Secure Always on Networking

Jean Turgeon (JT), MBA
Director, Enterprise Solutions Engineering
CTO office
jturgeon@nortel.com
Australia – July 2007

NORTEL
Business made simple

1 - QUESTnet 2007

Biography – Jean Turgeon

- Jean Turgeon, MBA
  - Director, Enterprise Solutions Engineering at Nortel
  - 23 years of experience in networking solutions
- Jean Turgeon speaks frequently on this and other Enterprise related topics at:
  - Nortel Enterprise Technology Forum (NETF) – Formally NPW
  - Distributor Alliance Council (DAC)
  - Global Sales Customer & Partner events
  - Executive Business Center visits
  - Networld Interop (N+I) Asia & NA

2 - QUESTnet 2007

Industry Landscape

Past, Present, Future

	2001 – 2006	2007 – 2012+
Industry Focus/Era	**Intelligence & Mobility**	**Pervasive Personal Broadband**
Challenge	Making fast, "dumb" networks intelligent and fast	1) Hyper-Connectivity • density/diversity 2) Application-aware networks 3) "True" broadband

Nortel is positioned to lead the transition to this new era

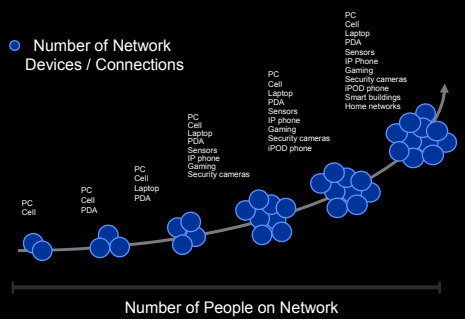
Limited vendor differentiation

3 - QUESTnet 2007

Hyperconnectivity

A foundational catalyst that is driving change in the communications world

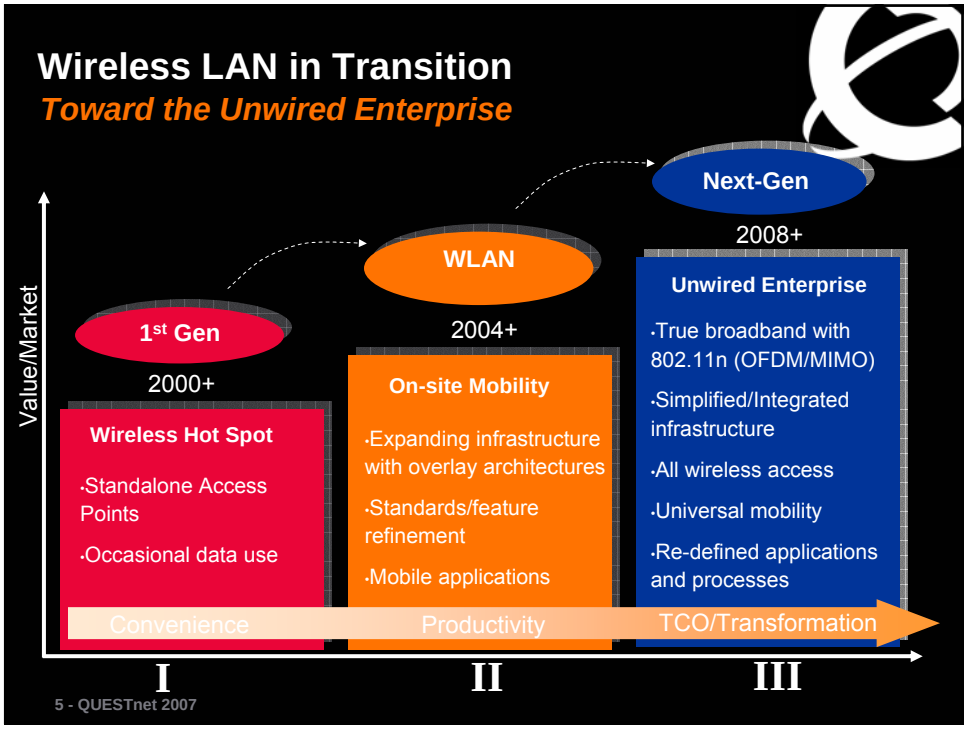
Hyper-Connectivity: Addressing the Challenge of Density and Diversity



- Will put staggering loads on enterprise networks
- *Identity Mgmt & RFID/Sensors*
- *Accelerates the need for True Broadband and Communication Enabled Applications*
- Makes us fundamentally rethink *how we build applications, services and networks*

Enterprises must be prepared for the disruptions and opportunities presented by this catalyst

