

Common VoIP problems, How to detect, correct and avoid them.

Who am I ?

- David Attias
- Installing VoIP systems for over 7 years
- Mikrotik user for 5 years
- Mikrotik certifications
MTCNA, MTCRE & MTCWE

Purpose of this lecture

To inform Mikrotik users on how to identify and resolve voip problems

Agenda

- 1) Identify factors which will affect VoIP call quality
- 2) Correct call quality issues with RouterOS QoS
 - Marking packets with Mangle
 - Shaping VoIP traffic with Queues
- 3) Detecting VoIP call quality problems
 - Check for dropped packets
 - Using RouterOS packet sniffer & wireshark
- 4) Avoid call quality issues

What is VoIP?

Several protocols used together to send and receive REAL TIME voice calls through an IP network(s).

Identify factors that affect
call quality

Considerations about VoIP call quality

- VoIP calls are REAL TIME!!
- Connection between phones and voip servers must have low delay and very low Jitter.
- Must have enough available symmetrical bandwidth.

g711 uLaw codec = 87.2k per channel

[20ms voice payload per packet]

Sip = 65k (max sip message size)

The Problems

What can affect call quality?

*Not considering hardware problems

- High jitter levels
 - What is Jitter? Packet Delay Variation / The time lapse between each packet for a given data stream
- Packet Loss
- Delay

In the real world.

- Jitter, packet loss and delay can happen anywhere between the phone and (hosted) server.
- However, 90% of call quality issues happen at the customer location.

Why? Because customer networks are rarely configured properly – if configured at all for VoIP QoS.

USE MIKROTIK!!!

Correcting issues with RouterOS QoS

Quality Of Service (QoS)

- Techniques that **categorize** and **prioritize** packets
- Ensures sufficient bandwidth, controls latency, jitter, and **reduces** data loss.
- Regulate data flows by classifying, scheduling, and marking packets based on priority and by shaping traffic

MikroTik Mangle

Mikrotik Mangle

- Mangle is a Mikrotik routerOS facility that marks packets for future processing.
- The mangle marks exist only within the router.
- Also used to modify some fields in the IP header, like DSCP and TTL fields
- Only 1 packet mark per packet
Only 1 connection mark per packet

To conserve processor resources:

First mark the connection

Once the session is in “connection tracker” all packets for that session are marked.

This is more efficient because Mangle doesn't need to scrutinize every packet. It just needs to know if the packet is in “that” connection.

Qualify Traffic

- SiP server = 1.2.3.4
- SiP port = 5060 tcp
- RTP port range = 10000 ~ 20000 udp

Mark the SiP connection

Mangle Rule <1.2.3.4:5060>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: invalid established related new

Connection NAT State:

Mangle Rule <1.2.3.4:5060>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Connection Mark:

Passthrough

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

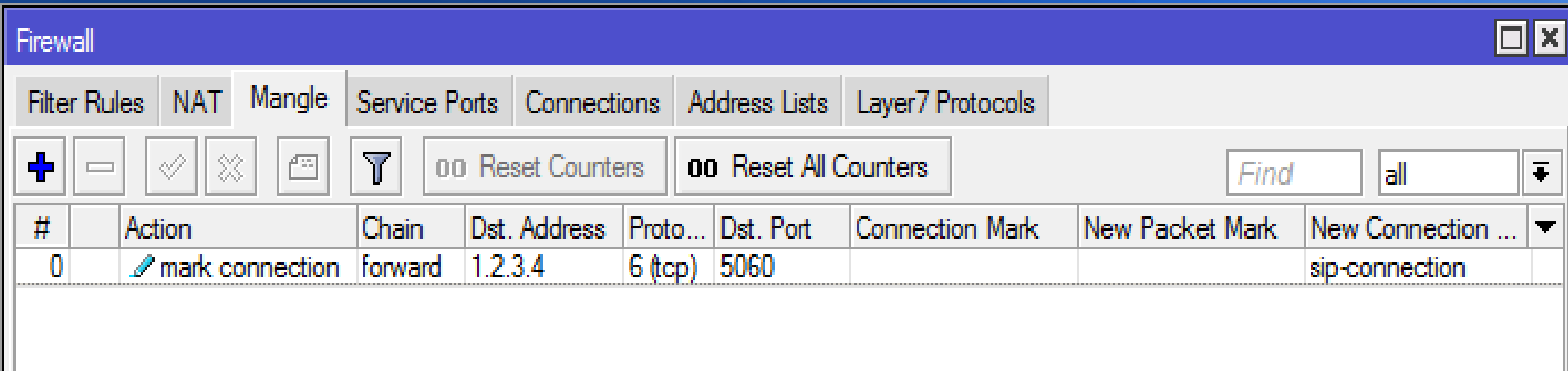
Reset All Counters

Mark the SIP connection


```
/ip firewall mangle
```

```
add chain=forward dst-address=1.2.3.4  
    protocol=tcp dst-port=5060 action=mark-  
    connection new-connection-mark=sip-  
    connection
```

Mark the SiP connection



The screenshot shows the Mikrotik WinBox Firewall configuration interface. The 'Connections' tab is selected. A table lists a single rule with the following details:

#	Action	Chain	Dst. Address	Proto...	Dst. Port	Connection Mark	New Packet Mark	New Connection ...
0	 mark connection	forward	1.2.3.4	6 (tcp)	5060			sip-connection

Additional interface elements include tabs for Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. Below the tabs are buttons for adding (+), removing (-), enabling (checkmark), disabling (X), and deleting (trash) rules, along with filter icons and counter reset buttons.

