



Greg Sowell Consulting



Troubleshooting MUM 2010

Who Am I

- Greg Sowell – A+, Network+, CCNA, CCNP, CCIE Written, MTCNA, MTCRE, Mikrotik Certified Trainer
- Network Engineering Manager
FIBERTOWN Datacenters
- Consultant – GregSowell.com
- Trainer – MikrotikUniversity.com
- And also...

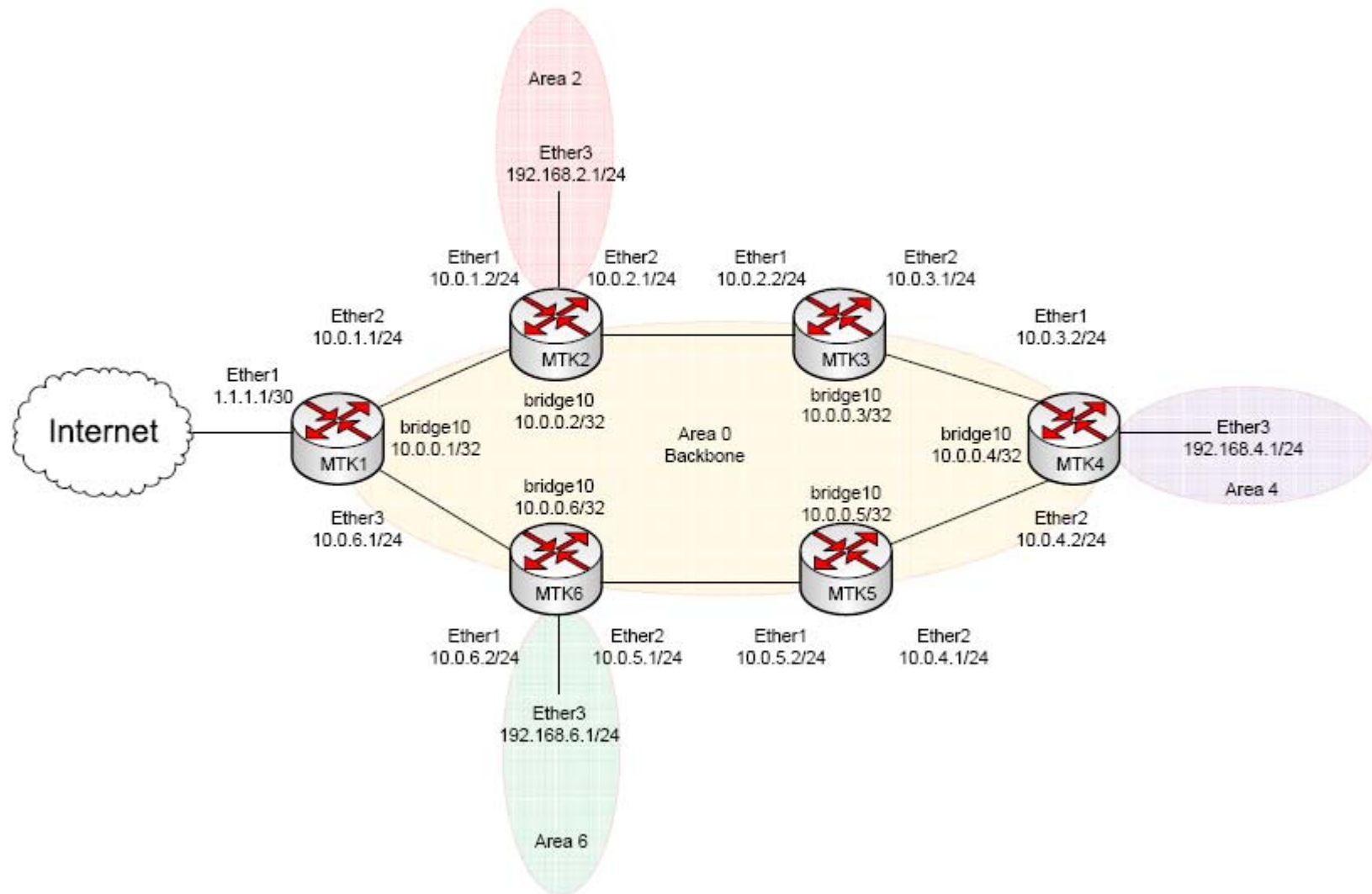
Wedding Photographer



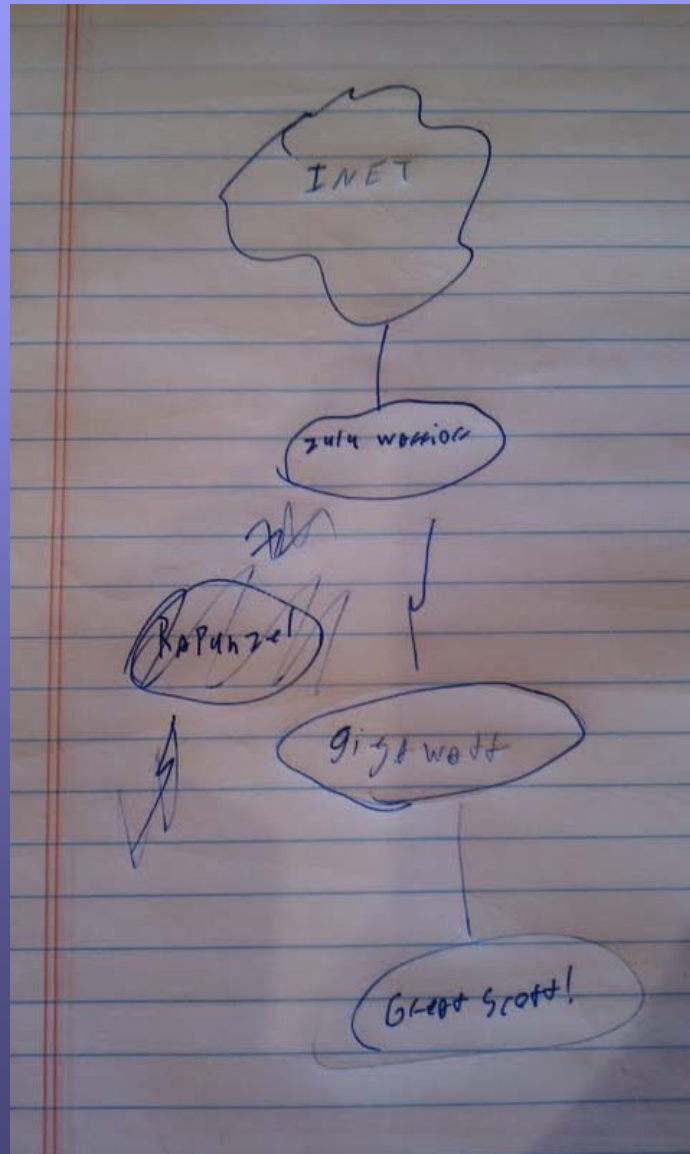
Show Me Your Network

- DOCUMENTATION!
 - Detailed network diagrams of existing network.
 - IP addresses
 - Links
 - Device descriptions
 - Frequencies
 - IP pools
 - Detailed diagrams of planned upgrades.
 - Show new links
 - Addressing

