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 Gateway (firewall) that re-writes specific Application Layer 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 192.168.26.100 ALG MAS HERE 75.142.151.49

Basic terms

SIP and SDP

- SIP and SDP are VoIP Layer 7 protocols
- SIP <u>Session Initiated Protocol are commands</u> exchanged between sip devices (register, invite, trying, hold, xfer, bye)
- SDP <u>Session Description Protocol is</u> 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
Milcrotile 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?

Penny Tone LLC - www.pennytone.com

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> The fields ALG will change 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

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=191914b06bee0 To: "David Attias" <sip:525@207.252.1.148> After ALG Call-ID: 6894e30c-h1c8d357@192.168.20.100 The "respond to" CSeq: 1373 REGISTER IP and port 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

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@107.252.1.148>;tag=f95367fa52060ce5o0 To: "Voice Mail" <sip:*98@207.252.1.148> Call-ID: 9c8a315e-419d32d1@192.168.2c.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</sip:525@192.168.20.100:5060></sip:*98@207.252.1.148></sip:525@107.252.1.148>	SIP Headers
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE Supported: replaces Content-Type: application/sdp v=0 o= 176664 176664 IN IP4 192.168.20.100 s=-	Before ALG modifies layer 7 data
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@.07.252.1.148>;tag=f95367fa52060ce5o0 To: "Voice Mail" <sip:*98@207.252.1.148> Call-ID: 9c8a315e-419d32d1@192.168.2c.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</sip:525@75.142.151.49;1024></sip:*98@207.252.1.148></sip:525@.07.252.1.148>	SIP Headers
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER UPDATE Supported: replaces Content-Type: application/sdp v=0 o= 176664 176664 IN IP4 75.142.151.49 s=-	After ALG modifies layer 7 data
c=IN IP4 75.142.151.49 t=0 0 m=audio 19032 K rP/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

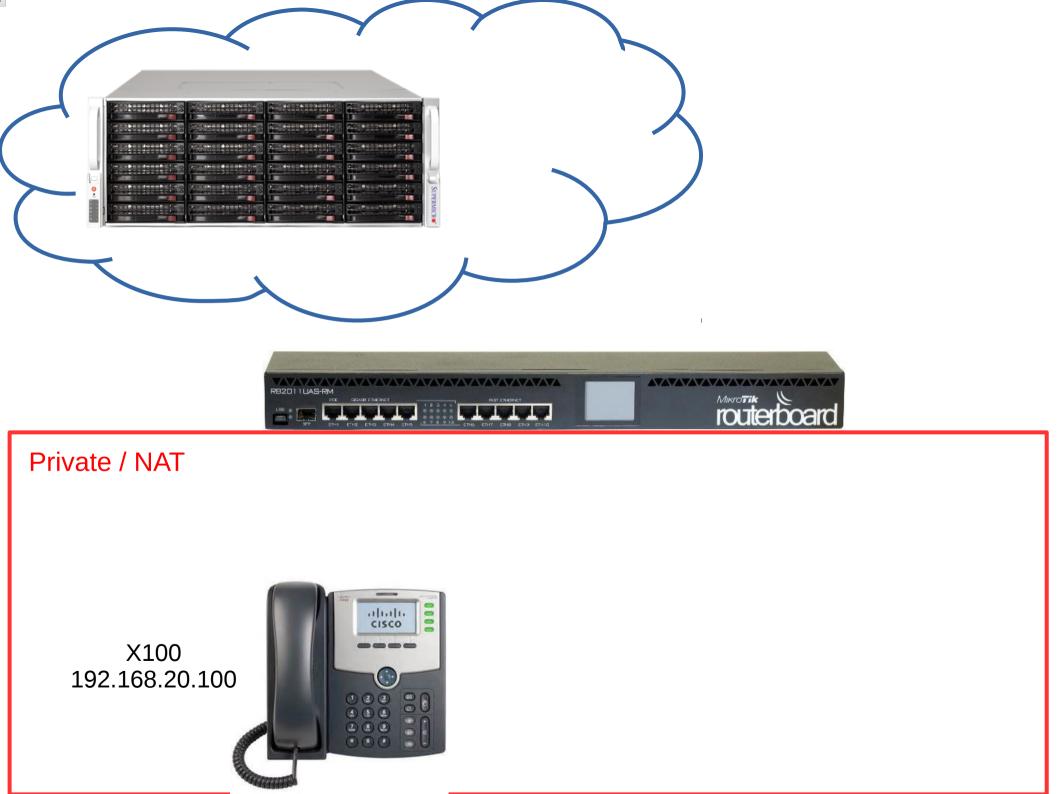
SIP devices that are not "NAT Aware"

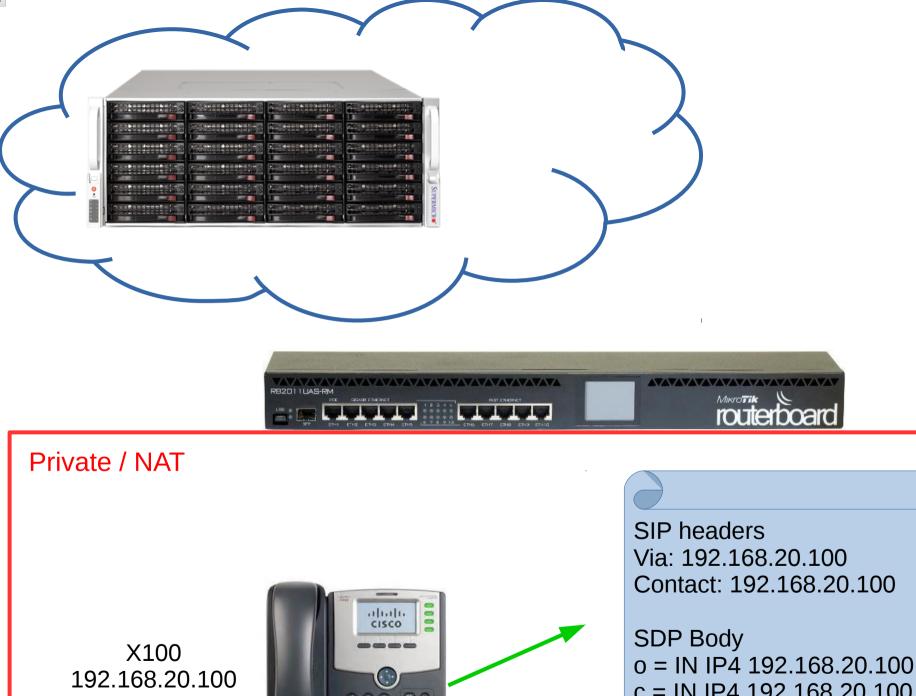
- Some SIP devices are not NAT aware and write their (private) device IP in layer 7 messages to the server.
- The <u>remote</u> SIP server receives the layer 7 message which specifies a private reply address.
- The server sends replies to the private address, which can never be reached.

SIP servers that are not "NAT Aware"

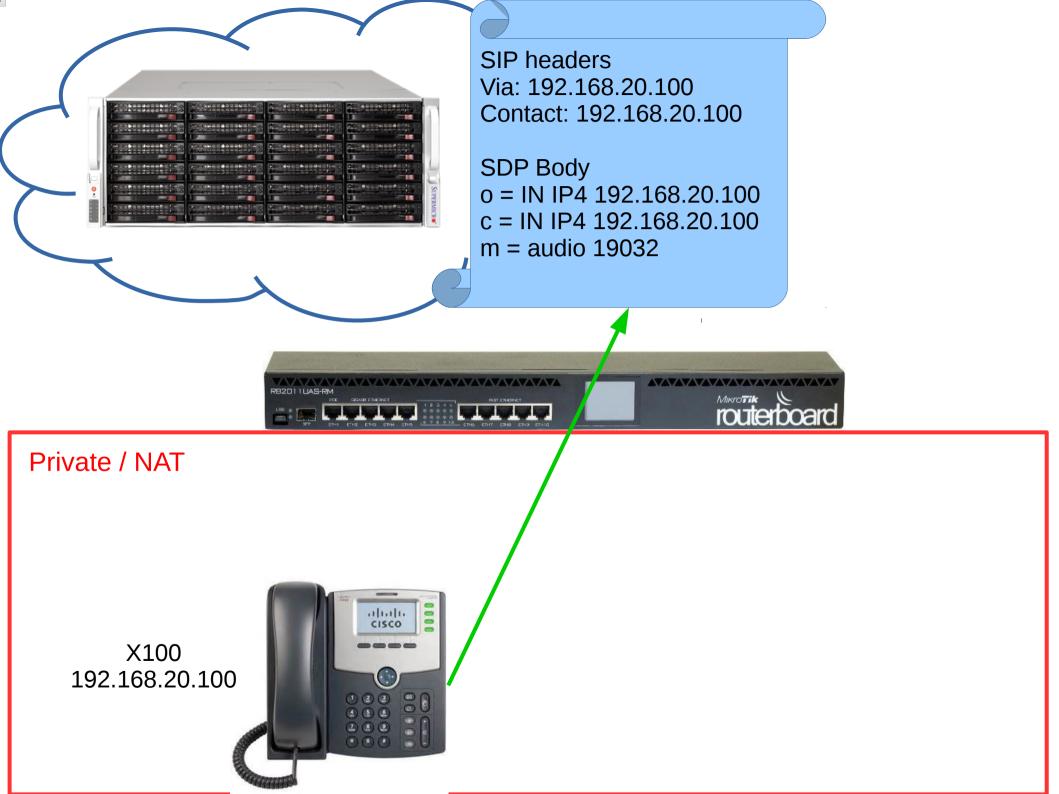
The public server can receive data, but reply packets are dropped.