Mark the SIP packets

Mangle Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mangle Rule <>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Packet Mark:

Passthrough

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mark the SiP packets

```
/ip firewall mangle  
add chain=forward  
    connection-mark=sip-connection  
    add action=mark-packet  
    new-packet-mark=SIP
```

Mark the SIP packets

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ ☰ ⚙ 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Dst. Address	Proto...	Dst. Port	Connection Mark	New Packet Mark	New Connection ...
0	mark connection	forward	1.2.3.4	6 (tcp)	5060			sip-connection
1	mark packet	forward				sip-connection	SIP	

2 items

Mark the RTP connection

Mangle Rule <1.2.3.4>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: invalid established related new

Connection NAT State:

Mangle Rule <1.2.3.4>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Connection Mark:

Passthrough

Mark the RTP connection

```
/ip firewall mangle
```

```
add action=mark-connection chain=forward dst-  
address=1.2.3.4 new-connection-mark=rtp-  
connection port=10000-20000 protocol=udp
```


Mark the RTP connection

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

+ - ✓ ✗ [icon] [funnel] [00] Reset Counters [00] Reset All Counters Find all [dropdown]

#	Action	Chain	Dst. Address	Protocol	Dst. Port	Any. Port	Connection Mark	New Packet Mark	New Connection Mark	[dropdown]
0	mark connection	forward	1.2.3.4	6 (tcp)	5060				sip-connection	
1	mark packet	forward					sip-connection	SIP		
2	mark connection	forward	1.2.3.4	17 (udp)		10000-20000			rtp-connection	

3 items

Mark the RTP packets

Mangle Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mangle Rule <>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

New Packet Mark:

Passthrough

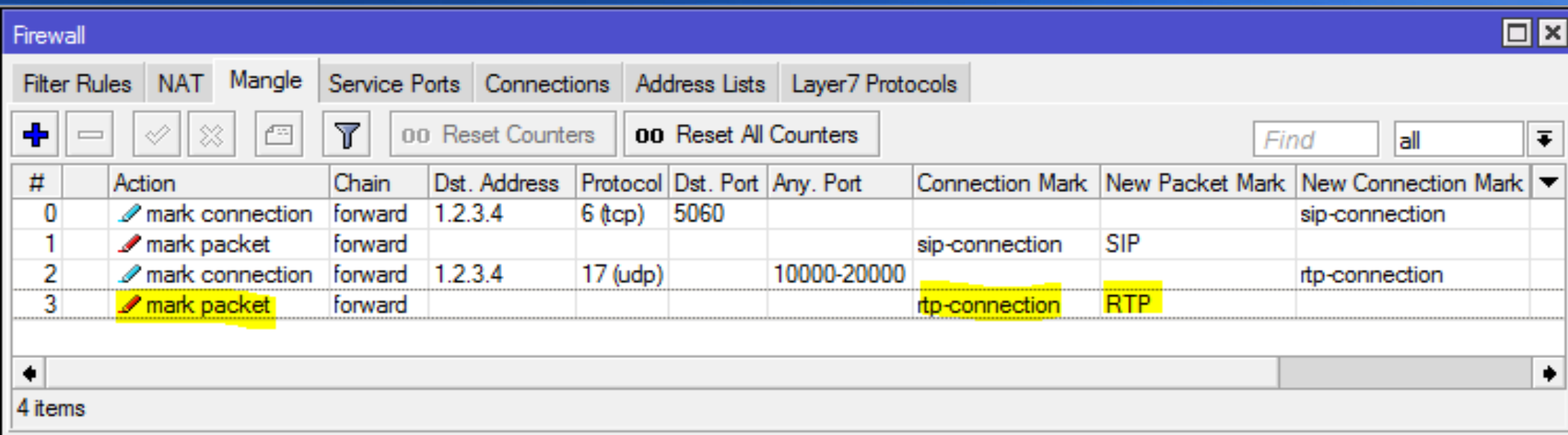
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mark the RTP connection

```
/ip firewall mangle
```

```
add action=mark-packet chain=forward  
    connection-mark=rtp-connection new-packet-  
    mark=RTP
```

Mark the RTP Packet





The screenshot shows the Mikrotik WinBox Firewall configuration window, specifically the Layer7 Protocols tab. The interface includes a toolbar with icons for adding, deleting, and enabling rules, as well as buttons for 'Reset Counters' and 'Reset All Counters'. A search bar is present with the text 'Find' and 'all'. Below the toolbar is a table of firewall rules. The table has columns for '#', 'Action', 'Chain', 'Dst. Address', 'Protocol', 'Dst. Port', 'Any. Port', 'Connection Mark', 'New Packet Mark', and 'New Connection Mark'. Rule 3 is highlighted in yellow, showing an action of 'mark packet' for protocol 17 (udp) on ports 10000-20000, with connection mark 'rtp-connection' and new packet mark 'RTP'. The bottom of the window shows '4 items'.


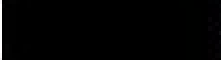

#	Action	Chain	Dst. Address	Protocol	Dst. Port	Any. Port	Connection Mark	New Packet Mark	New Connection Mark
0	mark connection	forward	1.2.3.4	6 (tcp)	5060				sip-connection
1	mark packet	forward					sip-connection	SIP	
2	mark connection	forward	1.2.3.4	17 (udp)		10000-20000			rtp-connection
3	mark packet	forward					rtp-connection	RTP	

How do we know its working?

