VoIP Troubleshooting and Monitoring

Terry Slattery
Principal Consultant
CCIE #1026
Chesapeake Netcraftsmen
netcraftsmen.net

Troubleshooting

• Provide examples of common problems
• Identify sources of problems and their symptoms
• Remediation
• Techniques you can use in your network
• Monitoring requirements
• What to monitor
• Useful metrics
The Network is the Foundation for VoIP

- VoIP depends upon the network
  1. Network hardware and links
  2. Network protocols (routing & switching)
  3. Transport protocols (TCP/UDP)
  4. VoIP protocols and operation

- Other features
  - QoS
  - Redundancy

- Use VoIP operational model to aid troubleshooting and monitoring

How VoIP Works

- Connectivity and Registration
  - Power requested by continuous Fast Link Pulse (FLP)
  - DHCP request & response (UDP)
  - Get config from TFTP server (UDP)
  - Register with call controller (TCP)
How VoIP Works (cont)

- Call setup and operation
  1. Off-hook, Dialtone, Phone 1
  2. Collect digits and call setup, Phone 1
  3. Ringback tone, Phone 1
  4. Call setup, Phone 2
  5. Ring Phone, 2
  6. Off-hook, Phone 2
  7. Connect RTP stream

* Basic steps; a lot more happens than in this high-level description

Troubleshooting Diagnostic Aids
Connectivity – VLAN

- **Voice VLAN mis-configured**
  - Phone comes up in the wrong VLAN
  - Static configuration on phone (eBay purchase)
  - Switch misconfigured

- **No Voice VLAN**
  - Phone connected to data port
  - Switch misconfigured (include voice vlan)
    
    ```
    interface FastEthernet0/9
    switchport access vlan 100
    switchport mode access
    switchport voice vlan 411
    ```

Connectivity – DHCP

- **IP address assignment, default gateway, addl boot info** - Cisco: option 150, Avaya: option 176

- **Local vs Central DHCP server**
  - Short lease vs Long lease
  - Administrative overhead
  - Tracking address utilization
Connectivity – DHCP Location Tradeoffs

- **Central**
  - Multi-day address lease – longer than typical downtime
  - Reduces network equipment configuration
  - Good if many small branches exist
  - Handling long connectivity downtime due to disaster

- **Local**
  - Short address lease
  - Manage DHCP config at each site
  - More appropriate at larger remote sites.
  - Good if downtime is more extensive
  - Very remote offices with poor connection reliability

Connectivity - TFTP

- Download the phone config and OS
- Connectivity between phone and TFTP server
  - Co-located with central DHCP server is good
  - TFTP uses UDP – Firewall or ACL configuration
- TFTP timeout on long delay and lossy paths
Connectivity – TFTP

• TFTP server failure
  – Address in DHCP option 150 for Cisco; 176 for Avaya
  – Redundant server specification is good

• Bad TFTP file
  – Doesn't exist – often wrong phone MAC address
  – Bad format or contains typos

• Long system boot times, due to power outage
  – Example: 20 minutes to get all phones working
  – Network infrastructure boot time
  – DHCP/TFTP/Call servers booting, then overloaded
  – Download congestion!
  – Use load balancing

Registration

• Can’t connect to the Call Server
  – Routing problem between phone and call server
  – Incorrect firewall, or ACL configuration

• Test with ping and traceroute from call server

• Which phones are affected?

• New site?
  - No route to call controller
  - Firewall, ACL, or routing problem
  - No route to phones
Registration

• Can’t connect to the Call Server
  – Phone not configured in Call Server
  – MAC address wrong in Call Server
  – Default TFTP config file has wrong Call Controller address

Wrong call controller address

Phone MAC address wrong or not configured

Registration

• Can’t connect to the Call Server
  – Call server capacity (e.g., after power outages)
  – Call server is down
    • Use redundant call servers on different subnets

Redundant servers but the subnet is unreachable

Overloaded call server
Call Setup

• Incorrect destination call routing
  – Dial plan problems
  • Overlapping dial spaces

4-digit dialing:
736-8[0-4]XX
355-8[5-9]XX
Then add:
736-85XX

• Incorrect dial search spaces

7-digit dialing:
939XXXX (Internal)
939XXXX (Local)
9.939XXXX (Local)
9.393@ (Local or LD)

