Infrastructure Administration: Automated Infrastructure Management (AIM) Systems

Gene E. Malone, Sr. – RCDD
TE Connectivity
• Review relevant Content of Automated Infrastructure Management (AIM) systems in the draft revision of TIA-606-B

• Determine which capabilities of AIMs are important, appropriate and useful

• Evaluate any benefits and drawbacks of Different AIM technologies
Needs and Reasons for Sound Network Administration
Needs and Reasons for Sound Network Administration
Needs and Reasons for Sound Network Administration

The need for thorough cabling infrastructure administration is driven by the desire to:

- Reduce the labor expense of maintenance
  - Faster Diagnosis
  - Ease of navigation
  - Improved MAC Coordination

(Enable focused tasking and assignments)
Needs and Reasons for Sound Network Administration

The need for thorough cabling infrastructure administration is driven by the desire to:

- Extend the useful economic life
  - Better utilization of equipment
  - Controlled Migration/Upgrades
  - Improved accountability of Assets

(The Network is realized as a valued asset)
Needs and Reasons for Sound Network Administration

The need for thorough cabling infrastructure administration is driven by the desire to:

• Provide effective service to users
  – Improved service provisioning
  – Improved MAC processes/coordination
  – Enables Physical Layer as a service

(IT focus shifts to proactive support of the USER)
Needs and Reasons for Sound Network Administration

The need for thorough cabling infrastructure administration is driven by the desire to:

• Increase the value of the owner’s investment
  – Extends network controls to physical layer
  – Quality and history of the Network is logged
  – Improves Physical layer Security and accountability

(Documented Networks are Transferable)
The need for thorough cabling infrastructure administration is being driven by:

- Larger Network Infrastructures
- Increased Complexity
- Increased Administrative Burden
- Increasing Importance of Information on the IT Network

Universal Administration Standards improve the use, control and servicing of the network
How standards are addressing the technology

ANSI/TIA-606-B (Currently In Ballot)

This standard provides guidelines and choices of classes of administration for maintaining telecommunications infrastructure.

With the participation of over 30 Organizations, this standard replaces ANSI/EIA/TIA-606-A dated May 2002.
Evaluating the Complexities of Network Administration
Physical Layer Connectivity
The foundation of every network

Layer 1
Physical Layer

Layer 2
Data Link
Switches

Layer 3 and Above
Network Layer
Routers, Servers and Storage

Desktop / Laptop

IP Phones

Managed Connectivity delivers availability, security and compliance
Technology is providing solutions

Network Administration methods, process and technology had remained relatively static until convergence of the ITS pushed Traditional Network Administration into the new millennium.

New process, Cable management software and Automation technology have been developed and introduced Globally.
Traditional Methods

• **Individual or Personal Memory**
  – We’re only human...

• **Written Ledger**
  – How legible is your handwriting?

• **Software Spreadsheet**
  – No standard report formats
  – Many spreadsheets are difficult to sort or read.
Modern Methods

- **Cable Management Software (CMS)**
  - Introduces documentation and reporting tools
  - Requires Inclusion in the Update Process
  - Requires Strict process adherence and discipline
Modern Methods

• Inference Based systems (IBs)
  – Utilizes a CMS
  – Limited Automation Functionality
  – Changes are inferred by chronological/step order
  – Historical logs and reporting are available
  – Requires Strict process adherence
Modern Methods

• Automated Infrastructure Management (AIM)
  – Utilize CMS
  – Changes are detected automatically as they occur
  – Processes can be monitored
  – Documentation is automatic
  – Historical logs and reporting are available
  – Records are more accurate
  – Security is enhanced

(AIMs are recommended for Class 2-4 Networks)
AIM systems are typically comprised of:

- Cable Management Software (CMS)
- Detection Hardware (or scan-able Labels or Tags)
- Process and controls
  - MAC controls
  - Alerts and notifications

Automated systems strive to provide transparent processes and controls to the IT staff’s day-to-day operation.
Available AIM Technologies

Commercially available AIM Systems include:

- 10-Wire Patch based systems
- RFID based systems
- Chip based systems
- 9\textsuperscript{th} Wire Continuity Based systems

Above is a representative sampling of AIM systems. Other systems, methods and processes are available but less wide-spread.
Cable Management Software (CMS)

• **Pros:**
  – Provides Documentation tools
  – May rely on Bar Code or Text Labeling
  – Introduces canned reporting capabilities
  – Typically tied to strict MAC process controls

• **Considerations:**
  – Not automated
What technologies are available

Inference Based systems (IBs)

• **Pros:**
  – Introduces Limited Automation
  – Provides Documentation tools
  – Provides canned reporting capabilities
  – Tied to strict MAC process controls

• **Considerations:**
  – Patching process is singular ‘one link at a time’
  – No Retrofit of existing panels (proprietary Panels)
  – Technology not typically applicable directly to switches
  – Process (failure) is easily fooled or corrupted
What technologies are available

10-Wire Patch Systems

• **Pros:**
  – Automated Patch detections
  – Provides canned reporting capabilities
  – Provides Monitored MAC process

• **Considerations:**
  – Proprietary Jack & Plug (10-position)
  – Not retrofitable
  – Technology not typically applicable directly to switches
RFID-Based systems

• **Pros:**
  – Automated Patch detections
  – Can imbed patch cord details on RFID chip
  – Provides canned reporting capabilities
  – Provides Monitored MAC process

