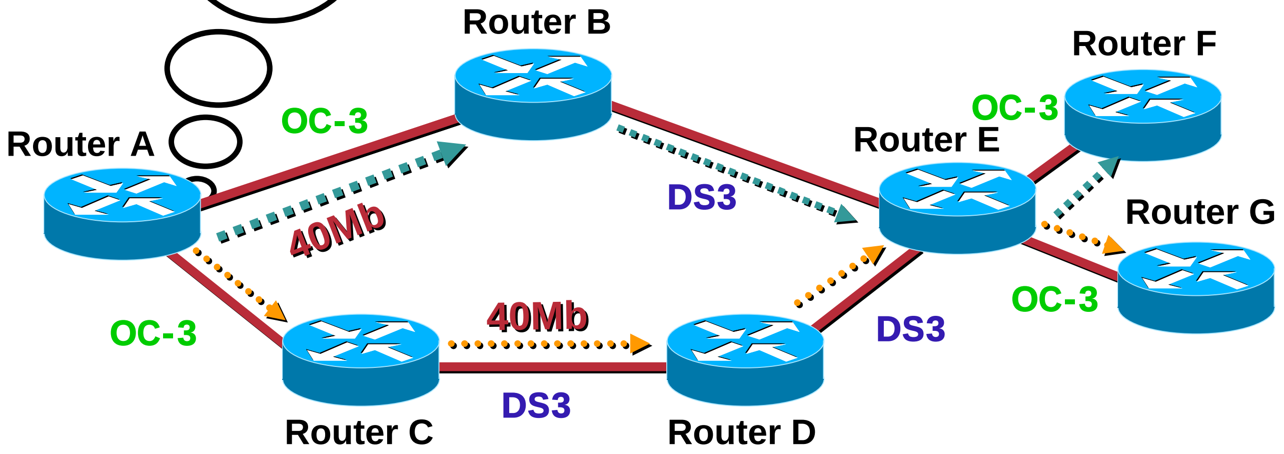


# How MPLS TE Solves the problem



| 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!**



# 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
- TE flooding is local to a single {area|level}
- Inter-Area TE available today; Inter-AS TE in the future

# Path Calculation

Cisco.com

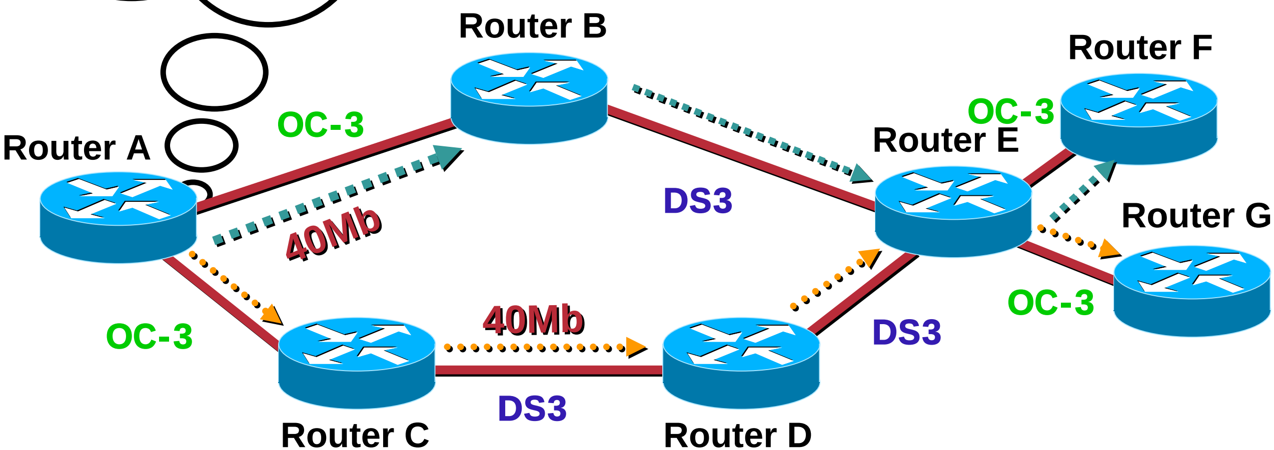
- Modified Djikstra at tunnel head-end
- Often referred to as CSPF
    - Constrained SPF
- ...or PCALC (path calculation)

# Path Calculation



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

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



# Path Calculation



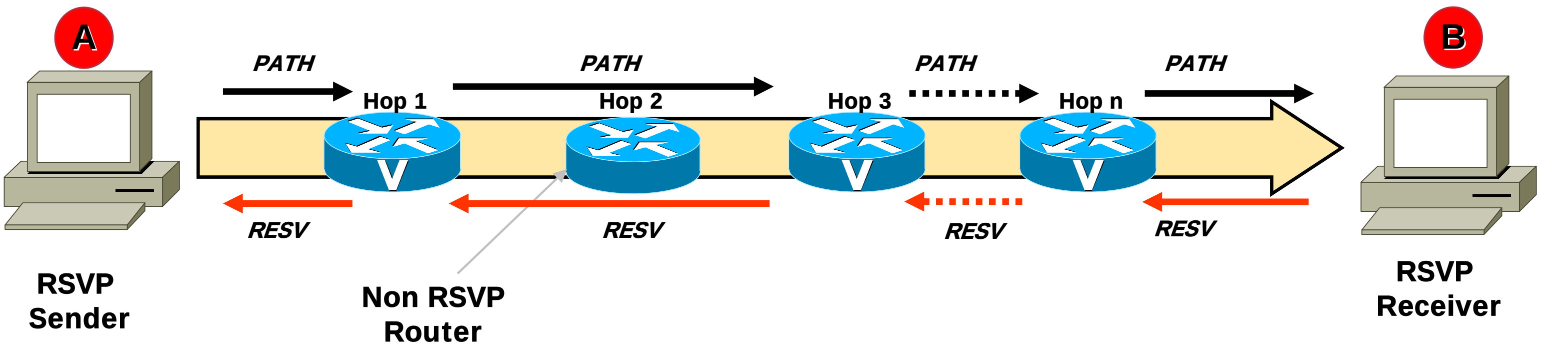
- What if there's more than one path that meets the minimum requirements (bandwidth, etc.)?
- PCALC algorithm: Find all paths with the lowest IGP cost
  1. Pick the path with the highest minimum available bandwidth along the path
  2. Then pick the path with the lowest hop count (not IGP cost, but hop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

# Path Setup: RESV and PATH Messages

Cisco.com

- Path messages

A Server generates PATH message toward requested receiver. PATH messages are fwd'ed to each hop



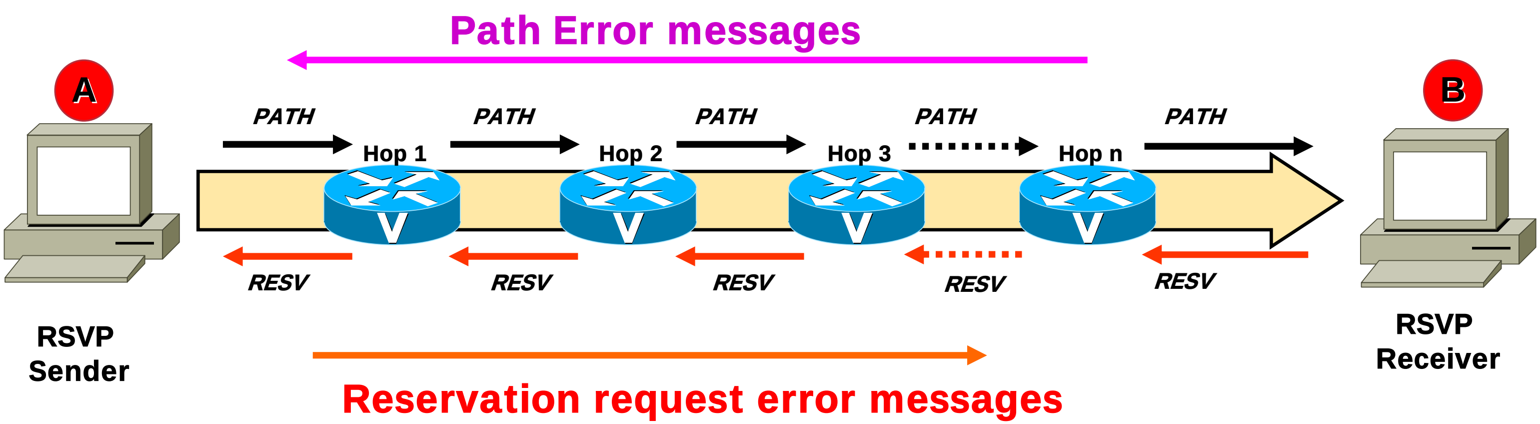

B *Receiver generates RESV message which inversely traverses the path.*

- Reservation request messages

# ERROR Messages

Cisco.com

- Path Error messages result from path messages and travel toward senders

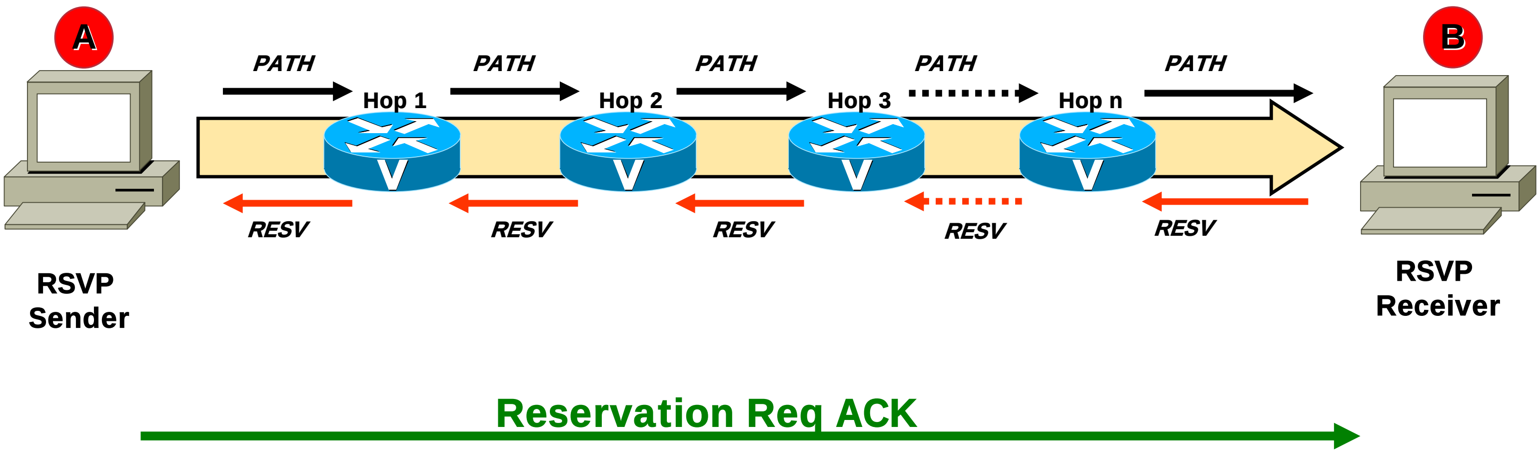



- Reservation request error messages →
  - Admission failure
  - Bandwidth unavailable
  - Service not supported
  - Bad flow specification
  - Ambiguous path

# Confirmation Messages

Cisco.com

- Reservation request acknowledgment messages

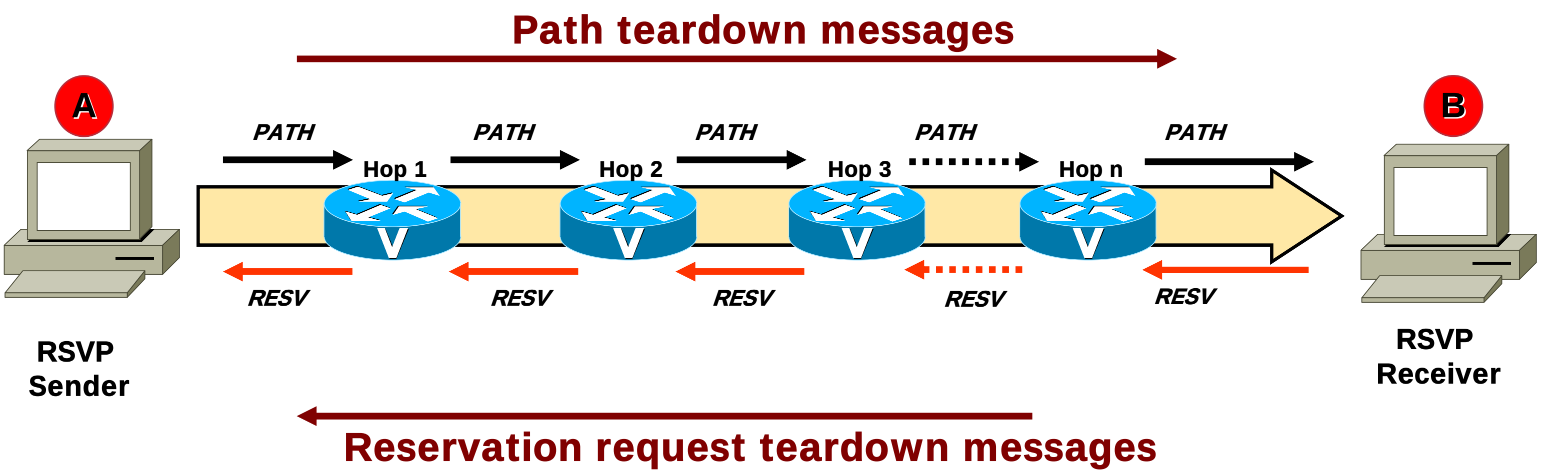



- These messages travel towards the receiver.

