Balancing Security and Performance in Videoconferencing Deployments

Prasad Calyam, Ph.D. (Senior Systems Developer), Gregg Trueb (Student), Nathan Howes (Student)

Internet2 Spring Member Meeting
April 22nd, 2008
Topics of Discussion

• Introduction

• Issues with Videoconferencing and Firewalls
  – Focus is on H.323 set of standards

• Firewall Traversal Solutions

• Signaling and Multimedia Flow Paths

• Performance comparison of Firewall Traversal Solutions
  – Interoperability
  – Load Tolerance
  – Robustness against Vulnerabilities

• Best Practices for Secure Videoconferencing

• Conclusion
Introduction

• OSCnet supports H.323-based videoconferences for Ohio universities and Internet2 Commons

• Need for deploying videoconferencing end-points in a secure manner at several OSCnet customer-campuses

• Goals of the “Secure Videoconferencing” Project
  – Survey state-of-the-art:
    (i) Firewall Traversal Solutions
    (ii) Signaling-and-Multimedia Flow Architectures
  – Evaluate different Firewall Traversal Solutions:
    (i) Interoperability Testing
    (ii) Load Testing
    (iii) Vulnerability Testing
  – Outreach whitepaper with case studies and recommendations

• Project Sponsors: Ohio Board of Regents, Polycom
H.323 and Firewalls

• H.323 is a popular standard for Internet Videoconferencing
  – Supports real-time voice & video (i.e., multimedia) communications
  – Uses some fixed (e.g., 1719, 1720) and some dynamic ports (port range: >$2^{10}$ & $<2^{16}$) during sessions

• Firewalls protect networks against cyber-attack threats
  – Firewalls control incoming/outgoing traffic by blocking ports
  – Also provide NAT functionality

• But, H.323 + Firewalls = Poor performance!
H.323 + Firewalls = Poor performance!

- **Unusable** or **unexpected behaviour** for several reasons
  - Per-packet inspection by firewalls of address, port and message type slows down video and voice traffic
  - Other application packet-processing loads on firewalls aggravate slowness
  - Ever-changing security policies at last-mile sites
    - Patches against cyber-attacks, Upgrades, User requirements
  - Encrypted multimedia (H.235) blocked by firewalls
    - Blank screen at receiver
H.323 and Firewalls – Problem Case Study

- Problem report due to firewall mis-configuration
  - Intermittent frame freezing
  - Lot of pixilation
  - No significant audio problems
  - Sudden disconnections

- H.323 Beacon tool test report for troubleshooting
  - Sluggish call-setup
  - Delayed packet-events
  - Initial jitter variations in poor range

(a) Effect of a mis-configured firewall

(b) Jitter variations measured by H.323 Beacon

Firewall re-configuration solved the problem!
Firewall Traversal Solutions

- **Open** – no intermediate firewalls between end-points
  - Security of data is compromised to support multimedia requirements
    - Not practical given the security risks on the Internet
  - Could use separate multimedia VLANs that bypass firewall blocking
    - Not scalable, limited mobility, not practical if firewall at a downstream router or remote end-point behind a firewall
Firewall Traversal Solutions (2)

• **End-point behind Firewall**
  - **Static** (open ports in pre-configuration)
    - Pro: Can be implemented with any firewall
    - Con: Increased security risk, not scalable
  - **Dynamic** (open ports using stateful-packet-inspection)
    - Pro: Greatly reduced security risk
    - Con: Need specialized (expensive) firewalls - E.g., *Cisco PIX H.323 fixup*, need to keep up with software upgrades, and test extensively after upgrade

**Stateful-Packet-Inspection:**
- Firewall keeps track of out-bound packets, and associates in-bound packets with hosts of out-bound packets
- Thus allows safe handling of traffic without complex configuration of firewall rules
DMZ (De-Militarized Zone):
- Military term – “Nations separate armies through the use of a DMZ”
- Provides a buffer zone that separates an internal network from the often hostile territory of the Internet

Firewall Traversal Solutions (3)

• End-point in **DMZ** alongside Firewall

• **Gatekeeper-proxy in DMZ alongside Firewall**
  – *Polycom V^2IU, GNU Gatekeeper*

