



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS  
CONTROLLERS



STORAGE



## ***Future-Ready Infrastructure: Ensuring the Longevity of Infrastructure Investments***

**Networld+Interop, May 2005**

**Nafea Bishara, nafeab@marvell.com**

# Objectives

- Future Enterprise Network Requirements
- Latest and Upcoming Technologies
- Future-proofing the network



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS  
CONTROLLERS



STORAGE

# Problem statement

- Forklift upgrades are expensive, complex and impact business continuity
- However, Networks are getting smarter, more applications, more protocols..
  - Evolving protocols: IPv6, iSCSI, VoIP....
  - Evolving media: 10/100, Gigabit, WiFi
  - Increasing security treats
  - B2B and B2C
  - Increased capacity: more clients, servers, APs.....
  - Mobility
  - .....

# Presentation flow

- Typical enterprise, and network partitioning
- New requirements and challenges all of the enterprise network
- Requirements in specific portions of the networks
- Summary list of the guidelines given



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



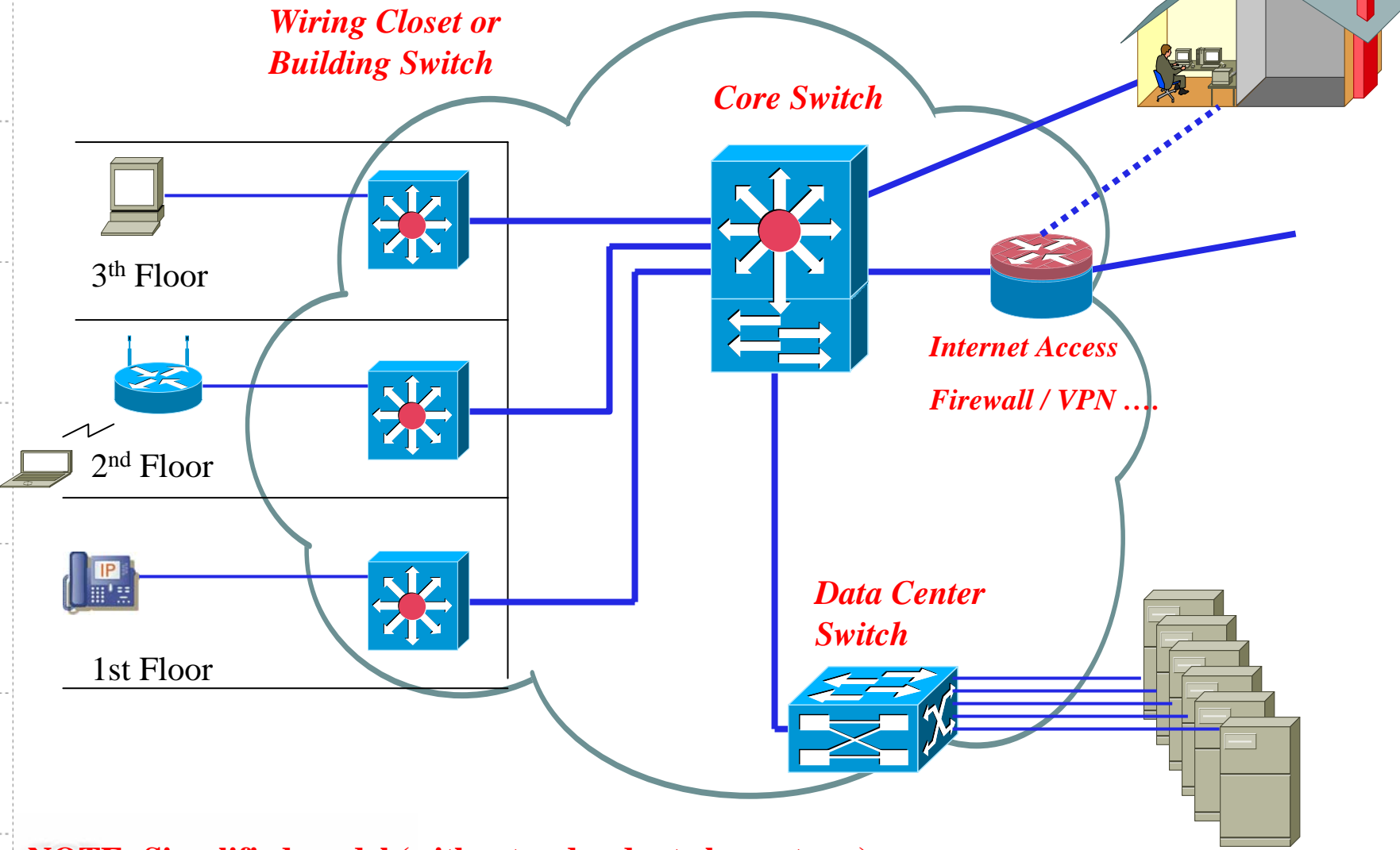
COMMUNICATIONS  
CONTROLLERS



STORAGE

# Typical Enterprise Network

- SWITCHING
- TRANSCEIVERS
- POWER MANAGEMENT
- WIRELESS
- PC CONNECTIVITY
- GATEWAYS
- COMMUNICATIONS CONTROLLERS
- STORAGE



**NOTE: Simplified model (without redundant elements....)**

Marvell Confidential

*Data Center*

# New Requirements and Challenges

- Evolving protocols
- Never-ending security threats
- Mobility
- Capacity scalability
- Management scalability



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS  
CONTROLLERS



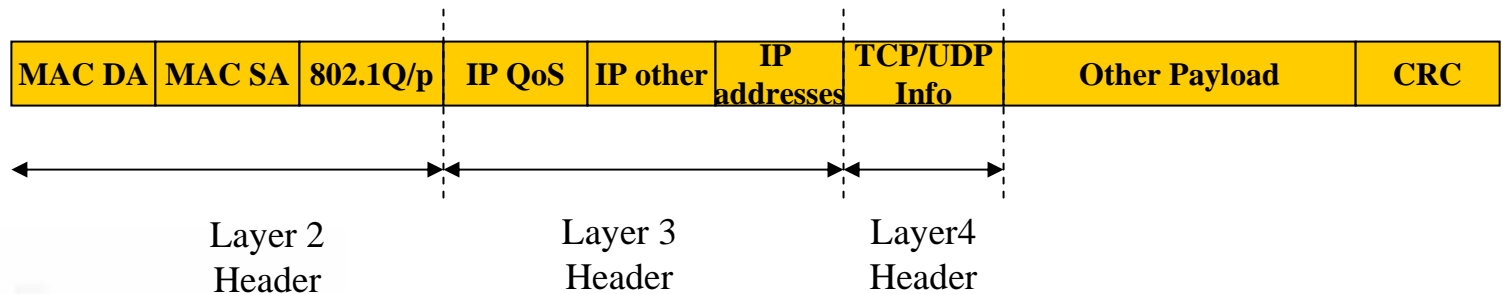
STORAGE

# Network-wide issues - Protocols

- Technology evolves, needs evolves → new protocols

Protocol categories:

