Converged Transport Solutions for Mobile SP's

BRKMWI-3006

Giouami Fruscio

Cisco Networkers 2007

HOUSEKEEPING

- We value your feedback, don't forget to complete your online session evaluations after each session and complete the Overall Conference Evaluation which will be available online from Friday.
- Visit the World of Solutions on Level -01!
- Please remember this is a 'No Smoking' venue!
- Please switch off your mobile phones!
- Please remember to wear your badge at all times including the Party!
- Do you have a question? Feel free to ask them during the Q&A section or write your question on the Question form given to you and hand it to the Room Monitor when you see them holding up the Q&A sign.

Agenda

- Mobile operators transport evolution
- Design consideration for deploying IP/MPLS core

Mobile Operators Transport Evolution

Mobile Operators Proliferation of Disparate Networks

- Voice
  - 2G Voice
  - 3G Voice
  - Enterprise
  - Retail stores
  - Call centres
  - Corporate access
- Data
  - 2.5G GPRS
  - 3G GPRS
  - Enterprise
  - Retail stores
  - Call centres
  - Corporate access
  - Management

WAP

V110 dial

WLAN

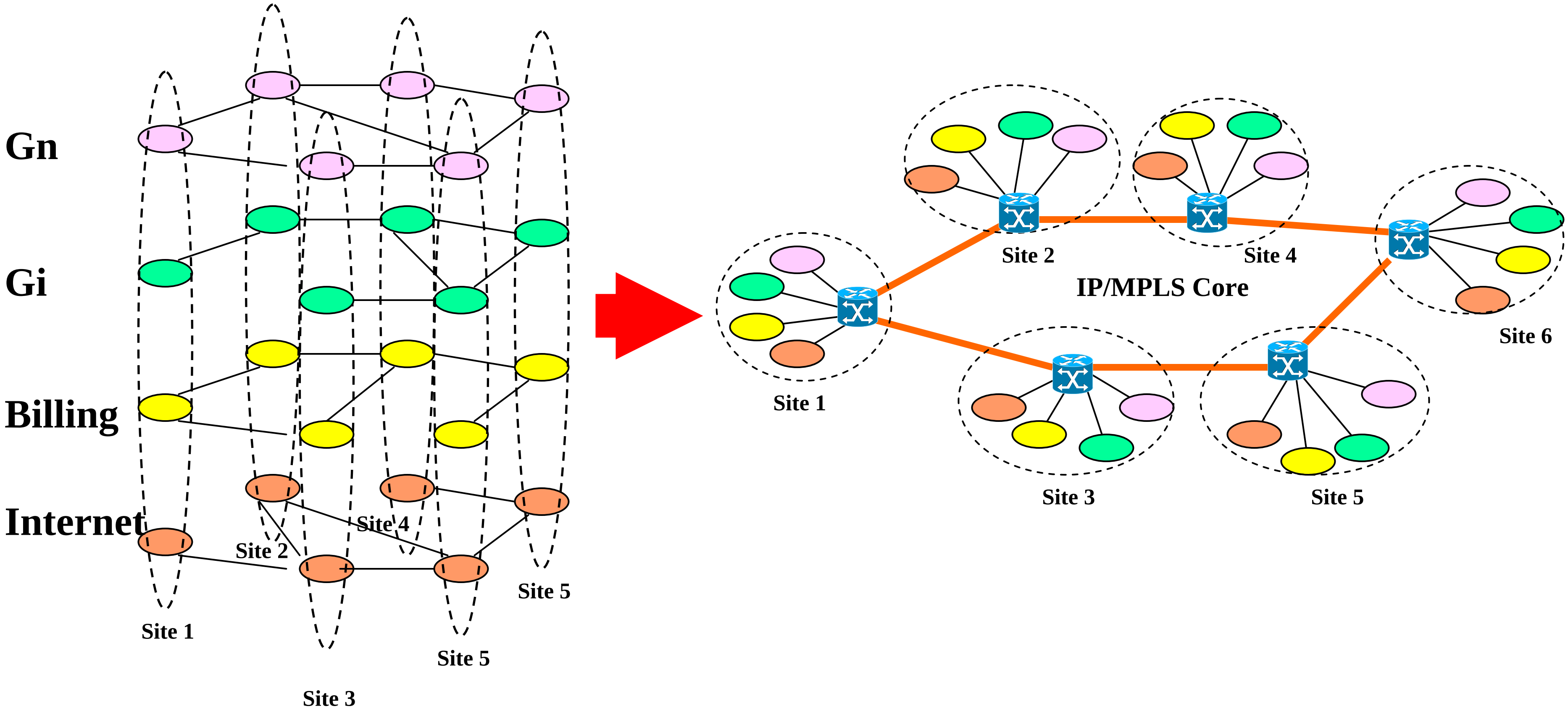
Billing

IPSec

Signalling

Paging

Stage 1: Migrate Disparate Networks to Single MPLS Core



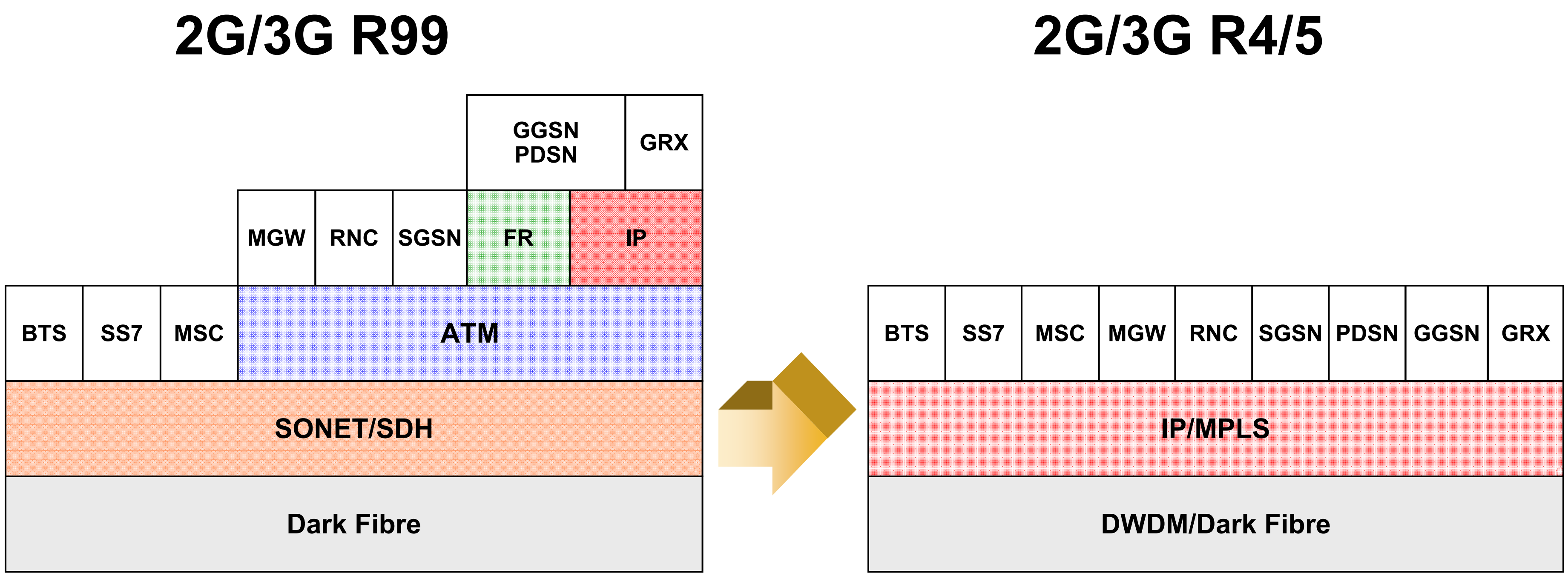
Many networks on common sites with different edge devices and transmission

Single network over high capacity transmission carrying all services

The Business Case for a Converged Network

- By reducing the number of networks
  - Lower transmission costs
    - E.g. cost of 9xE1 = 1xSTM1
    - Use alternates such as GE/10GE
  - Less maintenance contracts
  - Single management solution
  - Quickly deploy new services

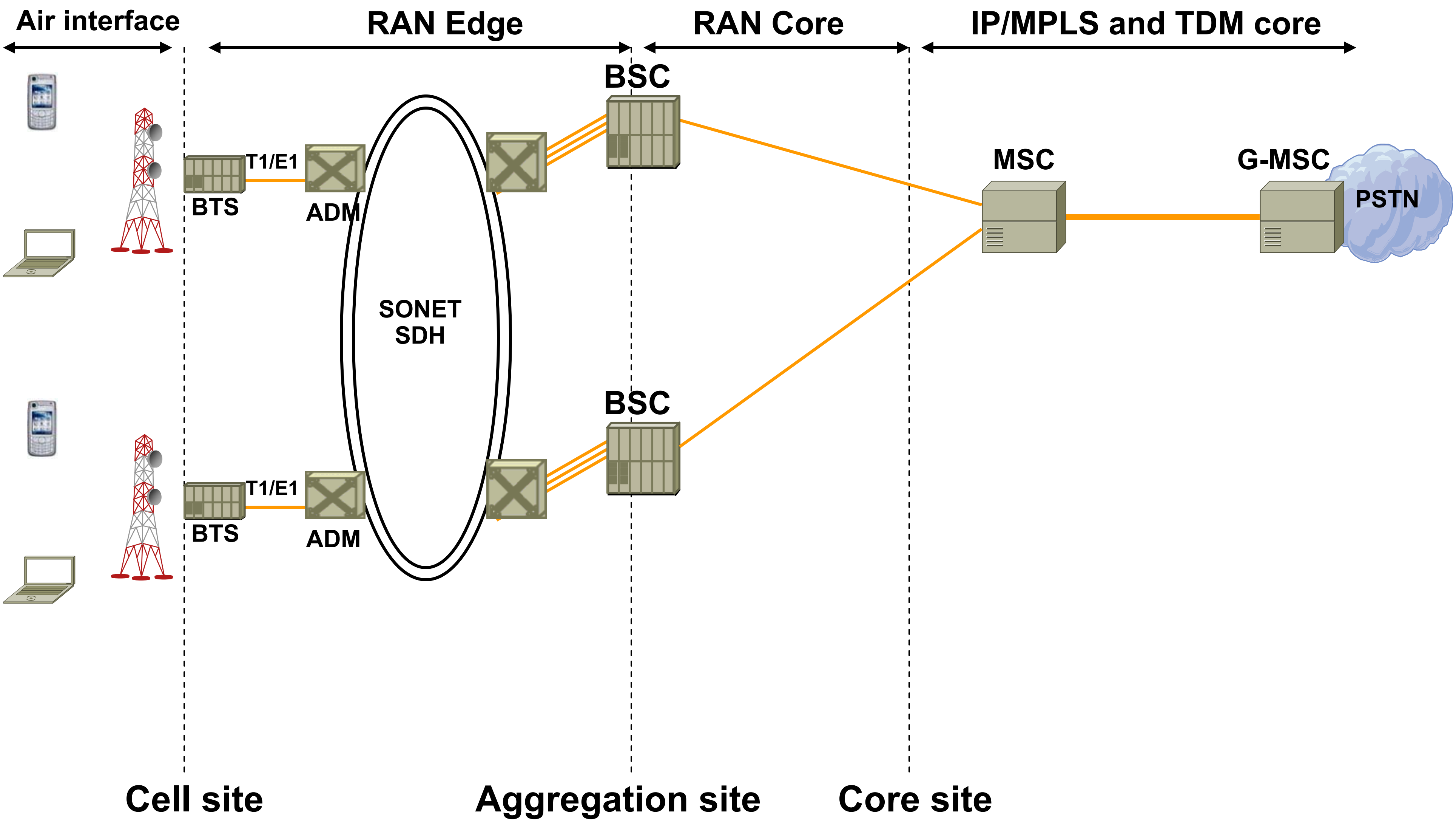
Stage 2: Reducing Complexity and Overlap



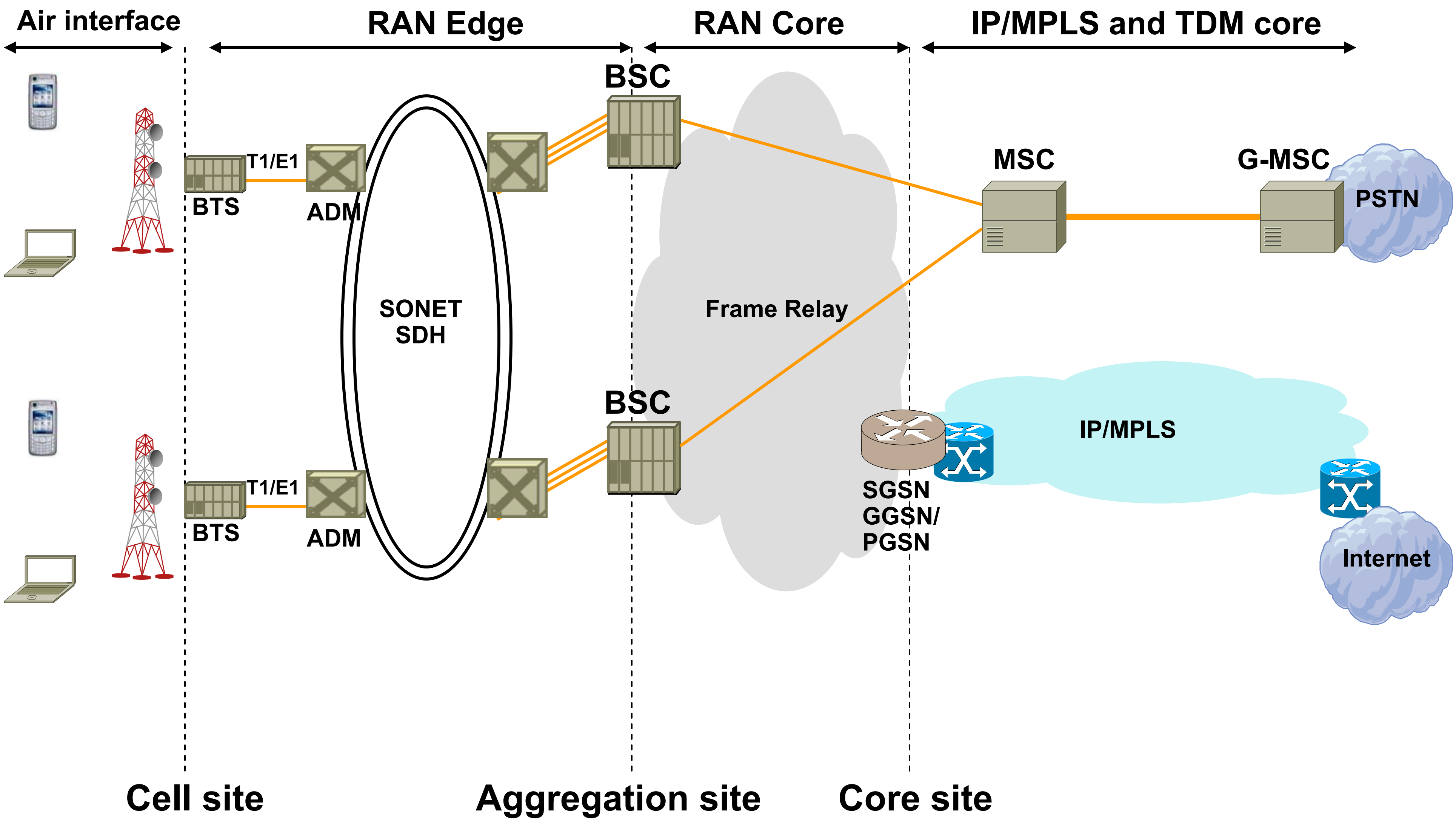
What Next for IP/MPLS Core in Mobile

- Next stage driving deployment is the R4 split architecture with VoIP
- Operators looking to retire existing MSCs early to reduce OPEX and cap investment
- Availability of R4 IP deployments is accelerating
- Voice drives bandwidth with mobile providers looking to upgrade optical networks to provide additional bandwidth 10Gig+

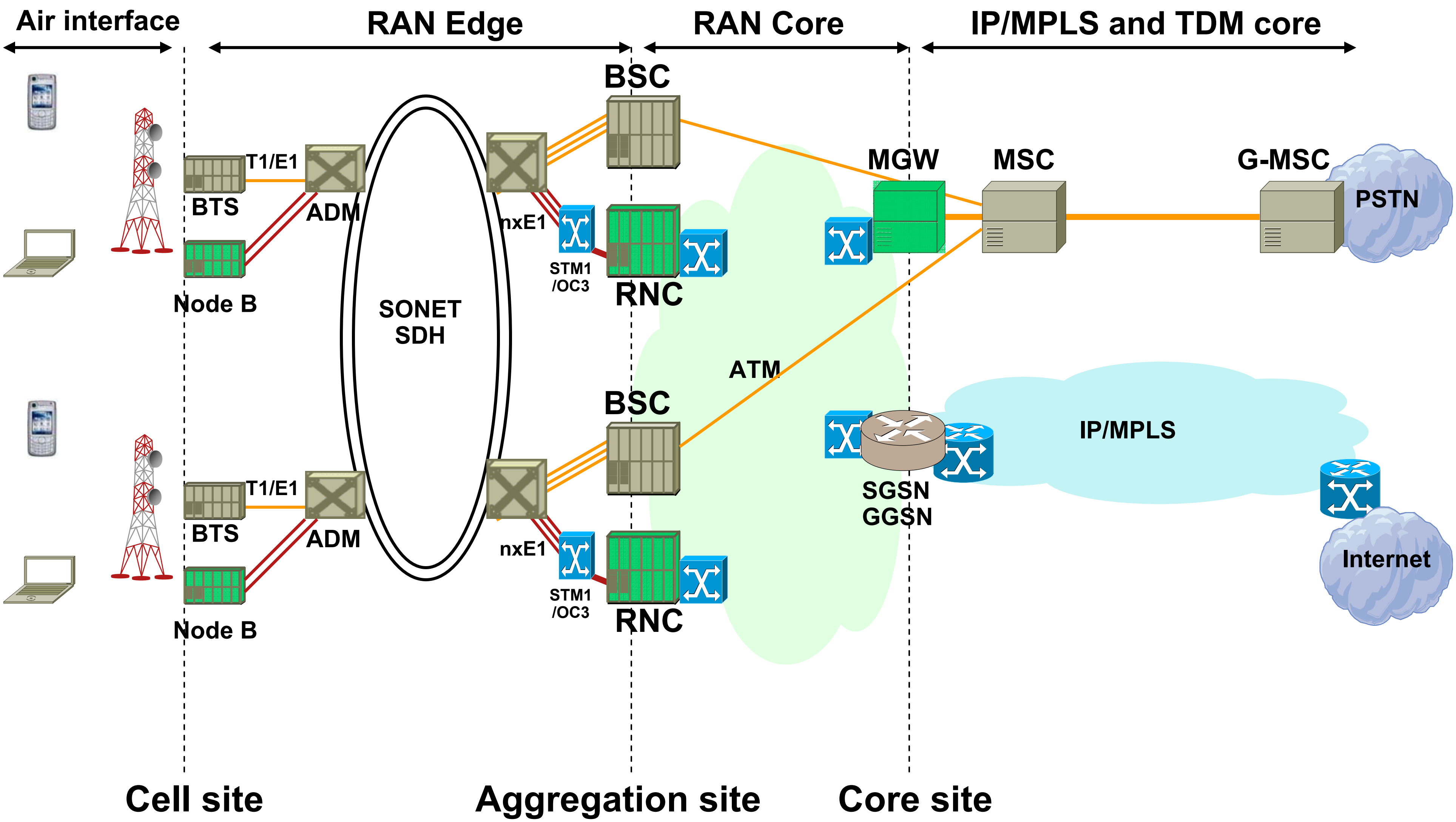
2G TDM Voice Solution



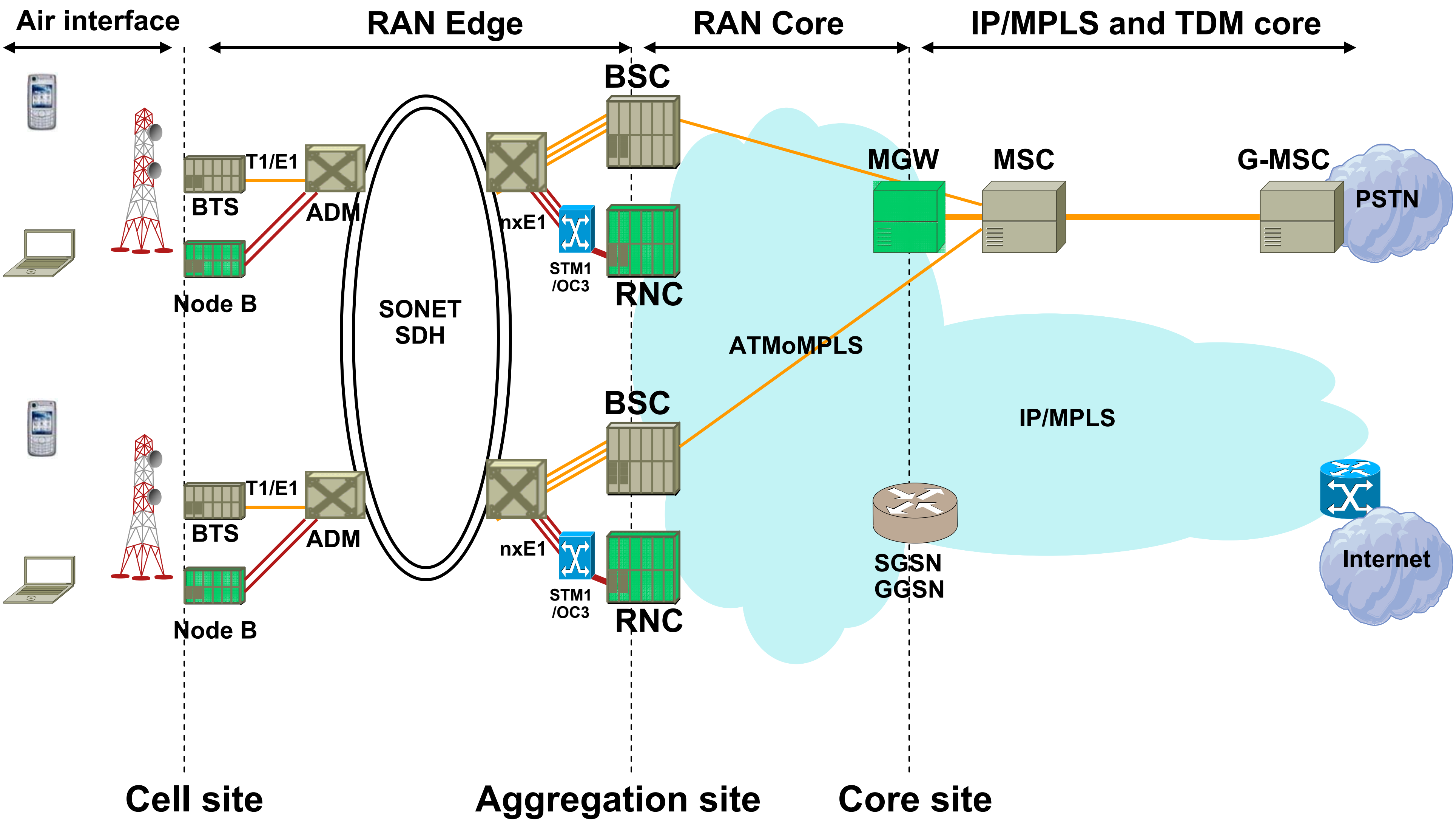
2.5G Adds GPRS Low Speed Data



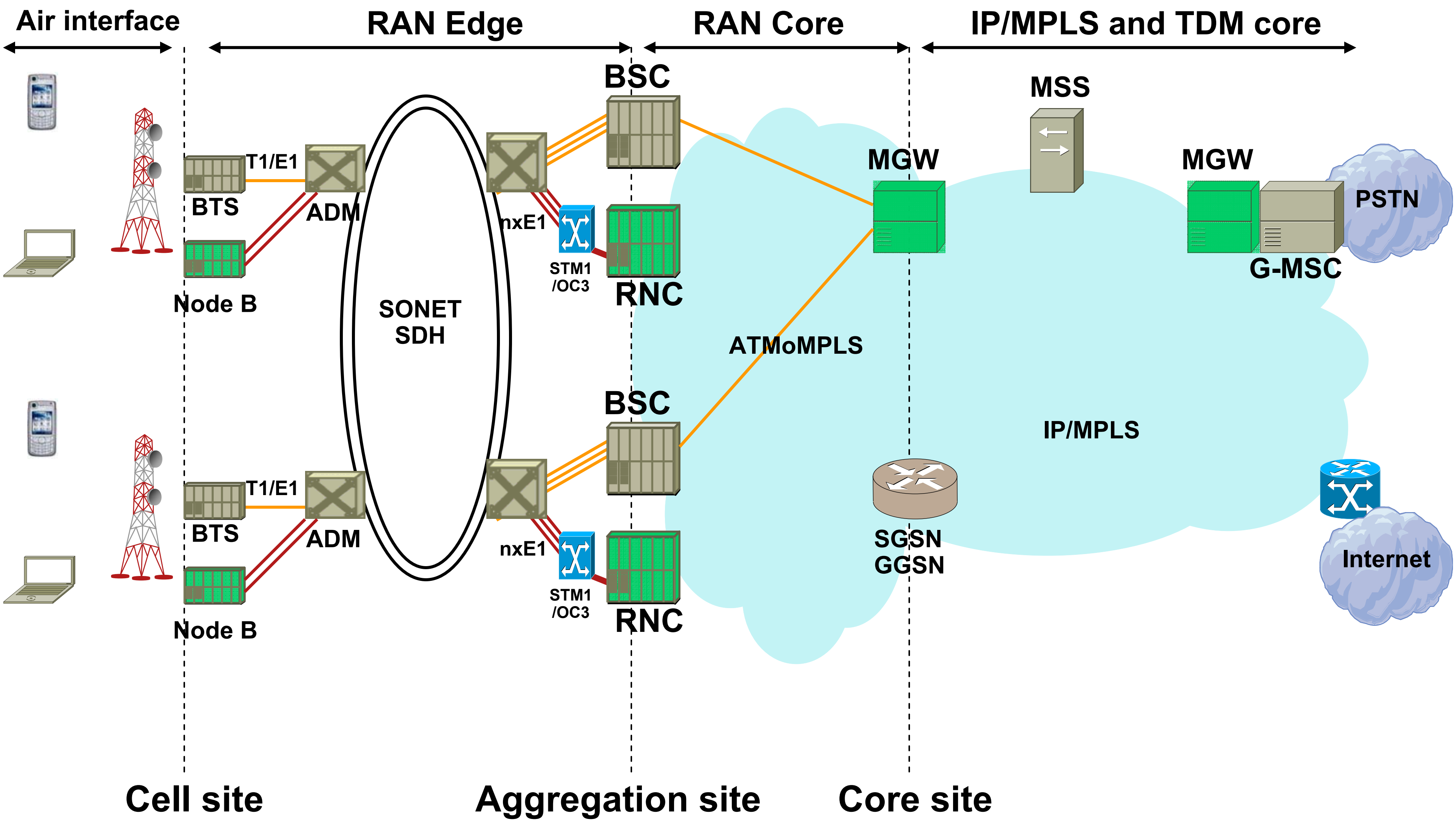
3G R99 Adds ATM RAN and Higher Speed Data



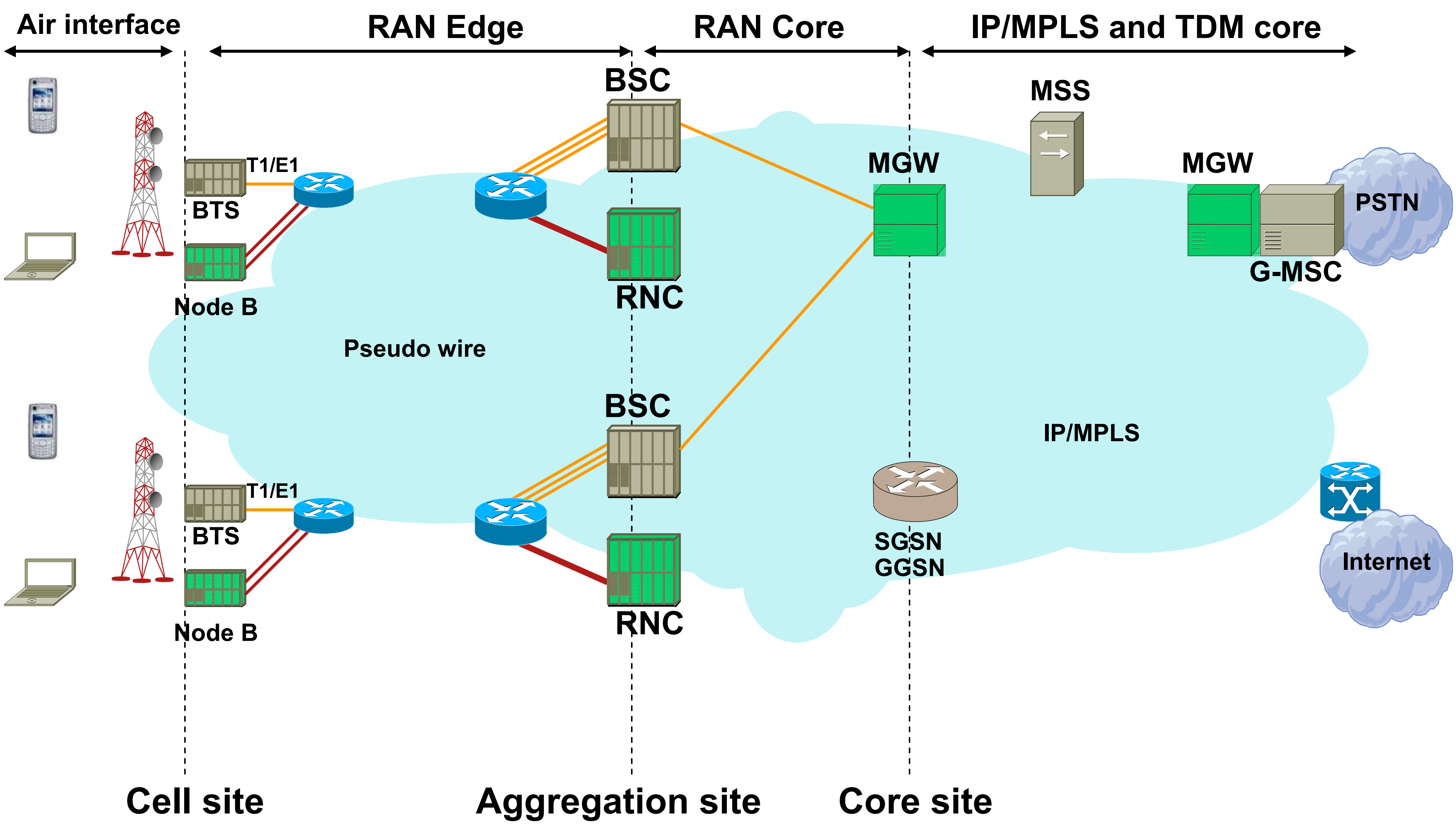
ATM Pseudowire in the RAN Core Allow Operator to Cap Investment in ATM