4 - QUESTnet 2007


Wireless LAN in Transition
Toward the Unwired Enterprise
Value/Market
1st Gen
2000+
Wireless Hot Spot
•Standalone Access Points
•Occasional data use
WLAN
2004+
On-site Mobility
•Expanding infrastructure with overlay architectures
•Standards/feature refinement
•Mobile applications
Next-Gen
2008+
Unwired Enterprise
•True broadband with 802.11n (OFDM/MIMO)
•Simplified/Integrated infrastructure
•All wireless access
•Universal mobility
•Re-defined applications and processes
Convenience
Productivity
TCO/Transformation
I
II
III
5 - QUESTnet 2007


Q: What's the greatest new threat; what should people be most worried about?
• A :The consumerization of IT; mobile devices, working from home, etc., that's the biggest issue. [IT departments] aren't heading toward more control [over IT assets], in reality we're heading toward less control. (Gartner vice president and distinguished analyst John Pescatore)

The blurring of the network edge

Policy, not topology, defines the edge

Who, what, where, why, how … and is it safe?????

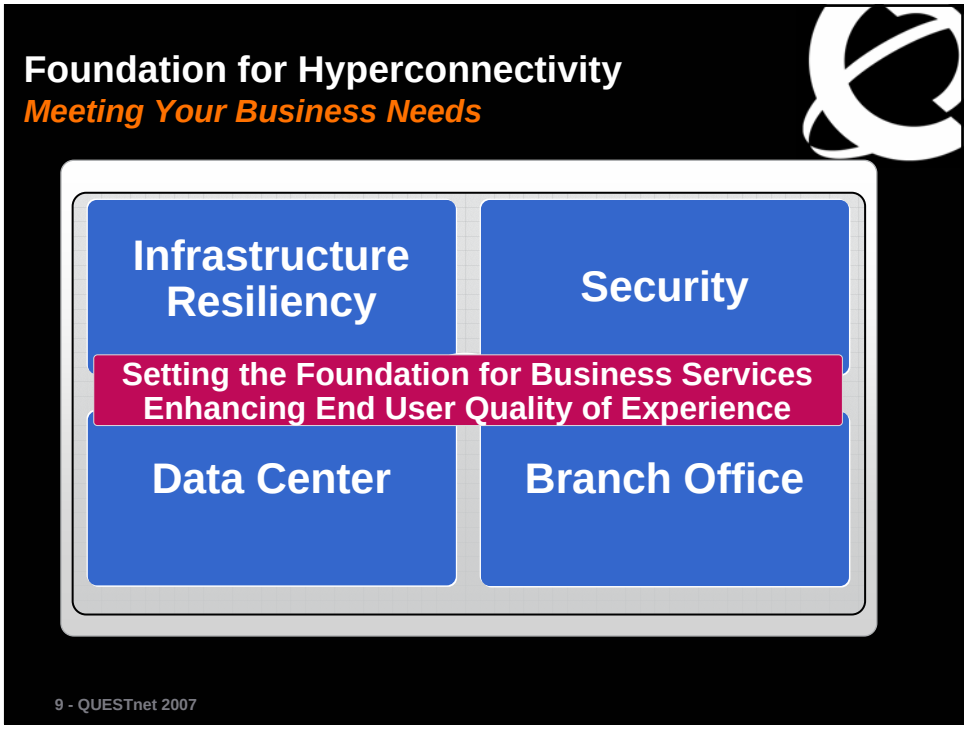
7 - QUESTnet 2007

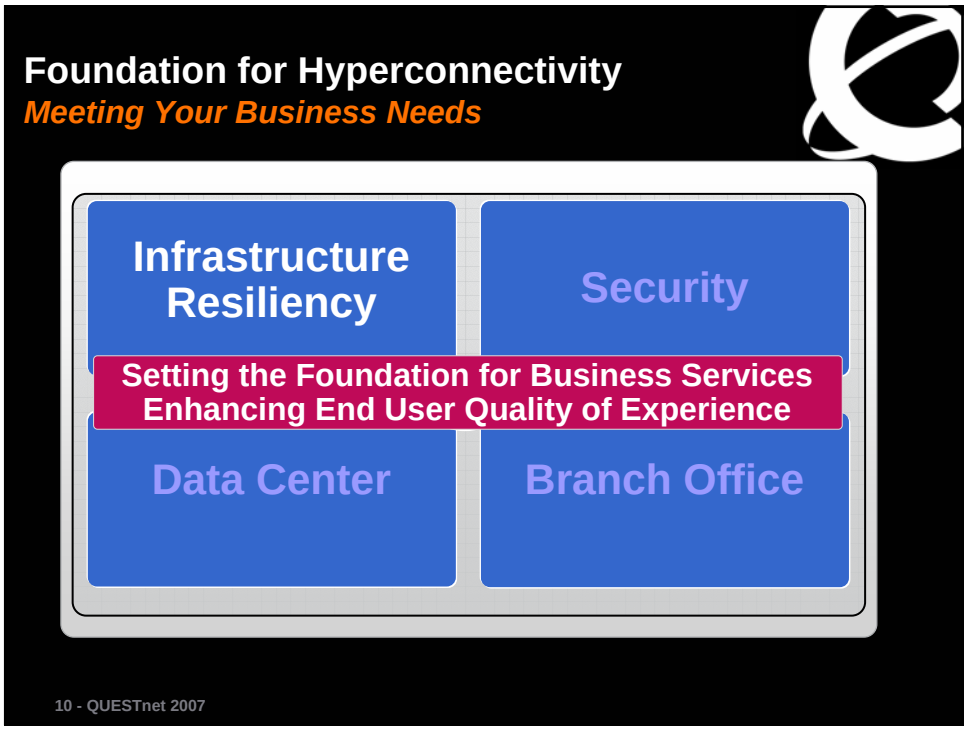
Infrastructure Requirements

Education

- Reliability – Adaptable to various needs
- Scalability – Ability to scale bandwidth when required
- Multi-vendor support – Open Standards or guaranteed inter-operability
- Mobility – Indoor and Outdoor
  - Ability to implement Sensors/RFID technology
- Security – Access Control
  - OS independent
  - Preferably no agent or resident software on devices
