Troubleshooting IP Videoconferencing

Session VVT-330
Goals Of This Session

• Give you an in-depth understanding of how H.323 operates so you will know where to look when diagnosing problems
• Look at several example problem scenarios and how to resolve them
• Give you the tools you need to troubleshoot Cisco IP/VC and MCM products

Recommended Prerequisites For This Session

• An understanding of H.323 components, protocols and message flows
• VVT-130, VVT-230 and VVT-213 sessions recommended
  Our troubleshooting examples are based on the topologies illustrated in VVT-230
  QoS is covered in detail in VVT-213
• The information contained in this session will apply generically to any H.323 product, and we will indicate when covering any vendor-specific features
Session Outline—Agenda

• Review components/functions of an H.323 network
• Review H.323 sub-protocols/message flows, addressing schemes and bandwidth requirements
• Identify typical/common error scenarios and how to systematically troubleshoot them
• Identify what troubleshooting tools are available for H.323
• Where to go for additional help and information

H.323 Components And Functions

• Gatekeepers
   Call processing agent for H.323 networks, just like CallManager is the call processing agent for IP telephony networks
   Direct vs. GKRCS

• Terminals

• Gateways
   PSTN/H.323; H.320/H.323; H.323/H.323; other protocols (e.g. SIP, MGCP, Skinny)

• MCU’s
   MC vs. MP functionality
H.323 Protocol Review

- H.225 (RAS, Q.931)
- H.245 (capabilities negotiation/channel control)
- RTP/RTCP (media channels)
- Audio codecs (G.711, G.728, G.722, etc.)
- Video codecs (H.261, H.263, etc.)
- Data (T.120)

H.323 Protocol Review

H.225

- RAS (Registration, Admission and Status)
  - Endpoint ////////// gatekeeper communications
- GUP (Gatekeeper Update Protocol)
  - Cisco proprietary protocol for Gatekeeper clustering
- Q.931
  - Setup, proceeding, alerting, connect
H.323 Protocol Review

H.225 RAS Definitions

- GRQ (Gatekeeper Request)
- RRQ (Registration Request)
- ARQ (Admission Request)
- LRQ (Location Request)
- RIP (Request In Progress)
- BRQ (Bandwidth Request)
- DRQ (Disengage Request)
- RAI/RAC (Resource Availability Indication/Confirm)
- IRQ/IRR (Information Request/Response)

Usage differs between H.323v1 and H.323v2

H.323 Protocol Review

H.245

- Capabilities negotiation
  Capabilities Set (advertisement)
  Capabilities Ack (acknowledgement)

- Open/close logical channels
  OLC (open logical channel)
  OLC Ack (acknowledgement)

- H.245 control channel stays open for duration of call
H.323 Protocol Review
RTP/RTCP

- Uses UDP for transport
- RTCP timestamps are used to maintain lip-sync

Endpoints need to support RTCP

<table>
<thead>
<tr>
<th>4 Bytes</th>
<th></th>
<th></th>
<th>4 Bytes</th>
<th>4 Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VER</td>
<td>CC</td>
<td>M</td>
<td>Payload Type</td>
</tr>
<tr>
<td></td>
<td>RTP Timestamp</td>
<td></td>
<td></td>
<td>Synchronization Source (SSRC) ID</td>
</tr>
</tbody>
</table>

H.323 Protocol Review
Audio/Video Codecs

- Audio codecs
  - G.711 (8kHz/64kbps)
  - G.728 (8kHz/16kbps)
  - G.722 (16kHz/64kbps)
- Video codecs
  - H.261, H.263 (H.263+, ++)
**H.323 Protocol Review**

**Direct Mode Interzone Call Example**

- 3-LRQ
- 4-LCF

---

**IP Network**

- Gatekeeper
- Gatekeeper

---

- 6-Q.931 Setup
- 7-Q.931 Proceeding
- 10-Q.931 Alerting
- 11-Q.931 Connect
- 12-Q.931 Connect Ack
- 13-H.245 Capabilities Set
- 14-H.245 Capabilities Ack
- 15-H.245 Capabilities Ack
- 16-H.245 Open Logical channels
- 17-H.245 Open Logical Channels Ack
- 18-H.245 Open Logical Channels Ack
- 19-RTP Media Channels Established

