

SIP session helper / ALG

Starting @ 1:30pm

Who am I ?

- David Attias
- Installing VoIP systems for over 11 years
- Owner of Penny Tone LLC
- Mikrotik user for 6 years
- Mikrotik Trainer
MTCNA, MTCRE & MTCWE

Purpose of this lecture

To inform Mikrotik users on the purpose and functions of SIP ALG.

Agenda

- 1- What is ALG & what does it do.
- 2- The problem with VoIP and NAT
- 3- When is SIP ALG necessary and unnecessary?
- 4- How SIP ALG corrects problems.
- 5- Testing with Wireshark
- 6- SIP ALG Timeout
- 7- SIP ALG direct-media

WHAT IS ALG?

WHAT IS ALG?

- Application Layer Gateway
- A **G**ateway (firewall) that re-writes specific **A**pplication **L**ayer data fields.
- ALG is a firewall feature that rewrites Layer 7 data for specific applications.

Keep in mind

- Only applies to NAT translation rules.
- NAT'ed devices are unaware that ALG is changing anything.
- Also known as:
 - NAT helper (Linux)
 - NAT session helper
 - SIP Transformations
 - Service ports

The Problem with VoIP and NAT

The Problem with VoIP and NAT

- SIP servers need to know the IP of all registered phones.
- Phones register their locally configured IP with the SIP server.
- If the phone and server are in the same network, no problems.
- If the phone is behind NAT and reports its IP to a remote server, the server responses will NOT be able to reach the phone.

The Result

- Phone can not receive calls
- One way audio

What ALG Does.

What ALG Does.

- **ALG does exactly the same thing NAT translation does, but at layer 7**
- ALG intercepts the application messages before they leave the router
- Then inspects and replaces the “private client ip:port” with the “public ip:port” of the router (nat rule)

What ALG Does



Dear SIP Server,
I've been thinking about you and I want to
INVITE you to SIP and RTP with me.
Contact 192.168.20.100

What ALG Does



Dear SIP Server,
I've been thinking about you and I want to
INVITE you to SIP and RTP with me.
Contact ~~192.168.20.100~~

75.142.151.49

ALG WAS HERE

Basic terms

SIP and SDP

- SIP and SDP are VoIP Layer 7 protocols
- SIP – Session Initiated Protocol are commands exchanged between sip devices (register, invite, trying, hold, xfer, bye)
- SDP – Session Description Protocol is information about the audio (RTP) stream of a call.

RouterOS SIP ALG settings

RouterOS SIP ALG options

/ip firewall service-port

- Ports:**
- Remote Sip Server listening port. default values are 5060,5061
 - Applies to TCP and UDP
 - Single port, no ranges
 - Up to 8 entries
- Sip-direct-media**
- Allows a redirect of the RTP media stream to go directly from sip device to sip device
 - Default value is yes.
- Timeout:**
- Sets the sip UDP timeout in connection tracker.
 - Default is 1 hour

Mikrotik CLI

/ip firewall service-port

set sip ports=5060,5061 sip-direct-media=yes sip-timeout=01:00:00 disabled=no

How does ALG correct SIP problems?

How does ALG correct SIP problems?

- By replacing specific private IP:port with router's wan side IP:port

ALG changes:

SIP headers: Via, Contact

SDP Body: m= o= c=

- ALG makes changes to Layer 7 data transparently as it passes through the NAT rule.

Layer 7 data before and after (with ALG enabled)

Layer 7 Data with before ALG

SIP REGISTER message **BEFORE** ALG modification:

REGISTER sip:207.252.1.148 SIP/2.0

Via: SIP/2.0/UDP **192.168.20.100:5060**;branch=z9hG4bK-8fb0e171

From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06bec0

To: "David Attias" <sip:201525@207.252.1.148>

Call-ID: 6894e30c-h1c8d357@192.168.20.100

CSeq: 1373 REGISTER

Max-Forwards: 70

Contact: "David Attias" <sip:201525@**192.168.20.100:5060**>;expires=3600

User-Agent: Cisco/SPA504G-7.6.2b

Content-Length: 0

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE

Supported: replaces



The fields ALG
will change

Layer 7 Data with after ALG

SIP REGISTER message **AFTER** ALG modification:

REGISTER sip:207.252.1.148 SIP/2.0

Via: SIP/2.0/UDP **75.142.151.49:1024**;branch=z9hG4bK-8fb0e171

From: "David Attias" <sip:525@207.252.1.148>;tag=191914b06bec0

To: "David Attias" <sip:525@207.252.1.148>

Call-ID: 6894e30c-h1c8d357@192.168.20.100

CSeq: 1373 REGISTER

Max-Forwards: 70

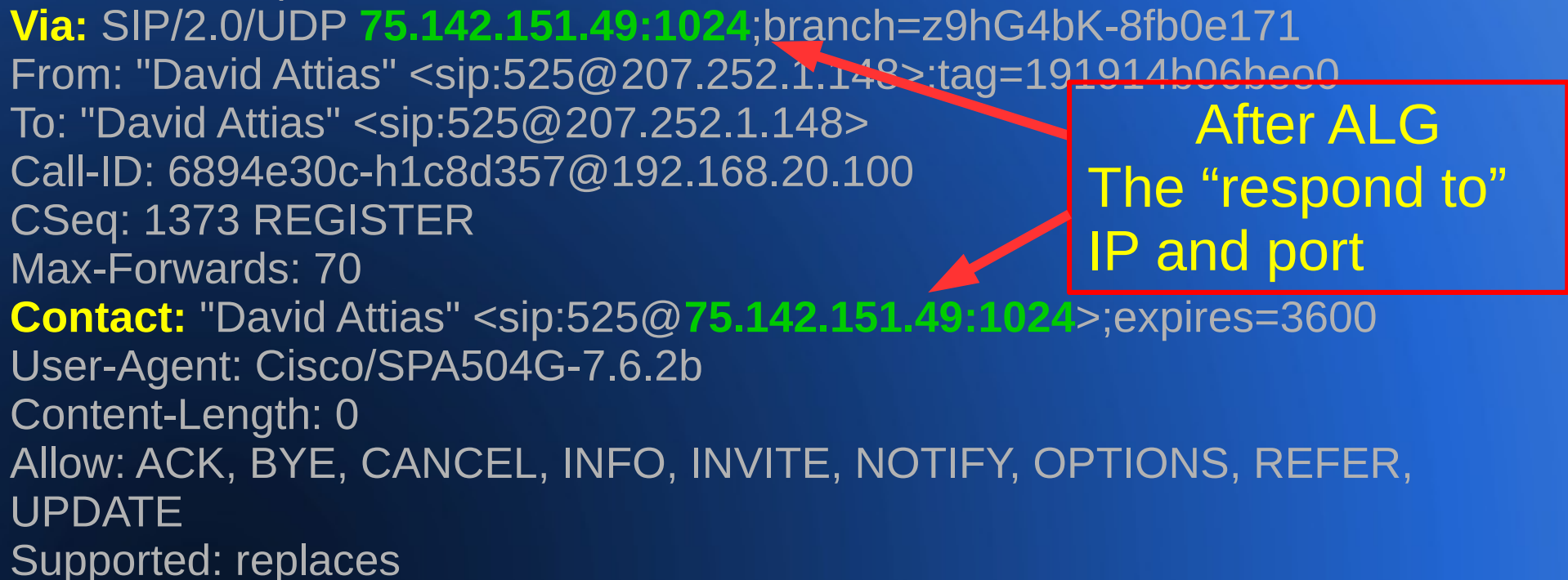
Contact: "David Attias" <sip:525@**75.142.151.49:1024**>;expires=3600

User-Agent: Cisco/SPA504G-7.6.2b

Content-Length: 0

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE

Supported: replaces



After ALG
The "respond to"
IP and port

Layer 7 Data with before ALG

```
INVITE sip:*98@207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-7badf56d
From: "David Attias" <sip:525@207.252.1.148>;tag=f95367fa52060ce5o0
To: "Voice Mail" <sip:*98@207.252.1.148>
Call-ID: 9c8a315e-419d32d1@192.168.20.100
CSeq: 101 INVITE
Max-Forwards: 70
Contact: "David Attias" <sip:525@192.168.20.100:5060>
Expires: 240
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 397
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
Content-Type: application/sdp
```

SIP Headers

Before ALG
modifies layer 7
data

```
v=0
o= 176664 176664 IN IP4 192.168.20.100
s=-
c=IN IP4 192.168.20.100
t=0 0
m=audio 14254 RTP/AVP 0 2 8 9 18 96 97 98 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtpmap:2 G726-32/8000
a=fmtp:101 0-15
a=ptime:30
a=sendrecv
```

SDP Body

Layer 7 Data with after ALG

```
INVITE sip:*98@207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 75.142.151.49:1024;branch=z9hG4bK-7badf56d
From: "David Attias" <sip:525@207.252.1.148>;tag=f95367fa52060ce5o0
To: "Voice Mail" <sip:*98@207.252.1.148>
Call-ID: 9c8a315e-419d32d1@192.168.20.100
CSeq: 101 INVITE
Max-Forwards: 70
Contact: "David Attias" <sip:525@75.142.151.49:1024>
Expires: 240
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 397
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
Content-Type: application/sdp
```

SIP Headers

After ALG
modifies layer 7
data

```
v=0
o= 176664 176664 IN IP4 75.142.151.49
s=-
c=IN IP4 75.142.151.49
t=0 0
m=audio 19032 RTP/AVP 0 2 8 9 18 96 97 98 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtpmap:2 G726-32/8000
a=fmtp:101 0-15
a=ptime:30
a=sendrecv
```

SDP Body

When is SIP ALG necessary?

When is SIP ALG necessary?

When the SIP device behind NAT is NOT NAT aware

SIP devices that are not “NAT Aware”

- Some SIP devices are not NAT aware and write their (private) device IP in layer 7 messages to the server.
- The remote SIP server receives the layer 7 message which specifies a private reply address.
- The server sends replies to the private address, which can never be reached.

