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

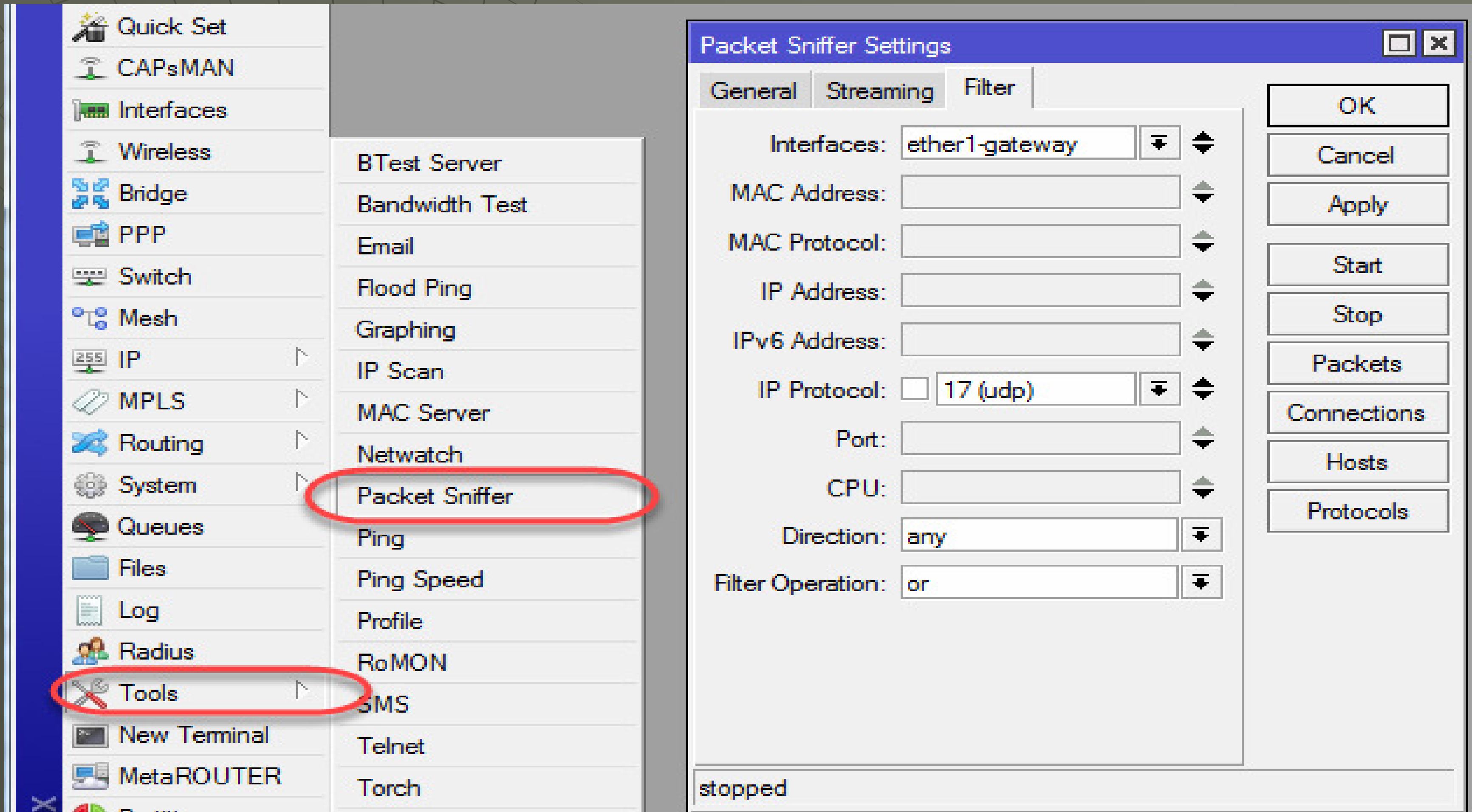
2 issues:

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

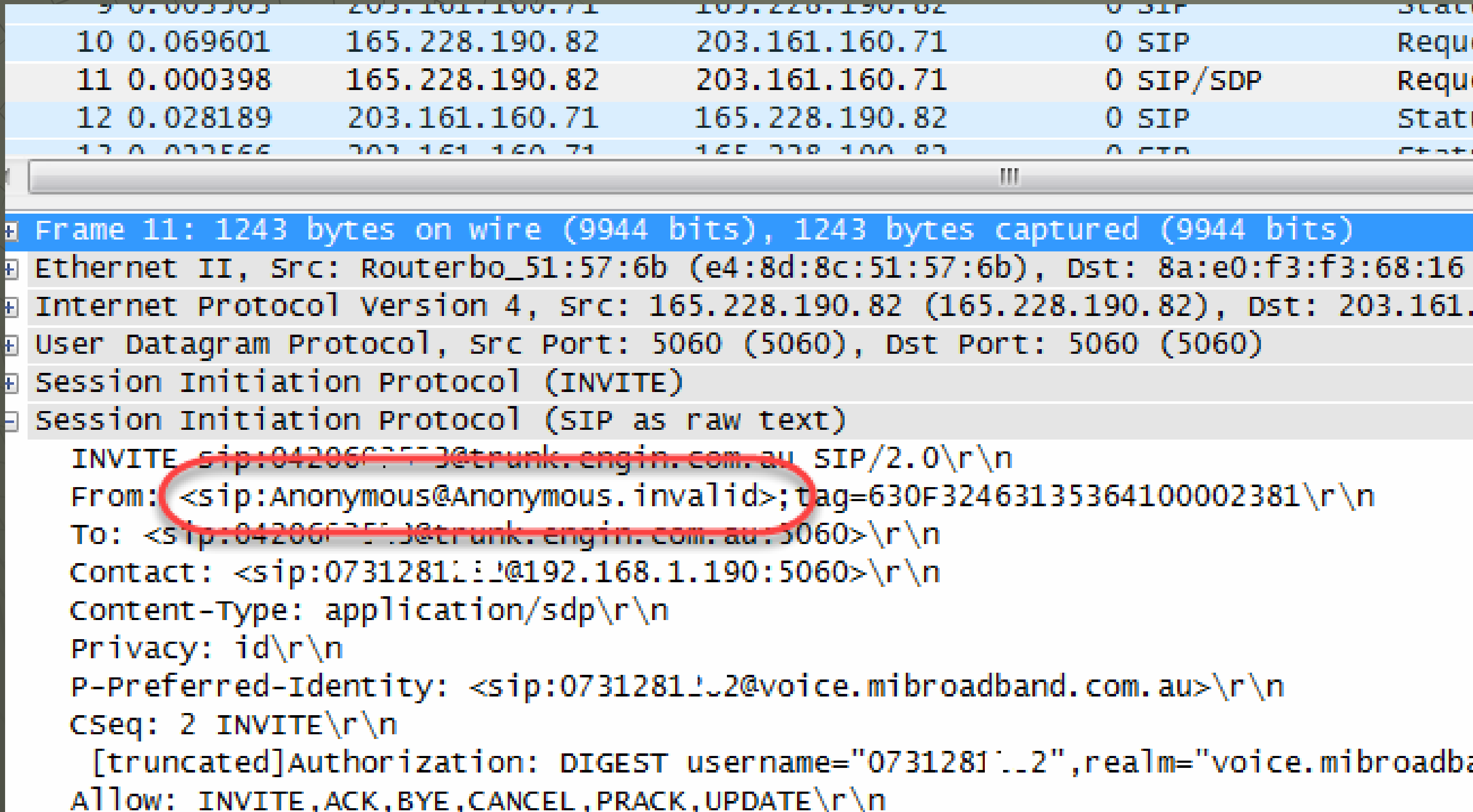
Common causes….

