Thomas Robinson

Unit 5, Assignment 1

Network Managers

Solihull College
October 2022

Task One P1

Technologies

Layouts

Topologies

A network's topology describes how it is laid out.

The **physical topology** of a network is how the devices—such as end devices and network devices—are physically placed and connected in the real world. This includes lengths and types of cabling (fibre, copper, etc) and where devices are located (on a desk, mobile, in a rack, etc).
It does not refer to specific protocols used to communicate or detailed information about the devices.

There are many types of physical topologies, each with their own benefits and drawbacks.

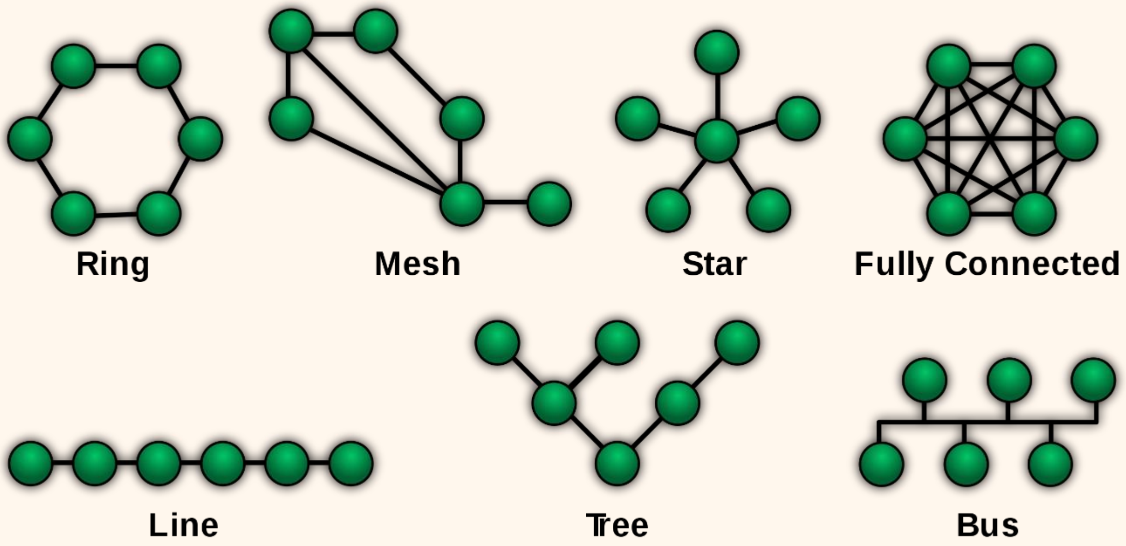


Image: Examples of physical topologies. While older networks made use of a bus or ring topology, modern networks are usually in a star, tree or mesh configuration. *Public Domain by Malyszkz on Wikimedia Commons*

A **logical topology** defines how data actually flows through a network, making use of the physical topology. The logical topology includes details such as which protocols are used to communicate between devices.

Physical Topologies

Ring

In a ring topology, each *node* on the network is connected to two other nodes, forming a continuous loop. Data travels around the ring in one direction, from device-to-device, until it reaches its destination.

Star

A star topology is a network in which each node is connected to a central device, typically a hub or a switch, which acts as a single point of connection for all nodes.

Bus

A bus network consists of a single cable or ‘backbone’ that runs between all the nodes on the network. All data that is sent across the network is broadcasted to all of the nodes on the bus.

Mesh & Partial-Mesh

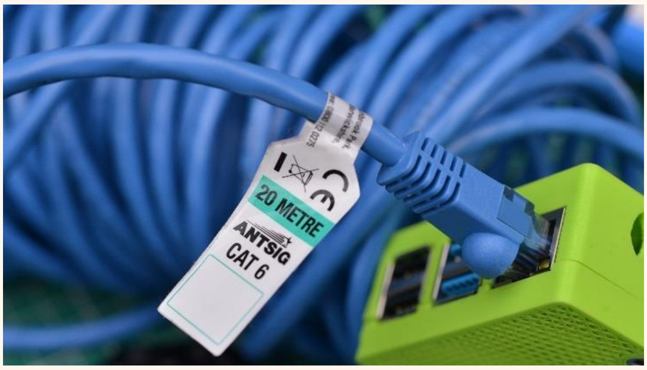
In a mesh network, each node is connected to every other node on the network. This provides redundant paths between nodes and allows for each node to communicate directly with every other node. A partial-mesh network means that not every node is connected to each other.

Connection Media

Connection Media refers to how devices are physically connected to each other at Layer 1 of the TCP/IP Stack/OSI model. This is how the bits (1s and 0s) are physically transmitted from device-to-device.

Copper

Copper cabling sends the bits of information using electrical charges sent along the wire. Without signal repeaters, they are limited by distance when compared to fibre or wireless connections and if improperly shielded they can be susceptible to electrical interference.



Ethernet networks most commonly make use of twisted-pair copper cabling. These can be found connecting computers and other devices within essentially all homes and businesses.

Image: A copper-based Ethernet cable terminated in an RJ-45 connector.
Gavin Allanwood on Unsplash

Fibre Optic

Rather than using electricity, fibre optic cabling sends data using pulses of light along thin tubes made of glass or plastic. These types of cables are more expensive however they can transfer a higher amount of data over significantly longer distances compared to copper cabling.

Fibre optic connections are most often used between high-speed network devices, such as switches and routers, and over long-distances, such as between a home or business and an ISP’s network. The ‘backbone’ of the Internet consists of dozens of undersea fibre optic cables connecting continents.

Image: A selection of fibre optic cables. *Lars Kienle on Unsplash*

Wireless

To connect devices together without using wires, radio frequency technology is used. This is sending radio waves over-the-air from a transmitter to a receiver.

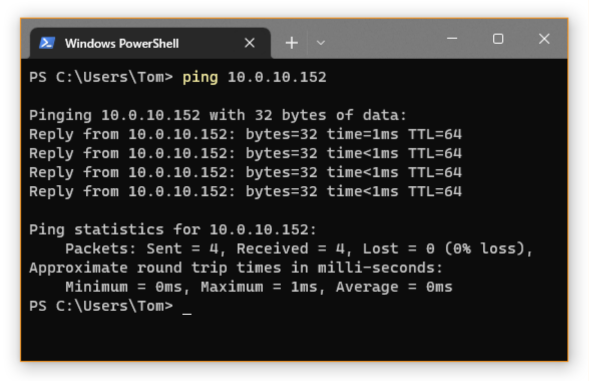
An application of wireless networking technology is Wi-Fi, which is a ubiquitous standard.

Image: A home wireless access point. *Andres Urena on Unsplash*

Protocols

ICMP

Internet Control Message Protocol is a simple protocol which is primarily used by commands such as ping and traceroute to validate a connection between two devices on a network. It is useful for diagnosing issues with network connectivity and latency.

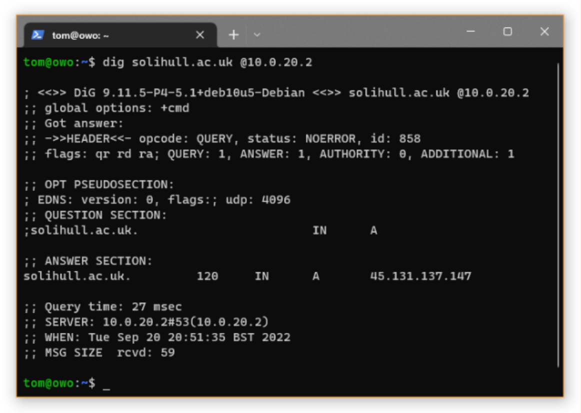


```
PS C:\Users\Tom> ping 10.0.10.152

Pinging 10.0.10.152 with 32 bytes of data:
Reply from 10.0.10.152: bytes=32 time=1ms TTL=64
Reply from 10.0.10.152: bytes=32 time<1ms TTL=64
Reply from 10.0.10.152: bytes=32 time<1ms TTL=64
Reply from 10.0.10.152: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.10.152:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Users\Tom> _
```

Image: The ‘ping’ command in Windows sends ICMP echo-requests to a device and measures the response time of the ICMP echo-reply.

DNS

The **Domain Name System** acts as a computers’ phonebook. A DNS server translates from human-readable hostnames—such as google.co.uk or server01.example.org—into an IP address that a computer can use—like 142.250.178.3. DNS makes use of UDP port 53 on the server-side.



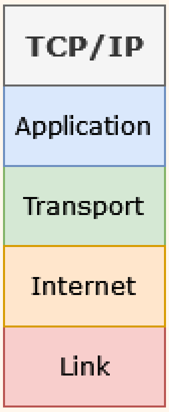
```
tom@owo:~$ dig solihull.ac.uk @10.0.20.2

; <<>> DiG 9.11.5-P4-5.1+deb10u5-Debian <<>> solihull.ac.uk @10.0.20.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 858
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;solihull.ac.uk.                        IN      A

;; ANSWER SECTION:
solihull.ac.uk.         120     IN      A       45.131.137.147

;; Query time: 27 msec
;; SERVER: 10.0.20.2#53(10.0.20.2)
;; WHEN: Tue Sep 20 20:51:35 BST 2022
;; MSG SIZE  rcvd: 59

tom@owo:~$ _
```

Image: The ‘dig’ command in Linux performs a DNS query.

TCP/IP

The **Transmission Control Protocol/Internet Protocol** Stack is a suite of protocols that dictates how data should be split into packets, routed, sent and received across a network. It is the set of protocols used by the Internet.

Image: The four layers of the TCP/IP stack.



TCP/IP
Application
Transport
Internet
Link

SNMP

Simple Network Management Protocol is an application-layer protocol for collecting information about devices such as routers, switches and servers on a network. A management server is able to read (and potentially write) variables exposed by a device.

Network Devices

Host

A **host** is an independent end device on a network which has its own unique address(es). It can be any device—from a server to a smartphone.

Server

A **server** is a computer on the network that provides one or more services. Examples of services provided by a server include HTTPS for web traffic, FTP and SMB for file sharing, DNS and DHCP for network functionality.

While not required, they often consist of specialised pieces of hardware designed for performing a specific purpose. A rackserver is a server that can fit in a standardised networking cabinet—or 'rack.'

Image: A Hewlett Packard Enterpriser tower server. Some features that differentiate it from a consumer computer include eight hot-swappable hard disk drive bays and an IPMI interface for remote management. *HPE*

Switch

A **switch** is used to allow more devices to connect to a network. A Layer 2 switch will 'switch' packets to the correct device by checking the destination MAC address of each incoming frame.

Image: A five-port unmanaged ethernet switch *Netgear*

Router

A **router** is a device used to connect multiple networks together and distribute traffic between them. They route packets based on their destination IP address at Layer 3 of the OSI model.

NIC

A **Network Interface Card** or **Network Interface Controller** refers to a component of a host that allows it to connect to a network. This can be either wired or wireless.

