Unix/Linux Networking Introduction

Mike Harris

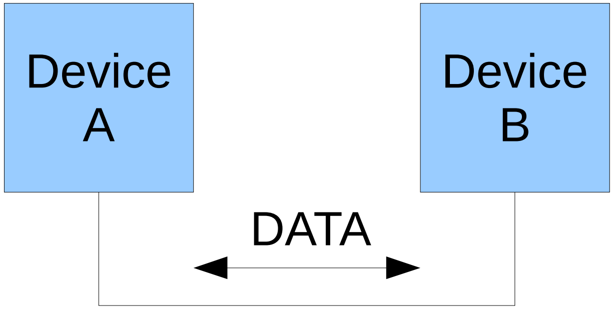
Lean Bytes

Workshop Goals

- To give a broad understanding of network concepts and where different acronyms, tools & devices fit into it.
- Taking this understanding to help one know where to look for more information, diagnose issues and what to look for.

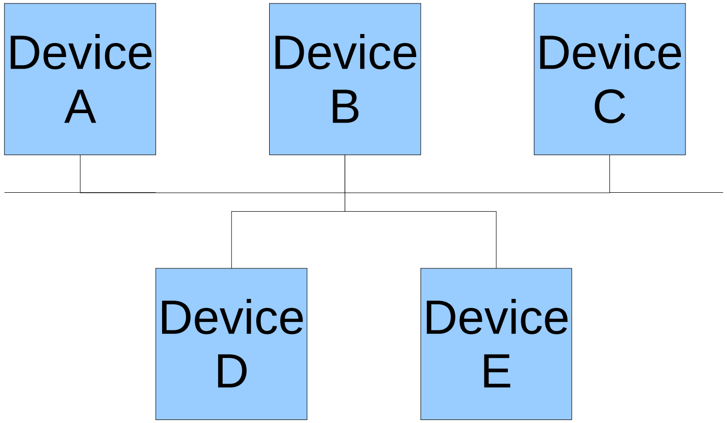
Network concepts

- A computer network consists of one or more computers connected together and able to share data between them.
- The simplest network can be two PCs connected via a serial cable – e.g. Apple's LocalTalk.



Local Area Networks (LANs)

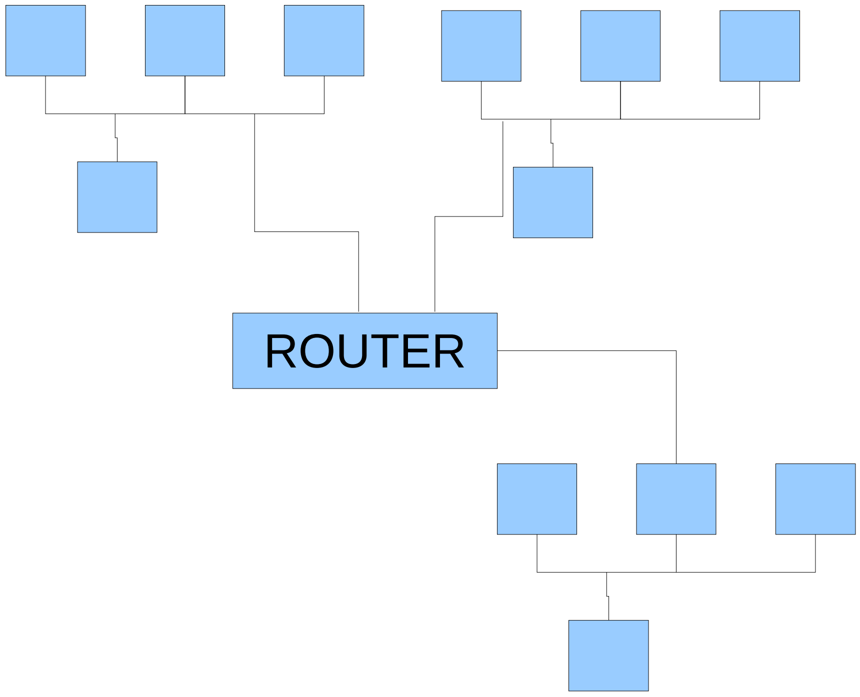
- A LAN is a simple network of computers and is common in most organisations.
- It may feature more than one network *segment.*
- It will probably only be in a *class C IP address range.*
- Class C is X.Y.Z.0



A Local Area Network
(using bus topology)