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

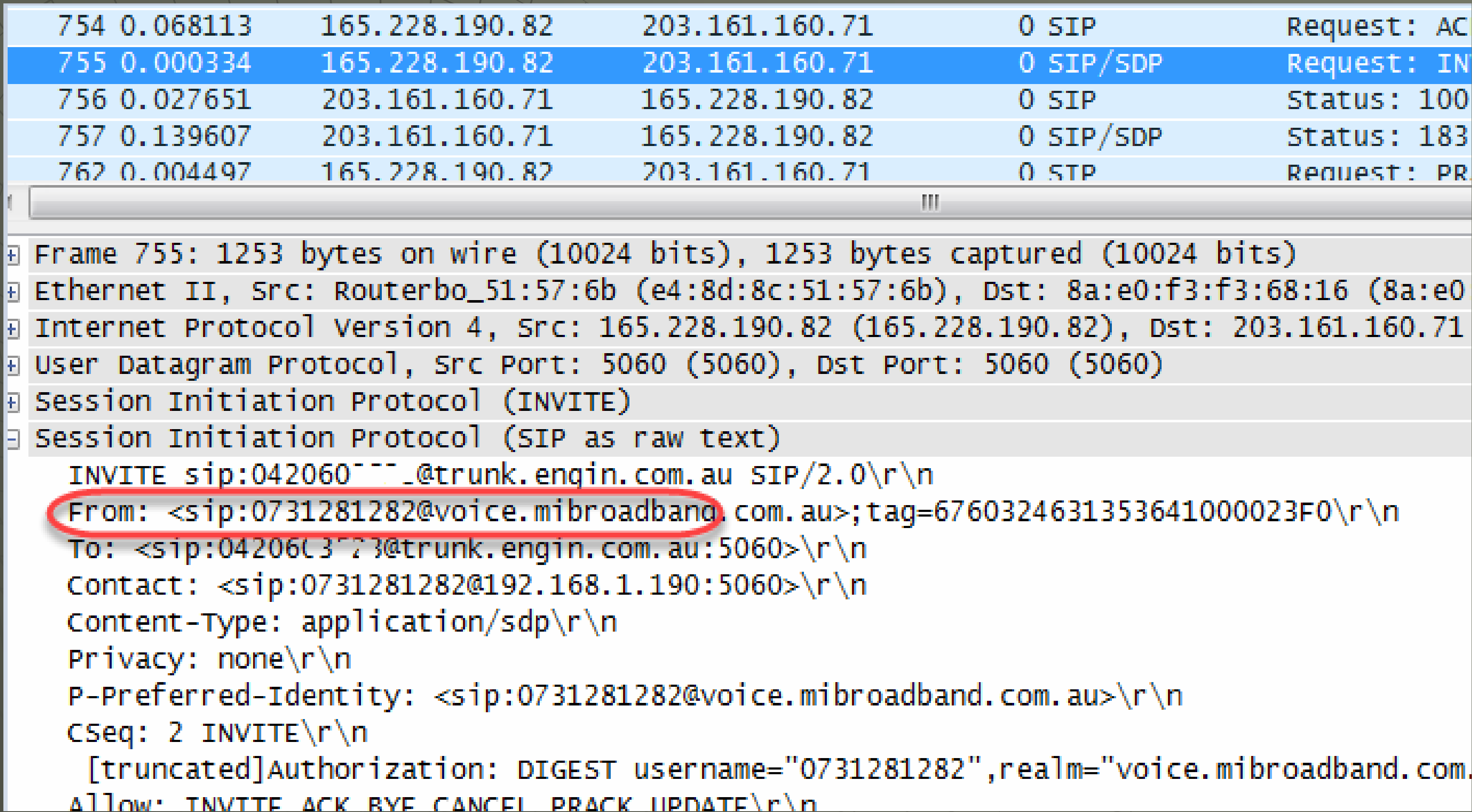
Capture your fault



Finding your fault



Finding your fault



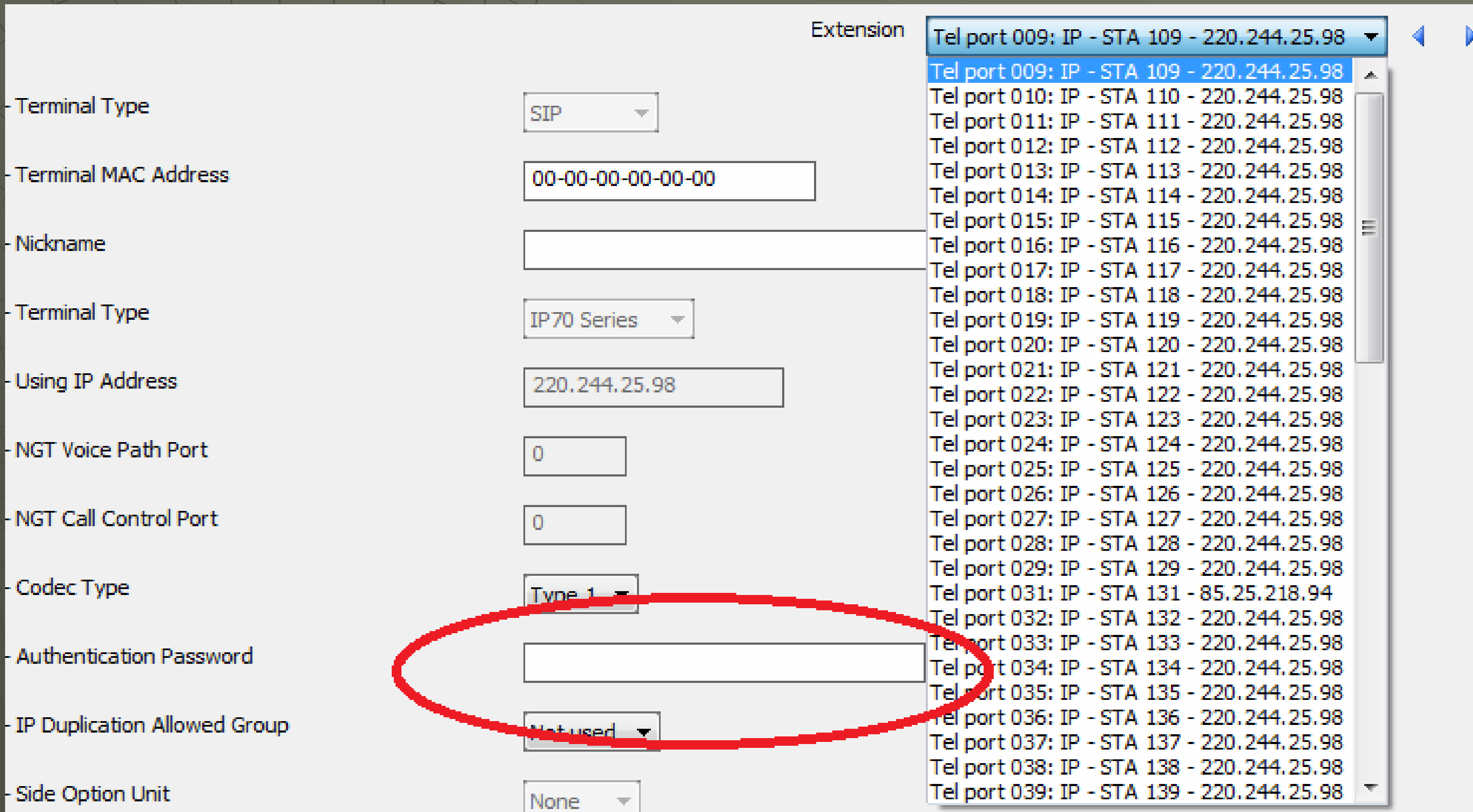
Call Quality

- 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 ..