# Teardown Messages

Cisco.com

Two Types
- Path teardown messages
- Reservation request teardown messages

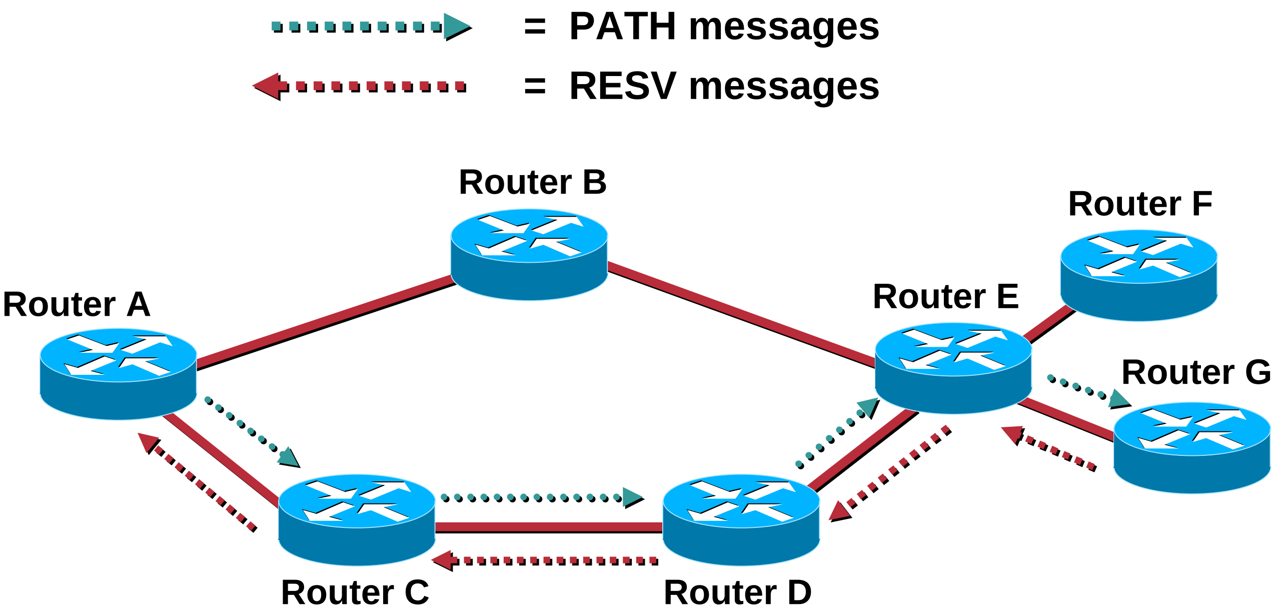



**Both types travel from the point of initiation**

# Path Setup for MPLS TE



- 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



# Forwarding Traffic Down a Tunnel



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

# Auto-Route

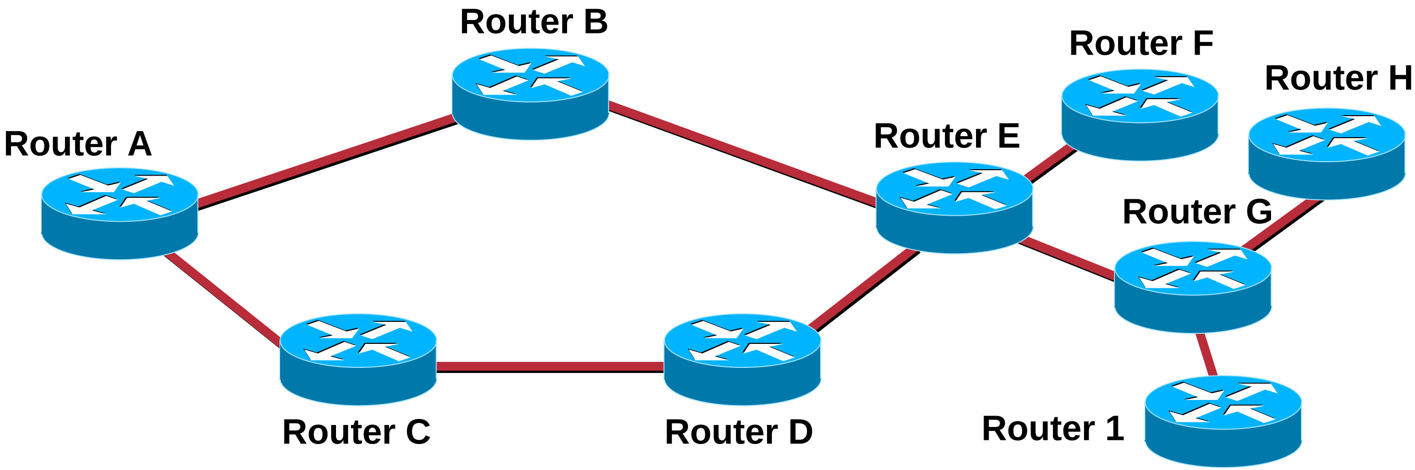
Cisco.com

- Auto-route = “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

# Auto-Route



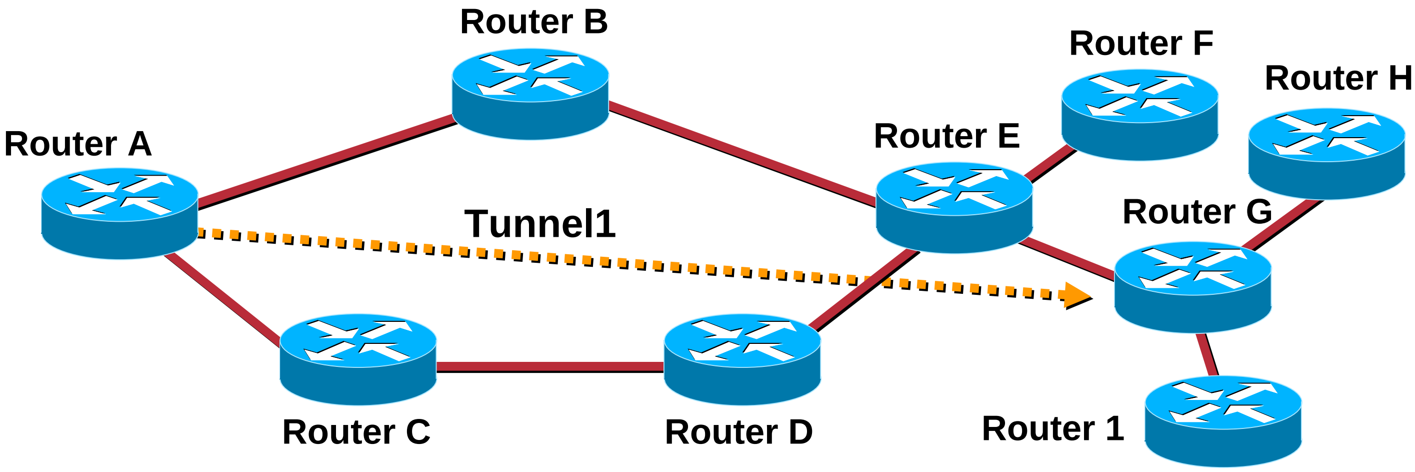
## This Is the Physical Topology



# Auto-Route



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

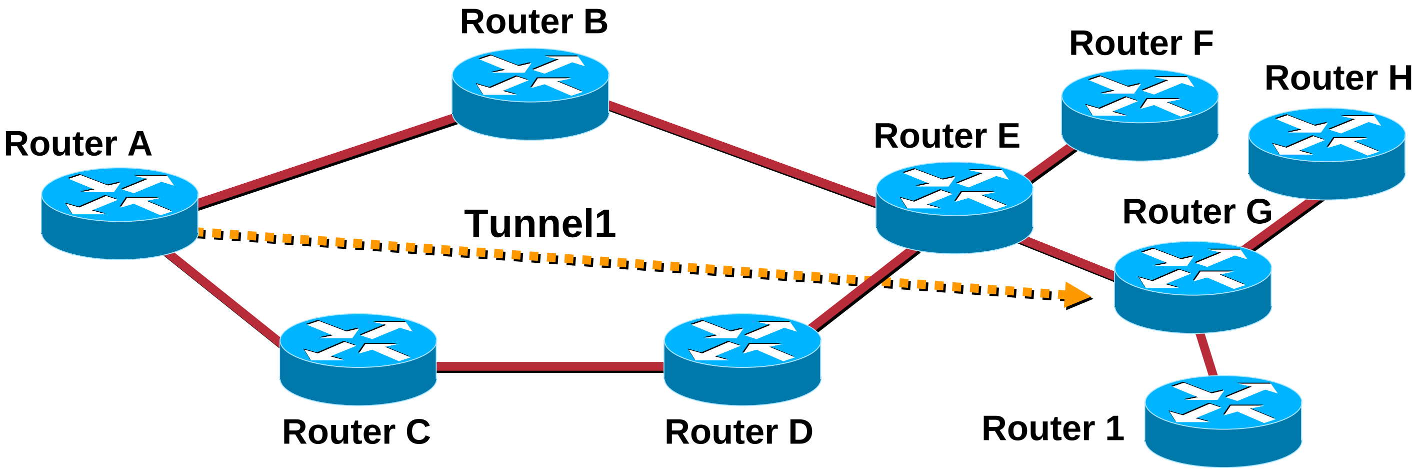


# Auto-Route



| 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



# Unequal Cost Load Balancing

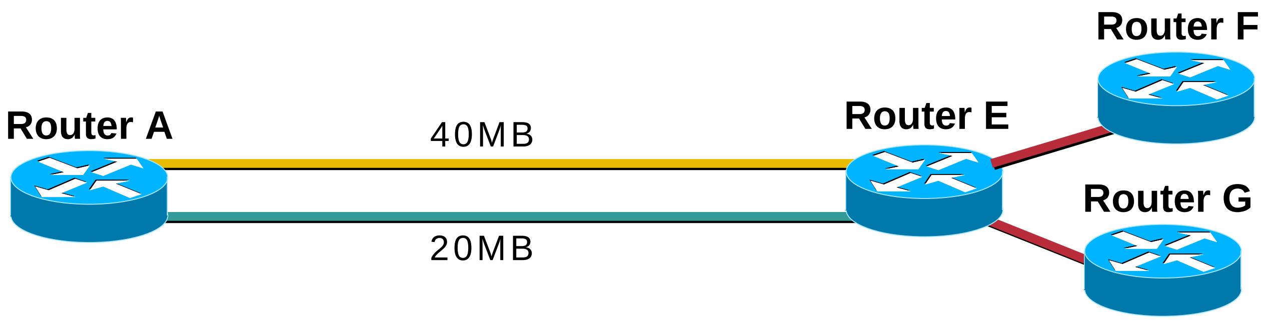


- IP routing has equal-cost load balancing, but not unequal cost*
- Unequal cost load balancing difficult to do while guaranteeing a loop-free topology
- Since MPLS doesn't forward based on IP header, permanent routing loops don't happen
- 16 hash buckets for next-hop, shared in rough proportion to configured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

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

# Unequal Cost Load Balancing

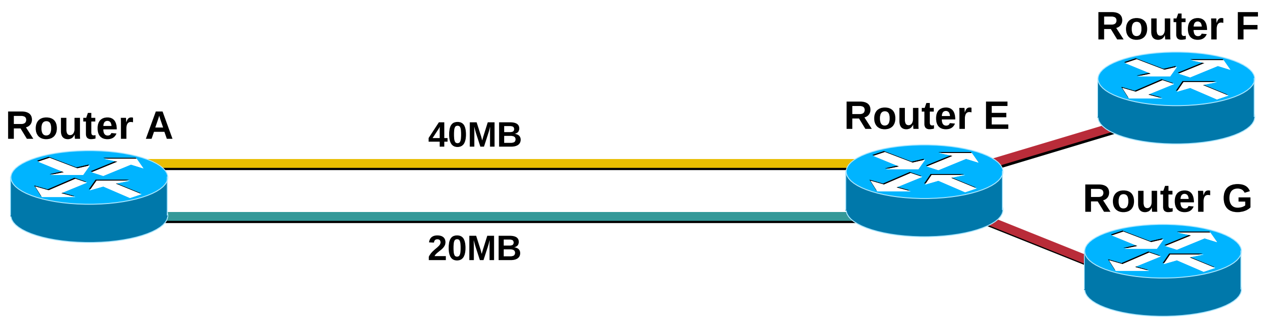
Cisco.com




```
gsr1#show ip route 192.168.1.8
Routing entry for 192.168.1.8/32
  Known via "isis", distance 115, metric 83, type level-2
  Redistributing via isis
  Last update from 192.168.1.8 on Tunnel0, 00:00:21 ago
  Routing Descriptor Blocks:
  * 192.168.1.8, from 192.168.1.8, via Tunnel0
      Route metric is 83, traffic share count is 2
    192.168.1.8, from 192.168.1.8, via Tunnel1
      Route metric is 83, traffic share count is 1
```

# Unequal Cost Load Balancing

Cisco.com




```
gsr1#sh ip cef 192.168.1.8
........
Load distribution: 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 (refcount 1)
  Hash   OK   Interface                 Address          Packets  Tags imposed
  1      Y    Tunnel0                   point2point            0    {23}
  2      Y    Tunnel1                   point2point            0    {34}
........
```

**Note That the Load Distribution Is 11:5—Very Close to 2:1, but Not Quite!**

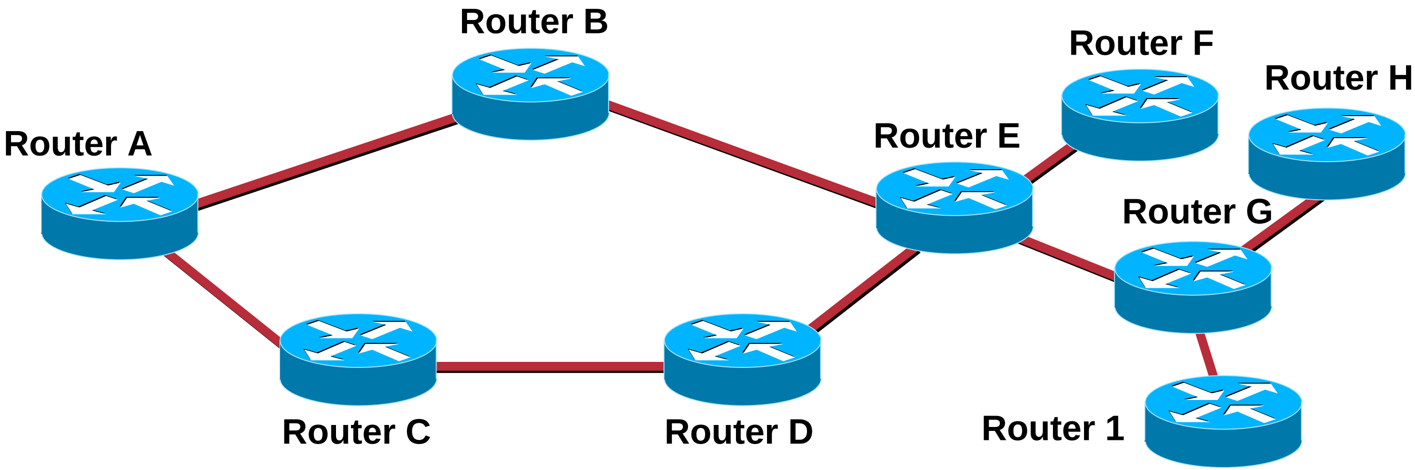
# Static Routing



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

**OR**

**RtrA(config)#ip route vrf FOO H.H.H.H 255.255.255.255 Tunnel1**

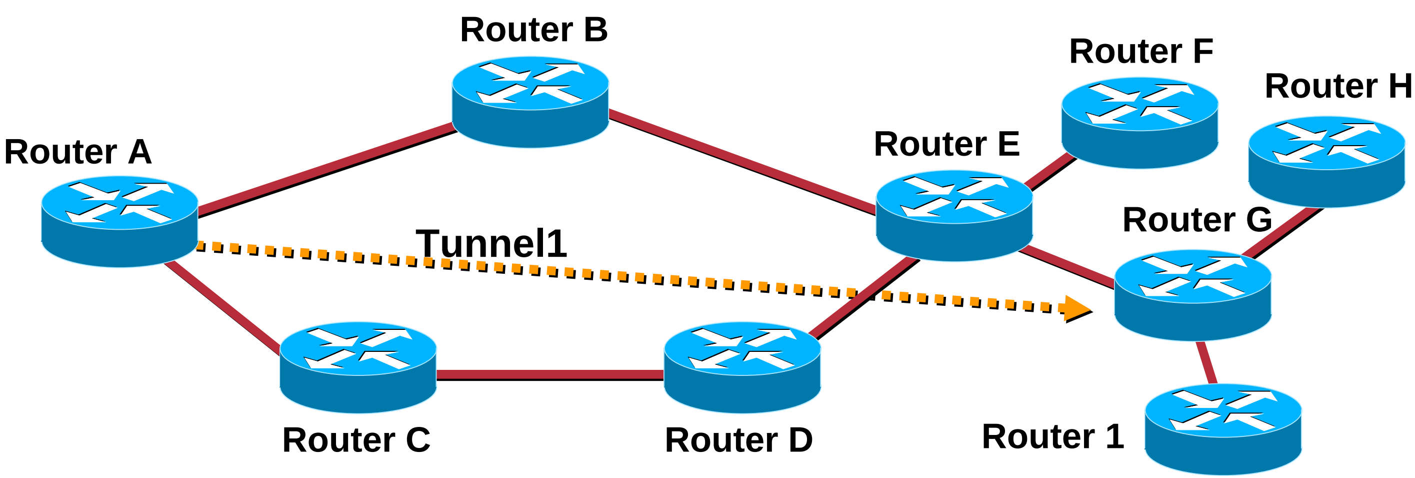


# Static Routing

Cisco.com

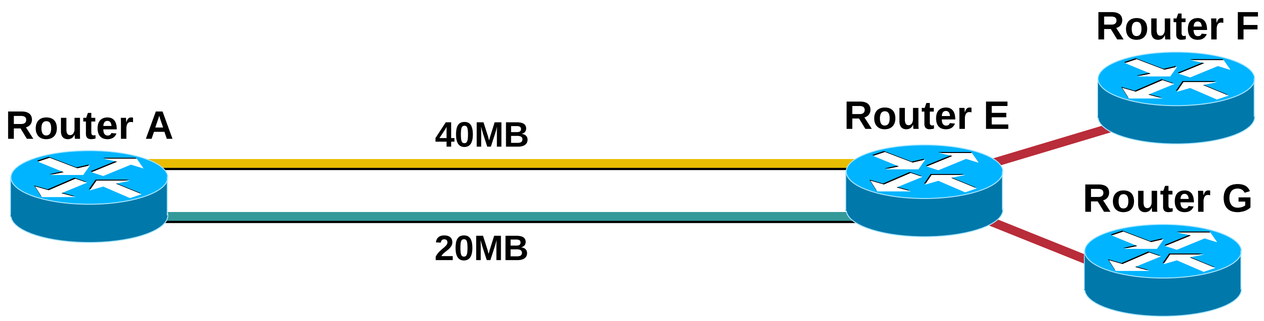
| Node | Next-Hop | Cost |
|---|---|---|
| B | B | 10 |
| C | C | 10 |
| D | C | 20 |
| E | B | 20 |
| F | B | 30 |
| G | B | 30 |
| H | Tunnel 1 | 40 |
| I | B | 40 |

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



# Static Routing





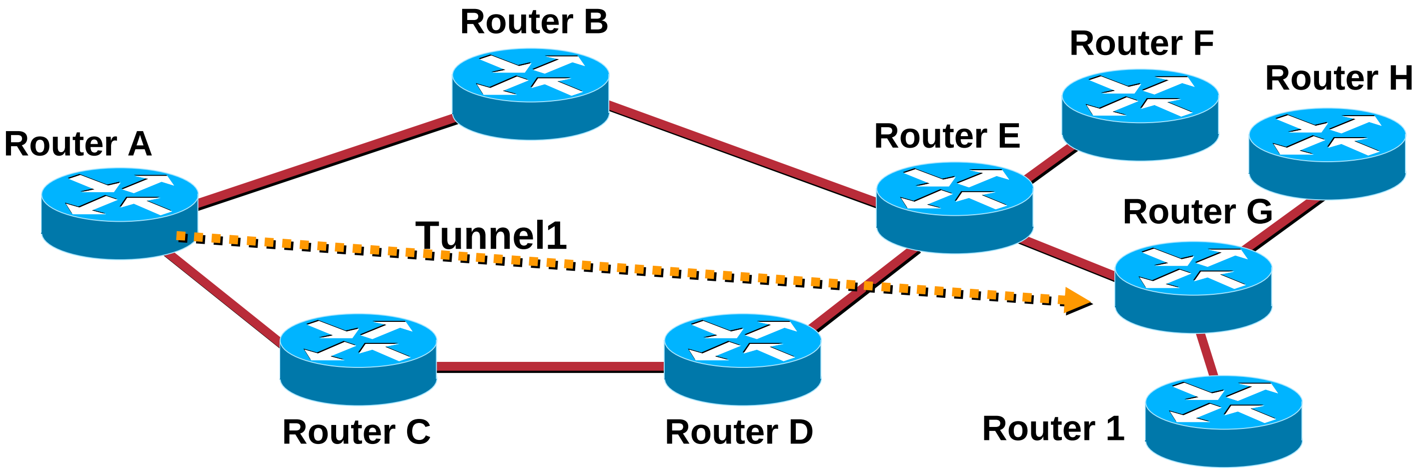

```
gsr1(config)#ip route 1.2.3.4 255.255.255.255 192.168.1.11
gsr1#sh ip cef 1.2.3.4
……..
Load distribution: 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 (refcount 1)
  Hash  OK  Interface                 Address         Packets  Tags imposed
  1      Y   Tunnel0                   point2point           0    {23}
  2      Y   Tunnel1                   point2point           0    {34}
……..
```

**Static Routes Inherit Unequal Cost Load-Sharing When Recursing through a Tunnel**

# Policy Routing



```
RtrA(config-if)#ip policy route-map set-tunnel
RtrA(config)#route-map set-tunnel
RtrA(config-route-map)#match ip address 101
RtrA(config-route-map)#set interface Tunnel1
```

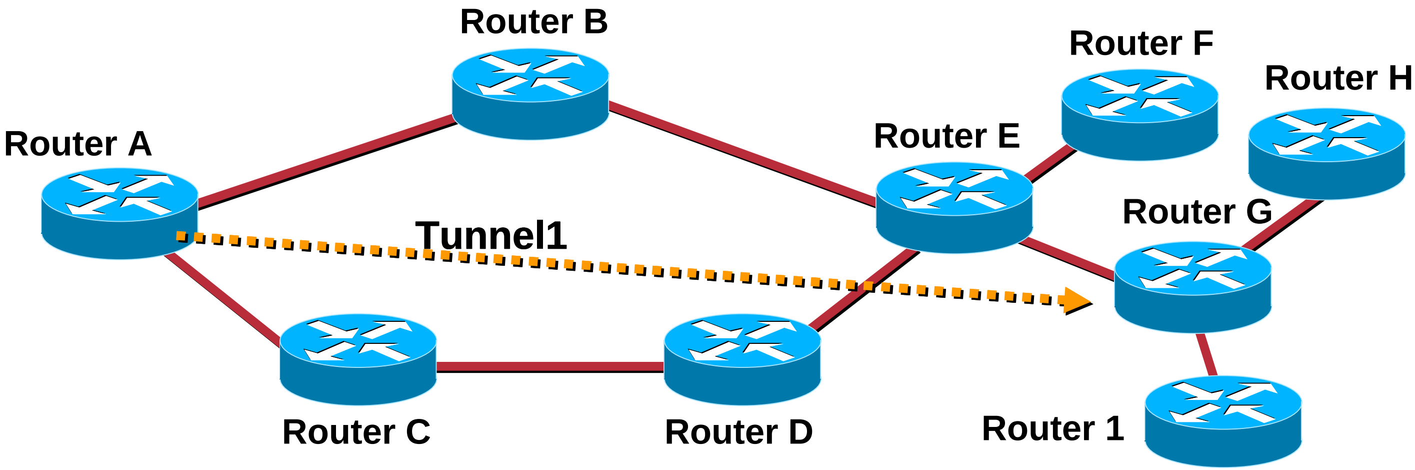


# Policy Routing



| 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)**



# Standardization - IETF



- **Information Distribution**
  - **OSPF Working Group**
    **Uses type 10 (opaque area—local) LSAs**
    **See draft-katz-yeung-ospf-traffic (9th version)**
  - **IS-IS Working Group**
    **Uses Type 22 TLVs**
    **See draft-ietf-isis-traffic (4th version)**
- **Path Setup**
  - **Rfc2205 – Resource ReSerVation Protocol**
  - **Rfc3209 – Extensions to RSVP for LSP Tunnels**

