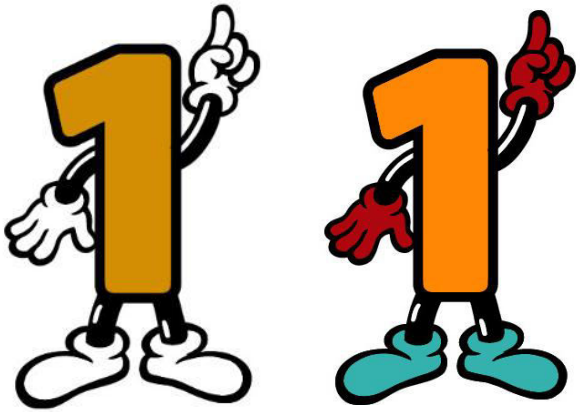


Network Troubleshooting & TCP/IP Utilities

1. Verification
2. Troubleshooting
3. Troubleshooting with the OSI model
4. Network Utilities
    - Ipconfig
    - Ping
    - Tracert
    - Nslookup

One thing before we hit troubleshooting.....

Verification refers to the process of confirming whether a network is working as designed

Troubleshooting

Follow-on process that occurs when the network is not working as designed

Tries to determine the real reason why the network is not working correctly, so that it can be fixed.

Least appreciated skill that technicians possess

We Could Hire A Trained Monkey To Do Your Job!

Troubleshooting

Process of diagnosing (identifying and fixing) the source of a problem

Most people get Microsoft certification, Cisco certs and college degrees

But

Not enough technicians sit down and try to really understand the troubleshooting methodology

&

How to grasp how you find the problem that you need to fix

Basic Troubleshooting Theory

Start with the most general (and often most obvious) possible problems
Then narrow it down to more specific issues

Troubleshooting revolves around three big ideas

Predicting what should happen

Determining what is happening that is different than what should happen

Figuring out why that different behavior is happening

Proper documentation must be maintained

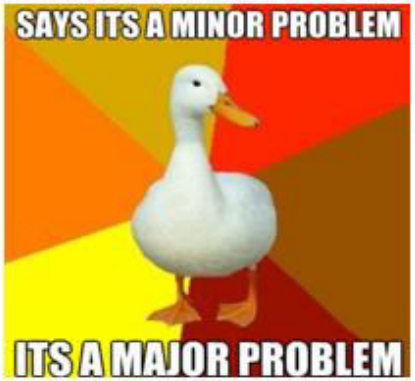
Problem encountered

Steps taken to determine the cause of the problem

Steps to correct the problem and ensure that it will not reoccur

Be careful, take your time and be slow i.e. better to be right than to be fast

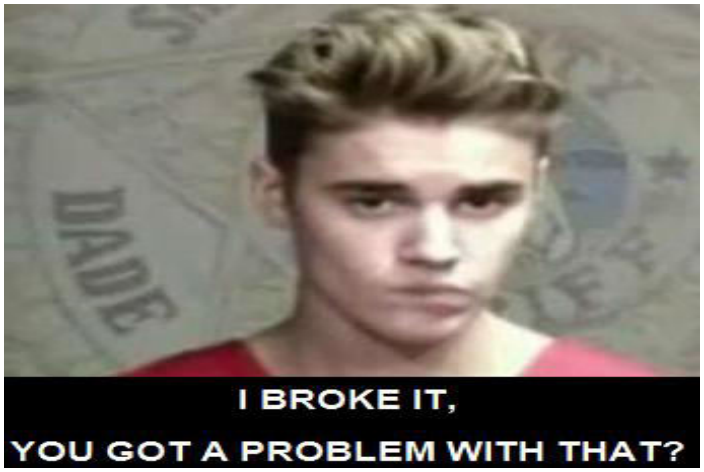
It's easy to fix one minor problem and then create a major problem



Be careful, go slow and before you take any action rethink it through your head 2/3 times

Realize, to fix something you may have to break something to make that thing work

e.g. take another thing offline, replace parts etc.