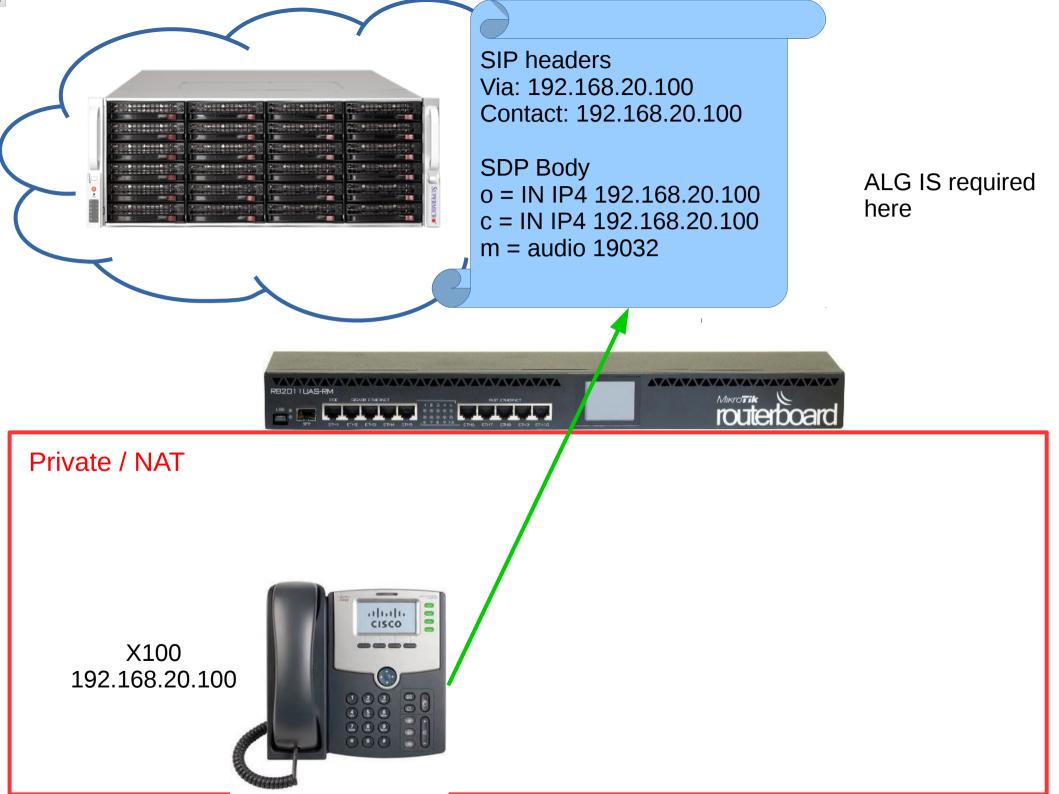
Example of a SIP device that is not NAT aware



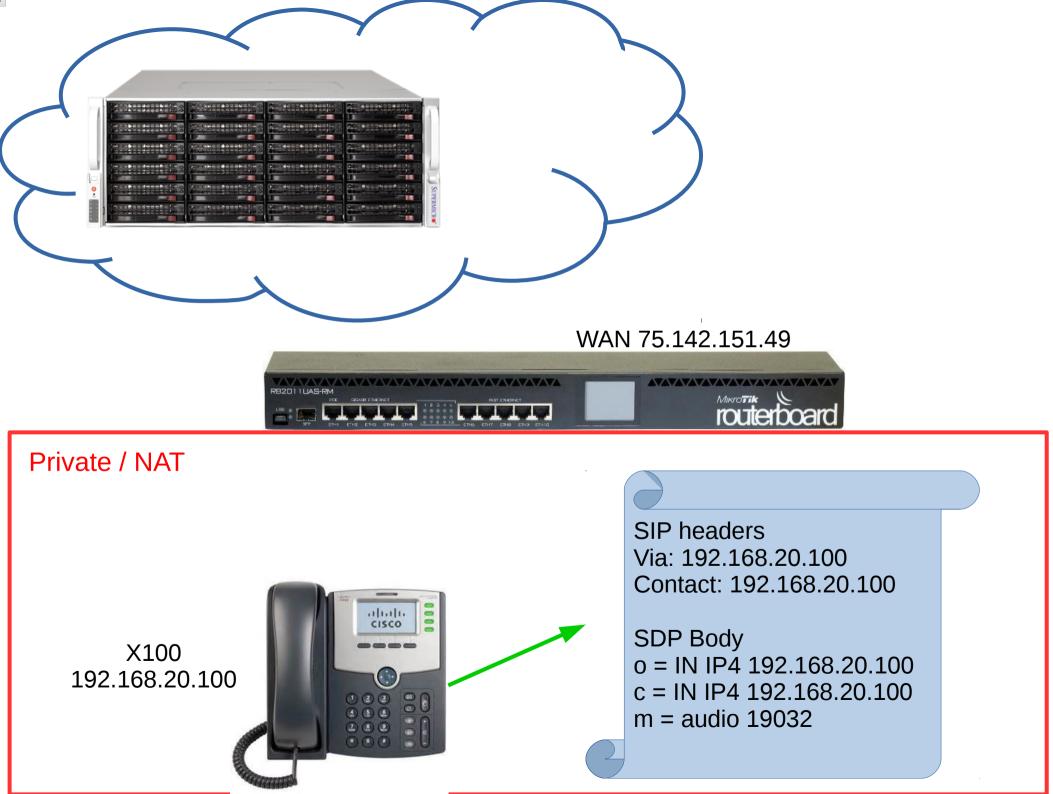


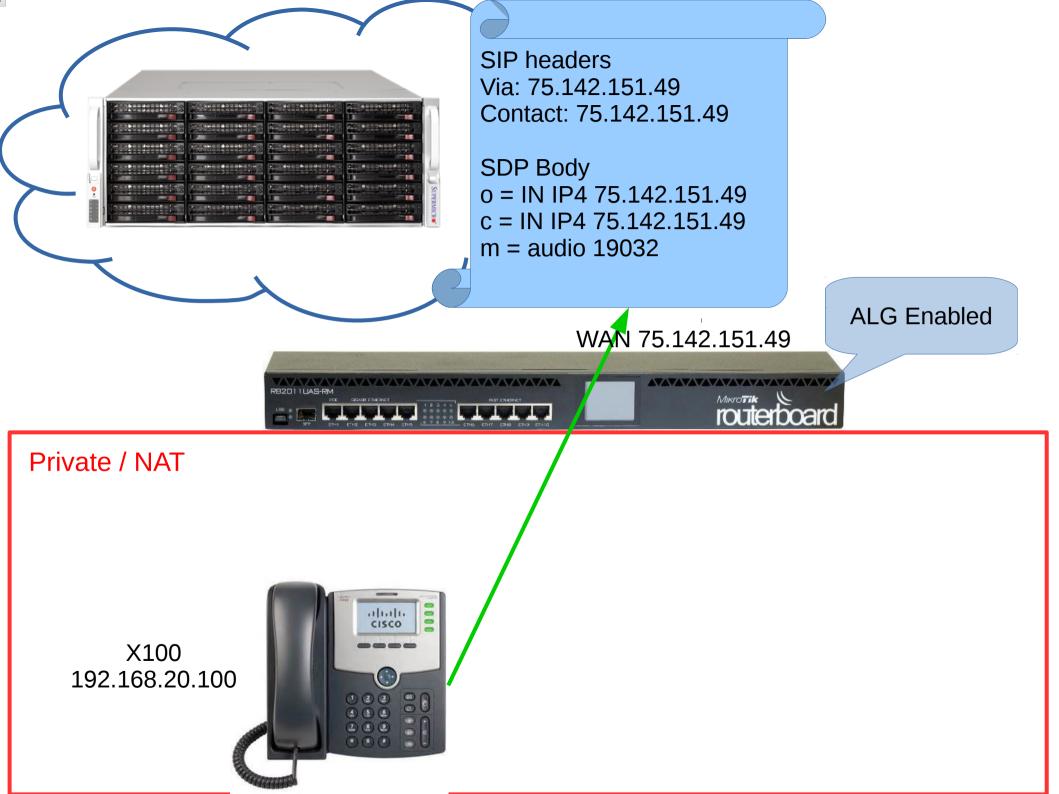
o = IN IP4 192.168.20.100 c = IN IP4 192.168.20.100m = audio 19032





With RouterOS SIP ALG enabled





Is your SIP device NAT Aware?

