Healthcare Network Pain: Causes and Treatments

Terry Slattery
Steve Meyer

Your Level of Pain?

Wong-Baker Faces Pain Rating Scale
Agenda

• Healthcare Requirements
• Typical Network
• Operational Needs
• Healthcare Network Case Study

Healthcare Requirements

• Improving healthcare
  – Avoid errors
  – Improve timeliness and quality of care
  – Reduce frequency and duration of visits
  – Increase efficiency of operations

• Similar to requirements in many businesses
Cisco Medical-Grade Network Goals

- Resilient
  - Fault-tolerant and capable of business continuity
  - No single point of failure
  - Serves mission-critical needs

- Protected
  - Security for patient privacy and system availability
  - Compliant with regulatory requirements
  - Protection against security breaches

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

- Interactive
  - Facilitates Collaboration
  - Enables application access
  - Integrates data, voice, video and imaging

Cisco Medical-Grade Network 2.0

IT As An Enabler

- Life-critical systems
- Clinical systems
- Admission processing & back office
- Electronic Medical Records (EMR)
IT As An Enabler (cont.)

• Enhancing productivity, improving outcomes

How IT and Networking Can Help

• Resilient networks
• Adequate bandwidth
• Application support
• Data Center
• Wireless & mobile devices
• Security
Redundant vs Resilient

- **re·dun·dan·ce (r-dndn-s) n.**
  6. *Electronics* Duplication or repetition of elements in electronic equipment to provide alternative functional channels in case of failure.

- **re·sil·ience (r-zlyns) n.**
  1. The ability to recover quickly from illness, change, or misfortune; buoyancy.

- **Resilient networks**
  - Tolerate single failures
  - Gracefully degrade with multiple failures
  - Quickly recover when a failure is repaired

Network Design

- **Understand failure modes**
  - Design around them
  - Avoid single points of failure

- **Limit failure domain size**
  - Avoid STP between data centers
  - A/B halves of big data centers
  - Separate services subnets

- **Fast failover**
  - Bi-directional Forwarding Detection
  - Non-Stop Forwarding
Network Design (cont)

- Data center connectivity options
  - TRILL: Transparent Interconnection of Lots of Links
  - Cisco OTV: Overlay Transport Virtualization

Redundancy

- Data center, devices, and links
  - Properly located
  - Capacity to handle load
- First Hop Redundancy Protocols
  - HSRP/GLBP (Cisco), VRRP (multi-vendor)
  - Each has unique operating characteristics
- Allow link capacity for redundancy
  - Beware of uplink oversubscription
  - Need 100% in reserve or suffer degraded service in an outage
- Excessive redundancy is bad
## Application Support

- **Clinical & Life-Critical**  
  - Multicast vs broadcast to find server
- **Voice & Video**  
  - Nurse call functionality  
  - Telemedicine and medical robotics
- **QoS – prioritize patient applications**  
  - De-emphasize streaming entertainment audio

<table>
<thead>
<tr>
<th>QoS Class Names</th>
<th>Layer 3 DSCP Markings</th>
<th>IPP / CoS Markings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>CS8</td>
<td>48</td>
</tr>
<tr>
<td>Voice / IP Telephony</td>
<td>EF</td>
<td>46</td>
</tr>
<tr>
<td>Clinical Life Critical</td>
<td>CS5</td>
<td>48</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
<td>34</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
<td>32</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
<td>26</td>
</tr>
<tr>
<td>Call Signaling</td>
<td>CS3</td>
<td>24</td>
</tr>
<tr>
<td>Low-Latency Data</td>
<td>AF21</td>
<td>18</td>
</tr>
<tr>
<td>CIR (Net Metric)</td>
<td>CS2</td>
<td>18</td>
</tr>
<tr>
<td>High-Throughput Data</td>
<td>AF11</td>
<td>10</td>
</tr>
<tr>
<td>Low-Priority Data</td>
<td>CS1</td>
<td>8</td>
</tr>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

## Data Center

- **Electronic Medical Records**  
  - Mobile device access (VDI with Citrix, etc)  
  - Computing & Storage  
  - High availability - see CIO Magazine reprint  
  - Private cloud
- **Data retention policies**  
  - How long?  
  - Common or independent repository
- **Network infrastructure**  
  - Non-stop operation  
  - High bandwidth (moving to 10G)
Wireless