3G R4 IP or ATM Removes Legacy MSC



3G R4 IP or ATM True Converged IP Backbone



Design Consideration for Deploying IP/MPLS Core

Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

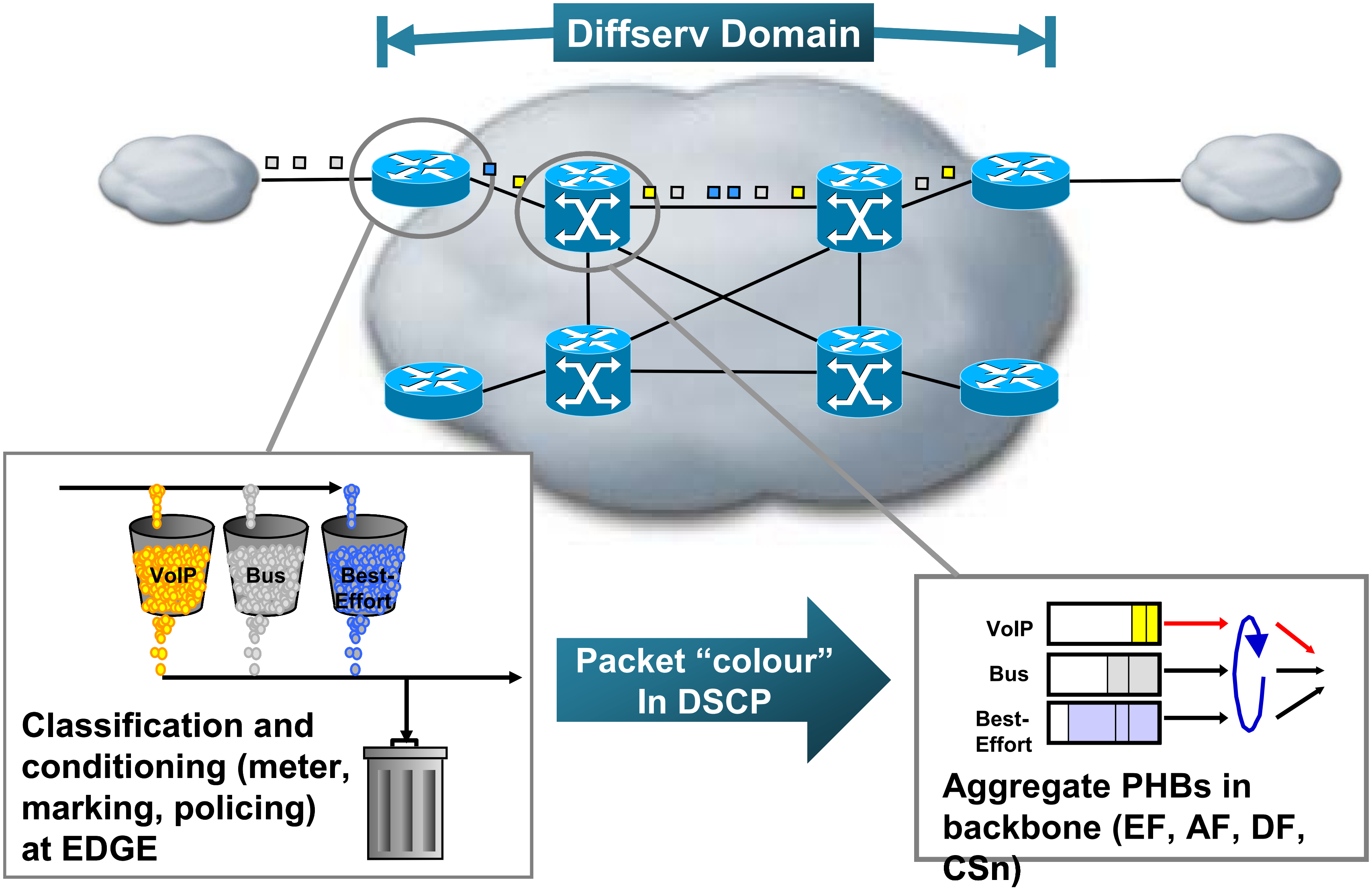
Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

Deploying Tight-SLA Services on an IP Backbone

- Number of tools are available to enabled tight SLA services
  - Physical network design and topology
  - Capacity planning and active monitoring
  - Diffserv: per-hop congestion management
  - Traffic engineering: avoid aggregation on shortest path
  - Convergence
    - FRR Protection
    - Tuning IGP Convergence

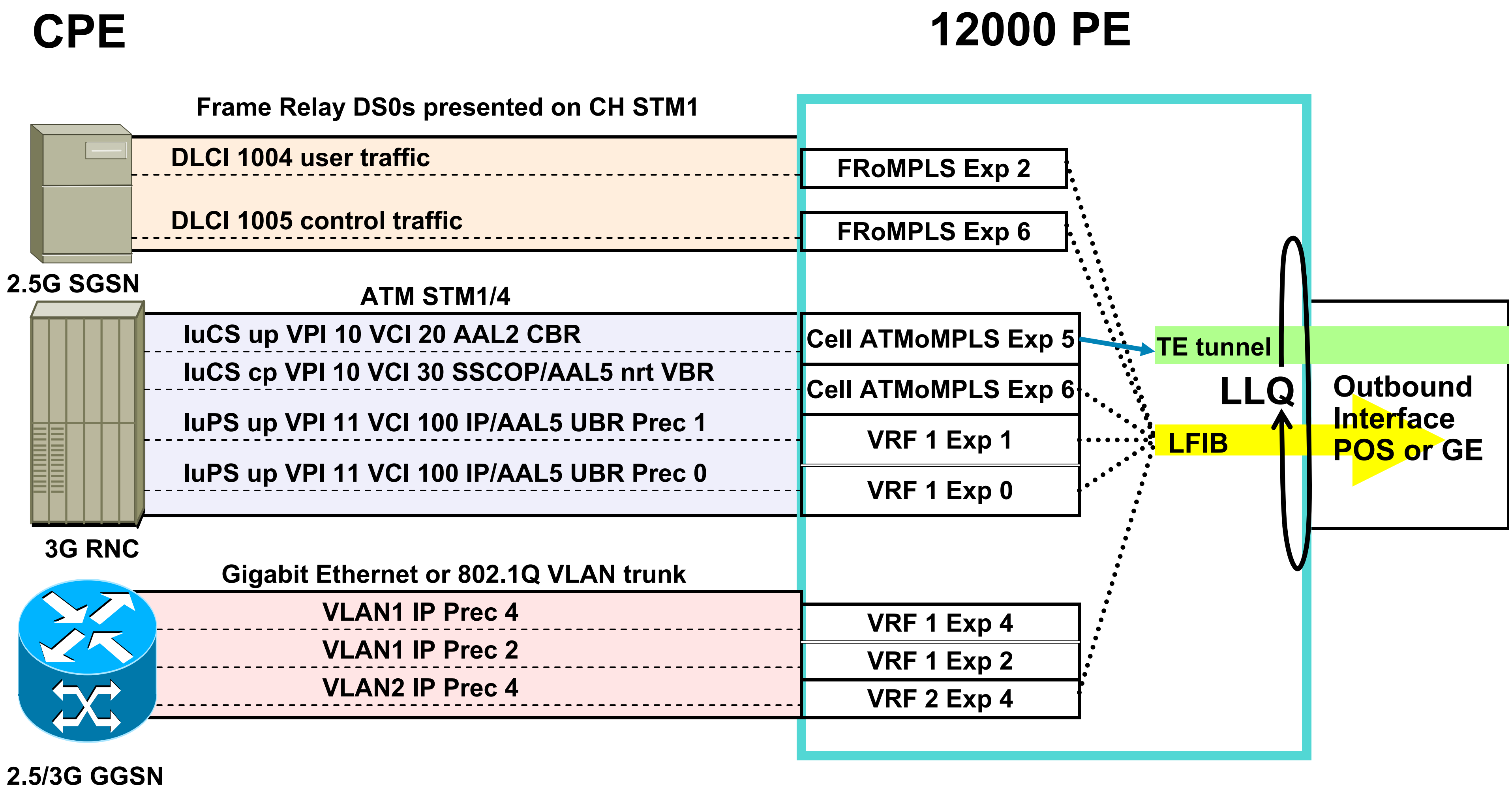
Solution Diffserv Architecture: RFC2475



Simple View of Deploying QoS

- Correctly mark all traffic entering the network
- Deploy a single queuing scheme based on proportional differentiation model on all links
- Capacity planning essential to ensuring adequate provisioning of bandwidth
- Strictly manage the volume of traffic in classes with a low drop tolerance

Marking at the Edge



QoS Mapping for 3G Data Roaming (From GSMA PRD IR.34)

3GPP QoS Information		Diffserv PHB	DSCP	QoS Requirement on GRX				Service Example
Traffic Class	THP			Max Delay	Max Jitter	Packet Loss	SDU Error Ratio	
Conversational	N/A	EF	101110	20ms	5ms	0.5%	10^{-6}	VoIP, Video Conferencing
Streaming	N/A	$AF4_1$	100010	40ms	5ms	0.5%	10^{-6}	Audio/Video Streaming
Interactive	1	$AF3_1$	011010	250ms	N/A	0.1%	10^{-8}	Transactional Services
	2	$AF2_1$	010010	300ms	N/A	0.1%	10^{-8}	Web Browsing
	3	$AF1_1$	001010	350ms	N/A	0.1%	10^{-8}	Telnet
Background	N/A	BE	000000	400ms	N/A	0.1%	10^{-8}	E-mail Download

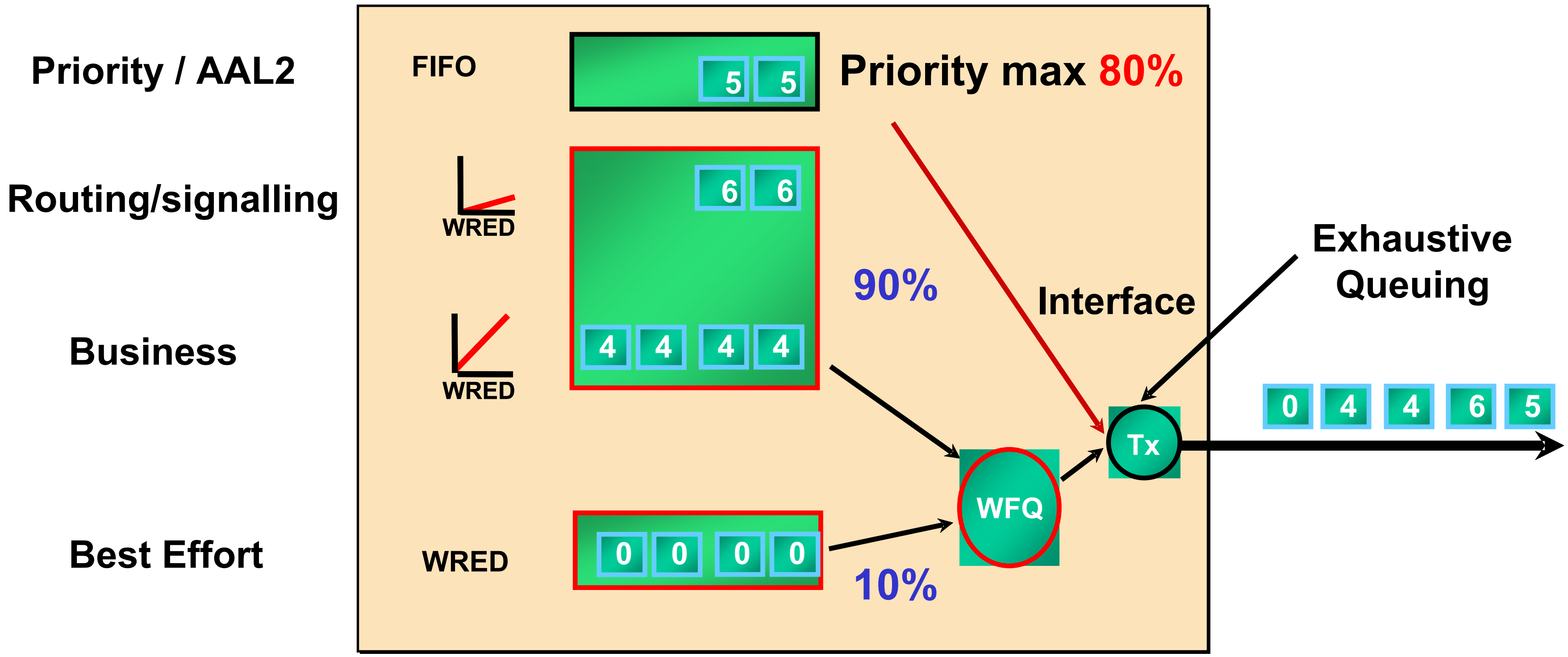
3GPP to Diffserv Marking the Edge

3GPP Class	Diffserv	DSCP	IP Prec	MPLS Exp
Routing/signalling	AF	48	6	6
Conversational AAL2 voice	EF	40	5	5
Streaming	AF	32	4	4
Interactive Gold	AF	24	3	3
Interactive Silver	AF	16	2	2
Interactive Bronze	AF	8	1	1
Best Effort	BE	0	0	0

3GPP to Diffserv and MPLS Exp Marking in the Core

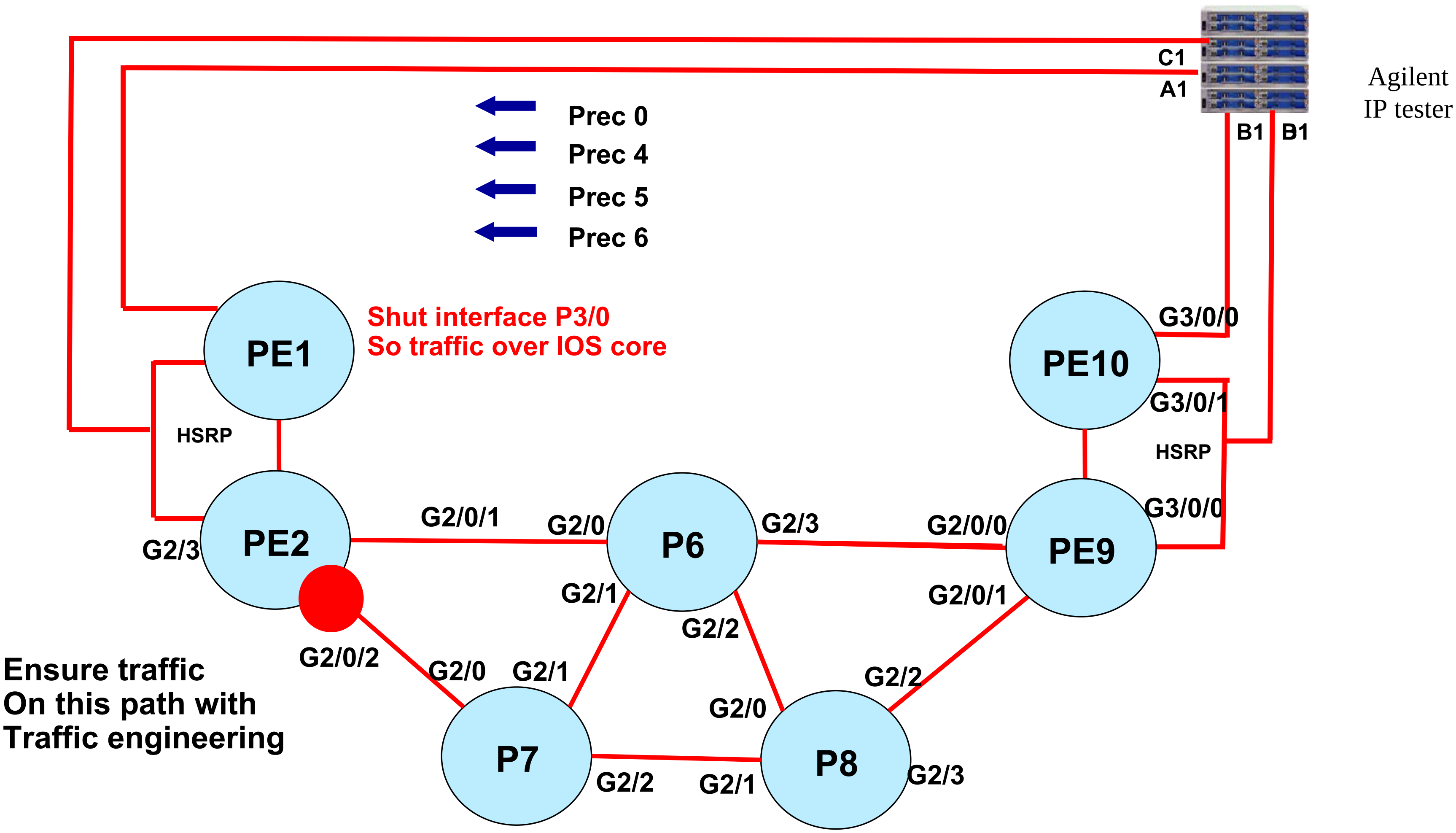
Class	Diffserv	DSCP	IP Prec	MPLS Exp
Routing/signaling	AF	48	6	6
Conversational IP/AAL2 voice	EF	40	5	5
Business	**AF**	**32**	**4**	**4**
Best Effort	Default	0	0	0

MQC Queuing Setup



% is of remaining bandwidth after priority queue

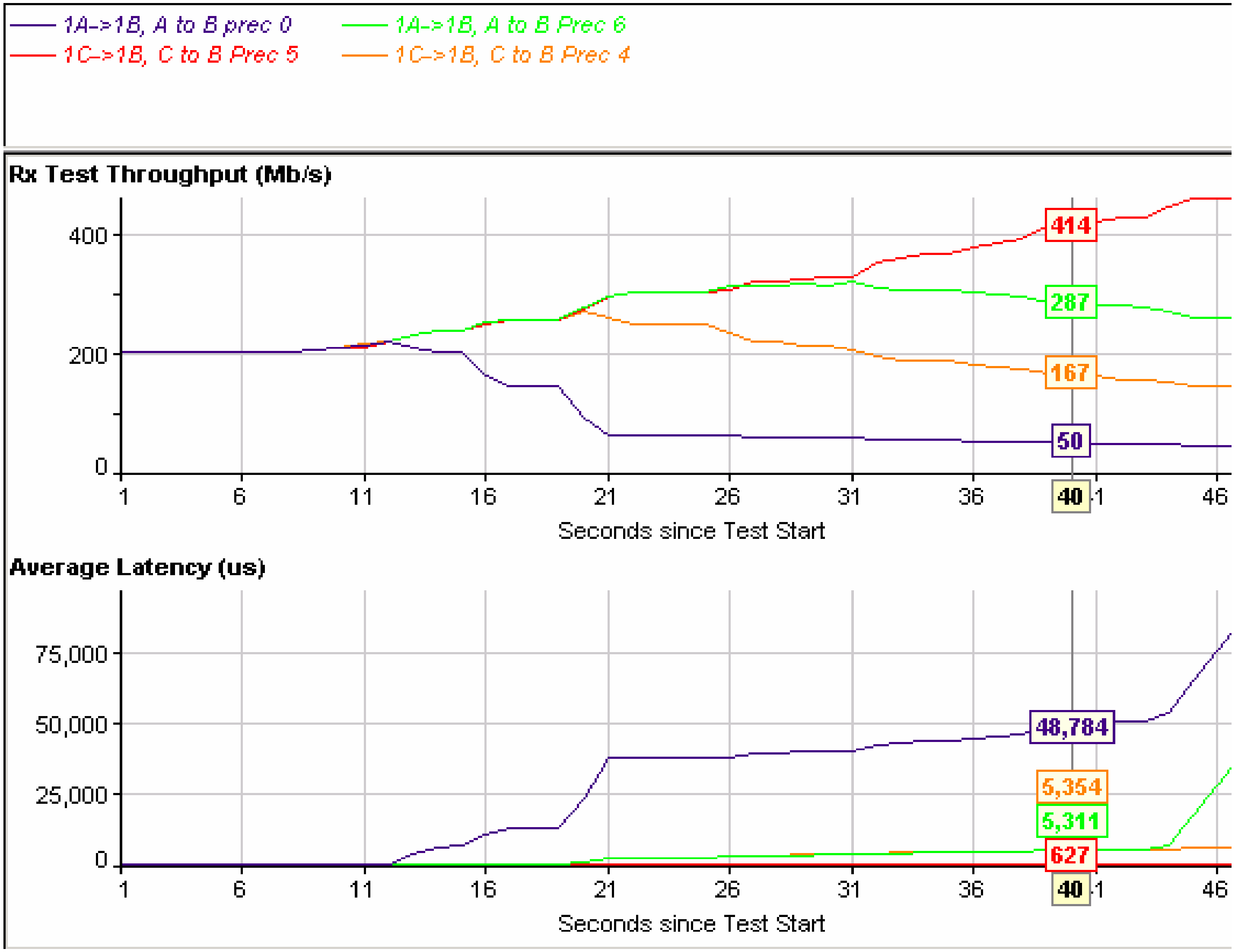
QoS on GE



C1
A1
Agilent IP tester
B1
B1
Prec 0
Prec 4
Prec 5
Prec 6
PE1
Shut interface P3/0
So traffic over IOS core
PE10
G3/0/0
G3/0/1
HSRP
HSRP
PE2
G2/3
G2/0/1
G2/0
P6
G2/3
G2/0/0
PE9
G3/0/0
G2/1
G2/2
G2/0/1
G2/0/2
G2/0
G2/1
G2/0
G2/2
P7
P8
G2/2
G2/1
G2/3
Ensure traffic
On this path with
Traffic engineering

Results

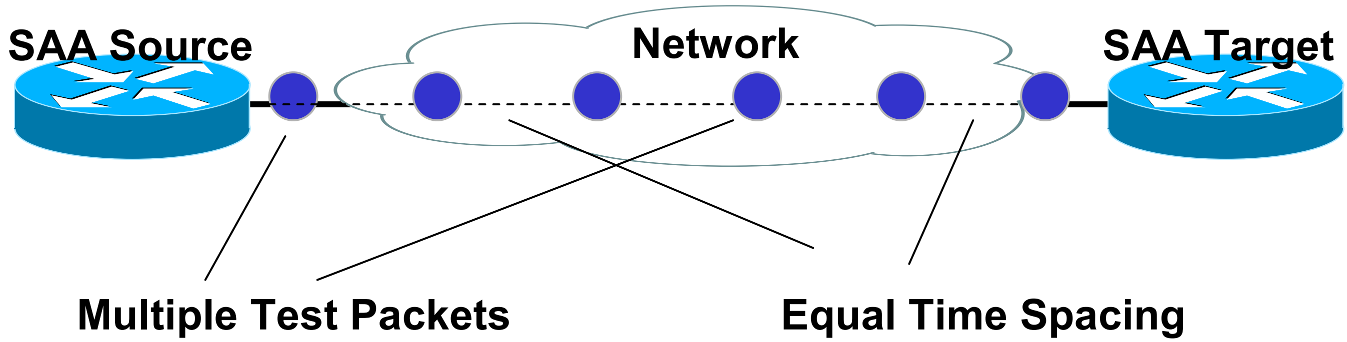
Steadily increase all Four flows until congestion Correctly drop lower Classes first and get low Latency for Prec 5 traffic



Measuring SLA Metrics

- Availability and performance
  - IP SLA probes
- Traffic type and volume
  - Netflow Traffic monitoring

Availability and Measurement
IP SLA (Was Service Assurance Agent)



- SAA actively sends user defined probes into the network
- Used to measure delay, jitter application responsiveness HTTP,DNS etc
- SAA is available in all IOS images at no additional cost

ISC SAA Report

SAA prob from PE2 to PE9

Summary Jitter Report for 10/9/05 - 10/15/05 - Microsoft Internet Explorer provide...

Summary Jitter Report for 10/9/05 - 10/15/05

Forward Packet Drops(#)	Avg Forward Jitter (ms)	Avg Positive Forward Jitter (ms)	Avg Negative Forward Jitter (ms)	Min Forward Jitter (ms)	Max Forward Jitter (ms)	Backward Packet Drops(#)	Avg Backward Jitter(ms)	Avg Positive Backward Jitter(ms)	Avg Negative Backward Jitter(ms)	Min Backward Jitter(ms)	Max Backward Jitter(ms)
0.00	1.05	1.04	1.06	1.00	4.00	0.00	1.02	1.02	1.02	1.00	5.00

Modify | Refresh | Print | Close

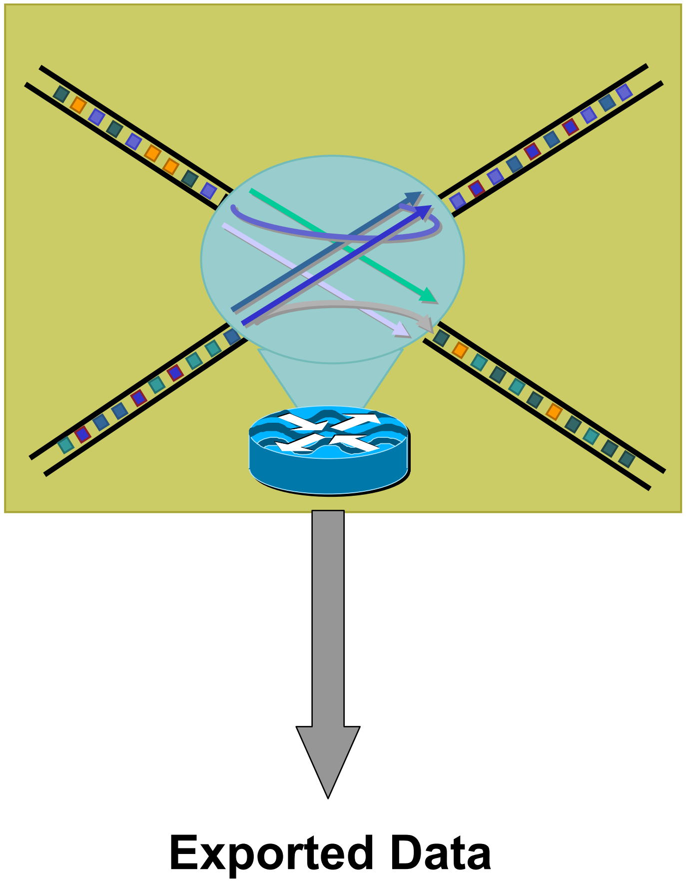
Generated at Fri Oct 14 16:50:47 BST 2005

Traffic Type and Volume
Netflow Traffic Monitor

Netflow can be enabled on IOS routers in order to monitor traffic flows

7 unique keys define a flow:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS byte (IP DSCP + ECN bits)
- Input logical interface (ifIndex)



Netflow v9 Example

- Sampled MPLS aware Netflow enabled on 12000 P router Engine 3 GE line card
- Sampling at 1 in 1000 packets
- Netflow looking at top 3 labels
- Attach to line card to see stats

    Attach 2

    show ip cach verbose flow (full stats)

    show ip cach flow (IP only)

Netflow Results

```
LC-Slot2#show ip cach verbose flow
IP packet size distribution (1652 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .169 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .830 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 35653632 bytes
  4 active, 524284 inactive, 386 added
  382 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 0 seconds
  last clearing of statistics never
```

Netflow Results Second Part

```
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other           54      0.0         1   300      0.0       0.3       0.0
Total:              54      0.0         1   300      0.0       0.3       0.0

SrcIf     SrcIPaddress    DstIf   DstIPaddress    Pr TOS Flgs  Pkts Port Msk AS Port Msk AS  NextHop  B/Pk  Active

Gi2/0        40.1.1.4       Gi2/2        40.1.4.2       06 A0  00      2      0000 /0  0       0000 /0  0     0.0.0.0       512     0.0

Pos:Lbl-Exp-S 1:40-5-0 (TE-MIDPT/0.0.0.0) 2:40-5-1

Gi2/0        40.1.1.4       Gi2/2        40.1.4.2       06 80  00      1      0000 /0  0       0000 /0  0     0.0.0.0       512     0.0

Pos:Lbl-Exp-S 1:40-4-0 (TE-MIDPT/0.0.0.0) 2:40-4-1

Gi2/0        40.1.3.2       Gi2/2        40.1.4.2       06 00  00      4       0000 /0  0      0000 /0  0     0.0.0.0       512     0.5

Pos:Lbl-Exp-S 1:38-0-0 (TE-MIDPT/0.0.0.0) 2:40-0-1o
```

Netflow Report Example

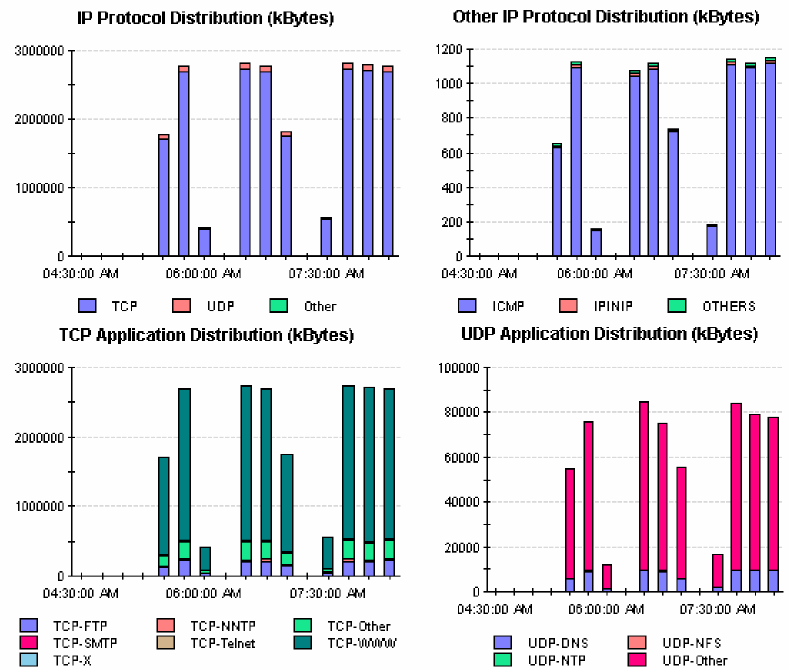
Router - Top 10 Talker and Protocol Distribution

InfoVista
NetFlow Collector - Cisco

Generated: 21 October 2002 - 08:15:00 AM
Periodicity: Every 15 minutes
Report for: 192.168.210.205

Top 10 Talker

TID	Source Address	Destination Address	kBytes
9	216.100.71.3	193.48.189.74	26198.6
8	209.185.180.232	132.227.72.137	26021
7	209.132.66.208	130.66.104.62	60902.2
6	209.104.88.187	192.54.193.137	37204.9
5	207.77.58.226	195.83.155.55	26961.8
4	207.211.168.93	194.199.131.114	31439.5
3	206.204.7.43	194.199.64.108	54808.2



- Cisco NetFlow Performance Reporting
- Protocol Distribution and Top Talkers
- AS Distribution and Top Talkers
- Performance Detail Drilldown

Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

Define Requirements for Each Service

- What is the service availability requirement
  - Often quoted 5-9's target equal to 5 minutes down time
  - Is end application resilient
- What is the convergence requirement in event of failure
  - For IP user data an outage of 3 seconds may be acceptable
  - For signalling an outage of 60 seconds may be acceptable if using diverse paths (SCTP will recover) or 800ms unprotected
  - For user voice an outage of less than 300-500ms may be required
  - If targeting SDH/SONET protection may require sub 50ms for all services

Platform Availability

12406 theoretical MTBF based availability

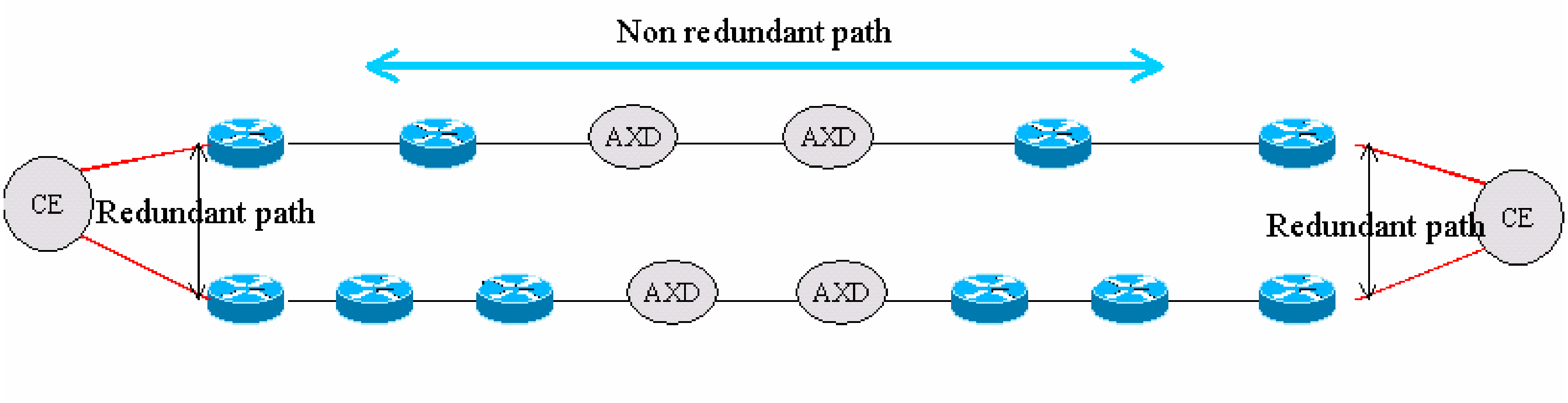
- availability non redundant 99.985 % or 79 minutes
- availability with redundant power 99.993% or 37 minutes
- availability with redundant power and GRP 99.996% or 21 minutes

Transmission availability

Typical figure offered by a service provider 99.94% or 5 ¼ hrs

This is a predicted MTBF (Mean Time Between Failures) that is based on the Telcordia (formerly Bellcore) "Parts Count Method".