• **Standalone Gatekeeper-proxy with Integrated Firewall**
  – *Polycom V^2IU*

*End-points can be anywhere inside the firewall-protected network*
End-Point (EP) in DMZ alongside Firewall

**Pro:**
- Security of data not compromised to support multimedia requirements
- No need to buy and maintain a gatekeeper-proxy device

**Con:**
- Requires a special room for videoconferencing that is connected to DMZ
  - Users cannot videoconference from their desktops (PVX, X-Meeting, etc.)
- Need to register local EPs with an external gatekeeper
Gatekeeper-Proxy (GP) in DMZ alongside Firewall

- **Pro:**
  - Security of data not compromised to support multimedia requirements
  - Users need not be in DMZ – can videoconference from their desktop

- **Con:**
  - Need to buy a gatekeeper-proxy (GP) device and maintain it
  - If the GP is compromised, hacker has access to internal network!
Standalone GP with Integrated Firewall

- **Pro:**
  - Security of data not compromised to support multimedia requirements
  - No need for DMZ – users can videoconference from their desktop
  - GP is less vulnerable to attacks due to integrated firewall
    - Vendor makes a focused effort to harden the Gatekeeper-proxy appliance
  - Gatekeeper-proxy/firewall (GP-FW) can be in parallel with any other existing firewall
    - Sites can continue to use an already configured and deployed firewall if so desired

- **Con:**
  - Need to buy a GP-FW device and maintain it
ITU-T H.460 Standard

- H.460 allows firewall traversal for EPs behind firewalls (that block incoming ports) using a remote GP or GP-FW
  - H.460.18 (signal proxy for H.225/H.245), H.460.19 (media proxy for RTP)
    - Ratified by ITU-T in 2005
  - EP must be capable of H.460 signaling
  - Private-side EP initiates session with remote EP behind a GP or GP-FW
    - Upon session initiation, the proxy knows if an EP is behind firewall and hence rewrites all the signaling addresses to the (detected) public IP on the firewall
  - Keep-alive messages are sent by EP to keep the firewall open *(Default: 30s)*
  - Outgoing ports shown below must be open

### H.323 Protocol Transport Protocol Port Numbers

<table>
<thead>
<tr>
<th>H.323 Protocol</th>
<th>Transport Protocol</th>
<th>Port Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAS</td>
<td>UDP</td>
<td>1719</td>
</tr>
<tr>
<td>Q.931 (H.225)</td>
<td>TCP</td>
<td>1720</td>
</tr>
<tr>
<td>H.245</td>
<td>TCP</td>
<td>14085:15084</td>
</tr>
<tr>
<td>RTP</td>
<td>UDP</td>
<td>16386:34386</td>
</tr>
</tbody>
</table>
Polycom V²IU Solution

• Widely used and well-supported appliances built on a hardened Linux operating system
  – Gatekeeper-proxy (GP)
    • V²IU Traversal devices
      – E.g., V²IU 4350-T; Vendor Specs – Can handle upto 3 Mbps of multimedia and 25 - 30 Mbps of data traffic at an instant
    – Gatekeeper-proxy with Integrated Firewall (GP-FW)
      • V²IU Enterprise devices
        – E.g., V²IU 5300-E; Vendor Specs – Can handle upto 10 - 25 Mbps multimedia traffic and 75 - 90 Mbps of data, respectively at an instant
        – H.460 compliant

• Both provide:
  – Traffic shaping, router functionality, NAT server, DHCP server
  – Guaranteed QoE for Video traffic using prioritization and best effort QoS for data service
  – “Stateful-packet-inspection firewall” to dynamically open ports
    • Opens pinholes in firewall to allow voice and video traffic pass through
GNU Gatekeeper (GNU GK) Solution

• GNU Gatekeeper (GNU GK) - [http://www.gnugk.org](http://www.gnugk.org)
  – Open-source Gatekeeper
  – Proxy feature in GNU GK provides firewall traversal solution
  – Our hardware specs: 2.4 GHz, 1GB RAM, 80GB Hard disk, 100 Mbps NIC (i.e, a Modern 1U server)
  – Software specs: Secured and hardened Linux OS
    – Supports ITU-T E.164/IETF ENUM standards; ITU-T H.460 compliant