- High density
  - 30ft - 40 ft separation (1 AP/1500 sq ft) & 802.11a
  - AP transmit power management

- Mobile devices
  - Smartphones, tablets, wireless VoIP phones
  - Patient data on the device?
  - Sharing devices among staff

- EMR support
  - Sufficient bandwidth?
  - Reliability for thin client

- FDA regulated (see ComputerWorld reprint)

EMR over Wireless

- Case Study With EMR Vendor
  - Poor network performance over wireless
  - Researched possible problems (NICs, settings, etc)
  - Onsite: settings OK; 802.11b; big zones; many clients
  - Ping EMR server from WoW (Workstation on Wheels): 125-250ms !!!
  - Ping drops to 5ms??
  - Vendor: Just finished transfer of patient data
  - How much data? 15MB to each of 3-4 WoWs

- Conclusion: self-inflicted DoS
Context is Important

Security

• Payment Card Industry (PCI)
• HIPAA
• Protecting patient health information
  – Mobile devices
  – Journalists seeking info on famous patients
• Secure medical collaboration
  – Research data
  – Video conferencing
  – Telemedicine
• Plus typical security
Agenda

• Healthcare Requirements
• Typical Network
• Operational Needs
• Healthcare Network Case Study

Typical Network

• Big Layer 2 domains
• Some redundancy
• Some EMR and telemedicine
• Minimal Quality of Service (QoS)
• Small network staff
• Inconsistent security
• Limited network management
Big Spanning Tree Domains

• Convenient and easy
• What are some problems with Spanning Tree?
  – Spanning tree loops - how do you diagnose them?
  – Root bridge location – at the end of a WAN link?
  – Spanning tree diameter – 7 hops
  – See CIO reprint
• Remedies
  – Loopguard, Rootguard, BPDUguard
  – Root Bridge selection
  – Layer 3 (routing)

Redundancy

• Excessive redundancy
  – Partial mesh
  – Failure engineering is difficult
  – Too many alternate paths
  – More expensive
• Redundancy failures
  – HSRP/VRRP/GLBP
  – Redundant hardware failure (PS, Sup, etc)
  – How to detect?
Engineering Failure Paths

- Hub, spoke, & wheel design
- 6 Pkt/Sec in/out each site
- Routing failure; unidirectional path
- Inbound traffic takes alternate path
- Alternate path is overloaded, causing it to fail!
- Result?
  The network traffic oscillates!!

Inconsistent Redundancy

Internet

Area 4

Area 1

Area 6

Area 3

Area 2

Area 5

Area 0

Area 8

Area 7

Area 9

Area 10

Area 11
Organized Redundancy

Documentation - Which Is Clearer: A
Video and Telemedicine

- Often driven by individual doctors
  - Research funding
  - Collaboration with other doctors
  - Teaching (video to/from classrooms)
  - Reduce travel time (and cost)
  - Aid difficult-to-reach patients

- Needs QoS

- Case Study:
  - Brain surgeon evaluating concussions
  - Displays: Medical record, brain scans, video link with patient
Electronic Medical Records

- Different levels of adoption & implementation
  - Significant cultural shift
  - Often coupled with VDI (no patient data on devices)
- Requires increased network availability

Quality of Service

- Multiple traffic classes – all Important
  - Voice
  - Interactive video
  - Streaming video
  - EMR
  - Server-to-server traffic flows
- Unimportant
  - Streaming entertainment (audio & video was 50% of traffic in one case)
  - Who watches March Madness?

<table>
<thead>
<tr>
<th>QoS Class Names</th>
<th>Layer 3 QoS Markings</th>
<th>IPV / CoS Markings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>CS6</td>
<td>6</td>
</tr>
<tr>
<td>Voice / IP Telephony</td>
<td>EF</td>
<td>46</td>
</tr>
<tr>
<td>Clinical Life Critical</td>
<td>CS5</td>
<td>49</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
<td>34</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
<td>32</td>
</tr>
<tr>
<td>Multimedia Streaming</td>
<td>AF31</td>
<td>26</td>
</tr>
<tr>
<td>Cell Signaling</td>
<td>CS3</td>
<td>24</td>
</tr>
<tr>
<td>Low-Latency Data</td>
<td>AF11</td>
<td>10</td>
</tr>
<tr>
<td>QAM (Net Mgmt)</td>
<td>CS2</td>
<td>16</td>
</tr>
<tr>
<td>High-Throughput Data</td>
<td>AF11</td>
<td>10</td>
</tr>
<tr>
<td>Low-Priority Data</td>
<td>CS1</td>
<td>6</td>
</tr>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

