NETWORKING & TELECOMMUNICATION FUNDAMENTALS

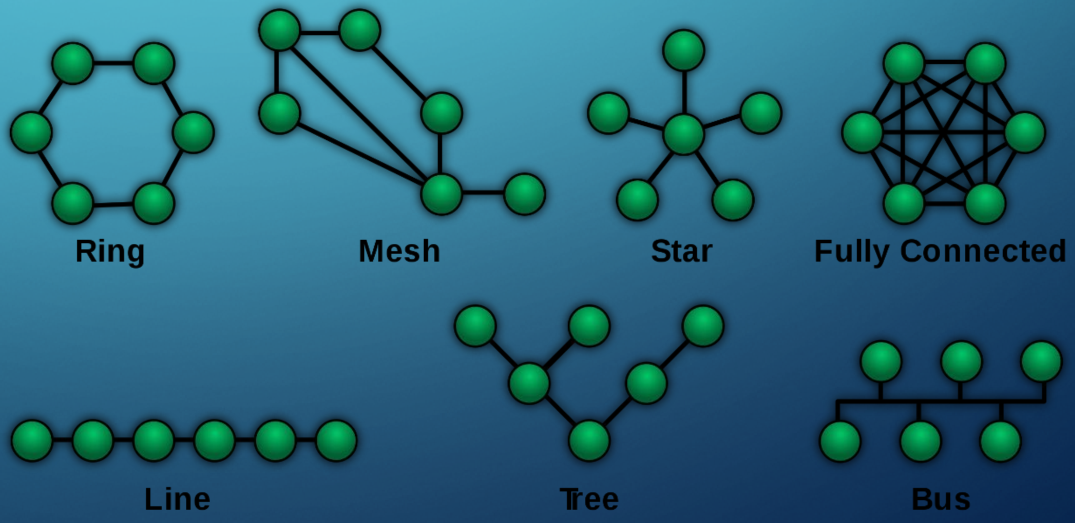
JEFF WHITESIDE

UNIVERSITY OF ALASKA

SR. NETWORK COMMUNICATION SPECIALIST

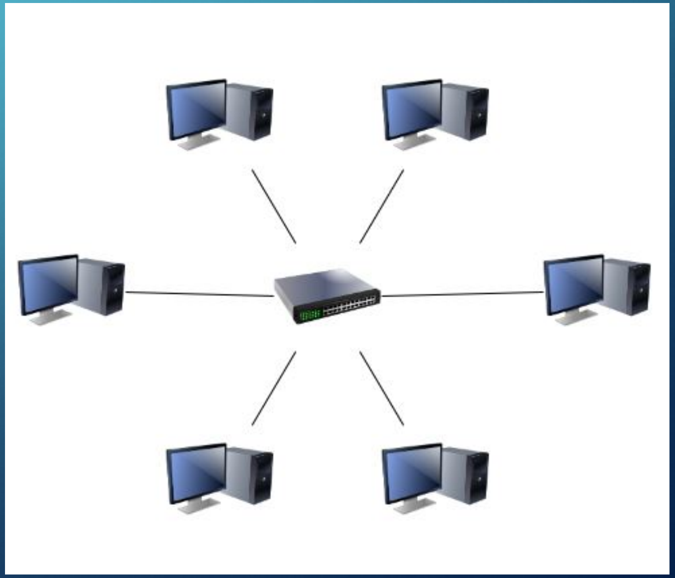
NETWORK TOPOLOGY BASICS

- Network topology is the arrangement of various communication devices within a network.
- Several network topologies exist as a way to describe various primary functions or purposes.



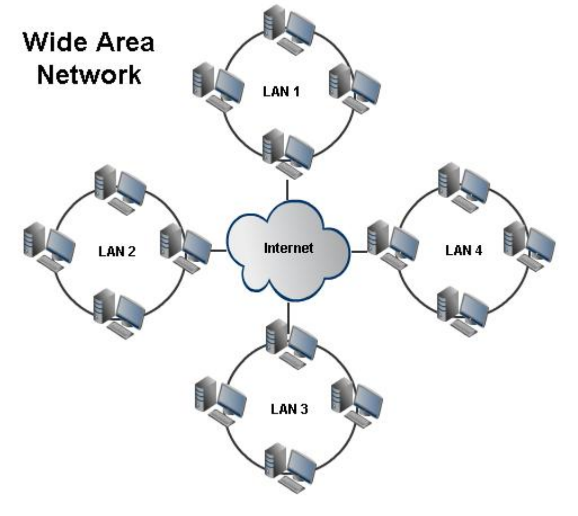
NETWORK TOPOLOGY BASICS

- LAN or Local Area Network: A computer network that connects devices within a limited area, such as a residence, building, campus or ship.
- Common modern technologies used for this are Ethernet and WiFi.



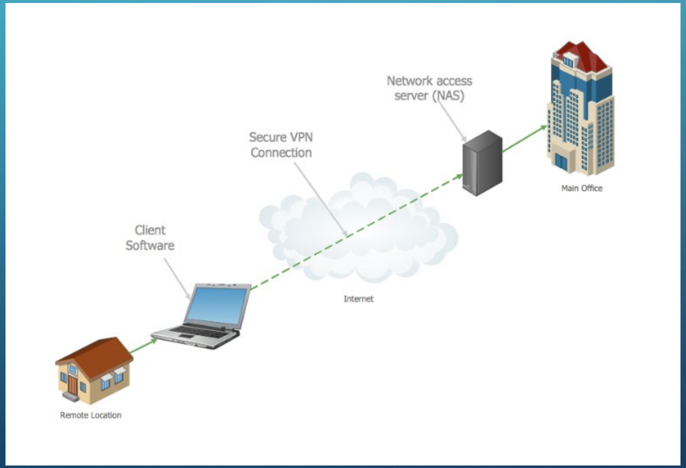
NETWORK TOPOLOGY BASICS

- WAN or Wide Area Network: A computer network that connects devices over a large geographic area, typically established over leased circuits of many different types of technologies.
- Most common use of WAN is to connect multiple LAN's together.



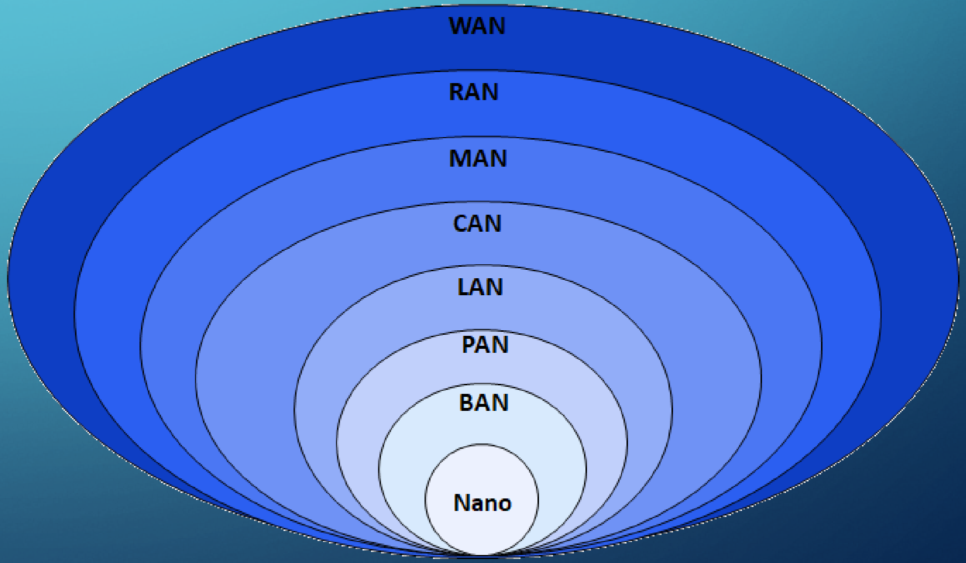
NETWORK TOPOLOGY BASICS

- VPN or Virtual Private Networks are used to extend private networks (i.e. LAN/WAN) across public networks. (i.e. internet)
- Typically provided by software, but can also be hardware devices.
- VPN's often included encryption as a component of the communication.



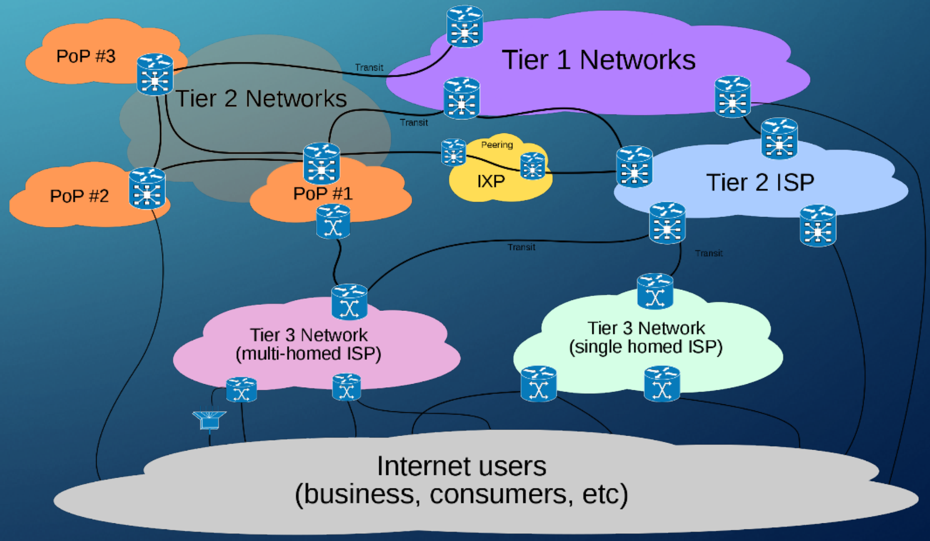
NETWORK TOPOLOGY BASICS

- Many other lesser used terms exist, and area organized in terms of scale, such as:
  - MAN: Metorpolitan Area Network
  - PAN: Personal Area Network
  - CAN: Campus Area Network



NETWORK TOPOLOGY BASICS

- “The Internet” is functionally a global network of interconnected wide area networks. Tiered providers working together make it work.
- The most distinguishing characteristic is that it uses many private connections, but does not have a singular governing body.