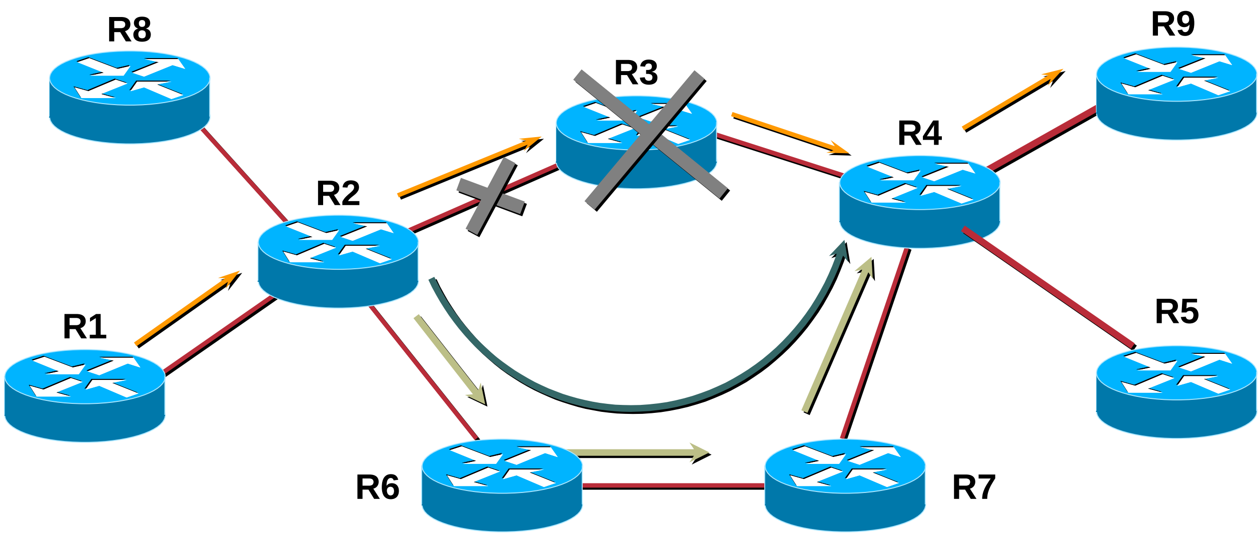
# Agenda



- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

# Protection Problem - Link and Node Protection



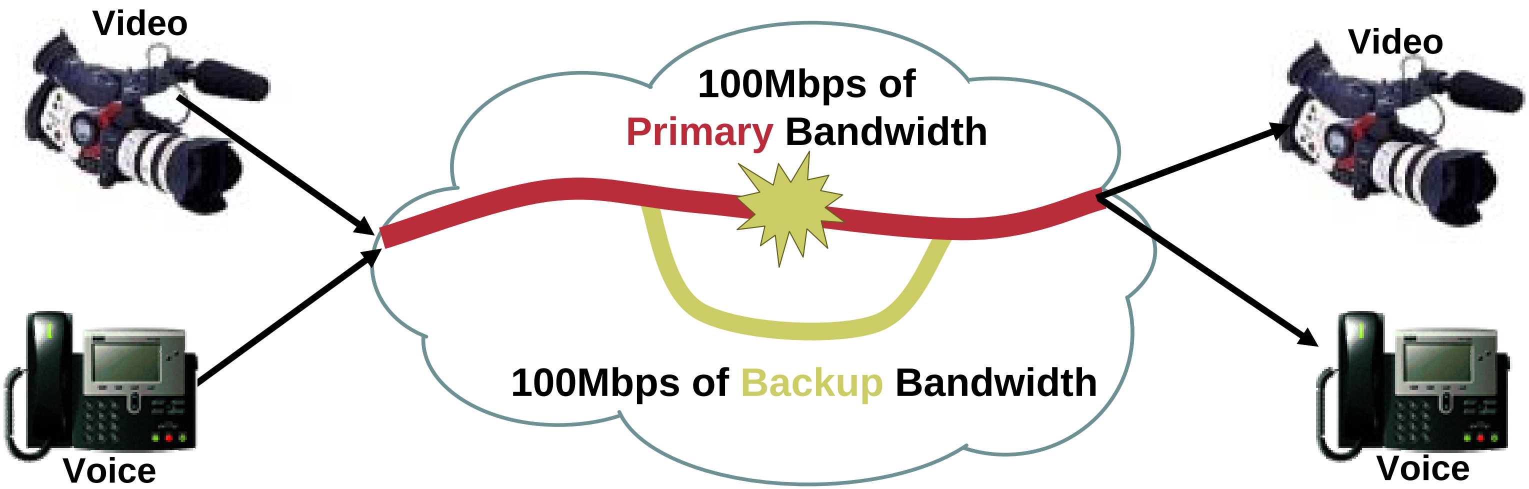



- Routing Convergence after failure takes minutes – advertise, computation time
- Mimic SONET/SDH Protection - Reroute in 50ms or Less
- Connectivity Protection => Bandwidth Protection

# What is Bandwidth Protection?

Cisco.com

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.

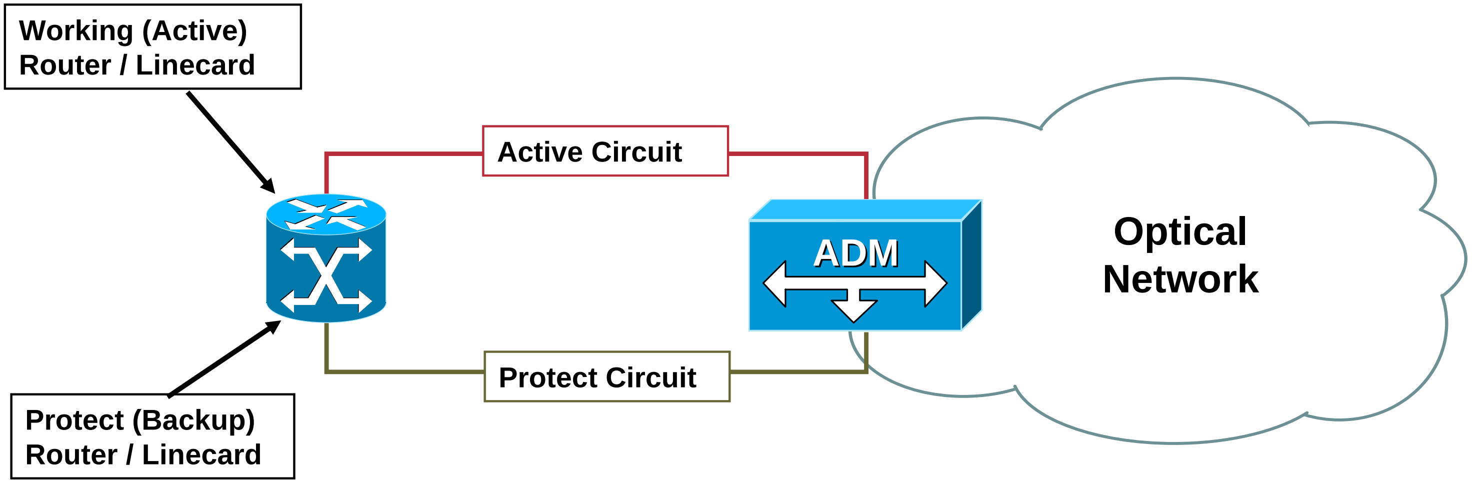



Bandwidth Protection is NOT a new problem – but using MPLS we have a new paradigm to provide a solution

# Current Approaches to Providing Bandwidth Protection

Cisco.com

## SONET Automatic Protection Switching (APS) / SDH Multiplexed Switching Protection (MSP)




**Results in 1:1 Backup Bandwidth that is non-revenue generating**

# Issues with SONET APS / SDH MPS



## Business

- Very High Operating Expenses (OPEX) – Recurring costs in redundant circuits
- High Capital Expenses (CAPEX) – External Muxes or Linecards/Router ports

## Technical

- Dedicated redundant circuits known as ‘protect circuit’ required
- Does not leverage unused bandwidth in a network
- Node/Router failures cannot be handled
- IP routing convergence still takes seconds, beyond 50ms of physical layer

*Very Expensive!!*

# What Service Providers Yearn for...

Cisco.com

## Business

- Increase Revenues – better SLAs – Ability to provide bandwidth from point A to B irrespective of the operational state of the network
- Reduce Capital Expenses – leverage existing infrastructure
- Reduce Operating Expenses – reduce recurring circuit costs

## Technical

- Backup Bandwidth needs to be shared – multiple simultaneous failures are rare
- Networks tend to run at sustained 50% 60% utilization – a lot of unused bandwidth is available
- Link failures are most common, however Node/Router failures need to be addressed
- Human brain can perceive bad voice quality within 150 milliseconds – failures need to happen well within this timeslot – 50 milliseconds

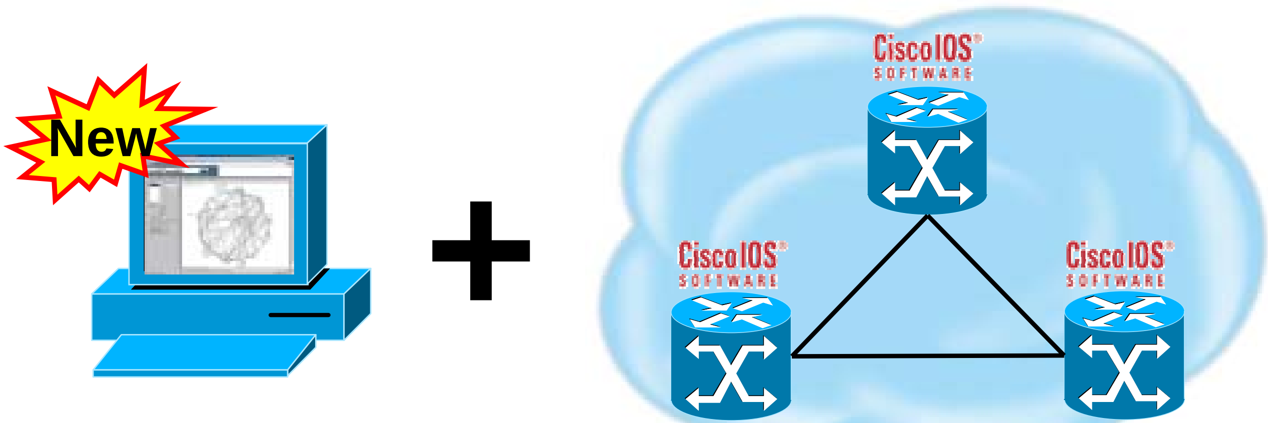
***Need flexible and cost effective protection scheme !!***

# Cisco's MPLS Bandwidth Protection Solution



## Introducing Tunnel Builder Pro & IOS Enhancements

**Solution consists of a Centralized Server - Tunnel Builder Pro - that computes backup tunnels used by MPLS Traffic Engineering Fast Reroute in Cisco IOS®, such that a bandwidth guarantee can be met during a failure condition**




**Tunnel Builder Pro** + **IOS® MPLS TE Fast Reroute**

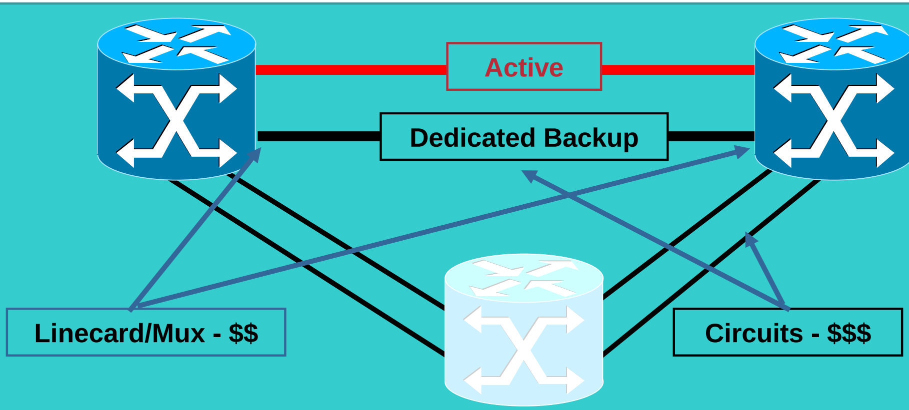
# SONET APS/SDH MSP vis-à-vis Cisco MPLS Bandwidth Protection



## SONET/SDH

**Considerations:**

- Cost of dedicated backup circuits
- Cost of additional ports
- Mesh underutilized



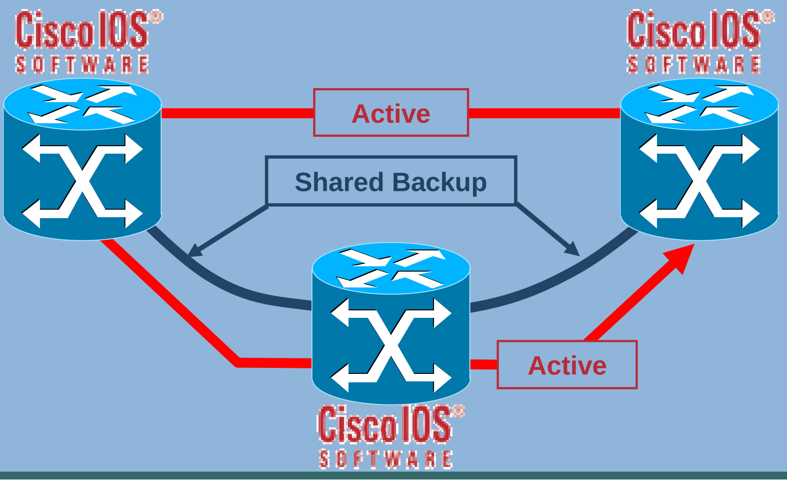

## Bandwidth Protection using MPLS

**Considerations:**

- Cost of Tunnel Builder Pro

**Advantages:**

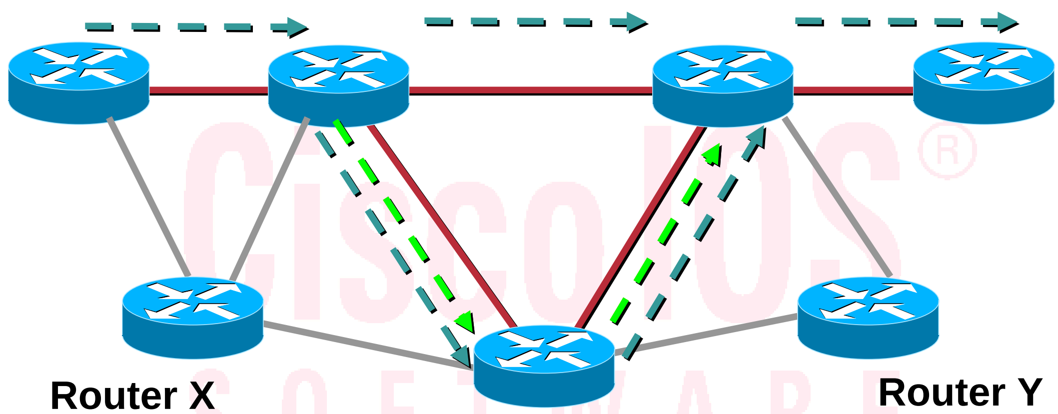
- Mesh fully utilized



# Link Protection*

Enhanced 12.0(22)S

Cisco.com



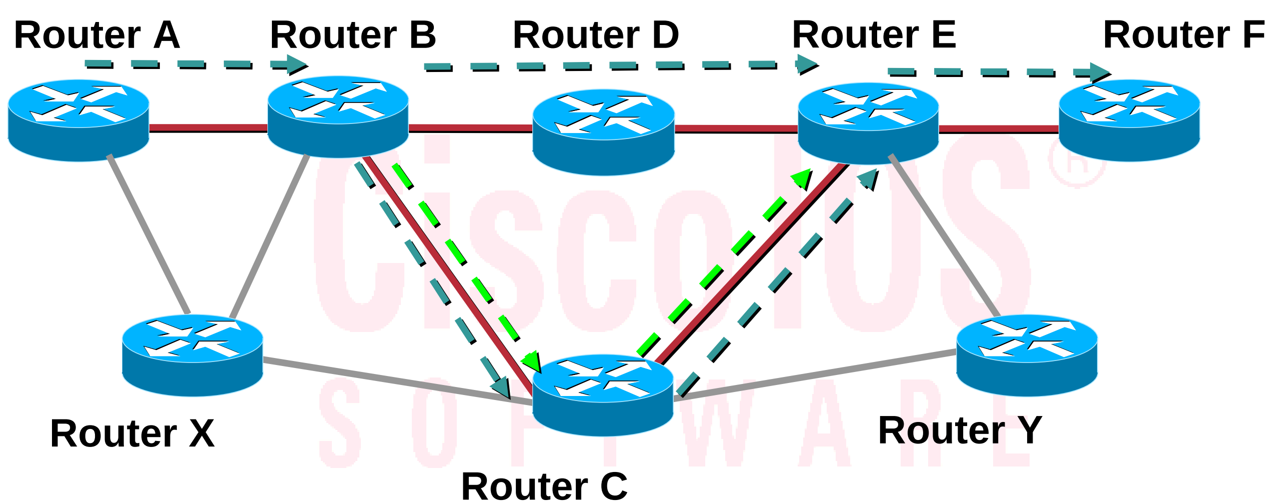

- Primary Tunnel: A->B->D->E
- BackUp Tunnel: B->C->D (Pre-provisioned)
- Recovery = ~50ms

*Introduced in 12.0(11)ST

# Node Protection

New
12.0(22)S

Cisco.com



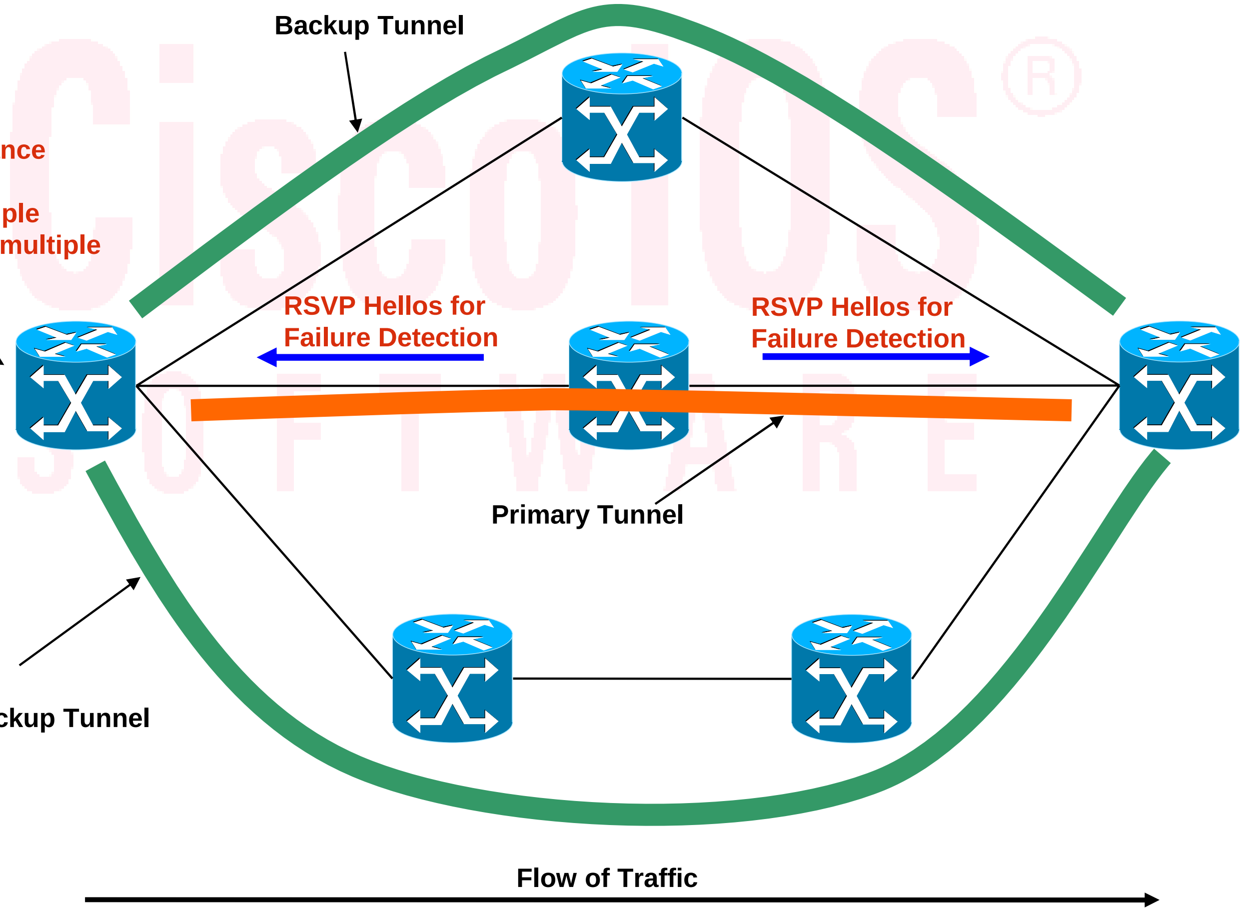

- **Primary Tunnel: A->B->D->E->F**
- **BackUp Tunnel: B->C->E (Pre-provisioned)**
- **Recovery = ~100ms**