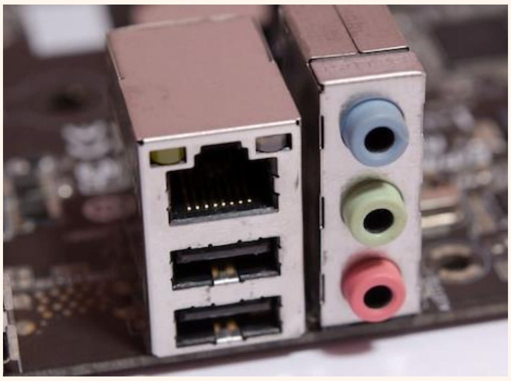


Image: Many modern motherboards include built-in Ethernet NICs. *sunnygb5 on Freepik*

Task Two P2

Tools

ping

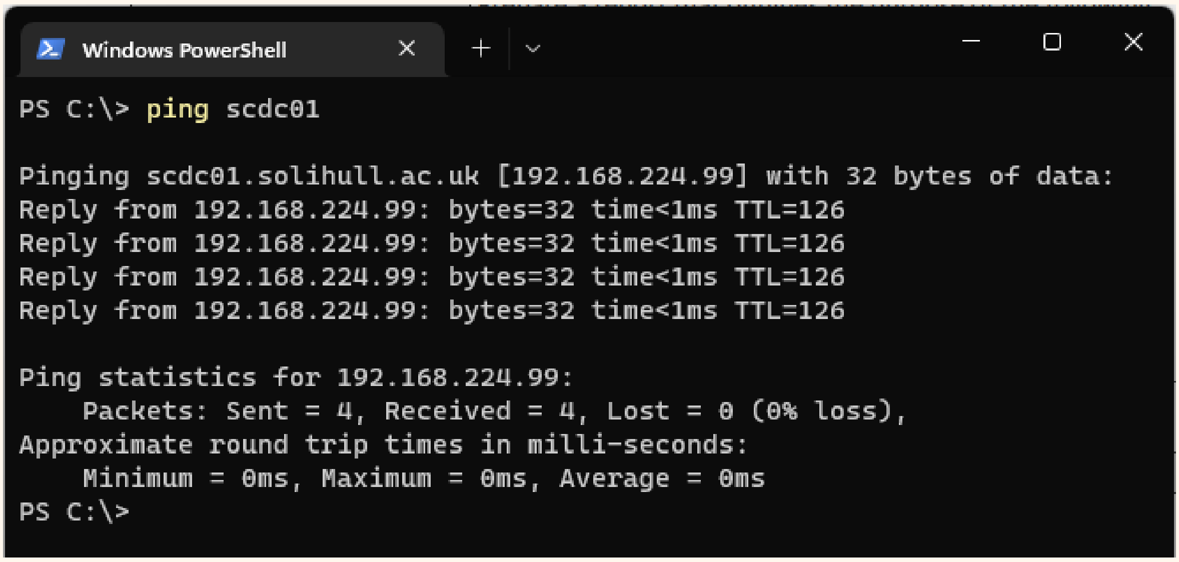
The *ping* command is used to send ICMP Echo requests to other devices to diagnose connectivity and latency issues.

It automatically resolves the IP address if a hostname is given using

DNS and it will also use rDNS to lookup the hostname of an IP address.

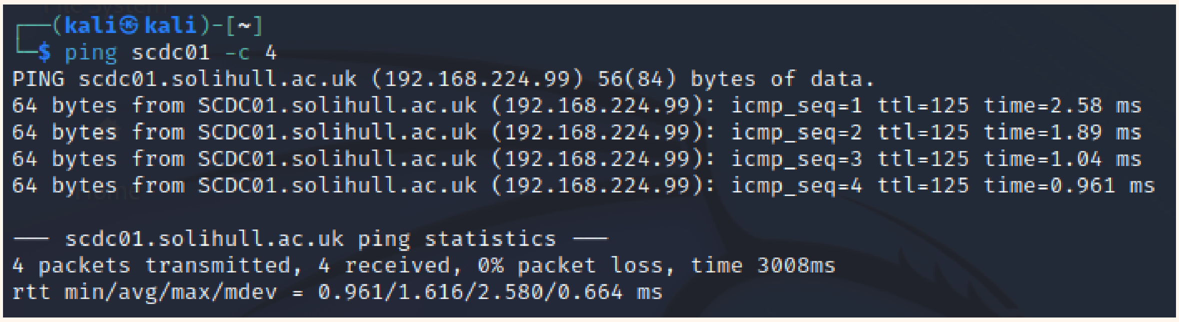
In the below example, we are pinging *192.168.224.99*—the IP address behind the hostname *scdc01.* Since this host is within the local network, the reply time is very short, at under 1ms for every PDU sent/received.

‘Round-Trip’ refers to the time taken to both send the ICMP echo-request and the time taken to receive the echo-reply.



```
PS C:\> ping scdc01

Pinging scdc01.solihull.ac.uk [192.168.224.99] with 32 bytes of data:
Reply from 192.168.224.99: bytes=32 time<1ms TTL=126
Reply from 192.168.224.99: bytes=32 time<1ms TTL=126
Reply from 192.168.224.99: bytes=32 time<1ms TTL=126
Reply from 192.168.224.99: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.224.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\>
```

In other operating systems, the command works much the same:

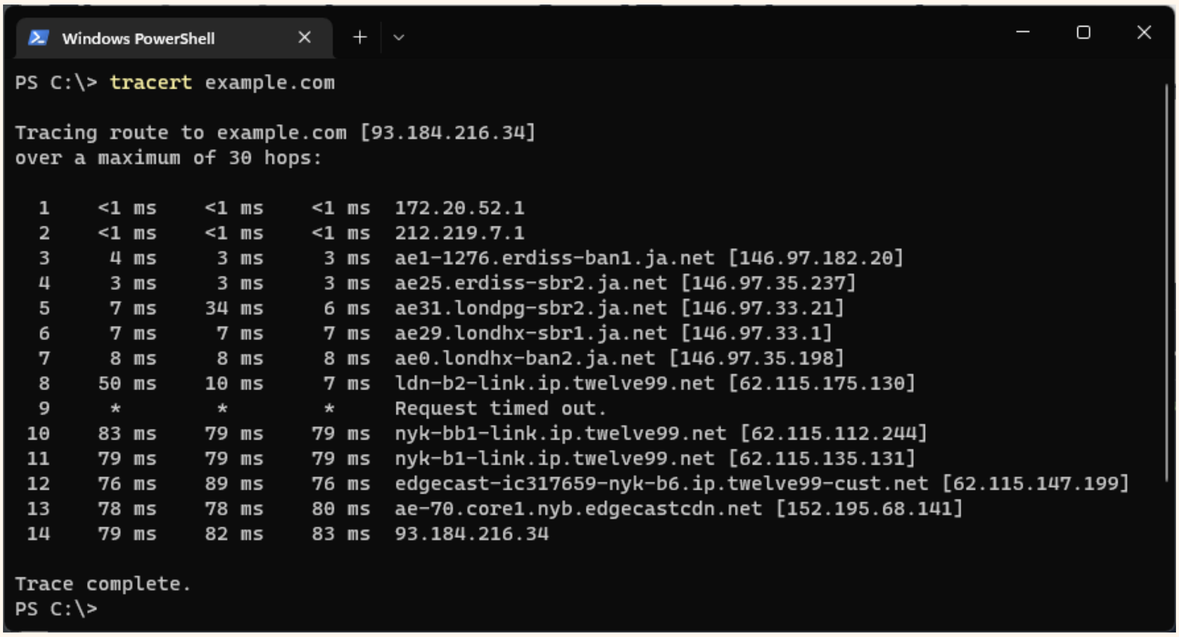


```
┌──(kali㉿kali)-[~]
└─$ ping scdc01 -c 4
PING scdc01.solihull.ac.uk (192.168.224.99) 56(84) bytes of data.
64 bytes from SCDC01.solihull.ac.uk (192.168.224.99): icmp_seq=1 ttl=125 time=2.58 ms
64 bytes from SCDC01.solihull.ac.uk (192.168.224.99): icmp_seq=2 ttl=125 time=1.89 ms
64 bytes from SCDC01.solihull.ac.uk (192.168.224.99): icmp_seq=3 ttl=125 time=1.04 ms
64 bytes from SCDC01.solihull.ac.uk (192.168.224.99): icmp_seq=4 ttl=125 time=0.961 ms

--- scdc01.solihull.ac.uk ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.961/1.616/2.580/0.664 ms
```

tracert & traceroute

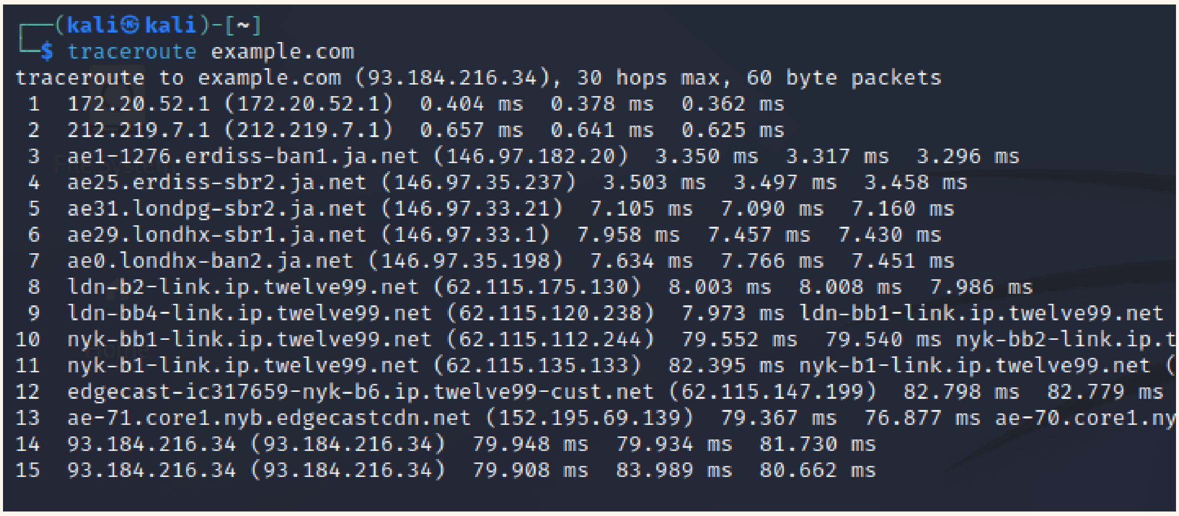
The *tracert* (Windows) or *traceroute* (other OSes) is a command used to investigate the ‘hops’ made to a destination device. It follows the path a packet takes through the routers that make up the Internet. For each hop it issues three ICMP Echo requests to measure the latency and an rDNS query to lookup the hostname.

In the below example, we trace the steps from the local computer at *172.20.52.1* to the IP address resolved for *example.com—93.184.216.34.*



```
PS C:\> tracert example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.20.52.1
  2    <1 ms    <1 ms    <1 ms  212.219.7.1
  3     4 ms     3 ms     3 ms  ae1-1276.erdiss-ban1.ja.net [146.97.182.20]
  4     3 ms     3 ms     3 ms  ae25.erdiss-sbr2.ja.net [146.97.35.237]
  5     7 ms    34 ms     6 ms  ae31.londpg-sbr2.ja.net [146.97.33.21]
  6     7 ms     7 ms     7 ms  ae29.londhx-sbr1.ja.net [146.97.33.1]
  7     8 ms     8 ms     8 ms  ae0.londhx-ban2.ja.net [146.97.35.198]
  8    50 ms    10 ms     7 ms  ldn-b2-link.ip.twelve99.net [62.115.175.130]
  9     *        *        *     Request timed out.
 10    83 ms    79 ms    79 ms  nyk-bb1-link.ip.twelve99.net [62.115.112.244]
 11    79 ms    79 ms    79 ms  nyk-b1-link.ip.twelve99.net [62.115.135.131]
 12    76 ms    89 ms    76 ms  edgecast-ic317659-nyk-b6.ip.twelve99-cust.net [62.115.147.199]
 13    78 ms    78 ms    80 ms  ae-70.core1.nyb.edgecastcdn.net [152.195.68.141]
 14    79 ms    82 ms    83 ms  93.184.216.34

Trace complete.
PS C:\>
```

In other operating systems, the command is *traceroute* and functions in an equivalent way with only minimal differences to the output formatting:



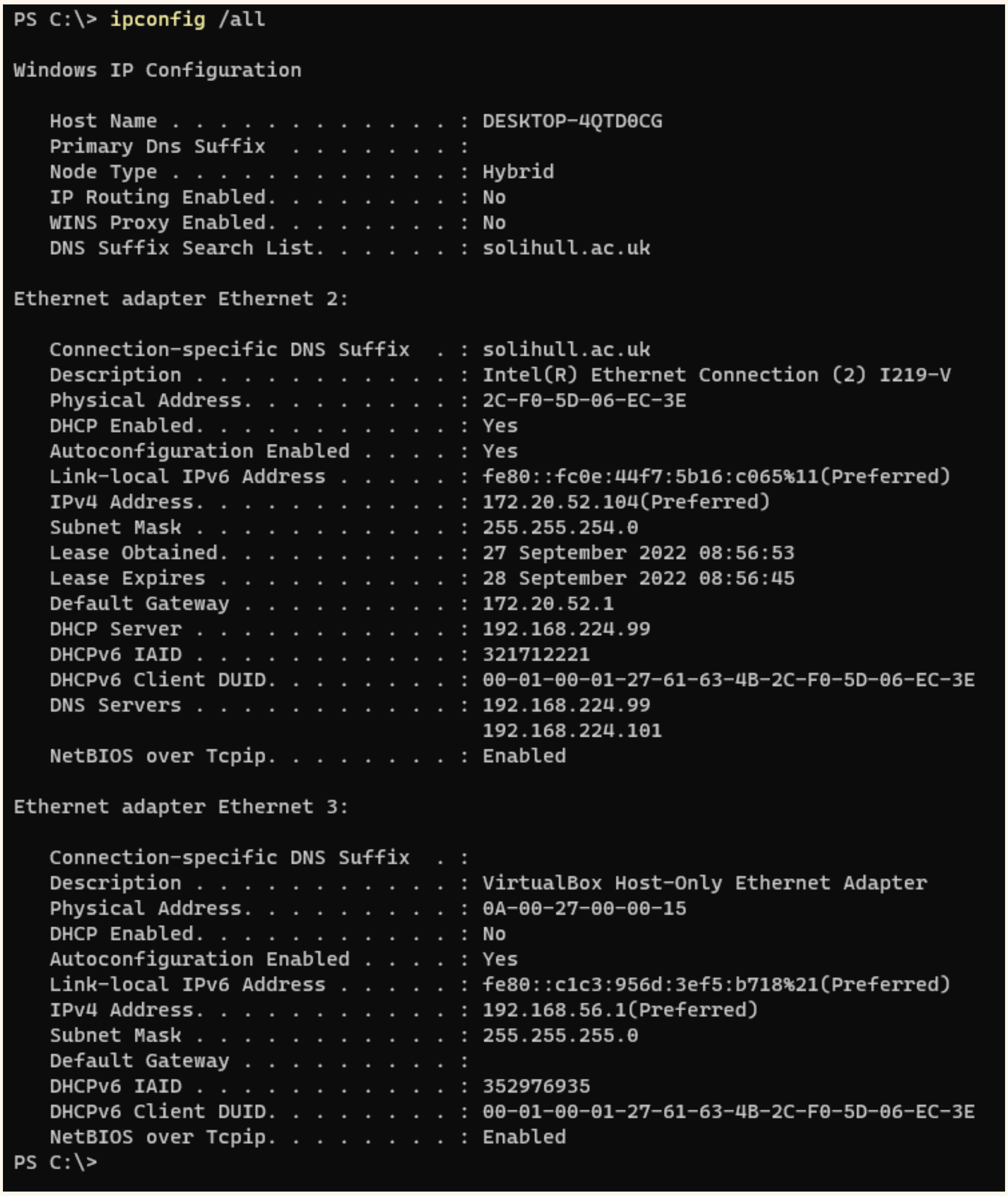
```
┌──(kali㉿kali)-[~]
└─$ traceroute example.com
traceroute to example.com (93.184.216.34), 30 hops max, 60 byte packets
 1  172.20.52.1 (172.20.52.1)  0.404 ms  0.378 ms  0.362 ms
 2  212.219.7.1 (212.219.7.1)  0.657 ms  0.641 ms  0.625 ms
 3  ae1-1276.erdiss-ban1.ja.net (146.97.182.20)  3.350 ms  3.317 ms  3.296 ms
 4  ae25.erdiss-sbr2.ja.net (146.97.35.237)  3.503 ms  3.497 ms  3.458 ms
 5  ae31.londpg-sbr2.ja.net (146.97.33.21)  7.105 ms  7.090 ms  7.160 ms
 6  ae29.londhx-sbr1.ja.net (146.97.33.1)  7.958 ms  7.457 ms  7.430 ms
 7  ae0.londhx-ban2.ja.net (146.97.35.198)  7.634 ms  7.766 ms  7.451 ms
 8  ldn-b2-link.ip.twelve99.net (62.115.175.130)  8.003 ms  8.008 ms  7.986 ms
 9  ldn-bb4-link.ip.twelve99.net (62.115.120.238)  7.973 ms ldn-bb1-link.ip.twelve99.net
10  nyk-bb1-link.ip.twelve99.net (62.115.112.244)  79.552 ms  79.540 ms nyk-bb2-link.ip.t
11  nyk-b1-link.ip.twelve99.net (62.115.135.133)  82.395 ms nyk-b1-link.ip.twelve99.net (
12  edgecast-ic317659-nyk-b6.ip.twelve99-cust.net (62.115.147.199)  82.798 ms  82.779 ms
13  ae-71.core1.nyb.edgecastcdn.net (152.195.69.139)  79.367 ms  76.877 ms ae-70.core1.ny
14  93.184.216.34 (93.184.216.34)  79.948 ms  79.934 ms  81.730 ms
15  93.184.216.34 (93.184.216.34)  79.908 ms  83.989 ms  80.662 ms
```

ipconfig & ifconfig

ipconfig (Windows) and *ifconfig* (other OSes) are commands used to view and modify information about the network adapters in a system.

ipconfig (Windows)

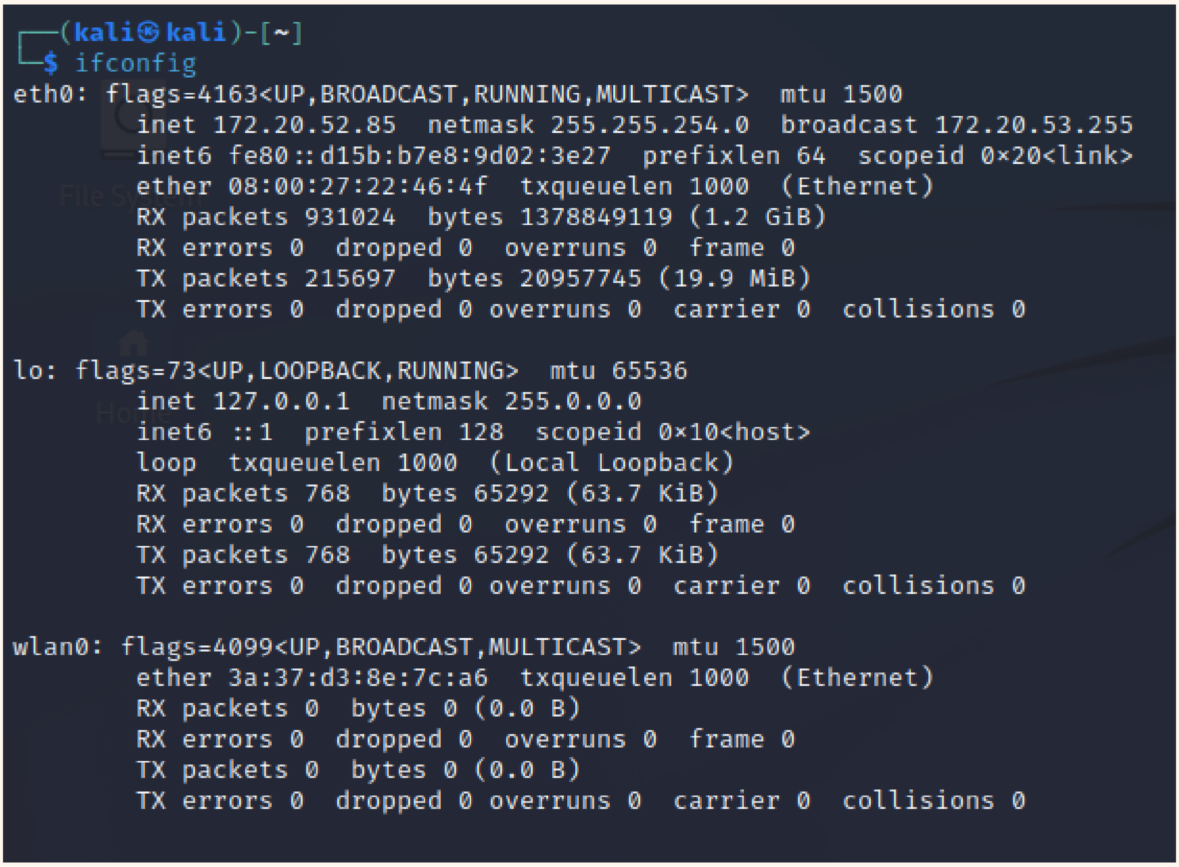
In Windows, a user or technician can use ipconfig to display and modify information about the network adapters on the device. This includes ethernet, Bluetooth, Wi-Fi and others.
There are various *flags* (command arguments) that can be provided to the ipconfig command. *renew* and *renew6* are used to request new DHCP IP addresses for IPv4 and IPv6 respectively, and *release* and *release6* are used to release assigned IP addresses. *flushdns* clears the Windows DNS cache and *all* reveals more detailed information about all the adapters.



```
PS C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-4QTD0CG
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : solihull.ac.uk

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : solihull.ac.uk
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-V
   Physical Address. . . . . . . . . : 2C-F0-5D-06-EC-3E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fc0e:44f7:5b16:c065%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.52.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : 27 September 2022 08:56:53
   Lease Expires . . . . . . . . . . : 28 September 2022 08:56:45
   Default Gateway . . . . . . . . . : 172.20.52.1
   DHCP Server . . . . . . . . . . . : 192.168.224.99
   DHCPv6 IAID . . . . . . . . . . . : 321712221
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-61-63-4B-2C-F0-5D-06-EC-3E
   DNS Servers . . . . . . . . . . . : 192.168.224.99
                                       192.168.224.101
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-15
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c1c3:956d:3ef5:b718%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 352976935
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-61-63-4B-2C-F0-5D-06-EC-3E
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\>
```

ifconfig (Linux)

On many Linux distributions, the ifconfig command available and is like its Windows counterpart. Unlike the Windows command however, it is able to set arbitrary IP address and other information for each of the network adapters. It can also be used for enabling and disabling interfaces.

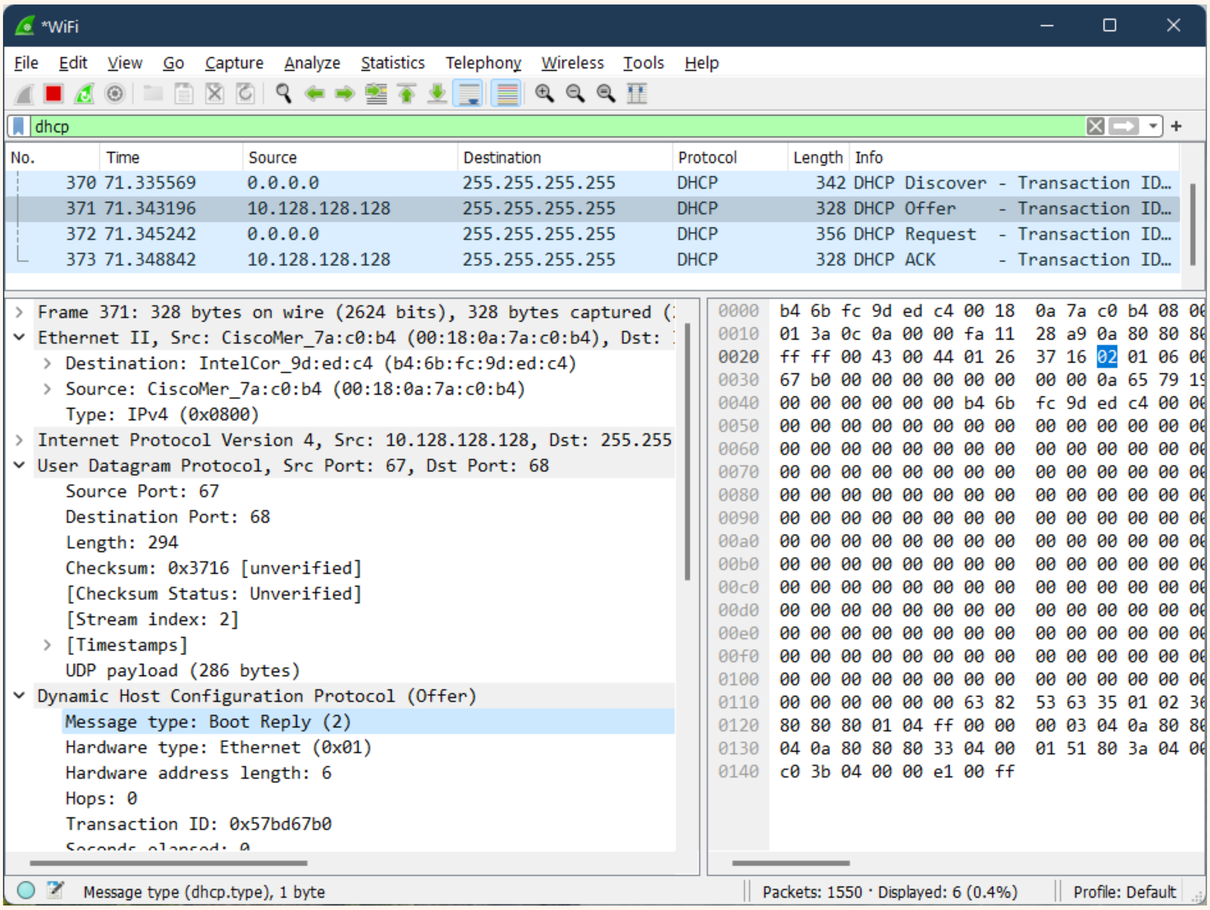


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.52.85  netmask 255.255.254.0  broadcast 172.20.53.255
        inet6 fe80::d15b:b7e8:9d02:3e27  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:22:46:4f  txqueuelen 1000  (Ethernet)
        RX packets 931024  bytes 1378849119 (1.2 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 215697  bytes 20957745 (19.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 768  bytes 65292 (63.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 768  bytes 65292 (63.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 3a:37:d3:8e:7c:a6  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Wireshark