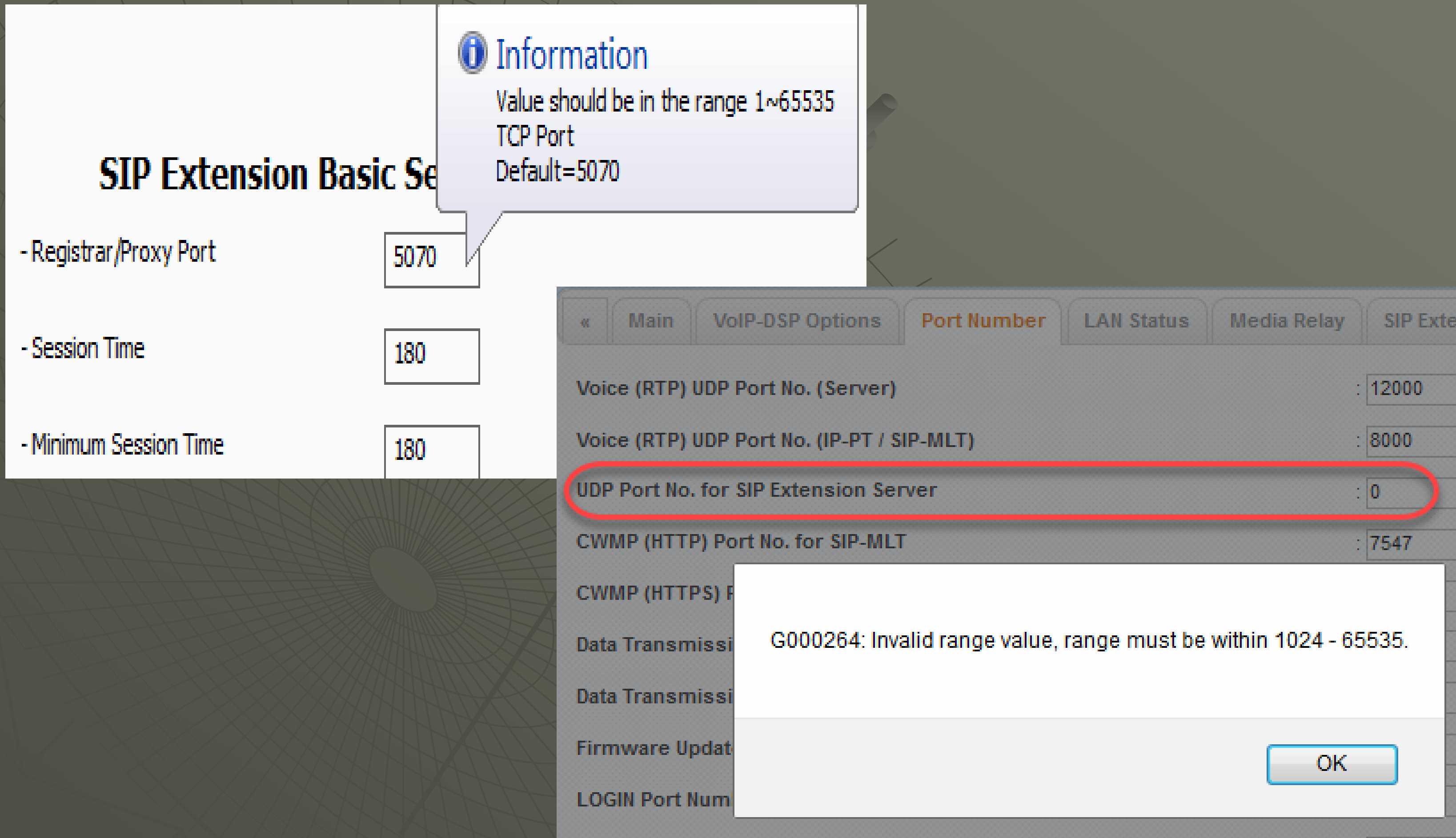
Toll Fraud

- 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



Register an account



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 KiB	21
drop	forward			17 (udp)		5060	ether1-gateway		0 B	0

Filter: sip Expression... Clear Apply Save

number	Time	Source	Destination	DSCP	Protocol	Info
713	1.414136	192.168.15	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....), Dst: 192.168.150.
User Datagram Protocol, Src Port: 4... (...70), Dst Port: 21222 (21222)
Session Initiation Protocol (404)
  Status-Line: SIP/2.0 404 Not Found
  Message Header
    From: "test-"<sip:123@59.100.2... >;tag=6e398b1e
    To: "test-"<sip:123@59.100.2...0>;tag=98063246313536414 21AE104
    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	Authentication Password
0733331234	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

