Welcome to Sydney Linux User Group

https://slug.org.au/

Networking:

Terminology,
Layer 2 vs Layer 3,
IP Addressing & Subnetting

SLUG Meetup

Phil Storey

28 June 2024

Agenda

The aim is to give you a quick run through of terminology and protocols involved in today's networks (focussing on layers 2 & 3).

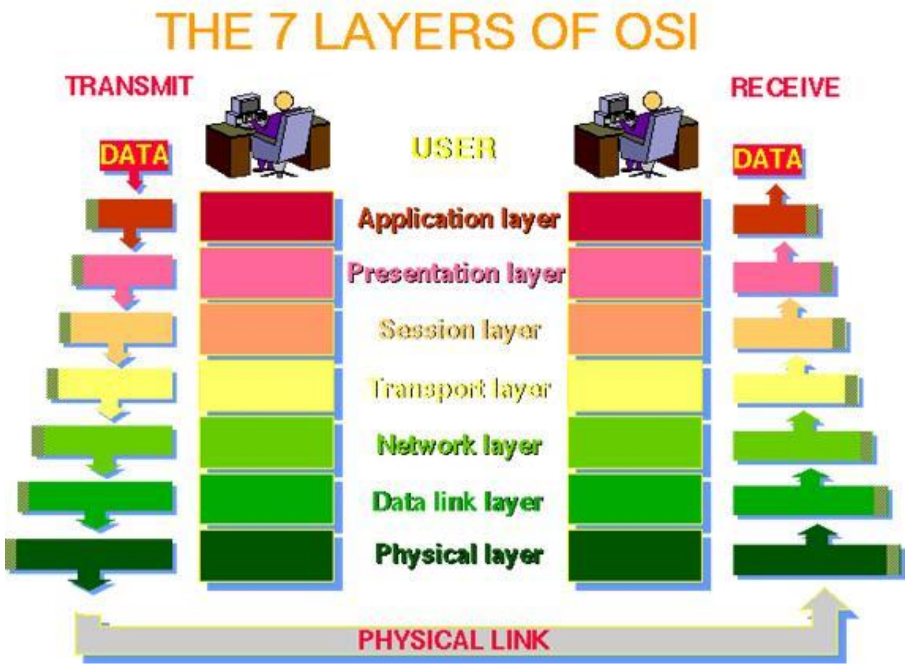
- What are "Layers".
- What is Ethernet and a little history
- What is IP (of TCP/IP fame) and a little history
- Terminology and "Things Worth Knowing"
- IP Addressing, Subnetting, Routing

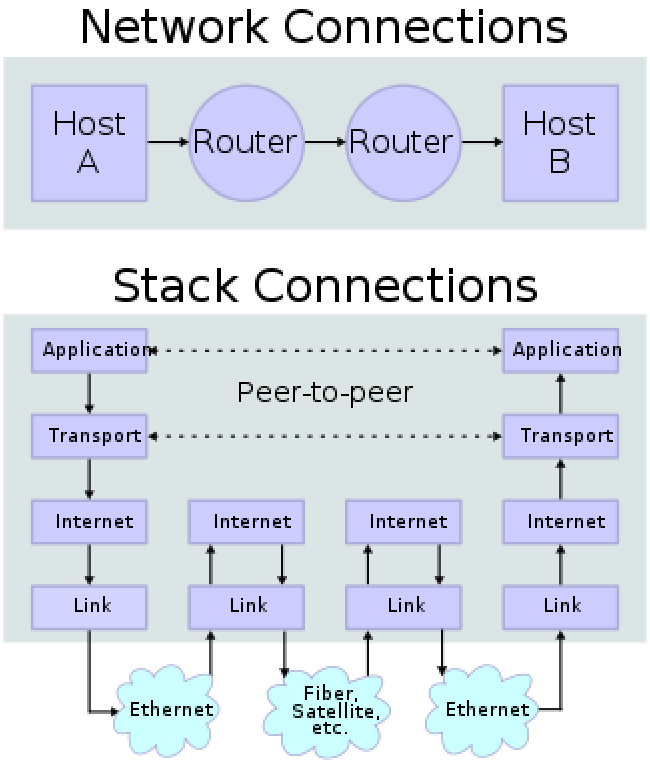
As usual → Interrupt and ask questions along the way

Network Layers: OSI vs TCP/IP

The "OSI Model" is where we get the terminology of network "Layers".

Although TCP/IP does **not** exactly fit the OSI layers, we still refer to TCP as Layer 4, IP as Layer 3 and Ethernet (& WiFi) as Layer 2.





Keywords:- Open Systems Interconnection Model, Protocol Stack, Transmission Control Protocol, Internet Protocol, Ethernet.

Tonight's Focus

The Internet Protocol Suite

Application Layer

BGP · DHCP · DNS · FTP · GTP · HTTP · IMAP · IRC · Megaco · MGCP · NNTP · NTP · POP · RIP · RPC · RTP · RTSP · SDP · SIP · SMTP · SNMP · SOAP · SSH · Telnet · TLS/SSL · XMPP · (more)

Transport Layer

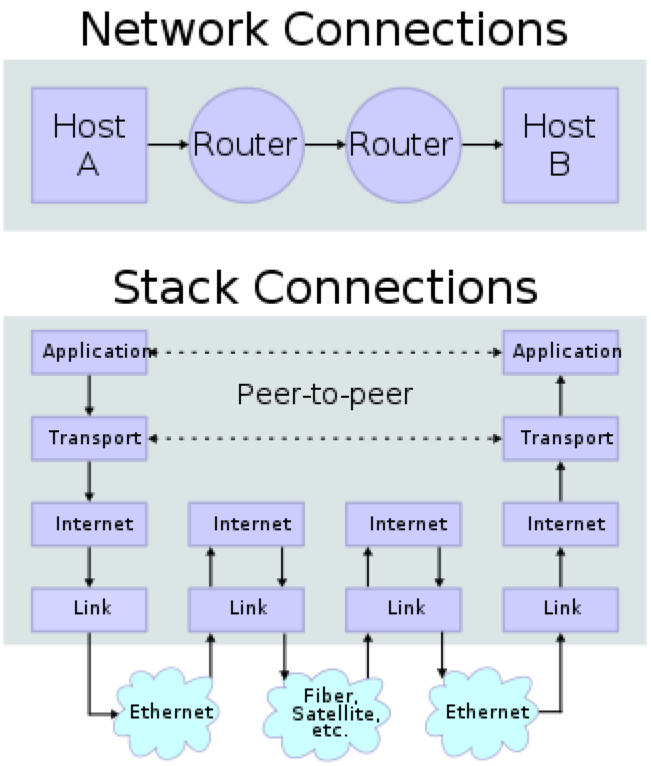
TCP · UDP · DCCP · SCTP · RSVP · ECN · (more)