Show Me Your Network - Good



Show Me Your Network - Bad

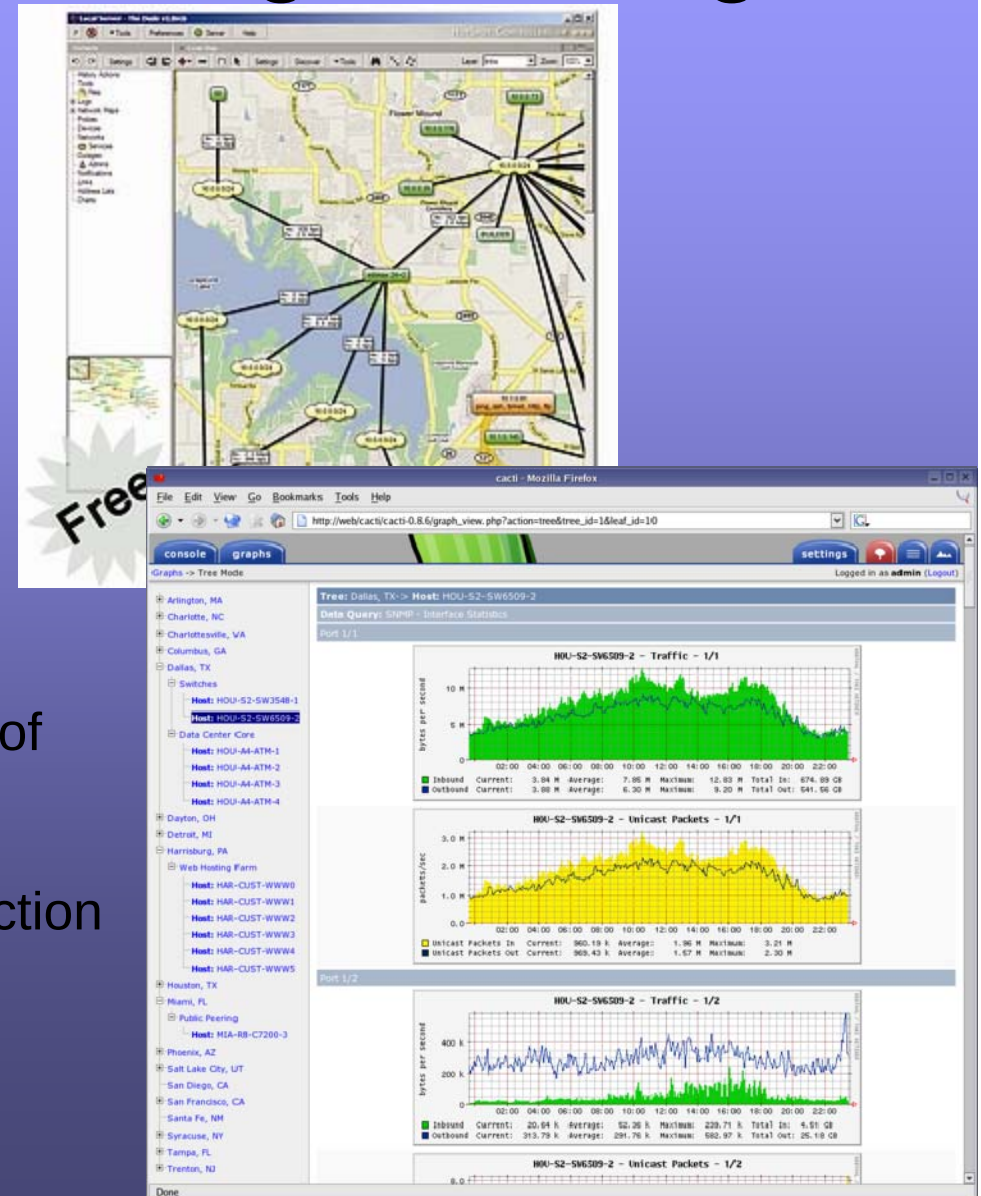


Show Me Your Network - Worse



Equipment Monitoring/Trending

- The Dude - Free
 - ICMP monitoring
 - Syslog collection
 - Weathermap
 - Great for live diagnosis
- Cacti - Free
 - Syslog collection
 - SNMP trap collection
 - Less flexible weathermap
 - Great for long term trending of SNMP information
 - Pretty good reporting
 - Extremely flexible data collection
 - Netflow collection

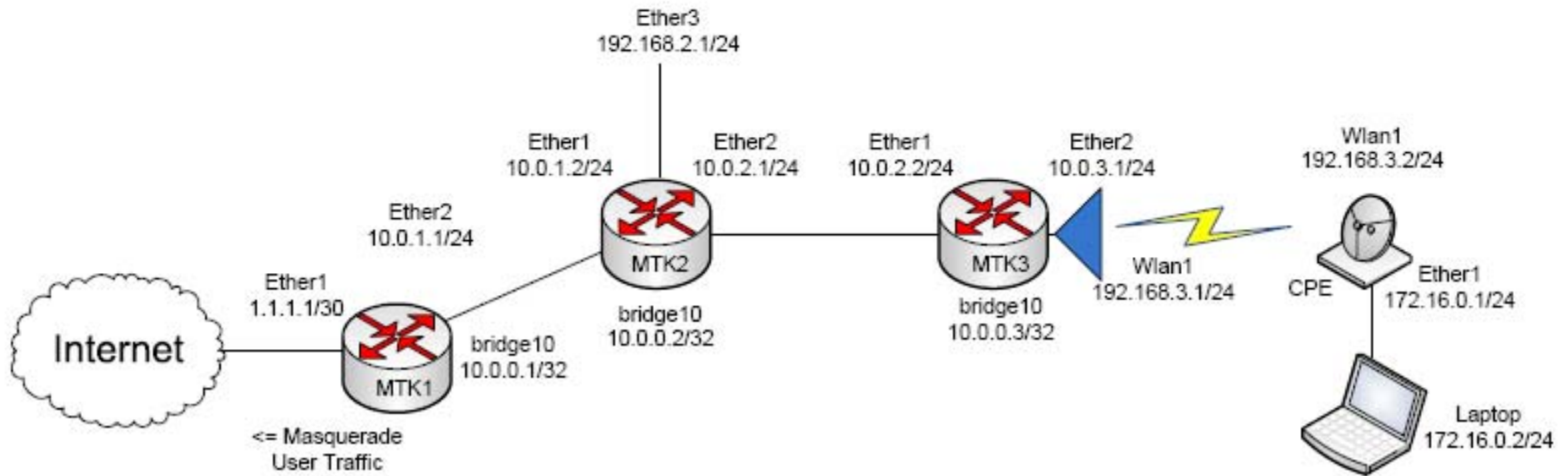


What's In Your Bag

- Spares for every major piece of equipment (how much equipment loss can you sustain?) Do you have enough gear to create a test lab?
 - Cables
 - Tools
 - Analyzers
 - Aspirin
- 
- A photograph showing a variety of networking tools and equipment arranged on a wooden surface. The items include several coiled cables in different colors (blue, green, white), a black laptop, a yellow digital multimeter, a green-handled crimping tool, a green-handled screwdriver, a red-handled wire cutter, a black soldering iron, a small white box, a black power supply unit, and various other small components and connectors.



