< 3G Networks>

Mikrotik Basics

Terms Used

- Layer X – When I refer to something being at layer X I'm referring to the OSI model.
- VLAN – 802.1Q Layer 2 marking on traffic used to segment sets of traffic. VLAN tags are applied on access ports.
- Trunk – I'm referring to an 802.1Q trunk port. This is a method to transmit frames across an L2 link with a VLAN tag intact.
- Outside/Inside – Outside refers to the interface connecting you to the Internet where as Inside refers to the interface connecting you to the LAN side of your router. I'll use these terms most often when talking about NAT.

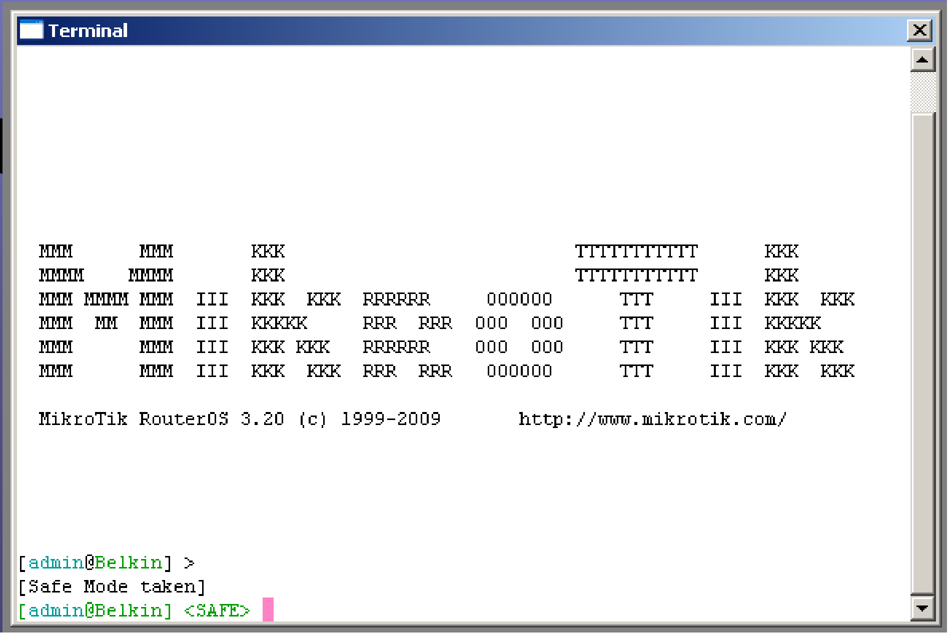
- NAT/PAT – Network Address Translation. This take a private address (RFC1918) and translates it to a publically routable IP. Port Address Translation is a method to translate multiple private addresses to a single public IP (masquerade).
- DHCP – Dynamic Host Configuration Protocol – Auto assign IP on hosts. TCP port 67.
- NTP – Network Time Protocol. Synchronizes your system time to an external time server.
- Bridging – Refers to layer 2 connectivity between multiple ports.

Connect To Router

- Serial connection – 9pin BD9 connector with speed set to 115200.
- Winbox – windows GUI tool. Can also run under wine or darWine for Macs.
- SSH
- Telnet
- MAC Telnet – Must be on same L2 segment.

Safe Mode

- Your best friend…and occasionally, worst nightmare. New Terminal -> Ctrl-X to enable and Ctrl-X to release.
- To save changes, you must release safe mode. If you simply close Winbox without releasing, you will lose all changes!



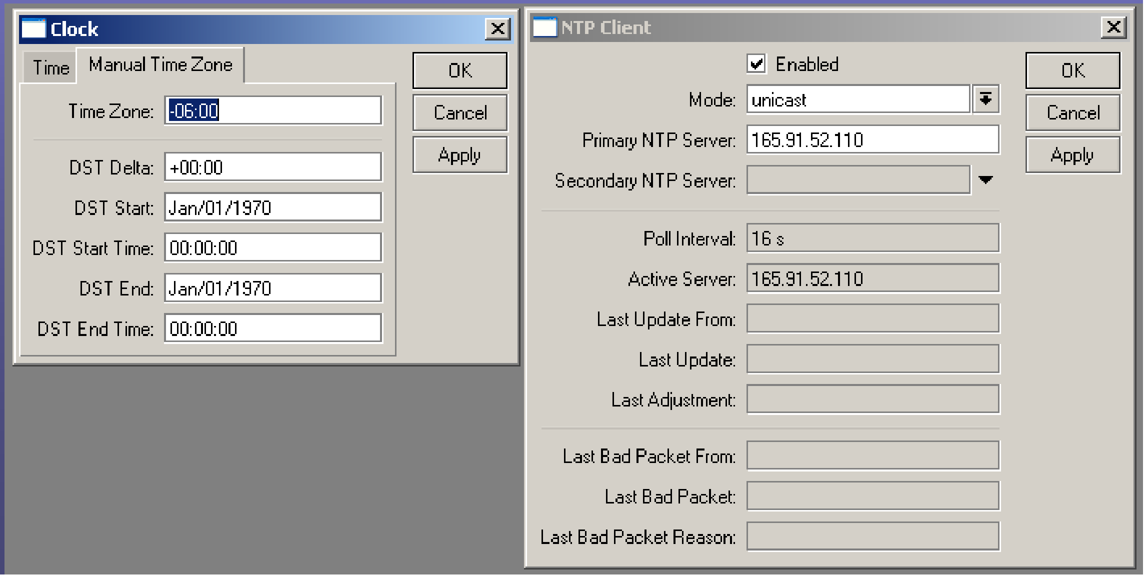
```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 3.20 (c) 1999-2009       http://www.mikrotik.com/


[admin@Belkin] >
[Safe Mode taken]
[admin@Belkin] <SAFE>
```

System -> NTP Client and System -> Clock

- Clock, set your time zone.
- NTP Client, enable choose mode unicast and put in your servers.
- NTP Servers – http://www.pool.ntp.org/en/

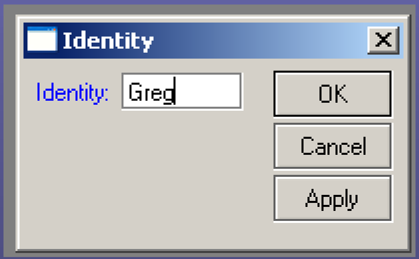


Time Zone: -06:00
DST Delta: +00:00
DST Start: Jan/01/1970
DST Start Time: 00:00:00
DST End: Jan/01/1970
DST End Time: 00:00:00

☑ Enabled
Mode: unicast
Primary NTP Server: 165.91.52.110
Secondary NTP Server:
Poll Interval: 16 s
Active Server: 165.91.52.110
Last Update From:
Last Update:
Last Adjustment:
Last Bad Packet From:
Last Bad Packet:
Last Bad Packet Reason:

System Identity

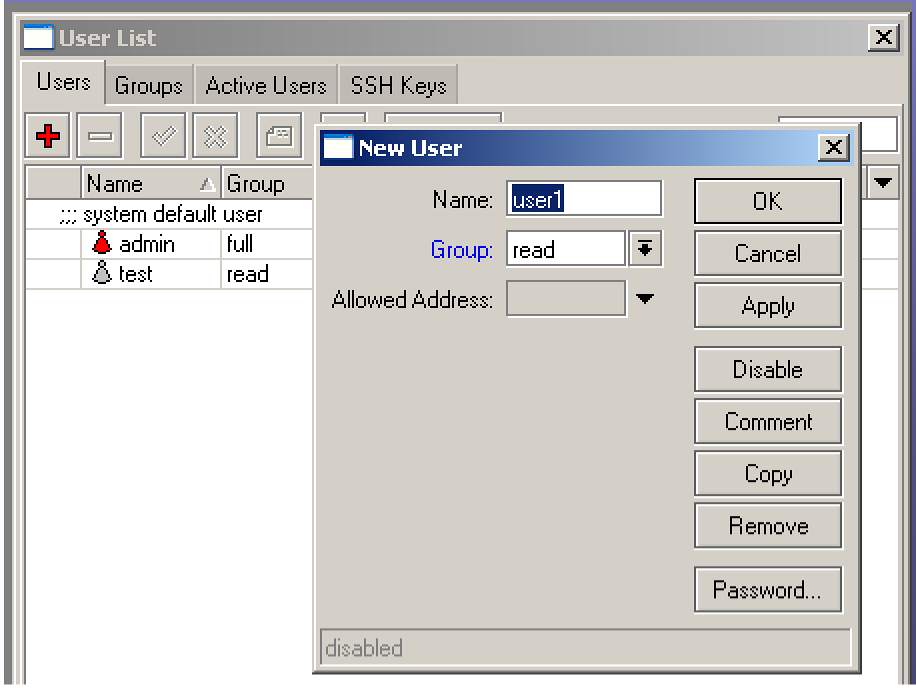
- Name the router. This is more of a convenience.
- When connecting to another AP your router will register as the Identity name.



