

# Voice-Ready Data Equipment What You Need

# Session Description

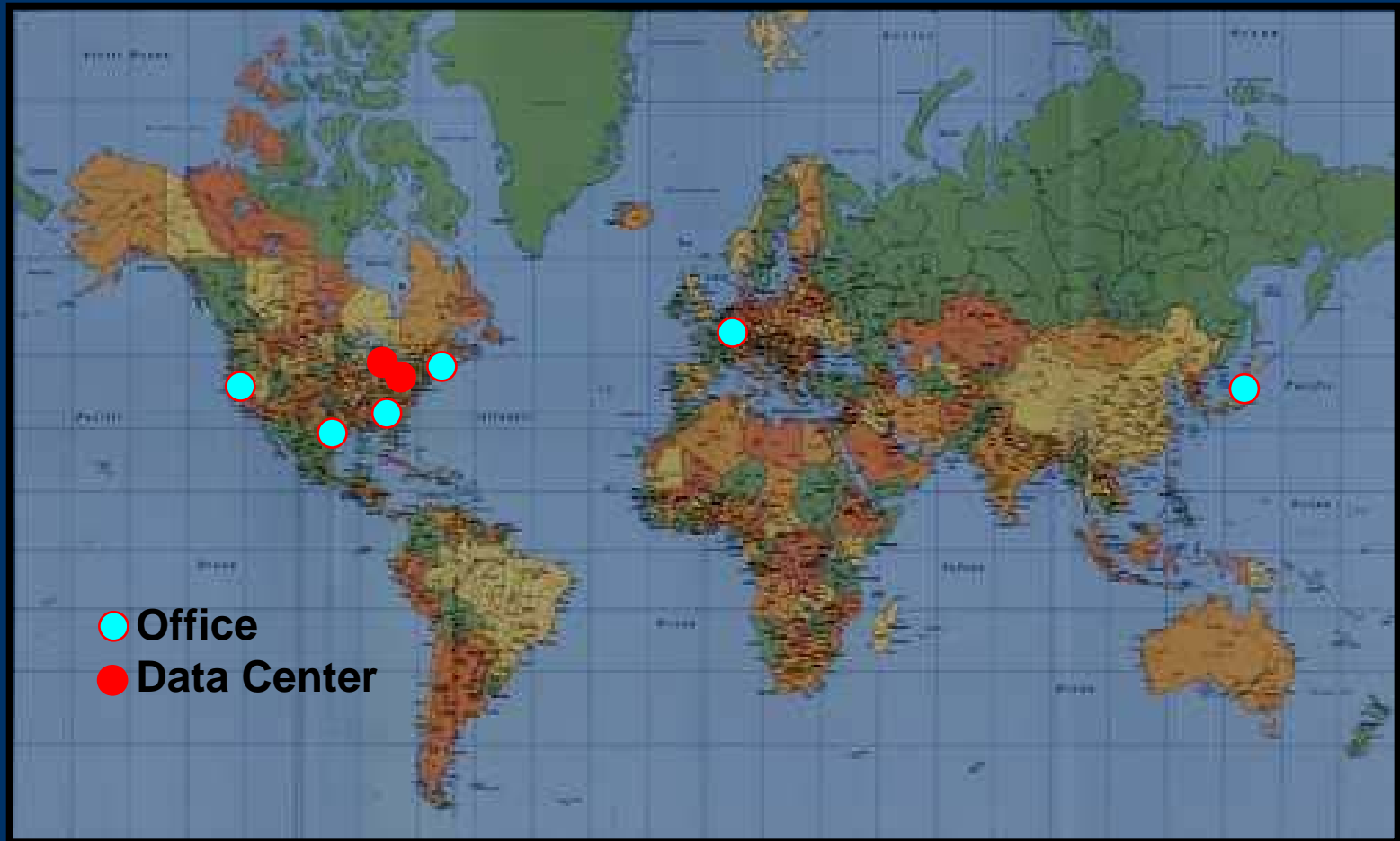
- We asked 4 network vendors to design a voice-ready network
- Today's Speakers:
  - **Scott Lucas**, Director, Solutions Marketing, Extreme Networks
  - **Mike Flaum**, Product Brand Manager, Nortel Networks
  - **Gary Hemminger**, Foundry Networks, Director of Product Marketing
  - **Dan Keller**, Customer Support Engineer, UCBU Tech Marketing - Cisco Systems
  - Then back to John Bartlett for Discussion and Q&A

# The Network Requirements

- Greenfield environment
- Enterprise Description
  - Multi site enterprise
  - Dual-site data centers in Chicago and Columbus
  - Office buildings with information workers in San Francisco, Austin, Atlanta, Boston, Tokyo and Brussels
  - Information Workers at each site:

