

Management and Security Issues for IP-PBX's – Lessons from the Trenches

David Stein, Principal
Ken Agress, Senior Consultant

Agenda

- Introductions & Background
- Transitioning From Vendor Team to Your Team
- Handling the First Problems
- Common First Year Problems
- Essential Management Tools
 - FCAPS
 - What Do You Need to Know?
 - How Does Management fit into Your Staffing Model?
 - FAQ's and Examples
- Securing Your System
 - Threats to be Aware Of.
 - “Defense in Depth”
 - Mitigation Techniques
 - Lessons Learned
 - FAQ's and Examples

Firm Background

PlanNet Consulting

- Independent communications technology consulting (voice, data, video, cabling, AV, Infosec)
- Project consulting and managed services for wide range of enterprises
- Sixth VOICECON! , Many other conference presentations
- Numerous articles in BCR

Ken Agress

- 16 years communications experience
- Extensive network, performance experience

David Stein

- 25 years in communications technology
- Managed hundreds of voice and data projects

Services



Physical Infrastructure



Communications Technology



Systems and Storage



Information Security



Business Continuity



Managed Services

Transitioning From Vendor Team to Your Team

- First – Define Who’s on the Transition Team
 - Vendor PM?
 - Vendor Technicians (Lead/Trainer/All)?
 - Key Staff Resources
 - Voice Support
 - Data Support
 - Help Desk
- Second – Define Roles Clearly
 - “The winning respondent shall provide no less than three on-site technicians from the date of cut-over until one week after formal system acceptance...”
 - “The winning respondent shall provide problem identification and resolution assistance for all aspects of support from date of cut-over until...”
- Third – Don’t Let the Vendor PM Leave Until You’ve Accepted the System!

Setting up a Successful Transition

- Require on-site assistance from your vendor for some period after system acceptance and during the cut-over period
 - Be specific as to roles provided (Help Desk, Voice Specialist, Data Specialist, General Support)
 - Be realistic about staffing levels required (you will pay for this in fees)
 - Include requirements in the RFP
- Before the cut-over occurs, begin transition meetings with your staff and the vendor's team to:
 - Define who will fill what role
 - Determine where resources will be located during cut-over
 - How much "On The Job Training" will be provided
 - How issues will be escalated.
- Place staff and vendor resources where they're likely to do the most good (no sitting around in "War Rooms")!

Your First Days After Cut-Over

- Get Non-Help Desk Staff Out and About!
 - Immediate assistance to those with problems is “good press” even if things are going wrong.
 - Allows you to use simple tools (raising a flag, waving a colored cloth) in critical areas to attract support personnel.
 - Helps to prevent the Help Desk from becoming a support bottleneck.
- Have Your Staff “Shadow” Vendor Support
 - Learning troubleshooting approaches is at least as important as understanding configurations and technologies.
 - “Real World” experience with experienced staff helps build their confidence.
 - Allows you to phase in your staff as a replacement for vendor with immediate assistance available.
- Make Sure Your Dispatch Team is Up To Speed and Able to Communicate.

Handling Your First Problems

- Gear Your Approach to Your Staff's Skill Levels
 - Do you want the vendor to take the lead?
 - Do you want your staff to lead and the vendor “consult” on direction and decisions?
 - Who will be on the phone with the manufacturer for the first support calls?
- Pay Attention to the Early Issues
 - Look for end-user training issues, and direct resources appropriately.
 - Look for staff training issues and identify areas for additional study/courses.
 - Make sure the vendor is playing their role effectively.
 - Use help desk logs, trouble tickets, staff and end users as feedback for system acceptance.
- Involve IT/Voice Management in Early Problems if it Will Help Ensure Positive Outcomes

Moving on From the First Problems

- Make Sure the Vendor Provides a Well Documented “Run Book”
 - Know what was installed
 - Know how it was configured
 - Make sure changes have been logged properly
 - Make sure management tools are running properly prior to acceptance
- Push Your Staff to Lead Problem Identification and Resolution as You Move Towards Acceptance
 - Vendor Staff should become assistive, not codependent.
 - But don’t let the vendor “off the hook” for contracted support.
 - Find a reason to call manufacturer support to learn their systems and what they’ll want to know.
- Verify That Change and Configuration Management Policies are Being Followed!

What to Prepare For...