NETWORK HARDWARE FUNDAMENTALS

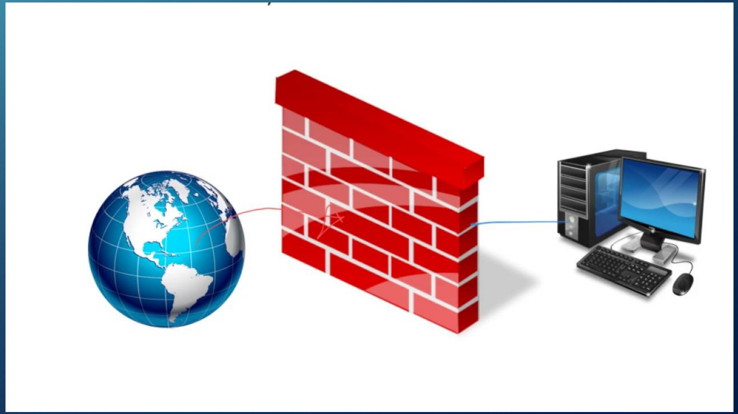
- Switches are used to interconnect devices on computer networks (typically LAN's). It is responsible for receiving and forwarding data.
- Most switches use MAC addresses (unique device identifiers, layer 2) to send or receive traffic to the appropriate destination.
- Can itself be a LAN or can be interconnected to form a more complex LAN.
- Switches should never be connected back to themselves unless you know what you are doing!

NETWORK HARDWARE FUNDAMENTALS

- Routers are used to forward data packets between computer networks. They can interconnect switches, wide area networks or provide connectivity to the internet.
- They typically have complex information about where devices are, based on the network address. (IP address, or layer 3)

NETWORK HARDWARE FUNDAMENTALS

- Firewalls are a network security device that monitors and controls inbound and outbound traffic, based on pre-determined rules or policies.
- It often acts like a router with enhanced security capabilities.
- It is most often used as a device between public networks (i.e. internet) and private networks, but can also regulate local networks.

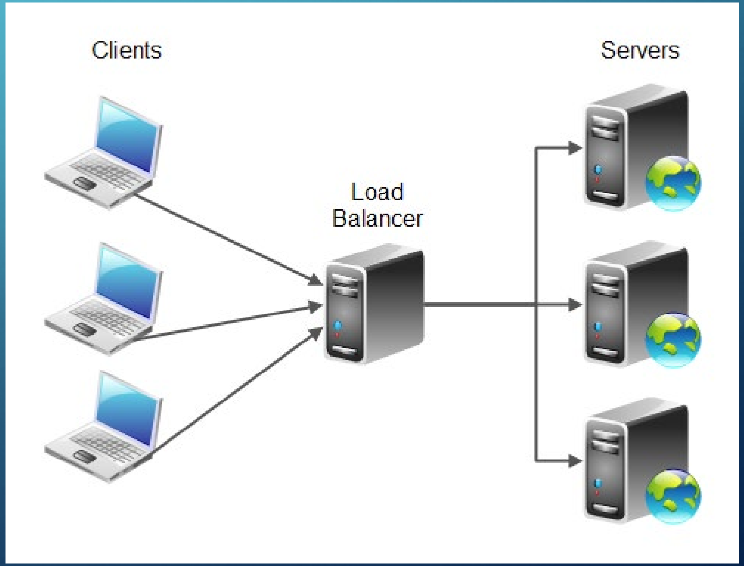


NETWORK HARDWARE FUNDAMENTALS

- Wireless access points (WAP or just AP) are used to provide Wi-FI connections and typically bridge wired and wireless networks.
- Wireless controllers are (sometimes) used to regulate WAP's to simplify management and make dynamic wireless decisions about things like signal strength, channels used and other factors.

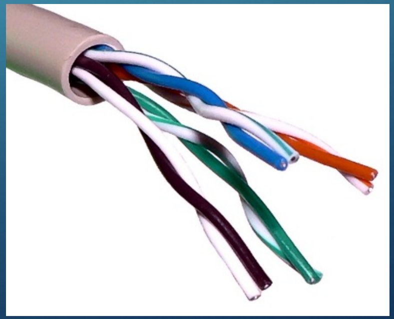
NETWORK HARDWARE FUNDAMENTALS

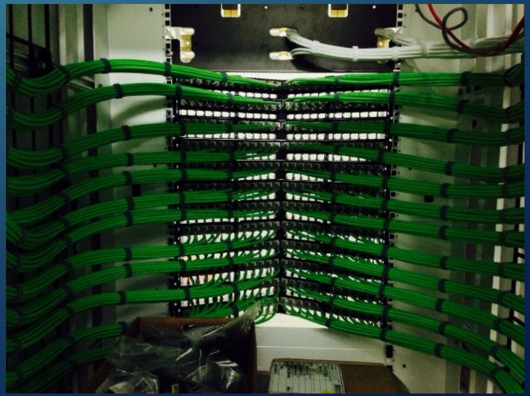
- Load balancers are used to dynamically route (or balance) traffic between two or more devices, networks or servers.
- Often features complex rule sets to define what traffic gets routed where.



NETWORK INFRASTRUCTURE FUNDAMENTALS

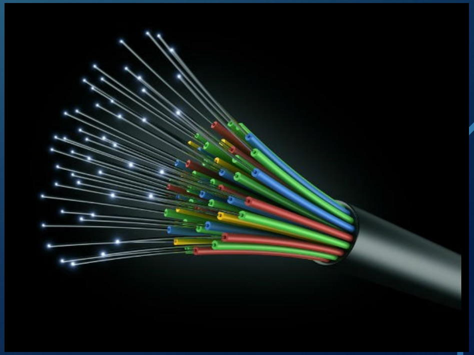
- Ethernet is the most common cable used to provide wired network connectivity. It typically uses a twisted pairs of copper.
- Twisted pairs are used to improve reduce electromagnetic radiation and cross talk between neighboring cables.
- Classified by category to indicate capabilities, such as CAT5, CAT5e CAT6, CAT7. Bigger is usually better, and more expensive.





NETWORK INFRASTRUCTURE FUNDAMENTALS

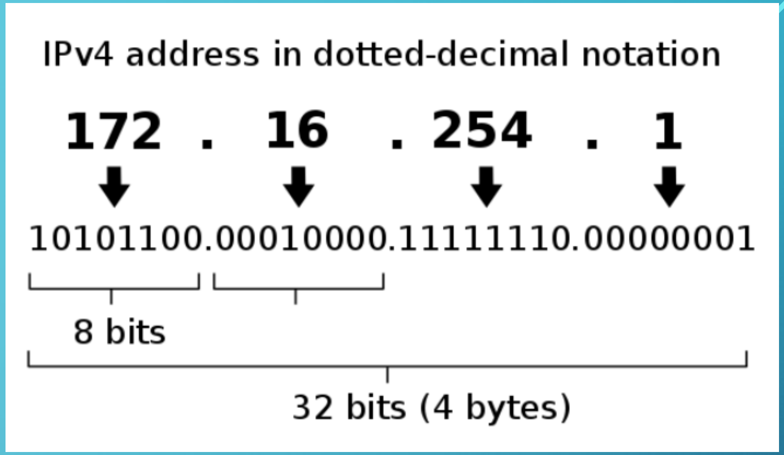
- Optical fiber, or fiber optics, use light to transmit data across the length of the cable.
- Ideal for long distance as it is immune to electromagnetic interference and features less loss compared to electrical signaling.
- Different grades of fiber feature different physical characteristics, typically allowing more data to be transmitted or less loss over distance.



NETWORK INFRASTRUCTURE FUNDAMENTALS

- Network infrastructure can also include wireless communications. Typical technologies used are WiFi and microwave.
- Common applications are bridges, in a point-to-point or point-to-multipoint set up, where WiFi is used to bridge two wired networks.
- Typically less efficient than wired networks, but helpful when wired networks are impractical.

IP ADDRESSING FUNDAMENTALS



IPv4 address in dotted-decimal notation

172 . 16 . 254 . 1

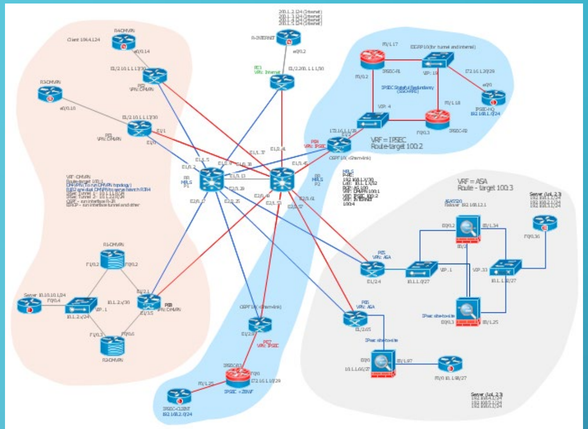
10101100.00010000.11111110.00000001

8 bits

32 bits (4 bytes)

- An IP address is a numeric identifier used in IP network communication.
- It features two pieces of information for routing network traffic, a network interface identification (who you are) and a location identification (where you are).
- IP addresses are used typically used by routers and firewalls to get traffic you request where it needs to go and to return that traffic to you.
- Almost every network has three components: Network ID, host IP’s and broadcast IP.

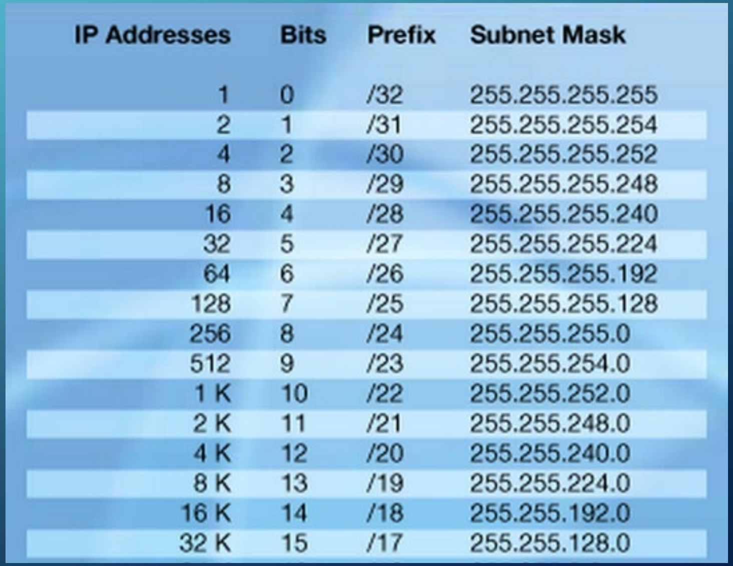
IP ADDRESSING FUNDAMENTALS



- IP addresses are divided into sub-networks, or subnets. Subnets are effectively the "where you are" component of IP addresses.
- Routers, firewalls and other network equipment use these subnetworks to efficiently route traffic to the appropriate destination. Routers don't care exactly where you are, they just need to know how to get to you.
- Optimal network design allows for levels of granularity. For example, you're in Alaska, then you're at UAF, then you're in Woods Center, then you're on the 2nd floor of the Woods Center.
- Subnets establish broadcast domains, or the extents to which broadcast traffic can reach. Broadcast traffic can reach all clients on a network.