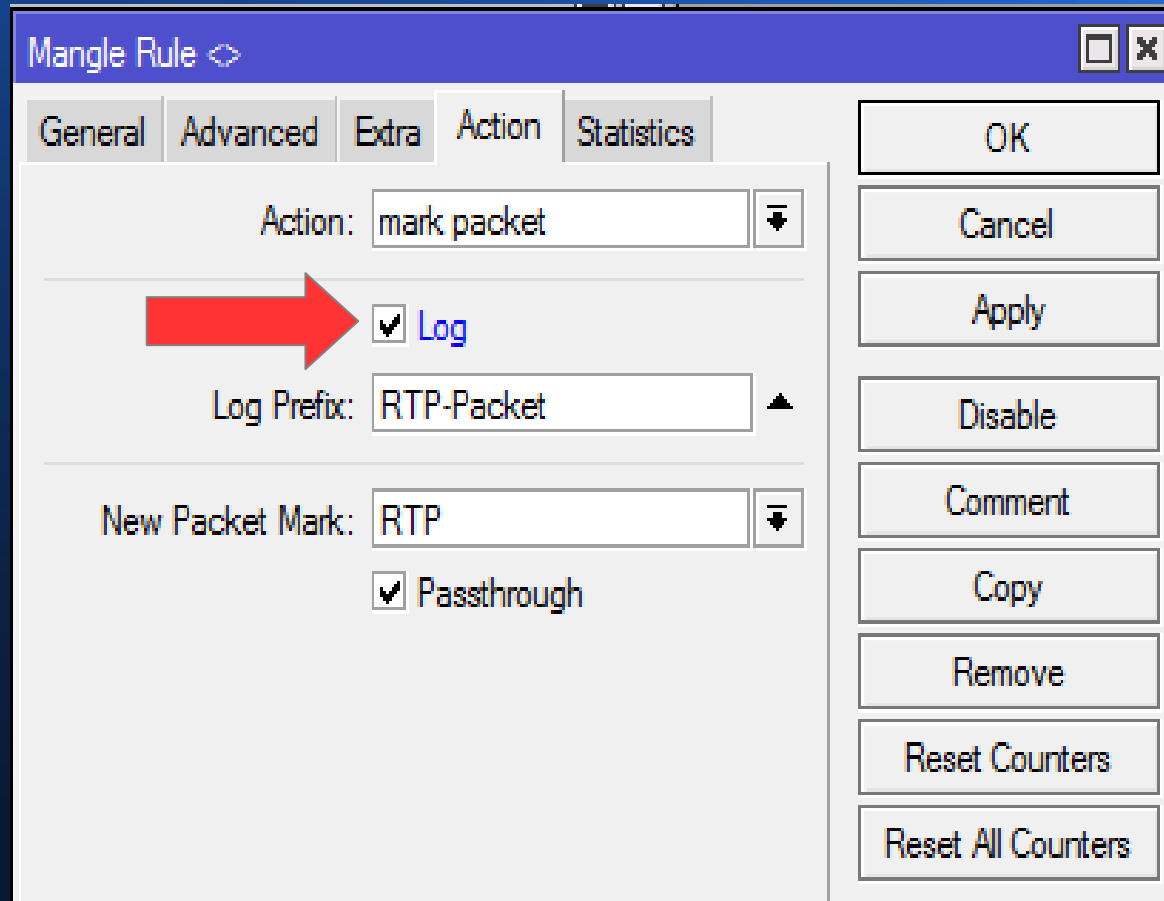
Firewall

Filter Rules NAT Mangle Service Ports **Connections** Address Lists Layer7 Protocols

  Tracking

	Src. Address	Dst. Address	Protocol	Connection Mark	
SACs	192.168.20.100:5060	 :5060	17 (udp)	sip-connection	
SACs	192.168.20.101:5060	 :5060	17 (udp)	sip-connection	
SACs	192.168.20.100:14534	 :12154	17 (udp)	rtp-connection	

How do we know it's working?



Apr/20/2016 10:46:14 memory firewall, info RTP-Packet forward: in:vlan20 out:ether1-gateway, src-mac ec:e1:a9:cd:aa:7d, proto UDP, 192.168.20.100:18338->7

Change DSCP

Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic.

Change DSCP

Mangle Rule ◁

General | Advanced | Extra | Action | Statistics

Chain: ▾

Src. Address: ▾

Dst. Address: ▾

Protocol: ▾

Src. Port: ▾

Dst. Port: ▾

Any. Port: ▾

P2P: ▾

In. Interface: ▾

Out. Interface: ▾ ▲

Packet Mark: ▾ ▲

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mangle Rule ◁

General | Advanced | Extra | Action | Statistics

Action: ▾

Log

Log Prefix: ▲

New DSCP (TOS): ▾

Passthrough

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Mikrotik Queues

Mikrotik Queues

- limit data rate for certain IP addresses, subnets, protocols, ports, and other parameters
- limit peer-to-peer traffic
- prioritize some packet flows over others
- configure traffic bursts for faster web browsing
- apply different limits based on time
- share available traffic among users equally, or depending on the load of the channel

Mikrotik Queues

Parent Queues (inner queues) – distribute bandwidth

Child Queues (leaf queues) – consume bandwidth

Mikrotik Queues

The screenshot shows the Mikrotik Queue List interface. It features a table with columns for Name, Parent, and Packet Marks. A red arrow labeled 'Parent Queue' points to the 'download' queue, and another red arrow labeled 'Child Queues' points to the 'download_pri_1' and 'download_pri_2' queues.

