Redesigning the Wireless Network for IoT

Session #116, February 21, 2017
Gary Horn, V.P. Technical Services & CTO Advocate Health Care

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.
Speaker Introduction

Gary Horn, MSEE

V.P. Technical Services & CTO
Advocate Health Care
Conflict of Interest

Gary Horn, MSEE
Has no real or apparent conflicts of interest to report
Agenda

• About Advocate
• What is IoT
• IoT Trends
• Security and IoT
• IoT and the Business
• Wireless Networking
• Containerization
• IoT Value Proposition
Learning Objectives

• List key network capabilities that hospital systems must put in place to accommodate the growing movement towards mobility
• Identify the steps necessary for ensuring security when adding IoT devices to the network infrastructure
• Discuss the patient, caregiver, and operational benefits that can be achieved from moving to a mobile-first hospital environment
• Describe how the wireless network has become a strategic asset to modern hospital systems
• Describe how network policy and priorities must be updated to address IoT wireless technologies
Summary of Operational Benefits

Ease of wireless network administration
Elimination of proprietary wireless networks
Enhanced wireless infrastructure allows for significant increase in devices
Single point of wireless control and monitoring

Operational Savings

Containerization isolates critical IoT traffic flows
In-depth network monitoring and control
Comprehensive patch and vulnerability management
Better outcomes through real-time data and analytics
Enhanced Safety through real-time monitoring

Enhanced Network Security
Clinical Outcomes
Advocate Health Care

• Largest health system in Illinois
• 250 sites of care, including 12 hospitals and the state's largest integrated children’s network
• Best Places to Work in Illinois (Daily Herald/Business Ledger)
• 35,000 associates, 6,000 affiliated physicians and 10,000 nurses
• Thirteen-time recipient of Hospitals & Health Networks 100 “Most Wired” award
• Academic and teaching affiliations with all major universities in the Chicago Metropolitan area
• Advocate is committed to create the safest and best place for patients to heal, physicians to practice and associates to work. Safety, quality, service - Always
The Internet of Things

What does it all mean?
What is the IoT?

• … is the network of physical objects not limited to devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data
• IoT goes by various names but the concept is the same
  – M2M (Machine to Machine)
  – World Size Web (Bruce Schneier)
  – Internet of Everything - IoE (Cisco Systems)
• IoT is everywhere
IoT Is Everywhere!
IoT (M2M) World of Connected Services

The Healthcare and Life Sciences Service Sector

- **Care** - Hospitals, ER, Mobile POC, Clinics, Doctor Office, etc.
- **In Vivo/Home** - Implants (pace makers, etc.), Home Monitoring Systems
- **Research** - Drug Discovery, Diagnostics and Lab equipment
The Growing Trends of Mobility and IoT

1.5B Smartphones shipped in 2016 *1

270B App Downloads by 2017 *2

Enterprise mobile app. X4 by 2018 and 60% of apps created will have no PC antecedent *4

IoT endpoints will grow to 20.8B units in 2020 *3

83% of the 22M smart eyewear devices shipped in 2019 will go to enterprise use cases *5

*1 IDC press release on 03Mar2016 - http://www.idc.com/getdoc.jsp?containerId=prUS41061616
World of Wearable Applications

- Wearables collect a huge amount of personal data as well as environmental information.
- Significant impact on privacy rights of these technologies requires a careful review.
- Great concern for health-related sensitive data (i.e. medical devices and fitness applications).
- Confidential info easily disclosed to 3rd parties.
- A significant threat to the enterprise perimeter.

Individuals as a Data Cluster
The Basic Concerns Around IoT

• An IoT device is just another computer, correct?
  – All of the same issues with vulnerability management, access control monitoring, patching, etc.
  – High-impact with hundreds of thousands or more IoT devices on the network
  – Any compromised device can take a foothold on the network

• What additional risks does IoT Pose?
  – Definition of the network perimeter (objects not designed to be Internet connected)
  – Device capture during vulnerability scans
  – Consumer devices interfering with critical network devices and services
  – Lack of device management software
  – Data breaches and inadvertent breaches
  – An easy attack vector
IoT Security

• Why IoT Devices are subject to attack
  – Difficult to update OS and firmware
  – Default, weak, or hardcoded credentials
  – Vulnerable web interfaces (XSS, SQL injection)
  – Poor vendor support
  – Coding errors (buffer overflow)
  – DoS / DDOS
  – Physical theft and tampering
  – Clear text protocols, unnecessary services, and unneeded open ports