# RSVP Hellos and Backup Path Management

New 12.0(22)S

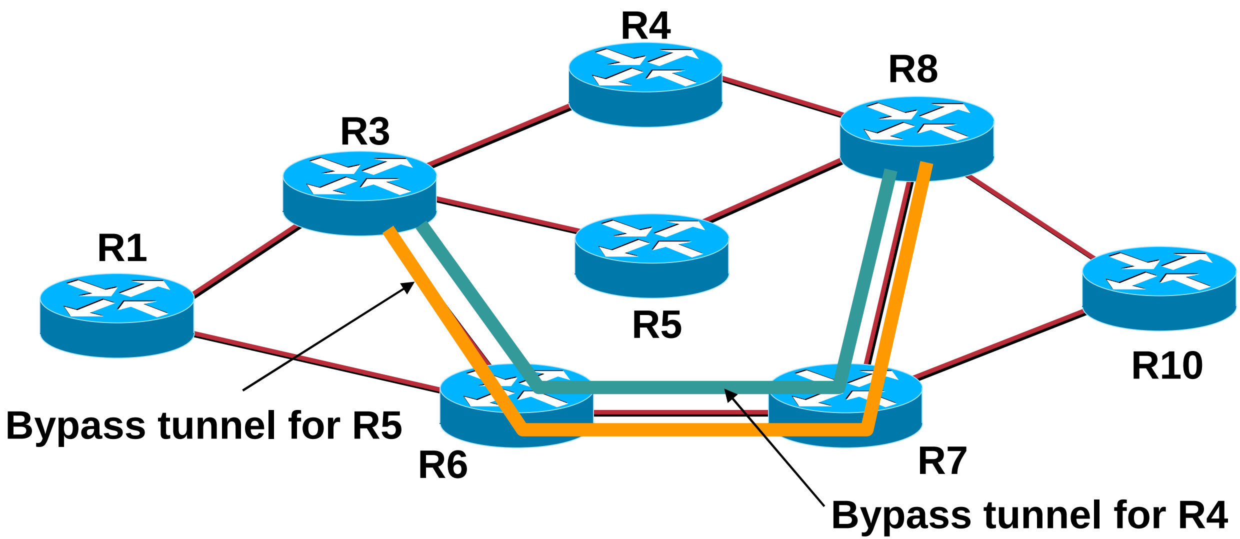
Cisco.com

•Ability to load balance
•Ability to promote
•Ability to use multiple backup tunnels for multiple primary tunnels



# Scenario 1: Backup Bandwidth Sharing

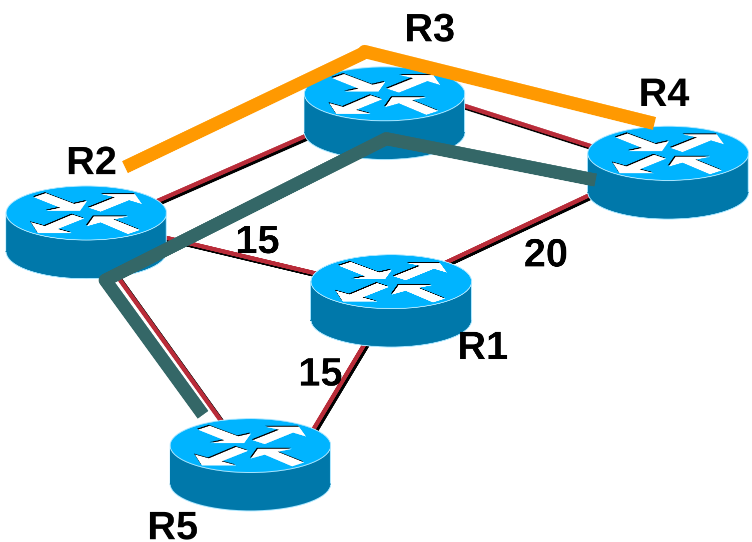





- **Only need to allocate enough BW on R3-R6-R7-R8 to protect for a single node failure – "N:1" protection**

# 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

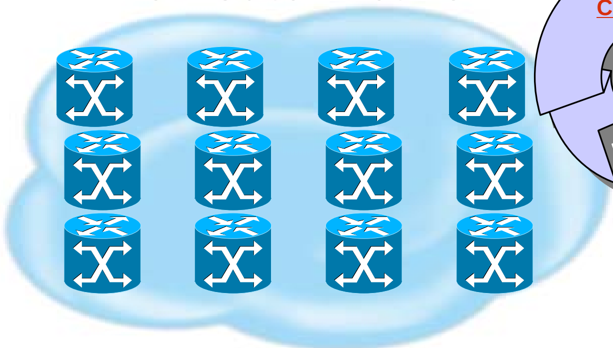
# Bandwidth Protection – The Complexity

Cisco.com

## 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**

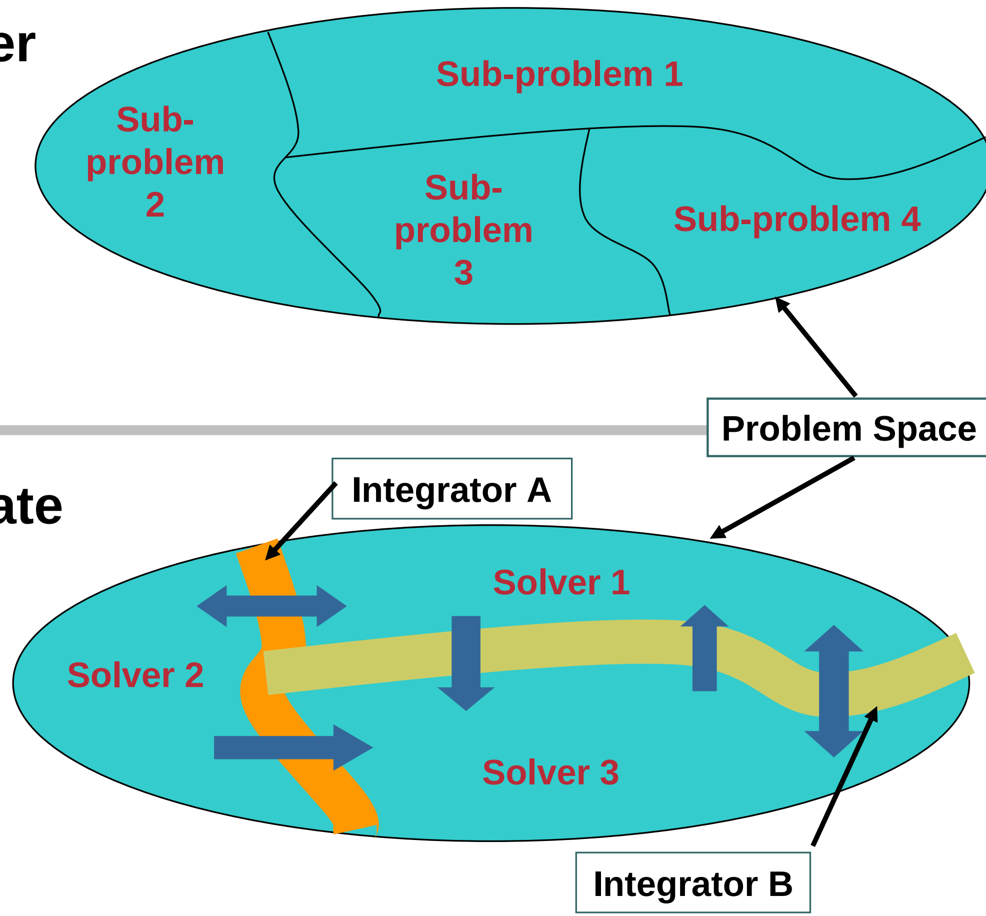
***A sophisticated mathematical algorithm is needed !!***

# Hybrid Optimization Algorithms at Work



## 1. Divide and Conquer

## 2. Search and Integrate



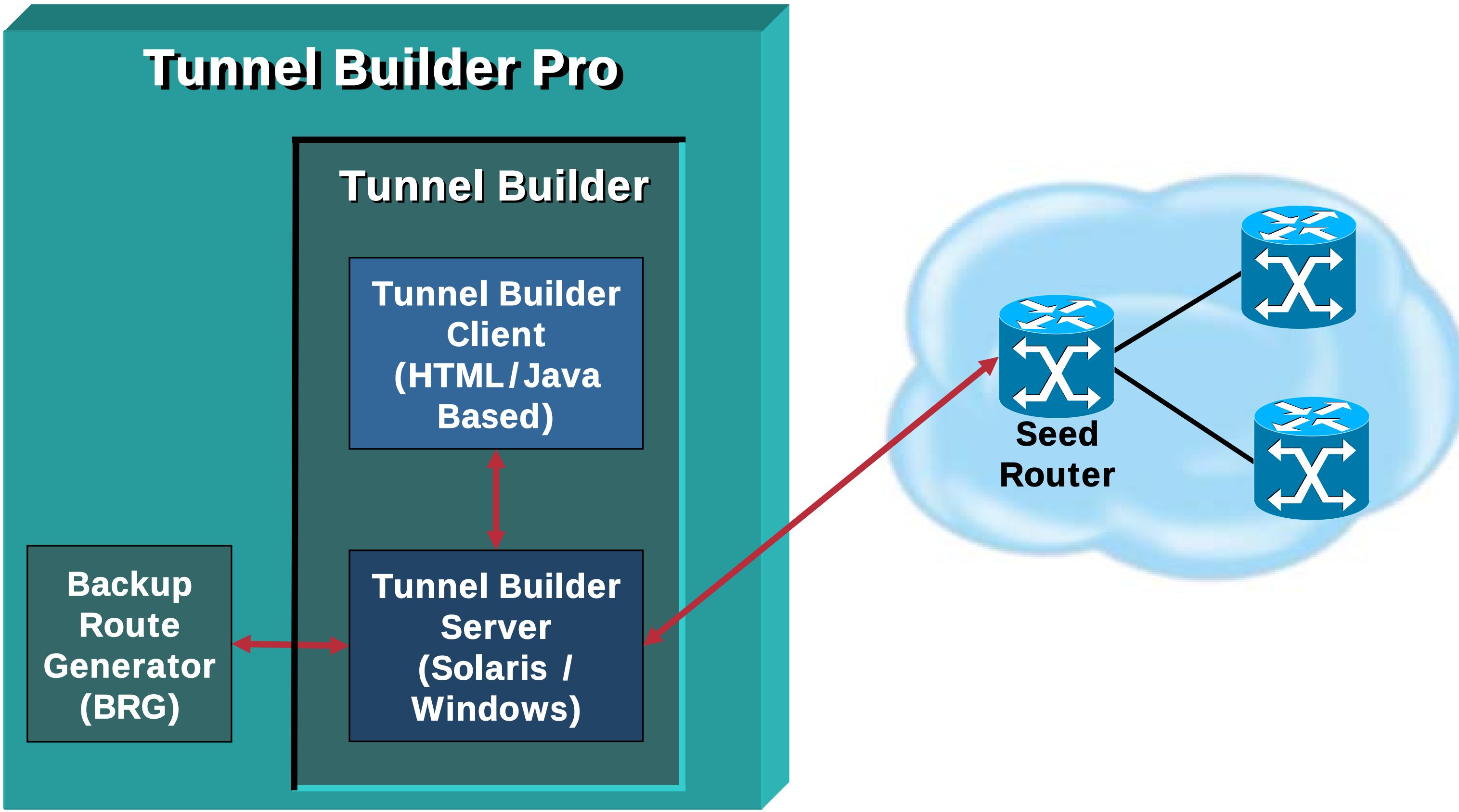
# Cisco MPLS Tunnel Builder Pro – A brief history



- A Cisco centralized server application
- Joint development with PARC Technologies for backup route generation
- PARC Technologies:
  - Headquartered in London, England
  - PARC Technologies is a leading developer of optimization and search software – especially Hybrid Optimization problems that are NP-complete
  - Has proven solutions in other areas - Airline Industry Operations Management

# Cisco MPLS Tunnel Builder Pro





# TB Pro versus Constrained Shortest Path First (CSPF)

Cisco.com

## Node Protection, Comparative Results

**Network 1 Backbone - 152 router protection scenarios**

| Algorithm | Protected | Proved Impossible | No solution found |
|---|---|---|---|
| CSPF Based | 54 | 12 | 86 |
| TB Pro | 134 | 17 | 1 |

**Network 2 backbone - 100 router protection scenarios**

| Algorithm | Protected | Proved Impossible | No Solution found |
|---|---|---|---|
| CSPF Based | 28 | 0 | 72 |
| TB Pro | 98 | 2 | 0 |

**TB Pro running on a Intel PIII @ 1Ghz with 1G RAM for approx. 20 minutes**

# Cisco Differentiation: Bandwidth Protection Using MPLS



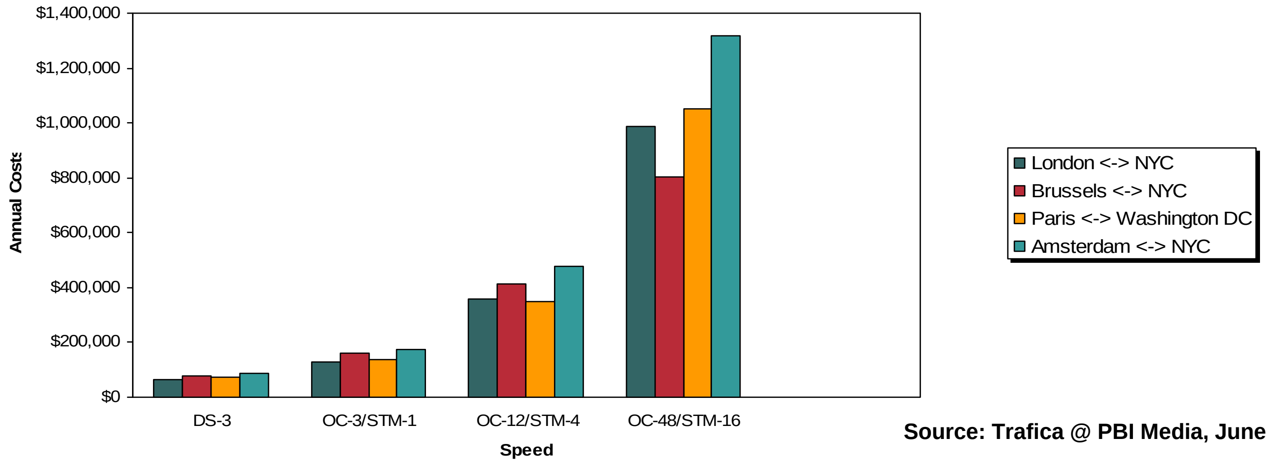
Cisco IOS SOFTWARE

| | Cisco FRR with TBPro | FRR w/o BW Protection | SONET APS / SDH MSP |
|---|---|---|---|
| Recovery in milliseconds | Y | Y | Y |
| Link Protection | Y | Y | Y |
| Node Protection | Y | Y | N |
| Efficient Use of Bandwidth | Y | Y | N |
| Bandwidth Guarantees | Y | N | Y* |
| Cost | $** | $ | $$$ |

* Against link failure only ** Cost of TB Pro is relatively small

# A Quick ROI Analysis






**Source: Trafica @ PBI Media, June 2002**

| | SONET APS/ SDH MSP | Cisco MPLS Bandwidth Protection |
|---|---|---|
| Capital Expenses | ~$150,000 – OC-48 Linecard | $300,000 – TB Pro List |
| Operating (Recurring) Expenses | $800,000 – OC-48 Circuit | No additional costs |
| Total (for 10 Routers)* | $16.15 million | $5.55 million |

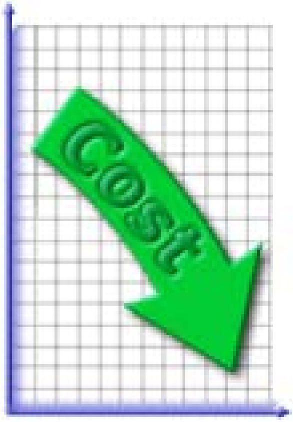
**Phenomenal Savings!!!**

*Degree of connectivity – 3.4; Total – 17 links; 70% adoption rate of MPLS BW Protection; Training Costs - $400K

# Bandwidth Protection using MPLS: Reduced Costs



Provide a simple low cost alternative to SONET/SDH Protection Solution
Can also be used in a complimentary manner




- Reduces overall cost of network protection by eliminating non revenue producing backup circuits and associated additional routers/linecards
- Leverages unused bandwidth and eliminates over-provisioning
- Reduces penalty payments for SLA violations
- Enables infrastructure convergence by reliable transport of Voice, Video and Data over MPLS enabled IP networks
- Reduces Management costs by providing easy to use GUI

# Bandwidth Protection using MPLS: Increased Revenues



**Provide a flexible "carrier class" SLA**


- **Allows for higher degree of bandwidth control**
  - **Lesser Packet Loss for Voice / Video traffic**
  - **Better control on Delay – higher Voice / Video quality**
  - **Reduced Jitter providing for fewer out of order packets**
- **Allows "carrier class" SLAs**
  - **Offer "Protected" circuits**
  - **Offer "Unprotected" circuits**