Internet Layer

IP (IPv4, IPv6) · ICMP · ICMPv6 · IGMP · IPsec · (more)

Link Layer

ARP · RARP · NDP · OSPF · Tunnels (L2TP) · PPP · Media Access Control (Ethernet, MPLS, DSL, ISDN, FDDI) · Device Drivers · (more)



Ethernet History: Stage 1 - Coaxial Cable

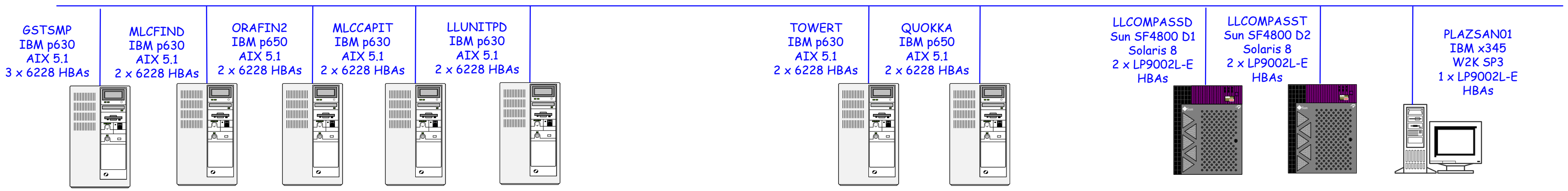
Why do we tend to draw Ethernet LANs as a straight line?

Because Ethernet used to be a straight line!

Ethernet is the standard LAN protocol used in modern networks.
"MAC addresses" are 6 bytes and written in hexadecimal (eg, C4-34-6B-04-C9-F9)

Some of the early competition for Ethernet included:-
Token Ring from IBM,   AppleTalk,   several others that didn't last long.

Ethernet was originally based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium.

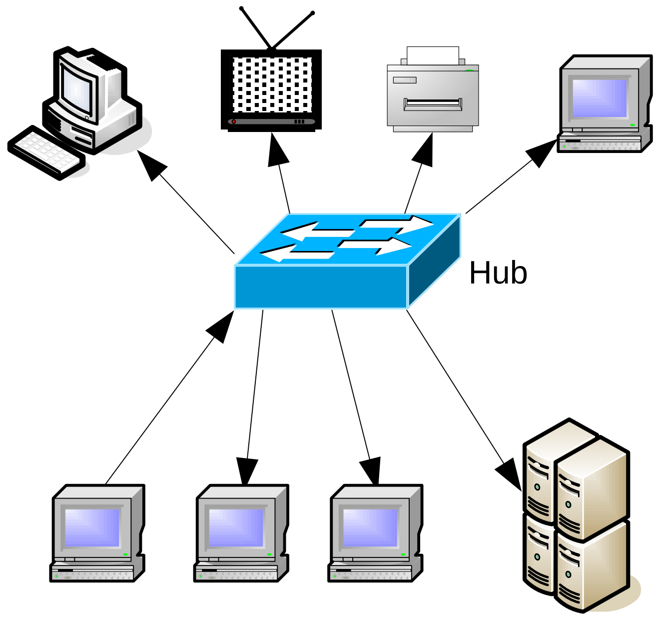


Keywords:- Thick Ethernet, Thin Ethernet, Layer 2, CSMA/CD, Collision Domain, Broadcast Domain

Ethernet History: Stage 2 Hubs – Coax to UTP

The advent of hubs turned Ethernet into a “Star” topology.

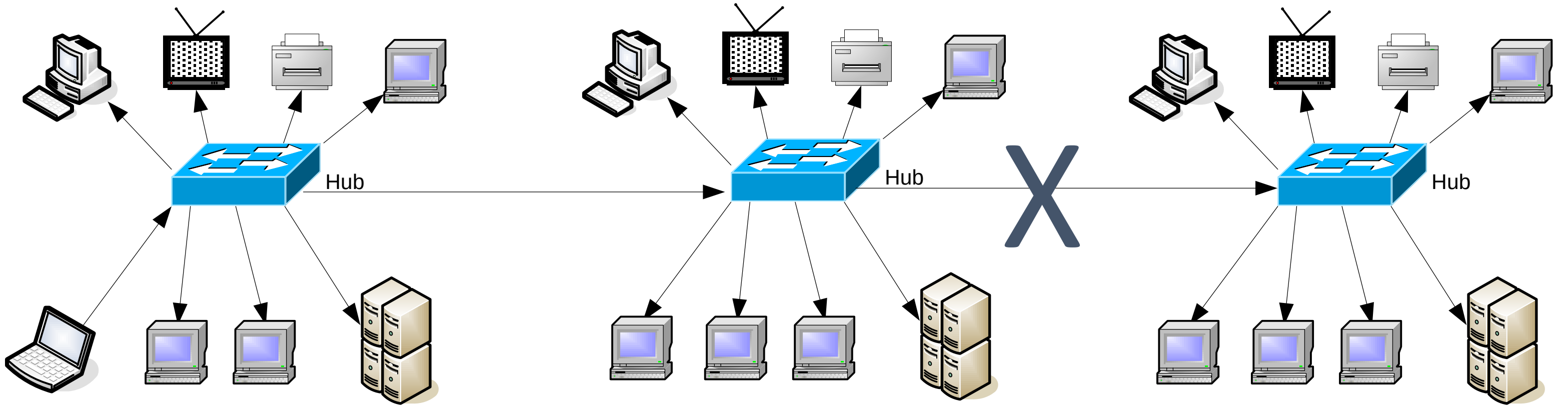
However, it still had to pretend to be a shared cable! Any frame that arrives at the hub, on any port, must be retransmitted to every other station.