– Troubleshoot with DNA (Dialed Number Analyzer)

Call Setup

• Phones get calls for other locations
  – Numbers and hunt groups tied to phone, not line
  – Phone moved but call server not updated

• Spend time on a good dial plan!
  – 10-digit, multi-tenant plan
  – Map dial spaces onto this plan
  – Can still do 4-digit (or N-digit) dialing
  – Allows for growth, merger, acquisition
  – Much, much less expensive to maintain
  – Note: include planning to avoid toll fraud
Call Setup

- TCP is used between call server and endpoints
  - Routing problem between call controller & endpoints
  - Typically won't get dial tone or registration
  - Ping, traceroute, ACL checks, etc (sound familiar?)
  - Endpoints include PSTN gateways and DSPs*

---

Call Setup

- DSP required to match codecs or for conf calls
- Troubleshooting
  - CUCM log: “no resources”
  - Monitor DSP pool utilization
    - Cat 6500: show port voice active
    - Command syntax and limits depend on hardware
- Solution: buy more hardware

---

*Digital Signal Processor
Call Operation - No-Way Audio

- Audio RTP data sent in UDP datagrams
- Endpoints don't have connectivity
  - Routing problem
  - Firewall or ACL blocking a path
  - Cisco Skinny payload carries IP addr (NAT must know to change the embedded address)
- Use ping & traceroute to check reachability

Call Operation - One-Way Audio

- Check basic connectivity
  - Firewall or ACL blocking one path
  - Routing problem
- Two-way, then one-way
  - Change in routing or configuration
  - DSP crash (when transcoding or conference call)
  - Link congestion and no QoS or bad QoS
- Troubleshooting
  - What changed? (routing & configuration)
  - Who was affected?
  - Log analysis
Call Operation - Delay, Jitter, Packet Loss

• Causes:
  – Inconsistent or no QoS
  – Duplex mismatch or bad link
  – Routing problems (loss) or multipath (jitter)
  – Oversubscribed links (congestion & loss)

• Know when it's happening
  – Be able to detect the cause of each problem
  – Monitoring depends on vendor
    • RTCP stream (Avaya, Nortel)
    • Call stats on call server (Cisco)
    • ITU specs: 150ms delay, 30ms jitter, 1% loss

G.729 Good
60ms Jitter
10% packet loss

Call Operation - Delay

• ITU Spec: 150ms one-way delay

• Reduces interaction of a call
  – Wait for voice to travel to the other end of the call
  – Worst case is like a push-to-talk radio (Nextel?)
  – Roughly 10ms per 1000 miles (~30ms across the US)

• Causes:
  – Sub-optimum route path selection
    • New York to Atlanta via San Francisco
  – Long delay path, e.g., satellite circuit
    (250ms one-way)
Call Operation - Jitter

- Phones buffer packets to handle minor jitter
  - Packets with large jitter arrive too late and are dropped
  - Route flapping
  - Multipath load balancing

ITU Spec: 30ms jitter
- Big packets delay voice on low speed links
- Use Link Fragmentation and Interleaving (LFI)
  - Choose fragment size for delays of about 15 ms

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>64</th>
<th>128</th>
<th>256</th>
<th>512</th>
<th>1024</th>
<th>1500</th>
</tr>
</thead>
<tbody>
<tr>
<td>64Kbps</td>
<td>8 ms</td>
<td>16 ms</td>
<td>32 ms</td>
<td>64 ms</td>
<td>128 ms</td>
<td>187 ms</td>
</tr>
<tr>
<td>128Kbps</td>
<td>4 ms</td>
<td>8 ms</td>
<td>16 ms</td>
<td>32 ms</td>
<td>64 ms</td>
<td>93 ms</td>
</tr>
<tr>
<td>256Kbps</td>
<td>2 ms</td>
<td>4 ms</td>
<td>8 ms</td>
<td>16 ms</td>
<td>32 ms</td>
<td>46 ms</td>
</tr>
<tr>
<td>512Kbps</td>
<td>1 ms</td>
<td>2 ms</td>
<td>4 ms</td>
<td>8 ms</td>
<td>16 ms</td>
<td>23 ms</td>
</tr>
<tr>
<td>768Kbps</td>
<td>0.6 ms</td>
<td>1.2 ms</td>
<td>2.5 ms</td>
<td>5.1 ms</td>
<td>10.2 ms</td>
<td>15 ms</td>
</tr>
</tbody>
</table>