SIP servers that are not “NAT Aware”

The public server can receive data, but reply packets are dropped.

Example of a SIP device that is not NAT aware



Private / NAT

X100
192.168.20.100





Private / NAT

X100
192.168.20.100



SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032



SIP headers

Via: 192.168.20.100

Contact: 192.168.20.100

SDP Body

o = IN IP4 192.168.20.100

c = IN IP4 192.168.20.100

m = audio 19032



Private / NAT

X100
192.168.20.100





SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032

ALG IS required
here



Private / NAT

X100
192.168.20.100



With RouterOS SIP ALG enabled



WAN 75.142.151.49



Private / NAT

X100
192.168.20.100



SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032



SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032



WAN 75.142.151.49

ALG Enabled

Private / NAT

X100
192.168.20.100

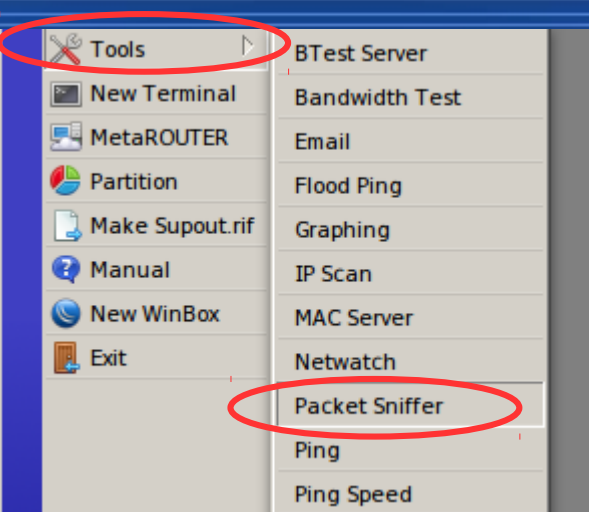


Is your SIP device NAT Aware?

- Packet capture in routerOS
 - Capture packets before and after they get modified by ALG
- Decode the capture files in Wireshark

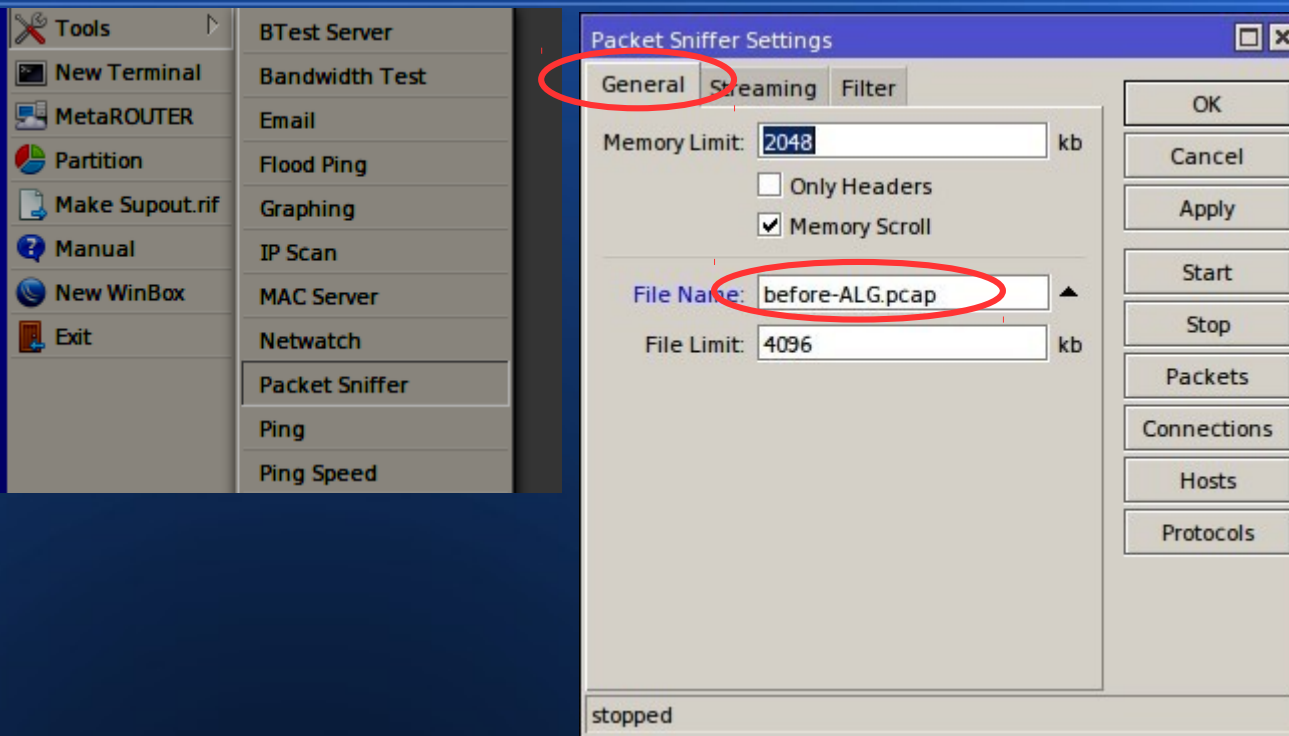
Setting up the packet capture

Before ALG modifications pcap



/tool sniffer

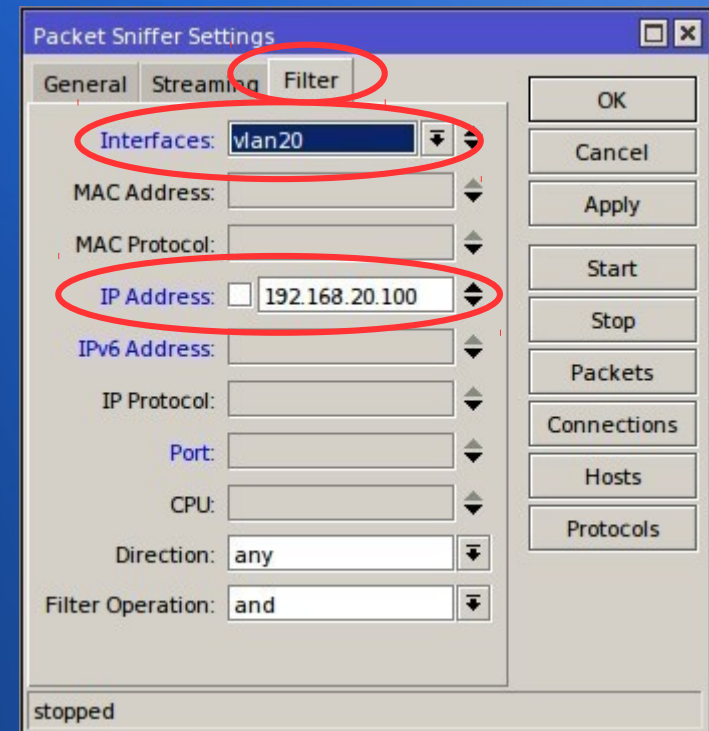
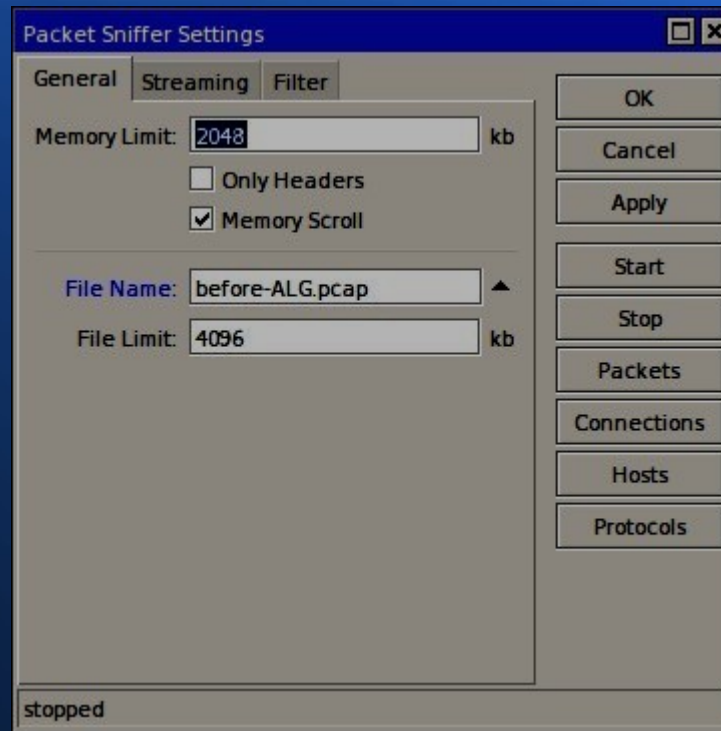
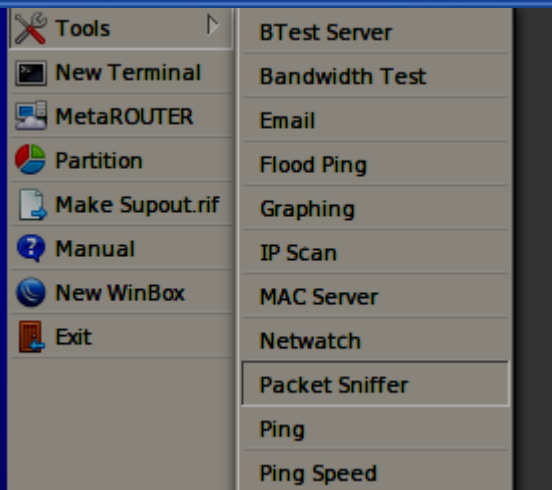
Before ALG modifications pcap



