VoIP for Network Operators

Andy Davidson

NANOG 44, October 2008

Motivation / Aim

- Help IP network professionals make good VoIP networks

Agenda

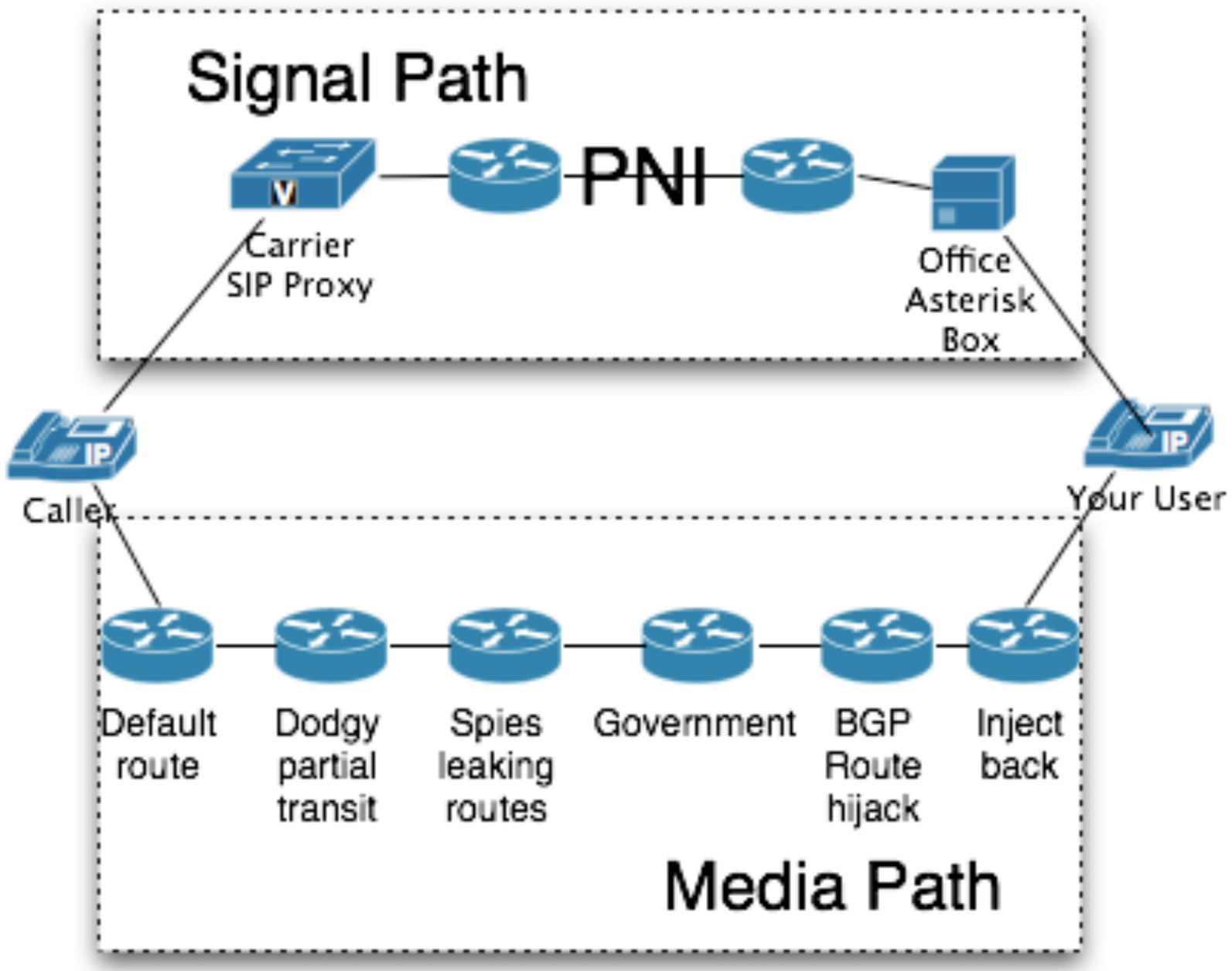
- VoIP basics
- What operators need to know when building VoIP networks
- Voice Peering
- Measuring VoIP/Industry Metrics
- VoIP network security