– Chicago	500	– Boston	50
– San Francisco	200	– Tokyo	50
– Austin	100	– Brussels	150
– Atlanta	50	– Columbus	0

# Enterprise Map



# Applications

- Pure Data Applications
  - Legacy applications using Citrix from remote to data centers
  - Web-based HR app, hosted in data center
  - Exchange-based email for all employees hosted in data center
  - Background apps including backup, provisioning, updates, etc. using 0.5Mbps per office

# Applications (cont.)

- Pure Real-Time Applications
  - Full VoIP between all offices
  - 3 Video Conferencing rooms in each office building
  - MultiPoint Conferencing Unit located in the Chicago data center
- Mixed mode applications
  - CRM Call Centers in Brussels, Tokyo and Austin
  - CRM application is hosted on servers in the data center
  - CRM uses VoIP connected to gateways in Japan, US and Europe

# Application Performance Goals

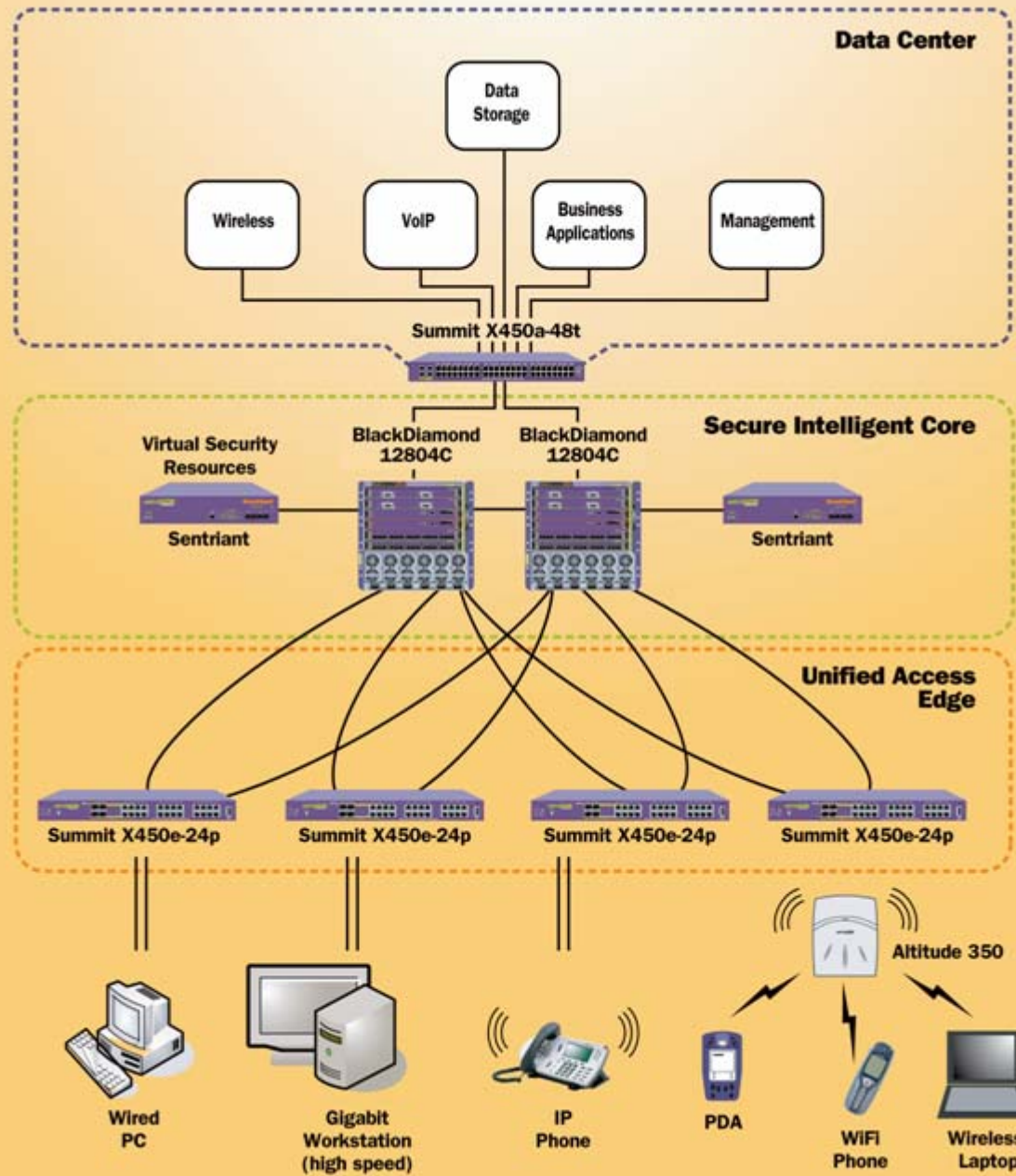
- Voice – MOS of 4.0
- Video Conferencing
  - Packet loss < 0.1%
  - Jitter < 50ms
- Exchange Email load in < 9 seconds
- Web based HR loads in < 6 seconds
- Citrix interactions < 2 seconds
- CRM Data loads in < 3 seconds

