



Troubleshooting Network

Topics To Cover :

- ❑ Introduction to troubleshooting
- ❑ Troubleshooting Methodology
- ❑ Troubleshooting Network devices
- ❑ Troubleshooting Network Slowdowns
- ❑ Troubleshooting Wireless devices
- ❑ TCP/IP Troubleshooting Utilities



❑ Introduction to troubleshooting



- One of the hardest things you'll come up against in troubleshooting network issues is identifying exactly what the problem is.
- Confirm that the computer can reach a remote host.
- Some tools to troubleshoot ping, traceroute / tracert, nslookup

❏ Troubleshooting Methodology



➤ Troubleshooting methodology contains seven steps:

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory of probable cause.
4. Establish a plan of action and identify potential effects.
5. Implement the plan or escalate.
6. Verify full system functionality.
7. Document findings, actions, and outcomes.

1. Identify the problem:

- This step involves gathering information to learn what is actually occurring or not occurring and where.

- Multiple problems should be approached individually and handled one at a time.

- Many problems that are reported within a network are the result of an end user needing to be educated, or re-educated, in proper procedures.

- Determining if anything has changed will often help in identifying the problem.



2. Establish a theory of probable cause:

- To develop this list of possible causes, he or she should consider multiple approaches to the problem, from bottom to top and then from top to bottom of the OSI model.
- The list of possible causes should then be divided into three ranked sections. They should be "not likely," "likely," and "most likely."
- e.g. if the network printer doesn't work, the first step should be to make sure that it is turned on.



3. Test the theory of probable cause

- If the theory is confirmed, the technician should move on to the next step.
- If the theory is proven to be incorrect, then it will be necessary to reestablish a new theory of probable cause.
- If the issue persists, escalate the issue up the troubleshooting chain.

4. Establish a plan of action and identify potential effects:

- Once issue has confirmed a theory of probable cause, the next step is to establish a plan of action and identify potential effects.
- In some cases, it is a good idea for a technician to write the plan out step by step in order to determine the best course of action.
- This plan should also identify any possible repercussions that the resolution to the problem may introduce into the network.



5. Implement the plan or escalate:

- To implement the plan or to escalate the problem.
- If a technician has the authority, he or she can put the plan into action.
- If not, the technician should escalate the problem along with all of the facts and determinations up the troubleshooting chain.



6. Verify full system functionality:

- Once the plan has been implemented, next is to verify full system functionality.
- Technicians should not just verify that the original problem has gone away. Sometimes a fix will introduce a new issue into the system.
- If a new issue has occurred, it's time to go back to step one, or to escalate the problem.
- If a technician has verified full system functionality, it is time to implement any appropriate preventative measures that could keep the problem from reoccurring.



7. Document findings, actions, and outcomes:

- This will save time if and when the problem reoccurs.
- A technician's documentation may lead to new best practices for an organization.
- It's important to document any missteps as well to keep the next technician from making those same missteps.
- Documenting missteps is also important; it will keep the next technician from making the same missteps.

❑ Troubleshooting Network devices



➤ Diagnosing IP Addressing Problems:



```
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\mirox3>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : domain.name
    Link-local IPv6 Address . . . . . : fe80::f165:6a64:af16:b1c0%11
    IPv4 Address. . . . . : 192.168.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::b8c1:a2ff:fe18:ad94%11
                                192.168.2.1
```

- One of the first steps in troubleshooting a network connection problem is figuring out if you have a valid IP address, and if it was configured automatically or manually.



- To see all of the information about your network adapter, go to command prompt and type `ipconfig /all`, and press enter.
- Check the option that says DHCP Enabled. If it says no, it means that at some point a static IP address was configured.
- If the network DHCP Enabled, then look at your IPv4 Address, Subnet Mask and Default Gateway.

➤ Diagnosing Hardware Issues:



- If the computer will not connect to the network at all, and it doesn't connect to other networks, it's a good chance that have a hardware problem.
- Check the drivers to make sure there are no issues or updates, but if it isn't a driver issue, check the NIC card.

➤ Diagnosing DNS Server Problems:

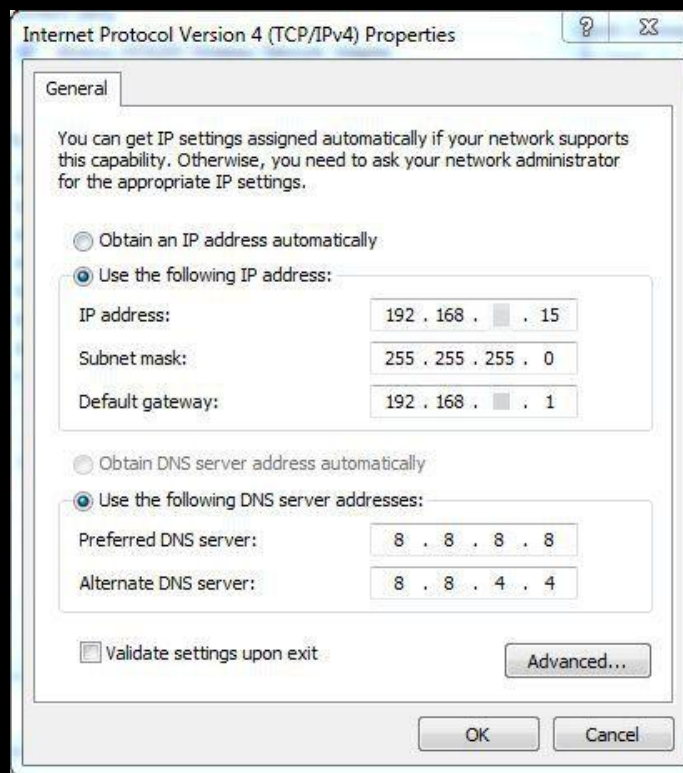


- Network is connected, but not to the internet, there will be a chance to have DNS Server problem.
- Router will have a built in DNS server, check the DNS Server as it shows the ISP DNS as well as Google DNS Server IP Address.
- Google DNS Server IP Addresses:

IPv4: 8.8.8.8 and 8.8.4.4

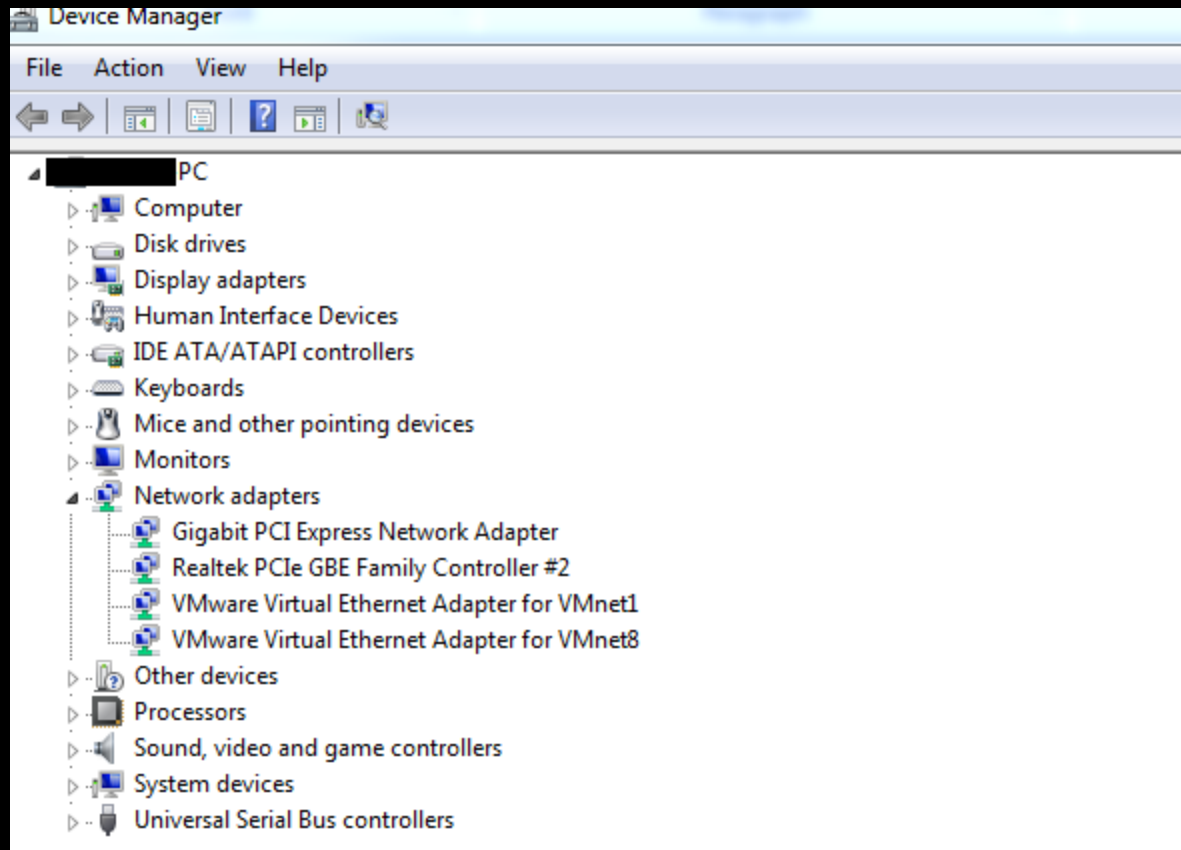
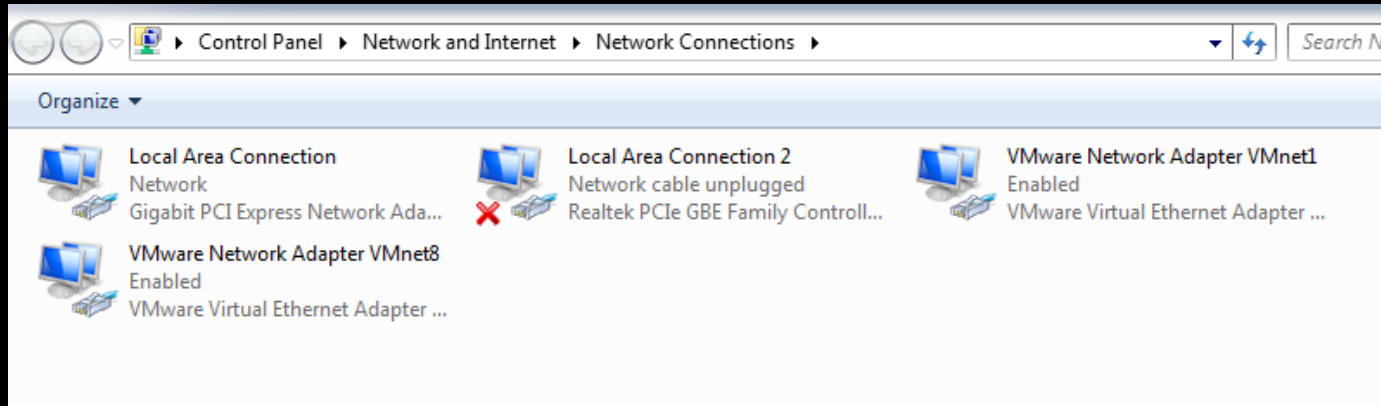
IPv6 : 2001:4860:4860::8888 and 2001:4860:4860::8844