- Converging Support Groups Adds Challenges
 - “Support by Committee” is likely to be a new factor (and an issue)
 - Many organizations are too quick to let go of voice support staff.
 - “Language Barriers” can create issues (a pilot will help here)
- Remember that PBX projects can be “emotionally charged”
 - Staff may resist new roles and responsibilities.
 - The groups they support may be neutral or negative regarding the new system.
 - The quality (and timing) of training will greatly impact the support load.
- Staff will need time to make good use of new tools, adjust to processes.

Common First Year Problems

- Making Significant Design Changes “On The Fly” or Without Careful Consideration
- “Ad Hoc” Purchases (Usually Headsets)
- Outdated or Infrequently Updated Auto-Attendant Recordings
- Sorting Out What the Help Desk Does
- Firewall Configuration Issues
- Call Routing/Coverage Holes
- Voice Clipping and Similar Codec Issues

More Common First Year Problems

- Mistakes Configuring Devices Result in Unforeseen Issues and Consequences
- Bugs, Bugs, Bugs...
- Echo Issues
- Carrier finger-pointing (everything is the new system's problems)
- Unexpected or new application flows cause bandwidth/quality issues
- Accurately predicting impact of changes on voice and data flows
- Voice flaws are relatively "chaotic" and may shift for unforeseen reasons

Essential Management Tools

- Convergence adds complexity, calls for improved tools.
 - Do you want routine reports on call quality?
 - Do you need to be able to isolate and analyze specific application or call flows?
 - Do you want proactive notification of likely issues?
- Selecting the right tools is more important than “just deploying something.”
 - Focus tool purchases on your mission critical support goals.
 - Involve support staff (heavily) in selection process.
 - Look beyond systematically manufacturer offerings!

Before You Buy a Tool . . .

- Adopt a “Manage the Service” Approach
 - Raw performance statistics aren’t likely to be all you need.
 - Tie the metrics you measure to goals and service levels.
 - Leverage reporting capabilities to provide visibility to management executives, key users.
 - Remember - It’s the user experience that matters.
- Ensure your hardware reports the right data to the system.
- Verify that systems have enough memory and processing power.
- Once you’ve narrowed the field, check real-world references.
- Work to understand custom report and view demands and demo your ability to create or modify them.

FCAPS

- ITIL based management framework
- Divides management functions into domains:
 - Fault Management
 - Configuration Management
 - Accounting Management
 - Performance Management
 - Security Management
- While domains address different Functions, they are mutually related and supportive.
- Select tools that help you “plug holes” in processes and/or staff relating to a domain
- Requires that you evaluate processes to address functional domains effectively

FCAPS Domains

Fault Management	Configuration Management	Accounting Management	Performance Management	Security Management
alarm handling	system turn-up	track service usage	data collection	control NE access
trouble detection	network provisioning	bill for services	report generation	enable NE functions
trouble correction	Auto discovery		data analysis	access logs
test and acceptance	back up and restore			
network recovery	database handling			

What Do You Need to Know?

- FCAPS is a tool to develop processes, not guide tool selection
- Tools should supplement, enforce, streamline processes
- Tools may (and are likely to) cross functional domains
- As your network grows, you probably need to cover more domains
 - Fault Management
 - Performance Management
 - Configuration Management
 - Security Management
 - Accounting Management
- Cost for Tool(s) will increase as additional domains are addressed

Essential Tools for Applying FCAPS

- Fault management – detecting , isolating and resolving faults
 - Network monitoring software such as CiscoWorks (DFM), EpiCenter, HPOV
 - Root Cause Analysis software such as EMC SMARTS
 - Resources capable of understanding the software, determining the resolution, and/or managing the resources to resolution
 - Sound processes for detecting, isolating and resolving faults
 - Fully documenting the fault for future reference is one of the most important tools

What to Get From Fault Management

- Strong fault correlation
 - Limit number of alarms/alerts
 - Provide good assistance with fault isolation
 - Preferably provides some automation for problem resolution activities
- Ability to report/correlate “faults” that go beyond up/down status
 - “Flapping” connections
 - Route table changes/issues
 - Performance issues
- Ability to accept data from external sources
 - IP PBX
 - Servers or specific processes
 - Network probes

Essential Tools for Applying FCAPS

- Configuration Management – managing configurations of servers, gateways, routers and switches
 - Develop a process for configuration changes that is integrated with change management process
 - Make sure automatic logging of ALL configuration changes is enabled
 - Perform frequent verifications of configurations, firmware and software versions and update the tracking information
 - Subscribe to e-mail lists or other forms of updating services to stay on top of new versions of software and firmware changes as well as configuration improvements

What to Get From Configuration Management

- Enforcement of configuration management/change management policies
 - Limited device access
 - Approval chains/processes
 - Alerts of changes or automatic roll-back
- Support for Device Templates
 - Analysis of configurations against model
 - Automated application of templates to new devices
 - Bulk update of devices based on template changes
- Archive of configurations
 - Change review/rollback
 - Assist in problem analysis and resolution
- Impact analysis (if we change this what will happen?)

