

The Internet2 Vendor Alliance Committee (VAC)
Presents the first in a series of Informational
briefings...

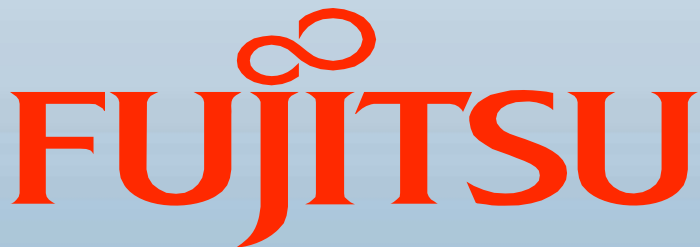
RHCPP Last Mile Access Overview

September 16, 2008

It is our goal to maintain a vendor neutral space for these briefings.
Providing an overview of technology without preference.



Your speakers today come to us from:



AGENDA

Requirements for RHC Networks
Brian Cashman, Internet2

Overview of Leased Line Service and Wireless Options
Eric Strand, Fujitsu

Making Ethernet Carrier Grade
Seth Higgins, ADVA Optical Networking

Understanding Layer 1 and Layer 2 Ethernet Service Transport Options
Dave Parks, Ciena

Security
Eddy Boujaoude, Juniper

Brian Cashman - Moderator

Network Planning Engineer
Internet2

Brian joined Internet2 August 2006. He led the rollout of the Internet2 Observatory. He is also involved in numerous projects including HOPI, VINI and several National Science Foundation funded projects including 100x100 and UltraLight. Previously he served as Manager of Backbone Engineering for Merit Network; responsibilities included capacity planning and network design. Brian spent 21 years at the University of Michigan as Manager of Network Hardware Engineering. He has served as NSF Proposal Reviewer; member of Accredited Standards Committee ANSI X3T9.5 (X3T12), the standards committee that developed the FDDI standard; and technical representative to the ATM Forum. And although he can legitimately sign the same autograph, Brian was never the General Manager of the NY Yankees.



Requirements for Rural Health Care Networks

Technology Saves Lives!

- Mortality rates are 7.2 %
LOWER in the “most wired”
hospitals (refer to notes for context)

*(Source :Hospitals and Health
Networks magazine (H&HN) 2005
Study)*



What networking challenges do our healthcare customers face?

- Inconsistency and difficulty of planning future bandwidth and network demands
- Escalating costs of network connectivity for extending and networking storage applications
- Increased management and maintenance costs
 - Lack of flexibility in their network platforms
- High amounts of network latency jeopardizing application performance

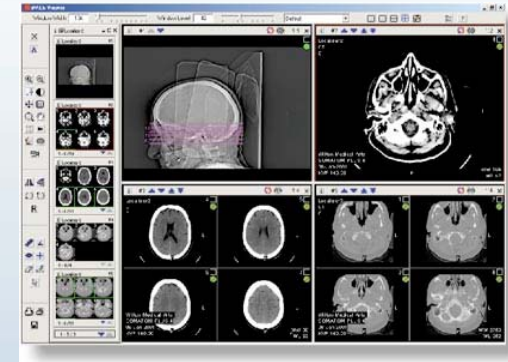
Patient Data Back up and Disk Mirror over a Private Network

Business problems

- Increase in EMR and EHR implementations are driving exponential storage traffic
- Compliance requirements are driving the need for flawless storage solutions
- High availability and reliability are necessities and not simply “nice to haves”
- Bandwidth demand growth is unpredictable
- Provisioning times for new services and bandwidth are long and cumbersome to implement

Applications Driving Bandwidth and Storage Demands

- PACS / Mammography example:
 - Patient population of 10,000 women = ~ 12 TB of data
 - 75 MB digital images
 - 4 images per scan → 500 MB moving to 1 GB
 - Typical screening centers scan 100 patients per day
 - **Database grows 30 - 100 GB per day**
 - Average of 16 images per patient → 1.2 GB of data (16 * 75 MB)
 - Average woman will be having her fourth scan
 - 3 previous screening sessions' worth of data (plus any other investigative data)
 - Physician needs to see single 16-image patient record within 30 seconds
 - ~20 Gbps for remote physician screening



Bandwidth and Storage Driving Applications

- **EMR / EHR**
- **Patient Tracking and management**
- **Asset Tracking and management**
- **Tele – Presence / Remote Video**
- **Remote Diagnosis**
- **BC / DR**
- **High Availability**

What are Healthcare Providers Considering when Designing their networks?

- Cost
 - Must meet Budget Constraints
 - Often bandwidth make up >70% of the project cost
- Performance
 - Minimal Impact on the Application with a High Throughput, Low Latency, and Rapid Restore Times

Sustainability and Future-proofing

- Intelligent utilization of network
- Flexible support for all applications and data types (Storage, Voice, Data, Video)
- Low management and maintenance cost over time

High Availability and Security

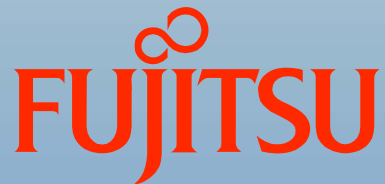
- Five 9's, with the Ability to Monitor/Report/Protect to Maximize Performance and Perform Rapid Fault Isolation
- Guaranteed Isolation of Sensitive Data
- Guaranteed Data Delivery

Eric Strand

Manager, Sales Engineering Group



Eric Strand manages the Sales Engineering Group at Fujitsu Network Communications in Richardson, TX. Eric has an excellent knowledge background in optical networking and has been heavily involved in building and operating high speed fiber networks since 1994. Eric has also worked for multiple large ILEC carriers, that add to his knowledge and experience from both a solution provider and user prospective.



Leased Line Services

Access Decisions

Several factors influence access technologies:

- Current and future bandwidth needs
- Rural / Metropolitan environment
- Availability of Transmission Media
- \$\$\$

Items to consider:

- Protection
- Reliability
- Security
- Scalability

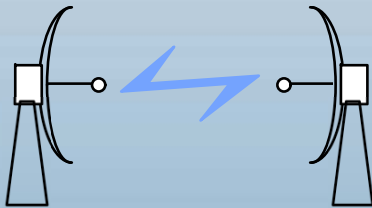


Access Transmission Media



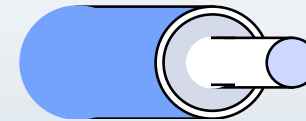
Twisted Pair

1 to 10 megabits/sec
1-10 kilometers



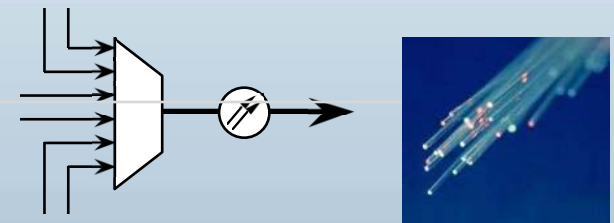
Microwave Radio Technologies

-100 megabits/sec
10-100 kilometers



Coaxial Cable

-100 megabits/sec
1-10 kilometers



Fiber Optic Transmission Systems

Multimode: -100 megabits/sec
Singlemode: 10,000+ megabits/sec per wavelength
CWDM (Coarse Wave Division Multiplexing)
DWDM (Dense Wave Division Multiplexing)
100+ kilometers

Leased Lines

Traditional SONET Multiplexing

Carriers offer many options:

- Voice
- Data (internet / VPN / etc.)
- Combination

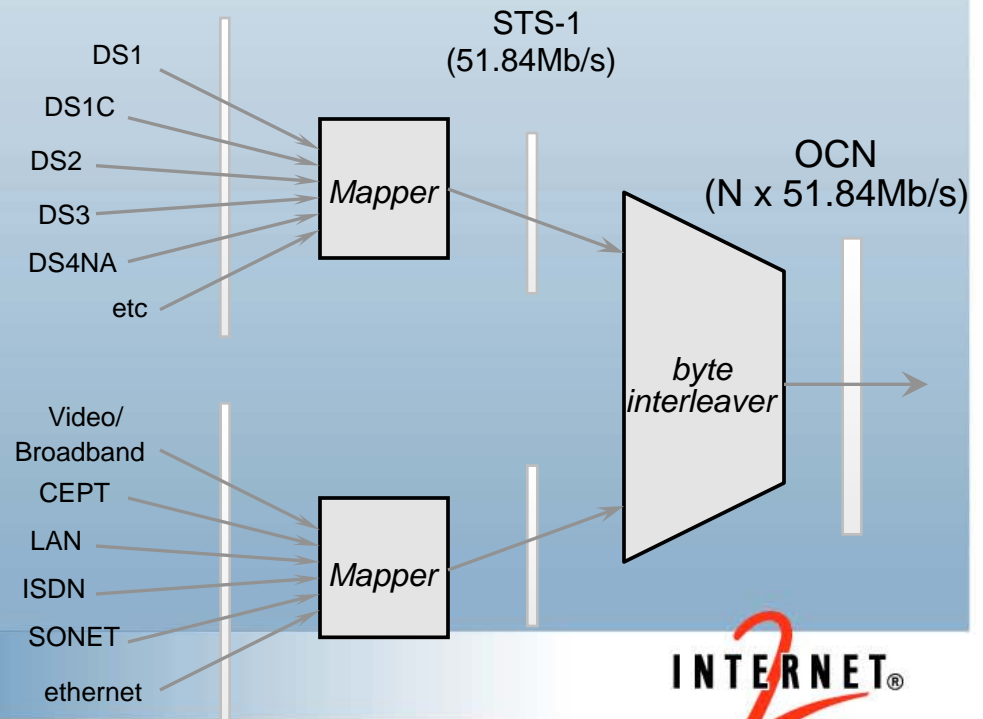
Access Speed Choices:

