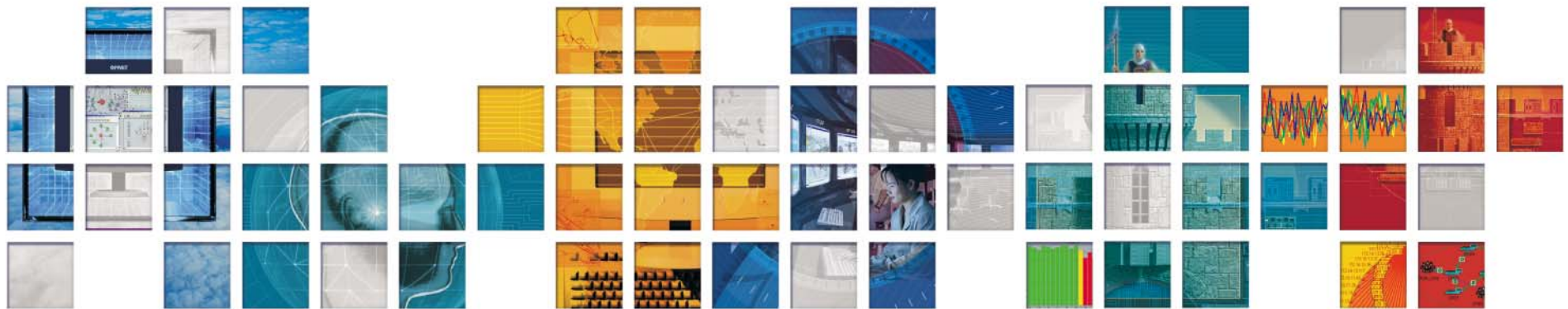




*Making Networks and Applications Perform™*



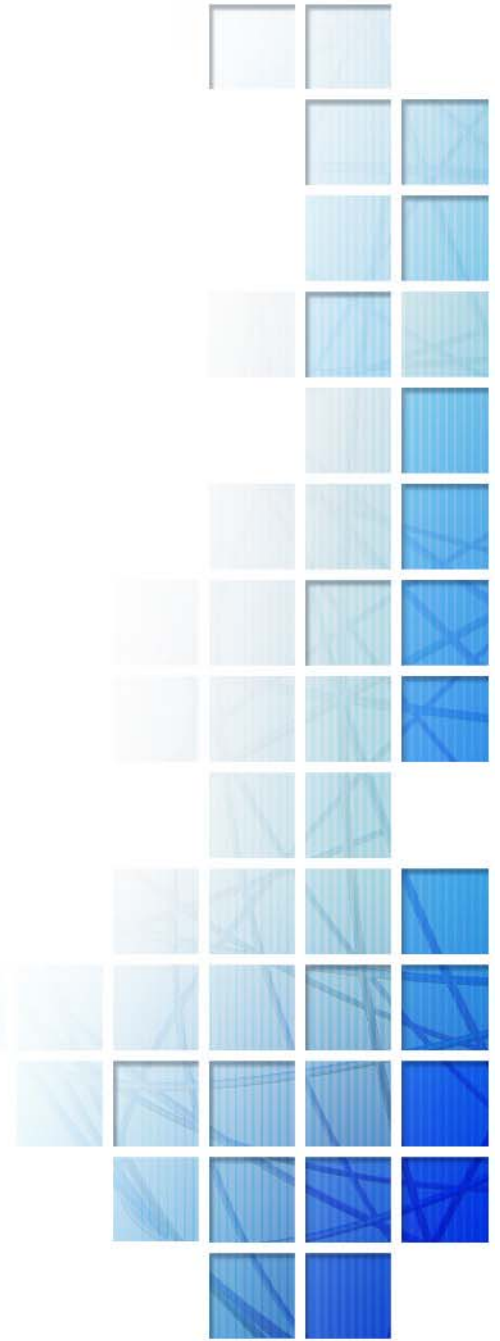
# IP / MPLS: Challenges for Network Planner

**Dr. Martin Klapdor**  
**Senior Application Engineer**  
**[mklapdor@opnet.com](mailto:mklapdor@opnet.com)**



# Agenda

- **Introduction**
- **MPLS and Triple Play**
- **Traffic Engineering**
- **Resilience and Traffic Protection**
- **Summary**





# About OPNET Technologies, Inc.

## Corporate Overview

- Founded in 1986
- Publicly traded (NASDAQ: OPNT), IPO Aug. 2000
- HQ in Bethesda MD
- Approximately 400 employees
- Worldwide presence through direct offices and channel partners
- Cisco worldwide OEM starting summer 2005

## Best-in-class Software and Services

- Application & network performance management
- Network audit and configuration management
- Capacity planning, modeling, and design

## Strong Financial Track Record

- Long history of profitability
- Revenues of \$64.2M in past year
- Approximately 25% of revenue re-invested in R&D

## Broad Customer Base

- Corporate Enterprises
- Government Agencies/Contractors
- Service Providers
- R&D Organizations



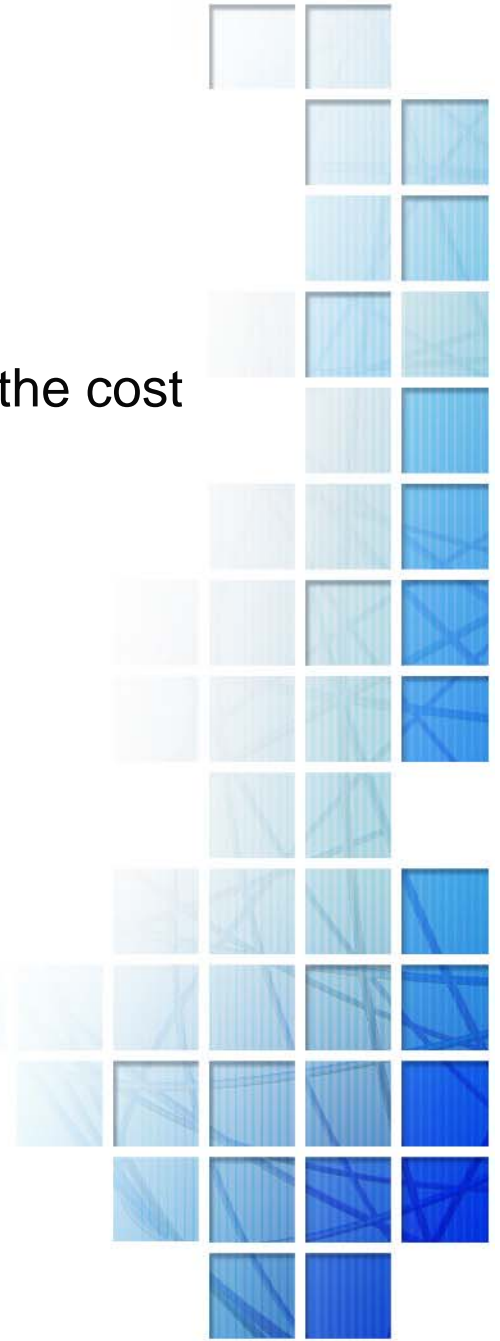
In Recognition of  
Visionary use of  
Information  
Technology





# Motivation for MPLS

- Demand for QoS services
  - Demand for ATM-like classes of services without the cost of ATM
  - Convergence to a single unified network
  - Diverse service types and QoS requirements
- Bandwidth management
  - Growing number of users
  - Increasing appetite for bandwidth
  - Efficient use of current bandwidth
  - Defer buying bandwidth



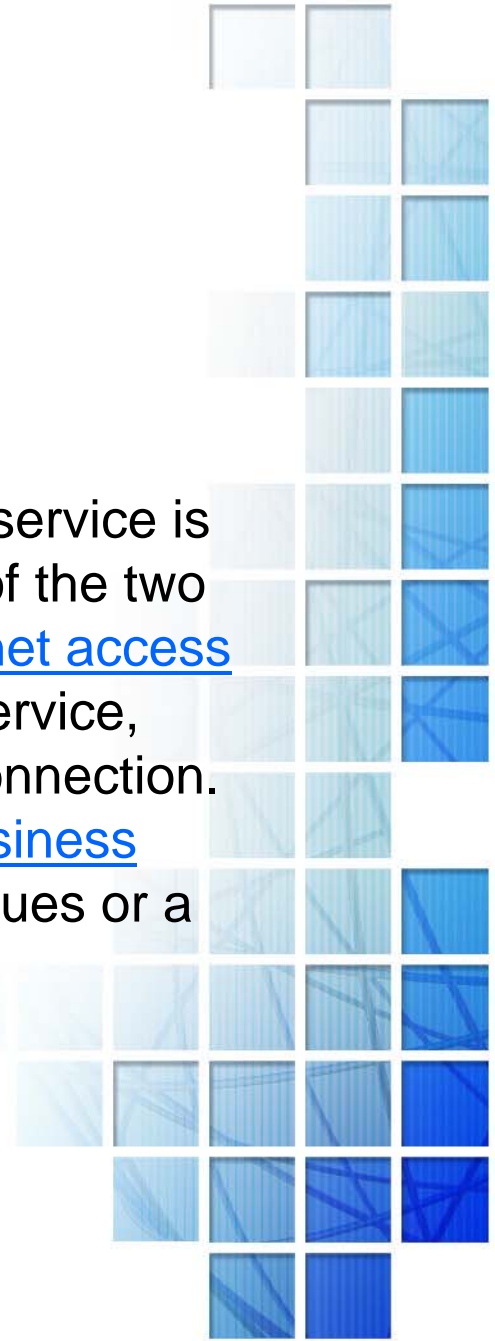


# MPLS – Converged Networks

## Triple Play



In [telecommunications](#), the triple play service is a marketing term for the provisioning of the two broadband services, [high-speed Internet access](#) and television, and one narrowband service, [telephone](#), over a single [broadband](#) connection. *Triple Play* focuses on a [combined business model](#) rather than solving technical issues or a common standard.





# Triple Play – Comments from “Stiftung Warentest”

**Major criticism depends on the used carrier:**

**Cable Provider:** Good TV quality but unreliable telephony

**Telephone Provider:** Reliable telephony, good quality but shaking TV

## Final Conclusion

Article from 10.08.2007

*„Tripple play is not ready yet. Based on the technology TV and video over the Internet is not fast enough to become an alternative to Standard TV.“*



# What are the major challenges today?

Every service data, voice and video has different parameters that need to be taken into account for designing a network.

	Delay	Jitter	Packet Loss	Bandwidth
Data	Red	Yellow	Orange	Yellow
Voice	Orange	Red	Orange	Orange
Video	Yellow	Orange	Red	Orange

## Bottom Line:

Network engineers need to have a strategy for protecting traffic and QoS to guaranty performance metrics

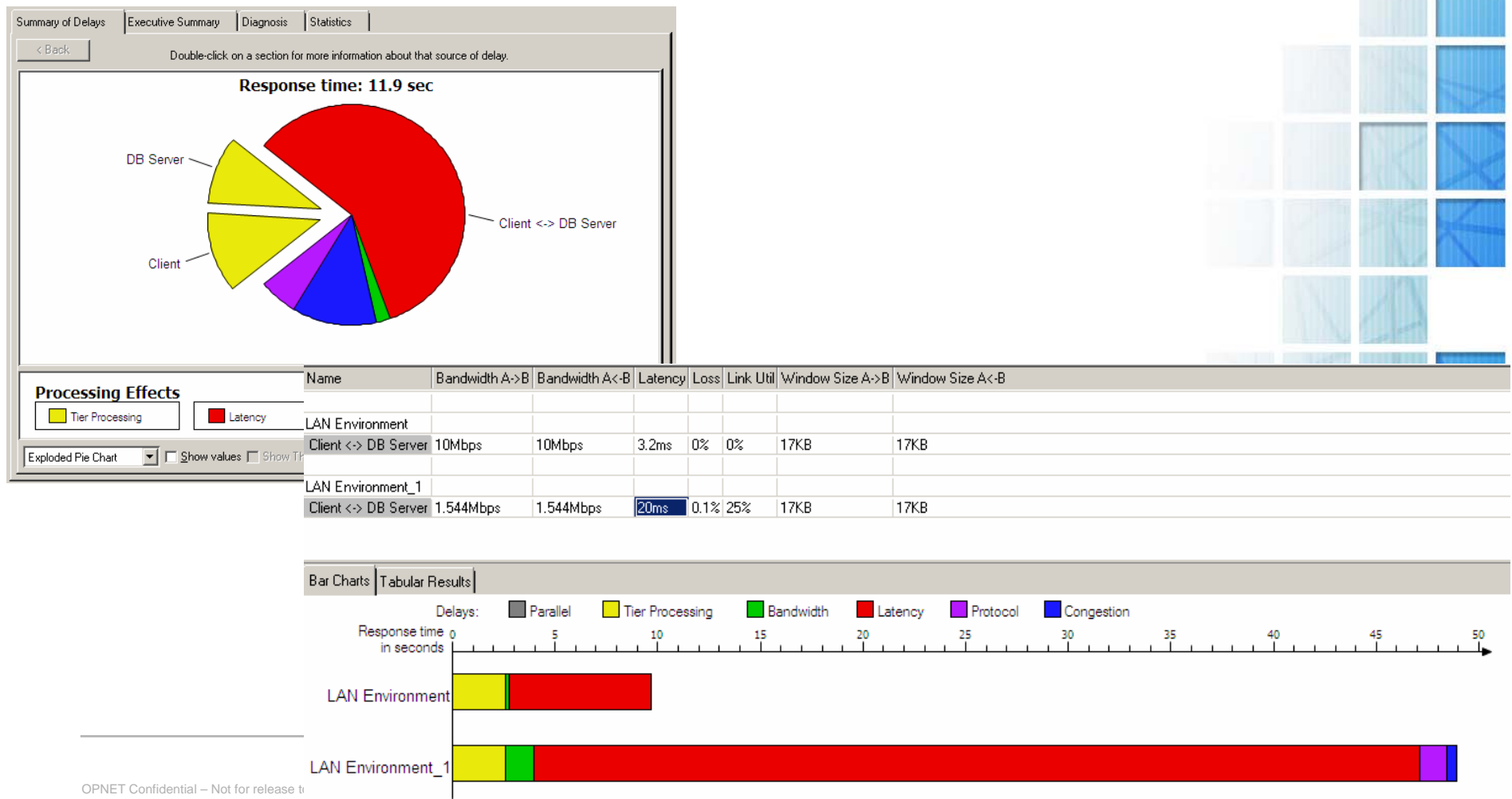


# Data Service

Not all data services are equal.

