



Mikrotik from a PABX technician's perspective

Joel Cornale
joel@gotelco.com.au

About Me

- ◆ Electronics Trade at NSW TAFE '97
- ◆ Started my career helping setting up ISP's in the late 1990's using;
 - KTX dial up modems on Livingstone Port masters
 - CISCO Routers
 - With services on FreeBSD UNIX like
 - RADUIS
 - SQUID
 - APACHE
- ◆ I left the ISP industry in 2000 and entered the PABX industry. Leaving IP behind me... Well so I thought.
- ◆ Mikrotik user for about 4 years

A PABX HISTORY

- ◆ 1870's first telephone invented
- ◆ 1930's first PBX
- ◆ 1970's first PABX
- ◆ 1980's ARPANET adopted TCP/IP

PABX Architecture & a PABX Technician

- ◆ Most PABX's Vendors use proprietary code.
- ◆ This gives the users continuity between their Non IP and IP handset.
 - Example – every key stroke pressed by the user on a proprietary handset sends an INFO packet to the PABX.
Unlike open standard SIP terminals, they will send an INVITE packet once the user has entered all the digits.

Issues experienced on IP PABX's behind your Mikrotik's

- ◆ Call Block
- ◆ Call Quality
- ◆ Toll Fraud
- ◆ Eves Dropping

Call Block

2 issues:

- ◆ Complete in/out bound call block, busy tone
- ◆ Voice block, one way or both

Common causes....

- ◆ DST NAT rules not programmed
- ◆ Incorrect SIP ALG usage
 - SIP session helper / ALG, David Attias
- ◆ PABX mis-configuration

Capture your fault

The image shows a network management interface with a sidebar on the left and a main window on the right. The sidebar contains a list of tools and features, with 'Tools' and 'Packet Sniffer' highlighted by red circles. The main window displays the 'Packet Sniffer Settings' dialog box, which is currently set to 'stopped'.

Packet Sniffer Settings

General | Streaming | Filter

Interfaces: ether1-gateway

MAC Address: []

MAC Protocol: []

IP Address: []

IPv6 Address: []

IP Protocol: 17 (udp)

Port: []

CPU: []

Direction: any

Filter Operation: or

Buttons: OK, Cancel, Apply, Start, Stop, Packets, Connections, Hosts, Protocols

Status: stopped

Finding your fault

9	0.003303	203.161.160.71	165.228.190.82	0 SIP	Stat
10	0.069601	165.228.190.82	203.161.160.71	0 SIP	Requ
11	0.000398	165.228.190.82	203.161.160.71	0 SIP/SDP	Requ
12	0.028189	203.161.160.71	165.228.190.82	0 SIP	Stat
13	0.022566	203.161.160.71	165.228.190.82	0 SIP	Stat

Frame 11: 1243 bytes on wire (9944 bits), 1243 bytes captured (9944 bits)

Ethernet II, Src: Routerbo_51:57:6b (e4:8d:8c:51:57:6b), Dst: 8a:e0:f3:f3:68:16

Internet Protocol Version 4, src: 165.228.190.82 (165.228.190.82), Dst: 203.161.

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol (INVITE)

Session Initiation Protocol (SIP as raw text)

```
INVITE sip:0420662573@trunk.engin.com.au SIP/2.0\r\n
From: <sip:Anonymous@Anonymous.invalid>;tag=630F32463135364100002381\r\n
To: <sip:0420662573@trunk.engin.com.au:5060>\r\n
Contact: <sip:07312811..2@192.168.1.190:5060>\r\n
Content-Type: application/sdp\r\n
Privacy: id\r\n
P-Preferred-Identity: <sip:07312811..2@voice.mibroadband.com.au>\r\n
CSeq: 2 INVITE\r\n
[truncated]Authorization: DIGEST username="07312811..2",realm="voice.mibroadba
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE\r\n
```


Finding your fault

754	0.068113	165.228.190.82	203.161.160.71	0 SIP	Request: AC
755	0.000334	165.228.190.82	203.161.160.71	0 SIP/SDP	Request: IN
756	0.027651	203.161.160.71	165.228.190.82	0 SIP	Status: 100
757	0.139607	203.161.160.71	165.228.190.82	0 SIP/SDP	Status: 183
762	0.004497	165.228.190.82	203.161.160.71	0 STP	Request: PR

Frame 755: 1253 bytes on wire (10024 bits), 1253 bytes captured (10024 bits)

Ethernet II, Src: Routerbo_51:57:6b (e4:8d:8c:51:57:6b), Dst: 8a:e0:f3:f3:68:16 (8a:e0:f3:f3:68:16)

Internet Protocol Version 4, Src: 165.228.190.82 (165.228.190.82), Dst: 203.161.160.71

User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5060 (5060)

Session Initiation Protocol (INVITE)