• **Considerations:**
  – Proprietary ‘Tags’
  – Not retrofittable
  – Technology not typically applicable directly to switches
  – Introduces RF into the patch panel
What technologies are available

Chip-Based AIM systems

• Pros:
  – Automated Patch detections
  – Imbeds Manufacturer details on Components
  – Automated detection of Network build
  – Provides single ended detections
  – Provides canned reporting capabilities
  – Provides Monitored MAC process

• Considerations:
  – Not retrofittable
  – Technology not typically applicable directly to switches
What technologies are available

9th Wire Continuity AIM Systems

• **Pros:**
  - Automated Patch detections
  - Support Dry Contact Integration
  - Provides canned reporting
  - Provides Monitored MAC process
  - Mature technology
  - Broadest Industry Support / Availability
  - Supports Cross-Patch and Cross-connect architectures

• **Considerations:**
  - Requires 9th wire Cords
  - Only detects full connects or disconnects (no single ended)
AIM Features

• Improved and timely Diagnostics
• Holistic Physical Layer circuit traces
• Floor-plan Displays
• Graphical Rack Elevations
• Work-Order (MAC) processes
• Security enhancement and Rogue detection
• Network-Attached-Asset management
• ‘Instant Audits’ and structured reports
• Environmental Sensor Monitoring
AIM Features

• Improved and timely Diagnostics
AIM Features

• Holistic Physical Layer circuit traces
AIM Features

• Floor-plan Displays
AIM Features

• Graphical Rack Elevations
AIM Features

- **Work-Order (MAC) processes**

  **Manager** – Approves work requests for release as work orders, assigns appropriate technician and timing to perform the work.

  **Planner** – Receives, assigns and defines tasks to satisfy requests.

  **Technician** – Performs work order per instructions.

  **Requestor** – Originates the work request.

* Work orders can be pushed digitally to the patch field, allowing technicians quick and easy access to work tasks and verification in the field.
AIM Features

- Security enhancement and Rogue detection
AIM Features

• Network-Attached Asset-management
AIM Features

• ‘Instant Audits’ and structured reports

Information Technology Audit Report

Audit Objectives:

• To assess [Name of Company/Group]’s information systems
• To determine whether [Name of Standard] was met

Overall conclusion:

Based on our observations, the [Name of Standard] was met in most cases. However, there were some exceptions which required remediation.

Summary of Findings:

The audit team noted [specific exceptions]. Recommendations for improving future performance [optional suggestions].

Types of Report:

Type I - Initial Audit
Type II - Follow-up Audit
Type III - Irregular Audit

Building

<table>
<thead>
<tr>
<th>Building</th>
<th>Floor</th>
<th>Location</th>
<th>Enclosure (if Applicable)</th>
<th>Network Device</th>
<th>Class</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WG5</td>
<td>hq-ws-175</td>
<td>Workstation</td>
<td>192.168.0.51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WE6</td>
<td>hq-ws-179</td>
<td>Workstation</td>
<td>192.168.1.180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WG6</td>
<td>hq-ws-182</td>
<td>Workstation</td>
<td>192.168.1.164</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WH4</td>
<td>hq-ws-183</td>
<td>Workstation</td>
<td>192.168.0.36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WE3</td>
<td>hq-ws-187</td>
<td>Workstation</td>
<td>192.168.7.104</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WF5</td>
<td>hq-ws-193</td>
<td>Workstation</td>
<td>192.168.1.199</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Headquarters</td>
<td>02</td>
<td>02WE4</td>
<td>hq-ws-181</td>
<td>Workstation</td>
<td>192.168.1.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remote Building

<table>
<thead>
<tr>
<th>Building</th>
<th>Floor</th>
<th>Location</th>
<th>Faceplate</th>
<th>Total # of Jacks</th>
<th># of Free Jacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Building 01</td>
<td>01</td>
<td>1B6</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Remote Building 01</td>
<td>01</td>
<td>1B7</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Remote Building 01</td>
<td>01</td>
<td>1C6</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Remote Building 01</td>
<td>01</td>
<td>1C7</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
AIM Features

- Environmental Sensor Monitoring
Benefits

• Reduces cost and burden of documentation
• Provides remote visibility
• Reduction in Downtime
• Improved MAC coordination and verification
• Planned changes are visualized and verified
• Improved Equipment efficiencies
• Reduced Disaster Recovery cost
• Enhanced layer-1 security and accountability
Considerations

• Cost of Deployment
• Increased Footprint (in some systems)
• Restricts Network Architecture/Standards
• Requires Strict Process Adherence
• Periodic Audits needed to verify accuracy
• Is it compatible with Facility drawing formats
• Interfacing with Facilities work order systems
• Is it Power Management interface able
Return on Investment (ROI) for AIMs vary by size, Make, Architecture, and Criticality of the network.

Typical AIM system ROI:
• Data Center / SANs Environment (4-9 Months)
• Remote Site Management / Campus or WAN (9-12 Months)
• Traditional Office building network (9-18 Months)

On-going maintenance and support of the system are fractions of the cost to continue manual documentation processes.
Summary

Successful IT depends on coordination between different services, competencies and departments within an organization.

AIM is a key element for aligning and assisting IT Service Management with business processes and for controlling IT services according to customer needs.
Thank You

The benefits of a good AIM outweigh the associated costs of not managing the ITS.
Thank you!