• Success stories in Internet2 and ViDeNet H.323 communities [kewin-sura06] [christian-sura06]
  – Supporting > 500 calls per month in University of Washington, USA and Max-Planck, Germany
Signaling-and-Multimedia Flow Paths

• Figure shows EP Registration and GP/GP-FW Neighboring in a distributed and heterogeneous proxy environment
### Signaling-and-Multimedia Flow Paths (2)

<table>
<thead>
<tr>
<th>EP-Pair</th>
<th>Signaling Flow Path</th>
<th>Media Flow Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP-1 ↔ EP-2</td>
<td>GP-FW-1</td>
<td>None</td>
</tr>
</tbody>
</table>

### End-Point Configuration

<table>
<thead>
<tr>
<th>End-Point</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP-1</td>
<td>EP behind Firewall</td>
</tr>
<tr>
<td>EP-2</td>
<td>EP in DMZ</td>
</tr>
<tr>
<td>EP-3</td>
<td>EP inside private network with GP in DMZ and 3rd party firewall</td>
</tr>
<tr>
<td>EP-4</td>
<td>EP inside private network with GP integrated firewall</td>
</tr>
<tr>
<td>EP-5</td>
<td>EP inside private network with GP integrated firewall</td>
</tr>
</tbody>
</table>

- **Worst case scenario can have multimedia between EPs passing through 2 GPs**
- **Actual large-scale deployment of GPs and GP-FWs at NOECA [polycom-twppt04]**
Goals for Experiments at OSC

• **Goal-1: Interoperability Testing** - Verify interoperability of firewall traversal solutions
  – V2IU – Open
  – V2IU – V2IU
  – V2IU – PIX with H.323 fixup
  – V2IU – GNU GK

• **Goal-2: Load Testing** - Compare performance of firewall traversal solutions with standard-definition and high-definition videoconferencing
  – Polycom V2IU 4350-T, Polycom V2IU 5300-S, GNU Gatekeeper Proxy (GNU GK), Cisco PIX with H.323 fixup
  – Experiments in controlled traffic load scenarios in a LAN
    • Traffic loads: Low, Medium, High
      – Iperf UDP streams, videoconferencing cross-traffic streams

• **Goal-3: Vulnerability Testing** - Assess V2IU and GNU GK for robustness against attacks
  – Nessus Port Scan to check severity of security loop holes
Goals for Experiments at OSC

• **Goal-1: Interoperability Testing** - Verify interoperability of firewall traversal solutions
  – V²IU – Open
  – V²IU – V²IU
  – V²IU – PIX with H.323 fixup
  – V²IU – GNU GK

• **Goal-2: Load Testing** - Compare performance of firewall traversal solutions with standard-definition and high-definition videoconferencing
  – Polycom V²IU 4350-T, Polycom V²IU 5300-S, GNU Gatekeeper Proxy (GNU GK), Cisco PIX with H.323 fixup
  – Experiments in controlled traffic load scenarios in a LAN
    • Traffic loads: Low, Medium, High
      – Iperf UDP streams, videoconferencing cross-traffic streams

• **Goal-3: Vulnerability Testing** - Assess V²IU and GNU GK for robustness against attacks
  – Nessus Port Scan to check severity of security loop holes
Testbed Setup for Interoperability Testing

• Connections with all combinations successful!

NOTE: For V²IU - PIX with H.323 fixup test case, V²IU only in GK mode
Goals for Experiments at OSC

• **Goal-1: Interoperability Testing** - Verify interoperability of firewall traversal solutions
  - V^2^IU – Open
  - V^2^IU – V^2^IU
  - V^2^IU – PIX with H.323 fixup
  - V^2^IU – GNU GK

• **Goal-2: Load Testing** - Compare performance of firewall traversal solutions with standard-definition and high-definition videoconferencing
  - Polycom V^2^IU 4350-T, Polycom V^2^IU 5300-S, GNU Gatekeeper Proxy (GNU GK), Cisco PIX with H.323 fixup
  - Experiments in controlled traffic load scenarios in a LAN
    - Traffic loads: Low, Medium, High
      - Iperf UDP streams, videoconferencing cross-traffic streams

• **Goal-3: Vulnerability Testing** - Assess V^2^IU and GNU GK for robustness against attacks
  - Nessus Port Scan to check severity of security loop holes
Testbed Setup for Load Testing