# Scott Lucas

Sr. Director, Solutions Marketing

Extreme Networks

[www.extremenetworks.com](http://www.extremenetworks.com)



# Solution Issues

- LAN Issues @ The Edge
  - Controlling access of devices and users
  - Lowering the administrative burden for a distributed Enterprise
  - Establishing a simple & effective QoS strategy
- LAN Issues @ The Core
  - Insight into operations and issues
  - Business continuity & performance under duress
- WAN Issues
  - Supporting centralized services
  - Anticipating growth and change
  - Planning for traffic before users, applications, and connections are in place
  - Seasonality & disaster recovery
- Issues Not Covered
  - PoE and resiliency are assumed to be integral parts of the vendor's solution and the network design

# Key LAN Strategy: Segmentation

- 6 Enterprise-Wide Virtual LAN's
  - CRM Voice, Standard Voice, Video, Data Center High, Data Center Low, Background
- Problems solved
  - Inherent Security: Traffic segregation delivers safer networks
  - Straightforward Classification: VLAN assignment drives QoS marking and subsequent scheduling
  - Distributed Management with Limited IT Staff: Consistent config across the Enterprise; event-driven provisioning

# Key LAN Strategy: Instrumentation

- Statistical Insight Using sFlow in Edge & Core
  - Forensics & trending: useful for understanding traffic patterns and what went wrong
  - Value: planning and fine-tuning over time
- Wire-Rate, Per-Packet Insight in Core
  - Real-time inspection: versatile, per-packet traffic inspection
  - Value: creating events for real-time detection & correction of security and loading issues

# Key WAN Strategy: Carrier Ethernet

- E-Line services connect international locations & business offices to Chicago, E-LAN services connect high-bandwidth domestic locations
- Dramatically simpler and more flexible inter-site solutions
  - Premises interface is a simple Ethernet jack
  - Transparent LAN extensions eliminate configuration challenges and application disruption associated with routed connections
  - Bandwidth can be scaled in 1Mbps increments
  - Performance equivalence to traditional WAN with ability to spec CIR/EIR
  - Some carriers can re-provision in *5 minutes!*
  - Implications
    - Much lower penalty if your plan was wrong
    - Easy to scale up or down for seasonal staffing or traffic variations
    - Multi-site disaster recovery

# Mike Flaum

Product Marketing Manager

Nortel

[www.nortel.com](http://www.nortel.com)

# Key decision points

Only buy networking products that support-

Power over Ethernet (802.3af) – (For the Edge network)

- 10/100/1000 PoE is preferable to 10/100
- 10/100 PoE

QoS – VoIP phone, Edge and Core, WAN & Internet

- IEEE 802.1P and IETF RFC 2474 DiffServ
- IEEE 802.1ab automates QoS (relatively new)
- The same Internet provider for Internet access in all locations
- Does your Internet provider honor DiffServ?

Resiliency – License or Free?

- Layer 2 (STP, RSTP, SMLT) vs. Layer 3 OSPF
- Test choices and compare performance vs. price

Security- Does it work with VoIP?

- Must work with the phone as the edge of the network
- Must be built to accommodate VoIP

# Overlooked key points

## VoIP Handsets

- 10/100/1000 PoE is preferable to 10/100
- Wirespeed & QoS tested just like an Ethernet Switch

## Laptop

- 2.0 GHz Processor+
- 1.0 Gigabyte of RAM+
- Built in wireless
- 4 USB Ports
- Gigabit NIC
- QoS in Operating System

## Remote Users

- SSL VPN Clientless
- IPSec VPN Client
- Policy and feasibility
- DSL or Cable Modem

## Tested solutions-

- Multi-Vendor vs. Single-Vendor
- 3<sup>Rd</sup> party test reports of complete solution
- Configuration guide for VoIP on Data with Security
- Proven deployments
- Proven integration and testing
- Interoperability  $\neq$  ease of deployment

# Network Topology

The great WAN choice

Internet (w/IPSec) vs. Frame Relay and MPLS

Internet –(one provider)

