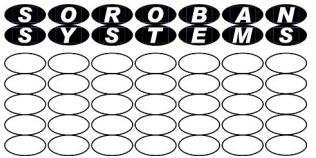


How the Internet works

John Steele

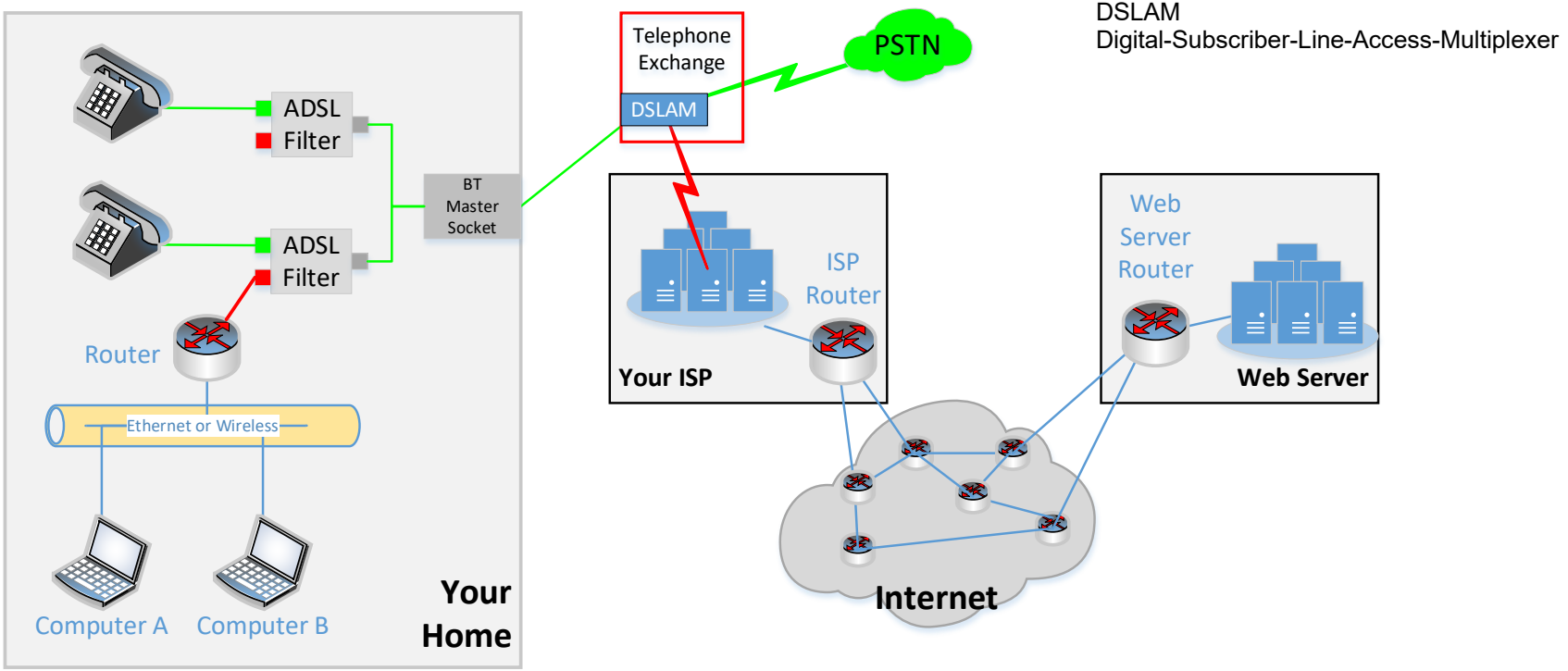
Overview of talk

- Introduction to some important terminology
  - Internet Web sites uses names e.g. www.gxcc.org.uk what does this mean
- What is an IP address and how does it relate to the web site address also known as a Domain
  - What are subnets and why they are important
  - We are running out of IP addresses – how has this been addressed
- Introduction to “protocols” and some of the important ones
  - Layers - what is IP and what is TCP
- The services that are provided by your own router
- How does it all fit together to serve you a web page
- Additional material if time available, or can be viewed later
  - Useful tools
  - An animated film that illustrates many of the topics (and more) - 13 minutes
  - Encoding of data on your local network

