Greg Sowell Consulting

Troubleshooting MUM 2010

Who Am I

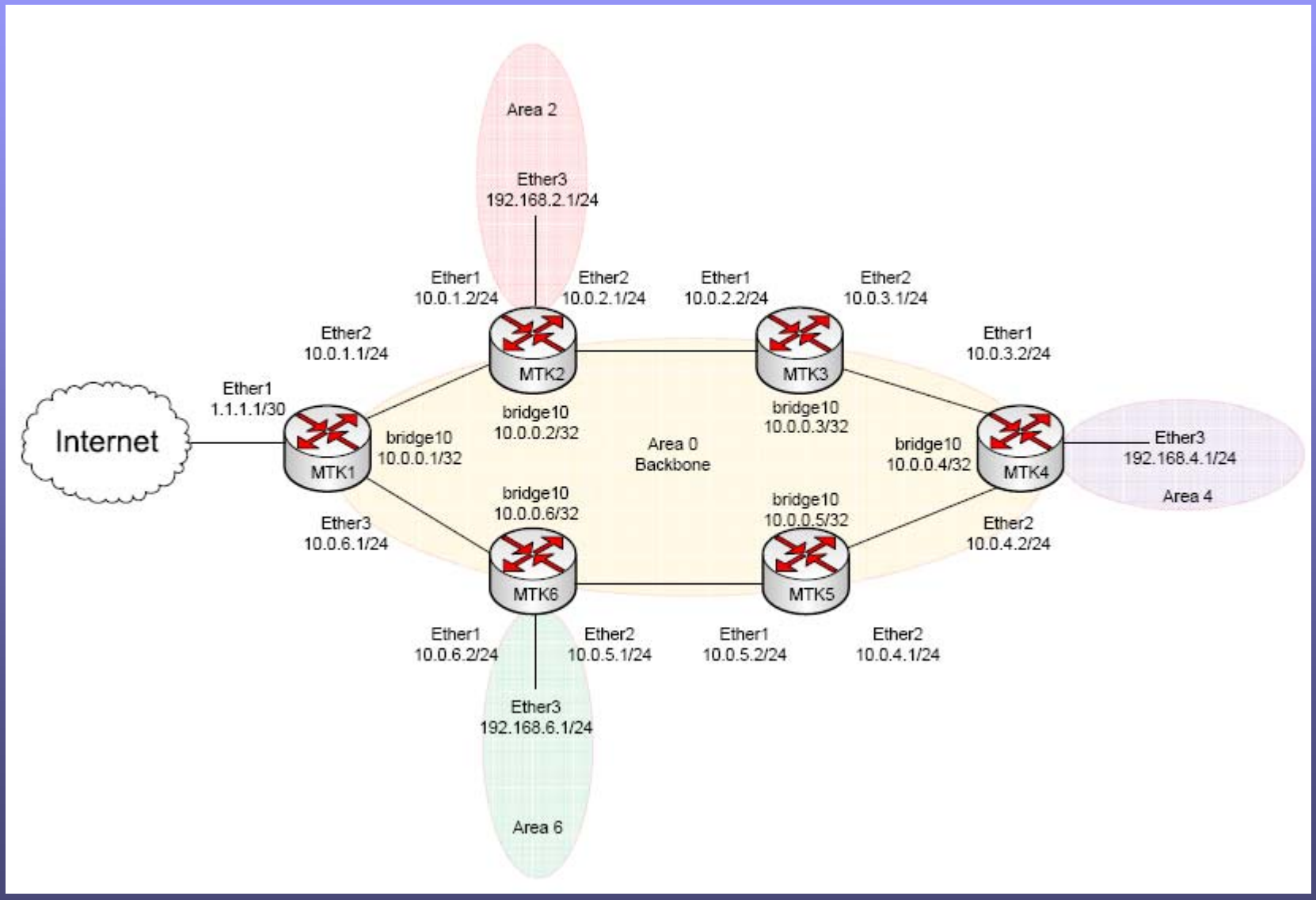
- Greg Sowell – A+, Network+, CCNA, CCNP, CCIE Written, MTCNA, MTCRE, Mikrotik Certified Trainer
- Network Engineering Manager FIBERTOWN Datacenters
- Consultant – GregSowell.com
- Trainer – MikrotikUniversity.com
- And also…