VoIP Basics :: Overview

- I assume you know its 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



Security

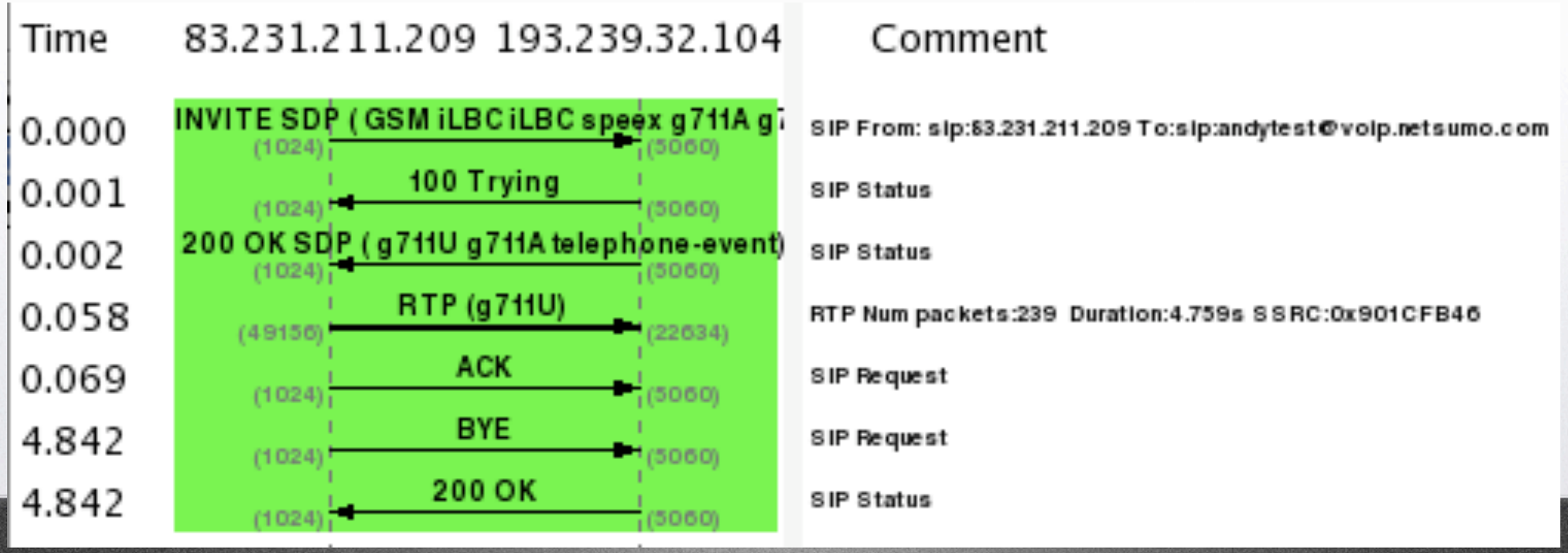
Debugging

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

```
20:29:21.055780 IP (tos 0x0, ttl 58, id 25917, offset 0, flags [none], proto UDP (17), le
dsl.prodigynet.co.uk.1024 > voip0.sov.netsumo.com.sip:[udp sum ok] SIP, length: 837
        INVITE sip:andytest@voip.netsumo.com SIP/2.0
        Via: SIP/2.0/UDP 83.231.211.209:1025;rport;branch=z9hG4bK0a010102000001d48e7c7427a87afb50000000c
        Content-Length: 370
        Contact: <sip:83.231.211.209:5060>
        Call-ID: A5C12C2C-1DD1-11B2-874D-E70FE3516DA5@10.1.1.2
        Content-Type: application/sdp
        CSeq: 1 INVITE
        From: "unknown"<sip:83.231.211.209>;tag=3378666728184631682 8
        Max-Forwards: 70
        To: <sip:andytest@voip.netsumo.com>
        User-Agent: SJphone/1.60.299a/L (SJ Labs)

        v=0
        o=- 3432138178 3432138178 IN IP4 83.231.211.209
        s=SJphone
        c=IN IP4 83.231.211.209
        t=0 0
        a=direction:active
        m=audio 49156 RTP/AVP 3 97 98 110 8 0 101
        a=rtpmap:3 GSM/8000
```

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

	Description	Network Bandwidth
G.711	PSTN-like. uLaw aLaw	Average
G.729a	Max compression	Small
G.722	Wideband, high quality	High
GSM	From Mobile industry	Small
Speex	Adaptive	Variable

* 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

Usual IP network traffic profile	VoIP traffic profile
Mostly TCP	Mostly UDP
Transaction based	Connectionless
Tolerates latency and delay	Latency sensitive
Packets of all sizes, many large	Lots of small packets, sent often
User expectations high	User expectations **very** high

Tiny Packets

- **Huge packet per second volumes**

- PPS count more likely to saturate routers than “high bandwidth”

Networks :: Latency

- Latency is **delay**
- ITU Recommendation G.114 suggests delays > 150ms make conversation "significantly affected"

Networks :: Jitter

- 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

```
exten => 500,1,Answer()
exten => 500,n,Set(CALLFILENAME=andy-voiptesting-${TIMESTAMP}-${CALLERID(num)})
exten => 500,n,Monitor(wav,${CALLFILENAME},m)
```