Session Initiation Protocol (SIP as raw text)

```
INVITE sip:042060...@trunk.engin.com.au SIP/2.0\r\n
From: <sip:0731281282@voice.mibroadband.com.au>;tag=6760324631353641000023F0\r\n
To: <sip:042060...@trunk.engin.com.au:5060>\r\n
Contact: <sip:0731281282@192.168.1.190:5060>\r\n
Content-Type: application/sdp\r\n
Privacy: none\r\n
P-Preferred-Identity: <sip:0731281282@voice.mibroadband.com.au>\r\n
CSeq: 2 INVITE\r\n
[truncated]Authorization: DIGEST username="0731281282",realm="voice.mibroadband.com.
Allow: INVITE ACK BYE CANCEL PRACK UPDATE\r\n
```

Call Quality

- ◆ Missing packets must not exceed 1%
- ◆ Out of order packets - you only have about 80ms to put packets back in order.
- ◆ packet egress... Make sure packets leave your network **In time and On time !!!**
- ◆ packet ingress ... Not to much we can do there apart from shaping non VoIP traffic.
- ◆ Attend a "MikroTik Certified Traffic Control Engineer" course ..

Toll Fraud

- ◆ Hop on Hop off attack
- ◆ Register as an existing user account
- ◆ Hack the DB,
 - create yourself a valid account
 - use the details elsewhere

Register an account

Extension: Tel port 009: IP - STA 109 - 220.244.25.98

Terminal Type: SIP

Terminal MAC Address: 00-00-00-00-00-00

Nickname:

Terminal Type: IP70 Series

Using IP Address: 220.244.25.98

NGT Voice Path Port: 0

NGT Call Control Port: 0

Codec Type: Type 1

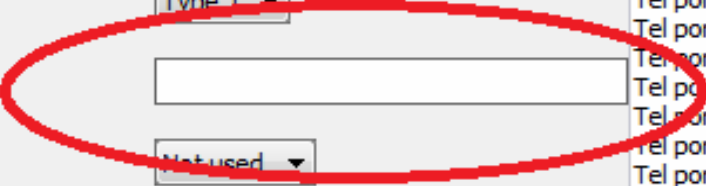
Authentication Password:

IP Duplication Allowed Group: Not used

Side Option Unit: None

Extension list:

- Tel port 009: IP - STA 109 - 220.244.25.98
- Tel port 010: IP - STA 110 - 220.244.25.98
- Tel port 011: IP - STA 111 - 220.244.25.98
- Tel port 012: IP - STA 112 - 220.244.25.98
- Tel port 013: IP - STA 113 - 220.244.25.98
- Tel port 014: IP - STA 114 - 220.244.25.98
- Tel port 015: IP - STA 115 - 220.244.25.98
- Tel port 016: IP - STA 116 - 220.244.25.98
- Tel port 017: IP - STA 117 - 220.244.25.98
- Tel port 018: IP - STA 118 - 220.244.25.98
- Tel port 019: IP - STA 119 - 220.244.25.98
- Tel port 020: IP - STA 120 - 220.244.25.98
- Tel port 021: IP - STA 121 - 220.244.25.98
- Tel port 022: IP - STA 122 - 220.244.25.98
- Tel port 023: IP - STA 123 - 220.244.25.98
- Tel port 024: IP - STA 124 - 220.244.25.98
- Tel port 025: IP - STA 125 - 220.244.25.98
- Tel port 026: IP - STA 126 - 220.244.25.98
- Tel port 027: IP - STA 127 - 220.244.25.98
- Tel port 028: IP - STA 128 - 220.244.25.98
- Tel port 029: IP - STA 129 - 220.244.25.98
- Tel port 031: IP - STA 131 - 85.25.218.94
- Tel port 032: IP - STA 132 - 220.244.25.98
- Tel port 033: IP - STA 133 - 220.244.25.98
- Tel port 034: IP - STA 134 - 220.244.25.98
- Tel port 035: IP - STA 135 - 220.244.25.98
- Tel port 036: IP - STA 136 - 220.244.25.98
- Tel port 037: IP - STA 137 - 220.244.25.98
- Tel port 038: IP - STA 138 - 220.244.25.98
- Tel port 039: IP - STA 139 - 220.244.25.98



Register an account

SIP Extension Basic Settings

- Registrar/Proxy Port

- Session Time

- Minimum Session Time

Information
Value should be in the range 1~65535
TCP Port
Default=5070

« Main VoIP-DSP Options **Port Number** LAN Status Media Relay SIP Extension

Voice (RTP) UDP Port No. (Server) : 12000

Voice (RTP) UDP Port No. (IP-PT / SIP-MLT) : 8000

UDP Port No. for SIP Extension Server : 0

CWMP (HTTP) Port No. for SIP-MLT : 7547

CWMP (HTTPS) Port No. for SIP-MLT : 7547

Data Transmission Port No. for SIP-MLT : 7547

Data Transmission Port No. for SIP-MLT : 7547

Firmware Update Port No. for SIP-MLT : 7547

LOGIN Port No. for SIP-MLT : 7547

G000264: Invalid range value, range must be within 1024 - 65535.