Essential Tools for Applying FCAPS

- Accounting Management – Documenting resources and utilization
 - Develop metrics to document the performance of the system (busy hour traffic, PRI utilization, number of calls dropped per hour, etc.) Populate database tables or spreadsheets with data that can be graphed in different ways based on need
 - Possible use for chargeback
 - Analyze collected data in relation to past trends and attempt to correlate questionable data with information from the fault, configuration and performance information

What to Get From Accounting Management

- Track usage/utilization
 - Chargeback to departments
 - Detailed records of calls/connections
 - Bandwidth consumed by port/IP address
- Call Detail Records
- Bill Analysis/Comparison

Essential Tools for Applying FCAPS

- Performance Management – Ensuring overall performance
 - Periodic tests to measure utilization, throughput, latency, delay, jitter, etc. should be performed and analyzed in relation to accounting information to assess and ensure proper performance
 - Use collected performance and accounting information to judge the health of the system as a whole (e.g. Concord)
 - Data is useful to develop trending patterns

What to Get From Performance Management

- Critical Metric Reporting
 - Latency
 - Jitter
 - Utilization
 - Availability
 - MOS/R-Factor
- Usage Trending
 - Leverage Historical Data
 - Historical data
 - “Hot Spot” identification
- Performance Forecasting

Essential Tools for Applying FCAPS

- Security Management – Processes to secure the environment
 - Use AAA to authenticate, authorize and account for user actions (RADIUS, TACACS+, etc.)
 - Utilize IDS sensors for monitoring activity, inspect alerts regularly
 - Use secure shell access (SSH) and secure management VLAN for remote console operations
 - Use VPN to remotely administer devices
 - Day 0 Attacks – Anomaly Detection
 - Physically secure equipment (make it hard for non-authorized personnel to access and tamper with systems)

What to Get from Security Management

- Authenticated Access and Management

How Does Management fit into Your Staffing Model?

- View tools as a requirement to assist your staff in their job, not as a “luxury”
 - Converged networks are more complex and can appear more opaque
 - Dependency on network for services increased
 - Support activities made more difficult without tools
- Tools can assist your staff in following updated policies and procedures
 - Particularly strong for Configuration (Change) Management
 - Supports/Allows use of Service Level Agreements
 - Availability (Service/System/Network)
 - Performance (Response Time, Call Completion %, MOS/R-Factor)
 - Can increase management visibility into network and/or staffing issues

FAQ

- How much should I budget for tools?
 - Small organizations - \$50,000 (Fault, Configuration, and some Performance Management)
 - Large Organizations - \$250,000+ (all domains with specialized coverage of key areas)
- Organizations typically don't budget adequately for tools in initial deployment.
 - Many assume existing tools will suffice, but make additional purchase within twelve months
 - General assumption that prior systems will suffice, usually inaccurate
 - Even if existing tools do provide necessary capabilities, budget for customization, reporting
- Before selecting any package ask "Will this help manage my network as a service to users?"

Example (Good and Bad)

- Engaged to provide configuration support to test equipment.
- Relatively low-end management system deployed
- Provided Fault, Configuration, and limited Performance Management
- Test team began modifying switch and router configurations to execute test plans.
- Within five minutes, configuration changes had “vanished”
- Loss of configuration changes detected when identical test results occurred
- Management System detected modification to configuration files through CLI, pushed old configuration back to device

Example (Good)

- International Carrier having difficulty reporting on Service Levels
- Existing Systems provided some performance insight, but limited proactive notification of pending issues
- Management systems generally did not provide long term trends of performance data
- Reports provided to support staff and customers generated from different systems – created communications issues
- Deployed new data collection/aggregation tool for performance management
- Reports customized to match SLA commitments
- Customers and internal reports on common system
- Alerts and notifications generated for internal support prior to SLA violation

Securing Your System

- The Bad: Converged networks introduce new vulnerabilities to your environment
 - Voice Network now traverses common network
 - In some configurations, separate logical networks cannot be maintained
 - Direct IP communications to partners, carriers, or via the Internet for voice introduces new variables
 - IP-based services also create new vulnerabilities for carriers (bill review/audit implications)
- The Good: Vendors are already releasing products to address vulnerabilities
 - “SIP Aware” Firewalls
 - IDS/IPS with IP Telephony knowledge
 - Generally improved security products
- The Ugly: We don’t know what we don’t know yet

How Bad Can It Be?