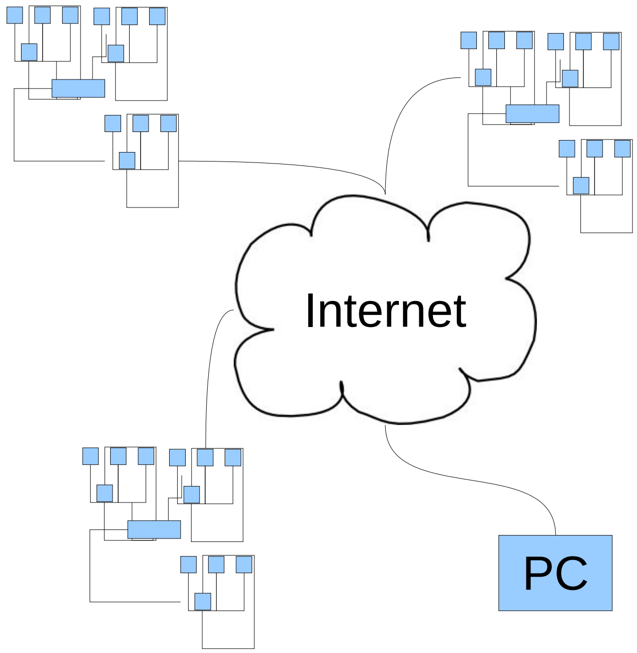
Metropolitan Area Networks (MANs)

- These are (often) city-wide networks of interconnected LANs (network segments)
- The interconnected links might be over fibre-optic, copper-wire, wifi or microwave connexions.
- Address range is A or B.
- Class A is X.0.0.0 and class B is X.Y.0.0



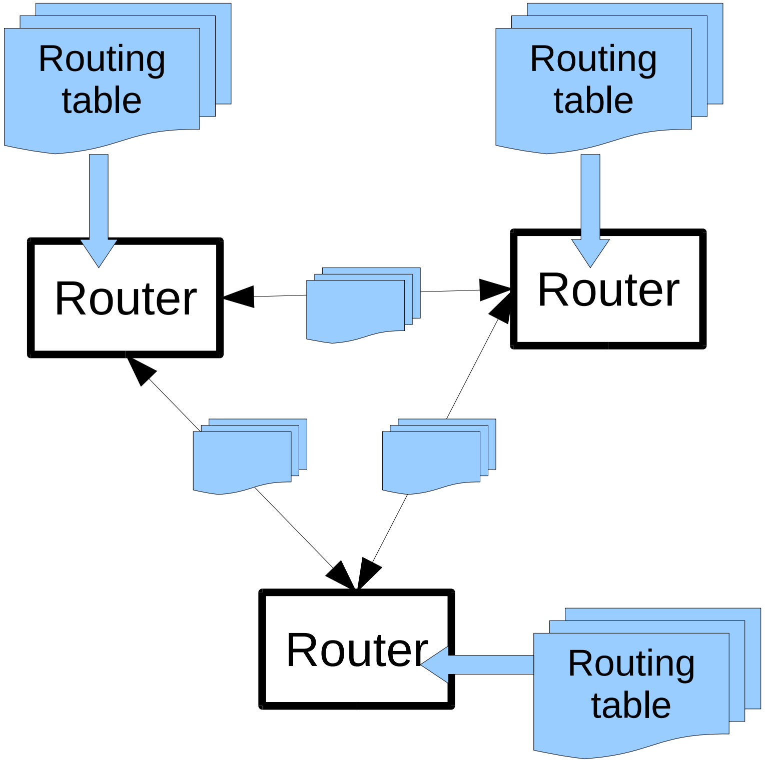
Wide Area Networks (WANs)

- This is a network of interconnected LANs.
- Large multi-national organisations will have WANs.
- Address ranges can be class B upwards.
- The biggest example of a WAN is the Internet, but JANET is another.



Open Shortest Path First (OSPF)

- We use a suite of routing software called Quagga. As well as OSPF, Quagga also provides support for RIP & BGP.
- OSPF is an **Interior Gateway Protocol**.
- Routers configured with OSPF that are in the same **area** (or connected to the backbone area) exchange their routing tables with each other automatically, which saves on the manual process of doing this using ifconfig and route.
- This is very useful in a network such as BW where there are many segments.
- The BW configuration is simple with a single **backbone area** aka **area 0.0.0.0**



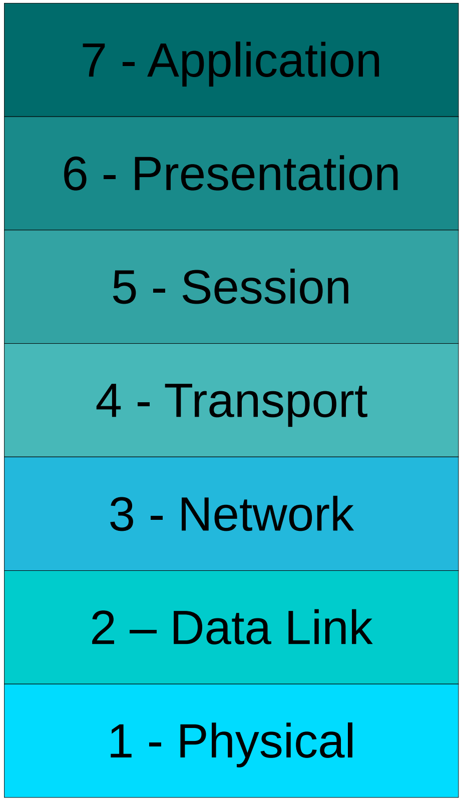
OSPF enabled routers exchanging their routing tables