Wireshark is an open-source packet analysis tool that provides a graphical user interface for inspecting captured network traffic.

The program is able to display, sort and filter packets as well as exposing the protocol-level information contained within them.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

```
No.   Time       Source           Destination       Protocol  Length Info
  370 71.335569  0.0.0.0          255.255.255.255   DHCP         342 DHCP Discover - Transaction ID…
  371 71.343196  10.128.128.128   255.255.255.255   DHCP         328 DHCP Offer    - Transaction ID…
  372 71.345242  0.0.0.0          255.255.255.255   DHCP         356 DHCP Request  - Transaction ID…
  373 71.348842  10.128.128.128   255.255.255.255   DHCP         328 DHCP ACK      - Transaction ID…
```

```
> Frame 371: 328 bytes on wire (2624 bits), 328 bytes captured (
v Ethernet II, Src: CiscoMer_7a:c0:b4 (00:18:0a:7a:c0:b4), Dst:
    > Destination: IntelCor_9d:ed:c4 (b4:6b:fc:9d:ed:c4)
    > Source: CiscoMer_7a:c0:b4 (00:18:0a:7a:c0:b4)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.128.128.128, Dst: 255.255
v User Datagram Protocol, Src Port: 67, Dst Port: 68
      Source Port: 67
      Destination Port: 68
      Length: 294
      Checksum: 0x3716 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 2]
    > [Timestamps]
      UDP payload (286 bytes)
v Dynamic Host Configuration Protocol (Offer)
      Message type: Boot Reply (2)
      Hardware type: Ethernet (0x01)
      Hardware address length: 6
      Hops: 0
      Transaction ID: 0x57bd67b0
      Seconds elapsed: 0
```

```
0000  b4 6b fc 9d ed c4 00 18  0a 7a c0 b4 08 00
0010  01 3a 0c 0a 00 00 fa 11  28 a9 0a 80 80 80
0020  ff ff 00 43 00 44 01 26  37 16 02 01 06 00
0030  67 b0 00 00 00 00 00 00  00 00 0a 65 79 19
0040  00 00 00 00 00 00 b4 6b  fc 9d ed c4 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 36
0120  80 80 80 01 04 ff 00 00  00 03 04 0a 80 80
0130  04 0a 80 80 80 33 04 00  01 51 80 3a 04 00
0140  c0 3b 04 00 00 e1 00 ff
```

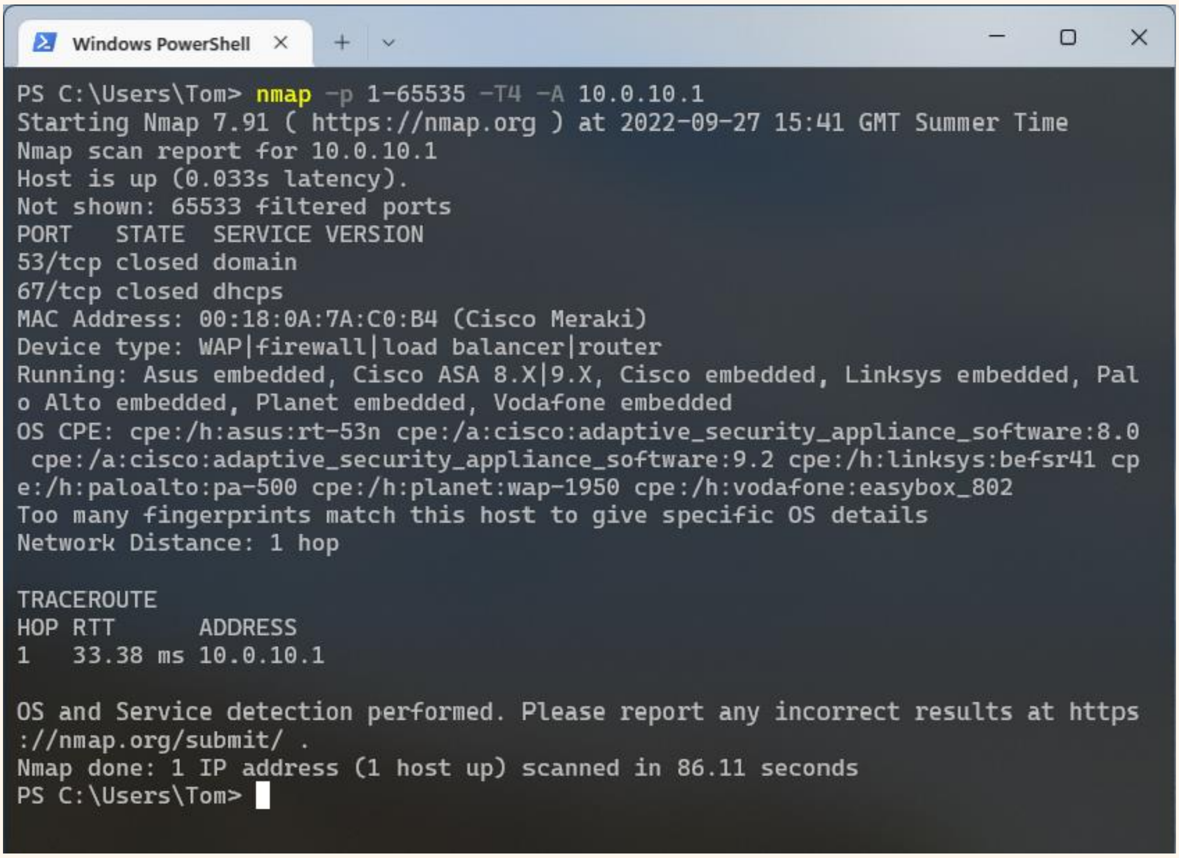
Message type (dhcp.type), 1 byte | Packets: 1550 · Displayed: 6 (0.4%) | Profile: Default

Using Wireshark to inspect a captured DHCP Offer packet. The packet list filtered to only display DHCP-related entries. The top pane contains a list of captured packets, the lower left pane contains information about the selected packet and the lower right pane shows the raw packet data.

The lower left pane is grouped by layers: in this screenshot, the first and second groups correspond to Layer 2 and show information about the frame and the devices’ MAC addresses; the third group shows Layer 3 IP information, including source and destination IP addresses; the fourth shows the Layer 4 protocol information including TCP/UDP ports; and the final group shows Application data.

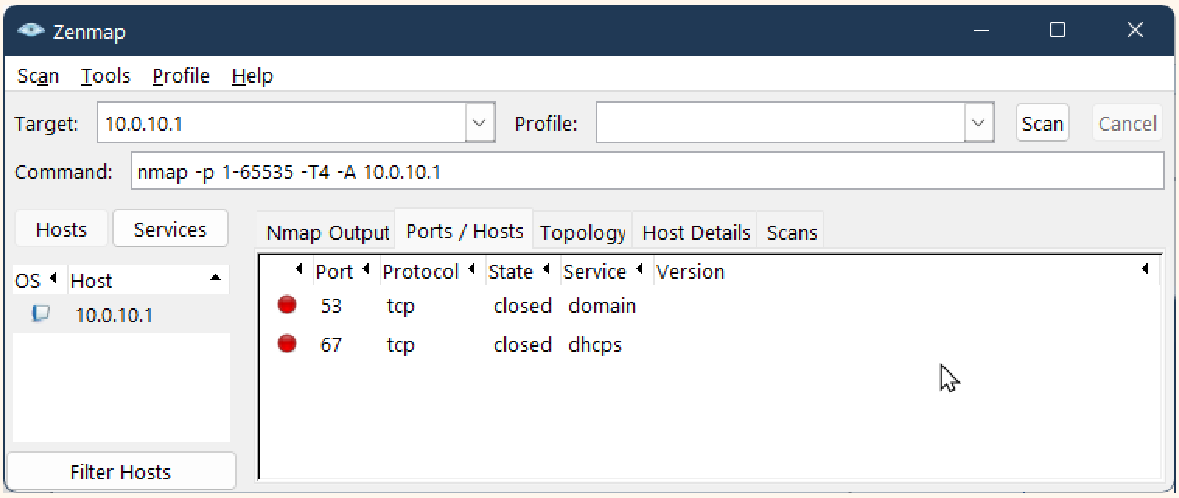
Nmap

Nmap is a command-line tool used to probe hosts on a network for open ports and other information, such as operating system version and vendor. It can discover running services and applications that could potentially contain exploitable vulnerabilities or security issues.



```
PS C:\Users\Tom> nmap -p 1-65535 -T4 -A 10.0.10.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-27 15:41 GMT Summer Time
Nmap scan report for 10.0.10.1
Host is up (0.033s latency).
Not shown: 65533 filtered ports
PORT   STATE  SERVICE VERSION
53/tcp closed domain
67/tcp closed dhcps
MAC Address: 00:18:0A:7A:C0:B4 (Cisco Meraki)
Device type: WAP|firewall|load balancer|router
Running: Asus embedded, Cisco ASA 8.X|9.X, Cisco embedded, Linksys embedded, Pal
o Alto embedded, Planet embedded, Vodafone embedded
OS CPE: cpe:/h:asus:rt-53n cpe:/a:cisco:adaptive_security_appliance_software:8.0
 cpe:/a:cisco:adaptive_security_appliance_software:9.2 cpe:/h:linksys:befsr41 cp
e:/h:paloalto:pa-500 cpe:/h:planet:wap-1950 cpe:/h:vodafone:easybox_802
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   33.38 ms 10.0.10.1

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.11 seconds
PS C:\Users\Tom>
```

A screenshot of the Nmap command's output after being ran. It has scanned all 65535 TCP ports on the host 10.0.10.1 and found two closed services. Below is the same command having been ran in **zenmap**, the official GUI for the Nmap tool.