Keywords:- Hub, UTP, Category 5/5e/6, RJ45, Half Duplex

Ethernet History: Hubs = More Flexibility

To make a larger LAN, simply connect hubs together.



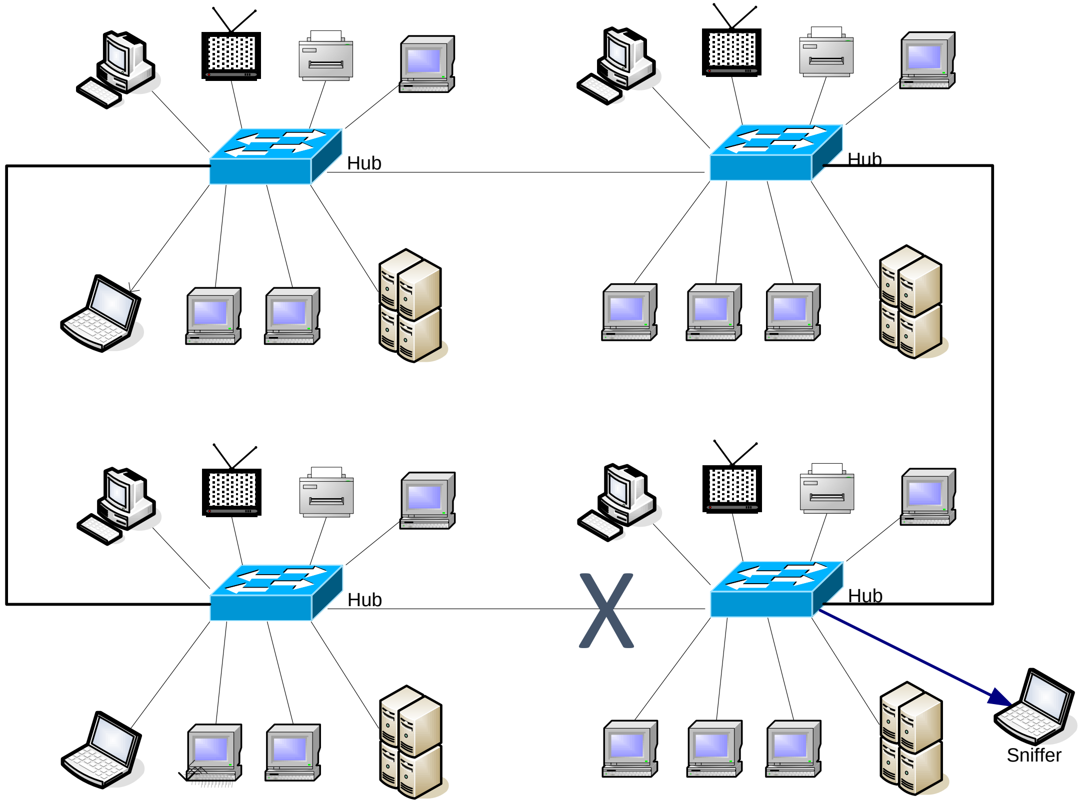
Of course, if a hub fails – we lose connectivity!

We also need to provide power to each hub.

[This wasn't a problem with a coax cable.]

Ethernet History: Limitations

But the original specifications place various limits on the extent that the LAN can grow.
There are also limits to the way that hubs can be connected.

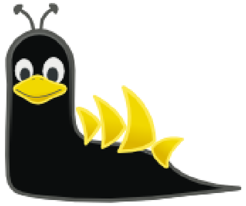


If we need more than one LAN, eg, to have a separate Prod, Test & Dev or Management networks, then we need multiple sets of hubs – each with their own interconnects.

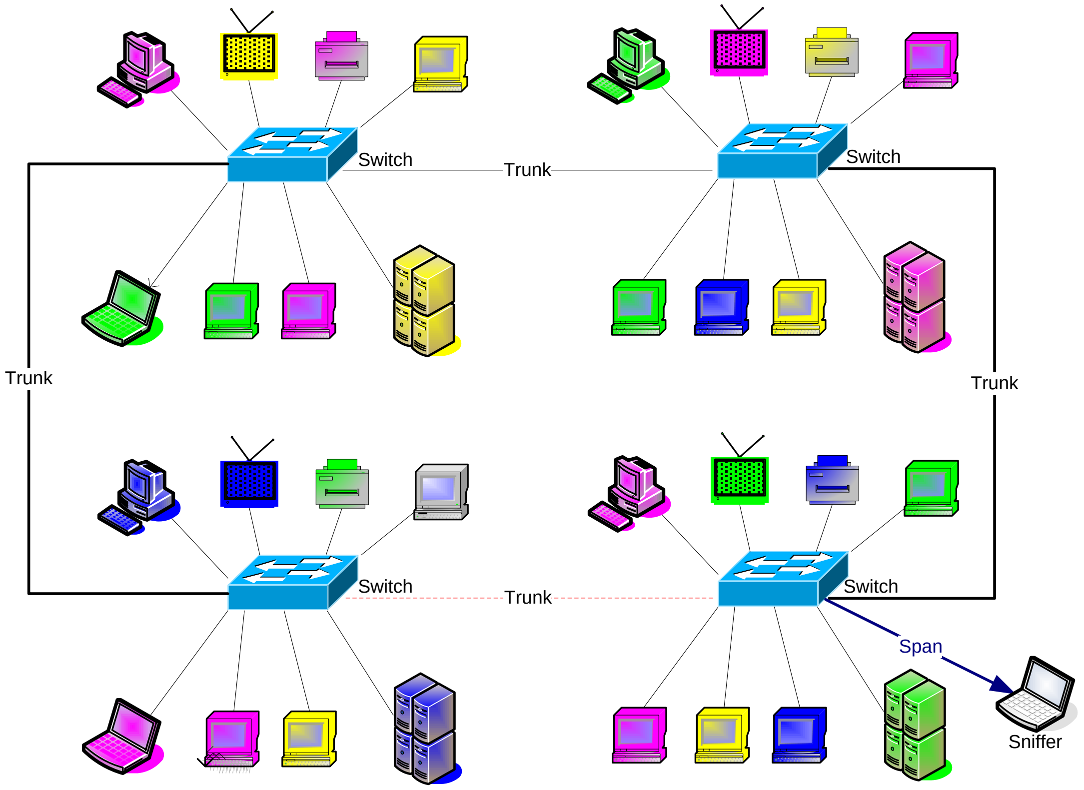
Further, this is not the most efficient use of the new “star” connection method.