Wedding Photographer

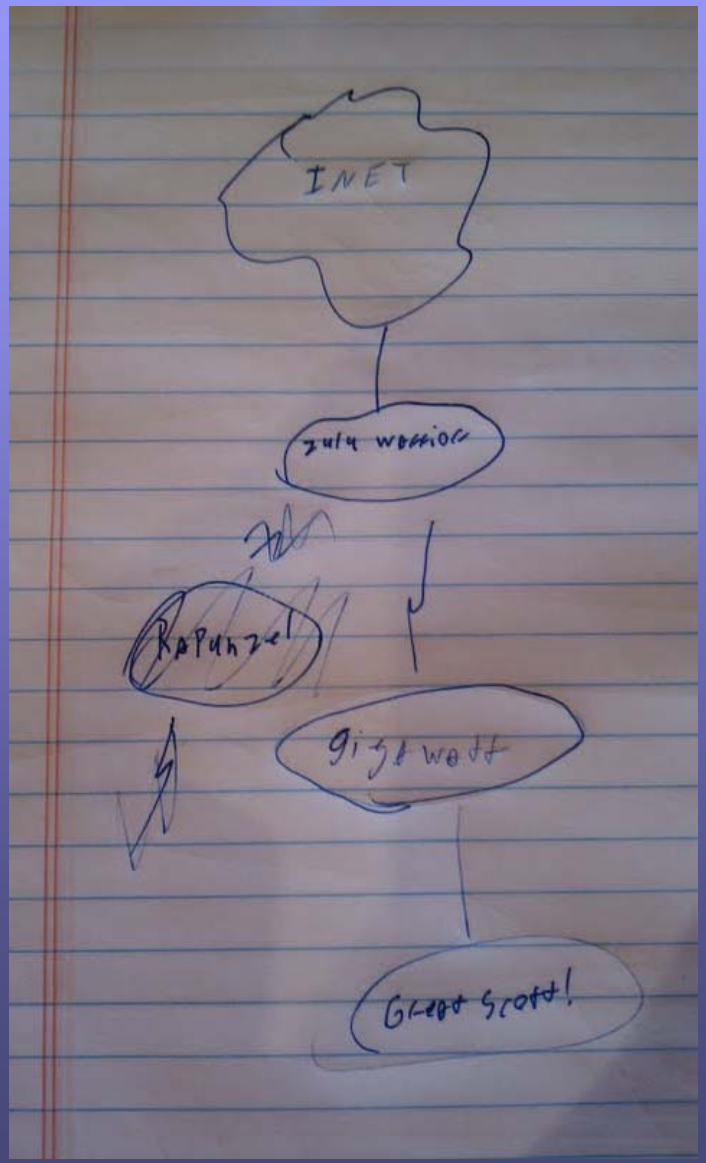
Show Me Your Network

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

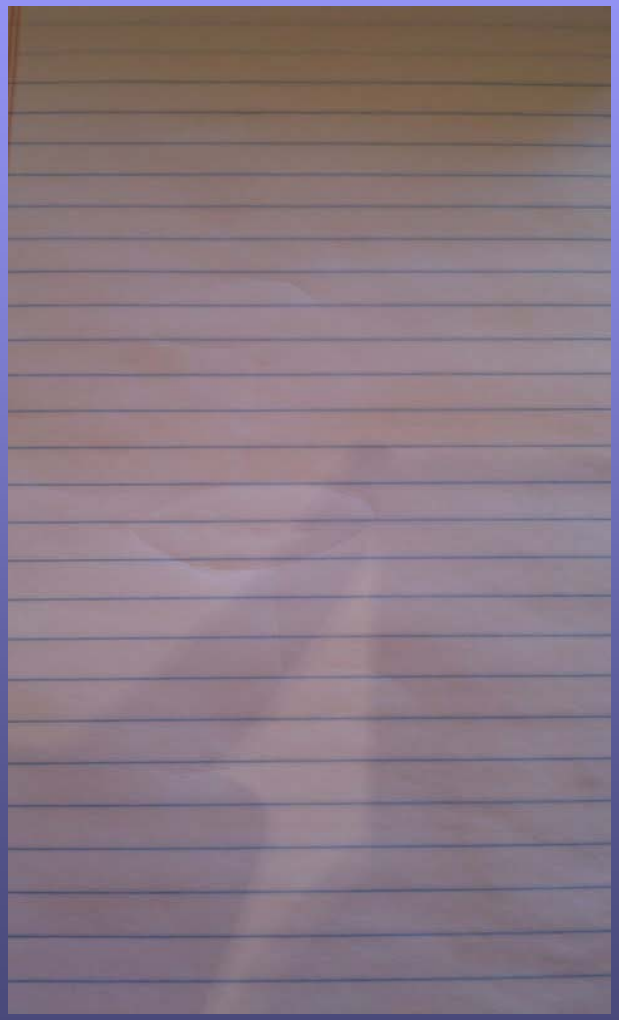
Show Me Your Network - Good



Show Me Your Network - Bad

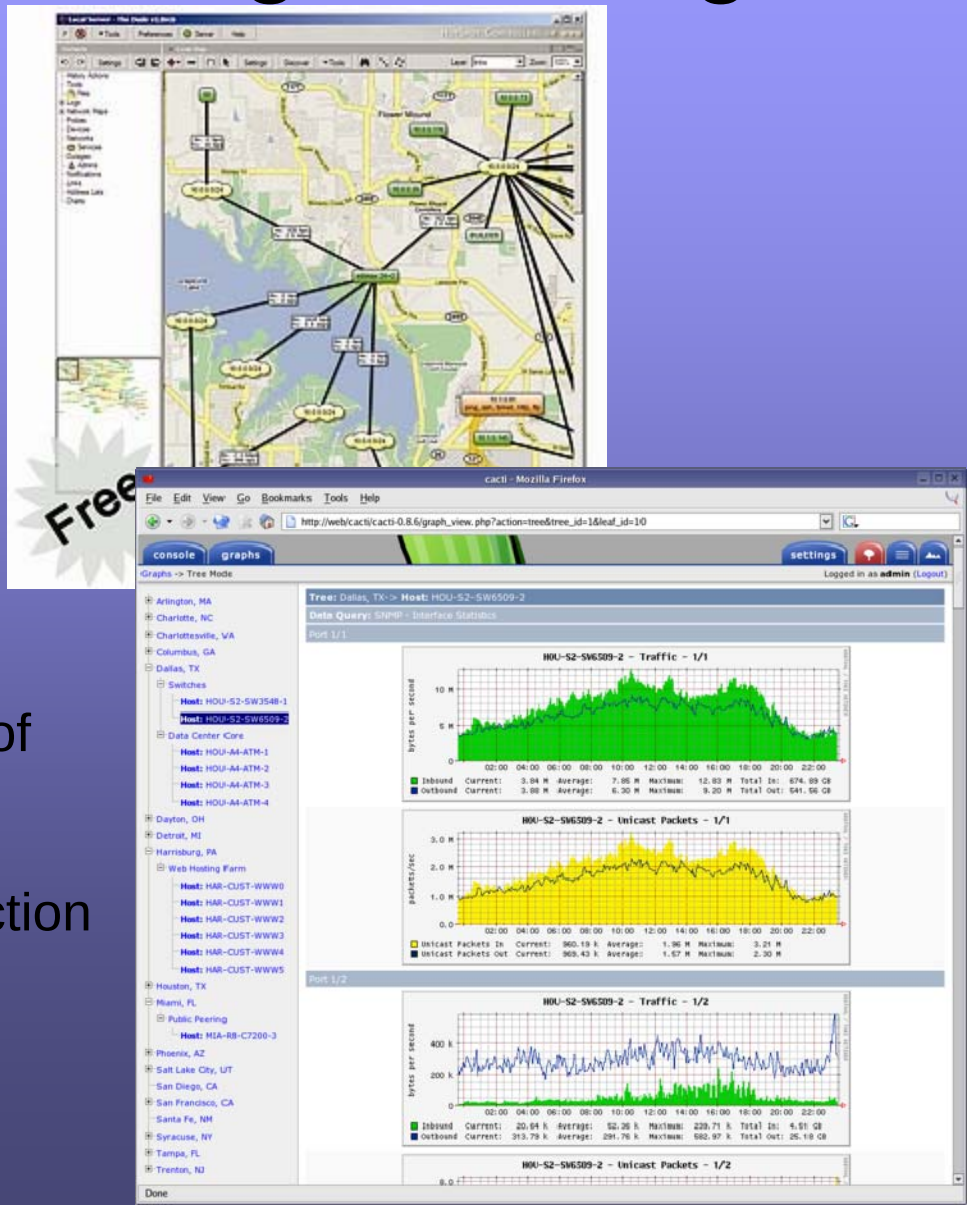


Show Me Your Network - Worse



Equipment Monitoring/Trending

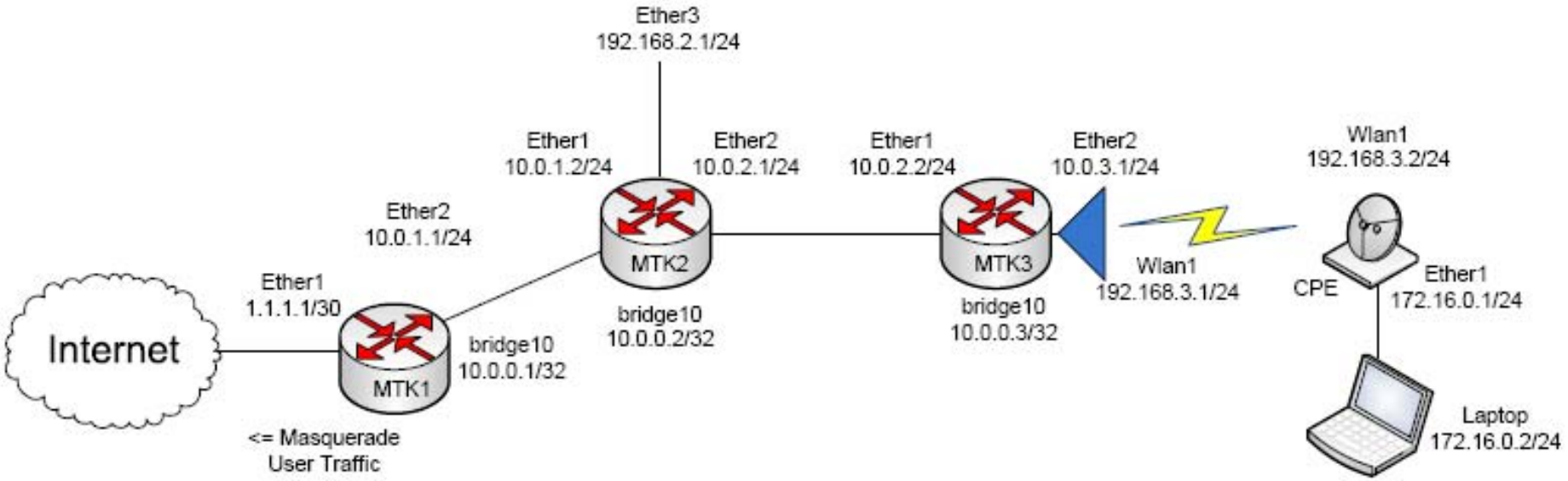
- The Dude - Free
  - ICMP monitoring
  - Syslog collection
  - Weathermap
  - Great for live diagnosis
- Cacti - Free
  - Syslog collection
  - SNMP trap collection
  - Less flexible weathermap
  - Great for long term trending of SNMP information
  - Pretty good reporting
  - Extremely flexible data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