/tool sniffer

set only-headers=no file-name=before-ALG.pcap file-limit=4096

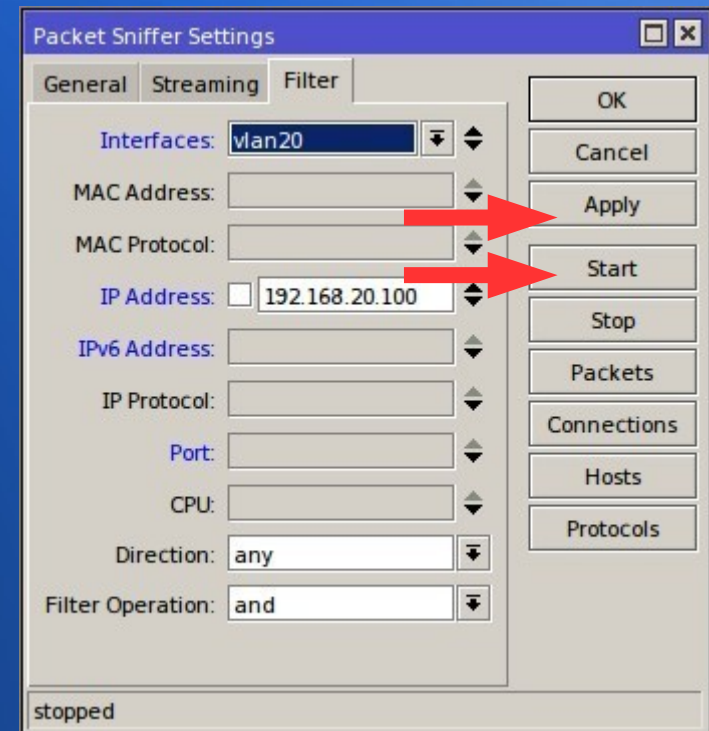
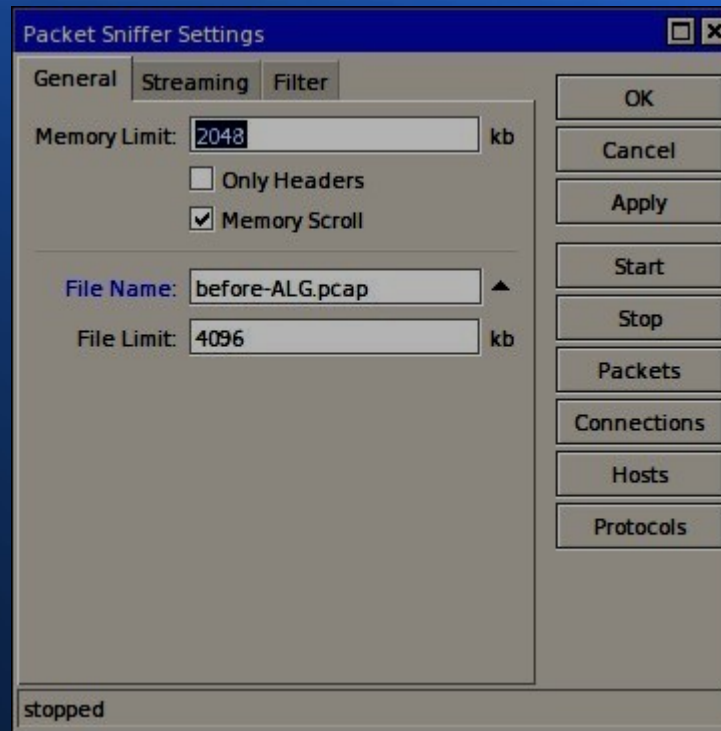
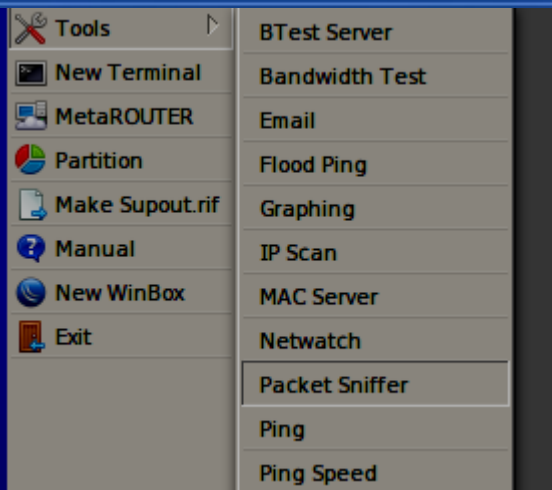
Before ALG modifications pcap



/tool sniffer

set only-headers=no file-name=before-ALG.pcap file-limit=4096 filter-interface=vlan20 filter-ip-address=192.168.20.100/32 filter-direction=any

Before ALG modifications pcap



```
/tool sniffer
```

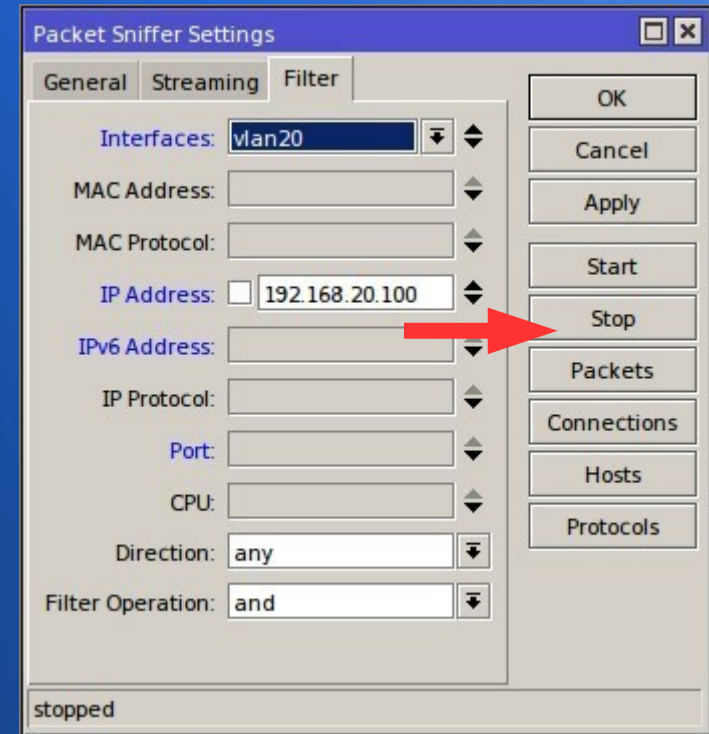
```
set only-headers=no file-name=before-ALG.pcap file-limit=4096 filter-interface=vlan20 filter-  
ip-address=192.168.20.100/32 filter-direction=any
```

```
start
```

Generate some traffic while the sniffer is capturing packets.

Before ALG modifications pcap

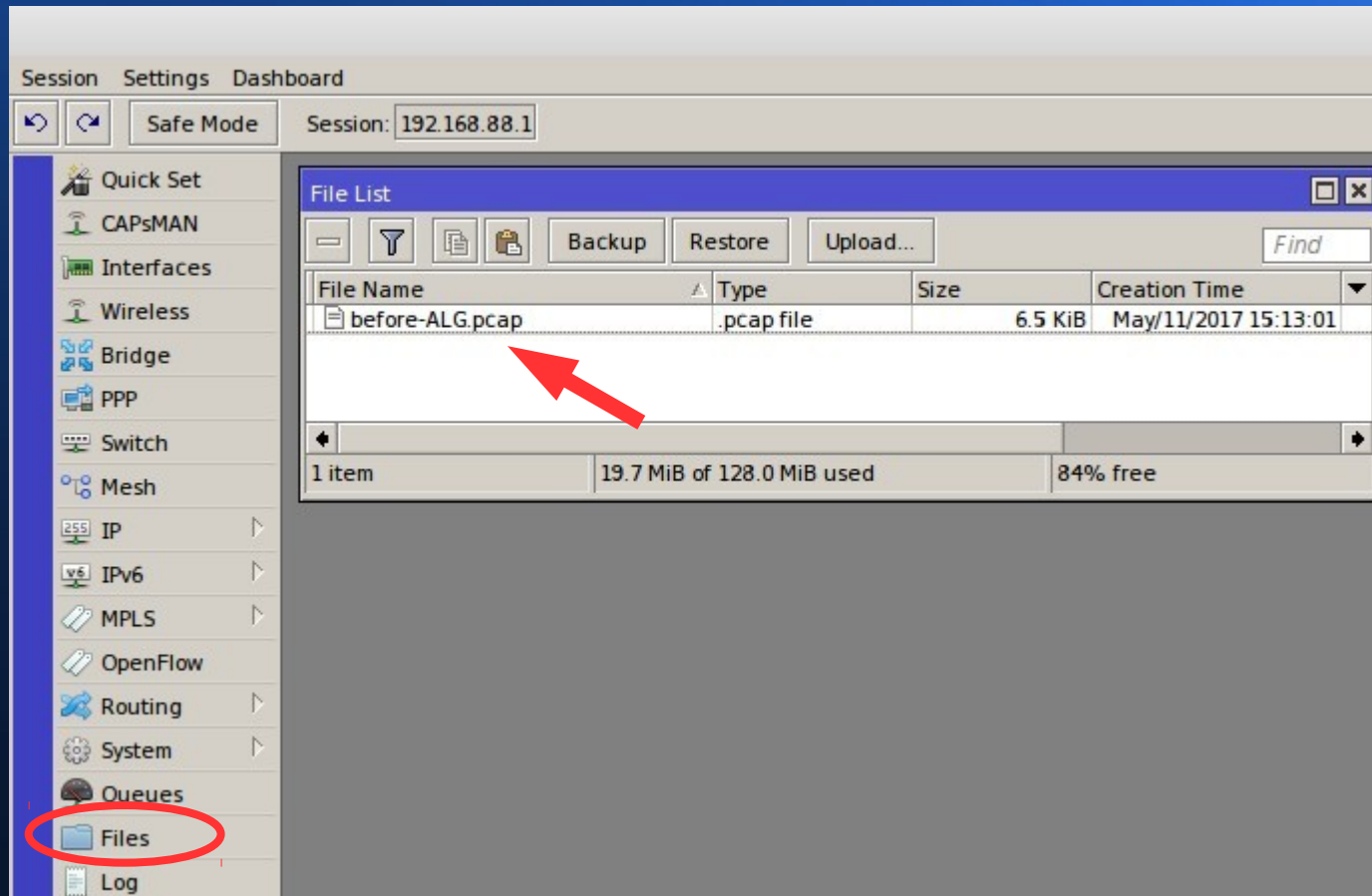
Make sure to stop the sniffer



```
/tool sniffer
```

```
stop
```