Any spare port can be used to “sniff” all traffic.

Ethernet Today: Stage 3 - Switches / VLANs



As technology advanced, we moved from hubs to much "smarter" switches. One of the key "smarts" is that the switch memorises the MAC addresses of observed nodes – and can send the frame only to the one port. It can also "store & forward".



We can now have full duplex, faster speeds, parallel traffic and more.

Automatic "spanning tree" calculations choose which switch-to-switch link to disable ("converge").

VLANs: Switches can segregate different LANs.

Trunks between switches can carry frames from multiple VLANs.

No more collisions (or Sniffing)

Keywords:- Spanning Tree, VLAN, 802.1q Trunking, Span Port, Full Duplex

A Cisco Desk Phone Contains a 2-Port Switch

[Hopefully not your comms room!]

Ethernet “Frame”

802.3 Ethernet packet and frame structure

Layer	Preamble	Start frame delimiter (SFD)	MAC destination	MAC source	802.1Q tag (optional) VLAN “ID”	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap (IPG)
Length (octets)	7	1	6	6	(4)	2	42–1500[c]	4	12
Layer 2 Ethernet frame	(not part of the frame)		← 64–1522 octets →						(not part of the frame)
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →

The optional 802.1Q tag consumes additional space in the frame. Field sizes for this option are shown in brackets in the table above. IEEE 802.1ad (Q-in-Q) allows for multiple tags in each frame. This option is not illustrated here.

Source: https://en.wikipedia.org/wiki/Ethernet_frame

IANA OUI Ethernet Numbers (MAC Addresses)

6 Byte MAC addresses are assigned to organisations by the **Internet Assigned Numbers Authority**.

The first 3 bytes of every MAC represent the “**Organizationally Unique Identifiers**”.
That organisation can allocate the remaining 3 bytes to each device.

Every device must have a unique MAC address.

We use hexadecimal notation to display MAC addresses, eg, C4-34-6B-04-C9-F9.

No standard for separators such as “-” or “:”.

Some of the numbers aren’t assigned.
There are reserved ranges for various functions.

```
20:9B:CD Apple                 # Apple, Inc.
20:A2:E4 Apple                 # Apple, Inc.
20:A2:E7 Lee-Dick              # Lee-Dickens Ltd
20:A6:80 HuaweiTe              # HUAWEI TECHNOLOGIES CO.,LTD
20:A7:87 BointecT              # Bointec Taiwan Corporation Limited
20:A9:0E TctMobil              # TCT mobile ltd
20:A9:9B Microsof              # Microsoft Corporation
20:AA:25 Ip-NetLl              # IP-NET LLC
20:AA:4B Cisco-Li              # Cisco-Linksys, LLC
20:B0:F7 Enclustr              # Enclustra GmbH
20:B3:99 Enterasy              # Enterasys
20:B5:C6 MimosaNe              # Mimosa Networks
20:B7:C0 OmicronE              # OMICRON electronics GmbH
20:BB:C0 CiscoInc              # Cisco Systems, Inc
```

https://www.iana.org/assignments/ethernet-numbers/ethernet-numbers.xhtml#ethernet-numbers-2

MAC of This Laptop

macaddress.io | Database Download | Lookup | API | Generator | Statistics | FAQ | Login | Sign up

C4-34-6B-04-C9-F9 MAC address details

MAC address or OUI | New search

Vendor details

OUI	C4:34:6B
Is private	False
Company name	Hewlett Packard
Company address	11445 Compaq Center Drive Houston 77070 US
Country code	US

Block details

Is registered	True
Border left	C4:34:6B:00:00:00
Border right	C4:34:6B:FF:FF:FF
Block size	16,777,216
Assignment block size	MA-L
Date created	25 February 2014
Date updated	12 October 2015

MAC address details

Is valid	True
Virtual Machine	Not detected
Transmission type	Unicast
Administration type	UAA
Applications	Not detected
Wireshark notes	No details

IANA (ICANN) IP Address Allocation

IP addresses are distributed in a hierarchical system.

As the operator of Internet Assigned Numbers Authority (IANA) functions, Internet Corporation for Assigned Names and Numbers (ICANN) allocates IP address blocks to the five Regional Internet Registries (RIRs) around the world.

(The “regions” of the Regional Internet Registries are roughly continental in size.)

The RIRs then allocate smaller IP address blocks to ISPs and other network operators.

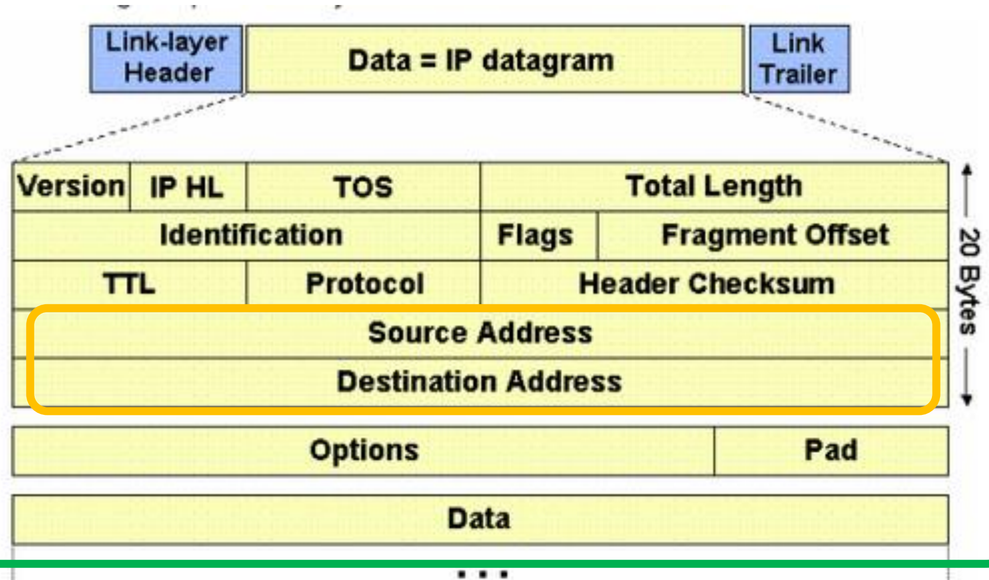
From there, the ISPs and other Internet operators assign the addresses to the individual Internet connections you are probably accustomed to.