• What has been learned from recent IoT related incidents
  – Vendors delay or ignore response to issues
  – All software and firmware can and probably does contain vulnerabilities
  – Product lifecycles & end-of-support ignored
  – Patching IoT devices often does not scale well in large environments
  – Significant delay in informing the public of vulnerabilities and related issues
IoT Security Recommendations

• Cover IoT devices within current practices
  – Awareness Training
  – Procedures, policies, and standards
  – Forensics
  – Risk management
  – Vulnerability Management

• Plan for continued IoT growth
  – Enhance wireless infrastructure
  – Additional logging and log storage
  – Upgrade firewalls, IPS, and IDS
  – Increase available network bandwidth
  – Availability of IP addresses, both IPv4 and IPv6
  – Network segmentation and containerization
    • Traditional or SPB-M
  – Enhance partnerships with vendors, procurement groups
IoT Deployment Strategies
Two Driving Forces Shaping Tomorrow’s Digital Business

The Evolving Digital Business

**Network Infrastructure**
- Higher resilience
- Comprehensive security
- More wireless coverage
- Higher performance
- Low latency
- IoT traffic containment

**Mobility**
- Connectivity anywhere
- More apps diversity
- More devices/person
- Faster response time
- Beyond employees

**IoT**
- More lines of Business adopting IoT
- More devices to connect
- PoE for direct IoT power
- Beyond carpeted areas

Increased dependency on the network
Typical IoT Demands Coming from Business Units

• Operational
  – Freedom to deploy devices when and where they want without asking permission from IT
  – Their own Ethernet network for traffic segregation (quality/integrity)
  – Seamless endpoint connectivity

• Technical requirements (between IoT platform and endpoints)
  – L2 broadcast
  – QoS
  – Fixed IP addressing
  – Fixed VLAN numbering

• Security
  – Prevent inappropriate endpoint access
  – Concern with compliance
Company & IT Concerns

- High cost of independent networks
- Procurement
- Deployment
- Maintenance
- Cabling
- Operations and administration
- Overall asset security
- Training
- Overhead and depreciation
Healthcare Depends on Wireless Networking

• Patient Benefits
  – Quality of care
  – Modern applications such as telemetry, infusion pumps, glucometers, etc.
  – Patient experience
  – In-room services

• Caregiver Benefits
  – Staff efficiency
  – Mobile communications; nurse call integration
  – Physician retention
  – State-of-the-art applications

• Facility Benefits
  – Emergency preparedness
  – Adaptive capacity
  – Cost containment
  – Asset utilization through RFID
  – RTLS for patient tracking
  – Internet of Things (IoT)

Floor nurses average 36 minutes per shift walking to a phone

Wireless networking has become a strategic resource
Wireless Distributed Enterprise

AirWave Network Management

Mobility Controller

ClearPass Access Management

NOC

Internet / WAN

Home Office

 instant / RAP

Branch Controller

CAPs

Branch

OR

Mobility Switch

Instant Cluster

Virtual Intranet Access (VIA) Client

On The Road

Home Office

 instant / RAP

Branch Controller

CAPs

Branch

OR

Mobility Switch

Instant Cluster

Virtual Intranet Access (VIA) Client

On The Road

Home Office

 instant / RAP

Branch Controller

CAPs

Branch

OR

Mobility Switch

Instant Cluster

Virtual Intranet Access (VIA) Client

On The Road
Redesigning The Wireless Network

The enterprise network infrastructure has to dynamically adapt

Ubiquitous connectivity, simple access, always on, anywhere, any device, anytime to provide a consistent high-quality user experience
Unified Access Strategy

✓ Provide a seamless, consistent high quality user experience
✓ Simplify operations and improve network security
✓ Protect investment

Network Operations & Programmability

<table>
<thead>
<tr>
<th>User Management</th>
<th>Device Management</th>
<th>Application QoS</th>
<th>Application Analytics</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Media</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE/GigE</td>
<td>802.11n/ac</td>
</tr>
</tbody>
</table>

Same network services on wired and wireless
802.11ac Waves 1&2

160 MHz Channel

160 MHz channels cannot be used in enterprise environments (yet): currently only two channels available

802.11n: 64-QAM
40 MHz
Wave 1: 256-QAM
80 MHz
Wave 2: 256-QAM
160 MHz

160 MHz Channel

Four Spatial Streams

3 SS (wave 1) 4 SS (wave 2)

Limited number of clients currently support 4SS due to space and power

Rates:
Wave 1: up to 1.3Gbps
Wave 2: up to 3.4Gbps

Single User MIMO (wave 1)