Need to have a common picture of the communication behavior of an application.

Not all performance problems can be solved with hardware / equipment





# VoIP

## Example of Delay Budget

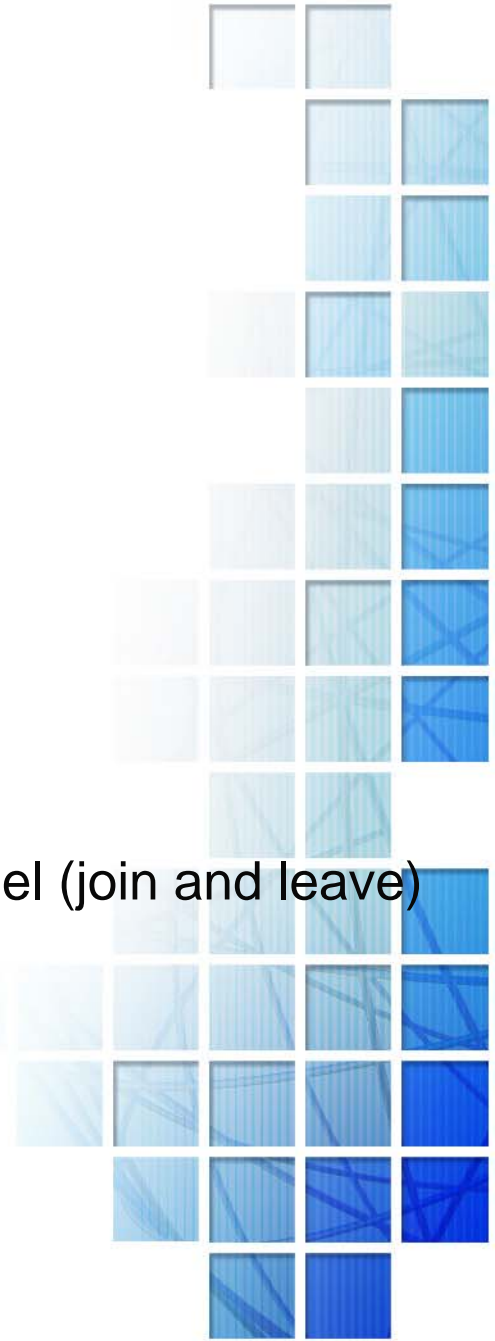
- Delays of less than 150 ms are sought
  - But the fixed components of delay can be high
  - Careful control of the variable components (queuing) required

Delay Component	Fixed/Variable	Delay (msec)
Codec-Related		
g729a Compression Delay	fixed	5
g729a Sampling Delay (10 ms x 2)	fixed	20
Queuing Delay on Trunk	variable	5
Transmission Delay	fixed	3
Propagation Delay	fixed	25
Queuing at Intermediate Hops	variable	20
De-jitter buffer	fixed	50
<b>Total of Fixed Delays</b>		<b>103</b>
<b>Total of Variable (Queuing) Delays</b>		<b>25</b>
<b>Total Delay</b>		<b>128</b>



## Video / TV

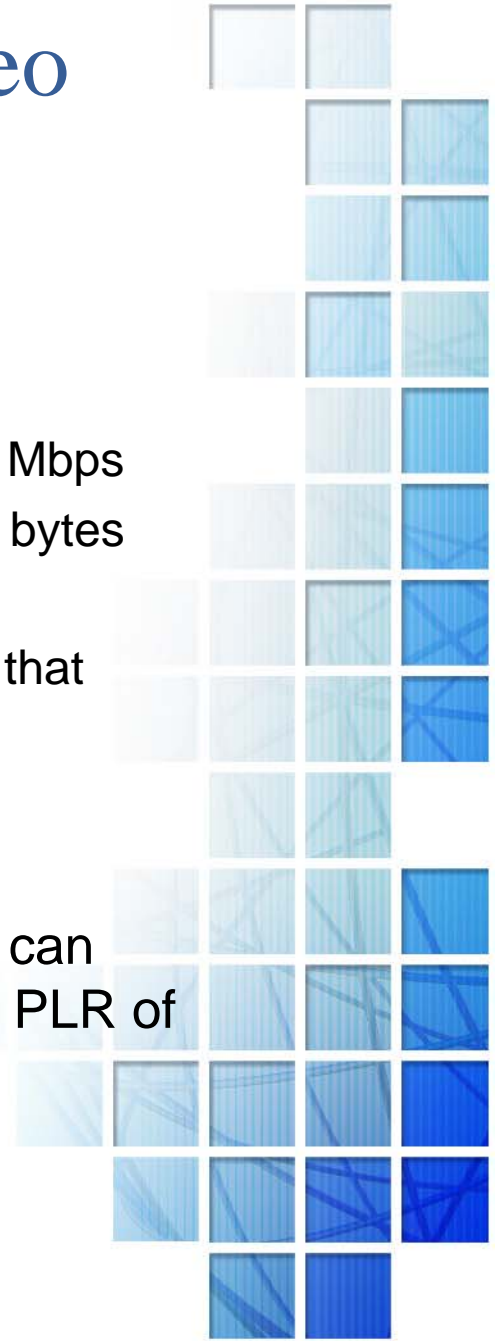
- High availability
- High sensitivity to packet loss –integrity
- Low tolerance for jitter –continuity
- Bandwidth Requirements based on MPEG-2
  - 4 Mbps for SD compressed
  - 13 Mbps for HD compressed
- Responsive to user “channel switching”
  - quickly deliver video stream as user switches channel (join and leave)





# IGP Convergence Impact on Video

- IGP convergence is not good enough for video
  - Assuming MPEG-2 stream that would translate 3.7 Mbps
  - That translates into 350 pps @ packet size of 1356 bytes
  - For PLR of one loss per hour, that is  $1 \cdot 10^{-6}$
  - IP convergence and PIM-SSM is about 1000 msec that would translate into PLR of 350 packets
- MPL-based recovery is good enough
  - MPLS-based recovery with point-to-multipoint can become around 50 msec, which translates into PLR of 18 packets





# Where OPNET can help

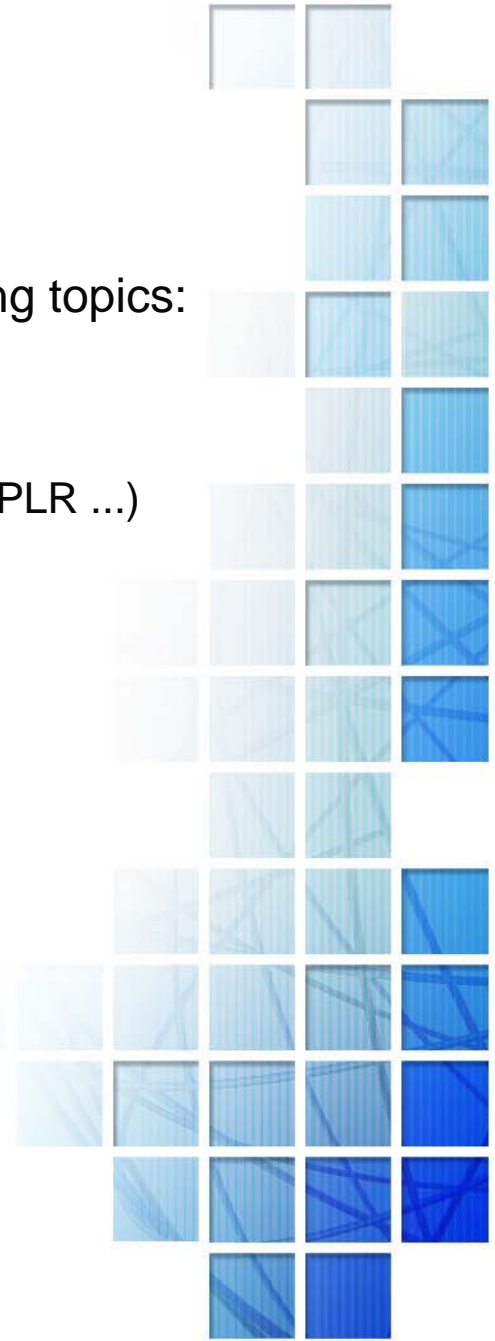
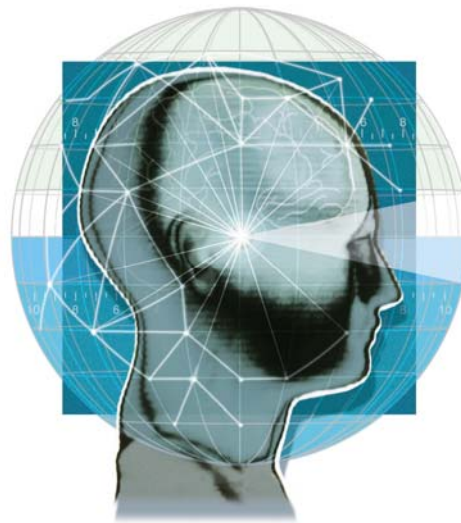
OPNET has analytical offline solutions to support the following topics:

- **Application profiling:**

- understanding critical requirements of an application (latency, PLR ...)

- **Network Planning**

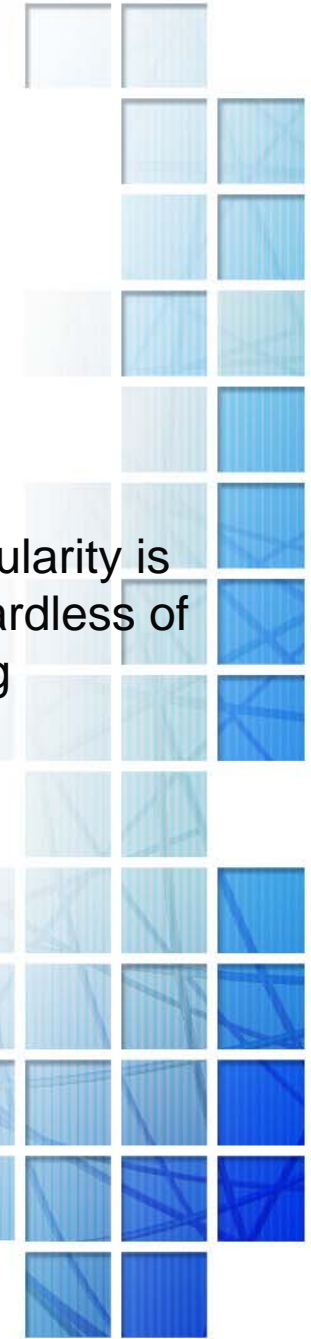
- Traffic Engineering
  - Tactical TE
  - Diffserv aware TE
- Traffic protection
  - Optical protection
  - Explicit routes
  - Fast Reroute
- Failure Analysis
- Capacity planning
- Roll-out planning





# Traffic Engineering

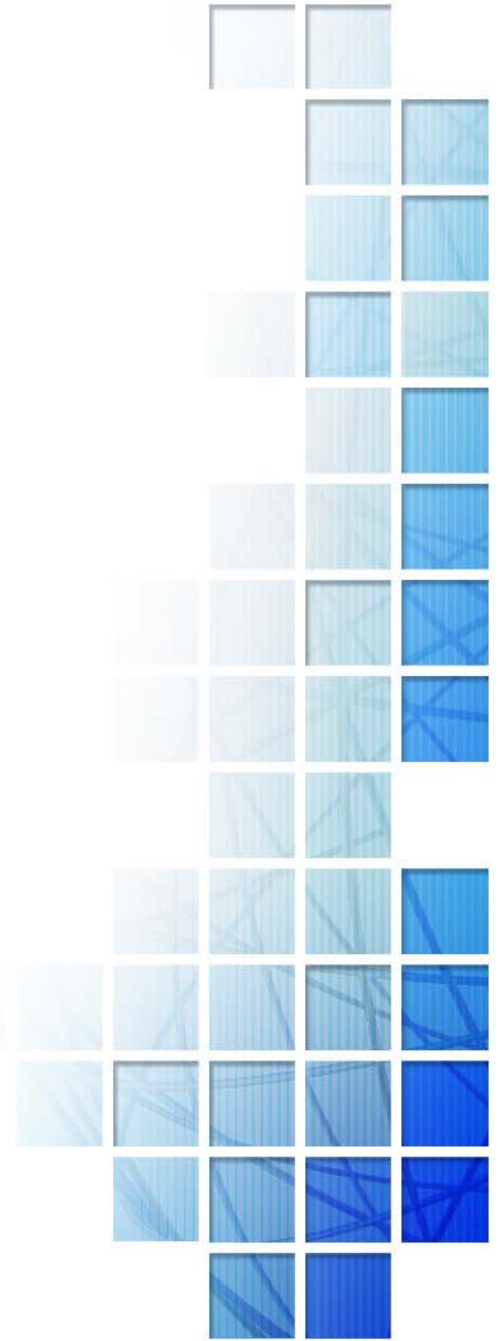
- Top-level view
  - Capacity Planning: placing bandwidth to support traffic
  - Traffic Engineering: placing traffic where there is bandwidth
- MPLS' ability to arbitrarily segregate flows at whatever level of granularity is desired and to route those flows independently of one another (regardless of source/destination addresses) forms the basis for traffic engineering
- Three types
  - Inline           TE performed on a device using local information
  - Online           TE done using global information by a central server connected to the network
  - Offline           TE done by a server external to the network using global information