https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf

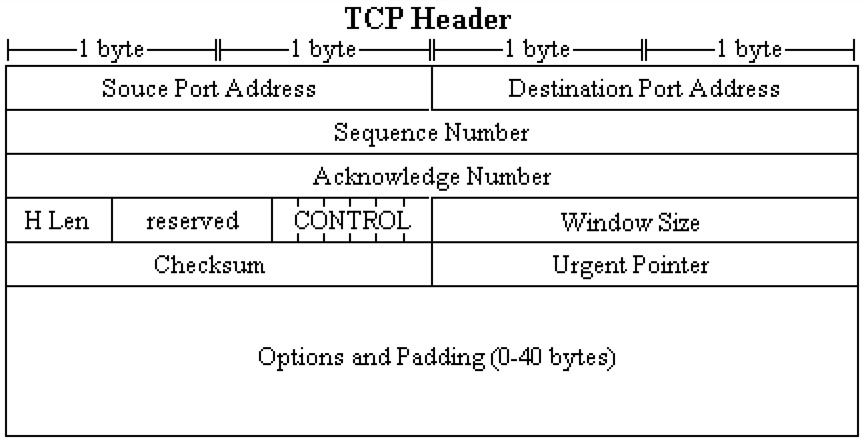
https://pressbooks.howardcc.edu/cmsy164/chapter/packet-analysis-ip-headers-tools-and-notes/
https://www.ardenstone.com/projects/seniorsem/reports/TCP_Protocol.html

Ethernet frame maximum size is 1500 bytes.

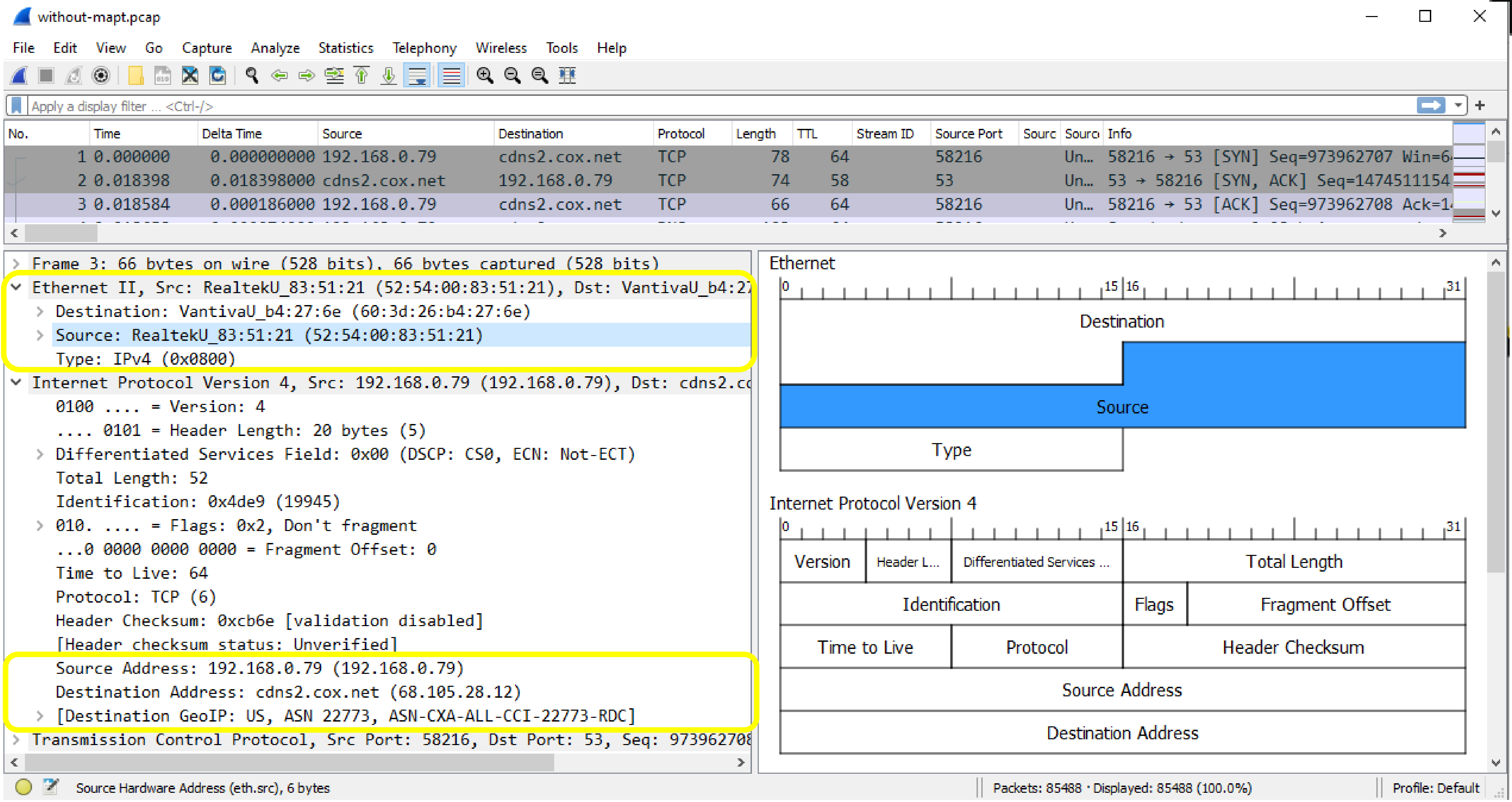
IP header is 20 bytes, leaving 1480 bytes for the IP data payload.