(a) Setup for GNU GK Testing

(b) Setup for Polycom V²IU Testing
Performance Evaluation Metrics for Load Testing

• To evaluate video and voice signal degradation of a session through the V^2IU and GNU GK solutions under different traffic loads
  – Subjective MOS (1 – 5)
    • Human subject testing
  – Objective MOS (1 – 5)
    • NTIA-VQM Tool
  – Mouth-to-Ear (M2E) Delay (ms)
    • Using Oscilloscope and Pulse generator
NTIA VQM Tool Overview

• NTIA VQM tool is based on the ITU-T J.144 recommendation for video quality estimation in VVoIP
  – Performs PSNR calculation and thus requires original and reconstructed video frames for frame-by-frame comparisons
  – Outputs PSNR-mapped-MOS measurements

\[
PSNR(n)_{dB} = 20\log_{10}\left(\frac{V_{peak}}{MSE}\right)
\]

\[V_{peak} = 2^k - 1; K = \text{number of bits per pixel (luminance component)}\]

\[MSE = \text{mean square error of the } N_{col}^{th} \text{ and } N_{row}^{th} \text{ of sent and received video signal frames}\]

PSNR values are mapped to MOS values as follows:

<table>
<thead>
<tr>
<th>PSNR (dB)</th>
<th>MOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;37</td>
<td>5 (Excellent)</td>
</tr>
<tr>
<td>31 - 37</td>
<td>4 (Good)</td>
</tr>
<tr>
<td>25 - 31</td>
<td>3 (Fair)</td>
</tr>
<tr>
<td>20 - 25</td>
<td>2 (Poor)</td>
</tr>
<tr>
<td>&lt;20</td>
<td>1 (Bad)</td>
</tr>
</tbody>
</table>
QoE for V²IU-4350 under different loads

- Network Load – Iperf cross-traffic
  - Low ~ 15Mbps; Medium ~ 40Mbps; High ~ 70Mbps

- Results measured for a video call
  - Both subjective and objective QoE measurements show notable degradation in device performance for network loads > 30 Mbps due to processing power limitations
  - Switch is not a bottleneck even at high network loads
M2E Delay for V^2IU 4350 under different Loads

- Network Load – Iperf cross-traffic from 0 – 70 Mbps
- Results measured for a video call
  - Peak M2E delay measurements show notable degradation for network loads for network loads > 30 Mbps (consistent with QoE results)
  - Peak delay >300ms is considered to hamper interactive communications (ITU G.114)
  - Control M2E Delay due to (Encode + Switch Propagation + Decode) processing
QoE for V²IU-5300 under different loads

- Network Load – Iperf cross-traffic
  - Low ~ 15Mbps; Medium ~ 40Mbps; High ~ 70Mbps
- Results measured for a video call
  - Both subjective and objective QoE measurements show negligible degradation in device performance even for network loads up to 70 Mbps – thus, shows high-end processing power of the unit
  - Switch is not a bottleneck even at high network loads
M2E Delay for V²IU 5300 under different Loads

- Network Load – Iperf cross-traffic from 0 – 90 Mbps
- Results measured for a video call
  - Peak M2E delay measurements show no degradation even for network loads up to 70 Mbps (consistent with QoE results)
  - Control M2E Delay due to (Encode + Switch Propagation + Decode) processing
QoE for GNU GK under different loads

- Network Load – Videoconferencing cross-traffic
  - Testing was done up to 15 Mbps load of just videoconferencing cross-traffic
    (NOTE: GNU GK does not pass through Iperf traffic because it is only a video proxy device)

- Results measured for a video call
  - Both subjective and objective QoE measurements show negligible degradation while using commodity hardware
M2E Delay for GNU GK under different Loads

- Network Load – Videoconferencing cross-traffic from 0 – 15 Mbps
- Results measured for a video call
  - Peak M2E delay measurements show *negligible but increasing* degradation (consistent with QoE results) in device performance
  - Control M2E Delay due to (Encode + Switch Propagation + Decode) processing
## Results Summary of Load Testing