OK

DB Hack Prevention

Action	Chain	Src. Address	Dst....	Protocol	Sr...	Dst. Port	In. Interface	C	Bytes	Packets
✓ acc...	forward	203.161.160.71		17 (udp)		5060	ether1-gateway		11.0 KB	21
✗ drop	forward			17 (udp)		5060	ether1-gateway		0 B	0

Filter: sip

number	Time	Source	Destination	DSCP	Protocol	Info
713	1.414136	192.168.151	59.100.21	0	SIP	Request: REGISTER sip:59.100.21.2
714	0.100771	59.100.21	192.168.1	0	SIP	Status: 404 Not Found

Frame 714: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interf

- Ethernet II, Src: Draytek_b2:1a:a0 (00:1d:aa:b2:1a:a0), Dst: IntelCor_0d:8f:e4 (3c
- Internet Protocol Version 4, Src: 59.10... (59.100.21.2), Dst: 192.168.150.
- User Datagram Protocol, Src Port: 4... (5060), Dst Port: 21222 (21222)
- Session Initiation Protocol (404)
 - Status-Line: SIP/2.0 404 Not Found
 - Message Header
 - From: "test-"<sip:123@59.100.21.2>;tag=6e398b1e
 - To: "test-"<sip:123@59.100.21.2>;tag=9806324631353641421AE104
 - Call-ID: OGMxZTVhNjMxZDdmNjZlNGEyzWMxNTBhZjFlYWU3ZDc.
 - Cseq: 1 REGISTER
 - Server: NEC SL2100 01.04.08/2.1
 - Via: SIP/2.0/UDP 192.168.150.105:21222;branch=z9hg4bk-d87543-b57a62003460694f-
 - Content-Length: 0

DB Hack Attack

Authentication User ID

0733331234

Authentication Password

P@ssw0rd

	User Name (64 characters)	Authentication ID (64 characters)	Authentication Password (32 characters)
		0733331234	P@ssw0rd

PABX Database Hack prevention

- ◆ Simply Firewall all inbound requests not coming from the PABX technicians

Action	Chain	Src. Address	Dst....	Protocol	Sr...	Dst. Port	In. Interface	C	Bytes	Packets
✓ acc...	forward	1.2.3.4		6 (tcp)		8000	ether1-gateway		0 B	0
✗ drop	forward			6 (tcp)		8000	ether1-gateway		620 B	11

Eves dropping

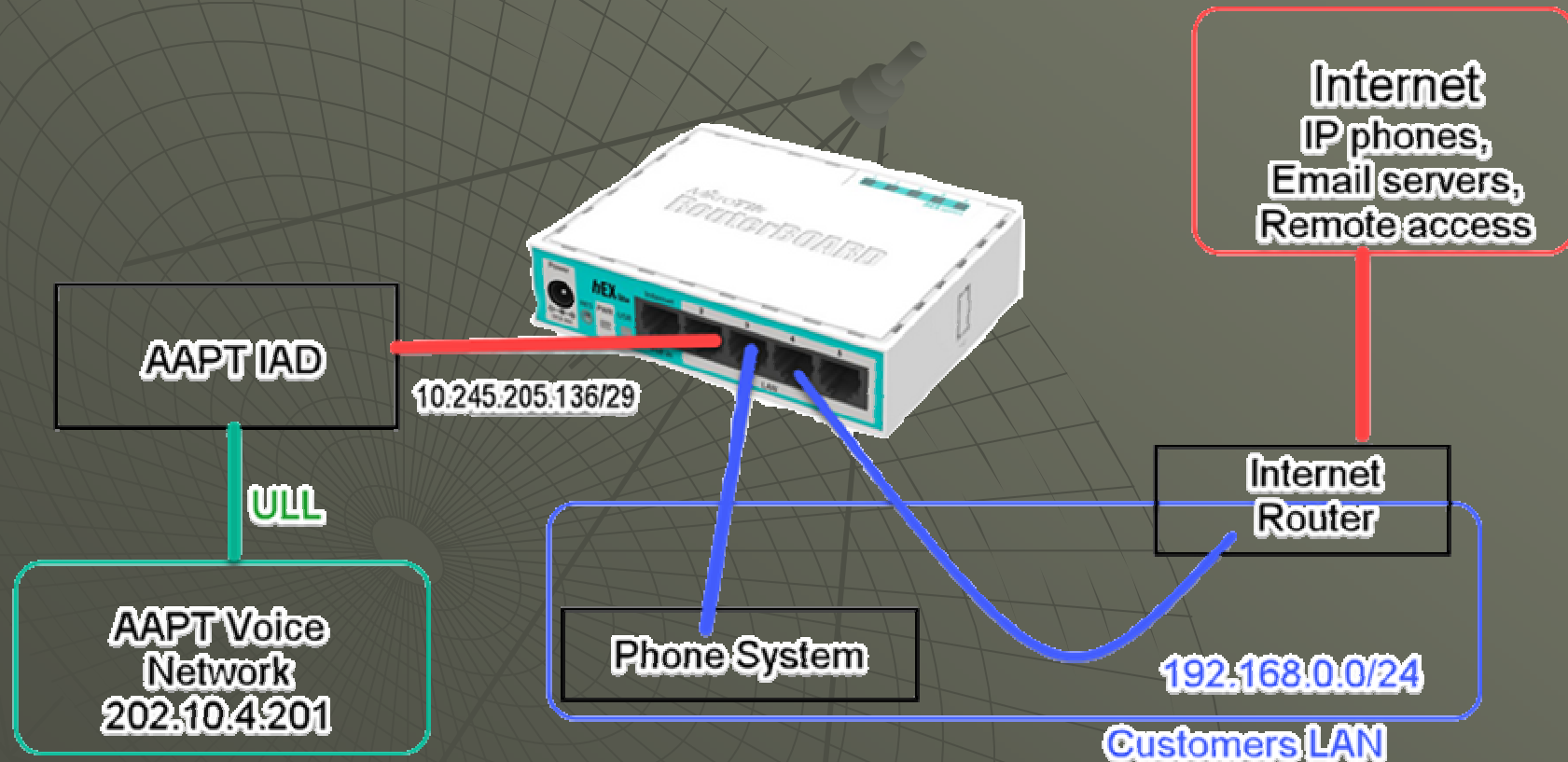
Not common but can be a consideration with higher end clients.