Before 

<table>
<thead>
<tr>
<th>60-Bytes</th>
<th>1500-Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>Data</td>
</tr>
</tbody>
</table>

After 

<table>
<thead>
<tr>
<th>128-Bytes</th>
<th>60-Bytes</th>
<th>128-Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Voice</td>
<td>Data</td>
</tr>
</tbody>
</table>
Call Operation - Jitter

- Inconsistent or no QoS implemented
  - Series of big packets delay voice
  - Only occurs when a link is oversubscribed
  - Priority queue moves voice to the front of the queue
  - Caution: Priority queue can starve lower priority queues; use policing to limit its effect
  - Configuration details vary among products

G.711
Before
- 218-Bytes Voice 40 pkts @ 1500-Bytes 6ms of Data 19ms 218-Bytes Voice
- 5ms jitter

After ...
- 218-Bytes Voice 33 pkts 5ms of Data 19ms 218-Bytes Voice
- 5ms jitter
- 33 pkts 5ms of Data
- 7 pkts 19ms 218-Bytes Voice
- 1ms of Data

Call Operation – Packet Loss

- ITU Spec: 1% packet loss (codecs handle 5%)
- Incorrect or no QoS configuration
  - Oversubscribed priority queue with policing
    - Designed for 4 concurrent calls, 20ms rate
      - G.729 on Frame Relay: 28.14 kbps *
      - G.711 on Ethernet: 91.56 kbps *
    - Facility expands and 8 concurrent calls occur
    - Policing on priority queue drops excess traffic
      - Monitor QoS queue drops
  - VoIP traffic not properly classified
    - Dropped when congestion occurs
      - * google: “cisco codec bandwidth” for calculators
Call Operation – Packet Loss

• Duplex mismatch (very common)
  – Fixed configuration on one end of link
  – The fixed configuration end doesn't negotiate
  – Look for errors: FCS, Runts, Late Collisions
  – Use Auto-negotiate for phones
    
    ```
    interface FastEthernet 0/1
    duplex auto
    ```

• Bad cabling
  – Bad crimp
  – Cat 3 cable
  – Pinched cable

• Use 'duplex auto'

Call Operation – Echo

• Symptom: Excessive talker echo (the most common)
• Acoustic echo - speaker output feed-back
  – Speaker phone or cheap earphone on remote end
  – Increase echo processing timer
• Electrical echo
  – Connection to analog via two-wire to four-wire hybrid
  – Reduce output gain & increase input attenuation in small steps (10% - 20%)
  – DSP bugs
• Delays inherent in IP telephony accentuate echo
Music on Hold

- Symptom: Music on Hold not on some phones
  - No MoH resource defined for the phones
  - MoH resources exhausted, typically when unicast playback is selected
  - Multicast routing not consistently configured when multicast MoH is used

Survivable Remote Site Telephony (SRST)

- Symptom: Phones can’t register with SRST Router
  - SRST not configured on phone & router
  - More phones or directory numbers than SRST router supports
  - Short DHCP lease (increase to 8 days)
Summary: Troubleshooting

- Configuration mistakes are the major cause of problems
- Collect data; subdivide the problem
- Test hypothesis and repeat
- Use the Network and Operational Models to subdivide the problem and aid troubleshooting

<table>
<thead>
<tr>
<th>Call Operation</th>
<th>Misc Operation and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Setup</td>
<td></td>
</tr>
<tr>
<td>Connectivity and Registration</td>
<td></td>
</tr>
</tbody>
</table>

Applications (VoIP)
Communication Protocols (TCP/UDP/IP)
Routing & Switching Protocols (OSPF, STP)
Network Hardware & Links (Routers & Switches)

Manual Monitoring Doesn't Scale

- Above 20-50 devices is too big
- Check system interdependencies
  - Root bridge depends on the switches in the STP domain
  - Duplex mismatch depends on connected device
  - Routing protocol consistency
  - VoIP call quality
  - QoS configurations
Monitoring Requirements