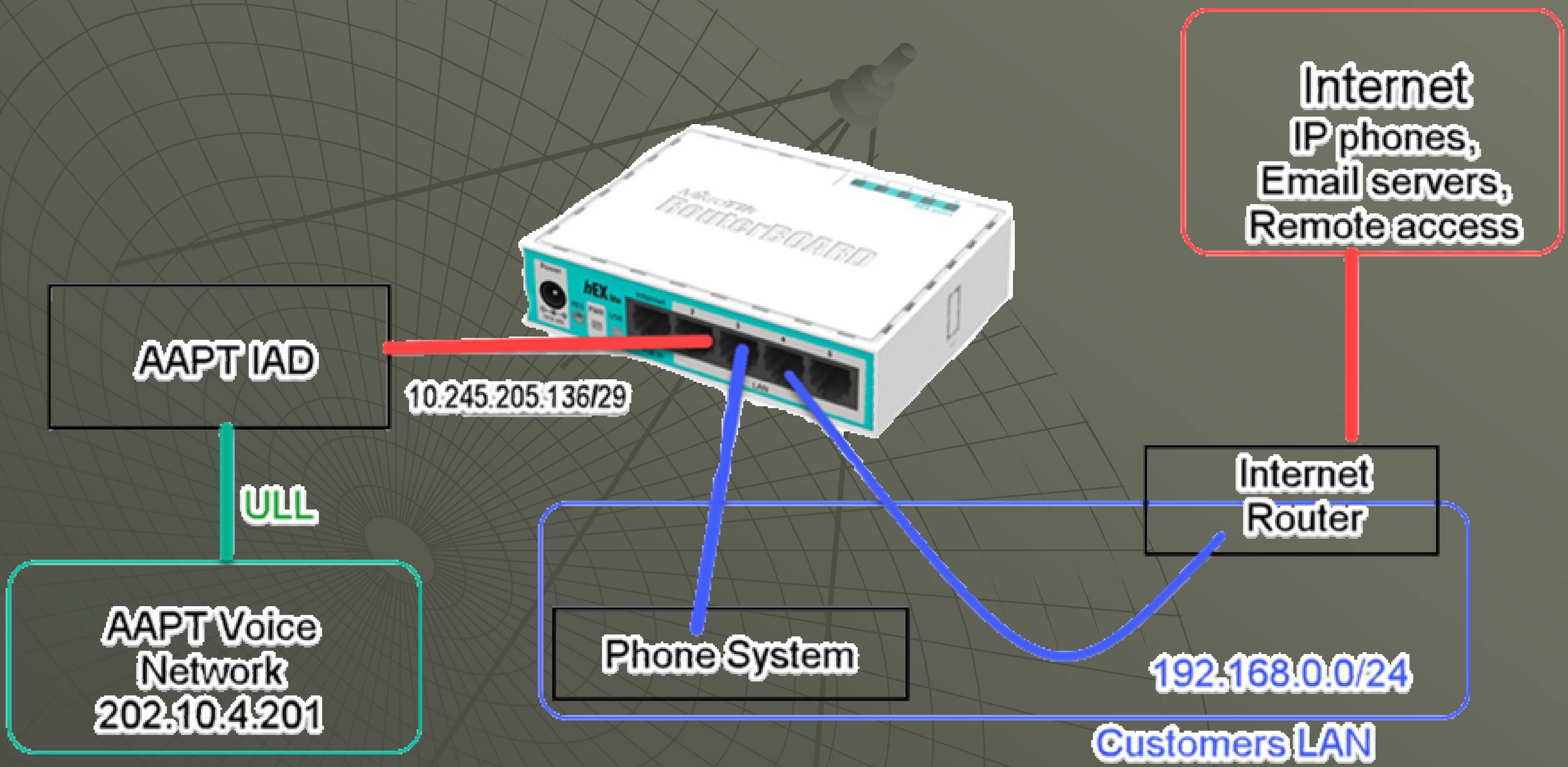
Not common but can be a consideration with higher end clients.