Target: 10.0.10.1
Profile:
Command: nmap -p 1-65535 -T4 -A 10.0.10.1

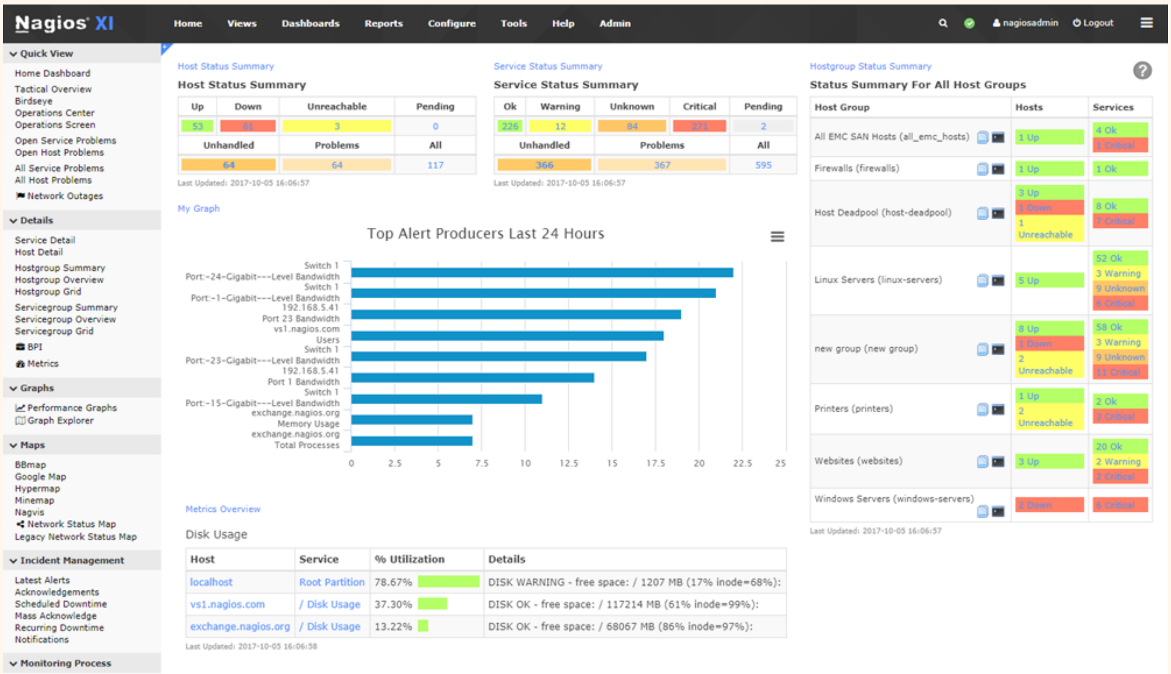
OS	Host
	10.0.10.1

	Port	Protocol	State	Service	Version
●	53	tcp	closed	domain	
●	67	tcp	closed	dhcps	

Zabbix & Nagios XI

Zabbix and Nagios XI are both network monitoring suites that are able to monitor hosts using an agent (application installed on each host) or by using protocols such as SNMP. They are used to monitor downtime and other incidents to maintain the health of a network and its devices.

Zabbix is free open-source software while Nagios XI is paid.



Host Status Summary

Up	Down	Unreachable	Pending
53	61	3	0

Unhandled	Problems	All
64	64	117

Last Updated: 2017-10-05 16:06:57

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
226	12	84	271	2

Unhandled	Problems	All
366	367	595

Last Updated: 2017-10-05 16:06:57

Status Summary For All Host Groups

Host Group	Hosts	Services
All EMC SAN Hosts (all_emc_hosts)	1 Up	4 Ok 1 Critical
Firewalls (firewalls)	1 Up	1 Ok
Host Deadpool (host-deadpool)	3 Up 1 Down 1 Unreachable	8 Ok 7 Critical
Linux Servers (linux-servers)	5 Up	52 Ok 3 Warning 9 Unknown 6 Critical
new group (new group)	8 Up 1 Down 2 Unreachable	58 Ok 3 Warning 9 Unknown 11 Critical
Printers (printers)	1 Up 2 Unreachable	2 Ok 3 Critical
Websites (websites)	3 Up	20 Ok 2 Warning 2 Critical
Windows Servers (windows-servers)	2 Down	6 Critical

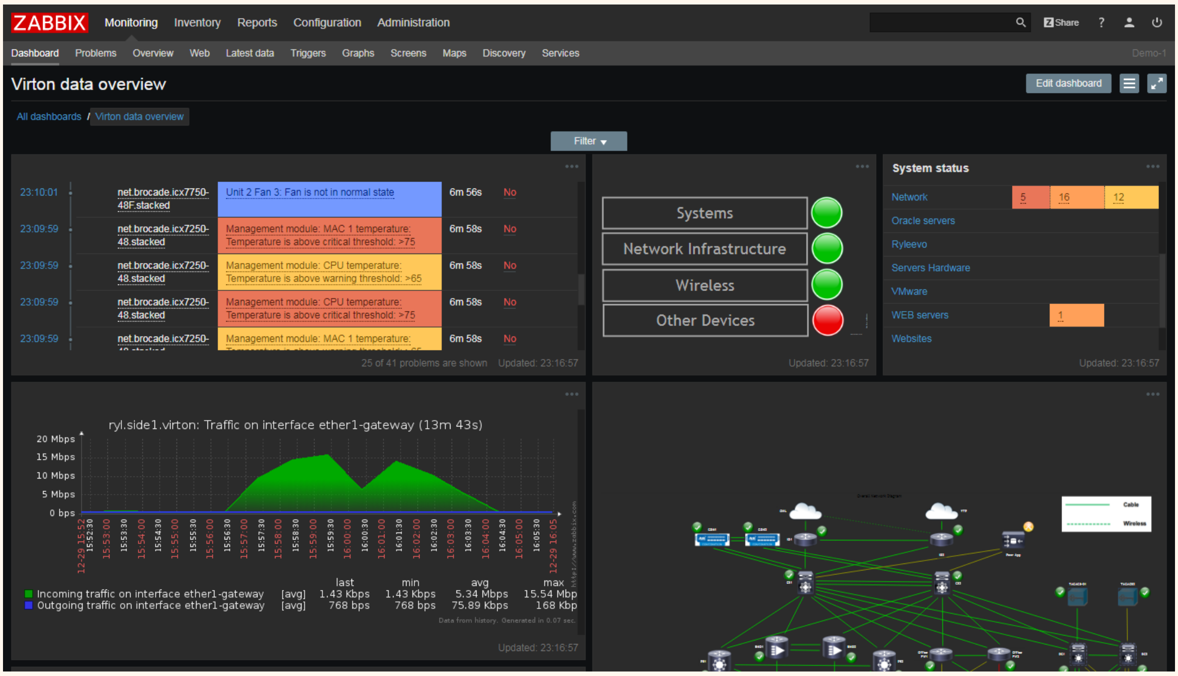
Last Updated: 2017-10-05 16:06:57

Disk Usage

Host	Service	% Utilization	Details
localhost	Root Partition	78.67%	DISK WARNING - free space: / 1207 MB (17% inode=68%):
vs1.nagios.com	/ Disk Usage	37.30%	DISK OK - free space: / 117214 MB (61% inode=99%):
exchange.nagios.org	/ Disk Usage	13.22%	DISK OK - free space: / 68067 MB (86% inode=97%):

Last Updated: 2017-10-05 16:06:58

Above: A screenshot of the Nagios XI web interface. *Nagios.com*
Below: A screenshot of the Zabbix web interface. *Zabbix.com*



Virton data overview

All dashboards / Virton data overview

23:10:01	net.brocade.icx7750-48F.stacked	Unit 2 Fan 3: Fan is not in normal state	6m 56s	No
23:09:59	net.brocade.icx7250-48.stacked	Management module: MAC 1 temperature: Temperature is above critical threshold: >75	6m 58s	No
23:09:59	net.brocade.icx7250-48.stacked	Management module: CPU temperature: Temperature is above warning threshold: >65	6m 58s	No
23:09:59	net.brocade.icx7250-48.stacked	Management module: CPU temperature: Temperature is above critical threshold: >75	6m 58s	No
23:09:59	net.brocade.icx7250-	Management module: MAC 1 temperature:	6m 58s	No

25 of 41 problems are shown Updated: 23:16:57

Updated: 23:16:57

System status

Network	5	16	12
Oracle servers			
Ryleevo			
Servers Hardware			
VMware			
WEB servers		1	
Websites			

Updated: 23:16:57

ryl.side1.virton: Traffic on interface ether1-gateway (13m 43s)

		last	min	avg	max
🟩 Incoming traffic on interface ether1-gateway	[avg]	1.43 Kbps	1.43 Kbps	5.34 Mbps	15.54 Mbp
🟦 Outgoing traffic on interface ether1-gateway	[avg]	768 bps	768 bps	75.89 Kbps	168 Kbp

Data from history. Generated in 0.07 sec.

Updated: 23:16:57

Task Four, Part One P4, M2

Functions & Fault Management

Fault Management

Fault management is the process of identifying, diagnosing and correcting faults within a network. Faults can include network outages, performance degradation, configuration errors and security breaches.

Fault management typically begins with identifying potential faults through monitoring and analysis. Once a fault is detected, it is then diagnosed to determine the root cause. Once the initial cause is identified, corrective action can be taken to fix the problem and prevent it from happening again in the future.

Device Configuration

Device Configuration is the process of setting up devices on a network so that they can communicate with each other. This includes configuring IP addresses, subnet masks, gateway addresses, and other network settings.

This can help with fault management by ensuring that all devices are properly configured and have the same, correct settings. Automated device configuration means that every device does not need to be set up individually and new settings and information can be pushed to each device as needed.

Account Management

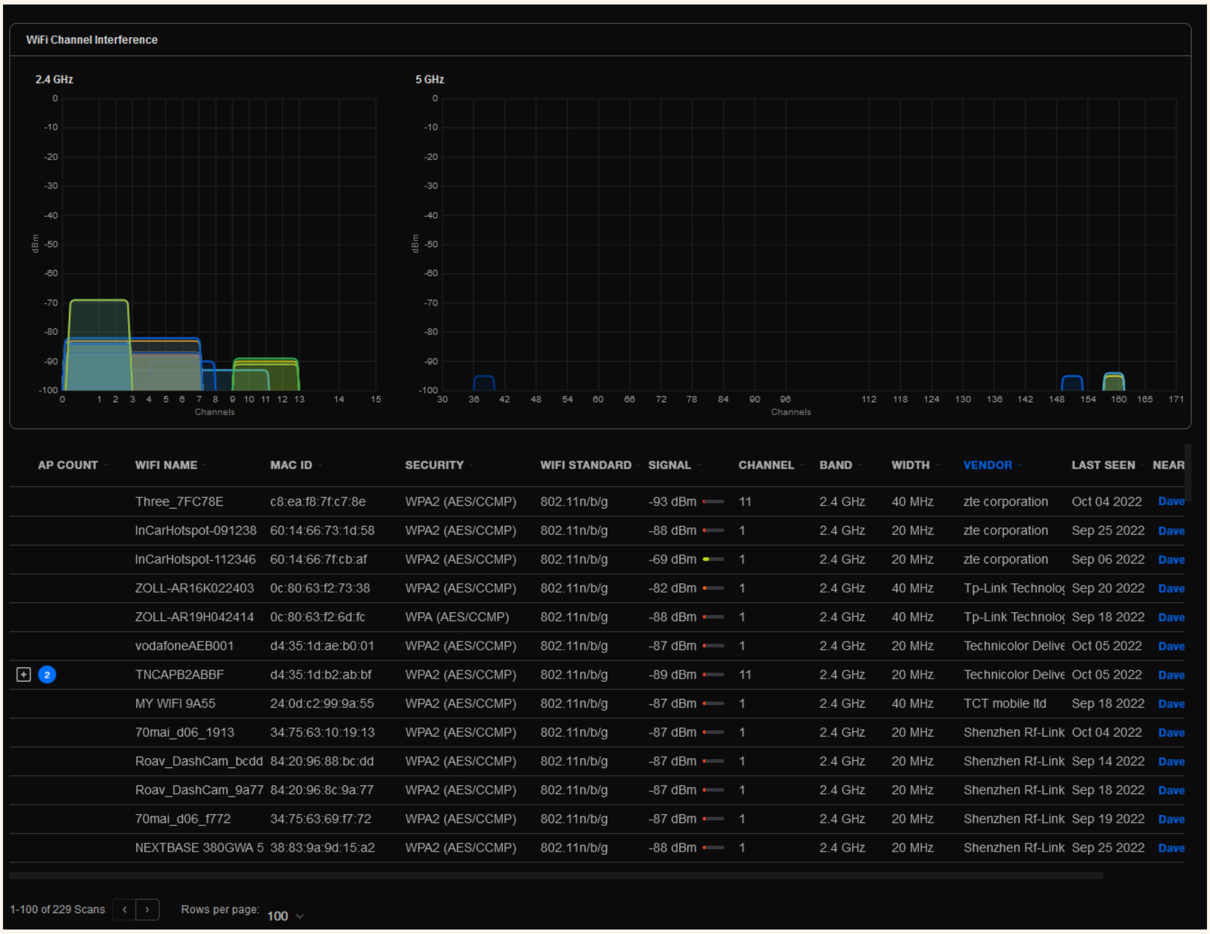
Account Management refers to maintaining user accounts within a network. This can include creating new accounts, modifying existing accounts, and deleting accounts as needed.