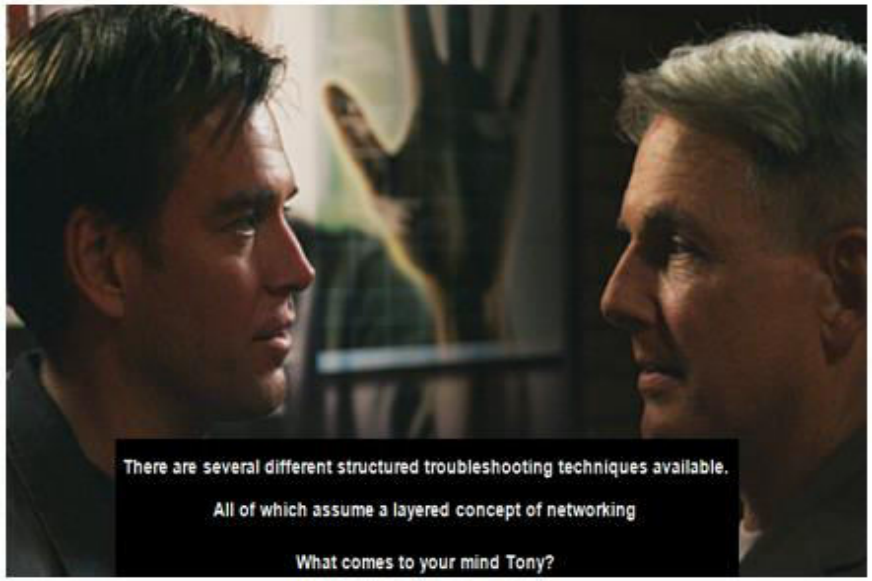


You may deal with technologies that are out of your specialty

If you run like a bull in a china shop, ripping stuff up then you need a new career.

Try and think three steps ahead
(If this is the problem, who do I call so I can get authorization to work on this matter)


Hey Boss,
What are the networking troubleshooting approaches?


There are several different structured troubleshooting techniques available.
All of which assume a layered concept of networking
What comes to your mind Tony?


Structure of these approaches makes them ideally suited
for the novice troubleshooter!

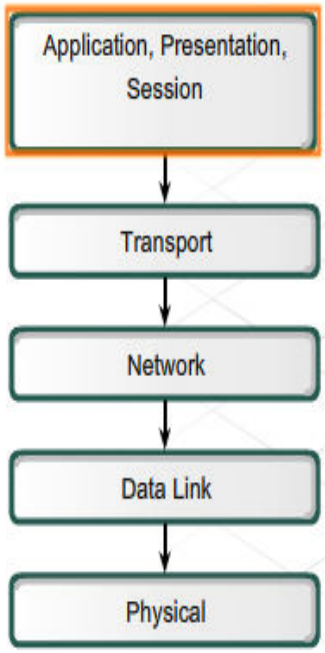

NCIS
More experienced individuals
(like me)
Often bypass structured approaches and
Rely on instinct and experience
(Trial and Error or Substitution)

Top-Down

Starts with the application layer and works down.

Looks at the problem from the point of view of the user and the application.

e.g. can the user access various web pages on the Internet, but not email?



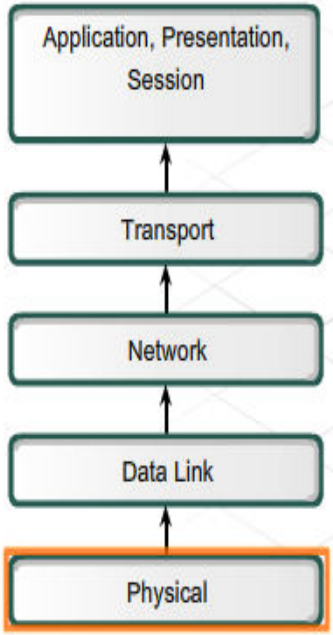
Troubleshooting Approach	How it operates	Cases for which it is suitable	Advantages/ Disadvantages
Top-down	Always starts at the application layer and works its way down until it finds a faulty layer.	More suitable for simpler problems or those that are suspected to be application/user or upper-layer related.	If the problem turns out to be related to lower layers, you have wasted a lot of time and effort at the upper or application layers.

Bottom-Up

Starts with the physical layer and works up.

Concerned with hardware and wire connections.

Have cables been pulled out of their sockets? Are equipment indicator lights on or off?