EMR
Small Network Staff

- Network viewed as “plumbing”
- Variable staff support
  - Tools
  - Training on tools
  - Processes and procedures for using the tools and their findings
- Older equipment
- Minimal network management

Inconsistent Security

- Complexity of security
  - Accessible to those who need it, yet protected
  - Compliance with many standards (PCI, HIPAA, etc)
- Technology categories for healthcare

<table>
<thead>
<tr>
<th>Category 1</th>
<th>User authentication, access rights, termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 2</td>
<td>Transmission and encryption</td>
</tr>
<tr>
<td>Category 3</td>
<td>Network security</td>
</tr>
<tr>
<td>Category 4</td>
<td>Logging, tracking, monitoring</td>
</tr>
<tr>
<td>Category 5</td>
<td>Remote access</td>
</tr>
<tr>
<td>Category 6</td>
<td>Wireless security</td>
</tr>
<tr>
<td>Category 7</td>
<td>Anti-virus and patch management</td>
</tr>
<tr>
<td>Category 8</td>
<td>Database security</td>
</tr>
</tbody>
</table>
Agenda

- Healthcare Requirements
- Typical Network
- Operational Needs
- Healthcare Network Case Study

Operational Needs

- Good design
- Current technologies
- Appropriate configurations
- Processes & procedures
- Network management
Good Design

- Structured, understood architecture
  - Based on known design principles
  - Good redundancy design - resilient
  - Easily understood
  - Easy to troubleshoot
  - Minimize failure modes – understand existing failure modes

- Our network is unique
  - Unique problems
  - Not good!

Current Technologies

- Stay current with best practices
  - Reduce STP w/ vPC
  - Layer 2 between DC without STP
  - Improved security

- Designs to support new initiatives
  - Using all uplinks
  - Greater need for 10G
  - Converged networking
  - Increase performance in the access layer
Appropriate Configurations

• Enable desired features

“Just because you can, doesn’t mean you should…”

– Production network is NOT a playground
– Limit failure domains
– Security features (of the devices and the network)
– Network management

Processes & Procedures

• Operational actions that enact the policies

• Procedures
  – What steps to take
  – Which switch ports to unplug to break a loop
  – What to do when a security event is detected
  – How to move a call center

• Processes
  – Defined conditions for enacting procedures
  – How STP loops are detected and when to execute the loop break procedure
  – Mechanisms for detecting and reporting security events
  – What triggers a call center move
Processes & Procedures

• Failure planning and procedures
  – Call server (or other mission-critical server) dies
  – Move a call center in natural disaster situation

• Configuration and change management
  – Change control board
  – Configuration update mechanism
  – Test plans & rollback

• Automatic ticket generation
• ITIL – Visible Ops Handbook

Network Management Architecture
Logging

• Syslog-ng
  – Central logging
  – Feeds other tools
  – Correlate w/ device & interface importance

Summary report
  – Mailed daily
  – Pinnacle errors
  – Environmental
  – Parity errors

Performance & Error Monitoring

• High utilization
• High errors
  – Impacts performance and productivity
  – Customers may not report: *It’s always slow.*
  – One site: 20 interfaces with > 1M packet errors/day
• Duplex mismatch common
Configuration Management

- Configuration archive
  - Keep all configurations
  - Changes: who, what, how, when, where

- Configuration compliance
  - Compliance with policies
  - Remediation of exceptions

**Policy**
- Hostname
- Internal DNS
- Internal NTP
- Router loop back

**Template**
- hostname router
  - ip name-server 10.1.1.12
  - ntp server 10.1.1.12
  - interface lo0
    - ip address 10.2.X.Y

**Device Config**
- hostname b3-core-1
  - ip name-server 10.1.1.12
  - ntp server 10.1.1.12
  - interface lo0
    - ip address 10.2.1.1

Configuration Management (cont)

- Configuration policy checks
  - Security, routing, switching, interfaces

- Config push mechanism required
  - Update 600 devices in an hour
  - Notification when an update fails
  - Apply update only when appropriate