# Why TE?

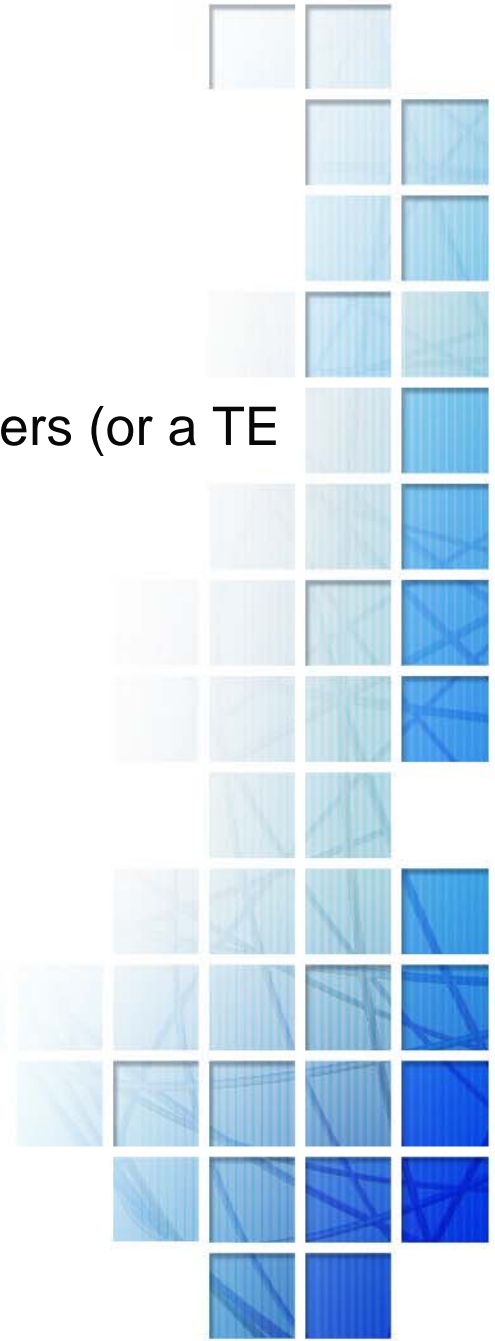
- Bandwidth availability
  - Infrastructure limitations, lead times
- Pipe size granularity issues
- Class-of-service routing
- Knobs to tweak under failure scenarios
- Hedge against traffic issues
  - Uncertainty, growth, fluctuations
- Economics
  - Especially today





# MPLS Topology – For Traffic Engineering

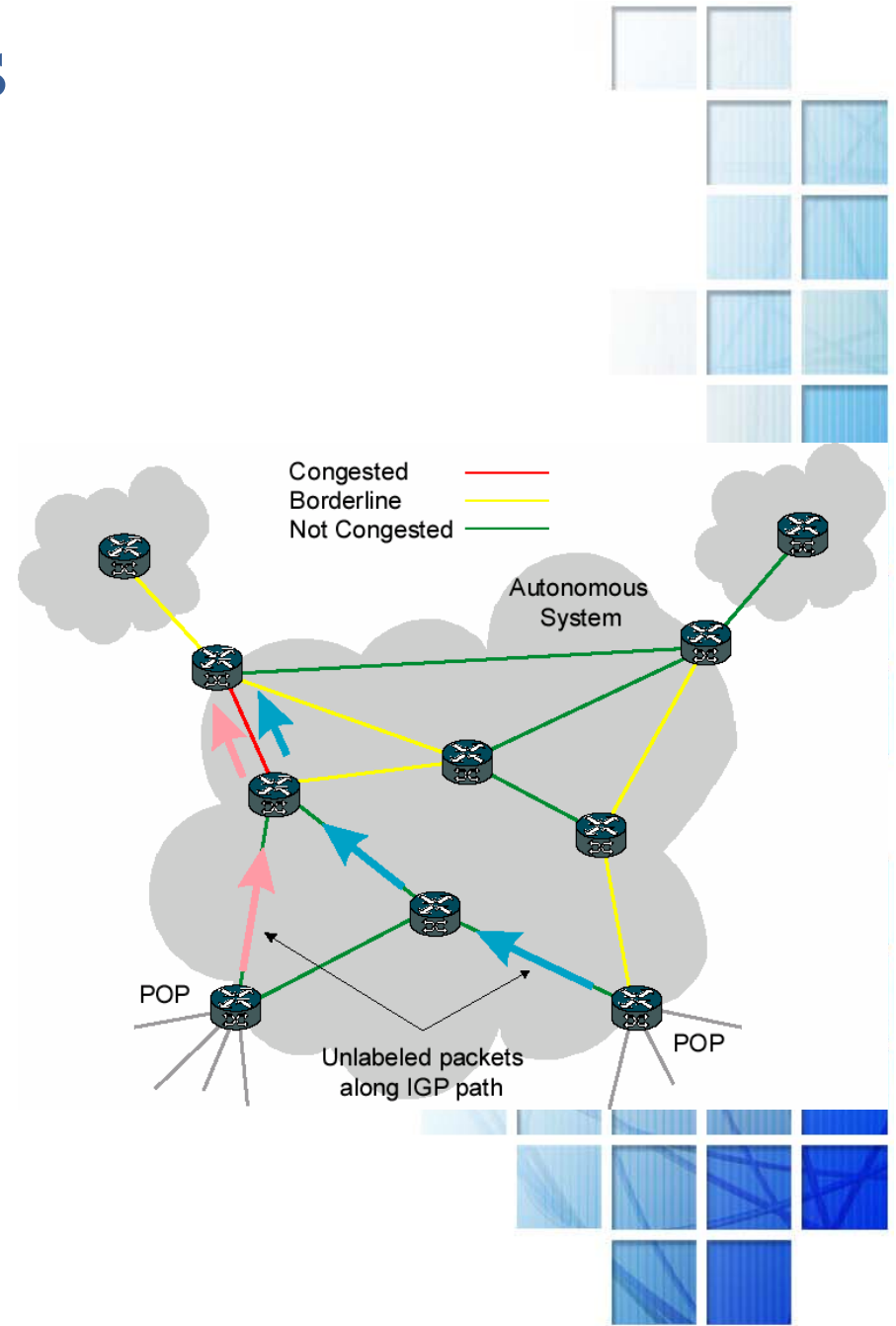
- For TE purposes, MPLS is deployed in the core routers (or a TE layer internal to the core routers)
- Deployment scenarios include
  - Tactical deployment to fix a particular problem
    - Alleviate congestion
    - Improve service level(s)
  - Fully traffic-engineered flows
    - Motivated by measurement it enables and control
    - Full-mesh or hierarchical





# IP Routing Limitations

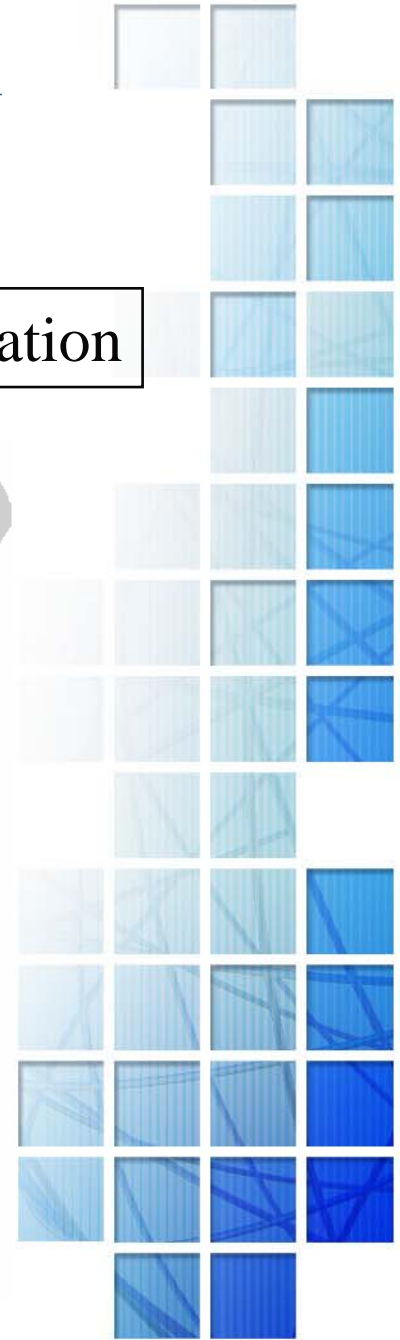
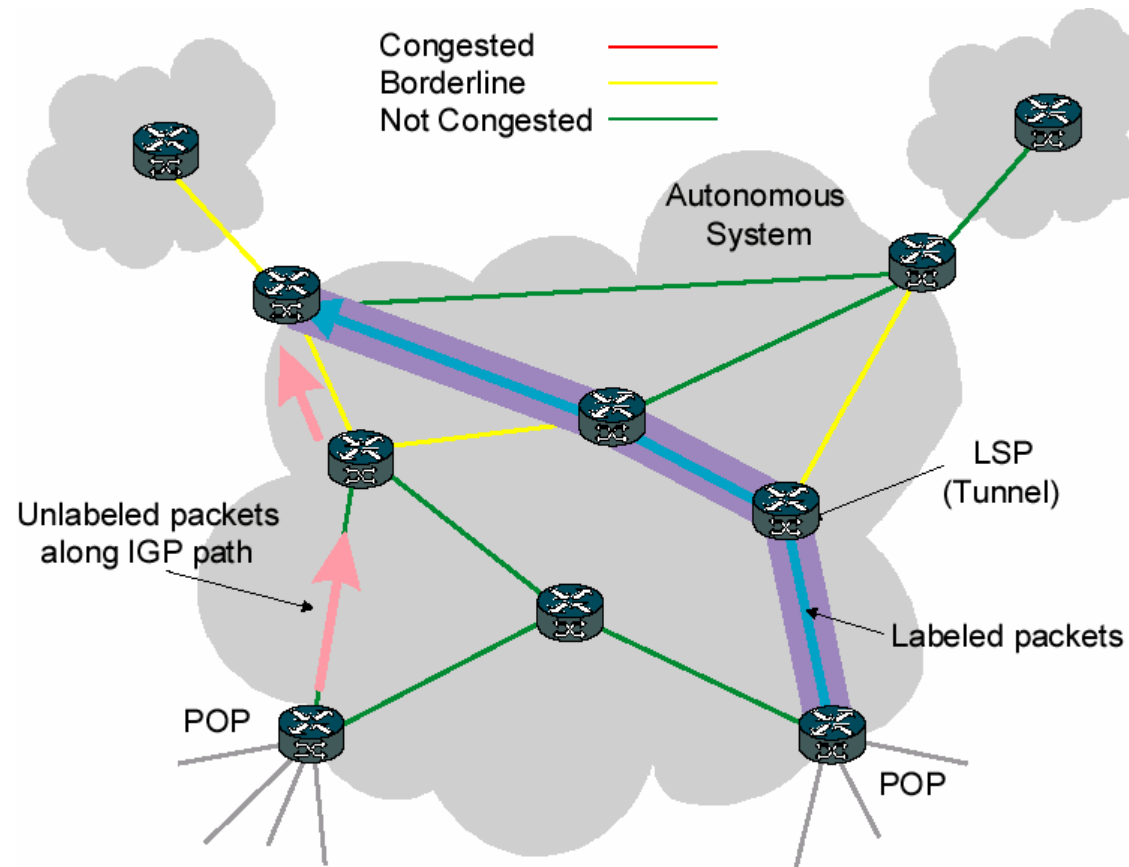
- Routing decisions are based only on packet destination
- Unable to discriminate based on
  - Source
  - Traffic type (QoS marking or port, etc.)
  - Network congestion or load balancing
    - Generally only able to route over equal-cost paths
    - Routing based on utilization information is not typically recommended due to the tendency to result in route oscillations and instability
  - Priority





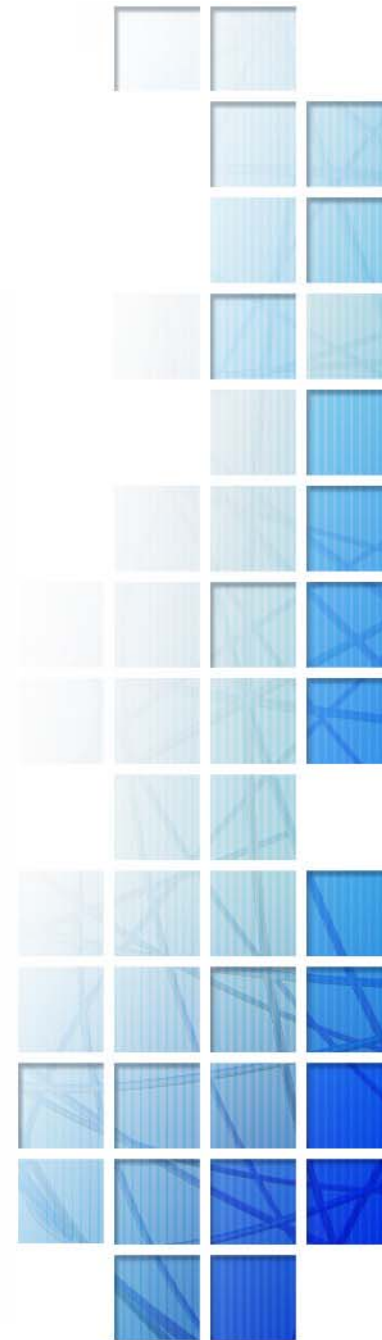
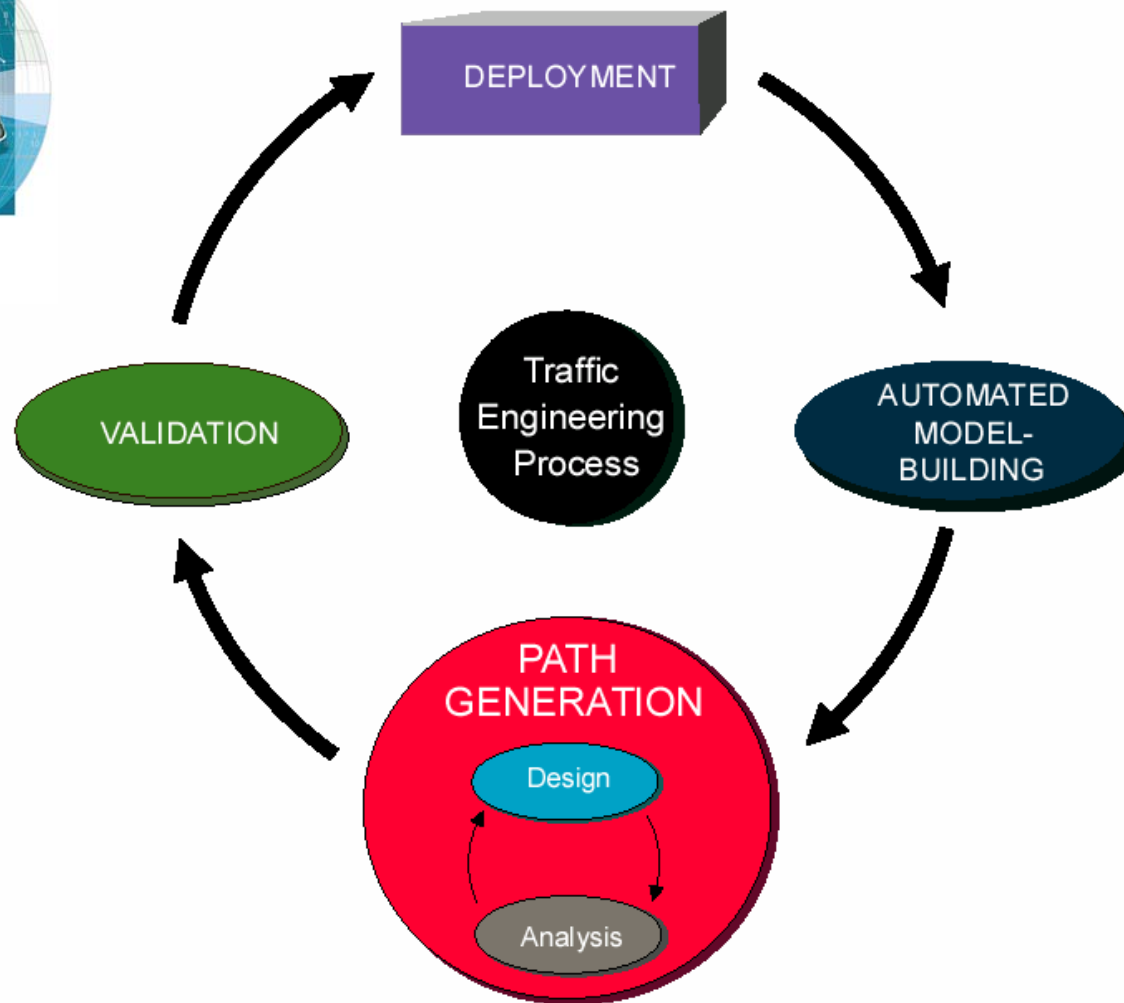
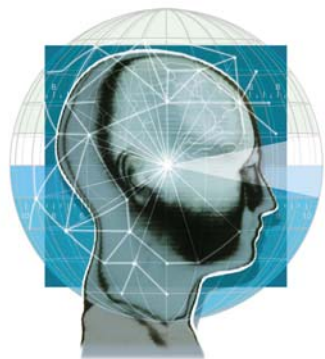
# MPLS Traffic Engineering Solution