Important point to note – ADSL filters

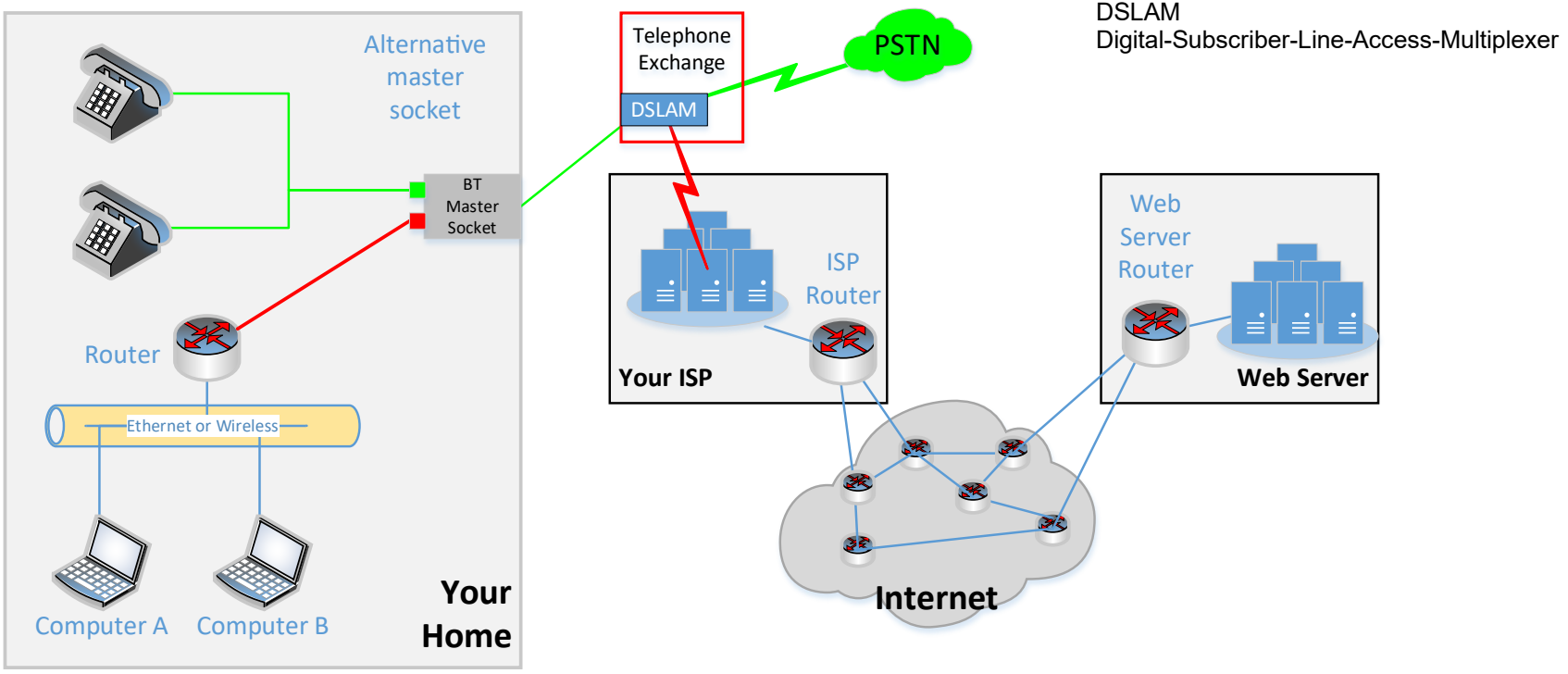
- If using ADSL to connect to the Internet i.e. NOT using a cable service or fibre directly to your home, you are using both standard telephone voice services and broadband down the same wires
  - If you have Fibre to the Cabinet (FTTC) then this separation happens much nearer your home
  - If you do not have FTTC then this happens at the telephone exchange
- As there are two services (voice and data) over the same copper wires these need to be separated
  - An ADSL filter provides this separation in the home. There MUST be
    - an ADSL filter on EVERY telephone as well as your router connection as shown on the diagram
    - OR there can be a filtered Master Socket where the telephone wires enters your property if your router is nearby. This is technically the best solution if feasible but is is less easy to install
  - If you do not have a filter on every phone (or a filtered master socket) an incoming call will cause your broadband to drop out and your broadband speed will be lower than you expect
- Fibre to the Premises (FTTP) is being threatened as an imminent upgrade to the telephone network but will have other issues that need to be addressed and is outside the scope of this talk