1. Network management protocols
2. L2 protocols
3. Internet protocols
4. Multi-media distribution
5. Application protocols



# Network-wide issues – Protocols (Cont)



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

<i><b>Protocol Category</b></i>	<i><b>Example</b></i>	<i><b>Chances to be changed</b></i>	<i><b>Recommend Guidelines</b></i>
Network mgmt	SNMPv3, SSH ... (Does not require hardware upgrade)	Evolves slowly	<b>GL#1 – Make sure networking gear has spare CPU power, memory footprint for future protocol upgrades</b>
	Multiple Spanning tree,.... (Protocols impacting forwarding)	L2 protocols are quite mature	<b>GL#2 – Pick the solution with the latest IEEE and IETF standards, reduce the risk of an upgrade</b>

# Network-wide issues – Protocols (Cont)



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

<i>Protocol Category</i>	<i>Example</i>	<i>Chances to be changed</i>	<i>Recommend Guidelines</i>
Layer 2 data protocols	Ethernet	Products are pretty mature, not much changes	<b>GL#3 – Don't forget to put Cat5 wiring cable</b>

- **But, how about all the new Ethernet standards:**

- 802.1ab
- 802.1ad
- 802.1ae
- 802.3ah
- 802.3ar
- 802.3ap
- 802.3aq

Marvell Confidential

# Latest Ethernet specifications in IEEE



- Remember the background – Ethernet is reaching beyond the LAN
  - Ethernet in the Metro (MAN)
  - Ethernet in Embedded/Backplanes (Server Blades, ATA)
- New applications is driving new requirements. Most of it does not impact Local Area Networks within an enterprise.
- 802.1ad is for Switches used in Service provider networks
- 802.1ae is for securing the Ethernet link – outside the enterprise
- 802.3ah is for service provider network OAM
- 802.3ar/ap/aq is for embedded Ethernet within ATCA chassis and Server Blade
- 802.1ab is the only exception – it is really good for LAN !