Diagram For Troubleshooting



ICMP – Internet Control Message Protocol

Payload

Bits	0-7	8-15	16-23	24-31
0	Type	Code	Checksum	
32	ID		Sequence	

- **Type** - ICMP type as specified below.
- **Code** - further specification of the ICMP type; e.g. : an ICMP Destination Unreachable might have this field set to 1 through 15 each bearing different meaning.
- **Checksum** - This field contains error checking data calculated from the ICMP header+data, with value 0 for this field. The algorithm is the same as the header checksum for IPv4.
- **ID** - This field contains an ID value, should be returned in case of ECHO REPLY.
- **Sequence** - This field contains a sequence value, should be returned in case of ECHO REPLY.

- **Type – Code – Description**
- 8 – 0 – Echo Request
- 0 – 0 – Echo Reply
- 3 – 0 to 13 – Destination Unreachable

Ping/Trace Route

- Ping
 - Created in 1983.
 - Sends ICMP type 8 – Echo Request.
 - Measures the round-trip-time. The amount of time it takes a ping to travel to a host and return.
- Trace Route
 - Created in 1987.
 - Sends ICMP type 8 – Echo Request.
 - Sends request with a TTL (Time To Live) set to 1. Then the next request sent has a TTL of 2. This continues until the destination responds.

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\greg>ping 4.2.2.2

Pinging 4.2.2.2 with 32 bytes of data:

Reply from 4.2.2.2: bytes=32 time=33ms TTL=58
Reply from 4.2.2.2: bytes=32 time=31ms TTL=58
Reply from 4.2.2.2: bytes=32 time=32ms TTL=58
Reply from 4.2.2.2: bytes=32 time=54ms TTL=58

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 54ms, Average = 37ms

C:\Documents and Settings\greg>_
```

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\greg>tracert 4.2.2.2

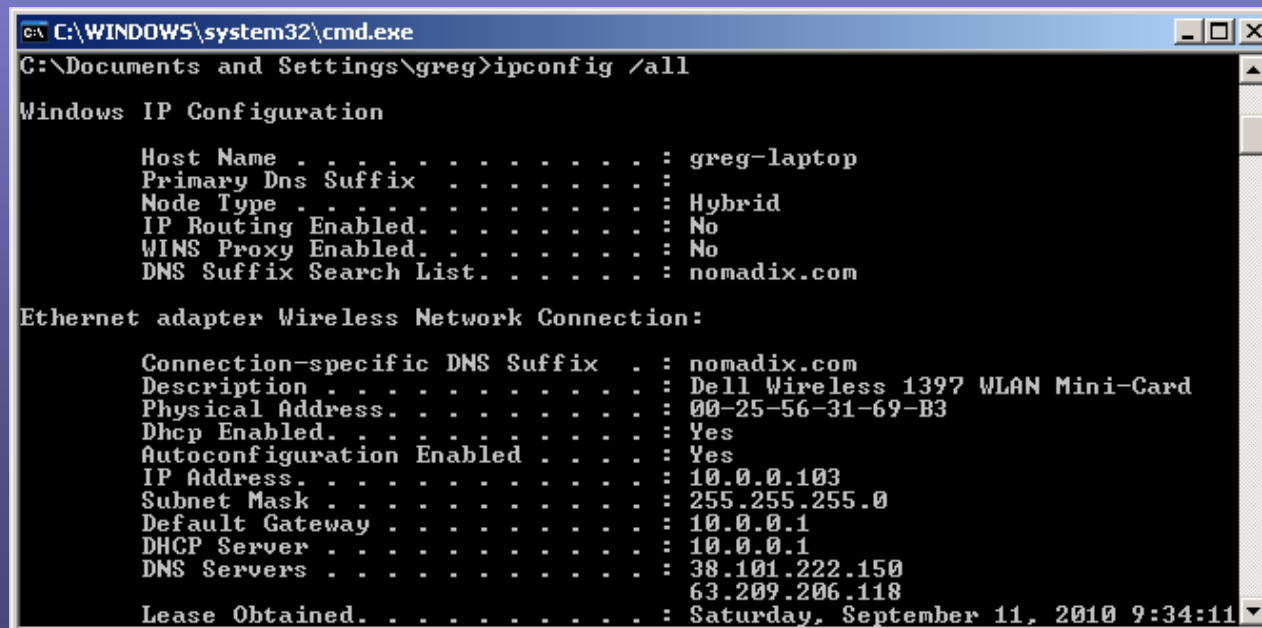
Tracing route to vns-c-bak.sys.gte.net [4.2.2.2]
over a maximum of 30 hops:
  0  27 ms  25 ms  25 ms  mail.bonnetcpa.com [71.113.222.1]
  1  30 ms  28 ms  28 ms  at-6-1-0-1711.dfw01-core-rtr2.verizon-gni.net [130.81.135.60]
  2  30 ms  29 ms  31 ms  as0-0.dfw01-hb-rtr2.verizon-gni.net [130.81.20.6]
  3  32 ms  35 ms  31 ms  0.xe-9-1-0.bri.dfw13.alter.net [152.63.2.149]
  4  32 ms  31 ms  30 ms  te-5-1-0.edge2.dallas3.level3.net [4.68.111.121]
  5  32 ms  30 ms  32 ms  ae-21-70.car1.dallas1.level3.net [4.69.145.67]
  6  33 ms  30 ms  30 ms  vns-c-bak.sys.gte.net [4.2.2.2]

Trace complete.

C:\Documents and Settings\greg>_
```

Client Troubleshooting

- Does the client have a valid IP for the CPE.
- Does the client have the proper DNS servers.
- Can you ping the CPE/AP?