➤ Fixing IP Addressing Issues:



- Check the Network Adapter settings in **Change adapter settings** option.
- If the Network have a DHCP Server, then configure the settings as **Obtain an IP address automatically**.
- Check the DNS Server address.

➤ Updating a Driver:





➤ MAC Address Restrictions:

- Routers support a feature called MAC address filtering.
- Disabled by default, router administrators can turn this feature on and restrict connections to only certain devices according to their MAC address number.

➤ Loose or Disconnected Cables:

- The router is turned off, or someone in the family accidentally unplugs power to it.
- Any Ethernet cables are firmly seated - the connectors should make a clicking sound when snapping into position.
- Ensure any modem cables are connected properly.

➤ Overheating or Overloading:

- Downloading large files or streaming data for long periods causes a home network router to generate heat.
- An overheated router will behave unpredictably, eventually disconnecting devices from the local network and crashing.
- Shutting down the router and allowing it to cool down solves the problem temporarily, but if this issue occurs often, ensure the router has proper ventilation.
- Consider adding a second router to the network in these cases to better handle the load.



➤ Defective or Outdated Hardware or Firmware:

- Lightning strikes or other electrical power surges can also damage the circuitry of network equipment.

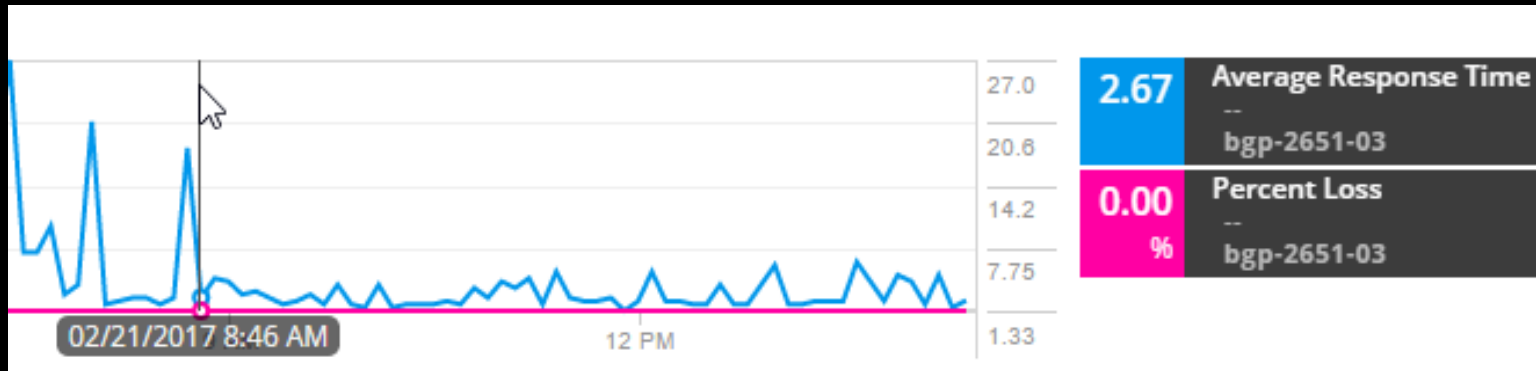
- Consider keeping some spare cables and a cheap backup router to help with emergency troubleshooting.

- Before finally giving up a router, try updating the router's firmware first.

- Sometimes no firmware update will be available, but in other cases newer firmware may contain fixes for overloading or signaling issues.



❏ Troubleshooting Network Slowdowns



➤ Bad NICs:

- Intermittent network errors, particularly those isolated to a specific workstation or server, can often be traced to a failing network interface card.
- Inspect the card's LED link lights.
- A solid green (or amber) LED indicates the NIC has a good active physical connection with another network device. A flashing green (or amber) LED shows active connection and is processing network traffic.



➤ Failing Switches/Routers:

- Rebooting or power cycling the WAN modem can often return the network to proper operation.

- Often the best remedy for inconsistent network outages and/or slowdowns is to reboot or power cycle the network's routers/switches.

➤ NetBIOS conflicts:

- NetBIOS, still in use on many Windows NT 4.0 networks in particular, contains many built-in processes to catch and manage conflicts.
- The result can be inaccessible file shares, increased network congestion, and even outages.
- when two systems are given the same computer name.