  - Strong Filtering and Policies support – Ease of deployment
  - Centralized for ease of mgmt
- IPv4 & IPv6 ready, QoS support
- Ability to trial evolving standards (protocols, etc..) without disrupting operations
- Multimedia ready
  - Unified Communications, VoIP, etc…
  - Multicast Support (L2-L3)

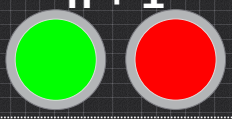
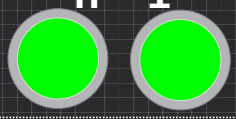
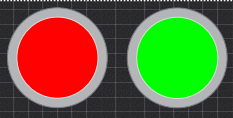
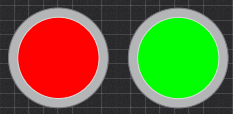
8 - QUESTnet 2007


Foundation for Hyperconnectivity
Meeting Your Business Needs
Infrastructure Resiliency
Security
Setting the Foundation for Business Services
Enhancing End User Quality of Experience
Data Center
Branch Office
9 - QUESTnet 2007


Foundation for Hyperconnectivity
Meeting Your Business Needs
Infrastructure Resiliency
Security
Setting the Foundation for Business Services
Enhancing End User Quality of Experience
Data Center
Branch Office
10 - QUESTnet 2007

Reliability Optimization

Choosing the right model

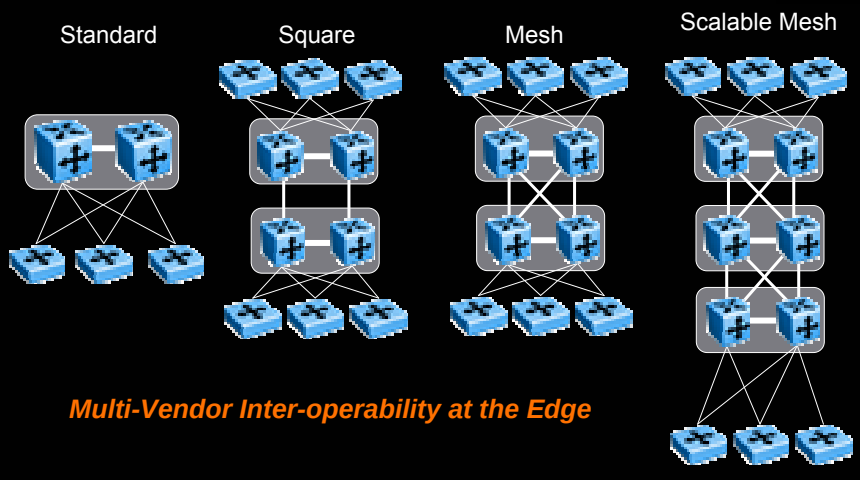
	Active–Passive	Active–Active
	n + 1	n – 1
Normal Operation		
Failure Operation		
	• Hot Standby • Size to constant capacity • Cost = 1/Avail x Price • Transition Timing	• Distributed Use • Size to Need • Reduce Capacity in Failure • Use Business Rules

Information Security is fundamentally about ensuring:
Confidentiality, Integrity, Availability

11 - QUESTnet 2007

Taking advantage of Switch Clustering

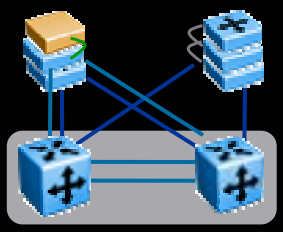
Delivering Scalability & Resiliency without Complexity