• Real-time
  – Events; Performance; Error detection

• Trending
  – Historical utilization and operational data

• Configuration management
  – Saving configs and checking against policies

• Latent problem detection
  – Combining data to find potential problems

Metrics

• Measurable
  – Link, CPU, memory utilization
  – QoS queue drops
  – Interface errors

• Actionable
  – Must be usable for identifying and fixing problems

• Update frequency
  – Nyquist sampling theorem: sample at 2X the freq of the data
  – Dependent on the use
    • Trending and historical
    • Real-time & diagnostic
Realtime – Events

• Syslog & SNMP traps
  – Sent asynchronously by network gear
  – High volume (particularly firewalls)
  – UDP-based (unreliable delivery)
  – Informational through critical severity

• Log everything
  – Keep for historical reference

• Filters for different recipients
  – Network operations team
  – Unified communications team
  – Security team

• Sync device clocks with NTP
  – Correlate timestamps from multiple devices

Realtime – Event Processing

• Handling the volume
  – Filter out unimportant events
  – Tune filters over time

• Daily summary report
  Summary of GNS Cisco syslog Messages on Wed Jan 17 23:59:00 EST 2007
  Cisco Messages:
    437 DUAL-5-NBRCHANGE
    353 LINEPROTO-5-UPDOWN
    114 CRYPTO-6-IKMP_MODE_FAILURE
  ...
  Messages sorted by frequency and source device:
    346 test1.com DUAL-5-NBRCHANGE
    114 test2.com CRYPTO-6-IKMP_MODE_FAILURE
    84 test3.com LINEPROTO-5-UPDOWN Tunnel119
    67 test4.com DUAL-5-NBRCHANGE
Realtime – Cisco Events

- Cisco: “System Error Messages for Cisco Unified Communications Manager”
  - CCM_CALLMANAGER-CALLMANAGER-3-CallManagerFailure
  - CCM_CALLMANAGER-CALLMANAGER-3-SDLLinkOOS: Cluster communications link failure
  - CCM_CALLMANAGER-CALLMANAGER-4-MediaResourceListExhausted: media resource type not found
  - CCM_CALLMANAGER-CALLMANAGER-3-TspError: phone registration problem
  - LINK-3-UPDOWN: backbone and important links
  - CDP-4-DUPLEX-MISMATCH: high utilization links
  - LINK-4-ERROR: excessive link errors
  - SYS-5-RESTART: device restarted
  - DUAL-3-SIA: EIGRP routing protocol problem
  - SYS-{1345}-SYS-LCPERR{1345}: Cat 6500 internal error

Realtime – VoIP Performance

- Delay, Jitter, Loss stat collection
  - Cisco: Call Detail Record (CDR) & Call Maintenance Record (CMR) collection
  - Avaya: RTCP stream directed to collector
- ITU specs:
  - Delay: 150ms one-way
  - Jitter: 30ms
  - Loss: 1%
- Determine your thresholds
  - Military often uses much higher values
  - 1% packet loss is terrible for data
  - NY to SF is 30ms one-way
Realtime – Triggers

• Call completion failure codes
  – search cisco.com “Call Termination Cause Codes”

• Environmental failures other than events
  – High power supply utilization
  – Fan failure (should be an event, but uses UDP)
  – Temperature
  – UPS battery reserve, AC supply status, etc
  – Change in STP root bridge
  – Redundant router (HSRP/VRRP) change

Trending

• Correlate with configurations to find latent problems

• Trends in call quality (CDR/CMR trending)

• UPS battery life and planning replacements

• CPU & Memory utilization trends, particularly in software-based routers

• QoS queue drops
Trending Example

- **Memory leak – router crash every twelve days**

  Drill-down to 10.17.8.102 stats, monthly view

  The following routers and switches experienced at least a 2% decrease in free memory during the day of 2003-12-23:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Device Name</th>
<th>Free Memory Start</th>
<th>Free Memory End</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.8.102</td>
<td>32-tech-3244</td>
<td>16MB</td>
<td>12MB</td>
</tr>
</tbody>
</table>