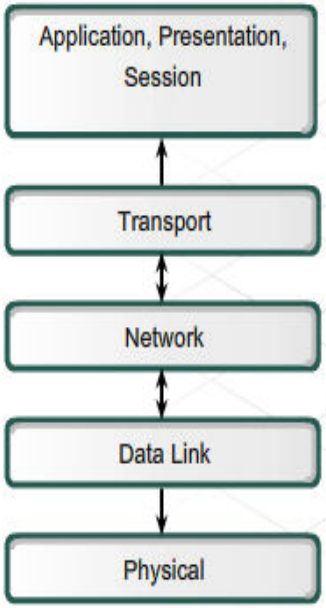


Troubleshooting Approach	How it operates	Cases for which it is suitable	Advantages/ Disadvantages
Bottom-up	Always starts at the physical layer and works its way up until it finds a faulty layer.	More Suited for complex cases.	It is a slow, but solid approach. When the problem is application (or upper layer) related, this approach can take a long time.

Divide-and-Conquer

Begins at one of the middle layers and works up or down from there.

e.g. troubleshooter may begin at the network layer, by verifying IP configuration information.



Troubleshooting Approach	How it operates	Cases for which it is suitable	Advantages/ Disadvantages
Divide-and-conquer	Based on the circumstances (reported issues) and your experience, you might decide to start at any layer and work up or down the OSI stack.	Most suitable when you are experienced and the problem has precise symptoms.	It approaches the layer of the culprit faster than the other approaches. You need experience to use this approach effectively.

Trial and Error

Relies on individual knowledge to determine the most probable cause of a problem.

Educated guess based on past experience and knowledge

Potential to be extremely

Can result in incorrect assumptions and overlooking simple solutions

Substitution

Problem is assumed to be caused by a specific hardware component/configuration file.

Defective part or code is replaced by a known good device or file e.g. a new cable

Relies on the availability of substitute parts, components

Help identify network problems.

Allows you to go out on the network and see if other computers/network are there?

e.g. IP config, Ping, Tracert, Nslookup (DOS commands)

IP config

Replaced winipcfg which ran on old Windows versions e.g. 95/98/ME
Shows basic TCP/IP configuration information
e.g. IP address, subnet mask, IP of default gateway

```
C:\Users\HJG>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : uci.edu
   IPv4 Address. . . . . . . . . . . : 169.234.xxx.xxx
   Subnet Mask . . . . . . . . . . . : 255.255.255.xxx
   Default Gateway . . . . . . . . . : 169.234.xxx.xxx
```

IP config /all

Shows additional TCP/IP information e.g. DHCP, DNS servers

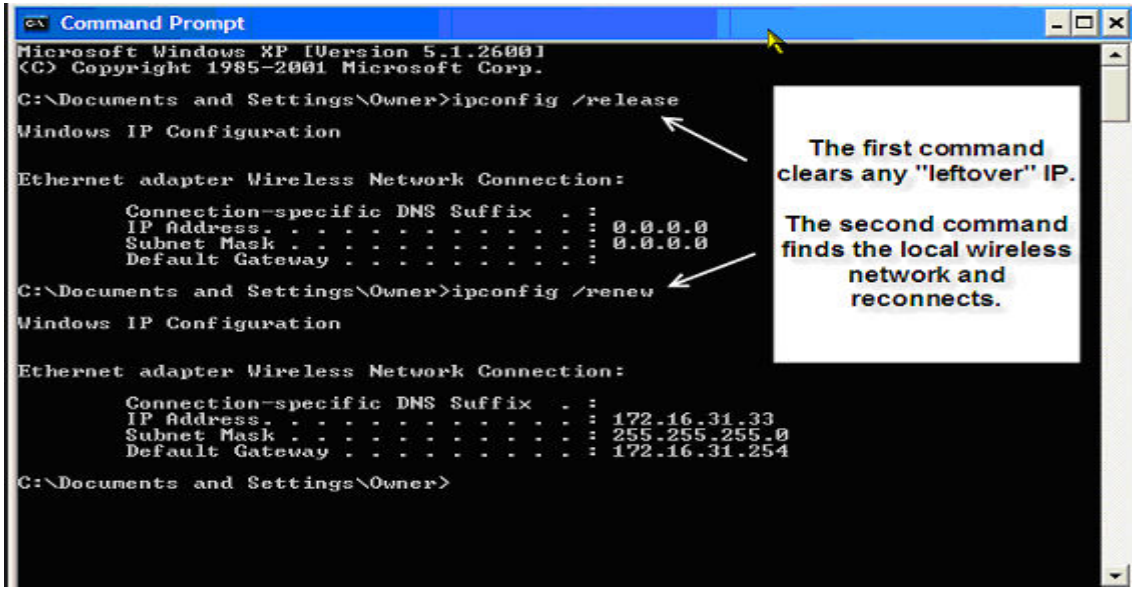
```
C:\>ipconfig /all

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6235
   Physical Address. . . . . . . . . : C8-F7-33-1A-C0-89
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::353b:3969:f4ff:f429%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, January 24, 2014 9:31:34 AM
   Lease Expires . . . . . . . . . . : Saturday, January 25, 2014 9:31:34 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 331937587
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-18-CA-95-C6-50-B7-C3-78-67-A

   DNS Servers . . . . . . . . . . . : 192.168.1.1
```

