// Assignment 1

// Network Managers

/ by George Hotten

// Network Technologies

// Layouts – Topologies

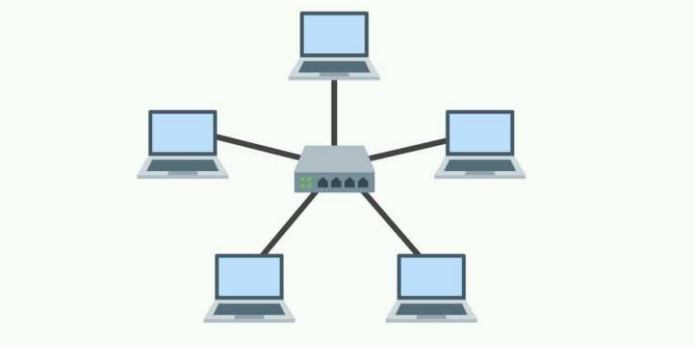
There are two types of topologies: physical and logical.

/ Physical Topology

A physical topology describes the physical way that a network is arranged, which is made up of nodes (devices such as PCs and routers) and cables (such as RJ45). A physical topology focuses on the essentials of a network, not the devices used in a network.

/ Logical Topology

Meanwhile, a logical topology describes how the devices communicate, concerned about the transmission of data and the devices used to do so such as switches and routers. A logical topology focuses on ensuring data flows optimally throughout a network, running into as little traffic as possible.

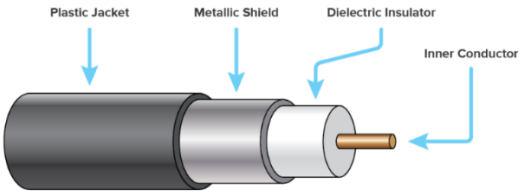


// Layouts – Connection Media

Connection media are the physical cables used to connected devices on a network together. There are multiple types of connection media, for example: coaxial, optical fibre and twisted copper pairs.

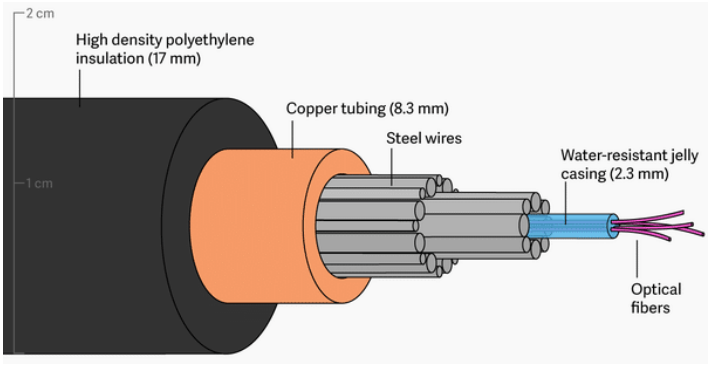
/ Coaxial

Used by telecom and internet providers, Coaxial cables allow people to receive and send data from the internet all around the world. Coaxial has an inner conductor, surrounded by layers of insulation and an insulating outer jacket. Using the centre conductor, data is transmitted via electrical signal.



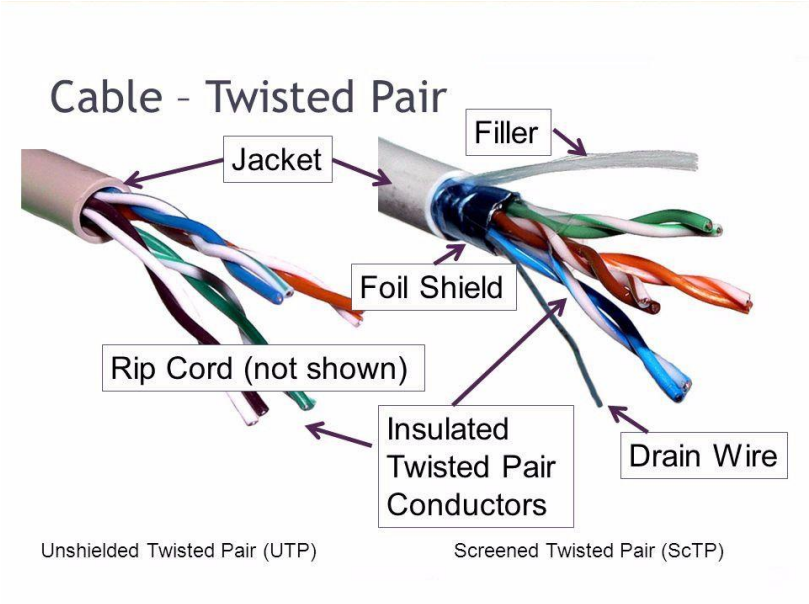
/ Optical Fibre

Optical fibre cables are made up of thin and long pure glass, about the diameter of a human hair, that are arranged in bundles. This is known as the core. There is cladding around the core which reflects light back into the core. The cladding is surrounded by a buffer coating, which's purpose is to protect from moisture and damage. Light is then sent through the cable to transmit data.



/ Twisted Copper Pairs

Twisted Copper Pairs have a twisted layout, giving them a very suitable name. They are twisted to reduce interference. In comparison, a coaxial cable has a single thick wire, whilst twisted copper pairs use multiple thin wires. To further protect from interference, some cables are known as shielded twisted copper pairs which add a shield surrounding the cables to prevent energy that may interfere with the signal.