IP ADDRESSING FUNDAMENTALS

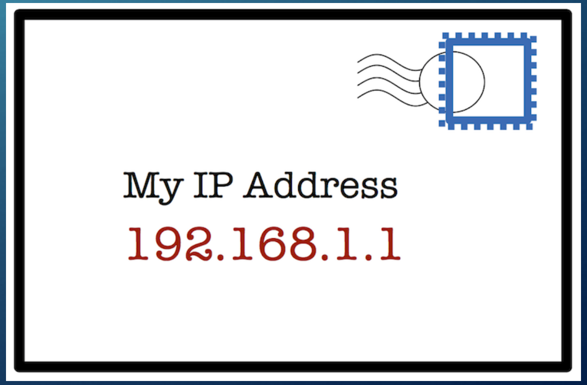
- Subnet masks determine the size of the network, or how many hosts can be placed into a given network.
- Common subnet masks and CIDR notations are:
  - 255.255.255.0 = /24 = 254 hosts
  - 255.255.0.0 = /16 = 65K hosts
  - 255.0.0.0 = /8 = 16M hosts
  - 255.255.255.255 = /32 = 1 host
  - 255.255.255.252 = /30 = 2 hosts



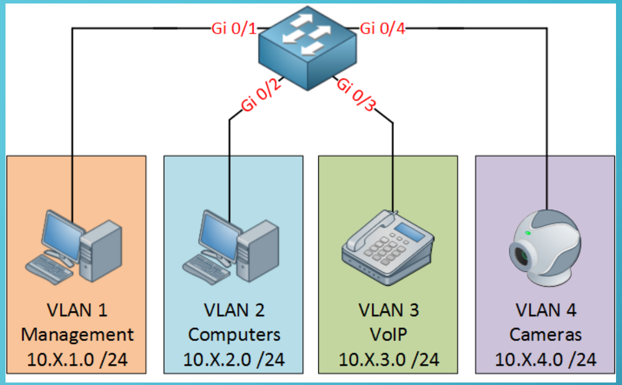
IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0

IP ADDRESSING FUNDAMENTALS

- IP Addresses are divided into three main categories. These are:
  - Public – Most addresses fall into this category, they are public in nature and globally accessible on the internet. Always globally unique.
  - Private – Typically used within organizations and are not routed on the internet. Can be duplicated globally, unique locally.
    - 10.0.0.0 to 10.255.255.255 (24 bits, 16+ million addresses)
    - 172.16.0.0 to 172.31.255.255 (20 bits, 1+ million addresses)
    - 192.168.0.0 to 192.168.255.255 (16 bits, 65k addresses)
  - Dedicated – Reserved for specific purposes.
    - Examples include carrier grade NAT, multicast, etc.

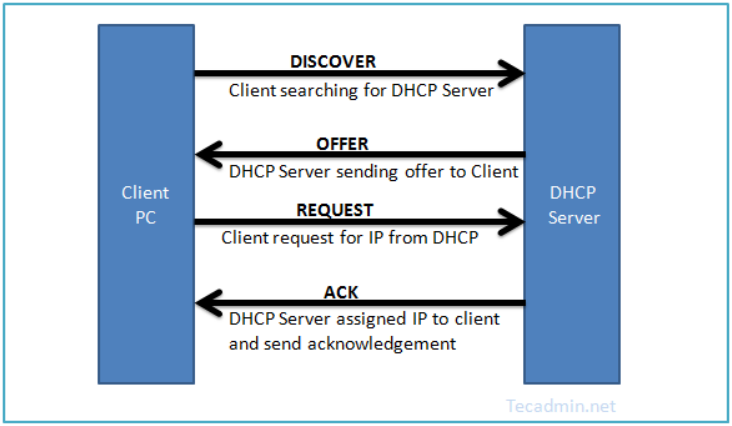


IP ADDRESSING FUNDAMENTALS



- VLAN's (or virtual LAN's) are used to create multiple network subnets (or networks) on the same physical network hardware. They can also be used to create the same logical network across multiple physical networks.
- They are typically used to distinguish/segregate major technologies, establish security zones or to treat different types of network traffic uniquely.
- Trunks are used to allow a single physical interface to transmit several VLAN's of traffic.
- Allows multiple broadcast domains both across different hardware or on the same hardware.

IP ADDRESSING FUNDAMENTALS



DISCOVER
Client searching for DHCP Server

OFFER
DHCP Server sending offer to Client

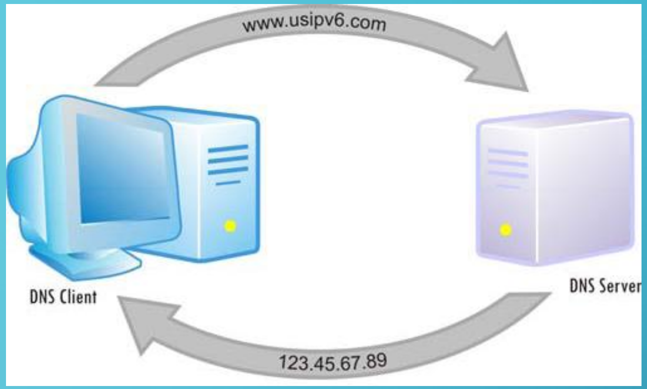
REQUEST
Client request for IP from DHCP

ACK
DHCP Server assigned IP to client and send acknowledgement

Tecadmin.net

- DHCP, or dynamic host configuration protocol, is used to automate the assignment of network addresses, subnets and other parameters.
- DHCP prevents many things like duplicate IP addresses and misconfigurations.
- DHCP addresses can change over time and are not guaranteed.
- Two static address alternatives exist:
  - Static addresses are when you configure the IP on the device
  - Static reservations use DHCP to consistently offer the same address

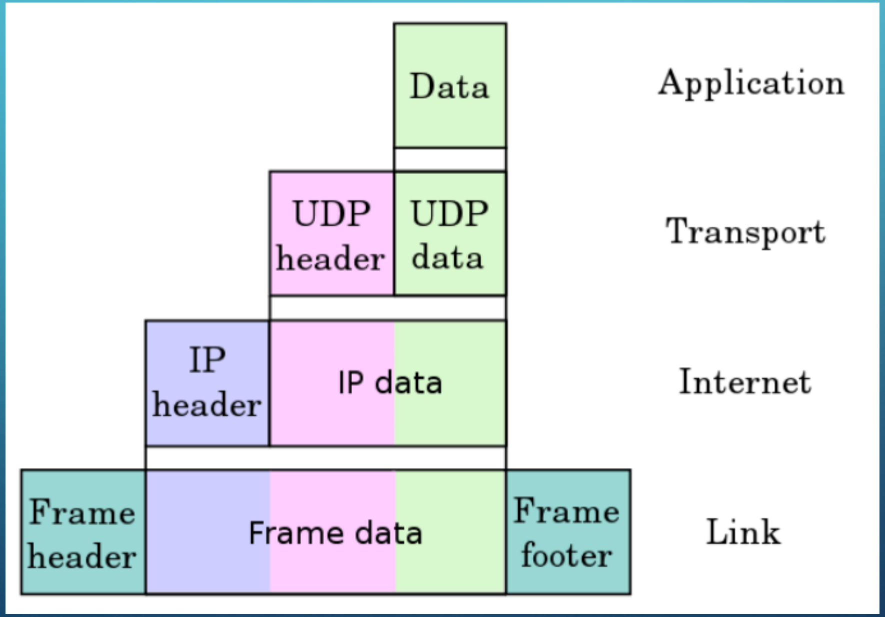
IP ADDRESSING FUNDAMENTALS



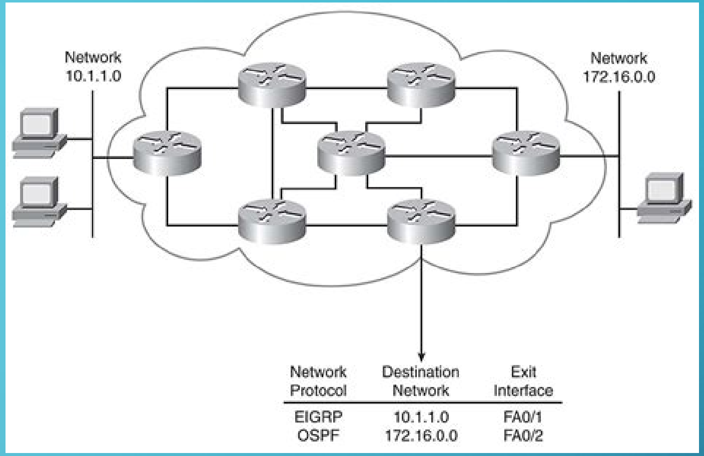
- DNS, or domain name system, is used to make IP addresses easier to remember and more human friendly.
- A DNS server will translate a domain name (e.g. google.com) into an IP address, or possibly a set of IP addresses.
- DNS is used not just on the internet, but also private networks.
- Reverse DNS is the process of matching a specific IP address to a domain name.

WHAT'S IN A PACKET?

- Packets are used to transmit data across networks. Every packet contains both the information as well as metadata used to get the packet where it's going.