Ipconfig /release

Forces a client to give up its current IP address

After issuing a release command, your network adapter will no longer be able to connect to the network

Unless you use the command ipconfig /renew or you restart the adapter/computer



Ipconfig /renew

Obtain a new IP address

Once you make sure you are on the network
Then make sure you can talk to other computers on the network

Ping

Works on any device using TCP/IP

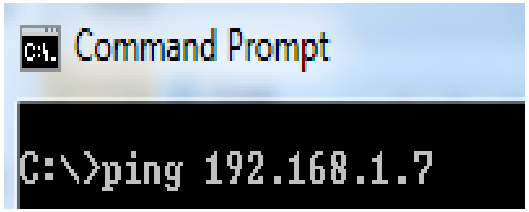
Determines if a computer (destination) is reachable & if its active or not

'hey computer 5 are you there?' ↔ Yes, I'm here

If no 'hi back' then you have a problem

Verifies end-to-end connectivity

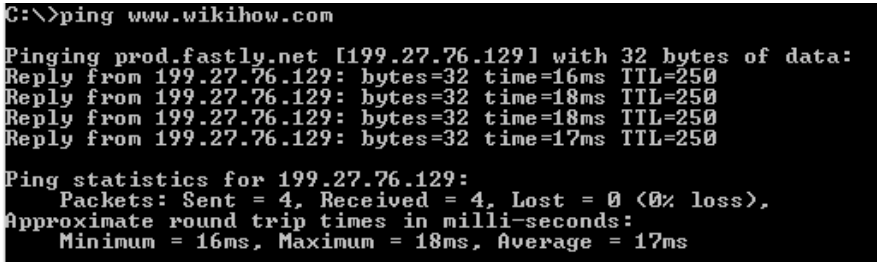
Does not indicate where the connection was actually dropped



Often used in DOS attacks so administrators turn off Ping and Echo reply

In the DOS world we can ping either the IP address or Domain Name

(domain name is the 'friendly name for the computer)



Ping talks to the DNS server and figures out what is the IP address and then pings it

If you type in **ping /?** Then you will get a list of arguments that you can use with the ping command

```
C:\>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
```