Network Availability



- Based on worst path with all 12406 routers
  - Network availability 99.99980%
  - Or 1 minute downtime per year

Network Restoration

Summarizing the restoration operation, the total restoration delay can be computed as follows:

- Failure Detection Delay **(SDH and/or LoS and/or BFD)** +
- Failure Propagation Delay **(IGP and/or BGP)** +
- Update Network View **(IGP and/or LDP and/or BGP)** +
- Update Forwarding Plane == Service Restoration Time

- To optimize network convergence and service restoration, one or several steps must be minimized or avoided
- Control Plane optimizations, Platform optimizations and design all contribute

Improving the restoration process

Function	Restoration Component	Platform Specific
Loss-of-Signal Detection	**Failure Detection Delay**	**No**
BFD	**Failure Detection Delay**	**Centralized vs. Distributed**
Fast IGP	**Failure Detection Delay** **Failure Propagation Delay** **Update Network View**	**No (Fast hellos)** **No** **No**
Fast BGP	**Failure Propagation Delay** **Update Network View**	**No** **BGP Prefix Independence**
BGP Prefix Independence	**Update Forwarding Plane**	**12000 Series and CRS-1 Series**
BGP Convergence avoidance	**Update Network View** **Update Forwarding Plane**	**No** **BGP Prefix Independence**
TE Fast Reroute	**LOS triggered** **Failure Propagation Delay** **Update Network View** **Update Forwarding Plane**	**Yes** **No** **No** **FRR Prefix Independence**
FRR Prefix Independence	**Update Forwarding Plane**	**12000 Series and CRS-1 Series**

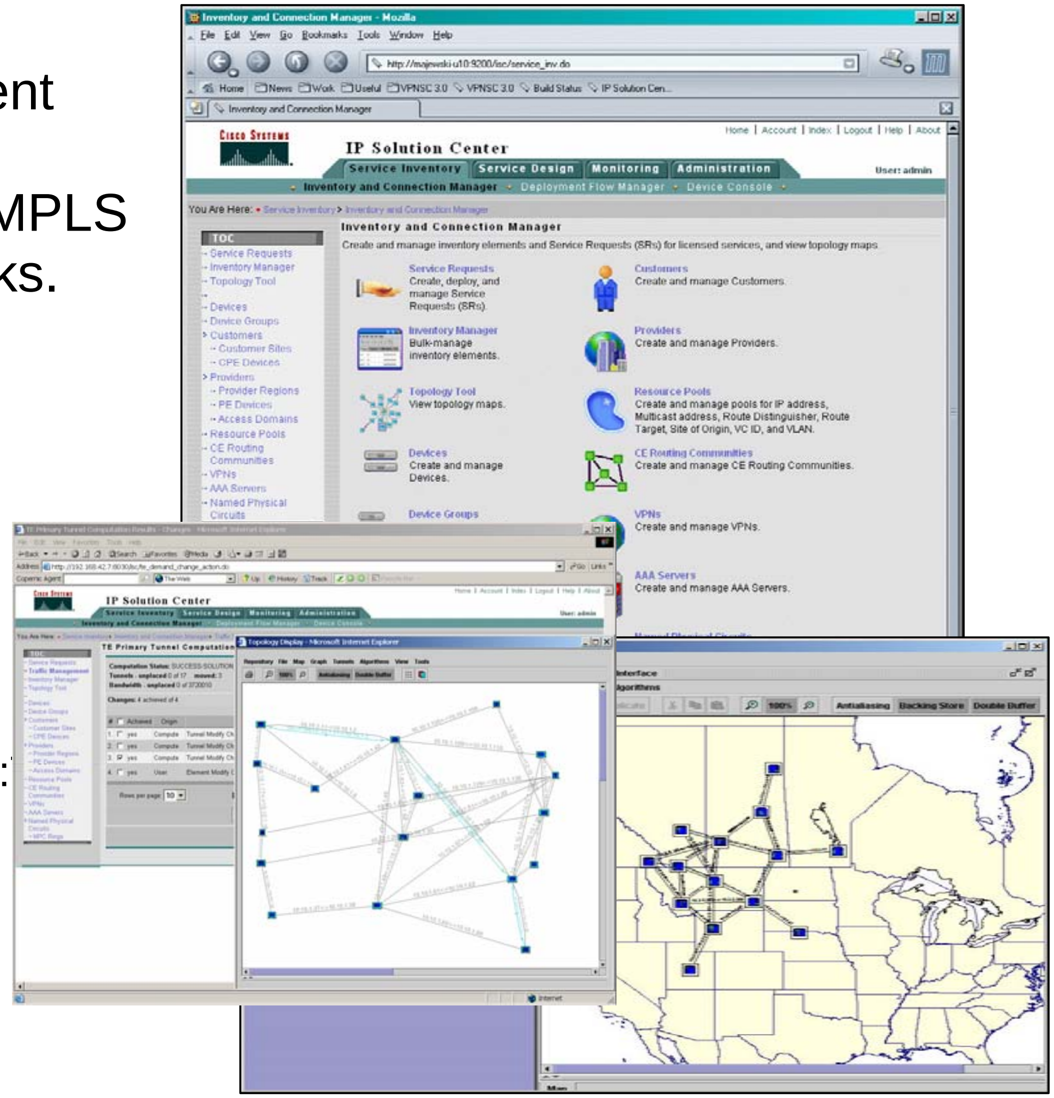
Good Operation and Maintenance Increases Uptime → IP Solution Center

- A family of network-intelligent element management applications for managing MPLS and Metro Ethernet networks.

  MPLS Virtual Private Network Management Application (ISC:MPLS)

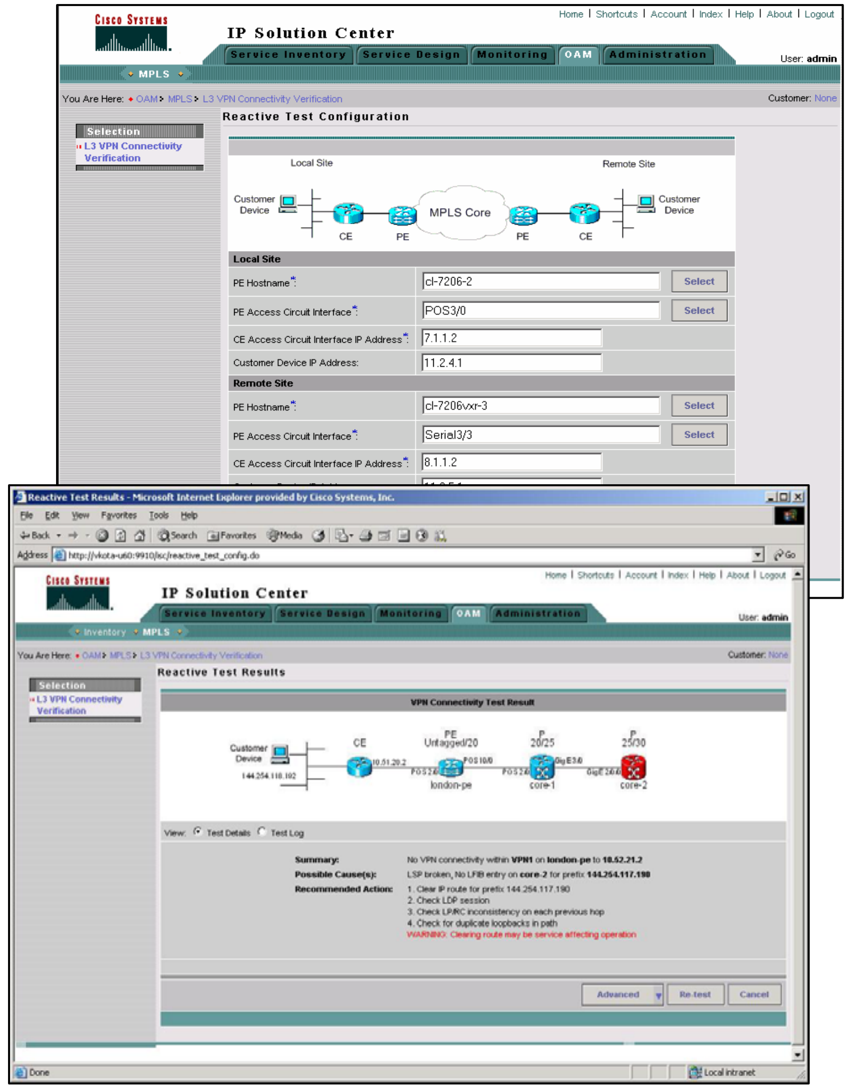
  Layer 2 Virtual Private Network and Metro Ethernet Application (ISC:L2VPN, ISC:METRO)

  Traffic Engineering Management Application (ISC:

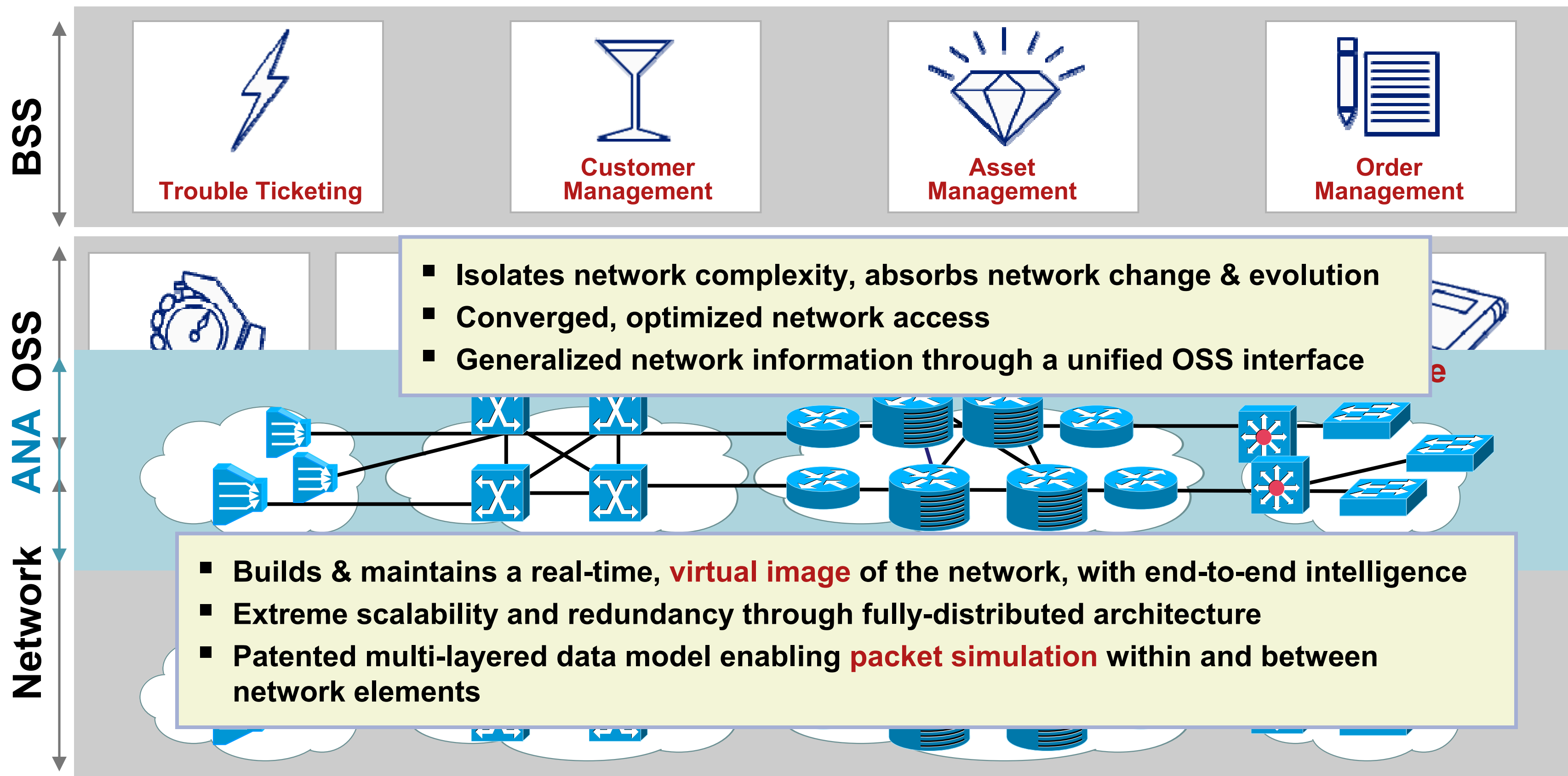


Cisco MPLS Diagnostics Expert Product Overview

- Automated Troubleshooting and Diagnosis of MPLS VPN problems—
80/20 Rule approach
- Diagnoses problems in MPLS VPN core, edge and access… and can isolate problems to the end customer network also!
- Reduces MPLS outages from hours to minutes using MPLS VPN Failure Knowledge Base developed by NMTG—with TAC & ITD support
- Unique Cisco capability, complementary to existing, traditional fault OSSs
- Dec 05—GA Release—ISC framework
- Deployable in customers who don't use ISC as well as those who do
- Mar 06—(Limited) Early Access Release on Sheer acquisition—NMTG Convergence platform



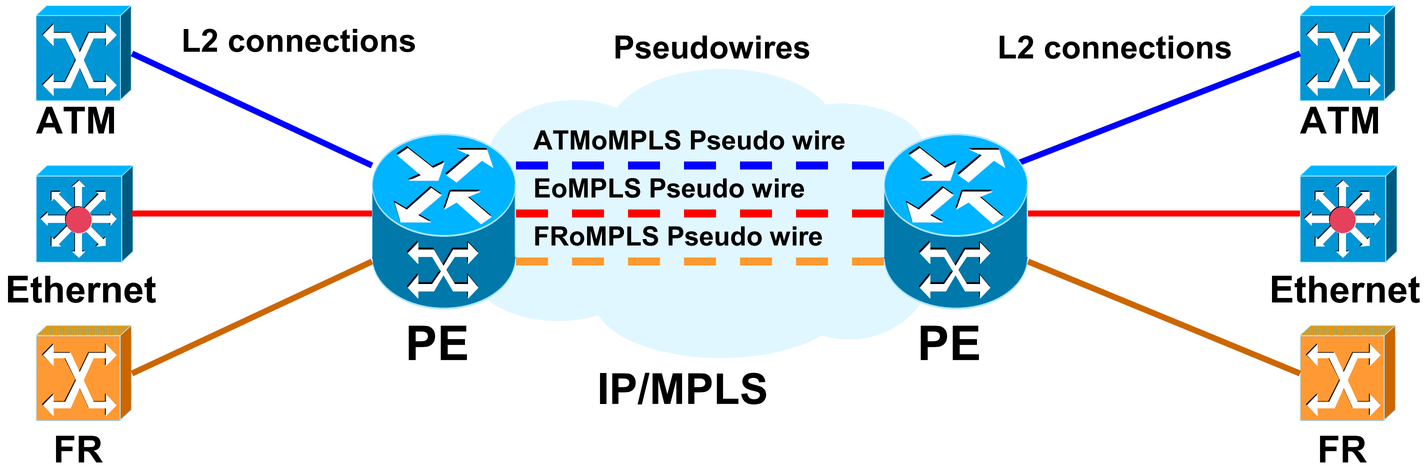
SP NMS Converged Architecture – ANA



Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

Pseudo Wire



- Any Transport over MPLS (AToM) Supports

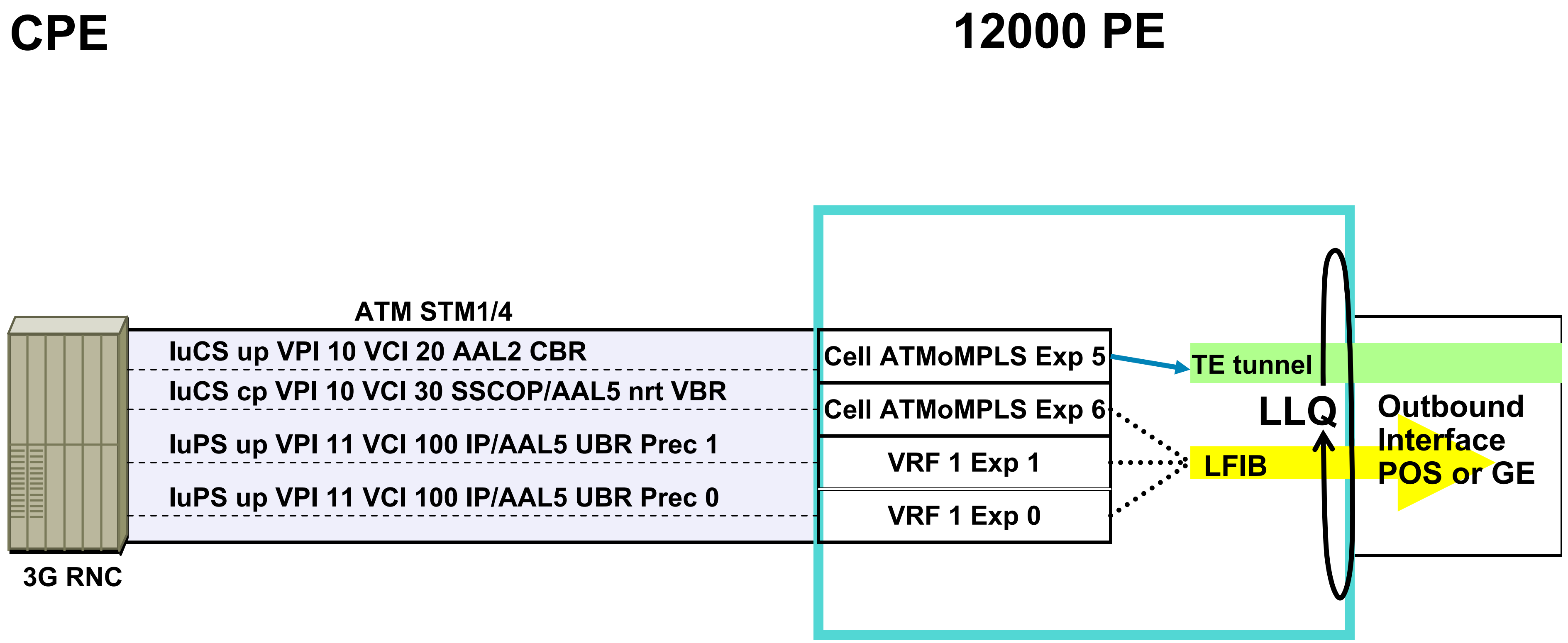
  Ethernet (port, VLAN), ATM VC/VP, FR DLCI, PPP, HDLC

- Directed LDP used for VC-Label Negotiation, withdrawal and Error Notification
- Martini encapsulation for PDU transport
- Integrates with Diffserv QoS, TE and FRR

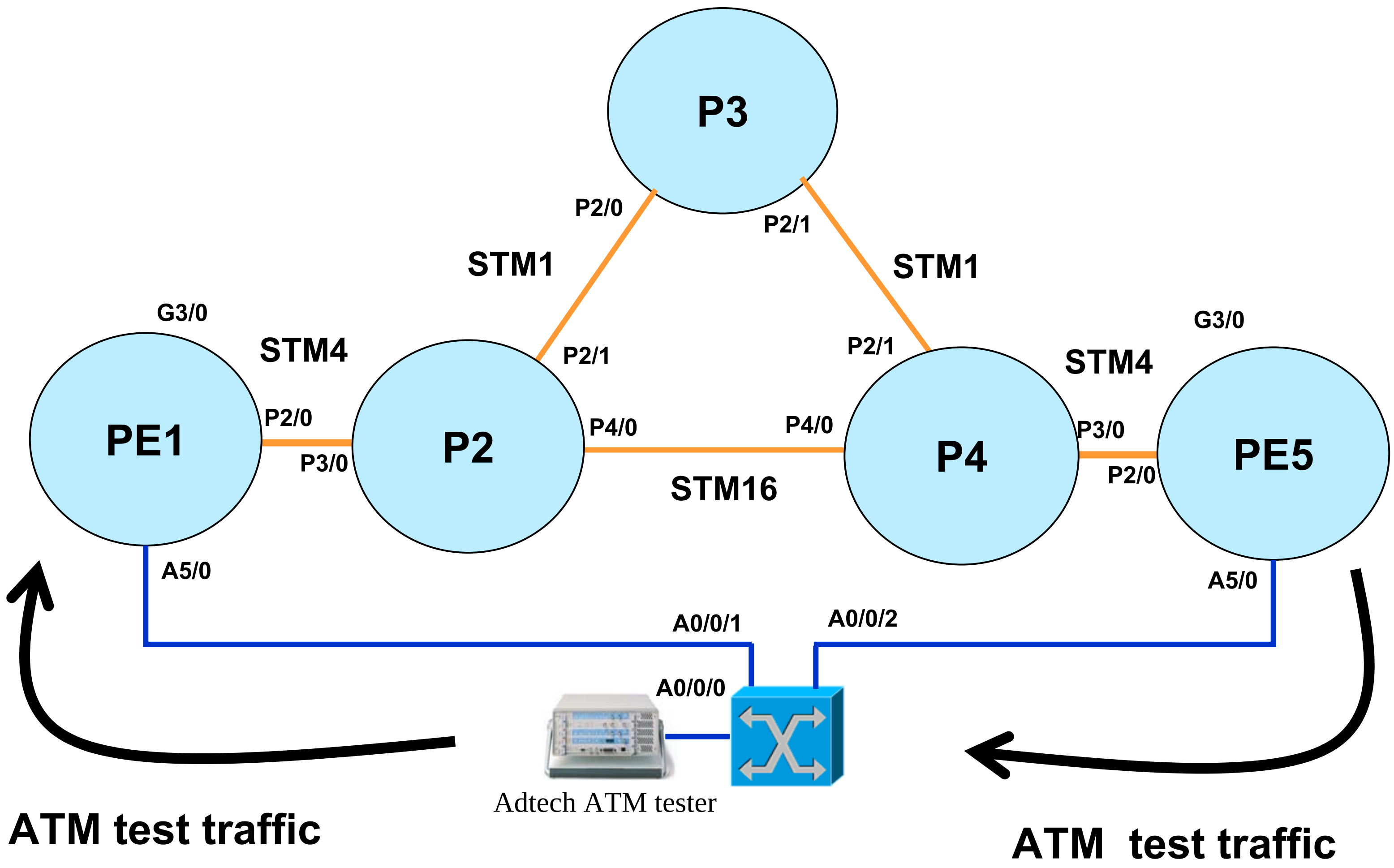
ATM Pseudowire Allow Migration to IP Core

- ATM pseudowires provide ATM services over an IP/MPLS backbone
- Supports AAL5, AAL2, AAL1 for CBR, UBR and VBR traffic types
- Supports 3G Iur, Iu-cs and Iu-ps control and user plane
- Allows operator to cap investment in legacy ATM equipment and deploy IP/MPLS in RAN today
- Lays the foundation for migration to R5 IP RAN core