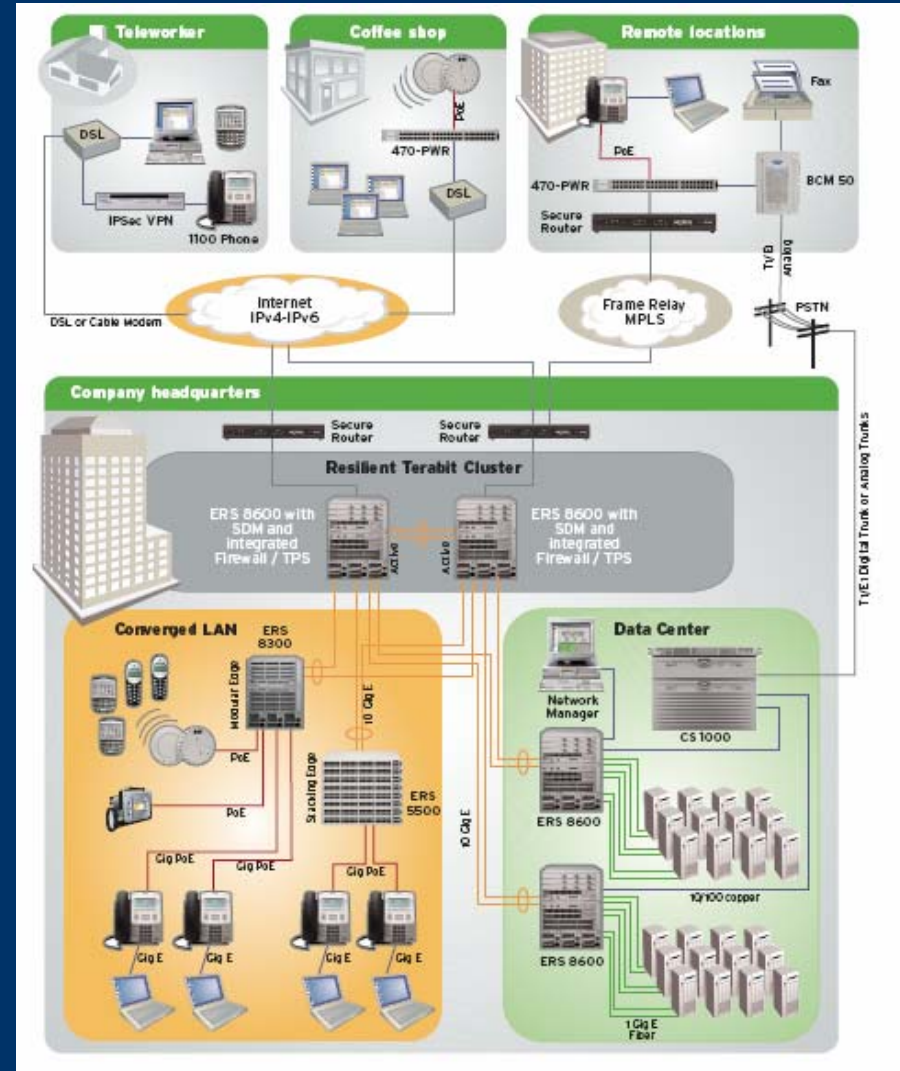
- Typically no peering points
- Consistent and support QoS policy

Internet – (Multiple providers)

- Peering Points
- Different QoS policies

Availability of bandwidth in each location and remote user-

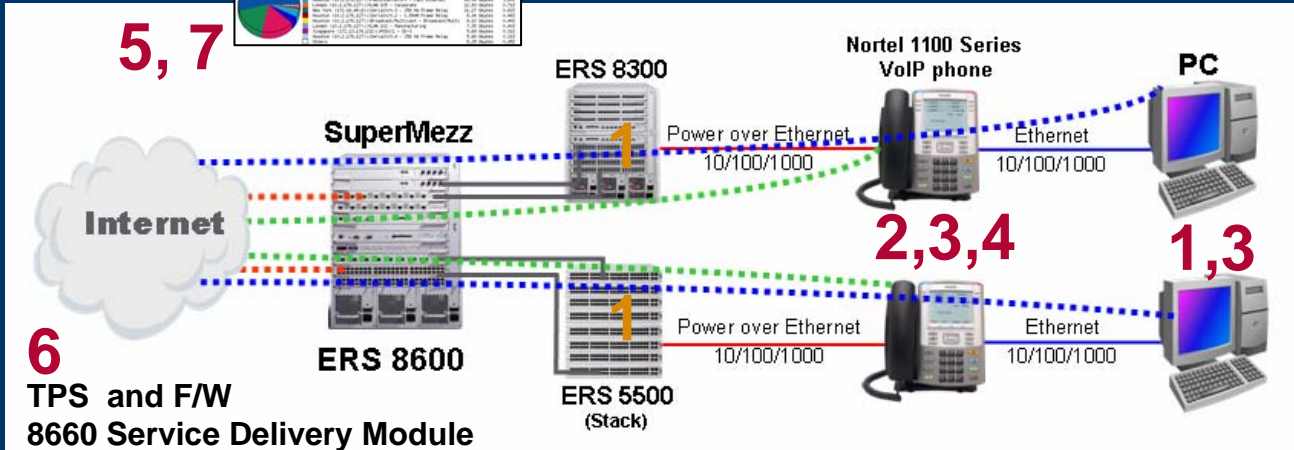
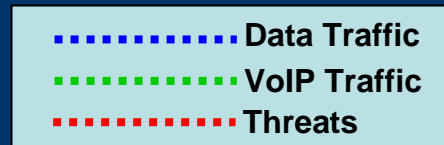
- Metro Ethernet
- Fiber
- DS3
- DSL / Cable Modem



