Cisco Medical Grade Network Campus Architectures

Michal Remper, CCIE#8151

Account Manager – Public, mremper@cisco.com
What Is the Cisco Medical-Grade Network?

- The Cisco Medical-Grade Network is an optimized architecture for the healthcare industry based on Cisco’s best practices for security, campus, data center, remote office, and wireless networks.

- The Cisco MGN 2.0—campus architecture:
  - Industry-specific framework following a set of proven best practices
  - Provides a mapping of clinical and business needs to technology solutions
  - Optimizes interactions between processes, applications, and technical architecture components
  - Facilitates business and clinical communications throughout the continuum of care
  - Enhances collaboration across the technology partner ecosystem
Cisco’s Medical-Grade Network Framework for Healthcare

Enabled by Borderless Networks

- Allow nurses and doctors to administer patient care from anywhere, anytime through secure wireless capabilities.
- Enable patients and guests to stay connected through secure connectivity.
- Enable an interoperable healthcare ecosystem through a flexible and scalable network framework.
- Meet government and industry mandates through a regulatory compliant architecture (ex: PCI).
- Bring connectivity to the hospital’s infrastructure through automated biomed devices.

Data Center
Cisco Medical-Grade Network Goals

Resilient
- Fault-tolerant and capable of business continuity
- No single point of failure
- Rapid convergence

Protected
- Protection for any patient data on rest and in transit
- Compliant with regulatory requirements
- Posture for each device with ePHI access

Responsive
- Network adapts to change and business/clinical needs
- Has ability to incorporate new technologies

Interactive
- Ability of care providers and vendors to interact with net seamlessly
- Wireless, VPN extends net into BN
- Integrates data, voice, video and imaging
Biomedical Devices

Considerations in Campus Requirements

- **Unique Layer 2 and Layer 3 requirements**
  - Many vendors require separate parallel Layer 2 VLANs
  - Layer 3 and multicast functionality may be limited

- **Traffic Flows Vary**
  - Patient monitors: Small (300 byte), but frequent (4x/sec) broadcasts, multicasts or unicast (vendor-specific)
  - IV pumps: Formulary and firmware updates are usually small and not a daily occurrence
  - Biomedical devices often communicate back to central monitoring station

- **SLA Requirements**
  - Prevent < 50ms jitter
  - Maintain < 20ms connectivity loss from patient monitor to central station

- **Path Isolation may be required**

---

**Patient Monitors**
- Provides real time monitoring of vital signs (blood pressure, oximetry etc) on continuous basis.
- May connect to central station

**Infusion (IV) Pumps**
- Administers medication to patients and requires formulary and drug library updates on an intermittent basis.

**Portable Radiology Devices**
- Connects to the RIS and PACS system.
Biomedical Devices
Wireless considerations

Wireless Challenges

- **Special RF Requirements**
  - Vendor specific requirements for 802.11 a/b/g/n usage
  - Dedicated SSIDs interference elimination recommendations, etc.

- **Varying Authentication/Encryption Methods**
  - WEP, WPA, WPA2
  - 802.1x not common on today's biomedical devices

- **Unique Layer 2 (L2) and Layer 3 (L3) requirements**
  - Many vendors require separate parallel Layer 2 VLANs
  - Layer 3 and multicast functionality may be limited
  - A 1:1 SSID/VLAN mapping generally required or recommended

- **Traffic Flows Vary**
  - Patient monitors: small (300 byte), but frequent (4x/sec) broadcasts, multicasts or unicast (vendor-specific)
  - IV pumps: formulary and firmware updates are usually small and not a daily occurrence
  - Biomedical devices often communicate back to central monitoring station
  - Portable radiology devices store studies on the PACS while the device is in use at the point of care
**Patient Monitor Wireless Guidelines**

- **RF Requirements**
  - 1:1 SSID/VLAN mapping
  - 25 dB min SNR co-channel separation

- **Authentication and Encryption**
  - Utilize WPA or WPA2

- **Unique Layer 2 and Layer 3 requirements**
  - Dedicate separate VLAN for each patient monitor vendor type
  - Layer 3 and multicast functionality may be limited

- **SLA Requirements**
  - Prevent <50ms jitter
  - Maintain <20ms connectivity loss from patient monitor to central station, QoS !!!
What’s Available and on the Horizon

Mobile Units
- Stationary Care: Patient comes to the clinic
- Mobile Care: Care comes to the patient
- Tandberg Carts

Desktop Video
- Desktop care: Low cost, Low-bandwidth

Mobile Devices
- SmartPhones
- Wireless Tablets
- Mobility
Clinical Systems

Wireless Challenges

- Legacy applications intolerant of connectivity loss due to signal or roaming issues
  
  If designed for LAN and not tuned for WAN/VPN/WLAN some applications may fail to respond or recover