- ◆ Mikrotik Programming suggestions to prevent Eves Dropping
 - IP SEC tunnels between sites !
 - Use Non Internet based SIP Trunks







Internet or Non-Internet based VoIP service

	Internet based	Carrier Network
Voice quality guaranteed	NO	YES
Secure	NO	YES *
Cheap	YES	NO
Number portability	YES	NO

Example of Carrier delivered VoIP service.

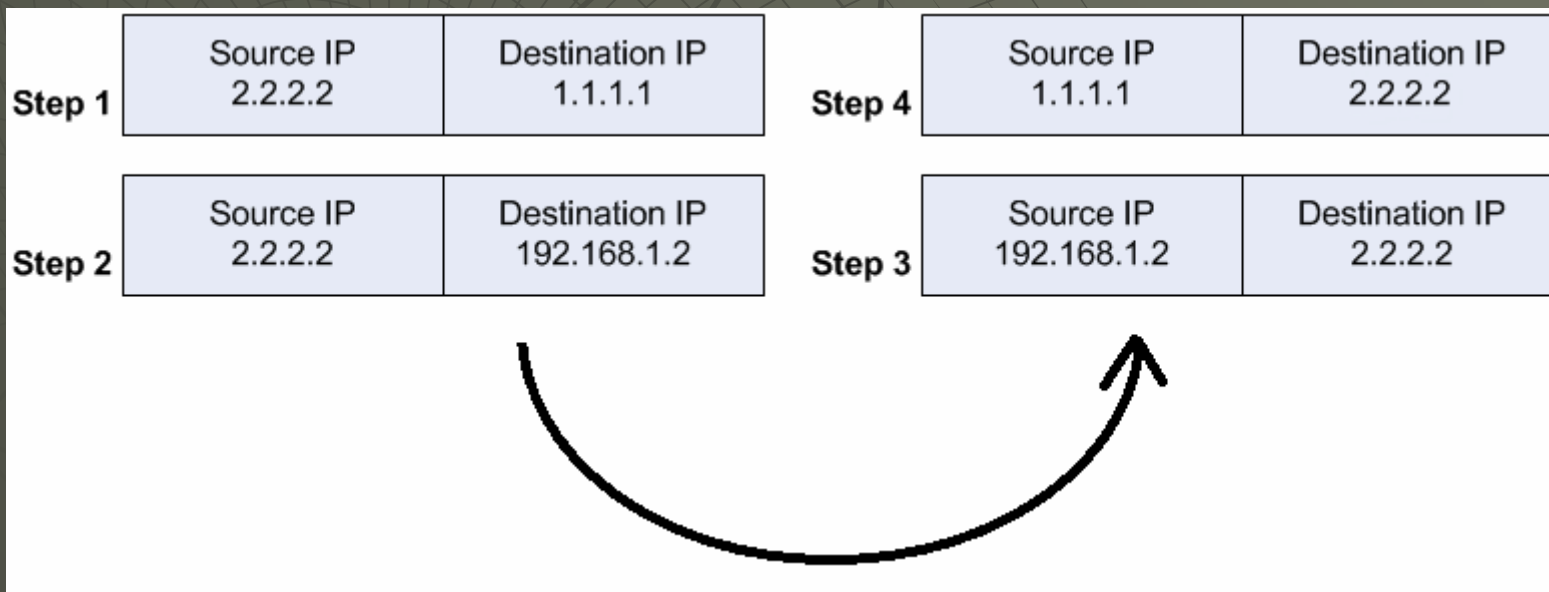
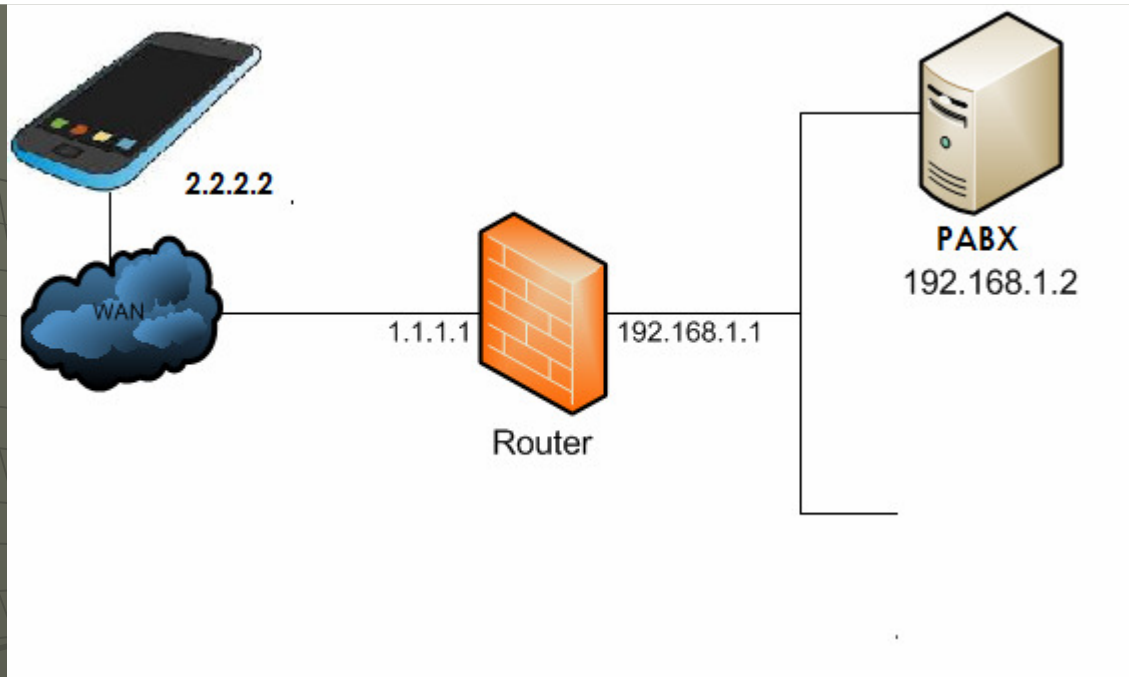