Multi User MIMO (wave 2)

Clients need to support wave 2

160 MHz Channel

1SS
1SS
1SS
1SS

160 MHz

80 MHz

40 MHz

802.11n: 64-QAM
Wave 1: 256-QAM
Wave 2: 256-QAM

160 MHz

160 MHz Channel
802.11ac Wave 2: Prepare the LAN

- Most Wave 2 AP’s require PoE+ (30W) and potentially more than 1Gbps LAN connection
- 10GbE lacks PoE and is cost prohibitive
- Invest in access switches that support the 802.3bz multi-gig standard that can run on existing Cat 5e/6 cabling
- Cost of an additional cable pull to support multi-gigabit throughput: $300-$1000
- Wave 1 leverages existing PoE/PoE+ and 1GbE access - no need to upgrade the wired network

Multi-gigabit standard: IEEE 802.3bz

Make sure you have PoE+, 10G uplinks on switches and edge switches that are compatible with 802.3bz for 2.5GBASE-T
Secure and Scalable IoT Deployment

An IoT Container is a secure virtualized network

- Accessible only by compliant devices
- Contains only the traffic from the IoT system
- Provides the quality necessary to run the IoT application successfully

Enabled by a single network with simple operations, high reliability, and tight security
IoT According to Gartner
The Business Benefit of the IoT Container

Endpoint connectivity is standardizing on Ethernet, Wi-Fi, wireless gateways, and PoE
IoT Containers: Why Choose SPB-M?

Network requirements
• Increase bandwidth utilization
• Resource optimization
• Reduce latency
• High availability
• Simple management
• Consistent SLA enforcement
• SLA monitoring
• Security
• Dynamic access and mobility
• Micro-segmentation

SPB response
• All network links are use
• Spanning Tree Protocol replacement
• Uses the shortest path end to end
• Natively protect failures and reroute
• End-point provisioning
• Symmetrical and congruent paths
• OAM capabilities
• Flexible and scalable service separation
• Extended L2 domain
• Each SPB-M service is a single layer 2 virtual network and can scale to 16.7 Million separate services
One Network Using Traditional VLANs

ONE Network
Intelligent Fabric
Auto Virtual Chassis
Auto Topology
Self Healing

Network Virtualization
Biomedical Facilities
Office Automation

Office Automation Network
Profiling for Policy Enforcement

User Profile
- Network Provisioning
- Security Profile
- Quality of Service
- Priority

User Device

Universal Profile
- Authorize
- Classify
- Auto Provision
  - Container
  - Quality/Priority
  - Security

- Container: VLAN, ISID
- Quality/Priority: QoS, Bandwidth
- Security: ACL, App Visibility & Control
IoT Containers
Independent, secure, and simple moves, adds and changes

- Universal Profile
  - Authorize
  - Classify
  - Auto Provision
  - Container
  - Quality
  - Security

Biomedical Network
Sensor VLAN
Actuator VLAN
IoT Value Proposition
The IoT is propelled by an exceptional convergence of trends: mobile phone ubiquity, open hardware, big data, Artificial Intelligence, cloud computing, 3D printing, and crowdfunding

The world is rapidly evolving to where just about everything will be connected

The number of cyber attacks will rapidly increase

Privacy and security must be fully addressed

So...

If misunderstood and misconfigured, IoT poses risk to data, privacy, and safety

But...

If understood & secured, IoT will enhance communications, lifestyle, and delivery of services
Pros and Cons of the IoT

• Automation and Control
  – Efficient M2M communication results in time savings
• Information and Big Data
  – Knowledge is power
• Communication
  – Complete transparency, fewer inefficiencies, and greater quality
• Monitor
  – Real-time measurement of just about anything
• Overall quality of Life

• Compatibility
  – No high-level international standard
• Complexity
  – Many points of failure, technical and operational
• Privacy and Security
  – Sensitive data in the wild
• Safety
  – Manipulation of data
• Loss of human skills
  – Social interaction
Summary of Operational Benefits

Ease of wireless network administration
Elimination of proprietary wireless networks
Enhanced wireless infrastructure allows for significant increase in devices
Single point of wireless control and monitoring

Operational Savings

Containerization isolates critical IoT traffic flows
In-depth network monitoring and control
Comprehensive patch and vulnerability management
Better outcomes through real-time data and analytics
Enhanced Safety through real-time monitoring

Enhanced Network Security
Clinical Outcomes
Questions

Gary Horn
gary.horn@advocatehealth.com
https://www.linkedin.com/in/gary-horn-1936366