TCP header is 20-40 bytes, leaving 1440-1460 bytes for the TCP data payload.



Wireshark (with Name Resolution & "Packet Diagram")



IP Address Types & Ranges

Originally, IP address ranges were designated into 3 classes (A, B & C based on 1st 2 bits).
Organisations were typically allocated a whole "class".

Types	IP Address Range
Private (Can't be used on the Internet)	10.x.x.x 172.16.x.x to 172.31.x.x 192.168.x.x 100.64.0.0 /10 (from 2012 - carrier grade NAT)
Automatic Private	169.254.x.x (assigned by local device if DHCP fails)
Reserved	0.x.x.x 127.x.x.x ("Loopback" - usually 127.0.0.1)
Public	Everything else

Examples	IP Addresses
AT&T	1.x.x.x
IBM	9.x.x.x
Typical Home Router	192.168.0.0 /24

Smile?

There are 10 kinds of people in the world …..

- Those who understand binary arithmetic.
- Those who don’t.

A Typical Subnet (Say the floor of a corporate office)

IP Addresses	Description
10.99.23.0	Not assigned to a “node”. Used to describe the subnet.
255.255.255.0	Subnet Mask in “dotted decimal”
11111111.11111111.11111111.00000000	Subnet Mask in binary
FF.FF.FF.00	Subnet Mask in hexadecimal
10.99.23.0 / 24	Subnet definition in “slash” or “CIDR” notation (next slide)
10.99.23.1 to 10.99.23.254	Usable addresses
10.99.23.255	“Broadcast” Address

There are 10 kinds of network people in the world …..

IP Addresses	Description
10.99.23.1	The “default gateway” (most common in 2024).
10.99.23.254	The “default gateway” (used to be an IBM “standard”).

CIDR (Classless Inter-Domain Routing)

Introduced by IETF in 1993.

A new “slash” terminology to define subnet ranges.

Instead of,

“My subnet is 10.99.23.0 with a subnet mask of 255.255.255.0”

We now say,

“My subnet is 10.99.23.0 /24”

https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Subnet Masks in Binary

CIDR Block	Slash	Network IP	BroadcastIP	Subnet Mask	Subnet Mask (Binary)	IPQuantity
1.0.0.0/1	1	1.0.0.0	127.255.255.255	128.0.0.0	10000000.00000000.00000000.00000000	2147483648
128.0.0.0/1	1	128.0.0.0	255.255.255.255	128.0.0.0	10000000.00000000.00000000.00000000	2147483648
1.0.0.0/2	2	1.0.0.0	63.255.255.255	192.0.0.0	11000000.00000000.00000000.00000000	1073741824
1.0.0.0/3	3	1.0.0.0	31.255.255.255	224.0.0.0	11100000.00000000.00000000.00000000	536870912
1.0.0.0/4	4	1.0.0.0	15.255.255.255	240.0.0.0	11110000.00000000.00000000.00000000	268435456
8.0.0.0/5	5	8.0.0.0	15.255.255.255	248.0.0.0	11111000.00000000.00000000.00000000	134217728
12.0.0.0/6	6	12.0.0.0	15.255.255.255	252.0.0.0	11111100.00000000.00000000.00000000	67108864
14.0.0.0/7	7	14.0.0.0	15.255.255.255	254.0.0.0	11111110.00000000.00000000.00000000	33554432
15.0.0.0/8	8	15.0.0.0	15.255.255.255	255.0.0.0	11111111.00000000.00000000.00000000	16777216
15.128.0.0/9	9	15.128.0.0	15.255.255.255	255.128.0.0	11111111.10000000.00000000.00000000	8388608
15.192.0.0/10	10	15.192.0.0	15.255.255.255	255.192.0.0	11111111.11000000.00000000.00000000	4194304
15.222.0.0/11	11	15.222.0.0	15.255.255.255	255.224.0.0	11111111.11100000.00000000.00000000	2097152
15.192.0.0/12	12	15.192.0.0	15.207.255.255	255.240.0.0	11111111.11110000.00000000.00000000	1048576
15.200.0.0/13	13	15.200.0.0	15.207.255.255	255.248.0.0	11111111.11111000.00000000.00000000	524288
15.200.0.0/14	14	15.200.0.0	15.203.255.255	255.252.0.0	11111111.11111100.00000000.00000000	262144
15.202.0.0/15	15	15.202.0.0	15.203.255.255	255.254.0.0	11111111.11111110.00000000.00000000	131072
15.203.0.0/16	16	15.203.0.0	15.203.255.255	255.255.0.0	11111111.11111111.00000000.00000000	65536
15.203.128.0/17	17	15.203.128.0	15.203.255.255	255.255.128.0	11111111.11111111.10000000.00000000	32768
15.203.192.0/18	18	15.203.192.0	15.203.255.255	255.255.192.0	11111111.11111111.11000000.00000000	16384
15.203.224.0/19	19	15.203.224.0	15.203.255.255	255.255.224.0	11111111.11111111.11100000.00000000	8192
15.203.224.0/20	20	15.203.224.0	15.203.239.255	255.255.240.0	11111111.11111111.11110000.00000000	4096
15.203.232.0/21	21	15.203.232.0	15.203.239.255	255.255.248.0	11111111.11111111.11111000.00000000	2048
15.203.232.0/22	22	15.203.232.0	15.203.235.255	255.255.252.0	11111111.11111111.11111100.00000000	1024
15.203.232.0/23	23	15.203.232.0	15.203.233.255	255.255.254.0	11111111.11111111.11111110.00000000	512
15.203.233.0/24	24	15.203.233.0	15.203.233.255	255.255.255.0	11111111.11111111.11111111.00000000	256
15.203.233.0/25	25	15.203.233.0	15.203.233.127	255.255.255.128	11111111.11111111.11111111.10000000	128
15.203.233.64/26	26	15.203.233.64	15.203.233.127	255.255.255.192	11111111.11111111.11111111.11000000	64
15.203.233.64/27	27	15.203.233.64	15.203.233.95	255.255.255.224	11111111.11111111.11111111.11100000	32
15.203.233.64/28	28	15.203.233.64	15.203.233.79	255.255.255.240	11111111.11111111.11111111.11110000	16
15.203.233.72/29	29	15.203.233.72	15.203.233.79	255.255.255.248	11111111.11111111.11111111.11111000	8
15.203.233.72/30	30	15.203.233.72	15.203.233.75	255.255.255.252	11111111.11111111.11111111.11111100	4
15.203.233.74/31	31	15.203.233.74	15.203.233.75	255.255.255.254	11111111.11111111.11111111.11111110	2
15.203.233.75/32	32	15.203.233.75	15.203.233.75	255.255.255.255	11111111.11111111.11111111.11111111	1