Overview of what we are talking about



DSLAM
Digital-Subscriber-Line-Access-Multiplexer

Alternate home wiring – Master socket replacement

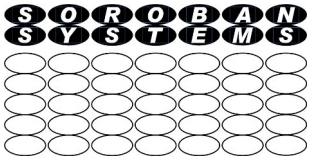


DSLAM
Digital-Subscriber-Line-Access-Multiplexer

Internet – Web site addresses - URL

- We are all familiar with web site addresses
  - http://soroban.co.uk/preview.html
  - The first part https:// tells us what type of connection we are making. You usually do not need to type it, https is encrypted, http is not encrypted but mist sites now support https.
  - The second part is specific to the site and typically identifies which server is being used to serve the page – it is often omitted and can be optional e.g. www.soroban.co.uk and soroban.co.uk both work
- The whole part www.soroban.co.uk (begore the optional /) is called the Fully Qualified Domain Name (FQDN) and identifies the site you want to reach
  - The co.uk part of the domain identifies the Top Level Domain (TLD) i.e. the country where the site is registered – not necessarily where it is hosted. .co.uk means the site is registered in the UK
  - This presentation will concentrate mainly on how we reach this site
- The final part e.g. /preview.html is optional and if present, is specific to a site and indicates that a subset of the site is being accessed or a non default start page is being used. Here it is a test page.
  - If omitted then a standard default page of index.html is assumed

We have a domain – what is an IP address?



- The Fully Qualified Domain Name e.g. soroban.co.uk identifies the site we need but is not what we actually need to access the site
  - We need an Internet Protocol (or IP) address to do that
- To get the IP address we need to look up the Domain to get the IP address for the site
  - To do this we need help from a Domain Name Server to get the IP address
    - The Internet works using IP addresses
  - We will discover how these are related and how we find, and then access, a web site later
  - We must first understand IP addresses

What is an IP address

- Simplistically an IP address is a 32 bit binary number and is the actual unique address on the Internet for the service you want to reach
  - Note that we are talking about IP Version 4 and there are 4,294,967,296 addresses theoretically available
    - Not all IP v4 addresses can be used and you will soon see why, and why these are running out!
    - There is a IP Version 6 which has a considerably larger 128 bit address range but for the purposes of this presentation provides the same features but is more complex to describe
  - There is however a structure associated with this number which is important to understand

Digression into binary/boolean functions

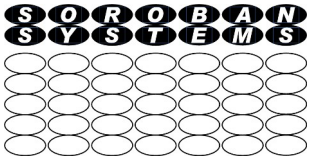
- These are all of the binary operations that can be applied to sets of binary digits (Bits) illustrated here using two Bits
- The value for each bit can only be 0 or 1. Alternatively then can be called False or True
  - NOT inverts the value i.e.
    - 1 → 0
    - 0 → 1
  - XOR = Exclusive OR
  - NAND = Not AND
  - NOR = Not OR

A	B	NOT A	NOT B	A AND B	A OR B	A XOR B	A NAND B	A NOR B	A Not XOR B
0	0	1	1	0	0	0	1	1	1
1	0	0	1	0	1	1	1	0	0
0	1	1	0	0	1	1	1	0	0
1	1	0	0	1	1	0	0	0	1

IP address – structure and notation

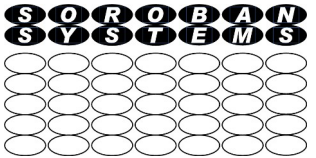
- You will probably have seen IP addresses on your network, or elsewhere, displayed in the format
  - 192.168.1.73
    - This format is called “dotted decimal” and is read as “one nine two dot one six eight dot one dot seventy three”. Each part is an 8 bit binary number between 0 and 255 and is referred to by network experts as an “Octet”, most of us would call it a “Byte”
  - In binary this is `11000000 10101000 00000001 01001001`
    - Within this IP address the first 24 bits (binary digits) or 3 Octets are the network address (your site) and the rest are the address within your site – a subnet
  - We can select the network address simply by using a Subnet Mask and a boolean AND function on each Bit. An AND of NOT(subnet mask) returns the subnet address.
  - `11000000 10101000 00000001 01001001` = IP address = 192.168.1.73
    `11111111 11111111 11111111 00000000` = Subnet mask 255.255.255.0 or /24
  - `11000000 10101000 00000001 00000000` = The Network address = 192.168.1.0 (AND mask)
    `00000000 00000000 00000000 01001001` = A Subnet address = 0.0.0.73 (AND NOT(mask))

IP Address Classes – just for the record



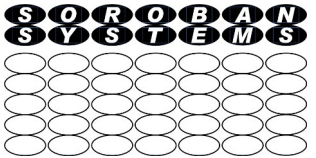
- There are five named ranges of IP addresses (three A, B and C are most usually referred to)
  - 1.0.0.0/8 to 126.0.0.0/8 – Called “Class A” addresses
    - Only 126 addresses exist! MoD owns 25.0.0.0
  - 128.0.0.0/16 to 191.255.0.0/16 – Called a “Class B” addresses
    - 16,382 addresses exist
  - 192.0.0.0/24 to 223.255.255.0/24 – called “Class C” addresses
    - 2,097,150 addresses exist
  - 224.0.0.0 to 239.255.255.254 – Called “Class D” addresses
    - Used for a special purpose – multi-casting
  - 240.0.0.0 to 255.255.255.255 – Called “Class E”
    - Reserved for research purposes
- Apart from the Private Addresses (comes later) an IP address is allocated by a “National Authority”
  - In the UK this is an organisation called Nominet