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Network-wide issues – Protocols (Cont)



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

<i><b>Protocol Category</b></i>	<i><b>Example</b></i>	<i><b>Chances to be changed</b></i>	<i><b>Recommend Guidelines</b></i>
<b>Layer 2 data protocols</b>	Wireless LAN	Still evolving: 1) QoS and Security protocols side (802.11e, 11i) 2) Management Protocols 3) RF (802.11n)	<b>GL#4 – Pick a WLAN solution with CPU horse power to enable future protocol upgrades (802.11e, 11i)</b>  <b>GL#5 – Centralized WLAN switch is an easier way for future protocol upgrade</b>

# Network-wide issues – Protocols (Cont)



<i><b>Protocol Category</b></i>	<i><b>Example</b></i>	<i><b>Chances to be changed</b></i>	<i><b>Recommend Guidelines</b></i>
<b>Layer 3 data protocols</b>	IP has 99.9% dominance	High, IPv6 !! The biggest change in networking gear, with wide impact and big return	<b>GL#6 – All network gears need to be ready for IPv6</b>
<b>Multicast protocols</b>	Video content distribution, training ..	Pretty stable, due, not deployed much	<b>GL#7 – All network gears need to be ready for L2 (IGMP) or L3 (PIM) multicasting !</b>

# Network-wide issues – Protocols (Cont)



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

<i><b>Protocol Category</b></i>	<i><b>Example</b></i>	<i><b>Chances to be changed</b></i>	<i><b>Recommend Guidelines</b></i>
<b>Application protocols</b>	iSCSI, Oracle, Webmail, Instant messages, Kaaza....	Very high, keeps evolving.	<p>Since most of this is transparent to the network gear, as long as appropriate QoS is provided</p> <p><b>GL#8 – All network gears need to support L2 and L3 QoS, with guarantees</b></p>

# Network-wide issues - Security

- Will continue to evolve, never ending race
- Most difficult challenge, solution must be:
  - Adaptive
  - Rapid response
  - No performance hit
  - Obsequies and non-intrusive
- Solution – Build a future proof security architecture
- Split the security into two:
  - Detection (PDP)– the fastest evolving technology in the enterprise: Intrusion Detection, Content Filters, Distributed DoS probes .....
  - Enforcement (PEP) – blocking or rate limiting based on the detection pattern, provided by PDP



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Network-wide issues – Security (Cont)

- Detection tools, appliances and software will keep evolving
  - ➔ **GL#9: Always stay tuned to latest technologies in attack detections**
- On the same time, the enforcers, residing across the network perimeters
  - ➔ **GL#10: All perimeter devices (Routers, Switches, Access points) must support policy-based filters, at least based on:**
    - Application TCP/UDP port numbers
    - Source identify (MAC, IP....)
- The equipment itself must be bullet-proof for any DoS attack
  - “The network gear has to be secure to secure the network “
  - ➔ **GL#11: Network gear itself must be defensible and protected against DoS attacks**



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Future-proof security architecture

