VoIP for Network Operators

Andy Davidson
NANOG 44, October 2008
Motivation / Aim

• Help IP network professionals make good VoIP networks
Agenda

• VoIP basics

• What operators need to know when building VoIP networks

• Voice Peering

• Measuring VoIP/Industry Metrics

• VoIP network security
VoIP Basics :: Overview

- I assume you know it’s about talking to your buddies over an IP Network!
- Bifurcation of call into Signaling and Media
  - Signaling = messages, “I have a call for you”
  - Media = the sound stream
Media / Signal split

Signal Path

Carrier SIP Proxy

Office Asterisk Box

Callee

Your User

Default route
Dodgy partial transit
Spies leaking routes
Government
BGP Route hijack
Inject back

Media Path

Security

Debugging
VoIP Basics :: Signaling

- Enables handling of events
  (Begin a call. Initiate a conference feature. You have a message!)

- Best known protocols
  SIP (IETF) H.323 (ITU)

- Cisco SCCP/SKINNY
  Nortel UNISTIM
  Digium IAX
VoIP Basics :: SIP

- Allows 2 phones to find each other
- “Bursty” traffic profile. Sip call = 7 messages
VoIP Basics :: SIP 2

- Looks a bit like HTTP
- Text based, with mail like routing Easy to parse
VoIP Basics :: SIP 3

- SIP IS LOOSELY IMPLEMENTED
- Interconnect takes time
- Extensive testing of user agents required
VoIP Basics :: SIP 4

• SIP means different things to different people

• End to end VoIP

• User - Carrier - User VoIP
VoIP Basics :: RTP

- Real-Time Transport Protocol
- Connectionless session
- Transports encoded sound within UDP
- Identify multiple streams on the same host
VoIP Basics :: Sound

- Sampling - turn sound into digital form
- Chart opposite shows
  - Low sample rate
  - Medium sample rate
  - High sample rate
VoIP Basics :: Sound 2

- Framing - turns sample into equal sized block of data for transport
- Encoding - Codecs
  Some codecs compress
### VoIP Basics :: Codecs

<table>
<thead>
<tr>
<th>Codec</th>
<th>Description</th>
<th>Network Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711</td>
<td>PSTN-like. uLaw aLaw</td>
<td>Average</td>
</tr>
<tr>
<td>G.729a</td>
<td>Max compression</td>
<td>Small</td>
</tr>
<tr>
<td>G.722</td>
<td>Wideband, high quality</td>
<td>High</td>
</tr>
<tr>
<td>GSM</td>
<td>From Mobile industry</td>
<td>Small</td>
</tr>
<tr>
<td>Speex</td>
<td>Adaptive</td>
<td>Variable</td>
</tr>
</tbody>
</table>

*G729 is a commercial codec*
Why is this of interest to operators ..... ?
Clients connect in

- Most client connections (e.g. http, imap...) begin from inside your network -- easy to make firewall rules for this traffic
- However, inbound calls are transactionless connections from off-net / outside firewall
- Alien security concept
Traffic looks different

<table>
<thead>
<tr>
<th>Usual IP network traffic profile</th>
<th>VoIP traffic profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mostly TCP</td>
<td>Mostly UDP</td>
</tr>
<tr>
<td>Transaction based</td>
<td>Connectionless</td>
</tr>
<tr>
<td>Tolerates latency and delay</td>
<td>Latency sensitive</td>
</tr>
<tr>
<td>Packets of all sizes, many large</td>
<td>Lots of small packets, sent often</td>
</tr>
<tr>
<td>User expectations high</td>
<td>User expectations <strong>very</strong> high</td>
</tr>
</tbody>
</table>
Tiny Packets

- Huge packet per second volumes

- PPS count more likely to saturate routers than “high bandwidth”
• Latency is **delay**

• ITU Recommendation G.114 suggests delays > 150ms make conversation “significantly affected”
• Jitter is **delay variation**.