# Nortel Secure VoIP

1. Detect Hosts and apply QoS (802.1AB & ADAC & NSNA)
2. Detect VoIP Handset and apply QoS (802.1AB & 802.1X & NSNA)
3. Detect Applications (TunnelGuard (PC), (PVQM VoIP Handset)
4. Synthetic Transactions (Simulate Application, RTCP, Phone Agent)
5. Pattern match anomalies (IPFIX RFC 3917)
6. Signature match known threats (Threat Protection System)
7. Apply policies to network (Enterprise Policy Manager)

## Network Management



# Gary Hemminger

Director of Product Marketing

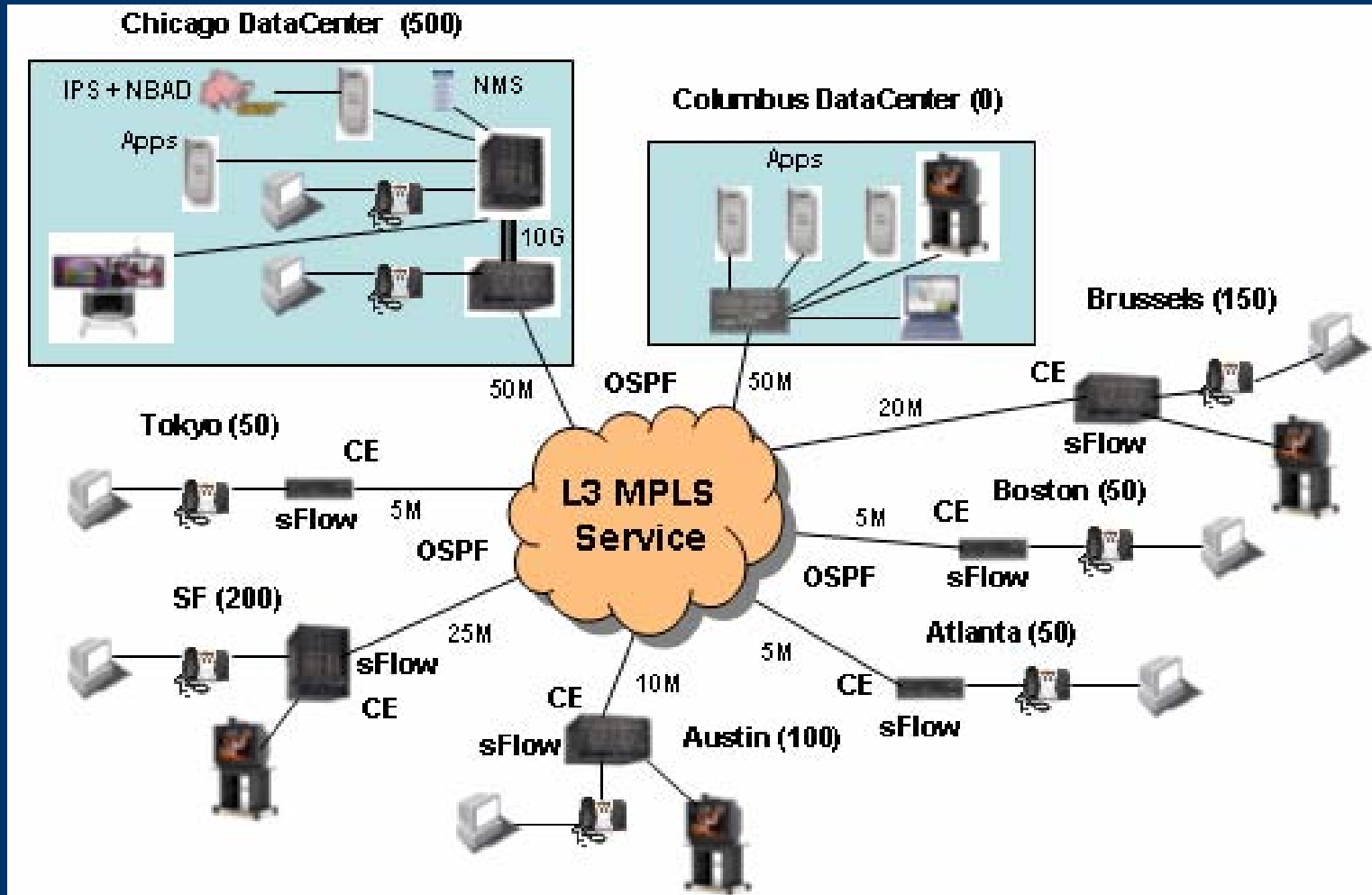
## Foundry Networks

[www.foundrynet.com](http://www.foundrynet.com)