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\greg>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : greg-laptop
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : nomadix.com

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : nomadix.com
    Description . . . . . : Dell Wireless 1397 WLAN Mini-Card
    Physical Address. . . . . : 00-25-56-31-69-B3
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.0.0.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1
    DHCP Server . . . . . : 10.0.0.1
    DNS Servers . . . . . : 38.101.222.150
                           63.209.206.118
    Lease Obtained. . . . . : Saturday, September 11, 2010 9:34:11
```

CPE Troubleshooting

- Does the CPE show up in the AP's registration table?
- What does signal strength look like at both sides?
- Is the client flapping?

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles

[-] [Filter] [Reset]

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Signal Strengt...	Tx/Rx Rate
000B6BD...	00:0B:6B:DA:A1:8C	wlan1	00:00:34	no	no	0.000	-88	12Mbps/6Mbps

AP Client <00:0B:6B:DA:A1:8C>

General | 802.1x | Signal | Nstreme

Last Activity: 0.010 s

Signal Strength: -81 dBm

Tx Signal Strength: -84 dBm

Signal To Noise: 16 dB

Tx/Rx CCQ: 61/38 %

P Throughput: 14336 kbps

Signal Strengths

Rate	Strength
6Mbps	-81
9Mbps	-80
12Mbps	-83
18Mbps	-84
24Mbps	-81

Interface <wlan1>

WDS | Nstreme | Status | Advanced Status | Traffic | ...

Band: 5GHz

Frequency: 5180 MHz

Tx/Rx Rate: 6Mbps/24Mbps

SSID: 4mansion

BSSID: 00:0B:6B:DA:A0:4D

Tx/Rx Signal Strength: -82/-85 dBm

Noise Floor: -96 dBm

Signal To Noise: 11 dB

Tx/Rx CCQ: 26/77 %

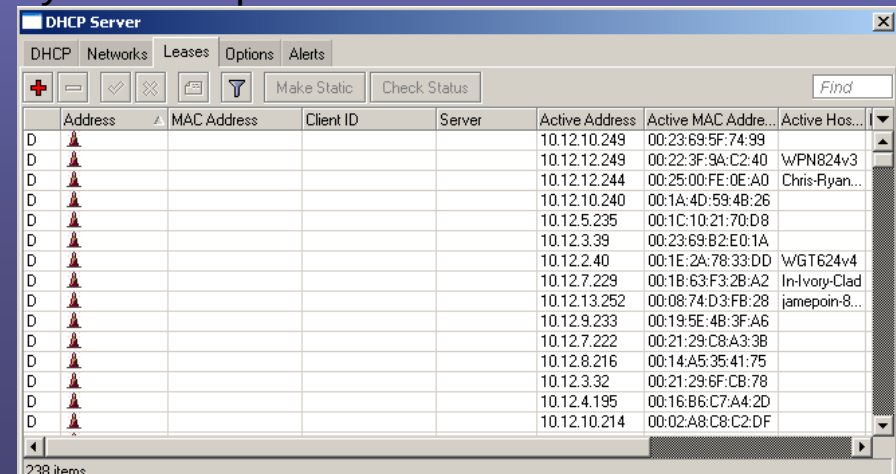
Overall Tx CCQ: 26 %

Ack. Timeout:

RouterOS Version: 3.10

CPE Troubleshooting

- Did the CPE pull an IP address from your DHCP server?
 - If not is your DHCP pool exhausted?
- Did the CPE pull an IP via PPPoE?
 - If not is your PPPoE pool exhausted?
 - Did the client fail authentication?
- The CPE is statically configured.
 - Did you use an IP address that is already in use?
 - Is the IP address valid – proper subnet?
- Ensure MAC addresses aren't the same on a single L2 segment.
 - If you copied and pasted a config, ensure you didn't paste the MAC-address.



The screenshot shows the 'DHCP Server' window in WinBox, specifically the 'Leases' tab. It displays a table of active DHCP leases with columns for Address, MAC Address, Client ID, Server, Active Address, Active MAC Address, and Active Hostname. The table contains 15 rows of data, each with a red tree icon in the first column. The status bar at the bottom indicates '238 items'.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Hostname
D					10.12.10.249	00:23:69:5F:74:99	
D					10.12.12.249	00:22:3F:9A:C2:40	WPN824v3
D					10.12.12.244	00:25:00:FE:0E:A0	Chris-Ryan...
D					10.12.10.240	00:1A:4D:59:4B:26	
D					10.12.5.235	00:1C:10:21:70:D8	
D					10.12.3.39	00:23:69:B2:E0:1A	
D					10.12.2.40	00:1E:2A:78:33:DD	WGT624v4
D					10.12.7.229	00:1B:63:F3:2B:A2	In-Ivory-Clad
D					10.12.13.252	00:08:74:D3:F8:28	jamepoin-8...
D					10.12.9.233	00:19:5E:4B:3F:A6	
D					10.12.7.222	00:21:29:C8:A3:3B	
D					10.12.8.216	00:14:A5:35:41:75	
D					10.12.3.32	00:21:29:6F:CB:78	