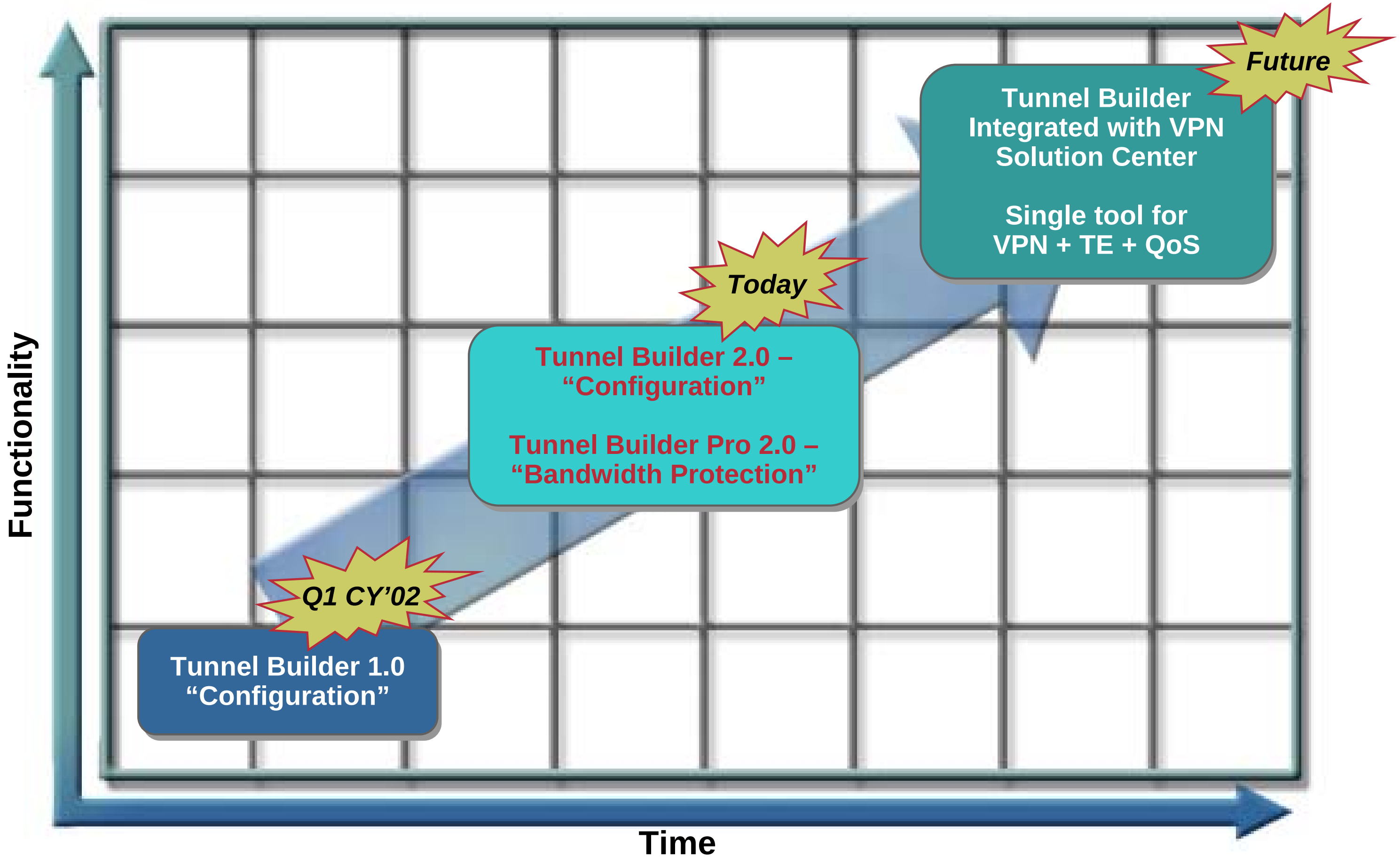
# Availability



| Technology | Availability | Value-add |
|---|---|---|
| Tunnel Builder 2.0<br>Tunnel Builder Pro 2.0 | September 2002 | Simplifies configuration of MPLS TE tunnels thru' GUI<br>Provides bandwidth protection for "carrier class" SLAs and reduced costs |
| MPLS TE Link and Node Protection, with RSVP Hellos Support | IOS® Release 12.0(22)S | Provides protection for link failure<br>Provides protection for node failure<br>Provides ability to have Backup Bandwidth Pool<br>Uses RSVP Hellos to support non-POS interfaces – Fast Ethernet / Gigabit Ethernet<br>Backup Path Management – Promotions, Multiple Backup Tunnels |

# Tunnel Builder Roadmap

Cisco.com



# Cisco MPLS Bandwidth Protection - Summary



- **Reduce costs** – cost effective alternate to SONET/SDH protection
- **Additional Level of Protection** – Complements SONET/SDH protection
- **Leverage Unused Bandwidth** in the Network
- Enable Packet based **Infrastructure Convergence**
- Reduce **Network Management** costs
- Allow for **tighter control on bandwidth** – packet loss, delay & jitter
- Enable **"carrier class" SLAs**

# Standardization - IETF



- MPLS Working Group
  - Fast Reroute Extensions:
    draft-ietf-mpls-rsvp-lsp-fastreroute-01.txt
  - Fast Reroute MIB:
    draft-ietf-mpls-fastreroute-mib-01.txt
- IETF Drafts
  - Bandwidth Protection
    draft-vasseur-mpls-backup-computation-01.txt
  - Path Computation (eg. Inter-AS)
    draft-vasseur-mpls-computation-rsvp-02.txt

# Agenda



- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

# Relationship between MPLS TE and MPLS Diff-Serv



- **Diff-Serv specified independently of Routing/Path Computation**
- **MPLS Diff-Serv (RFC3270) specified independently of Routing/Path Computation**
- **MPLS TE designed as tool to improve backbone efficiency independently of QoS:**
  - **MPLS TE compute routes for aggregates across all Classes**
  - **MPLS TE performs admission control over “global” bandwidth pool for all Classes (i.e., unaware of bandwidth allocated to each queue)**
- **MPLS TE and MPLS Diff-Serv:**
  - **can run simultaneously**
  - **can provide their own benefit (ie TE distributes aggregate load, Diff-Serv provides differentiation)**
  - **are unaware of each other (TE cannot provide its benefit on <u>a per class basis</u> such as CAC and constraint based routing)**

# DiffServ aware Traffic Engineering (DS-TE)



- **DS-TE is more than MPLS TE + MPLS DiffServ**
- **DS-TE makes MPLS TE aware of DiffServ:**
  - **DS-TE establishes separate tunnels for different classes**
  - **DS-TE takes into account the "bandwidth" available to each class (e.g. to queue)**
  - **DS-TE takes into account separate engineering constraints for each class**

    e.g. *I want to limit Voice traffic to 70% of link max, but I don't mind having up to 100% of BE traffic*.

    e.g *I want overbook ratio of 1 for voice but 3 for BE*
  - **DS-TE may take into account different metrics (eg. delay)**
- **DS-TE ensures specific QoS level of each DiffServ class is achieved**

# So what is DS-TE?



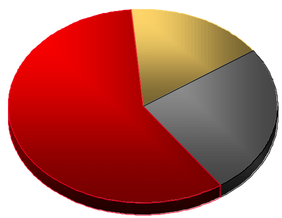
- DS-TE is an extension over existing MPLS TE
- DS-TE is a Control Plane (signalling) feature
- DS-TE is not a Data Plane (queuing, dropping, scheduling, classification) feature

# DS-TE Configuration Example
# Tunnel Midpoint



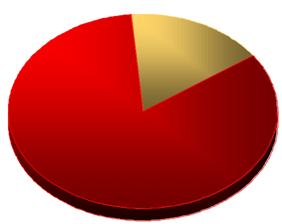
## Data Plane

Bandwidth Allocation



## Control Plane

Bandwidth Allocation



```
!
class-map match-all PREMIUM
 match mpls experimental 5
!
class-map match-all BUSINESS
  match mpls experimental 3 4
!
policy-map OUT-POLICY
  class GOLD
    priority 16384
  class SILVER
    bandwidth 65536
    random-detect
  class class-default
    random-detect
!
interface POS1/0
 ip address 10.150.1.1 255.255.255.0
 ip rsvp bandwidth 155000 155000 sub-pool 16384
 service-policy output OUT-POLICY
 mpls traffic-eng tunnels
 mpls ip
!
```

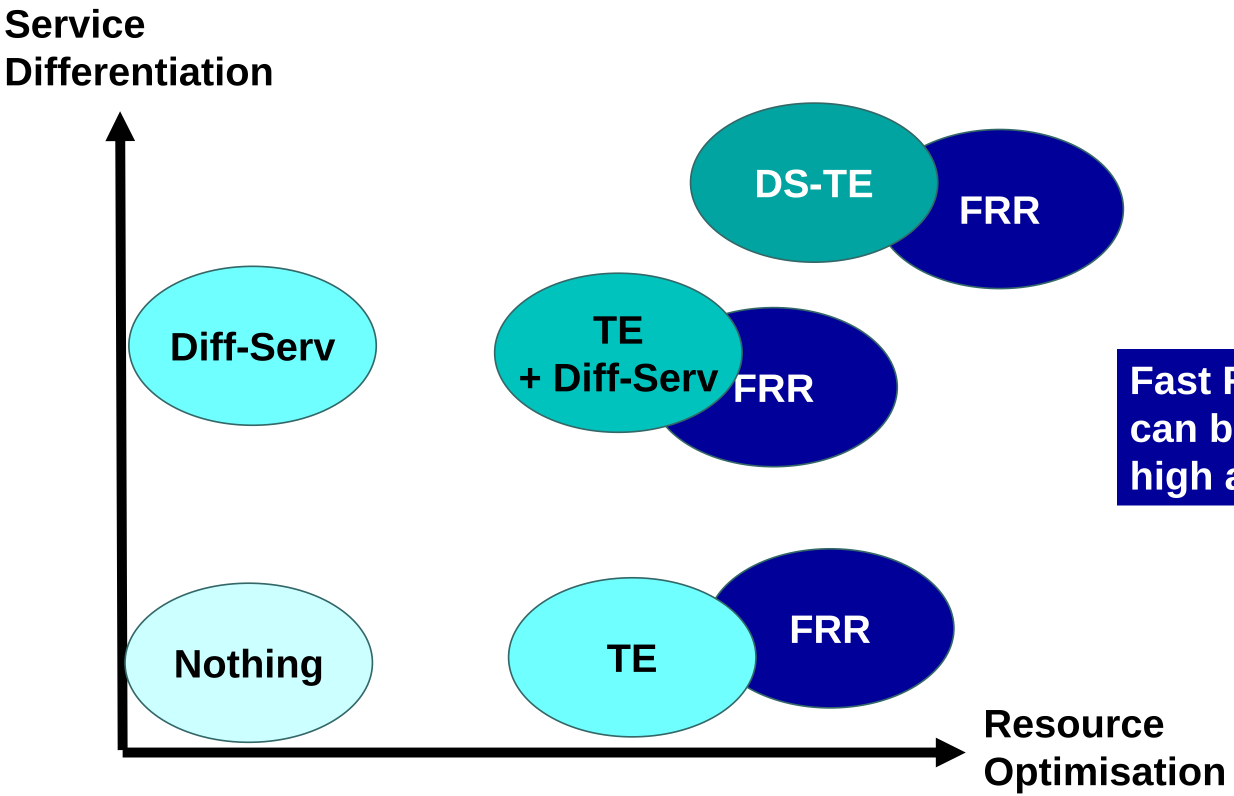
# DS-TE impact on IGP Scalability?



- IGP scalability is hardly impacted when going from TE to DSTE
  - IGP advertisement: Bw info is unchanged (ie still 8 Bw values)
  - IGP flooding: perhaps slightly more often (eg thresholds applied on multiple Unreserved Bw)
  - Path Computation: unchanged (only apply on different Bw value)

# Do I need DS-TE in my network?

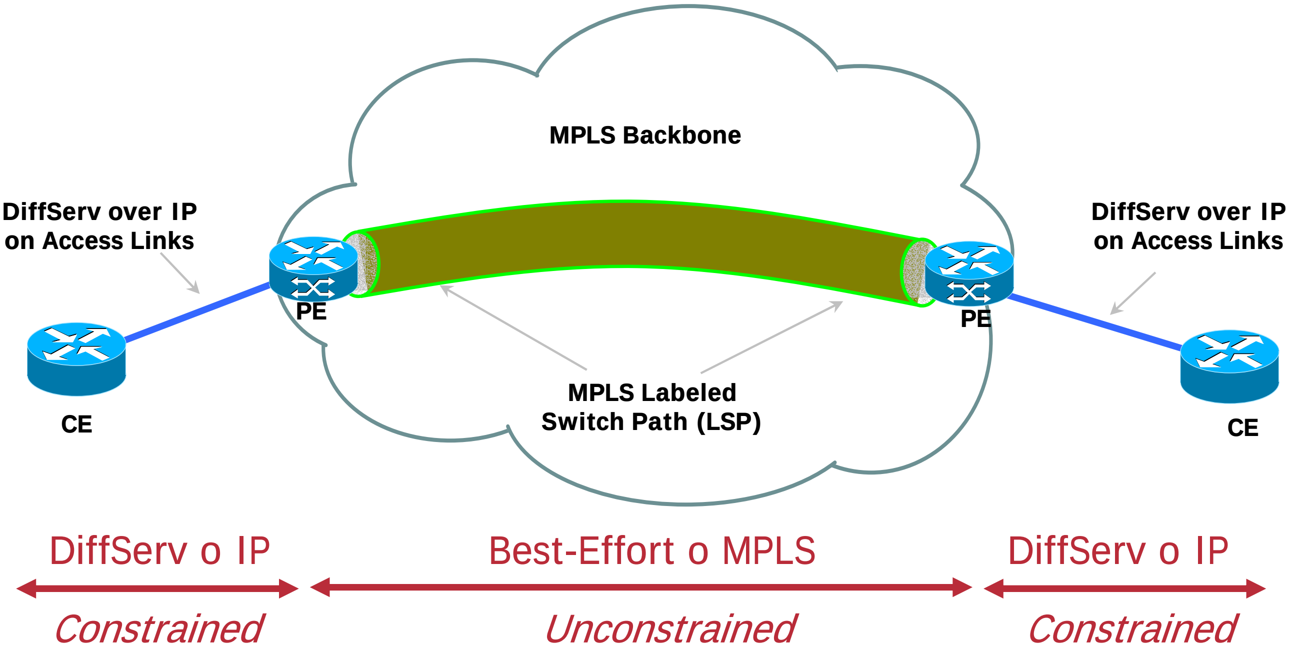





**Fast Reroute: can be added for high availability**

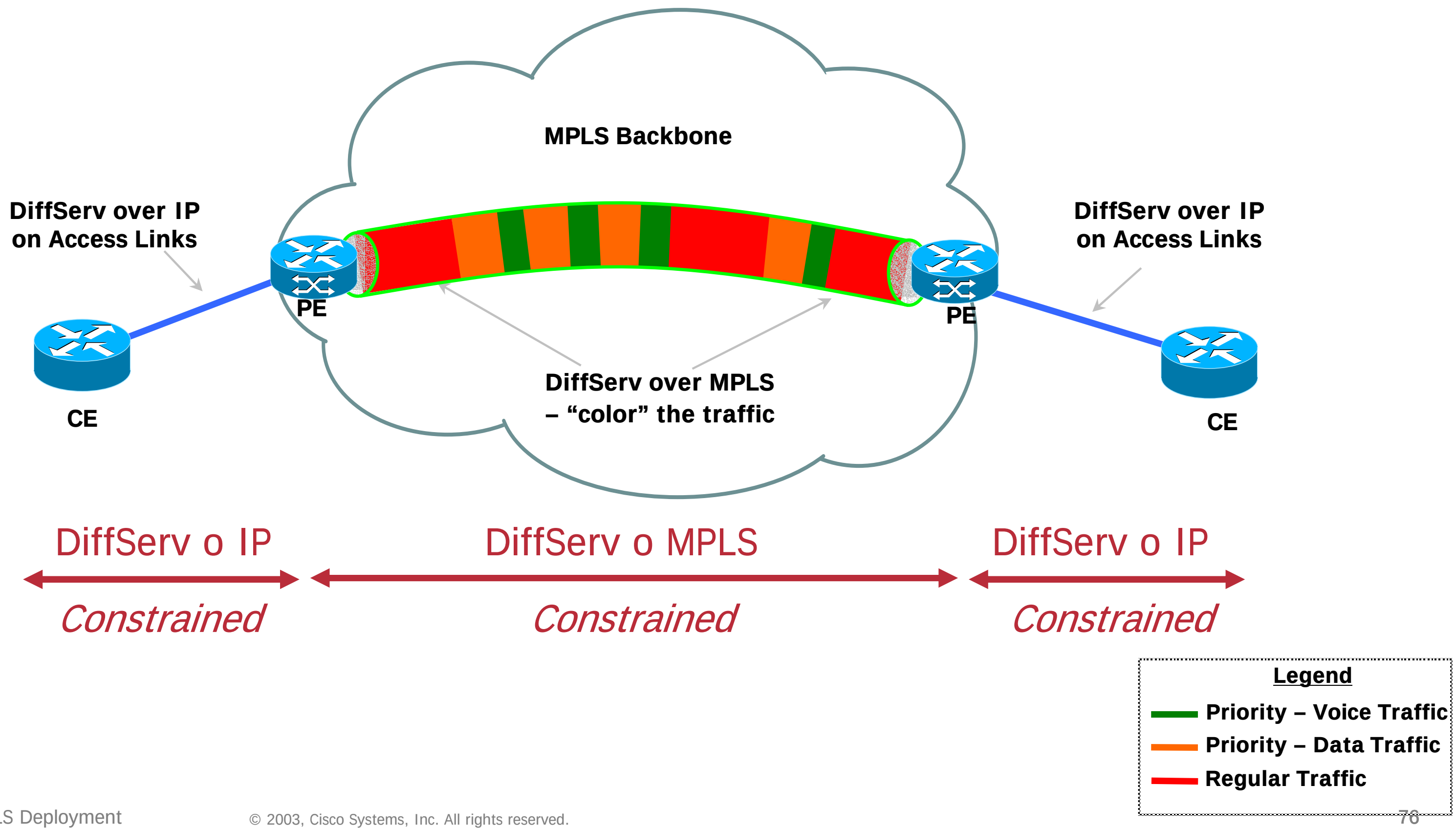
# Road to a QoS Optimized backbone – Step 1