- T1 (1.5 megabits/second)
- Fractional T3
- T3 (45 megabits/second)
- Fast Ethernet (100 megabits/second)
- OC3 (155 megabits/second)
- OC12 (622 megabits/second)
- GigE (1,000 megabits/second)
- WDM
- OC48
- 10 gigabit Ethernet

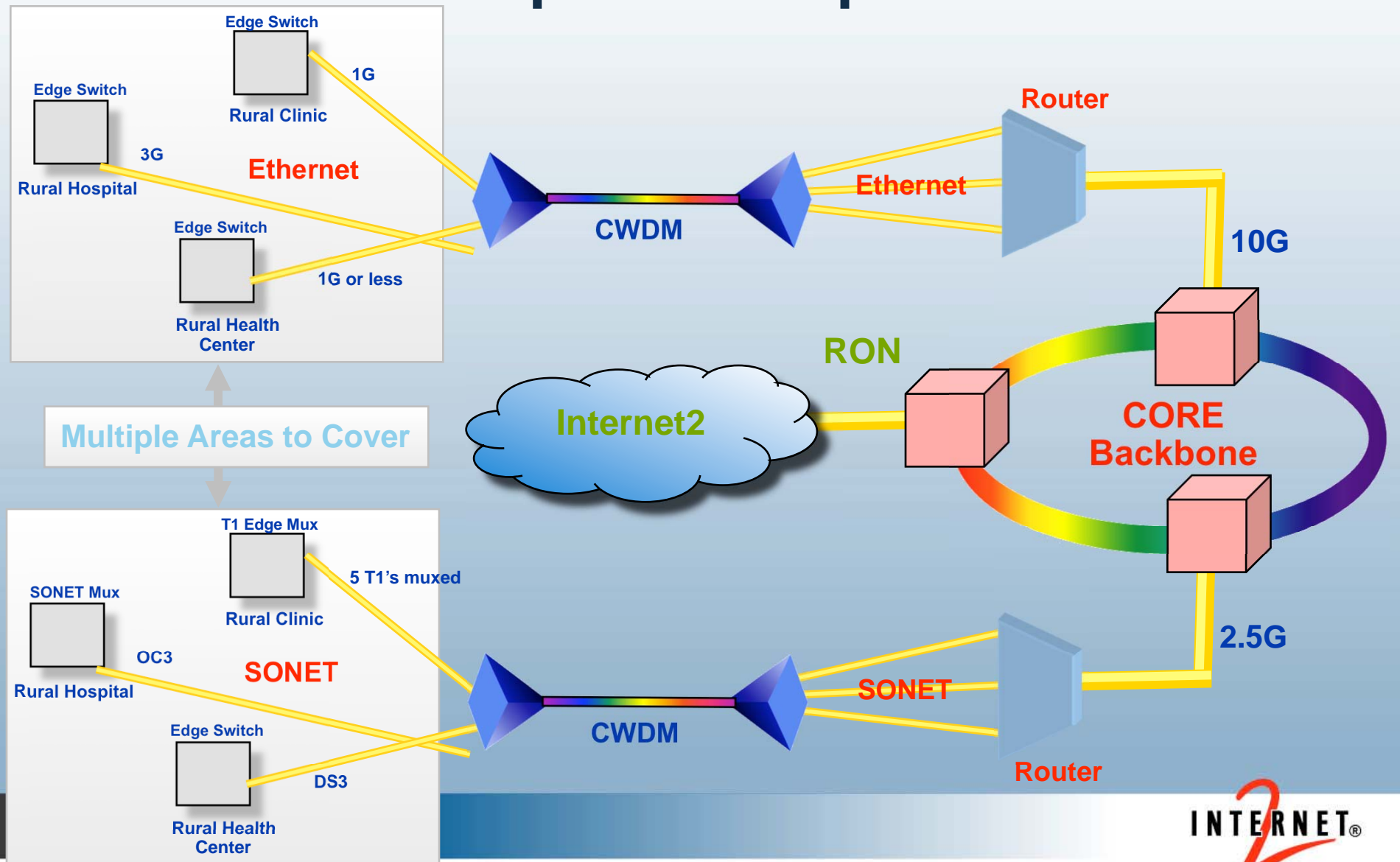
Key: not every option available at every site!

Digital signaling rates	
DS0	64 Kb/s
DS1	1.544 Mb/s
DS3	44.736 Mb/s

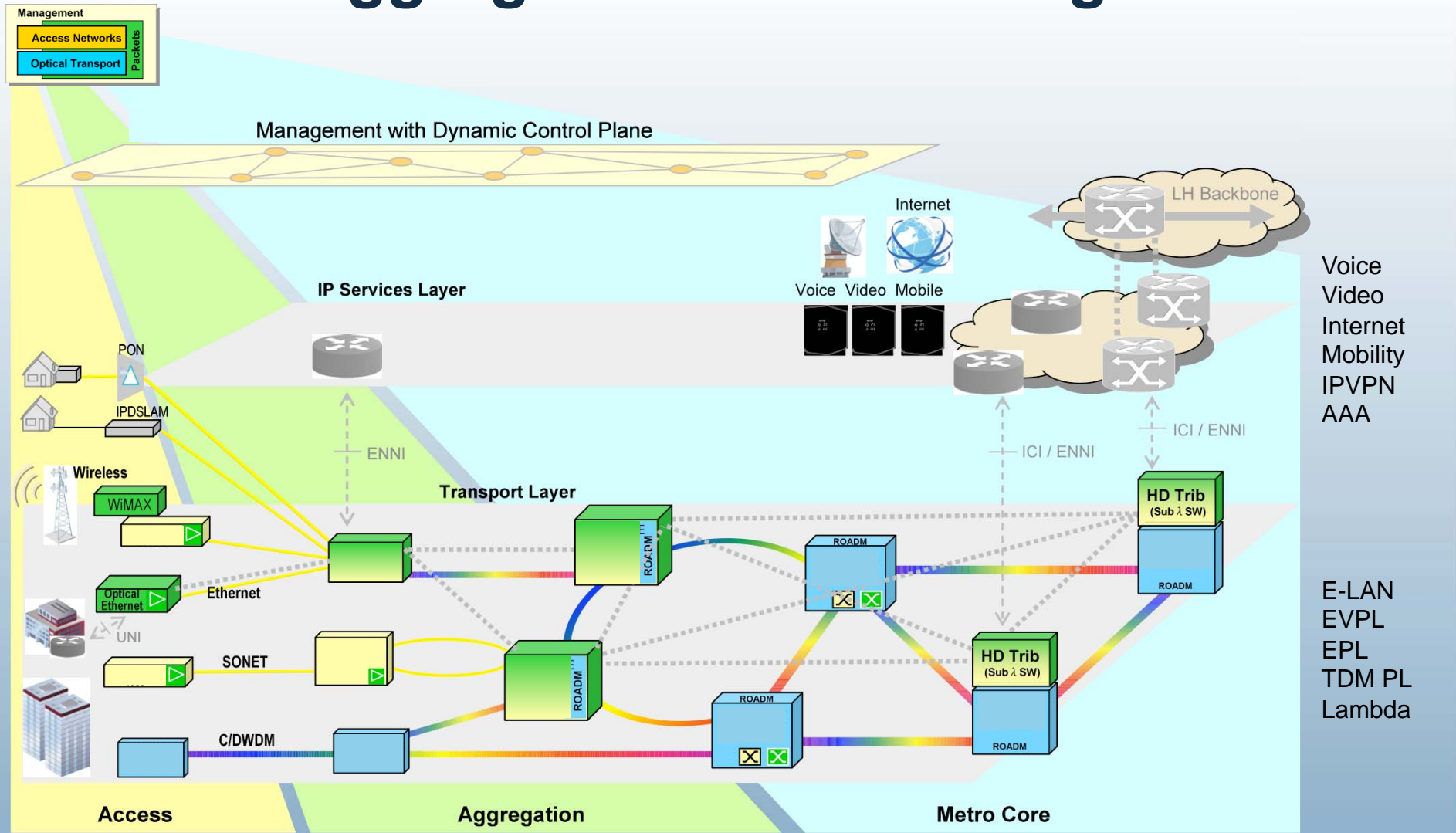
Standard Line Rates	
OC1	51.84Mb/s
OC3	155.52Mb/s
OC9	466.56Mb/s
OC12	622.08Mb/s
OC18	933.12Mb/s
OC24	1244.16Mb/s
OC36	1866.24Mb/s
OC48	2488.32Mb/s



RHCPP Transport Example



Access / Aggregation / Core / Long Haul



Voice
Video
Internet
Mobility
IPVPN
AAA

E-LAN
EVPL
EPL
TDM PL
Lambda

Access
Broadband packet services over *diverse access media* with *Ethernet* as the dominant interface

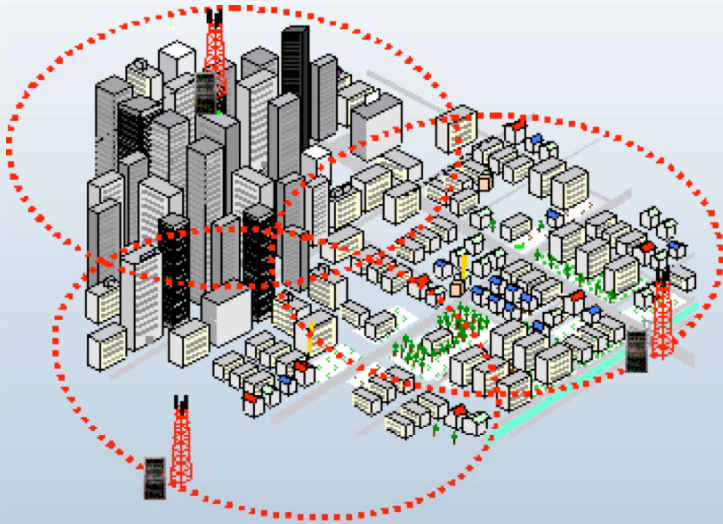
Packet
Packet optimized aggregation and *transport* leveraging connection oriented technologies for OAM, QoS, and scalability