- Wide range of implementations/requirements
  
  Even within a single vendors product line bandwidth, security, chattiness, delay tolerance may vary

- Patient privacy
  
  Protected Health Information (PHI) will be in the data transmitted across the network
  
  Access security and encryption must be used end-to-end

- Varied Wireless Client RF Characteristics
  
  Wireless clients of different models or vendors may have significantly different roaming or receiver sensitivities
# Healthcare Requirements in Campus

## Clinical App Requirement

### Biomedical Devices
- Mission critical
- Some layer 2 adjacency demands, L3 considerations
- Central station connectivity requirements
- Endpoint security

### Clinical Devices and Systems
- Mission critical
- Jitter/latency demands
- HIPAA and privacy
- Wired and wireless considerations

## Medical Grade Network

### Medical Grade Network
- Highly availability (fast recovery and convergence)
- Path isolation
- Flexible L2 and/or L3 to access
- Network access control and Identity based

### Clinical App Requirement
- Highly availability (fast recovery and convergence)
- Protection of ePHI and clinical systems
- Compute/storage/virtualization within Data Center
# Healthcare Requirements in Campus

## Clinical App Requirement

### PACS and Modalities
- Large image transfer
- Storage demands
- Quick access/retrieval
- Geographically remote modalities

## Medical Grade Network

- High throughput
- High availability
- Compute/storage/virtualization within Data Center

## Regulatory and Security

- HIPAA/joint commission
- Payment card industry
- Local country regulatory (EC 95/46)
- IEC-80001
- Fulfilling meaningful use requirements

## Intrusion prevention and patch management
- Device identity and access control
- HiTRUST
- Cisco security intelligence operations
# Healthcare Requirements in Campus

## Clinical App Requirement

### Guest Services
- Wireless
- Network access control
- Acceptable use policy
- Visiting physician access

### Voice/Video/Collaboration
- Emerging trends
  - Medical device integration
- Cisco Healthcare solutions
  - HMI collaboration, Nurse Connect
  - Biomed NAC, Health Presence etc

## Medical Grade Network

- Internet access and logical segmentation
- Network admission control
- Posture assessment
- Acceptable use policy

### Quality of service
- Network responsiveness
- Network interactivity
- Modular design
An Optimized Network Architecture for the Healthcare Industry
Hierarchical designs

No single points of failure

Utilize in box redundancy

Optimize convergence

Best practices must adapt to unique healthcare requirements

R&S enables such interconnection

Legacy Apps and devices result in suboptimal, overlay design, often dedicated networks
MGN 2.0
Wireless Architecture

Cisco Catalyst® 3750G Integrated Wireless LAN Controller

Cisco ISR Wireless LAN Controller Module

Cisco Catalyst 6500 Wireless Services Module (WISM)

Wireless LAN Controller (WLC)

Voice and QoS Enabled L3 Access Switches

NAC
MSE
ACS
WCS

Third-Party Integration to RTLS (Nurse Call, BioMed, EMR)

MGN 2.0 Campus

Wireless Management PC—Browser Based

SSC

© 2011 Cisco Systems, Inc. All rights reserved.
Cisco MGN 2.0 Campus Design

- **Access**
- **Distribution**
- **Core**
- **Distribution**
- **Access**

Layer 3 stackable switches

VSS Access

VSS Distribution

VSS/Hybrid Core

Data Center 10Gbps Nexus

WAN
MGN High Availability Campus Design

- Eliminate all single points of failure
  - Implement hierarchical designs
  - Utilize redundant chassis or smart stackable switches
- Redundant switching and power fabrics
- In the box and network redundant services
- Utilized IGP protocols that quickly detect faults and provide sub-second failover
Supervisor Redundancy Is Provided by Stateful Switch Over (SSO)

- Active/Standby supervisors run in synchronized mode
- Depending on platform, line card and protocol this incurs from 0 to 3 seconds of outage
- Switch processors synchronize Layer 2 and Layer 2/Layer 3 FIB, QoS and ACL tables
- Line cards with DFC are populated with Layer 2/Layer 3 routing information and ACL tables
- Line card protocol status is maintained during failover reducing impact and improving clinical access
Healthcare Campus Challenges

Age Old Problem
- Remember old days of flexibility, add/move and mobility promise?
- Spanning VLAN solved that and created some more problems of
  Stability
  Response times
  Inefficient use of resources
  Managing end host behavior

Historically —A Compromise
- Do not span VLANs.
- No Loops no underlying threat to the network
- Solution gave up critical need of not able to span VLANs.
- However, in many healthcare deployments, clinical and biomedical devices requires vendor dedicated VLANs
Virtual Switch
Virtual Switching System 1440 (VSS)