Multi-Vendor Inter-operability at the Edge

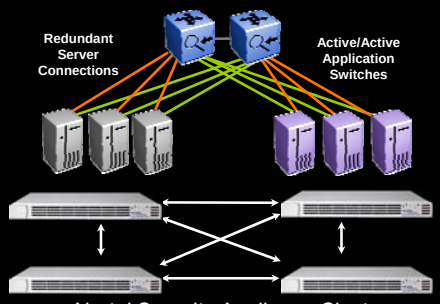
12 - QUESTnet 2007

An Architecture for Always-On Security



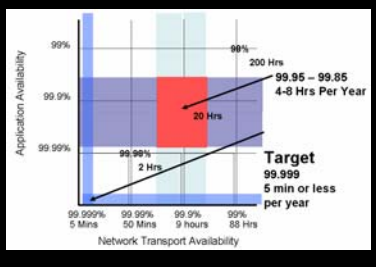
Nortel Ethernet Routing Switch Clustering

+



Nortel Security Appliance Clusters & Single System Image Management

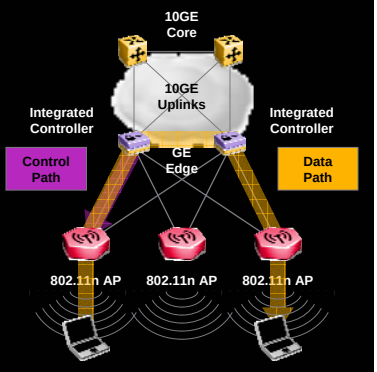
=



- **Active/Active Resiliency**
- **High-Performance**
- **Scalability**
- **Service Availability**
- **Support for reduction of planned and un-planned downtime**

Next Gen - 802.11 Wireless LANs Architecture

- Controller functions integrated and distributed within the Network infrastructure
  - Thin architecture remains the same but provides integration
    - Self discovery / configuration
    - Reduced latency
    - Improved data forwarding
    - Identity Based Networking
    - QoS, filtering, inspection etc..
  - Highly scalable
    - 802.11a/b/g/n Access
    - Large number of users with bursting
    - Multiple applications
    - Medium and large deployments
  - Reduced OPEX & CAPEX
    - Fewer devices to manage
    - Less complexity
    - Single management interface



14 - QUESTnet 2007

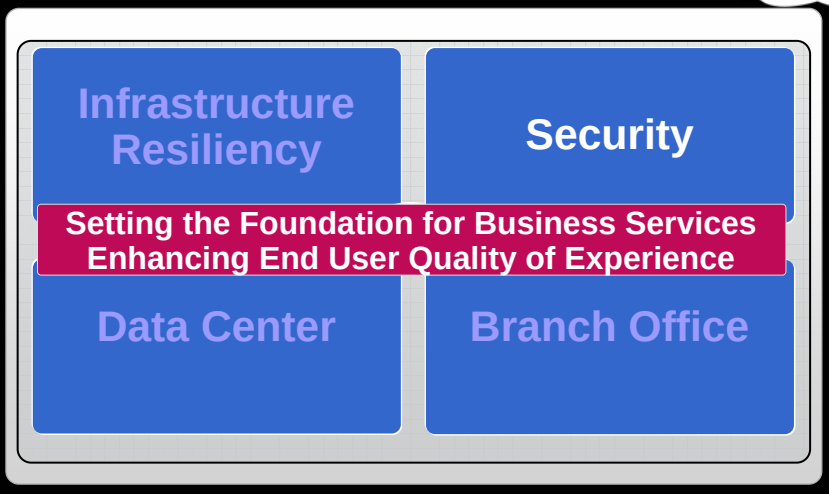
Addressing congestion (QoS/QoE)

- During Congestion, QoS maintains critical business services
- Ensure you have an easy to use and powerful QoS deployment tool
- Test and validate end to end characteristics
  - Delay & Jitter for apps (QoE)
  - Test all characteristics under failure
  - Test deployment of QoS and validate impact (does it work?)
    - Get end user feedback throughout all validation
  - What tools are in place to monitor network behavior?

15 - QUESTnet 2007

Foundation for Hyperconnectivity

Meeting Your Business Needs

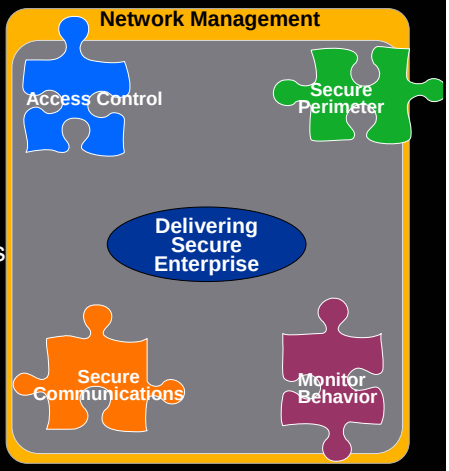


16 - QUESTnet 2007

Securing the Enterprise

Architecture Components

- Access Control
  - LAN Access Control : Wired & Wireless
    - Client and Clientless solutions
  - Secure Remote Access
    - Client and Clientless Solutions
  - Remediation support
- Secure Perimeter - DMZ
  - Public Internet Access
  - Intelligent Traffic Management
  - Threat Protection / Switched Firewall
  - VPN Gateway (IPSec, SSL)
- Secure Voice / Multimedia Applications
  - Secure Multimedia Controller
  - Unified Communications
  - Branch to Branch
- Monitor Behavior
  - TPS, IPFIX, etc…
- Network Management
  - Centralized Secure Management
  - Compliance & reporting