Optical
Convergence on WDM layer with unrestricted grooming, integrated circuit and packet switching, at 40G - 100G

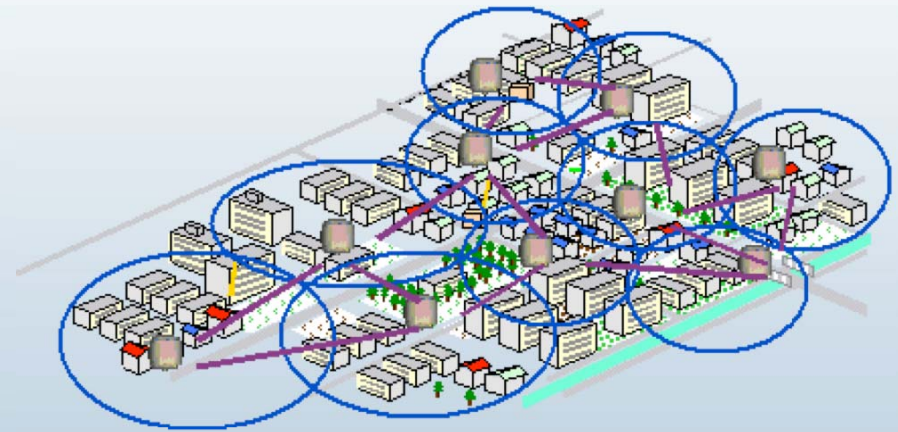


Wireless Options

Wireless Access Options



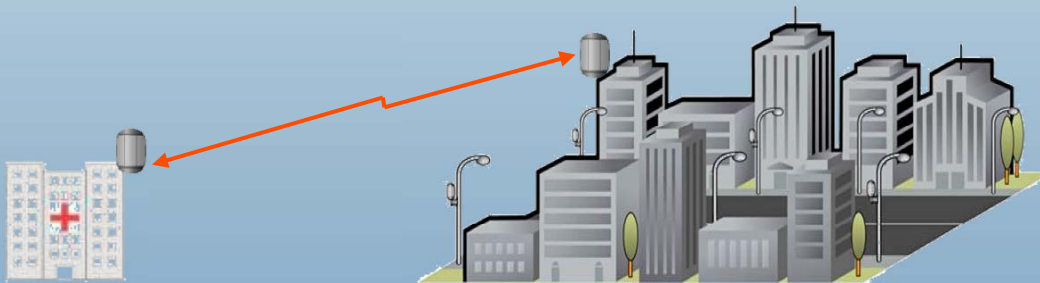
WiMAX



WiFi MESH

Items to consider:

- Line of Sight
- Bandwidth
- Distance
- These technologies are complementary

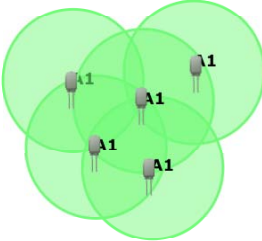
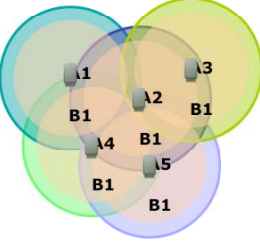
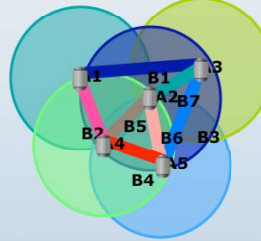
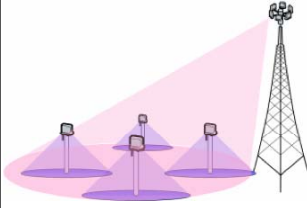


Point to Point

Frequency Strategies

Frequency (GHz)	Technology	Comments
2.4	WiFi	Public
5.1-5.8		
4.9		
2.3	WiMAX	WCS
2.5		PCS
3.5		Global/US Military
3.65		Global
4.9		Municipal/Public Safety
5.8		Public

Wireless Access Solutions

	Single Radio	Dual Radio	Multi Radio	WiMAX/Wi-Fi
Technology				
Capacity per access point	2-6Mbps	5-10Mbps	20-25Mbps	Variable
Capacity per sq mile	5-15Mbps	12-25Mbps	100-400Mbps	18-35Mbps
Voice	Very Limited	Limited	Yes	Yes
Video	Very Limited	Limited	Yes	Yes
TDM	No	No	Yes	Yes
Egress types	Ethernet Fiber DOCSIS	Ethernet Fiber DOCSIS	Ethernet Fiber DOCSIS	Ethernet Fiber

Seth Higgins

Sr. Dir. Ethernet Access Technical Strategy
ADVA Optical Networking, N.A.



Responsible for strategic and technical direction of ADVA Optical Networking's Ethernet solutions for carrier and enterprise customers throughout North America. Focus on Layer-2 service delivery and transport convergence for efficient and reliable Ethernet connectivity.

Prior to ADVA Optical Networking, Seth worked at Cisco Systems in worldwide service provider technical operations, fostering communications between customers and product development related to metro Ethernet, IP+Optical and IPTV quad-play applications. Beforehand, Seth worked at Sprint designing and troubleshooting data services including Frame Relay, ATM and IP-VPN for large businesses.

Making Ethernet Carrier-Grade

- Solutions for monitoring and testing
- Ethernet service verification primer

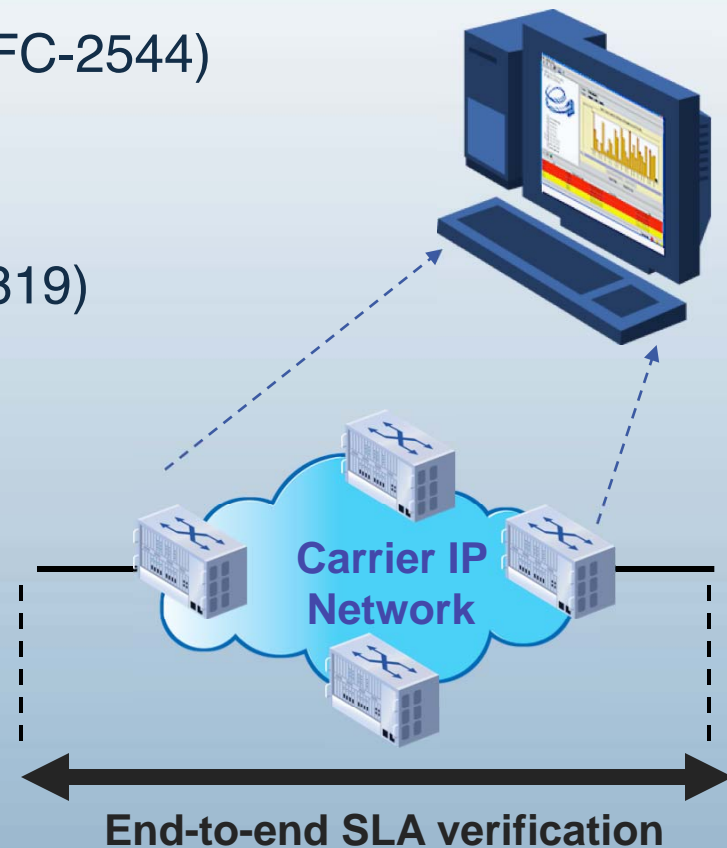
Frame Relay set the bar

- Connectivity similar to private line, plus...
 - Service multiplexing
 - Oversubscription with CIR/EIR profiles
- Service Level Agreement: delay and packet loss
- Combination of packet and TDM techniques
 - Loop demarc and inject BERT traffic
 - Automated PVC routing with delay and hop metrics
 - Top fixes: check CPE configuration, bounce the PVC, BERT test