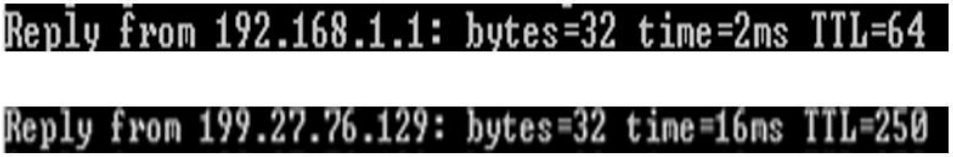
One of these arguments **–n** allows you put in how many pings that will happen
You send out 4 pings, 2 come back good, 1 weird and the next ok.
You now want to get an idea how dodgy is this network connection
Send out 200 pings and check the results (better idea of what's going on)

```
C:\>ping 192.168.1.1 -n 200

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

TTL (Time To Live)

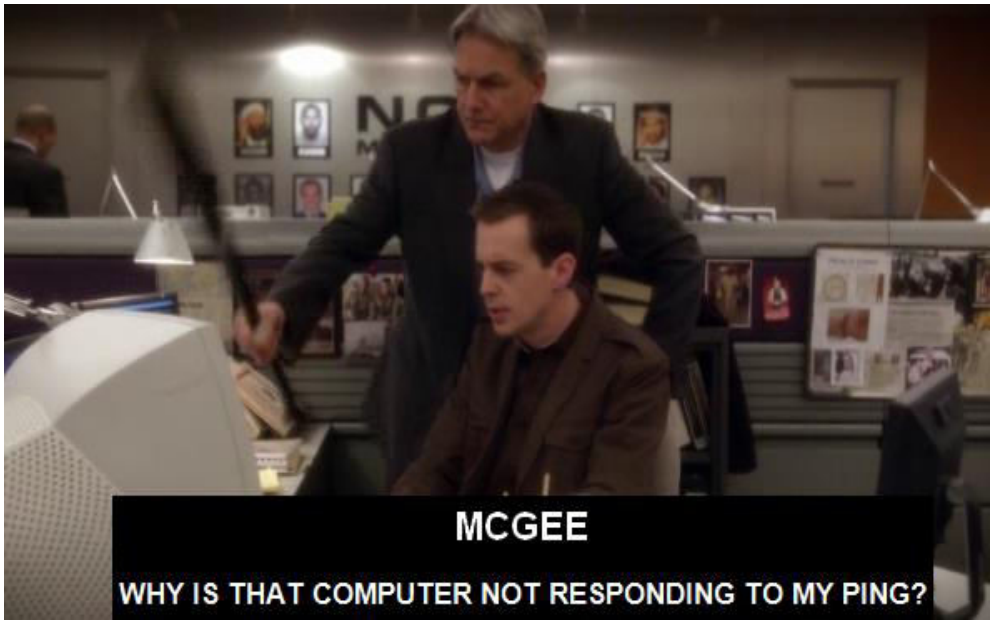
How quickly this communication happens (higher the number then delay in the system)

TTL says that if I do not hear a response within so many milliseconds, then I will assume that the ping failed.



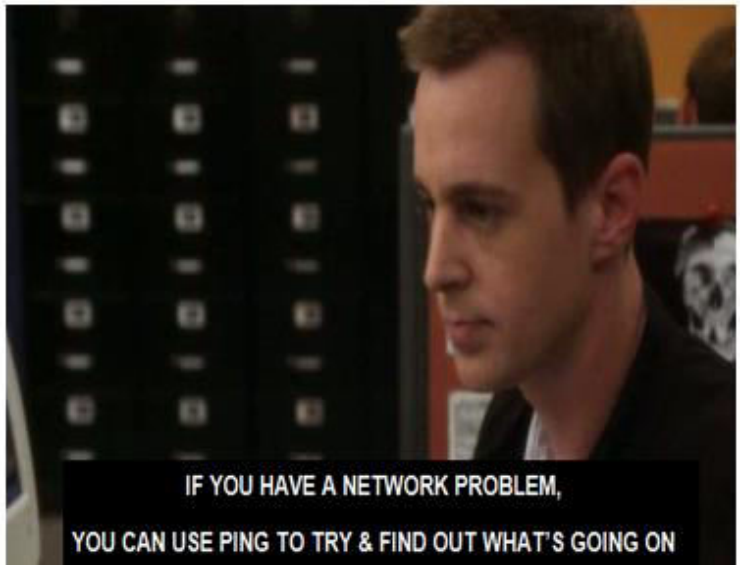
Sometimes, the server may be slow to respond to a ping request.

The connection may be poor and require a longer TTL i.e. “up” the TTL

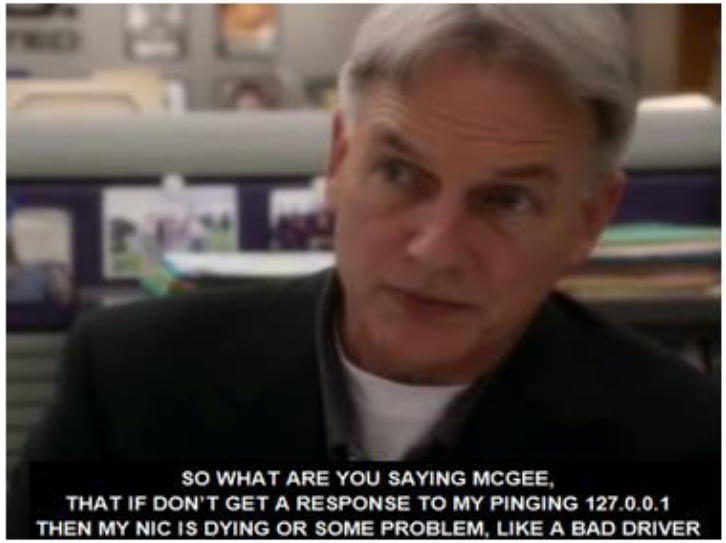