Identity: Greg

System -> Users

- Users are assigned to groups.
- Groups specify what access you get.
- User section allows password changes.



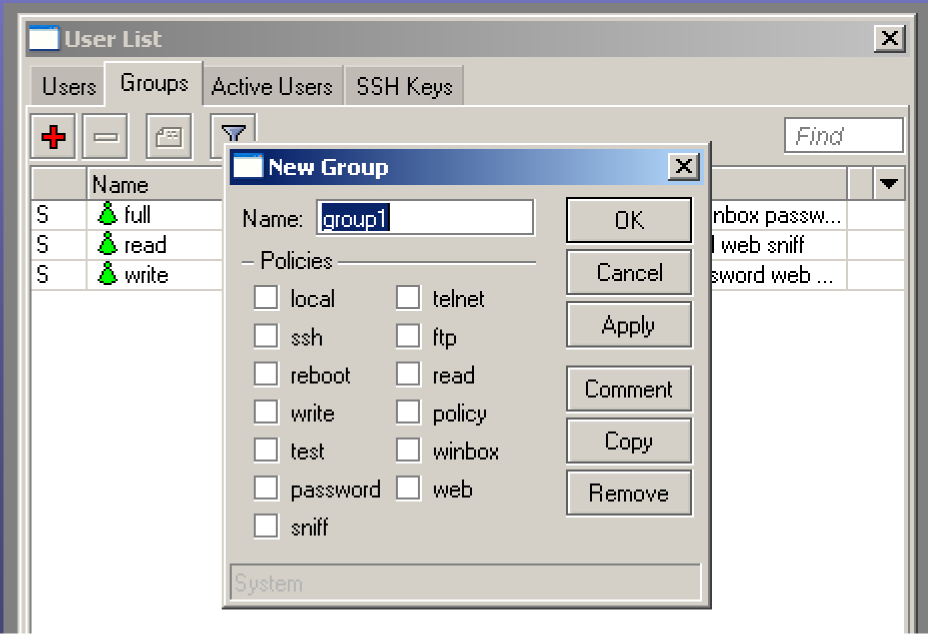
	Name	Group
	;;; system default user	
	admin	full
	test	read

Name: user1

Group: read

Allowed Address:

disabled



	Name	
S	full	nbox passw...
S	read	l web sniff
S	write	sword web ...

Name: group1

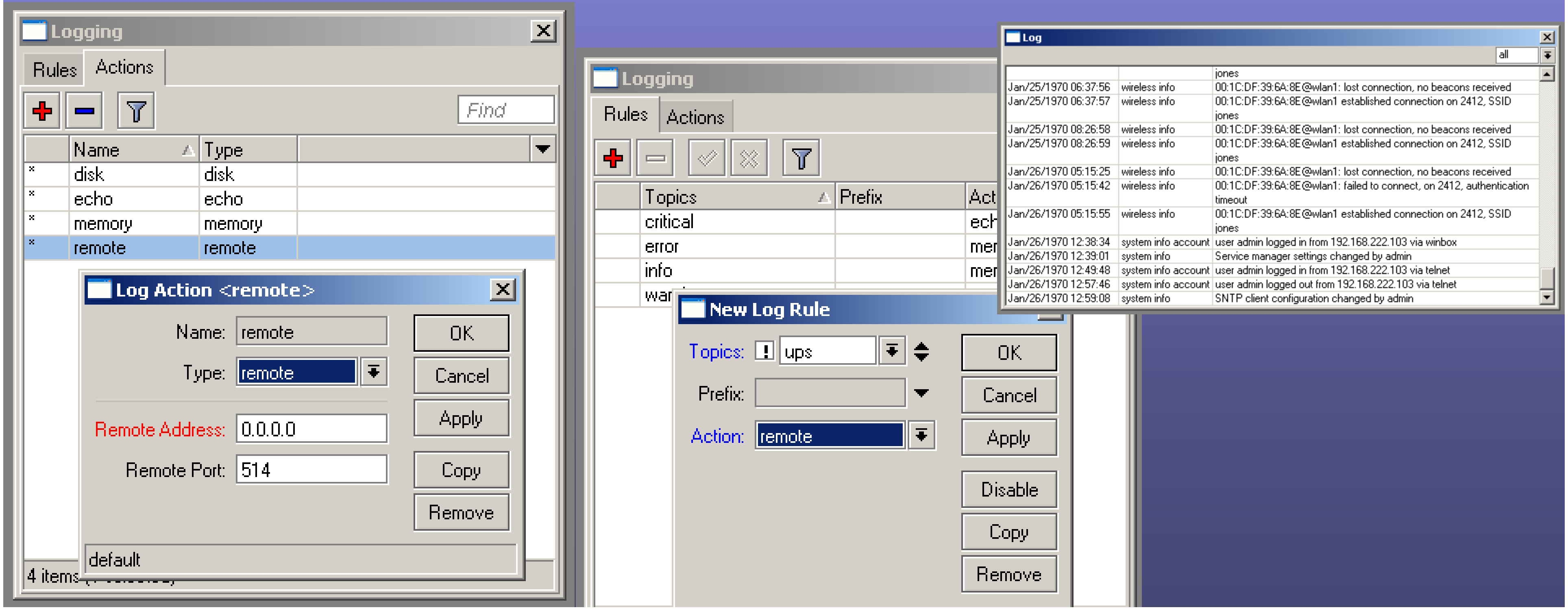
Policies

□ local □ telnet
□ ssh □ ftp
□ reboot □ read
□ write □ policy
□ test □ winbox
□ password □ web
□ sniff

System

System -> Logging and Log

- Setup special actions to get more detail on a specific subject.
- Send to syslog server (CactiEZ).



Name	Type
disk	disk
echo	echo
memory	memory
remote	remote

4 items

Log Action <remote>

Name: remote

Type: remote

Remote Address: 0.0.0.0

Remote Port: 514

default

Topics	Prefix	Act
critical		ech
error		mer
info		mer
war		

New Log Rule

Topics: ! ups

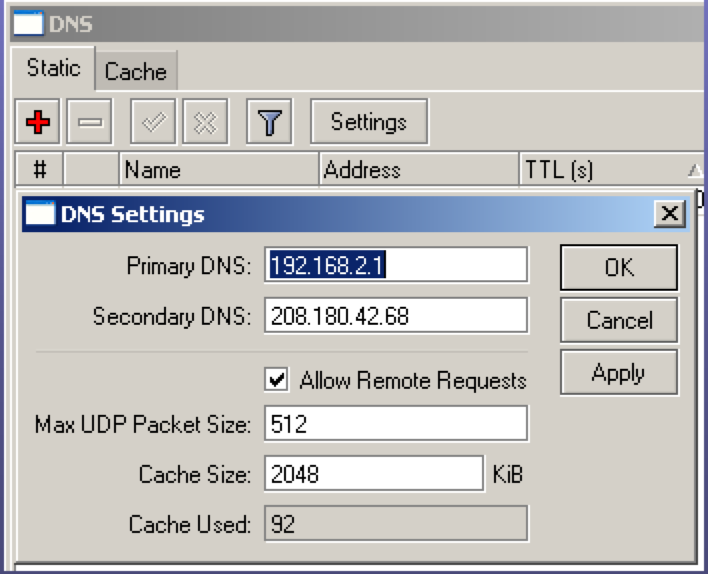
Prefix:

Action: remote

```
                                          jones
Jan/25/1970 06:37:56  wireless info       00:1C:DF:39:6A:8E@wlan1: lost connection, no beacons received
Jan/25/1970 06:37:57  wireless info       00:1C:DF:39:6A:8E@wlan1 established connection on 2412, SSID
                                          jones
Jan/25/1970 08:26:58  wireless info       00:1C:DF:39:6A:8E@wlan1: lost connection, no beacons received
Jan/25/1970 08:26:59  wireless info       00:1C:DF:39:6A:8E@wlan1 established connection on 2412, SSID
                                          jones
Jan/26/1970 05:15:25  wireless info       00:1C:DF:39:6A:8E@wlan1: lost connection, no beacons received
Jan/26/1970 05:15:42  wireless info       00:1C:DF:39:6A:8E@wlan1: failed to connect, on 2412, authentication
                                          timeout
Jan/26/1970 05:15:55  wireless info       00:1C:DF:39:6A:8E@wlan1 established connection on 2412, SSID
                                          jones
Jan/26/1970 12:38:34  system info account user admin logged in from 192.168.222.103 via winbox
Jan/26/1970 12:39:01  system info         Service manager settings changed by admin
Jan/26/1970 12:49:48  system info account user admin logged in from 192.168.222.103 via telnet
Jan/26/1970 12:57:46  system info account user admin logged out from 192.168.222.103 via telnet
Jan/26/1970 12:59:08  system info         SNTP client configuration changed by admin
```

DNS Server

- To speed up DNS requests for your network, you can enable DNS caching on your MTK.
- IP -> DNS, then click settings. Check allow remote requests.