MPLS LSP can be assigned to path with lower utilization





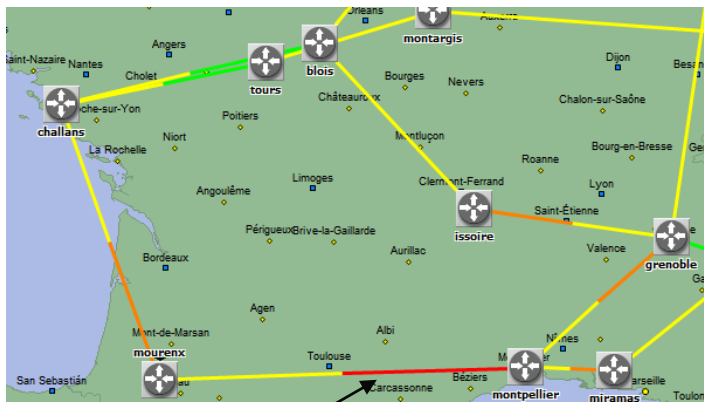
# MPLS Online/Offline TE Process





# Quick Plan Tactical TE Workflow

- Alleviate congestion on an overutilized link
  - Launch MPLS Tactical TE wizard from a link's right-click menu
  - Identifies users of the link (IP traffic flows or LSPs)
  - Divert traffic onto new LSPs or reroute existing



MPLS Tactical TE - Link Usage for montpellier <-> marseille

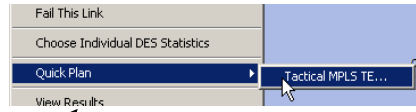
Select a link direction and class type and click Next

Direction	Link Bw (Mbps)	Link TE Bw (Mbps)	Link Subscription (%)	Link Utilization (%)	Util. Due to Traffic Flows (%)	Number of Traffic Flows	Util. D
montpellier->	44.736	44.736	0.00	64.59	64.59	10	
marseille->	44.736	44.736	0.00	96.89	96.89	15	

Class Type: All

Use tactical TE to eliminate hot spots in the network

Right-click on the congested link to launch the wizard



The Link Usage table provides statistics on the current utilization of the link



# Quick Plan Tactical TE Workflow (Cont)

- Create a new LSP to divert a specific set of flows

MPLS Tactical TE - Link Users for montpellier -> mouroenx

Select a user of the link and click Next to choose a route

User Name	User Type	Class	Contribution to Utilization (%)	Traffic Volume (Mbps)	Contribution to Subscription (%)	Reserved TE Bw (Mbit/s)
mourenx -> issouire	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> mulhouse	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> nancy	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> montpellier	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> miramas	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> briancon	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
mourenx -> grenoble	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
blois -> miramas	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
tours -> miramas	Flow	Best Effort (0)	6.46	2.89	0.00	0.00
tours -> montpellier	Flow	Best Effort (0)	6.46	2.89	0.00	0.00

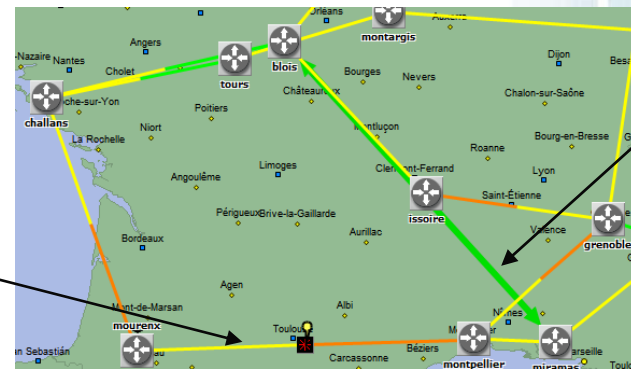
Filter options:  
 Show LSPs  
 Show flows  
Max users to display: 500

The current set of flows using a link are shown in a table

Link utilization is now below threshold



The current route of the selected flow is shown

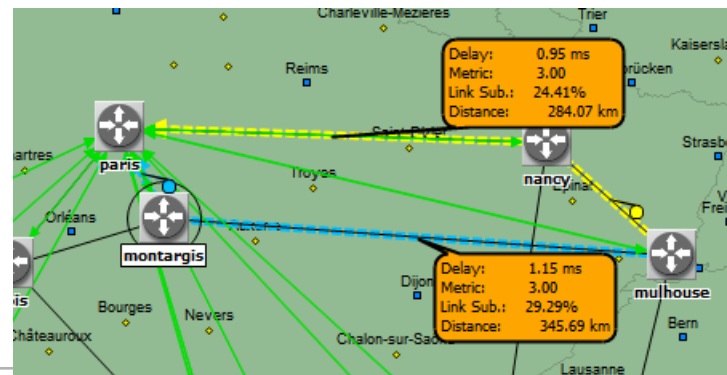
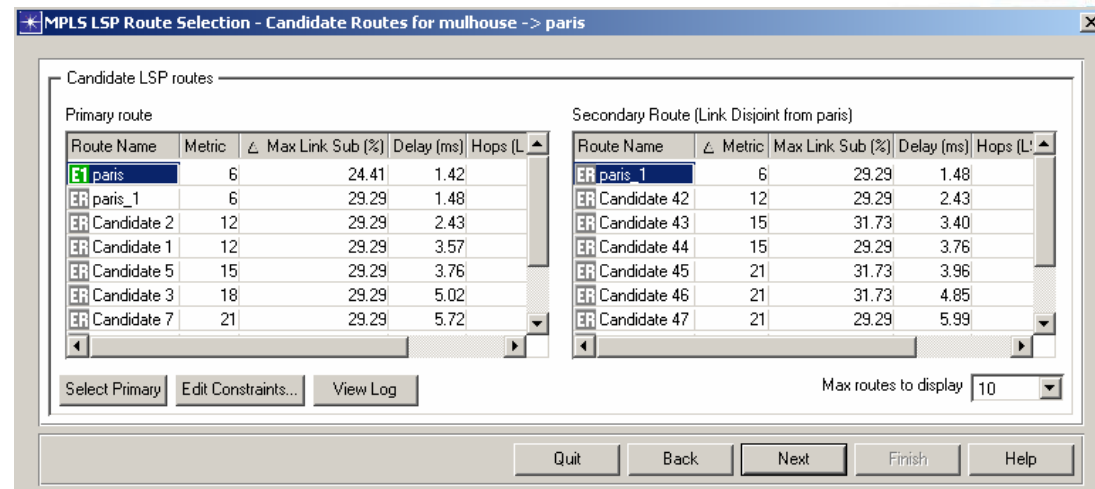
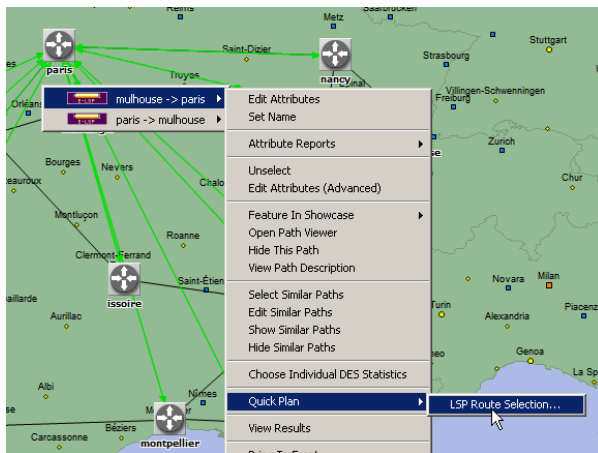


A new LSP diverts flow onto an alternate path



# Quick Plan LSP Route Selection Workflow

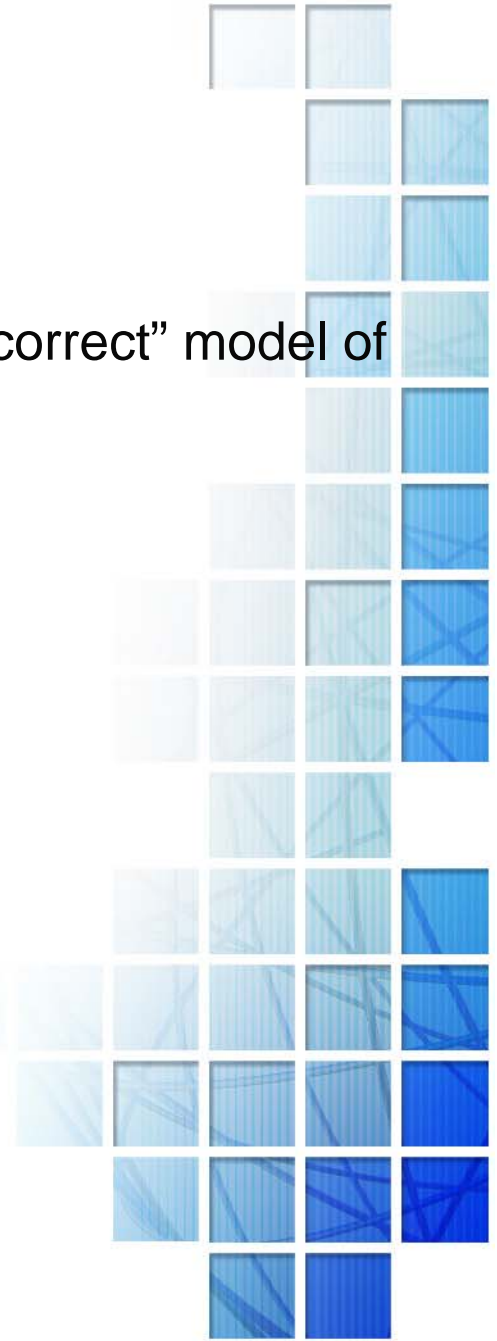
- Reroute existing LSPs
  - Launch LSP Route Selection wizard from an LSP's right-click menu
  - Select primary and optionally secondary explicit routes





# MPLS TE – Automated Model-Building

- Automatically constructing a detailed, “operationally correct” model of the existing network
  - Topology (nodes and links)
  - Detailed device and protocol configuration
  - Existing LSPs, their configuration, routes
  - Link and LSP usage information
    - IF-MIB (Cisco), IF-MIB extension (Juniper)
  - (Optionally) traffic
    - Usual imperfect sources
    - 3rd party systems
    - Traffic inference





# MPLS TE – Explicit Route Generation

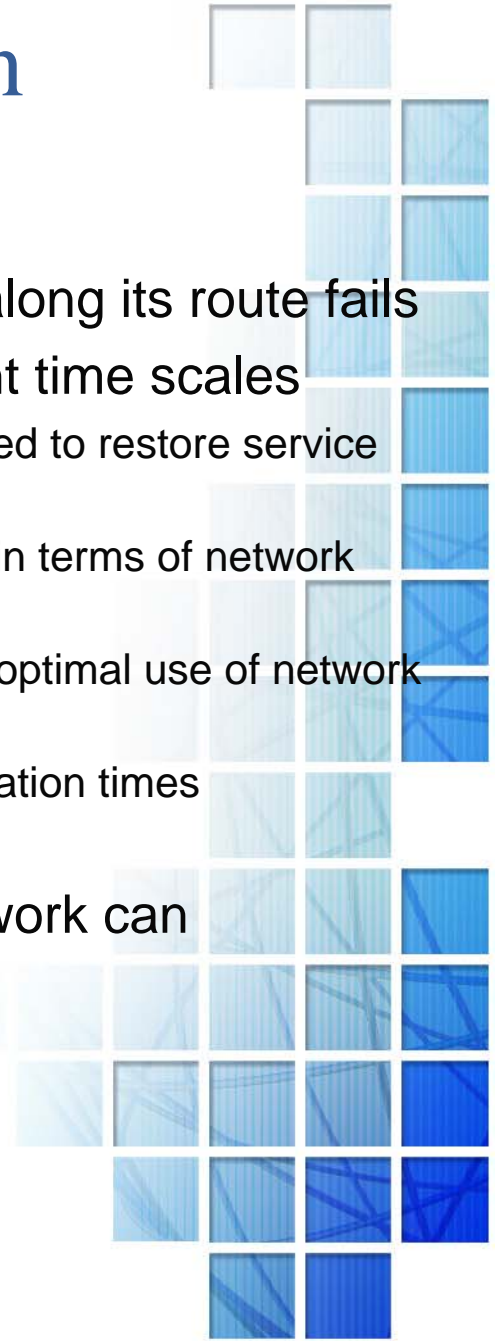
- Automated design and analysis of traffic engineering solutions against operational goals
  - Design
    - CSPF versus explicit routing
    - Explicit route computations (primary, secondary, restoration, etc.)
  - Analysis
    - Performance analysis (e.g., design utilization metrics, device and link usage/subscription metrics, delay metrics, etc.)
    - Failure analysis
    - Traffic growth analysis
    - Topology analysis