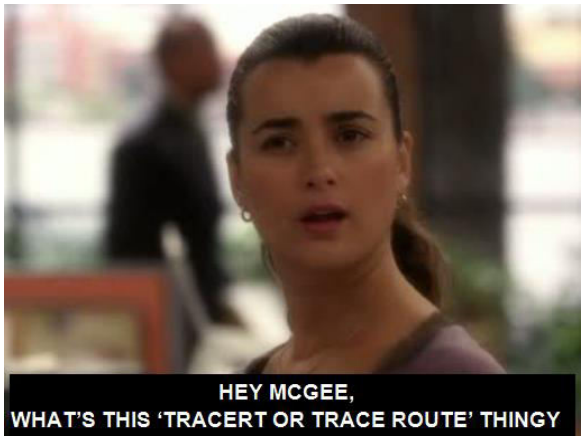
It is either off or broken
or
It may be configured to NOT respond to Ping traffic


WHAT ELSE CAN PING DO?


IF YOU HAVE A NETWORK PROBLEM,
YOU CAN USE PING TO TRY & FIND OUT WHAT'S GOING ON


FIRST THING TO DO BOSS IS PING 127.0.0.1
(YOU ARE BASICALLY PINGING YOURSELF)
If your NIC is installed properly with the drivers installed,
then you should be able to ping this loopback address (127.0.0.1)


SO WHAT ARE YOU SAYING MCGEE,
THAT IF DON'T GET A RESPONSE TO MY PINGING 127.0.0.1
THEN MY NIC IS DYING OR SOME PROBLEM, LIKE A BAD DRIVER

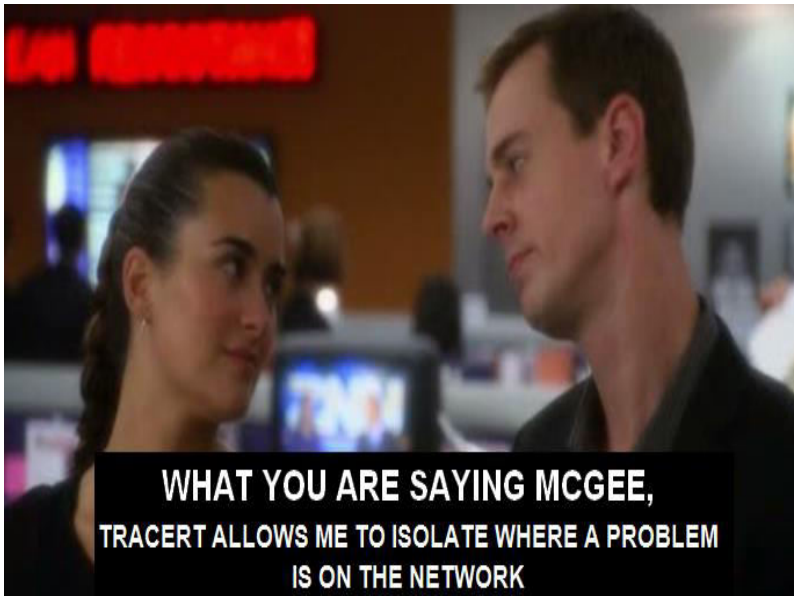


You're at your computer trying to access a server

As your packets go through the different hops to get to that server

Tracert will send a reply back to you for each router it goes through

So if there a problem, then you know exactly where the traffic stopped