A central account management system can help with fault management by providing a central location for managing user accounts. This can help to identify and resolve problems with user accounts more quickly.

Network Performance Variables & Traffic

Network performance variables can help with fault management by providing data that can be used to identify and diagnose network problems. This data can include information on network traffic, bandwidth usage, and latency.

By monitoring these variables, network administrators can quickly identify and resolve issues that may be affecting network performance. This information can also be used to determine where bottlenecks are occurring, what type of traffic is causing problems, and what changes need to be made to the network to improve performance.



AP COUNT	WIFI NAME	MAC ID	SECURITY	WIFI STANDARD	SIGNAL	CHANNEL	BAND	WIDTH	VENDOR	LAST SEEN	NEAR
	Three_7FC78E	c8:ea:f8:7f:c7:8e	WPA2 (AES/CCMP)	802.11n/b/g	-93 dBm	11	2.4 GHz	40 MHz	zte corporation	Oct 04 2022	Dave
	InCarHotspot-091238	60:14:66:73:1d:58	WPA2 (AES/CCMP)	802.11n/b/g	-88 dBm	1	2.4 GHz	20 MHz	zte corporation	Sep 25 2022	Dave
	InCarHotspot-112346	60:14:66:7f:cb:af	WPA2 (AES/CCMP)	802.11n/b/g	-69 dBm	1	2.4 GHz	20 MHz	zte corporation	Sep 06 2022	Dave
	ZOLL-AR16K022403	0c:80:63:f2:73:38	WPA2 (AES/CCMP)	802.11n/b/g	-82 dBm	1	2.4 GHz	40 MHz	Tp-Link Technolo	Sep 20 2022	Dave
	ZOLL-AR19H042414	0c:80:63:f2:6d:fc	WPA (AES/CCMP)	802.11n/b/g	-88 dBm	1	2.4 GHz	40 MHz	Tp-Link Technolo	Sep 18 2022	Dave
	vodafoneAEB001	d4:35:1d:ae:b0:01	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	20 MHz	Technicolor Delive	Oct 05 2022	Dave
⊞ 2	TNCAPB2ABBF	d4:35:1d:b2:ab:bf	WPA2 (AES/CCMP)	802.11n/b/g	-89 dBm	11	2.4 GHz	20 MHz	Technicolor Delive	Oct 05 2022	Dave
	MY WIFI 9A55	24:0d:c2:99:9a:55	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	40 MHz	TCT mobile ltd	Sep 18 2022	Dave
	70mai_d06_1913	34:75:63:10:19:13	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	20 MHz	Shenzhen Rf-Link	Oct 04 2022	Dave
	Roav_DashCam_bcdd	84:20:96:88:bc:dd	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	20 MHz	Shenzhen Rf-Link	Sep 14 2022	Dave
	Roav_DashCam_9a77	84:20:96:8c:9a:77	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	20 MHz	Shenzhen Rf-Link	Sep 18 2022	Dave
	70mai_d06_f772	34:75:63:69:f7:72	WPA2 (AES/CCMP)	802.11n/b/g	-87 dBm	1	2.4 GHz	20 MHz	Shenzhen Rf-Link	Sep 19 2022	Dave
	NEXTBASE 380GWA 5	38:83:9a:9d:15:a2	WPA2 (AES/CCMP)	802.11n/b/g	-88 dBm	1	2.4 GHz	20 MHz	Shenzhen Rf-Link	Sep 25 2022	Dave

1-100 of 229 Scans ‹ › Rows per page: 100

Image: Local Wi-Fi networks are an example of a variable that can impact performance. Continuous scans can inform a network administrator on the least congested channels to use for wireless access points. *Own Screenshot*

Security

Network security is the practice of securing a computer network from unauthorised access by both third parties and internally. There are many methods of implementing network security, such as firewalls and associated rules to stop illegitimate traffic, and Intrusion Detection Systems to discover and deal with unusual traffic. Data encryption can ensure security while at rest and in transit since it prevents unauthorised parties from reading potentially sensitive information.

There are many ways that network security can help with fault management. For example, it can help to identify the source of an attack so that it can be more easily stopped. It can also help to identify any damage caused by an attacker and any data that may have been compromised.

Reporting & Documentation

Documenting a network is the process of writing descriptions of operating procedures, configuration, and layout. This is useful since it allows the easy transfer of knowledge about the network between technicians as well as serving as a central source of knowledge.

This can be useful in fault management since if previous incidents are reported and documented along with the steps taken to mitigate the problem, if it then occurs in future, it is known what to do. In this way, they can also serve as a learning resource to demonstrate things that may happen.

Being able to provide reports on-demand with information pertinent to the business can enable those outside of IT to understand changes within the organisation. This can include information such as network performance, most-used services, user growth/loss and any issues that may arise.

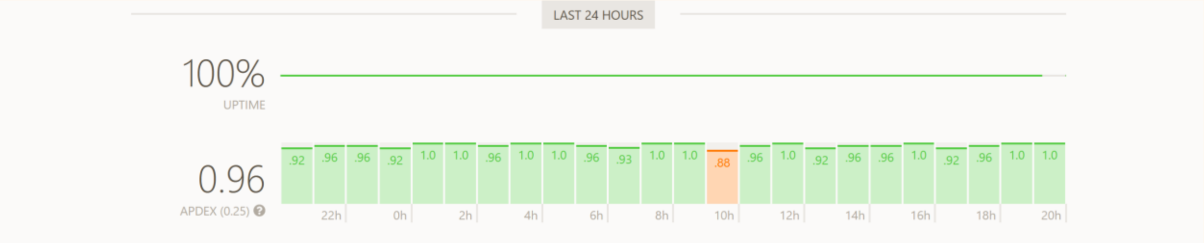
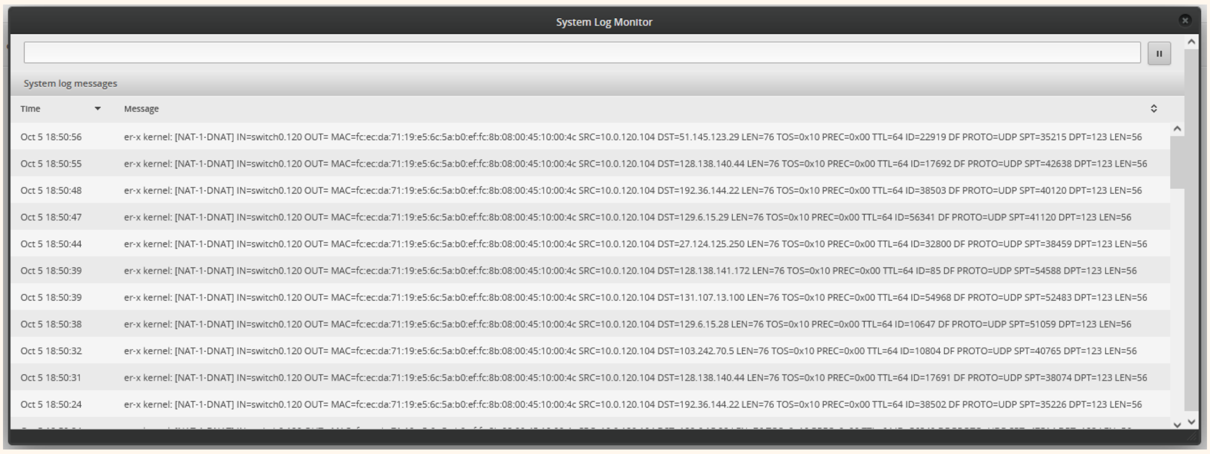


Image: Automated monitoring of websites and systems can alert a network manager to downtime and other issues and this information may be useful for performance/satisfaction reporting *Own Screenshot*

Data Logging

Data logging is the process of recording information about the activity of a network and the traffic flowing through it. Happenings can be logged at both network devices and end devices. Tools like Graylog, Datadog and Splunk can capture logs using protocols such as SNMP as well as analysing a variety of log file formats used by different vendors and programs.

This information can be used to help identify and diagnose problems with the network and the devices on it. This can include connection issues, incorrect permissions, and misconfigured or compromised devices.



```
Time            Message
Oct 5 18:50:56  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=51.145.123.29 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=22919 DF PROTO=UDP SPT=35215 DPT=123 LEN=56
Oct 5 18:50:55  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=128.138.140.44 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=17692 DF PROTO=UDP SPT=42638 DPT=123 LEN=56
Oct 5 18:50:48  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=192.36.144.22 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=38503 DF PROTO=UDP SPT=40120 DPT=123 LEN=56
Oct 5 18:50:47  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=129.6.15.29 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=56341 DF PROTO=UDP SPT=41120 DPT=123 LEN=56
Oct 5 18:50:44  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=27.124.125.250 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=32800 DF PROTO=UDP SPT=38459 DPT=123 LEN=56
Oct 5 18:50:39  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=128.138.141.172 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=85 DF PROTO=UDP SPT=54588 DPT=123 LEN=56
Oct 5 18:50:39  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=131.107.13.100 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=54968 DF PROTO=UDP SPT=52483 DPT=123 LEN=56
Oct 5 18:50:38  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=129.6.15.28 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=10647 DF PROTO=UDP SPT=51059 DPT=123 LEN=56
Oct 5 18:50:32  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=103.242.70.5 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=10804 DF PROTO=UDP SPT=40765 DPT=123 LEN=56
Oct 5 18:50:31  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=128.138.140.44 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=17691 DF PROTO=UDP SPT=38074 DPT=123 LEN=56
Oct 5 18:50:24  er-x kernel: [NAT-1-DNAT] IN=switch0.120 OUT= MAC=fc:ec:da:71:19:e5:6c:5a:b0:ef:fc:8b:08:00:45:10:00:4c SRC=10.0.120.104 DST=192.36.144.22 LEN=76 TOS=0x10 PREC=0x00 TTL=64 ID=38502 DF PROTO=UDP SPT=35226 DPT=123 LEN=56
```

Image: Inspecting the logs of a router, in this case ensuring that a NAT rule is configured correctly *Own Screenshot*

Task Four, Part Two D1

Routine Performance Management

Backups

Backups are an invaluable asset to a network manager’s routine management activities.

Loss of data can happen in a multitude of ways, from targeted ransomware affecting every system to an accidental deletion of a file. Unexpected hardware failure is also an inevitability within most organisations. Properly configured, frequent backups of important data and system images can be used to quickly restore an organisations operation to normal.

Backups can also safeguard against errors in configuration that could cause problems. If this were to happen—for example, a mistyped command--an administrator could simply roll back the device or the settings to a previous version using a recent backup. This effectively provides an ‘undo’ function where one might not otherwise be available and can minimise a devices’ downtime since it does not need to be reconfigured from scratch.

Ideally, backups should be taken as often as data is changed. It is common for businesses to take regular, daily onsite backups and then upload data to an offsite provider on a less regular basis. This shields the organisation from major physical disasters should one occur.