Download pcap files



Decode in wireshark

before-ALG.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.20.1	192.168.20.100	DHCP	357	DHCP Offer - Transaction ID 0xbed323ae
2	1.003062	192.168.20.1	192.168.20.100	DHCP	357	DHCP ACK - Transaction ID 0xbed323ae
3	1.688359	192.168.20.100	192.168.20.1	DNS	72	Standard query 0x0001 A pool.ntp.org
4	1.702269	192.168.20.1	192.168.20.100	DNS	136	Standard query response 0x0001 A pool.ntp.org A...
5	1.703640	192.168.20.100	208.75.89.4	NTP	90	NTP Version 3, client
6	1.706975	192.168.20.100	192.168.20.1	TFTP	93	Read Request, File: SEPECE1A9CDAA7D.cnf.xml, Tr...
7	1.707186	192.168.20.1	192.168.20.100	ICMP	121	Destination unreachable (Port unreachable)
8	1.708256	192.168.20.100	192.168.1.254	TCP	74	1024 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1456 W...
9	1.726550	208.75.89.4	192.168.20.100	NTP	90	NTP Version 3, server
10	2.061140	192.168.20.100	224.168.168.168	IGMPv2	56	Membership Report group 224.168.168.168
11	2.087226	192.168.20.100	207.252.1.148	SIP	524	Request: REGISTER sip:207.252.1.148 (1 binding...
12	2.088547	207.252.1.148	192.168.20.100	SIP	580	Status: 401 Unauthorized
13	2.293830	192.168.20.100	207.252.1.148	SIP	678	Request: REGISTER sip:207.252.1.148 (1 binding...
14	2.296420	207.252.1.148	192.168.20.100	SIP	601	Request: OPTIONS sip:100@192.168.20.100:5060
15	2.296603	207.252.1.148	192.168.20.100	SIP	599	Status: 200 OK (1 binding)
16	2.297538	207.252.1.148	192.168.20.100	SIP	605	Request: NOTIFY sip:100@192.168.20.100:5060
17	2.341624	192.168.20.100	207.252.1.148	SIP	460	Status: 200 OK
18	2.352654	192.168.20.100	207.252.1.148	SIP	367	Status: 200 OK
19	2.648746	192.168.20.100	224.168.168.168	IGMPv2	56	Membership Report group 224.168.168.168
20	5.308720	192.168.20.100	255.255.255.255	UDP	70	55656 → 55656 Len=28
21	6.708057	192.168.20.100	192.168.20.1	TFTP	93	Read Request, File: SEPECE1A9CDAA7D.cnf.xml, Tr...
22	6.708229	192.168.20.1	192.168.20.100	ICMP	121	Destination unreachable (Port unreachable)
23	7.348782	192.168.20.100	192.168.1.254	TCP	74	[TCP Retransmission] 1024 → 80 [SYN] Seq=0 Win=...

Frame 19: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
Ethernet II, Src: CiscoInc_cd:aa:7d (ec:e1:a9:cd:aa:7d), Dst: IPv4mcast_28:a8:a8 (01:00:5e:28:a8:a8)
Internet Protocol Version 4, Src: 192.168.20.100, Dst: 224.168.168.168
Internet Group Management Protocol

before-ALG Packets: 23 · Displayed: 23 (100.0%) · Load time: 0:0.0 Profile: Default

Decode in wireshark

The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file is 'before-ALG.pcap'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows a list of captured packets, with packet 18 selected and highlighted in orange. A red circle and arrow point to the 'sip' filter in the filter bar. The packet details pane on the right shows the decoded structure of packet 18, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Session Initiation Protocol (SIP).

No.	Time	Source	Destination	Protocol	Length	Info
11	2.087226	192.168.20.100	207.252.1.148	SIP	524	Request: REGISTER sip:207.252.1.148 (1 binding...
12	2.088547	207.252.1.148	192.168.20.100	SIP	580	Status: 401 Unauthorized
13	2.293830	192.168.20.100	207.252.1.148	SIP	678	Request: REGISTER sip:207.252.1.148 (1 binding...
14	2.296420	207.252.1.148	192.168.20.100	SIP	601	Request: OPTIONS sip:100@192.168.20.100:5060
15	2.296603	207.252.1.148	192.168.20.100	SIP	599	Status: 200 OK (1 binding)
16	2.297538	207.252.1.148	192.168.20.100	SIP	605	Request: NOTIFY sip:100@192.168.20.100:5060
17	2.341624	192.168.20.100	207.252.1.148	SIP	460	Status: 200 OK
18	2.352654	192.168.20.100	207.252.1.148	SIP	367	Status: 200 OK

Frame 18: 367 bytes on wire (2936 bits), 367 bytes captured (2936 bits)
▶ Ethernet II, Src: CiscoInc_cd:aa:7d (ec:e1:a9:cd:aa:7d), Dst: Routerbo_c3:62:47 (4c:5e:0c:c3:62:47)
▶ Internet Protocol Version 4, Src: 192.168.20.100, Dst: 207.252.1.148
▶ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)
▶ Session Initiation Protocol (200)

Session Initiation Protocol: Protocol Packets: 23 · Displayed: 8 (34.8%) · Load time: 0:0.3 · Profile: Default

Decode in wireshark

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets. Packet 11 is selected, and a context menu is open over it. The menu options include: Mark/Unmark Packet (Ctrl+M), Ignore/Unignore Packet (Ctrl+D), Set/Unset Time Reference (Ctrl+T), Time Shift... (Ctrl+Shift+T), Packet Comment..., Edit Resolved Name, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize Conversation, SCTP, Follow, Copy, Protocol Preferences, Decode As..., and Show Packet in New Window. The 'Follow' option is highlighted, and a submenu is open showing 'TCP Stream', 'UDP Stream', and 'SSL Stream'. The 'UDP Stream' option is highlighted. A red arrow points from the 'Follow' option to the 'UDP Stream' option. Another red arrow points from the 'UDP Stream' option to the packet details pane. The packet details pane shows the following information: Frame 11: 524 bytes on wire (4192 bits), 524 bytes captured on interface (4192 bits) on interface 0. Ethernet II, Src: CiscoInc_cd:aa:7d (ec:e1:a9:cd:aa:7d), Dst: 207.252.1.148. Internet Protocol Version 4, Src: 192.168.20.100, Dst: 207.252.1.148. User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060. Session Initiation Protocol (REGISTER).

No.	Time	Source	Destination	Protocol	Length	Info
11	2.087226	192.168.20.100	207.252.1.148	SIP	524	Request: REGISTER sip:207.252.1.148 (1 binding...)
12	2.088547	207.252.1.148	192.168.20.100			
13	2.293830	192.168.20.100	207.252.1.148			
14	2.296420	207.252.1.148	192.168.20.100			
15	2.296603	207.252.1.148	192.168.20.100			
16	2.297538	207.252.1.148	192.168.20.100			
17	2.341624	192.168.20.100	207.252.1.148			
18	2.352654	192.168.20.100	207.252.1.148			

Session Initiation Protocol: Protocol

Packets: 23 · Displayed: 8 (34.8%) · Load time: 0:0.3 · Profile: Default

Decode in wireshark

Wireshark · Follow UDP Stream (udp.stream eq 4) · before-ALG

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eefddbff
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-
eefddbff;received=207.252.1.145
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>;tag=as43d68f7c
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Server: FPBX-13.0.190.19(13.15.0)
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO,
PUBLISH, MESSAGE
Supported: replaces, timer
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="01a48834"
Content-Length: 0