Name	Parent	Packet Marks
download	bridge-local	
download_pri_1	download	RTP
download_pri_2	download	SIP

Mikrotik Parent Queues

- Parent Queues only responsibility is to distribute traffic to child queues.
- Parent queue will first satisfy the child queue's "limit-at" traffic then try and reach child "max-limit".
- Priorities are ignored on Parent Queues.

Mikrotik Queue priorities

- 8 is the lowest priority, 1 is the highest.
- Queue with higher priority will have a chance to satisfy its max-limit value before lower priority queues.
- Actual traffic prioritization will work **only** if limits are specified.

Create A Queue Tree

- Scenario:

My home office

5 phones

internet bandwidth = 35Mb download
4Mb upload

Create A Queue Tree

- First create a queue
 /queue tree
add limit-at=4M max-limit=4M
name=upload
parent=ether1-gateway
priority=8 queue=default

Queue <upload>

General Statistics

Name:

Parent:

Packet Marks:

Queue Type:

Priority:

Limit At: bits/s

Max Limit: bits/s

Burst Limit: bits/s

Burst Threshold: bits/s

Burst Time: s

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Create A Child Queue

- Create an RTP queue and select it's "parent" as "upload"

add limit-at=440k
max-limit=440k
name=upload_pri_1
packet-mark=RTP
parent=upload
priority=1
queue=default

The screenshot shows a window titled "Queue <upload_pri_1>". It has two tabs: "General" (selected) and "Statistics". The "General" tab contains the following fields:

- Name: upload_pri_1
- Parent: upload
- Packet Marks: RTP
- Queue Type: default
- Priority: 1
- Limit At: 440k (bits/s)
- Max Limit: 440k (bits/s)
- Burst Limit: (empty) (bits/s)
- Burst Threshold: (empty) (bits/s)
- Burst Time: (empty) (s)

On the right side of the window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. At the bottom left of the window, the text "enabled" is visible.

Create A Child Queue

- Create a SIP queue and select it's "parent" as "upload"

add limit-at=325k
max-limit=325k
name=upload_pri_2
packet-mark=SIP
parent=upload
priority=2
queue=default

The screenshot shows a configuration window titled "Queue <upload_pri_2>". It has two tabs: "General" and "Statistics". The "General" tab is active. The fields are as follows:

- Name: upload_pri_2
- Parent: upload
- Packet Marks: SIP
- Queue Type: default
- Priority: 2
- Limit At: 325k (bits/s)
- Max Limit: 325k (bits/s)
- Burst Limit: (empty) (bits/s)
- Burst Threshold: (empty) (bits/s)
- Burst Time: (empty) (s)

On the right side, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. At the bottom left, there is a checkbox labeled "enabled" which is checked.

Create A Child Queue

What about packets without any marks?

Create A Child Queue

- Create a “no mark” queue and select it's “parent” as “upload”

add limit-at=3M
max-limit=3M
name=upload_pri_2
packet-mark=SIP
parent=upload
priority=2
queue=default

The screenshot shows a configuration window titled "Queue <upload_pri_8>". It has two tabs: "General" and "Statistics". The "General" tab is active. The fields are as follows:

- Name: upload_pri_8
- Parent: upload
- Packet Marks: no-mark
- Queue Type: default
- Priority: 8
- Limit At: (empty) bits/s
- Max Limit: 3M bits/s
- Burst Limit: (empty) bits/s
- Burst Threshold: (empty) bits/s
- Burst Time: (empty) s

On the right side, there are several buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters. At the bottom left, there is a checkbox labeled "enabled" which is checked.

Queue Tree GUI view

Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

Name	Parent	Packet M...	Limit At ...	Max Limit...	Avg. Rate	Packets	Dropped
upload	ether1-gateway			4M	88 bps	4 020 701	0
upload_pri_1	upload	RTP	440k	440k	0 bps	318 512	0
upload_pri_2	upload	SIP	325k	325k	0 bps	244 094	0
upload_pri_8	upload	no-mark		3M	88 bps	2 127 445	37 475
download	bridge-local			35M	53.9 kbps	2 829 375	0
download_pri_1	download	RTP	440k	440k	0 bps	316 299	0
download_pri_2	download	SIP	325k	325k	0 bps	244 847	0
download_pri_8	download	no-mark		34M	53.9 kbps	1 858 708	0

Queue Tree GUI view

Queue List

Simple Queues Interface Queues **Queue Tree** Queue Types








Name	Parent	Packet M...	Limit At ...	Max Limit...	Avg. Rate	Packets	Dropped
download	bridge-local			35M	59.5 kbps	2 831 854	0
download_pri_1	download	RTP	440k	440k	0 bps	316 299	0
download_pri_2	download	SIP	325k	325k	6.7 kbps	245 095	0
download_pri_3	download	TCP-ACK	1M	1M	128 bps	201	0
download_pri_4	download	DNS	1k	128k	0 bps	0	0
download_pri_8	download	no-mark		34M	52.6 kbps	1 860 738	0
upload	ether1-gateway			4M	8.5 kbps	4 021 472	0
upload_pri_1	upload	RTP	440k	440k	0 bps	318 512	0
upload_pri_2	upload	SIP	325k	325k	7.8 kbps	244 341	0
upload_pri_3	upload	TCP-ACK	1M	1500k	480 bps	299	0
upload_pri_4	upload	DNS	1k	128k	0 bps	0	0
upload_pri_8	upload	no-mark		3M	192 bps	2 127 670	37 475

Detecting Problems

Detecting problems

- Check for “dropped packets” in queue tree
- Enable the “dropped packets” view

Detecting problems

The screenshot shows the Mikrotik WinBox interface with the 'Queue List' window open. The window displays a table of queues with columns for Name, Parent, Packet Marks, Limit At, Max Limit, Avg. Rate, and Dropped. A context menu is open over the 'Dropped' column header, with the 'Show Columns' option selected. A secondary column selection menu is also visible on the right side of the screen, showing a list of columns with checkboxes. The 'Dropped' checkbox is checked, and a red arrow points to it.