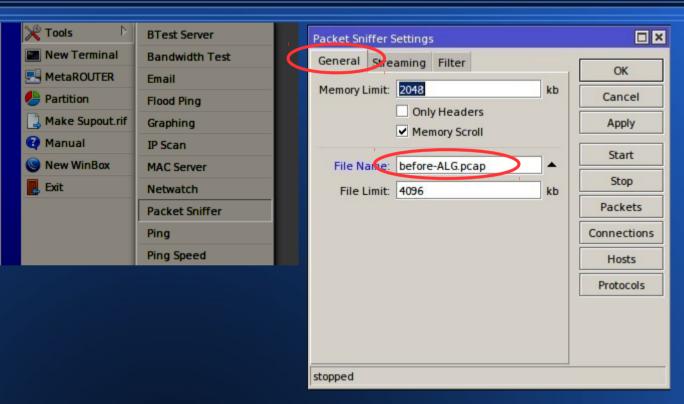
Packet capture in routerOS

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

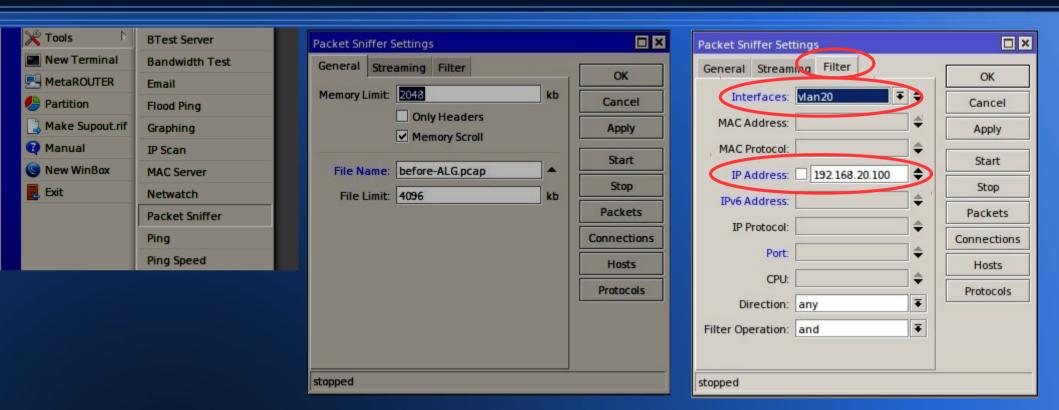
Setting up the packet capture



/tool sniffer



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



/tool sniffer

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

Tools New Terminal HetaROUTER Partition Make Supout.rif	BTest Server Bandwidth Test Email Flood Ping Graphing	Packet Sniffer Settings General Streaming Filter Memory Limit: 2048 Only Headers Memory Scroll	OK Cancel Apply	Packet Sniffer Settings General Streaming Filter Interfaces: Man20 MAC Address: ♀	OK Cancel Apply
 Manual New WinBox Exit 	IP Scan MAC Server Netwatch Packet Sniffer Ping Ping Speed	File Name: before-ALG.pcap	Start Stop Packets Connections Hosts	MAC Protocol:	Start Stop Packets Connections Hosts
		stopped	Protocols	CPU: Direction: any Filter Operation: and stopped	Protocols

/tool sniffer

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

start

Generate some traffic while the sniffer is capturing packets.

Make sure to stop the sniffer

Packet Sniffer Settings General Streaming Filter OK ∓ ♠ Interfaces: vlan20 Cancel MAC Address: Apply MAC Protocol: Start 192,168,20,100 \$ IP Address: Stop IPv6 Address: Packets IP Protocol: Connections Port: Hosts CPU ÷ Protocols Ŧ Direction: any Ŧ Filter Operation: and stopped

/tool sniffer

stop

Penny Tone LLC - www.pennytone.com

Download pcap files

Se	ssion Settings Das	hboard			
5	Safe Mode	Session: 192.168.88.1			
	🔏 Quick Set	File List			
			Backup Restore Upload		Find
	Interfaces	File Name	∆ Type	Size	Creation Time
	🔔 Wireless	🖹 before-ALG.pcap	.pcap file	6.5 K	iB May/11/2017 15:13:01
	Bridge				
	📑 PPP				
	🛫 Switch	•			•
	^o tesh	1 item	19.7 MiB of 128.0 MiB used	8	34% free
	255 IP 🗅				
	👳 IPv6 🗈				
	🖉 MPLS 🛛 🗅				
	OpenFlow				
	😹 Routing 💦 🖹				
	🚱 System 🗅				
	Cueues				
	Files				
	E Log				

	before-ALG.pcap – + >								
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze <u>S</u>	atatistics Telephony <u>W</u>	ireless <u>T</u> ool	s <u>H</u> elp				
		🗎 🖹 🚺	۹ 🔶 😫						
Ар	Apply a display filter <ctrl-></ctrl-> Expression +								
No.	Time	Source	Destination	Protocol Ler	ngtł Info				
-	1 0.000000	192.168.20.1	192.168.20.100	DHCP 3	357 DHCP Offer - Transaction ID 0xbed323ae				
	2 1.003062	192.168.20.1	192.168.20.100	DHCP 3	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 1	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 1	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		524 Request: REGISTER sip:207.252.1.148 (1 binding				
	12 2.088547	207.252.1.148	192.168.20.100		580 Status: 401 Unauthorized				
	13 2.293830	192.168.20.100	207.252.1.148		578 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		599 Status: 200 OK (1 binding)				
	16 2.297538	207.252.1.148	192.168.20.100		605 Request: NOTIFY sip:100@192.168.20.100:5060				
	17 2.341624	192.168.20.100	207.252.1.148	SIP 4	460 Status: 200 OK				
	18 2.352654	192.168.20.100	207.252.1.148	SIP 3	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 1	121 Destination unreachable (Port unreachable)				
	23 7.348782	192.168.20.100	192.168.1.254	TCP	74 [TCP Retransmission] 1024 \rightarrow 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-A	ALG.pcap								_	+ ×)
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyz	ze <u>S</u> t	tatistics	Teleph	ion <u>y W</u>	ireless	<u>T</u> ools	<u>H</u> elp							
			۲		×	0	٩	Image: A marked and a marked		A	Ł 💽		÷	Θ	€,				
I sip	,														Đ	< →	- Expr	ession	+
	11 2 12 2 13 2 14 2	Fime 2.087226 2.088547 2.293830 2.296420 2.296603	7 9 9	Source 192.168 207.252 192.168 207.252 207.252	.1.148 .20.100 .1.148		192.16 207.25 192.16	tion 2.1.148 8.20.100 2.1.148 8.20.100 8.20.100	9	Protocol SIP SIP SIP SIP SIP	524 580 678 601	Info Request Status: Request Request Status:	401 Ur : REGIS : OPTIC	nautho STER s DNS si	rized ip:20 p:100	 7.252. @192.1	1.148	(1 bi	nding
	17 2	2.297538 2.341624 2.352654	4	207.252 192.168 192.168	.20.100		207.25	8.20.100 2.1.148 2.1.148		SIP SIP SIP	460	Request Status: Status:	200 Ok	< L	:1000	192.10	8.20.1	.00:506	
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)																			

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

Profile: Default

Session Initiation Protocol: Protocol

1

	before-ALG.pcap – + ×									
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	<u>S</u> tatistics Telephony <u>V</u>	<u>V</u> ireless <u>T</u> ools <u>H</u> elp						
📕 sip	sip Expression +									
No.	Time	Source	Destination 207.252.1.148	Protocol Lengtl Info SIP 524 Request: REC	GISTER sin'207	252.1.148 (1 binding…				
	12 2.088547 13 2.293830 14 2.296420 15 2.296603 16 2.297538 17 2.341624	207.252.1.148 192.168.20.100 207.252.1.148 207.252.1.148 207.252.1.148 192.168.20.100	192.168.20.100 207.252.1.148 192.168.20.100 192.168.20.100 192.168.20.100 207.252.1.148	<u>M</u> ark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift	Ctrl+M	252.1.148 (1 binding…)2.168.20.100:5060 2.168.20.100:5060				
	18 2.352654	192.168.20.100	207.252.1.148	Packet Comment Edit Resolved Name Apply as Filter Prepare a Filter Conversation Filter Colorize Conversation SCTP	4					
 Et In Us 	hernet II, Src: C ternet Protocol V er Datagram Proto	iscoInc_cd:aa:7d (e ersion 4, Src: 192.), 524 bytes captured c:e1:a9:cd:aa:7d), Ds 168.20.100, Dst: 207. (5060), Dst Port: 50	Follow Copy Protocol Preferences Decode <u>A</u> s Show Packet in New <u>W</u> indow	•	TCP Stream UDP Stream SSL Stream				
0 7	Session Initiation	Protocol: Protocol		Packets: 23 · Displayed: 8 (3	34.8%) · Load time:	0:0.3 Profile: Default				

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:1000207.252.1.148>;tag=36d71bb091995583o1 To: "100" <sip:1000207.252.1.148> 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=z9hG4bKeefddbff;received=207.252.1.145 From: "100" <sip:100@207.252.1.148>;tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>;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:1000207.252.1.148> Call-ID: 6593bf0b-e1cc0d64@192.168.20.100 CSeq: 60160 REGISTER May Forwards, 70 4 client pkt(s), 2 server pkt(s), 4 turns.