- Virtual Switching System consists of two Cisco Catalyst 6500 Series defined as members of the same virtual switch domain
- Single control plane with dual active forwarding planes
- Design to increase forwarding capacity while increasing availability by eliminating STP loops – a loop-free topology
- Reduced operational complexity by simplifying configuration

![Virtual Switch Domain Diagram](image)
Virtual Switching

- Solving the same **old** design problem and yet not lose the benefits of stability and mobility

- Virtual Switching allows elimination of loops in the network, while allowing for spanning of VLANs

```
VLAN 10  VLAN 10  VLAN 10
VLAN 20  VLAN 20  VLAN 20

VSS Enabled Loop Free Topology
VLANs spans Access-switches
```
VSS Enabled Healthcare Campus Design
End-to-End VSS Design Option

STP-based Redundant Topology

\[ \text{R} = \text{STP Blocked Link} \]

Fully Redundant Virtual Switch Topology
Three Options for Multi-Chassis EtherChannel Designs to Remove Spanning Tree

Virtual Switching System
- Single control plane
- Single management plane
- Single supervisor per chassis
- Automatic port config sync (single control plane)
- Single L3 domain (single SVI) **no need for FHRP**

Virtual Port Channel
- Separate control plane
- Separate management plane with VPC state synchronization (CFS)
- Redundant supervisors per chassis with hitless SSO
- Manual port sync config (DataCenterNetworkMgr)
- Local SVI **HSRP/PIM forwarding enhancements to act as active-active pair**

Stackwise+
- Single control plane controlled by Master Switch
- Master switch controls etherchannel
- Redundant master switches per stack
- Automatic port config sync (single control plane)
- Stack appears as a single router, **no need for FHRP**
Campus Design Option: VSS

Key Benefits to Healthcare Providers

- Eliminates complexity of Spanning Tree Protocol and prevents potential for loops in network.
- Faster failover by eliminating need for gateway redundancy protocols (HSRP, VRRP, GLBP)
- Simplified network management (less links/configuration, fewer operational points)
- Conserves bandwidth (no unicast flooding, MEC optimizes number of hops)
Environmental Considerations

Power
- Separate grid based power feeds
- Building based Backup Generator Power
- Localized UPS Power especially for PoE deployments
- Redundant Power Supplies

Cooling
- Examine BTU generation compared to HVAC systems
- Redundant HVAC chillers on separate power
- Consider rRack design for front to back vs side to side airflow

Physical Security
- Monitor and maintain access to IT infrastructure
- Log access to key distribution areas
- Utilize video surveillance
- Take precautions to prevent unauthorized access and prevent data loss

Monitoring
- Use 802.11 based thermal & humidity monitoring
- Implement smart building technologies (Cisco Connected Real Estate) for power and cooling monitoring
- Track battery health for localized UPS devices
- Utilize under floor water detectors

Cisco Medical-Grade Network 2.0
Convergence of Biomedical and General Purpose IT Networks

- In the past – biomedical devices lived on dedicated networks/frequencies, no IT connection
- Biomedical devices very expensive – no HA
- Vendors touch IT networks – adoption IP and Eth
- Due to the regulatory and vendor restrictions – results in unpatched OS running critical apps
- Biomedical devices very fast populate IT networks – Network Virtualization and Path Isolation Requirements in Healthcare Networks !!!
Biomedical Devices
Path Isolation Options

- Generic Routing Encapsulation (GRE) Tunneling
  Create Closed User Groups

- Virtual Routing and Forwarding (VRF-lite)
  Lightweight
  Single routing device

- Multiprotocol Label Switching (MPLS)
  Cisco Catalyst 6500

- Overlay Transport Virtualization (OTV)
  Emerging Technology in Data Center

For More Information:
Functional Elements in Virtualized Campus Networks

Access Control
- Branch - Campus

Path Isolation
- WAN - MAN - Campus
- GRE
- MPLS
- VRFs

Services Edge
- Data Center - Internet Edge - Campus

Functions
- Authenticate client (user, device, app) attempting to gain network access
- Authorize client into a Partition (VLAN, ACL)
- Deny access to unauthorized clients
- Maintain traffic partitioned over Layer 3 infrastructure
- Transport traffic over isolated Layer 3 partitions
- Map Layer 3 Isolated Path to VLANs in Access and Services Edge
- Provide access to services: Shared, Dedicated
- Apply policy per partition
- Isolated application environments if necessary
IEC 80001: Application of risk management for IT-networks incorporating medical devices

- IEC-80001 is a voluntary international standard, dealing with risk management of IT networks incorporating medical devices
- Provides framework for the “Application of risk management for General purpose IT-networks incorporating medical devices”
- Three “Key Properties”—Safety, Effectiveness, Data and System Security
- Four supplementary documents or Technical Reports (TR’s) in development:
  - Wireless Guidance
  - Healthcare Delivery Organization (HDO) Step-by-Step guide
  - Security Guidance
  - HDO Implementation Guidance
QoS in Healthcare