# Converged Network Design

*Ethernet LAN Switching, L3 Routing, and L3 MPLS Service*



# Converged Network Design

- Chassis switches all provide fully redundant PoE power, management modules, and backplanes
  - Phones and PC share same port for cost saving
  - Videoconferencing equipment on separate ports
  - Edge switches are CE routers connected to SP PE routers
  - L2 Switching within site, L3 Routing to cloud where SP provisions L3 MPLS-VPN service
- QoS Deployment
  - Data is on untagged VLAN, gets remarked (DiffServ/ToS) to P0 (best effort queue)
  - IP Phone on tagged voice VLAN has DiffServ/ToS markings for P7 (lowest latency, highest priority queue)
  - Videoconferencing equipment can be on untagged or tagged port and is marked or remarked with P6 (next highest priority queue)
  - Strict priority is used for P6 and P7 queue, P0-5 queue is setup in WRR (weighted round robin) to prevent queue starvation
  - If the phone or videoconferencing equipment can only support 802.1p markings, then remark to DiffServ/ToS
  - MPLS EXP service provides proper QoS mapping service from DSCP onto a single LSP only (for cost saving...later, may use Label Mapping for enhanced performance)

# Converged Network Design

- **Bandwidth Management and WAN requirements**
  - On CE to PE link, use rate shaping to set the following:
    - CIR for video conferencing traffic at 2Mbps, a bit more for Chicago site.
    - CIR for Voice traffic is about 2Mbps per 50 Users. Chicago site will need additional CIR to handle incoming remote site Voice traffic
    - Columbus site is probably data only, so data CIR should be full bandwidth and must handle including remote site traffic
- **Edge and VoIP Security**
  - Use flow based security analytics. Integrated IPS is too costly and hard to deploy/manage at each site
  - sFlow supported in each switch. Multiple collection technology exists to handle network anomaly detection, Signature IPS analysis, and reporting.
  - NMS interacts with security analytics solutions to provide security policy support (i.e. can turn off specific edge port or use MAC ACL to shut off attacker)
- **MPLS WAN Provider Issues**
  - Must provide SLA and hosted reporting (by application type)
  - What kind of traffic engineering support do they have (IS-IS/TE, OSPF/TE, RSVP-TE)?
  - Must provide E-LSP (EXP based) and optionally L-LSP (Label based) support
  - Do they support MPLS resiliency functions like fast reroute?
  - Should also provide Mixed L2/3 VPN service along with IP MPLS service
  - Do they provide OAM functionality?

# Dan Keller

Customer Support Engineer, UCBU Tech Marketing

Cisco Systems, Inc.

[www.cisco.com](http://www.cisco.com)





# Quality of Service Methodology

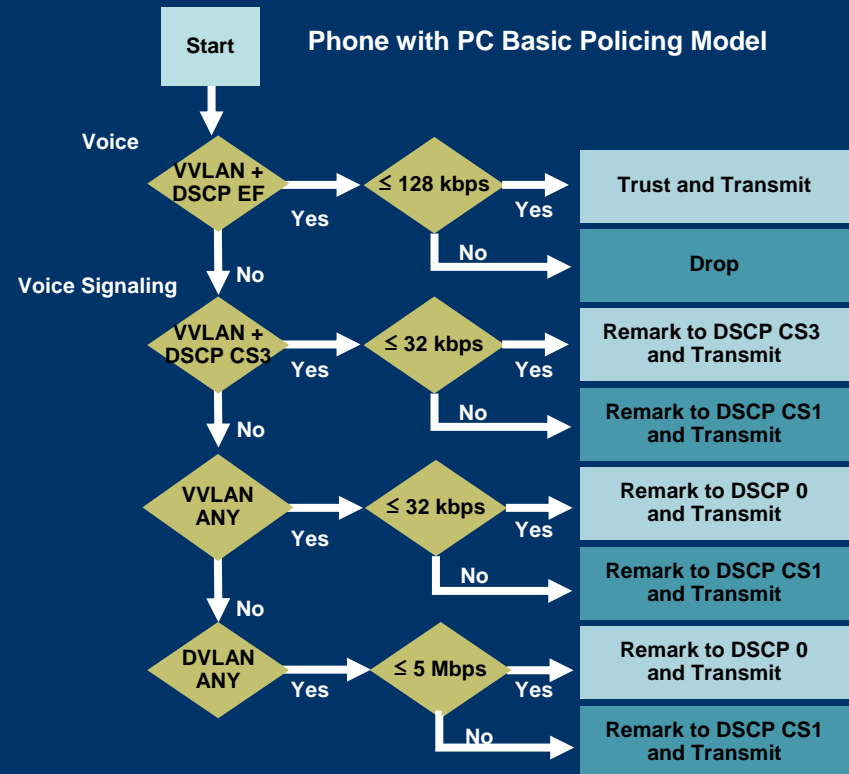
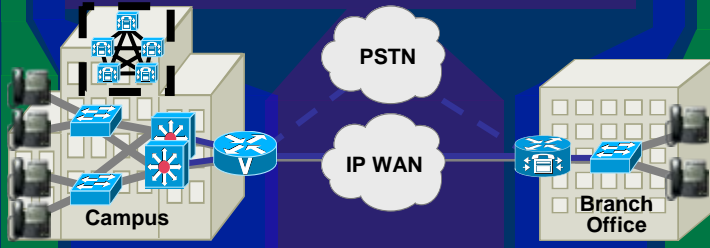
## Classification, Trust and Policing

