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
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
Mark the SiP packets
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

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Dst. Address</th>
<th>Proto</th>
<th>Dst. Port</th>
<th>Connection Mark</th>
<th>New Packet Mark</th>
<th>New Connection Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>mark connection</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>6 (tcp)</td>
<td>5060</td>
<td>sip-connection</td>
<td>SIP</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>mark packet</td>
<td>forward</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 items
Mark the RTP connection
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

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Dst. Address</th>
<th>Protocol</th>
<th>Dst. Port</th>
<th>Any. Port</th>
<th>Connection Mark</th>
<th>New Packet Mark</th>
<th>New Connection Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>mark connection</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>tcp (6)</td>
<td>5060</td>
<td></td>
<td>sip-connection</td>
<td>SIP</td>
<td>rtp-connection</td>
</tr>
<tr>
<td>1</td>
<td>mark packet</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>udp (17)</td>
<td>10000-20000</td>
<td></td>
<td>sip-connection</td>
<td>SIP</td>
<td>rtp-connection</td>
</tr>
<tr>
<td>2</td>
<td>mark connection</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>udp (17)</td>
<td>10000-20000</td>
<td></td>
<td>sip-connection</td>
<td>SIP</td>
<td>rtp-connection</td>
</tr>
</tbody>
</table>
Mark the RTP packets
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

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Chain</th>
<th>Dst. Address</th>
<th>Protocol</th>
<th>Dst. Port</th>
<th>Any. Port</th>
<th>Connection Mark</th>
<th>New Packet Mark</th>
<th>New Connection Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>mark connection</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>6 (tcp)</td>
<td>5060</td>
<td></td>
<td></td>
<td>sip-connection</td>
<td>SIP</td>
</tr>
<tr>
<td>1</td>
<td>mark packet</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>6 (tcp)</td>
<td>5060</td>
<td></td>
<td></td>
<td>sip-connection</td>
<td>SIP</td>
</tr>
<tr>
<td>2</td>
<td>mark connection</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>17 (udp)</td>
<td>10000-20000</td>
<td></td>
<td></td>
<td>rtp-connection</td>
<td>RTP</td>
</tr>
<tr>
<td>3</td>
<td>mark packet</td>
<td>forward</td>
<td>1.2.3.4</td>
<td>17 (udp)</td>
<td>10000-20000</td>
<td></td>
<td></td>
<td>rtp-connection</td>
<td>RTP</td>
</tr>
</tbody>
</table>
How do we know it's working?

![Firewall Table]

<table>
<thead>
<tr>
<th>Src. Address</th>
<th>Dst. Address</th>
<th>Protocol</th>
<th>Connection Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>SACs 192.168.20.100:5060</td>
<td>&lt;/br&gt;</td>
<td>17 (udp)</td>
<td>sip-connection</td>
</tr>
<tr>
<td>SACs 192.168.20.101:5060</td>
<td>&lt;/br&gt;</td>
<td>17 (udp)</td>
<td>sip-connection</td>
</tr>
<tr>
<td>SACs 192.168.20.100:14534</td>
<td>&lt;/br&gt;</td>
<td>17 (udp)</td>
<td>rtp-connection</td>
</tr>
</tbody>
</table>
How do we know it's working?
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
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

Parent Queue

Child Queues
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
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
Create A Child Queue

- Create a SIP queue and select its "parent" as "upload"
  
  add limit-at=325k  
  max-limit=325k  
  name=upload_pri_2  
  packet-mark=SIP  
  parent=upload  
  priority=2  
  queue=default
Create A Child Queue

What about packets without any marks?
Create A Child Queue

- Create a “no mark” queue and select its “parent” as “upload”

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Parent</th>
<th>Packet Model</th>
<th>Limit At</th>
<th>Max Limit</th>
<th>Avg. Rate</th>
<th>Packets</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>upload</td>
<td>ether1-gateway</td>
<td>RTP</td>
<td>440k</td>
<td>440k</td>
<td>0 bps</td>
<td>4 020 701</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_1</td>
<td>upload</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>318 512</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_2</td>
<td>upload</td>
<td>SIP</td>
<td>325k</td>
<td>325k</td>
<td>0 bps</td>
<td>2 440 944</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_8</td>
<td>upload</td>
<td>no-mark</td>
<td>3M</td>
<td>88 bps</td>
<td></td>
<td>2 127 445</td>
<td>37 475</td>
</tr>
<tr>
<td>download</td>
<td>bridge-local</td>
<td></td>
<td>35M</td>
<td>53.9 kbps</td>
<td></td>
<td>2 829 375</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_1</td>
<td>download</td>
<td>RTP</td>
<td>440k</td>
<td>440k</td>
<td>0 bps</td>
<td>316 299</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_2</td>
<td>download</td>
<td>SIP</td>
<td>325k</td>
<td>325k</td>
<td>0 bps</td>
<td>2 440 847</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_8</td>
<td>download</td>
<td>no-mark</td>
<td>34M</td>
<td>53.9 kbps</td>
<td></td>
<td>1 858 708</td>
<td>0</td>
</tr>
</tbody>
</table>
Queue Tree GUI view

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

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

- Check for "dropped packets" in queue tree
- Enable the "dropped packets" view

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Parent</th>
<th>Packet Marks</th>
<th>Limit At</th>
<th>Max Limit</th>
<th>Avg. Rate</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>download</td>
<td>bridge-local</td>
<td></td>
<td>35M</td>
<td>35M</td>
<td>16.8 kbps</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_1</td>
<td>download</td>
<td>RTP</td>
<td>440k</td>
<td>440k</td>
<td>0 bps</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_2</td>
<td>download</td>
<td>SIP</td>
<td>325k</td>
<td>325k</td>
<td>0 bps</td>
<td>0</td>
</tr>
<tr>
<td>download_pri_8</td>
<td>download</td>
<td>no-mark</td>
<td>34M</td>
<td>34M</td>
<td>16.8 kbps</td>
<td>759</td>
</tr>
<tr>
<td>upload</td>
<td>ether1-gateway</td>
<td></td>
<td>4M</td>
<td>4M</td>
<td>0 bps</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_1</td>
<td>upload</td>
<td>RTP</td>
<td>440k</td>
<td>440k</td>
<td>0 bps</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_2</td>
<td>upload</td>
<td>SIP</td>
<td>325k</td>
<td>325k</td>
<td>0 bps</td>
<td>0</td>
</tr>
<tr>
<td>upload_pri_8</td>
<td>upload</td>
<td>no-mark</td>
<td>3M</td>
<td>3M</td>
<td>0 bps</td>
<td>248</td>
</tr>
</tbody>
</table>
```
Detecting problems

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

Filer = rtp

Then select one RTP packet
Detecting problems

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

![Wireshark RTP Stream Analysis](image.png)

- **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**

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

- Duration 33.12 s (-62 ms clock drift, corresponding to 7985 Hz (-0.19%))
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

<table>
<thead>
<tr>
<th></th>
<th>AT&amp;T</th>
<th>CenturyLink</th>
<th>Cogent</th>
<th>Level3</th>
<th>Savvis</th>
<th>SBC</th>
<th>Sprint</th>
<th>Verizon</th>
<th>XO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Latency (ms)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Destination - Latency (ms) - Last 1 Hour</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Focus:</strong> From:</td>
<td>AT&amp;T</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>To:</strong></td>
<td></td>
<td>CenturyLink</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Metric:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Period:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>View:</strong></td>
<td></td>
<td>Destination by Origin</td>
<td>Metrics by Origin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **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