// Network Protocols

/ ICMP

ICMP, **I**nternet **C**ontrol **M**essage **P**rotocol, is a protocol used to check if a connection can be made to another device. ICMP is especially useful as it provides an error to why data cannot reach the device, making it perfect for debugging a network. ICMP typical is used through the *ping* command.

```
[~ » ping 192.168.0.1                                    george@CutieBook-Air ]
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=6.540 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=9.307 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=5.035 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=14.836 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=16.612 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=10.714 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=12.817 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=4.231 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=11.581 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=11.827 ms
^C
--- 192.168.0.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.231/10.350/16.612/3.880 ms
```

/ DNS

DNS, **D**omain **N**ame **S**ystem, is a protocol used to translate a domain name such as *google.com* into an IP address such as *216.58.213.14* so that your computer can communicate with the server of the resource you're trying to access. This removes the need for humans to remember IP addresses, especially with the introduction of IPv6, which looks like this: *2400:cb00:2048:1::c629:d7a2*!

```
> Frame 78: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{491F424A-A5C2-4253-A3B1-ED6641D07B50}
> Ethernet II, Src: Sophos_fc:00:09 (c8:4f:86:fc:00:09), Dst: Micro-St_06:ec:64 (2c:f0:5d:06:ec:64)
> Internet Protocol Version 4, Src: 192.168.224.99, Dst: 172.20.52.109
> User Datagram Protocol, Src Port: 53, Dst Port: 63463
v Domain Name System (response)
    Transaction ID: 0xc9c0
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v hotten.uk: type A, class IN, addr 172.67.175.41
        Name: hotten.uk
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 300 (5 minutes)
        Data length: 4
        Address: 172.67.175.41
```

/ TCP/IP

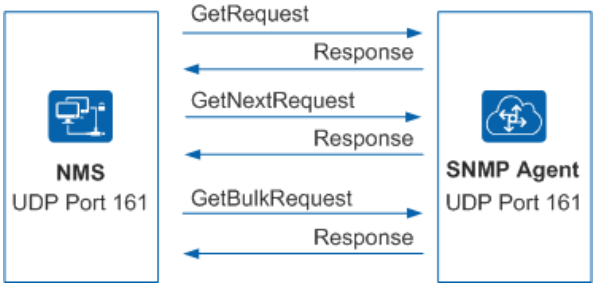
TCP/IP, **T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol, are both protocols used to send data on a network.

IP is responsible for addressing and routing packets so that devices on a network can communicate and send data to the correct location. However, Internet Protocol is a connectionless protocol meaning it doesn't make any connection to the receiving device, meaning the sending devices won't know if data has been successfully received.

This is where TCP comes in. Transmission Control Protocol is used together with IP to provide packets numbers so packets can be reordered and can be error checked. With each packet, it is given a packet number and once it has been received, the end device checks the packet number and orders the data accordingly. If any data is missing, the receiver can request the data is resent. This is because TCP establishes a connection with the receiving device using a three-way handshake.

/ SNMP

SNMP, **S**imple **N**etwork **M**anagement **P**rotocol, is a protocol used to monitor and manage SNMP-enabled devices on a network, such as a router or a printer. These are called SNMP agents. To interact with these agents, a Network Management System is used. NMS provides an interface so that administrators can easily issue commands, read/write data and receive monitoring alerts. Using a router as an example, SNMP can change the router's name and monitor its interface to check if its state changes.



// Network Devices

/ Host

A host is a device on a network that can communicate with other devices on a network. Hosts are usually devices such as clients or servers. Switches and routers don't usually fall under the "hosts" category. Host devices will have a host number, which form their IP address. For example, the IP address **192.168.0.19** can be split into two parts: the network bits and the host bits. **192.168.0** are the network bits, whilst **19** are the host bits which represent the device's host number.

/ Server

A device is classed as a server when it provides a service to another device. Some examples of services are: NGINX for a web server, Hyper-V for virtualisation and Active Directory for user and computer management. Servers are usually more powerful than end devices, potentially having over 100GB of memory and terabytes of storage. However, the specifications of a server depend on its use-case, for example a storage server wouldn't need as many CPU cores as a virtualisation server. Nonetheless, a device does not need top-end specifications to be a server.

/ Switch

A switch is a layer 2 networking device that routes data to the correct device based off their MAC address. Unlike a hub, a switch keeps a switching table of what MAC address is connected to each port, meaning data can be sent directly the intended device instead of being broadcasted.

/ Router

A router is a layer 3 networking device that routes data to the correct device based off their IP address. Unlike a switch, routers often cannot take a direct connection to the intended device meaning they will need to take multiple hops to different routers before reaching its intended address. Routers use routing tables to know what networks are connected to it, so it knows where any received data can be sent if it isn't intended for itself.

/ Network Interface Card

A NIC, **N**etwork **I**nterface **C**ard, is a component connected internally in a device which allows it to send and receive data. The NIC handles the requirements at the first layer of the OSI model to send data down an ethernet cable. The NIC also conforms to layer 2, as the NIC has a burnt in MAC address meaning it cannot be changed. Each NIC has its own unique MAC so it can have data sent specifically to itself, typically used by layer 2 switches.