<table>
<thead>
<tr>
<th>Traversal Solution</th>
<th>Suitability</th>
<th>DMZ Requirement</th>
<th>Proxy/Firewall Requirement</th>
<th>Level of Maintenance</th>
<th>Setup Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco PIX with “H.323 Fixup”</td>
<td>Enterprise and ISP (can sustain multimedia+data loads up to 70 Mbps and possibly beyond)</td>
<td>No</td>
<td>No Proxy required; Device is an H.323 protocol aware firewall</td>
<td>High (software upgrades, testing after major rule updates)</td>
<td>High (requires skilled engineering expertise)</td>
</tr>
<tr>
<td>Polycom V2IU 4350</td>
<td>Enterprise (cannot sustain multimedia+data loads beyond 30 Mbps)</td>
<td>Yes - if used only as proxy; No - if used as a firewall or in parallel with 3rd party firewall</td>
<td>Device acts as a Proxy and has integrated firewall; Third party firewall required that needs high maintenance and setup complexity</td>
<td>Low (software upgrades, extensive testing to verify upgrade done by vendor)</td>
<td>Low (requires video conferencing administrator expertise)</td>
</tr>
<tr>
<td>Polycom V2IU 5300</td>
<td>Enterprise and ISP (can sustain multimedia+data loads up to 70 Mbps and possibly beyond)</td>
<td>Yes - if used only as proxy; No - if used as a firewall or in parallel with 3rd party firewall</td>
<td>Device acts as a Proxy and has integrated firewall; Third party firewall required that needs high maintenance and setup complexity</td>
<td>Low (software upgrades, extensive testing to verify upgrade done by vendor)</td>
<td>Low (requires video conferencing administrator expertise)</td>
</tr>
<tr>
<td>GNU GK</td>
<td>Enterprise (can sustain multimedia loads up to 15 Mbps, and may fail at 20 Mbps; highly dependent on the device hardware)</td>
<td>Yes - only used as proxy</td>
<td>Device acts as a Proxy and has integrated firewall; Third party firewall required that needs high maintenance and setup complexity</td>
<td>High (software upgrades of GNU GK and Linux OS, extensive testing after upgrades)</td>
<td>Medium (requires skilled sys admin for OS hardening, and video conferencing administrator)</td>
</tr>
</tbody>
</table>
NOTES for Results Summary of Load Testing

• **Typical enterprise or small campus** (e.g. K-12 school) will have multimedia traffic loads that are less than 5 Mbps
  – One-to-three simultaneous high-quality SD or HD videoconferences may occur
  – *Recommended Solutions: Polycom V^2IU 4350, GNU GK*

• **Typical ISP or large campus** (e.g. OSU or UC) will have multimedia traffic loads that are less than 25 Mbps
  – Ten or so simultaneous high-quality SD or HD videoconferences may occur
  – *Recommended Solutions: Polycom V^2IU 5300, GNU GK, Cisco PIX with H.323 fixup*

• **Under special circumstances**, an ISP’s peak multimedia-only load if cascading multiple MCUs (e.g. Megaconferences, Key Stone Conferences) will be less than 40 Mbps
  – Ten or so MCUs may be cascaded to support 200+ participants simultaneously in a large-scale videoconference
  – *Recommended Solutions: Polycom V^2IU 6400*

* **NOTE:** Polycom V^2IU 6400 solution has not been evaluated by OSC; vendor specifications suggest it can handle 85 Mbps of multimedia traffic
Goals for Experiments at OSC

• **Goal-1: Interoperability Testing** - Verify interoperability of firewall traversal solutions
  - V2IU – Open
  - V2IU – V2IU
  - V2IU – PIX with H.323 fixup
  - V2IU – GNU GK

• **Goal-2: Load Testing** - Compare performance of firewall traversal solutions with standard-definition and high-definition videoconferencing
  - Polycom V2IU 4350-T, Polycom V2IU 5300-S, GNU Gatekeeper Proxy (GNU GK), Cisco PIX with H.323 fixup
  - Experiments in controlled traffic load scenarios in a LAN
    • Traffic loads: Low, Medium, High
      – Iperf UDP streams, videoconferencing cross-traffic streams

• **Goal-3: Vulnerability Testing** - Assess V2IU and GNU GK for robustness against attacks
  - Nessus Port Scan to check severity of security loop holes
Vulnerability Testing Results