Primary DNS: 192.168.2.1

Secondary DNS: 208.180.42.68

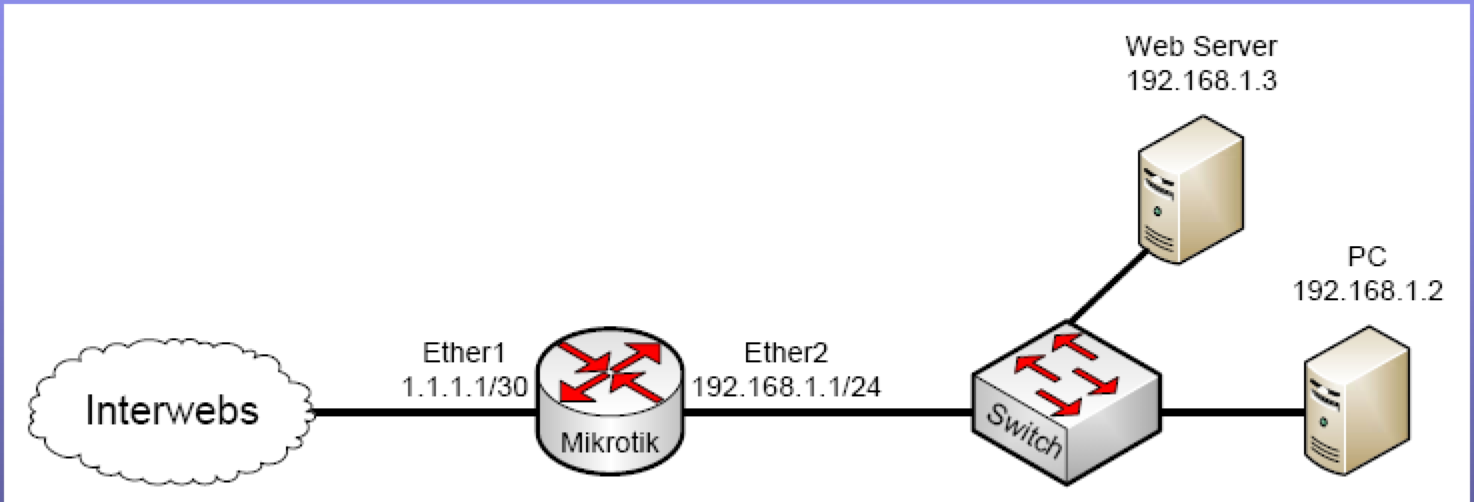
☑ Allow Remote Requests

Max UDP Packet Size: 512

Cache Size: 2048 KiB

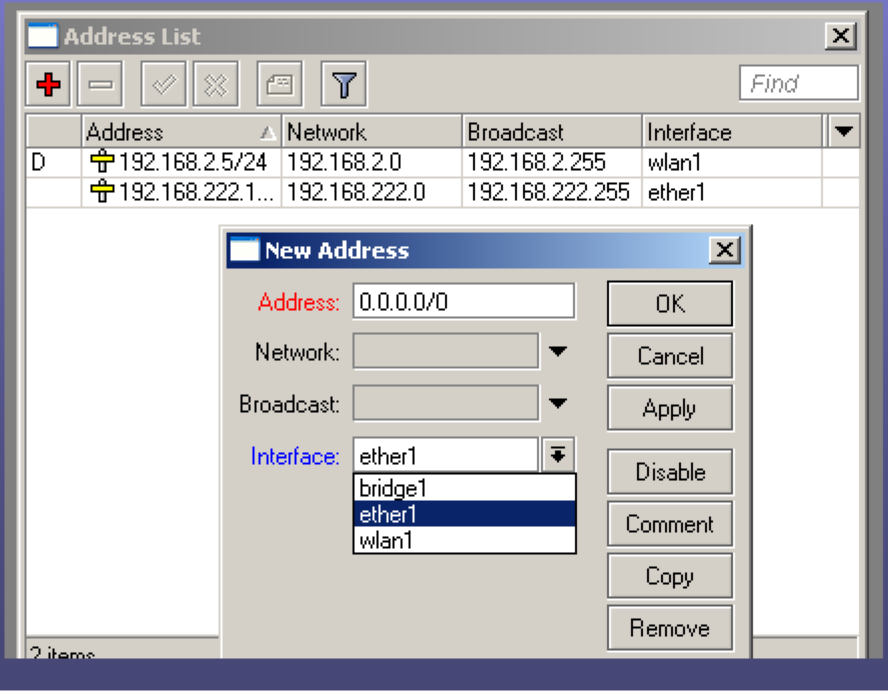
Cache Used: 92

Basic Diagram



IP - Addresses

- This is where we add our addresses. A quick tip is to add your address with the mask in the address field. This will auto populate the Network and Broadcast section.



	Address	Network	Broadcast	Interface
D	192.168.2.5/24	192.168.2.0	192.168.2.255	wlan1
	192.168.222.1...	192.168.222.0	192.168.222.255	ether1

2 items

Address: 0.0.0.0/0

Network:

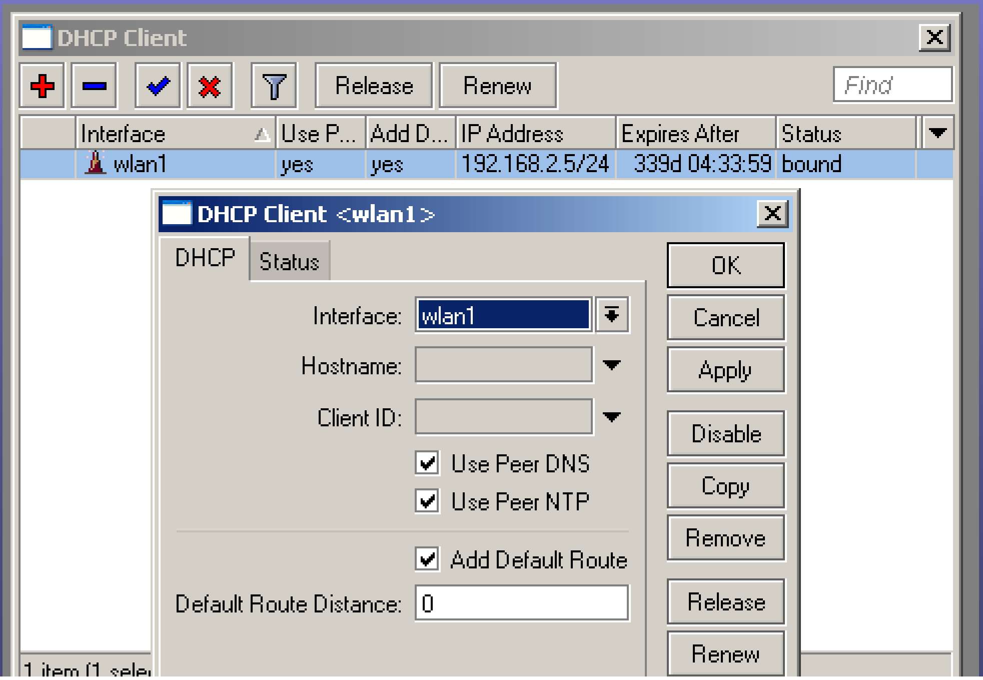
Broadcast:

Interface: ether1

bridge1
ether1
wlan1

IP -> DHCP Client

- This allows us to set one of the interfaces as a DHCP client. You can choose to accept DNS, NTP and Default route.