Diagram For Troubleshooting



ICMP – Internet Control Message Protocol

Payload

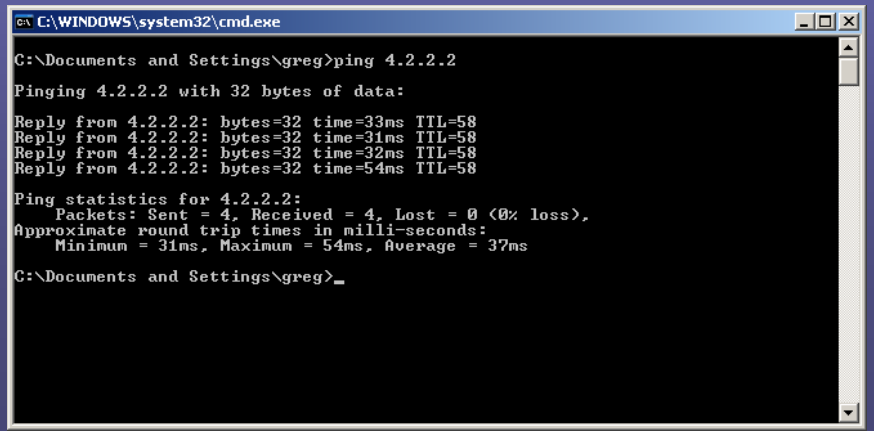
Bits	0-7	8-15	16-23	24-31
0	Type	Code	Checksum	
32	ID		Sequence	

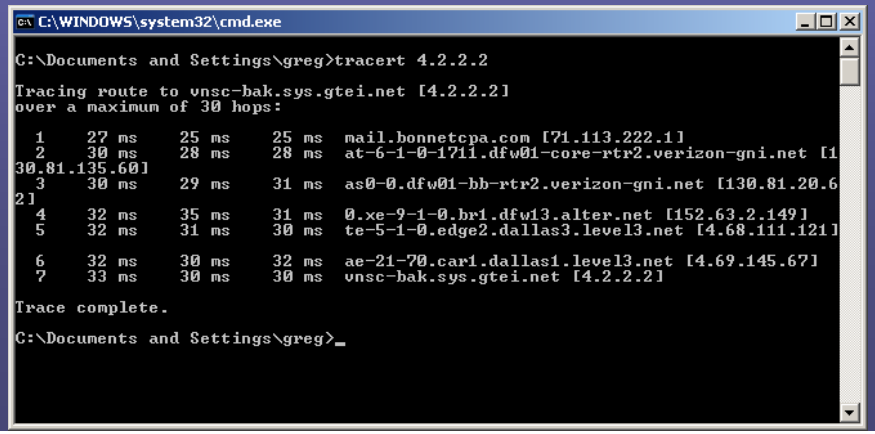
- **Type** - ICMP type as specified below.
- **Code** - further specification of the ICMP type; e.g. : an ICMP Destination Unreachable might have this field set to 1 through 15 each bearing different meaning.
- **Checksum** - This field contains error checking data calculated from the ICMP header+data, 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

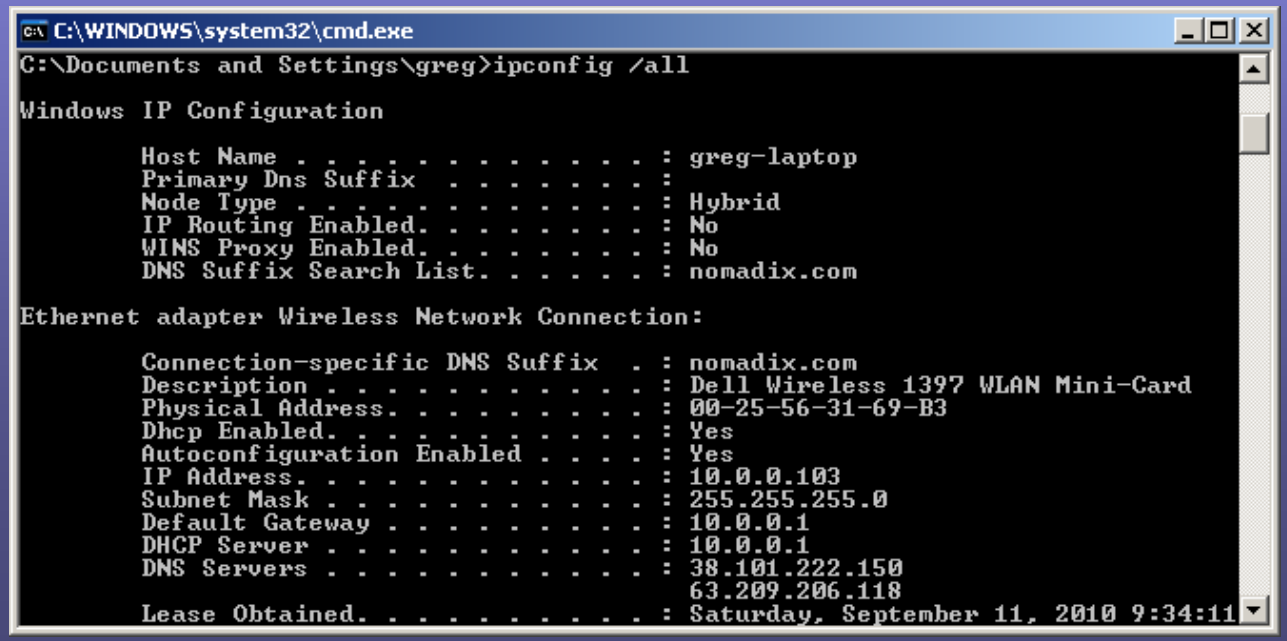
- Ping
  - Created in 1983.
  - Sends ICMP type 8 – Echo Request.
  - Measures the round-trip-time. The amount of time it takes a ping to travel to a host and return.
- Trace Route
  - Created in 1987.
  - Sends ICMP type 8 – Echo Request.
  - Sends request with a TTL (Time To Live) set to 1. Then the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