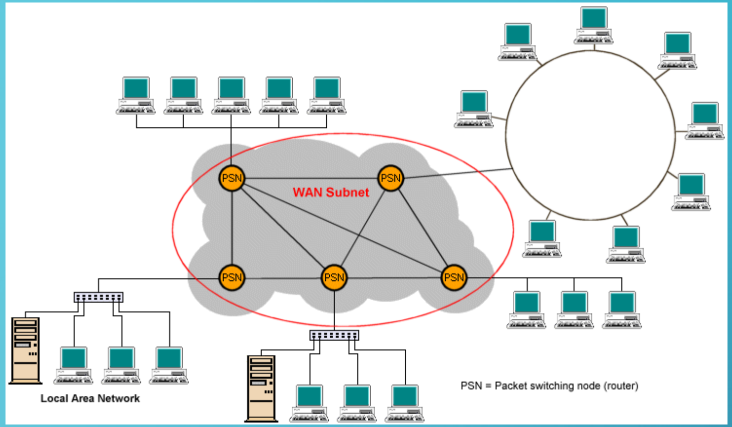
NETWORK ROUTING BASICS



Network Protocol	Destination Network	Exit Interface
EIGRP	10.1.1.0	FA0/1
OSPF	172.16.0.0	FA0/2

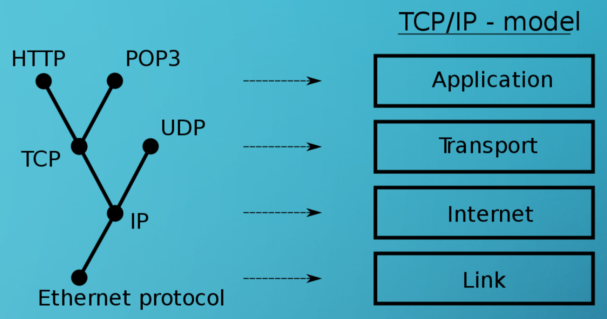
- Clients can communicate within their own network without a router.
- When communicating outside of their own network, a default gateway is used. The gateway, almost always a router or firewall, has more information about other networks and how to get to them.
- Routers also have default gateways. If the router doesn't know how to get there, it sends the traffic to its default gateway!
- Routers can have multiple paths to a destination, allowing it to select the most optimal path to get there and have a redundant path.
- Private networks cannot be routed over the internet, only over private networks or through VPN's.

NETWORK ROUTING BASICS



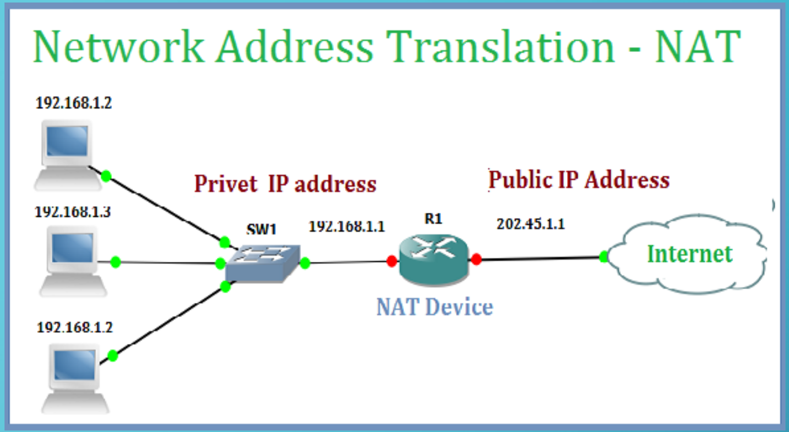
- In simple networks, static routes tell the routers “To get to X, you need to go to Y”.
- In complex networks, routing protocols learn about networks from other routers and possibly multiple ways to get there.
- Network administrators can assign metrics, costs or distance factors to multiple paths to create a preferred order from multiple pathways.
- Each router you hit is called a hop, you can easily see these in a traceroute.
- When private network routers don’t know about a network, they are typically configured to send requests to the internet.

COMMUNICATION PROTOCOL BASICS



- Communication protocols are used to define a common set of rules for two or more systems to communicate. Effectively, language.
- They define the rules, syntax and general behavior of the communication. Many thousands of protocols exist today.
- Protocol suites are used to broadly define a set of protocols used for communication, with the most popular one used today being TCP/IP.
- Other commonly used protocols are HTTP, HTTPS, POP, FTP, etc.

INTERNET FUNDAMENTALS



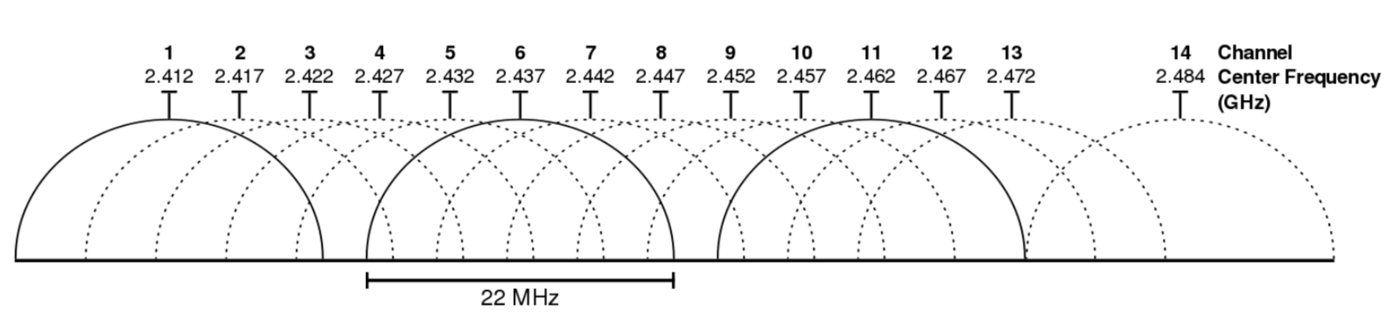
- Most networks are configured so that if a network address is unknown, it will send that traffic to the public internet.
- Network address translation (NAT) is a common technique used to mask many private IP addresses into a public address.
- NAT will keep track of various sessions to ensure traffic is delivered from and to the appropriate clients on the internal network.
- NAT pools are sometimes used in larger networks to prevent what is called port exhaustion.

WIRELESS COMMUNICATION FUNDAMENTALS

- WiFi is a family of radio technologies used for wireless network communications.
- It is based on the IEEE 802.11 standard, with many sub-standards that are constantly improved to increase bandwidth or adjust spectrums that are used.
- All WiFi is half-duplex, meaning transmit or receive on a given radio. Modern radio designs circumvent this with multiple radios. (i.e. MIMO)
- Collision avoidance is heavily used to prevent overlap that could disrupt communications with multiple transmitters or receivers on the same frequency.

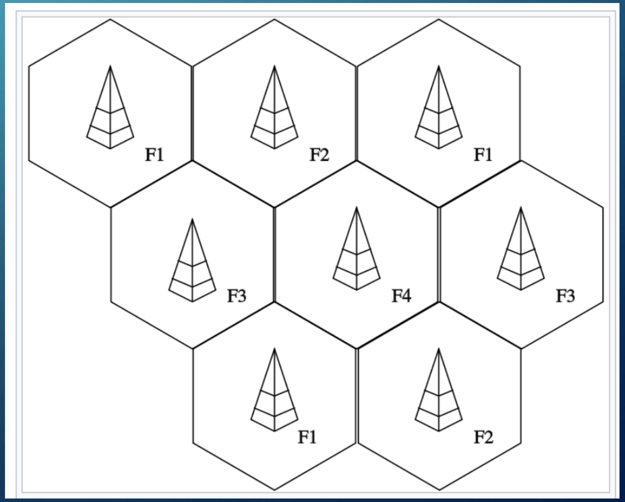
WIRELESS COMMUNICATION FUNDAMENTALS

- The most common frequency spectrums used today are 2.4GHz (2.4-2.5) and 5GHz (4.915 to 5.825), both of which are public ISM spectrums. The next generation of WiFi may introduce the 6GHz spectrum.
- Lower frequency spectrums (e.g. 2.4GHz) are better at physical penetration, whereas higher frequencies are better at carrying more bandwidth.
- The frequency spectrum is divided into channels, or specific frequencies.



WIRELESS COMMUNICATION FUNDAMENTALS

- Wireless networks are typically deployed using “cell” based concepts. This allows more optimal re-use of frequency spectrums.
- The goal of these cells is to allow some overlap, to permit transitioning or roaming, but also to maximize the potential for frequency usage. Three dimensional planes can make this very difficult.



WIRELESS COMMUNICATION FUNDAMENTALS

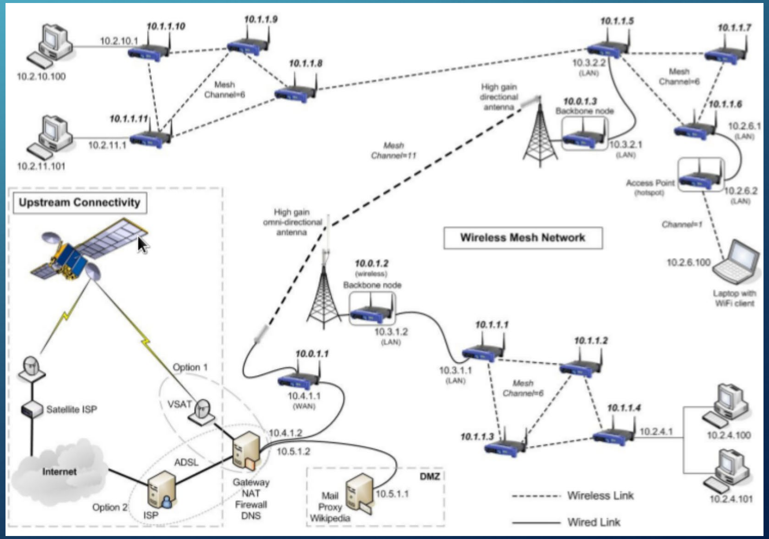
- SSID’s, or service set identifiers, are used to create common set of operating parameters across multiple physical devices.
- SSID’s often represent a singular logical network segment in smaller networks, but not in larger networks.
- Beacon packets are used to broadcast the SSID to allow it to be discovered by wireless devices.

WIRELESS NETWORK FUNDAMENTALS

- Almost all AP’s can perform simple mitigation of frequency and power utilization to prevent wireless network problems such as channel overlap.
- Wireless controllers permit greater visibility of the entire wireless network and allow dynamic mitigation of frequency and power across the entire network.
- Wireless controllers also make it easier to manage SSID’s and other configurations across many access points.