---

**H.323 Protocol Review**

**Addressing Schemes**

- E.164 addresses
- H.323-ID
  - Case sensitive
  - Requires DNS, sequential-LRQ or blast-LRQ
- Zone Prefixes
  - Multiple wildcard mask options (e.g. * or…)
- Service prefixes/technology prefixes
H.323 Protocol Review
Bandwidth Requirements

• H.225 RAS specifies that ARQ should indicate 2x the requested bandwidth
  (e.g. 768kbps for a 384kbps call to account for duplex media)
  This is only used for gatekeeper bandwidth management
  Some endpoints have bugs, and ask for the wrong amount, which breaks the gatekeepers’ ability to properly track bandwidth utilization

Bandwidth Requirements (Cont.)

• 13-15% overhead for RTP/UDP/IP headers in addition to audio/video bitrate
• Voice, video and data combined should never consume more than 75–80% of your link capacity
• cRTP not recommended for video
• LFI not recommended for video
H.323 Protocol Review
Bandwidth Requirements (Cont.)

Engineering The Network for Data, Voice, and Video

- LLQ = 33%
- Sum of Traffic = 75%
- Link Capacity

Link Capacity = (Min BW for Voice + Min BW for Video + Min BW for Data)/0.75

H.323 Protocol Review
Bandwidth Requirements (Cont.)

- Detailed example of 384kbps call over ATM:
  - RTP data (audio/video samples) combined = approximately 384kbps
  - Approximately 13% overhead for RTP/UDP/IP headers = approximately 434kbps
  - ATM carries 48 bytes of payload per cell, so 434kbps requires approximately 1,130 cells per second
  - Each ATM cell has an 8 byte header, so 1130cps * 8 bytes/cell = approximately 72kbps, or 17%
  - So 384kbps + 30% = approximately 500kbps of actual bandwidth required at layer-2
Session Outline/Agenda

- Review components/functions of an H.323 Network
- Review H.323 sub-protocols/message flows, addressing schemes and bandwidth requirements
- Identify typical/common error scenarios and how to systematically troubleshoot them
- Identify what troubleshooting tools are available for H.323
- Where to go for additional help and information

Common Error Scenarios

- Registration issues
- Call signaling/call setup issues
- H.320/H.323 gateway issues
- Misconfiguration of gateway/MCU services
- Codec negotiation issues (multi-vendor product interaction)
- Poor video quality (packet loss, QoS, latency)
Common Error Scenarios
Registration Issues

• E.164 address/H.323-ID conflicts
  Can conflict with other terminals, or with service/technology prefixes
  Example: Gateway service prefix = 9; terminal E.164 address = 9165551212
  Can conflict with a previous uncleared registration if IP address changes and original registration is still there.
  12.1(5)XM offers a new “endpoint-ttl” command to help alleviate this issue

Common Error Scenarios
Registration Issues (Cont.)

• Gatekeeper failover/re-registration issues
  HSRP—Cisco gatekeeper operates per the standard, but some endpoints don’t respond correctly
  Alternate Gatekeeper—Cisco gatekeeper supports it, but no H.323 videoconferencing endpoints support it yet

• Multicast gatekeeper discovery
  Endpoints could end up on the wrong gatekeeper
  Either route this multicast address to the correct gatekeeper or don’t use it
Common Error Scenarios
Registration Issues (Cont.)