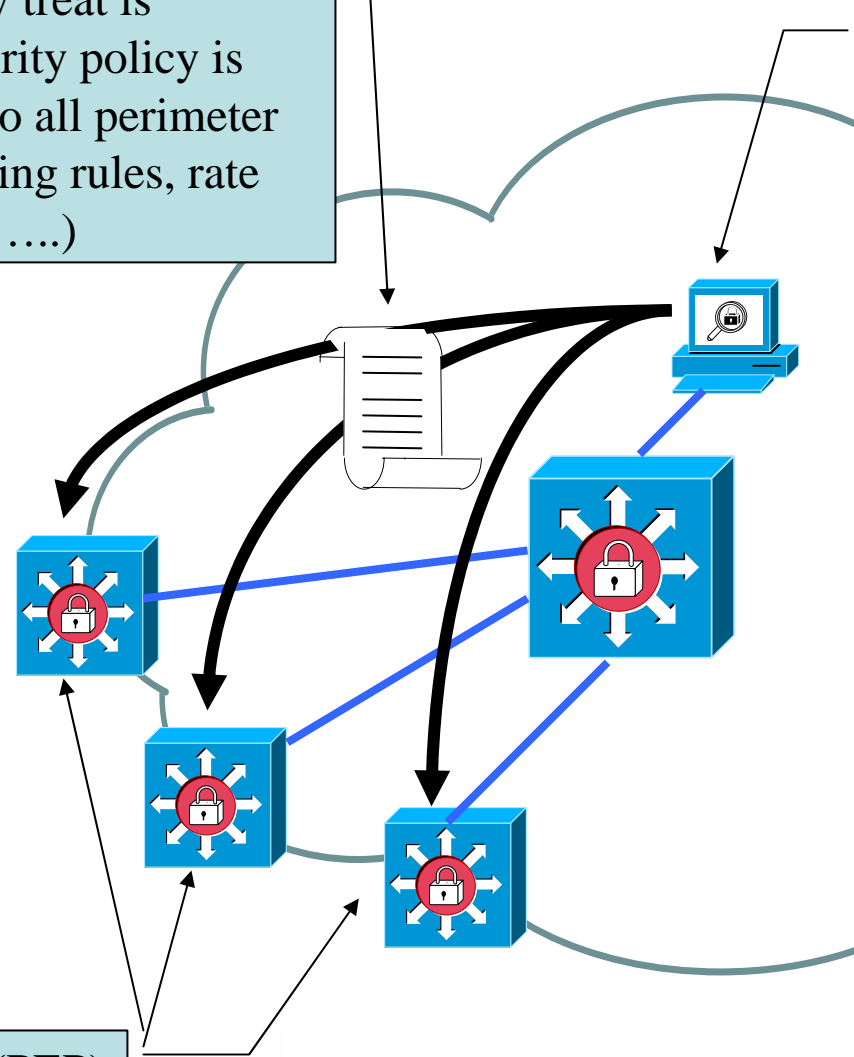


- SWITCHING
- TRANSCENT
- POWER MANAGEMENT
- WIRELESS
- PC CONNECTIVITY
- GATEWAYS
- COMMUNICATIONS CONTROLLERS

When security treat is detected, security policy is driven down to all perimeter devices (filtering rules, rate limiting rules.....)

**Security probes:**

- Firewall, Intrusion detection, Distributed DoS prevention, Content Filter.....
- Keeps evolving, new devices, new probes, new software



Perimeter devices (PEP) must support flexible policy enforcement

# Network-wide issues – Mobility

- More road warriors, remote offices, home offices
- Traditionally mobility has been handled through IPsec-based VPN services. Deployment challenges, Client VPN software
  - ➔ **GL#12: Upgrade to SSL-based VPN is possible. Simpler, more secure, more scalable**
- WLAN is taken enterprises in a storm
  - ➔ **GL#13: Use converge wireless/wireline infrastructure, simpler to manage, police and upgrade**
  - ➔ **GL#14: Stick to standard solutions, avoid proprietary**
  - ➔ **GL#15: Be ready for dense deployment of APs if needed, keep PoE and port count scalability as an option**

# Network-wide issues – Management scaling

- **Must be able to scale in terms of port count, speeds and adding wireless without increasing management complexity**

**GL#16: Pick modular solutions for enterprise infrastructure that allow switch clustering, stacking or chassis. Single IP/CLI/GUI to manage it**

**(This is more than single network management station !**

**GL#17: Integrated wireless/wireless infrastructure**

**GL#18: Centralized network and policy management: LDAP, Radius...**

- **All equipment must support remote monitoring and fault reporting**

**GL#19: Avoid unmanaged infrastructure, ask for remote monitoring (SNMP/GUI), fault tolerance reporting (i.e. TDR)**



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Proper Design of Wiring closet

- When deploying for a new wiring closet, be ready for WLAN, VoIP and port scalability while keeping management simplified

**GL#20: Expect a ratio of 2 ports/user in an enterprise floor (AP, VoIP.....)**

**GL#21: Pick a modular solution (stackable, chassis) that can scale in ports without forklift not creating management nightmare**

- Performance: the infrastructure need to be ready for multimedia conferencing, thin clients or rapid backup, rich media download