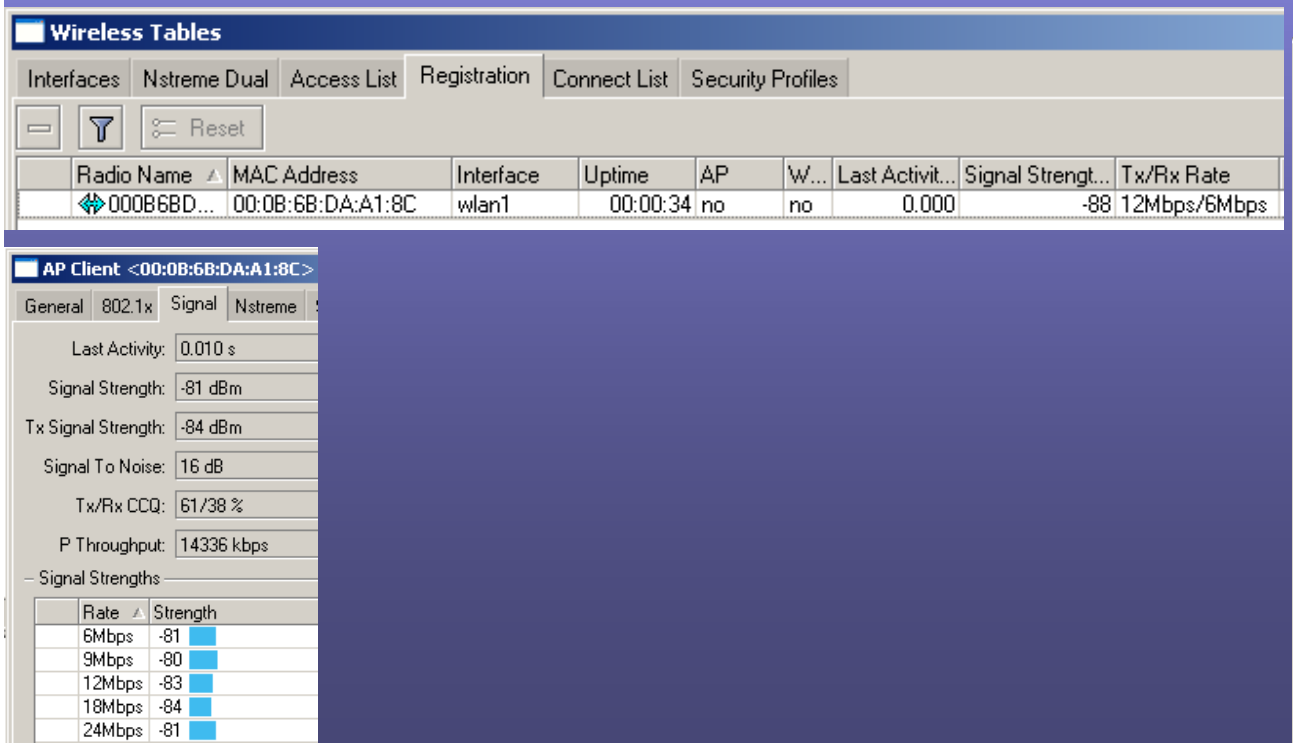
Client Troubleshooting

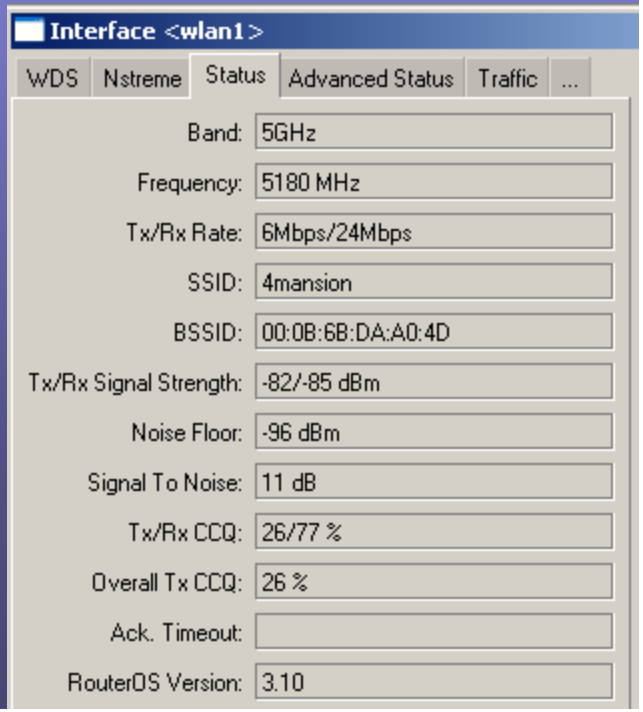
- Does the client have a valid IP for the CPE.
- Does the client have the proper DNS servers.
- Can you ping the CPE/AP?



CPE Troubleshooting

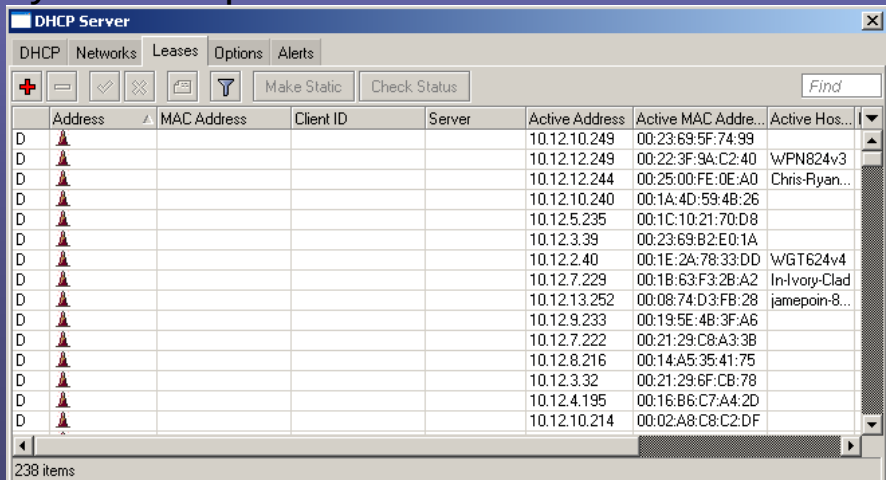
- Does the CPE show up in the AP's registration table?
- What does signal strength look like at both sides?
- Is the client flapping?





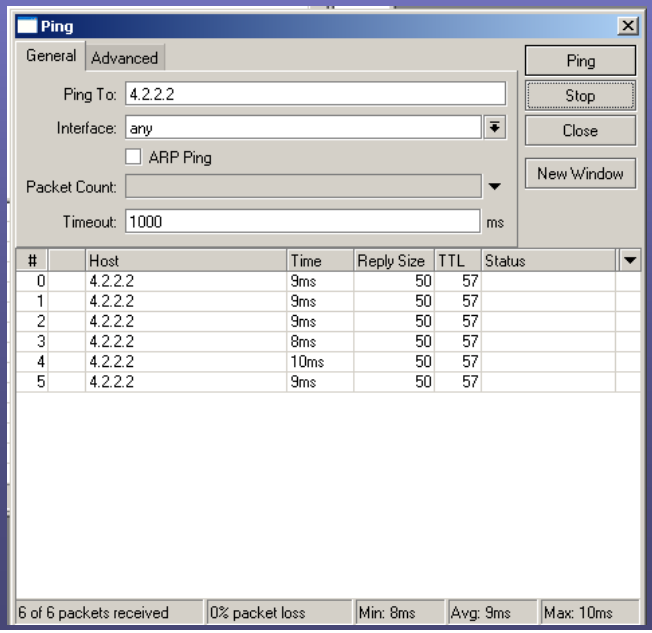
CPE Troubleshooting

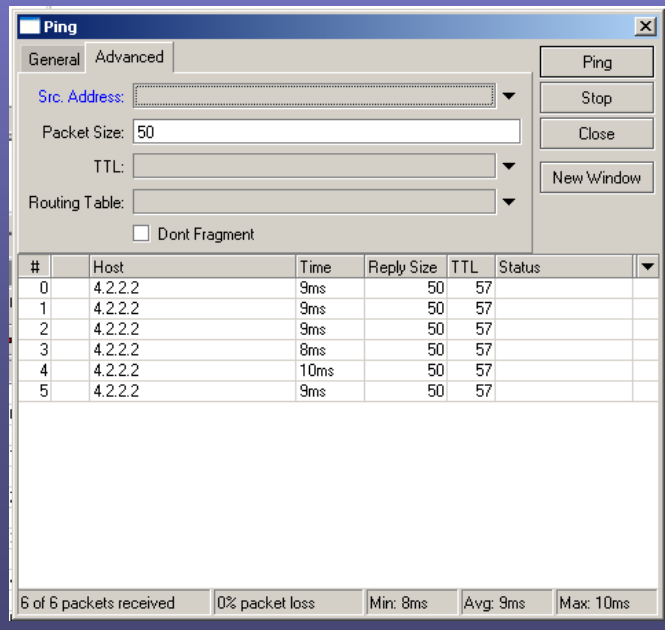
- Did the CPE pull an IP address from your DHCP server?
  - If not is your DHCP pool exhausted?
- Did the CPE pull an IP via PPPoE?
  - If not is your PPPoE pool exhausted?
  - Did the client fail authentication?
- The CPE is statically configured.
  - Did you use an IP address that is already in use?
  - 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.