Name	Parent	Packet Marks	Limit At ...	Max Limit...	Avg. Rate	Dropped
download	bridge-local		35M	35M	16.8 kbps	0
download_pri_1	download	RTP	440k	440k	0 bps	0
download_pri_2	download	SIP	325k	325k	0 bps	0
download_pri_8	download	no-mark		34M	16.8 kbps	759
upload	ether1-gateway		4M	4M	0 bps	0
upload_pri_1	upload	RTP	440k	440k	0 bps	0
upload_pri_2	upload	SIP	325k	325k	0 bps	0
upload_pri_8	upload	no-mark		3M	0 bps	248

8 items 0 B queued 0 packets queued

- Name
- Parent
- Packet Marks
- Queue Type
- Priority
- Limit At
- Max Limit
- Burst Limit
- Burst Threshold
- Burst Time
- Avg. Rate
- Avg. Packet Rate
- Queued Bytes
- Queued Packets
- Bytes
- Packets
- Dropped
- Parent Queues

Detecting problems

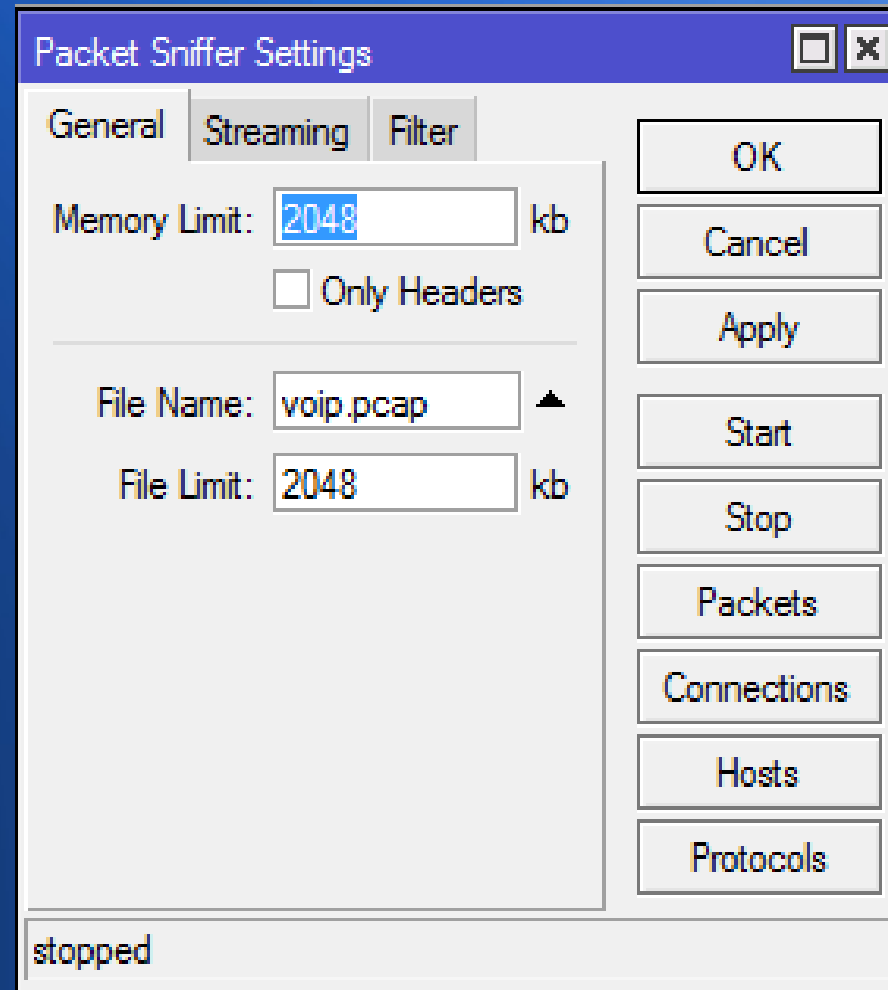
Mikrotik packet capture

Detecting problems

Mikrotik packet capture

From GUI:

Tools – Packet sniffer



Detecting problems

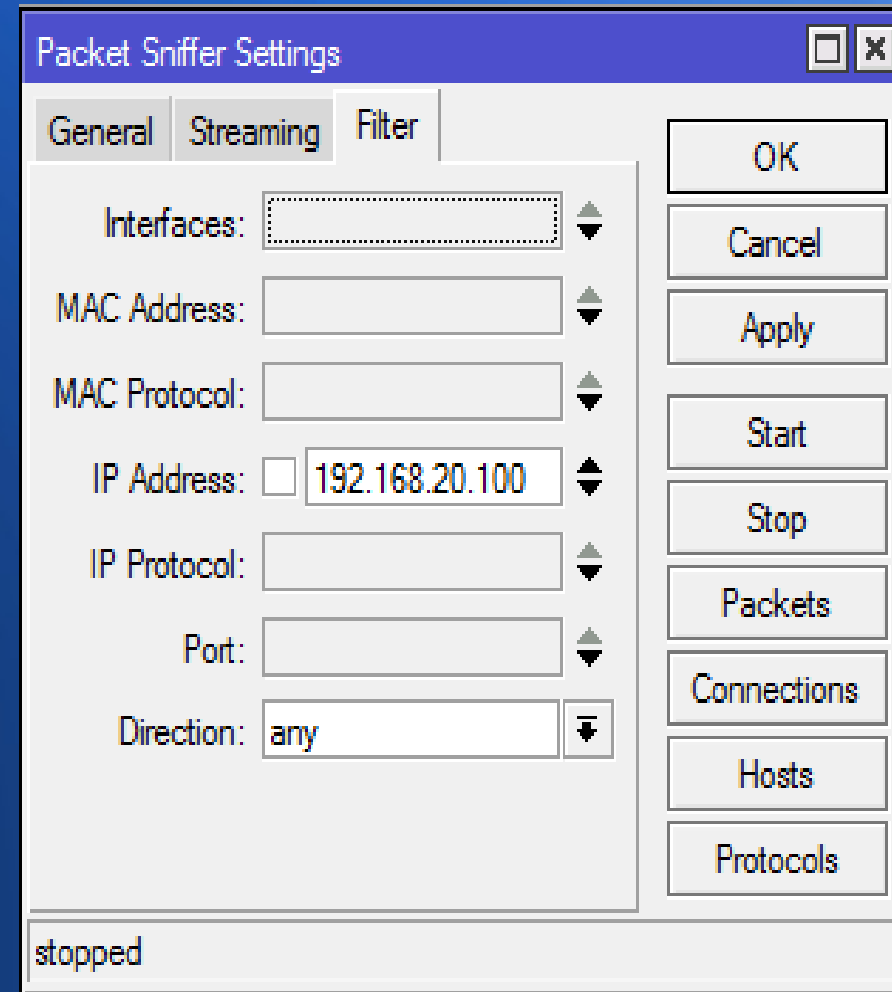
Mikrotik packet capture

From GUI:

Tools – Packet sniffer

Filter

IP



Detecting problems

Cap file voip.pcap will be created in “Files”

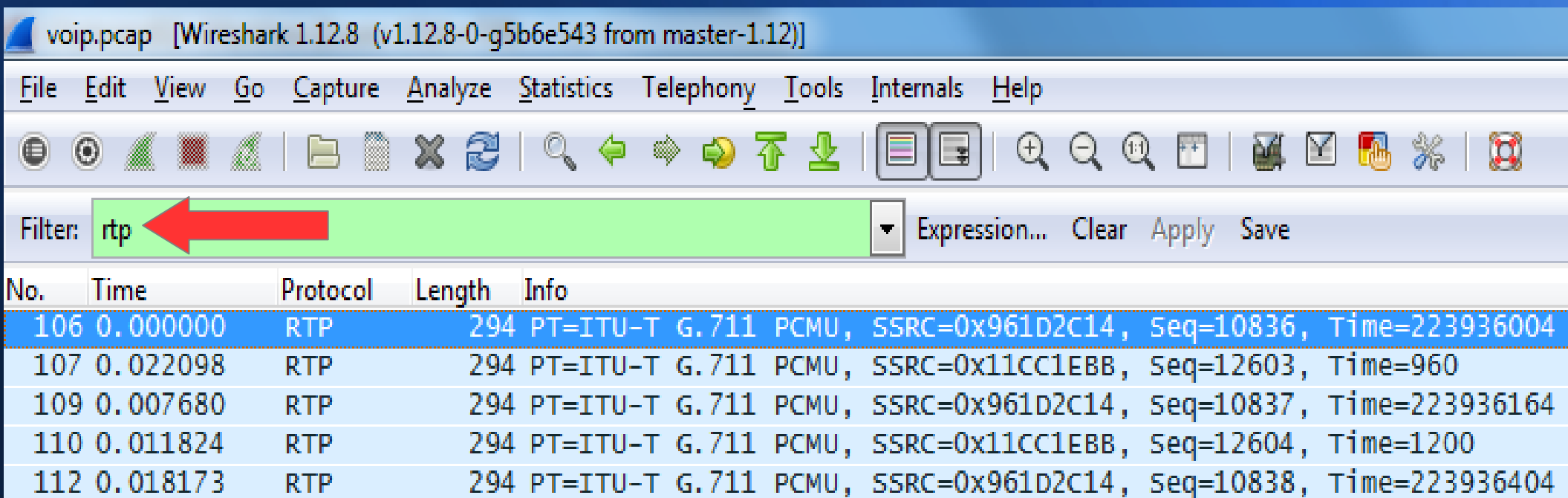
Download it

Then open voip.pcap in wireshark

Detecting problems

Filter = rtp

Then select one RTP packet



The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'voip.pcap' and the version is 'Wireshark 1.12.8 (v1.12.8-0-g5b6e543 from master-1.12)'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, search, and analysis. The filter field is set to 'rtp', with a red arrow pointing to it. The packet list pane shows several RTP packets, with packet 106 selected.