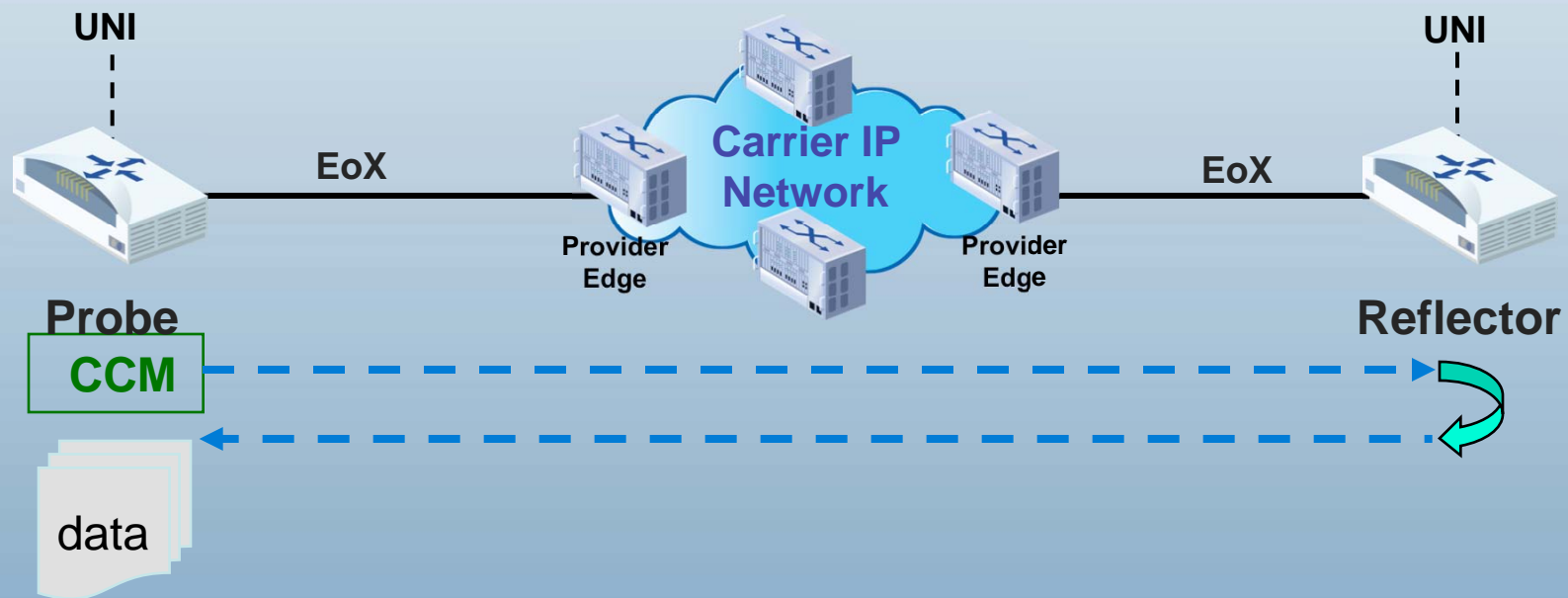
Carrier-grade Necessities

- Loopback and traffic generation (RFC-2544)
 - Turn-up and acceptance
 - Troubleshooting
- Statistical counters (RMON RFC-2819)
 - Packet and byte counts
 - Utilization
 - Errors
- Alarms and Thresholds
 - Fault detection
 - SLA violation
- Network Management System
 - Collect and store Key Performance Indicators
 - EMS provides data to OSS for visualization



SLA Verification

- Service Assurance (frame loss, delay and jitter)
 - Send synthetic frames on EVC path at negligible rate
 - IP-based or 802.1ag/Y.1731



Dave Parks

Director of Solutions Packet Products Portfolio



Director of Solutions for Ciena's Packet Products Portfolio. This includes positioning Ciena's Carrier Ethernet service switching and packet optical networking solutions to meet customer network requirements. Dave is also the Marketing Committee Chairman for the IP/MPLS Forum.

Before Ciena, Dave was a senior analyst with the Yankee Group covering enterprise Ethernet and IP VPN network services and market trends. Before Yankee, Dave supported product management and marketing for Lucent Technologies and Ascend /Cascade Communications.

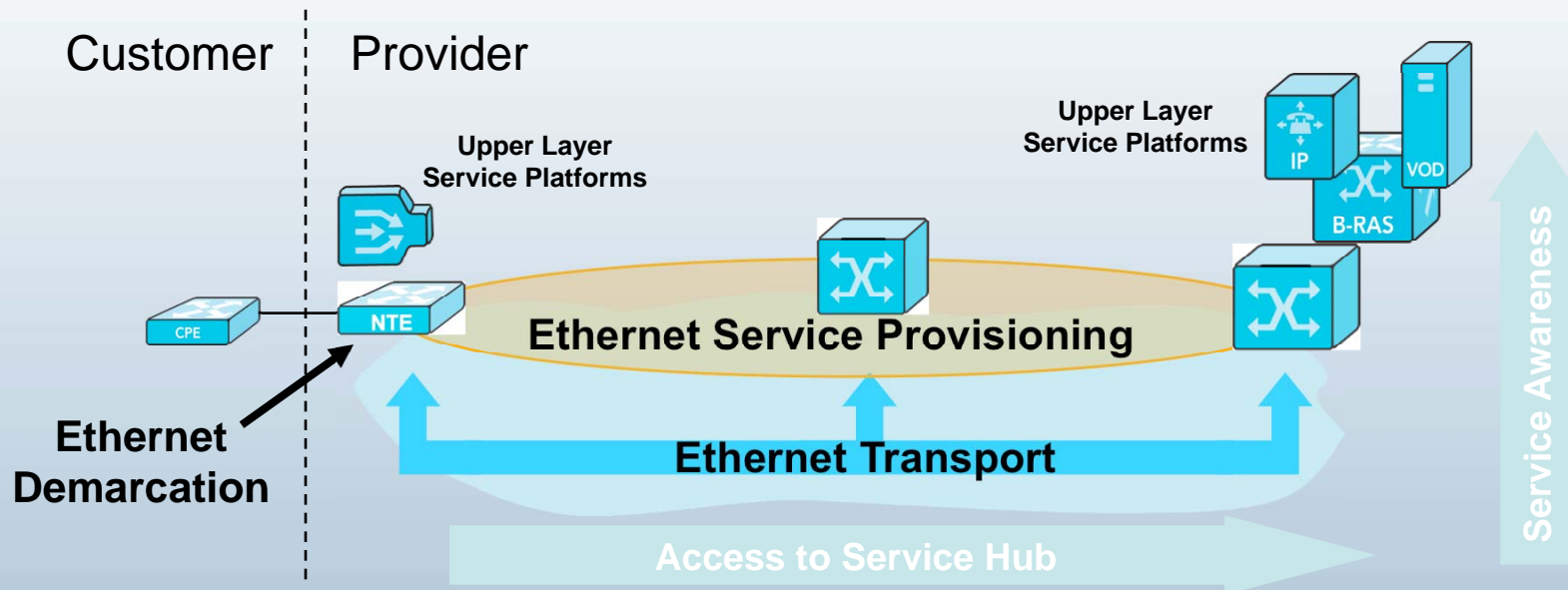


Understanding Layer 1 and Layer 2 Ethernet Service Transport Options

Agenda

- Ethernet-based service transport requirements in metro & access
- Ethernet service transport options in the market today
 - Deterministic Ethernet options in metro & access
 - Ethernet transport at Layer 1
 - Ethernet transport at Layer 2/2.5

Segmenting the Ethernet functions



Three identifiable functions comprise a full Ethernet solution

- Ethernet Demarcation: The Provider Edge. Entry point to carrier Ethernet network.
- Ethernet Transport: Deterministic aggregation and forwarding of packet flows amongst demarcation and service elements
- Ethernet Service Provisioning: Service creation point (e.g. for MEF E-LINE & E-LAN), per-user treatments

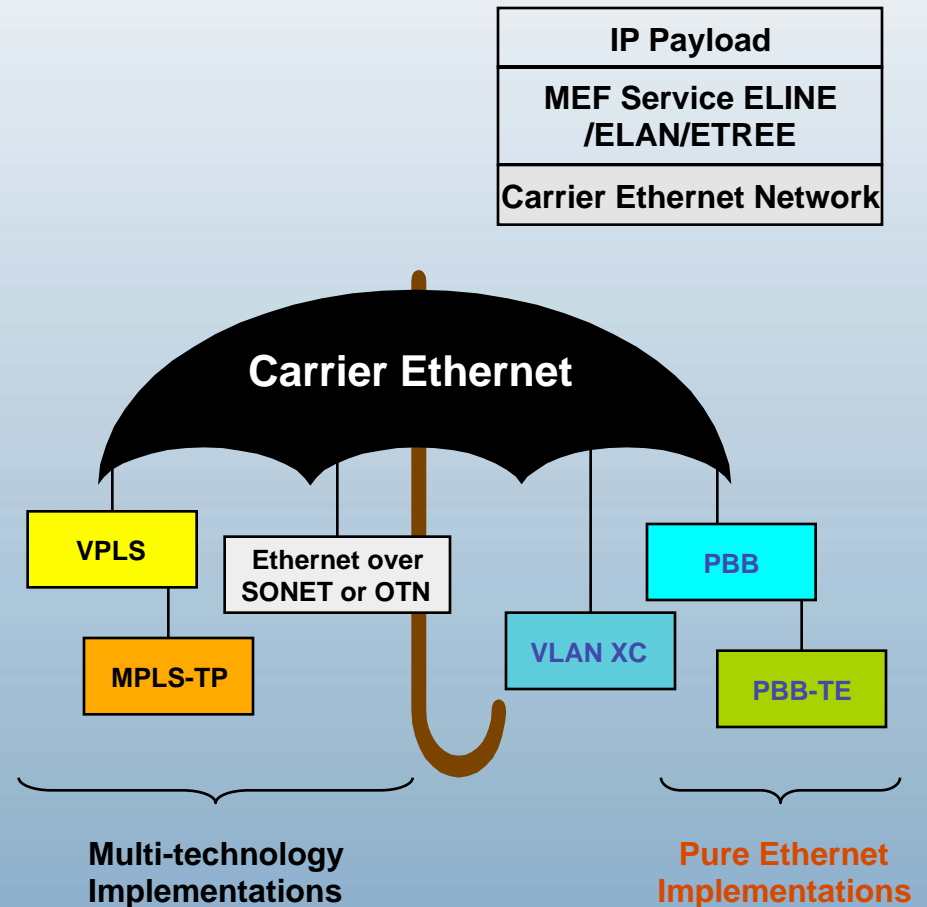
Evaluating Ethernet-based service transport requirements in metro & access

Critical Aspects	Business Services
Services Portfolio Evolution	L1, L2, L3 (v)pns to Managed Services, BC/DR, hosting, web services, etc.
Service Topology	Pt-Pt: Yes Pt-Mpt: Yes Mpt: Yes
Transparency	Yes. L1 vs L2 vs L3 (V)PNs
Scalability	100+ endpoints per VPN 1000+ of customers
QoS	Multiple CoS per customer with strict priority queuing SLA
Security	access control
Reliability	50ms protection, 5-nines