DHCP Client

Interface	Use P...	Add D...	IP Address	Expires After	Status
wlan1	yes	yes	192.168.2.5/24	339d 04:33:59	bound

1 item (1 sele

DHCP Client <wlan1>

Interface: wlan1

Hostname:

Client ID:

☑ Use Peer DNS

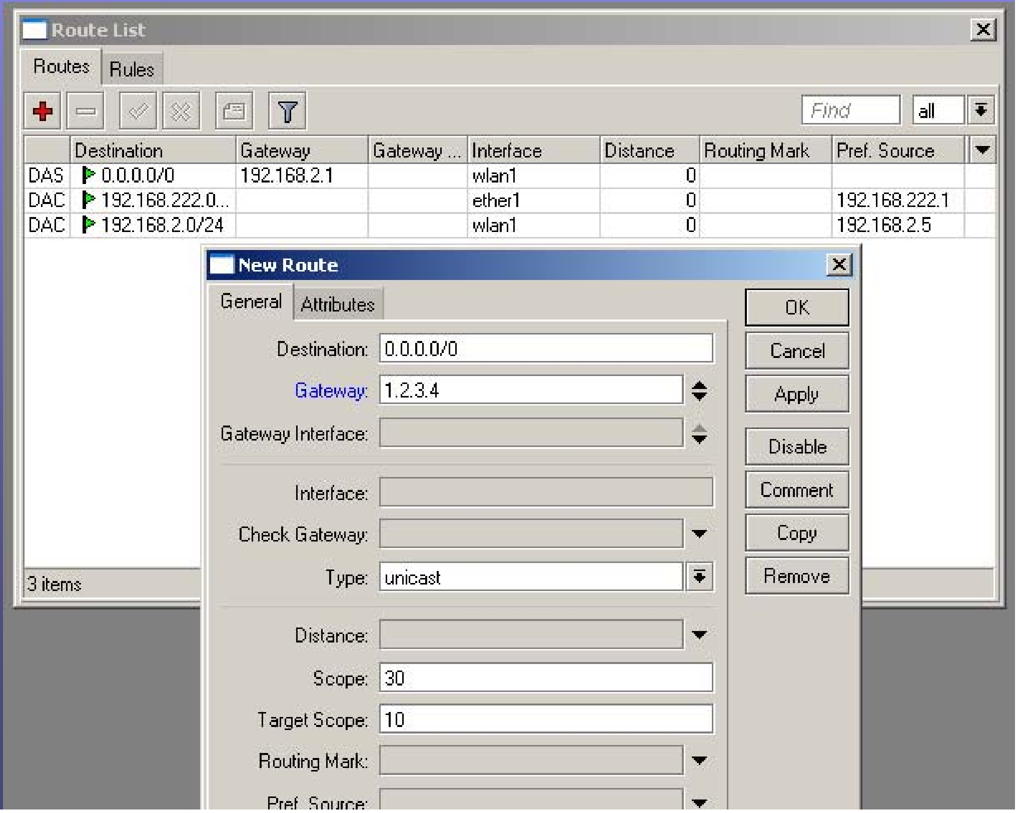
☑ Use Peer NTP

☑ Add Default Route

Default Route Distance: 0

IP -> Routes

- This is where you add your static routes.
- Default route is 0.0.0.0/0 with a gateway of you next hop.



	Destination	Gateway	Gateway ...	Interface	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	192.168.2.1		wlan1	0		
DAC	192.168.222.0...			ether1	0		192.168.222.1
DAC	192.168.2.0/24			wlan1	0		192.168.2.5

3 items

Destination: 0.0.0.0/0

Gateway: 1.2.3.4

Gateway Interface:

Interface:

Check Gateway:

Type: unicast

Distance:

Scope: 30

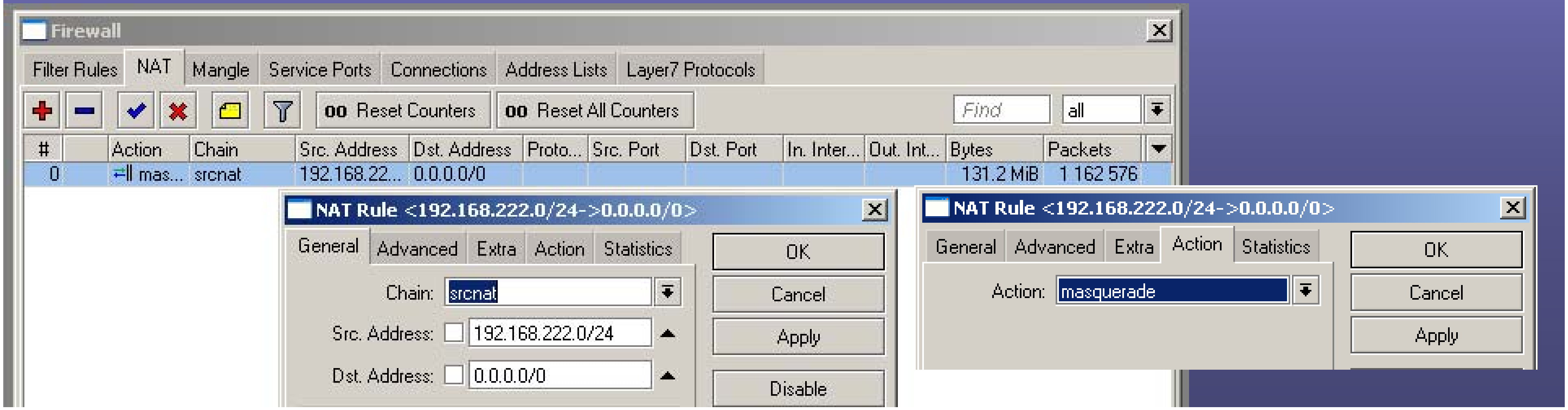
Target Scope: 10

Routing Mark:

Pref. Source:

IP -> Firewall then NAT

- A typical SOHO setup will do PAT. MTK calls PAT Masquerade. We create a source NAT rule with source as our inside range and outside range as any. Our action is set to Masquerade.



#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0		mas...	srcnat	192.168.22...	0.0.0.0/0						131.2 MiB	1 162 576

NAT Rule <192.168.222.0/24->0.0.0.0/0>

Chain: srcnat

Src. Address: □ 192.168.222.0/24

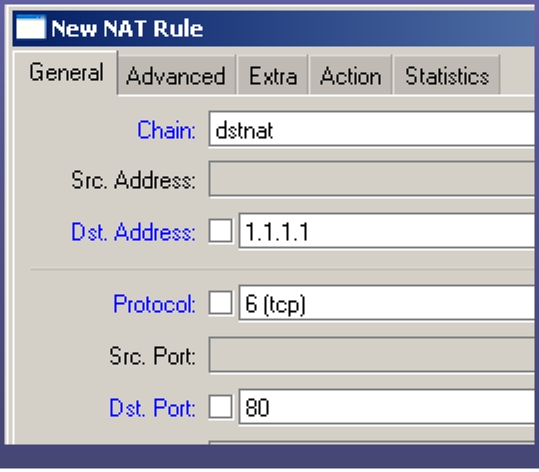
Dst. Address: □ 0.0.0.0/0

NAT Rule <192.168.222.0/24->0.0.0.0/0>

Action: masquerade

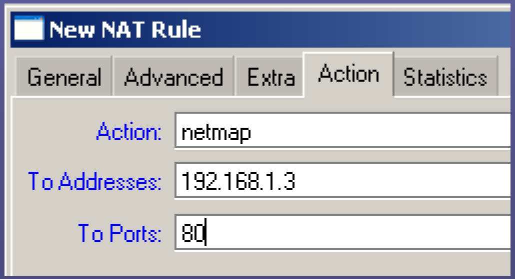
NATing specific ports or “Port Forwarding”

- The below example shows using the public IP on the outside interface and nating that to our webserver on the inside.
- I specify anyone going to the public IP destined for port 80 on chain dstnat.
- We then specify action of netmap and specify the inside IP of the webserver going to port 80.



New NAT Rule

Chain: dstnat
Src. Address:
Dst. Address: □ 1.1.1.1
Protocol: □ 6 (tcp)
Src. Port:
Dst. Port: □ 80

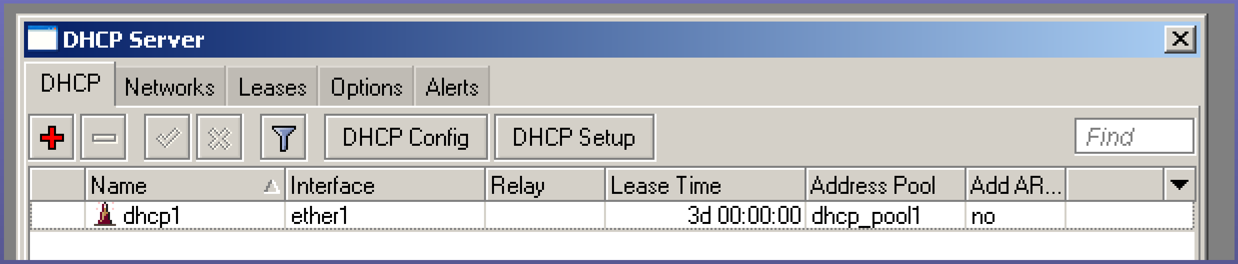


New NAT Rule

Action: netmap
To Addresses: 192.168.1.3
To Ports: 80

DHCP Server

- DHCP Setup is your friend. This will guide you wizard style to setup your network, pool and associated interface.