# MPLS Resiliency and Restoration

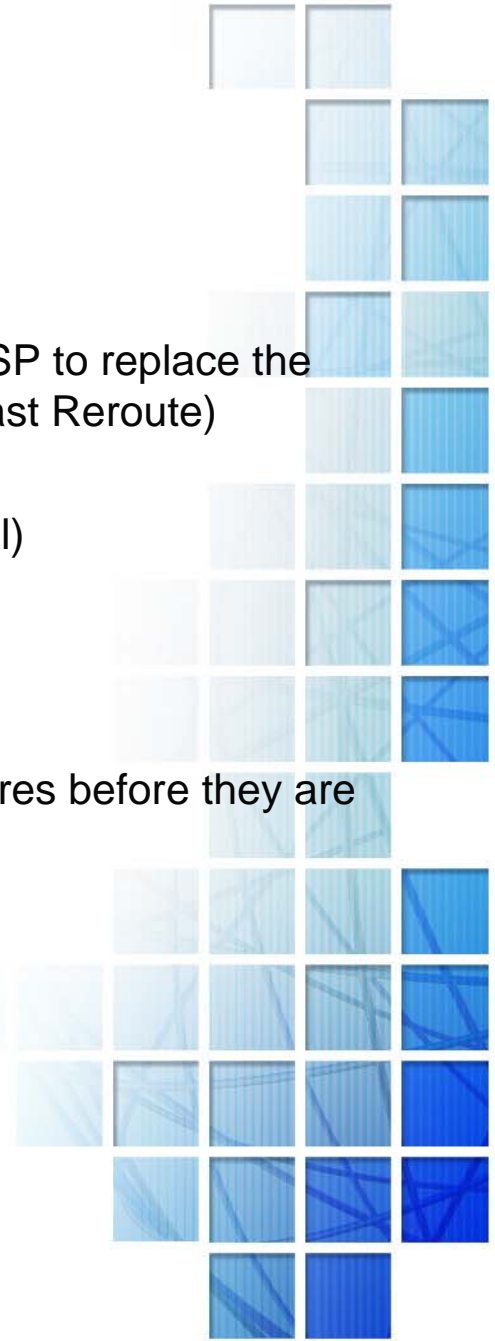
- An LSP becomes unusable if any network resource along its route fails
- LSP restoration mechanisms can be setup at different time scales
  - Mechanisms generally have a tradeoff between the time required to restore service after a failure, resources used, and complexity of configuration
  - Slower mechanisms tend to provide better long-term solutions in terms of network resources
  - Faster mechanisms protect in-flight data but at the cost of sub-optimal use of network resources
    - Some carriers seeking near SONET (50 milliseconds) restoration times
  - Multiple mechanisms make sense
- A network's resiliency is the degree to which the network can successfully survive failures





# MPLS Protection Approaches

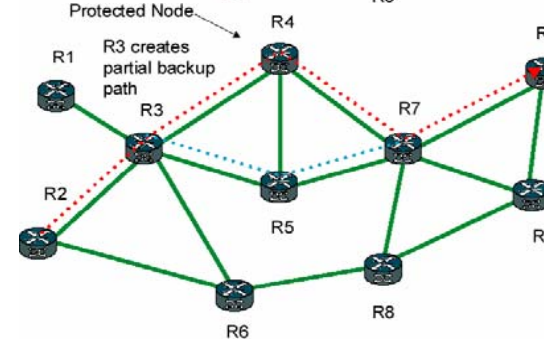
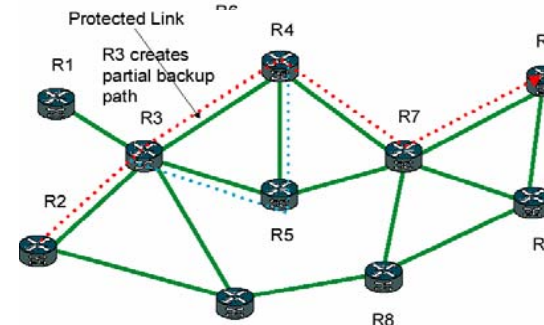
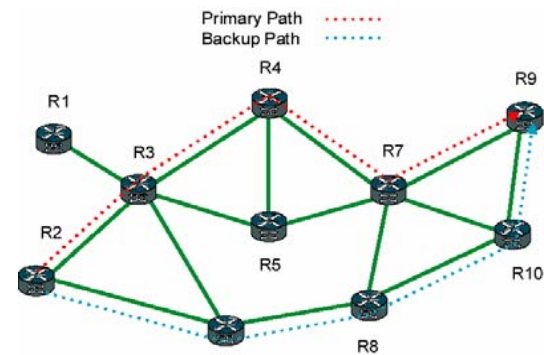
- Local protection
  - Each LSR in the path has a precomputed alternate next-hop LSP to replace the physical next hop if the primary becomes unavailable (Cisco Fast Reroute)
  - Requires stackable LSPs (LSPs riding other LSPs)
  - Does not require head-end signaling (45-50 milliseconds typical)
  - Does not use additional resources until the failure occurs
  - Temporary solution until head-end router can restore the LSP
- Physical layer protection
  - Relying on the SONET redundancy features to handle link failures before they are detected by IP/MPLS (< 50 milliseconds)
- Hybrid strategies
  - Example protection strategy:
    - Platinum/Real-time traffic (VoIP/Video): FRR
    - Gold/Premium: secondary explicit routes
    - Bronze/Best effort: no protection





# Resiliency Strategies

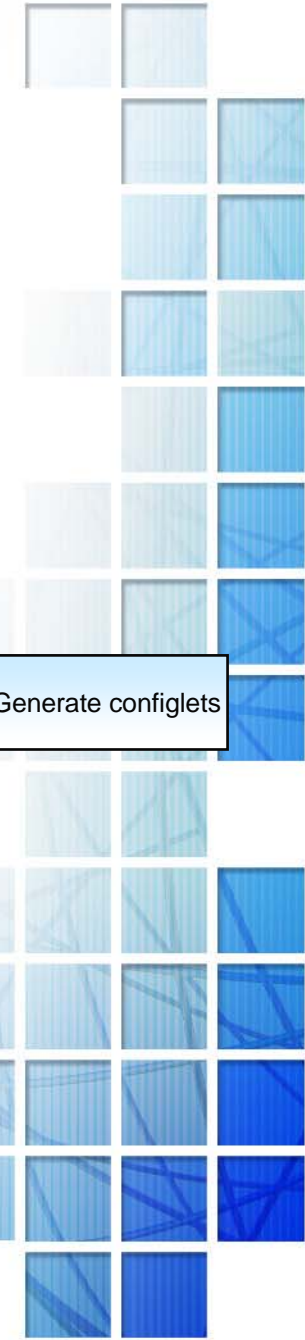
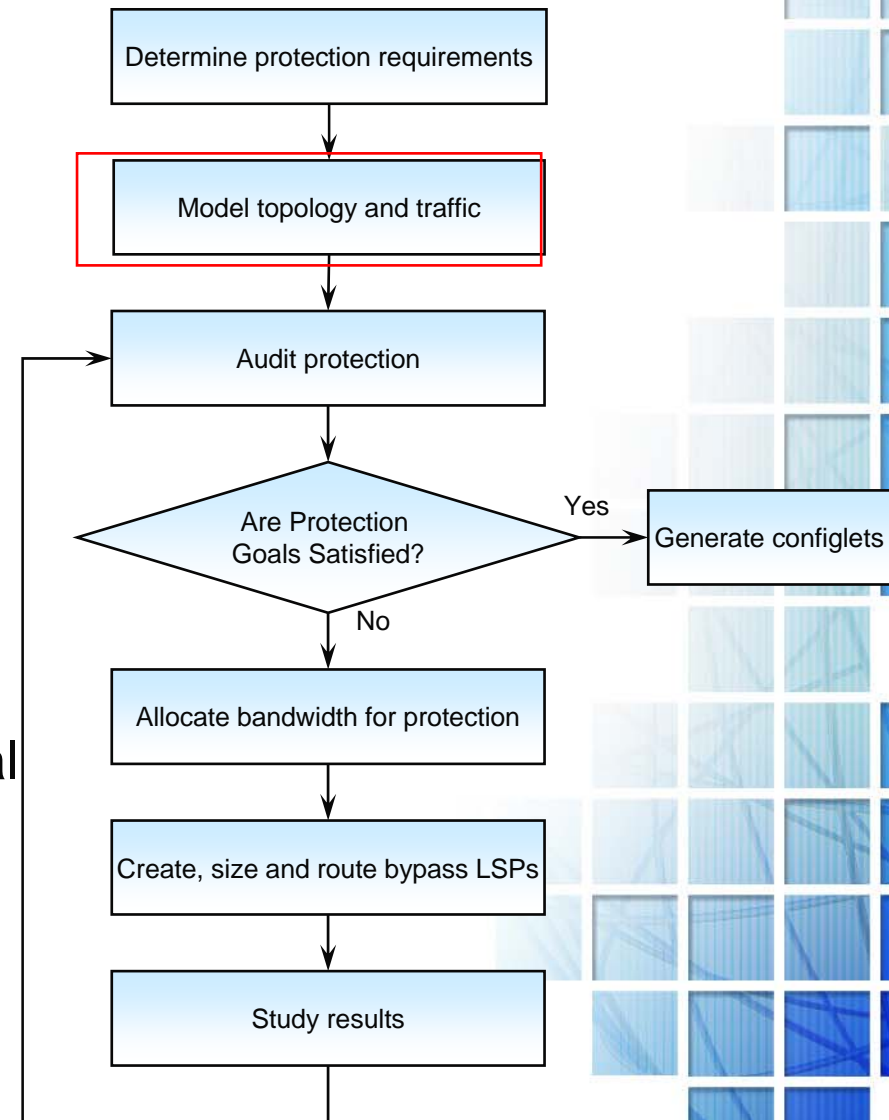
- Path Backup
  - CSPF recomputation
  - Secondary Paths
- Local Backup: Link protection
- Local Backup: Node protection





# Determine Protection Requirements

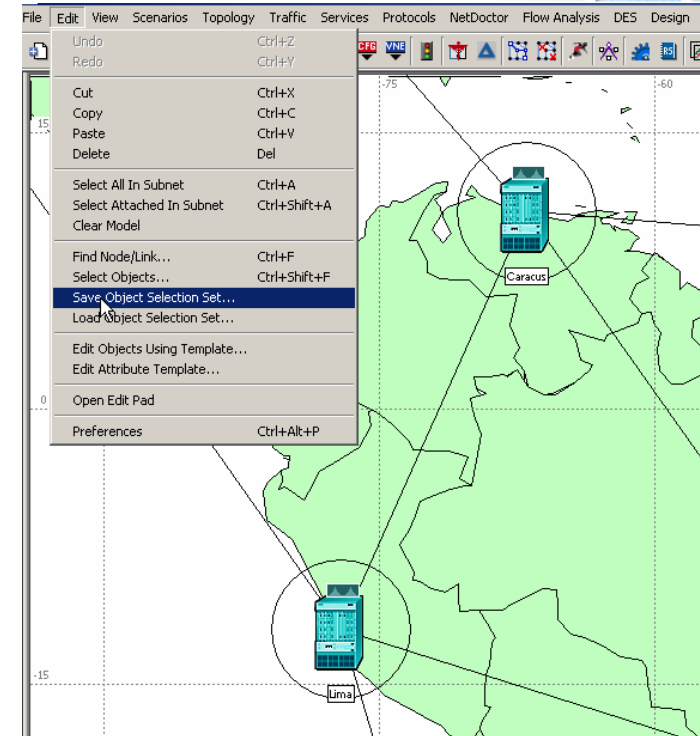
- What services do you want to protect?
  - Voice, Video, VPN, etc.
- Which type of failures need protection?
  - Links or nodes
  - Backbone or access
  - Specific geographic locations
  - Specific bandwidth pools
- What type of protection is optimal (FRR and/or secondary paths)?





