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 takes 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!
System -> NTP Client and System -> Clock

- Clock, set your time zone.
- NTP Client, enable choose mode unicast and put in your servers.
System Identity

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

- Users are assigned to groups.
- Groups specify what access you get.
- User section allows password changes.
System -> Logging and Log

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

Interwebs

Ether1
1.1.1.1/30

Ether2
192.168.1.1/24

Mikrotik

Switch

Web Server
192.168.1.3

PC
192.168.1.2
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.
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.
IP -> Routes

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

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

GregSowell.com
Wireless Security Profile

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

• Create the bridge
• Add ports to the bridge.
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.
Trunking Design

Interwebs

Mikrotik

Ether1
1.1.1.1/30

Ether2

VLAN 10
192.168.10.1/24

VLAN 20
192.168.20.1/24

VLAN 30
192.168.30.1/24

Switch

Trunk

PC
192.168.10.2
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.
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
- CactiEZ - http://cactiez.cactiusers.org/download/
- Cacti Video Tutorials - http://gregsowell.com/?page_id=86
- Great Consultant ;) - http://gregsowell.com/?page_id=245