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

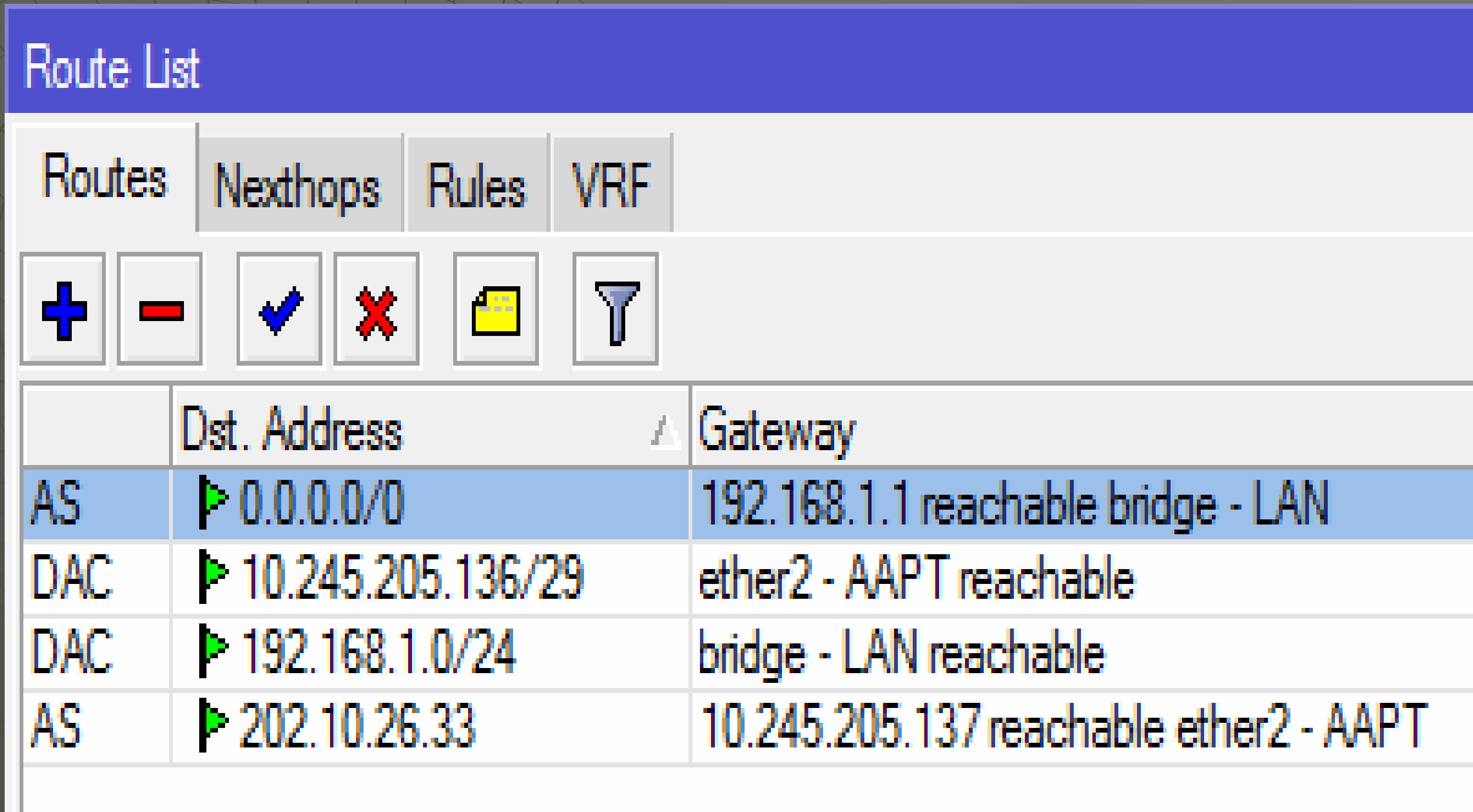
Internet or Non-Internet based VoIP service

	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.