⚠️ Warning

Message:

Config file does not contain any lines matching 'logging 10.2.50.223'.
Configuration Management (cont)

- **Analyze operational data**
  - Configuration not saved
  - HSRP peer not found
  - Spanning tree too large
  - Interface discards: congested link
  - Subnet mask inconsistent

- **Automate the analysis**
  - Manual processes don’t scale

<table>
<thead>
<tr>
<th>Severity</th>
<th>Last Seen</th>
<th>Title</th>
<th>Status</th>
<th>Component</th>
<th># Affected</th>
<th># New</th>
<th># Res</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>2011-03-20 09:30:33</td>
<td>Policy Violation: L. Leaping</td>
<td>Current</td>
<td>Configurations</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>2011-03-20 09:31:45</td>
<td>VLAN Member Priority</td>
<td>Current</td>
<td>VLANs</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>2011-03-20 09:31:26</td>
<td>VLAN Member Minimum Priority</td>
<td>Current</td>
<td>VLANs</td>
<td>164</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>2011-03-20 09:27:59</td>
<td>HSRP Not Recognizing Peer</td>
<td>Current</td>
<td>Routing</td>
<td>8</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Trouble Ticket System

- **Trouble ticket generation**
  - Pick biggest problems
  - Automatic generation for critical errors and events

- **Making tickets visible**
  - Email and dashboards
  - Incentives for correctly fixing problems
Network Management

- Proactively identify problems and remediate
  - Manual processes don’t scale
- Architecture - FCAPS
  - Events – log analysis
    - Fault, Accounting, Security
  - Configuration management
    - Configuration, Security
  - Performance
    - Performance, Fault, Accounting
- Mechanism to automatically identify problems

Testing

- Lab facility – replicate key network components
- Production testing – use maintenance windows
- What to test
  - Devices & links
  - Protocol failures: STP loops & routing
  - High utilization on links (tests QoS)
  - Services subnet failure (simulates DoS attack)
  - Failover to backup DC, devices, paths
- Understand the impact on voice & video
- It’s like fire drills for your network!
The Cost of Network Downtime

• Varies by industry
  – $264: The cost of a minute of HIS downtime, 500-bed hospital ($15,840/hr)
  – Each incremental 1% of downtime per year could cost a 500-bed hospital more than $1.4 million
  – Excludes the cost of errors in healthcare

Source: Healthcare Informatics

<table>
<thead>
<tr>
<th>Industry</th>
<th>Business Operation</th>
<th>Industry Cost Range Per Hour</th>
<th>Average Cost Per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Brokerage</td>
<td>5.6 to 7.3M</td>
<td>6.43M</td>
</tr>
<tr>
<td>Financial</td>
<td>Credit Card Sales</td>
<td>2.2 to 3.1M</td>
<td>2.6M</td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation</td>
<td>Airline</td>
<td>67 to 112K</td>
<td>89.9K</td>
</tr>
<tr>
<td>Transportation</td>
<td>Shipping</td>
<td>24 to 32K</td>
<td>28K</td>
</tr>
<tr>
<td>Retail</td>
<td>Catalog Sales</td>
<td>60 to 120K</td>
<td>80K</td>
</tr>
</tbody>
</table>

Source: Dataquest, in Performance Technologies whitepaper

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Outages</th>
<th>Degradations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>72%</td>
<td>28%</td>
</tr>
<tr>
<td>High tech</td>
<td>15%</td>
<td>85%</td>
</tr>
<tr>
<td>Health care</td>
<td>33%</td>
<td>67%</td>
</tr>
<tr>
<td>Travel</td>
<td>56%</td>
<td>44%</td>
</tr>
<tr>
<td>Finance (U.S.)</td>
<td>53%</td>
<td>47%</td>
</tr>
<tr>
<td>Finance (Europe)</td>
<td>51%</td>
<td>49%</td>
</tr>
</tbody>
</table>

Source: telephonyonline.com/analysts/infonetics/telecom_cost_network_downtime/

Conclusion (Part 1)

• Emphasize design strengths
  – Avoid common failures

• Employ automation
  – Manual processes don’t scale
  – Reduce human error

• Be prepared for failures

• Incremental improvement
  – Proactively detect and remediate failures in redundant systems