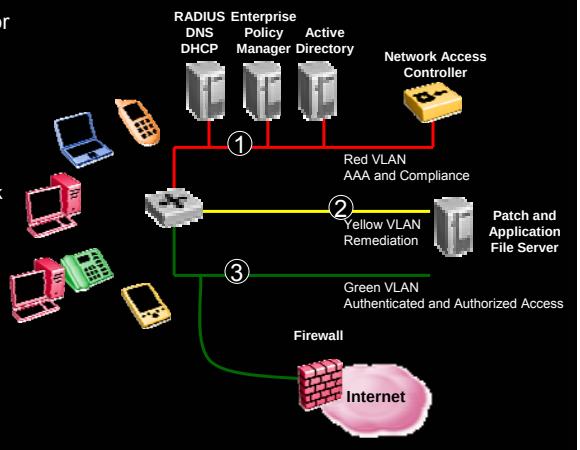


17 - QUESTnet 2007

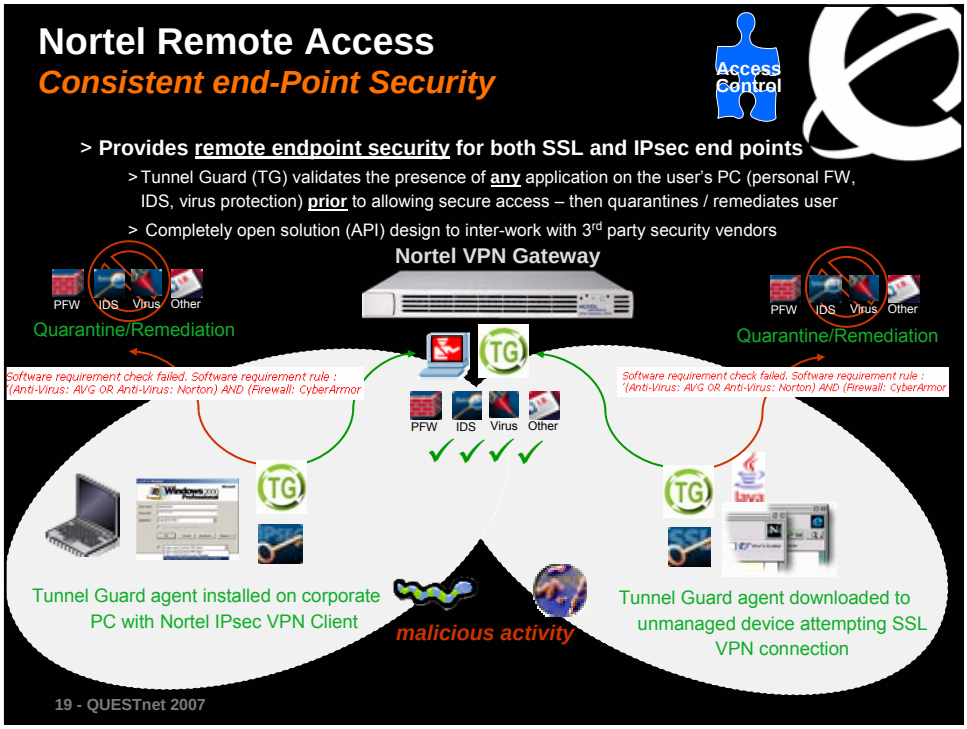
Secure Network Access Control

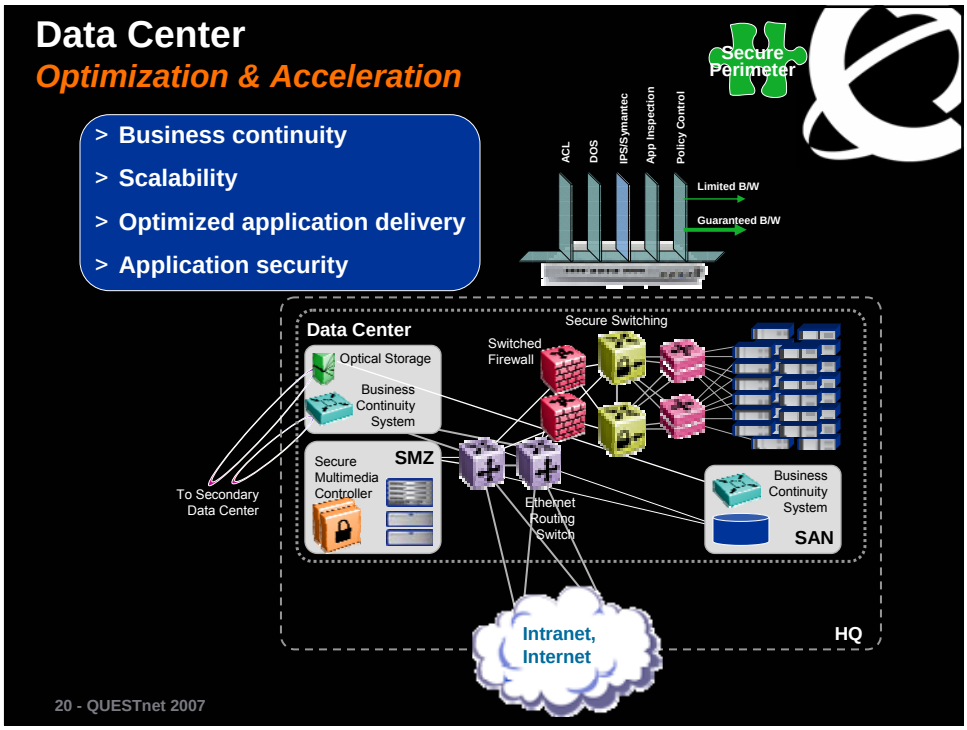
Clientless - High Level View
Perfect for Education

- Open access endpoint security for remote (IPSec/SSL), LAN and Wireless LAN users using fixed and mobile devices
- Evaluates compliance before network connection is made
  - Proactive checks to allow network access only by compliant devices
  - Reactive checks to detect and isolate non-compliant devices
- Seamless device quarantine/containment, remediation and repair
- Decreases risk of infected or vulnerable systems from connecting to the network,
- 802.1X EAPOL



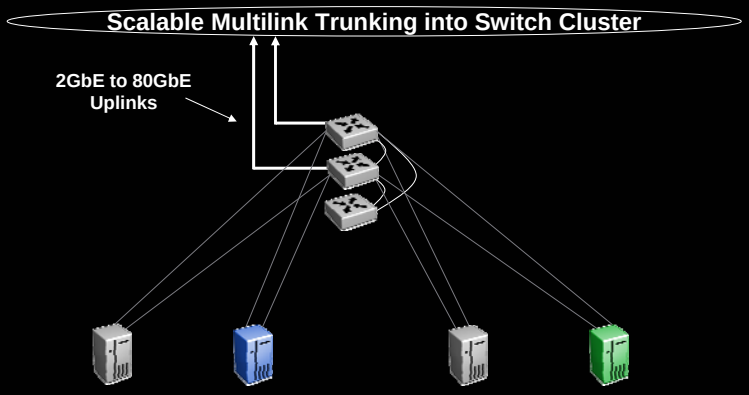
18 - QUESTnet 2007


Nortel Remote Access
Consistent end-Point Security
Access Control
> Provides remote endpoint security for both SSL and IPsec end points
> Tunnel Guard (TG) validates the presence of any application on the user's PC (personal FW, IDS, virus protection) prior to allowing secure access – then quarantines / remediates user
> Completely open solution (API) design to inter-work with 3rd party security vendors
Nortel VPN Gateway
PFW IDS Virus Other
Quarantine/Remediation
Software requirement check failed. Software requirement rule : '(Anti-Virus: AVG OR Anti-Virus: Norton) AND (Firewall: CyberArmor
TG
Tunnel Guard agent installed on corporate PC with Nortel IPsec VPN Client
malicious activity
Tunnel Guard agent downloaded to unmanaged device attempting SSL VPN connection
19 - QUESTnet 2007


Data Center
Optimization & Acceleration
Secure Perimeter
> Business continuity
> Scalability
> Optimized application delivery
> Application security
ACL
DOS
IPS/Symantec
App Inspection
Policy Control
Limited B/W
Guaranteed B/W
Data Center
Secure Switching
Switched Firewall
Optical Storage
Business Continuity System
Secure Multimedia Controller
SMZ
To Secondary Data Center
Ethernet Routing Switch
Business Continuity System
SAN
Intranet, Internet
HQ
20 - QUESTnet 2007