➤ IP conflicts:

- Windows typically prevents two devices with the same IP address from logging on to the same network (when using DHCP).
- one system could receive an address automatically, while another computer logs on using a static address specified by a user.
- When such conflicts occur, network slowdowns result (and the systems sharing the same address frequently experience outages).

➤ Spyware/Virus infestation:

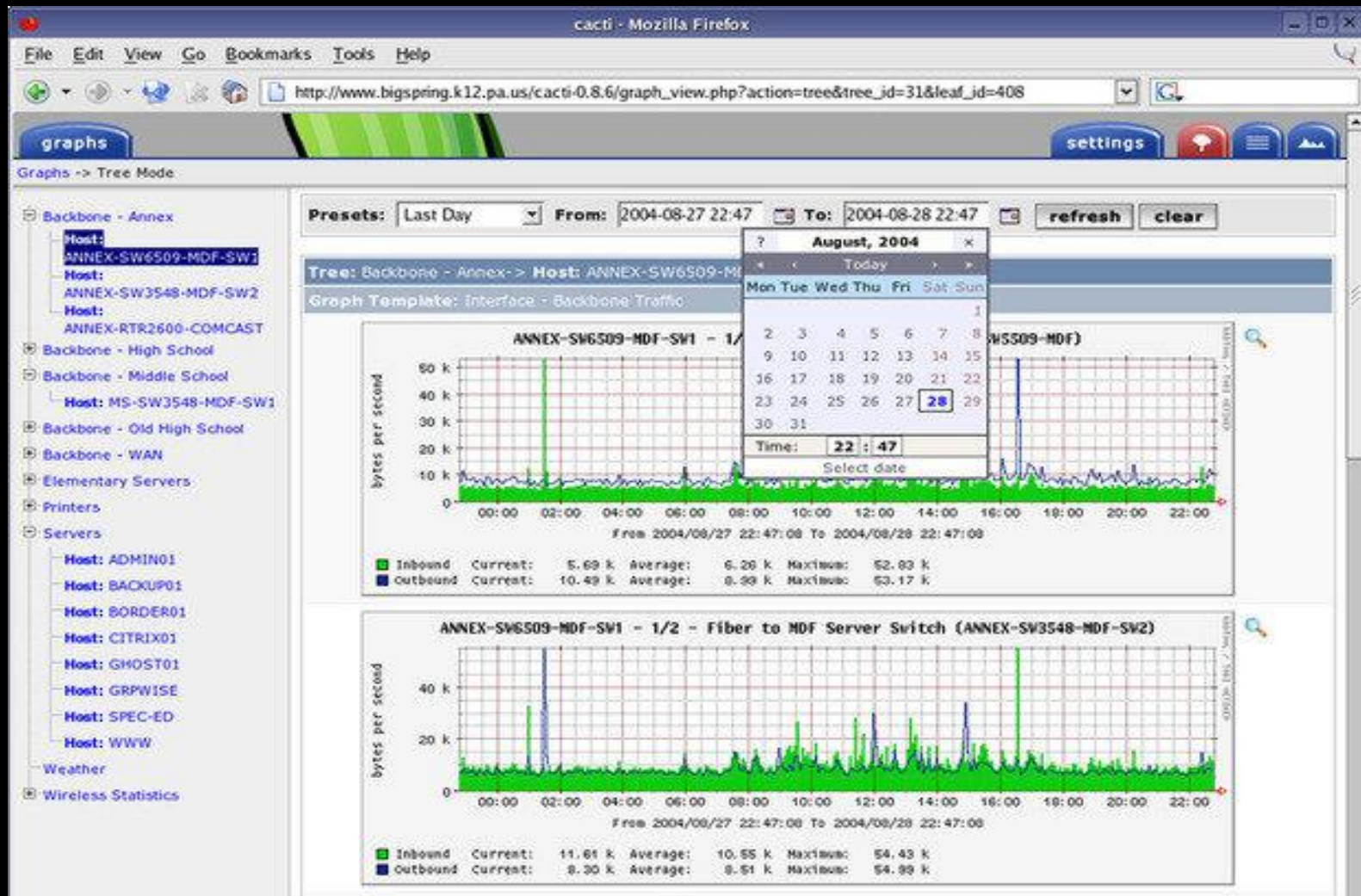
- Implement strong user policies and either gateway-based protection or individual client applications to prevent Spyware/Virus programs from consuming precious network bandwidth.

➤ Insufficient bandwidth:

- Network just doesn't have the throughput it requires.
- Besides boosting up- and downstream speeds, some networks may require additional dedicated connections.
- Some organizations may need to upgrade existing 10/100 Mbps networks to gigabit speeds.
- By upgrading NICs, cabling, and devices to 10/100/1000 Mbps equipment and replacing any remaining hubs with switches many firms can realize significant capacity gains.
- Necessary to subnet networks to localize particularly intense traffic to specific network segments.

➤ Bandwidth bottleneck on the network:

- Verify the usage statics on the Switches and Routers.



❑ Troubleshooting Wireless devices



➤ Check WAN and LAN connections:

- Check all wireless access point (AP) or wireless router ports to ensure that Ethernet cables are inserted tightly and link status LEDs are green at both ends.



➤ Verify wireless adapter:

- Check the wireless network adapter from the Network Connections Control Panel and check to see if its status is Enabled.