Ping Tool

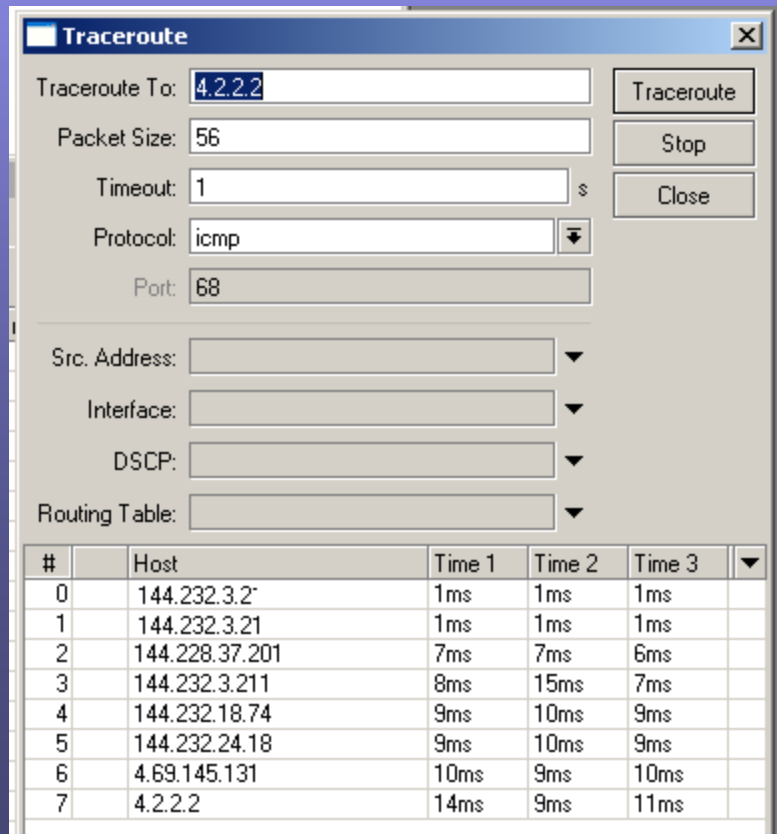
- /ping
- Source address can also be specified if you want the packet to appear to be sourced from a different interface.
- Packet size is useful for verifying MTU issues.





Traceroute Tool

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



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

Not only do I have to know how to reach my destination, but my destination has to know how to get back to me.

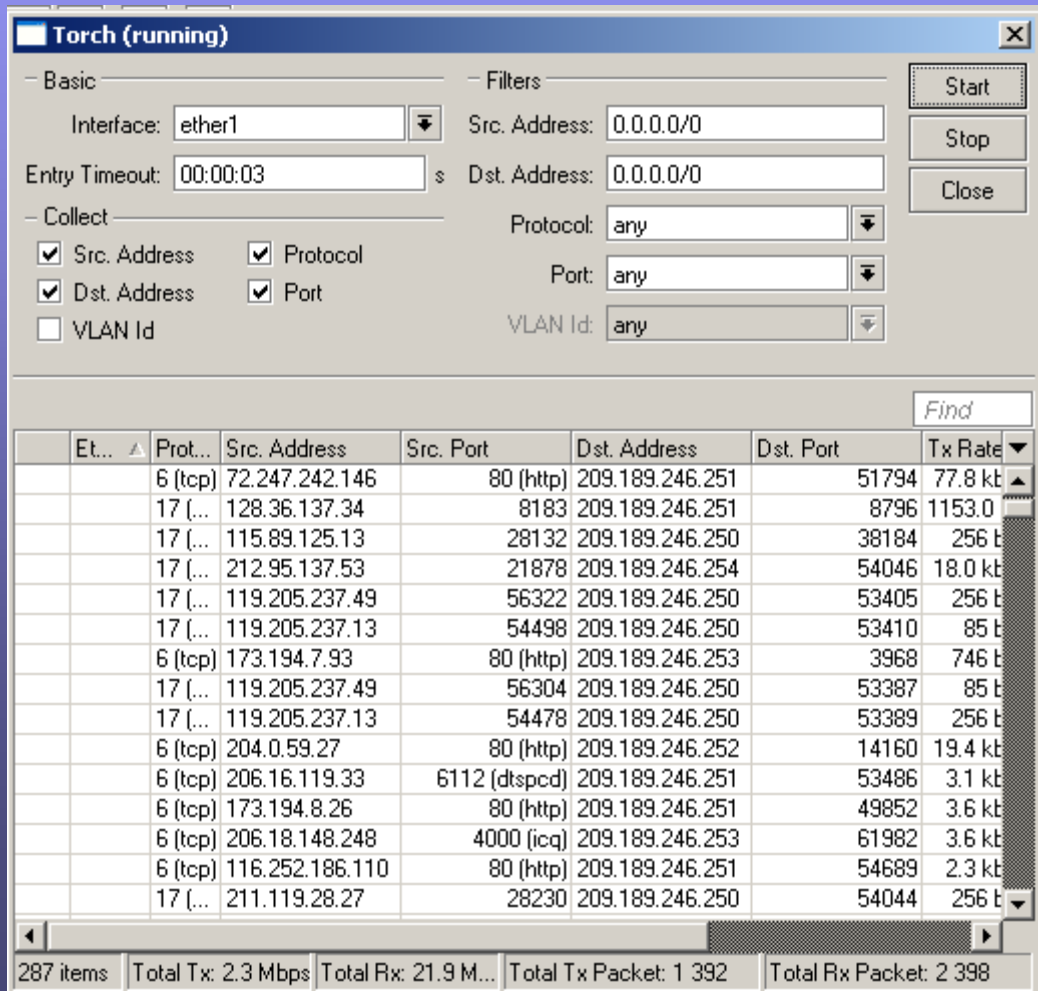
ISP Border Troubleshooting

- 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.