Marking at the Edge



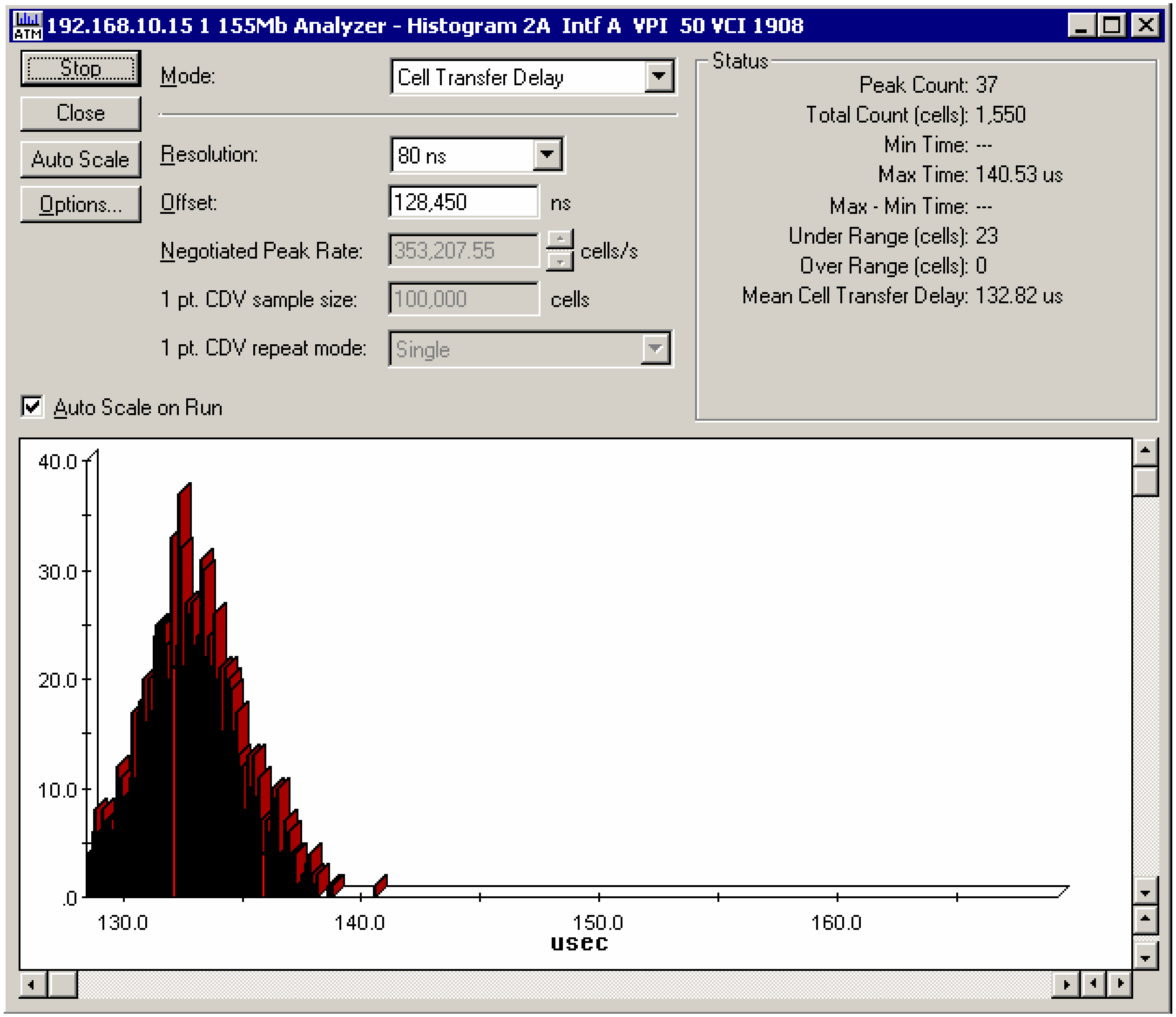
Example Test Network



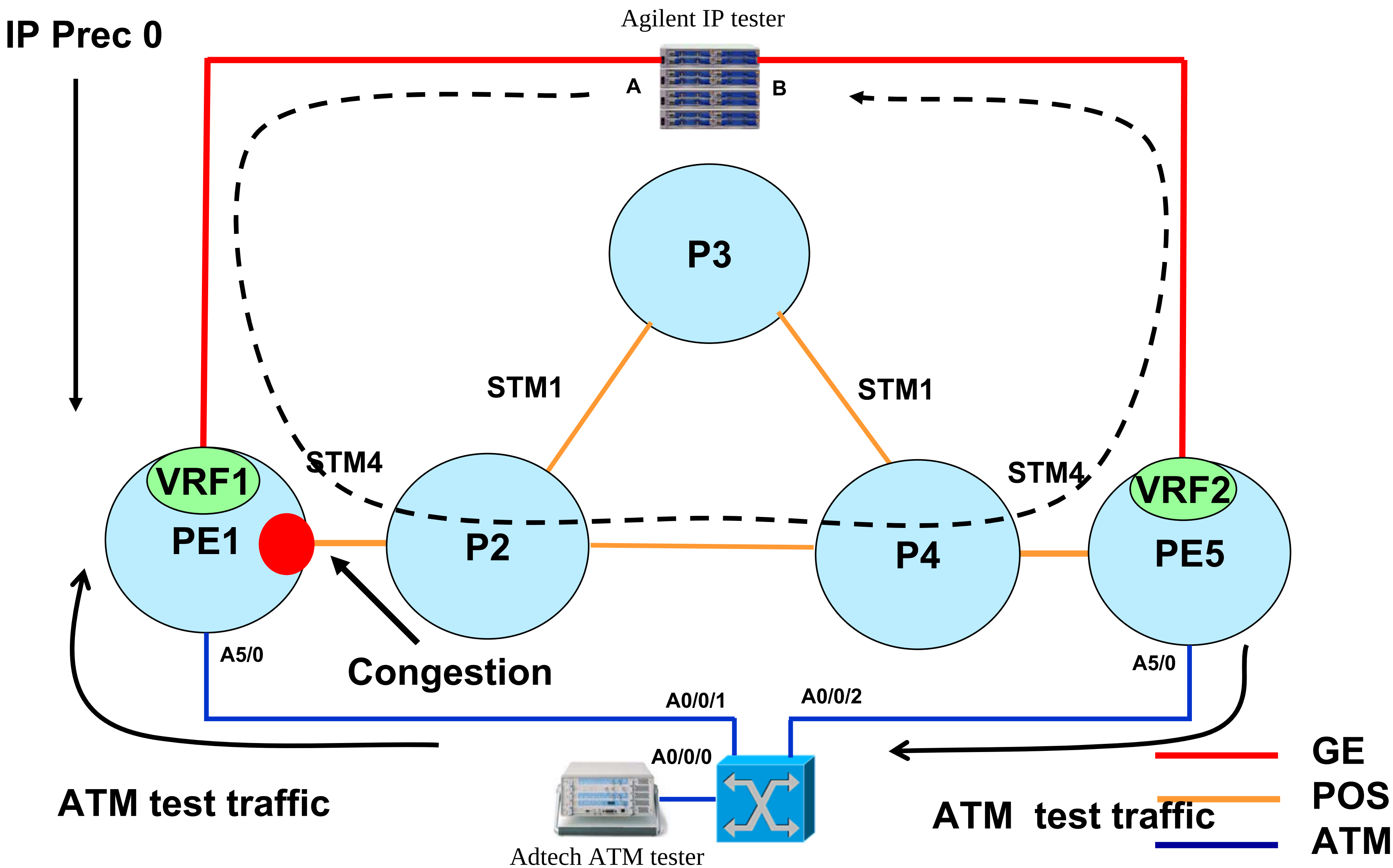
VCCV Test Results

```
PE2#show mpls l2transport summary

Destination address: 1.1.1.1, total number of vc: 1
  0 unknown, 1 up, 0 down, 0 admin down, 0 recovering
  1 active vc on MPLS interface Gi2/0
Destination address: 9.9.9.9, total number of vc: 2
  0 unknown, 2 up, 0 down, 0 admin down, 0 recovering
  1 active vc on MPLS interface Tu2
  1 active vc on MPLS interface Tu1

PE2#show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
AT4/0          ATM VCC CELL 50/1002       1.1.1.1         1002       UP
AT4/0          ATM VCC CELL 40/1000       9.9.9.9         1000       UP
AT4/0          ATM VCC CELL 40/1001       9.9.9.9         1001       UP

PE2#ping mpls pseudowire 9.9.9.9 1000
Sending 5, 100-byte MPLS Echos to 9.9.9.9/0,
     timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not transmitted,
      '.' - timeout, 'U' - unreachable,
      'R' - downstream router but not target,
      'M' - malformed request

Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

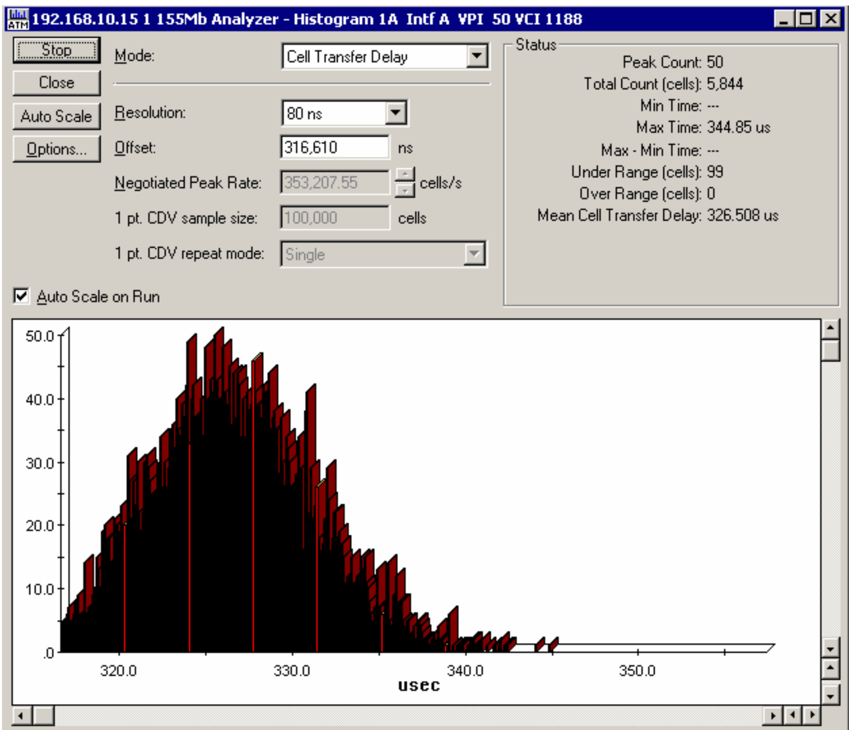
CBR Traffic Cell Transfer Delay



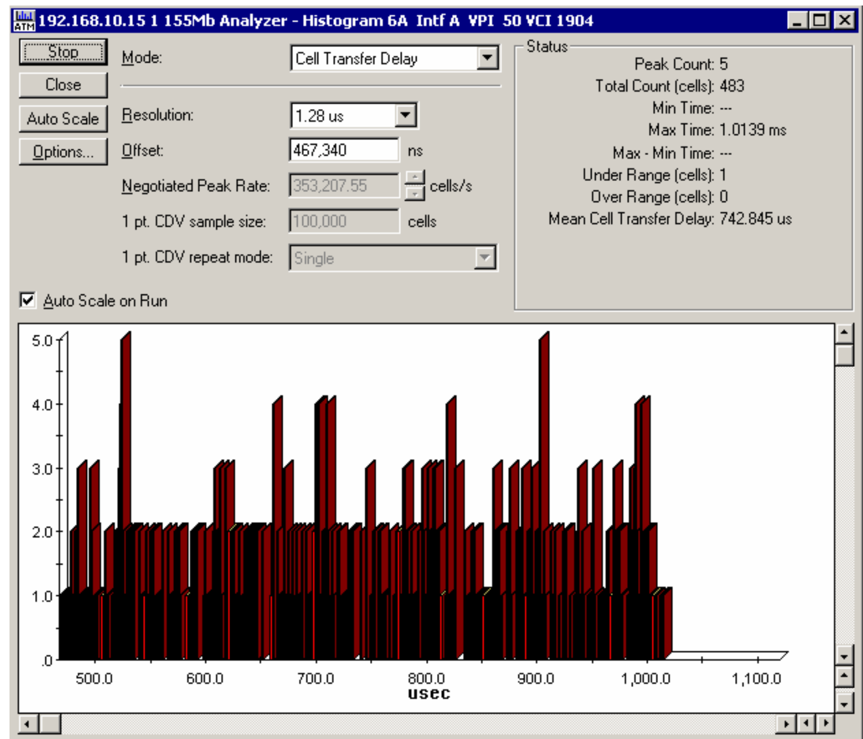
AToM Performance Under Congestion



Traffic Differentiation



CBR MPLS Exp 5



Nrt-VBR MPLS Exp 4

Deployment Considerations for ATM Enabled MGW Over and MPLS Backbone

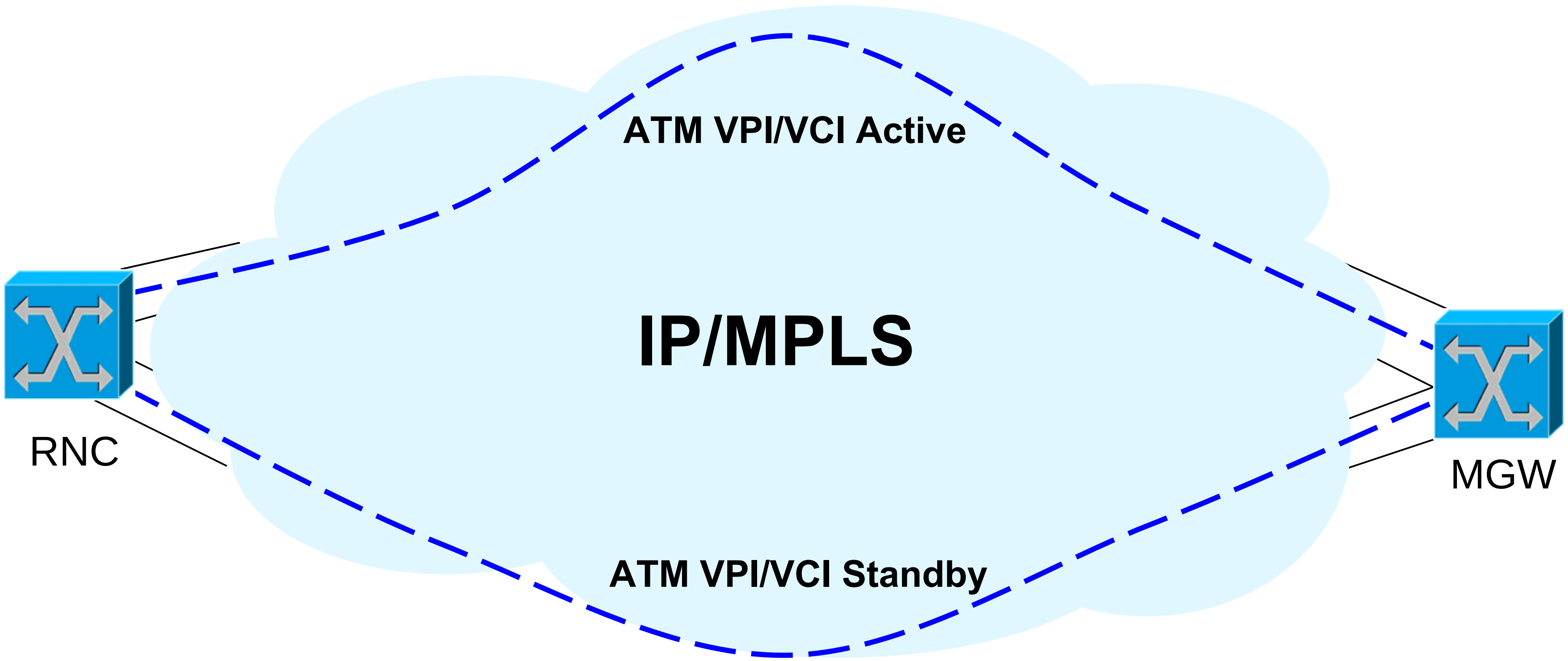
- Resilience
- Optimization

Deployment Considerations for ATM Enabled MGW Over and MPLS Backbone

- Resilience
- Optimization

R4 with ATM Enabled MGW

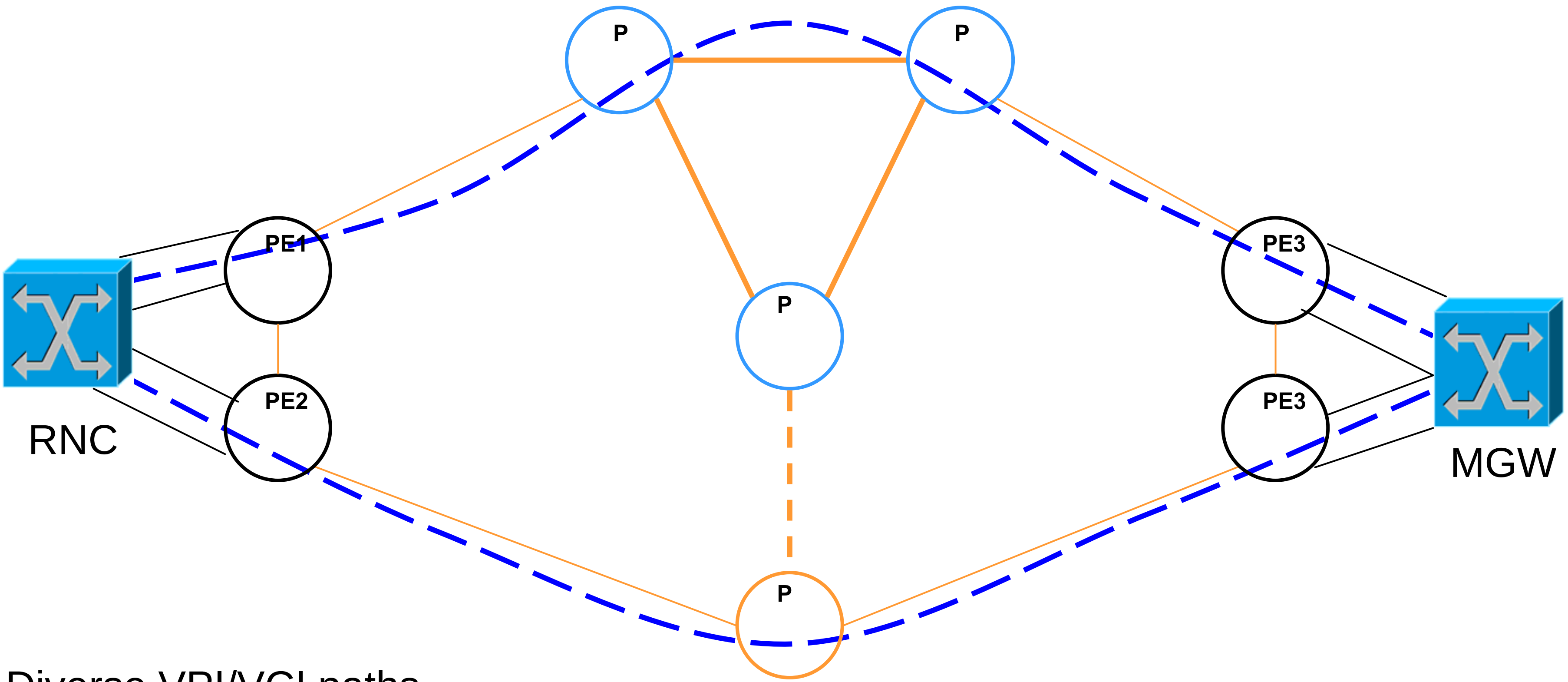
ATM service carries voice as AAL2 and data as AAL5



Diverse VPI/VCI paths
AToM single cell relay
Convergence requirement 500ms for link and node failure

Example ATMoMPLS Deployment

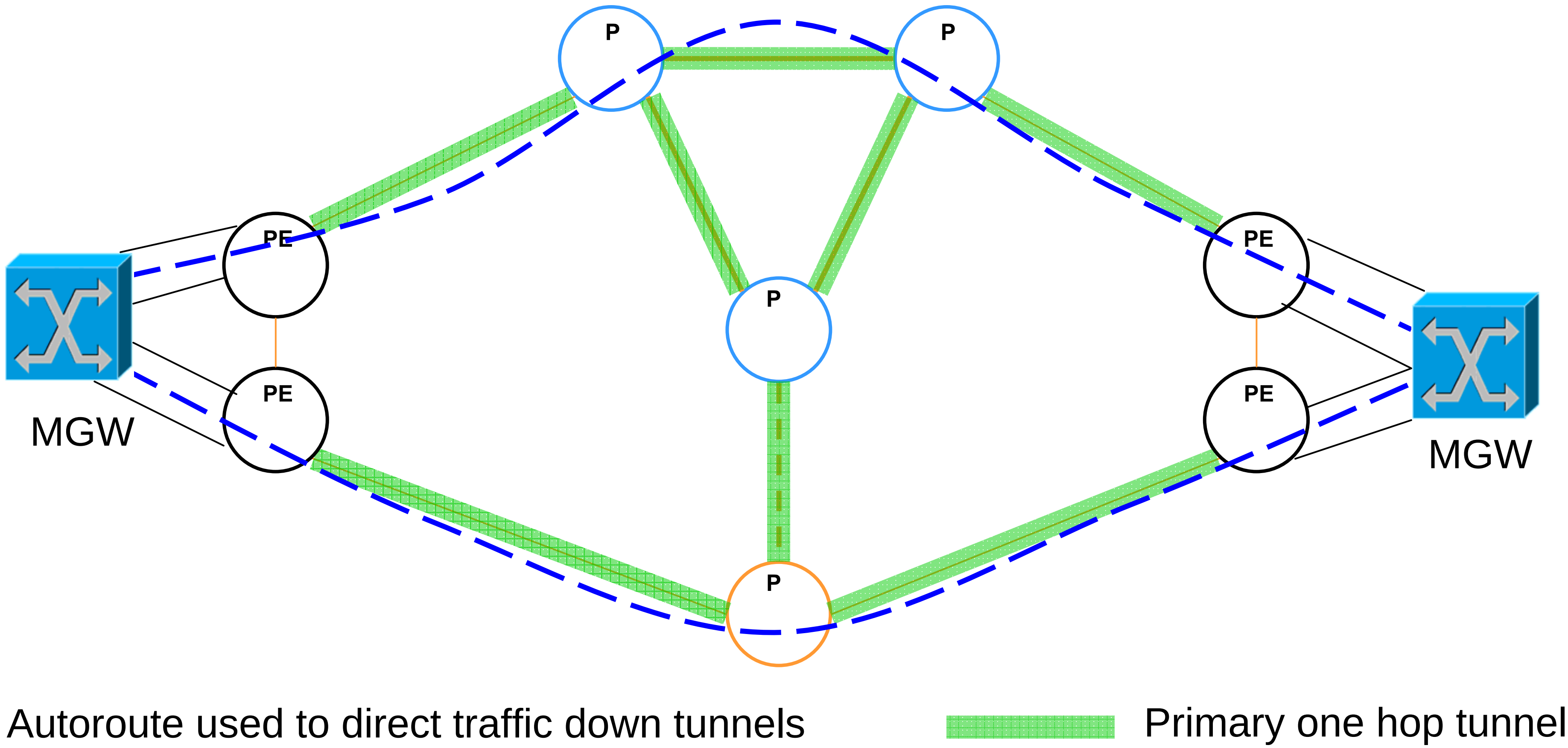