D					10.12.4.195	00:16:B6:C7:A4:2D	
D					10.12.10.214	00:02:A8:C8:C2:DF	

Ping Tool

- /ping
- Source address can also be specified if you want the packet to appear to be sourced from a different interface.
- Packet size is useful for verifying MTU issues.

The screenshot shows the Mikrotik Ping tool window with the 'General' tab selected. The 'Ping To:' field is set to '4.2.2.2', 'Interface:' is 'any', 'Packet Count:' is 6, and 'Timeout:' is 1000 ms. The 'Ping' button is highlighted. Below the settings is a table showing the results of the ping test.

#	Host	Time	Reply Size	TTL	Status
0	4.2.2.2	9ms	50	57	
1	4.2.2.2	9ms	50	57	
2	4.2.2.2	9ms	50	57	
3	4.2.2.2	8ms	50	57	
4	4.2.2.2	10ms	50	57	
5	4.2.2.2	9ms	50	57	

At the bottom, a status bar indicates: 6 of 6 packets received, 0% packet loss, Min: 8ms, Avg: 9ms, Max: 10ms.

The screenshot shows the Mikrotik Ping tool window with the 'Advanced' tab selected. The 'Src. Address:' field is empty, 'Packet Size:' is 50, 'TTL:' is 64, and 'Routing Table:' is empty. The 'Dont Fragment' checkbox is checked. The 'Ping' button is highlighted. Below the settings is a table showing the results of the ping test.

#	Host	Time	Reply Size	TTL	Status
0	4.2.2.2	9ms	50	57	
1	4.2.2.2	9ms	50	57	
2	4.2.2.2	9ms	50	57	
3	4.2.2.2	8ms	50	57	
4	4.2.2.2	10ms	50	57	
5	4.2.2.2	9ms	50	57	

At the bottom, a status bar indicates: 6 of 6 packets received, 0% packet loss, Min: 8ms, Avg: 9ms, Max: 10ms.

Traceroute Tool

- /tool traceroute
- Source address can also be specified if you want the packet to appear to be sourced from a different interface.

The screenshot shows the 'Traceroute' window with the following configuration:

- Traceroute To: 4.2.2.2
- Packet Size: 56
- Timeout: 1 s
- Protocol: icmp
- Port: 68
- Src. Address: (empty)
- Interface: (empty)
- DSCP: (empty)
- Routing Table: (empty)

Buttons: Traceroute, Stop, Close

#	Host	Time 1	Time 2	Time 3
0	144.232.3.2	1ms	1ms	1ms
1	144.232.3.21	1ms	1ms	1ms
2	144.228.37.201	7ms	7ms	6ms
3	144.232.3.211	8ms	15ms	7ms
4	144.232.18.74	9ms	10ms	9ms
5	144.232.24.18	9ms	10ms	9ms
6	4.69.145.131	10ms	9ms	10ms
7	4.2.2.2	14ms	9ms	11ms

CPE Troubleshooting

- Does a ping to the AP complete?
- Does a trace route from the CPE complete?
- Where does it fail?
- Are others having similar issues?
- When in doubt, change it out.
- Time to check our infrastructure!

Infrastructure Troubleshooting

- Use trace route to find at what point the traffic fails to forward.
- Begin to determine reason why traffic fails at this point.
 - Start by checking routing.

Routing Is A Two-way Street



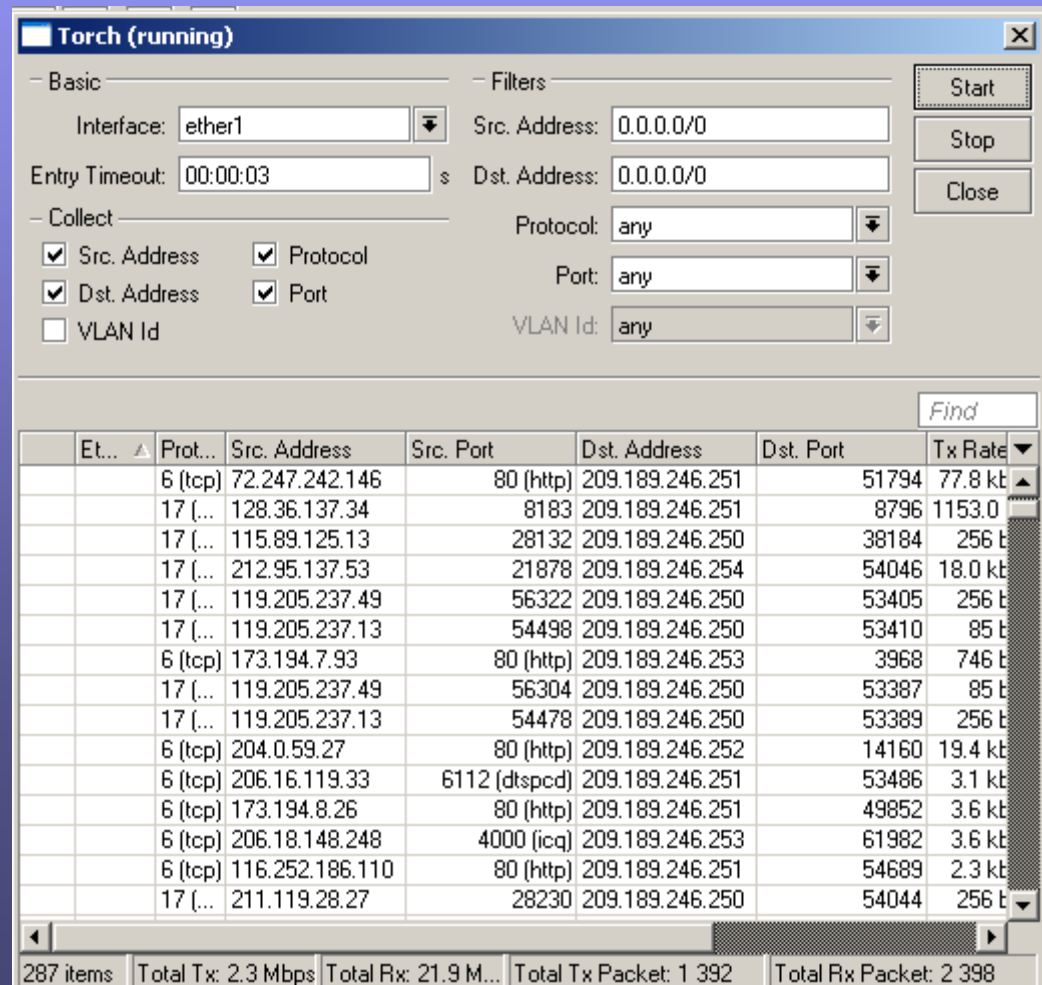
ISP Border Troubleshooting

- If your traffic makes it to the Internet border and fails, here are some common steps.
 - Check filter rules in firewall (/ip firewall filter).
 - If you have a large amount of rules, simply create an accept rule that matches your specific criteria and move it to the top.
 - *Order of operation.
 - Check NATing (/ip firewall nat).
 - Check NAT rules to ensure they cover the failing subnet.
 - *Order of operation.

Advanced Troubleshooting Tools

- Torch – Traffic sniffer

- You have the capability to specify interface, source, destination, port, protocol and VLAN.