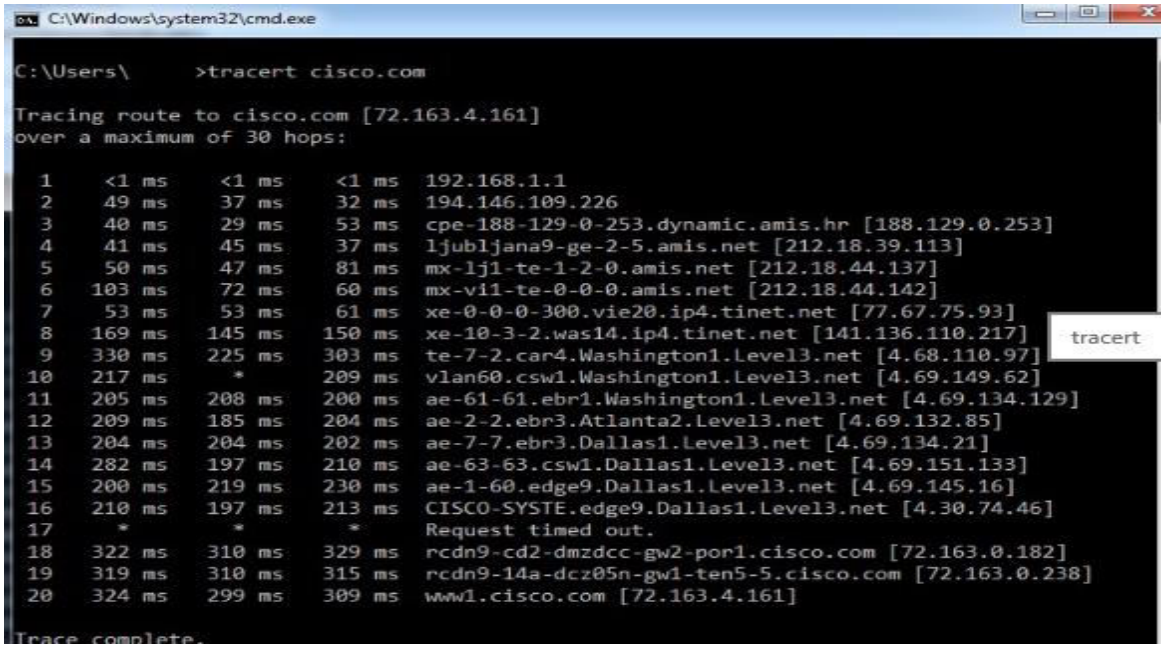

WHAT YOU ARE SAYING MCGEE,
TRACERT ALLOWS ME TO ISOLATE WHERE A PROBLEM
IS ON THE NETWORK


TRACERT IS LIKE PING
BUT
GIVES YOU AN ECHO RESPONSE FROM EACH NETWORKING
DEVICE THAT IT GOES THROUGH

With Tracert, you actually see the hops (routers) in order to get to cisco.com

Allows the user to observe the flow of information
(path a packets takes to reach its destination)

1st hop will be the default gateway



Use to discover where a problem lies

Identify where a packet may have been lost or delayed

Due to bottlenecks or slowdowns in the network.

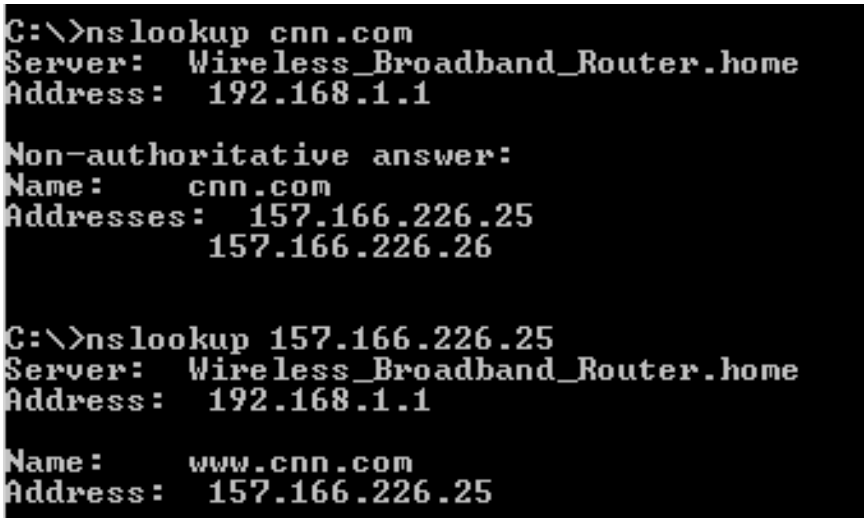
Basic Tracert utility will only allow up to 30 hops between a source and destination
Before it assumes that the destination is unreachable

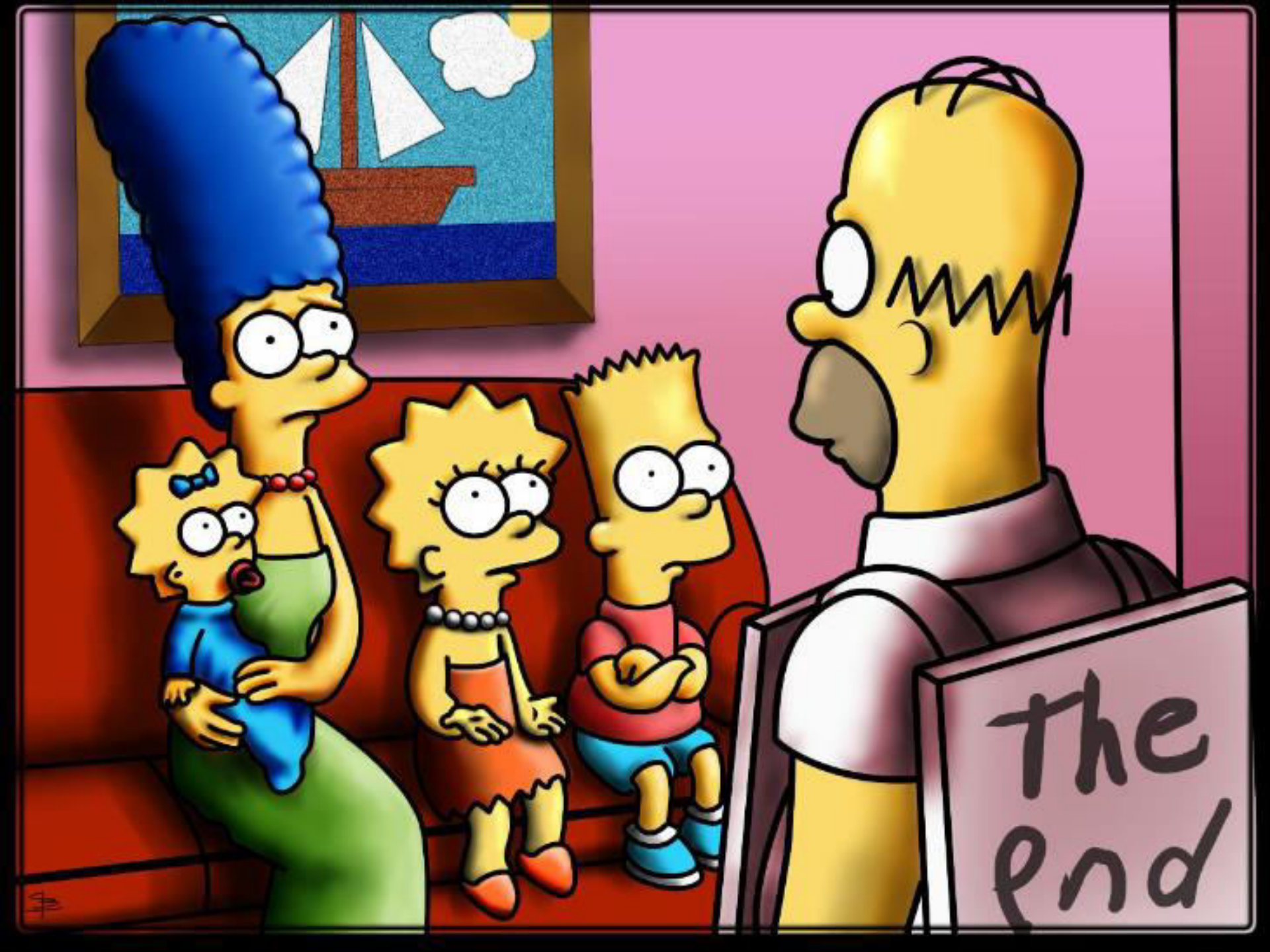
```
C:\Users\support.usonyx>tracert usonyx.net

Tracing route to usonyx.net [113.197.35.228]
over a maximum of 30 hops:

  1     1 ms     3 ms     1 ms  192.168.0.1
  2    81 ms    11 ms    11 ms  cm1.kappa104.maxonline.com.sg [58.182.104.1]
  3    17 ms     9 ms     7 ms  172.20.31.1
  4     8 ms    11 ms    11 ms  172.26.32.1
  5     9 ms    12 ms     9 ms  172.20.7.6
  6    11 ms    10 ms    19 ms  s6-0-1-2-r10.cyberway.com.sg [203.116.8.37]
  7     9 ms    11 ms    11 ms  203.117.164.34
  8   160 ms   188 ms   104 ms  maxwell-GE-6-1.singnet.com.sg [165.21.12.111]
  9    13 ms    10 ms    11 ms  165.21.240.86
 10    14 ms    10 ms    12 ms  113.197.32.250
 11    15 ms    10 ms    13 ms  usonyx.net [113.197.35.228]

Trace complete.
```

Indicates how long a packet takes to get from the source to each hop and back
(round trip time)

Nslookup (Name Services Lookup)

Allows an end-user to look up information about a particular DNS name in the DNS server




The End