// The Purpose of Network Management Tools

// Terminal Commands

/ ping

The purpose of the ping command is to check if a connection can be made to another device. Ping uses the ICMP protocol, meaning other data such as timings and error data if a connection cannot be made is provided. This makes ping a great tool for debugging a network.

```
~ » ping 192.168.0.1                                    george@CutieBook-Air
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=6.540 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=9.307 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=5.035 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=14.836 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=16.612 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=10.714 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=12.817 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=4.231 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=11.581 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=11.827 ms
^C
--- 192.168.0.1 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.231/10.350/16.612/3.880 ms
```

/ tracert

The purpose of the tracert command is to show the hops between routers to reach a desired IP address. Tracert also measures the timings between hops and can be used in diagnostics if the data cannot reach its intended location as you can see where the point of failure is. Tracert uses the ICMP protocol which collects data about the routers used during transmission and if they can transfer data effectively.

```
~ » traceroute hotten.uk                                    george@CutieBook-Air
traceroute: Warning: hotten.uk has multiple addresses; using 104.21.48.7
traceroute to hotten.uk (104.21.48.7), 64 hops max, 52 byte packets
 1  router.i.hotten.uk (192.168.0.1)  11.440 ms  4.375 ms  4.519 ms
 2  10.53.35.197 (10.53.35.197)  13.557 ms  12.762 ms  15.409 ms
 3  perr-core-2a-ae89-0.network.virginmedia.net (80.1.69.169)  15.699 ms  23.036 ms  19.111 ms
 4  perr-wblk-1b-xe-200-0.network.virginmedia.net (62.254.1.218)  18.305 ms  20.865 ms  10.537 ms
 5  * * *
 6  * * *
 7  uk-lon01c-ri2-ae-6-0.aorta.net (84.116.136.98)  24.008 ms  20.645 ms  22.891 ms
 8  213.46.175.154 (213.46.175.154)  23.932 ms  22.504 ms  24.269 ms
 9  172.70.160.4 (172.70.160.4)  38.708 ms  26.300 ms
    172.70.94.4 (172.70.94.4)  25.746 ms
10  104.21.48.7 (104.21.48.7)  27.972 ms  22.623 ms  24.203 ms
```

/ ipconfig

The purpose of the ipconfig command is to check IP information such as the device's IP address, what the default gateway or DNS server. This can be useful to see if your device has received an IP address from DHCP correctly, or to check if your default gateway is correct if you cannot access the internet. Running the ipconfig command on its own doesn't provide that much information, however appending /all to the end reveals more in-depth information about your configuration.

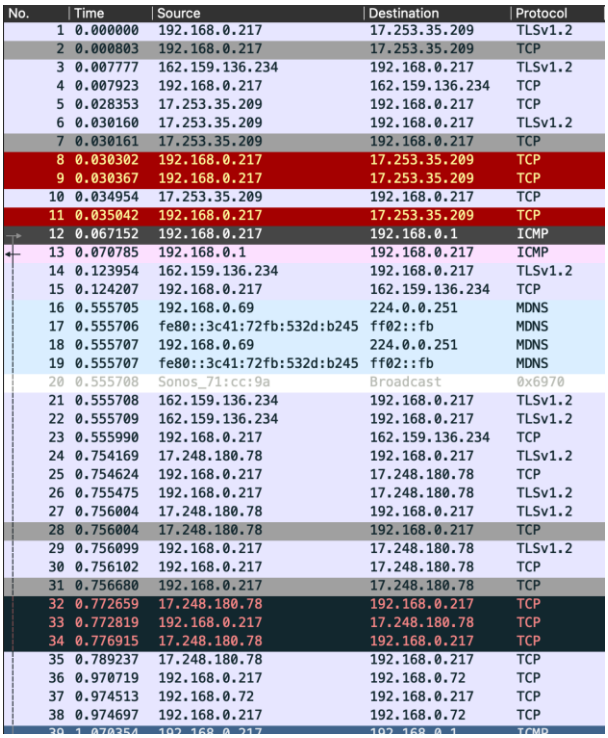
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Parallels VirtIO Ethernet Adapter
   Physical Address. . . . . . . . . : 00-1C-42-41-12-6D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdb2:2c26:f4e4:0:5c7c:d1d9:dd46:8594(Preferred)
   Temporary IPv6 Address. . . . . . : fdb2:2c26:f4e4:0:390c:8d56:ae64:752d(Preferred)
   Link-local IPv6 Address . . . . . : fe80::5c7c:d1d9:dd46:8594%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.211.55.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, September 25, 2022 4:38:48 PM
   Lease Expires . . . . . . . . . . : Sunday, September 25, 2022 5:08:49 PM
   Default Gateway . . . . . . . . . : 10.211.55.1
   DHCP Server . . . . . . . . . . . : 10.211.55.1
   DHCPv6 IAID . . . . . . . . . . . : 100670530
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-45-42-CF-00-1C-42-41-12-6D
   DNS Servers . . . . . . . . . . . : 10.211.55.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