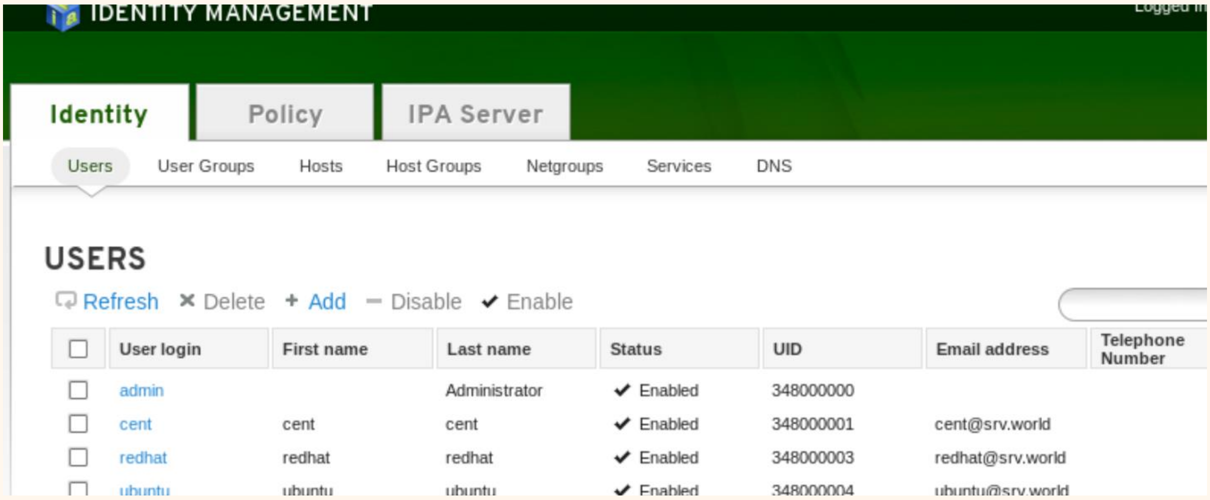
User Account Management

Regular management of user accounts can include activities such as checking permissions and analysing activity.

During a check, an administrator may wish to enumerate through accounts with elevated access and determine whether this privilege is still required. This can ensure that only people who require certain permissions are the ones to hold them, which can help ensure data confidentiality and increase security.

The culling of accounts that are no longer required—for example those of people no longer with the organisation or accounts used for demonstrations or testing—makes sure that the database of users is not excessively long. As above, this can also contribute towards data security since those who do not need access will not be provided it.

While checking user accounts, it may also be possible to check an account's recent activity. This can prove instrumental in discovering compromised accounts which could be being used to access information or otherwise compromise the network. Details such as login locations and failed login attempts can be used here.



□	User login	First name	Last name	Status	UID	Email address	Telephone Number
□	admin		Administrator	✓ Enabled	348000000		
□	cent	cent	cent	✓ Enabled	348000001	cent@srv.world	
□	redhat	redhat	redhat	✓ Enabled	348000003	redhat@srv.world	
□	ubuntu	ubuntu	ubuntu	✓ Enabled	348000004	ubuntu@srv.world	

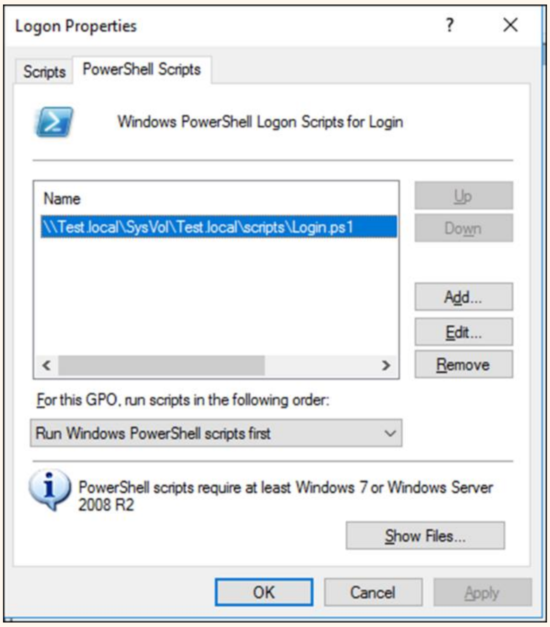
Image: Manging users within the web interface of FreeIPA, a free open-source directory/identity management server. *server-world.info*

Login Scripts

Login scripts are files and programs that are ran every time a user logs into a computer.

Such scripts could be used to run an antivirus scan on login to check the system or perform a search for missing drivers. They could also be used to apply themes and settings that are not configurable using other tools such as Group Policy. Per-user scripts can be used to apply different configurations to different users and user groups.

More pertinent to a network, a VPN connection could be automatically established to protect the incoming and outgoing data on unsecured external networks as well as providing access to internal company resources no matter where the device physically is.



Windows PowerShell Logon Scripts for Login

Name
\\Test.local\SysVol\Test.local\scripts\Login.ps1

For this GPO, run scripts in the following order:
Run Windows PowerShell scripts first

PowerShell scripts require at least Windows 7 or Windows Server 2008 R2

Image: Adding a script to run when a user logs in on Windows Server.
ntweekly.com

Malware Scans

Malware scans are the process of checking for viruses and other malicious software that may be present on a device. Different types of malware behave differently, for example a generic virus might turn the computer into a botnet participating in a DDOS attack or mine cryptocurrency. A more targeted piece of malware may aim to obtain copies of sensitive files or perform a phishing/social-engineering attack on a privileged individual.

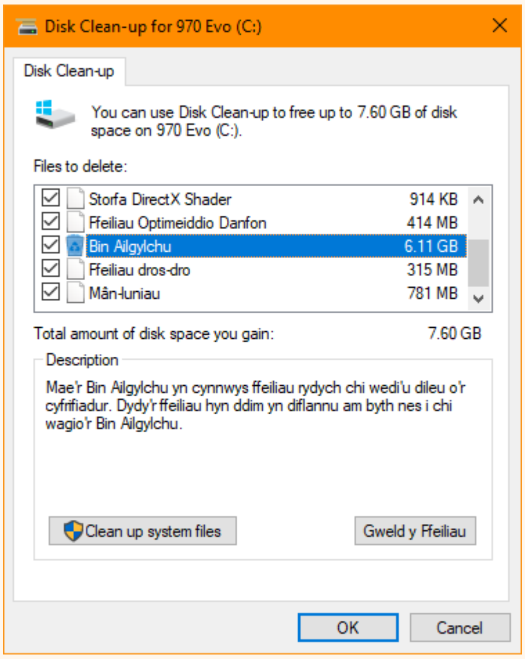
A frequent, through scan for malware on each host provides some assurance that there is no threat to the network posed by a device. Windows Defender, Bitdefender and Malwarebytes are examples of tools available.

File Clean-Up

Regular file-clean ups can help to save money, maintain good habits and continued efficient computer use.

Common bad habits, such as storing files in the recycle bin or deleted items folders, can be quickly broken with a scheduled file clean-up operation. If the recycle bin is emptied daily, for example, users will learn not to store files there.

Substantial amounts of temporary files, such as old Windows versions, log files and outdated lock files can hinder the performance of a system. This is particularly apparent on HDD-based systems. The frequent removal of these files, as well as other unneeded files, like those in the downloads folder, can help to increase the performance of a system.



Disk Clean-up for 970 Evo (C:)

Disk Clean-up

You can use Disk Clean-up to free up to 7.60 GB of disk space on 970 Evo (C:).

Files to delete:

☑ Storfa DirectX Shader	914 KB
☑ Ffeiliau Optimeiddio Danfon	414 MB
☑ Bin Ailgylchu	6.11 GB
☑ Ffeiliau dros-dro	315 MB
☑ Mân-luniau	781 MB

Total amount of disk space you gain: 7.60 GB

Description

Mae'r Bin Ailgylchu yn cynnwys ffeiliau rydych chi wedi'u dileu o'r cyfrifiadur. Dydy'r ffeiliau hyn ddim yn diflannu am byth nes i chi wagio'r Bin Ailgylchu.

Image: Using Windows Disk Clean-up to free up space. 7.6GB total are able to be freed, with 6.11GB being files in the Recycle Bin. *Own Screenshot*

Emerging Network Technologies

Unit 5, Assignment 1, Task 3 P3, M1

January 23

Thomas Robinson—Solihull College

Web-Based Apps

P3

What are Web-Based Apps?

- Run in a web browser rather than as a dedicated program within an OS. This means they are ‘sandboxed’ from the rest of the system by the browser which can offer higher security.
- Written in Web Languages
  - Backend Server (PHP, .NET, NodeJS, Go)
  - Frontend Client (HTML, CSS, JavaScript & Frameworks, WebGL)
- Usually able to be accessed in any modern browser
  - Google Chrome (and other Chromium-derived browsers)
  - Mozilla Firefox
  - Safari
- Often offer cloud syncing across devices
  - Can pick up where you left off on any device

Web-Based App Example:

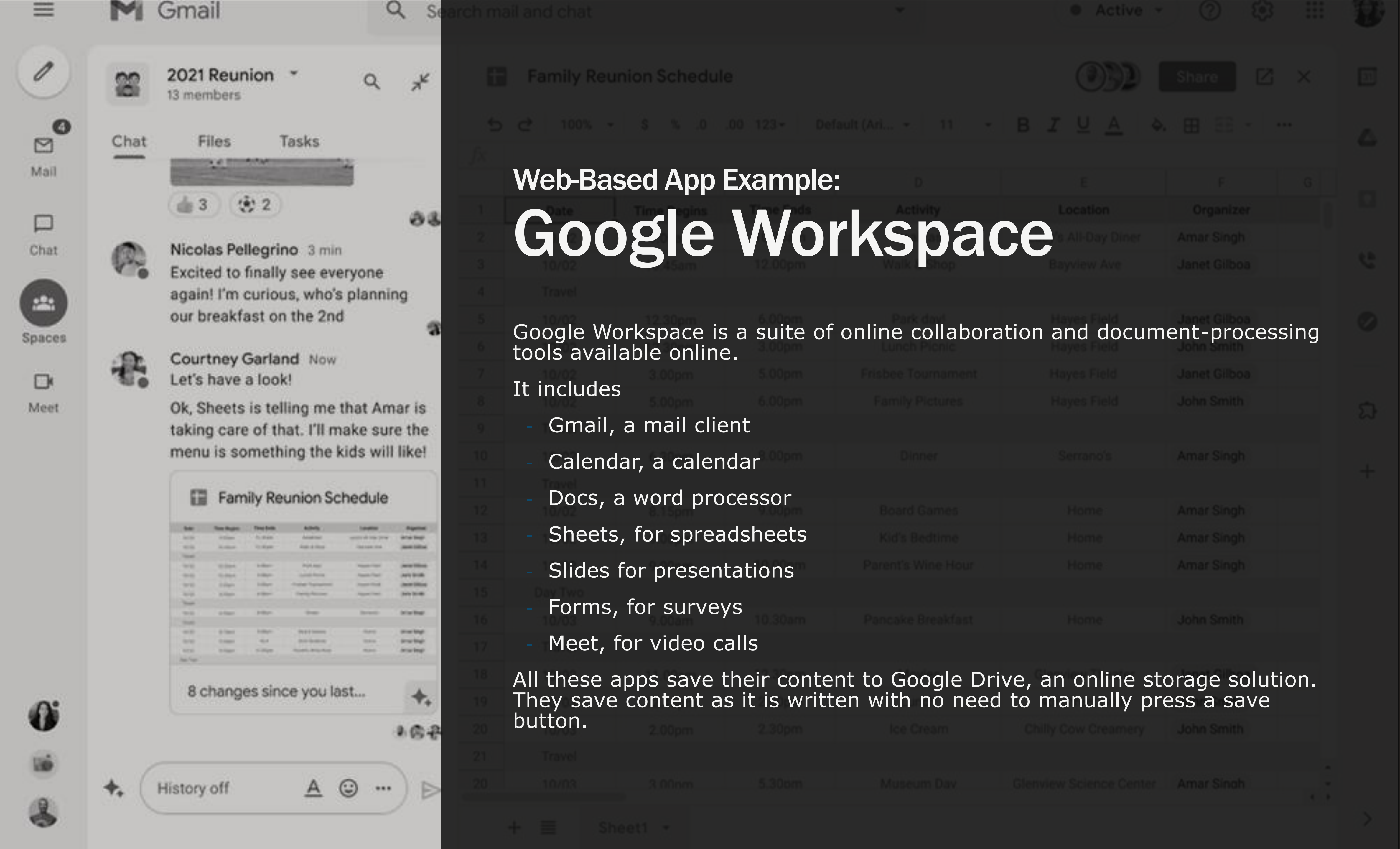
Google Workspace

Google Workspace is a suite of online collaboration and document-processing tools available online.