Quagga is an extinct type of zebra.

http://www.quagga.net

The OSI Network Model

- This 7-layered model is a good way to understand the different *layers* of network protocols.
- TCP/IP doesn't quite fit into this model, but it's good enough for this workshop!
- There are a series of official OSI specifications called X.200



7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

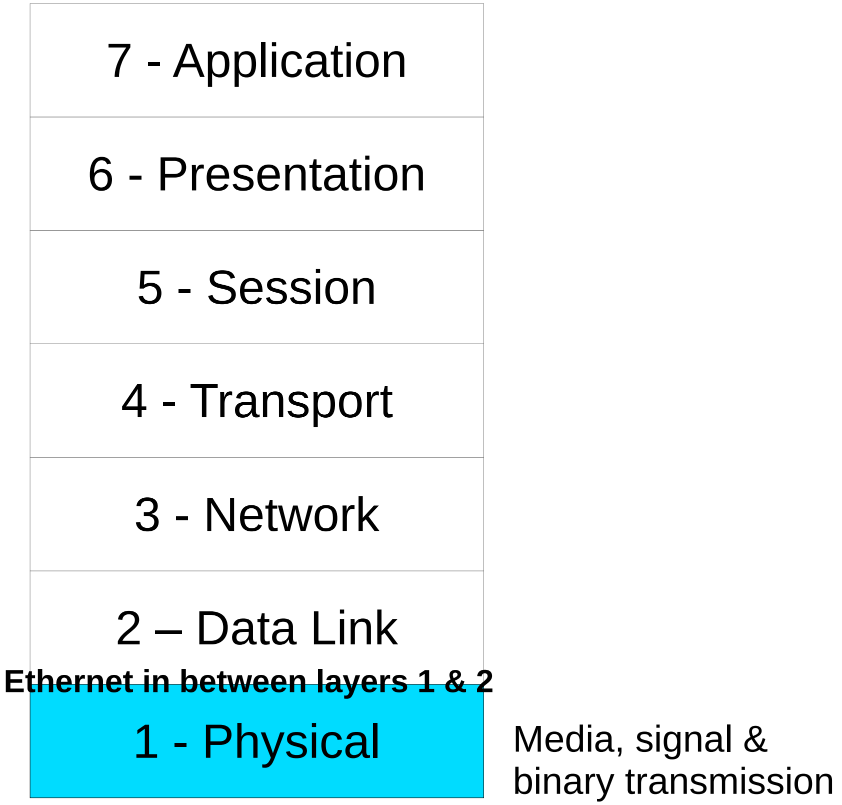
2 – Data Link

1 - Physical

http://en.wikipedia.org/wiki/OSI_model

The Physical Layer (1)

- Defines the physical and electrical connexion, via some form of medium.
- This medium could be copper wire, fibre-optic cable, coax, firewire, USB, air (wifi, bluetooth) or even pigeon!
- Specification could cover pin layout, voltages, cable specs, hubs, repeaters, network adapters, bit rate, simplex, duplex & network topology.
- Hubs operate at layer 1.
- Some examples of standards are RS-232, RJ-45, 10BASE-T, 10BASE2, 10BASE5, RG8 and V.92.



7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network

2 – Data Link

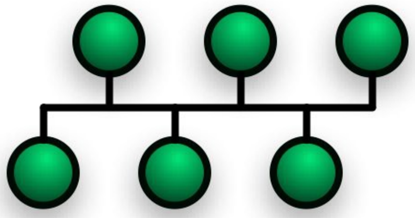
Ethernet in between layers 1 & 2

1 - Physical

Media, signal & binary transmission

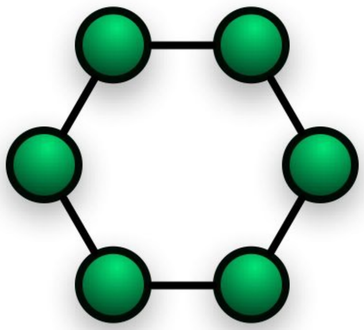
http://en.wikipedia.org/wiki/Physical_layer

The Physical Layer (1)
A quick aside on different Network Topologies



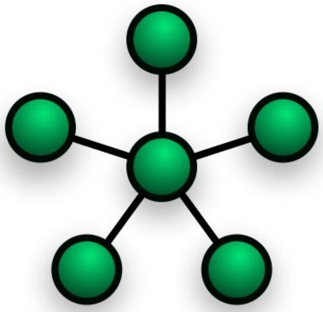
Bus

10BASE-2 - old fashioned coax *thinnet* networks.