➤ Verify AP and router settings:

- Use wireless access point or router's administrative GUI to verify network settings for the wireless network service set identifier (SSID) to which your Wi-Fi client is trying to connect.

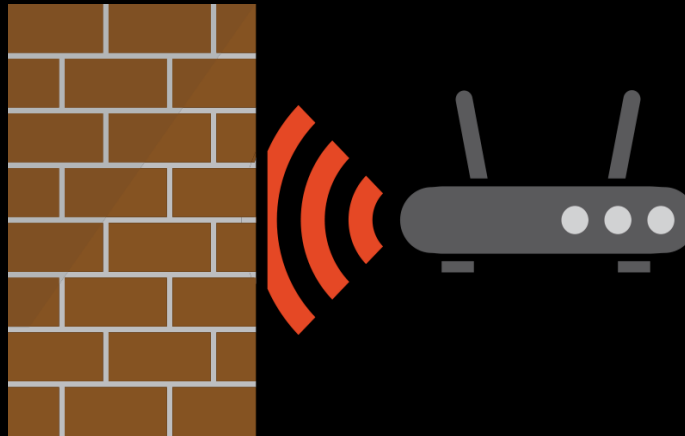
➤ Verify network connection with Ping:

- If the wireless client has a valid IP address, use ping to verify network connectivity.

➤ Look for a security mismatch:

- The client must support the security mode the AP or router requires: Open, WEP, WPA or WPA2.

➤ Interference from walls and floors:

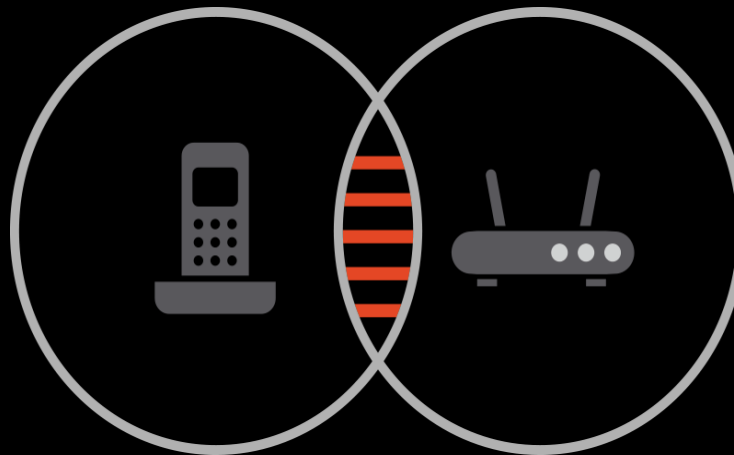


- The construction materials can greatly affect wireless communication speed and range.
- Even just a few inches or a couple of feet can make a big difference in signal strength.

- Interference from competing Wi-Fi networks:



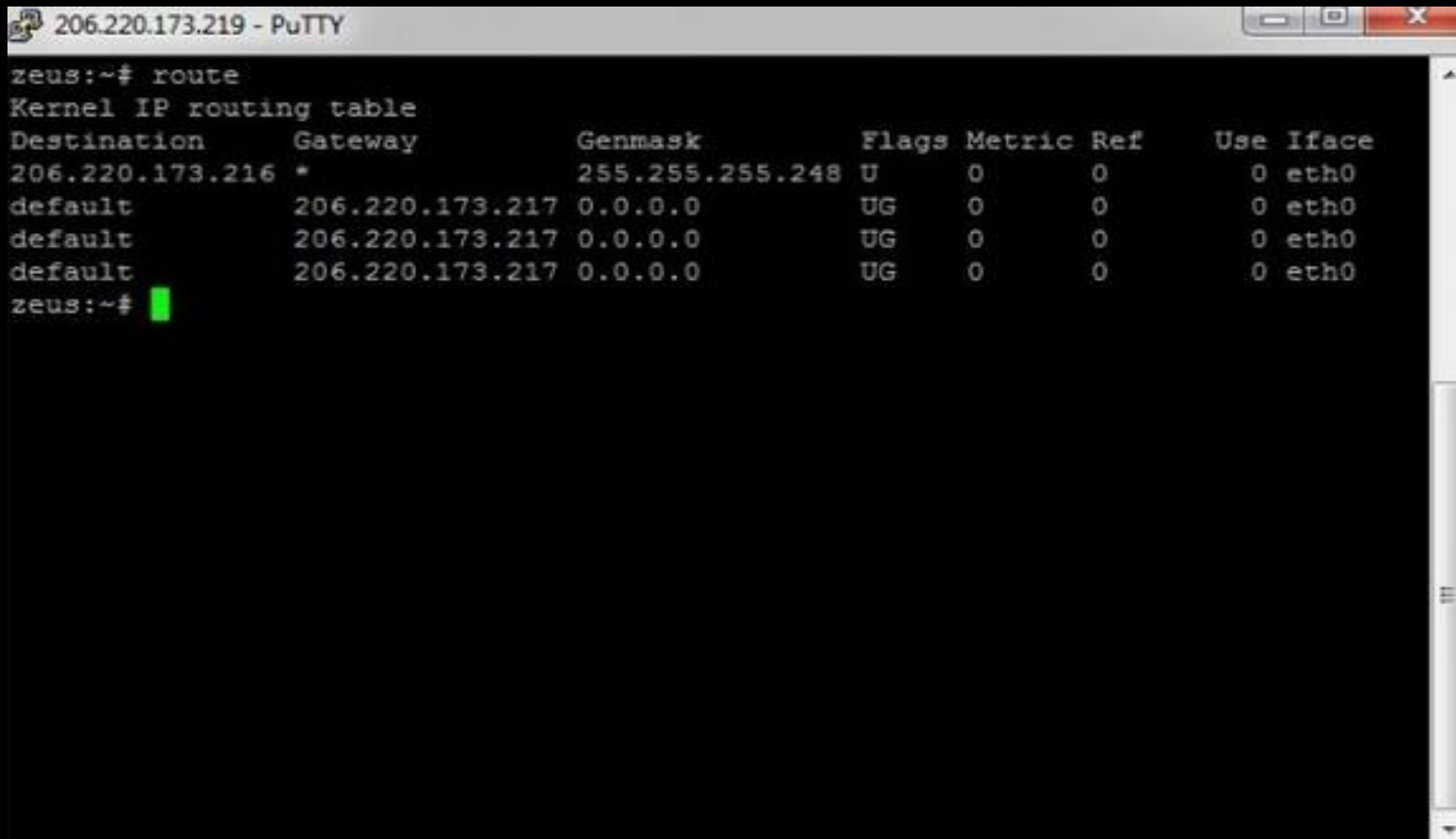
- Interference from other electronics:



❑ TCP/IP Troubleshooting Utilities

➤ Route

- This utility is used to display the current status of the routing table on a host.



The screenshot shows a PuTTY terminal window titled "206.220.173.219 - PuTTY". The user is at the prompt "zeus:~#" and has entered the command "route". The output displays the "Kernel IP routing table" with the following columns: Destination, Gateway, Genmask, Flags, Metric, Ref, Use, and Iface. The table contains four entries: a specific route to 206.220.173.216 via a gateway with a 255.255.255.248 netmask, and three default routes (0.0.0.0) via the gateway 206.220.173.217 with a 0.0.0.0 netmask. All routes have a metric of 0 and are associated with the eth0 interface. The terminal shows a green cursor at the end of the last line "zeus:~#".

```
zeus:~# route
Kernel IP routing table
Destination        Gateway            Genmask           Flags  Metric  Ref    Use  Iface
206.220.173.216    *                  255.255.255.248  U        0        0        0  eth0
default            206.220.173.217   0.0.0.0           UG        0        0        0  eth0
default            206.220.173.217   0.0.0.0           UG        0        0        0  eth0
default            206.220.173.217   0.0.0.0           UG        0        0        0  eth0
zeus:~#
```


➤ Pathping / mtr

- Combination of both the ping and tracert/traceroute commands.

```
Command Prompt
C:\Users\Sean Wilkins>pathping www.google.com

Tracing route to www.l.google.com [74.125.93.105]
over a maximum of 30 hops:
 0 seansdell [192.168.1.101]
 1 192.168.1.1
 2 192.168.100.2
 3 10.10.10.1
 4 nc-71-52-136-1.dhcp.embarqhsd.net [71.52.136.1]
 5 nc-69-69-52-245.sta.embarqhsd.net [69.69.52.245]
 6 host.lightcore.net [208.110.248.125]
 7 bb-rcmtncxa-jx9-02-ae0.core.centurytel.net [208.110.248.66]
 8 bb-asbnvacy-jx9-02-ae3.0.core.centurytel.net [208.110.248.170]
 9 bb-asbnvacy-jx9-01-ae0.0.core.centurytel.net [208.110.248.117]
10 72.14.219.254
11 216.239.48.112
12 209.85.248.75
13 209.85.254.237
14 64.233.175.14
15 qw-in-f105.1e100.net [74.125.93.105]

Computing statistics for 375 seconds...
Hop  RTT      Source to Here   This Node/Link
    Lost/Sent = Pct  Lost/Sent = Pct  Address
 0
 1    5ms      0/ 100 = 0%      0/ 100 = 0%    seansdell [192.168.1.101]
 2   17ms      0/ 100 = 0%      0/ 100 = 0%    192.168.1.1
 3   20ms      0/ 100 = 0%      0/ 100 = 0%    192.168.100.2
 4   91ms      0/ 100 = 0%      0/ 100 = 0%    10.10.10.1
 5  102ms      0/ 100 = 0%      0/ 100 = 0%    nc-71-52-136-1.dhcp.embarqhsd.net
 6   96ms      0/ 100 = 0%      0/ 100 = 0%    nc-69-69-52-245.sta.embarqhsd.net
 7  101ms      0/ 100 = 0%      0/ 100 = 0%    host.lightcore.net [208.110.248.125]
 8  108ms      0/ 100 = 0%      0/ 100 = 0%    bb-rcmtncxa-jx9-02-ae0.core.centurytel.net [208.110.248.66]
 9  114ms      0/ 100 = 0%      0/ 100 = 0%    bb-asbnvacy-jx9-02-ae3.0.core.centurytel.net [208.110.248.170]
10  119ms      0/ 100 = 0%      0/ 100 = 0%    bb-asbnvacy-jx9-01-ae0.0.core.centurytel.net [208.110.248.117]
11  112ms      0/ 100 = 0%      0/ 100 = 0%    72.14.219.254
12  114ms      0/ 100 = 0%      0/ 100 = 0%    216.239.48.112
13  114ms      0/ 100 = 0%      0/ 100 = 0%    209.85.248.75
14  121ms      0/ 100 = 0%      0/ 100 = 0%    209.85.254.237
15  116ms      0/ 100 = 0%      0/ 100 = 0%    64.233.175.14
16  116ms      0/ 100 = 0%      0/ 100 = 0%    qw-in-f105.1e100.net [74.125.93.105]
```