Need rich suite of connectivity options with “TE” capable packet transport

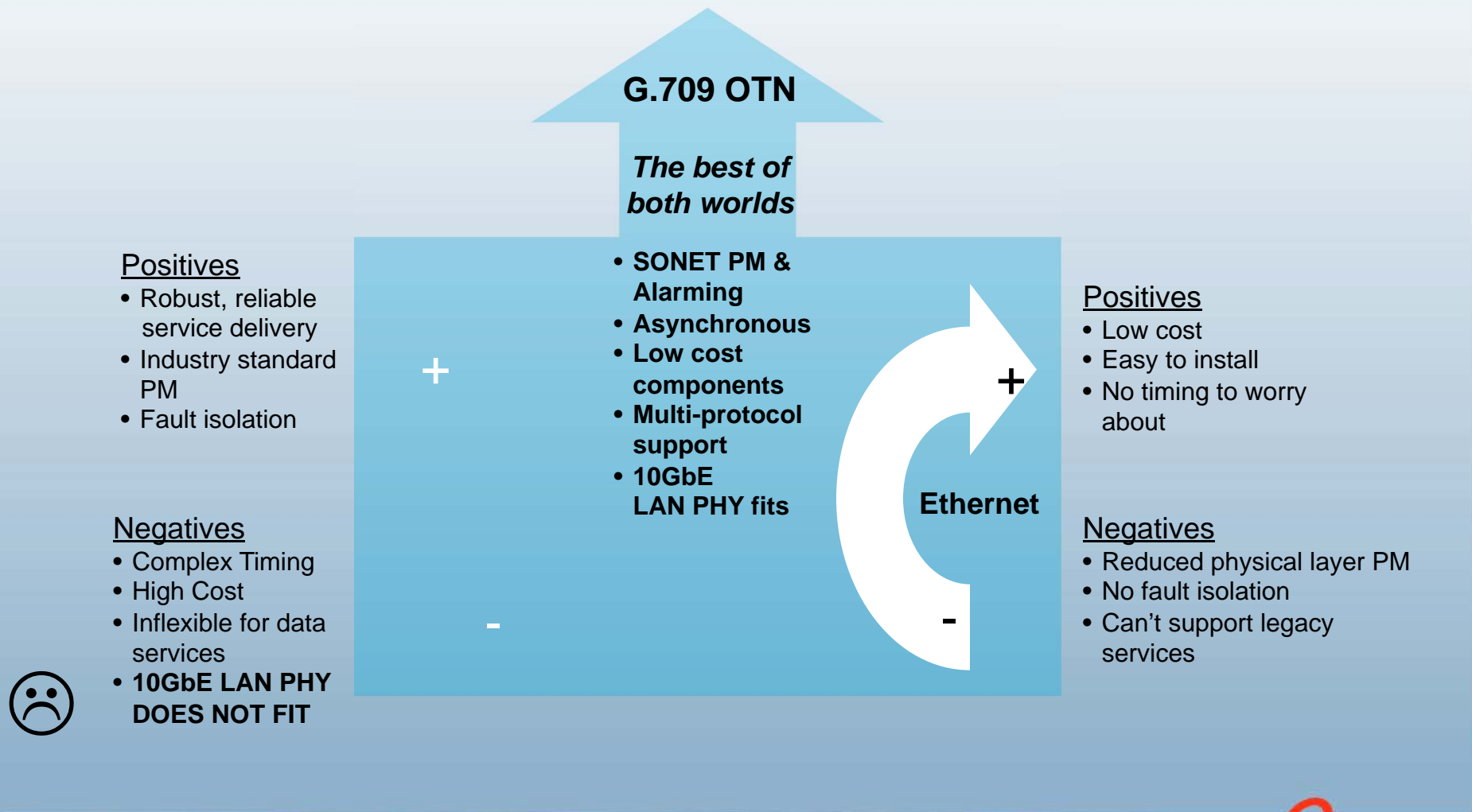
Deterministic Ethernet in metro and access

- Routing, i.e., forward IP packets
 - IP -over- MPLS: 2547 vpns
 - IP -over- IP
 - IP -over- IPSEC, GRE, L2TPv3
- Bridging, i.e., forward Ethernet frames
 - Ethernet -over- Ethernet : PBB
 - Ethernet -over- MPLS: VPLS
- Transport, i.e., switch Ethernet frames
 - Ethernet -over- Ethernet: PBB-TE
 - Ethernet -over- Ethernet: VLAN XC
 - Ethernet -over- MPLS / MPLS-TP
 - Ethernet -over- SONET
 - Ethernet -over- OTN



Deterministic Ethernet Transport at Layer 1

Ethernet over OTN G.709 encapsulation for multi-service transport



Ethernet Transport at Layer 2 & 2.5:

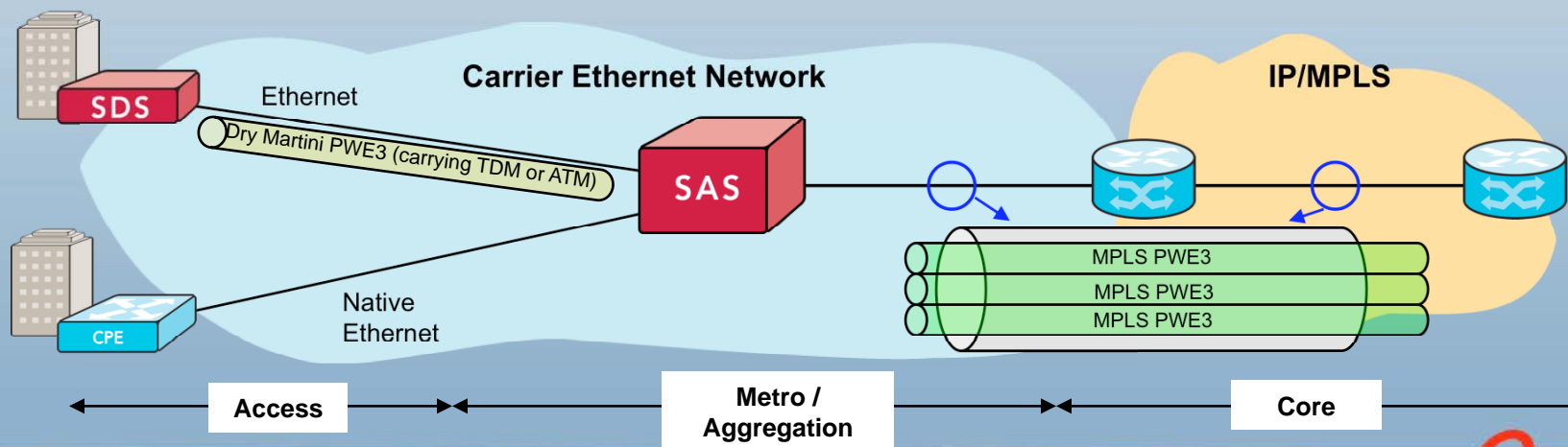
Approaches to achieving connection-oriented Ethernet

- VLAN Cross-Connects
 - Explicit forwarding paths using VLAN based classification. Tunneling via VLAN tag encapsulations and translations
- Provider Backbone Bridging (PBB-TE)
 - Explicitly forwarding paths using MAC + VLAN tag. Tunneling via MAC-in-MAC encapsulations. Being defined by IEEE
- MPLS & VPLS
 - Widely deployed in the core, less so in the metro / access. Uses pseudo wire emulation edge-to-edge (PWE3) for Ethernet and multiservice tunneling over IP/MPLS. Can be point-to-point or multi-point (VPLS)
- MPLS-TP
 - Formerly know as T-MPLS (defined by ITU-T). New working group formed in IETF now called MPLS-TP. Transport-centric version of MPLS for carrying Ethernet services based on PWE3 and LSP constructs

Pseudowires (PWE3) and VPLS

Layer 2 Transport over IP/MPLS

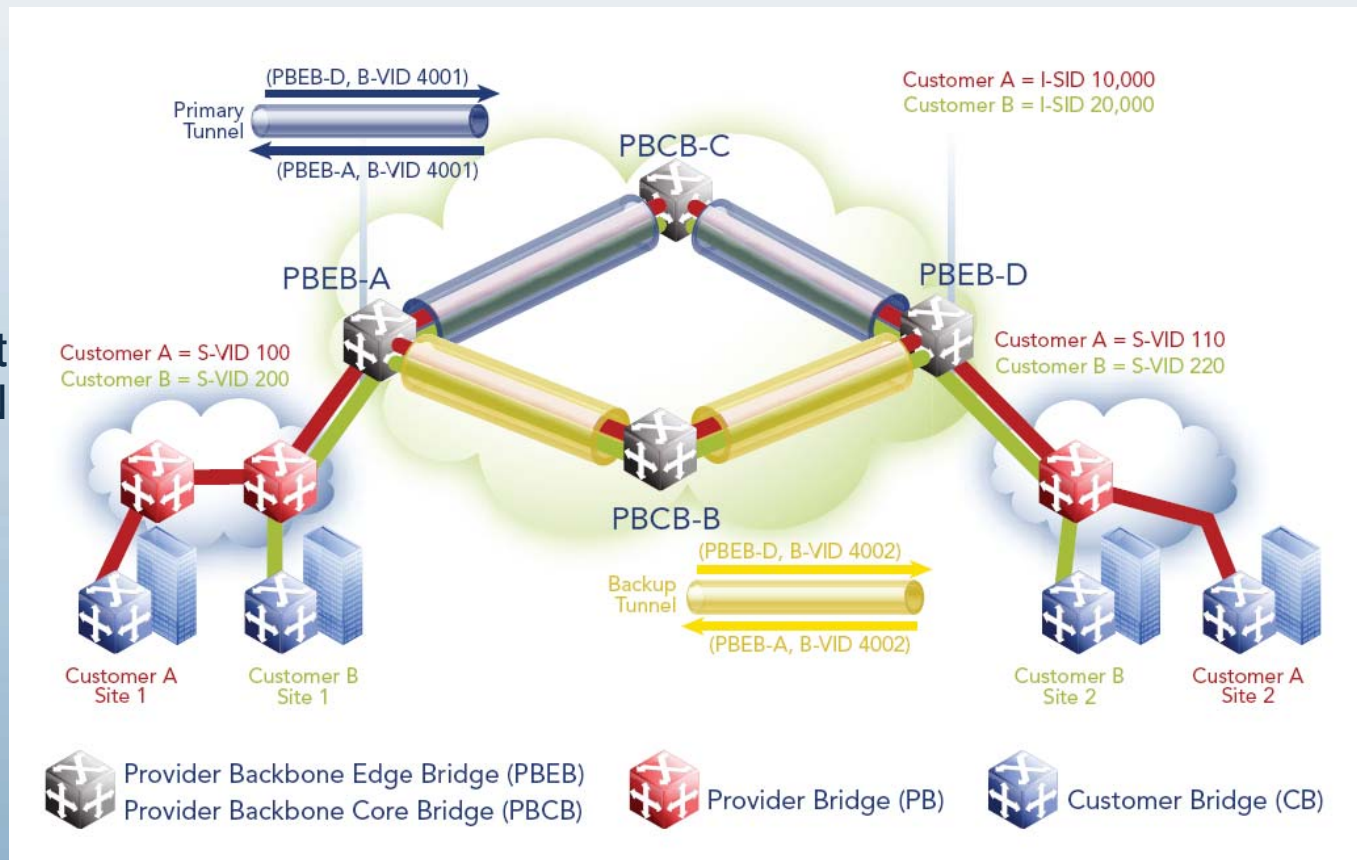
- Emulates attributes of non-IP services across IP or Ethernet network
- Adapts and transparently carries Layer 1 and Layer 2 services across a packet network
- Brings Virtual Circuit (VC) or connection-oriented services to IP/Ethernet
- Defined by the IETF
- Point-point and multi-point (VPLS) capabilities
- Non-MPLS, statically provision option using “Dry Martini” pseudowires