No.	Time	Protocol	Length	Info
106	0.000000	RTP	294	PT=ITU-T G.711 PCMU, SSRC=0x961D2C14, Seq=10836, Time=223936004
107	0.022098	RTP	294	PT=ITU-T G.711 PCMU, SSRC=0x11CC1EBB, Seq=12603, Time=960
109	0.007680	RTP	294	PT=ITU-T G.711 PCMU, SSRC=0x961D2C14, Seq=10837, Time=223936164
110	0.011824	RTP	294	PT=ITU-T G.711 PCMU, SSRC=0x11CC1EBB, Seq=12604, Time=1200
112	0.018173	RTP	294	PT=ITU-T G.711 PCMU, SSRC=0x961D2C14, Seq=10838, Time=223936404

Detecting problems

Select “Telephony” - “RTP” - “Stream Analysis”

The screenshot shows the Wireshark interface with the 'Telephony' menu open. A red arrow points to the 'Telephony' menu, and another red arrow points to the 'RTP' option within the menu. A third red arrow points to the 'Stream Analysis...' option in the sub-menu that appears after selecting 'RTP'. The main packet list shows several RTP packets with a filter of 'rtp'.

No.	Time	Protocol	Length	Info
106	0.000000	RTP	294	PT=ITU
107	0.022098	RTP	294	PT=ITU
109	0.007680	RTP	294	PT=ITU
110	0.011824	RTP	294	PT=ITU
112	0.018173	RTP	294	PT=ITU
113	0.022452	RTP	294	PT=ITU

Telephony menu items:

- ANSI
- GSM
- IAX2
- ISUP Messages
- LTE
- MTP3
- RTP
- RTSP
- SCTP

Sub-menu items for RTP:

- Show All Streams
- Stream Analysis...

Detecting problems

Wireshark: RTP Stream Analysis

Forward Direction | Reversed Direction

Analysing stream from 192.168.20.100 port 10920 to [redacted] port 16982 SSRC = 0x961D2C14

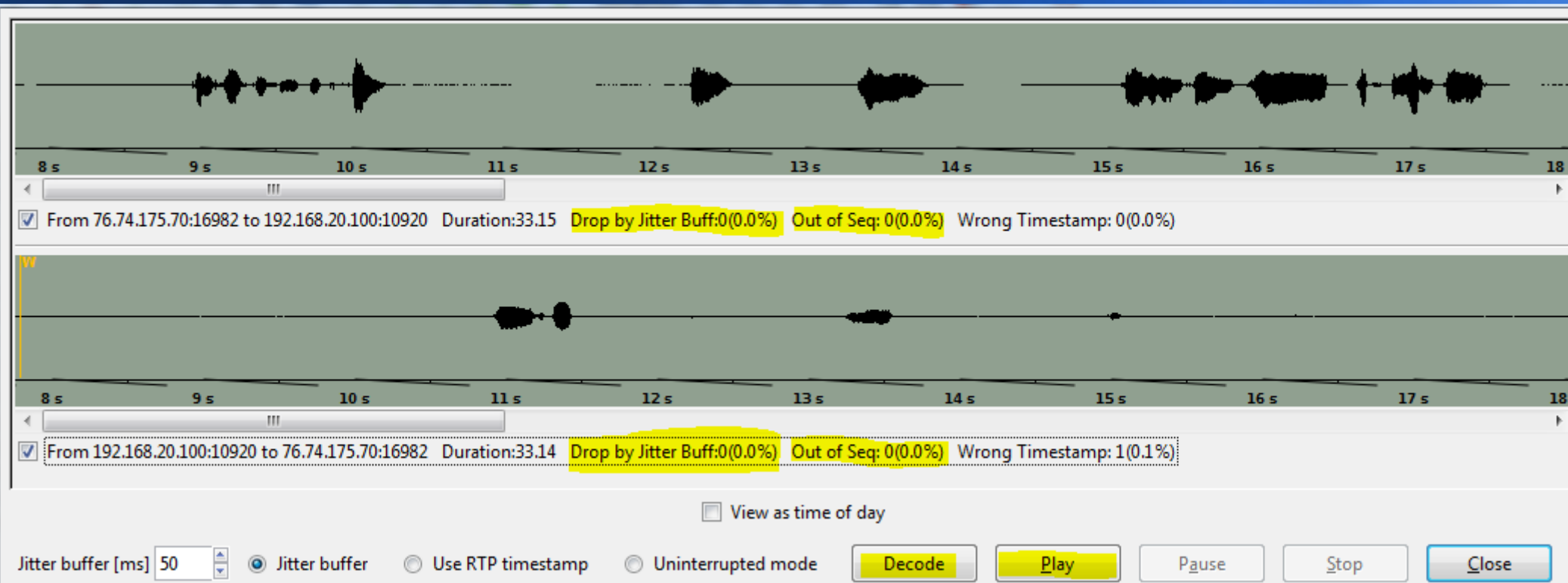
Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps)	Marker	Status
106	10836	0.00	0.00	0.00	2.24		[Ok]
109	10837	29.78	0.61	-9.78	4.48		[Ok]
112	10838	30.00	0.57	-9.77	6.72		[Ok]
115	10839	30.03	0.54	-9.81	8.96		[Ok]
118	10840	29.95	0.51	-9.76	11.20		[Ok]
121	10841	30.03	0.48	-9.80	13.44		[Ok]
124	10842	30.06	0.45	-9.85	15.68		[Ok]
127	10843	29.93	0.43	-9.79	17.92		[Ok]

Max delta = 32.87 ms at packet no. 2620
Max jitter = 0.61 ms. Mean jitter = 0.09 ms.
Max skew = -13.56 ms.
Total RTP packets = 1105 (expected 1105) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Duration 33.12 s (-62 ms clock drift, corresponding to 7985 Hz (-0.19%))

Save payload... | Save as CSV... | Refresh | Jump to | Graph | Player | Next non-Ok | Close

Detecting problems

Click “Player” - “Decode” - “Play”