- Classification
- Trust Boundaries
- Optional Policing
- Scheduling

**Classification:** Mark the packets with a specific priority denoting a requirement for class of service from the network  
**Trust Boundary:** Define and enforce trust boundary at network edge

**Scheduling:** Assign packets to one of multiple queues (based on classification) for expedited treatment throughout the network; use congestion avoidance for data

**Provisioning:** Accurately calculate the required bandwidth for all applications plus element overhead



# Quality of Service Methodology

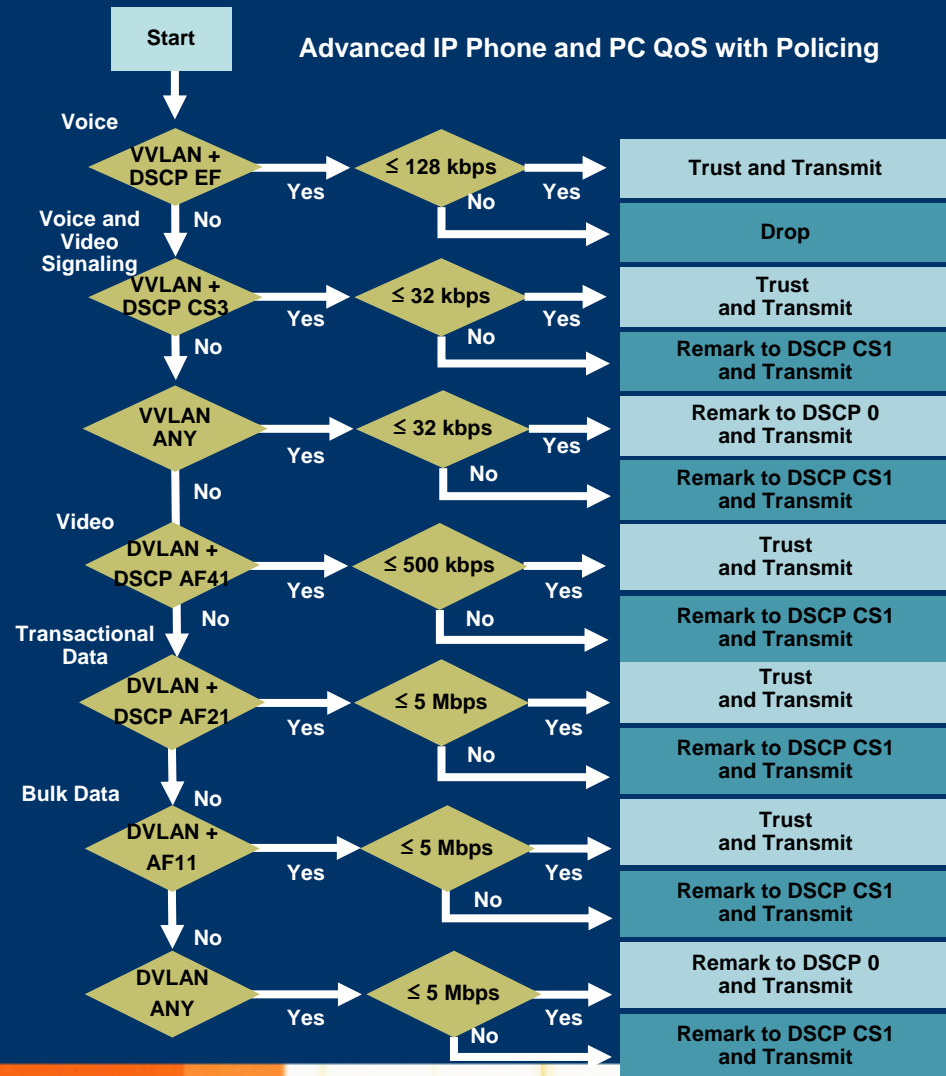
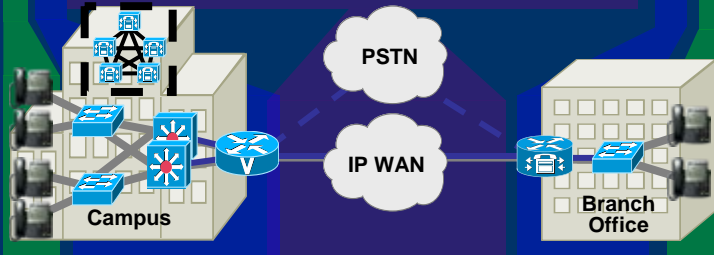
## Classification, Trust and Policing