MESH WIRELESS COMMUNICATION

- Most wireless networks simply bridge wireless networks into to wired networks.
- Wireless mesh networking functions similarly to this model, however, can use wireless communication as a backhaul to a device that does have wired connectivity. Often, the clients and backhaul use different frequency spectrums.



WIRELESS SECURITY

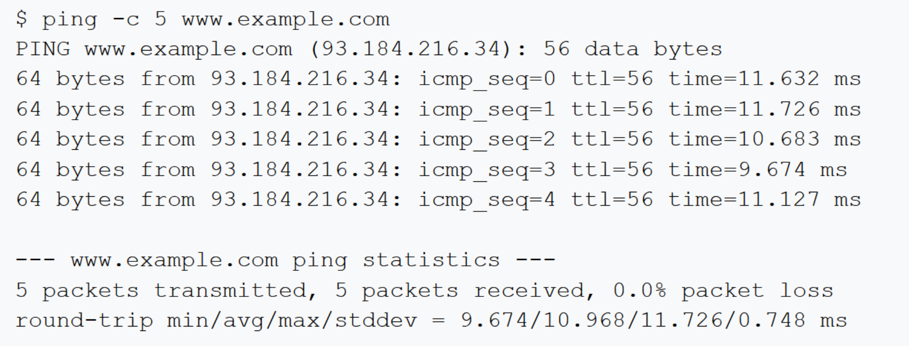
- Wireless security is vital. Wireless technology doesn't follow physical security rules.
- Open networks (e.g. hotspots) usually do not feature any encryption. Packets can literally be seen by a skilled person.
- Encryption is used to obfuscate the network communications. A common encryption and decryption method is used by the access point and client.
- WPA2 is the most secure, current encryption technique. Expect WPA3 soon, which promises to be more secure and also should simplify access for devices with limited accessibility. (e.g. no display)

WIRELESS SECURITY

- Encryption and authentication are not the same thing. Authentication is used to restrict unauthorized access to a wireless network, whereas encryption obfuscates the data once on the wireless network
- The most basic authentication technique is a preshared key, or common password.
- Enterprise networks commonly use 802.1x which authenticates specific users based on username/password credentials, and sometimes a certificate.

NETWORK TROUBLESHOOTING ESSENTIALS

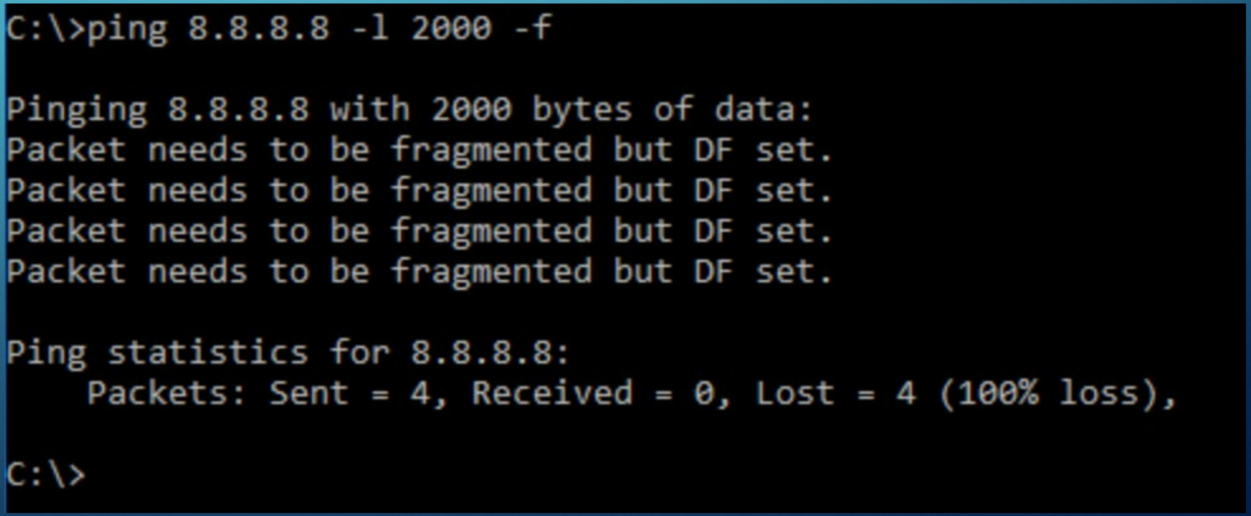
- Ping is used to verify the reachability of a host. It also measures latency (round trip time) and can help detect packet loss in a network.
- All operating systems and most network devices have some sort of ping function built into them.
- If you can ping, you have network connectivity from A to B. Other problems can exist, though.



```
$ ping -c 5 www.example.com
PING www.example.com (93.184.216.34): 56 data bytes
64 bytes from 93.184.216.34: icmp_seq=0 ttl=56 time=11.632 ms
64 bytes from 93.184.216.34: icmp_seq=1 ttl=56 time=11.726 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=56 time=10.683 ms
64 bytes from 93.184.216.34: icmp_seq=3 ttl=56 time=9.674 ms
64 bytes from 93.184.216.34: icmp_seq=4 ttl=56 time=11.127 ms

--- www.example.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.674/10.968/11.726/0.748 ms
```

NETWORKING TROUBLESHOOTING ESSENTIALS

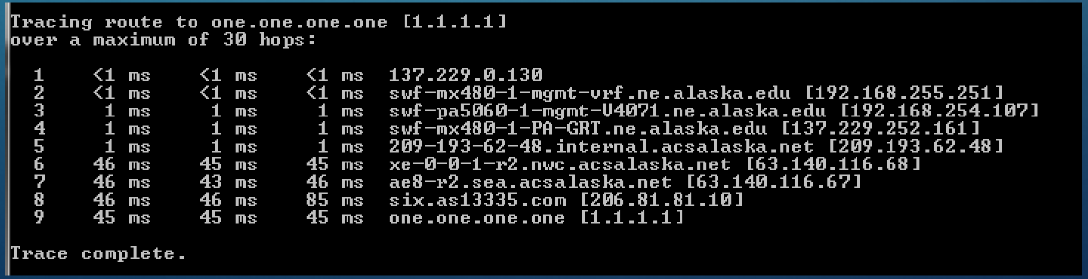
- Ping is very powerful. You can send different packet sizes and also prevent it from being fragmented into multiple packets.
- Adjusting ping sizes is a great way to identify MTU problems.
- It can also indicate problems that occur only with larger packets, compared to smaller ones.



```
C:\>ping 8.8.8.8 -l 2000 -f

Pinging 8.8.8.8 with 2000 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

NETWORK TROUBLESHOOTING ESSENTIALS

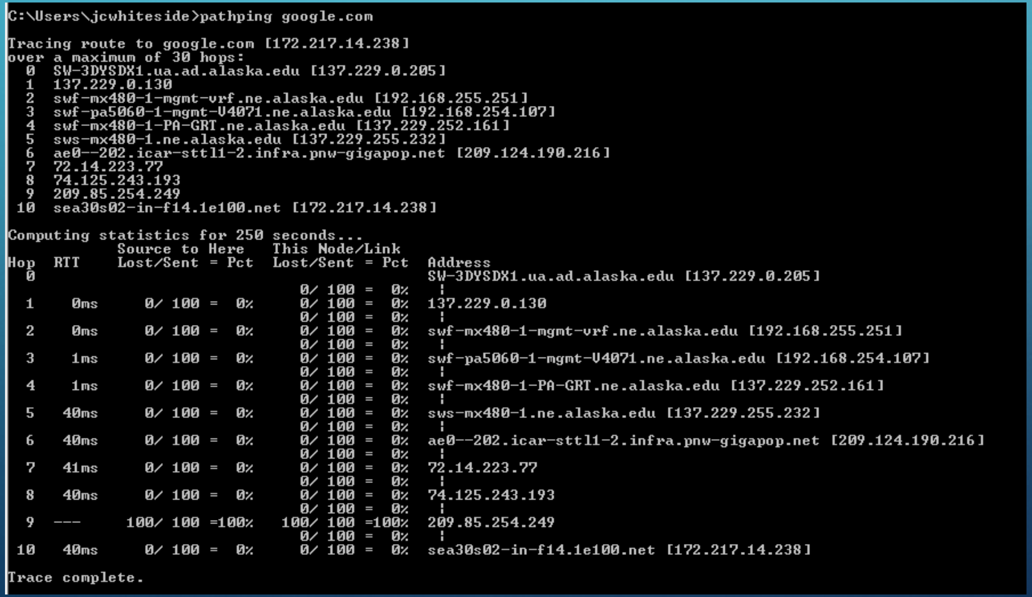
- Traceroute is used to determine the path traffic is taking through the network. It shows all routers, or hops, that packets have to take to get from A to B.
- Can show where latency is induced within the path or where network loss is occurring at.
- Hint: In Windows, it’s called tracert.
- When traceroute fails, it is almost always the hop right after your last good response that has failed. This can help narrow in what to look at.



```
Tracing route to one.one.one.one [1.1.1.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  137.229.0.130
  2    <1 ms    <1 ms    <1 ms  swf-mx480-1-mgmt-vrf.ne.alaska.edu [192.168.255.251]
  3     1 ms     1 ms     1 ms  swf-pa5060-1-mgmt-V4071.ne.alaska.edu [192.168.254.107]
  4     1 ms     1 ms     1 ms  swf-mx480-1-PA-GRT.ne.alaska.edu [137.229.252.161]
  5     1 ms     1 ms     1 ms  209-193-62-48.internal.acsalaska.net [209.193.62.48]
  6    46 ms    45 ms    45 ms  xe-0-0-1-r2.nwc.acsalaska.net [63.140.116.68]
  7    46 ms    43 ms    46 ms  ae8-r2.sea.acsalaska.net [63.140.116.67]
  8    46 ms    46 ms    85 ms  six.as13335.com [206.81.81.10]
  9    45 ms    45 ms    45 ms  one.one.one.one [1.1.1.1]

Trace complete.
```

NETWORK TROUBLESHOOTING ESSENTIALS

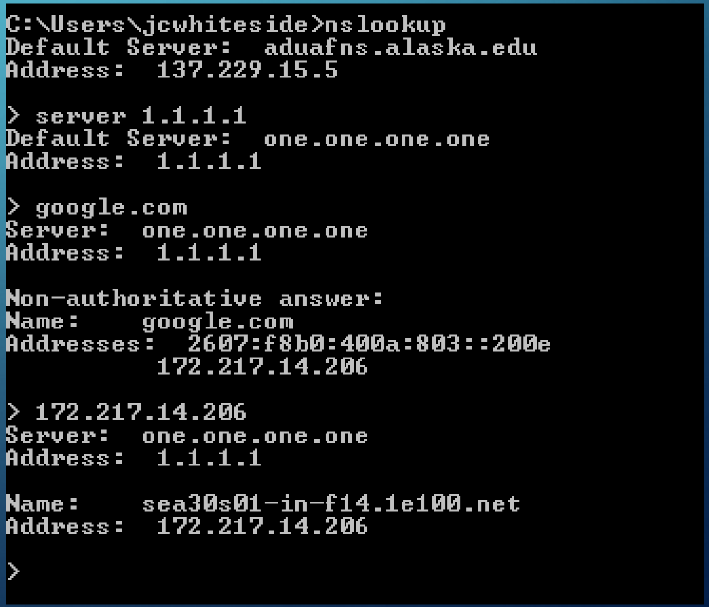
- Windows Only: Pathping can be used to see packet loss over a period of time across the entire network path.
- Other operating systems may have 3rd party programs that do this.