Trending – VoIP Resource Utilization

- **DSP pool utilization (CISCO-DSP-MGMT-MIB)**
  - `cdspCardResourceUtilization`
    - Indicates the percentage of current DSP resource utilization of the card
  - `cdspCardLastHiWaterUtilization`
    - Indicates the last high water mark of DSP resource utilization
  - Calculate total utilization across all cards

- **Trunk channel utilization & CUCM monitoring**
  - `CISCO-CCM-MIB-V1SMI: ccmGatewayTrunkTable`
  - Calculate utilization from total and in-use counts

- **Metric**
  - 70% for growing organization; 90% for no growth
Configuration Management

• Greatest impact on network stability and faults
  – Majority of network problems are due to configuration mistakes
  – More than 40%; amount depends on the analyst
  – Impossible to get to five-nines without it

• What to track
  – Who made the change
  – What changed
  – When was it changed
  – Use a AAA server (Radius or TACACS+)

• Critical in VoIP networks

Configuration Management

• Basic requirements
  – Configuration archive
  – Check Running vs Saved configurations
  – Log configuration changes
  – Tools to view changes

```
Running Config @ 2004-01-02 09:54:30
```

```
Saved Config @ 2003-12-01 04:03:23
```

```
---
1. version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname prc-srvn-2
aaa new-model
aaa authentication login default local
enable password 5$37311d6555c7a1e99

username greg password 7$1f8728648209f

to subnet-zero
---
```

```
1. version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
hostname prc-srvn-2
aaa new-model
aaa authentication login default local
enable password 7$1f008aef0c542e9a

username fred password 7$1146016d716c90
username daily password 7$202605743f839a
username john password 7$ec4a110704e38
to subnet-zero
```
Configuration Management

• Example: The Site That Lost Its VoIP
  – Major VoIP deployment
  – No automated tools in place
  – All routers and switched updated at the site
  – Two weeks later: power outage at the site
  – VoIP is down
  – Analysis: Configurations were not saved to NVRAM

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Device Name</th>
<th>Device Type</th>
<th>Saved Differences</th>
<th>Running vs. Saved Differences</th>
<th>Diff</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.23.24.1</td>
<td>NTP-42</td>
<td>Server</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>172.23.24.12</td>
<td>NTP-42</td>
<td>Server</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>172.23.23.15</td>
<td>Tel1</td>
<td>Router</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>172.23.24.13</td>
<td>Tel1</td>
<td>Router</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Policy

• Policy definition process
  1. Policy defined
  2. Template created
  3. Per-device modifications made to template
  4. Install final configuration in the device
• Policy is infrequently reviewed afterwards
  – Configs divert from policy as changes accumulate
  – Manual method are tedious and error-prone
Validating Configuration Policy

• Not just regulatory – check best practices
• Mechanism
  – Compare templates with device configs
  – Identify differences
  – Create an alert
• Value
  – Validate existing policies
  – Identify devices that don’t match a new policy

Fixing Configuration Policy Exceptions

• Remediation
  – Some policy exceptions can be automatically fixed
    • Duplex mismatch
    • Bridge priority
    • Router ARP timer > switch CAM timer
  – Service impacting changes need manual application

• Without automated policy validation, configs become inconsistent

• QoS policies
  – Trusting QoS in the right places?
  – Correct QoS marking policies in place?
Latent Problems – No Redundancy

• HSRP & VRRP
  – No redundant router
  – First failure was not noticed

Latent Problems – Wrong Root Bridge

• Root Bridge
  – Must determine switches in spanning tree domain
  – Check bridge priority on all switches in the domain
Summary

- The network is the foundation for VoIP
- VoIP is a complex system – many interdependencies
- Monitor key parameters with automated tools
- Use the Network and Operational Models to subdivide the problem and aid troubleshooting

<table>
<thead>
<tr>
<th>Call Operation</th>
<th>Misc Operation and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity and Registration</td>
<td>Call Setup</td>
</tr>
</tbody>
</table>

Applications (VoIP)
- Communication Protocols (TCP/UDP/IP)
- Routing & Switching Protocols (OSPF, STP)
- Network Hardware & Links (Routers & Switches)