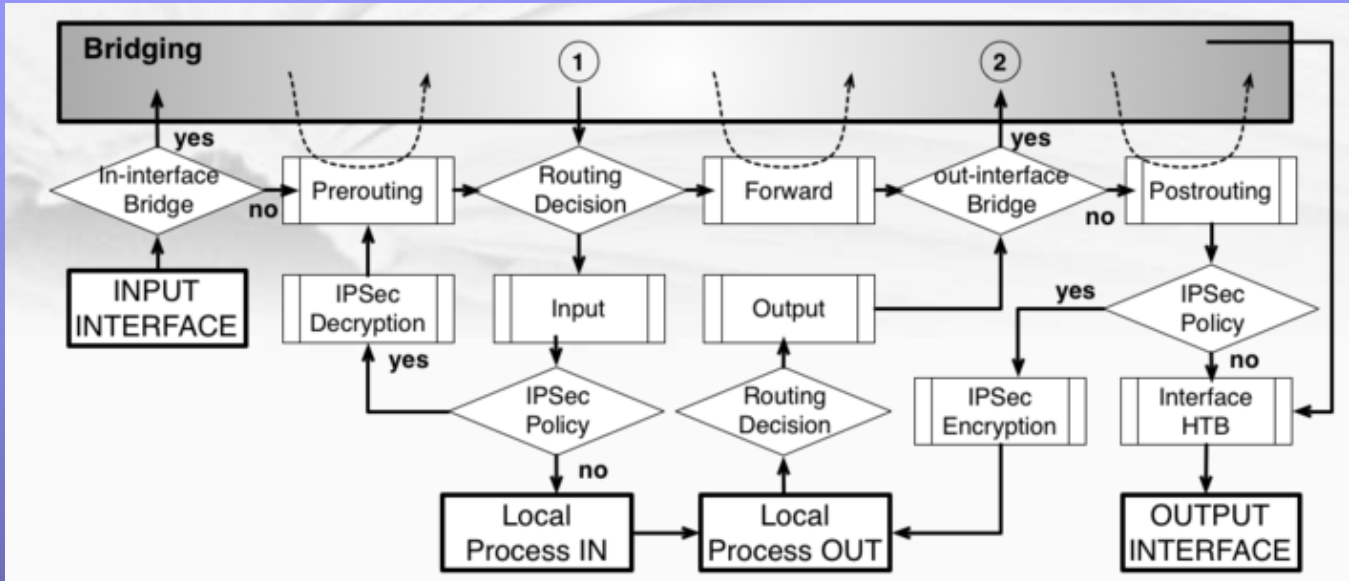


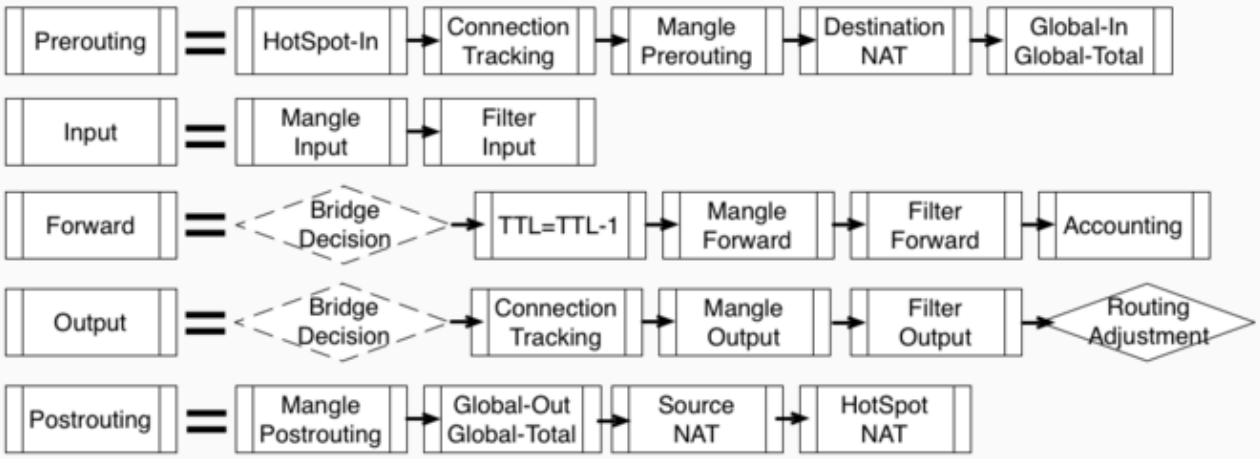
Advanced Troubleshooting - Mangle

- 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.