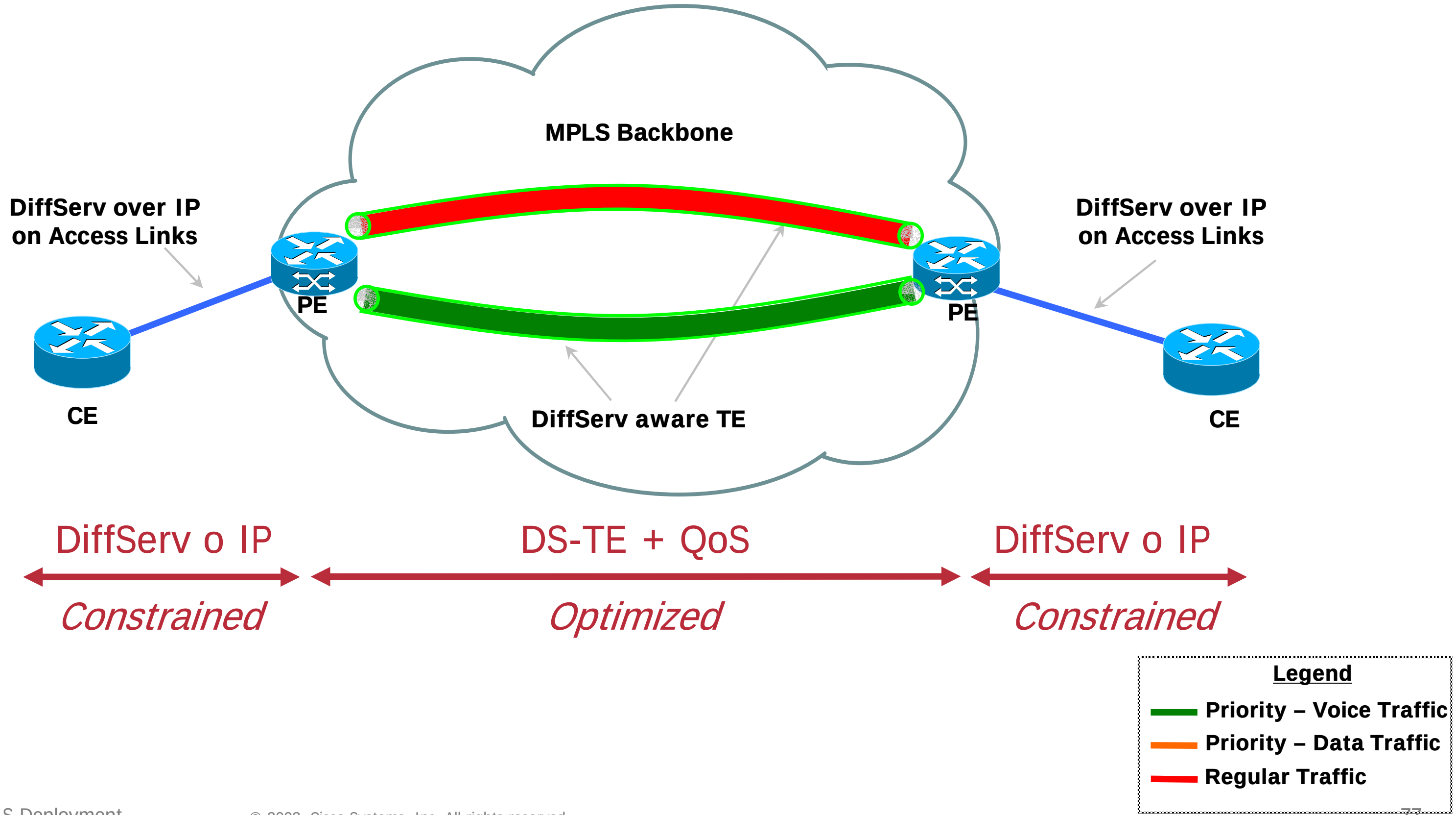
# Road to a QoS Optimized backbone – Step 2





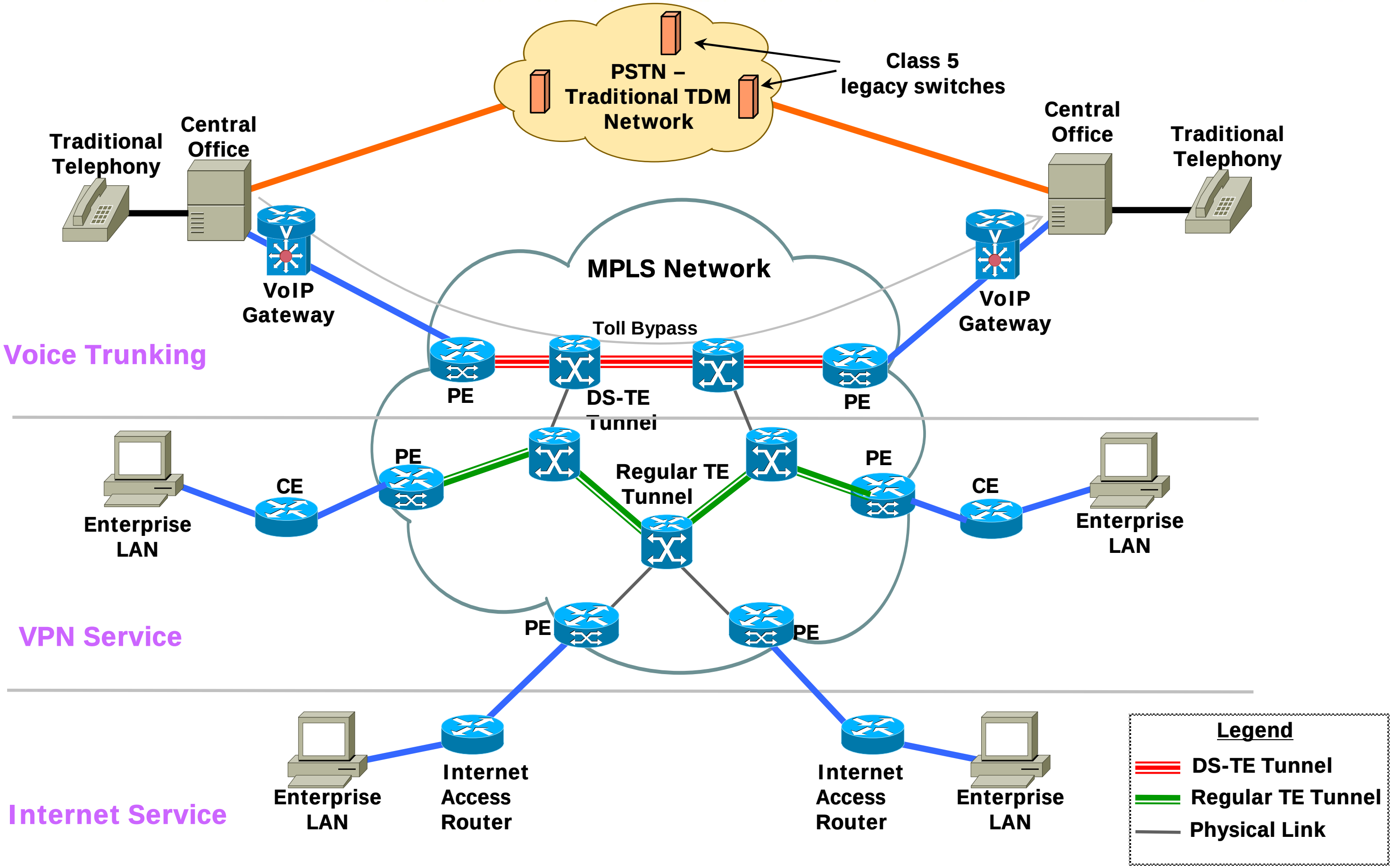
# Road to a QoS Optimized backbone – Step 3

Cisco.com



# Voice Trunking - Summary

Cisco.com



# Standardization - IETF



- Standardization effort initiated by Cisco mid 2000
- Now major work item of TEWG with broad support from SPs & vendors
- DS-TE Requirements: on its way to RFC (IETF Last Call)
  - draft-ietf-tewg-diff-te-reqts-06.txt
- DS-TE Protocol Extensions: Working Group document
  - Draft-ietf-tewg-diff-te-proto-02.txt
  - Consensus on protocol extensions
  - Selection of Bandwidth Constraints model still under discussion

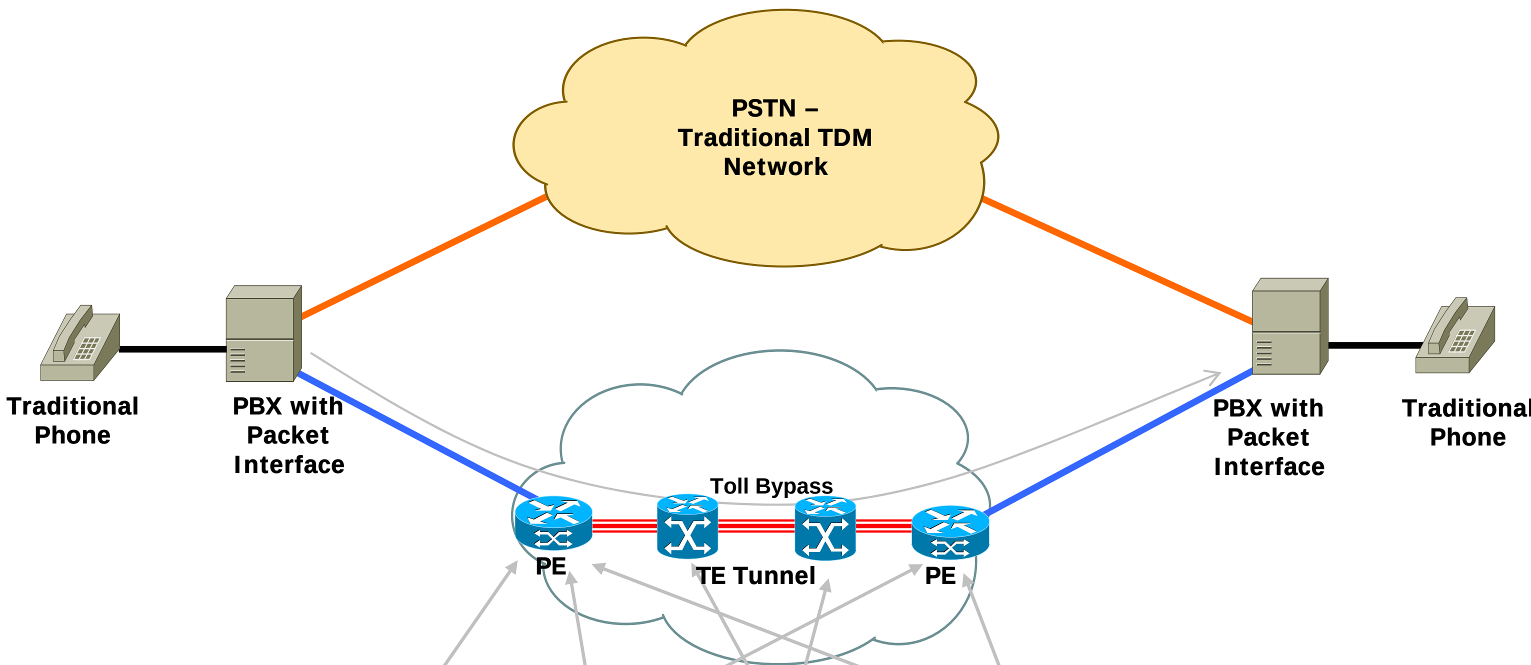
# Agenda



- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

# Solution 1: Toll Bypass with Voice Network

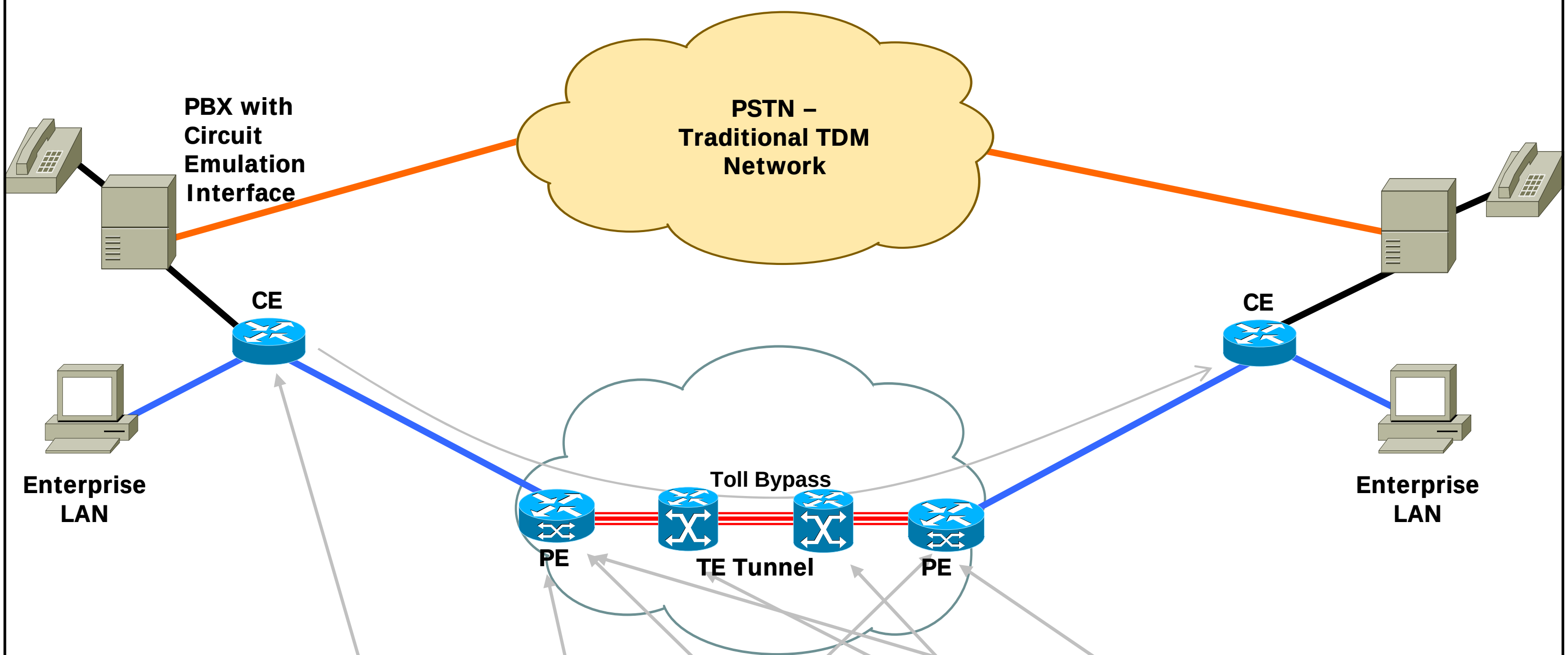





***Solution Requirements*** ⇒ QoS on PE Router + Mapping Traffic to Tunnels + QoS on Core Routers + TE or DS-TE

# Solution 2: Toll Bypass with Voice/Data Converged Network

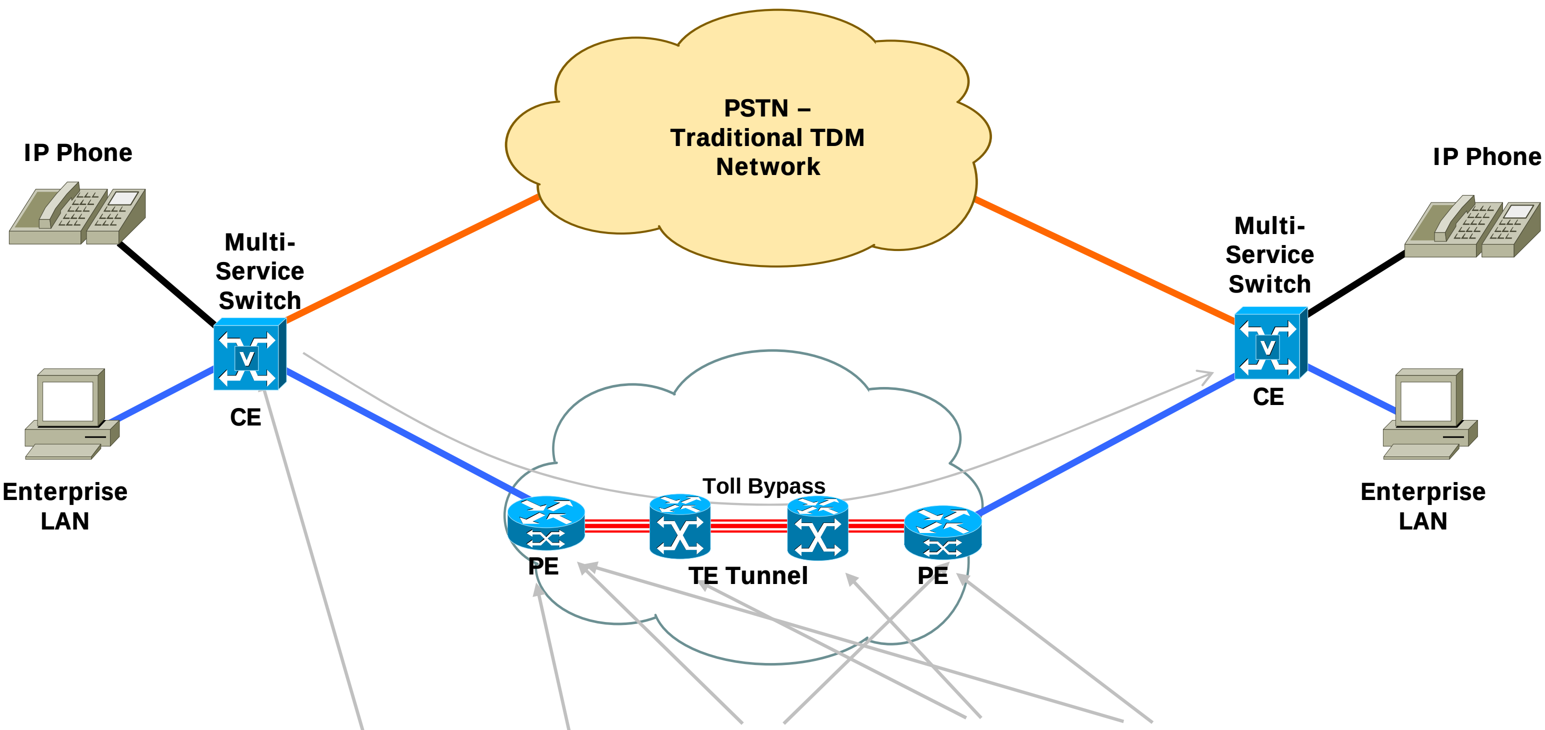
Cisco.com




*Solution Requirements* ⇒ QoS on CE Router + QoS on PE Router + Mapping Traffic to Tunnels + QoS on Core Routers + TE or DS-TE

# Solution 3: Toll Bypass with VoIP Network

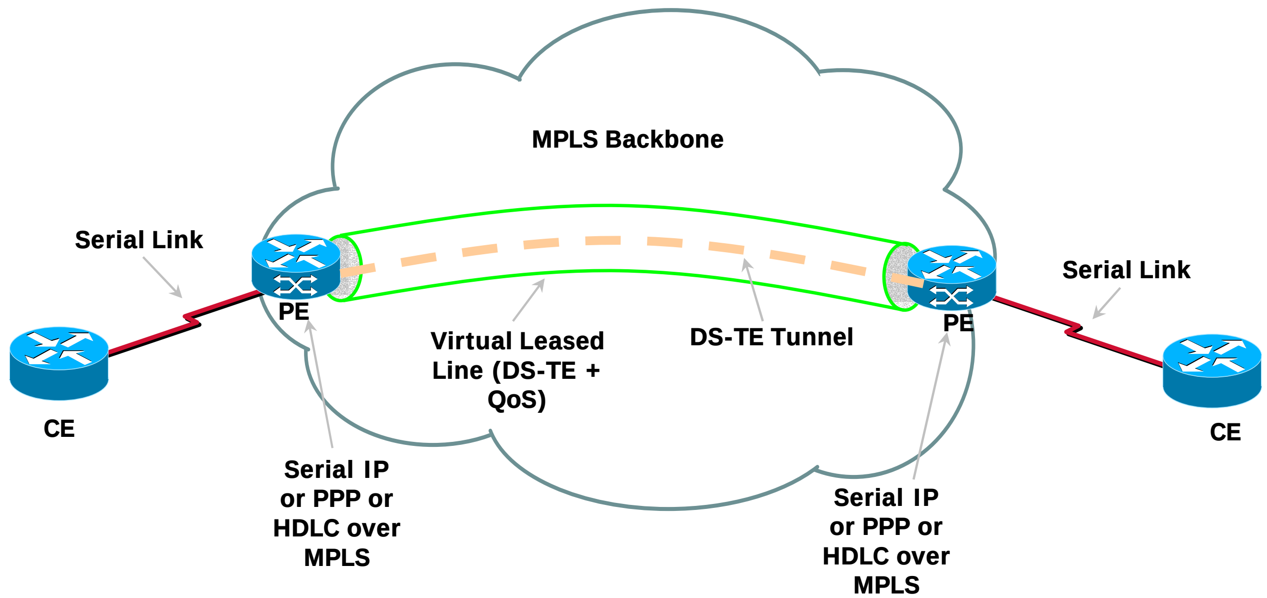





***Solution Requirements*** ⇒ QoS on CE Router + QoS on PE Router + Mapping Traffic to Tunnels + QoS on Core Routers + TE or DS-TE