 Entire conversation (14 kB)
 Show data as
 ASCII
 ✓
 Stream
 4

 207.252.1.148:5060 → 192.168.20.100:5060 (4428 bytes)
 Find Next
 Find Next

 192.168.20.100:5060 → 207.252.1.148:5060 (9940 bytes)
 Find Next
 Close

 Help
 Hide this stream
 Print
 Save as...
 Close

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;tranch=z9hG4bK-eefddbff From: "100" <sip:100@207.252.1.148>;tag=36d71bb09199558301 To: "100" <sip:100@207.252.1.148> Call-ID: 6593bf0b-e1cc0d64@192.168.20.100 CSeq: 60159 REGISTER Max-Forwards: 70</sip:100@207.252.1.148></sip:100@207.252.1.148>
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600 User-Agent: C1sco/SPA504G-7.6.2b Content-Length: 0 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE Supported: replaces</sip:100@192.168.20.100:5060>
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=36d71bb09199558301 To: "100" <sip:100@207.252.1.148> Call-ID: 6593bf0b-e1cc0d64@192.168.20.100 CSeq: 60160 REGISTER</sip:100@207.252.1.148></sip:100@207.252.1.148>
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</sip:100@192.168.20.100:5060>
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

Session Settings Dash	board	
Safe Mode	Session: 192.168.88.1	
Quick Set		
CAPSMAN		
Interfaces		
Wireless		
월월 Bridge		
PPP		
🙄 Switch		
°t¦8 Mesh		
턛 IP	ARP	
몇 IPV6 卜	Accounting	
🖉 MPLS 🛛 🗅	Addresses	
OpenFlow	Cloud	
🌌 Routing 🛛 🗅	DHCP Client	
錄 System 🗅	DHCP Relay	
Queues	DHCP Server	
Files	DNS	
📃 Log 🤇	Firewall	
A Radius	Hotspot	
🄀 Tools 🔹 🗅	IPsec	
New Terminal	Neighbors	
MetaROUTER	Packing	
🥭 Partition	Pool	
Aake Supout.rif	Routes	
😭 Manual	SMB	

Enable SIP ALG

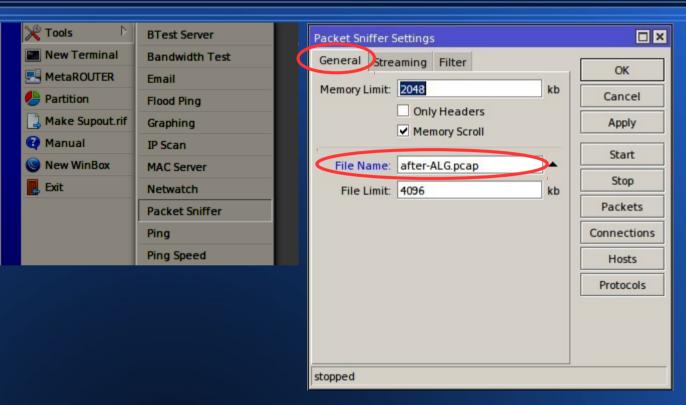
Session Settings Dash	board							
Safe Mode	Session: 192.168.88.1							
🔏 Quick Set								
CAPSMAN								
Interfaces								
2 Wireless		Firewall						
월문 Bridge		Filter Rules	NAT	Mangle	Raw Se	rvice Ports	Connections	Addr
PPP		X	-	-				al processors
🙄 Switch			Ports	SID Dire	ct Media	SIP Timeo	+	_
್ದಿ Mesh		Name A o dccp	Ports	SIP DIre	et meula	SIP TIMEO	ut	
≝ IP ♪	ARP	● ftp	21					
👳 IPv6 🗈	Accounting	 h323 irc 	6667					
Ø MPLS	Addresses	pptp						
OpenFlow	Cloud	 e sctp ⇒ sip 	5060	ves		01.00.1	10	
😹 Routing	DHCP Client	♦ tftp	69	1	10000	v Categorie	s	
⊕ System ▷	DHCP Relay	• udplite			Deta	il Mode		_
Queues	DHCP Server	9 items (1 sele	cted)		Show	v Columns	→∟	
Files	DNS				Find		Ctrl+F	
Log	Firewall				Find	Next	Ctrl+G	
A Radius	Hotspot				Sele	ci Ali	CLILA	
💥 Tools 🔹 🗅	IPsec				Enat	A	Ctrl+E	
New Terminal	Neighbors				Disa	ble	Ctri+D	I.
MetaROUTER	Packing							
Partition	Pool							
Make Supout.rif	Routes							
Manual	SMB							_
S New WinBox)I
S New WINDOX	SNMP							

/ip firewall service-port enable sip

capture packets after ALG modification



/tool sniffer



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

Image: Constraint of the second se	BTest Server Bandwidth Test Email Flood Ping Graphing IP Scan MAC Server	Packet Sniffer Settings General Streaming Filter Memory Limit: 2048 Only Headers Image: Memory Scroll File Name: after-ALG.pcap	OK Cancel Apply Start Stop	Packet Sniffer Settings General Streaming Filter Interfaces: ether1-gateway MAC Address: MAC Protocol: IP Address: 208.252.1.148	OK Cancel Apply Start Stop
		File Name: after-ALG.pcap ▲ File Limit: 4096 kb	Start Stop Packets Connections Hosts Protocols	IP Address: IPv6 Address: IP Protocol: Port: 5060 (sip) \$ CPU: Direction: any Filter Operation:	Start Stop Packets Connections Hosts Protocols
		stopped		stopped	

/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

🗶 Tools 🔹 🕨	BTest Server Bandwidth Test	Packet Sniffer Settings		Packet Sniffer Settings	
MetaROUTER Partition Make Supout.rif Manual New WinBox Exit	Email Flood Ping Graphing IP Scan MAC Server Netwatch Packet Sniffer Ping Ping Speed	General Streaming Filter Memory Limit: 2043 kb ○ Only Headers ✓ Memory Scroll File Name: after-ALG.pcap ▲ File Limit: 4096 kb	OK Cancel Apply Start Stop Packets Connections Hosts Protocols	General Streaming Filter Interfaces: ether1-gateway MAC Address: MAC Protocol: IP Address: 208.252.1.148 IPv6 Address: IP Protocol: Port: 5060 (sip) \$ CPU:	OK Cancel Apply Start Stop Packets Connections Hosts Protocols
		stopped		Direction: any Filter Operation: and stopped	

/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.

Make sure to stop the sniffer

Packet Sniffer Settings General Streaming Filter OK Interface: etherl-gateway ∓∣≜ Cancel MAC Address: Apply MAC Protocol Start IP Address: 207.252.1.148 ۲ Stop ŧ IPv6 Address: Packets ÷ IP Protocol Connections ∓ ♦ Port: 5060 Hosts CPU: ŧ Protocols Ŧ Direction any Ŧ Filter Operation and stopped

/tool sniffer

stop

Penny Tone LLC - www.pennytone.com

Download pcap files

File List						×
- 7 8 8 1	Backup Restore	Upload			Find	
File Name	🛆 Туре		Size	Creation	Time	-
🖹 after-ALG.pcap	.pcap fil	le	5.9 Kil	B May/11	1/2017 17:01:0	04
2 items (2 selected)	.pcap fil		Show Categorie Detail Mode	s	(2017 15:13:0	1
			Show Columns	•	_	
			Find	Ctrl+F		
			Find Next	Ctrl+G		
			Restore			
			Download			

	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:1000207.252.1.148>;tag=1d8c3b3fa6a8a34co1 To: "100" <sip:1000207.252.1.148> Call-ID: e68aae07-897b8a710192.168.20.100 CSeq: 18716 REGISTER Max-Forwards: 70 Contact: "100" <sip:1000207.252.1.145:1024>;expires=3600 User-Agent: C1sco/SPA504G-7.6.2b Content-Length: 0 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE Supported: replaces</sip:1000207.252.1.145:1024></sip:1000207.252.1.148></sip:1000207.252.1.148>	
	<pre>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:1000207.252.1.148>;tag=1d8c3b3fa6a8a34co1 To: "100" <sip:1000207.252.1.148> Call-ID: e68aae07-897b8a710192.168.20.100 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:1000207.252.1.145:1024>;expires=3600 User-Agent: Cisco/SPA504G-7.6.2b Content-Length: 0 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE</sip:1000207.252.1.145:1024></sip:1000207.252.1.148></sip:1000207.252.1.148></pre>	
	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	a w
	Find: Find Nex	t
	Help Hide this stream Print Save as Close	