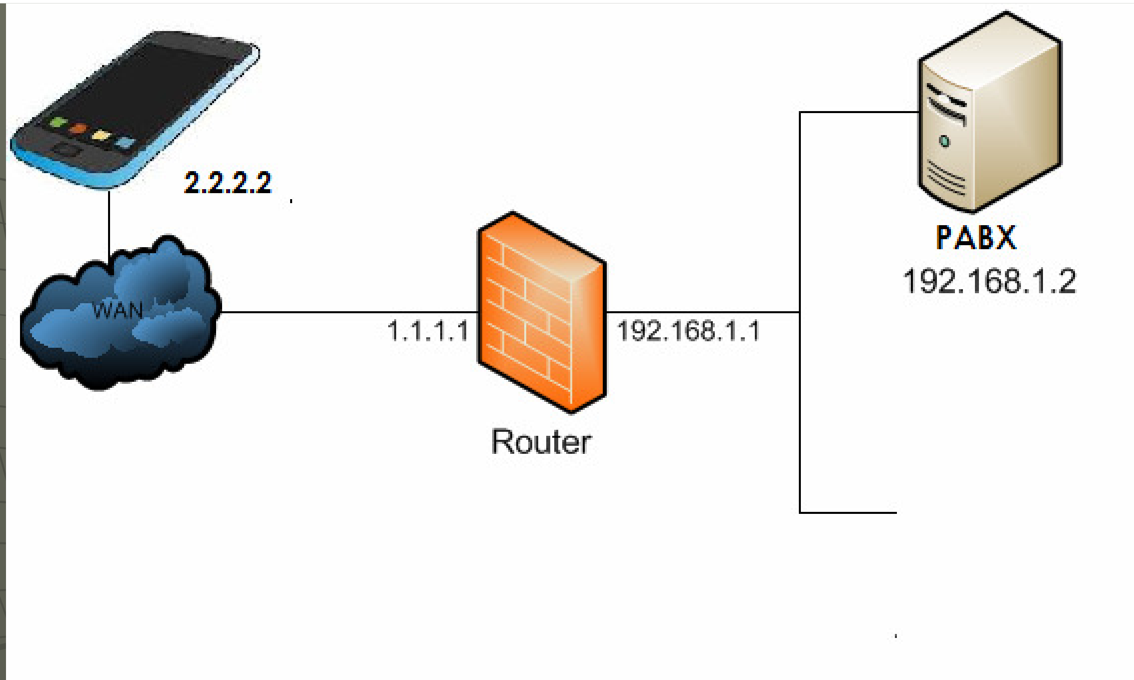
Carrier provided voice network

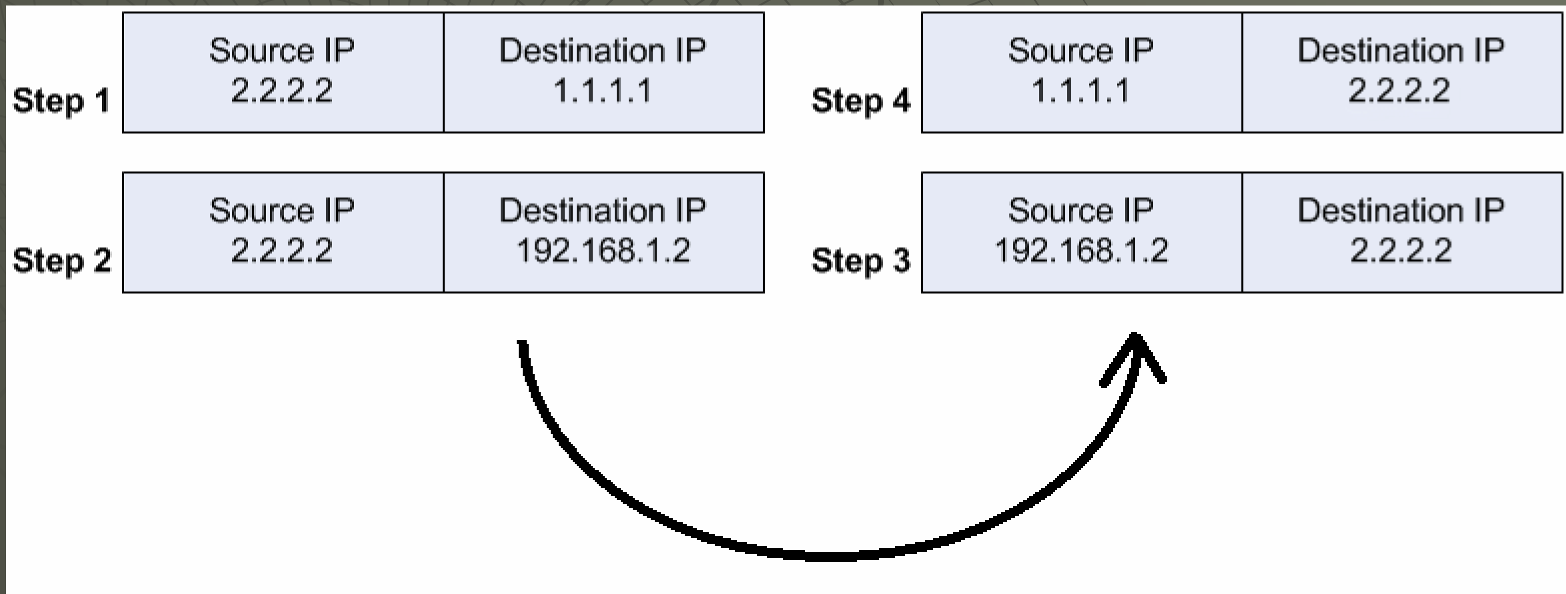


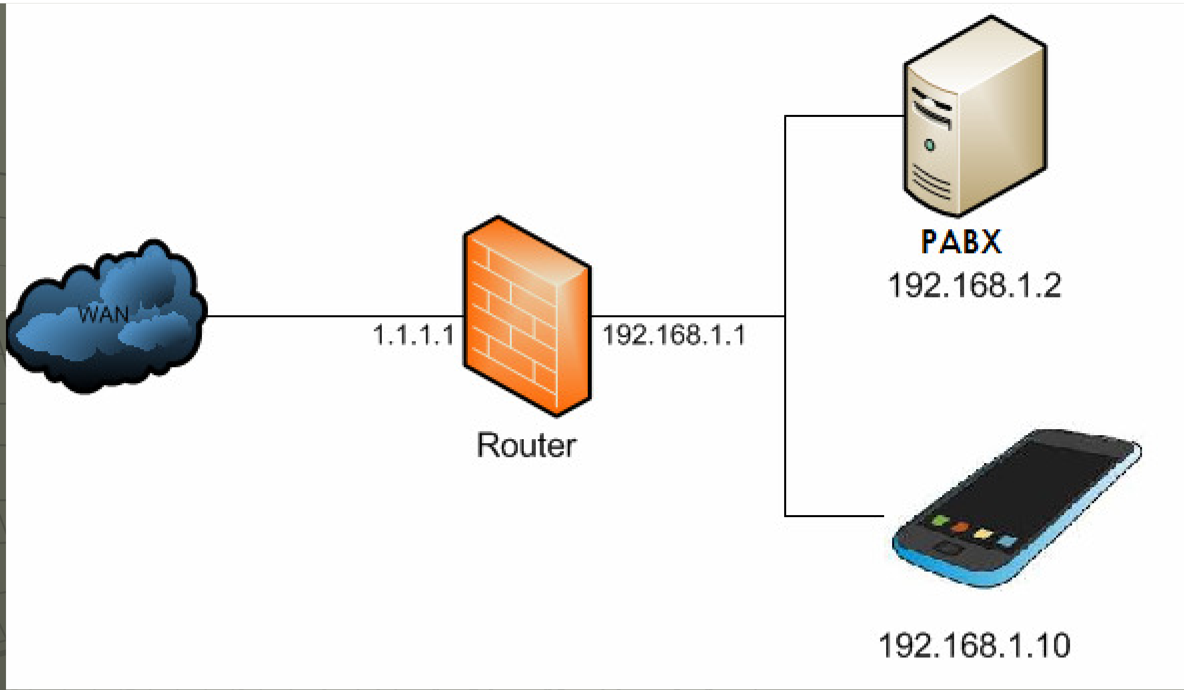
NAT Loop back / Hairpin

- 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


2.2.2.2
WAN
1.1.1.1
192.168.1.1
Router
PABX
192.168.1.2


Step 1
Source IP 2.2.2.2
Destination IP 1.1.1.1
Step 2
Source IP 2.2.2.2
Destination IP 192.168.1.2
Step 3
Source IP 192.168.1.2
Destination IP 2.2.2.2
Step 4
Source IP 1.1.1.1
Destination IP 2.2.2.2