# Solution 4: Virtual Leased Lines – Serial Links

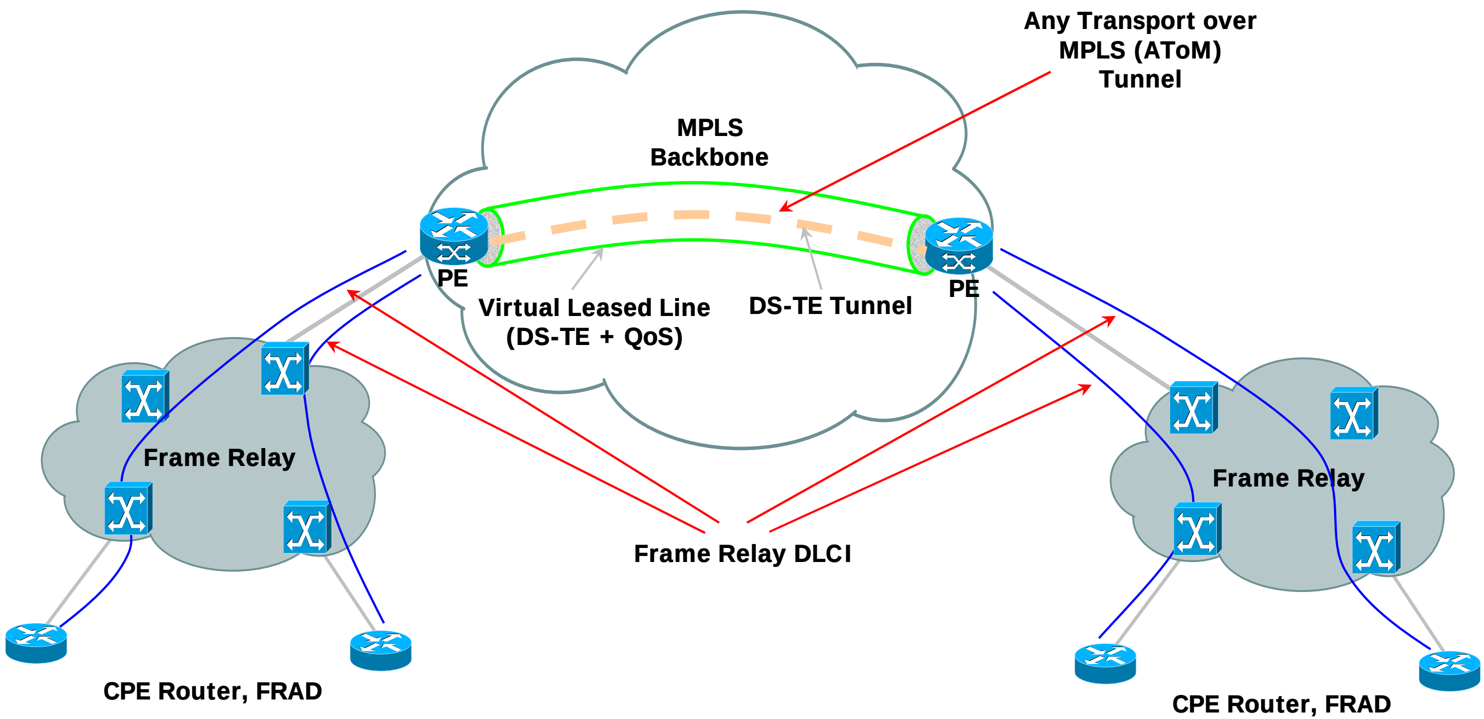
Cisco.com




*TE Tunnel Selection for AToM Attachment VCs*

# Solution 5: Virtual Leased Lines – FR Networks

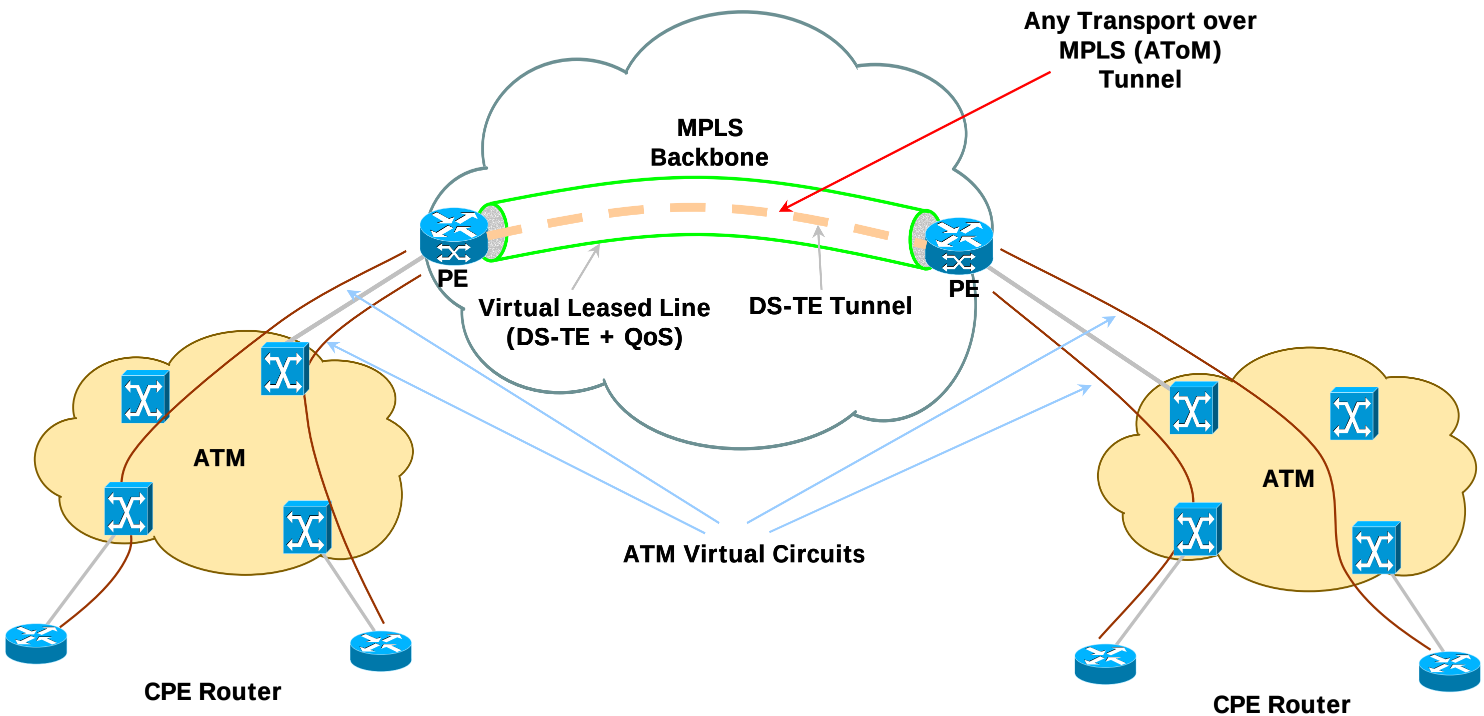





*TE Tunnel Selection for AToM Attachment VCs*

# Solution 6: Virtual Leased Lines – ATM Networks






*TE Tunnel Selection for AToM Attachment VCs*

# Agenda



- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- VPN + TE + QoS Solutions
- Traffic Engineering – Next Steps
- Summary

# MPLS Trafffic Engineering – New Features



- LSP Attributes
- AutoTunnel – Primary & Backup
- AutoTunnel – Mesh Groups
- RSVP Refresh Reduction
- RSVP Reliable Messaging
- RSVP Local Policy Support
- RSVP Header Compression (support for cRTP)
- RSVP Integrity Authentication
- Admission Control for VoIP for TE Tunnels
- Aggregate RSVP
- Hierarchical LSPs (TE Tunnels)
- RSVP Proxy Support
- RSVP Integrity Object Support
- IntServ- DiffServ Multiple PHB Support

# MPLS TE AutoTunnel

Cisco.com

- MPLS TE AutoTunnel is a new MPLS TE feature scheduled for 12.0(26)S
- AutoTunnel automatically creates TE Tunnels for Primary and Backup use
- Primary - AutoTunnel for Primary TE tunnels has the following characteristics:
  - Sets up a TE tunnel to every adjacent neighbor or a "1-hop" tunnel
  - With FastReRoute, "1-hop" tunnel protects not only TE LSP traffic, but also IP Traffic. Future versions will protect LDP LSP traffic as well
  - Does not appear in configuration files – system generated
- Backup – AutoTunnel for Backup TE Tunnels has the following characteristics:
  - Sets up a Next hop and Next Next Hop
  - N:1 concept applies here as well i.e. 1 Backup tunnel protects multiple Primary tunnels
  - A "manually" configured backup tunnel is preferred to a Backup AutoTunnel

# “Manual” TE vs AutoTunnel



**Configuration Tasks – Before AutoTunnel**

*Configure Link*

ip rsvp bandwidth....

.....

*Configure IGP*

router ospf ....

mpls traffic-eng area...

......

*Configure TE Tunnels*

int tun0

tunnel mode mpls .....

.......

int tun1

tunnel mode mpls .....

.......

**Configuration Tasks – After AutoTunnel**

*Configure Link*

ip rsvp bandwidth....

.....

*Configure IGP*

router ospf ....

mpls traffic-eng area...

......

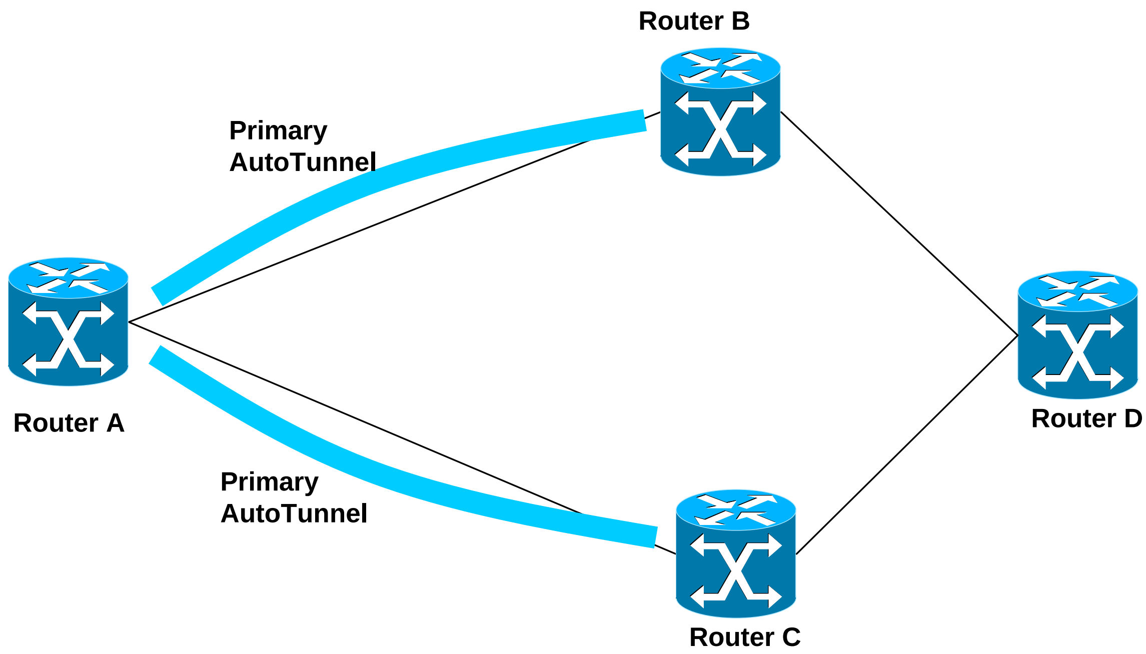
***Configure TE AutoTunnel***

**mpls traffic-eng auto-tunnel primary onehop**

**mpls traffic-eng auto-tunnel backup**

# MPLS TE AutoTunnel - Primary

Cisco.com

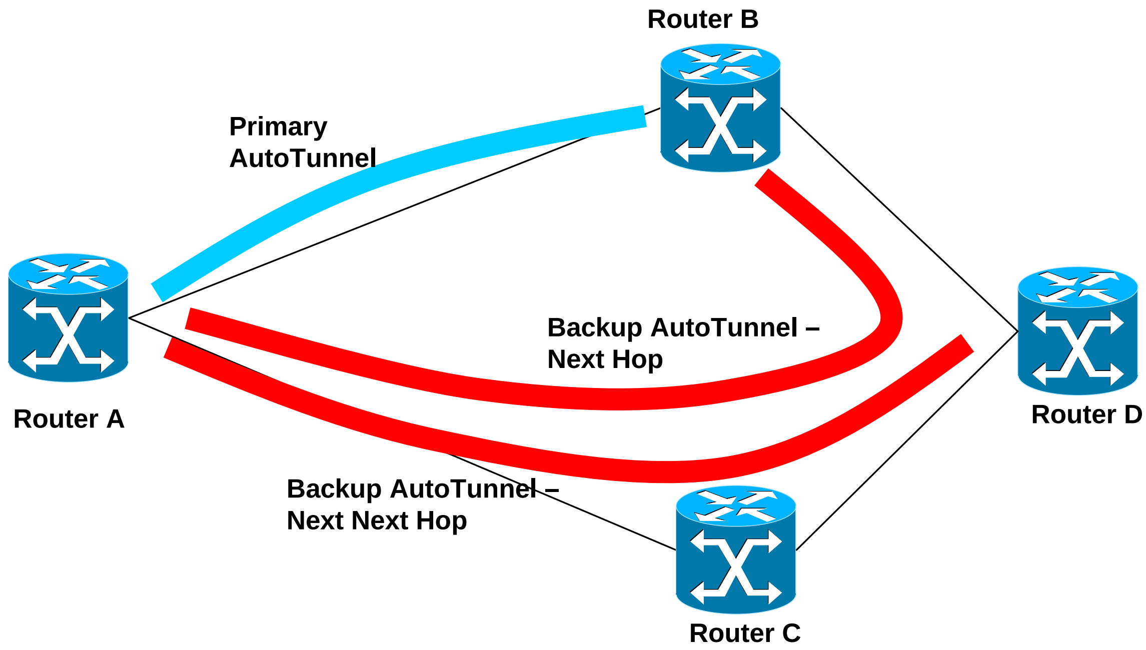



**Router A creates 2 AutoTunnels for each adjacent neighbor – Router B and Router C**

**All AutoTunnels are zero bandwidth tunnels**

# MPLS TE AutoTunnel – Primary & Backup

Cisco.com




Router A creates 2 Backup AutoTunnels for each connected link

Manual Tunnels take precedence over AutoTunnels – provides “tweaking” capability for customers

All AutoTunnels are zero bandwidth tunnels

# Issues with RSVP Refresh signaling

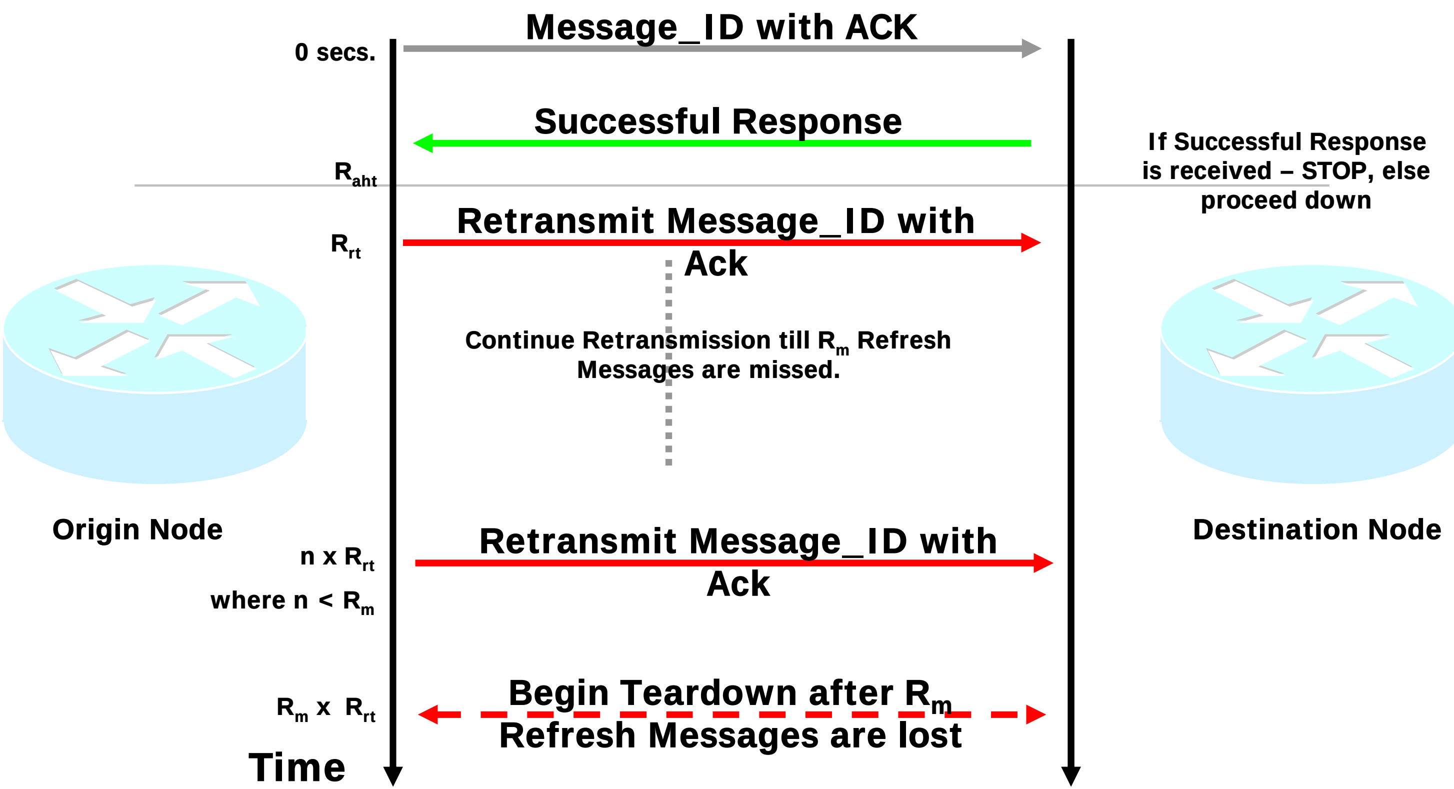
Cisco.com

- **RSVP is a "soft state" protocol; i.e., it maintains state in each router or host**
- **State needs to be periodically refreshed – thus Refresh Messages are required**
- **Refresh Messages are used for:**
  - **State Synchronization between RSVP neighbors**
  - **Recover from Lost RSVP Messages**
- **Operational problems with Refresh Signaling**
  - ***Scaling*** **– Number of RSVP sessions $\propto$ Overhead refresh traffic $\propto$ Resource Requirements (processing / memory)**
  - ***Reliability and Latency*** **– Based on Refresh Period:**
  - Greater Refresh Period $\Rightarrow$ Longer time to synchronize state
  - Lower Refresh Period $\Rightarrow$ Greater refresh signaling volume