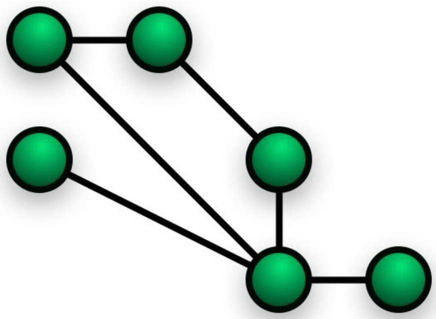
Ring

Expensive & reliable networks like Token Ring & FDDI



Star

10BASE-T – modern Ethernet networks
& wifi networks.

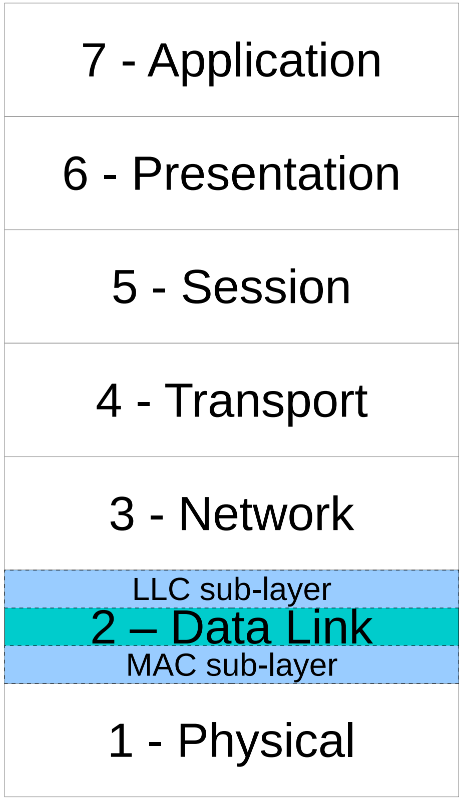


Mesh

Wifi & Bluetooth networks.

The (Data) Link Layer (2)

- Defines the means by which data is transferred between network devices and can correct errors that occur in the physical layer.
- The Media Access Control (MAC) sub-layer manages the interaction of devices and the Logical Link & Control (LLC) sub-layer provides for multiplexing of multiple layer 3 protocols, such as IP & IPX.
- Bridges operate at layer 2.
- Standards & protocols are IEEE 802.3, 802.2 (LLC) & 802.11, CSMA/CD, ARP, PPP & HDLC



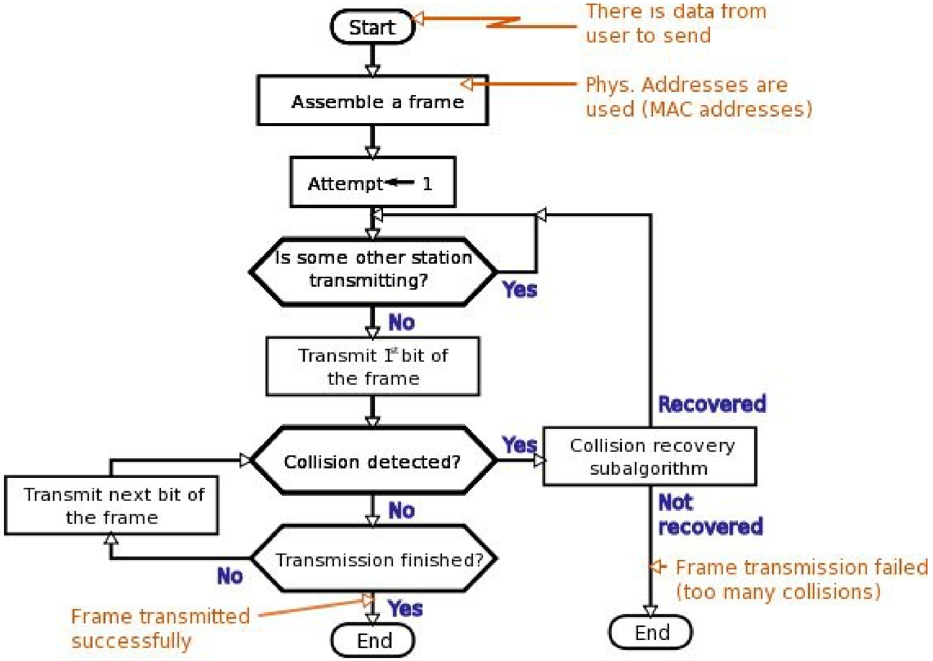
Physical addressing

Media, signal & binary transmission

http://en.wikipedia.org/wiki/Data_link_layer

The Data Link Layer (2)
A quick aside on Medium Access Control (MAC)

- The Medium Access Control (MAC) layer 2 sub layer is a protocol that controls how devices gain access to the medium of the physical layer.
- For Ethernet the **Carrier Sense Multiple Access With Collision Detection** (CSMA/CD) is the MAC protocol used.
- Carrier Sense means it listens for a carrier wave before trying to send.
- Multiple Access means simply that multiple devices can used the same medium.
- Collision Detection – means that the protocol can detect collisions and take action on them: e.g. wait and resend.