Provider Backbone Bridging – TE (PBB-TE)

Layer 2 Transport over Carrier Ethernet

- Addresses Carrier Ethernet limitations in scalability and reliability
- Uses point-to-point tunnels for L2VPN transport over Ethernet
- Provides traffic engineering for efficient capacity utilization
- Being defined by IEEE 802.1Qay



Conclusion

- Carrier Ethernet services require connection-oriented transport options for deterministic behavior and added scalability and reliability
- Multiple technologies and approaches for Ethernet Transport
- One size does not fit (or is available to) all and therefore a toolkit of transport options is ideal

Eddy Boujaoude

Director, Systems Engineering



Eddy Boujaoude is a Systems Engineering Director with Juniper Networks. He manages a team of 40 engineers, architects and specialists in the central United States. With over 18 years of experience, he has held several technical and managerial positions with end users and vendors in the networking and security industry. Eddy graduated with a Masters degree in Electrical Engineering from Oklahoma State University in 1992.



Agenda

- IPSec VPN
- Branch Survivability
- UTM

Branch Office Deployment Scenarios

Branch Office Type A – Basic

Single device, Single Internet Connection

Branch Office Type B – Optimized

Single device, connected to Internet and to Private WAN

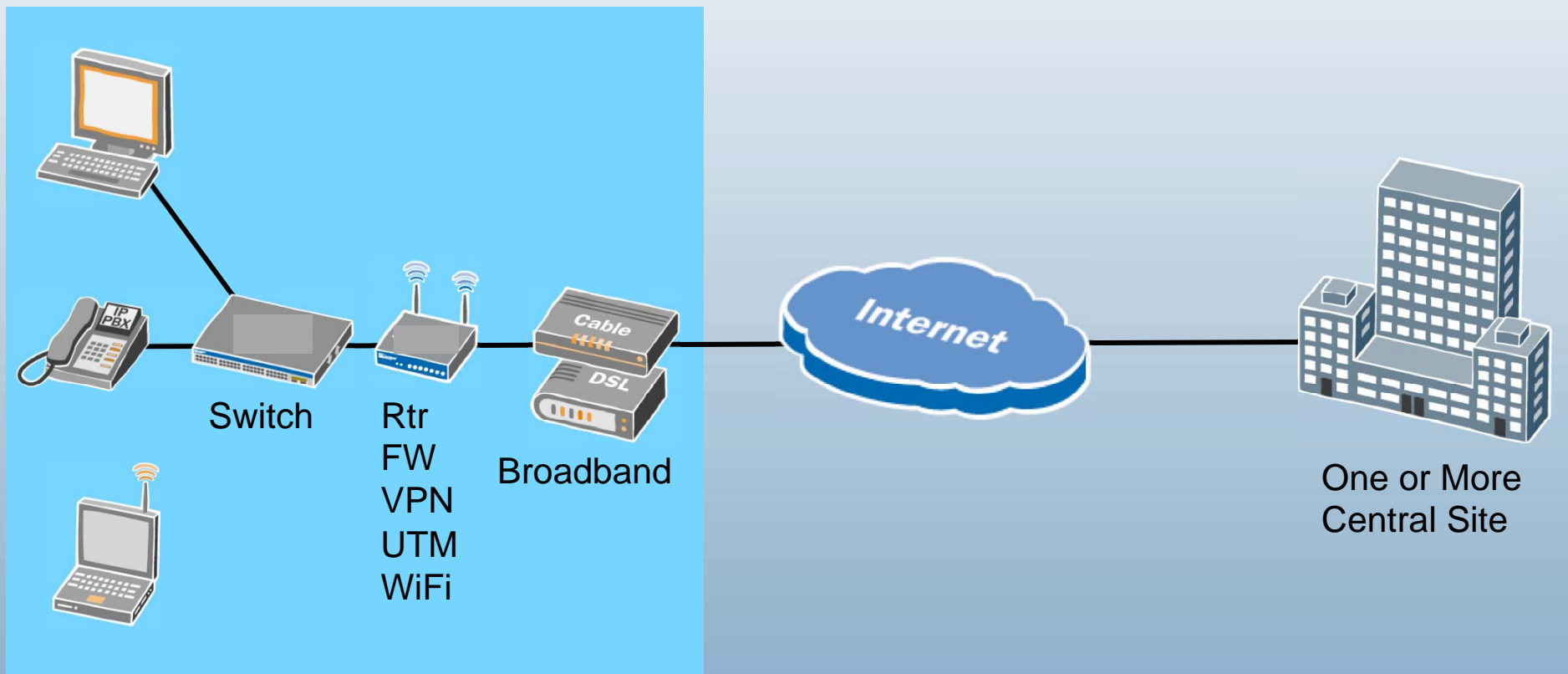
Branch Office Type C – Critical

Two devices, dual connections to Internet and Private WAN

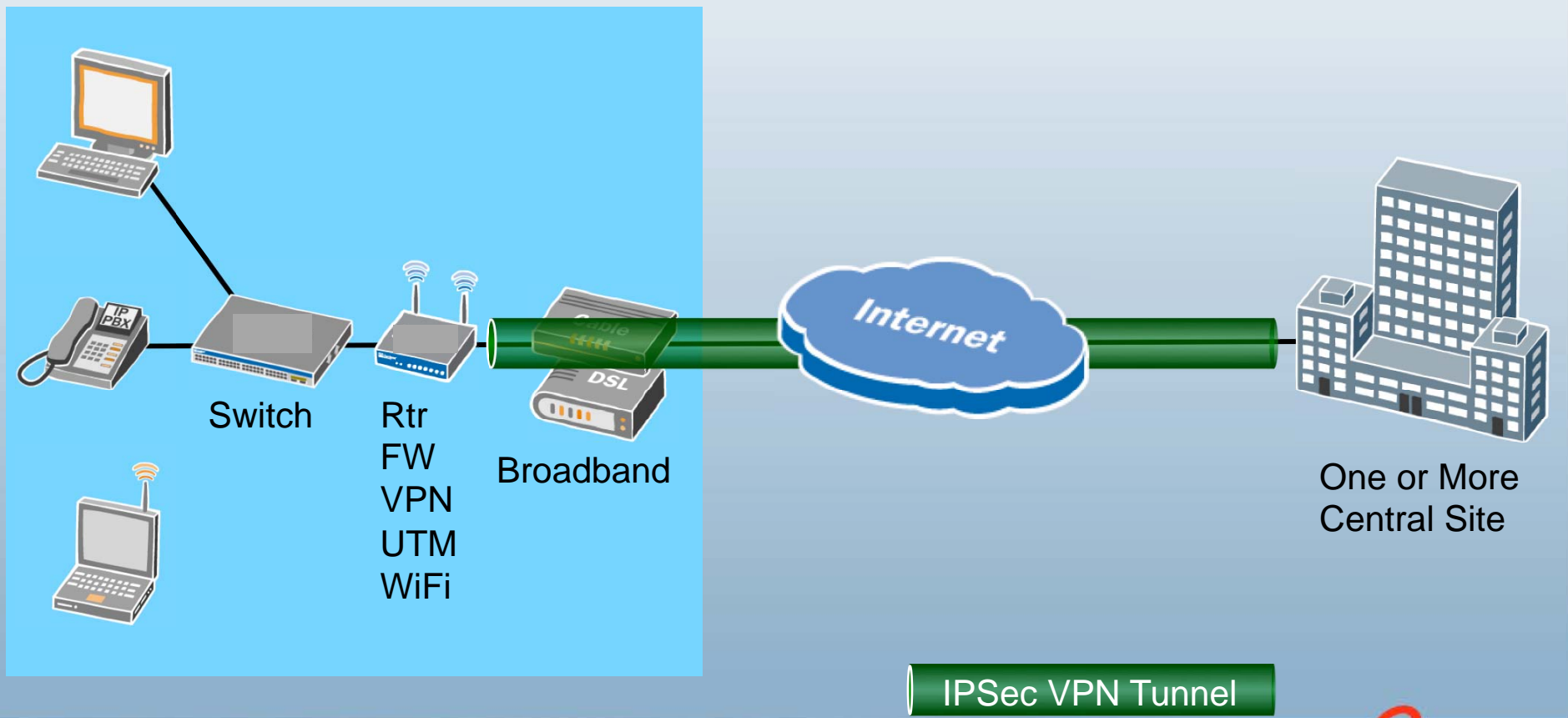
Branch Office Profiles

	Feature	Capability	Type A Basic	Type B Optimized	Type C Critical
Security	Unified Threat Management (UTM)	Deep Inspection	✓	✓	✓
		Anti-Virus	✓	✓	✓
		Web Filtering	✓	✓	✓
		Firewall	✓	✓	✓
Connectivity	Wide Area Network (WAN)	T1/E1	--	✓	✓
		MPLS	--	--	✓
		Broadband	✓	✓	✓
	LAN	Wired	✓	✓	✓
		Wireless	Optional	Optional	✓
High Availability	Redundancy	Device Redundancy	--	--	✓
		Link Redundancy	--	✓	✓
Performance Optimization	WAN Acceleration	WAN acceleration and Optimization	--	--	✓