Without Jitter

Click the blue square to play Audio

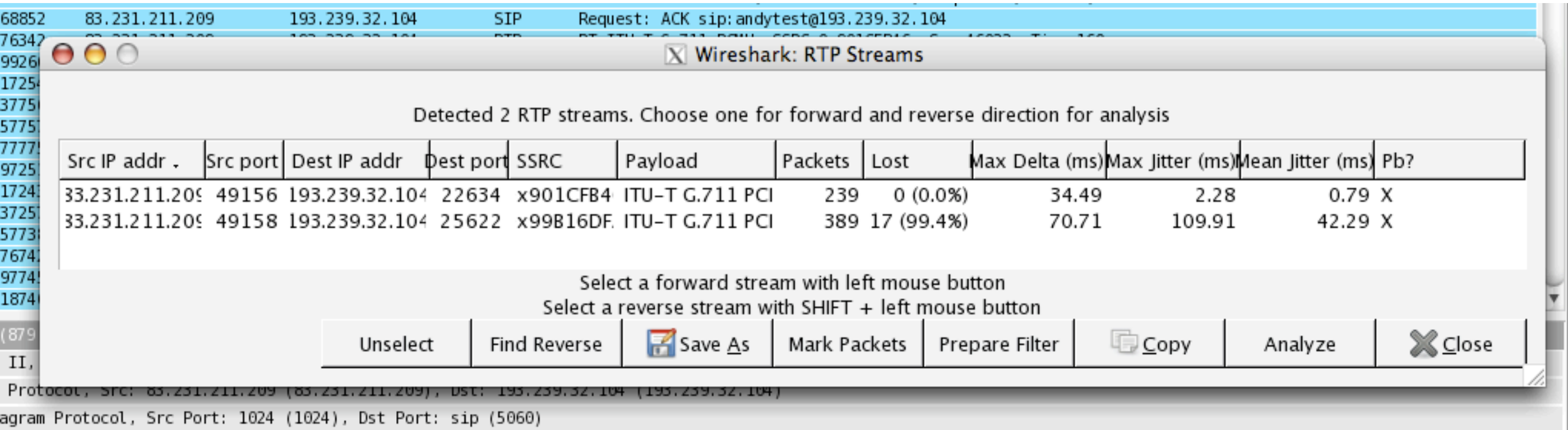
Add some jitter

```
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
00100 prob 0.200000 pipe 1 ip from any to any
bash-3.2# ipfw add prob 0.04 pipe 2 ip from any to any
00200 prob 0.040000 pipe 2 ip from any to any
bash-3.2# ipfw add pipe 3 ip from any to any
00300 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

Codec	Bandwidth Required	ms of Audio in Datagram	Packetisation Delay
g.711	87.2 kbps	20ms	1ms
g.729a	31.2 kbps	20ms	25ms
g.723.1	20kbps	30ms	67.5ms

Net :: Save Bandwidth

- RTP Header compression (but adds delay)
- Silence Suppression (but can confuse people - comfort noise)
- RTP Multiplexing (but adds delay)

Net :: Queueing

- 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 off
RTP Keepalive:	on off

```
bcliffe-gw(config)#access-l 103 permit udp any any range 30000 40000
bcliffe-gw(config)#access-l 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

ENUM

- 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

```
factory:~ andy$ dig +short 5.5.5.5.5.5.5.5.0.0.8.1.e164.org any
200 10 "u" "E2U+SIP" "!^\\+1800(.*)$!sip:1800\\1@tf.voipmich.com!" .
200 10 "u" "E2U+SIP" "!^\\+1800(.*)$!sip:1641641800\\1@sip.tollfreegateway.com!" .
200 10 "u" "E2U+SIP" "!^\\+1800(.*)$!sip:1800\\1@tollfree.sip-happens.com!" .
```

SRV

- _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

MOS	Quality	Impairment
5	Excellent	None
4	Good	Perceptible, not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