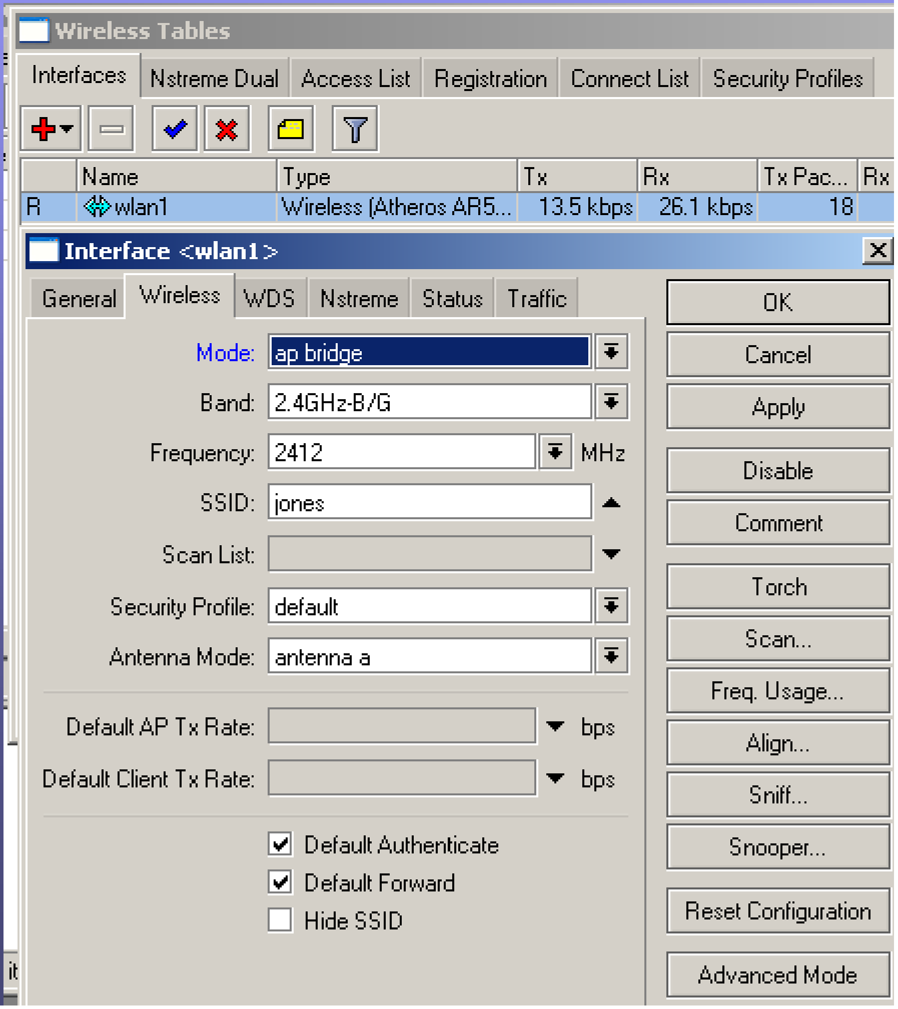
Name	Interface	Relay	Lease Time	Address Pool	Add AR...
dhcp1	ether1		3d 00:00:00	dhcp_pool1	no

Wireless Modes

- AP-Bridge – This will be your standard access point mode.
- Bridge – This will allow only a single client to connect, but will turn the link into a straight bridge connection.
- Station – This is where your MTK acts as a client and connects to an AP. In station mode you can't act as a straight bridge.
- Station-wds – This allows you to connect to an AP that is in WDS mode. This will allow you to do a straight bridge with multiple clients.
- There are more, but these are beyond the scope of this class.

Wireless AP-Bridge Mode

- Set mode to AP Bridge.
- You can adjust band, SSID and Security Profile.



	Name	Type	Tx	Rx	Tx Pac...	Rx
R	wlan1	Wireless (Atheros AR5...	13.5 kbps	26.1 kbps	18	

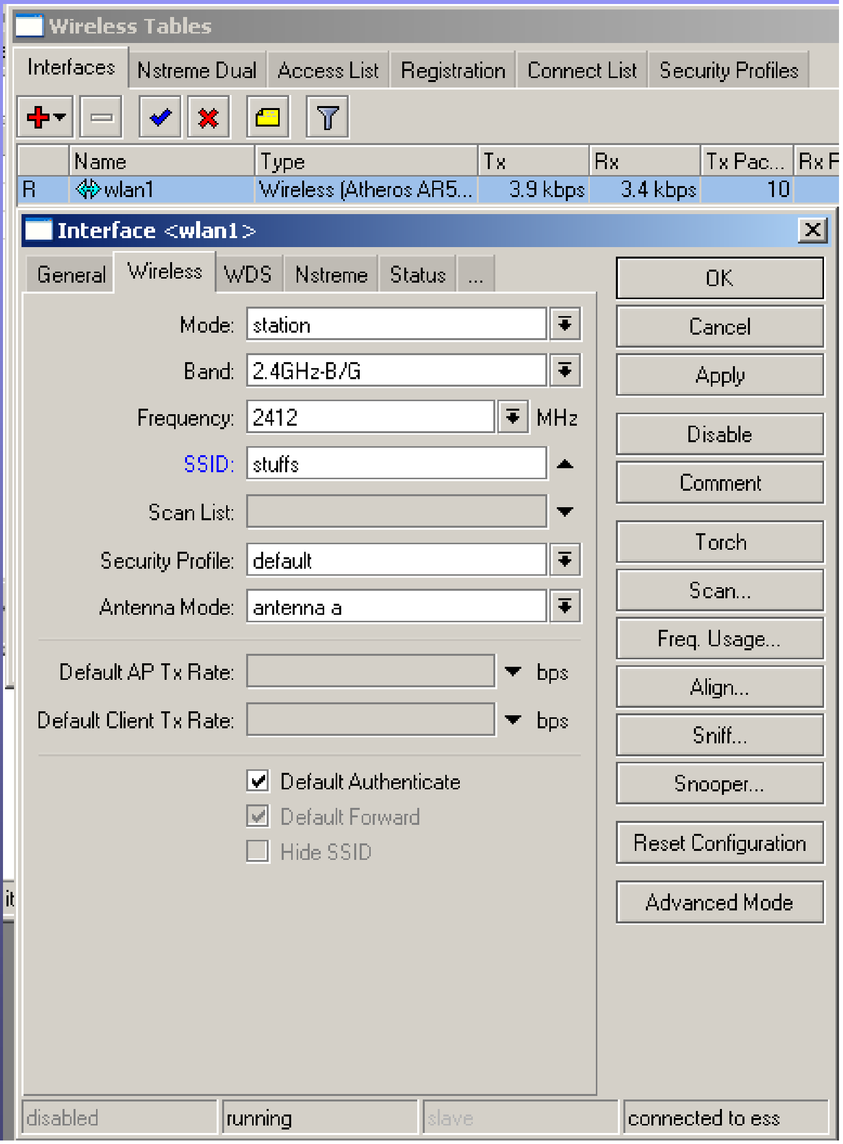
Mode: ap bridge
Band: 2.4GHz-B/G
Frequency: 2412 MHz
SSID: jones
Scan List:
Security Profile: default
Antenna Mode: antenna a

Default AP Tx Rate: bps
Default Client Tx Rate: bps

☑ Default Authenticate
☑ Default Forward
☐ Hide SSID

Wireless Station Mode

- Set mode to station and set your SSID to that of the AP you want to connect to.
- To quick find an open AP to connect to, click scan.
- Notice at the bottom once connected you get “connected to ess”.