NESSUS SCAN FOR V^2IU 4350

199.18.182.35 Scan Summary

Low Severity problem(s) Found

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>End time</td>
<td></td>
</tr>
</tbody>
</table>

Number of vulnerabilities:

- Open ports: 3
- Low: 15
- Medium: 0
- High: 0

NESSUS SCAN FOR V^2IU 5300

199.18.182.39 Scan Summary

Low Severity problem(s) Found

<table>
<thead>
<tr>
<th>Scan time</th>
<th>Fri Nov 2 14:41:40 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>Fri Nov 2 14:58:31 2007</td>
</tr>
<tr>
<td>End time</td>
<td></td>
</tr>
</tbody>
</table>

Number of vulnerabilities:

- Open ports: 3
- Low: 15
- Medium: 0
- High: 0

- V^2IU devices show low severity problems upon Nessus scanning
  - 3 open ports with factory default settings; device could be further locked down to only 1 open port (1720 – h323hostcall) with Ping (i.e., ICMP) answer turned-off
- GNU GK robustness depends on the Linux server hardening effort
Best Practices for Secure Videoconferencing

1. **Resource Planning is Critical**
   - Consider price-performance tradeoffs
   - Deploy solution based on proper estimation of data and multimedia traffic loads

2. **Provision Adequate Bandwidth**
   - Add 20% additional bandwidth to be provisioned for handling protocol overhead after bandwidth estimation based on traffic loads
   - Cascading MCUs, GPs or GP-FWs require additional bandwidth

3. **Avoid Solution Conflicts**
   - Configuring two competing solutions simultaneously (e.g. V2IU 5300 and Cisco PIX with H.323 fixup) may lead to conflicts and thus unexpected behavior

4. **Have Fail-over Options**
   - Have one or more spare firewall traversal solutions deployed or ready to deploy to avoid service outage

5. **Use a Dedicated GNU GK Device**
   - Turn off other services (e.g. web server) that compete for system & network resources
   - Keep the GNU GK secured and hardened

6. **Test and Document**
   - Test to ensure compatibility of EPs, MCUs and GP or GP-FW with the H.460 protocols especially in a multi-vendor videoconferencing deployments
Thanks!

• Ohio Supercomputer Center
  – Arif Khan, Steve Gordon, Aaron Lafferty, Paul Schopis, Pankaj Shah

• The Ohio State University
  – Dr. Bob Dixon, Gabe Moulton, Megan Troyer

• Edgewater Networks
  – Nick Imamura, Robert Smith

• Polycom
  – Tom Mills, Joseph Paolucci
References


Questions?
Appendix I: PIX Configuration

#allow all global traffic to access gatekeeper
access-list dmz_in permit ip any host <<Gatekeeper-proxy External IP>>

#allow traffic originating from gatekeeper access to inside
access-list proxy permit ip host 10.1.2.2 10.1.1.0 255.255.255.0

#apply acl dmz_in to outside
access-group dmz_in in interface outside

#apply acl proxy to inside
access-group proxy in interface inside

#establish global nat pool
global (outside) 1 <<External IP Range>>

#apply nat pool to inside
nat (inside) 1 10.1.1.0 255.255.255.0

#assign a static global nat to gatekeeper in dmz
static (dmz,outside) <<Gatekeeper-proxy External IP>> 10.1.2.2 netmask 255.255.255.255 0 0

#static nat inside interface to dmz allows access of gatekeeper from inside
static (inside, dmz) 10.1.1.0 10.1.1.0 netmask 255.255.255.0 0 0

NOTE: More details on H.323 Fixup and configs in [cisco-twpaper02] [roberts-twpaper01]
Appendix II: GNU GK Configuration

[Routed Mode]
GKRouted=1
H245Routed=0
CallSignalPort=1720
CallSignalHandlerNumber=2
RemoveH245AddressOnTunneling=1
DropCallsByReleaseComplete=1
SupportNATedEndpoints=1
Q931PortRange=30000-39999
H245PortRange=40000-49999

[Proxy]
Enable=1
InternalNetwork=10.0.0.0/8
T120PortRange=50000-59999
RTPPortRange=50000-59999

NOTE: More details on GNU GK installation and configs in [kewin-questnet05] [GNUGK-manual]