ALG Enabled

Before modification

after modification

Wireshark · Follow UDP Stream (udp.stream eq 4) · before-ALG	Wireshark · Follow UDP Stream (udp.stream eq 2) · after-ALG –
REGISTER sip:207.252.1.148 SIP/2.0 Via: SIP/2.0/UDP 192.168.20.100:5060; pranch=z9h64bK-eefddbff From: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 Call-ID: 6593bf0b-e1cc0d640192.168.20.100 CSeq: 60159 REGISTER Max-Forwards: 70 Contact: "100" <sip:1000192.168.20.100:5060>; expires=3600 User-Agent: C1sco/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=z9h64bK-e9fcb8df From: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 To: "100" <sip:1000207.252.1.148>; tag=36d71bb09199558301 Call-ID: 6593bf0b-e1cc0d640192.168.20.100 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:1000192.168.20.100:5060>; expires=3600 User-Agent: Cisco/SPA5046-7</sip:1000192.168.20.100:5060></sip:1000207.252.1.148></sip:1000207.252.1.148></sip:1000207.252.1.148></sip:1000207.252.1.148></sip:1000207.252.1.148></sip:1000192.168.20.100:5060></sip:1000207.252.1.148></sip:1000207.252.1.148>	REGISTER sip:207.252.1.148 SIP/2.0 Via: SIP/2.0/UDP 207.252.1.145:1024; prom: "100" <sip:1000207.252.1.148>; tag=1d8c3b3fa6a8a34co1 To: "100" <sip:1000207.252.1.148>; Call-ID: e68aae07-897b8a710192.168.20.100 CSeq: 18716 REGISTER Max-Eorwards: 70 Contact: "100" <sip:1000207.252.1.145:1024>; exported: replaces 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; byported: replaces REGISTER sip:207.252.1.148 SIP/2.0 Via: SIP/2.0/UDP 207.252.1.145:1024; byported: replaces REGISTER sip:207.252.1.148 SIP/2.0 Via: SIP/2.0/UDP 207.252.1.148:1024; byported: replaces REGISTER sip:207.252.1.148 Call-ID: e68aae07-897b8a710192.168.20.100 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:10< td=""></sip:10<></sip:1000207.252.1.145:1024></sip:1000207.252.1.148></sip:1000207.252.1.148>
4 client pkt(s), 0 server pkt(s), 0 turns.	Packet 5. 4 client pkt(s), 0 server pkt(s), 0 turns. Click to select.
192.168.20.100:5060 → 207.252.1.148:5060 (9940 by ▼ Show data as ASCII ▼	207.252.1.145:1024 → 207.252.1.148:5060 (1 ▼ Show data as ASCII ▼ Stream
Find:	Find: Find N
Help Hide this stream Print Save as	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 NAT2. 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



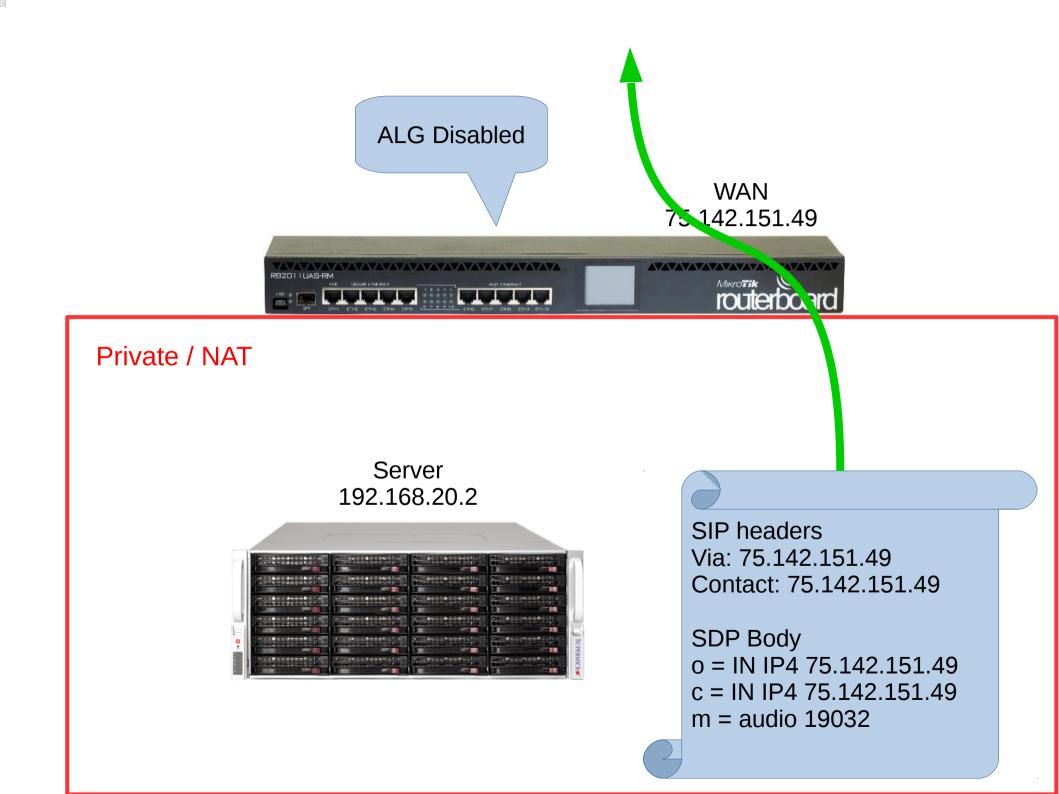
Private / NAT

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



Servers outside NAT (public server)

Servers outside NAT (public server)

SIP servers have NAT options for each extension

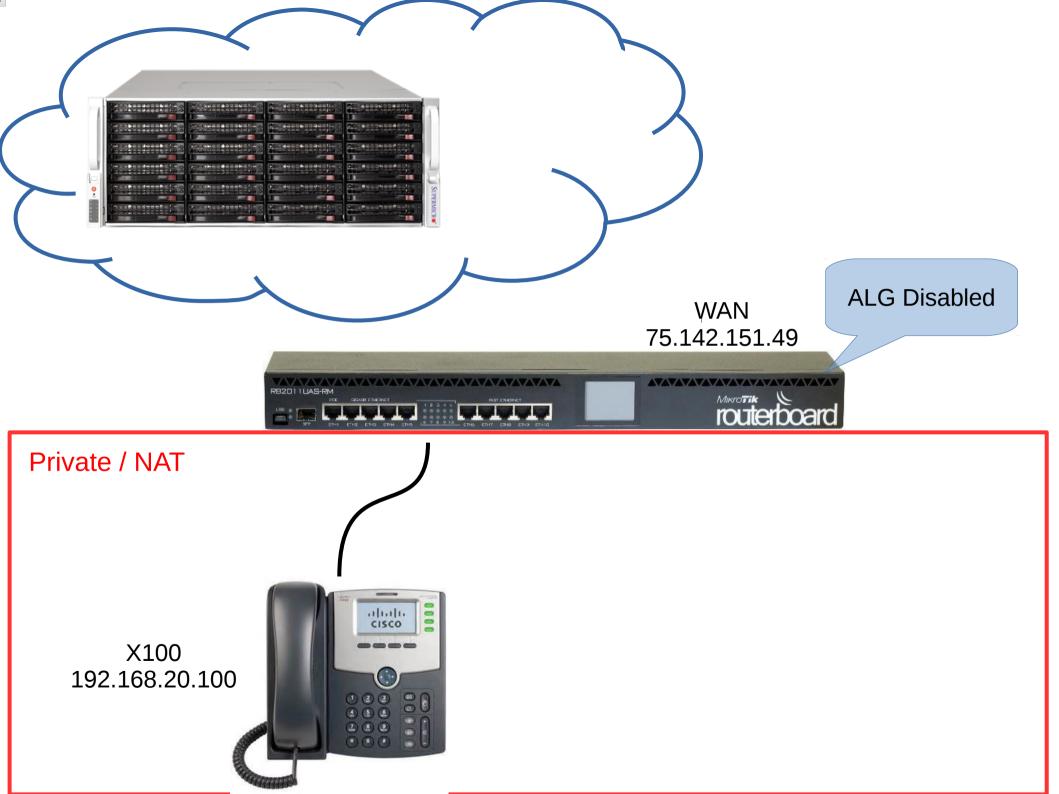
Servers outside NAT (public server)