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-e9fcb8df
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60160 REGISTER
Max-Forwards: 70
```

4 client pkt(s), 2 server pkt(s), 4 turns.

Entire conversation (14 kB)
207.252.1.148:5060 → 192.168.20.100:5060 (4428 bytes)
192.168.20.100:5060 → 207.252.1.148:5060 (9940 bytes)

Show data as ASCII Stream 4 Find Next

Help Hide this stream Print Save as... Close

Decode in wireshark

Wireshark - Follow UDP Stream (udp.stream eq 4) - before-ALG

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eefddbff
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-e9fcb8df
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60160 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="01a48834",uri="sip:207.252.1.148",algorithm=MD5,response="36cd61d13d1c58ed830cf64e3b47b82a"
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

4 client pkt(s), 0 server pkt(s), 0 turns.

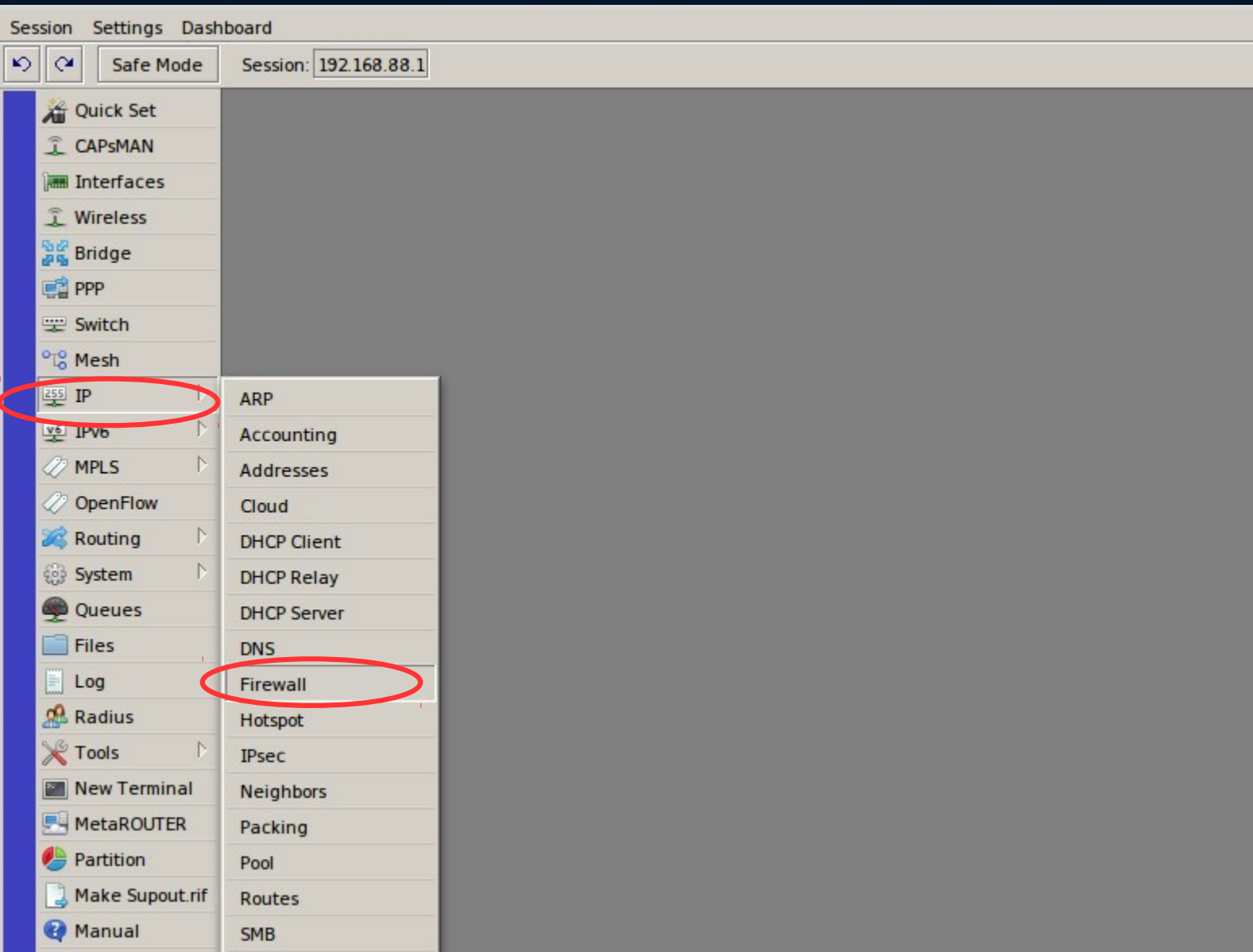
192.168.20.100:5060 → 207.252.1.148:5060 (9940 by ▼ Show data as ASCII ▼ Stream 4 ▼

Find: Find Next

Help Hide this stream Print Save as... Close

If your SIP device is not NAT Aware
Enable SIP ALG !

Enable SIP ALG



Enable SIP ALG

Session Settings Dashboard

Safe Mode Session: 192.168.88.1

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh

IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox

ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Add

Name	Ports	SIP Direct Media	SIP Timeout