# FRR workflow

- A list of objects can be saved to a file to be referred to by design actions
  - Files are called “object selection sets”
  - Suffix is .sset
  - Files can contain nodes, links, demands, paths and subnets
  - Refer to objects by name and hierarchy
  - Changing names or subnet hierarchy will invalidate selection set





# FRR workflow cont.

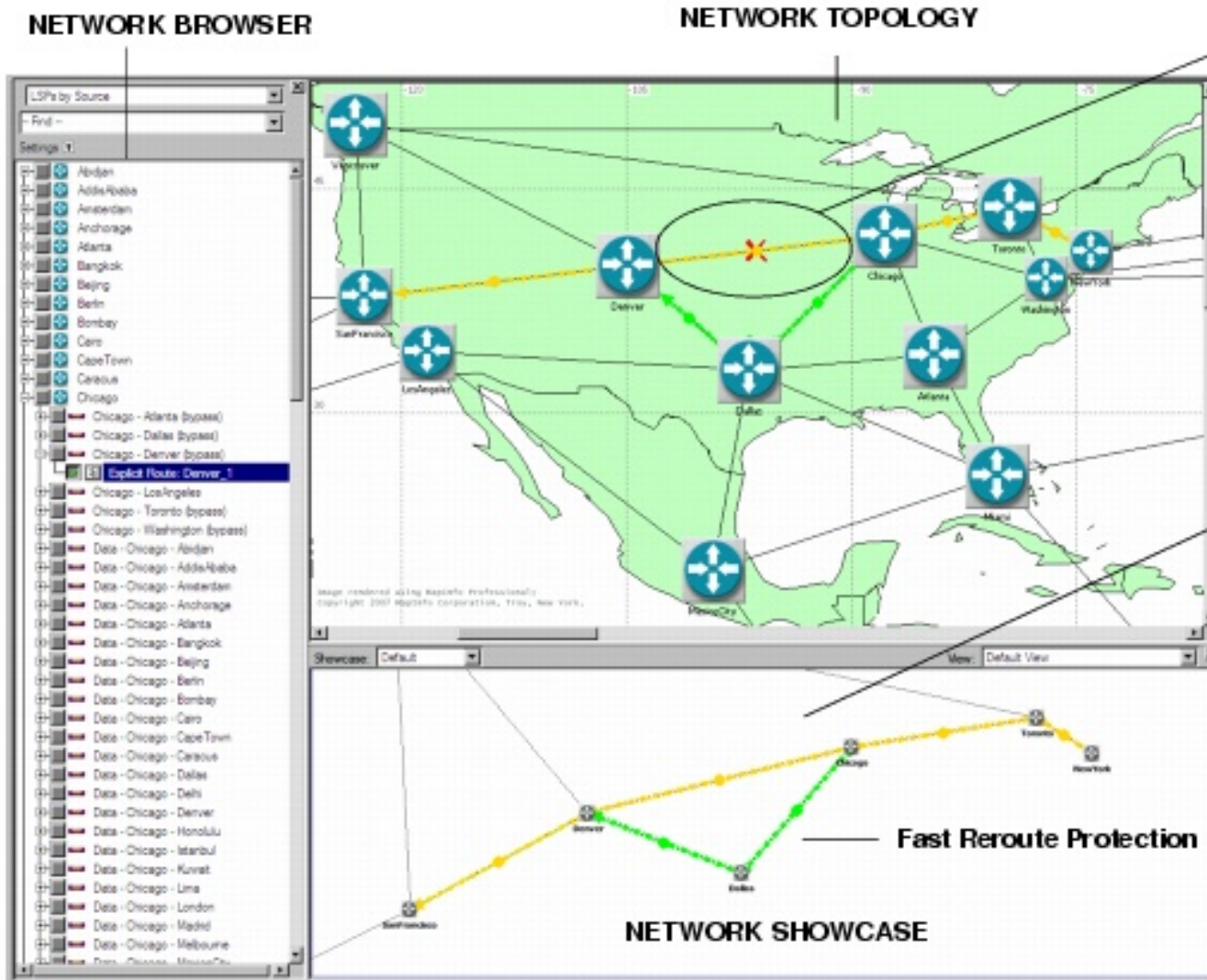
- Design action allows specifying a list of protected facilities
  - Multiple entries supported in the table
  - Specify object selection sets for facilities and bypass tunnel endpoints

The screenshot shows the 'Configure/Run Design Action' window. The 'Design Action: mpls\_frr\_bypass\_lsp\_generation' is selected. The 'Protected Facility' attribute is expanded to show a table of protected objects. A red box highlights the table content.

Protected Object Set	Protected Object Type	Bandwidth Pool	PLR/MP	SR Object Set
ALL	Link	anypool	ALL	
south_american_routers	Node	subpool		north_american_routers



# FRR example



When a link fails between Chicago and Denver, an explicit route bypass LSP protects the LSPs to Denver via Dallas.

Selected objects in the network browser:

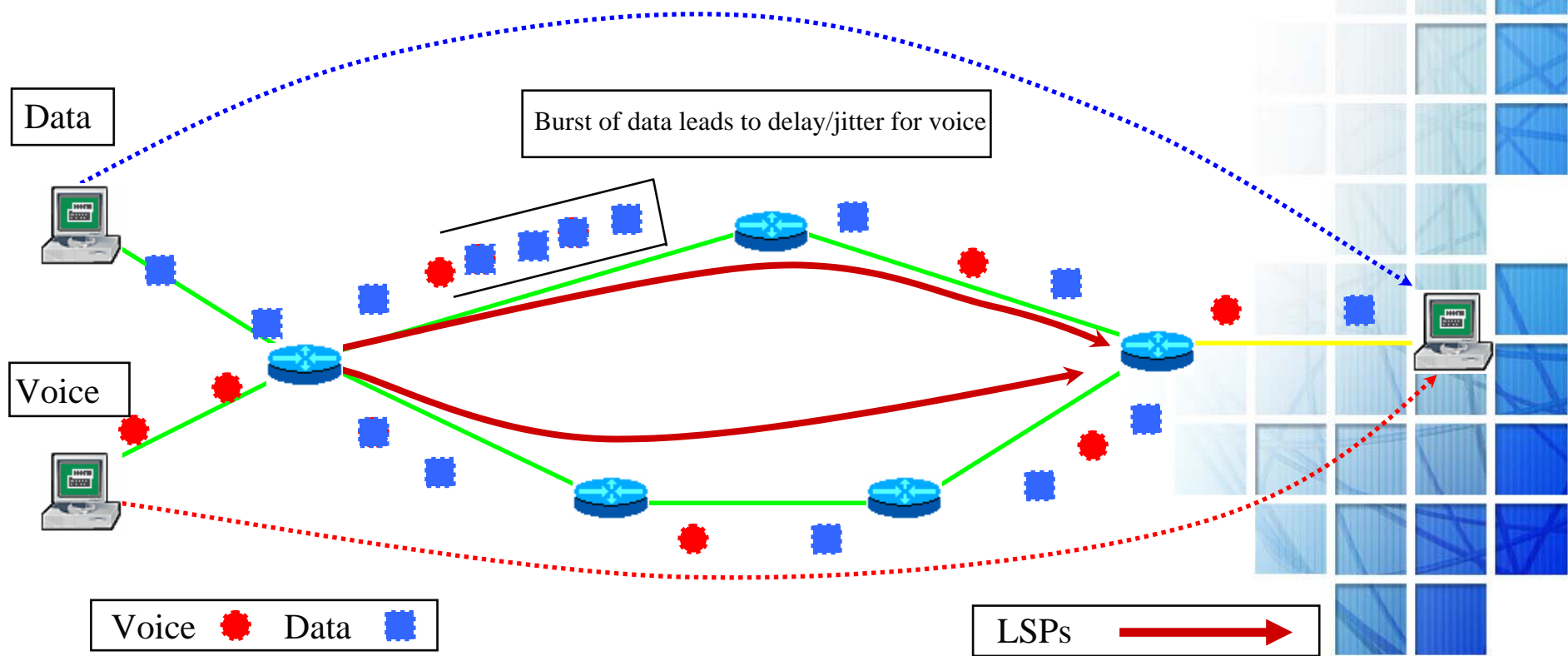
- Bypass route between Chicago and Denver - - - -
- Protected LSP between New York and San Francisco (also selected in the network browser but not shown) - - - -





# Traffic Engineering Isn't Enough

- TE without congestion management is not sufficient for delay and jitter sensitive traffic
  - Bursts of one traffic type may introduce unacceptable delays for other traffic types even when total traffic is under subscribed rates

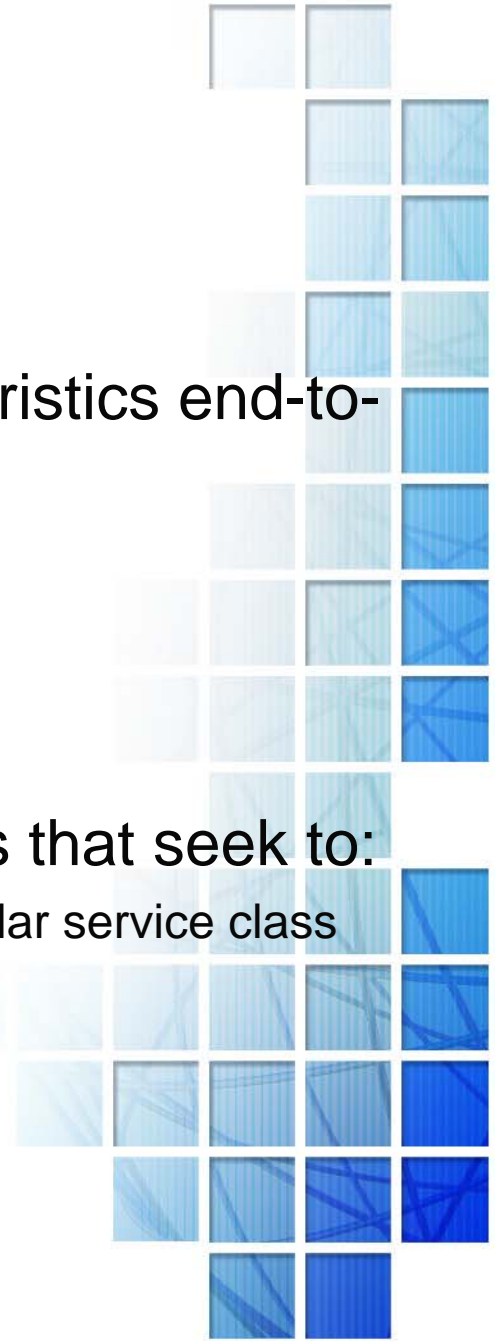




# Quality of Service - Definition

## QoS (Quality of Service)

- Ability to guarantee transmission characteristics end-to-end such as:
  - Throughput
  - delay
  - jitter/delay variation
  - loss
- Various resource management techniques that seek to:
  - Guarantee or improve the performance of a particular service class
  - Provide differentiation among service classes

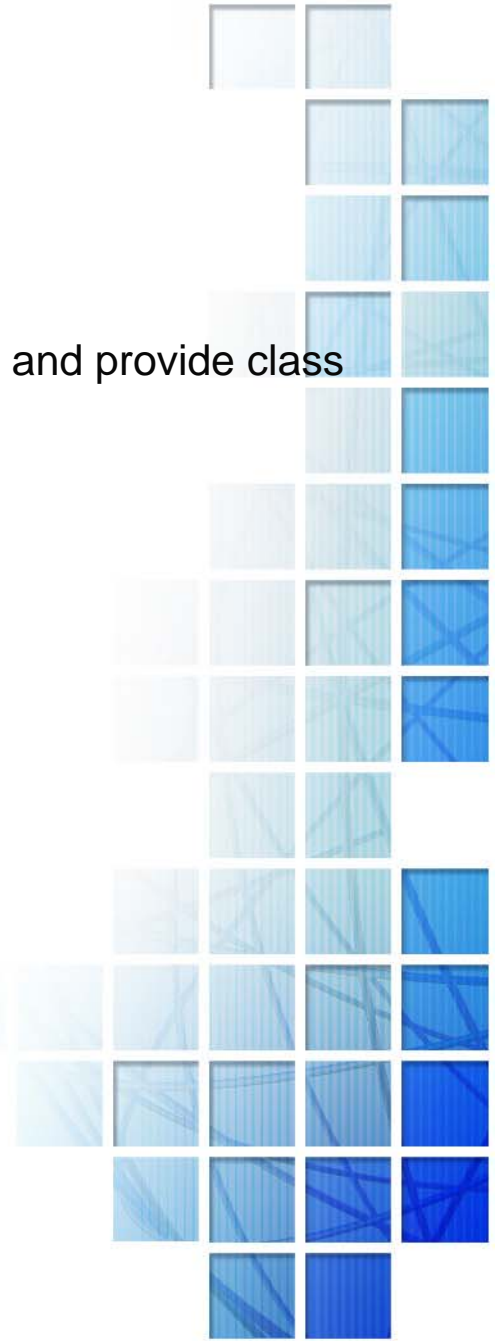




# Class of Service

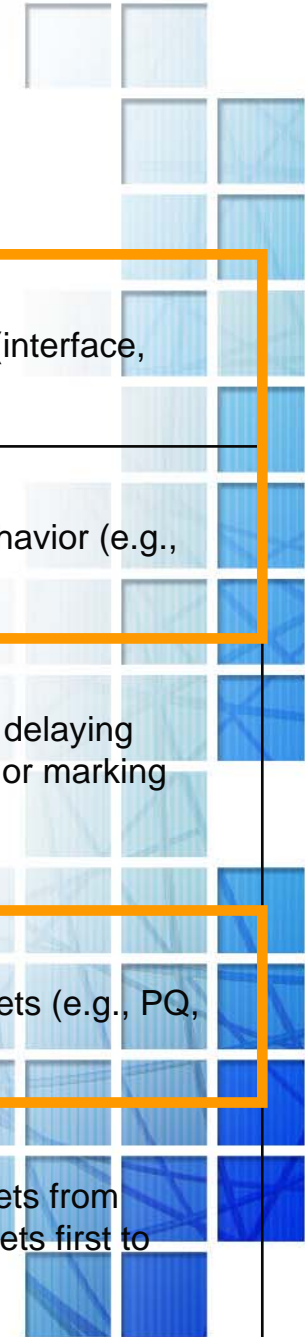
- CoS (Class of Service)

- Ability of network devices to classify traffic into aggregate flows and provide class specific treatment
- No absolute guarantees (only relative ones)
- Requires:
  - Classifying flows for same level of treatment
  - Class state information (not per flow information)
- Level of treatment depends on class and state of network