Start
There is data from user to send
Assemble a frame
Phys. Addresses are used (MAC addresses)
Attempt ← 1
Is some other station transmitting?
Yes
No
Transmit 1st bit of the frame
Recovered
Collision detected?
Yes
Collision recovery subalgorithm
Transmit next bit of the frame
No
Not recovered
Transmission finished?
No
Frame transmission failed (too many collisions)
Frame transmitted successfully
Yes
End
End

The CSMA/CD algorithm

The Data Link Layer (2)
A quick aside on MAC addresses

- A MAC address is a unique serial number assigned to an item of network hardware at the time of it's manufacture and is analogous to a street address.
- Enables traffic to be routed to the device using protocols such as the Address Routing Protocol (ARP)
- MAC addresses are normally in 48-bit hexadecimal notation written with semi-colon or hyphen separators, or Cisco use dots!
- Used in Ethernet, WLANs, Bluetooth, Token Ring, Fibre Channel, Serial Attached SCSI, FDDI, ATM

00-17-f2-db-b6-5e

00:1b:63:06:c9:c5

Cisco format 001.7f2.dbb.65e

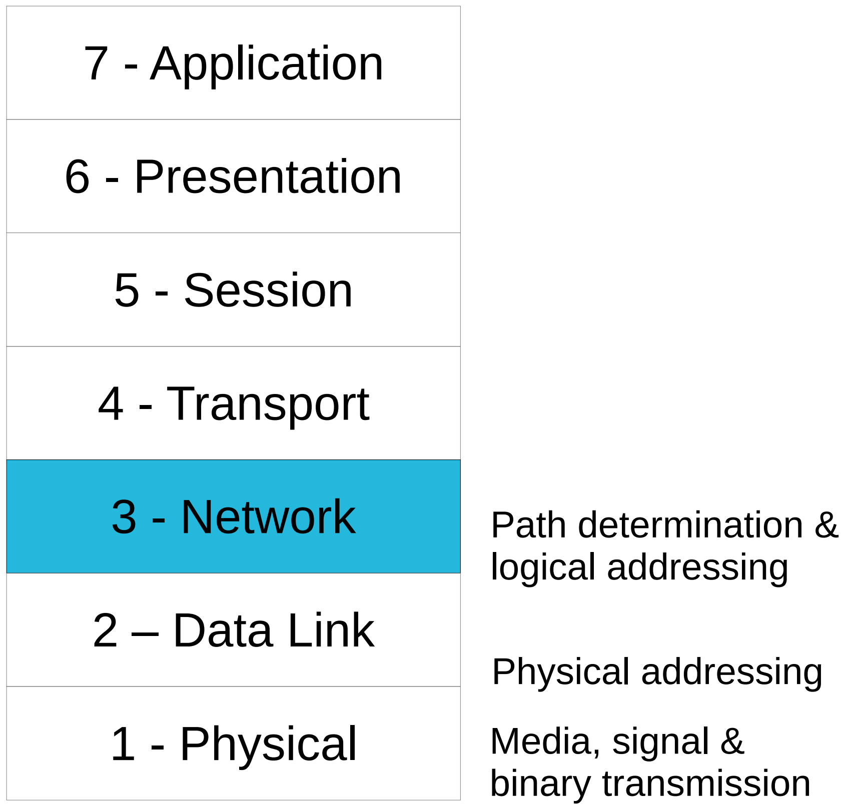
2^48 = 281,474,976,710,656 possible MAC addresses!
This is estimated to be enough to last until 2100

But just in case IPv6 & Firewire use newer 64-bit MAC addresses.

```
snooker:~ adelayde$ arp -a
? (192.168.100.1) at 0:1a:70:a0:77:72 on en1 ifscope [ethernet]
? (192.168.100.103) at 0:1a:73:67:de:4e on en1 ifscope [ethernet]
? (192.168.100.255) at ff:ff:ff:ff:ff:ff on en1 ifscope [ethernet]
```

The Network (IP) Layer (3)

- Probably the best known layer, it provides the means of delivering variable length data from source to destination and provides for a quality of service.
- The best known of all layer 3 protocols is the Internet Protocol (IP), but others are out there such as Novell Netware's IPX and Microsoft's NetBIOS Frames (NBF).
- Routers operate at layer 3.
- Some examples of protocols at this level are ICMP, IP (v4 & v6), IPSec and OSPF.