// Applications

/ Wireshark

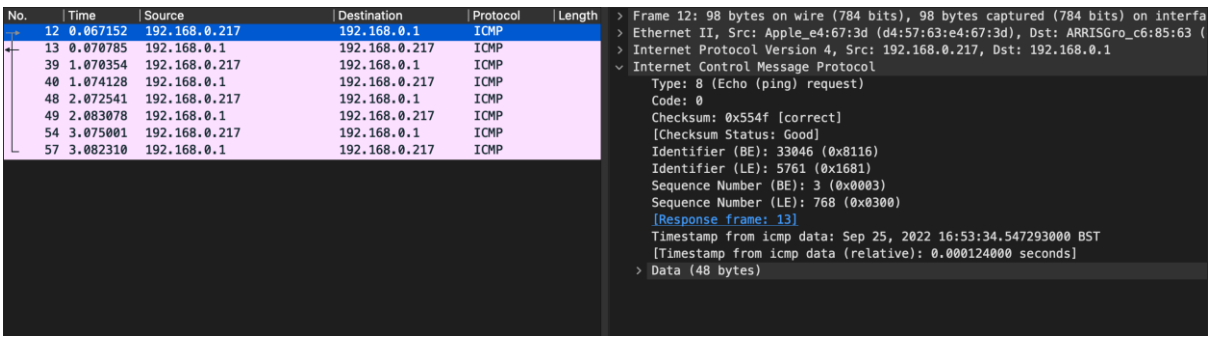
The purpose of Wireshark is to capture and analyse traffic coming in and out of your interface card. This can be used analyse your network traffic for a more in-depth understanding of what an application is sending on the internet or for more malicious purposes.



No.	Time	Source	Destination	Protocol
1	0.000000	192.168.0.217	17.253.35.209	TLSv1.2
2	0.000803	192.168.0.217	17.253.35.209	TCP
3	0.007777	162.159.136.234	192.168.0.217	TLSv1.2
4	0.007923	192.168.0.217	162.159.136.234	TCP
5	0.028353	17.253.35.209	192.168.0.217	TCP
6	0.030160	17.253.35.209	192.168.0.217	TLSv1.2
7	0.030161	17.253.35.209	192.168.0.217	TCP
8	0.030302	192.168.0.217	17.253.35.209	TCP
9	0.030367	192.168.0.217	17.253.35.209	TCP
10	0.034954	17.253.35.209	192.168.0.217	TCP
11	0.035042	192.168.0.217	17.253.35.209	TCP
12	0.067152	192.168.0.217	192.168.0.1	ICMP
13	0.070785	192.168.0.1	192.168.0.217	ICMP
14	0.123954	162.159.136.234	192.168.0.217	TLSv1.2
15	0.124207	192.168.0.217	162.159.136.234	TCP
16	0.555705	192.168.0.69	224.0.0.251	MDNS
17	0.555706	fe80::3c41:72fb:532d:b245	ff02::fb	MDNS
18	0.555707	192.168.0.69	224.0.0.251	MDNS
19	0.555707	fe80::3c41:72fb:532d:b245	ff02::fb	MDNS
20	0.555708	Sonos_71:cc:9a	Broadcast	0x6970
21	0.555708	162.159.136.234	192.168.0.217	TLSv1.2
22	0.555709	162.159.136.234	192.168.0.217	TLSv1.2
23	0.555990	192.168.0.217	162.159.136.234	TCP
24	0.754169	17.248.180.78	192.168.0.217	TLSv1.2
25	0.754624	192.168.0.217	17.248.180.78	TCP
26	0.755475	192.168.0.217	17.248.180.78	TLSv1.2
27	0.756004	17.248.180.78	192.168.0.217	TLSv1.2
28	0.756004	17.248.180.78	192.168.0.217	TCP
29	0.756099	192.168.0.217	17.248.180.78	TLSv1.2
30	0.756102	192.168.0.217	17.248.180.78	TCP
31	0.756680	192.168.0.217	17.248.180.78	TCP
32	0.772659	17.248.180.78	192.168.0.217	TCP
33	0.772819	192.168.0.217	17.248.180.78	TCP
34	0.776915	17.248.180.78	192.168.0.217	TCP
35	0.789237	17.248.180.78	192.168.0.217	TCP
36	0.970719	192.168.0.217	192.168.0.72	TCP
37	0.974513	192.168.0.72	192.168.0.217	TCP
38	0.974697	192.168.0.217	192.168.0.72	TCP

Using a filter, you can filter down the capture to exactly what you are looking for which in this example is ICMP.

No.	Time	Source	Destination	Protocol	Length
12	0.067152	192.168.0.217	192.168.0.1	ICMP	
13	0.070785	192.168.0.1	192.168.0.217	ICMP	
39	1.070354	192.168.0.217	192.168.0.1	ICMP	
40	1.074128	192.168.0.1	192.168.0.217	ICMP	
48	2.072541	192.168.0.217	192.168.0.1	ICMP	
49	2.083078	192.168.0.1	192.168.0.217	ICMP	
54	3.075001	192.168.0.217	192.168.0.1	ICMP	
57	3.082310	192.168.0.1	192.168.0.217	ICMP	