• Receiving side expects to receive packets at a constant rate

• VoIP calls break if jitter is larger than buffer size
Simulation

- Record telephone call, check jitter of RTP with `ethereal`, play audio and judge quality

- Use FreeBSD `dummynet` to “make conditions worse”

- Record another call, compare performance with first call
Without Jitter

Click the blue square to play Audio
Add some jitter

bash-3.2# ipfw -q flush
bash-3.2# ipfw pipe 1 config delay 50ms
bash-3.2# ipfw pipe 2 config delay 300ms
bash-3.2# ipfw pipe 3 config delay 1ms
bash-3.2# ipfw add prob 0.2 pipe 1 ip from any to any
bash-3.2# ipfw add prob 0.04 pipe 2 ip from any to any
bash-3.2# ipfw add pipe 3 ip from any to any
With Jitter

Click the blue square to play Audio
Results

The lost packets are out of order packets which were dropped

The connection was otherwise so usable, I forgot to ipfw -q flush for an hour
Networks:: Packet Loss

- Packet Loss manifests as missing audio
- No time to retransmit lost audio, so audio signal degrades with the loss of any rtp packet
- Random loss - congestion
- Burst is >1 consecutive lost packet
- Jitter has unexpected effect on packet loss
Packet Loss

- Constant transport and propagation delay for all codecs
- Variable Packetisation delay
- Jitter buffer

<table>
<thead>
<tr>
<th>Codec</th>
<th>Bandwidth Required</th>
<th>ms of Audio in Datagram</th>
<th>Packetisation Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>g.711</td>
<td>87.2 kbps</td>
<td>20ms</td>
<td>1ms</td>
</tr>
<tr>
<td>g.729a</td>
<td>31.2 kbps</td>
<td>20ms</td>
<td>25ms</td>
</tr>
<tr>
<td>g.723.1</td>
<td>20kbps</td>
<td>30ms</td>
<td>67.5ms</td>
</tr>
</tbody>
</table>
Net :: Save Bandwidth

• RTP Header compression (but adds delay)
• Silence Suppression (but can confuse people - comfort noise)
• RTP Multiplexing (but adds delay)
• Weighted Fair Queueing
• Priority Queueing
• Class-Based Weighted Fair Queueing
PQ Example

**RTP/RTCP:**
- Dynamic RTP port start: 30000
- Dynamic RTP port stop: 40000
- DTMF Payload Type: 101
- RTCP Support: on
- RTP Keepalive: on

```bash
bcliffe-gw(config)#access-list 103 permit udp any any range 30000 40000
bcliffe-gw(config)#access-list 103 permit udp any any eq 5060
bcliffe-gw(config)#priority-list 1 protocol ip high list 103

bcliffe-gw(config)#int dia 1
bcliffe-gw(config-if)#pri
bcliffe-gw(config-if)#priority-group 1
```
Queueing flaw

- Software vs Hardware wait queue
  Can push packets to front of software q but not hardware queue

- Delay caused by serialization of packets (speed of interface matters)
Congestion Avoidance

- WFQ, PQ, etc. deal with existing congestion
- Prevent Congestion, by dropping packets from nominated flows
- WRED
NAT

- Minefield
- Destroys ability for end-to-end media path
- Requires media proxy
- Issues manifest as one way audio
Voice Peering
Not like IP peering

- Doesn’t normally mean Settlement Free Interconnection
- Telcos are used to billing wholesale interconnect rates
- Peering is about saving operators money, not saving customers money
... but then very similar

• Federations between smaller operators (MLP)

• Big operators with tightly controlled, private, contractually guaranteed interconnect
Interop of new services

- So why peer .... ?
- Default PSTN routing is not good enough
  - Presence
  - Wideband audio
Voice peer over IP PNI

- Carriers not willing to use "the internet" to peer, but they do want to use IP networks
- Voice operators private/public peering
DNS and VoIP
• Phone Number in DNS