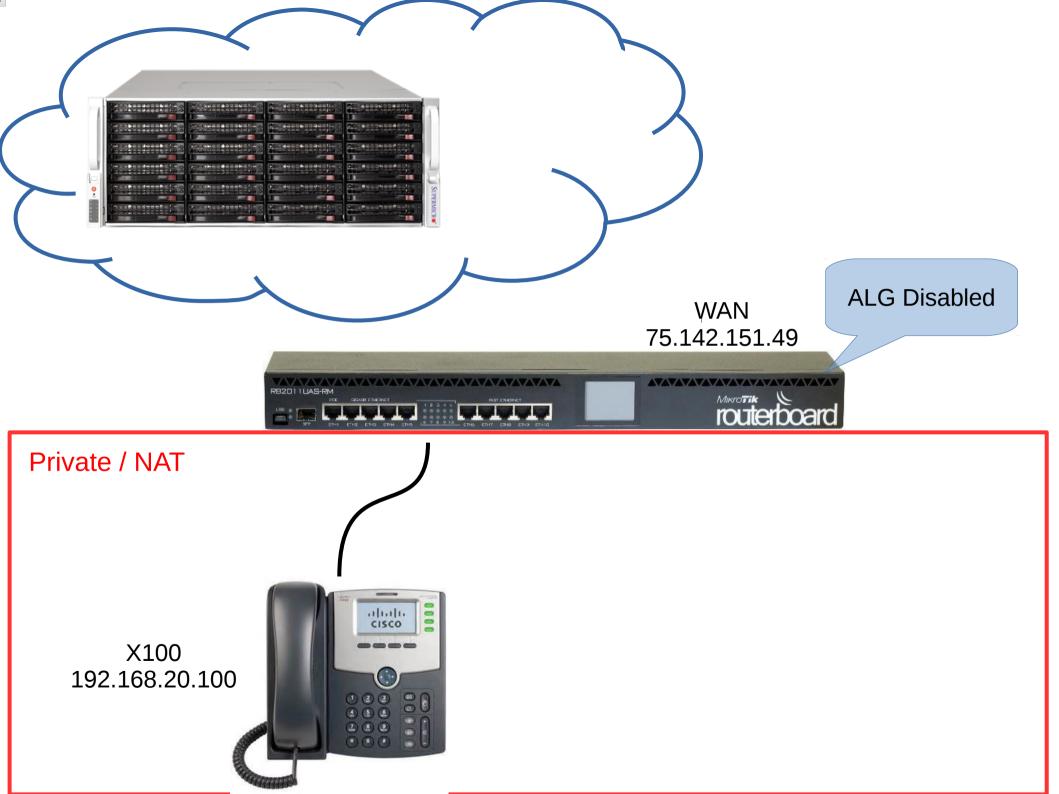
- SIP servers have NAT options for each extension
- If server side extension states NAT=Yes then send all responses to the client originating IP and Port.