IP address – within a subnet



- Each device within a network must have a unique IP address in its subnet
  - Each subnet can be further divided into smaller subnets
- Within each subnet there are two addresses that have a special meaning
  - No device can have 1...1 as its subnet address = broadcast address
  - No device can have 0...0 as its subnet address = network address
  - **Most networks you will meet at home use a subnet mask of 255.255.255.0 or /24 giving 254 usable addresses**
    - **Your router normally has a subnet address of 1 or 254 i.e. the first or last possible address in its subnet**
  - The smallest possible subnet is /30 (30 bits) which has two usable addresses
    - You are very unlikely to see this at home but it is useful on complex networks
- This addressing scheme is very wasteful of IP addresses as many networks have far fewer than 254 devices!

IP Addresses – Network Address Translation



- All IP addresses on the Internet must be unique but there are not enough addresses
- Private Address Space – solves this problem (at least for a long time)
  - Your network at home, and even quite large organisations, can have many devices connected but only has ONE public IP address for all devices
    - All of your local devices have a unique address in YOUR Private Address space
  - Your Router (your method of connecting to the Internet) – can identify which of your devices needs to communicate with a remote device on the internet and will convert your request to use its single PUBLIC address from your individual PRIVATE address so that all requests appear to come from a single device – your router
    - This process is called Network Address Translation or NAT – more later
    - You can have one device, or hundreds of devices, but use only ONE IP address on the boundary to the outside world

Private address space ranges

- The IP network standards have reserved three separate Private Address Space ranges and your home network will use one of these, typically with a /24 bit subnet mask (255.255.255.0) as defined by your router configuration
  - 10.0.0.0 to 10.255.255.255 – rare but has been seen on some home networks
    - A very large address space that can be sub-netted locally many times
    - Typically each subnet on a home network would only use 256 addresses but could be huge in a large organisation (but each subnet is rarely more than 1024)
  - 172.16.0.0 to 172.31.255.255 – I have never seen this used on home networks
  - 192.168.0.0 to 192.168.255.254 – Most common for home use
    - Third octet is often 1 but not always, 0 to 255 are all valid values

Local services provided to your internal network

- Your Router
  - Authenticates your site to your ISP before it will allow you to communicate with the Internet
  - Manages your internal Private Address Space IP addresses for your local devices through Dynamic Host Configuration Protocol (DHCP).
    - You do not need to know, in most cases, what IP address your computer has been given
  - Provides a default gateway to route traffic to the “next hop” on the network – typically an ISP router
  - Provides a Domain Name server address to look up domain names
  - Provides Network Address Translation (NAT) on all outbound connections
    - Hides your internal private address space IP address and replaces it with your site Public IP address
    - Replaces your “TCP Port” with one of its own choosing in case another device on your network has used the same one for itself
  - Also provides NAT on inbound responses from an established connection so initiator of the session sees the correct port number
  - Unless explicitly configured – will block all inbound attempts to connect to devices on your internal network
    - This is a significant security benefit – only change it if you are certain you know what you are doing

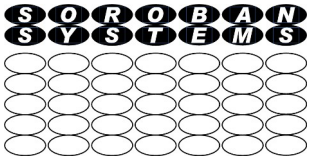
Inbound connections – Plug and Play

- Most routers have configuration options to allow certain inbound connections
  - These can even be permitted to happen automatically – Plug and Play
- In most cases this is a BAD IDEA and you should disable the feature unless you REALLY need it
  - Typically gaming may be one case, or running a local web server
- Why is it a bad idea?
  - If you permit inbound connections you are unnecessarily opening up your network to an attack from outside
    - Bad actors can attempt to connect to your internal devices
    - Non PCs can be especially vulnerable as they di not have firewalls or antivirus defences e.g.
      - Door entry devices
      - Heating controls
      - Toys especially
      - Security cameras
      - etc