Avoid Problems

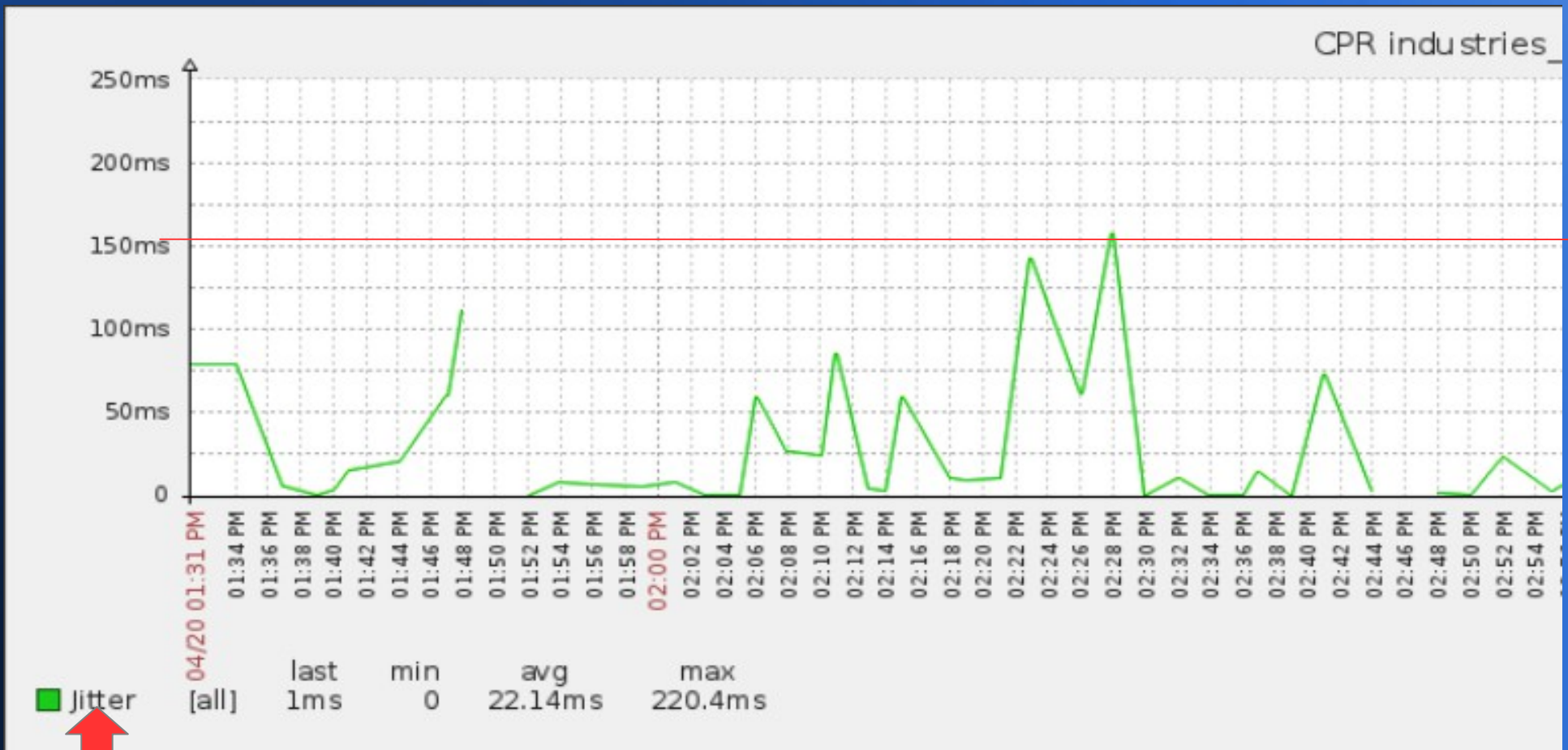
Before on-boarding a customer:

Make sure their internet connection is adequate!

Monitor their WAN

Review the monitoring data!

Avoid Problems



Avoid Problems

- Packet capture every call! www.sipcapture.org
- Also be aware of internet carrier problems
www.internethealthreport.com

Avoid Problems

internethealthreport.com | Search

faxsipit portal

dynatrace keynote

Internet Health Report Generated from 4/20/2016 12:30:46 PM to 4/20/2016 1:30:46 PM (PDT)
[Monitor your performance](#) | [Help](#)

Focus: From: To: Metric: Period:

View: **Destination by Origin** Metrics by Origin

Destination - Latency (ms) - Last 1 Hour

! abc [AT&T](#) [CenturyLink](#) [Cogent](#) [Level3](#) [SBC](#) [Sprint](#) [Verizon](#) [XO](#)

Origin	AT&T	CenturyLink	Cogent	Level3	SBC	Sprint	Verizon	XO
AT&T	3	54	45	81	49	75	62	41
CenturyLink	54	6	34	29	28	28	53	25
Cogent	45	31	14	34	29	17	39	27
Level3	82	23	21	18	12	16	27	31
Savvis	47	21	20	7	2	24	29	19
SBC	50	28	22	11	1	25	33	22
Sprint	76	29	18	26	25	2	32	34
Verizon	67	36	32	66	29	27	9	42
XO	50	19	25	34	15	30	31	15

Healthy < 90ms Latency. Warning < 180ms Latency

Summary

- 1- Learned about some factors that affect VoIP call quality
- 2- Learned how to reduce or eliminate call quality issues
- 3- Learned how to find issues and diagnose issues
- 4- Learned how to avoid issues