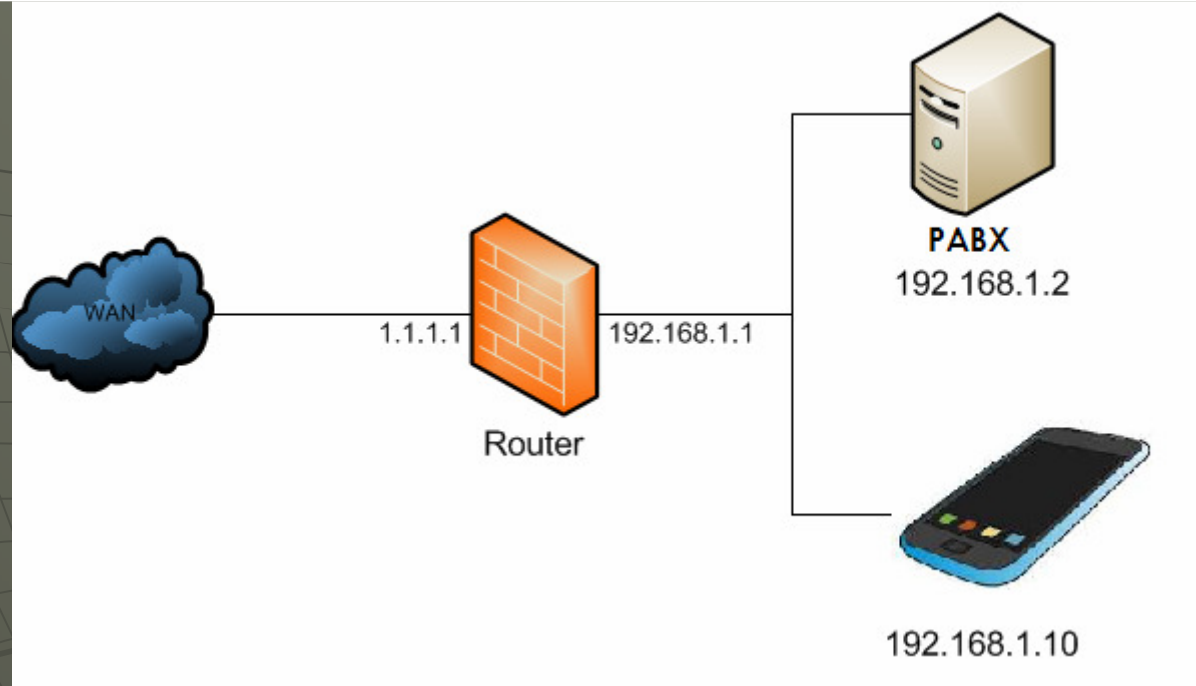
Carrier provided voice network

Route List					
Routes	Nexthops	Rules	VRF		
					
	Dst. Address	Gateway			
AS	▶ 0.0.0.0/0	192.168.1.1 reachable bridge - LAN			
DAC	▶ 10.245.205.136/29	ether2 - AAPT reachable			
DAC	▶ 192.168.1.0/24	bridge - LAN reachable			
AS	▶ 202.10.26.33	10.245.205.137 reachable ether2 - AAPT			