Additional local services – Wi-Fi and Ethernet Switch

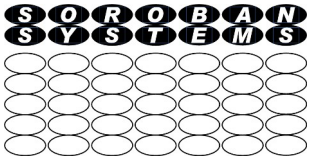
- Most routers now also provide wireless connectivity for local Wi-Fi connected devices
  - Note that Wi-Fi is strongly encrypted (now) but you share the wireless spectrum and hence bandwidth with all your neighbours within range – I have seen 40 networks listed
    - This means you are sharing the available bandwidth with them
    - There are multiple channels available which helps to optimise bandwidth use
  - There are now two bands available 2.4 GHz and 5 GHz
    - 5 GHz is supported by most NEW devices, is faster, but has limited range
    - 2.4 GHz is supported by all Wi-Fi devices but there tend to more neighbours competing for bandwidth
  - You can survey your local environment using the free Acrylic network analyser
- Most routers now have more than one Ethernet port for providing wired connections to local devices and provide an Ethernet Switch function to connect local devices together
  - One of these could be connected to a Powerline Ethernet adaptor for difficult sites

What happens when the Router boots up



- Your router will typically have certain information preconfigured when you receive it, or you have to provide during initial setup – be guided by your ISP setup instructions
  - e.g. your ISP access credentials
  - the name or IP address of your ISP – the details depend on the method of connecting
- It will connect to your ISP, authenticate you and and then obtain from your ISP when the connection is established at least the following information
  - An IP address on the ISP network – this is your PUBLIC address
    - This will not necessarily always be the same one, it can change!
      - It may dynamically change while the router is being used
      - You can sometimes request a fixed IP address depending on your ISP
  - The ISP default gateway IP address to be used when routing to an external site
  - An IP address for the Domain Name server for converting domain names to IP addresses
  - Probably obtain an accurate time from an Internet source to be used in any logs it keeps

What happens when your Computer boots up



- Your computer will typically broadcast a Dynamic Host Configuration Protocol (DHCP) request onto the local network. This will include the unique burned in hardware address of your network interface = MAC address
  - This will be received by the local DHCP server – typically your router
  - Your DHCP server will return
    - An IP address and subnet mask to be used by your PC, and the lease time
    - The Default Gateway IP address to be used for traffic outside the local network
    - The Domain Name Server IP address to be used to look up domain names
- The DHCP server maintains a list of already allocated IP addresses against MAC addresses
  - If your computer is already in that list it will get the same IP address
  - If it is not it will get an address allocated from the configured pool of available addresses
  - The server will record the time the IP address is offered and manage the “Lease” time
  - If the pool has all been used any unallocated IP address or those with expired leases can be reallocated
  - An IP address can usually be “reserved” in the pool (manually configured) so it will never be reallocated
- If/when the DHCP lease expires the computer will renew the lease

Example DHCP table in Router

Device	MAC Address	IP Address	Lease Time
CCTV	ec:c8:9c:8b:4e:cb	192.168.1.221	00:22:04:13
GatewayD9AED1	00:d0:2d:d9:ae:d1	192.168.1.200	00:22:04:35
HUAWEI_P8	04:02:1f:a6:98:e6	192.168.1.66	00:21:29:03
soro-arch02	00:11:32:f0:ee:df	192.168.1.220	00:23:40:34
soro-lap08	70:cf:49:39:40:54	192.168.1.69	00:16:53:27
udhcp-1-18-5-18-5-2c-08-8c-73-10-54	2c:08:8c:73:10:54	192.168.1.201	00:18:40:03

What happens when you first open a URL

- When you enter a URL into your browser your computer does not know the IP address related to the URL
  - It parses the URL and picks out the “Domain Name” e.g. www.soroban.co.uk
  - It sends a Domain Network Service request to the DNS server to look up the name and obtain an IP address
    - The computer is told the DNS server IP address to use when it first contacts the router
    - This is typically the router!
  - The router will forward the request to the DNS server(s) it knows about
    - This server may have this information but, if not, it forwards the request to other DNS servers until one responds with an IP address (or an error if it cannot be found)
    - The response is passed back through the chain to the router and then to the requester who now has the IP address it needs
- Your computer will typically cache this name and IP address in case it is needed again

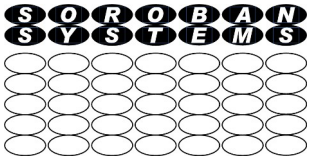
Routing the traffic to the IP address

- We have an IP address so how does this get to it's destination?
- A computer that has a target IP address compares the Network Address of the destination with its own IP address as follows
  - Apply the subnet mask to the target IP address and compare with its own network address – this comparison is easy using binary XOR and then AND with the subnet mask
    - If they are the same – the target is on its own network
    - If they are different – the target is on a remote network
      - `255.255.255.0 = 11111111.11111111.11111111.00000000 =` Subnet mask
      - `192.168.1. 69 = 11000000.10101000.00000001.01000101 =` Source address
      - `192.168.1.254 = 11000000.10101000.00000001.11111110 =` Local address
      - `Result = 00000000.00000000.00000000.00000000 =` Same network
      - `109.228.37.73 = 01101101.11100100.00100101.01001001 =` gxcc.org.uk
      - `Result = 10101101.01001100.00100100.00000000 =` Different network