ATM service carries voice as AAL2 and data as AAL5



Diverse VPI/VCI paths
AToM single cell relay
Convergence requirement 500ms for link and node failure

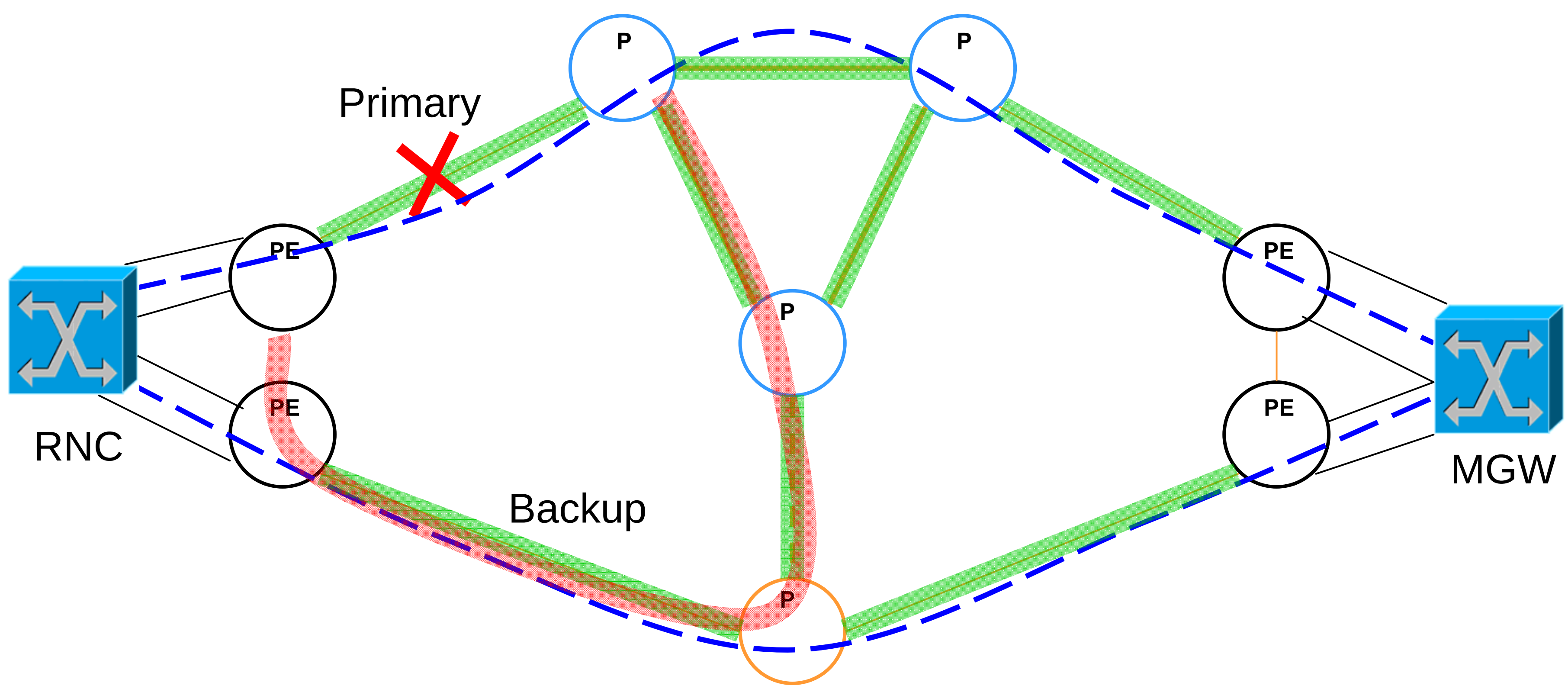
One Hop Primary Tunnels Link Protection

One hop tunnels reduces total number of tunnels



Autoroute used to direct traffic down tunnels
All tunnels are static

FRR Link Protection of All Links Sub 50ms Restoration



Link Failure Detection

- POS

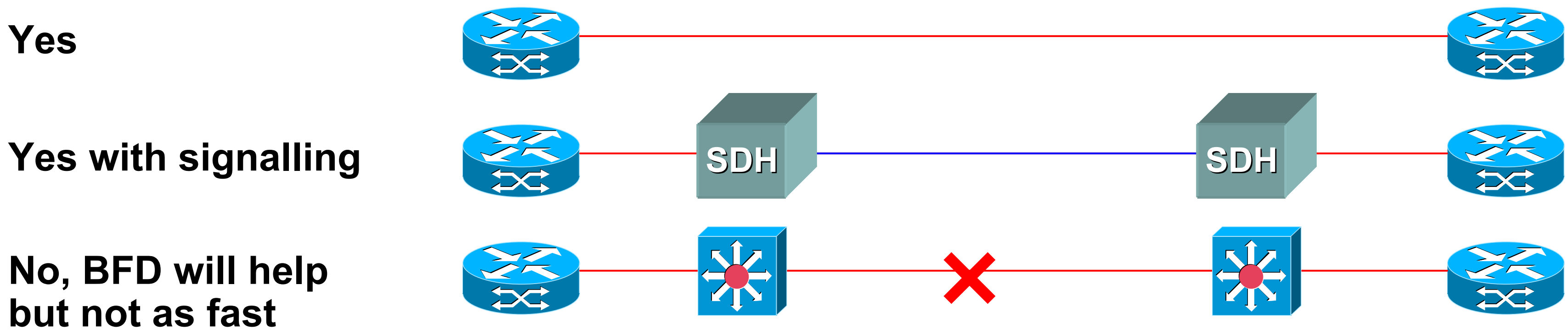
  AIS alarm is used to trigger FRR protection, detected within a few ms

  SDH/SONET has end to end signalling

- GE

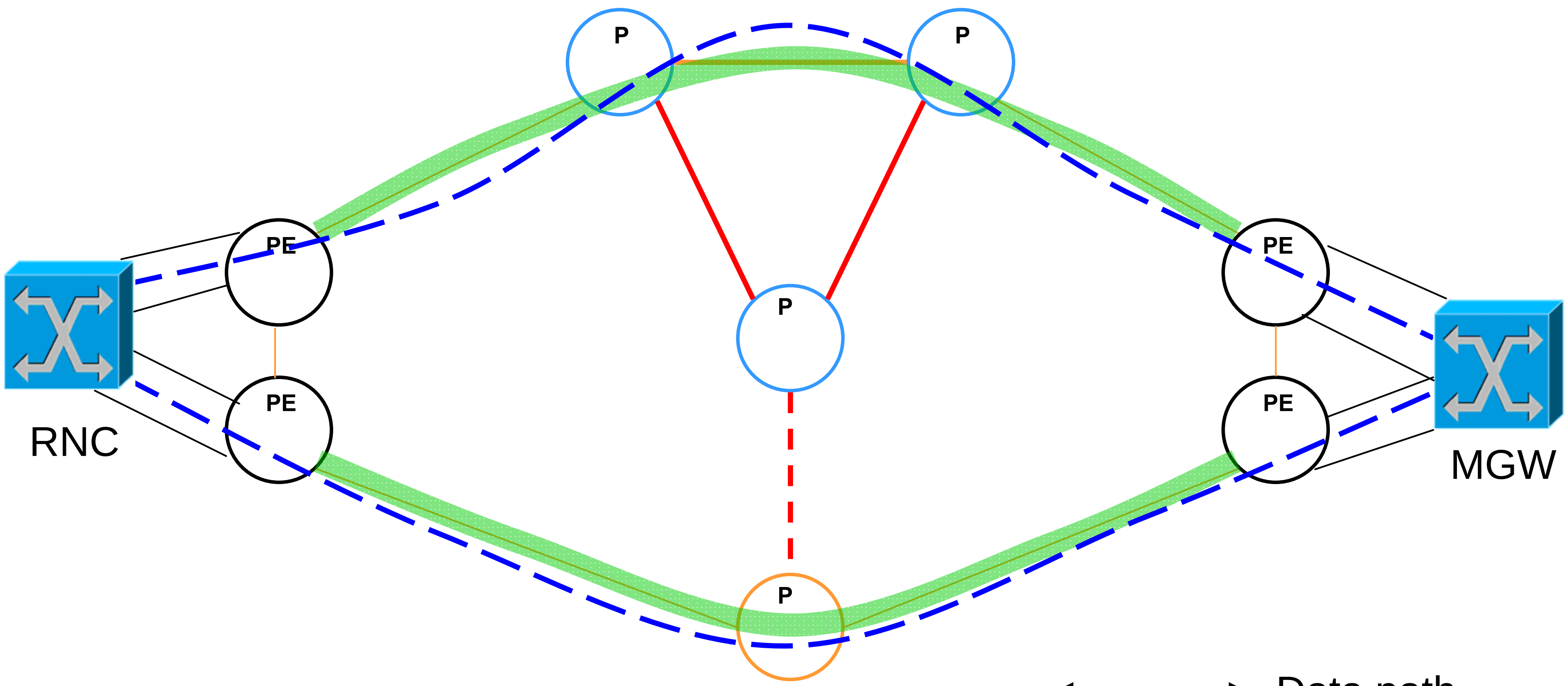
  LOS based GE triggers FRR when GE interface goes down

  Can be as fast as POS but should only be deployed over dark fibre or optical network with end to end signalling

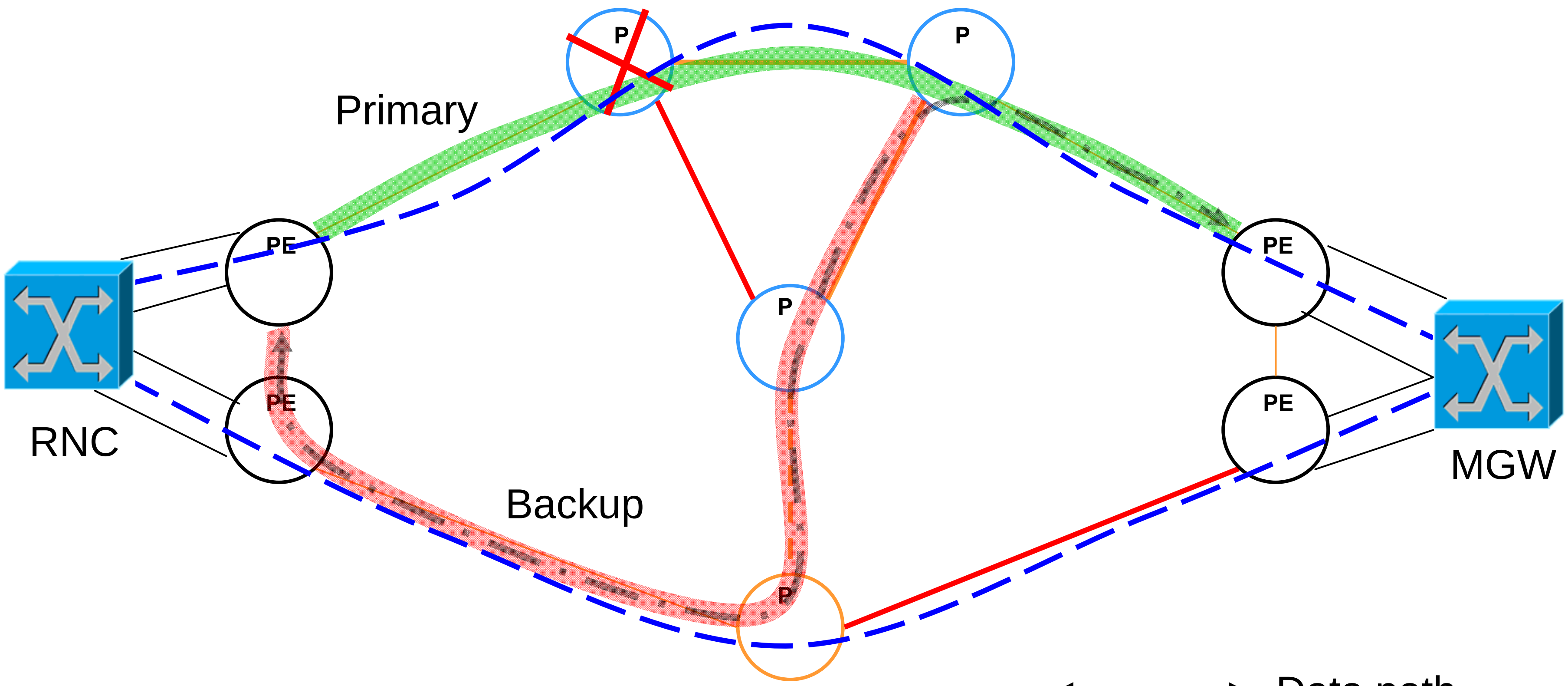


Traffic Directed Down Full Mesh of End to End Tunnels

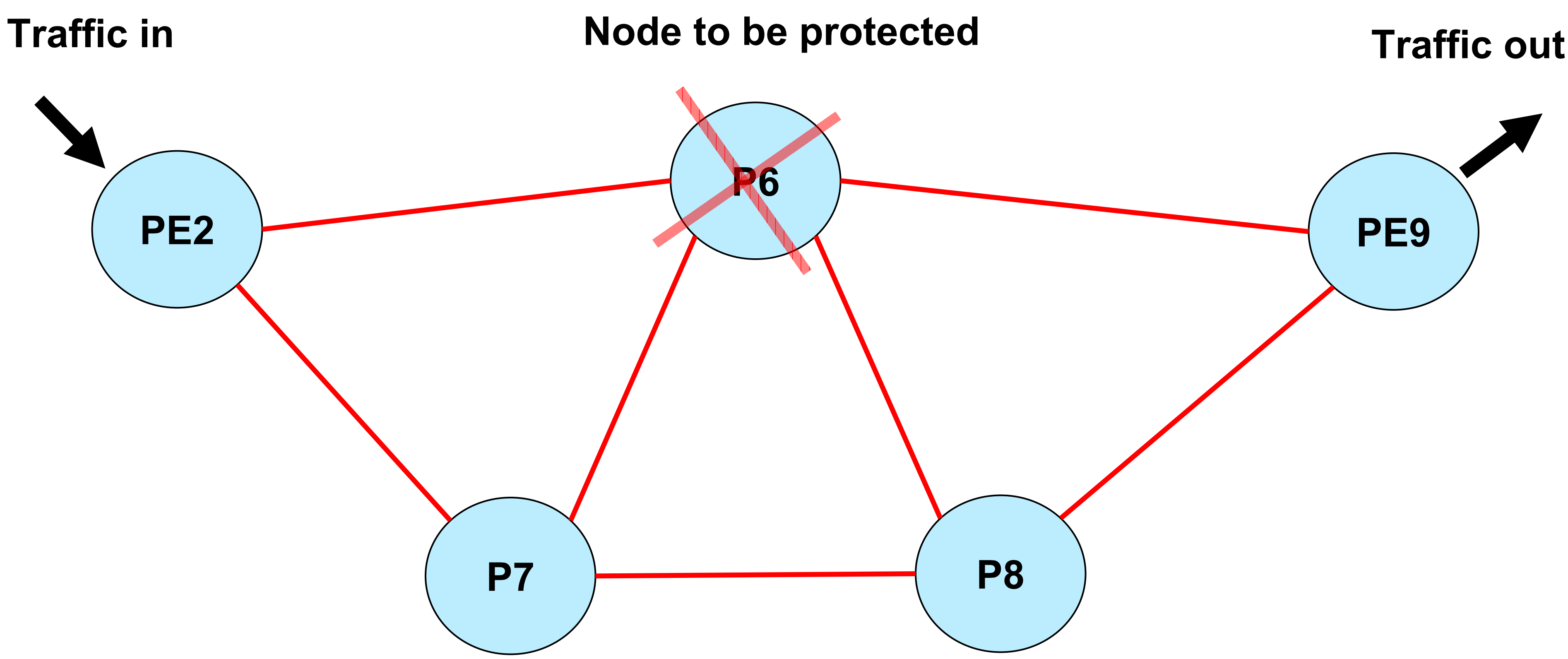
Full mesh of tunnels needs to managed carefully



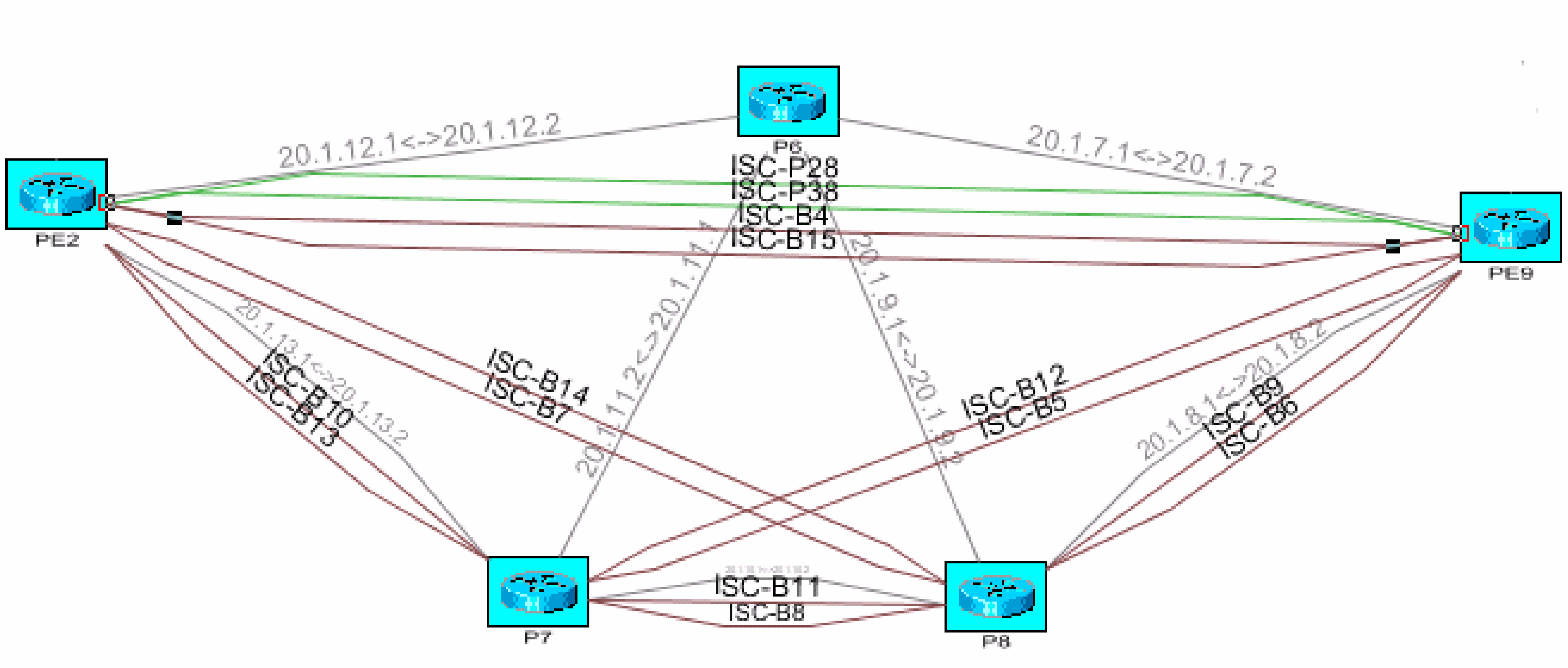
Node Protection for P Node Failure Sub 50ms Restoration



Deploying FRR Node Protection for Router P6

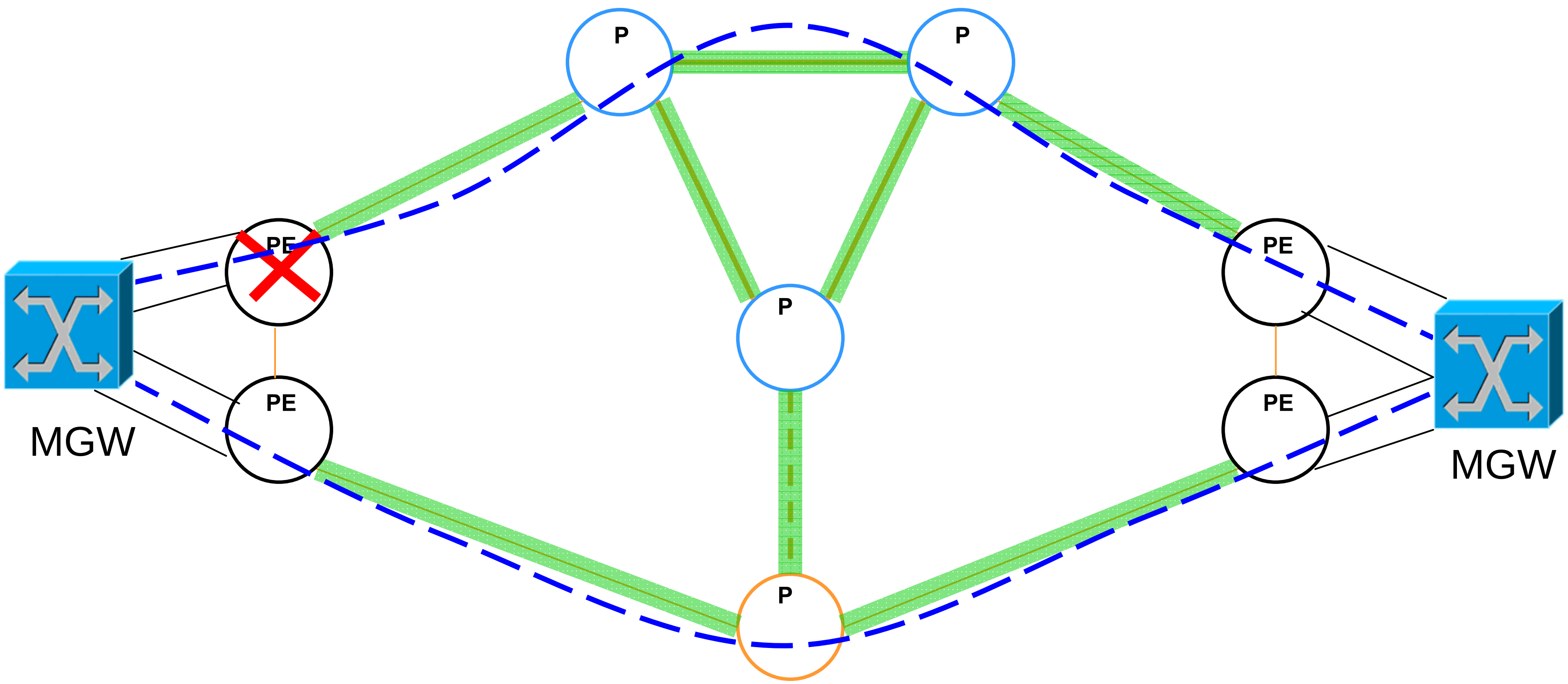


ISC-TM Discover Network and Plans All Tunnels



Failures Not Protected by FRR

Can build HA into platform but will not achieve platform availability of 5 9's



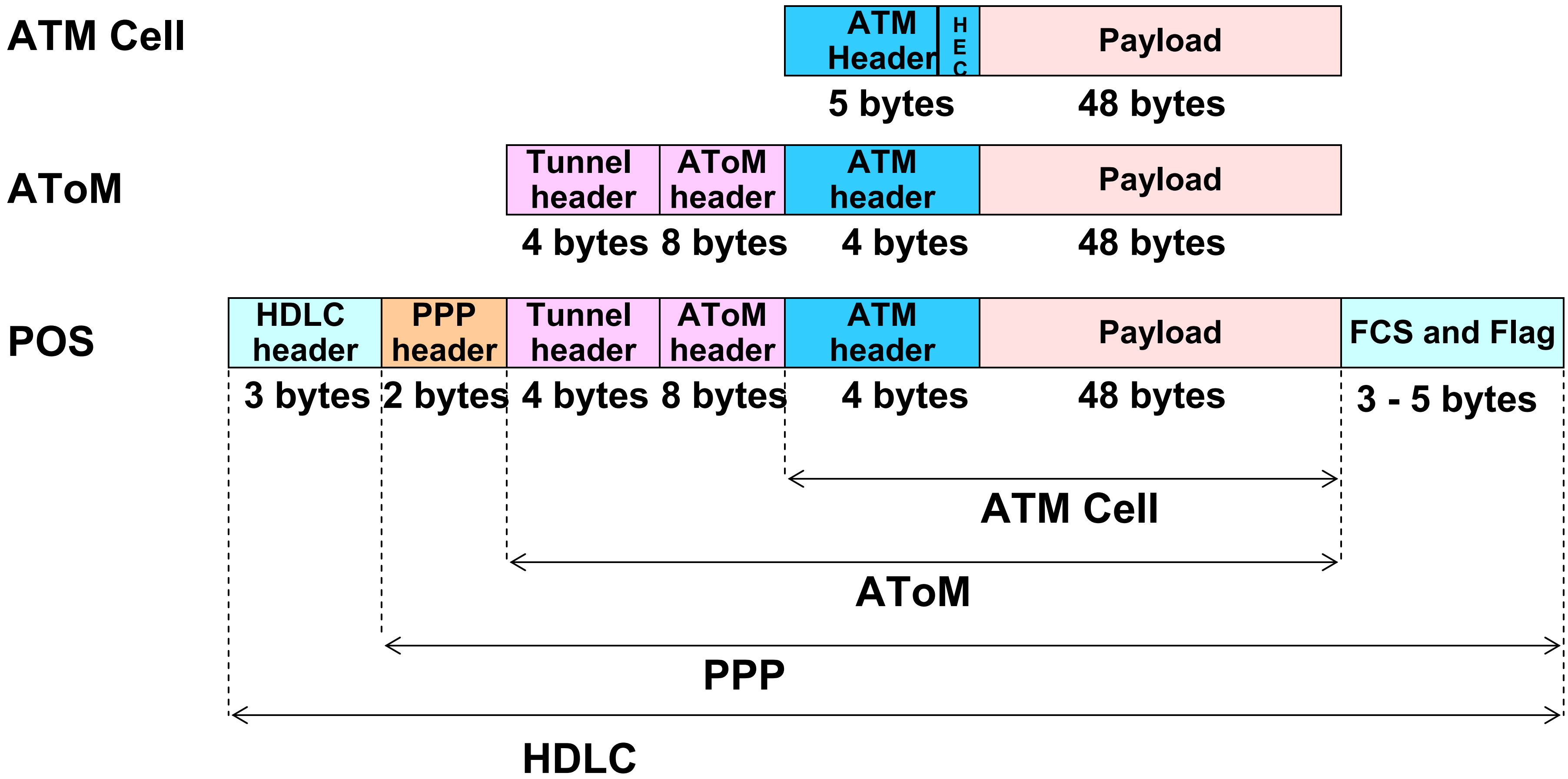
AToM Resilience for PE Failure

- OAM RDI is sent out on ATM VC and MGW uses redundant path 12.0.26S
- MR-APS 12.0.30S
- Backup Pseudowire 12.0.31S

Deployment Considerations for ATM Enabled MGW Over and MPLS Backbone

- Resilience
- Optimization

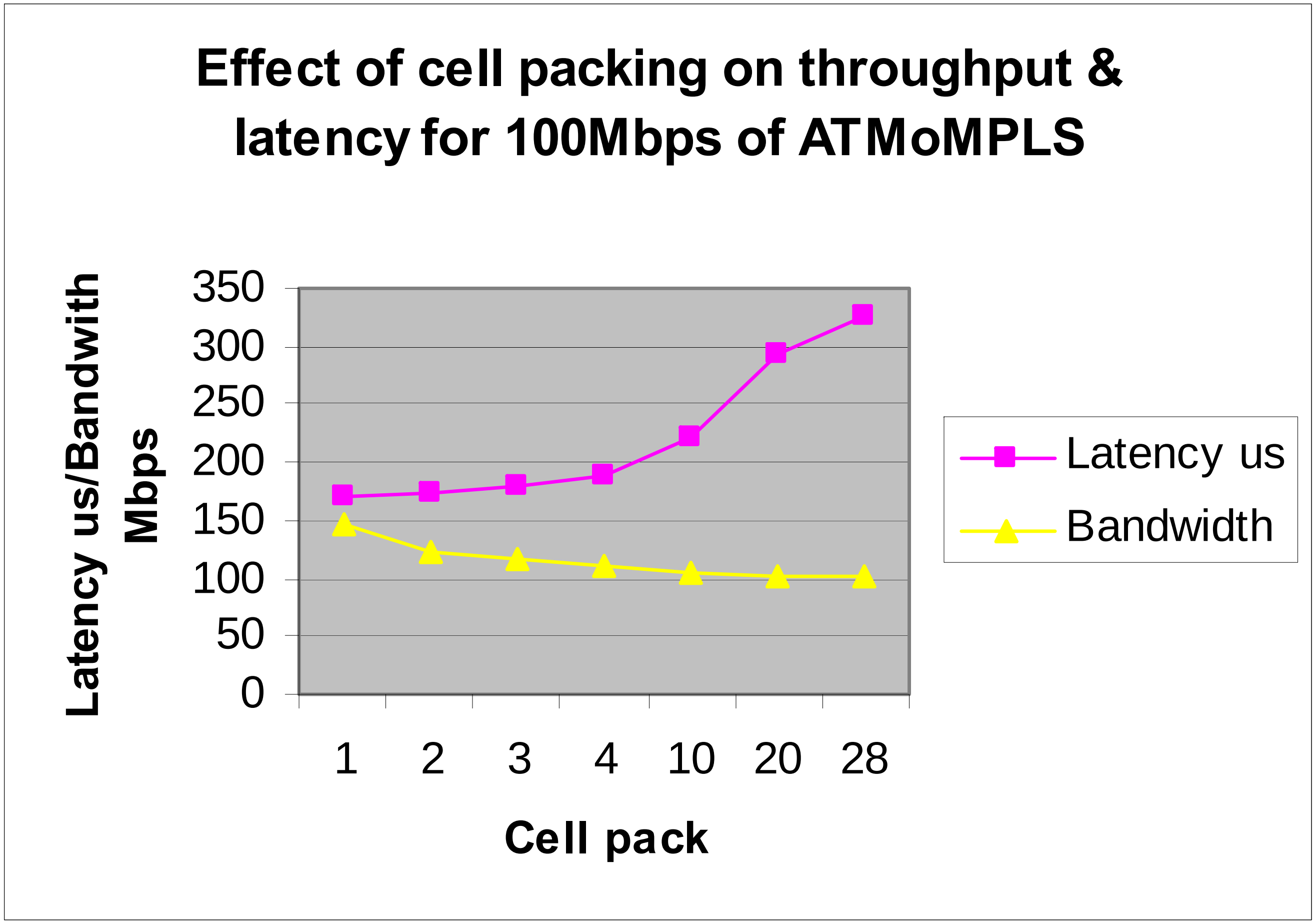
ATM over MPLS



ATM over MPLS 22 bytes per ATM Cell

VC, VP and port mode

Cell Packing on 4 port STM1 ATM Engine 3



ATM Cell Packing—
Maximum Cell Packing Timers (MCPT)