Step 1

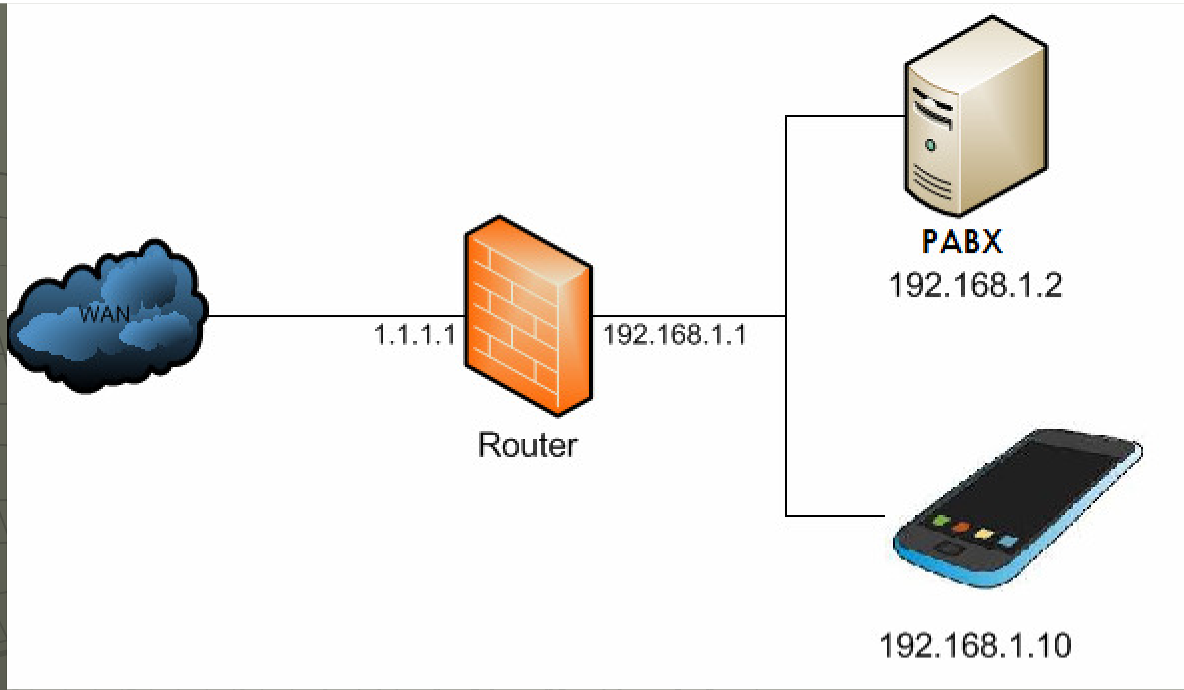
Source IP	Destination IP
192.168.1.10	1.1.1.1

Step 2

Source IP	Destination IP
192.168.1.10	192.168.1.2

Step 3

Source IP	Destination IP
192.168.1.2	192.168.1.10



Step 1

Source IP	Destination IP
192.168.1.10	1.1.1.1

Step 2

Source IP	Destination IP
192.168.1.10	192.168.1.2

Step 3

Source IP	Destination IP
192.168.1.2	192.168.1.1

Step 4

Source IP	Destination IP
1.1.1.1	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!