No.	Time	Source	Destination	Protocol	Length
12	0.067152	192.168.0.217	192.168.0.1	ICMP	
13	0.070785	192.168.0.1	192.168.0.217	ICMP	
39	1.070354	192.168.0.217	192.168.0.1	ICMP	
40	1.074128	192.168.0.1	192.168.0.217	ICMP	
48	2.072541	192.168.0.217	192.168.0.1	ICMP	
49	2.083078	192.168.0.1	192.168.0.217	ICMP	
54	3.075001	192.168.0.217	192.168.0.1	ICMP	
57	3.082310	192.168.0.1	192.168.0.217	ICMP	

```
> Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interfa
> Ethernet II, Src: Apple_e4:67:3d (d4:57:63:e4:67:3d), Dst: ARRISGro_c6:85:63 (
> Internet Protocol Version 4, Src: 192.168.0.217, Dst: 192.168.0.1
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x554f [correct]
    [Checksum Status: Good]
    Identifier (BE): 33046 (0x8116)
    Identifier (LE): 5761 (0x1681)
    Sequence Number (BE): 3 (0x0003)
    Sequence Number (LE): 768 (0x0300)
    [Response frame: 13]
    Timestamp from icmp data: Sep 25, 2022 16:53:34.547293000 BST
    [Timestamp from icmp data (relative): 0.000124000 seconds]
  > Data (48 bytes)
```

After selecting a packet, you can analyse the layers of the packet and the exact data sent inside them. In the above image, you can see the two devices MAC addresses, IP addresses and the data sent for the ICMP request.

/ Nmap

The purpose of Nmap is to check networks for vulnerabilities, open ports on devices and to map out what devices are connected to the network. This can be used for penetration testing to see if any devices have vulnerable ports accessible.

Nmap has a wide variety of command line switches, allowing you to modify your scan to your needs. For example, scan a specific range of ports or turn on aggressive mode that attempts to perform OS detection, version detection and script scanning. However, aggressive scans send more probes (data sent to learn information about a device) making it more susceptible to being detected.

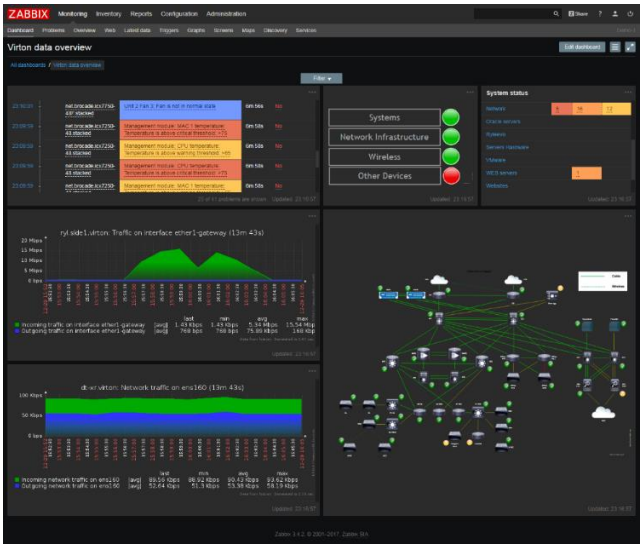
Here is an example of an aggressive scan, using one of my raspberry pi's as the subject.

```
~ » nmap -A blackhole.i.hotten.uk                                                george@CutieBook-Air
Starting Nmap 7.93 ( https://nmap.org ) at 2022-09-29 12:26 BST
Nmap scan report for blackhole.i.hotten.uk (192.168.0.3)
Host is up (0.0064s latency).
rDNS record for 192.168.0.3: pi.hole
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Raspbian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 2c7a0f65ae5f970ab698096d5ba1f136 (RSA)
|   256 7177ff5ff1e53045fe6c42d522309cdb (ECDSA)
|_  256 e5b2a83fe3fe757ae0d430d31189f9eb (ED25519)
53/tcp   open  domain  dnsmasq pi-hole-v2.87rc1
| dns-nsid:
|_  bind.version: dnsmasq-pi-hole-v2.87rc1
80/tcp   open  http    lighttpd 1.4.59
|_http-server-header: lighttpd/1.4.59
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
5900/tcp open  vnc     RealVNC Enterprise 5.3 or later (protocol 5.0)
| vnc-info:
|   Protocol version: 005.000
|   Security types:
|     Unknown security type (13)
|     RA2 (5)
|     RA2ne (6)
|     Unknown security type (130)
|_    Unknown security type (192)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.56 seconds
```