Principles of Routing

- Is the IP address on same network? - compare network address using subnet mask
  - If the source computer has previously recently communicated with this IP address the address will be locally cached
    - Otherwise the source computer broadcasts an Address Resolution Protocol (ARP) request and receives back the MAC address (physical address of the network device) of the target.
      - A timeout will occur if there s no response – device unreachable
    - The IP address is cached
  - **The data packet can be sent directly to the correct local computer using the MAC address – not the IP address**
    - The IP data is encapsulated into the network packet sent
- Is IP address is on Different network? - network comparison is non zero
  - Send the packet to the “Default Gateway” i.e. typically your local Router on your local network
    - The IP address of the default gateway is provided via DHCP when your computer receives its IP address
  - Your router will receive the data packet and forward it to its own default gateway for onward routing
    - The receiving router will have routing tables and will either
      - Have a direct connection to the target network
      - Know a “next hop” to forward the data packet to and so on until it arrives at its destination
    - There may be several viable routes but there will always be a “lowest cost” route that each router in the chain will choose

Example of tracing route to soroban.co.uk



- PS C:\Users\john> tracert soroban.co.uk
-
- Tracing route to soroban.co.uk [109.228.37.73]
- over a maximum of 30 hops:
-
- 1 2 ms 1 ms 1 ms dsldevice.lan [192.168.1.254]
- 2 6 ms 5 ms 5 ms 172.16.11.211
- 3 * * 7 ms 141.hiper04.sheff.dial.plus.net.uk [195.166.143.141]
- 4 9 ms 9 ms 8 ms 140.hiper04.sheff.dial.plus.net.uk [195.166.143.140]
- 5 8 ms 7 ms 57 ms peer8-et0-1-5.telehouse.ukcore.bt.net [109.159.252.102]
- 6 9 ms 10 ms 10 ms linx.bb-d.ba.slo.gb.oneandone.net [195.66.236.98]
- 7 12 ms 12 ms 12 ms port-channel-4.gb-glo-sgngdsr02.oneandone.net [88.208.255.4]
- 8 12 ms 12 ms 12 ms 109.228.63.230
- 9 13 ms 13 ms 12 ms server.dovedaledesign.co.uk [109.228.37.73]
-
- Trace complete.

Transferring data using IP

- IP packets are limited in size by the network being used
  - If any router in the chain cannot handle a packet size it is being offered it can “fragment” the packet into two or more parts
    - With IP v4 it will never be recombined into a larger packet
    - The type of packet is called a “datagram”
  - Each packet contains (not a full list)
    - A header containing a number of fields including
      - Protocol version (assumed to be 4 in this case)
      - Header length and Type of data
      - Source and destination IP Address
      - Total Size including header (up to 65535 octets)
      - Fragmentation control – can prevent fragmentation but might lead to data being undeliverable
      - Header checksum
    - A data block (can be empty)
  - Note that there is no overall checksum on the entire packet

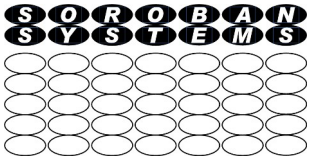
Higher level Protocols

- IP is the common most basic lower level protocol
- Additional protocols can be applied to the data to make the data transfer more robust
  - The most common is Transport Control Protocol = TCP (or sometimes written as TCP/IP as it is possible to use TCP over alternative lower level protocols)
- TCP adds error detection and recovery, where possible, by retransmission
- TCP/IP was designed to be quite literally “bomb proof” as the early work was for the US Military
  - There are further protocols (not an exhaustive list) that can be applied above TCP/IP
    - HTTP or HTTPS – Hypertext Transport Protocol (or plus encryption)
    - FTP – File Transfer Protocol
    - SMTP – Simple Mail Transfer protocol – Sending email
    - POP3 - Post Office Protocol 3 – Receiving email
    - Etc.
- We will look further at HTTP as the protocol that we are most directly exposed to via web URLs