7 - Application

6 - Presentation

5 - Session

4 - Transport

3 - Network — Path determination & logical addressing

2 – Data Link — Physical addressing

1 - Physical — Media, signal & binary transmission

http://en.wikipedia.org/wiki/Network_layer

The Network Layer (3)
A quick aside on IP addresses

- IPv4 addresses are in dotted decimal notation:
  - Class A addressing allows for up to 16,777,216 addresses: 10.0.0.0
  - Class B addressing allows for 65,536 addresses: 192.168.0.0
  - Class C addressing allows for 256 addresses: 192.168.100.0

- The network address is a special address that marks the bottom of the set of available addresses: 192.168.1.0.
- Broadcast address is a special address that marks the top of the set of available addresses. Pinging this address will ping all addresses in the range: 192.168.1.255.
- The network mask determines how many addresses are available in the range: 255.255.255.0. The / notation is the number of binary bits set in the network mask counting from the left: so for 255.255.255.0, 11111111.11111111.11111111.00000000 is 24 bits, so we write /24.

The Network Layer (3)
A quick aside on subnet masks & the / notation

```
10.100.128.16 – 0000 1010 . 0110 0100 . 1000 0000 . 0001 0000
```

10.100.128.17 – 0000 1010 . 0110 0100 . 1000 0000 . 0001 0001

Try pinging 10.100.128.18

```
     10          100          128          18
0000 1010 . 0110 0100 . 1000 0000 . 0001 0010

    255         255          255          252
1111 1111 . 1111 1111 . 1111 1111 . 1111 1100    /30 bits set

0000 0000 . 0000 0000 . 0000 0000 . 0000 0010    non-zero = yes!
```

Try pinging 10.100.128.20

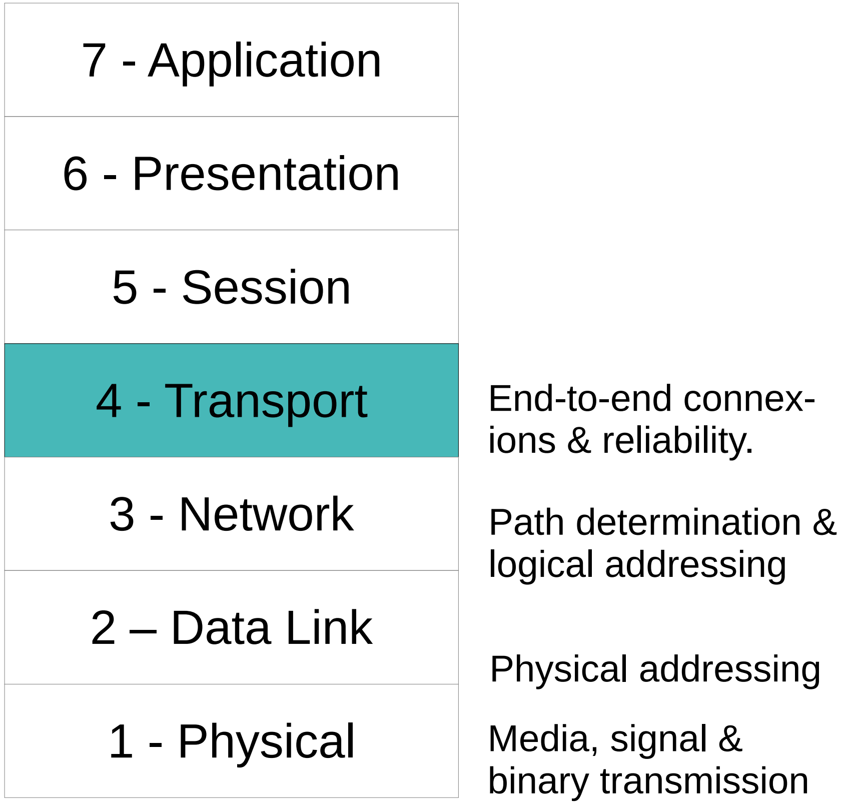
```
     10          100          128          20
0000 1010 . 0110 0100 . 1000 0000 . 0001 0100

    255         255          255          252
1111 1111 . 1111 1111 . 1111 1111 . 1111 1100

0000 0000 . 0000 0000 . 0000 0000 . 0000 0000    zero = no!
```

The Transport Layer Layer (4)

- The transport layer provides reliable and invisible data transfer services between end users to the upper layers using segmentation, flow control and error control.
- The best known of all layer 4 protocols is the Transport Control Protocol (TCP) and is used where reliability is the key, such as email, web, FTP, ssh.
- User Datagram Protocol (UDP) is another major protocol and is often used where where speed over accuracy is important: e.g. streaming, Second Life, World of Warcraft, DNS, VoIP, TFTP
- Both UDP and TCP provide *ports* in order to multiplex different session layer services.