• AAA Authentication (Cisco gatekeeper specific feature)
  Endpoints E.164-ID/H.323-ID must match the username/password in AAA server
  Cisco gateways and MCU’s use unique E.164/H.323-ID’s
  3540 MCU example:
    E164-ID: 776785023218
    H323-ID: RV-MCU-023218

Common Error Scenarios
Call Signaling Issues

• Intrazone H.323 call failures
  Wrong E.164-ID dialed or endpoint not registered (destination not found)
  E.164-ID conflicts with service/technology prefix
    Example: Gateway service prefix = 9; terminal E.164 address = 9165551212
  E.164-ID conflicts with remote zone prefix
    Example 1: directory gatekeeper zone prefix = *
    Example 2: E.164 address dialed = 9161234, remote zone prefix = 916*
  Intrazone or session bandwidth exceeded
Common Error Scenarios
Call Signaling Issues (Cont.)

- **Interzone H.323 call failures**
  - Wrong E.164-ID dialed, no zone prefix match
  - Remote gatekeeper sends LRJ (destination not found)
  - LRQ timers/TTL issues with sequential/blast-LRQ methods
  - Called number not found or routed to the wrong destination due to parsing order issues (see examples on previous slide)
  - Interzone or remote bandwidth exceeded

- **Proxy usage misconfigured**
  - Default setting on Cisco gatekeeper is to “use-proxy” inbound-to/outbound-from terminal

  ```
  PROXY USAGE CONFIGURATION:
  Inbound Calls from all other zones:
  to terminals in local zone sj-13-vsc-gk: use proxy
  to gateways in local zone sj-13-vsc-gk: do not use proxy
  Outbound Calls to all other zones:
  from terminals in local zone sj-13-vsc-gk: use proxy
  from gateways in local zone sj-13-vsc-gk: do not use proxy
  ```
Common Error Scenarios
Call Signaling Issues (Cont.)

- ILS/GAB call failures
  
  Gatekeeper may reject terminating ARQ
  
  Some do—ours used to but no longer does as of 12.1(5)T
  
  Bypasses gatekeeper by dialing IP address directly; gatekeeper will be incapable of tracking bandwidth usage, and CAC mechanism will break down

Common Error Scenarios
H.320/H.323 Gateway Issues

- ISDN provisioning is the #1 issue in TAC cases
  
  Must be provisioned for “voice and data”
  
  Bonding must be enabled
  
  Error message on gateway debug will be “incompatible destination”
  
  NPI/TOA settings on certain IXC’s circuits
  
  Translating from “unknown/unknown” to circuit-specific messaging format
  
  PRI line-buildout (i.e. LBO) on 3525 gateways
Common Error Scenarios
H.320/H.323 Gateway Issues (Cont.)

- Inbound H.320/H.323 call failures
  Bonding/line-hunting issues
  Gateway may not have enough B-channels available to complete the call
- DID vs. IVR/TCS4
  DID number must match the E.164 address
  Look at the gateway debug log to see how many digits the telco is passing

Common Error Scenarios
H.320/H.323 Gateway Issues (Cont.)

- DID inbound call failure example
  User dials "4085551212"
  Telco passes "5551212" to gateway
  Gateway queries gatekeeper for "5551212"
  Gatekeeper
  IP/VC 3525 Gateway
  Did Range = (408) 555-1000 through (408) 555-1999
  E.164 = 51212

Get the Telco to pass the correct number of digits, or change your internal dial plan
Common Error Scenarios
H.320/H.323 Gateway Issues (Cont.)

• Outbound H.323/H.320 call failures
  
  Dialing the wrong speed/prefix
  
  Example: service prefix 9 is provisioned for 384kbps; user dials 914085551212 at 128kbps
  
  RAI/RAC and line-hunting (Direct vs. GKRCs)
  
  Even with RAI/RAC, gateway could still be busy or lack sufficient resources; choose your RAI threshold carefully

• H.261 versus H.263
  
  H.263 requires additional resources on IP/VC gateways
  
  3525 can do three 384kbps calls using H.261, but only two when H.263 is used
  
  Future Cisco gateway offerings will eliminate this
Common Error Scenarios
H.320/H.323 Gateway Issues (Cont.)