**GL#22: Keep 10/100/1000 connectivity to users, APs (ready for 802.11n) and VoIP Phones**



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Ready for Voice/Video over IP

- **VoIP is a fact, application/usage will evolve**  
**GL#23: Standard based VoIP (SIP preferred, H.263 OK)**
- **VoIPoWiFi will catch up very quickly, when you can walk with your WiFi phone in the office uninterrupted**
- **There is no official roaming standard yet, multiple applications exists**
- **Due to lack of standardization, get a commitment from the vendor to support IEEE and IETF standards when they are ratified**  
**GL#24: Wireless infrastructure must support roaming, and VoWiFi handset !**



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Core and Data center

- **Reliability and Resiliency are nonnegotiable**
  - GL#25: Redundancy at every device and every link
  - GL#26: All devices and links to support Ultra Fast Recovery
- **Scalability and density are increasing rapidly**
  - The core and data center are the most sensitive to forklifts
  - In the same time, they are the one the need the performance and density increase the fastest
  - GL#27: Pick a scalable solution that can scale without forklift, i.e. multi-chassis technologies
- **Be ready for 10Gbps interconnects**
  - GL#28: Switch/Router ready for multi-10G
  - GL#29: Use Cat6 cables in data center, ready for 10G over copper



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



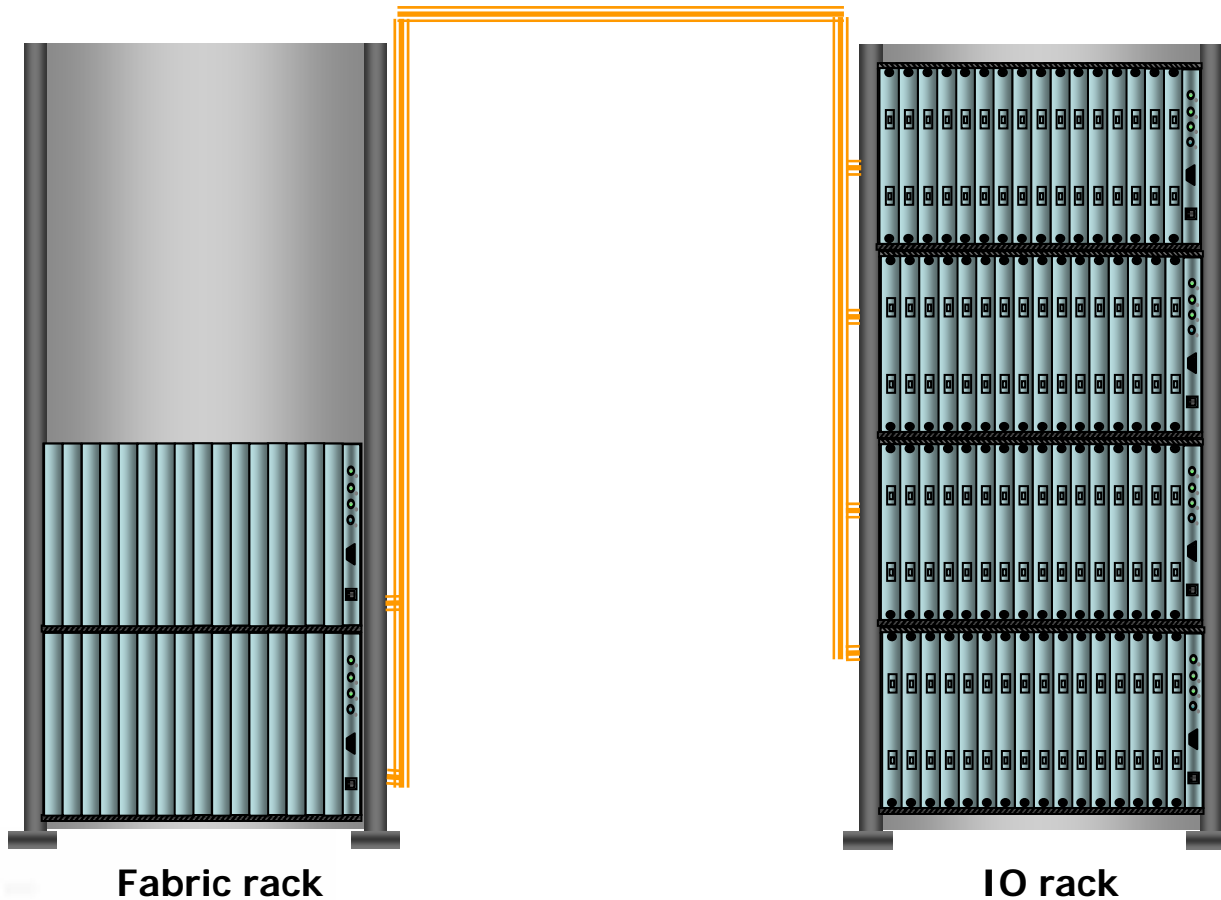
COMMUNICATIONS  
CONTROLLERS



STORAGE

# Core and Data Center (Cont)

- **Scaling the core switch without forklift**
  - Idea already adopted by service providers



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Summary

- We summarized enterprise challenges for next 5 years
- Hard to predict all possible changes
- Simple guidelines can be followed in the network design and equipment purchasing to future-proof the network



SWITCHING



TRANSCIVERS



POWER  
MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS  
CONTROLLERS



STORAGE

# Guidelines Summary

Number	Description
1	<b>Make sure networking gear has spare CPU power, memory footprint for future protocol upgrades</b>
2	<b>Pick the solution with the latest IEEE and IETF standards, reduce the risk of an upgrade</b>
3	<b>Don't forget to put Cat5 wiring cable</b>
4	<b>Pick a WLAN solution with CPU horse power to enable future protocol upgrades</b>
5	<b>Centralized WLAN switch is an easier way for future protocol upgrade,</b>