It includes

- Gmail, a mail client
- Calendar, a calendar
- Docs, a word processor
- Sheets, for spreadsheets
- Slides for presentations
- Forms, for surveys
- Meet, for video calls

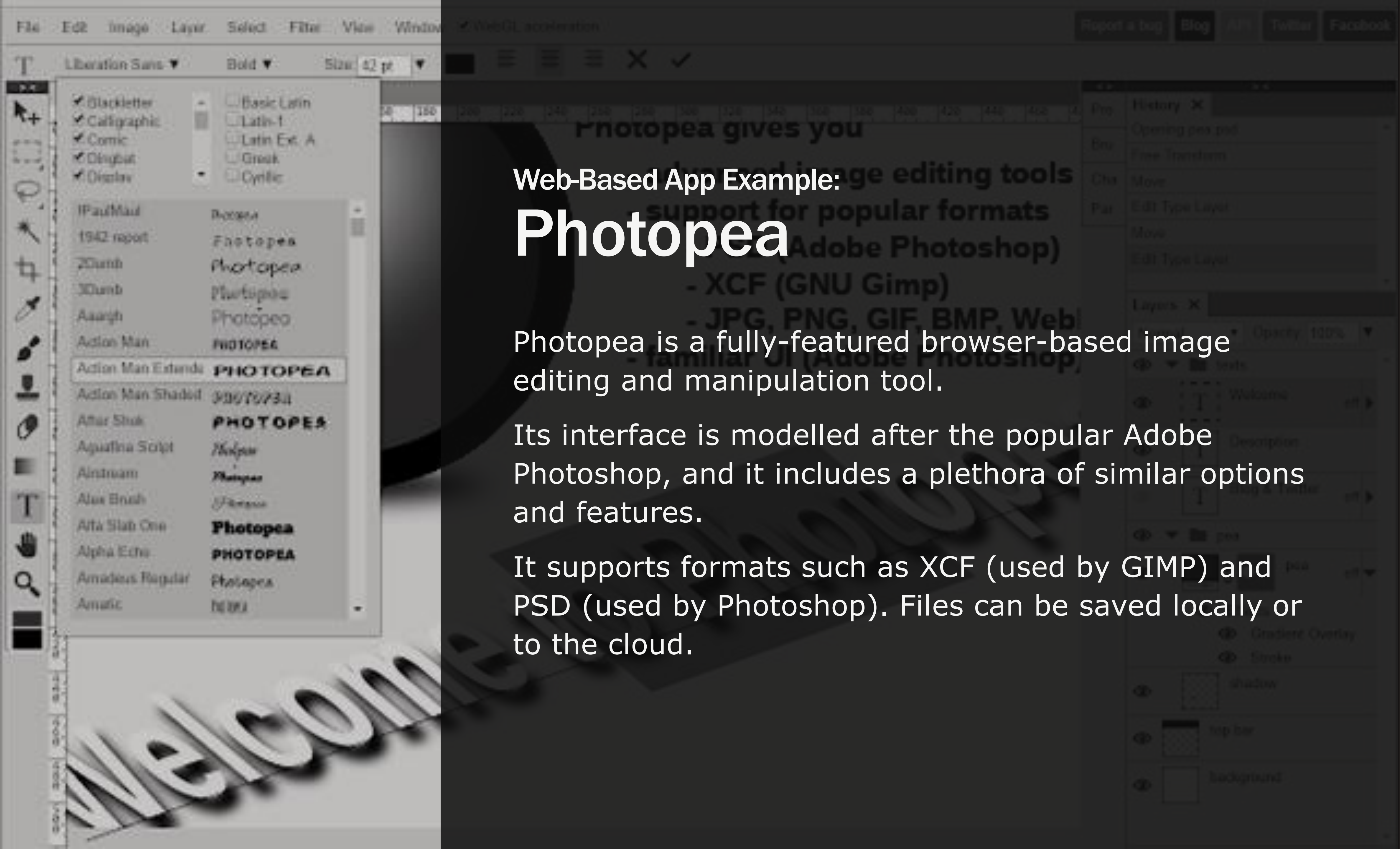
All these apps save their content to Google Drive, an online storage solution. They save content as it is written with no need to manually press a save button.



Nicolas Pellegrino 3 min
Excited to finally see everyone again! I'm curious, who's planning our breakfast on the 2nd

Courtney Garland Now
Let's have a look!
Ok, Sheets is telling me that Amar is taking care of that. I'll make sure the menu is something the kids will like!

Family Reunion Schedule
8 changes since you last...



Web-Based App Example:

Photopea

Photopea is a fully-featured browser-based image editing and manipulation tool.

Its interface is modelled after the popular Adobe Photoshop, and it includes a plethora of similar options and features.

It supports formats such as XCF (used by GIMP) and PSD (used by Photoshop). Files can be saved locally or to the cloud.

Benefits of Web-Based Apps

Available on any device with a browser, anywhere

Same user experience across platforms and operating systems

Cloud saving means no local file management required with backups and replication often handled for you

Strong collaboration features bundled with many online-first tools

Programs do not take up additional space on a local device so can be ran on systems with little storage

Limitations of Web-Based Apps

Browser apps are unable to access the full power of a hosts' hardware and are sandboxed within the browser and its limitations

Web-based apps often contain less features than desktop alternatives due to the difficulty of creating feature-rich webpages

Often only available with an internet connection, limited offline functionality

Privacy issues from work being saved externally

Security issues from lack of encryption & security

What if the service ceases to exist? Do you trust the company to still be around in future?
Google has sunset 199 services and 54 apps since its inception

Web-Based Storage

P3

What is Web-Based Storage?

- Web-Based storage is the practice of storing data on a remote server on the Internet (in ‘The Cloud’) rather than on a local computer or within an organisation’s network.
- Examples of cloud-based storage providers:
  - Microsoft OneDrive, SharePoint
  - Google Drive
  - Apple iCloud Drive
  - Dropbox
  - Box
  - Mega

Benefits of Web-Based Storage

Available anywhere with an internet connection

Near-infinite scalability: petabytes of storage available on-demand as-needed

No need purchase hardware (servers, disk drives) that may not ever be fully utilised

Many providers offer extensive file version history for data security

No need to worry about logistics of file servers, backing up or configuring – frees up resources for IT teams

Downsides of Web-Based Storage

Files are rendered inaccessible without an internet connection

Storage costs are often pricier than buying the equivalent hardware

Access speed is limited by network bandwidth – will not be as fast as storage on the LAN or in the local computer.

Data is held by an external company: Will they still exist in the future? What if I need to move providers?

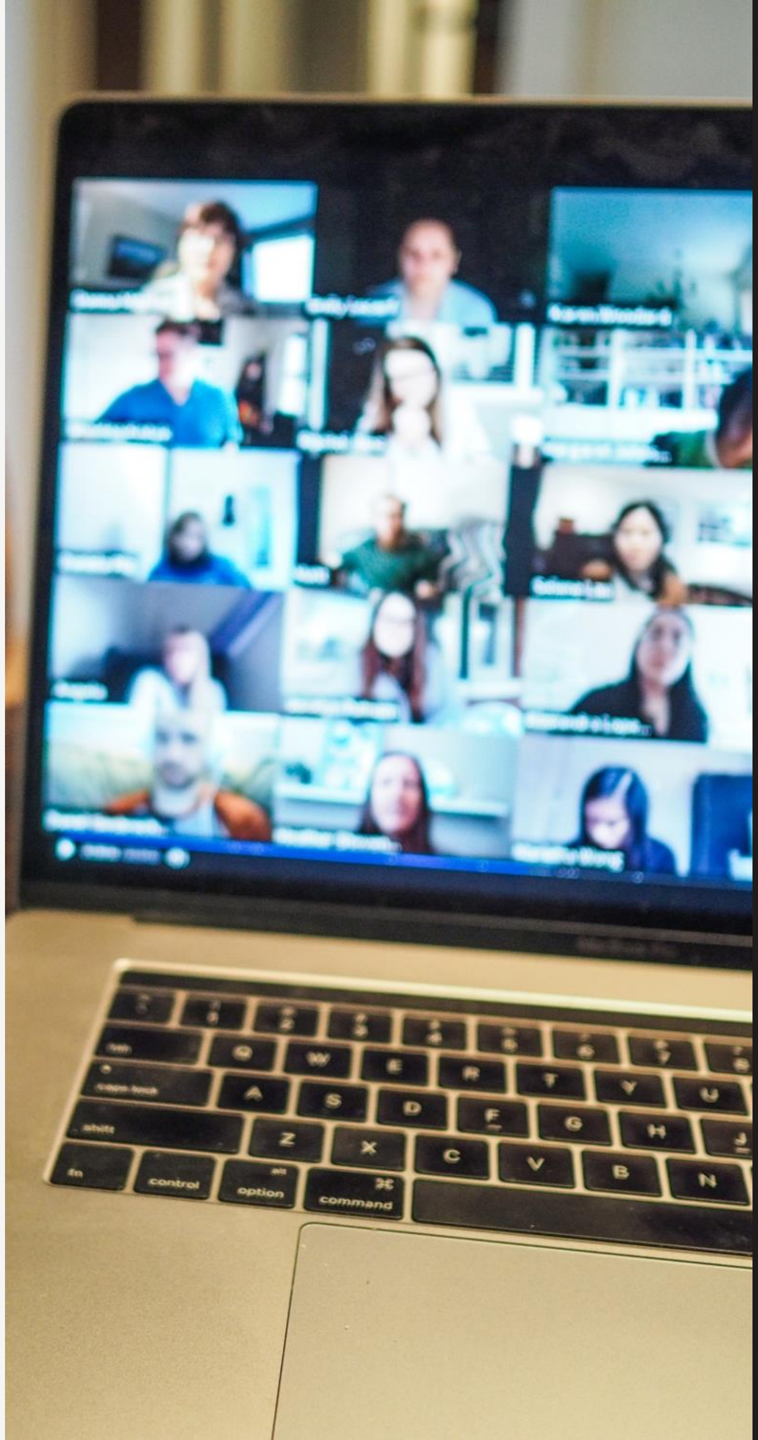
The Impact of Moving to The Web

M1

Enhanced Capabilities

- Web-apps allow a dynamic work environment with many different types of devices.

  Since they run in web browsers, there is no need to limit an organisation to a single type or vendor of desktop or laptop.
- Web-storage allows significantly greater storage capacities with a significantly less configuration and setup required.
- Both web-based storage and web-based applications foster collaboration and sharing with other users
- An organisation no longer needs to dedicate as many hours to the task of managing storage and tasks such as backups/file integrity checking. This means more time can be spent on other tasks to further the organisation.



Mobile Working & Working From Home

- Since web-based apps and web-based storage allow files and tools to be accessed from anywhere with an internet connection, they are an excellent companion to the newfound trends of mobile working and working from home
- There is no need to install additional programs to access data and files from any location since most everyone uses a web-browser
- Cloud-based hardware and software can accelerate the growth of a remote company while also reducing the resources required to dedicate to IT at the price of higher ongoing costs and trusting in external companies to provide quality services

Ease of Use

- Many users are already familiar with using a web browser and many web-apps are a simplified version of their desktop counterparts
  - Microsoft Office Online is an example of a simplified desktop app that has been translated into a web-based app
  - While simplification may increase ease-of-use, some important features may be missing
- Cloud storage solutions offer much faster AI-powered search functions that are unavailable on desktop operating systems which can make finding files and content significantly easier
- Web-apps are often able to integrate with other services and tools to increase productivity and features
- Instructing users to make use of web-applications and web-storage may prove a challenge to those used to desktop equivalents.

Resources Used

- What is a Web Application? (stackpath.com)
- Google Workspace (workspace.google.com)
- Introduction (photopea.com)
- Google Graveyard - Killed by Google (killedbygoogle.com)
- What is Cloud Storage | IBM (ibm.com)
- What is Cloud Storage? | AWS (aws.amazon.com)
- Cloud computing pros and cons: The good, the bad, and the gray areas (zdnet.com)