- Whatever device our trace stops at, we torch on the next hop router's incoming interface. We are looking to see if the traffic is being sent.
- This will aid us in determining where the break down is...which router to examine.



The screenshot shows the Mikrotik Torch (running) window. The 'Basic' tab is selected, showing the interface 'ether1', entry timeout '00:00:03', and filters for 'Src. Address', 'Dst. Address', 'Protocol', 'Port', and 'VLAN Id'. The 'Collect' tab is also visible, showing checkboxes for 'Src. Address', 'Dst. Address', 'Protocol', 'Port', and 'VLAN Id'. The 'Find' button is present. Below the settings is a table of captured traffic.

Et...	Prot...	Src. Address	Src. Port	Dst. Address	Dst. Port	Tx Rate
6 (tcp)		72.247.242.146	80 (http)	209.189.246.251	51794	77.8 kb
17 [...]		128.36.137.34	8183	209.189.246.251	8796	1153.0
17 [...]		115.89.125.13	28132	209.189.246.250	38184	256 b
17 [...]		212.95.137.53	21878	209.189.246.254	54046	18.0 kb
17 [...]		119.205.237.49	56322	209.189.246.250	53405	256 b
17 [...]		119.205.237.13	54498	209.189.246.250	53410	85 b
6 (tcp)		173.194.7.93	80 (http)	209.189.246.253	3968	746 b
17 [...]		119.205.237.49	56304	209.189.246.250	53387	85 b
17 [...]		119.205.237.13	54478	209.189.246.250	53389	256 b
6 (tcp)		204.0.59.27	80 (http)	209.189.246.252	14160	19.4 kb
6 (tcp)		206.16.119.33	6112 (dtspcd)	209.189.246.251	53486	3.1 kb
6 (tcp)		173.194.8.26	80 (http)	209.189.246.251	49852	3.6 kb
6 (tcp)		206.18.148.248	4000 (icq)	209.189.246.253	61982	3.6 kb
6 (tcp)		116.252.186.110	80 (http)	209.189.246.251	54689	2.3 kb
17 [...]		211.119.28.27	28230	209.189.246.250	54044	256 b

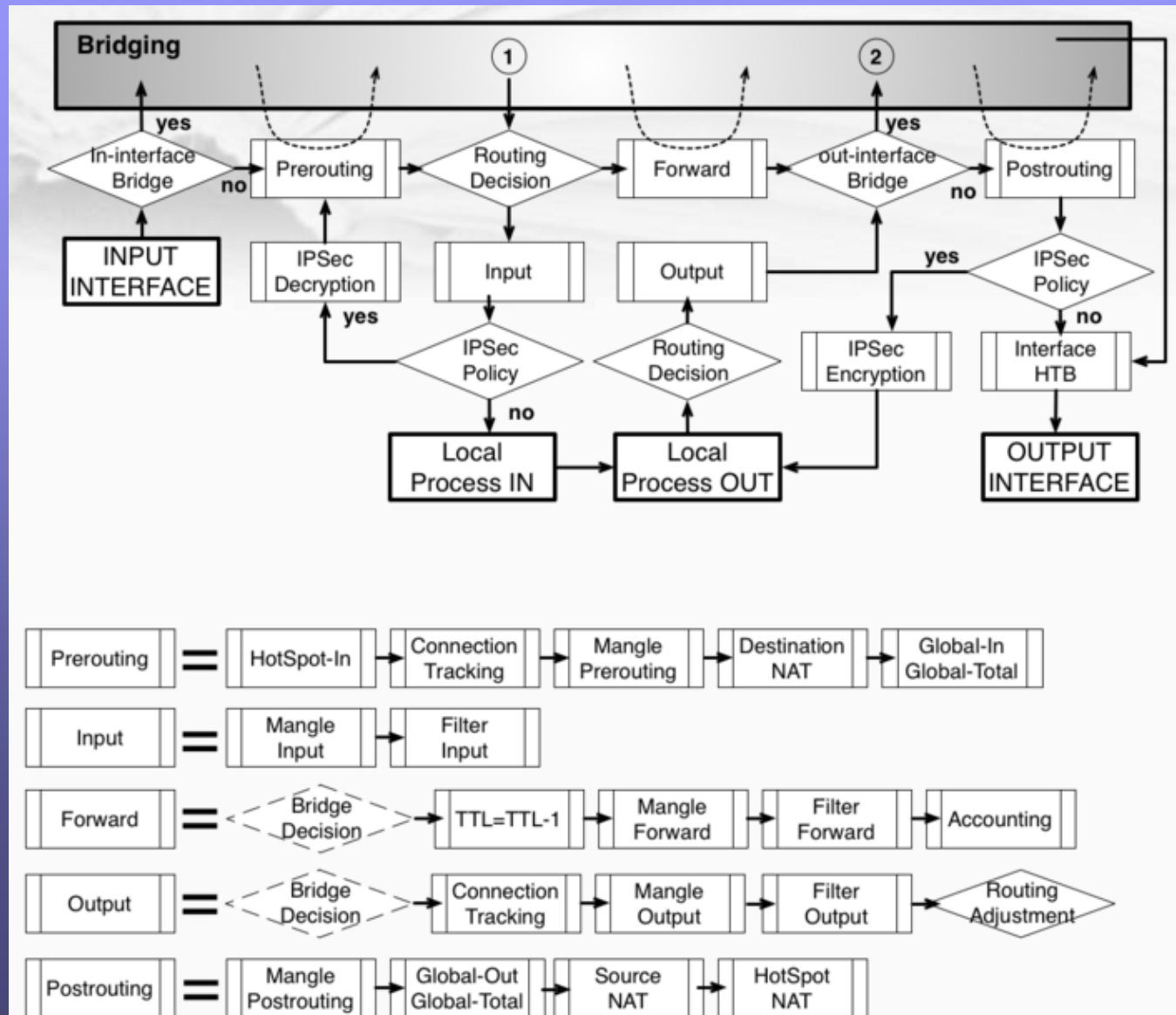
287 items Total Tx: 2.3 Mbps Total Rx: 21.9 M... Total Tx Packet: 1 392 Total Rx Packet: 2 398

Advanced Troubleshooting - Mangle

- Mangle Rules (/ip firewall mangle). Generally used to mark traffic or do some manipulation of traffic.
- If we've narrowed our issues to a single router and have exhausted all other options, we can use mangle to help us determine where in the router we are encountering issues.
- Using the packet flow diagram, begin creating mangles to pass through our specific traffic and follow it through the router.
 - /ip firewall mangle
 - add action=passthrough chain=prerouting comment="" disabled=no protocol=icmp src-address=192.168.3.2
 - add action=passthrough chain=forward comment="" disabled=no protocol=icmp src-address=192.168.3.2
 - add action=passthrough chain=postrouting comment="" disabled=no protocol=icmp src-address=192.168.3.2
- Once you create the mangle rules test run your connection again. Watch for the counters in the mangle rules to increment. If they don't increment at a certain spot you know traffic is being affected before this rule.

Advanced Troubleshooting Tools

- Packet Flow Diagram
- Most likely the single most amazing piece of documentation on the Wiki!
- Shows the steps data takes as it traverses the router.



Common Mistakes - Comments

- Bad Comments.
 - Create meaningful comments.
 - Record the date and user in your comments.
 - You will most likely end up with a large amount of rules. Keeping track of addition dates as well as who made the changes is important.
 - This is for you and also your consultant/Mikrotik support.