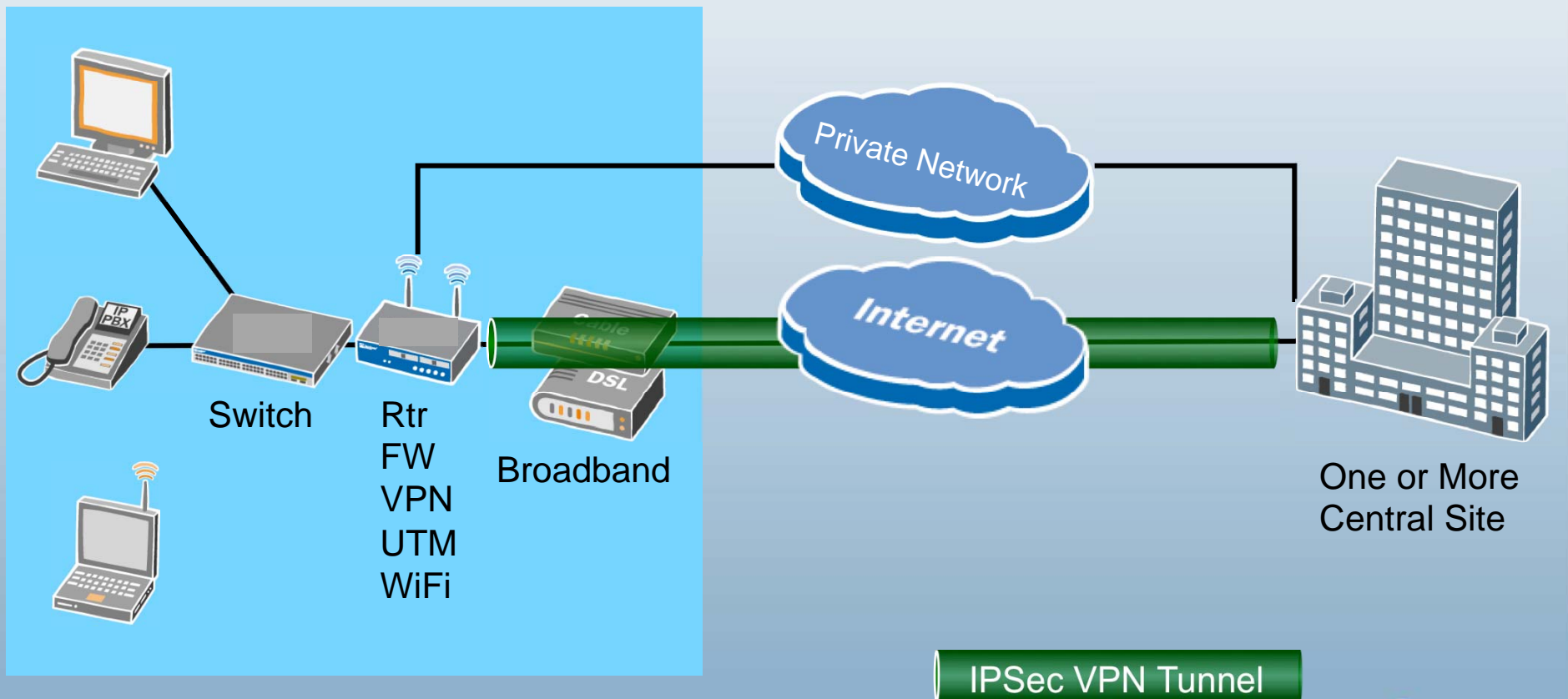
Branch Office Type A – Basic



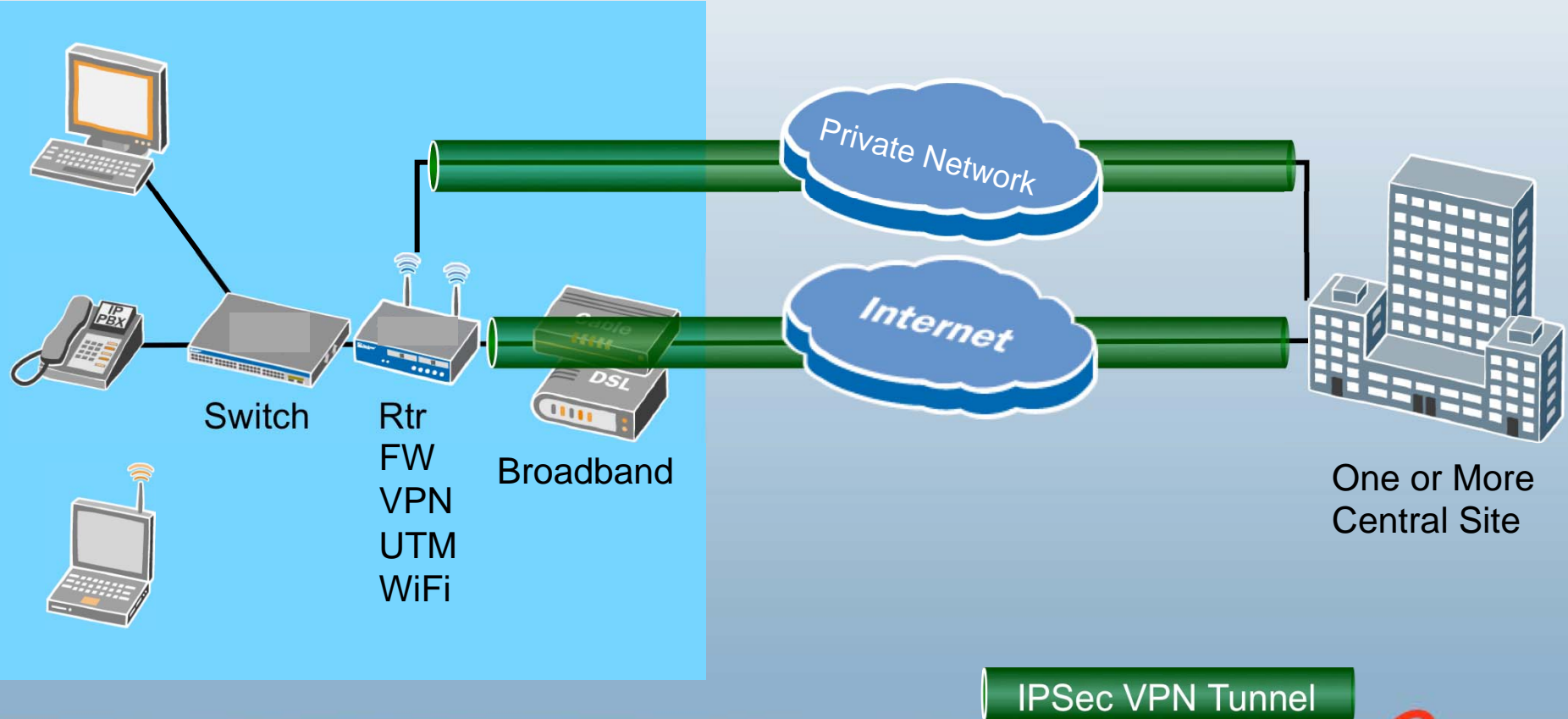
Branch Office Type A – Basic



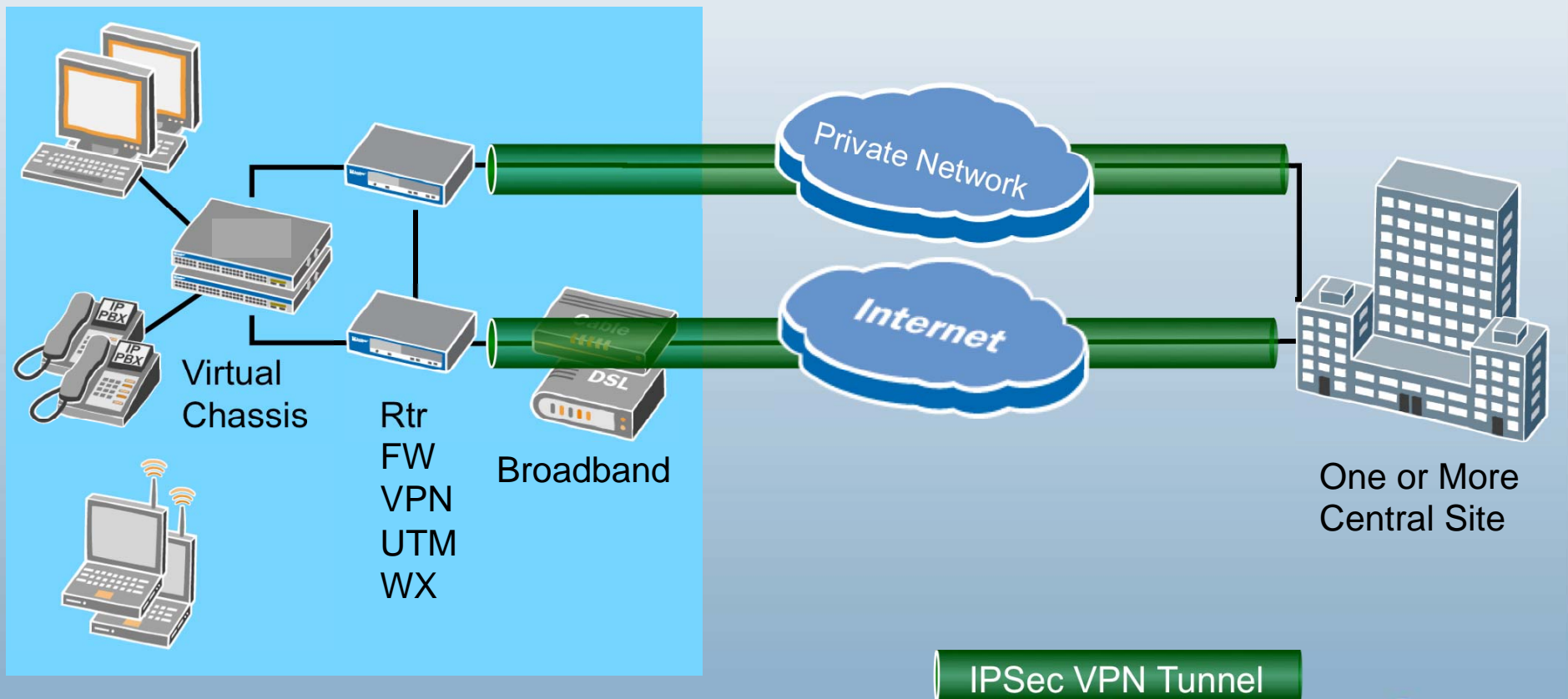
Branch Office Type B – Optimized



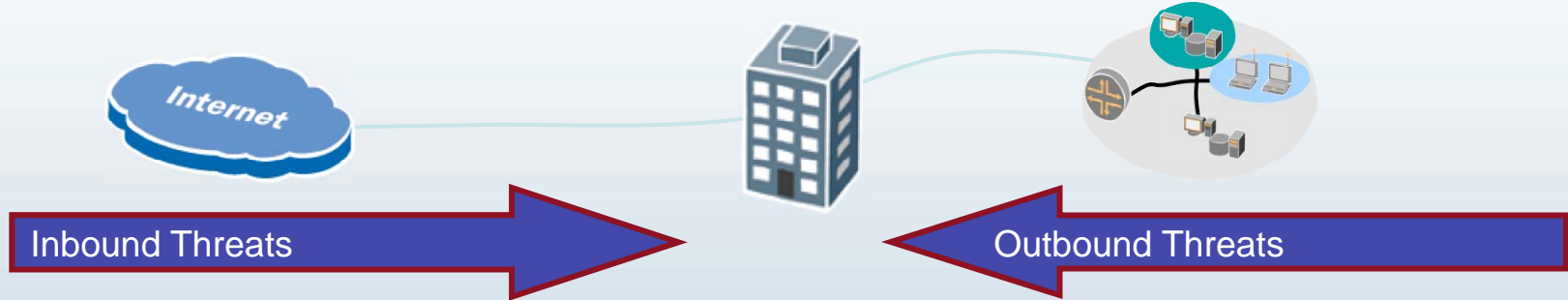
Branch Office Type B – Optimized

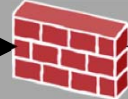
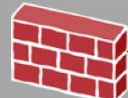
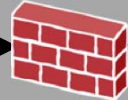
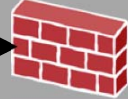



Branch Office Type C – Critical



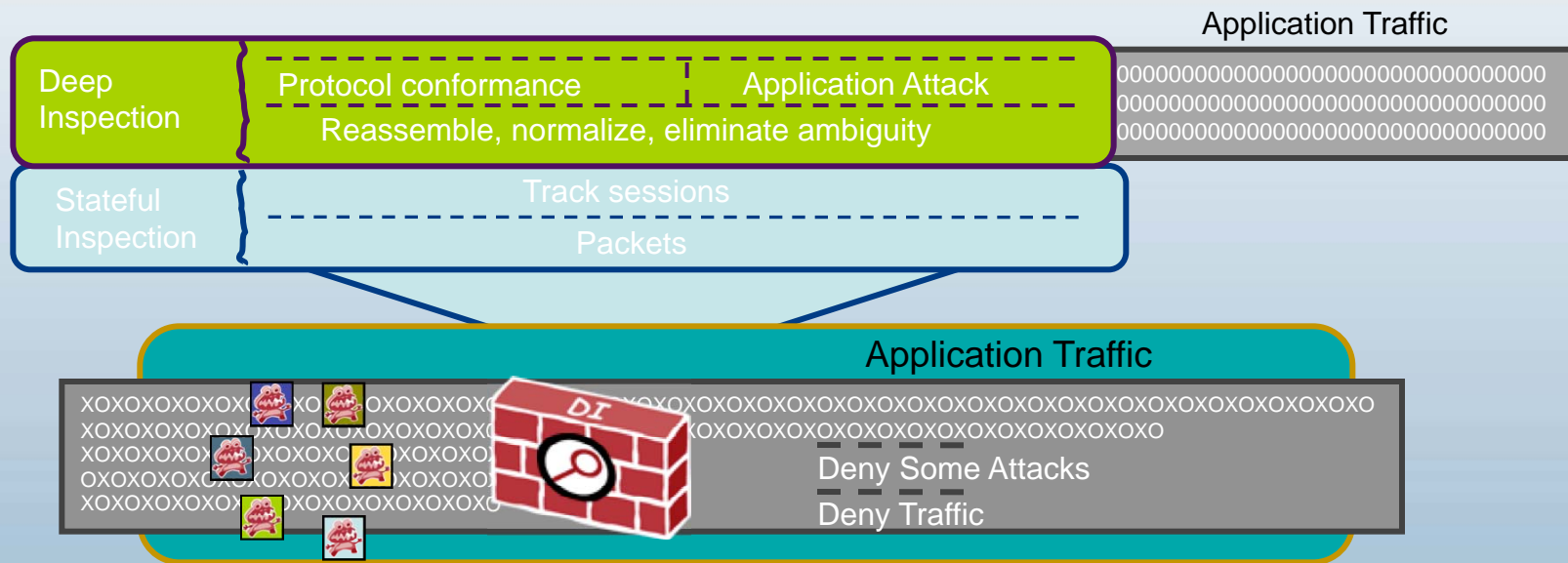
Enterprise UTM to Stop Common and Emerging Threats



IPS	Detects/stops Worms, Trojans, DoS (L4 & L7), Recon, Scans		Detects/stops Worms, Trojans
Web Filtering			Blocks Spyware / Phishing / Unapproved Site Access
AV	Stops Viruses, file-based Trojans, Spyware, Adware, Keyloggers		Stops Viruses, file-based Trojans or spread of Spyware, Adware, Keyloggers
Anti Spam	Stops Spam / Phishing		
Core Security	Stateful Firewall, VPN, Access Control		Stateful Firewall, VPN, Access Control

Deep Inspection

Stopping Application and Network Level Attacks