NAT Loop back / Hairpin

- ◆ Mobile users create another issue, moving between the LAN / Internet.
- ◆ DNS could resolve , however it is quite a complex configuration.
- ◆ Create 2 x SIP profiles
- ◆ Use Hairpin





Step 1

Source IP 192.168.1.10	Destination IP 1.1.1.1
---------------------------	---------------------------

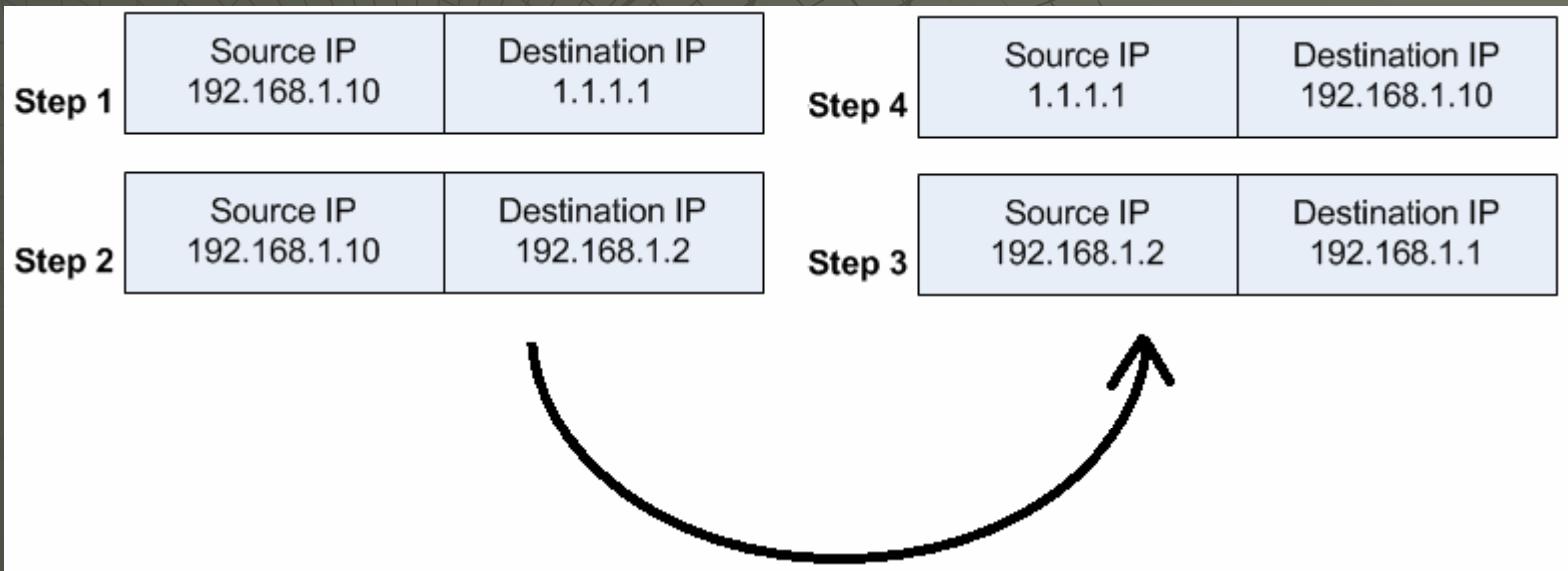
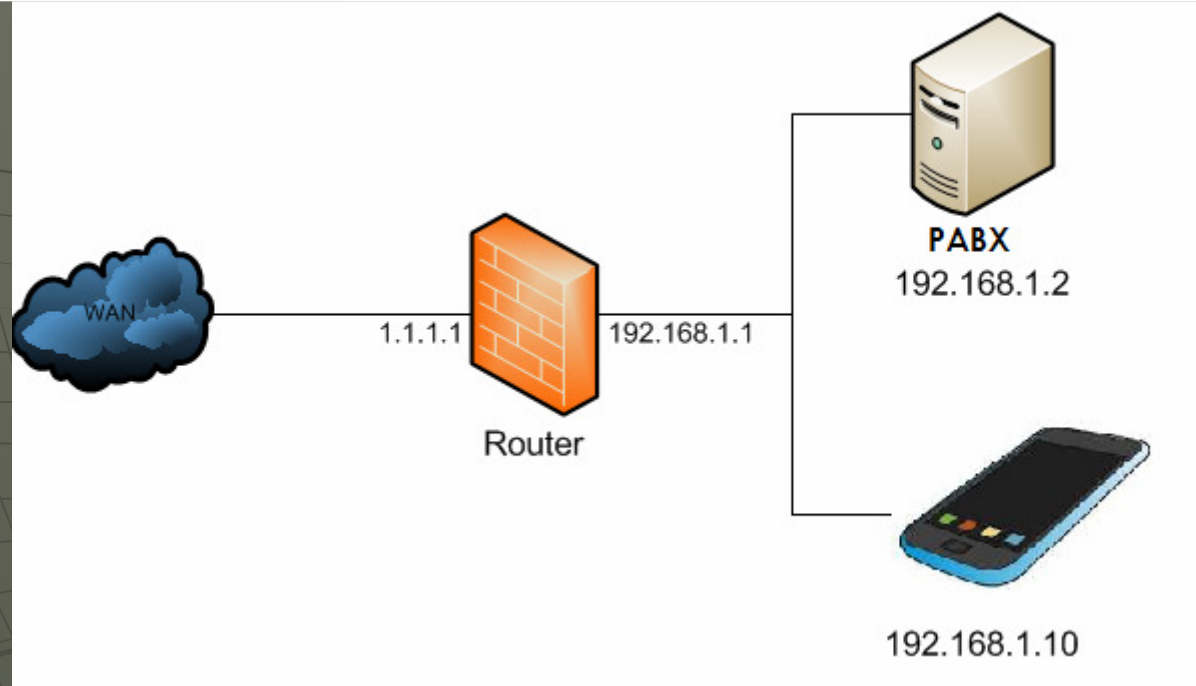
Step 2