/ Zabbix

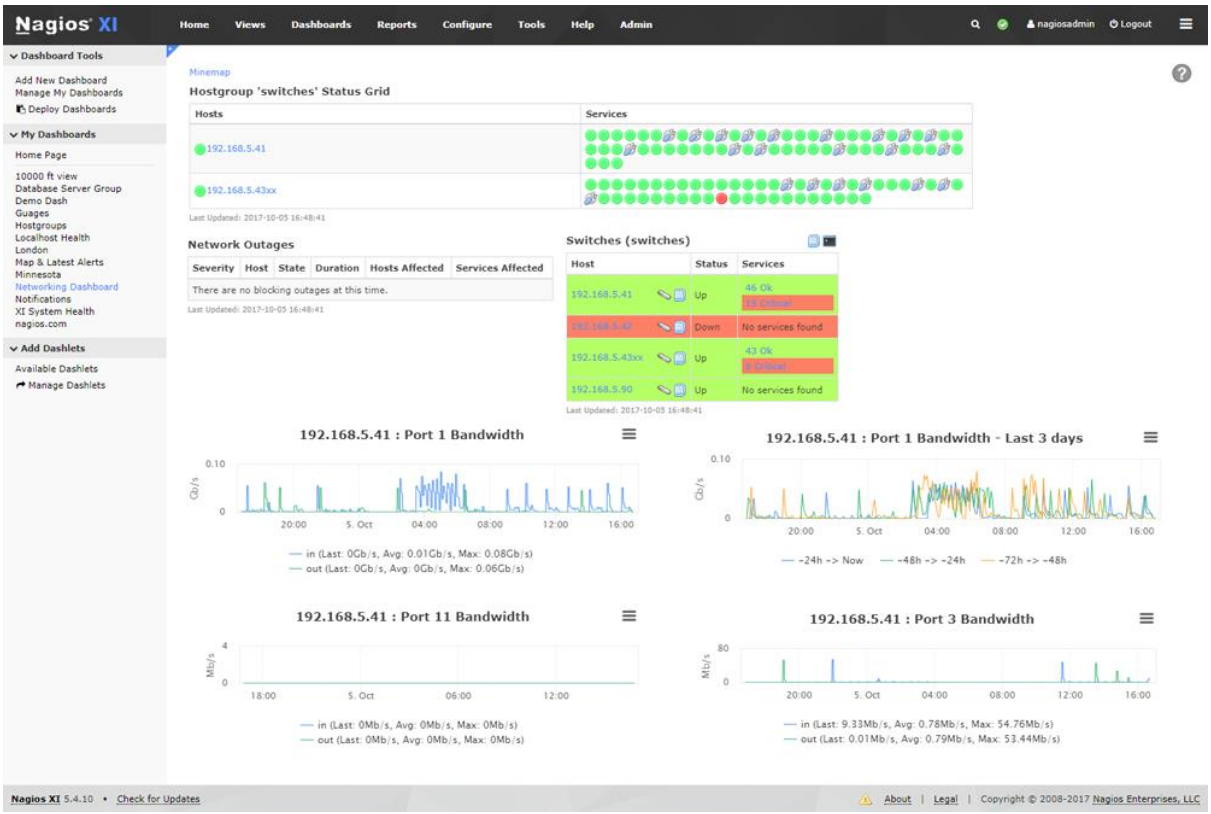
The purpose of Zabbix is to monitor a network and its devices. For example, servers, cloud services or virtual machines. Zabbix can provide metrics such as network utilisation, disk space consumption and component load – such as CPU and memory. It can also provide visualisations of your network to show where a fault lies and how it effects other devices on the network.



The software allows you to setup alerts when data passes a certain threshold, for example if the temperature of the system breaches 90 degrees. Alerts can be sent via email, SMS, MS Teams and more.

/ Nagios XI

Like Zabbix, the purpose of Nagios XI is to provide monitoring for a network and its devices. It has features such as monitoring the status of different services such as IMAP, FTP, HTTPS, etc. It can send configurable alerts via email, SMS and more. It can monitor the hardware of a network too checking if devices are online and functioning as they should. Nagios XI has the capability to check the status of ports on switches and routers meaning faults can be identified and resolved sooner.



// What are the different Network Management tools and how do they assist with Fault Management?

// Device Configuration

The function of device configuration is to allow network administrators to remotely edit the configuration of devices on a network. Devices on a network are often put into groups based on their usage, for example student computers would be in a different group to staff computers, this means devices can be configured in bulk, saving network administrators from individually configuring devices and allowing them to be in harmony with each other.

This helps with fault management as, for example, if a fault arises on the machines due to an error in configuration network administrators can remotely fix the issue and push the changes to all devices affected within minutes.

// Account Management

The function of account management is to allow network administrators to remotely manage user accounts on devices of a network, this is usually done via services such as Active Directory. Account management services allow you to create groups of users, giving them different privileges and access. This is often managed through the Group Policy snap-in. This allows users of the directory to login into any machine that is also part of the directory, allowing network administrators to easily setup and configure new/existing users without needing to add an account to every machine on a network.

This helps with fault management as if there is an issue with user accounts, network administrators will know where to find and fix the error as all accounts are managed centrally.

// Checking Network Traffic and Performance Variables

The function of network traffic and performance variables is that it allows network administrators to monitor the status of the network, checking the amount of data coming in and out of the network, along with latency. This allows them to check for any suspicious activity or for anything that seems out of their normal usage, potentially uncovering malware.

This helps with fault management as network administrators can easily identify any issues with the network by reviewing the data, high amounts of traffic could show a potential denial-of-service attack.

// Security

The function of security is to ensure all devices on a network remain secure and are protected from malware. This is often achieved through the installation of anti-malware software such as Malwarebytes and through configuration/access-levels of users and devices. For example, students don't need the same level of access as network administrators so access to features such as device configuration should be revoked. This ensures that configurations cannot be tampered with and are maintained to ensure security.

This helps with fault management as having proper security systems ensures that a fault caused by a breach or malware attack is significantly reduced. Without this, a network controlled by a central server could easily be brought to a halt if the controller is compromised.

// Reporting and Data Logging

The function of reporting is being able to generate reports of metrics within your network, such as number of users within the network and how many users have been recently deleted. Reports should be able to be generated on demand and ready to be presented if asked. The data for these reports are generated through data logging: keeping track of metrics such as the number of users, the bandwidth used or the peak number of active network users at one time. Data logging can be done manually or automatic, depending on the data being logged, and kept for a specific amount of time decided by the company.

This helps with fault management as network administrators will be able to see changes in their data and be able to identify the fault: for example, the network's bandwidth could be significantly reduced compared to the previous day's logging.