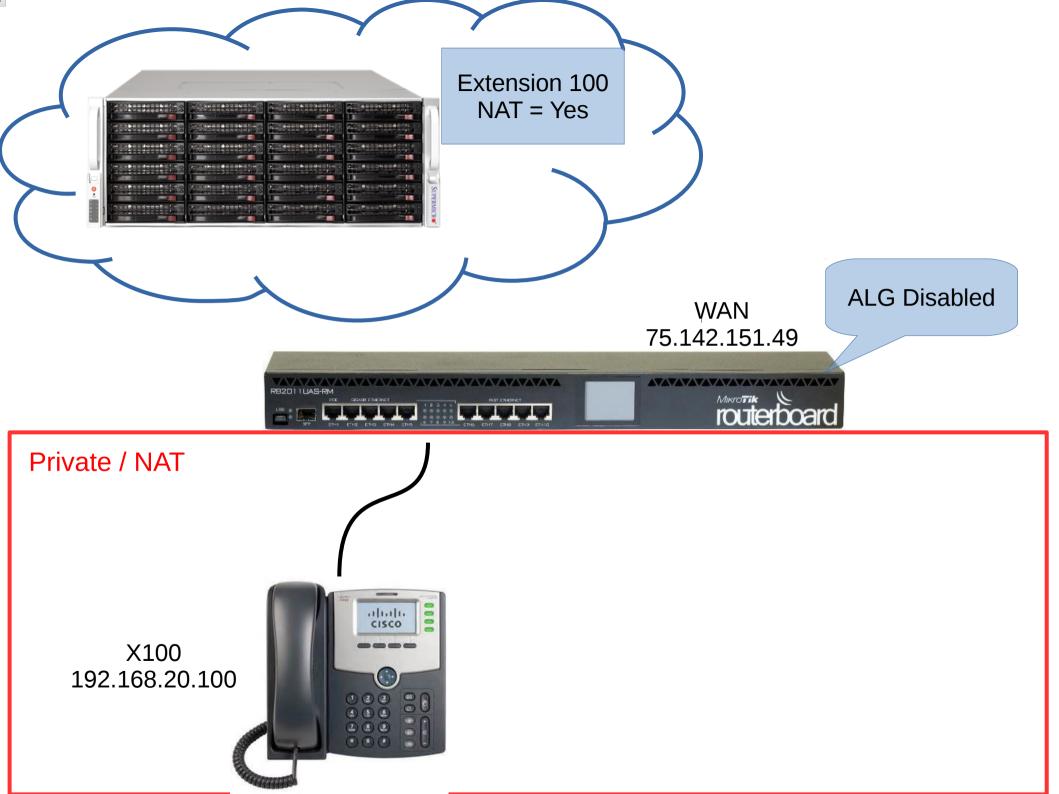


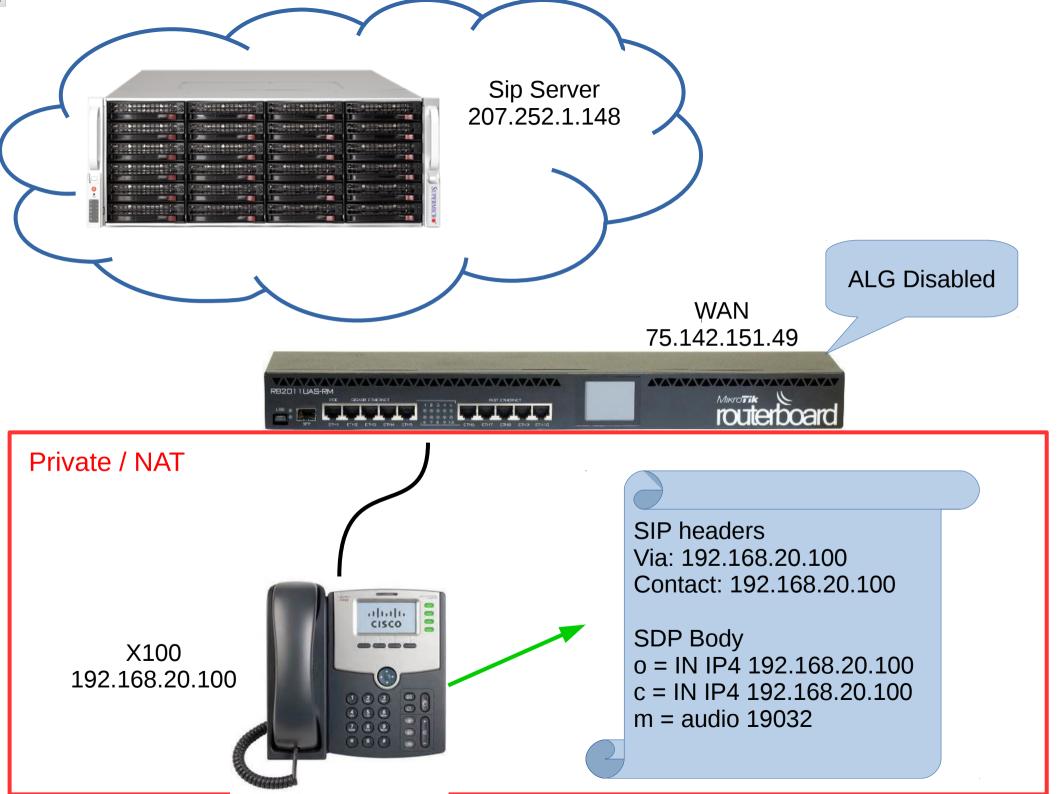
Private / NAT

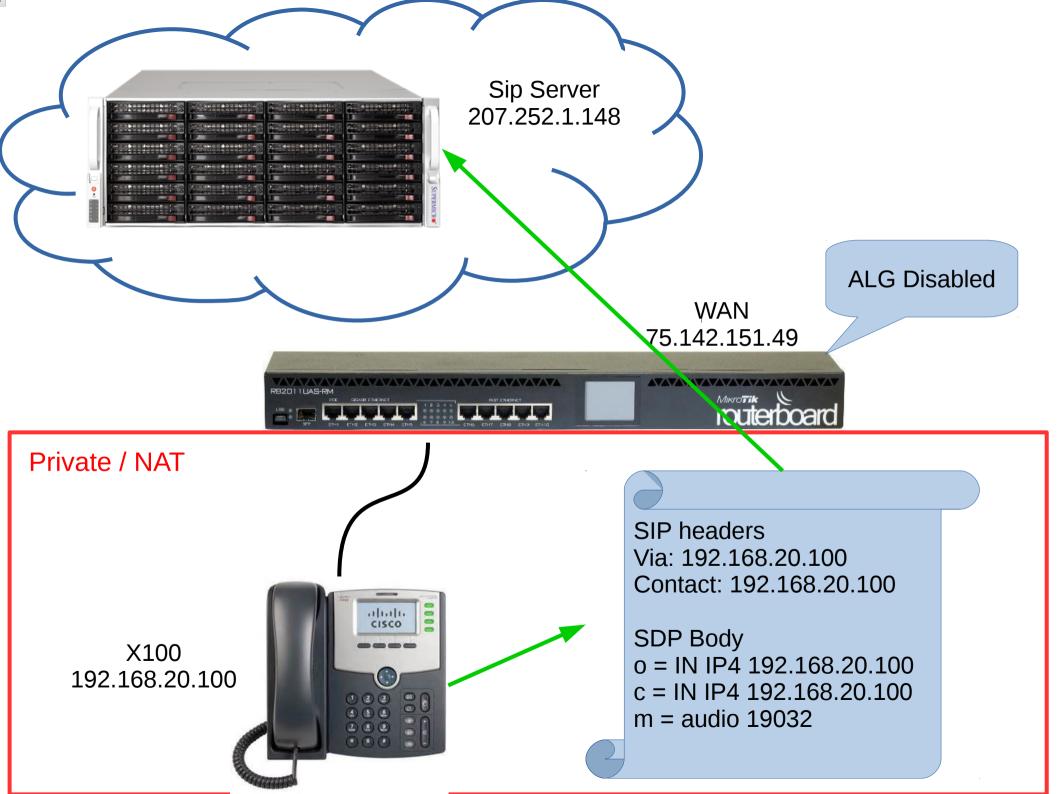


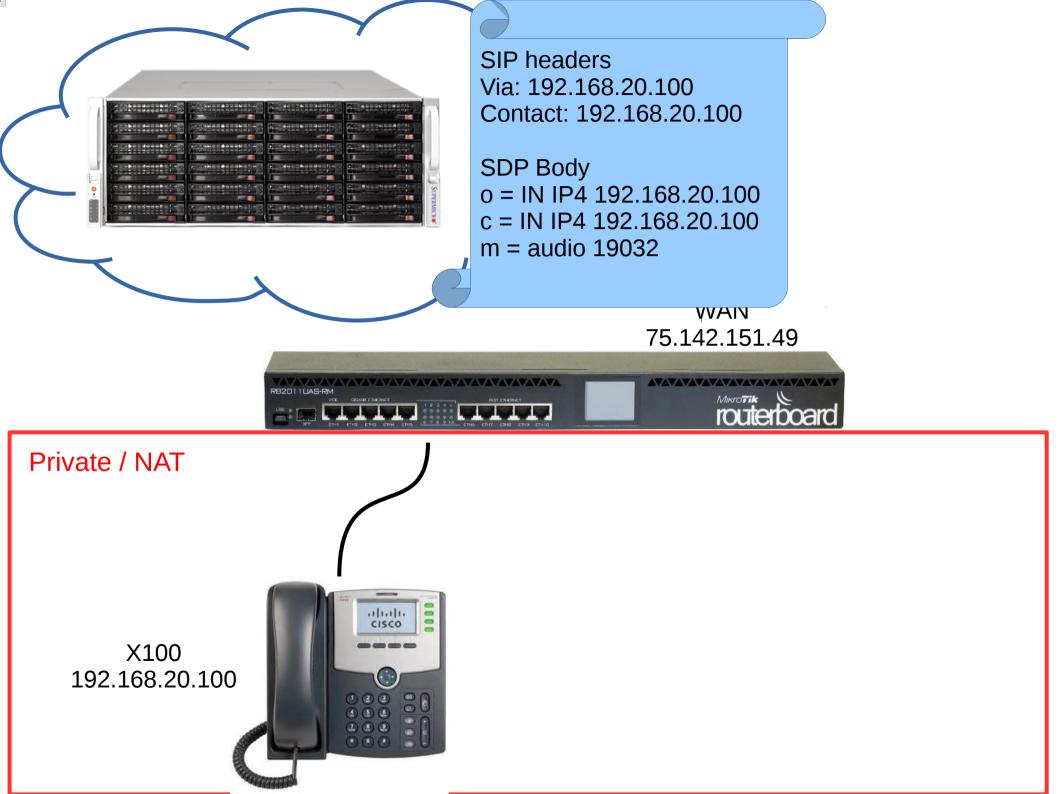


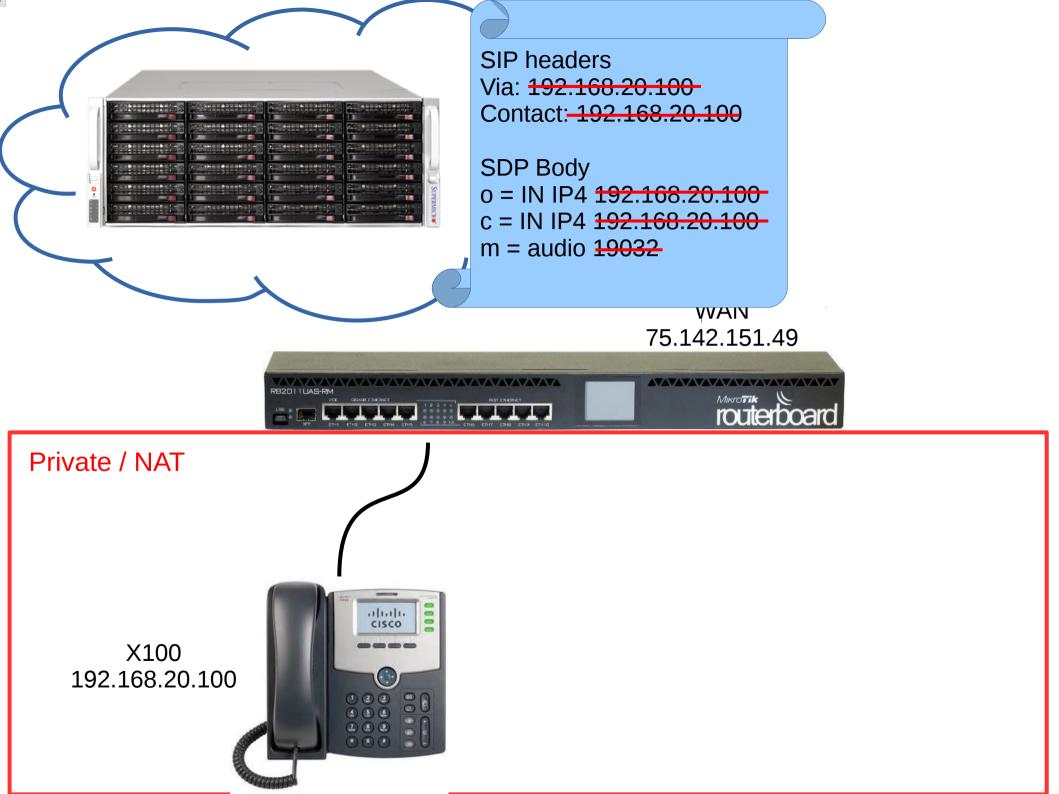


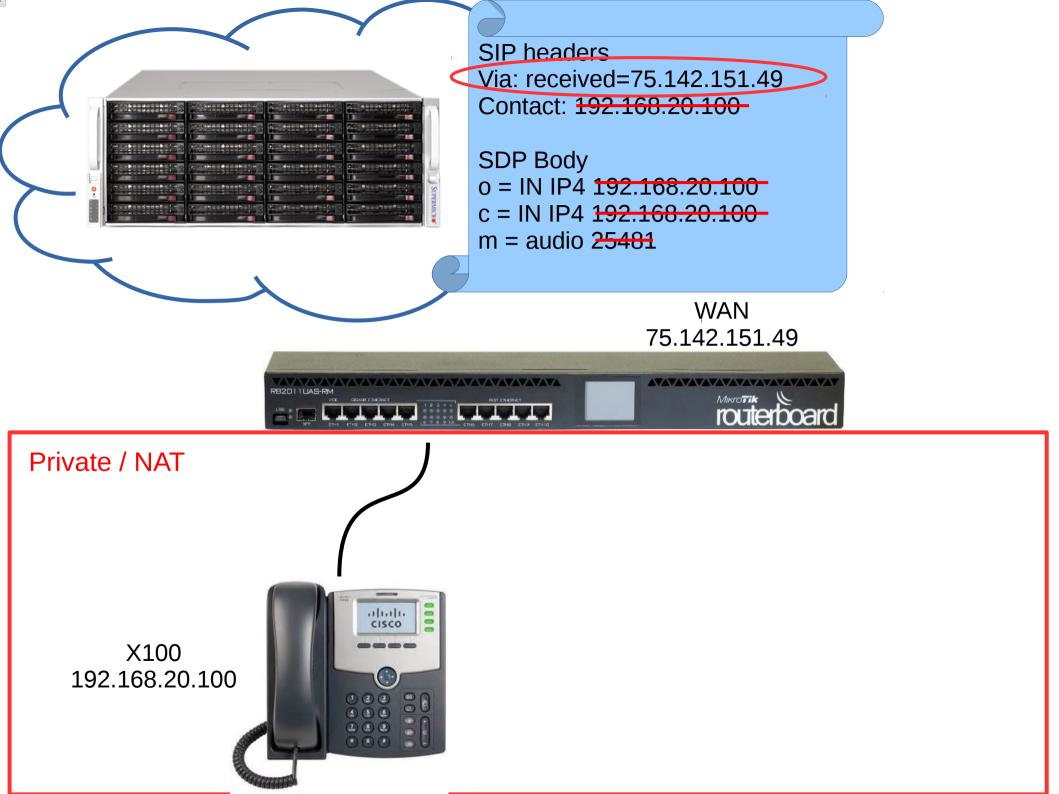












- DOES NOT HAPPEN WITH Mikrotik RouterOS !
- Poor quality ALG's replace ALL private IP's in SIP headers, including Call-ID