• Allows user agents to call user agents without carriers

(+44) 020 7993 1700 becomes 0.0.7.1.3.9.9.7.0.2.4.4.e164.arpa
• `_sip._udp IN SRV 1 0 5060 voip-in.example.com.`
• Sends `user@example.com` calls to voip-in
Monitoring VoIP Quality
Measuring VoIP - MOS

• MOS (Mean Opinion Score)

• You ask several people what they thought of the call, and take an average

<table>
<thead>
<tr>
<th>MOS</th>
<th>Quality</th>
<th>Impairment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Excellent</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>Good</td>
<td>Perceptible, not annoying</td>
</tr>
<tr>
<td>3</td>
<td>Fair</td>
<td>Slightly annoying</td>
</tr>
<tr>
<td>2</td>
<td>Poor</td>
<td>Annoying</td>
</tr>
<tr>
<td>1</td>
<td>Bad</td>
<td>Very annoying</td>
</tr>
</tbody>
</table>
Monitoring VoIP - ACD

• ACD
  • Average call duration
  • Users keep conversations brief when the sound quality is poor
  • Business case to build a good network?
  • Imperfect (varies with day of week/time)
Monitoring VoIP - CSR

- Call Success Rate
  - Used as measure of success by people who buy and sell wholesale voice minutes
  - Not completely accurate as engaged/no-reply drops score
  - Imperfect (when someone’s backup route - you only get calls which already failed)
VoIP Security
Open Relay

- "VoIP’s toll fraud"
- Nowadays it is common to see attempts to relay unintended calls through switch
- Protect at network layer by limiting who can send calls (if possible)
- Protect at application layer with dialplan
Media security

• Trivial to reconstruct conversations from RTP streams

• Different signal and media path
  - if signal path trustworthy
  - media path may still be untrustworthy

• May be commercially sensible or contractually required to mask media source
Reinvites

• Cause media to change path in call
  • Initiating conference
  • Transfer call
  • Configuration
• Debugging floating calls hard
• Path can change from secure to insecure path
• Call can suddenly stop (media profile changes)
Tampering with SIP

• Injection of packet to cause unexpected call termination, e.g. BYE to disrupt conversation

• Injection of BYE to cause billing to stop, but media to continue.....
SBC

- Session Border Controller
- B2BUA - pretends to be your end users to the outside world, and pretends to be the outside world for your end users
DNS Based attacks

- ENUM
- SRV

- Spoofing DNS results can lead to calls being sent to unintended parties
- Those visiting from under a rock should google Dan Kaminsky
Aims of Encryption

• A good encryption standard will :-
  • Prevent eavesdropping
  • Prevent tamper/alteration
  • Identify and authenticate speakers
• Typically runs on udp/5061 (SIPS)

• CA based, so signal channel is both encrypted, and known-safe

• But needs CA config to all peers - cumbersome

• Conversation is not encrypted unless Secure-RTP is deployed alongside

• New risk of TLS Connection Reset attacks
SRTP

- Protects confidentiality of RTP Payload (the conversation)
- Protects integrity of entire media packet
- Secure Key negotiation tends to be proprietary, however SDP Security Description in SIP TLS likely to replace
Packet Replay Attack

- Affects media
- Capture and resend out of sequence RTP
- Degrades call quality and adds delay to call in progress
Bouncing

- Phreaks legitimately create accounts on VoIP services in one country, in order to mask originator in attack against another service.
SPIT

• SPam over Internet Telephony

• Likely to increase as cost to make telephone call drops to zero
Learning points

• Signal / Media paths different
• Recognise effects of jitter, packet loss
• VoIP is very different sort of traffic to usual
• Specialist Voice security needs
• Peer with voice operators, as this will ultimately enable progress
Didn’t fit elsewhere...
INOC-DBA Scheme

• Emergency channel for network operators

• Can dial ASN*extension to reach netop

• www.pch.net/inoc-dba
Open Source Projects

- OpenSIPS (nee OpenSER)
- Freeswitch
- Asterisk
Questions?

Andy Davidson, NetSumo
Email/SIP: andy.davidson@netsumo.com