# Quality of Service Components

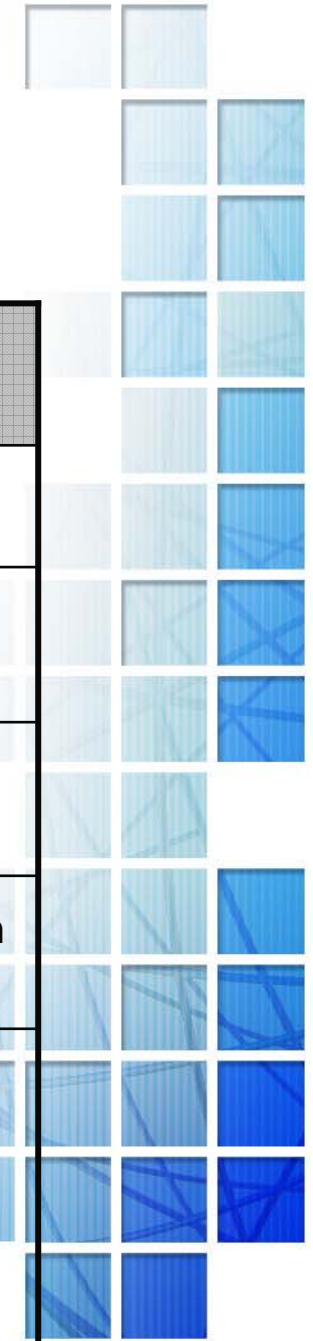


<b>Conditioning (Edge)</b>	<b>Classification</b> Categorize packets into traffic classes based on packet/flow characteristics (interface, addresses, ToS, etc.)
	<b>Packet Marking</b> Provide differentiation among packets for a particular per-hop forwarding behavior (e.g., DSCP, ToS, MPLS EXP bits)
	<b>Traffic Shaping and Policing</b> Ensure adherence of nonconforming traffic to committed information rate by delaying excess traffic in a buffer (shaping), dropping nonconforming traffic (policing) or marking (discard eligible)
<b>Forwarding (Core)</b>	<b>Congestion Management</b> Uses queuing and scheduling mechanisms that favor high precedence packets (e.g., PQ, CBWFQ, MDRR, DWRR)
	<b>Congestion Avoidance</b> Takes advantage of TCP's congestion control mechanism by dropping packets from congested queues to avoid tail drops. Can also drop lower precedence packets first to achieve differentiation (e.g. RED/WRED)



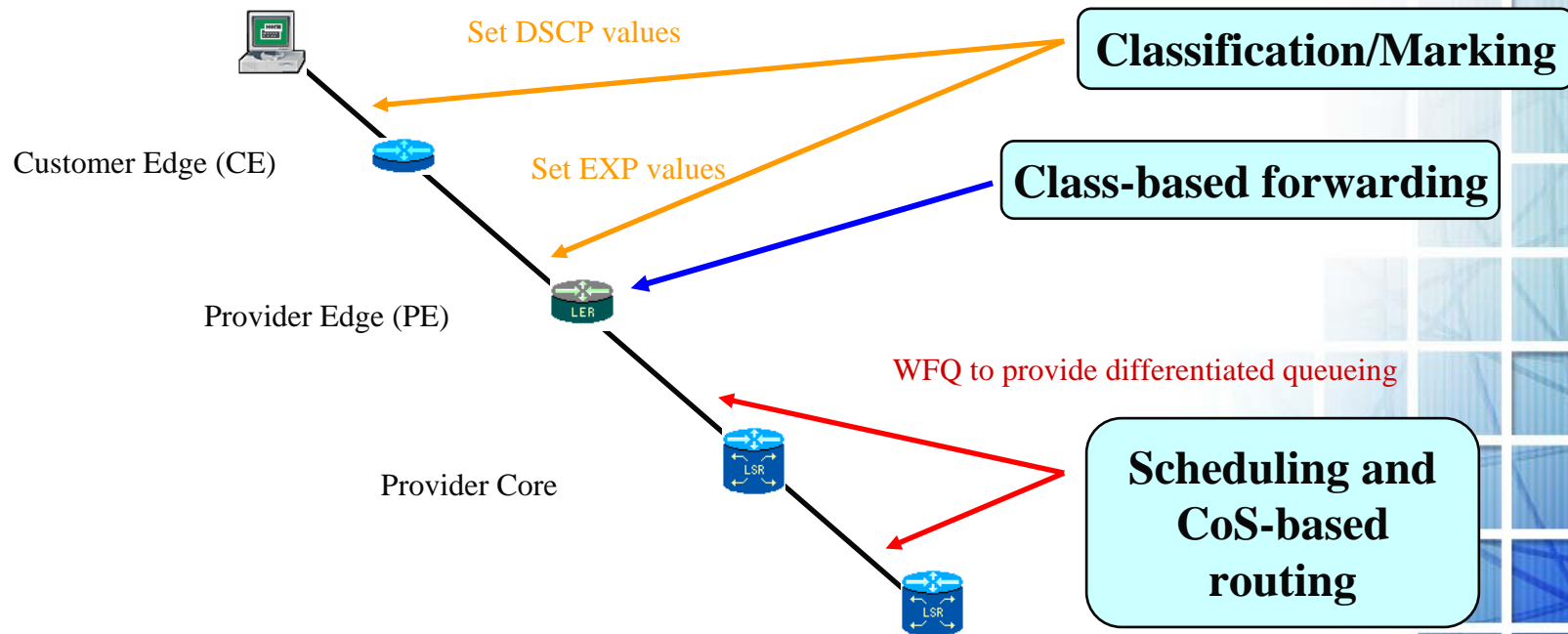
# MPLS Support for QoS

Component	Direct Support	Indirect Support
Classification		Traffic classes defined based on EXP bits
Marking		EXP bits in shim header used to carry mark
Policing/Shaping		Policing the tunnel interface associated with the LSP
Scheduling		Per-hop behaviors based on EXP bits
CoS Routing	Uses RSVP-TE to reserve bandwidth along LSP routes; CSPF routes LSPs subject to bandwidth constraint	



# Differentiated Services

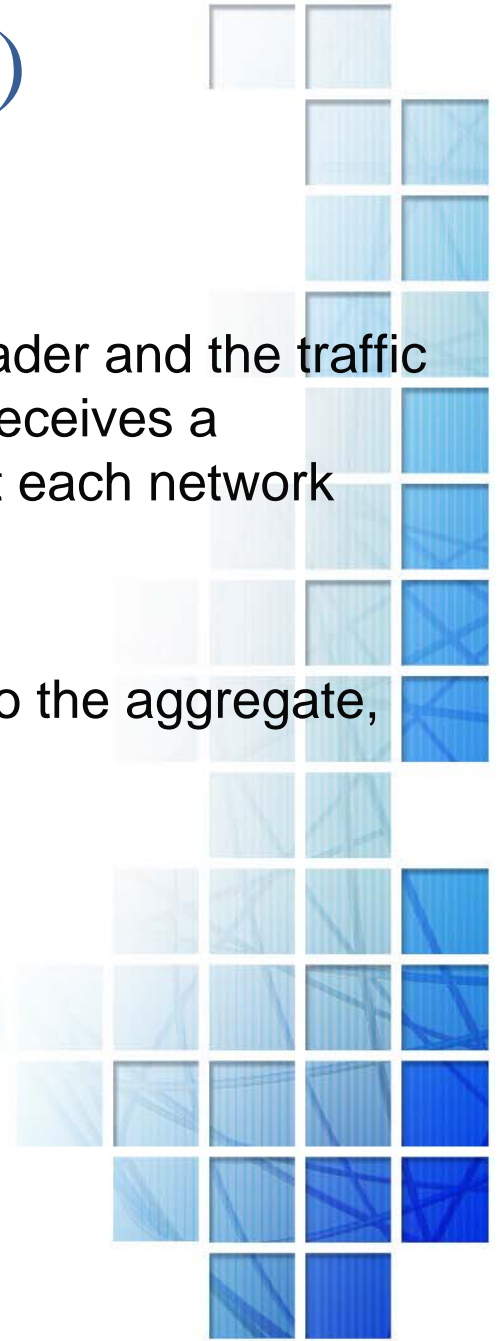
- Focus on QoS provisioning across single domain and not *end-to-end*
- Classification/Marking/Policing at the **edge**
- “*class-based*” forwarding through the **core**
- Use of IP ToS byte for DSCP (DiffServ Code Point)
- Allocate resources for aggregate traffic (Not individual flows)





# Differentiated Services (DiffServ)

- Provides building blocks to define a variety of services
- Defines DSCP byte (TOS/Precedence byte of IPv4 header and the traffic class byte for IPv6) and marks it such that the packet receives a particular forwarding treatment, or per-hop behavior, at each network node
- Services are typically for aggregate classes of traffic
- Implementations typically support resource allocation to the aggregate, but not explicit per-flow reservations
- DiffServ-related RFCs
  - ToS in IP, RFC 1349
  - DSCP Definition for IPv4 and IPv6, RFC 2474
  - EF PHB, RFC 2598
  - AF PHB, RFC 2597





# DiffServ PHBs

- **Per-Hop Behavior (PHBs)**

- Forwarding behavior of a DiffServ node that is applied to the set of packets (class) with the same DSCP
- Can be defined in terms of queuing priority, or observable traffic service characteristics such as delay, jitter, loss
- In other words, a PHB is an externally observable “black box” behavior whose implementation is not mandated

- **Two PHBs are standardized**

- Expedited Forwarding (EF)—RFC 2598
  - Dedicated low latency queue (LLQ)
- Assured Forwarding (AF)—RFC 2597
  - 4 queues × 3 drop precedences

- **Best Effort is default behavior**

- **DiffServ defines 14 service classes**

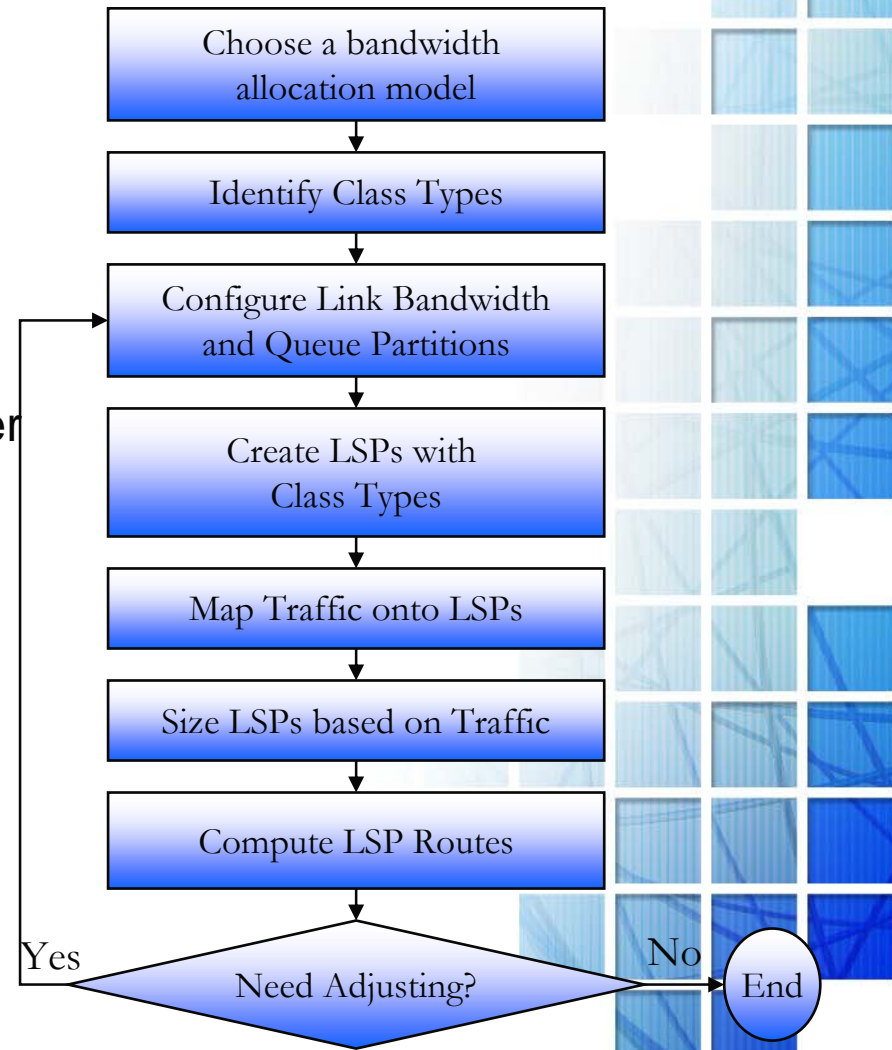
- Allows for 8 more for backward compatibility with the ToS definitions
- But there are  $2^6=64$  different possible settings for the 6 DSCP bits





# DS-TE Basic Workflow

- Choose a bandwidth allocation model
- Identify the class types to support and finalize the model
- Configure link bandwidth and queue partitions for these class types
- Create LSPs with class types
- Map traffic onto these LSPs, using either
  - Policy routing, or
  - Class-based tunnel selection
- Size LSPs based on their carried traffic
- Compute LSP routes





# MPLS + DiffServ—In Operation

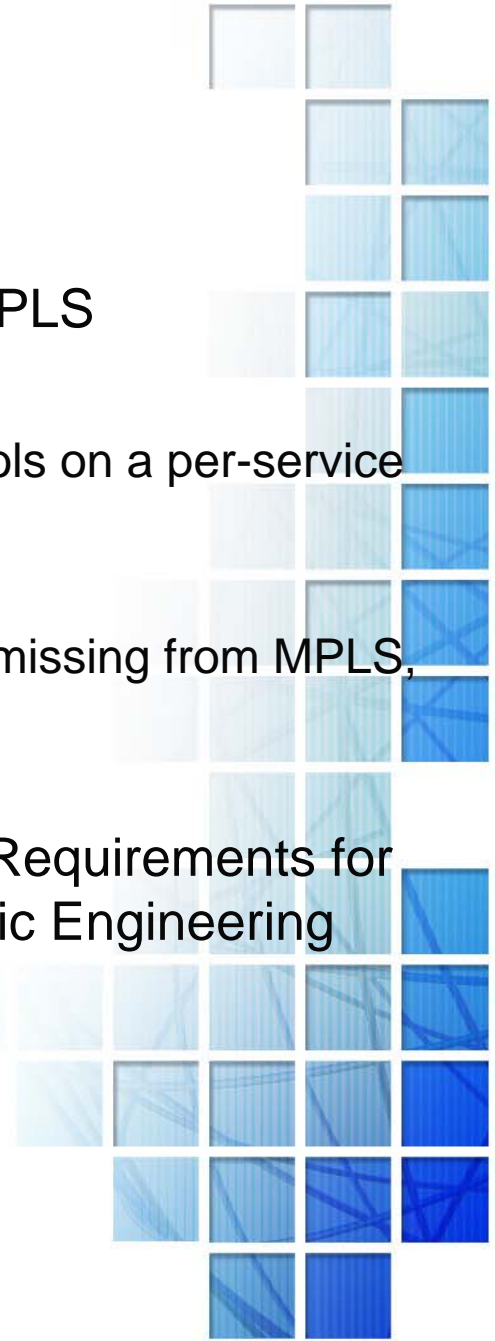
- In an IP DiffServ domain
  - Packets are handled (forwarding, queuing, etc.) based on the IP header's destination address and DSCP bits
- In an MPLS domain with DiffServ enabled
  - Packets are handled along an LSP based on the MPLS header's label that identifies a specific "forwarding equivalence class" (FEC)
  - MPLS domains look at only the MPLS header, not the IP header, so class-of-service queuing behavior is enabled through mapping the IP header DSCP bits to the MPLS header
- IETF RFC 3270 Multi-Protocol Label Switching Support of Differentiated Services is the primary standard