- Classification
- Trust Boundaries
- Optional Policing
- Scheduling

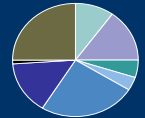
**Classification:** Mark the packets with a specific priority denoting a requirement for class of service from the network  
**Trust Boundary:** Define and enforce trust boundary at network edge

**Scheduling:** Assign packets to one of multiple queues (based on classification) for expedited treatment throughout the network; use congestion avoidance for data

**Provisioning:** Accurately calculate the required bandwidth for all applications plus element overhead



# Quality of Service Methodology Scheduling



Application	Application Type	L3 Classification			L2
		IPP	PHB	DSCP	CoS
	Routing	6	CS6	48	6
Voice over IP	Voice	5	EF	46	5
Video Conferencing	Video Conferencing	4	AF41	34	4
	Streaming Video	4	CS4	32	4
	Mission-Critical Data	3	AF31	26	3
Voice and Video Call Signaling	Call Signaling	3	CS3	24	3
Citrix	Transactional Data	2	AF21	18	2
	Network Management	2	CS2	16	2
Backup	Bulk Data	1	AF11	10	1
	Scavenger	1	CS1	8	1
Other Applications	Best Effort	0	0	0	0

4 Queue LAN Model
Voice
Video Conferencing
Call Signaling
Routing
Network Management
Transactional Data
Bulk Data
Best Effort
Scavenger

8 Class WAN Queuing Model	WAN BW %
Voice	10%
Video Conferencing	15%
Call Signaling	5%
Routing	4%
Network Management	
Transactional Data	25%
Bulk Data	15%
Best Effort	25%
Scavenger	1%

# Review and Discussion

- Lets take a look at the four designs
- What do we see in common
- What issues differ
- What issues were not discussed
- Send up your questions!

# Common Themes

- Resiliency
- Power over Ethernet (PoE)
- Security
- QoS Deployment
  - Classification
  - Priority Assignments
  - DiffServ and IEEE 802.1p/Q
- Real-time test and monitoring

# Security

- How do we secure the voice infrastructure?
- Are VLANs a critical component of the security design?
- Is endpoint authorization a critical component of the security design?

# Classification

- Automatic
  - 802.1X authentication
  - Radius assigned VLANs
  - Detect application by src/dst/port range
- Manual
  - Static IP address assignment
  - Static VLAN port assignment
- Network versus Endpoint

# Priority Assignments

- We almost agree on assignments

Application	Cisco	Foundry	Extreme	ietf-tsvwg*
	PHB	Priority	PHB	PHB
	CS6		CS6	CS6
Voice over IP	EF	P7	EF	EF
Video Conferencing	AF41	P6	AF41	AF41
	CS4			CS4
	AF31			AF31
Voice and Video Call Signaling	CS3			CS3
Citrix	AF21	??	AF21	AF21
	CS2			CS2
Backup	AF11	P0	AF11	AF11
	CS1			CS1
Other Applications	0	P0	0	0

# Layer 2 QoS

- IEEE 802.1p/Q appears to be the logical choice
- Is it necessary? We have high bandwidth in the LAN. How do I decide if L2 QoS is needed?
- Does L2 QoS have a role to play in security?
- Critical in Level 2 WAN VPN service?

# Test and Monitoring

- S-Flow, NetFlow, give us traffic information
- Many other vendors in this business
  - Apparent, Brix, Centrisoft, NetIQ, Qovia, Radcom, Viola and more ...
- How to accomplish end to end monitoring?

# Bandwidth

- Bandwidth Required over WAN
  - 3 Mbps / 50 users data? (Cisco, Foundry)
  - 2 Mbps / 50 users Voice CIR? (Foundry)
- No discussion on managing data application performance
- Analysis needs to be done to understand how to meet all application performance goals