- Convergence of medical systems onto a common network with ubiquitous access to info rises the potential network congestion and app failure

- Clinical Apps
- Medical Devices
- PACS
- Voice
- Video and Collaboration
- Network Control Protocols
- Device Control Protocols
- Guest Services
- Standard IT Traffic

**QoS necessary ... !!!**
## Medical Grade Network QoS Classifications

<table>
<thead>
<tr>
<th>Application Class</th>
<th>Per-Hop Behavior</th>
<th>Queuing and Dropping</th>
<th>Medical Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>CS6</td>
<td>BW Queue</td>
<td>Constant Bit Rate Biomed Feeds</td>
</tr>
<tr>
<td>VoIP Telephony</td>
<td>EF</td>
<td>Priority Queue (PQ)</td>
<td>Constant Bit Rate Biomed Feeds</td>
</tr>
<tr>
<td>Broadcast Video</td>
<td>CS5</td>
<td>(Optional) PQ</td>
<td>Cisco Healthcare, Telepresence</td>
</tr>
<tr>
<td>Realtime Interactive</td>
<td>CS4</td>
<td>(Optional) PQ</td>
<td>Cisco Unified Personal Communicator</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF4</td>
<td>BW Queue + DSCP WRED</td>
<td>Cisco Unified Personal Communicator</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF3</td>
<td>BW Queue + DSCP WRED</td>
<td>*Biomedical Telemetry Streaming</td>
</tr>
<tr>
<td>Call-Signaling</td>
<td>CS3</td>
<td>BW Queue</td>
<td>*Biomedical Devices, Critical Apps, WebEx</td>
</tr>
<tr>
<td>Ops/Admin/Mgmt (OAM)</td>
<td>CS2</td>
<td>BW Queue</td>
<td>PACS, Large File Apps</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>AF2</td>
<td>BW Queue + DSCP WRED</td>
<td>*Biomedical Devices, Critical Apps, WebEx</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF1</td>
<td>BW Queue + DSCP WRED</td>
<td>Back Office, Archiving, Patient Records</td>
</tr>
<tr>
<td>Best Effort</td>
<td>DF</td>
<td>Default Queue + RED</td>
<td>Back Office, Archiving, Patient Records</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>Min BW Queue (Deferential)</td>
<td>Guest Traffic</td>
</tr>
</tbody>
</table>
QoS Boundaries

- Summary of trust, marking, policing and queuing boundaries
- Correct Trust and Markings at Access
- Interswitch links in Campus will trust DSCP markings
- Perform Policing and Queuing where appropriate

For More Information:
Campus Voice and Collaboration Considerations

Challenges

- In Order to Provide Optimal Patient Care, Collaboration Among Caregivers is Essential

- Due to the Critical Nature of the Collaboration both the Campus Infrastructure and the Collaboration Systems Must be Constantly Available

- The Diversity of Caregivers Requires that a Wide Range of both Wired and Wireless Endpoints Must Be Supported
Campus Voice and Collaboration Considerations

- Power over Ethernet
  - Switches
  - End Points
- Voice over WLAN
  - VoWLAN QoS
  - Multicast
- Unified Communication
  - UC Manager Resiliency
  - Security
  - Session Manager Edition
  - SRST

For More Information:
Voice over Wireless LAN

Wireless Challenges

- Tighter Specifications than Data Wireless
  More overlap required
  Site survey essential

- Pervasive Coverage
  Including: Elevators, stairways, building walkways, campus grounds, parking garages

- Fast Roaming
  Poor roaming performance may drop or impair active voice calls

- Quality of Service
  Call quality impacted by jitter, delay, and signal quality
Voice over Wireless LAN

- **Security Recommendations**
  - Authentication—EAP-FAST
  - Key Management—WPA
  - Encryption—TKIP
  - Fast Roaming Protocol—CCKM

- **AP Placement**
  - AP Cell Boundary at -67dBm
  - AP Cell Overlap of 20%
  - Channel Separation of 19dB (CCA)
Guest Services—Wireless Architecture

Wireless Guest Services

- Provides patients and guests with wireless access to specific hospital “walled garden” resources or Internet
- Supports Login, Anonymous, and Acceptable Use Policy acceptance
- Can be provided by the hospital utilizing hospital’s Internet resources, or outsourced to a third-party wireless guest service provider utilizing existing WLAN infrastructure
Authentication and Access Control

- Who, when, where and how a group of individuals is allowed to use MGN services
- Cisco’s Network Access Control and BioMedical NAC Integration:
  - Physical access control
  - IP video surveillance
  - Door lock controllers
  - Badge or biomedical readers
  - Alarm controllers
  → Smart+Connected Control System