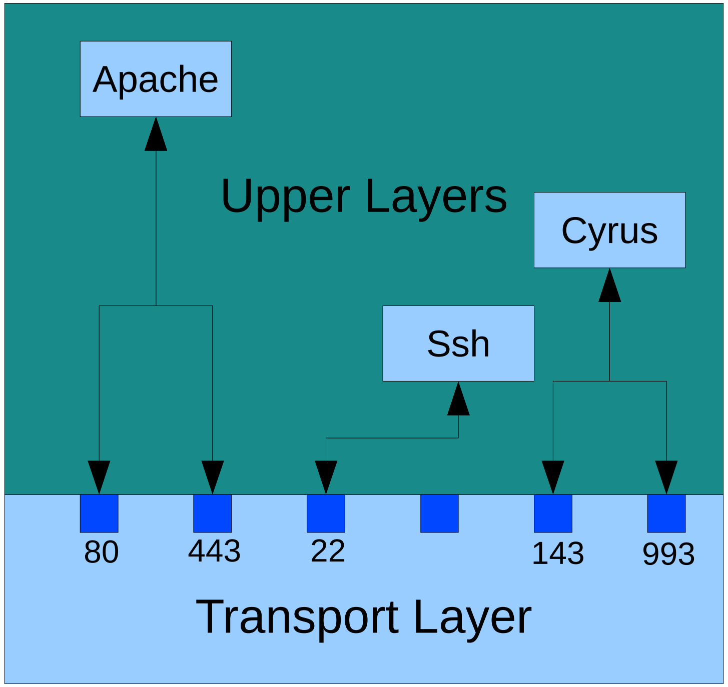


7 - Application	
6 - Presentation	
5 - Session	
4 - Transport	End-to-end connex-ions & reliability.
3 - Network	Path determination & logical addressing
2 – Data Link	Physical addressing
1 - Physical	Media, signal & binary transmission

http://en.wikipedia.org/wiki/Transport_layer

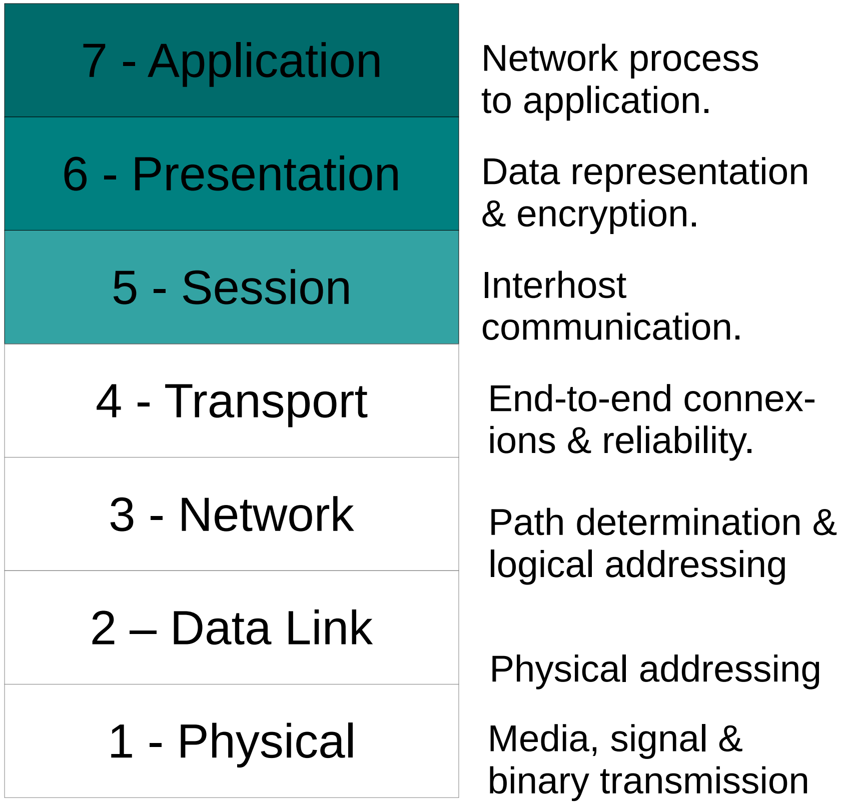
The Transport Layer (4)
A quick aside on TCP and UDP ports

- Both UDP and TCP protocols work to provide *ports* by which services from the upper three layers can communicate with the lower layers.
- There are 65,535 different ports available and ports numbered below 1024 are restricted to certain privileged user accounts (root, wheel, etc).
- Session, Presentation and Application layer services *bind* to the *ports.*
- The best source for a list of ports and services is /etc/services. Here's some common ports: 21 (ftp), 22 (ssh), 25 (smtp), 53 (dns), 80 (http), 110 (pop3), 115 (sftp), 143 (imap), 443 (https), 993 (imaps), 995 (pop3s).