// How Routine Performance Management Activities Aid with Network Management

// Backups

Backups aid with network management as if there is a fault due to a drive failure or configuration issue, network administrators can rollback their data to a state where the fault was not present. To ensure this is effective, backups should be taken as regularly as possible to both an on-site and off-site location. This further ensures if there are any disasters in the building of a network, such as fires, data is safe in an off-site location. The frequency of your backup should depend on how important your data is, for example the most sensitive and important data could be backed up twice daily, whilst system files could be backed up weekly.

// User Account Management

Regularly performing User Account Management activities involves performing tasks such as deleting old inactive user accounts, ensuring group policy is up to date and that appropriate access levels are given. This aids with network management as it helps keep the user directory clean and organised with active accounts, and it helps ensure that the network stays secure as users only have access to what they need to. Without the proper permissions setup on user accounts, the network could be at risk if an account is compromised.

// Login Scripts

Login scripts often include code to map network drives, setup the default printer for the user group and to log access. This aids with network management as it can help keep a log of which users have accessed a computer and when, which would assist if there was ever a breach. It also aids with network management as it allows network administrators to easily reconfigure machines for the user that is logging in. For example, if a student logs into a machine a login script can be used to assign network drives the student needs (for example, a student area) and configure the OS for the printer that students use. If a staff member logs into that same machine, the login script can reconfigure the drive mappings and other settings so it is tailored to staff members.

// Malware Scans

Malware scans are vital on a network as they scan a computer's drive to detect any viruses or malware. If malware gets onto a network computer, it could easily spread to other computers and infect the whole network. This aids with network management as these scans can be setup to be as regular as needed, from every hour to every week. As this is done automatically, it is a pain free process that contributes to the network's security.

// File Clean-up

File clean-up heavily aids in network management as by cleaning up unused and temporary files such as the downloads folder and the window's temporary and update files. By removing these unnecessary files, it helps reduce used disk space and helps speed up malware scans as they must check less files for viruses. This also reduces the amount of space needed for backups, making them faster and more effective. The faster you can backup data, the more frequently you can back it up.

// Emerging Network Technologies

/ by George Hotten

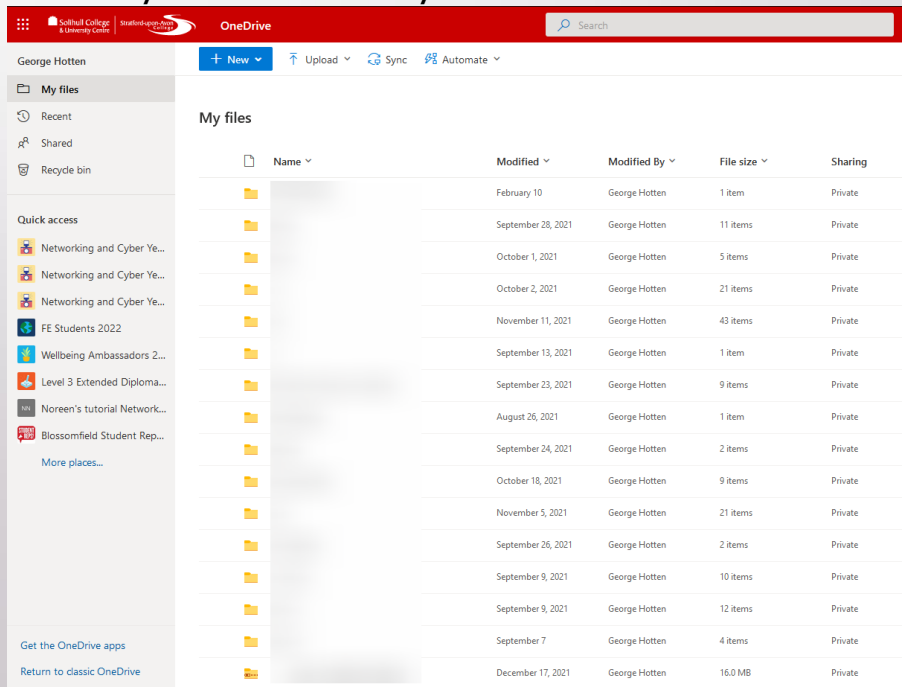
// Web Based Storage

What is Web Based Storage?

- Web Based Storage (WBS) is where you upload and store your data to an off-site location. This off-site location is usually owned by a third party provider, such as Microsoft OneDrive or Google Cloud.
- The storage provider is responsible keep your data secure and that it is accessible to you when you need it.
- WBS is usually very cost-effective and is easily scalable which can often be a better alternative to storing data locally. For example, in Google's London location the price per GB is $0.023 per month. 100GB of storage would equate to $2.30 per month. This can be infinitely scaled to the your needs and you will only be charged for what you use.
- However, if you don't have a good internet connection your experience with WBS will be poor. Upload and download times will be heavily increased and the service would be tedious to interact with. Users with a good internet connection often have a seamless experience as their files can be uploaded and downloaded within seconds.

What are the impacts of Web Based Storage?