• dccp			
• ftp	21		
• h323	6667		
• pptp			
• sctp			
• sip	5060	yes	01-00-10
• tftp	69		
• udplite			

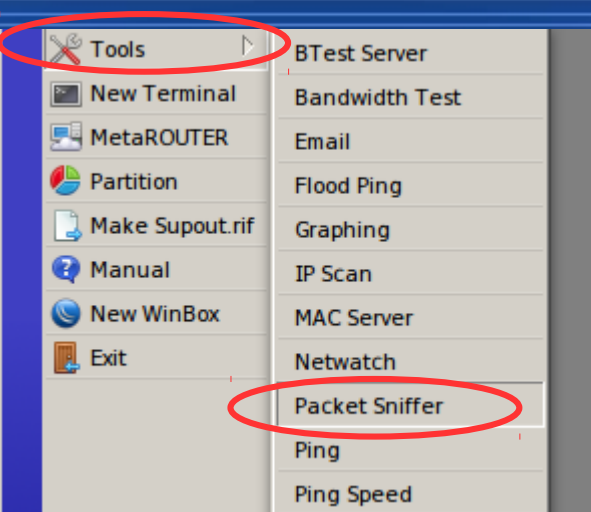
9 items (1 selected)

Show Categories
Detail Mode
Show Columns
Find Ctrl+F
Find Next Ctrl+G
Select All Ctrl+A
Enable Ctrl+E
Disable Ctrl+D

/ip firewall service-port
enable sip

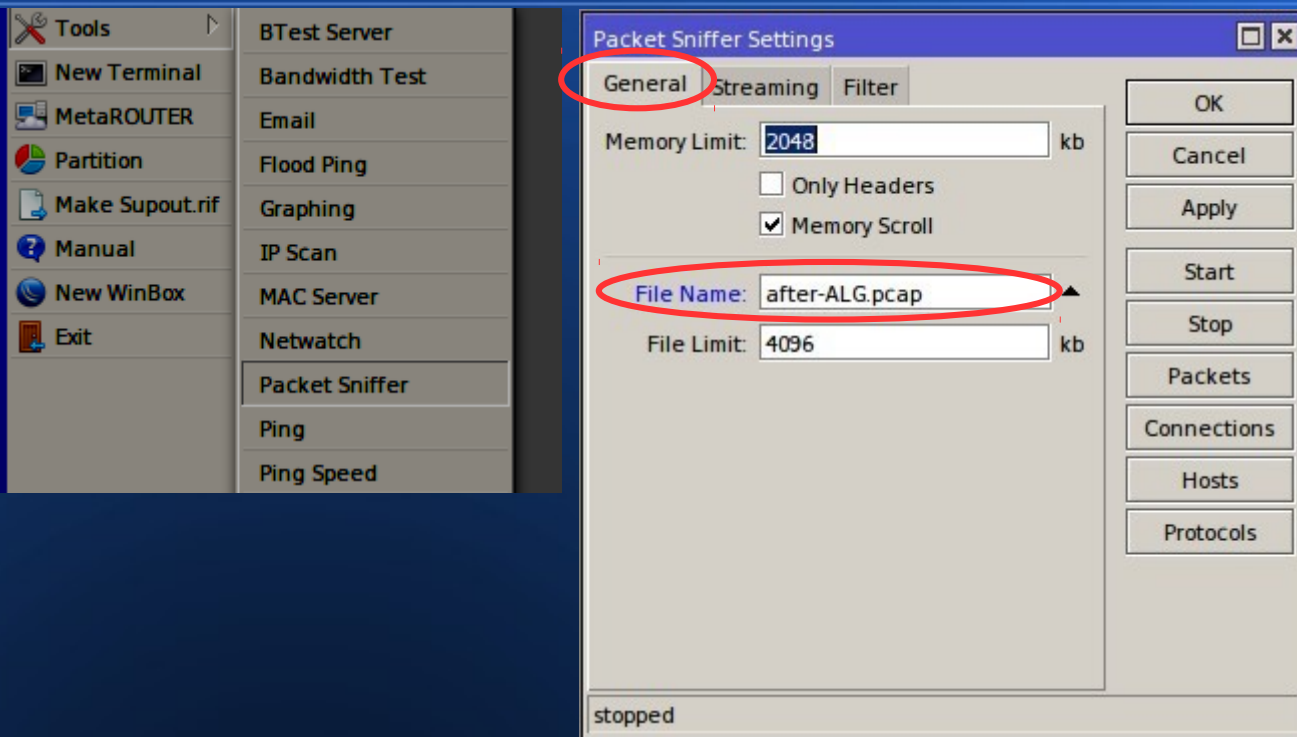
capture packets after ALG modification

After ALG modifications pcap



/tool sniffer

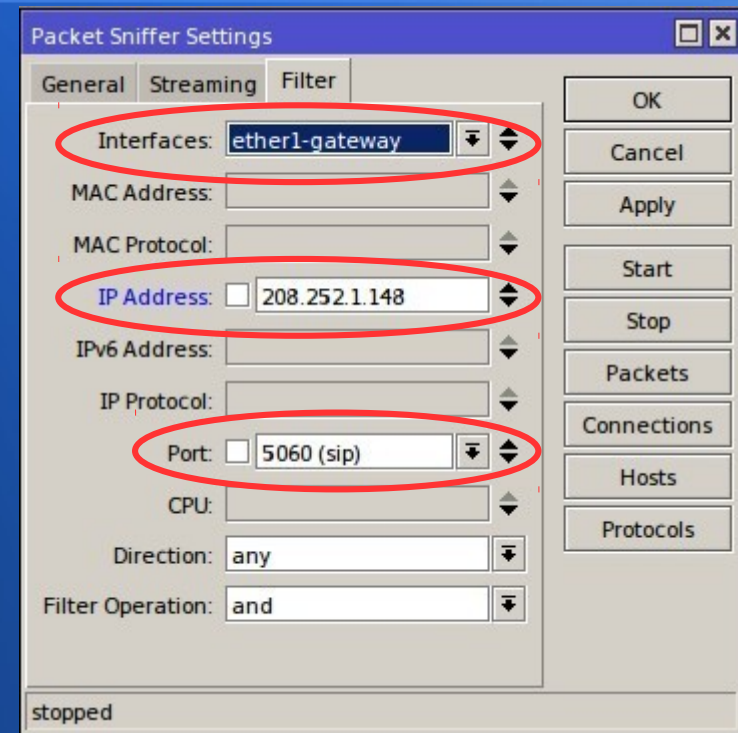
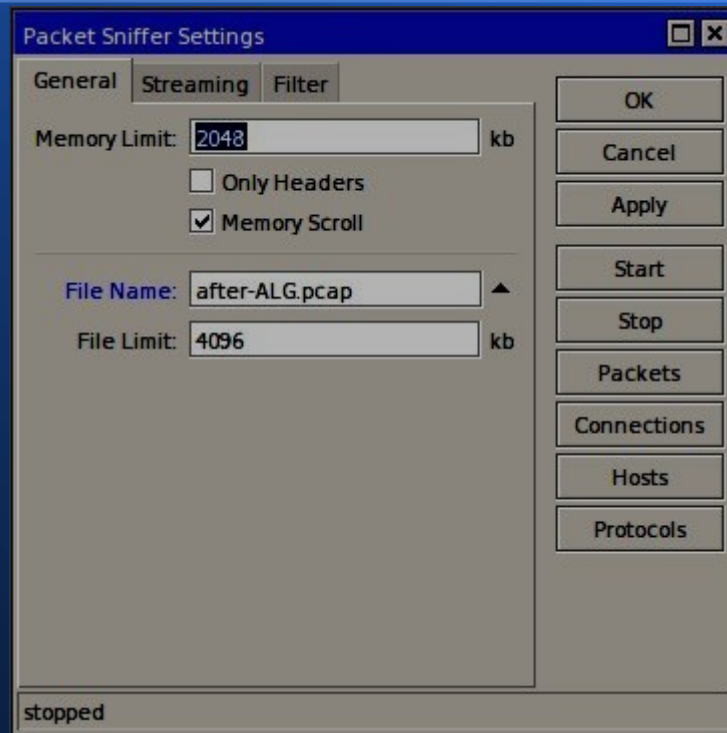
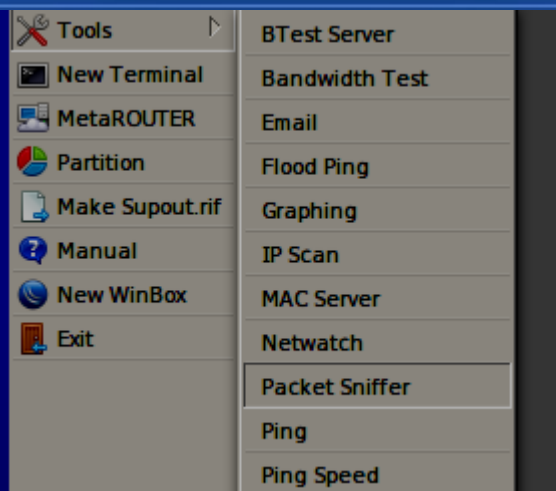
After ALG modifications pcap



/tool sniffer

set only-headers=no file-name=after-ALG.pcap file-limit=4096

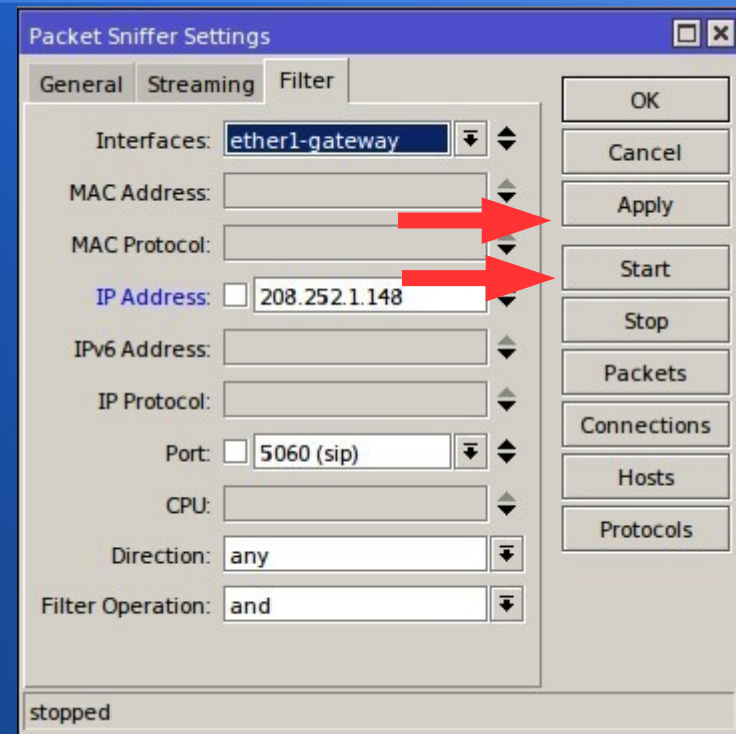
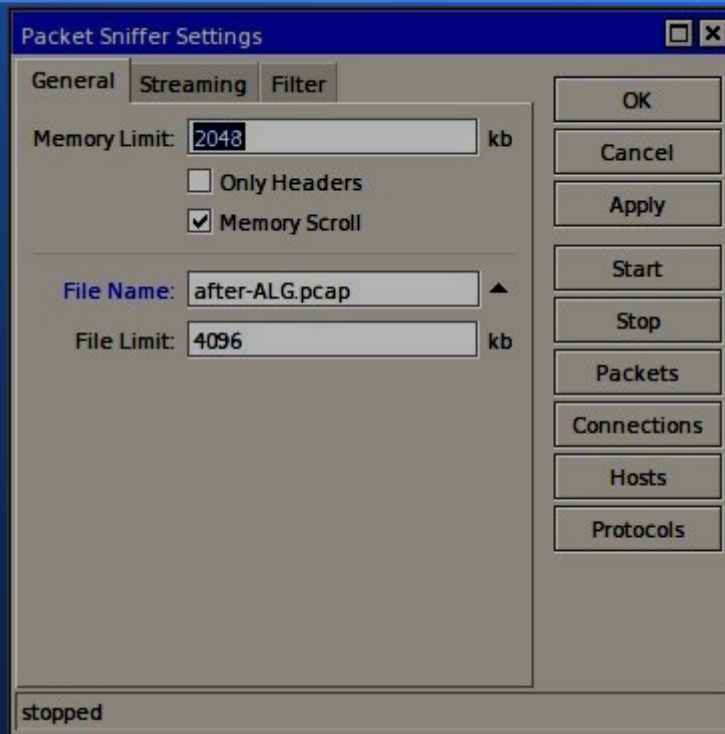
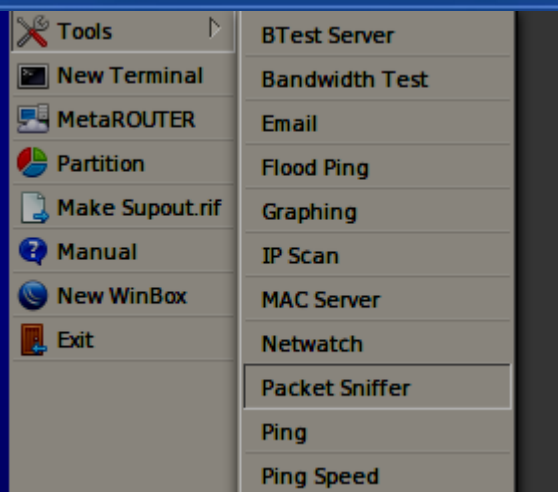
After ALG modifications pcap



/tool sniffer

set only-headers=no file-name=after-ALG.pcap file-limit=4096 filter-interface=ether1-gateway
filter-ip-address=207.252.1.148/32 filter-port=5060 filter-direction=any

After ALG modifications pcap



/tool sniffer

set only-headers=no file-name=after-ALG.pcap file-limit=4096 filter-interface=ether1-gateway
filter-ip-address=207.252.1.148/32 filter-port=5060 filter-direction=any

start

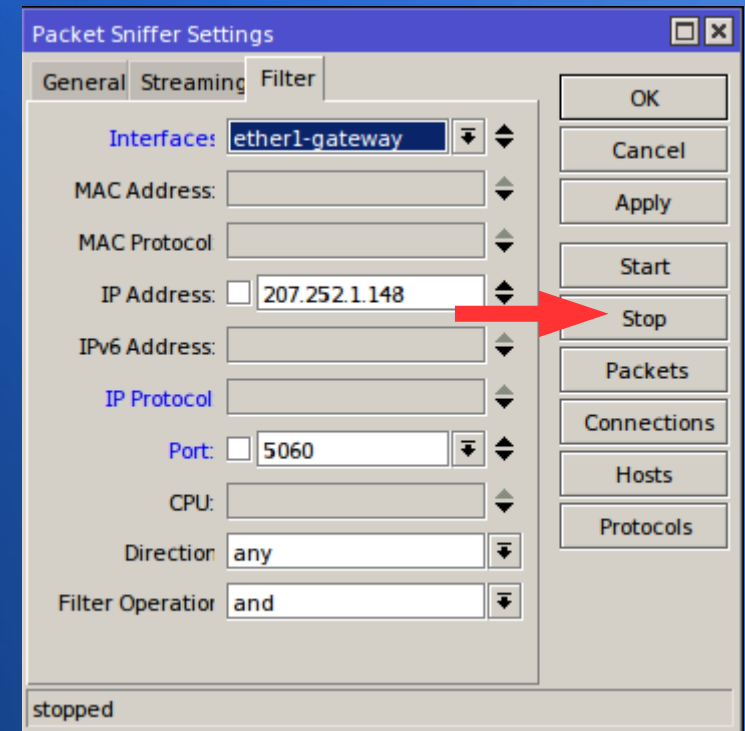
Generate some traffic while the sniffer is capturing packets.

After ALG modifications pcap

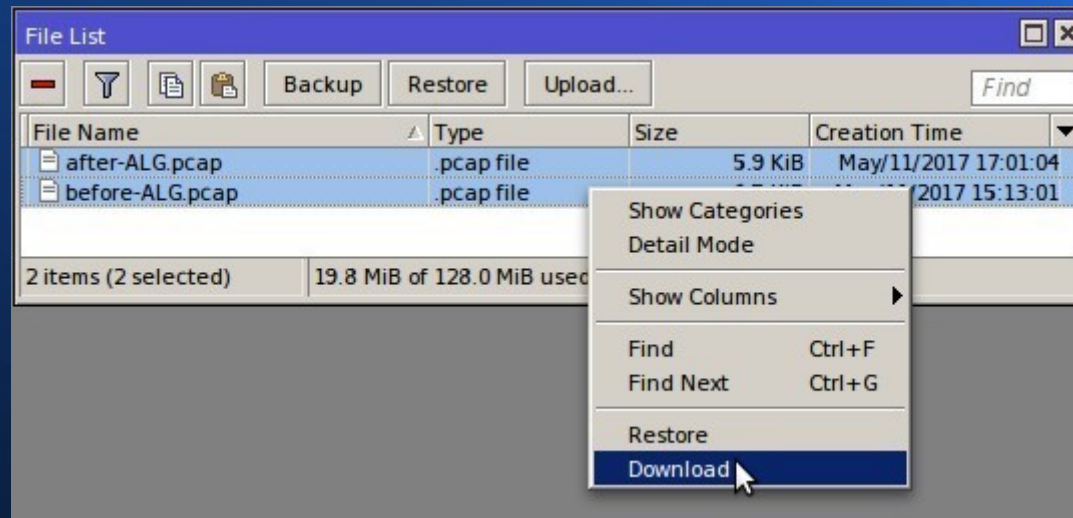
Make sure to stop the sniffer