Wireless Tables

	Name	Type	Tx	Rx	Tx Pac...	Rx P
R	wlan1	Wireless (Atheros AR5...	3.9 kbps	3.4 kbps	10	

Interface <wlan1>

Mode: station

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: stuffs

Scan List:

Security Profile: default

Antenna Mode: antenna a

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☑ Default Authenticate

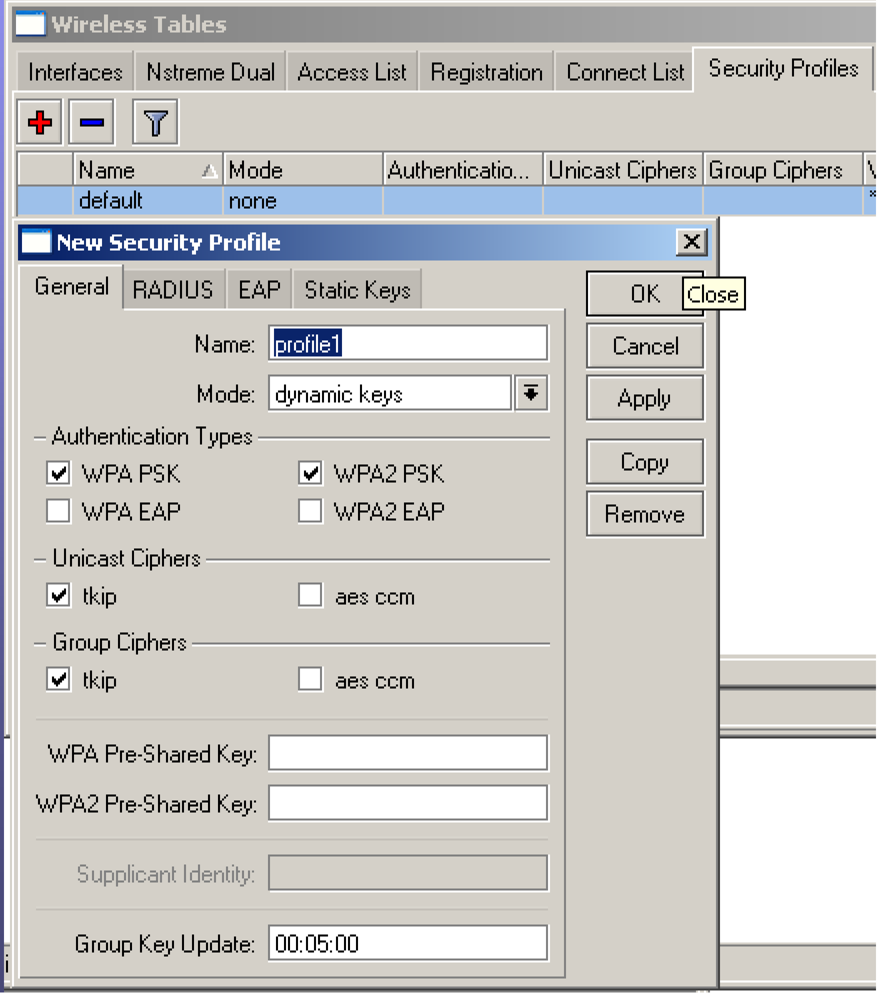
☑ Default Forward

☐ Hide SSID

disabled | running | slave | connected to ess

Wireless Security Profile

- The security profiles allow you to setup what kind of encryption your AP or station uses.



Name	Mode	Authenticatio...	Unicast Ciphers	Group Ciphers
default	none			

Name: profile1

Mode: dynamic keys

Authentication Types

☑ WPA PSK ☑ WPA2 PSK

□ WPA EAP □ WPA2 EAP

Unicast Ciphers

☑ tkip □ aes ccm

Group Ciphers

☑ tkip □ aes ccm

WPA Pre-Shared Key:

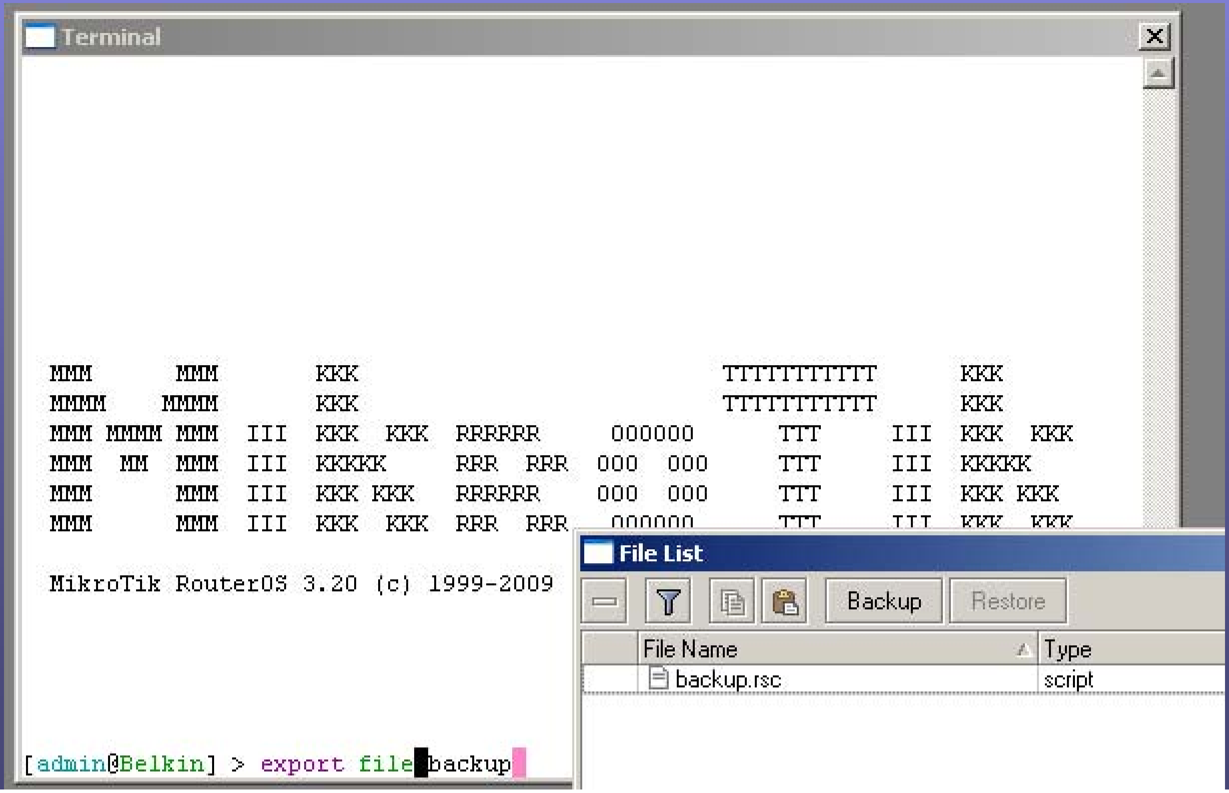
WPA2 Pre-Shared Key:

Supplicant Identity:

Group Key Update: 00:05:00

Backup Your Config

- From the terminal type “export file filename”. This creates a plaintext config file in flash. Drag and drop or FTP the file off.



```
MMM      MMM       KKK                          TTTTTTTTTTT      KKK
MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

MikroTik RouterOS 3.20 (c) 1999-2009


[admin@Belkin] > export file backup
```