Vertical Stacking

Ethernet Infrastructure – Server Access Layer



"Normal" Vertical Stacking

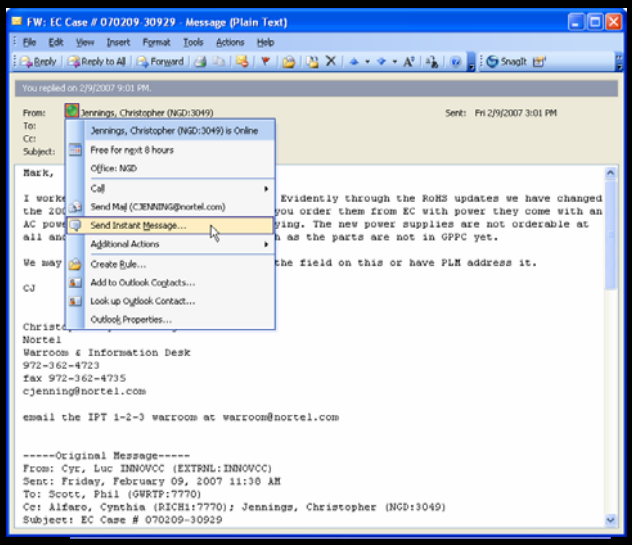
- Low latency between servers (9µs)
- Highly resilient stacking technology with scalable uplinks
- Must run cables to servers – difficult to manage

21 - QUESTnet 2007

Web Based Collaboration

Increasing Productivity & Mobility
IPSEC & SSL

Secure Communications

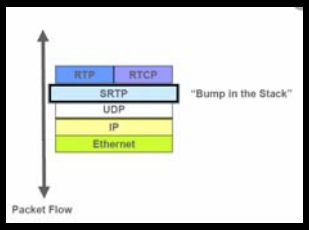


22 - QUESTnet 2007

Securing Multimedia

Secure Communications

- Understand and pay attention to end to end Encryption
- Protection for VoIP/Multimedia infrastructure
  - Signaling path
    - Encryption
    - Protecting against man-in-the-middle attacks
    - Anti-spoofing and Denial of Service Protection
    - Stateful inspection
  - Media path – sRTP
    - Between two Nortel IP phones
    - Confidentiality (AES Encryption)
    - Authentication (HMAC-SHA1)
    - Replay Protection
  - Or other solutions
    - IPSEC & SSL still viable
    - SIP TLS



23 - QUESTnet 2007

Threat Protection System

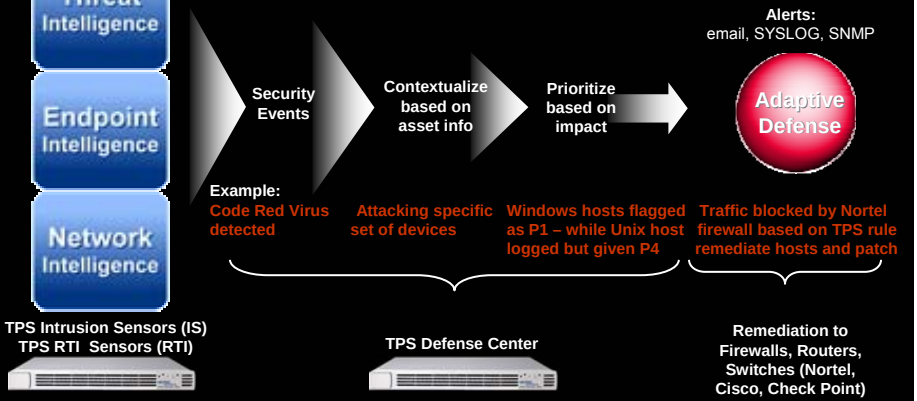
Monitor Behavior

Gathering real-time data on threats & vulnerabilities

***Discover** what's happening on the network*

***Determine** the threat level and impact*

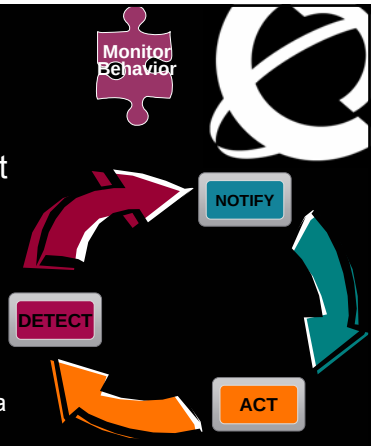
***Defend** against the threat - proactively*