➤ Speedtest.net/pingtest.net

- A very easy test that can be used to both determine the Internet bandwidth available to a specific host and to determine the quality of an Internet connection is the use of the tools available at the speedtest.net and pingtest.net websites.



SPEEDTEST.NET™ [LOGIN](#) [MY RESULTS](#) [SUPPORT](#)

Test your connection.
Then, get a fast web browser.



 PING 48 ms	 DOWNLOAD SPEED 2.96 Mbps	 UPLOAD SPEED 0.50 Mbps
---	---	---

[SHARE THIS RESULT](#)

TOO SLOW?
Try a faster web browser.



[Get Chrome](#) by Google


COMPARE YOUR RESULT


CONTRIBUTE TO NET INDEX

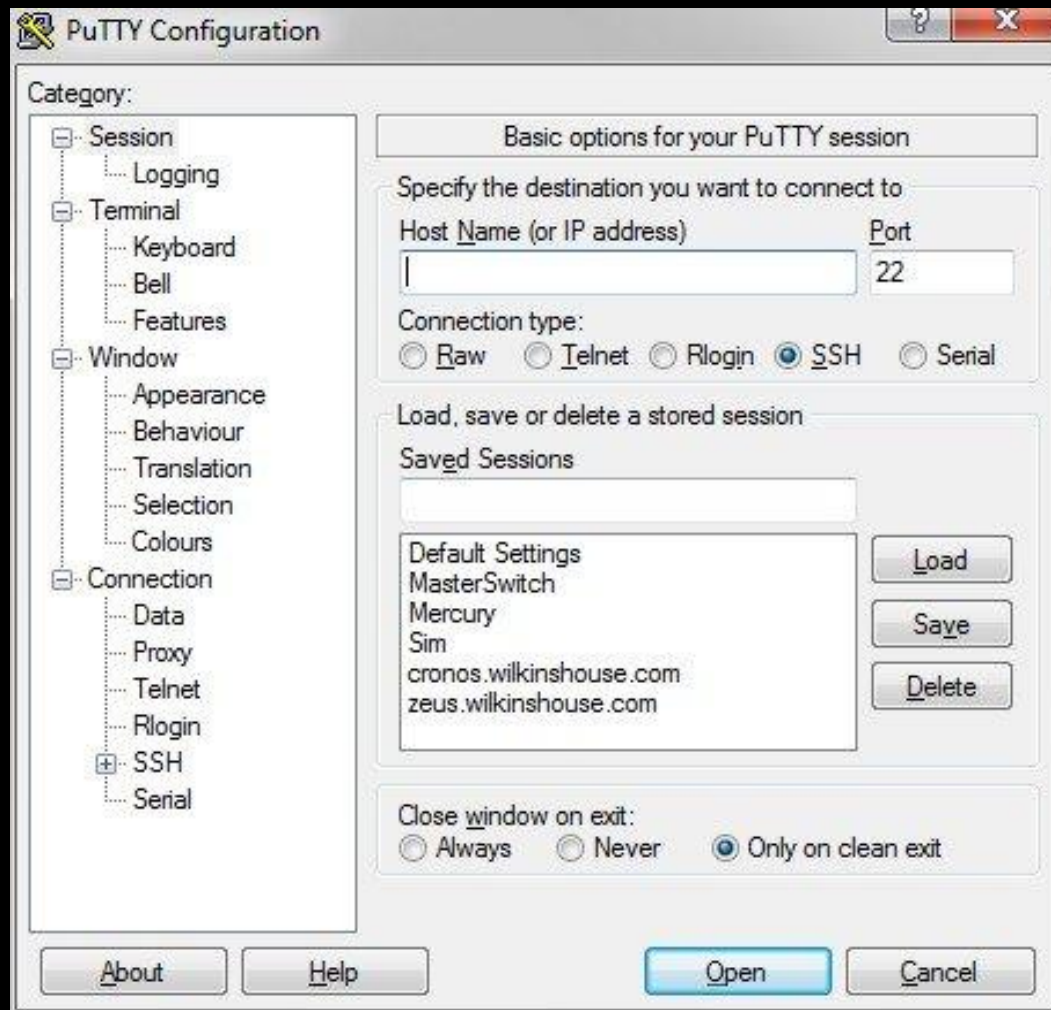
GET A FREE SPEEDTEST.NET ACCOUNT
Your Email Address

[CREATE](#)

Being logged in would allow you to start a Speed Wave here!
Registration is free and only requires a valid email address.