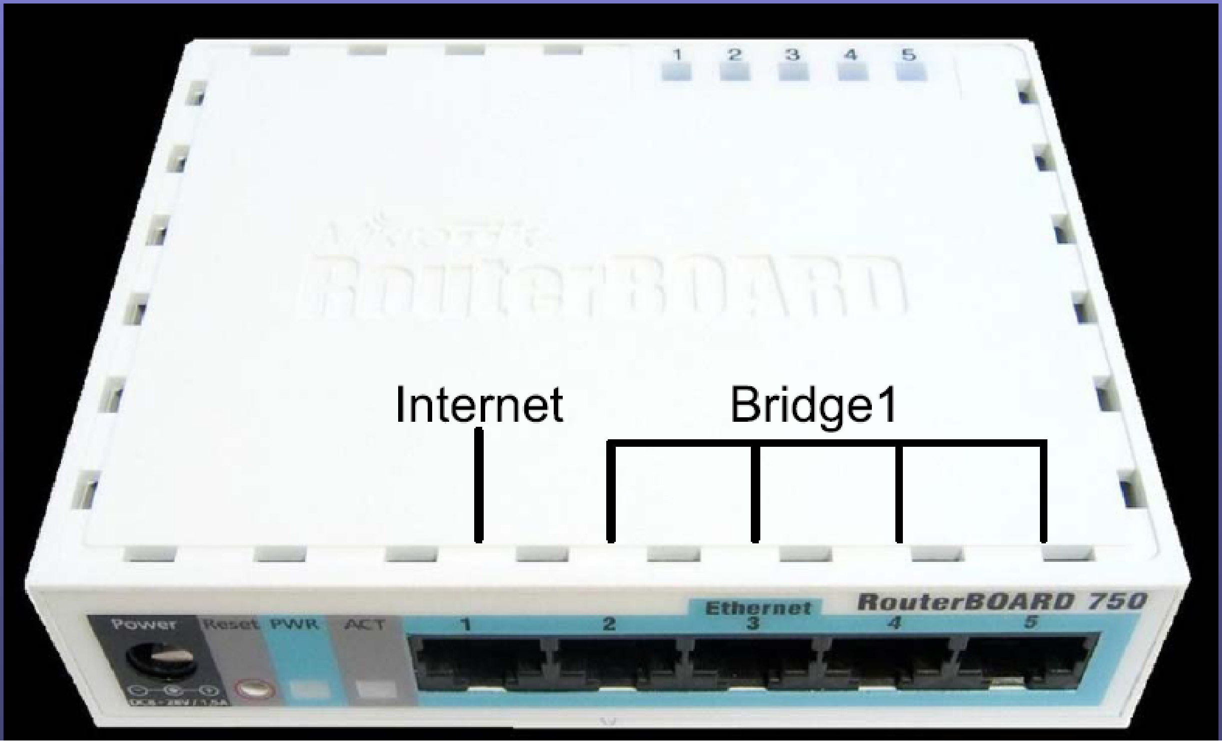
File Name	Type
backup.rsc	script

Upgrade The OS

- Download the combined package for your version of hardware from Mikrotik.com.
- Drag and drop the NPK file into the file window in Winbox.
- Reboot the router from system -> reboot. If you just kill power, the router won’t upgrade. After the reboot, the router will update the package. For a video tutorial see http://gregsowell.com/?p=700

Bridging Interfaces

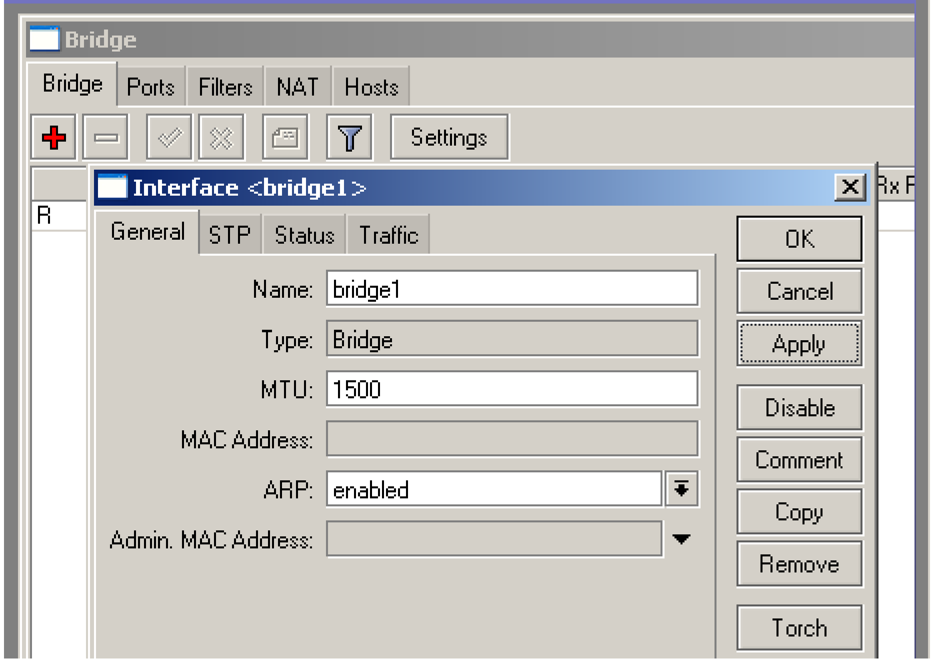
- For a 5 port RB, it is common to have a single internet interface and bridge the remaining interfaces together.
- An IP will be assigned to the Bridge interface.



GregSowell.com

Bridging Configuration

- Create the bridge
- Add ports to the bridge.



Name: bridge1

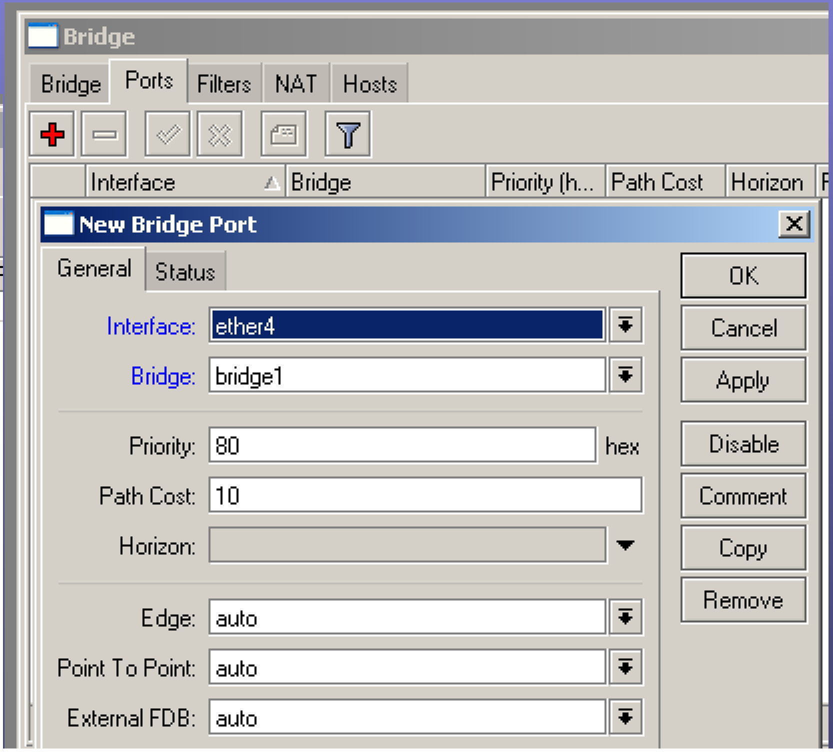
Type: Bridge

MTU: 1500

MAC Address:

ARP: enabled

Admin. MAC Address:



Interface: ether4

Bridge: bridge1

Priority: 80 hex

Path Cost: 10

Horizon:

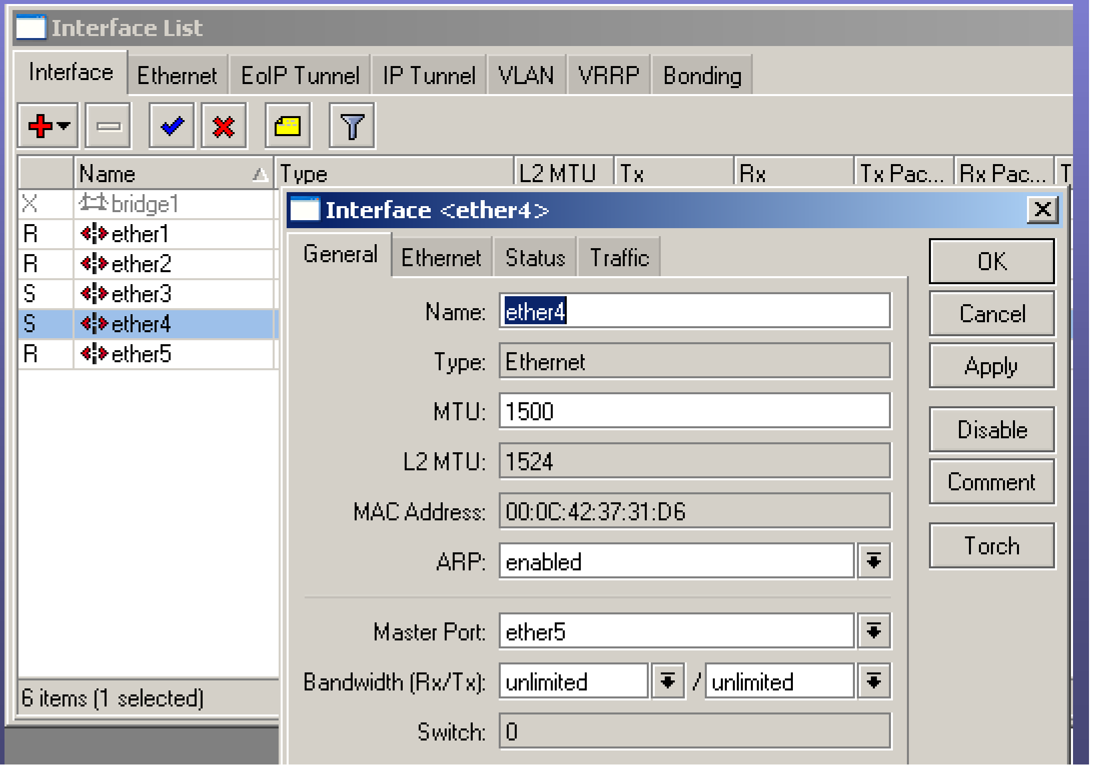
Edge: auto

Point To Point: auto

External FDB: auto

Switch Interfaces – Supported Routers

- Supported routers will be 150, 450, 450G and 750. This is the preferred method as all the switching is done in hardware and more efficient.
- Choose a port to be the master port that all other “switched” ports will slave off of. In the below example I’m using port 5 as the master.
- The master port can be given an IP or used in the normal way.
- Slave ports specify which port is to be the master. Slave ports show the S.