```
int atm 7/1
    atm mcpt-timer 50 100 300 ← In microseconds
    atm pvp 1 l2transport
       xconnect 122.122.102.102 101 encapsulation mpls
       cell-packing 5 mcpt-timer 1
```

Example Configuration for packing 5 cells with an MCPT of 50 microseconds (mcpt-timer 1)

- 1 MCPT timeout group per interface; 3 independent timers
- Values set in microseconds in 50 microsecond increments up to 25 milliseconds
- Maximum Cells set on the VC, VP, Port
- Cell-packing command specifies timer 1 is to be used

Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

Deployment Considerations for IP Enabled MGW

- Resilience
- Call admission control
- Overheads

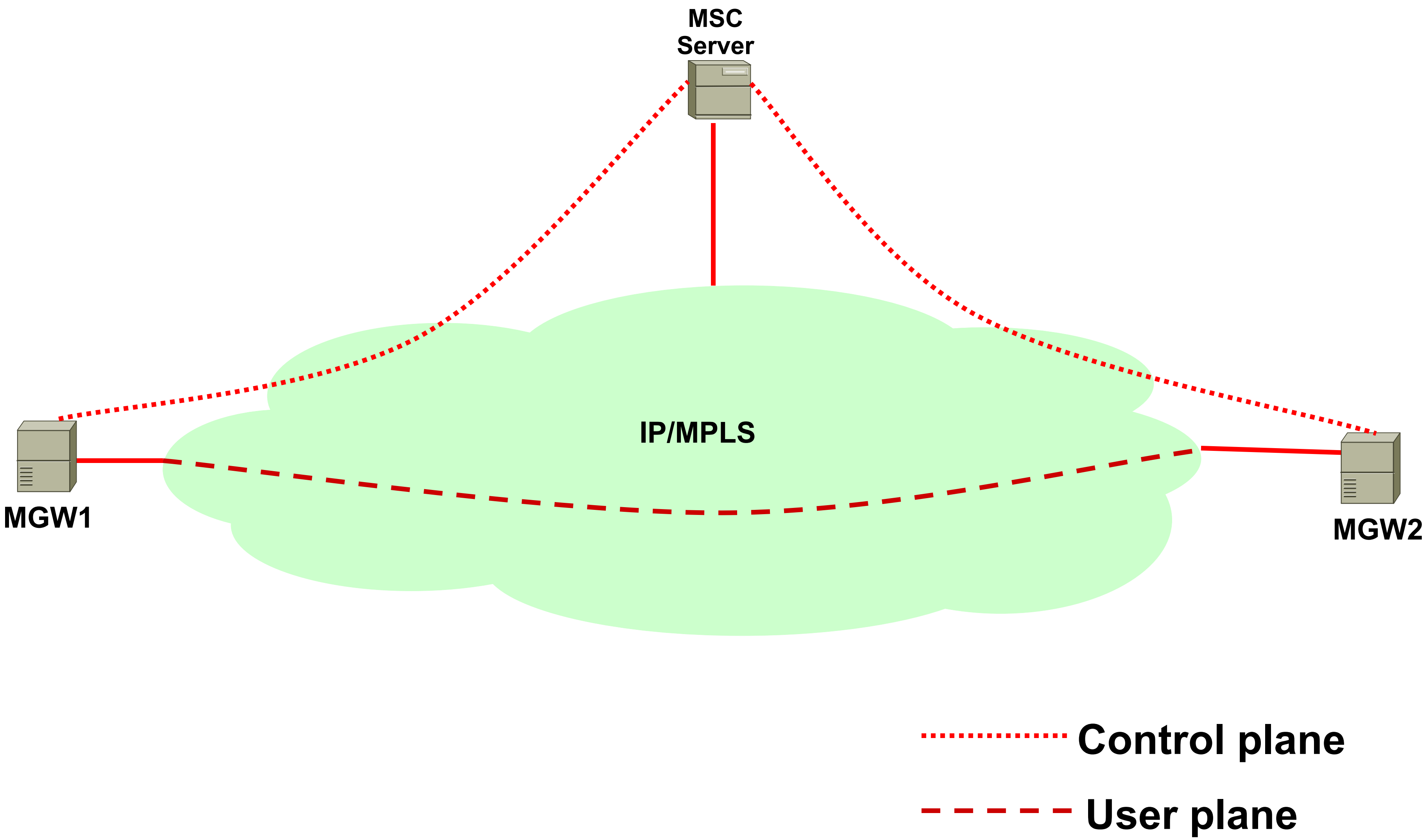
Deployment Considerations for IP Enabled MGW

- Resilience
- Call admission control
- Overheads

Deployment Considerations for IP Enabled MGW

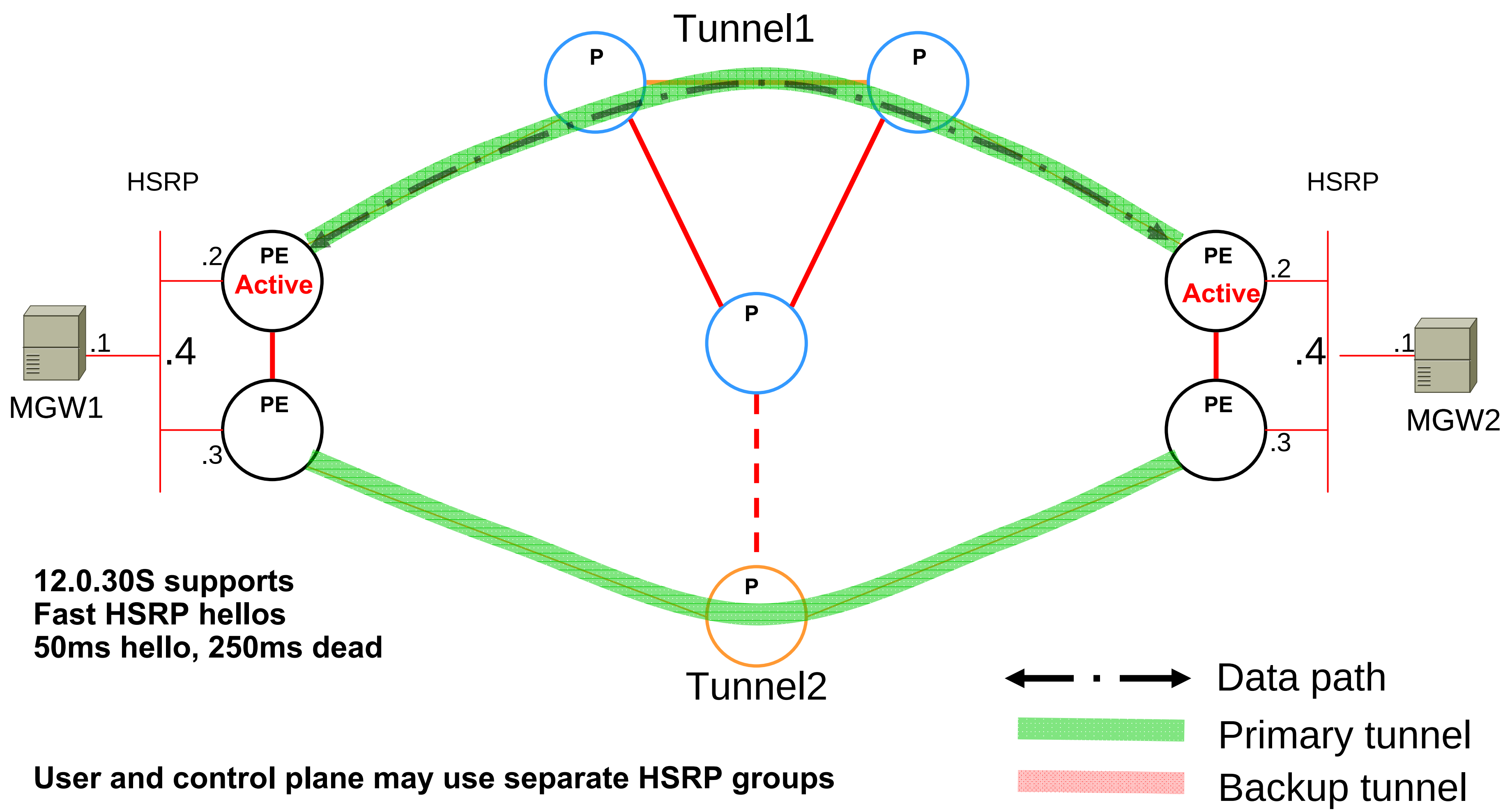
- PE or CE or hybrid?
- ATM, GE or POS connected?
- Dual homed?
  - Multiple IP addresses
  - Single destination IP address with mulitple physical connections
  - Multiple ATM VCs (L2)
- Is the MGW redundant path aware and does it converge?
- What are the effects of loss of control/user plain connections?
- Clocking and synchronisation?

Simple Deployment of Two MGW to Be Considered



Example of a MGW Connected via Multiple HSRP Groups

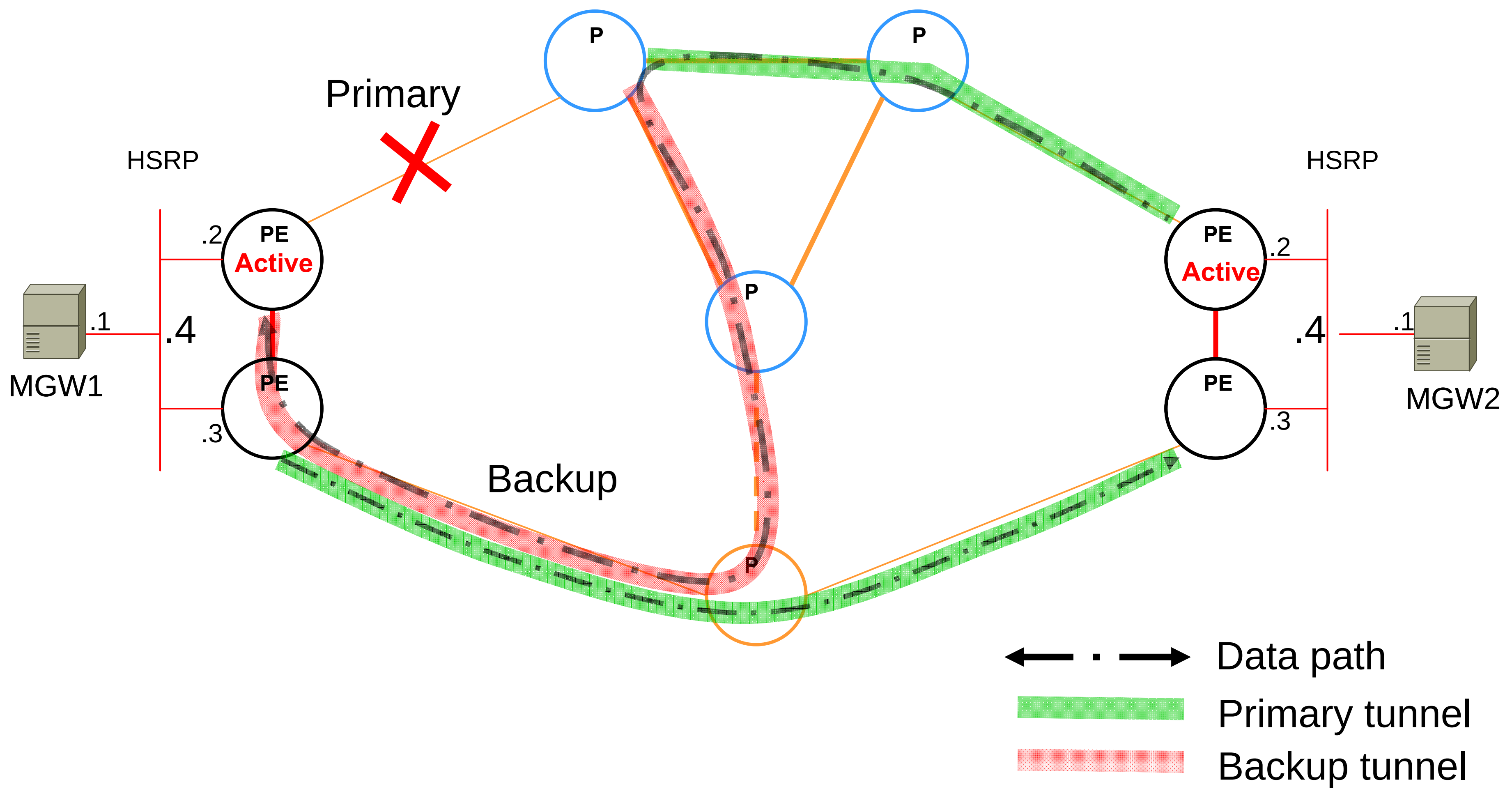
MSC Server not shown



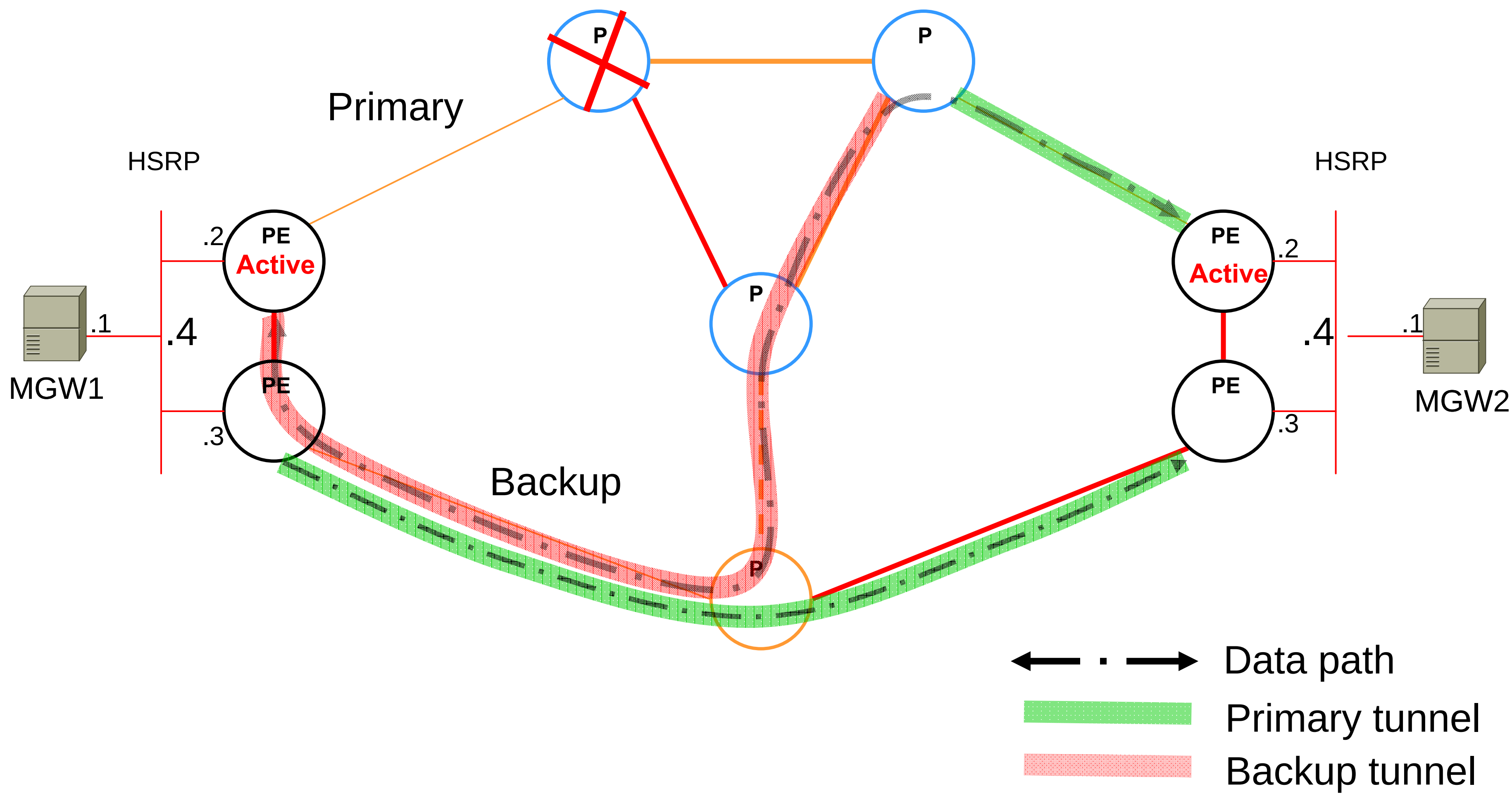
12.0.30S supports
Fast HSRP hellos
50ms hello, 250ms dead

User and control plane may use separate HSRP groups

Link Protection of All Links

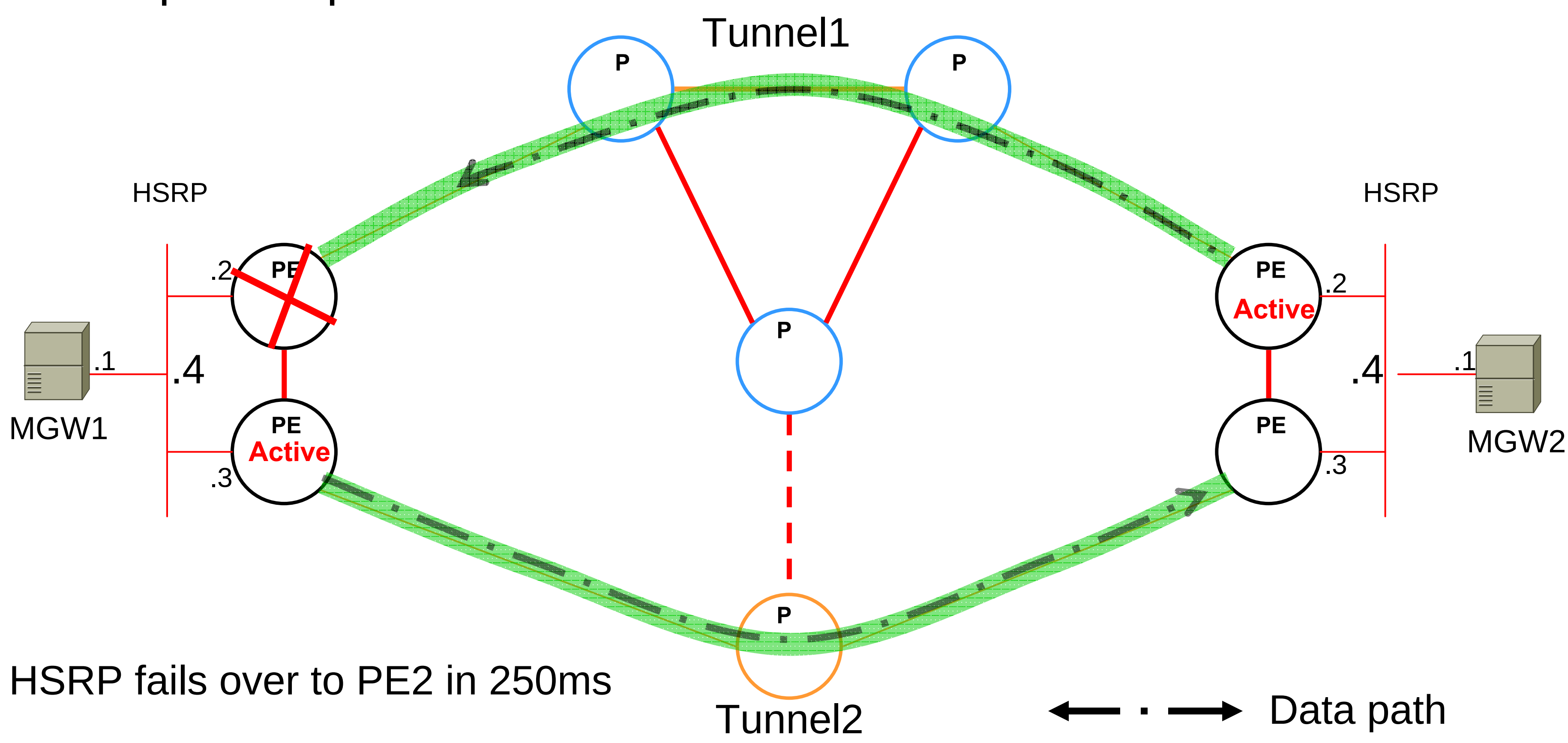


Node Protection for P Node Failure



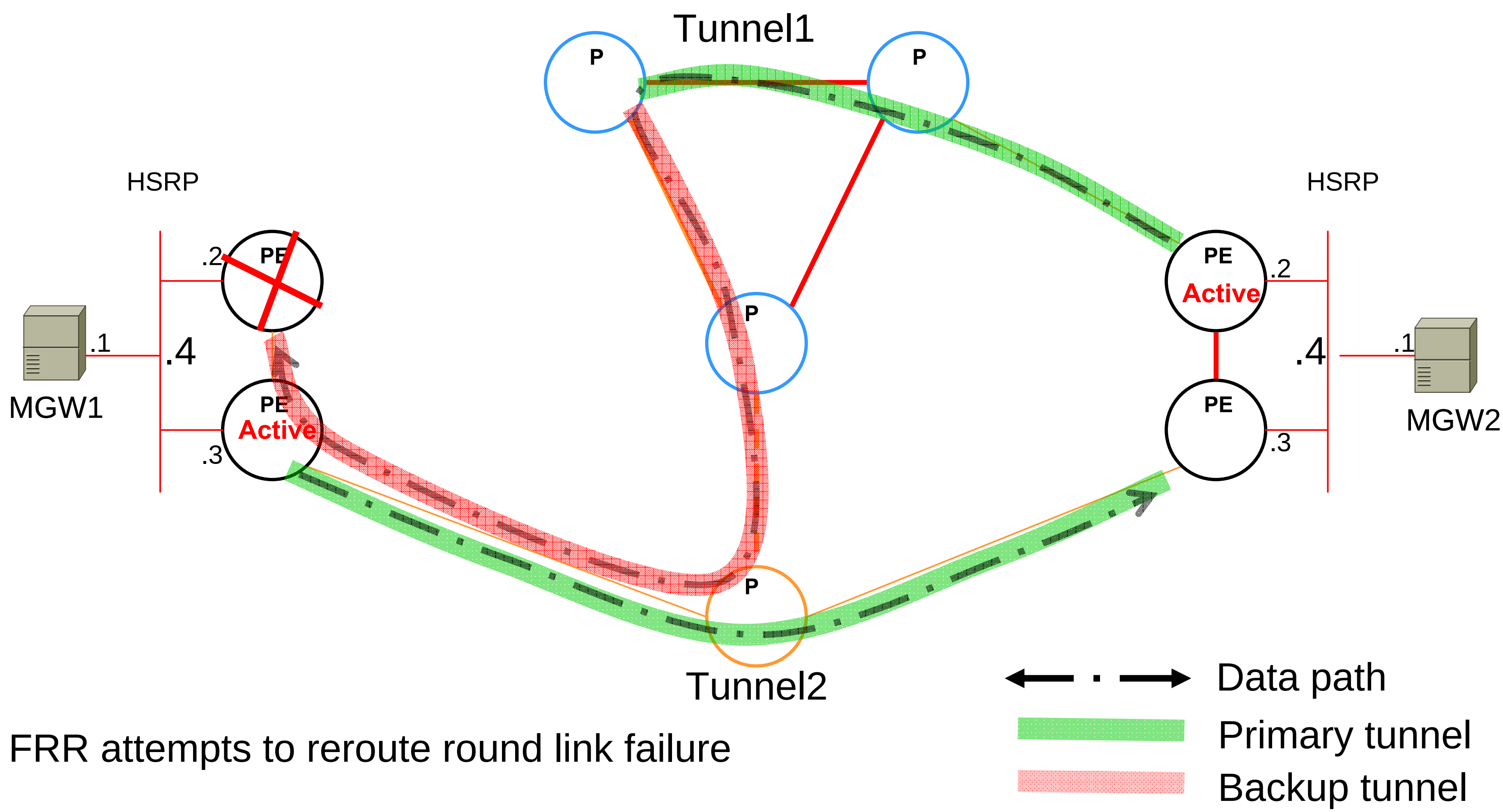
FRR Does Not Protect From PE Failure

MGW1 converges quickly
Return path is the problem



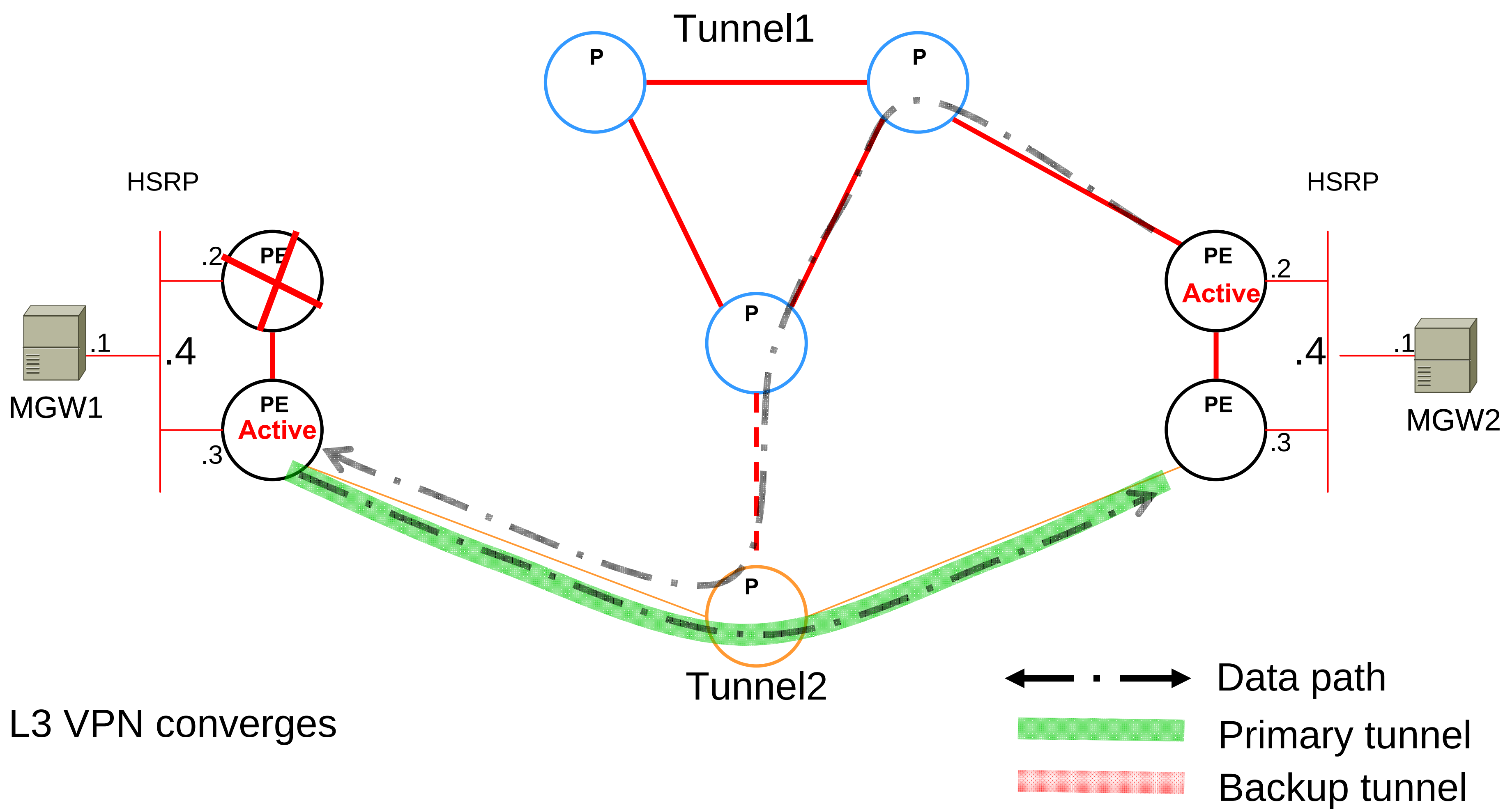
HSRP fails over to PE2 in 250ms

FRR Attempts a Fix



FRR attempts to reroute round link failure

MPLS VPN Eventually Converges

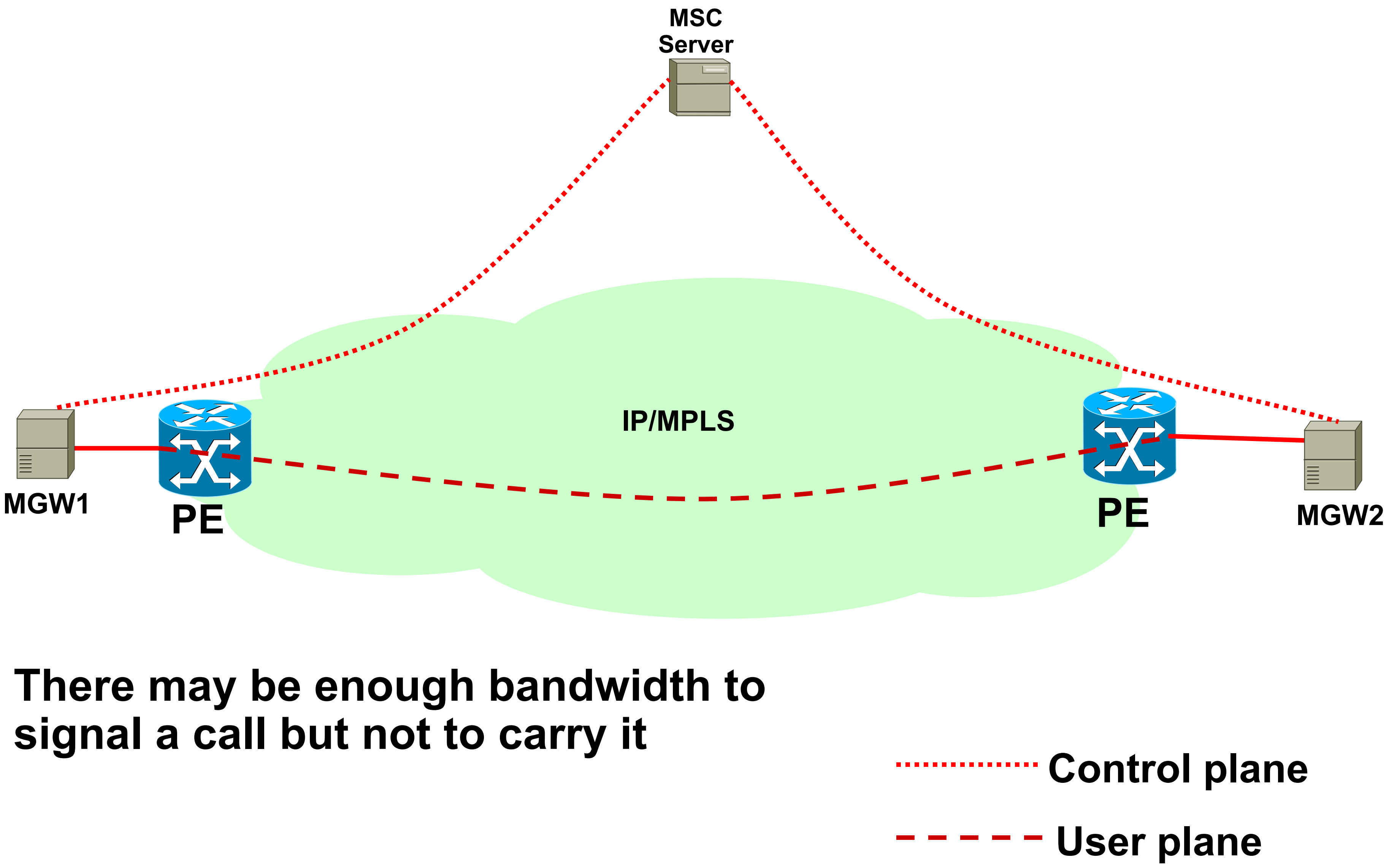


L3 VPN converges

Deployment Considerations for IP Enabled MGW

- Resilience
- Call admission control
- Overheads

In R4 split MSC the user plain and control plane are separate



There may be enough bandwidth to signal a call but not to carry it

Admission Control: Why?

Ensuring Traffic Fits in Network

- The Over-Provisioning Model: Adjust Network capacity to peak Traffic
- The TCP Congestion Control Model: Adjust every elastic flow to its share of Network capacity
- The Admission Control Model: Reject Flows that don't fit
- Many environments live happily through combination of Over-Provisioning and TCP Congestion Control

  e.g. The Internet, Campus networks, …

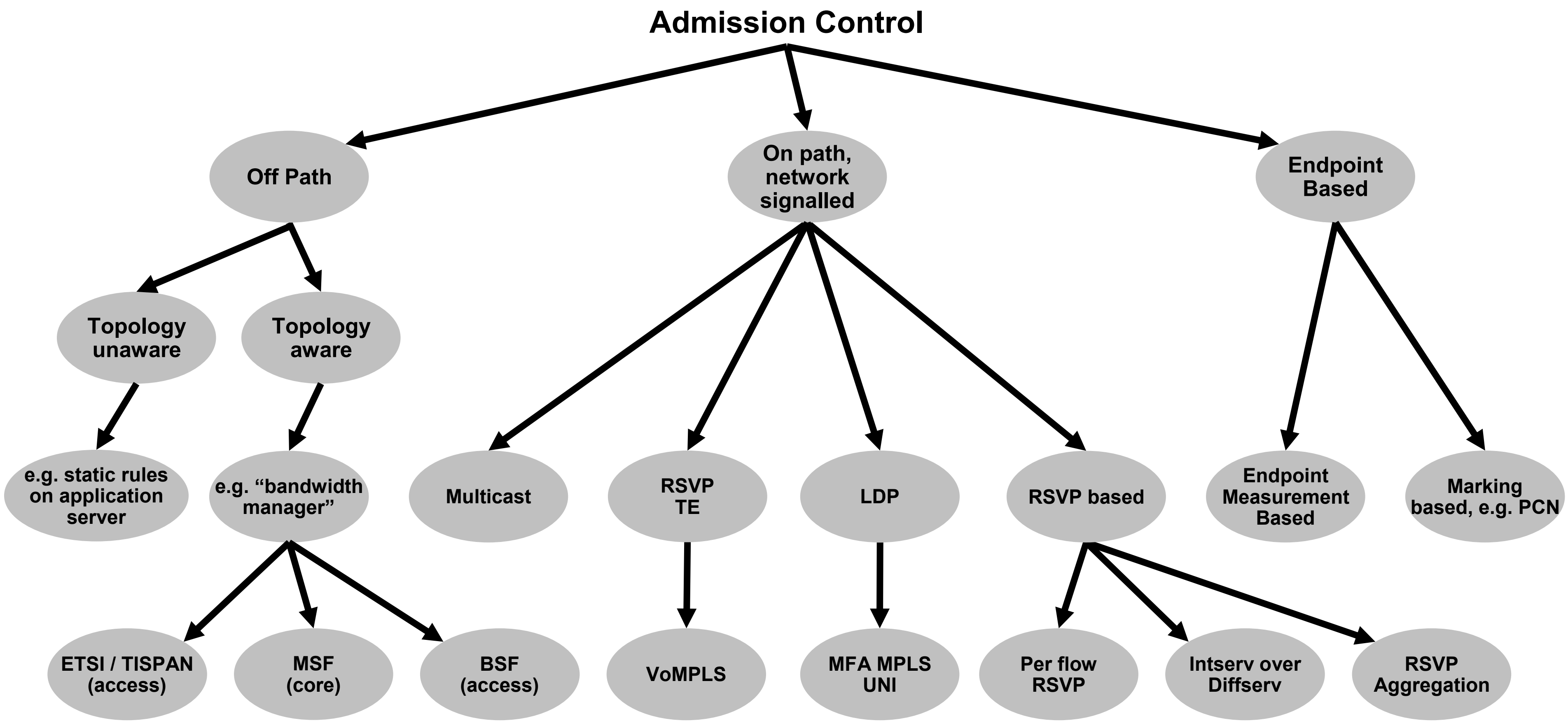
- Some environments require Admission Control. Typically, where
  - – Important Traffic is inelastic ("steep utility curve"), like Voice/Video
  - – inelastic traffic is in high proportion, like Video in Metro Aggregation
  - – Determinism is required

  e.g. Mobile Phone Trunking, Triple Play network, Enterprise WAN, Military Ad-hoc networks

Admission Control: What?

- A technology for:
  - (i) Deciding which flow fits or doesn’t fit into network.
  - (ii) Providing explicit notification to Application so it can do the right thing (e.g send busy tone). Often challenging, as it requires the “Network” and the “Application” to communicate

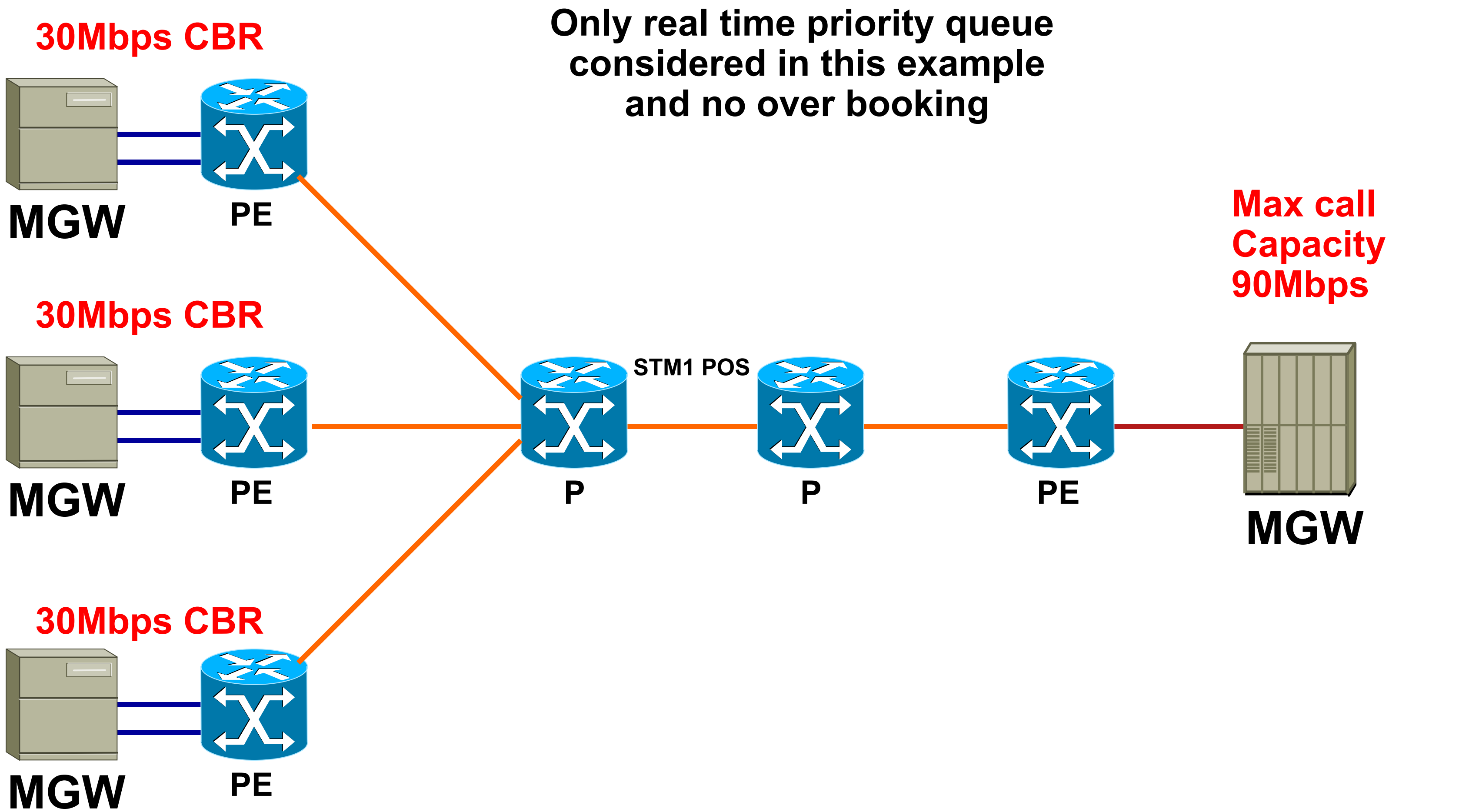
Admission Control: How? Taxonomy for Admission Control



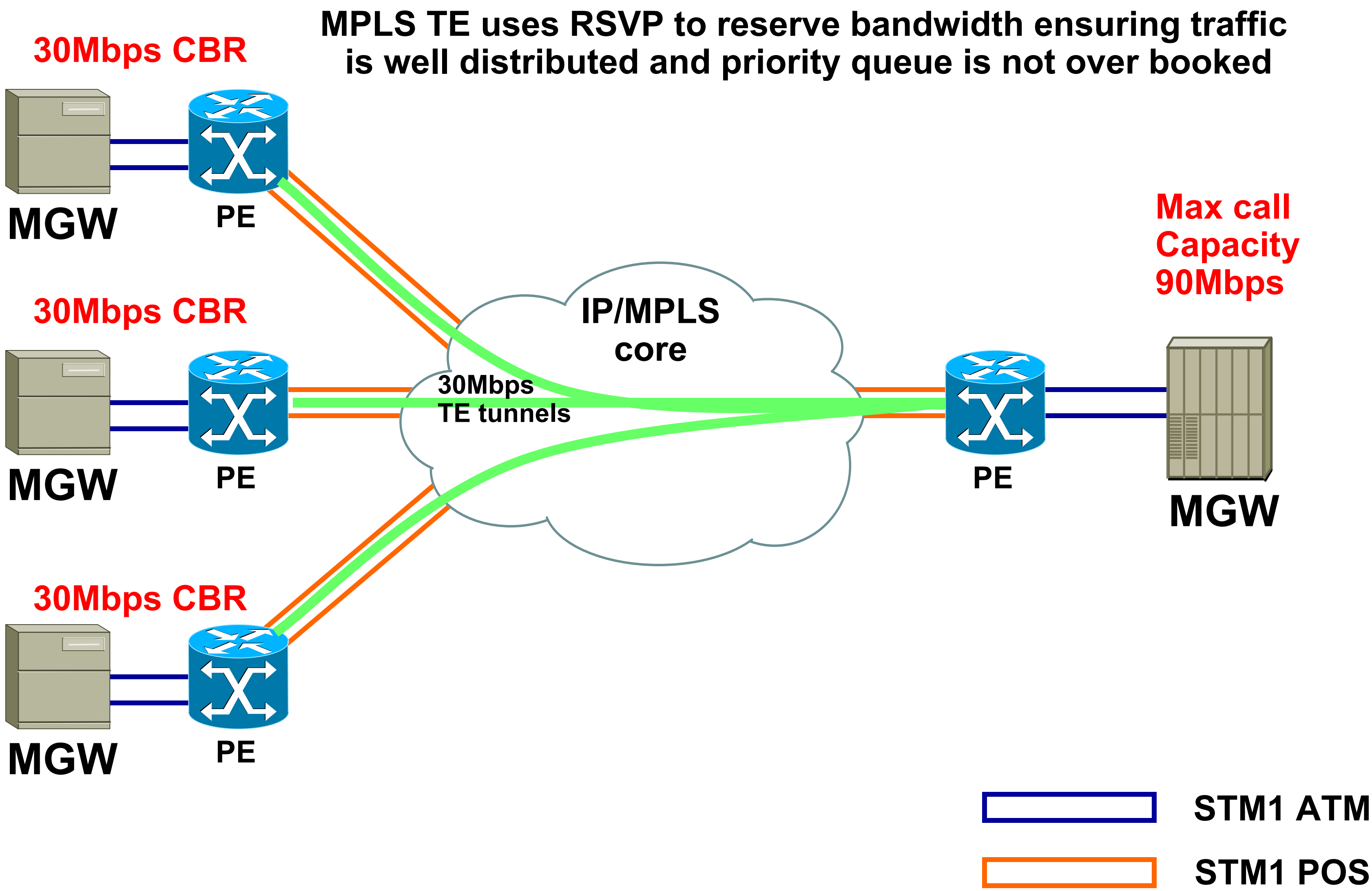
Call Admission Control solutions

- Full details of the Cisco CAC solutions are covered within the following sessions
- TECBBA – 1002 : Service and Session Management for Broadband users
- CAC is key technology in multi-service networks in both the core and access domains