6	<b>All network gears need to be ready for IPv6</b>
7	<b>All network gears need to be ready for L2 (IGMP) or L3 (PIM) multicasting !</b>
8	<b>All network gears need to support L2 and L3 QoS with guarantees</b>



# Guidelines Summary (Cont)

Number	Description
9	<b>Stay tuned to latest technologies in attack detections</b>
10	<b>All perimeter devices (Routers, Switches, Access points) must support policy-based filters, at least based on:</b> <ul style="list-style-type: none"> <li>•Application TCP/UDP port numbers</li> <li>•Source identify (MAC, IP.....)</li> </ul>
11	<b>Network gear itself must be defensible and protected against DoS attacks</b>
12	<b>Upgrade to SSL-based VPN is possible: Simpler, more secure, more scalable</b>
13	<b>Use converge wireless/wireline infrastructure, simpler to manage, police and upgrade</b>
14	<b>Stick to standard solutions, avoid proprietary</b>
15	<b>Be ready for dense deployment of APs if needed, keep PoE and port count scalability as an option</b>



SWITCHING



TRANSCIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Guidelines Summary (Cont)

Number	Description
16	<b>Pick modular solutions for enterprise infrastructure that allow switch clustering, stacking or chassis. Single IP/CLI/GUI to manage it</b>
17	<b>Integrated wireless/wireless infrastructure</b>
18	<b>Centralized network and policy management: LDAP, Radius</b>
19	<b>Avoid unmanaged infrastructure, ask for remote monitoring (SNMP/GUI), fault tolerance reporting (i.e. TDR)</b>
20	<b>Expect a ratio of 2 ports/user in an enterprise floor (AP, VoIP....)</b>
21	<b>Pick a modular solution (stackable, chassis) that can scale in ports without forklift not creating management nightmare</b>
22	<b>Keep 10/100/1000 connectivity to users, APs (ready for 802.11n) and VoIP Phones</b>



SWITCHING



TRANSCEIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE

# Guidelines Summary (Cont)

Number	Description
23	<b>Standard based VoIP (SIP preferred, H.263 OK)</b>
24	<b>Wireless infrastructure must support roaming, and VoWiFi handset</b>
25	<b>Redundancy at every device and every link</b>
26	<b>all devices and links to support Ultra Fast Recovery</b>
27	<b>Pick a scalable solution that can scale without forklift, i.e. multi-chassis technologies</b>
28	<b>Switch/Router ready for multi-10G</b>
29	<b>Use Cat6 cables in data center, ready for 10G over copper</b>



SWITCHING



TRANSCEIVERS



POWER MANAGEMENT



WIRELESS



PC CONNECTIVITY



GATEWAYS



COMMUNICATIONS CONTROLLERS



STORAGE