```
C:\Users\jcwhiteside>pathping google.com

Tracing route to google.com [172.217.14.238]
over a maximum of 30 hops:
  0  SW-3DYSDX1.ua.ad.alaska.edu [137.229.0.205]
  1  137.229.0.130
  2  swf-mx480-1-mgmt-vrf.ne.alaska.edu [192.168.255.251]
  3  swf-pa5060-1-mgmt-V4071.ne.alaska.edu [192.168.254.107]
  4  swf-mx480-1-PA-GRT.ne.alaska.edu [137.229.252.161]
  5  sws-mx480-1.ne.alaska.edu [137.229.255.232]
  6  ae0--202.icar-sttl1-2.infra.pnw-gigapop.net [209.124.190.216]
  7  72.14.223.77
  8  74.125.243.193
  9  209.85.254.249
 10  sea30s02-in-f14.1e100.net [172.217.14.238]

Computing statistics for 250 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           SW-3DYSDX1.ua.ad.alaska.edu [137.229.0.205]
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  137.229.0.130
                                0/ 100 =  0%   |
  2    0ms     0/ 100 =  0%     0/ 100 =  0%  swf-mx480-1-mgmt-vrf.ne.alaska.edu [192.168.255.251]
                                0/ 100 =  0%   |
  3    1ms     0/ 100 =  0%     0/ 100 =  0%  swf-pa5060-1-mgmt-V4071.ne.alaska.edu [192.168.254.107]
                                0/ 100 =  0%   |
  4    1ms     0/ 100 =  0%     0/ 100 =  0%  swf-mx480-1-PA-GRT.ne.alaska.edu [137.229.252.161]
                                0/ 100 =  0%   |
  5   40ms     0/ 100 =  0%     0/ 100 =  0%  sws-mx480-1.ne.alaska.edu [137.229.255.232]
                                0/ 100 =  0%   |
  6   40ms     0/ 100 =  0%     0/ 100 =  0%  ae0--202.icar-sttl1-2.infra.pnw-gigapop.net [209.124.190.216]
                                0/ 100 =  0%   |
  7   41ms     0/ 100 =  0%     0/ 100 =  0%  72.14.223.77
                                0/ 100 =  0%   |
  8   40ms     0/ 100 =  0%     0/ 100 =  0%  74.125.243.193
                                0/ 100 =  0%   |
  9  ---     100/ 100 =100%   100/ 100 =100%  209.85.254.249
                                0/ 100 =  0%   |
 10   40ms     0/ 100 =  0%     0/ 100 =  0%  sea30s02-in-f14.1e100.net [172.217.14.238]

Trace complete.
```

NETWORK TROUBLESHOOTING ESSENTIALS

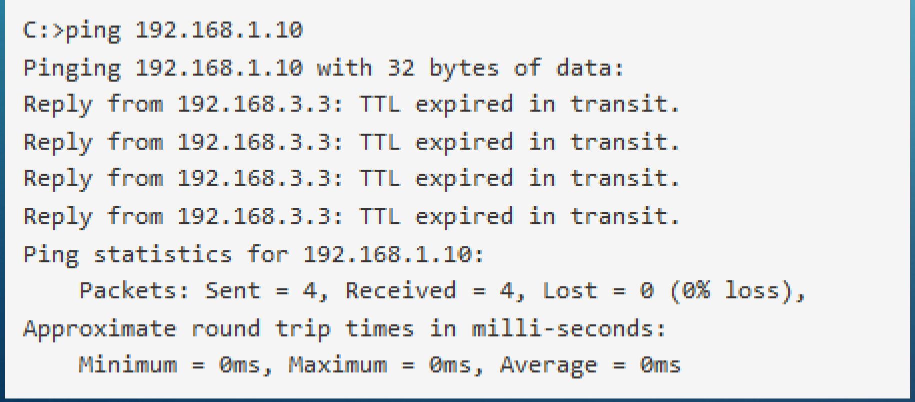
- NSLOOKUP can be used to verify DNS resolution. It can also see reverse DNS, or what DNS is assigned to what IP address.
- You can configure it to use any accessible DNS server, independent of how your device is configured.



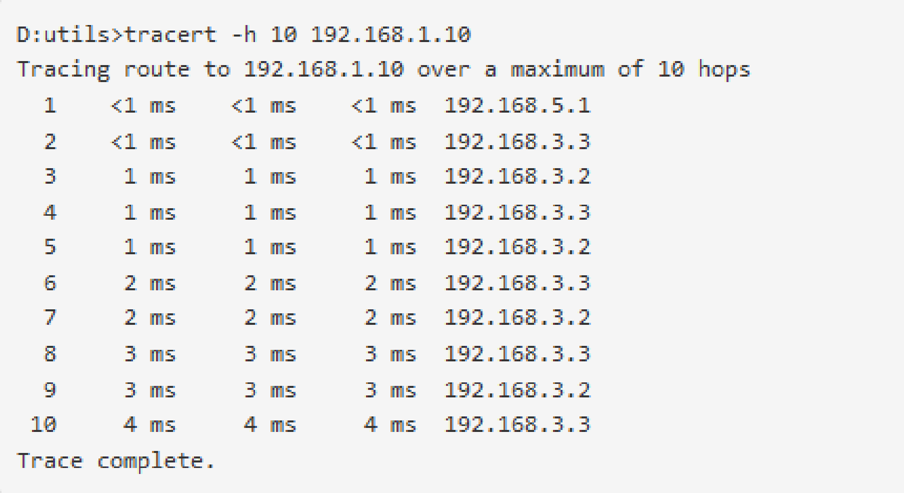
```
C:\Users\jcwhiteside>nslookup
Default Server:  aduafns.alaska.edu
Address:  137.229.15.5

> server 1.1.1.1
Default Server:  one.one.one.one
Address:  1.1.1.1

> google.com
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:400a:803::200e
          172.217.14.206

> 172.217.14.206
Server:  one.one.one.one
Address:  1.1.1.1

Name:    sea30s01-in-f14.1e100.net
Address:  172.217.14.206

>
```

WHAT A ROUTING LOOP LOOKS LIKE

- Routing loops are somewhat rare, but look very distinctive from a troubleshooting perspective.
- Routing loops are almost always configuration problems or a result of compounding dynamic routing protocol problems.



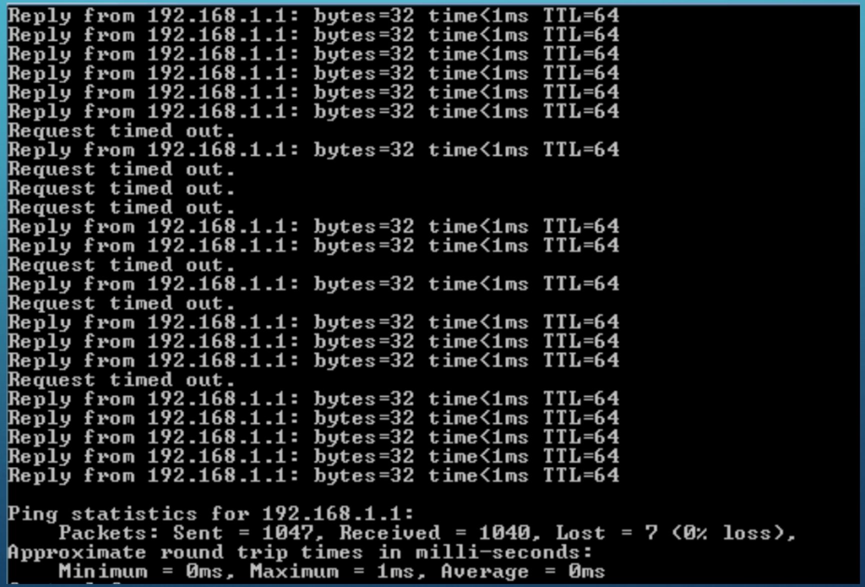
```
C:>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.3.3: TTL expired in transit.
Reply from 192.168.3.3: TTL expired in transit.
Reply from 192.168.3.3: TTL expired in transit.
Reply from 192.168.3.3: TTL expired in transit.
Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



```
D:utils>tracert -h 10 192.168.1.10
Tracing route to 192.168.1.10 over a maximum of 10 hops
  1    <1 ms    <1 ms    <1 ms  192.168.5.1
  2    <1 ms    <1 ms    <1 ms  192.168.3.3
  3     1 ms     1 ms     1 ms  192.168.3.2
  4     1 ms     1 ms     1 ms  192.168.3.3
  5     1 ms     1 ms     1 ms  192.168.3.2
  6     2 ms     2 ms     2 ms  192.168.3.3
  7     2 ms     2 ms     2 ms  192.168.3.2
  8     3 ms     3 ms     3 ms  192.168.3.3
  9     3 ms     3 ms     3 ms  192.168.3.2
 10     4 ms     4 ms     4 ms  192.168.3.3
Trace complete.
```