Subnetting for Experts

Whenever an IP address range is split into a “subnet”, the first address (usually but not necessarily the “.0”) can’t be used. The last address (usually but not necessarily the “.255”) is the Broadcast IP – which therefore also can’t be used in a device. Every “split” therefore “costs” 2 usable IP addresses.

IP Subnet	Subnet Mask	Subnet Mask in binary	Usable IP Address Range		Hosts	“Broadcast”
10.99.0.0 / 16	255.255.0.0	11111111.11111111.00000000.00000000	10.99.0.1	10.99.255.254	65534	10.99.255.255
10.99.23.0 / 24	255.255.255.0	11111111.11111111.11111111.00000000	10.99.23.1	10.99.23.254	254	10.99.23.255
10.99.22.0 / 23	255.255.254.0	11111111.11111111.11111110.00000000	10.99.22.1	10.99.23.254	510	10.99.23.255
10.99.23.0 / 25	255.255.255.128	11111111.11111111.11111111.10000000	10.99.23.1	10.99.23.126	126	10.99.23.127
10.99.23.128 / 25	255.255.255.128	11111111.11111111.11111111.10000000	10.99.23.129	10.99.23.254	126	10.99.23.255
10.99.23.0 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.1	10.99.23.2	2	10.99.23.3
10.99.23.4 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.5	10.99.23.6	2	10.99.23.7
10.99.23.8 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.9	10.99.23.10	2	10.99.23.11
…	…	…	…	…	…	…
10.99.23.244 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.245	10.99.23.246	2	10.99.23.247
10.99.23.248 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.249	10.99.23.250	2	10.99.23.251
10.99.23.252 / 30	255.255.255.252	11111111.11111111.11111111.11111100	10.99.23.253	10.99.23.254	2	10.99.23.255

What is the Subnet Mask Used For?

In actual usage, the subnet mask only has one purpose:

How can I (as a network device) determine whether my target host is:

- on the same subnet as me (so I’ll use Layer 2)
  - Do an ARP using local broadcast MAC to ask who has the IP I want to talk to
  - Send an Ethernet frame / IP packet directly to that MAC
- or is on a different subnet (OK, I’ll use Layer 3).
  - Lookup my route table to find out which local router (aka Gateway) I should aim at
  - Do an ARP using local broadcast MAC to ask who has that gateway IP
  - Send an Ethernet frame / IP packet directly to that MAC (which I know is a router)
  - I expect that local router to interpret the IP address information and forward the IP packet onwards, in the proper direction towards the destination

Is the Destination on My Subnet?

Local subnet	Mask (binary)	Mask (dotted decimal)
192.168.1.0 /24	11111111.11111111.11111111.00000000	255.255.255.0

My IP address	192.168.1.48	11000000.10101000.00000001.00110000	
Mask		11111111.11111111.11111111.00000000	
Logical “AND”		11000000.10101000.0000**0001**.00000000	
Destination IP 1	192.168.1.132	11000000.10101000.00000001.10000100	
Mask		11111111.11111111.11111111.00000000	
Logical “AND”		11000000.10101000.0000**0001**.00000000	Same
Destination IP 2	192.168.12.32	11000000.10101000.00001100.00110000	
Mask		11111111.11111111.11111111.00000000	
Logical “AND”		11000000.10101000.0000**1100**.00000000	Different

Is the Destination on My Subnet?

Local subnet	Mask (binary)	Mask (dotted decimal)
192.168.1.0 **/20**	11111111.11111111.11110000.00000000	255.255.**240**.0

My IP address	192.168.1.48	11000000.10101000.00000001.00110000	
Mask		11111111.11111111.11110000.00000000	
Logical “AND”		11000000.10101000.00000000.00000000	
Destination IP 1	192.168.1.132	11000000.10101000.00000001.10000100	
Mask		11111111.11111111.11110000.00000000	
Logical “AND”		11000000.10101000.00000000.00000000	Same
Destination IP 2	192.168.12.32	11000000.10101000.00001100.00110000	
Mask		11111111.11111111.11110000.00000000	
Logical “AND”		11000000.10101000.00000000.00000000	Same

IP Routing

A Router works at the IP level. Its job is to “know” which direction to send packets towards their destination IP address. If they don’t explicitly know the direction of a particular IP subnet, they are usually configured with a catch-all “default route”.