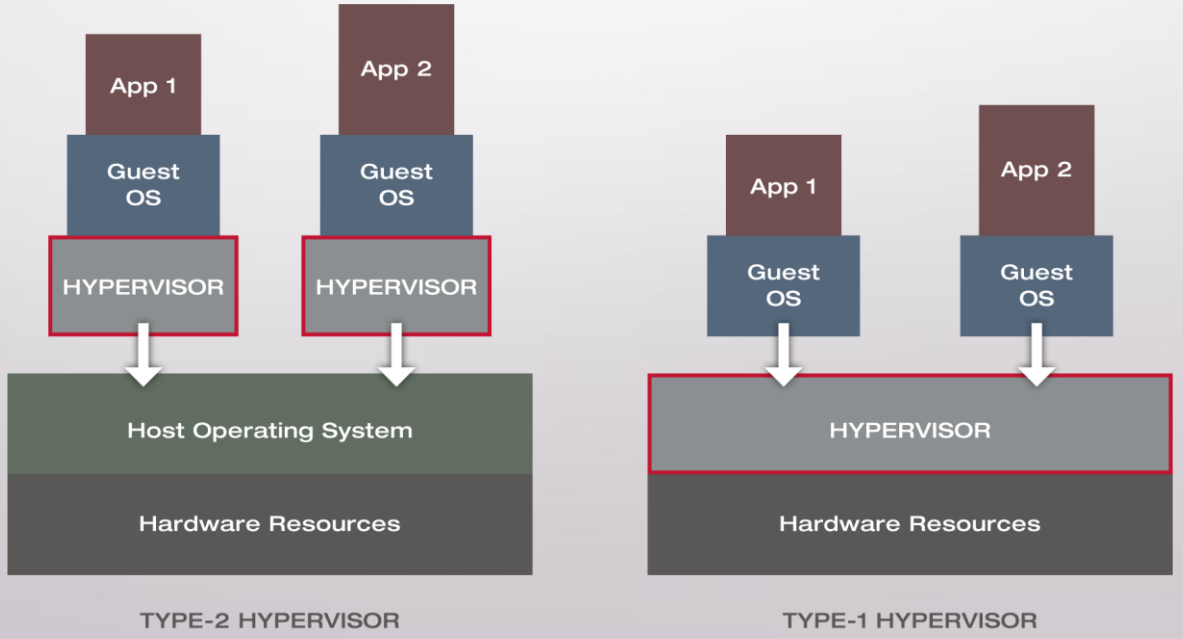
- New Working Practices – Web Based Storage allows for users to access their data anywhere where there is an internet connection. For example, if you worked in an office and needed to work on a document at home, you could upload the document to a WBS provider and then easily edit it from home. This saves users needed to purchase external drives and having to keep them in a safe place. An external drive has a finite amount of storage capacity, whereas WBS can store as much storage as you need.
- Ease of Use – WBS is very easy to use and login to. Usually, all you need to do is sign in and you have immediate access to browse your storage through a web UI. For example, let's look at OneDrive. Once you have signed in, you are presented with a UI that gives you easy access to all your files and files that have been shared with you.
- Online Storage Capacity and Access – with WBS you can have as much storage capacity as you can pay for. All that is needed to access your WBS is an internet connection and your login credentials.
- Enhanced Capability – as WBS is managed by third parties, there is little to no configuration needed by the user, allowing setup to be quick and easy. This makes it very accessible to new users of IT as WBS is intuitive to use.



// Server and Desktop Virtualization

What is Server and Desktop Virtualization?

- Server and Desktop Virtualisation (SDV) is a software-based computer and operating system which functions by splitting the physical resources of a computer so that it can be utilised by the hypervisor (the software that creates and runs the virtual machines). The Hypervisor then uses these resources to emulate a server or desktop environment, running an operating system such as Ubuntu Server or Windows 10.
- Hypervisors offer great flexibility, allowing you to easily allocate the right amount of resources you need for your virtual machine. If you have a CPU heavy application that doesn't need much RAM, you can allocate more CPU cores to the machine and less gigabytes of RAM. If this was the other way around, more RAM and less CPU can be just as easily allocated.



What are the impacts of Server and Desktop Virtualization?

- Impact on the Environment – SDV allows for better power efficiency and is overall better than the environment to have 1 bare-metal server hosting 10 virtual machines than 10 separate servers which may not utilize the full power of its hardware. With virtualizations you can allocate resources to be exactly what the machine needs
- New Working Practices – virtual machines can be used for staff members to access their work PC from home, giving them access to all network features such as storage and their files without needing to issue laptops and setup a VPN connection into your network which could increase security risk.
- Ease of Use – with a modern hypervisor it is easy to allocate resources as needed to existing virtual machine and deploy new machines within minutes. You can also setup pre-configured images which contain an image file with an operating system pre-installed and configured, as well as having its dedicated resources pre-configured. This can then be provisioned within seconds.
- Online Storage Capacity and Access – virtual machines can be accessed remotely or directly from the hypervisor. If virtual machines are configured with network access, they are automatically configured with an IP addresses if a DHCP server is present on the network. This allows for you to use the remote desktop protocol to access the desktop, or you could use secure shell protocol to access the command line if no desktop is present. The storage capacity of a virtual machine can be configured to what it needed, as all data is stored within a file on the host's secondary storage.

// Sources

- https://www.ibm.com/cloud/learn/cloud-storage
- https://cloud.google.com/storage/pricing
- https://www.youtube.com/watch?v=42fwh_1KP_0
- https://www.vmware.com/topics/glossary/content/hypervisor.html
- https://www.citrix.com/solutions/vdi-and-daas/what-is-hypervisor.html