➤ PuTTY / Tera Term

- When connecting to a variety of different types of equipment, a telnet, SSH or serial client is required; when this is required both the putty and Tera Term programs are able to provide these functionalities.



➤ Netstat

- Checking the current state of the active network connections on a host.
- Verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port.

```
C:\Users\ >netstat -ant
```

Active Connections

Proto	Local Address	Foreign Address	State	Offload State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:902	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	InHost
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING	InHost
TCP	127.0.0.1:1001	0.0.0.0:0	LISTENING	InHost
TCP	127.0.0.1:8307	0.0.0.0:0	LISTENING	InHost
TCP	127.0.0.1:49157	0.0.0.0:0	LISTENING	InHost
TCP	127.0.0.1:49199	127.0.0.1:49200	ESTABLISHED	InHost
TCP	127.0.0.1:49200	127.0.0.1:49199	ESTABLISHED	InHost
TCP	127.0.0.1:49201	127.0.0.1:49202	ESTABLISHED	InHost
TCP	127.0.0.1:49202	127.0.0.1:49201	ESTABLISHED	InHost
TCP	127.0.0.1:49205	127.0.0.1:49206	ESTABLISHED	InHost
TCP	127.0.0.1:49206	127.0.0.1:49205	ESTABLISHED	InHost
TCP	127.0.0.1:49275	127.0.0.1:49276	ESTABLISHED	InHost
TCP	127.0.0.1:49276	127.0.0.1:49275	ESTABLISHED	InHost
TCP	192.168.1.2:139	0.0.0.0:0	LISTENING	InHost
TCP	192.168.1.2:49204	172.217.31.35:443	TIME_WAIT	InHost
TCP	192.168.1.2:49218	117.18.237.29:80	TIME_WAIT	InHost
TCP	192.168.1.2:49220	172.217.26.195:443	TIME_WAIT	InHost
TCP	192.168.1.2:49225	172.217.26.162:443	TIME_WAIT	InHost
TCP	192.168.1.2:49278	52.222.183.154:443	TIME_WAIT	InHost
TCP	192.168.1.2:49288	54.69.224.218:443	TIME_WAIT	InHost
TCP	192.168.1.2:49290	54.69.57.167:443	TIME_WAIT	InHost
TCP	192.168.44.1:139	0.0.0.0:0	LISTENING	InHost
TCP	192.168.80.1:139	0.0.0.0:0	LISTENING	InHost
TCP	[::]:135	[::]:0	LISTENING	InHost
TCP	[::]:443	[::]:0	LISTENING	InHost
TCP	[::]:445	[::]:0	LISTENING	InHost
TCP	[::]:49152	[::]:0	LISTENING	InHost
TCP	[::]:49153	[::]:0	LISTENING	InHost
TCP	[::]:49154	[::]:0	LISTENING	InHost
TCP	[::]:49155	[::]:0	LISTENING	InHost
TCP	[::]:49156	[::]:0	LISTENING	InHost
TCP	[::]:49158	[::]:0	LISTENING	InHost
TCP	[::]:8307	[::]:0	LISTENING	InHost

➤ Nslookup

- Some of the most common networking issues revolve around with Dynamic Name System (DNS) address resolution issues.



```
C:\Users\      >nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> set type=ns
> www.google.com
Server:  UnKnown
Address:  192.168.1.1

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial      = 176049917
        refresh     = 900 (15 mins)
        retry       = 900 (15 mins)
        expire      = 1800 (30 mins)
        default TTL = 60 (1 min)

> _
```

➤ Ipconfig / ifconfig

- Find out the specific IP configuration of the variously affected hosts.



```
C:\Users'      >ipconfig
```

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix  . : domain.name
Link-local IPv6 Address . . . . . : fe80::f165:6a64:af16:b1c0%11
IPv4 Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::8226:89ff:fec7:cb52%11
                             192.168.1.1
```

Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::69e2:dab8:7774:604c%17
IPv4 Address. . . . . : 192.168.44.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
```

Ethernet adapter VMware Network Adapter VMnet8:

```
Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::cd58:4cc4:9bcc:35c1%18
IPv4 Address. . . . . : 192.168.80.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 
```

➤ Tracert/traceroute

- To determine basic connectivity, the tracert/traceroute utility can be used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts.

```
C:\Users\      >tracert google.com
```

```
Tracing route to google.com [172.217.26.206]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	19 ms	70 ms	18 ms	static.ill.218.248.126.214/24.bsn1.in [218.248.126.214]
3	37 ms	*	34 ms	218.248.235.161
4	*	33 ms	*	218.248.235.162
5	34 ms	33 ms	33 ms	72.14.195.21
6	33 ms	33 ms	45 ms	72.14.232.110
7	33 ms	34 ms	34 ms	108.170.237.55
8	34 ms	33 ms	34 ms	maa03s23-in-f206.1e100.net [172.217.26.206]

```
Trace complete.
```

➤ Ping

- This utility is used to provide a basic connectivity test between the requesting host and a destination host.
- This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host.



```
C:\Users\ >ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=39ms TTL=55
Reply from 8.8.8.8: bytes=32 time=38ms TTL=55
Reply from 8.8.8.8: bytes=32 time=39ms TTL=55
Reply from 8.8.8.8: bytes=32 time=39ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 39ms, Average = 38ms
```



THANK YOU !!!