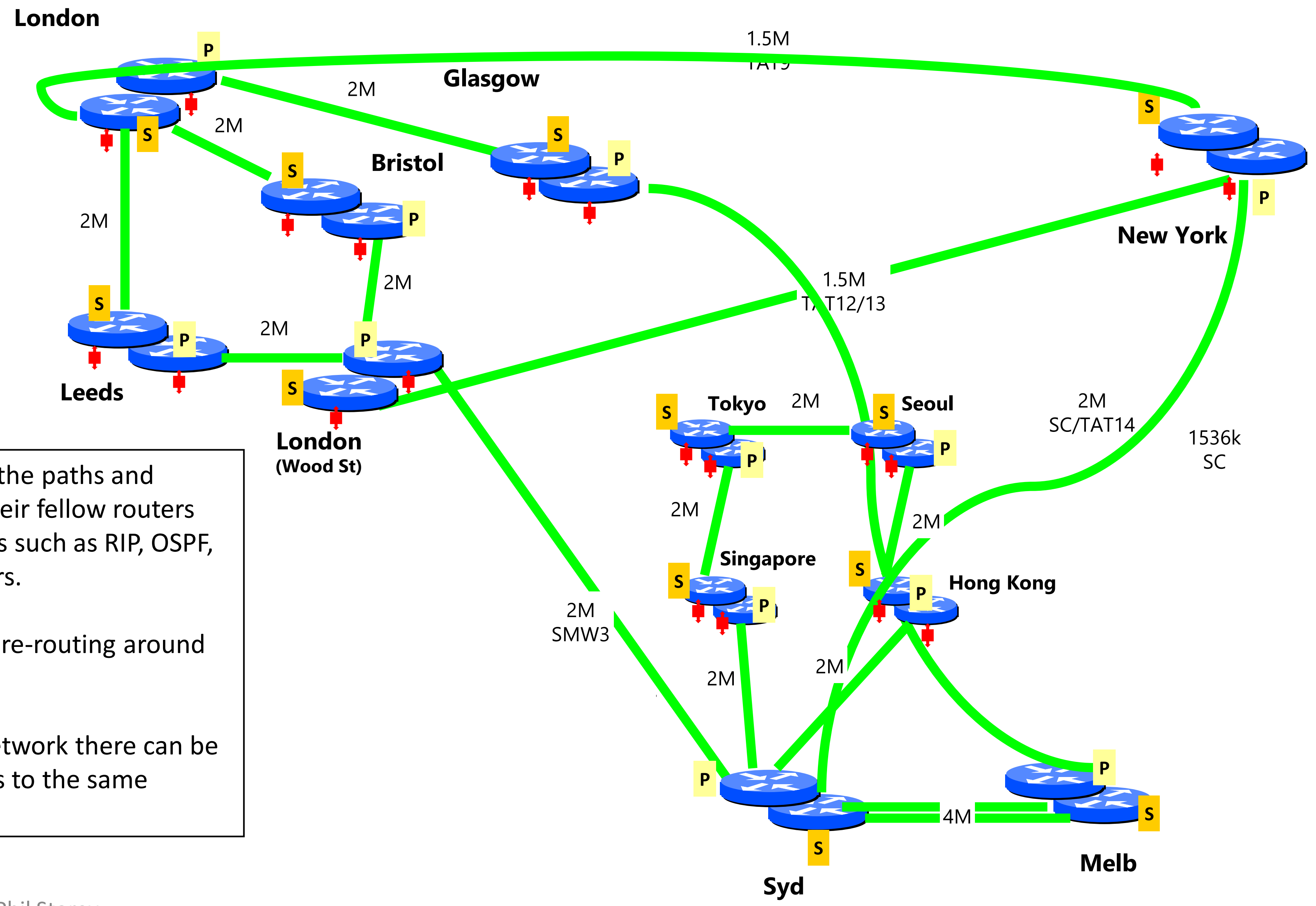
In fact, all devices need to “know” at least one local router (with an IP address on their LAN).
All devices have an internal “route table” that has to be populated somehow.

Originally, the terminology for a router was “gateway”. So you will still see the term “default gateway” commonly used.

At least one “default gateway” IP address is served up as part of the usual DHCP request that devices use to get their IP address.

Some of the early competition for TCP/IP included:-
- XNS from Xerox,   SPX/IPX from Novell,   NetBIOS / NetBEUI from Microsoft,   AppleTalk
- And arguably even SNA from IBM.

Routing Can Be Complex



Routers can "learn" the paths and destinations from their fellow routers via Routing Protocols such as RIP, OSPF, BGP, EGRP and others.

This allows dynamic re-routing around failures.

In a very complex network there can be many different paths to the same destination.

"Default Route" : Linux vs French Roads

```
$ ip route
   default via 10.0.0.1 dev wlp3s0 proto static metric 600 \
   10.0.0.0/24 dev wlp3s0 proto kernel scope link src 10.0.0.73 metric 600 \
   10.0.1.0/24 dev lxcbr0 proto kernel scope link src 10.0.1.1 \
   169.254.0.0/16 dev docker0 scope link metric 1000 linkdown \
   172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown \
   192.168.122.0/24 dev virbr0 proto kernel scope link src 192.168.122.1
```

https://ubuntu.com/core/docs/networkmanager/routing-tables

Windows: “ipconfig /all”

```
Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) Wireless-N 7260
   Physical Address. . . . . . . . . : 80-86-F2-7A-26-E1
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::eff5:bf4c:8a26:8067%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, 26 June 2024 2:34:25 PM
   Lease Expires . . . . . . . . . . : Thursday, 27 June 2024 1:34:25 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 142640882
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-65-6C-F2-C4-34-6B-04-C9-F9
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Addressing Summary

IPv4 addresses are 32-bits long, represented in “dotted decimal” notation and can be thought of as being split into 2 components:

Network or Subnet -> 192.168.|0.21 <- Host/Node Address within subnet.

The position of the split is determined by the “Subnet Mask” or “Slash”,

which in this example are 255.255.255.0 or “/24”.

Ethernet (and WiFi) MAC addresses are 48-bits long, represented in hexadecimal and can also be thought to have 2 components:

Vendor -> 80-86-F|2-7A-26-E1 < - Uniquely assigned to product by vendor.

In this example, 80-86-F2 is Intel.

IPv6 addresses are 128-bits long, represented as eight groups of four hexadecimal digits, each group representing 16 bits. The groups are separated by colons (:).

Example -> 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Phil Storey

Phil@NetworkDetective.com.au

www.NetworkDetective.com.au

au.linkedin.com/in/philipstorey3

@PhilStorey24

www.youtube.com/c/NetworkDetective

ask.wireshark.org: @philst

Networking:
Layer 2 vs Layer 3

SLUG Meetup

Phil Storey

28 June 2024

Download the Presentation PDF here:
http://www.networkdetective.com.au/PDFs/SLUG-Meetup-2024-06-28.pdf