WHAT PACKET LOSS LOOKS LIKE

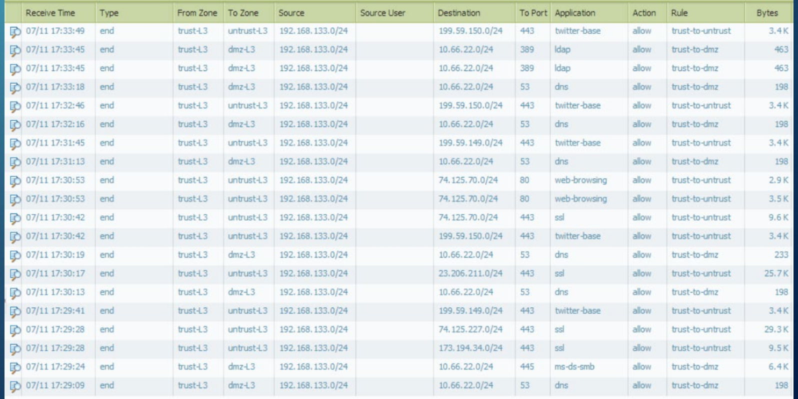
- Packet loss will often present in multiple ways, but will often affect all types of network communication.
- It is often caused by a single device but can be seen across multiple devices.



```
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
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
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
Request timed out.
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

Ping statistics for 192.168.1.1:
    Packets: Sent = 1047, Received = 1040, Lost = 7 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

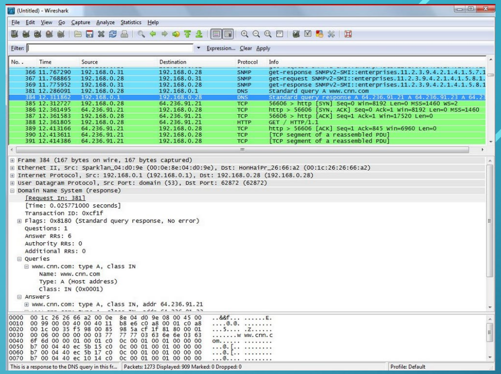
NETWORK TROUBLESHOOTING ESSENTIALS

- Firewalls often produce very verbose logs of traffic that can be used for troubleshooting.
- When having network problems, one of the first things that should be checked is whether the firewall is blocking traffic. Sometimes the policy isn't right, or sometimes it can confirm something is actually successful.



Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
07/11 17:33:49	end	trust-L3	untrust-L3	192.168.133.0/24		199.59.150.0/24	443	twitter-base	allow	trust-to-untrust	3.4 K
07/11 17:33:45	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	389	ldap	allow	trust-to-dmz	463
07/11 17:33:45	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	389	ldap	allow	trust-to-dmz	463
07/11 17:33:18	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	198
07/11 17:32:46	end	trust-L3	untrust-L3	192.168.133.0/24		199.59.150.0/24	443	twitter-base	allow	trust-to-untrust	3.4 K
07/11 17:32:16	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	198
07/11 17:31:45	end	trust-L3	untrust-L3	192.168.133.0/24		199.59.149.0/24	443	twitter-base	allow	trust-to-untrust	3.4 K
07/11 17:31:13	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	198
07/11 17:30:53	end	trust-L3	untrust-L3	192.168.133.0/24		74.125.70.0/24	80	web-browsing	allow	trust-to-untrust	2.9 K
07/11 17:30:53	end	trust-L3	untrust-L3	192.168.133.0/24		74.125.70.0/24	80	web-browsing	allow	trust-to-untrust	3.5 K
07/11 17:30:42	end	trust-L3	untrust-L3	192.168.133.0/24		74.125.70.0/24	443	ssl	allow	trust-to-untrust	9.6 K
07/11 17:30:42	end	trust-L3	untrust-L3	192.168.133.0/24		199.59.150.0/24	443	twitter-base	allow	trust-to-untrust	3.4 K
07/11 17:30:19	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	233
07/11 17:30:17	end	trust-L3	untrust-L3	192.168.133.0/24		23.206.211.0/24	443	ssl	allow	trust-to-untrust	25.7 K
07/11 17:30:13	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	198
07/11 17:29:41	end	trust-L3	untrust-L3	192.168.133.0/24		199.59.149.0/24	443	twitter-base	allow	trust-to-untrust	3.4 K
07/11 17:29:28	end	trust-L3	untrust-L3	192.168.133.0/24		74.125.227.0/24	443	ssl	allow	trust-to-untrust	29.3 K
07/11 17:29:28	end	trust-L3	untrust-L3	192.168.133.0/24		173.194.34.0/24	443	ssl	allow	trust-to-untrust	9.5 K
07/11 17:29:24	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	445	ms-ds-smb	allow	trust-to-dmz	6.4 K
07/11 17:29:09	end	trust-L3	dmz-L3	192.168.133.0/24		10.66.22.0/24	53	dns	allow	trust-to-dmz	198

NETWORK TROUBLESHOOTING ESSENTIALS

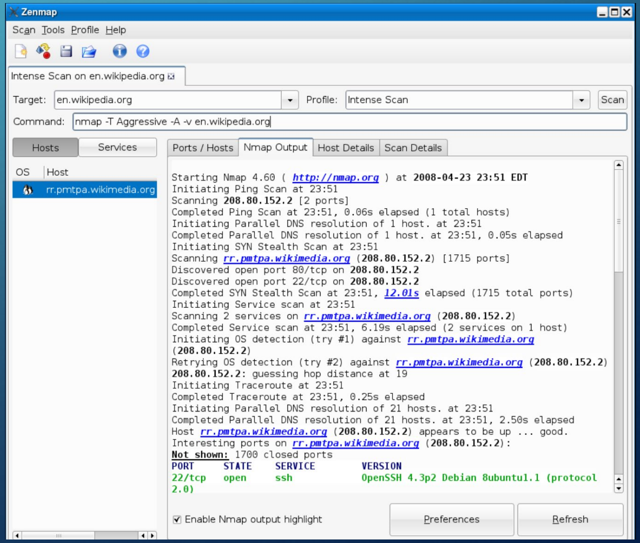

(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source          Destination     Protocol  Info
   366 11.767290   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.7.1
   367 11.768865   192.168.0.28    192.168.0.31    SNMP      get-request SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1.
   369 11.775952   192.168.0.31    192.168.0.28    SNMP      get-response SNMPv2-SMI::enterprises.11.2.3.9.4.2.1.4.1.5.8.1
   381 12.286091   192.168.0.28    192.168.0.1     DNS       Standard query A www.cnn.com
   384 12.311862   192.168.0.1     192.168.0.28    DNS       Standard query response A 64.236.91.21 A 64.236.91.23 A 64.2
   385 12.312727   192.168.0.28    64.236.91.21    TCP       56606 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   386 12.361495   64.236.91.21    192.168.0.28    TCP       http > 56606 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
   387 12.361583   192.168.0.28    64.236.91.21    TCP       56606 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
   388 12.361805   192.168.0.28    64.236.91.21    HTTP      GET / HTTP/1.1
   389 12.413166   64.236.91.21    192.168.0.28    TCP       http > 56606 [ACK] Seq=1 Ack=845 Win=6960 Len=0
   390 12.413611   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]
   391 12.414386   64.236.91.21    192.168.0.28    TCP       [TCP segment of a reassembled PDU]

⊞ Frame 384 (167 bytes on wire, 167 bytes captured)
⊞ Ethernet II, Src: Sparklan_04:d0:9e (00:0e:8e:04:d0:9e), Dst: HonHaiPr_26:66:a2 (00:1c:26:26:66:a2)
⊞ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.28 (192.168.0.28)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 62872 (62872)
⊟ Domain Name System (response)
    [Request In: 381]
    [Time: 0.025771000 seconds]
    Transaction ID: 0xcf1f
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 6
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.cnn.com: type A, class IN
        Name: www.cnn.com
        Type: A (Host address)
        Class: IN (0x0001)
  ⊟ Answers
    ⊞ www.cnn.com: type A, class IN, addr 64.236.91.21

0000  00 1c 26 26 66 a2 00 0e  8e 04 d0 9e 08 00 45 00   ..&&f... ......E.
0010  00 99 00 00 40 00 40 11  b8 e6 c0 a8 00 01 c0 a8   ....@.@. ........
0020  00 1c 00 35 f5 98 00 85  98 5a cf 1f 81 80 00 01   ...5.... .Z......
0030  00 06 00 00 00 00 03 77  77 77 03 63 6e 6e 03 63   .......w ww.cnn.c
0040  6f 6d 00 00 01 00 01 c0  0c 00 01 00 01 00 00 00   om...... ........
0050  b7 00 04 40 ec 5b 15 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0060  b7 00 04 40 ec 5b 17 c0  0c 00 01 00 01 00 00 00   ...@.[.. ........
0070  b7 00 04 40 ec 10 14 c0  0c 00 01 00 01 00 00 00   ...@.... ........

This is a response to the DNS query in this fr...   Packets: 1273 Displayed: 909 Marked: 0 Dropped: 0   Profile: Default
```

- Packet captures are one of the most authoritative methods of network troubleshooting available. It allows the viewing of every packet traversing the network.
- The most common tool used for this is Wireshark.
- Packets can be captured from the client or server itself, or from the network. Network applications often require mirroring packets from one interface to another.

NETWORK TROUBLESHOOTING ESSENTIALS

- NMAP is an open source, multi-OS and versatile network scanner & penetration tester that can be used to discover hosts, open communication ports and even vulnerabilities.
- Given the power of the tool, it should be used in white hat scenarios only, on devices you are authorized to investigate.