- Audio transcoding issues
  - Version 2.2 resolves this via flow-control messages
  - Pre-2.2; make sure all gateways are set to the same transcoding priority
  - Future audio transcoding module in MCU will resolve this as well

Common Error Scenarios
Misconfiguration of Services

- How to properly configure service settings on the MCU’s and gateways is the second most common issue in TAC cases
  - MCU bandwidth = video bit rate only
    - Example: 320k for a 384kbps call
      (64k left for G.711 audio)
  - Continuous presence bandwidth can be calculated two ways
    - High bandwidth example: 320k in/1280k out
    - Low bandwidth example: 80k in/320k out
Common Error Scenarios
Codec Negotiation Issues

- Few examples of codecs failing to negotiate; this all works quite well in general; the problem is that you have to know what each endpoint is capable of.

  Example: MCU set to H.263, but VCON 4.01 and below only does H.261; VCON 4.4 and above supports H.263 now.

  In a mixed endpoint environment, you have to know what everyone’s capabilities are, and plan accordingly.

Common Error Scenarios
Poor Video Quality

- Four primary sources of poor video quality:
  - Ethernet port settings
  - Lack of QoS
  - End-to-end latency
  - Endpoint encoding capabilities
Poor Video Quality (Cont.)

- The most common cause of packet loss is Ethernet port negotiation issues
  3510 is 10/half, and you have to set the switch port to 10/half, not auto, or you will see errors on the switch port
  3540 is 100/full but you have to set the switch port to auto, not 100/full, or you will see errors on the switch port
  Polycom FX is 100/full
  Other Polycom models are 10/half
  PC-based (NIC cards) have their own unique issues
  Bottom line = you need to experiment (using “show port” or “show interface” commands) with each device/port settings to get it to 0% errors; then the video will look great.

- The second most common cause of packet loss is the lack of QoS
  You must protect video from data, and voice from video
  Video packets are large (up to 1500Bytes/packet or MTU)
  Do not use LFI with video.
  Multiple QoS methods available
  Proxy with LLQ
  ACL with LLQ
  RSVP (currently have H.323/RSVP sync problem; future version of proxy may resolve this)

Common Error Scenarios
Poor Video Quality (Cont.)

- "I" frame is a full sample of the video
- "P" and "B" frames use quantization via motion vectors and prediction algorithms

Video Conferencing Traffic Packet Size Breakdown

- 1025–1518 Bytes
- 513–1024 Bytes
- 65–128 Bytes
- 65–128 Bytes
- 129–256 Bytes
- 65–128 Bytes
Common Error Scenarios
Poor Video Quality (Cont.)

• The third most common cause of poor video quality is end-to-end latency

  ITU-TG.114 (one-way transmission time) recommends >=150ms as the maximum desired one-way latency to achieve high-quality voice (http://www.protocols.com/voip/testing.htm)

  Video codecs alone introduce 100-300ms

  MCU’s and gateways add 100-500ms

  IP/VC MCU’s add some latency (~100ms); but some other vendors add significantly more (200-300ms) due to de-coding/re-encoding processes

  Non-terrestrial links add up to 1000ms

  Serialization and queuing delays as utilization approaches 100%

  Bottom line = The videoconferencing industry has some work to do to improve these delay figures, but the network should not add significant latency

Common Error Scenarios
Poor Video Quality (Cont.)

- The fourth most common cause of poor video quality is the endpoints encoding capabilities
  
  NetMeeting can only do 15FPS; we always recommend a hardware-based codec for enterprise quality video
  
  Polycom ViaVideo’s and VCON ViGO’s are dependant on PC’s speed/power
  
  Even many high-end desktop endpoints can only do 15fps encode/30fps decode; be sure to check the endpoint specs to understand what each is capable of
  
  IP/VC MCU only does 15fps in continuous-presence mode (but so do others when you look at the receive frame rate)