“We were well along in our deployment of IP-PBX’s, then along came the e-mail viruses – Sasser, Code Red, things that took our data network and crumpled it. Because our voice network rode on top of the network...we experienced some [voice] outages of anywhere from two to four hours before we could get access control lists in place [to block the attacks].”

- Vice President, major financial services firm
(from Network World Fusion)

**“It’s Just an
Application” – But
it’s Not**

- You’ll do well to follow “standard” information security best practices, but...
 - Will your firewall support QoS for processing/forwarding traffic?
 - Is your staff actively monitoring voice-specific security sites to understand emerging threats?
 - Do your supporting systems give you adequate visibility into “what’s going on?”
- When evaluating security systems and deployment
 - Evaluate processing delays that create additional latency
 - Bias selection towards solutions that react to QoS settings to minimize jitter
 - Ensure throughput supported matches demand and system placement
 - Verify that deployment does not overwhelm security system capabilities

Threats to be Aware Of

- DHCP Starvation – (Un)Intentional allocation of all available IP addresses for one or more segments
- Spam Telephony (SPIT) – Limited security issues (thus far), but consumes bandwidth and resources.
- Class of Service/Rate Limit Abuse – (Un)Intentional “upgrading” traffic to higher QoS setting, impacting bandwidth or causing DoS.
- Unauthorized Phones – Can anyone with a SIP handset make calls on your network?
- Viruses and Trojans
- Unauthorized Access to Call Processing Servers

First Major Exploit of IP Telephony Reported

- In June of 2006, two men arrested by the FBI and charges filed in New Jersey
- IP Telephony carrier hacked through brute force methods
 - Hacker stole valid dialing prefixes
 - Provided prefixes to accomplice
 - Accomplice used prefixes to deliver traffic to carrier network
- Exploit used to wholesale voice minutes to third parties
- Intermediate systems (routers, servers, workstations) hacked to disguise actual source of traffic from carrier
- While this exploit is more focused on carrier networks, lessons for the enterprise
 - Encrypt Call Signaling Traffic (With Quality Algorithm)
 - Make sure you can detect suspicious flows
 - Check your logs/configurations frequently
 - Be suspicious of all traffic to/from unknown/untrusted hosts

“Defense in Depth”

- The “traditional” single firewall at the Internet access point
 - Firewalls now secure multiple zones within a network
 - IDS/IPS systems seeing larger deployments
 - Internal threats recognized as significant exposures
- Organizations must deploy technology and training to provide appropriate security
 - Authenticated network access
 - Access restrictions by zone, segment, VLAN, system
 - More intelligent logging, reporting, analysis
- Look for “good” places to deploy security technologies
 - Typically, aggregation points where flows converge
 - Be aware of issues caused by asymmetric routes/paths

Mitigation Techniques

- Is your firewall SIP aware?
- Can you completely segregate voice and data traffic into VLANs?
 - Soft Phones can make this difficult/impossible
 - Integration of voice and data applications
 - Limiting voice access to authorized phones
- Is your existing security posture sufficient?
 - Default “deny all?”
 - Can you detect abnormal flows, port scans?
 - Have you examined your security policies and procedures with IP Telephony specifically in mind?
- How will SIP Trunking impact your security (could be carrier specific)?
- How will you handle VPN or Internet-based VoIP?