- A discussion giving a brief overview of the solutions that might apply to a Mobile transport network follows.

Capacity planning real time traffic based on known topology



Capacity planning real time traffic using TE

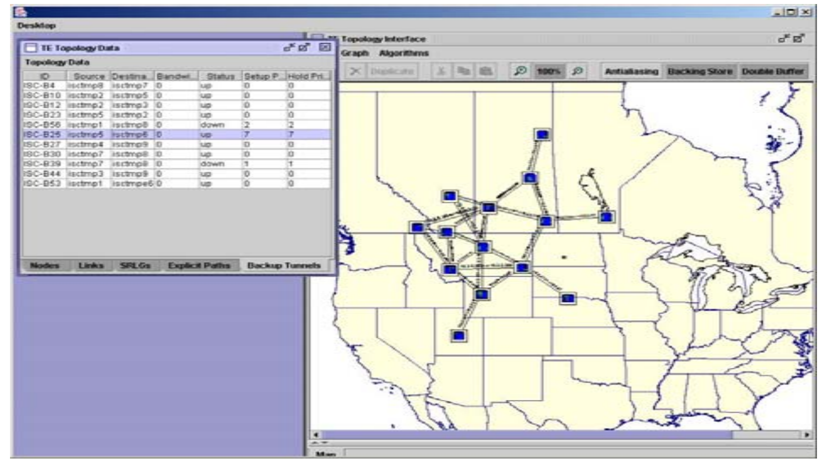


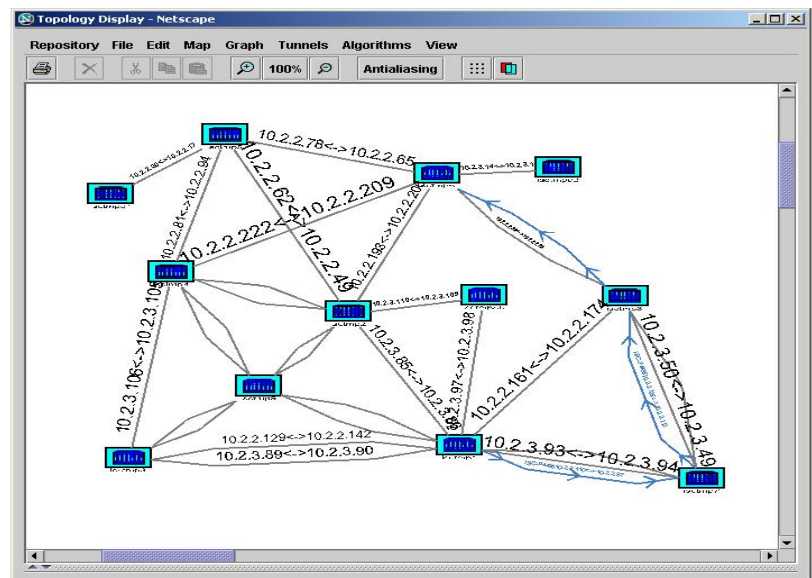
ISC:TEM

- Discovery, Audit and Provisioning
- Manage change
- Provision primary tunnels
- FRR link and node protection
- Bandwidth Protection

  Compute placement of Fast Reroute backup tunnels to protect critical network elements

  Protect bandwidth against link, node, or SRLG (Shared Risk Link Group) failures
- Can take into account delay figures for links from other sources ie find a path with 10Mbps and 5ms delay for primary and backup.

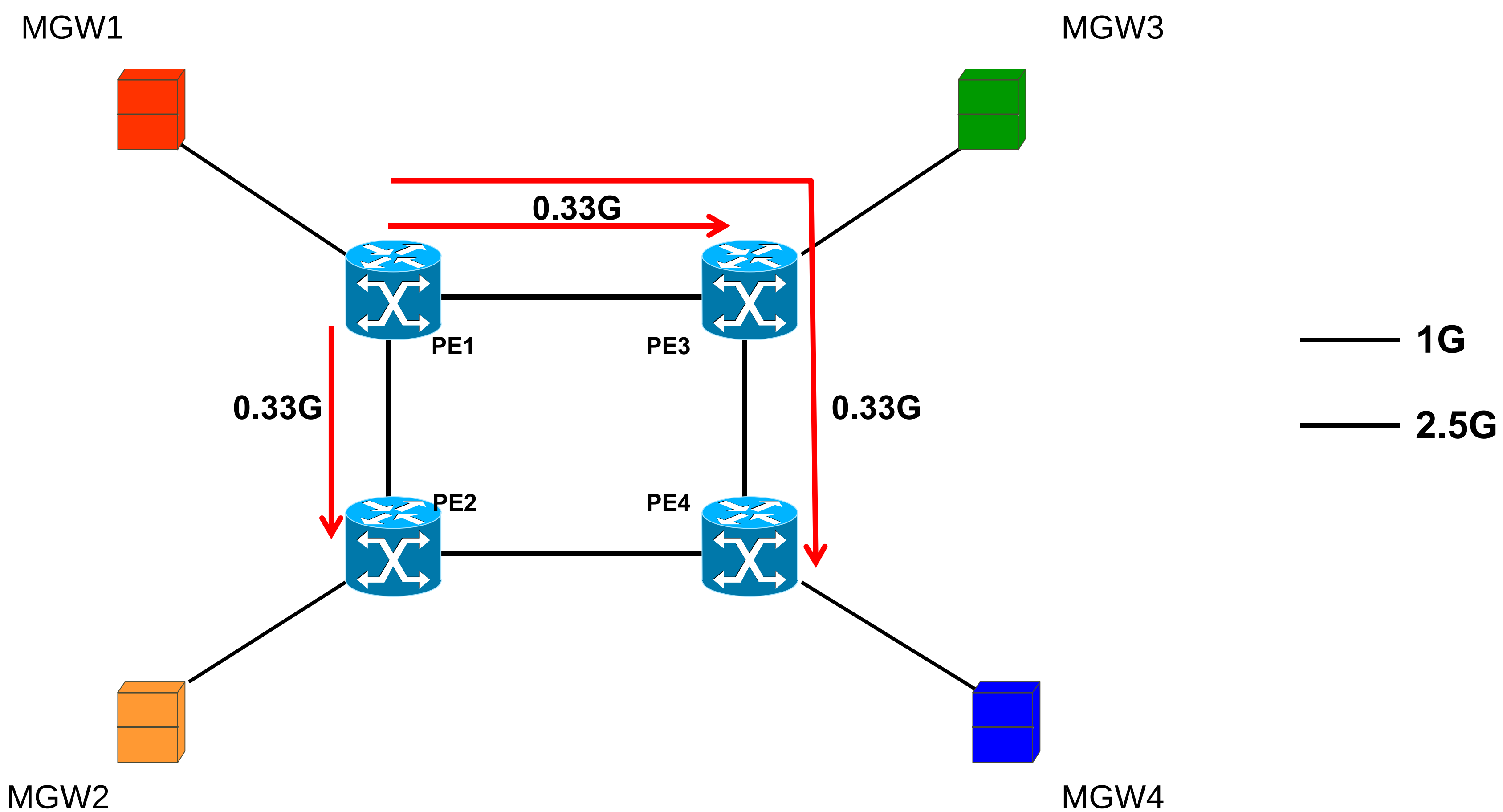




The CAC problem

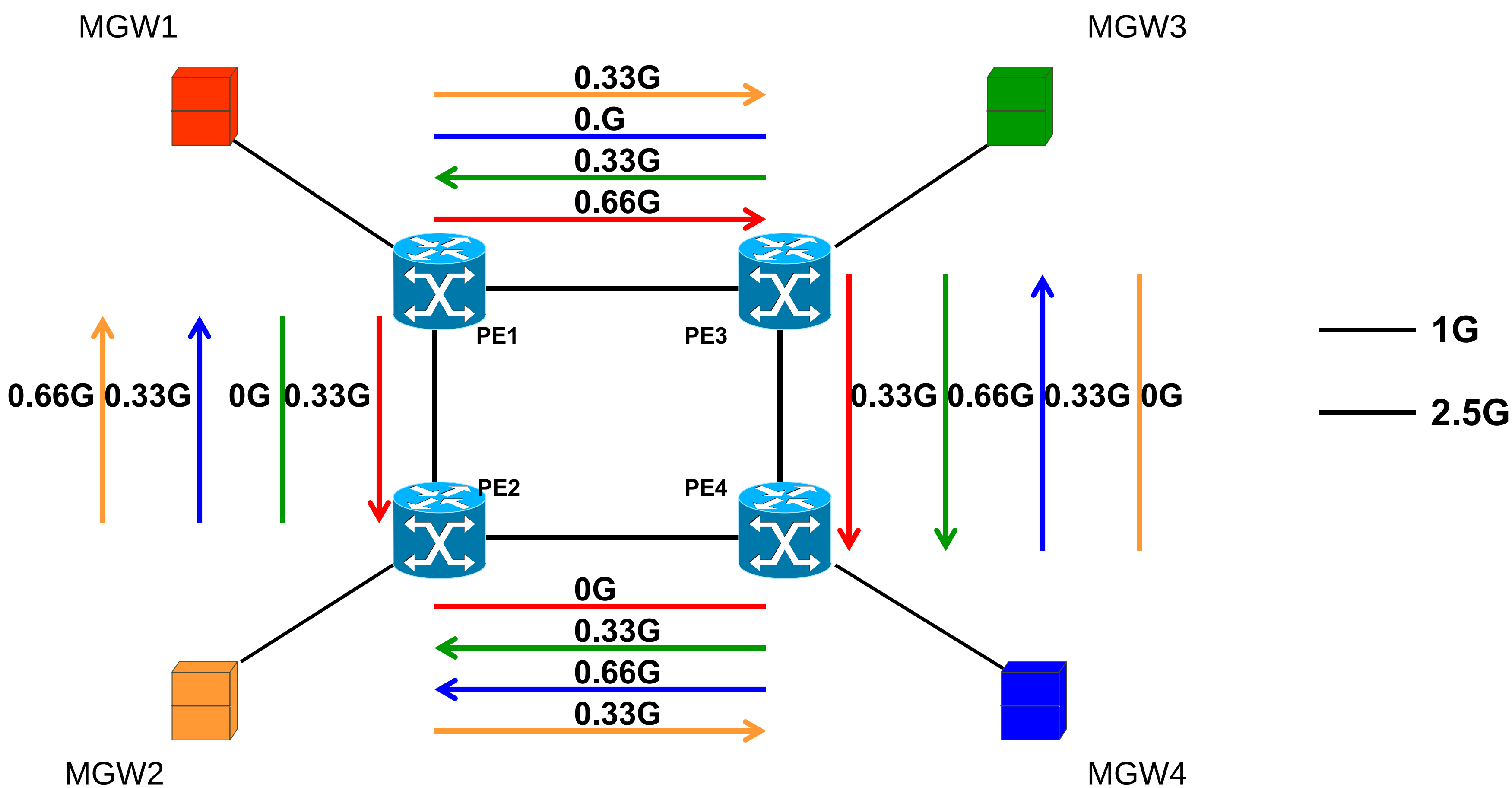
- Can use static TE tunnels across network to ensure required capacity is available
- but what traffic load do you base the tunnels on?
  - Busiest hour of the year (new years eve at 2359hrs)
    - Over provisioning can be expensive
  - As is often the case plan for 95th percentile relying on graceful degradation on other occasions
    - In an IP based solution degradation may not be graceful
  - What failure cases do you include?
    - Link or node failure could double bandwidth on links
    - Will this failure occur at the busiest hour?
- and How do you stop calls when they attempt to grow beyond the load you have engineered for, or when some tunnels no longer fit (eg during failure)?

Example traffic profile from red MGW even distribution of calls



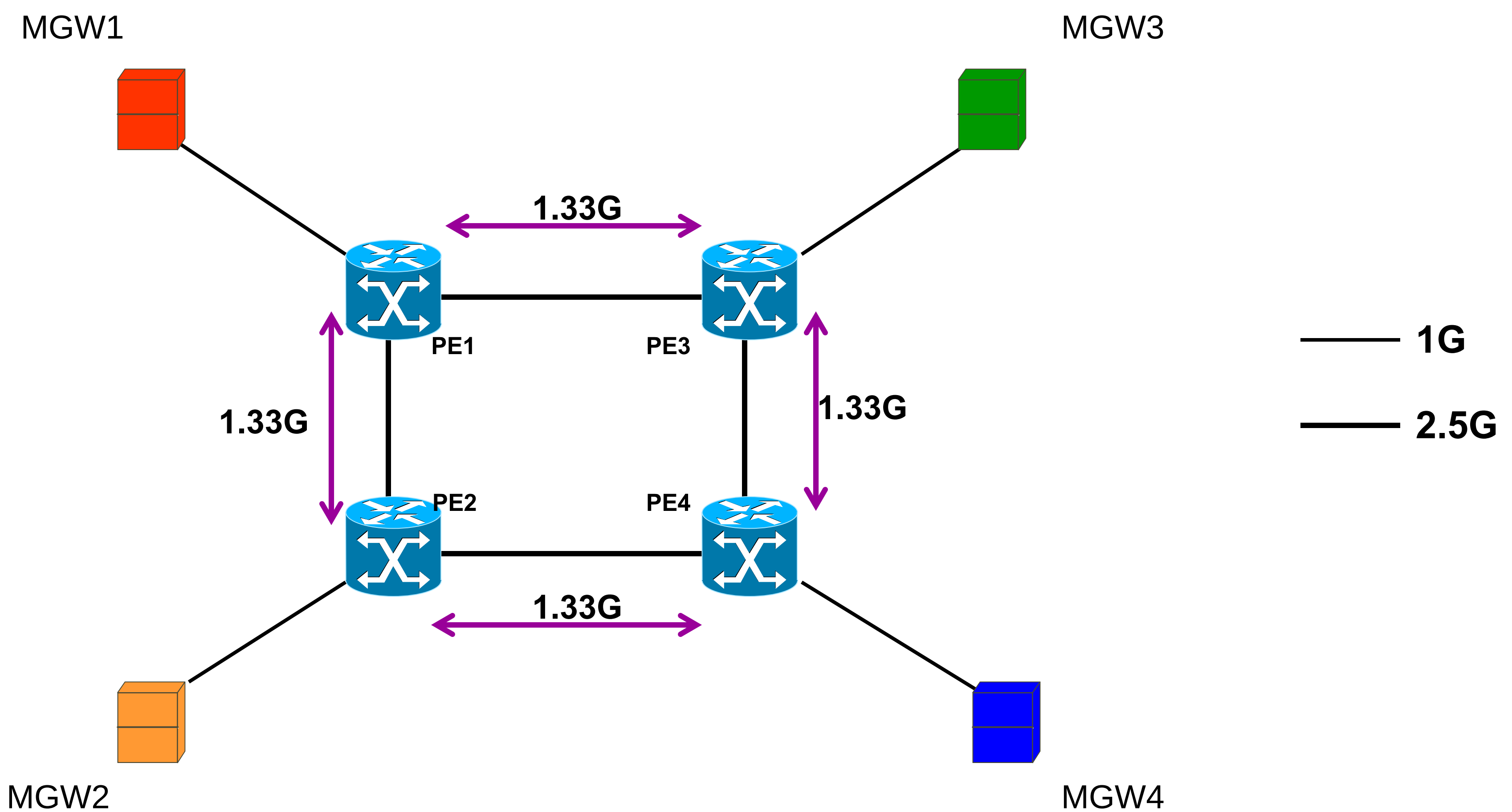
Each MGW can support up to 1G of calls, assume even distribution

Traffic profile from all MGW even distribution



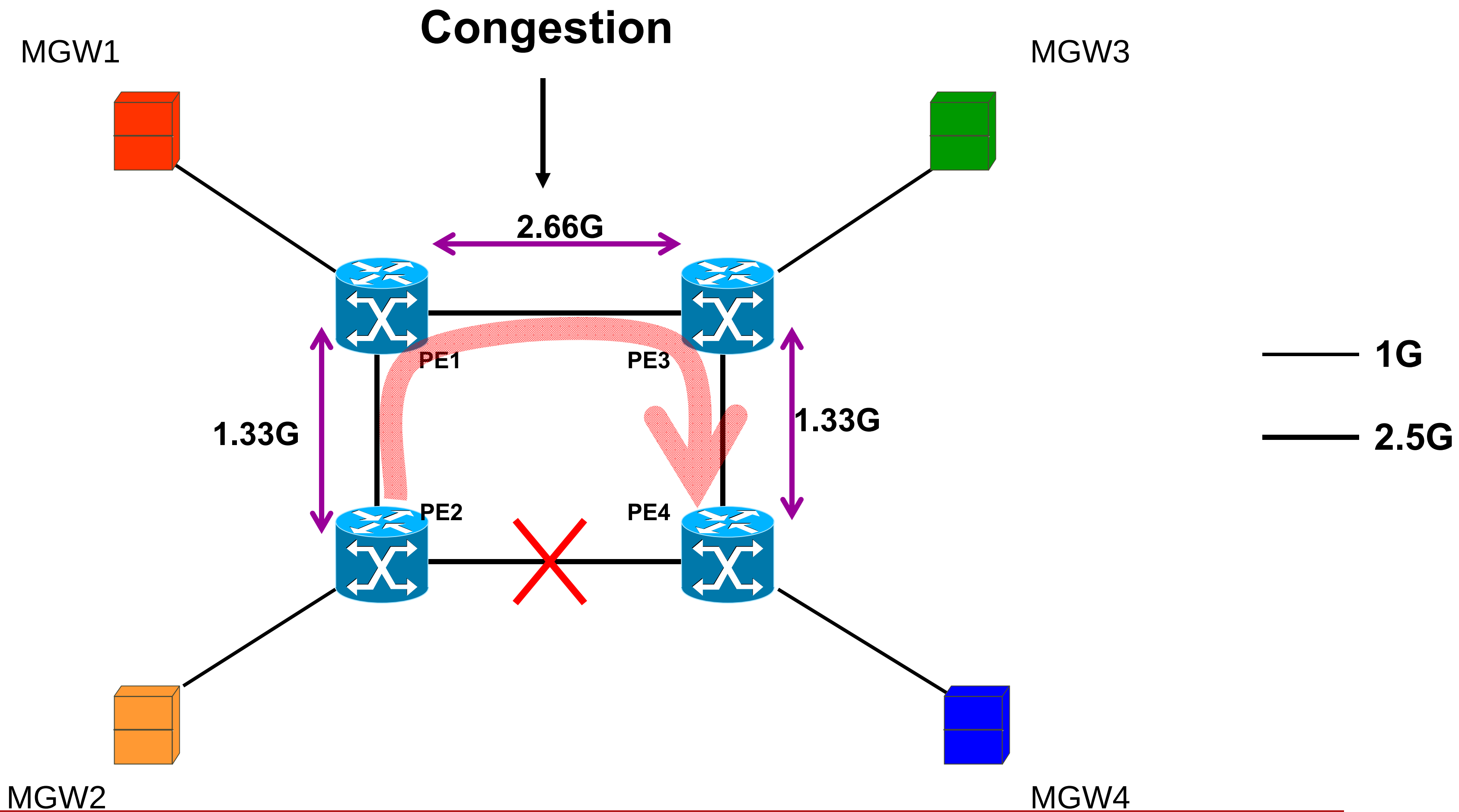
Each MGW can support up to 1G of calls, assume even distribution

Loading on links from all MGW even distribution



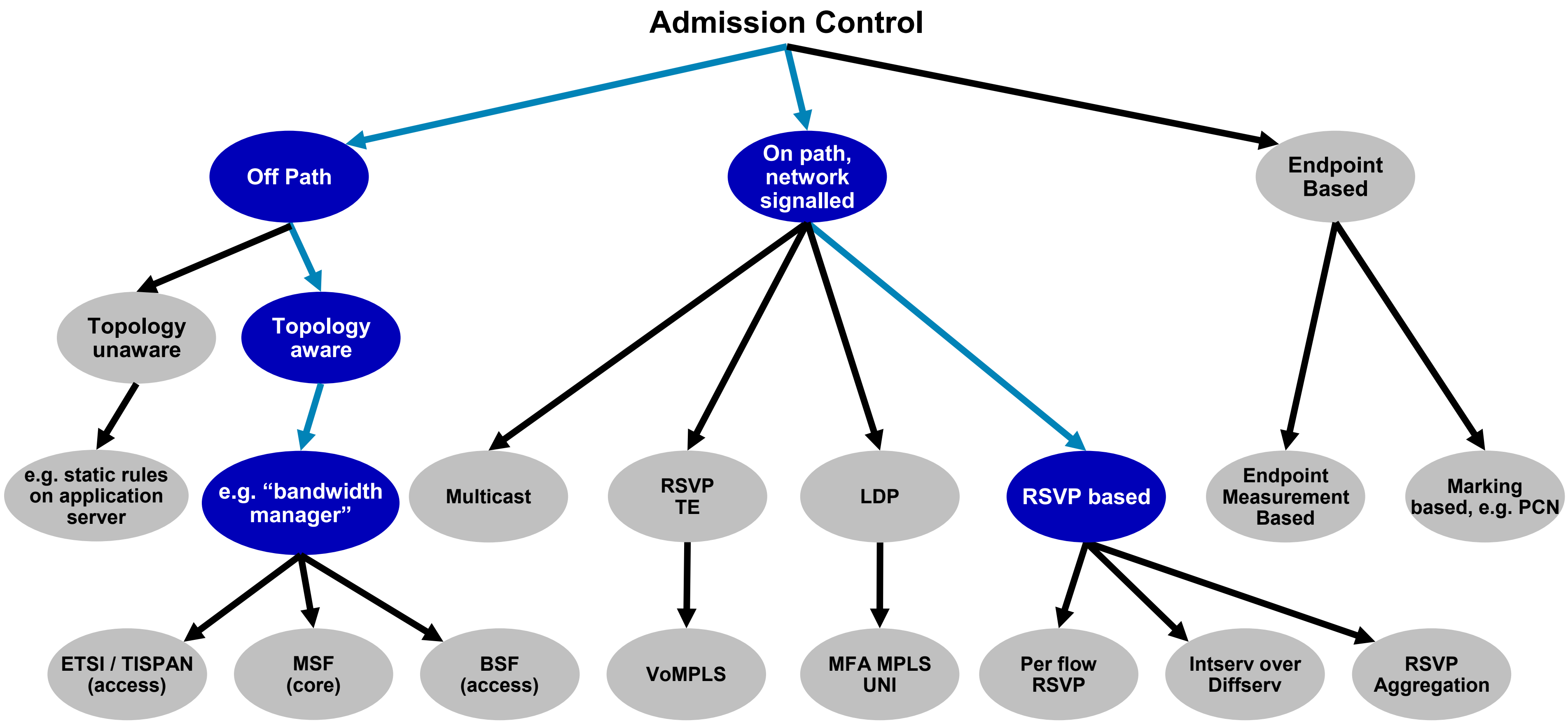
Each MGW can support up to 1G of calls, assume even distribution

Loading on links during failure



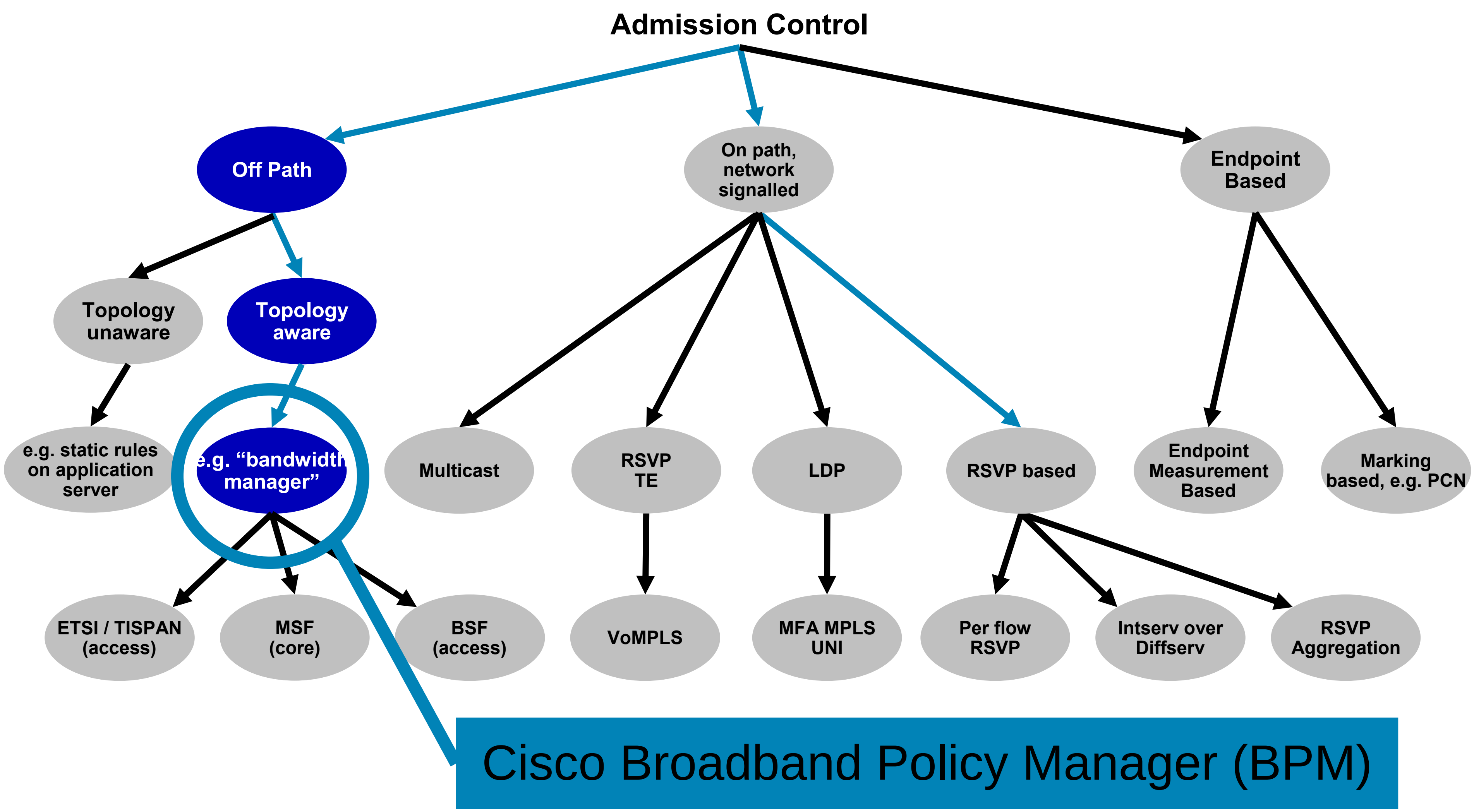
CAC Problem:
How to cope with reduced capacity during failure?

Admission Control: How?
Taxonomy for Admission Control

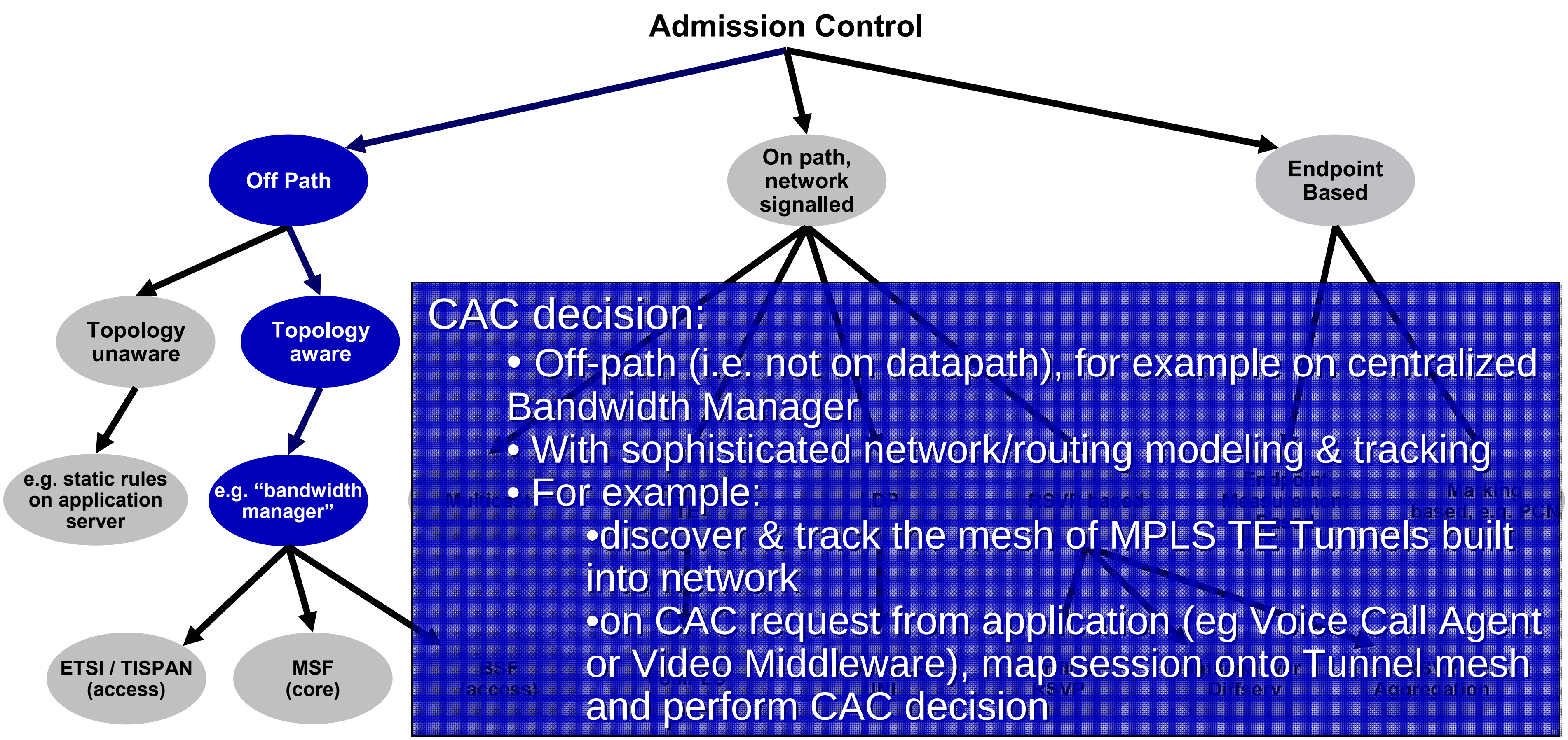


Most applicable to a Converged Mobile Backbone

Admission Control: How? Taxonomy for Admission Control



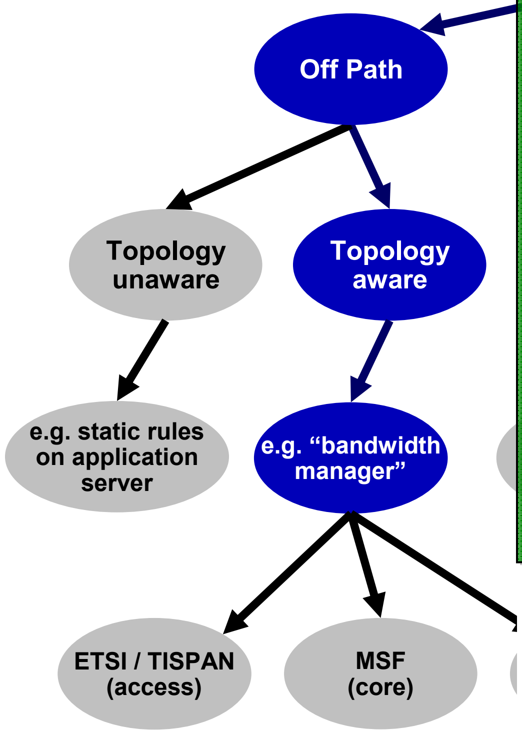
Off-Path Topology Aware CAC



CAC decision:

- Off-path (i.e. not on datapath), for example on centralized Bandwidth Manager
- With sophisticated network/routing modeling & tracking
- For example:
  - discover & track the mesh of MPLS TE Tunnels built into network
  - on CAC request from application (eg Voice Call Agent or Video Middleware), map session onto Tunnel mesh and perform CAC decision

Off-Path Topology-Aware CAC with Cisco BPM



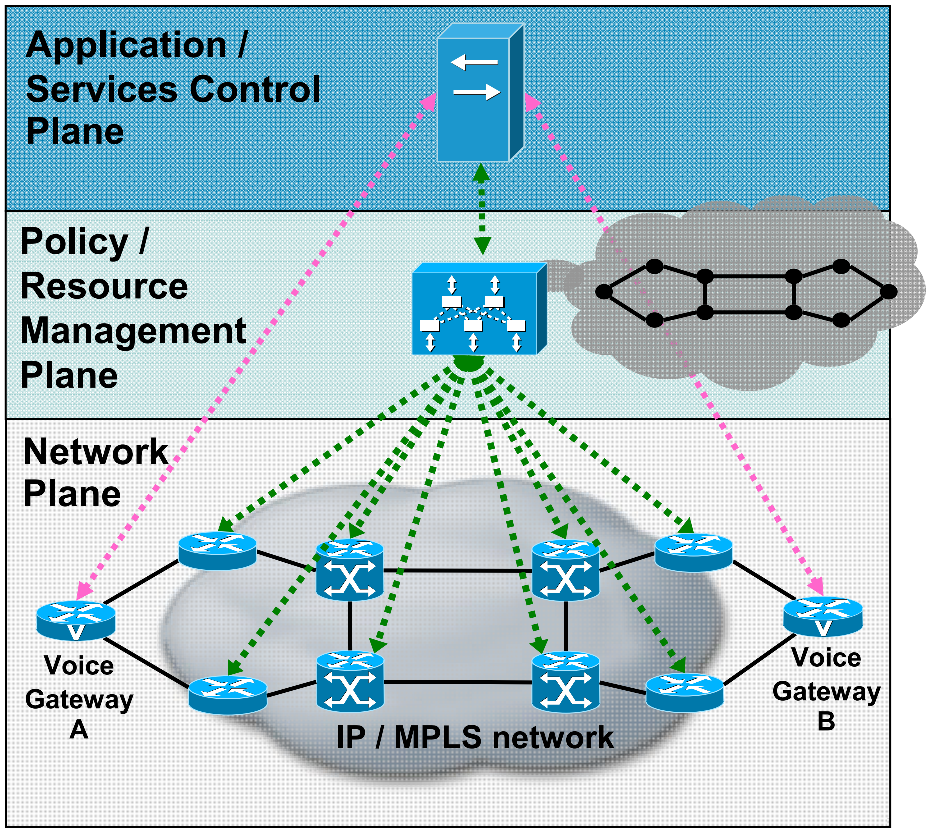
• Cisco Broadband Policy Manager (BPM) is a specific inception of a system capable of supporting the off-path resource/bandwidth management functions defined in the various standards

• Built on top of the industry leading network policy control server platform
  - •Flexible application interfaces
  - •Per-call CAC scaling to PSTN loads
  - •Carrier-class availability

• BPM is an integral part of Cisco's Policy Management Solution

Off-Path Topology Aware CAC with Cisco BPM

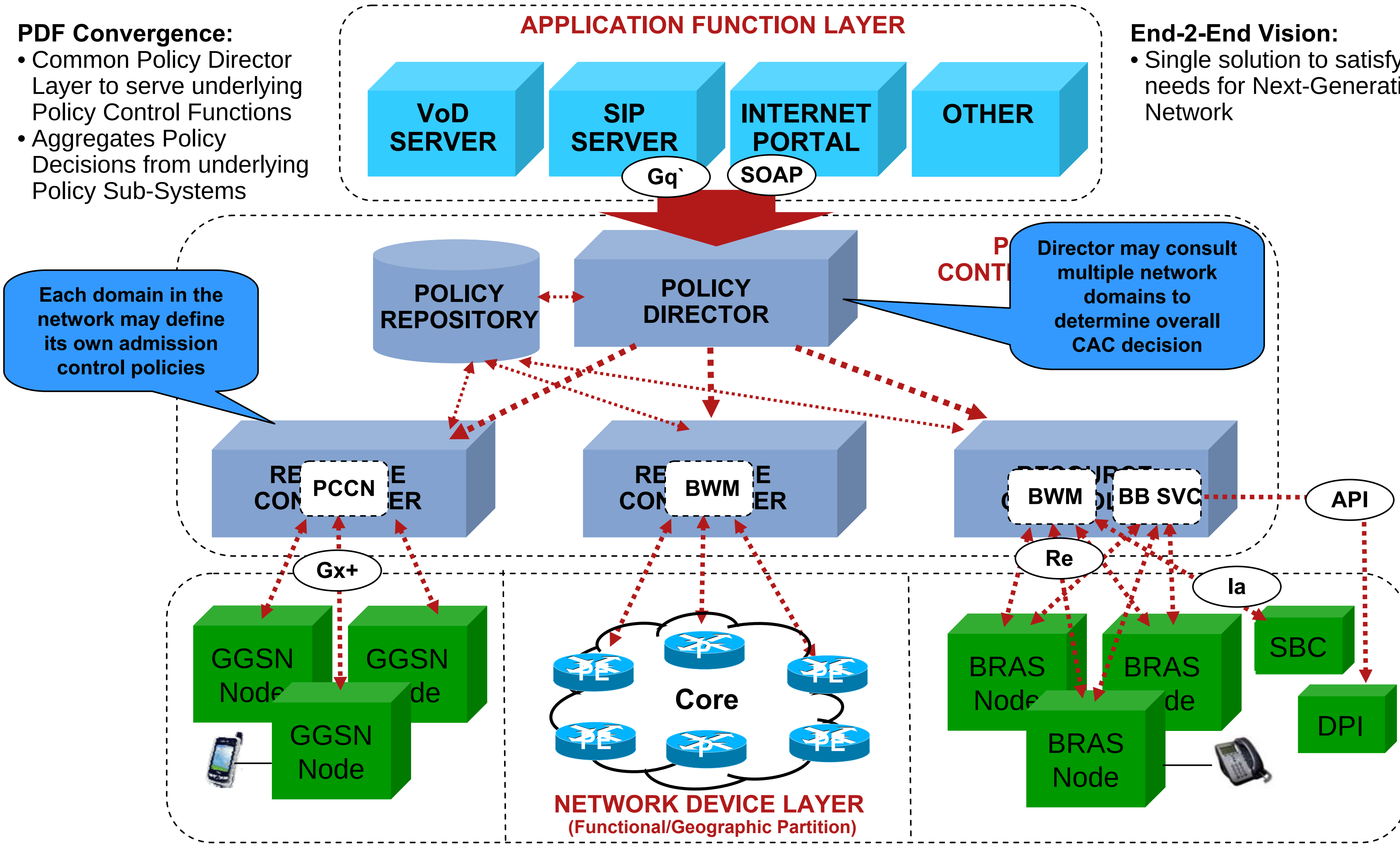
- BPM maintains a view of network bandwidth resources and processes admission control decisions based upon that view
  - View may be abstracted from physical topology
- Can be applied to access and core, L2, L3 and MPLS