Session Outline/Agenda

- Review components/functions of an H.323 network
- Review H.323 sub-protocols/message flows, addressing schemes and bandwidth requirements
- Identify typical/common error scenarios and how to systematically troubleshoot them
- Identify what troubleshooting tools are available for H.323
- Where to go for additional help and information
Troubleshooting Tools

- Gatekeeper debug options
- Gateway debug options
- MCU debug options
- Endpoint debug options
- Using a Packet Analyzer (i.e. “Sniffer”)

Gatekeeper Debug Options

- H.225 ASN1—RAS, Q.931
- H.245 ASN1—if proxy is used for call
- SNMP MIBS in Cisco MCM Gatekeeper
  Can be used to trap all RAS messages
- Cisco IOS® debug commands available
  ```
  debug RAS
  debug h225 asn1
  debug h245 asn1
  debug gatekeeper main 10
  debug proxy h323 statistics
  ```
Troubleshooting Tools

Gateway Debug Options

- Q.931 and capabilities negotiation process
  
  Cisco IP/VC gateways debug screen can be accessed via telnet
  
  No CLI commands on current products; debug messages will print to the screen by default

- SNMP
  
  Currently no specific MIB’s available, but you can at least monitor uptime

---

Troubleshooting Tools

MCU Debug Options

- Q.931, conference creation and capabilities negotiation process
  
  Cisco IP/VC MCU’s debug screen can be accessed via telnet
  
  No CLI commands on current products; debug messages will print to the screen by default

- SNMP
  
  Currently no specific MIB’s available, but you can at least monitor uptime
Troubleshooting Tools
Endpoint Debug Options

- Many endpoints now have HTML, SNMP and telnet interfaces
  
  Example: Polycom sends SNMP traps to GMS when problems are detected

- Many offer packet loss, latency and bit-rate statistics

Troubleshooting Tools
Using a Packet Analyzer

- A sniffer can show you things that the gatekeeper debugs won’t show you

  Direct-mode gatekeeper only shows you H.225 RAS information. Q.931, H.245 and RTP traffic is directly between the endpoints unless proxy is involved

  Make sure your sniffer can decode H.323
Session Outline/Agenda

• Review components/functions of an H.323 network
• Review H.323 sub-protocols/message flows, addressing schemes and bandwidth requirements
• Identify typical/common error scenarios and how to systematically troubleshoot them
• Identify what troubleshooting tools are available for H.323
• Where to go for additional help and information

Where to Get More Information

Online Documentation

• MCM configuration guide
• IP/VC users guides
• Design guides and white papers
  http://www.cisco.com/go/ese
• QoS design guide
  http://www.cisco.com/tac/iptelsolguide
• H.323 protocol information
  http://www.packetizer.com
  http://www.protocols.com
  http://www.itu.int
Networking Professionals Connection

Where to Get More Information
Networking Professionals Connection

- New E-Mail Subscriptions
- Discussion Forums
- Live, Online Presentations
- Message Board Discussions with Cisco Experts
- Biweekly Newsletter (6500+ Subscribers)
- Calendar of Events

http://www.cisco.com/go/netpro
Where to Get More Information
Networking Professionals Connection

Join a Conversation
VPN
Voice and Video
More to Come

Participate in Polls

Links to Relevant Information

Networking Professionals Connection

Join a Conversation
VPN
Voice and Video
More to Come

Participate in Polls

Links to Relevant Information

Where to Get More Information
Networking Professionals Connection

- Access to
  A “community” of professional peers
  Timely, relevant information

- Opportunity to
  Share expertise
  Learn from more experienced professionals
  Ask Cisco experts for answers
Where to Get More Information

Field Support

• Ask your Systems Engineer for assistance!
  Your SE has access to BU resources such as Product Managers, Technical Marketing and Developers
  They can escalate questions and problems when additional assistance is needed
  Many SE’s and CSE’s have specialized training on the video products (i.e. Convergence Virtual Team)

Troubleshooting IP Videoconferencing

Session VVT-330
Please Complete Your Evaluation Form

Session VVT-330