Provides customers a security assessment prior to deploying VoIP

24 - QUESTnet 2007

Monitoring - Leveraging IPFIX

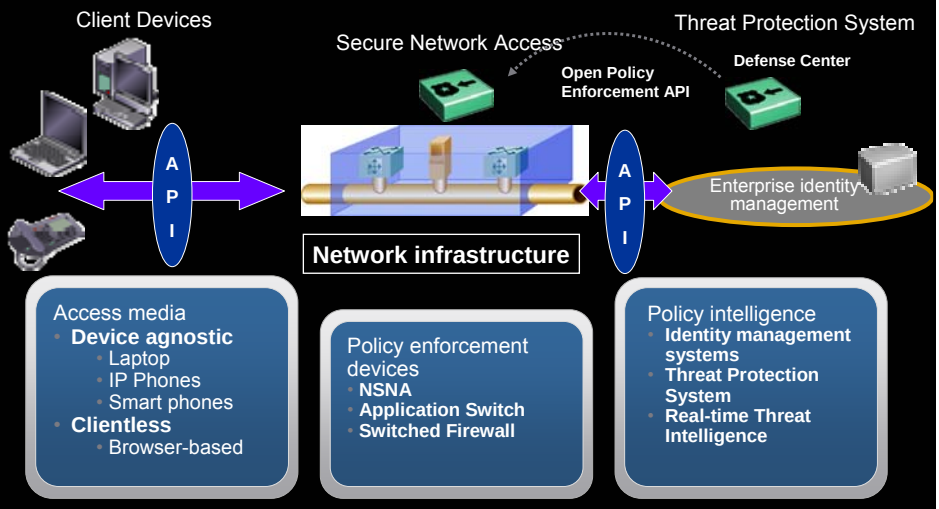


- IPFIX (Netflow 9.x) flow management
  - Standard based implementation
  - L2 and above
    - Destination/source IP address
    - BGP, MPLS labels
    - Bytes In/Out
  - Passive measurement
    - uninterrupted collection of performance data
  - Collection
    - In flow collection
    - Statistical sampling
- Can be used for Autonomic Networking detecting and defending against internal attacks
  - IPFIX detects/reports, Net Mgmt is notified, Policy controller acts !

25 - QUESTnet 2007

Secure Network Access & Threat Protection

Autonomic Networking Defense



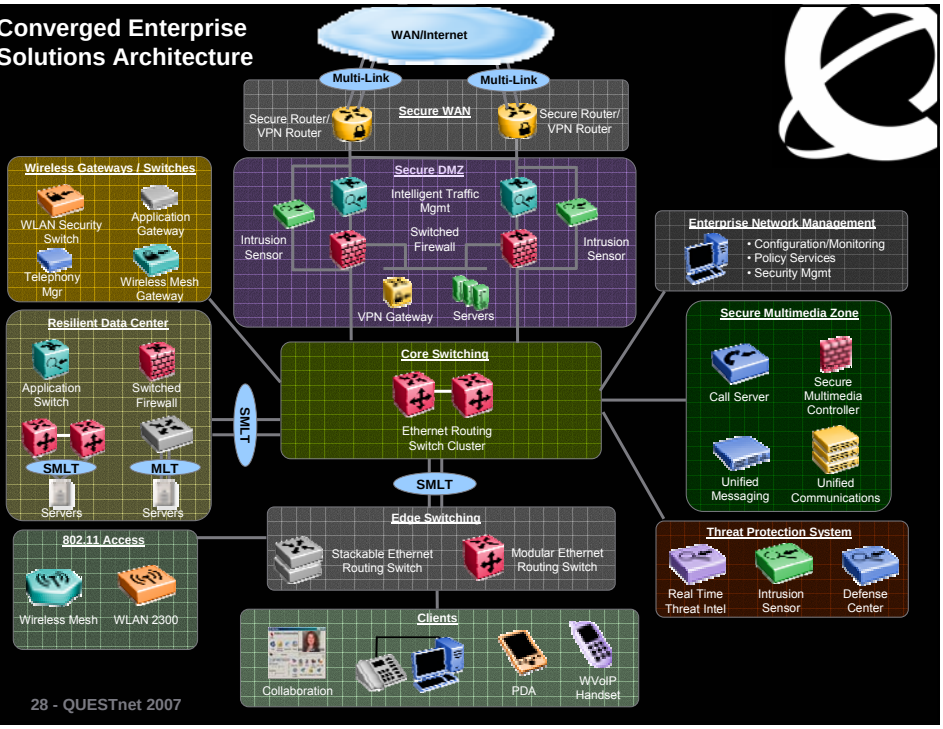
Secure Always-on Networking

"Best Practices"

- Eliminate as many (if not all) single point of failure
- Use Active/Active model for faster recovery and increased forwarding capacity
- Keep it simple, Resiliency ≠ Complexity
- Use Load Balancing, don't leave content idle
- Follow Best Practices recommendations : Converged Campus Solutions
- Ensure your Core & Data Center are protected
- Resiliency & Security go hand in hand
- Understand your business impact tolerance and apply it to your infrastructure
- Do not forget the WAN connectivity – Private or Public (Branch survivability)
- Don't get locked in – Ensure inter-operability and easy transition
- Review Converged Campus Solutions Guide
  - http://www.nortel.com/
    - Search for "Converged Campus Solutions Guide"
- Tolly Reports Web pages
  - http://www.nortel.com/promotions/converged_network_infrastructure/

27 - QUESTnet 2007

Converged Enterprise Solutions Architecture



28 - QUESTnet 2007