```
/tool sniffer
```

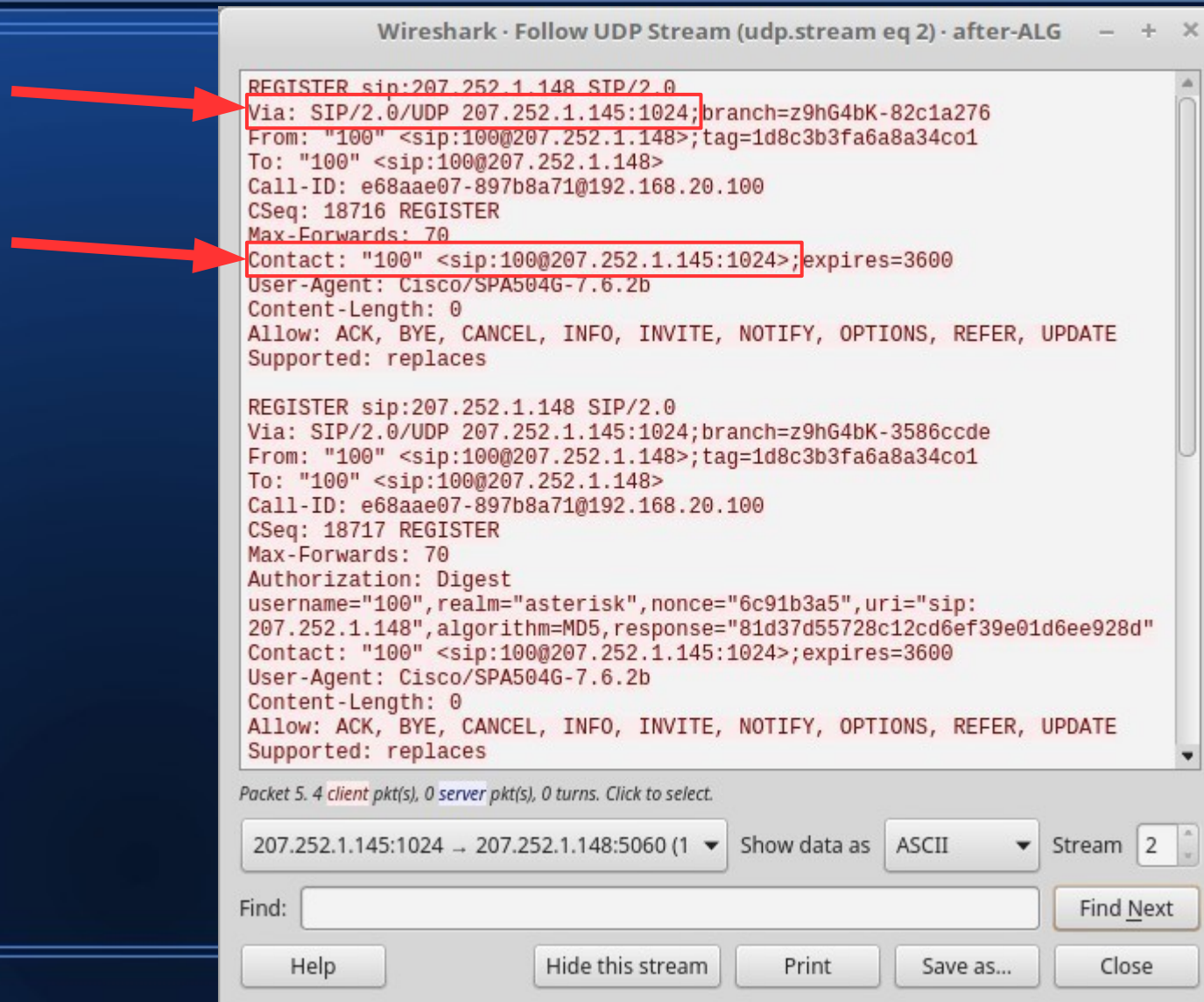
```
stop
```



Download pcap files



Decode in wireshark



Wireshark - Follow UDP Stream (udp.stream eq 2) - after-ALG

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-82c1a276
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae07-897b8a71@192.168.20.100
CSeq: 18716 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@207.252.1.145:1024>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-3586ccde
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae07-897b8a71@192.168.20.100
CSeq: 18717 REGISTER
Max-Forwards: 70
Authorization: Digest
username="100",realm="asterisk",nonce="6c91b3a5",uri="sip:
207.252.1.148",algorithm=MD5,response="81d37d55728c12cd6ef39e01d6ee928d"
Contact: "100" <sip:100@207.252.1.145:1024>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

Packet 5. 4 client pkt(s), 0 server pkt(s), 0 turns. Click to select.

207.252.1.145:1024 → 207.252.1.148:5060 (1) Show data as ASCII Stream 2

Find: Find Next

Help Hide this stream Print Save as... Close

ALG Enabled

Before modification & after modification

Wireshark · Follow UDP Stream (udp.stream eq 4) · before-ALG

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eefddbff
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-e9fcb8df
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60160 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="01a48834",
207.252.1.148",algorithm=MD5,response="36cd61d13d1c58ed830cf64e3b47b82a
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
```