TCP protocol

- An important aspect of TCP is that it introduces a concept of a “connection” that can transmit a “stream” of data.
- A stream has a Source Port and a Destination Port
  - Ports are just numbers up to 65535 that identify a “session”
  - Any computer can have several streams open to the same, or different, destinations
  - Some Port Numbers have specific purposes and are always the same
    - Port 80 is the default for standard HTTP traffic for example and a web server will “listen” on port 80
    - Port 8080 is used for encrypted HTTPS traffic
    - The session initiator e.g. your web browser will define a random port to receive responses
      - The port range, allocated for this purpose as “ephemeral ports”, are 49152-65535

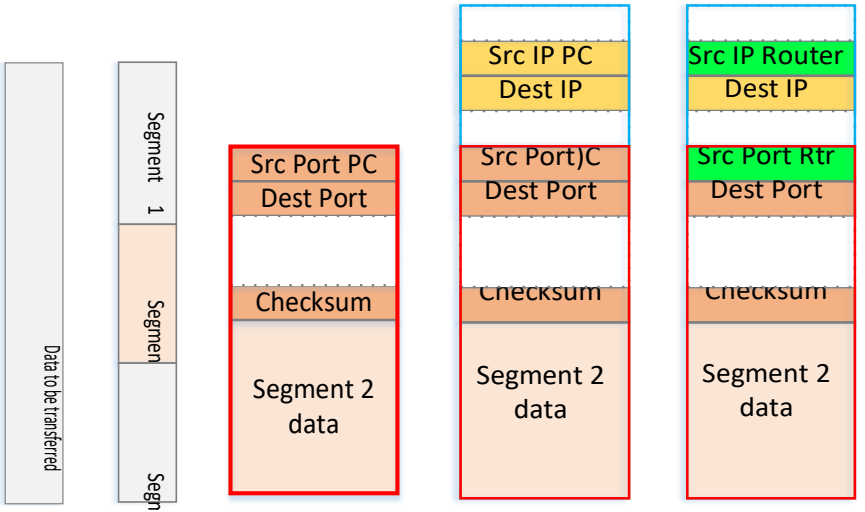
HTTP over TCP



- A program on your computer initiates a TCP connection e.g.
  - You type a URL into your browser and then Enter
  - Your computer will use Domain Name lookup to find the IP address
  - Your computer will initiate an HTTP connection by opening a TCP session with the remote web server using this address
    - It will normally assume a standard port (80) for the destination and pick a random port for replies
    - The process requires a “three way handshake” to confirm the connection
    - Once this has completed data can be sent to the web site and data can be received from the web site

Encapsulation of data into IP and then TCP

- Data to be transmitted
- Segmentation into Maximum Segment (MSS) size blocks
- Wrapping one segment (segment 2) into an IP packet
- Wrapping IP packet into a TCP/IP packet
- Applying Network Address Translation by router to hide private addresses
- Note that checksum field is set to zero before calculating the actual value and the calculated value is then inserted



Some Internet tools - Windows

- Some PowerShell tools (Windows only, MAC has equivalent programs to be run in Terminal but in some cases the names are different)
  - **ipconfig or ipconfig /all**
    - Details about your local network connections.
      - Use /all option for more detail
    - Note that ipconfig has many other options see ipconfig /?
  - **ping <ipaddress> or ping <domain name>**
    - Test whether IP address or domain (local or remote) is reachable, and how long the round trip takes
    - Expect well under 10 mS for local network, perhaps up to 30 to 75mS for a remote connection
      - The time may vary. The report gives minimum and maximum times
      - Some devices may block pings → unreachable
  - **tracert <ipaddress> or tracert <domain name>**
    - Lists all of the routing devices that you pass through to reach your target device
  - **route** print
    - Prints current local routing table to the screen (not the printer!)

ipconfig - sample

```
PS C:\Users\john> ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::bcd7:56e3:f244:4618%19
   IPv4 Address. . . . . . . . . . . : 192.168.1.69
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

ping - example

```
PS C:\Users\john> ping soroban.co.uk

Pinging soroban.co.uk [109.228.37.73] with 32 bytes of data:
Reply from 109.228.37.73: bytes=32 time=12ms TTL=56
Reply from 109.228.37.73: bytes=32 time=13ms TTL=56
Reply from 109.228.37.73: bytes=32 time=13ms TTL=56
Reply from 109.228.37.73: bytes=32 time=12ms TTL=56

Ping statistics for 109.228.37.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 13ms, Average = 12ms
PS C:\Users\john>
```

tracert - example

- **The three times displayed are round trip times for three separate requests made to the IP address.**

```
PS C:\Users\john> tracert gxcc.org.uk

Tracing route to gxcc.org.uk [109.228.37.73]
over a maximum of 30 hops:

  1     3 ms     1 ms     1 ms  dsldevice.lan [192.168.1.254]
  2     5 ms     5 ms     6 ms  172.16.11.211
  3     *        *        8 ms  141.hiper04.sheff.dial.plus.net.uk [195.166.143.141]
  4    11 ms     9 ms     9 ms  140.hiper04.sheff.dial.plus.net.uk [195.166.143.140]
  5     7 ms     7 ms     8 ms  peer8-et0-1-5.telehouse.ukcore.bt.net [109.159.252.102]
  6     9 ms     9 ms     9 ms  linx.bb-d.ba.slo.gb.oneandone.net [195.66.236.98]
  7    13 ms    14 ms    13 ms  port-channel-4.gw-ngcs-2.dc1.con.glo.gb.oneandone.net [88.208.255.4]
  8    13 ms    12 ms    12 ms  109.228.63.230
  9    13 ms    13 ms    13 ms  server.dovedaledesign.co.uk [109.228.37.73]

Trace complete.
```

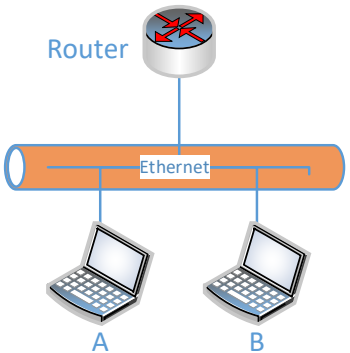
Some advanced tools for the curious

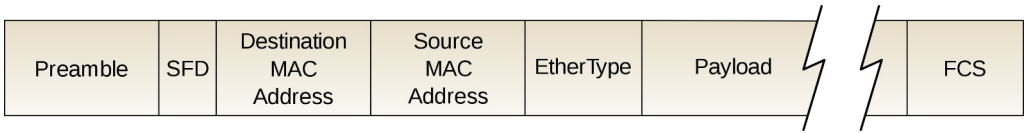
- The following programs (and many others) can all be found on the link
  - https://www.soroban.co.uk
    - Select menu item Support Pages → PC/Mac/Linux apps → Networks
      - [This was correct in Aug 2023]
- Acrylic – very good free Wi-Fi survey tool when used on a laptop
  - Display wireless networks available and their signal strengths
  - It can draw a time related graph of signal strength so good for surveying where weak signal spots are
  - A cached copy is currently available as the new version did not work as well as the previous one
    - This is under review and an alternative might be posted in this section!
- Wireshark – Experts tool, or for the keen enthusiast who wants to learn more
  - Shows network traffic in complete detail in real time
    - Data can be captured to a file for later off-line analysis
    - Filters can be applied to focus on specific items of interest e.g. IP addresses
    - Needs practice to use for diagnosis but is excellent if you have some idea what you are looking for or really want to learn the format of every packet in detail
-

Video – Warriors of the Internet

- Animated film illustrating what has been described (and more) – 13 minutes. It is quite an old film but very little has changed!
  - https://www.youtube.com/watch?v=PBWhzz_Gn10

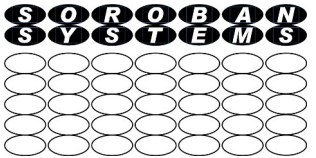
Basic Ethernet communication





- This diagram shows an Ethernet data packet (there is a variation allowed where there is an additional 8 octets of header data following a specific format Ethertype field)
- The maximum standard size is 1500 bytes of data. Later variations allow for larger Jumbo Frames
  - Preamble
    - 7 octets of binary 10101010 to get the receiver clock synchronised
    - A Start Frame Delimiter that terminates the preamble = 10101011
  - Destination MAC address – 6 octets
    - All ones (FFFFFF in hexadecimal) is a special Broadcast address
  - Source MAC address – 6 octets
    - A world wide unique number burned into the network controller
  - Ether type – 2 octets = type of data in the payload
  - Payload – the data to be transmitted
  - Frame Check Sequence
    - 4 octets checksum
  - Inter Record Gap – 12 octets before next frame is sent

Encoding of data on your local network



- Bits are transmitted sequentially starting with the most significant bit of the first octet
- They are “self clocking” which means the receiver can adapt to the bit rate
- Look up “Manchester Encoding” for details
- The sequence starts with a peramble of 7 octets to synchronise the receiver clock consisting of a binary sequence 10101010
- The 8th and final octet is slightly different 10101011 which tells the receiver that data follows
- The Frame Check Sequence verifies that the message has been received correctly
- In the original Ethernet any connected device listens to the network and if no other device is transmitting it just goes ahead. This does not happen now with Ethernet switches.
- There is a case that two devices start at the same time. This corrupts the message.
- They both listen to their own data and will retransmit if they see corruption.
- Each backs off for a random time before trying again.