Common Mistakes – Comments - Good

Firewall							
Filter Rules NAT Mangle Service Ports Connections Address Lists							
       Reset Counters  Reset All Co							
#		Action	Chain	Src. Address	Dst. Address	Proto...	Src.
::: Greg - 01-01-10 - drop netbios							
0		 drop	forward	0.0.0.0/0			
::: Greg - 01-01-10 - drop sql ports							
1		 drop	forward	0.0.0.0/0			
::: Greg - 01-01-10 - drop icmp to user subnet							
2		 drop	forward	0.0.0.0/0			
::: Greg - 01-01-10 - allow access to webserver 1							
3		 acc...	forward	0.0.0.0/0			
::: Greg - 01-01-10 - block everything else to webserver1							
4		 drop	forward	0.0.0.0/0			
::: Greg - 02-01-10 - allow users to gregsowell.com							
5		 acc...	forward	0.0.0.0/0			
::: Greg - 02-01-10 - block users from going to any other consulting sites							
6		 drop	forward	0.0.0.0/0			

Common Mistakes – Comments - Bad

Firewall						
Filter Rules NAT Mangle Service Ports Connections Address						
       Reset Counters  Re						
#	Action	Chain	Src. Address	Dst. Address	Prot	
::: Andrew from Australia THINKS he is a really cool guy						
0	 drop	forward	0.0.0.0/0			
::: I think this needs to stay						
1	 drop	forward	0.0.0.0/0			
::: Ninjas and pirates in Amsterdam						
2	 drop	forward	0.0.0.0/0			
::: Get to da choppa						
3	 acc...	forward	0.0.0.0/0			
::: No matter where you go, there you are						
4	 drop	forward	0.0.0.0/0			
5	 acc...	forward	0.0.0.0/0			
::: I slit the sheet, the sheet I slit, and on the slitted sheet I sit.						
6	 drop	forward	0.0.0.0/0			
::: moist green boogers						
7	 acc...	forward	0.0.0.0/0			
::: Packets...Packets... We don't need no stinking Packets...						
8	 drop	forward	0.0.0.0/0			
::: I play the vuvuzela						
9	 acc...	forward	0.0.0.0/0			
10	 drop	forward	0.0.0.0/0			
11	 acc...	forward	0.0.0.0/0			
12	 acc...	forward	0.0.0.0/0			

Firewall

Filter Rules

NAT

Mangle

Service Ports

Connections

Address Lists

Layer7 Protocols

+

-

✓

✗

📄

🔍

↺ Reset Counters

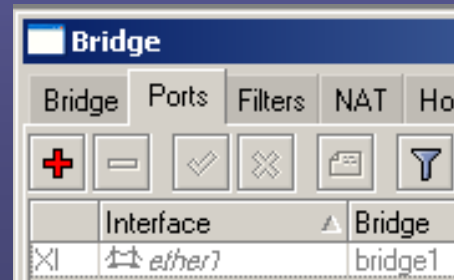
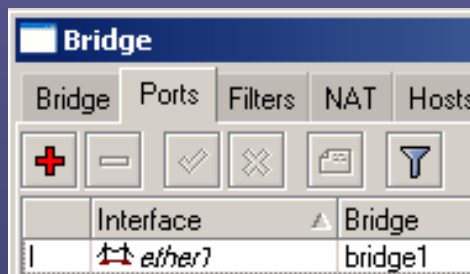
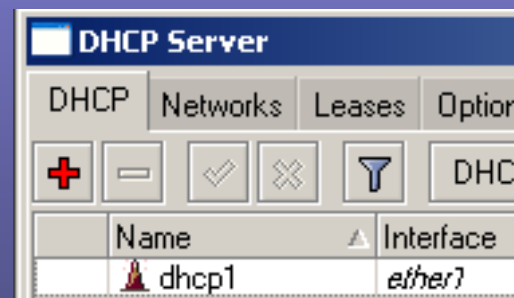
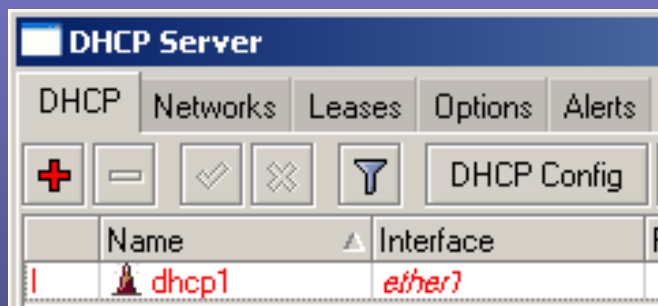
⏏ Reset All Counters

Find

#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte
0		✗ drop	forward	0.0.0.0/0					
1		✗ drop	forward	0.0.0.0/0					
2		✗ drop	forward	0.0.0.0/0					
3		✓ acc...	forward	0.0.0.0/0					
4		✗ drop	forward	0.0.0.0/0					
5		✓ acc...	forward	0.0.0.0/0					
6		✗ drop	forward	0.0.0.0/0					
7		✓ acc...	forward	0.0.0.0/0					
8		✗ drop	forward	0.0.0.0/0					
9		✓ acc...	forward	0.0.0.0/0					
10		✗ drop	forward	0.0.0.0/0					
11		✓ acc...	forward	0.0.0.0/0					
12		✓ acc...	forward	0.0.0.0/0					

Common Mistakes - Services

- Services won't start.
- Ensure the port the service is applied to isn't a port on a bridge or is configured as a slave port on the switching ASICs.
- Apply the service to the bridge interface or the master port.

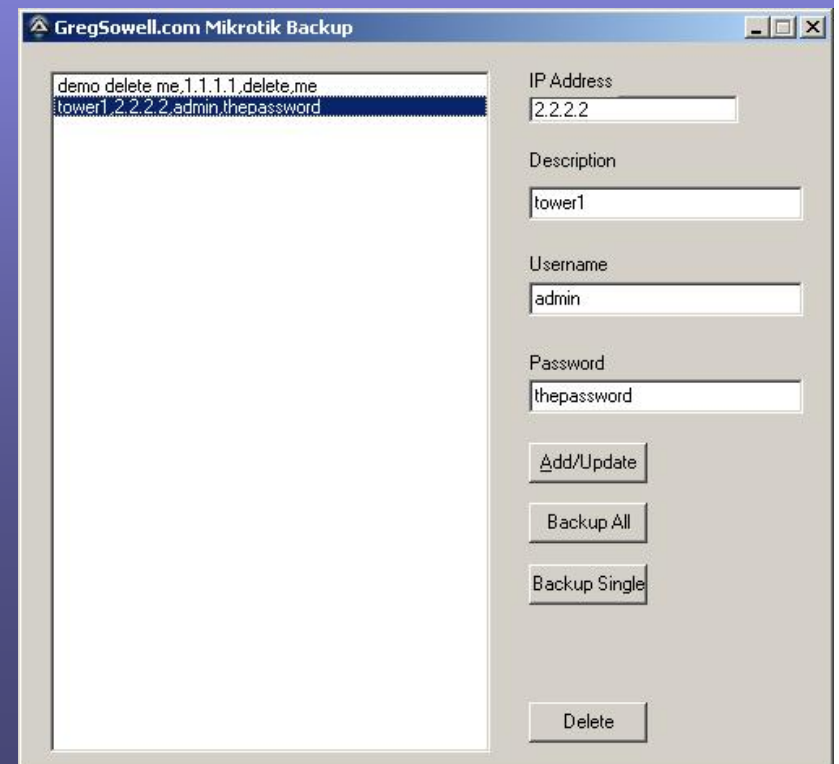


Common Mistakes - Addressing

- No subnet mask
 - You add an IP address to an interface, but forget to add a subnet mask, and thus the router assumes it is a host address.
- Wrong subnet or broadcast entry