- Can be applied to heterogeneous service environments (Voice, Video, Gaming,…)
- Integral part of Cisco Policy Control solution



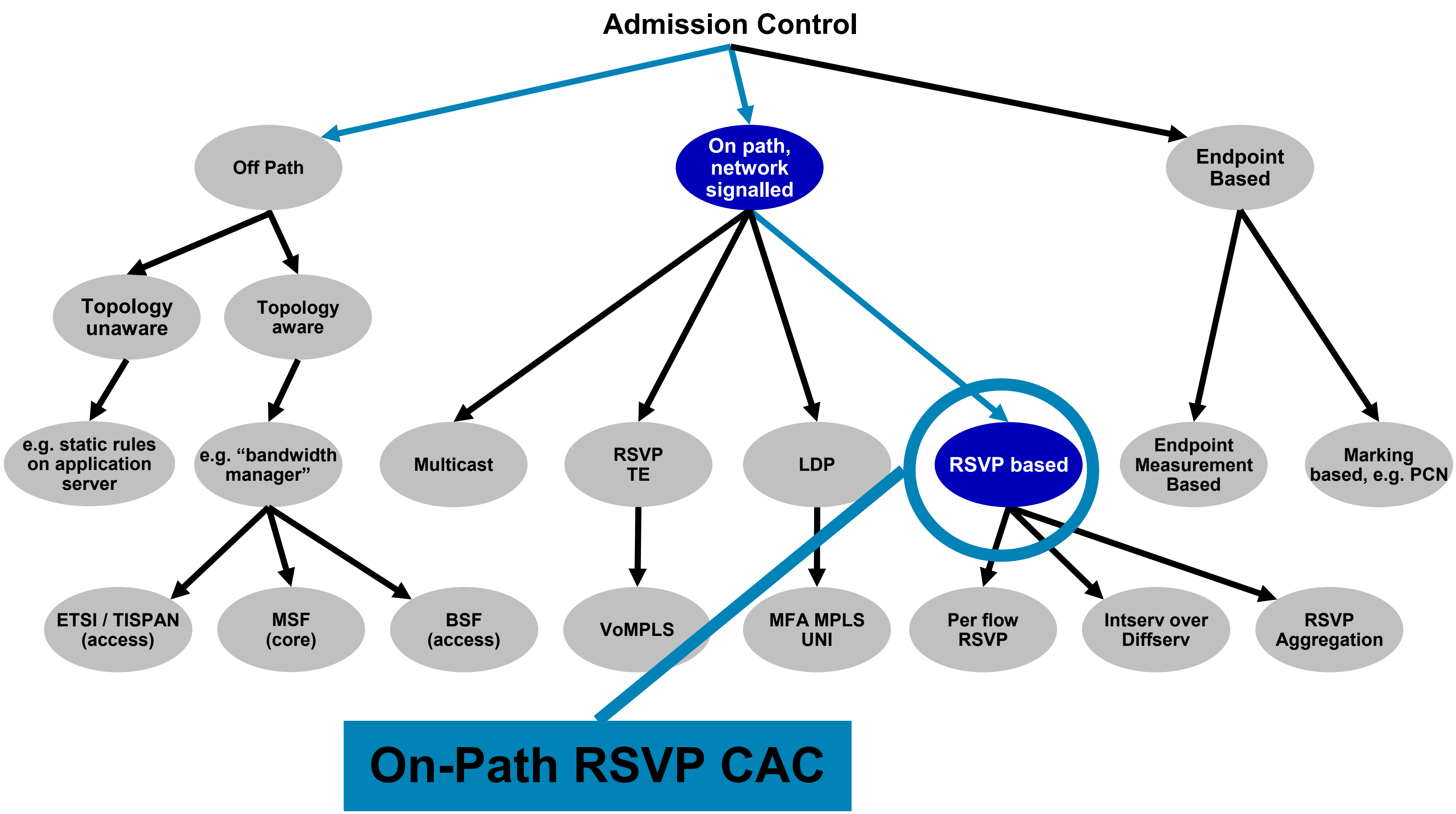
Cisco BPM:
Multi-Domain Admission Control

PDF Convergence:
- Common Policy Director Layer to serve underlying Policy Control Functions
- Aggregates Policy Decisions from underlying Policy Sub-Systems

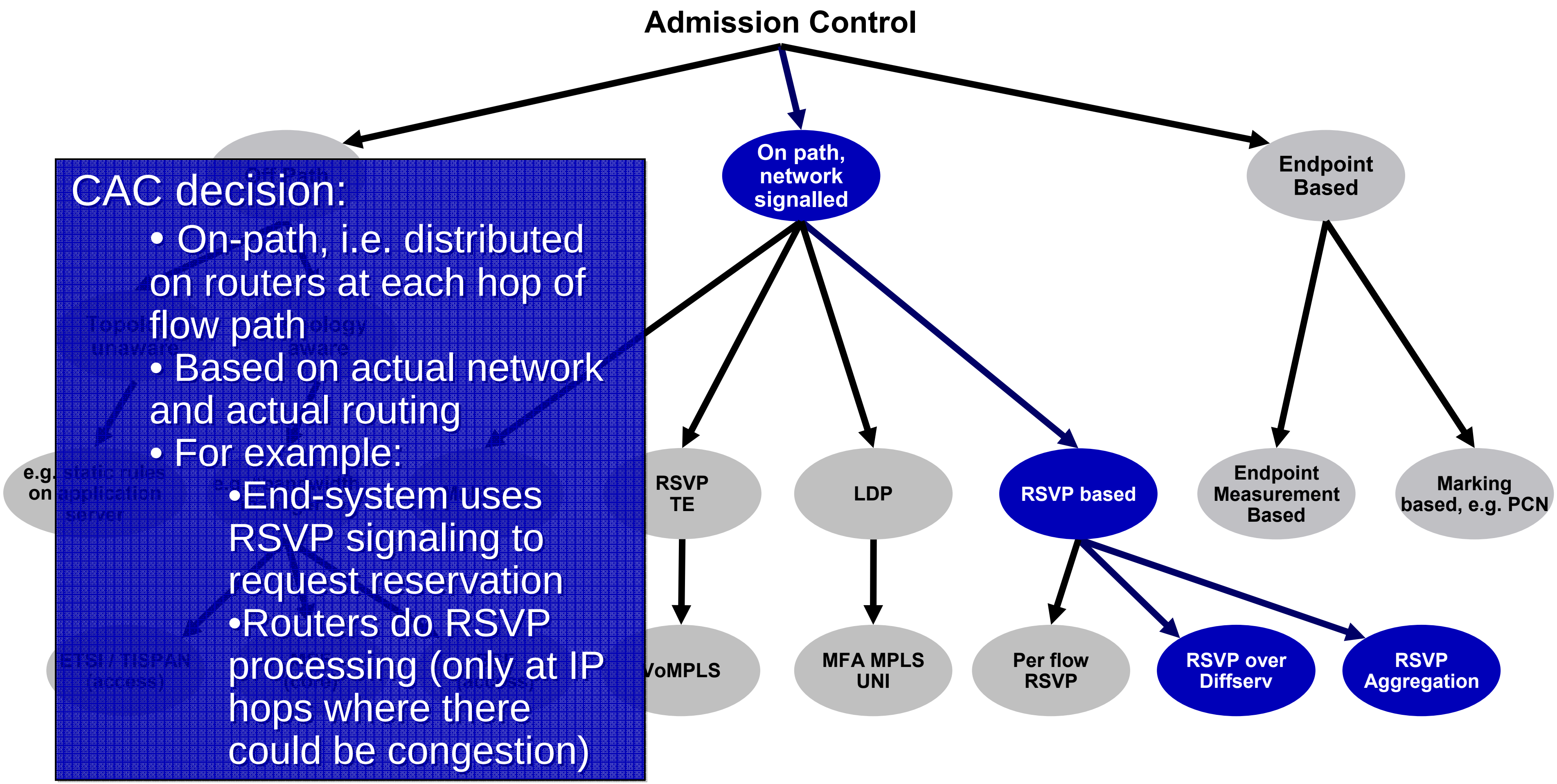
End-2-End Vision:
- Single solution to satisfy needs for Next-Generation Network



Admission Control: How?
Taxonomy for Admission Control



On-Path RSVP CAC

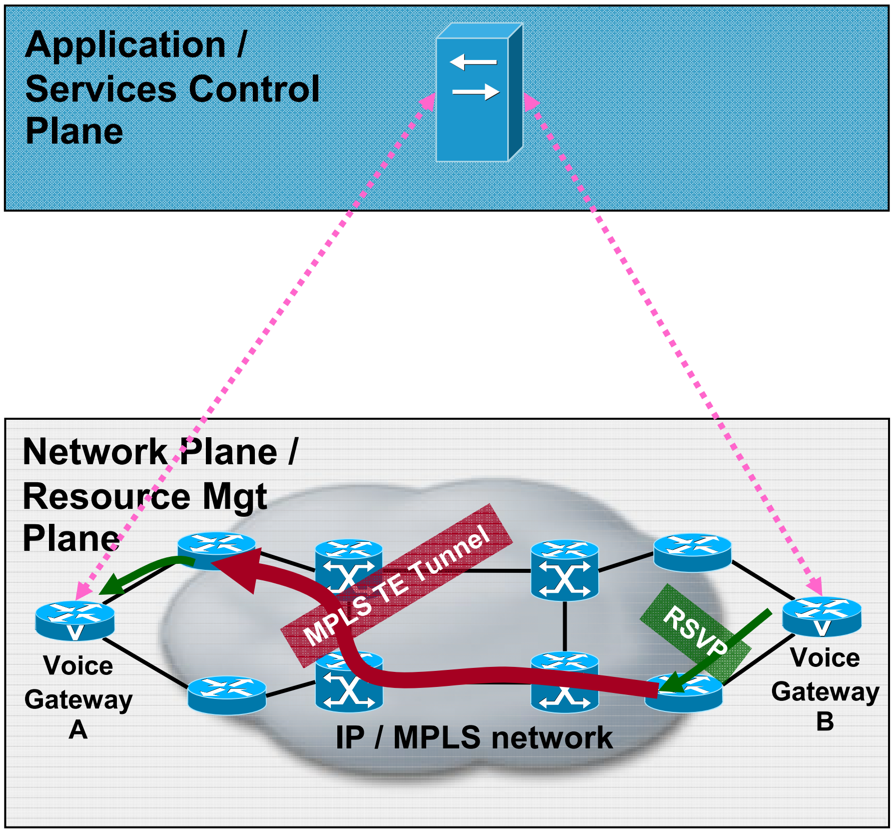


CAC decision:

- On-path, i.e. distributed on routers at each hop of flow path
- Based on actual network and actual routing
- For example:
  - •End-system uses RSVP signaling to request reservation
  - •Routers do RSVP processing (only at IP hops where there could be congestion)

On-Path RSVP CAC

- No external device modelling the network
- Resource Management is done by the network itself
- Can be applied to access and core, L3 today (and MPLS in next phase)
- Can be applied to heterogeneous service environments (Voice, Video,…)
- policy control will be integrated (in next phases) through ISG/RSVP integration



Deployment Considerations for IP Enabled MGW

- Resilience
- Call admission control
- Overheads

Voice over IP Encapsulation

G729 packet	RTP	UDP	IP Header
20 bytes	12 bytes	8 bytes	20 bytes

60 bytes

G729 packet	cRTP
20 bytes	2-4 bytes

24 bytes

cRTP reduces voice bandwith requirement by 60%

G.729 no cRTP / no VAD:

(20 + 40) * 8 * 50 = 26.4kbps

G.729 cRTP / no VAD:

(20 + 4) * 8 * 50 = 9.6kbps

***Sampling interval 20ms**

VoIP over MPLS VPN with TE

MPLS/POS	G729 packet	RTP	UDP	IP Header
22 bytes	20 bytes	12 bytes	8 bytes	20 bytes

- 20 byte voice becomes 82 bytes

  82x8x50 = 33kbps

- In an attempt to reduce latency sampling may be 100 times a second

  72x8x100 = 58kbps

Design Consideration for Deploying IP/MPLS Core

- QoS
- Availability and convergence
- ATM enabled RNC/MGW
- IP enabled MGW
- Deployment

Customer Example Vodafone UK

CHALLENGE

- Vodafone UK's legacy infrastructure – consisting of multiple heterogeneous networks – was costly and hindered the company's competitiveness
- The 'One Vodafone' programme provided the impetus for innovation, and Vodafone UK partnered with Cisco Systems to develop a solution

SOLUTION

- The majority of Vodafone UK's legacy networks have been replaced with a single IP Converged Packet Network (CPN)

BUSINESS VALUE

- Vodafone UK is now carrying 3G data and voice services – and other mission critical applications – over the CPN, with 2G voice traffic to be migrated next
- The operating company has halved its time to market – with even greater speed still to come – and reduced related operational costs by 20 per cent

Meet the Experts
Mobility

- Eric Hamel
  Consulting Systems Engineer

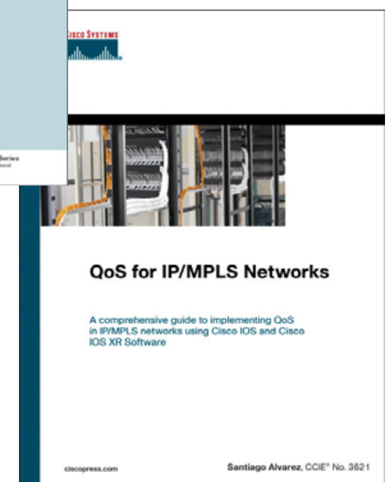
- Gaétan Feige
  Consulting Systems Engineer

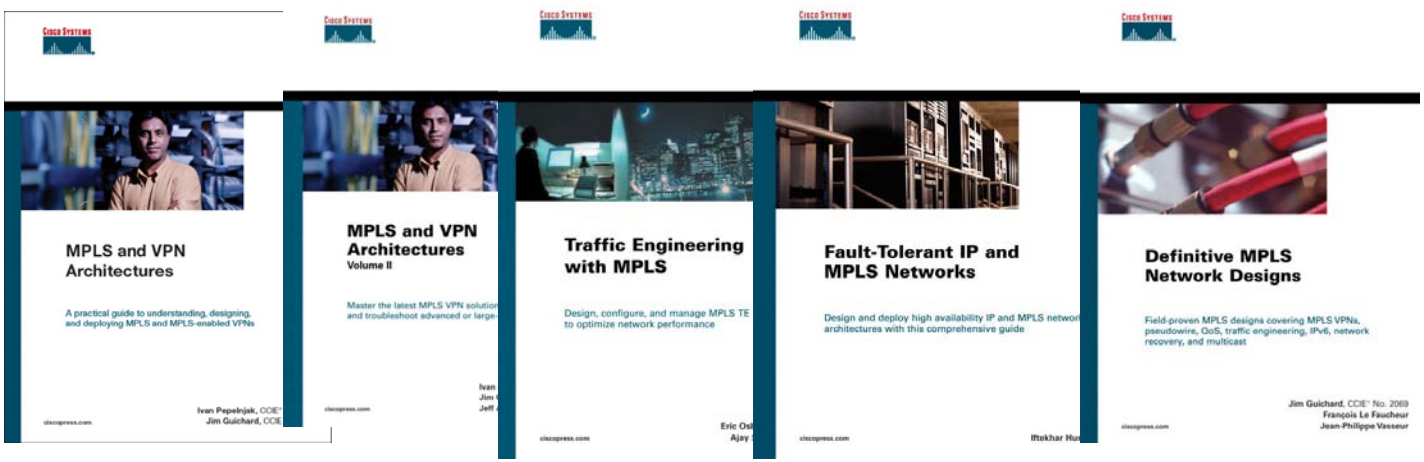
- Marco Centemeri
  Distinguished Systems Engineer

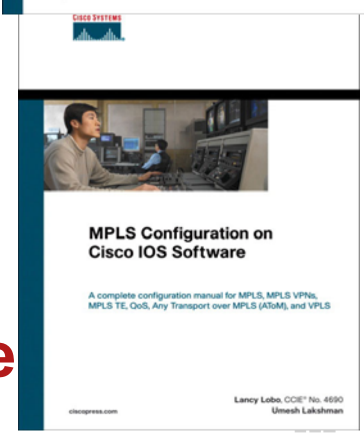
Recommended Reading

BRKMWI -3006

- MPLS and VPN Architectures
- MPLS and VPN Architectures, Volume II
- Traffic Engineering with MPLS
- Fault-Tolerant IP and MPLS Networks
- Definitive MPLS Network Designs
- MPLS Configuration on Cisco IOS Software
- QoS for IP/MPLS Networks
- MPLS and Next-Generation Networks
- MPLS Fundamentals







Available in the Cisco Company Store

Q and A

References

Other Relevant Networkers Sessions

- BRKMWI – 2004 : Bringing IP in the RAN
- BRKBBA – 3012 : Circuit Emulation over Packet Networks
- BRKIPM – 3004 : IGP, BGP, PIM Fast Convergence
- BRKIPM – 3011 : Building Highly Available IP and MPLS Networks