- Stops network & application level attacks with protocol anomaly and stateful signature attack detection mechanisms
- Apply granular inspection policies to key protocols, specific IP addresses or look for certain types of attacks

Antivirus

Stop Payload-based Attacks

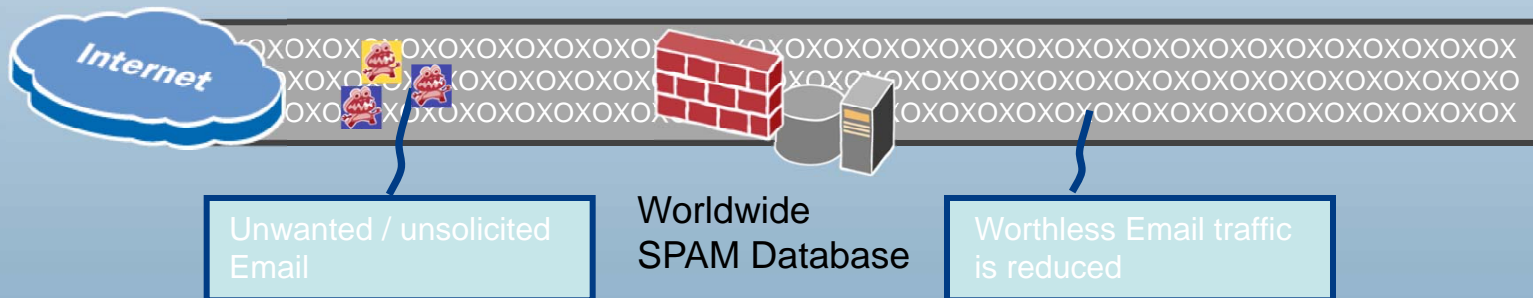
- Protect network against viruses, spyware / adware / keyloggers
 - Search and destroy viruses in SMTP, POP3, Webmail, FTP, IMAP, HTTP and IM
 - Virus scanning performed against inbound and outbound traffic



Anti-Spam

Filtering Unwanted Email at the FW Gateway

- Stop Spam and Phishing attacks
 - Continually update list of known spammers and phishers
 - Create custom “blacklist” and “whitelist” using specific domains, email senders, or IP addresses



We invite and encourage you to complete our online survey.

A link was sent to you via email and is listed below.

http://www.surveymonkey.com/s.aspx?sm=2SPzWxHuMYrzjEWs6jMmZA_3d_3d

We invite and encourage you to complete the survey for this webinar.

http://www.surveymonkey.com/s.aspx?sm=2SPzWxHuMYrzjEWs6jMmZA_3d_3d

www.internet2.edu