# Reliable Messages

$R_{rt}$ = Retransmit Time; $R_{aht}$ = Acknowledgement Hold Time;

$R_m$ = Successive Refresh Messages Missed

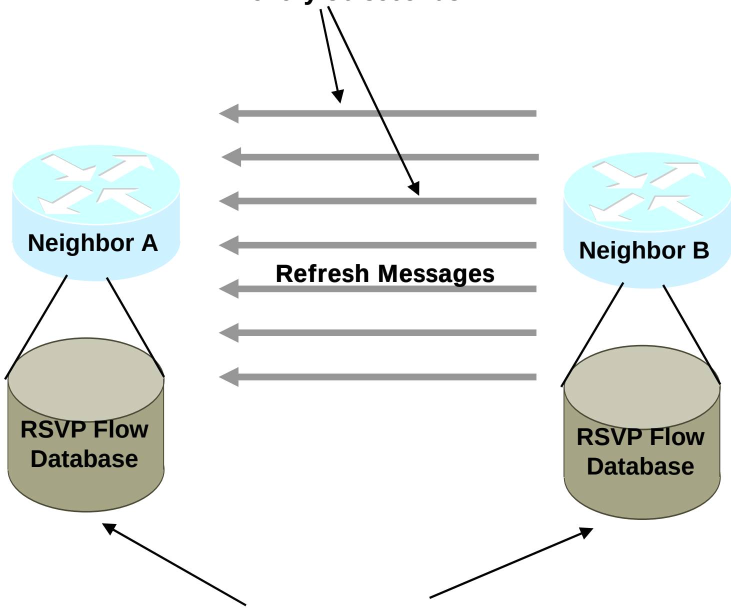


# Before & After Summary Refresh – "Refresh Aggregation"

Cisco.com

## *BEFORE*

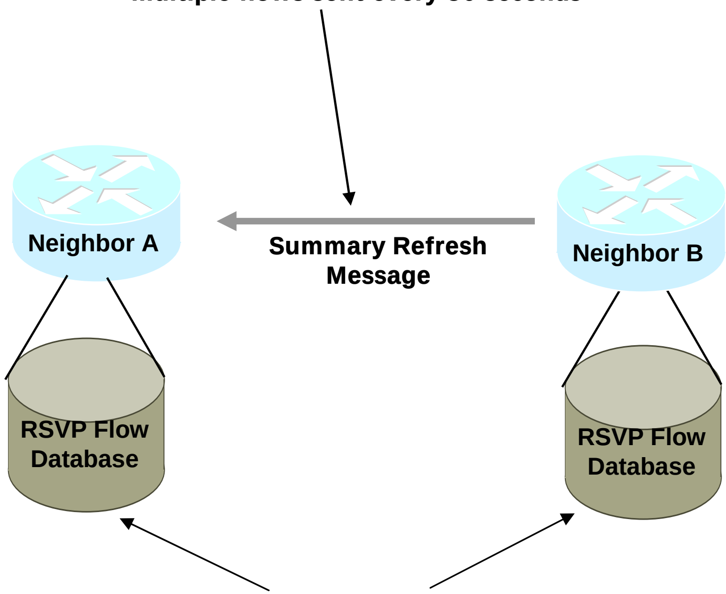
One Refresh Message for every flow sent every 30 seconds




Every Router maintains a database consisting of each flow – each entry needs to be periodically refreshed a.k.a. "RSVP is a soft-state protocol"

## *AFTER*

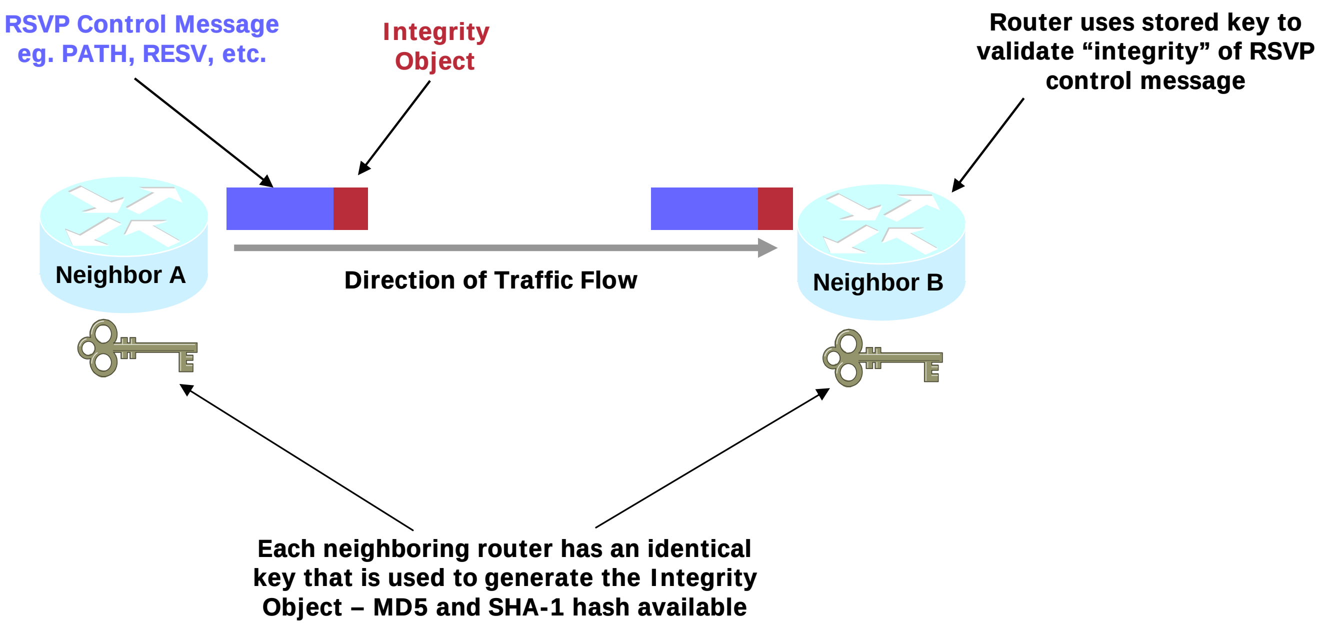
One Summary Refresh Message sent for multiple flows sent every 30 seconds




With Refresh Reduction, each entry in the DB gets a Message ID – thus the Summary Message contains a collection of message Ids for states to be refreshed

# Integrity Object Support – rfc2747

Cisco.com



# RSVP Local Policy Support



```
share-64-2(config)#
share-64-2(config)#ip rsvp policy local acl 101
sha(config-rsvp-policy-local)#?
Local policy mode commands:
  all                    Allow all RSVP message operations
  default                Set a command to its defaults
  exit-local             Exit local policy mode
  local-override         Local policy overrides COPS
  no                     Negate a command or set its defaults
  path-accept            Accept Path message
  path-all               Allow all Path operations
  path-forward           Accept and forward Path message
  patherror-accept       Accept PathError message
  patherror-forward      Accept and forward PathError message
  preempt-priority       Set preemption priority
  resv-accept            Accept Resv message
  resv-all               Allow all Resv operations
  resv-forward           Accept and forward Resv message
  resv-install           Accept and install Resv message
  resverror-accept       Accept ResvError message
  resverror-forward      Accept and forward ResvError message

sha(config-rsvp-policy-local)#path-accept
sha(config-rsvp-policy-local)#resv-install
sha(config-rsvp-policy-local)#
sha(config-rsvp-policy-local)#preempt-priority ?
  <1-65535>  Priority of reservation during creation

sha(config-rsvp-policy-local)#preempt-priority 65423
sha(config-rsvp-policy-local)#
```

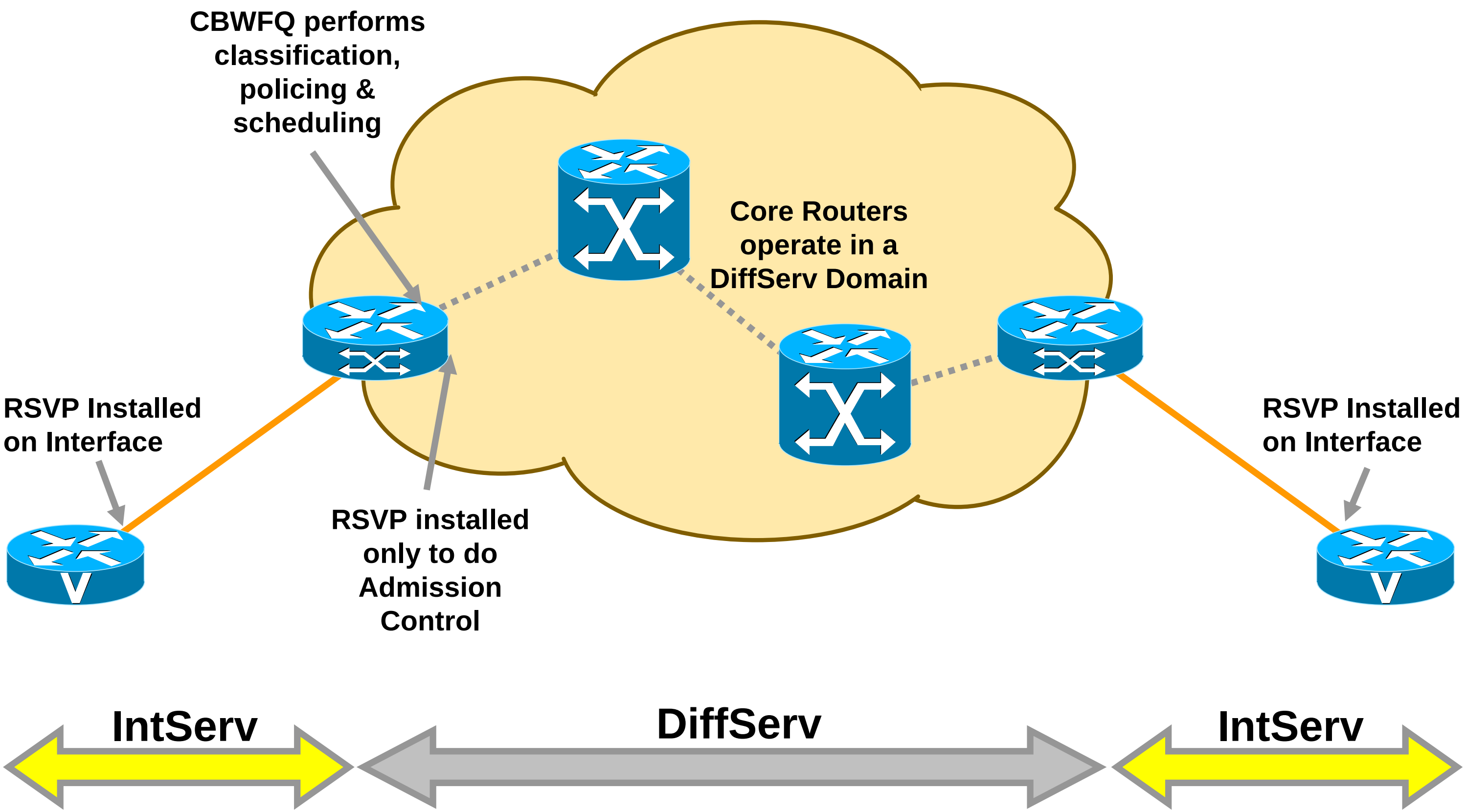
**Use standard ACLs for RSVP Message control**

**Configurable Policy Parameters**

**Preemption of RSVP Flows Eg. 911 calls**

# RSVP Scalability Enhancements – Intserv/DiffServ Integration Phase I

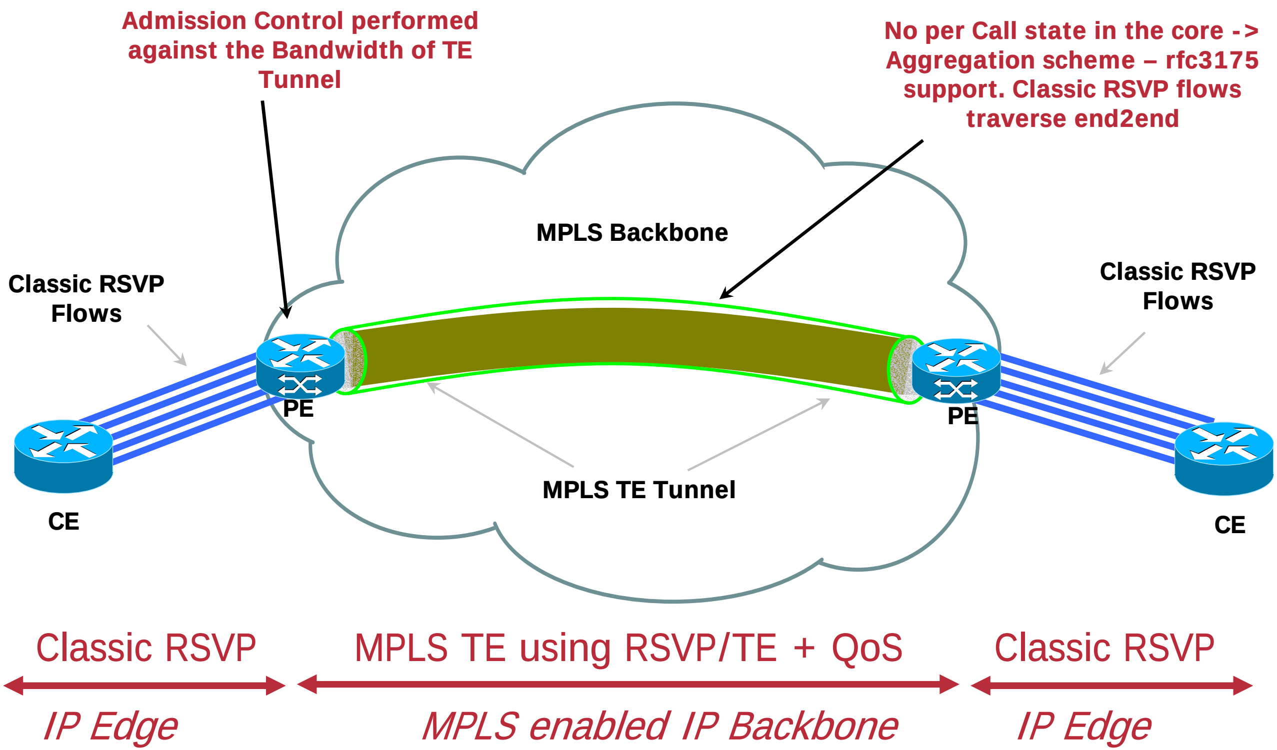




# Tunnel Based Admission Control - Planned

Future

Cisco.com



# Tunnel Based Admission Control – External Dependencies (Planned)

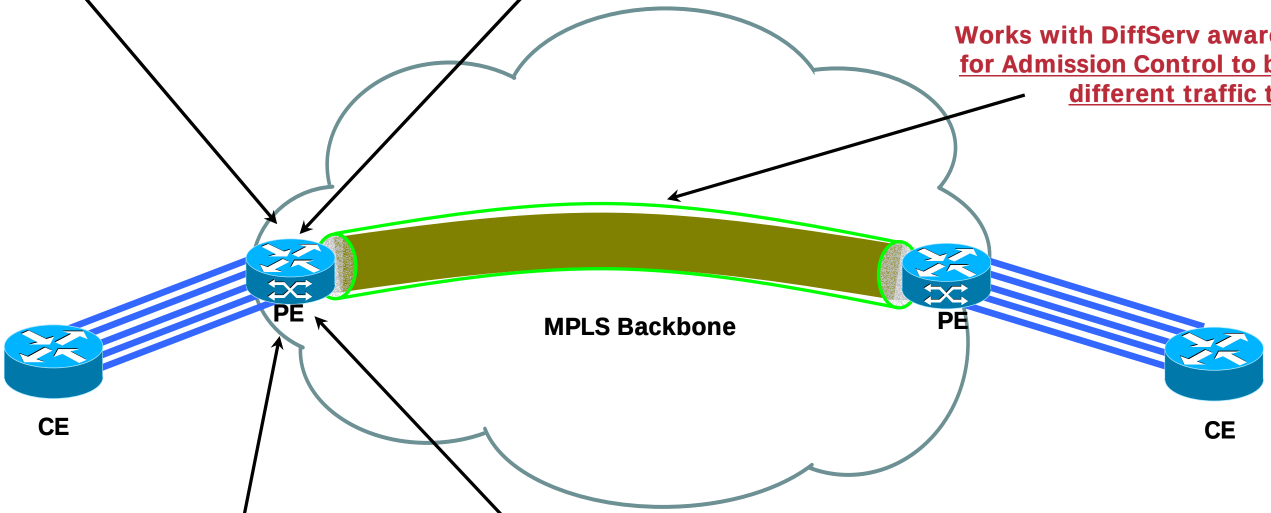
Future



TBAC works within an MPLS VPN Environment -> <u>More value added SLA</u>

Leverages Receiver RSVP Proxy to reduce post-dial delay -> <u>Calls are setup quickly as RSVP admission control need not traverse the link</u>

Works with DiffServ aware TE -> <u>Allows for Admission Control to be provided to different traffic types</u>




Provides per-subscriber Admission Control capabilities -> <u>Subscriber A gets 20 calls, while Subscriber B gets 40 calls</u>

Provides Pre-emption capabilities for Emergency calls -> <u>Subscriber A gets 20 calls with 5 calls with pre-emption capabilities</u>

# 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 (using tunnel based admission control)

**Benefits provided by MPLS Traffic Engineering**

**Benefits provided by MPLS Traffic Engineering with TBAC**

# Agenda

Cisco.com

- MPLS and TE Fundamentals
- Application 1: Increasing Bandwidth Inventory
- Application 2: Minimizing Packet Loss
- Application 3: Optimizing the Core
- Traffic Engineering – Next Steps
- Summary

# 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**

Cisco Systems

Empowering the Internet Generation

# Acronym Guide

Cisco.com

| | | | |
|---|---|---|---|
| APS | Automatic Protection Switching | POS | Packet over SONET |
| ATM | Asynchronous Transfer Mode | QoS | Quality of Service |
| CAPEX | Capital Expenditure | RSVP | Resource Reservation Protocol |
| CE | Customer Edge | SDH | Synchronous Digital Hierarchy |
| FRR | Fast Reroute | SLA | Service Level Agreement |
| GUI | Graphical User Interfacce | SONET | Synchronous Optical Network |
| IP | Internet Protocol | SP | Service Provider |
| ISP | Internet Service Provider | TB | Tunnel Builder |
| MPLS | Multiprotocol Label Switching | TB Pro | Tunnel Builder Pro |
| MSP | Multiplexed Switching Protection | TE | Traffic Engineering |
| MUXES | Multiplexers | UNI | User-Network Interface |
| OPEX | Operational Expenditure | VPN | Virtual Private Network |