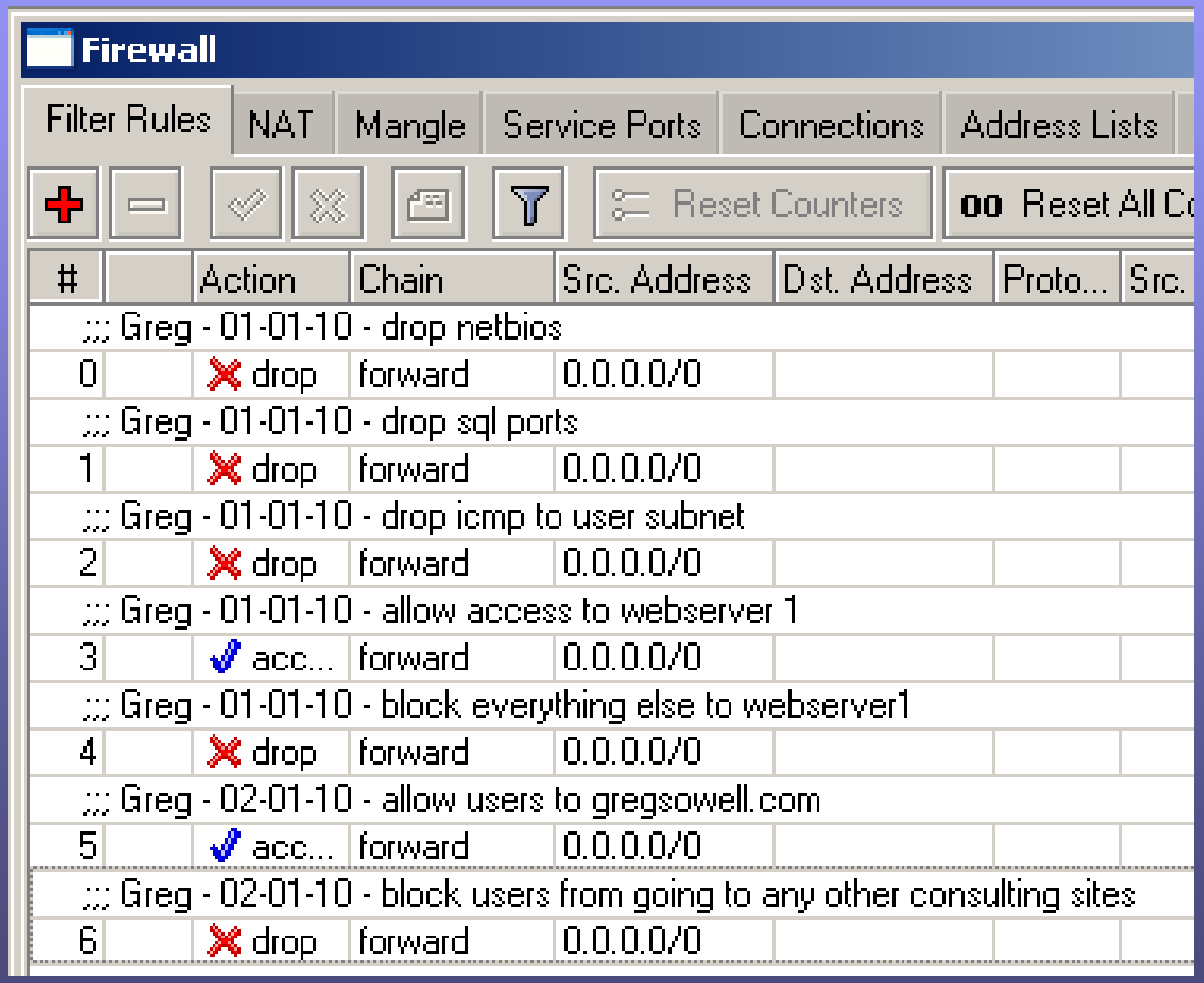




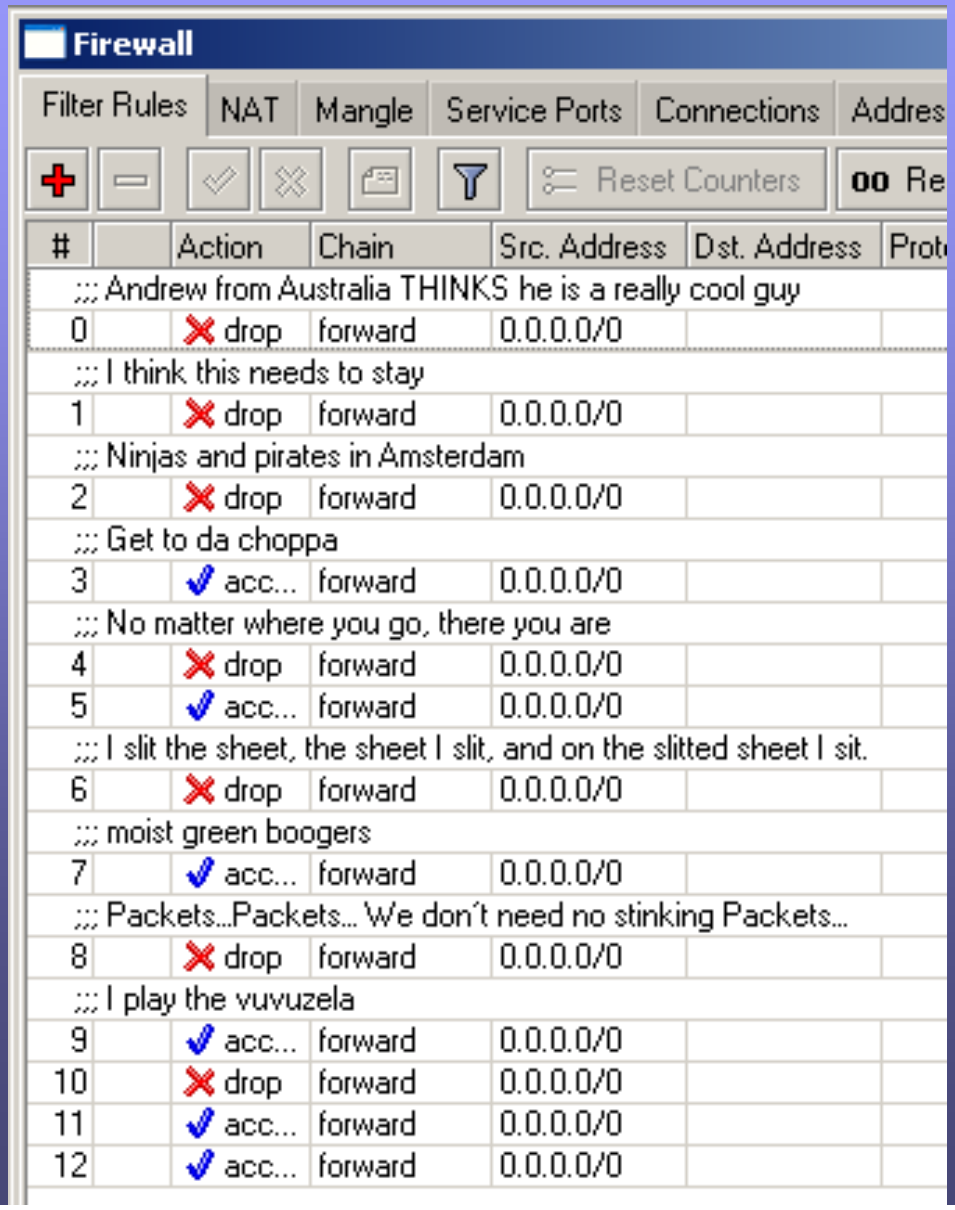
Common Mistakes - Comments

- 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.