# DiffServ-Aware MPLS TE

- Opportunity to more tightly integrate DiffServ and MPLS
  - Create, configure, and allocate resource reservation pools on a per-service class basis
  - Permit per-service class routing computations in CSPF
  - Note that these are some features from ATM that were missing from MPLS, but applied to an aggregate flow paradigm
- Major principles of DS-TE are defined in RFC 3564: Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering





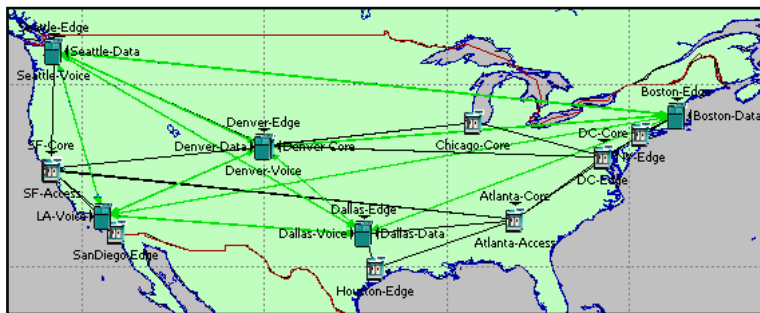
# Class Types

- RFC 3564 definition
  - Class Type (CT) - the set of traffic trunks crossing a link, that is governed by a specific set of bandwidth constraints. CT is used for the purposes of link bandwidth allocation, constraint based routing and admission control. A given traffic trunk belongs to the same CT on all links.
- Links define reservable bandwidth per class
- LSPs request bandwidth from a specific class
- Class types do not have any direct relationship with DSCP
- The DS-TE solution (standard) must support up to 8 class types
  - Same as the number of EXP values
  - Referred to as  $CT_i$  where  $i = 0, \dots, 7$
- A DS-TE implementation must support at least 2 CTs
  - Compliance with the standard requires implementation of at least 2 CTs
- The DS-TE solution must be able to enforce different bandwidth constraints for each class



# Example Study - Summary

- Big Picture of the Network in the following Reports
  - Demand Performance; Link Utilization; Diffserv-Interface Queue Utilization



Performance.Link Utilization						
File Edit View Help						
	Link Name	Utilization Fwd (%)	Throughput Fwd (Mbps)	Utilization Rtn (%)	Throughput Rtn (Mbps)	Details
1	Dallas-Edge <-> Atlanta-Access	89.71	6.28	92.0	6.44	<a href="#">Details</a>
2	SF-Access <-> Atlanta-Core	89.71	6.28	89.71	6.28	<a href="#">Details</a>
3	SF-Access <-> LA-Edge	89.71	6.28	89.71	6.28	<a href="#">Details</a>
4	Atlanta-Core <-> Atlanta-Access	89.71	6.28	89.71	6.28	<a href="#">Details</a>
5	Seattle-Edge <-> Denver-Core	88.57	6.2	89.71	6.28	<a href="#">Details</a>
6	DC-Core <-> Boston-Edge	88.57	6.2	89.71	6.28	<a href="#">Details</a>
7	Seattle-Edge <-> LA-Edge	78.5	3.14	78.5	3.14	<a href="#">Details</a>
8	DC-Edge <-> Boston-Edge	78.5	3.14	78.5	3.14	<a href="#">Details</a>

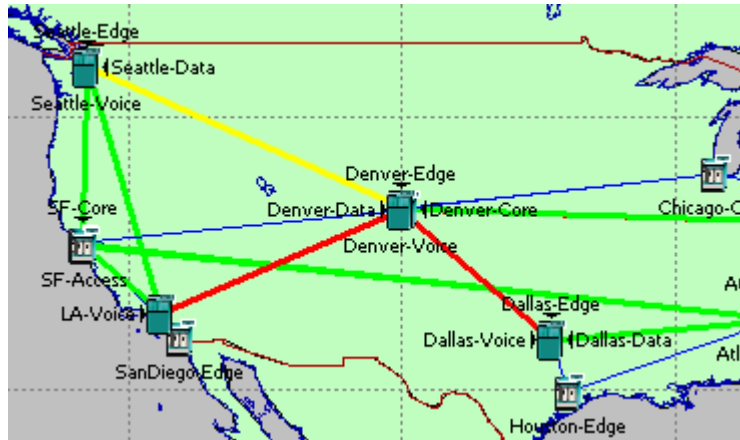
Performance.Demand Performance								
File Edit View Help								
	Demand Name	Address Family	Status	Hop Count	Average Bits Per Sec	Average Delay (msec)	End to End Jitter (msec)	Maximum Packet Loss (%)
1	VOICE_LA-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	28.381	0.089	0.0
2	VOICE_Denver-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	15.803	0.089	0.0
3	VOICE_Dallas-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	16.228	0.111	0.0
4	VOICE_Boston-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	23.972	0.072	0.0
5	VOICE_Boston-Voice_LA-Voice	IPv4	Successful	3	1,000,000	28.383	0.1	0.0
6	VOICE_Boston-Voice_Denver-Voice	IPv4	Successful	3	1,000,000	15.803	0.06	0.0
7	VOICE_Boston-Voice_Dallas-Voice	IPv4	Successful	3	1,000,000	14.311	0.165	0.0
8	VOICE_Dallas-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	28.946	0.048	0.0
9	VOICE_LA-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	8.103	0.004	0.0

Performance.Diffserv-Interface Queue Usage										
File Edit View Help										
	Node	Interface	Bandwidth (Mbps)	Total Interface Utilization (%)	Traffic Class	Queue	Configured Bandwidth Value (Mbps)	Interface Utilization By Queue (%)	Weight Proportional Utilization (%)	EF Queue
1	Atlanta-Access	IF14	7.0	44.86						
2					EF	Queue_EF	4.2	15.71	26.19	Yes
3					BE	Queue_BE	2.8	29.14	72.86	No
4		IF15	5.0	62.8						
5					EF	Queue_EF	3.0	22.0	36.67	Yes
6					BE	Queue_BE	2.0	40.8	102.0	No
7		IF16	7.0	92.0						
8					EF	Queue_EF	4.2	62.86	104.76	Yes
9					BE	Queue_BE	2.8	29.14	72.86	No
10		IF17	7.0	89.71						
11					EF	Queue_EF	4.2	31.43	52.38	Yes
12					BE	Queue_BE	2.8	58.29	145.71	No



# Example Study – Summary (2)

- The Utilization has to be controlled before DiffServ techniques are applied to provide graded levels of service



Inefficient use of network resources

Performance of voice demands improved but data still suffers

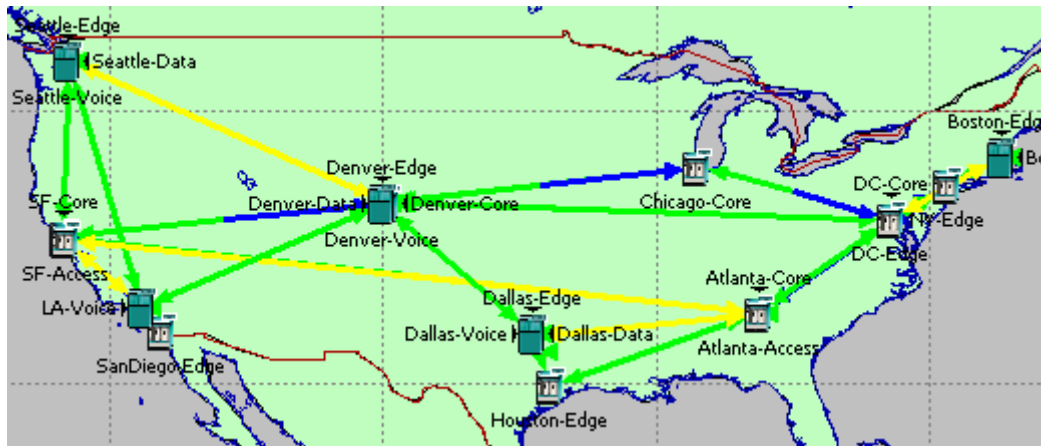
Performance.Demand Performance								
File Edit View Help								
	Demand Name	Address Family	Status	Hop Count	Average Bits Per Sec	Average Delay (msec)	End to End Jitter (msec)	Maximum Packet Loss (%)
1	DATA_Boston-Data_Dallas-Data	IPv4	Successful	3	2,000,000	358.326	38.784	55.882
2	DATA_LA-Data_Dallas-Data	IPv4	Successful	3	2,000,000	203.717	27.918	55.882
3	DATA_Dallas-Data_Boston-Data	IPv4	Successful	3	2,000,000	358.329	49.784	55.882
4	DATA_Denver-Data_Boston-Data	IPv4	Successful	3	2,000,000	255.521	41.877	55.882
5	DATA_Boston-Data_Denver-Data	IPv4	Successful	3	2,000,000	255.52	26.921	31.373
6	DATA_Dallas-Data_LA-Data	IPv4	Successful	3	2,000,000	203.72	26.921	31.373





# Example Study – Summary (3)

- TE and DiffServ are Complementary Techniques



Better performance overall  
Efficient utilization of  
network resources

**Performance.Demand Performance**  
File Edit View Help

	Demand Name	Address Family	Status	Hop Count	Average Bits Per Sec	Average Delay (msec)	End to End Jitter (msec)	Maximum Packet Loss (%)
1	VOICE_LA-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	28.381	0.089	0.0
2	VOICE_Denver-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	15.803	0.089	0.0
3	VOICE_Dallas-Voice_Boston-Voice	IPv4	Successful	3	1,000,000	16.228	0.111	0.0
4	VOICE_Boston-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	23.972	0.072	0.0
5	VOICE_Boston-Voice_LA-Voice	IPv4	Successful	3	1,000,000	28.383	0.1	0.0
6	VOICE_Boston-Voice_Denver-Voice	IPv4	Successful	3	1,000,000	15.803	0.06	0.0
7	VOICE_Boston-Voice_Dallas-Voice	IPv4	Successful	3	1,000,000	14.311	0.165	0.0
8	VOICE_Dallas-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	28.946	0.048	0.0
9	VOICE_LA-Voice_Seattle-Voice	IPv4	Successful	3	1,000,000	8.103	0.004	0.0



# OPNET Support for MPLS

- MPLS data collection
  - Routers, LSPs, configuration
  - LSP utilization
- MPLS modeling, simulation & optimization
  - CSPF (OSPF-TE, ISIS-TE), ERs
  - LDP, RSVP
  - QoS, Diffserv-TE
  - Failure analysis
  - Traffic engineering optimization
  - Resiliency design
- MPLS VPNs
  - L2 (Martini, Kompella) & L3 (RFC 2547)
  - Graphical provisioning wizard
  - Views to study logical VPN topology
- Support for MPLS-related R&D





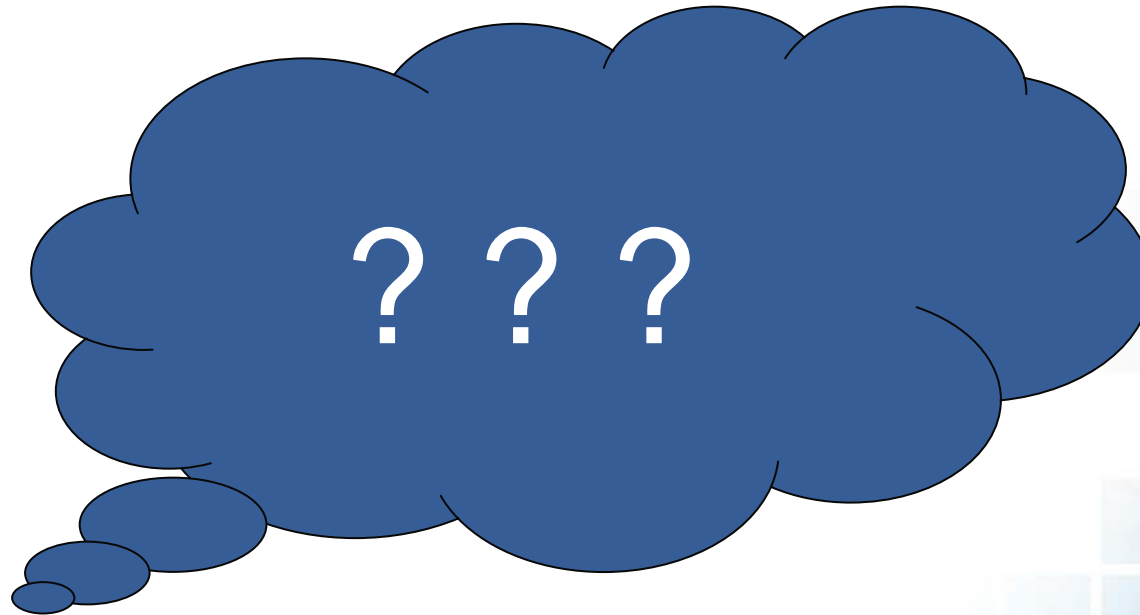
# Summary

- Multi-service networks have challenges regarding, delays, bandwidth, packet loss and delays.
- Traffic Engineering and enforcing QoS are technical approaches to guaranty that the different needs of the services are addressed.
- Both techniques have their own complexity and different sources for errors and misconfiguration
- Offline analytic tools can help to design and to plan resilient and well performing networks by using a „what-if“ approach.
- They can help to create needed TE tunnels, FRR and implement correct QoS.





Thanks a lot for your attention !



**Are there any questions**