4 client pkt(s), 0 server pkt(s), 0 turns.

192.168.20.100:5060 → 207.252.1.148:5060 (9940 by ▼

Show data as

ASCII ▼

Find:

Help

Hide this stream

Print

Save as...

Wireshark · Follow UDP Stream (udp.stream eq 2) · after-ALG

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-82c1a276
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae07-897b8a71@192.168.20.100
CSeq: 18716 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@207.252.1.145:1024>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-3586ccde
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae07-897b8a71@192.168.20.100
CSeq: 18717 REGISTER
Max-Forwards: 70
Authorization: Digest
username="100",realm="asterisk",nonce="6c91b3a5",uri="sip:
207.252.1.148",algorithm=MD5,response="81d37d55728c12cd6ef39e01d6ee928d
Contact: "100" <sip:100@207.252.1.145:1024>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
```

Packet 5. 4 client pkt(s), 0 server pkt(s), 0 turns. Click to select.

207.252.1.145:1024 → 207.252.1.148:5060 (1 ▼

Show data as

ASCII ▼

Stream

Find: Find N

Help

Hide this stream

Print

Save as...

Clos

When is SIP ALG unnecessary?

When is SIP ALG unnecessary?

When the SIP device is NAT aware.

1. Server is behind NAT
2. Server is outside NAT (public server)

When is SIP ALG unnecessary?

SIP servers behind NAT

- Nat aware SIP servers have the option to detect their WAN ip and write it in the SIP/SDP messages where necessary, before sending it.
- FreePBX detects the WAN ip and inserts it in SIP messages where necessary.

WAN
75.142.151.49



Private / NAT

Server
192.168.20.2



WAN
75.142.151.49



Private / NAT

Server
192.168.20.2



SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032

ALG Disabled

WAN
75.142.151.49



Private / NAT

Server
192.168.20.2



SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032

Servers outside NAT (public server)

Servers outside NAT (public server)

- SIP servers have NAT options for each extension

Servers outside NAT (public server)

- SIP servers have NAT options for each extension
- If server side extension states NAT=Yes then send all responses to the client originating IP and Port.

WAN
75.142.151.49

ALG Disabled



Private / NAT

WAN
75.142.151.49

ALG Disabled



Private / NAT

X100
192.168.20.100





WAN
75.142.151.49

ALG Disabled



Private / NAT

X100
192.168.20.100





WAN
75.142.151.49

ALG Disabled



Private / NAT

X100
192.168.20.100





Extension 100
NAT = Yes

WAN
75.142.151.49

ALG Disabled



Private / NAT

X100
192.168.20.100





Sip Server
207.252.1.148



WAN
75.142.151.49

ALG Disabled

Private / NAT

X100
192.168.20.100



SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032



Sip Server
207.252.1.148



WAN
75.142.151.49

ALG Disabled

Private / NAT

X100
192.168.20.100



SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032



SIP headers

Via: 192.168.20.100

Contact: 192.168.20.100

SDP Body

o = IN IP4 192.168.20.100

c = IN IP4 192.168.20.100

m = audio 19032

WAN
75.142.151.49



Private / NAT

X100
192.168.20.100





SIP headers

Via: ~~192.168.20.100~~

Contact: ~~192.168.20.100~~

SDP Body

o = IN IP4 ~~192.168.20.100~~

c = IN IP4 ~~192.168.20.100~~

m = audio ~~19032~~

WAN
75.142.151.49



Private / NAT

X100
192.168.20.100





SIP headers

Via: received=75.142.151.49

Contact: ~~192.168.20.100~~

SDP Body

o = IN IP4 ~~192.168.20.100~~

c = IN IP4 ~~192.168.20.100~~

m = audio ~~25481~~

WAN
75.142.151.49



Private / NAT

X100
192.168.20.100



When does ALG break VoIP?

When does ALG break VoIP?

- DOES NOT HAPPEN WITH Mikrotik RouterOS !
- Poor quality ALG's replace ALL private IP's in SIP headers, including Call-ID

When does ALG break VoIP?

REGISTER sip:207.252.1.148 SIP/2.0

Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-8fb0e171

From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06beo0

To: "David Attias" <sip:201525@207.252.1.148>

Call-ID: 6894e30c-h1c8d357@192.168.20.100

CSeq: 1373 REGISTER

Max-Forwards: 70

Contact: "David Attias" <sip:201525@192.168.20.100:5060>;expires=3600

User-Agent: Cisco/SPA504G-7.6.2b

Content-Length: 0

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE

Supported: replaces

When does ALG break VoIP?

REGISTER sip:207.252.1.148 SIP/2.0

Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-8fb0e171

From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06beo0

To: "David Attias" <sip:201525@207.252.1.148>

Call-ID: 6894e30c-h1c8d357@192.168.20.100

NEVER change
anything in this field !!!

CSeq: 1373 REGISTER

Max-Forwards: 70

Contact: "David Attias" <sip:201525@192.168.20.100:5060>;expires=3600

User-Agent: Cisco/SPA504G-7.6.2b

Content-Length: 0

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE

Supported: replaces

When does ALG break VoIP?

- DOES NOT HAPPEN WITH RouterOS !
- Poor quality ALG's replace ALL private IP's in SIP headers, including Call-ID
- Poor quality ALG's unnecessarily adds a ; which breaks the syntax of sip requests.

SIP ALG Timeout

The problem:

- The phone sets layer 7 session timeout on the server.
- The router sets the UDP timeout for the session.

SIP ALG Timeout

The problem:

- The phone sets layer 7 session timeout on the server.
- The router sets the UDP timeout for the session.
- If the router session timeout expires before the server session timeout, the server would send data to an expired session (closed return port)

SIP ALG Timeout

The Solution:

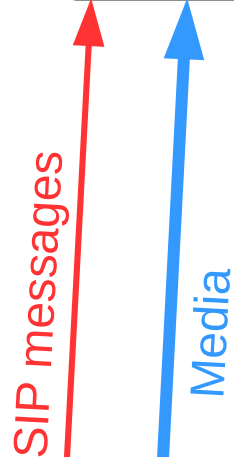
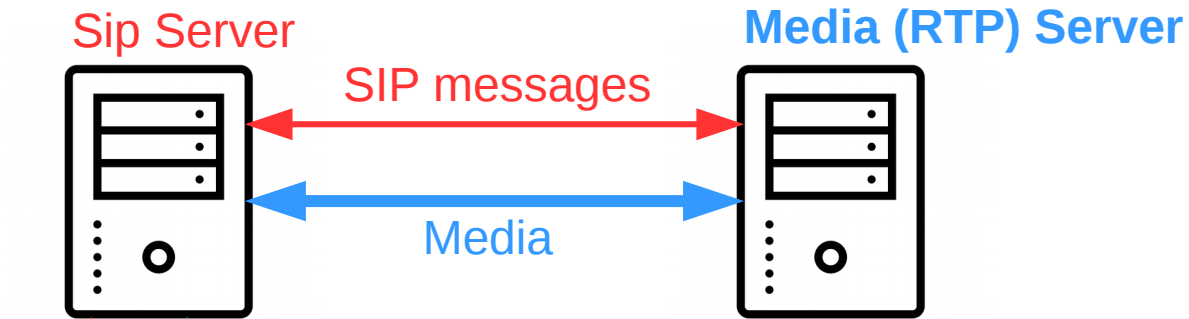
- Manually set SIP ALG timeout
- Set it higher than your lowest sip keepalive message interval (register, invite, options)

SIP Direct Media

SIP Direct Media

- Allows a redirect of the RTP media stream to go directly from SIP device to SIP device, “cutting out the middle man”
- The SIP servers are responsible for setting up the direct media stream.
- After the initial call is established the NAT’ed SIP server will re-invite the public media server to establish a direct media connection, bypassing the middle server

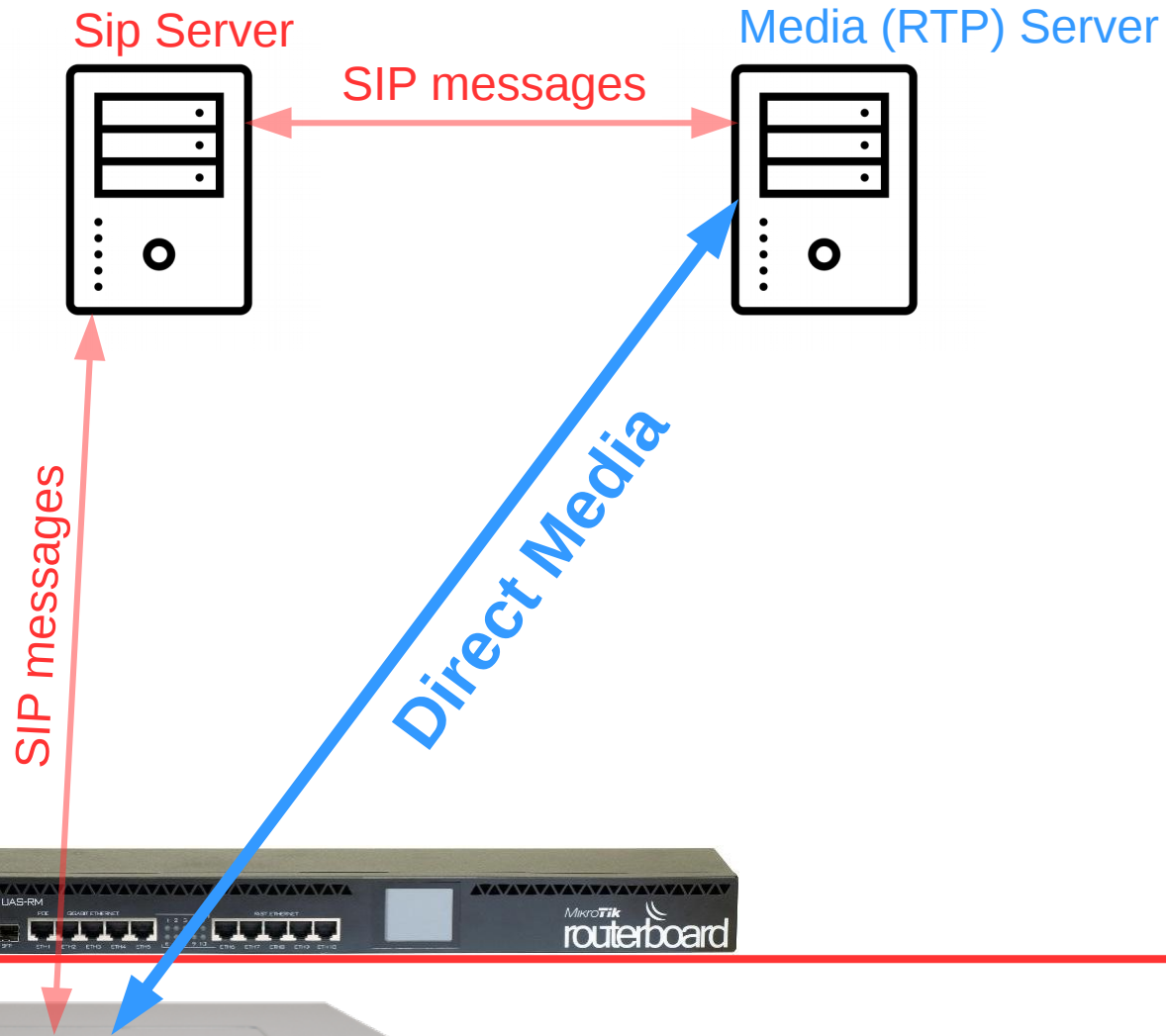
Standard Flow



Private / NAT



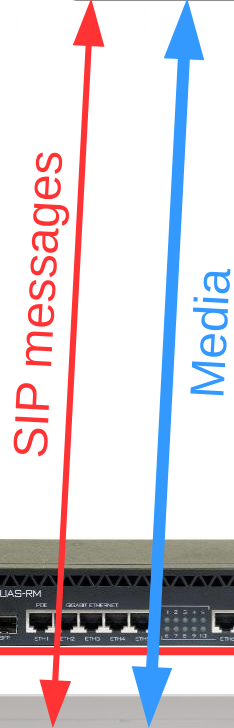
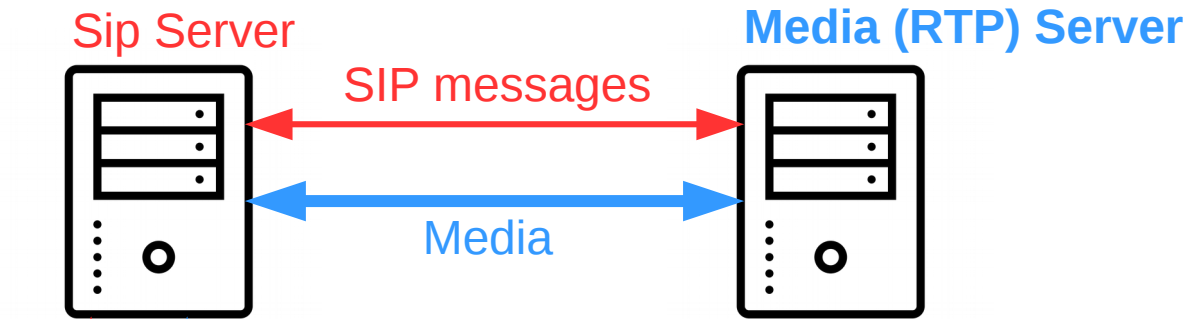
Direct-Media



SIP Direct Media

- The sip-direct-media option has the ability to block or allow the NAT'ed server from re-inviting the media server for a direct media session.
- sip-direct-media yes
Allows direct media re-invites
- sip-direct-media no
Blocks direct media re-invites

Standard Flow



Private / NAT



Re-cap

- 1- Use SIP ALG when your NAT'ed sip device is NOT NAT aware!
- 2- Make sure you set your SIP-Server ports correctly
- 3- Set your UDP timeout higher than your sip keep alive
- 4- Don't fear SIP ALG, it's designed to make your job easier !

Agenda

- 1- What is ALG & what does it do.
- 2- The problem with VoIP and NAT
- 3- When is SIP ALG necessary and unnecessary?
- 4- How SIP ALG corrects problems.
- 5- Testing with Wireshark
- 6- SIP ALG Timeout
- 7- SIP ALG direct-media