Source IP 192.168.1.10	Destination IP 192.168.1.2
---------------------------	-------------------------------

Step 3

Source IP 192.168.1.2	Destination IP 192.168.1.10
--------------------------	--------------------------------





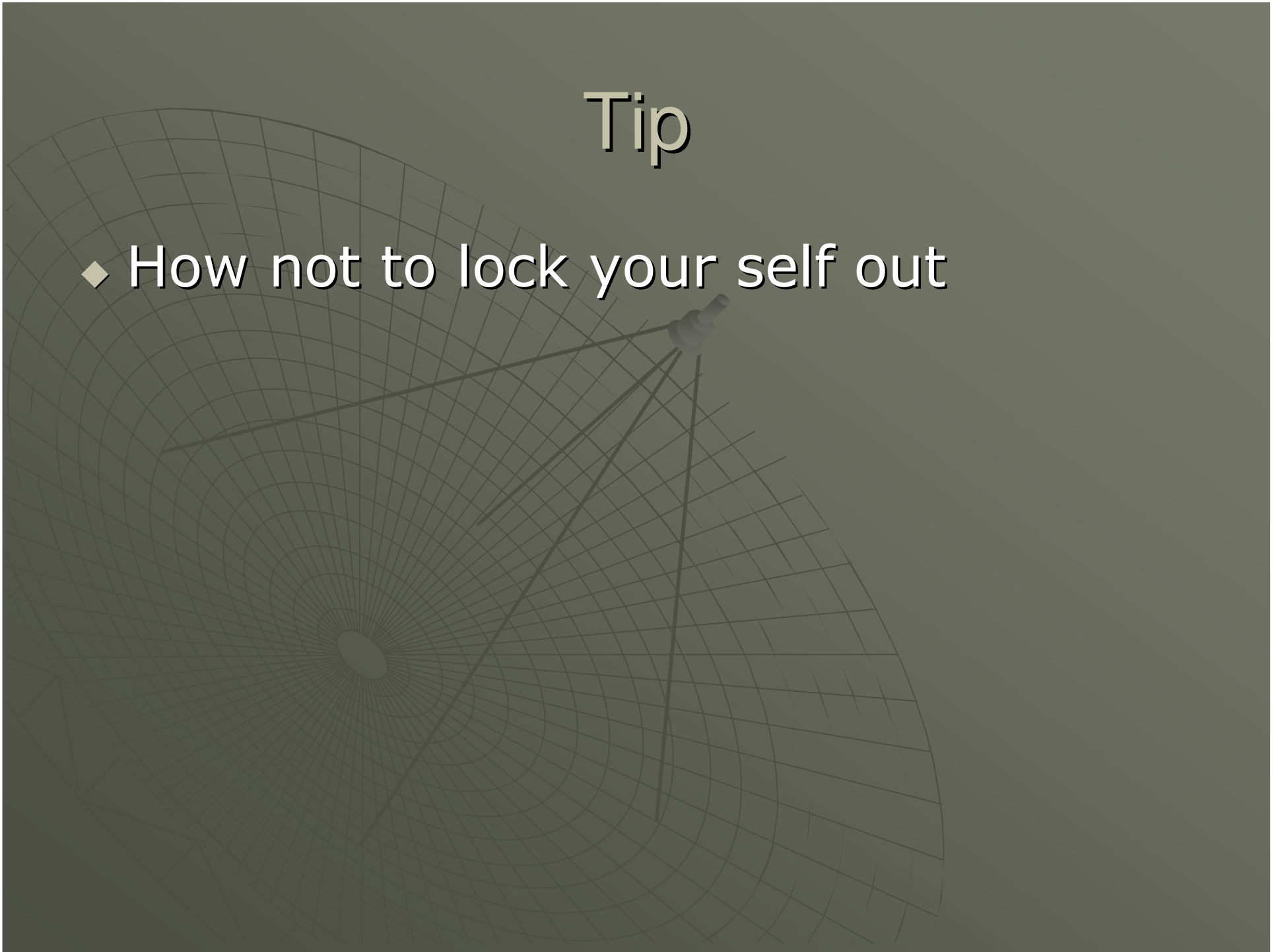
Mikrotik NAT rule

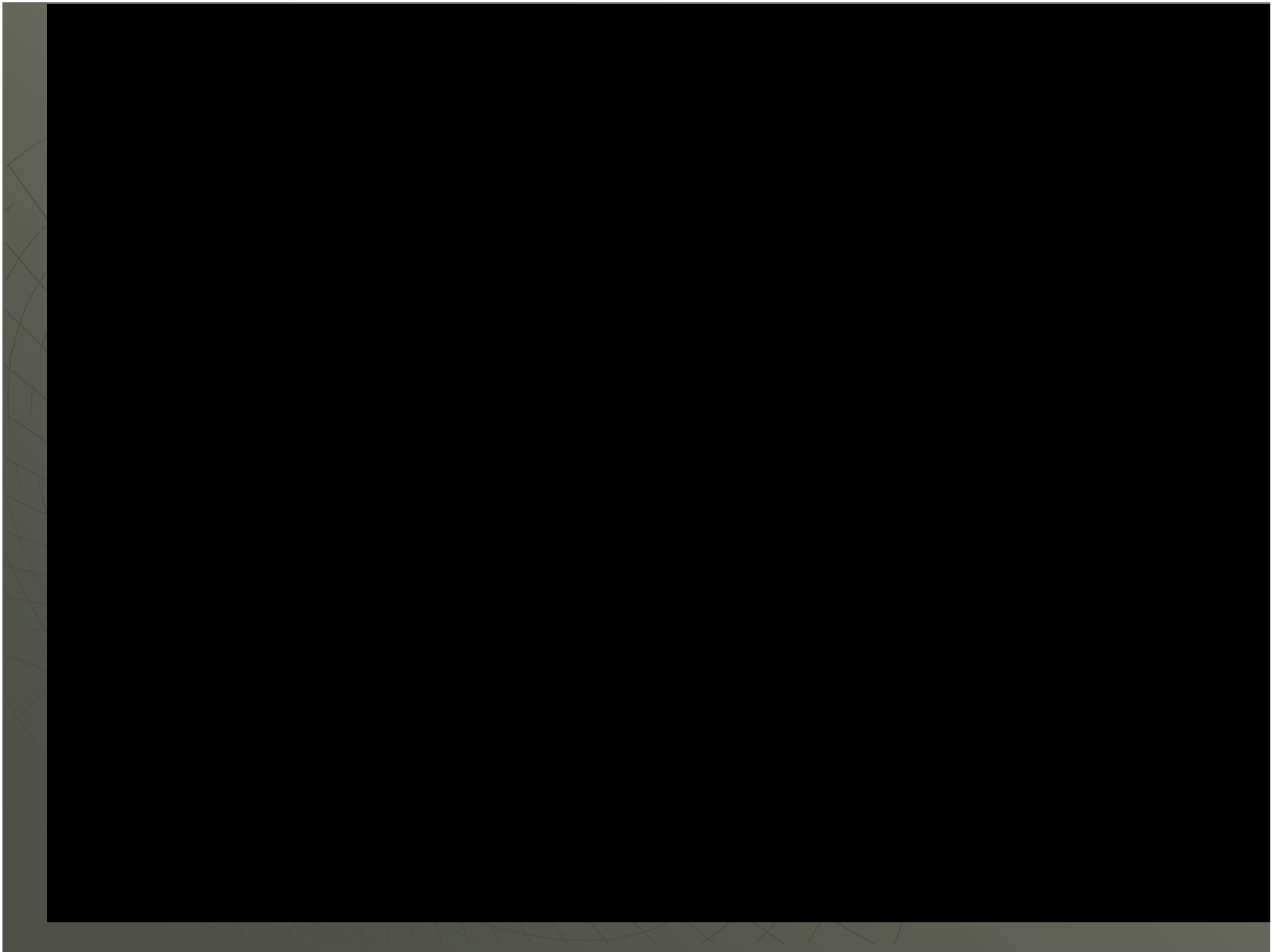
On top of your standard Dest NAT rule you need.

```
/ip firewall nat add chain=srcnat src-address=192.168.1.0/24 \  
dst-address=192.168.1.2 protocol=tcp dst-port=80 \  
out-interface=LAN action=masquerade
```

Tip

- ◆ How not to lock your self out





Summary

- ◆ You must tell your clients if their networks are not up to scratch for a VoIP system (there are still lots of ADSL 2 customers out there)
- ◆ Lock your systems down
- ◆ Ask your customers to bar IDD & INFO calls at the carrier end. That way there can be no toll fraud & blame you in any way!