 - Don't manually specify these values, let the router do it for you. For IP address, enter the address/subnet. Ex: 192.168.0.1/24. The router will then add the network and broadcast values for you.
- Overlapping subnets
 - Assigning the same subnet in two portions of the network.
 - Assigning 192.168.0.1/24 in the network at one location and then assigning 192.168.0.129/25 in another portion.
 - *Detailed diagrams.

Common Mistakes - Backups

- No backups.
- Infrequent backups.
- I wrote an automated windows based backup program. Free and includes code.

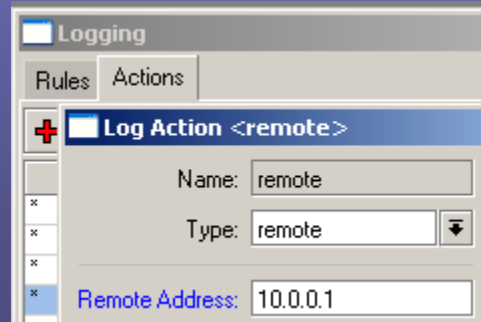
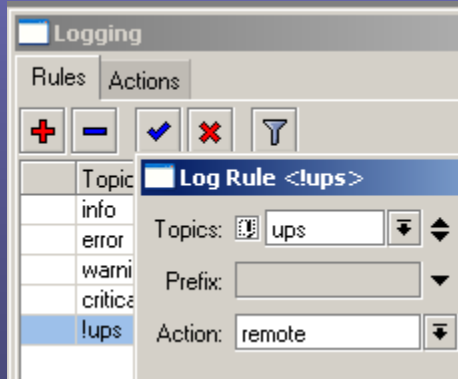


Common Mistakes - MTU

- Maximum Transmission Unit.
- Traffic failing or some sites not loading.
- MTU specifies the largest protocol data unit that a medium can transfer.
- At layer 3 if an MTU is exceeded, then fragmentation can occur. If the DF (do not fragment) bit is set, then the L3 device will drop the packet and send back a specialized ICMP packet.
- At layer 2 if an MTU is exceeded, then the frame is quietly discarded. No notification is sent.
- MTU needs to be consistent from end to end.
- PDUs that are larger than the standard 1518 are considered Jumbo. Not all vendors have a standard Jumbo size since there is no IEEE standard for Jumbo frames. Jumbos are often associated with Gigabit interfaces. Jumbos are generally around 9000.
- Mikrotik PPPoE defaults to an MTU of 1480 where most vendors default to 1492.
- Mikrotik wireless MTU is generally L3 - 1500 with an L2 at 2290.

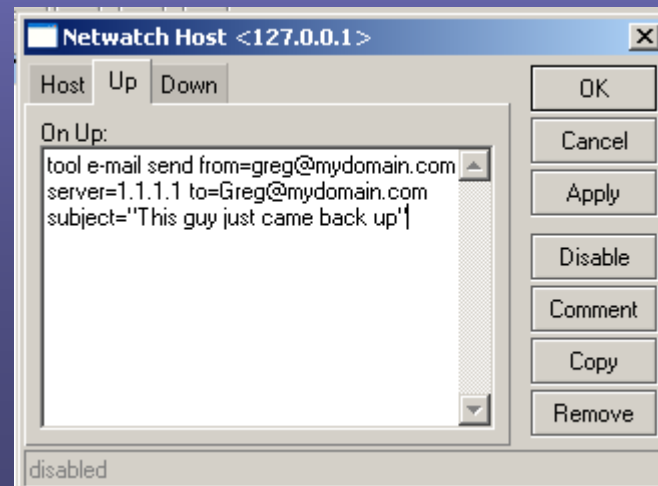
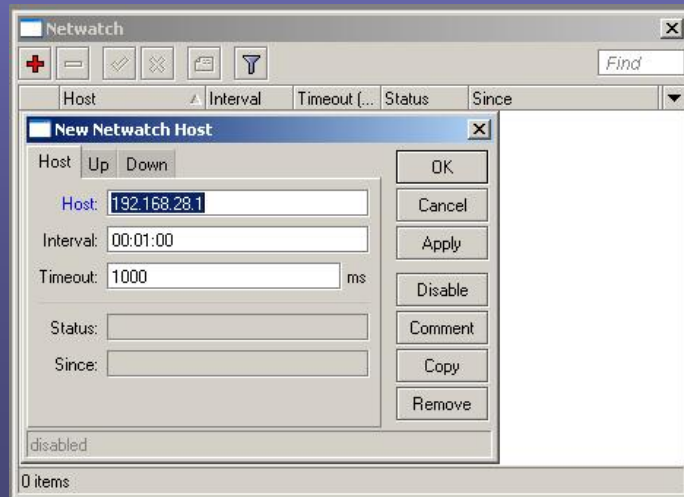
Additional Tools - Logging

- Mikrotik has a fairly robust logging facility.
- You can log to memory, terminal or syslog server. My facility of choice is syslog.
- /system logging



Additional Tools - Netwatch

- Netwatch pings a host and performs an action on up or down status.
- You can actuate a script or send an email.
- Useful for intermittent issue troubleshooting.



Resources

- Greg's Blog
 - <http://GregSowell.com>
 - <http://gregsowell.com/?p=1264> automated backup utility
 - <http://gregsowell.com/?p=819> Netwatch example
 - <http://gregsowell.com/?p=514> Common syslog alert statements
 - <http://gregsowell.com/?p=610> Netflow tutorial
- Training
 - <http://MikrotikUniversity.com>
- Mikrotik Video Tutorials
 - http://gregsowell.com/?page_id=304
- Mikrotik Support Docs
 - http://wiki.mikrotik.com/wiki/Main_Page
 - http://wiki.mikrotik.com/wiki/Manual:Packet_Flow
 - http://wiki.mikrotik.com/wiki/Manual:Maximum_Transmission_Unit_on_RouterBoards
 - <http://wiki.mikrotik.com/wiki/Netwatch>
 - http://wiki.mikrotik.com/wiki/Securing_New_RouterOs_Router#Logging_.26_Syslog
 - http://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools
 - http://wiki.mikrotik.com/wiki/Manual:Tools/Packet_Sniffer
 - http://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow
- Cacti
 - <http://cacti.net>
 - <http://cactiez.cactiusers.org/download/>
- Wikipedia
 - http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
 - <http://en.wikipedia.org/wiki/Ping>
 - <http://en.wikipedia.org/wiki/Traceroute>
 - http://en.wikipedia.org/wiki/Time_to_live
 - http://en.wikipedia.org/wiki/Maximum_transmission_unit

Thanks and happy troubleshooting!