“Proactive” Mitigation

- Where required, deploy “Voice Aware” firewalls
 - Prevents open ports
 - Provides more granular examination of voice streams for identified attacks
 - Designed to meet specific requirements of voice
 - Do you need one firewall for converged traffic, or two (one voice, one data)?
- Ensure IDS/IPS provides the right alarms
 - Voice-specific signatures
 - Traffic floods from one or more unknown hosts
 - “Unusual” traffic patterns
- Examine/correlate log files
 - Good tools available on the market today
 - If you don’t look, you can’t be sure you’re secure – set a regular schedule and stick to it (even with tools)

More “Proactive” Mitigation

- Consider overall security posture
 - Do you need 802.1x/Network Admission Control?
 - Can your phones authenticate to the network for admission?
 - Is your Antivirus/Personal Firewall update process working effectively?
- Encrypt where appropriate and possible (particularly signaling)
- Review your phone bills and CDR's
 - IP Telephony does not eliminate the potential for fraud
 - Standard fraud prevention measures may alert you to holes in your perimeter
 - Adjust dialing rules to limit or eliminate unauthorized calling
- Think very, very carefully about acceptable sources of IP calls and implement rules/technologies to enforce
 - Connecting to partners over a VPN?
 - Connecting to carriers over IP network?
 - Connecting via the Internet?

Regularly Assess Vulnerability

- View security as a process, not a technology
 - Threats evolve, change, and grow
 - “The bad guys” are more focused on exploits that can make them money (by taking yours) than doing damage
 - Deploying devices and “walking away” will eventually result in exposures
- Get into the practice of regularly examining your network for exposures
 - Port mapping tools
 - Scripts and processes found on Internet
 - Focused testing when exploits are reported
 - Outside parties when appropriate
- Check for the “tried and true” methods (like social engineering)

Don't Forget Those Voice Skills

- Apply standard toll fraud procedures
 - Limit dialing plans according to roles and need
 - Require accounting codes for calls from public phones
 - Train users to avoid transfers to outside lines
 - Regularly review call details and audit bills
- Carefully consider phones for public areas
 - Can an “old” analog or digital set suffice?
 - Check-in/check-out of speaker phones for conference rooms.
- Limit access to public ports
 - Do not allow access to voice VLAN from publicly accessible network ports
 - Examine use of 802.1x, NAC, Guest Portals
- Merge with IT Security Best Practices

Things to Demand From Your PBX

- Ability to encrypt streams
 - Call signaling
 - Bearer traffic
 - Encryption from end-points should preserve quality of service settings
- Two-way authentication
 - IP PBX systems usually can authenticate end points in some fashion
 - Can the phone authenticate the IP PBX?
- Ability to detect and refuse common exploits
 - DoS attacks
 - Brute Force exploits
 - Some Man-in-the-Middle exploits
- Support for Certificates or similar PKI

If You're Going Outside "Your Network"

- Require encryption using strong protocols for signaling and bearer traffic
- Demand network connections that are worthy of trust
 - End point to end point encryption
 - Encrypted tunnels between known, trusted hosts
 - Remote access technologies that comply with best practices, security policies
- Enhance your ability to view traffic streams and detect improper communications at network boundaries
- Ensure that firewalls and other systems are "Voice Aware"
- Verify that encryption employed, network design allow for preservation (and use) of QoS

Where to Go

- SANS – SysAdmin, Audit, Network, Security Institute
 - www.sans.org
- “Security Considerations for VoIP Systems”
 - <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>
- ISSA – International Systems Security Association
 - www.issa.org
- CERT – Computer Emergency Response Team
 - www.cert.org
- Voice over IP Online Resource Guide
 - www.networkworld.com/resources/voip05
- VOIPSA – Voice over IP Security Alliance
 - www.voipsa.org

Lessons Learned

- Updating security posture for convergence is required
 - Usually a critical service with high visibility
 - Voice-specific exploits have been identified
 - Any new application demands examination of rules, systems, deployment
- Don't let IP Telephony cost you real money
 - Bad security could result in calls made by unauthorized parties “on your nickel”
 - Bad security could cause your organization to become an “unwitting accomplice”
 - Bad security could create new service impacts that make voice communications difficult/impossible
- Examine overall posture, policies, and procedures and be ready to adjust

Good Security Gone Bad

- Customer deployed IP Telephony, upgraded network hardware for multiple organizations
 - One District Office
 - Two Affiliated Campuses
 - Two distinct locations
 - Three different support staffs
- Network Architecture certified as viable by manufacturer, including firewall capabilities and placement
- When security was enabled, network crashed on regular basis
 - Traffic loads through firewalls exceeded processing capacity
 - Firewalls participating in routing protocols caused invalid routes, route flaps, overall failure of routing process
 - Firewall placement and configuration required inspection of excessive traffic relative to security policy
- Both voice and data network unstable, required network redesign and hardware replacement