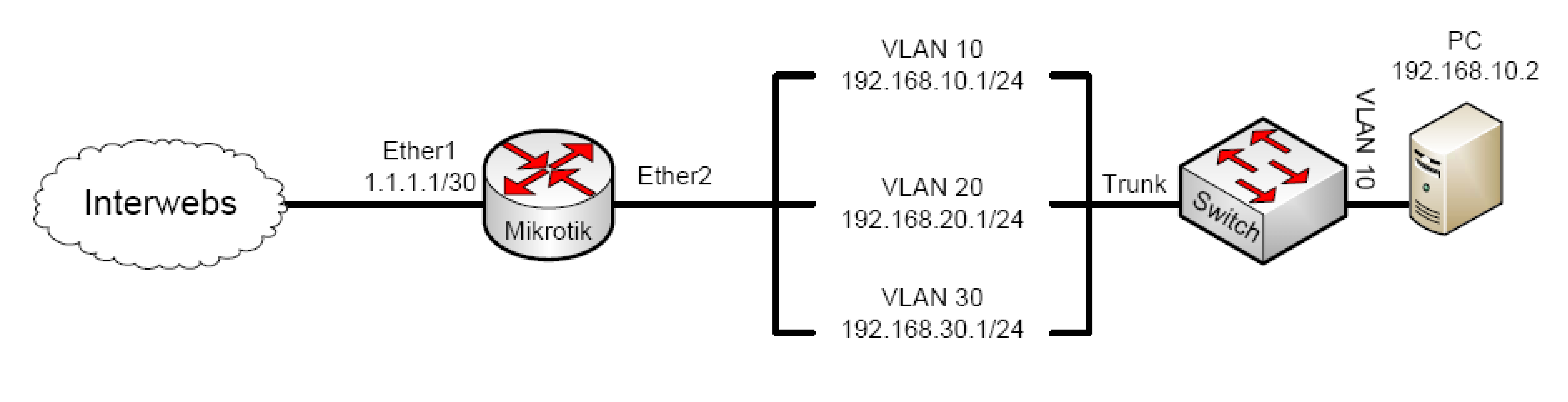


	Name	Type	L2 MTU	Tx	Rx	Tx Pac...	Rx Pac...	T
X	bridge1							
R	ether1							
R	ether2							
S	ether3							
S	ether4							
R	ether5							

6 items (1 selected)

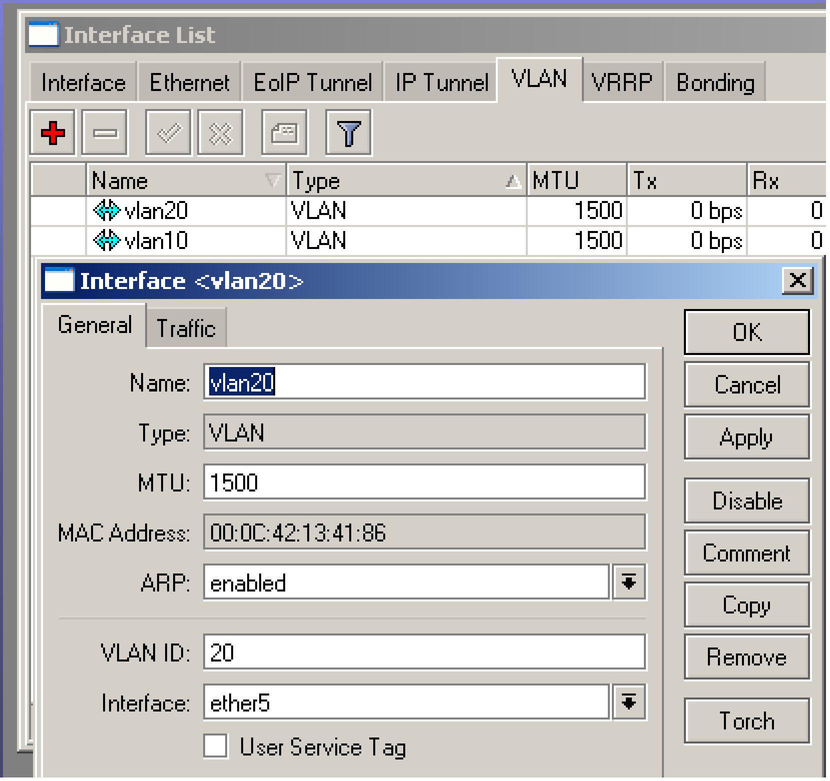
Name: ether4
Type: Ethernet
MTU: 1500
L2 MTU: 1524
MAC Address: 00:0C:42:37:31:D6
ARP: enabled
Master Port: ether5
Bandwidth (Rx/Tx): unlimited / unlimited
Switch: 0

Trunking Design



802.1Q Trunking

- We can trunk to another MTK or a switch setup for trunking simply by creating VLAN interfaces on the physical interface that connects the equipment



Name	Type	MTU	Tx	Rx
vlan20	VLAN	1500	0 bps	0
vlan10	VLAN	1500	0 bps	0

Interface <vlan20>

Name: vlan20

Type: VLAN

MTU: 1500

MAC Address: 00:0C:42:13:41:86

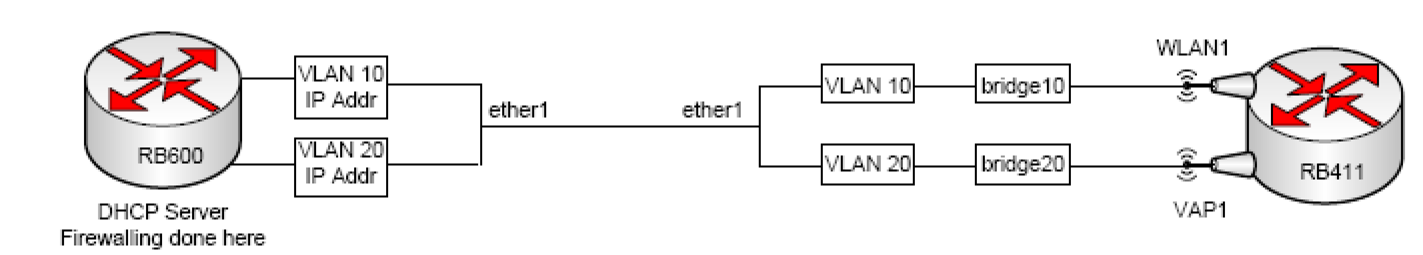
ARP: enabled

VLAN ID: 20

Interface: ether5

□ User Service Tag

Wireless VLAN Design



Tools

- Ping – Test network connectivity with ICMP. Test VPN tunnel connectivity.
- Traceroute – Trace path via ICMP.
- Torch – Much like TCPDump. Shows in/out packet flow.
- IP Scan – Scan a subnet with ICMP.
- Bandwidth Test – Client/Server – runs an application between two MTKs or an MTK and a windows machine to test throughput between the links. Caution, may saturate a link and causes high CPU utilization.
- Telnet – Allows you to telnet/ssh into any machine capable of such actions. MAC telnet can connect you from one MTK to another if they are connected via the same L2 segment, even if they don’t have IPs that are in the same subnet.

Resources

- Awesome Site – http://GregSowell.com
- Mikrotik Video Tutorials - http://gregsowell.com/?page_id=304
- Mikrotik Support Docs- http://www.mikrotik.com/testdocs/ros/3.0/
- CactiEZ - http://cactiez.cactiusers.org/download/
- Cacti Video Tutorials - http://gregsowell.com/?page_id=86
- Great Consultant ;)- http://gregsowell.com/?page_id=245