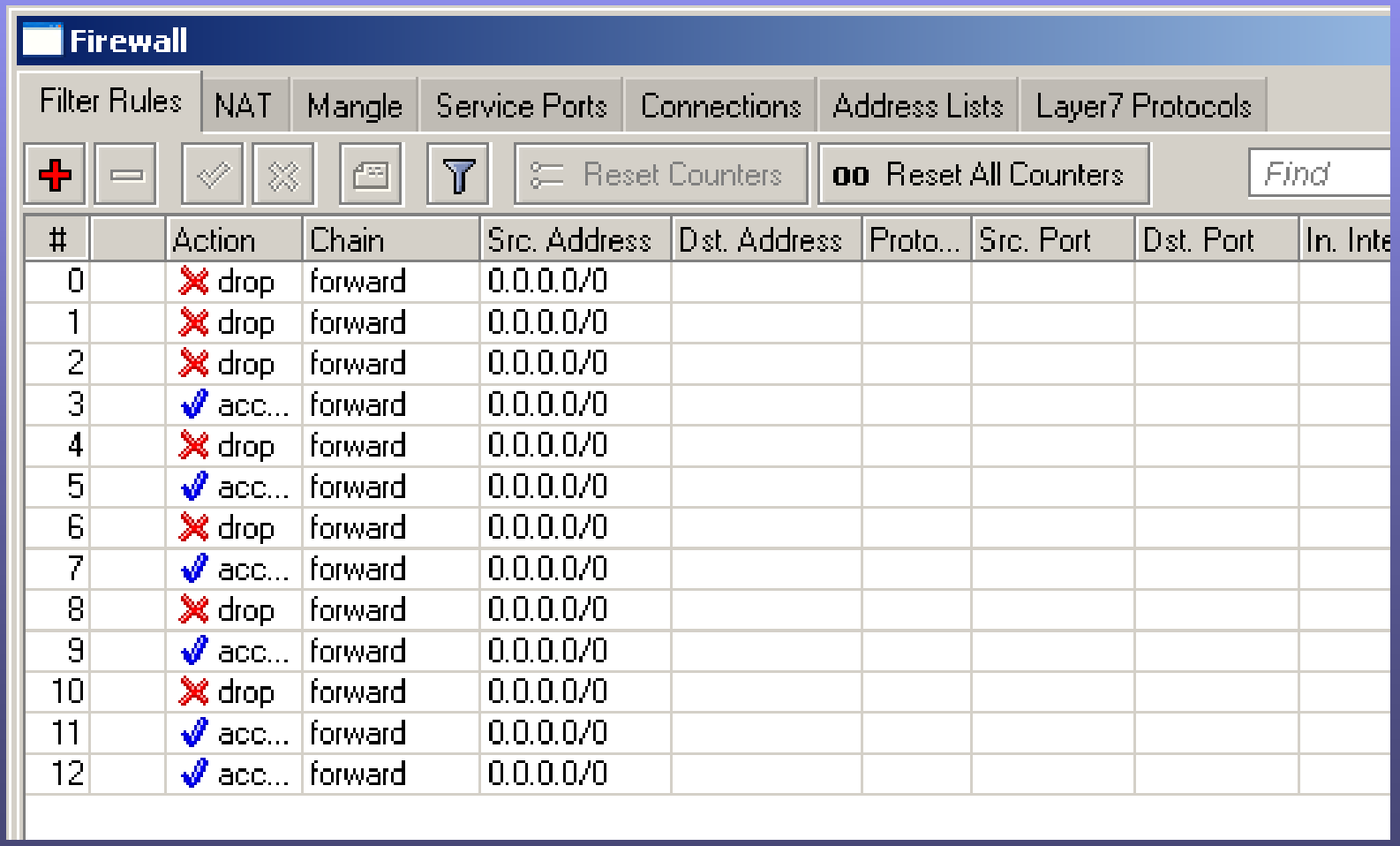
Common Mistakes – Comments - Good



Common Mistakes – Comments - Bad



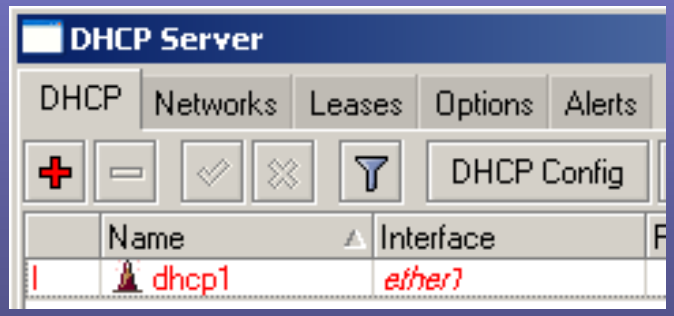
Common Mistakes – Comments - Worse

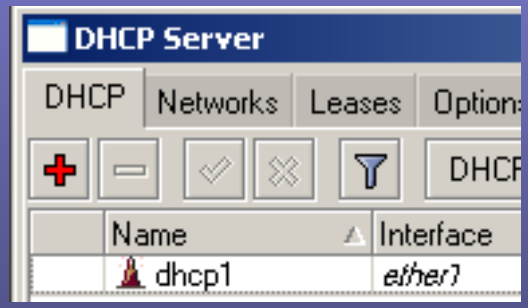


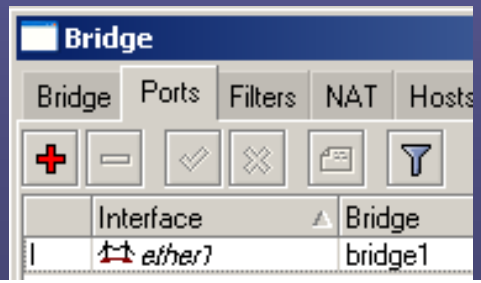
#		Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inte
0		drop	forward	0.0.0.0/0					
1		drop	forward	0.0.0.0/0					
2		drop	forward	0.0.0.0/0					
3		acc...	forward	0.0.0.0/0					
4		drop	forward	0.0.0.0/0					
5		acc...	forward	0.0.0.0/0					
6		drop	forward	0.0.0.0/0					
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					

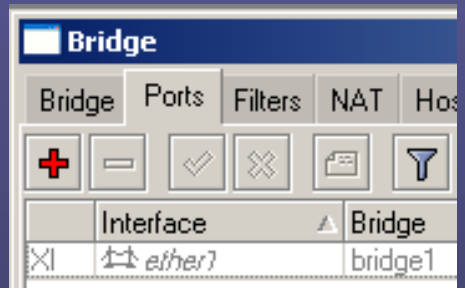
Common Mistakes - Services

- 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.









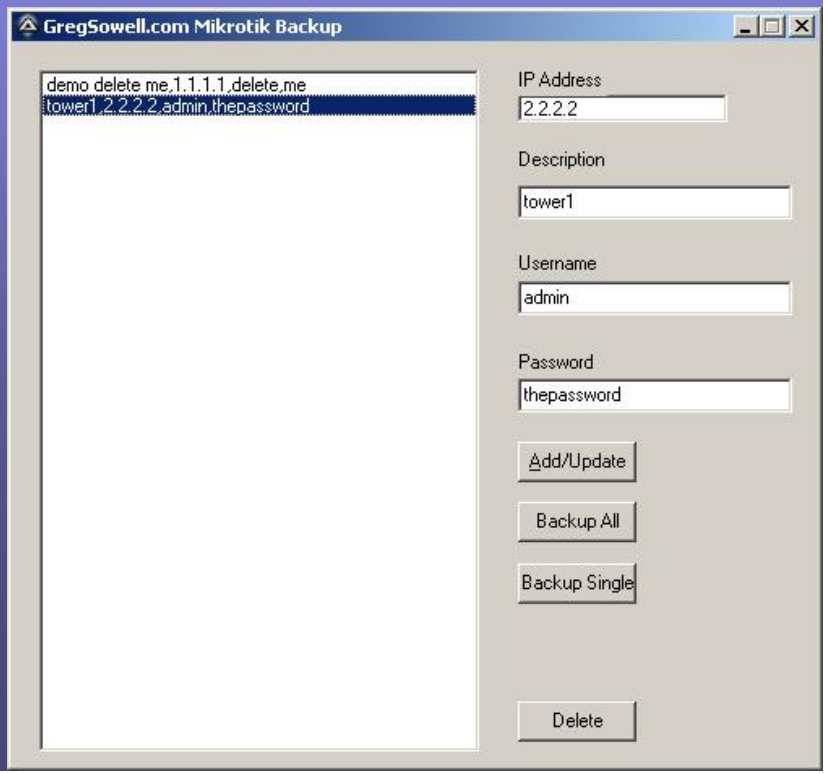
Common Mistakes - Addressing

- 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.

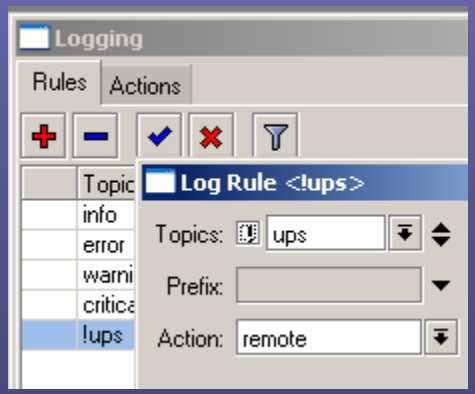


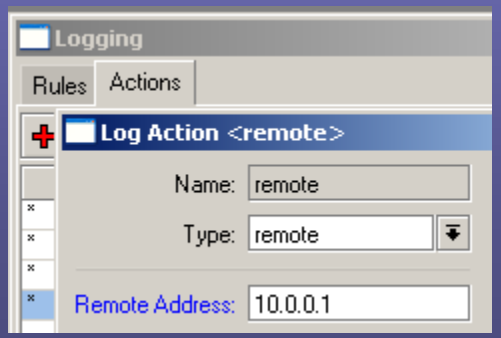
Common Mistakes - MTU

- 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

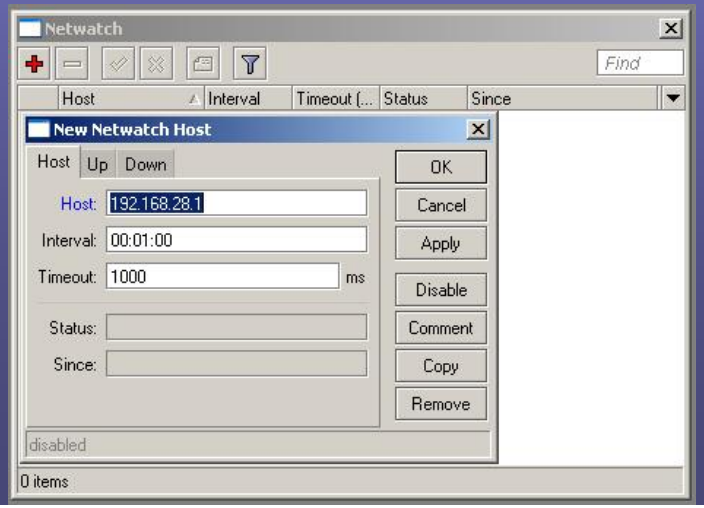
- Mikrotik has a fairly robust logging facility.
- You can log to memory, terminal or syslog server. My facility of choice is syslog.
- /system logging

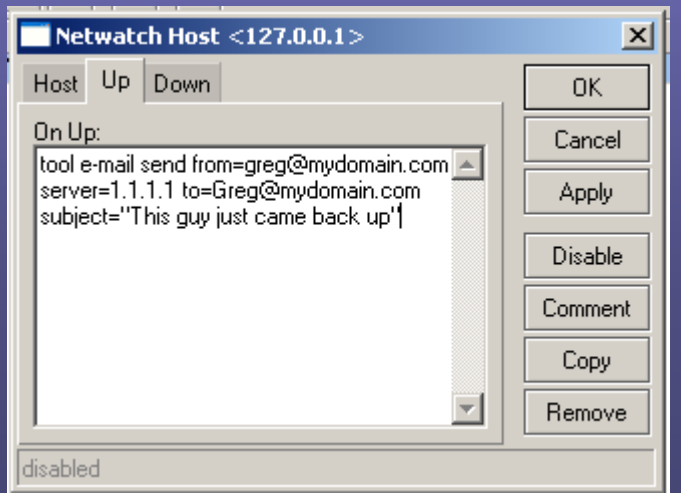




Additional Tools - Netwatch

- 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!