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

TLS / SSL

- 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

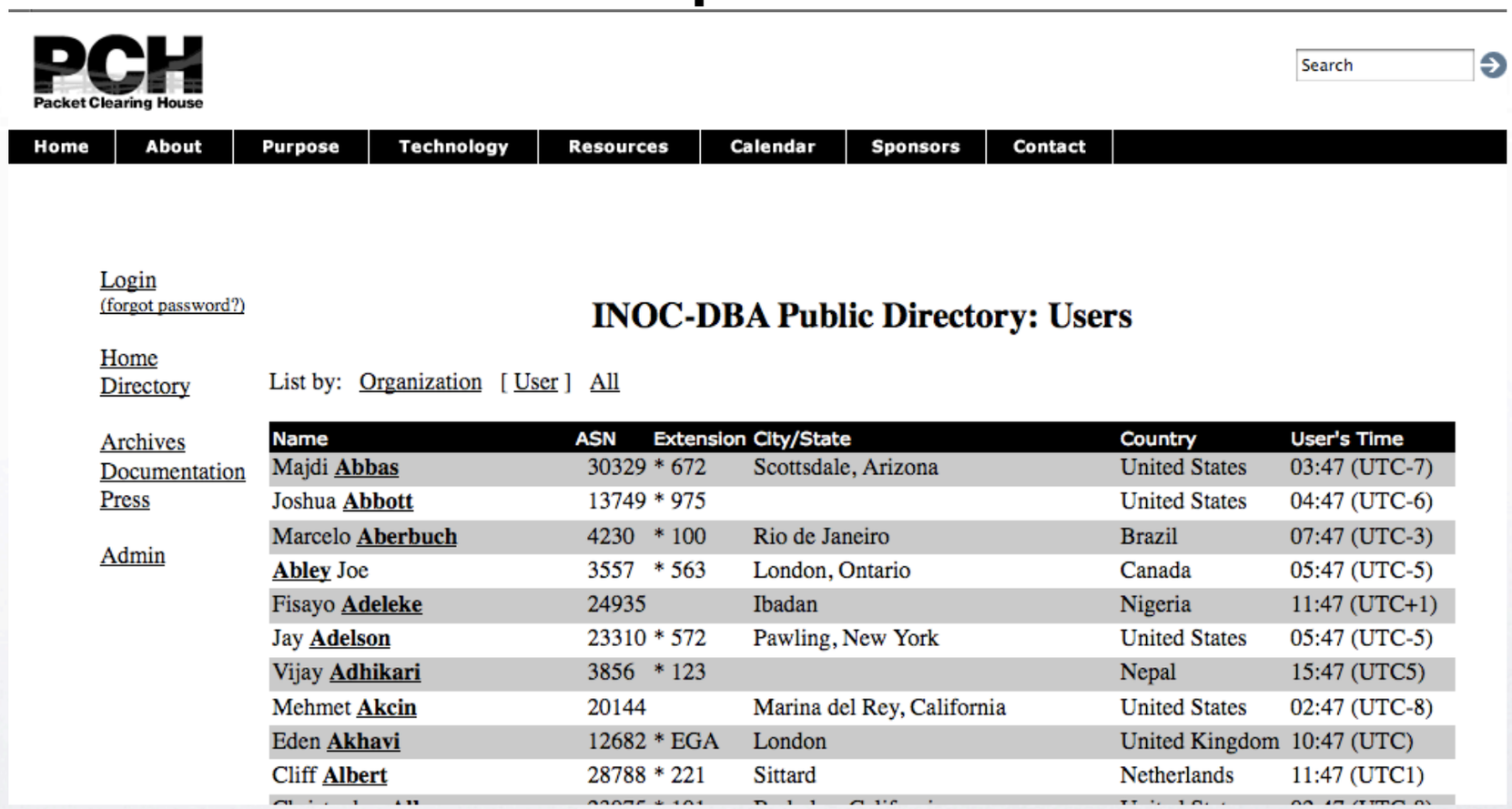
Learning points

- 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



PCH Packet Clearing House

Search

Home | About | Purpose | Technology | Resources | Calendar | Sponsors | Contact

Login
(forgot password?)

Home
Directory

Archives
Documentation
Press

Admin

INOC-DBA Public Directory: Users

List by: Organization [User] All

Name	ASN	Extension	City/State	Country	User's Time
Majdi **Abbas**	30329	* 672	Scottsdale, Arizona	United States	03:47 (UTC-7)
Joshua **Abbott**	13749	* 975		United States	04:47 (UTC-6)
Marcelo **Aberbuch**	4230	* 100	Rio de Janeiro	Brazil	07:47 (UTC-3)
Abley Joe	3557	* 563	London, Ontario	Canada	05:47 (UTC-5)
Fisayo **Adeleke**	24935		Ibadan	Nigeria	11:47 (UTC+1)
Jay **Adelson**	23310	* 572	Pawling, New York	United States	05:47 (UTC-5)
Vijay **Adhikari**	3856	* 123		Nepal	15:47 (UTC5)
Mehmet **Akcin**	20144		Marina del Rey, California	United States	02:47 (UTC-8)
Eden **Akhavi**	12682	* EGA	London	United Kingdom	10:47 (UTC)
Cliff **Albert**	28788	* 221	Sittard	Netherlands	11:47 (UTC1)

- Can dial ASN*extension to reach netop

- www.pch.net/inoc-dba

Open Source Projects

- OpenSIPS (nee OpenSER)
- Freeswitch
- Asterisk

Questions ?

netsumo
ispconsultancy

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