Target: en.wikipedia.org

Profile: Intense Scan

Command: nmap -T Aggressive -A -v en.wikipedia.org

```
Starting Nmap 4.60 ( http://nmap.org ) at 2008-04-23 23:51 EDT
Initiating Ping Scan at 23:51
Scanning 208.80.152.2 [2 ports]
Completed Ping Scan at 23:51, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:51
Completed Parallel DNS resolution of 1 host. at 23:51, 0.05s elapsed
Initiating SYN Stealth Scan at 23:51
Scanning rr.pmtpa.wikimedia.org (208.80.152.2) [1715 ports]
Discovered open port 80/tcp on 208.80.152.2
Discovered open port 22/tcp on 208.80.152.2
Completed SYN Stealth Scan at 23:51, 12.01s elapsed (1715 total ports)
Initiating Service scan at 23:51
Scanning 2 services on rr.pmtpa.wikimedia.org (208.80.152.2)
Completed Service scan at 23:51, 6.19s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against rr.pmtpa.wikimedia.org
(208.80.152.2)
Retrying OS detection (try #2) against rr.pmtpa.wikimedia.org (208.80.152.2)
208.80.152.2: guessing hop distance at 19
Initiating Traceroute at 23:51
Completed Traceroute at 23:51, 0.25s elapsed
Initiating Parallel DNS resolution of 21 hosts. at 23:51
Completed Parallel DNS resolution of 21 hosts. at 23:51, 2.50s elapsed
Host rr.pmtpa.wikimedia.org (208.80.152.2) appears to be up ... good.
Interesting ports on rr.pmtpa.wikimedia.org (208.80.152.2):
Not shown: 1700 closed ports
PORT     STATE    SERVICE        VERSION
22/tcp   open     ssh            OpenSSH 4.3p2 Debian 8ubuntu1.1 (protocol
2.0)
```

☑ Enable Nmap output highlight

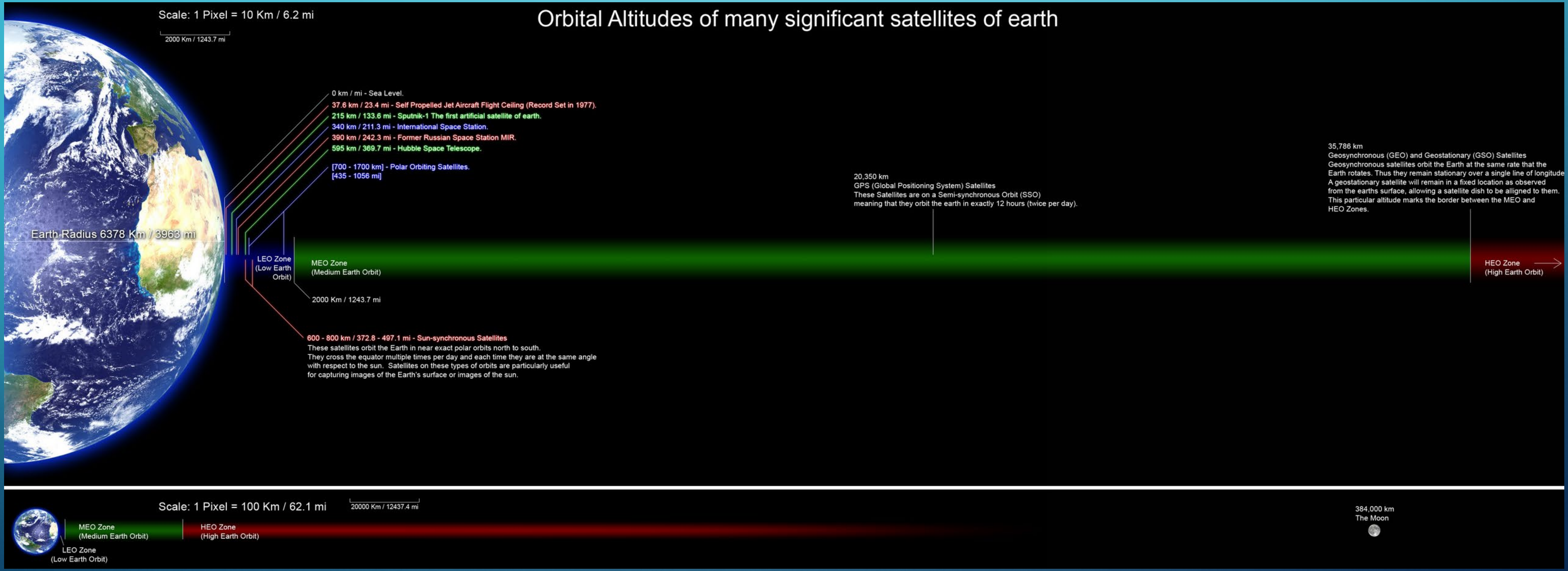
NETWORK TROUBLESHOOTING ESSENTIALS

- Identifying loss in a network often requires multiple techniques. It might combine traceroutes along with pings to identify the specific source of the loss.
- It’s important to isolate the possible sources. For example, do you only see it on wireless and not wired networks? Does it happen one direction and not another?
- What isn’t there can often be more important than what is there. Knowledge of protocols and expected behavior is sometimes required.

FUTURE OF SATELLITE INTERNET SERVICES

- Several companies are currently developing low-earth-orbit satellite arrays. OneWeb, StarLink/SpaceX and Astranis all have active projects happening right now. Other competing companies are still in the early stages.
- Test satellites have been launched by all three of the above competitors.
- Initial OneWeb testing has shown low latency (sub-40ms) and the ability to transfer downlink traffic at up to 400mbit/sec and could get better with optimization.
- Current indicators show possible service availability as soon as 2020 or 2021.
- Has been tried before, but the internet is slightly more popular now than the 90's.

FUTURE OF SATELLITE INTERNET SERVICES



Orbital Altitudes of many significant satellites of earth

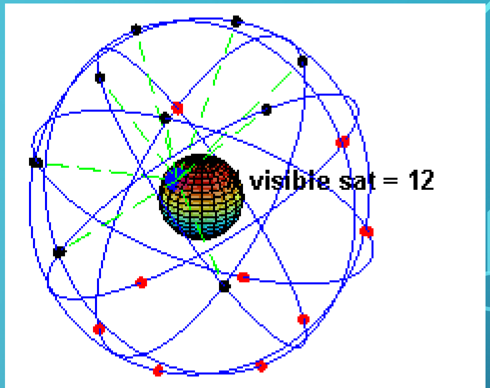
Scale: 1 Pixel = 10 Km / 6.2 mi
2000 Km / 1243.7 mi
0 km / mi - Sea Level.
37.6 km / 23.4 mi - Self Propelled Jet Aircraft Flight Ceiling (Record Set in 1977).
215 km / 133.6 mi - Sputnik-1 The first artificial satellite of earth.
340 km / 211.3 mi - International Space Station.
390 km / 242.3 mi - Former Russian Space Station MIR.
595 km / 369.7 mi - Hubble Space Telescope.
[700 - 1700 km] - Polar Orbiting Satellites.
[435 - 1056 mi]
Earth Radius 6378 Km / 3963 mi
LEO Zone
(Low Earth
Orbit)
MEO Zone
(Medium Earth Orbit)
2000 Km / 1243.7 mi
HEO Zone
(High Earth Orbit)

600 - 800 km / 372.8 - 497.1 mi - Sun-synchronous Satellites
These satellites orbit the Earth in near exact polar orbits north to south.
They cross the equator multiple times per day and each time they are at the same angle
with respect to the sun. Satellites on these types of orbits are particularly useful
for capturing images of the Earth's surface or images of the sun.

20,350 km
GPS (Global Positioning System) Satellites
These Satellites are on a Semi-synchronous Orbit (SSO)
meaning that they orbit the earth in exactly 12 hours (twice per day).

35,786 km
Geosynchronous (GEO) and Geostationary (GSO) Satellites
Geosynchronous satellites orbit the Earth at the same rate that the
Earth rotates. Thus they remain stationary over a single line of longitude
A geostationary satellite will remain in a fixed location as observed
from the earths surface, allowing a satellite dish to be alligned to them.
This particular altitude marks the border between the MEO and
HEO Zones.

FUTURE OF SATELLITE INTERNET SERVICES



- Technology has the potential to provide high speed internet access anywhere on earth.
- Primary customers will likely be ships, research vessels and airline operators. These customers are likely to get optimal results in their remote operating areas given limited competition.
- Future network designs may need to accommodate multiple providers for redundancy purposes.

FUTURE OF SATELLITE INTERNET SERVICES

- Technology is also likely to be used for backhaul services as well as retail/wholesale internet services. Could also be used to improve remote 4G/5G LTE services.
- Future networks will likely be a complex combination of low, medium and high earth orbit satellites with seamless handoffs, with each orbit handling what its best at.
- Satellite network density would theoretically allow less congested satellites to provide service when one becomes congested.
- Frequency spectrum tends to be very high, favorable for high bandwidth applications. Expect 12-18GHz (KU band) with progressive pitch preventing interference with existing geosynchronous satellite technologies.

FUTURE OF INTERNET SERVICES

- SpaceX is planning the constellation called StarLink.
- SpaceX has an advantage of less expensive launch services, however, it has struggled to get priority spectrum rights and is also still adjusting orbit plans.
- Their design calls for inter-satellite communication. This has a huge advantage that could allow it to actually beat terrestrial applications.
- Currently has planned the largest constellation of all the companies with over 12K satellites planned. Currently has 62 in-orbit with 57 functional.

FUTURE OF SATELLITE INTERNET SERVICES

- OneWeb is planning a constellation of 600 satellites in low earth orbit (1,200KM/750mi), with 48 on-orbit spares.
- Plan has been modified to allow an additional 720 satellites in Medium Earth Orbit.
- Currently has six successful satellites in orbit and is the only company to openly publish their test results thus far.
- Primary initial focus is on Alaska and other northern communities.

FUTURE OF SATELLITE INTERNET SERVICES

- Astranis is taking a different approach. Focusing on geo-synchronous low earth orbit services, as opposed to global services. Advantage, less cost and targeted services.
- Astranis is using Alaska and surrounding area as their primary test case and may look at other locations afterwards.
- Will resell services through Pacific Dataport, potentially as early as 2021. The full Aleutian chain will likely require additional satellites.

FUTURE OF INTERNET SERVICES

- In April 2019, Amazon has announced a potential constellation called Project Kuiper. Project is headed by Rajeev Badyal, former VP of SpaceX satellite internet business unit.
- Proposal includes 3,200+ satellites and is only in the initial stages of planning.
- No satellites have been launched, nor has a manufacturing facility been disclosed at this time.

FUTURE OF INTERNET SERVICES

- Primary concerns of LEO Satellite Internet:
  - These constellations could fundamentally change the look of our night sky.
  - Operation in some countries/areas may not be permitted.
  - High investment costs could result in expensive services, curtailment of the proposed plans or elimination of various competitors.
  - Despite end-of-life plans, there remains a high potential of collisions that could have disastrous consequences to the final frontier.

THANK YOU FOR VISITING UAF

- Questions?