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

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</sip:201525@207.252.1.148>	
To: "David Attias" <sip:201525@207.252.1.148></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</sip:201525@192.168.20.100:5060>	
User-Agent: Cisco/SPA504G-7.6.2b	
Content-Length: 0	
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE	
Supported: replaces	

- 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:

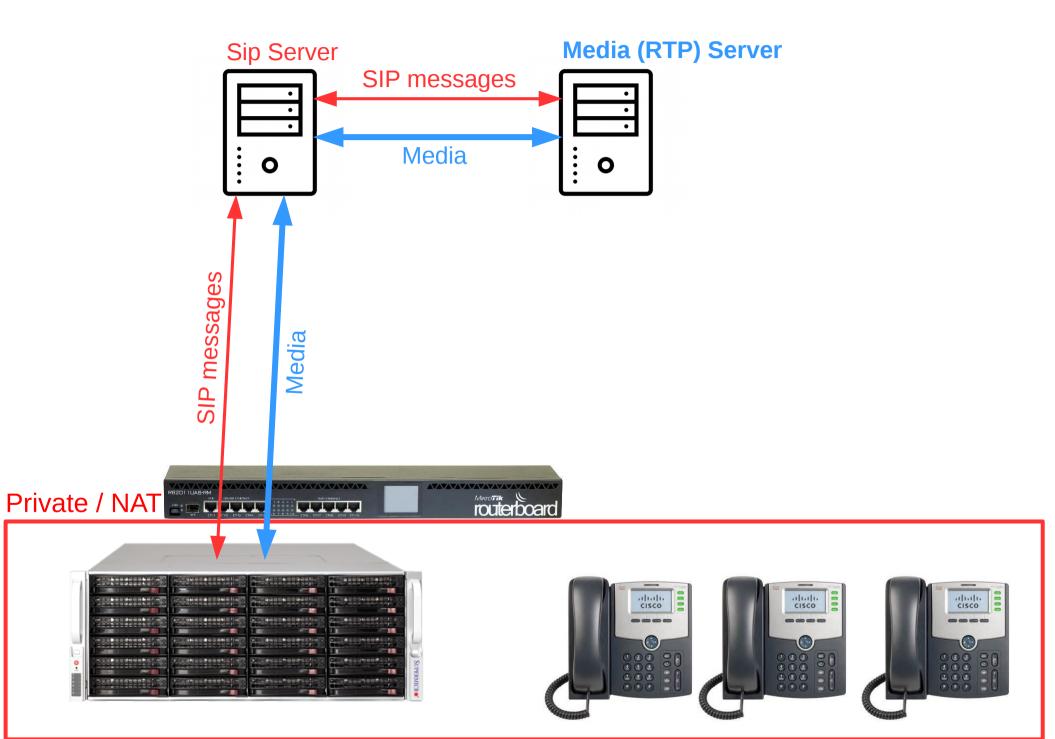
- Manually set SIP ALG timeout
- Set it higher than your lowest sip keepalive message interval (register, invite, options)

SIP Direct Media

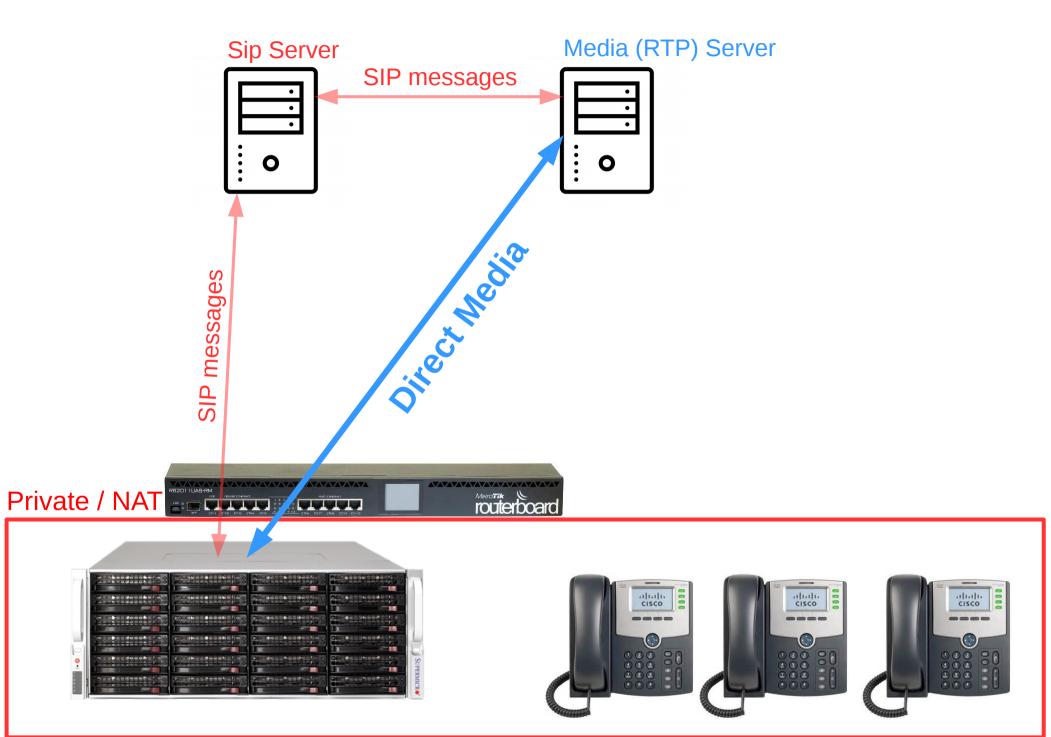
SIP Direct Media

- 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



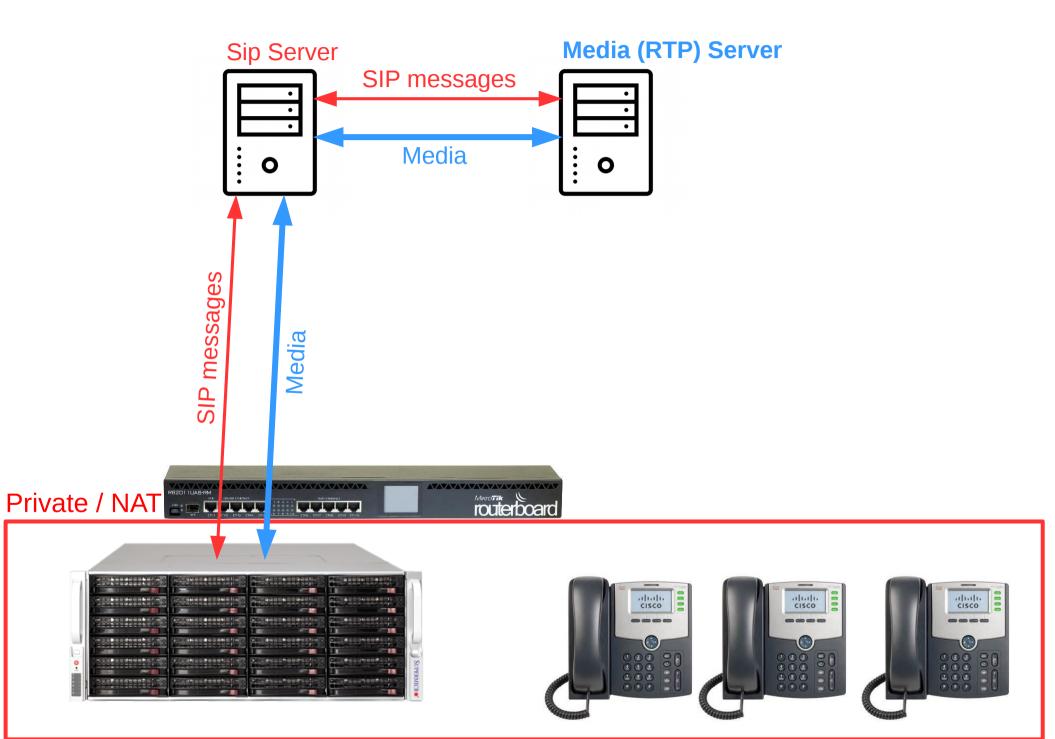
Direct-Media



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



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