The top layers (5-7)

- The OSI model goes on to define three further layers: the Session, the Presentation and the Application.
- The Session layer establishes, manages & terminations connexions in dialogues between computers and contains protocols such as scp, ssh, RPC & NetBIOS.
- The Presentation layer provides independence from differences in data representation (e.g. encryption or encoding) and contains protocols such as MIME, XDR, SSL & TLS.
- The Application layer is the one closest to the user and contains protocols such as SMB, POP3, IMAP, RTSP, HTTP, FTP, SMTP & SNMP.

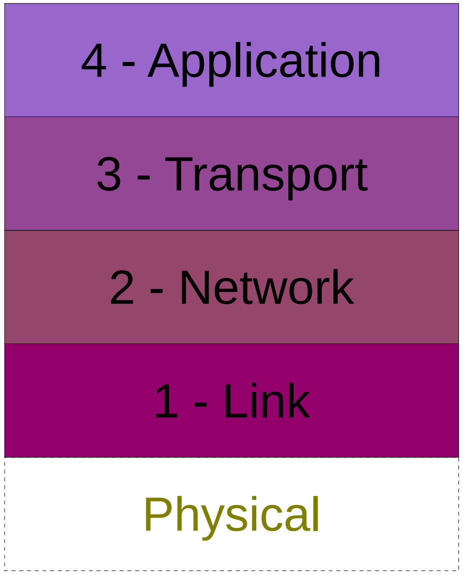


7 - Application	Network process to application.
6 - Presentation	Data representation & encryption.
5 - Session	Interhost communication.
4 - Transport	End-to-end connexions & reliability.
3 - Network	Path determination & logical addressing
2 – Data Link	Physical addressing
1 - Physical	Media, signal & binary transmission

http://en.wikipedia.org/wiki/Session_layer
http://en.wikipedia.org/wiki/Presentation_layer
http://en.wikipedia.org/wiki/Application_layer

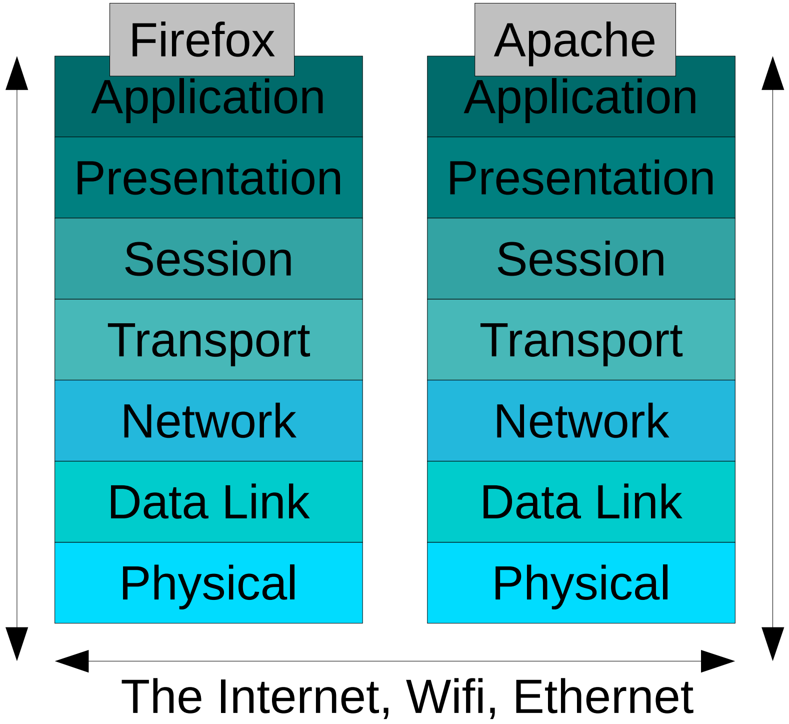
The TCP/IP four-layer model

- As mentioned at the beginning, the OSI model doesn't exactly fit the most commonly used network protocol suite, called (somewhat erroneously) TCP/IP.
- It doesn't define the physical layer, just layers to do with the transport of data over a network.
- The Link, Network & Transport layers very closely match the same ones in the OSI model, as we have seen.
- The Application layer encompasses the Session, Presentation & Application layers and makes life a lot less complicated.
- As this isn't a standard model, like OSI, it can vary, sometimes the physical layer is included to make a 5 layer model.



So what does all this mean?

- If you're diagnosing a problem with the network start at the bottom and work to the top.
- So, test the cables & the network card first; then test the IP address and routing (ping); then test the name resolution; and finally test the web server.



Some useful UNIX network tools

Command line configuration utilities

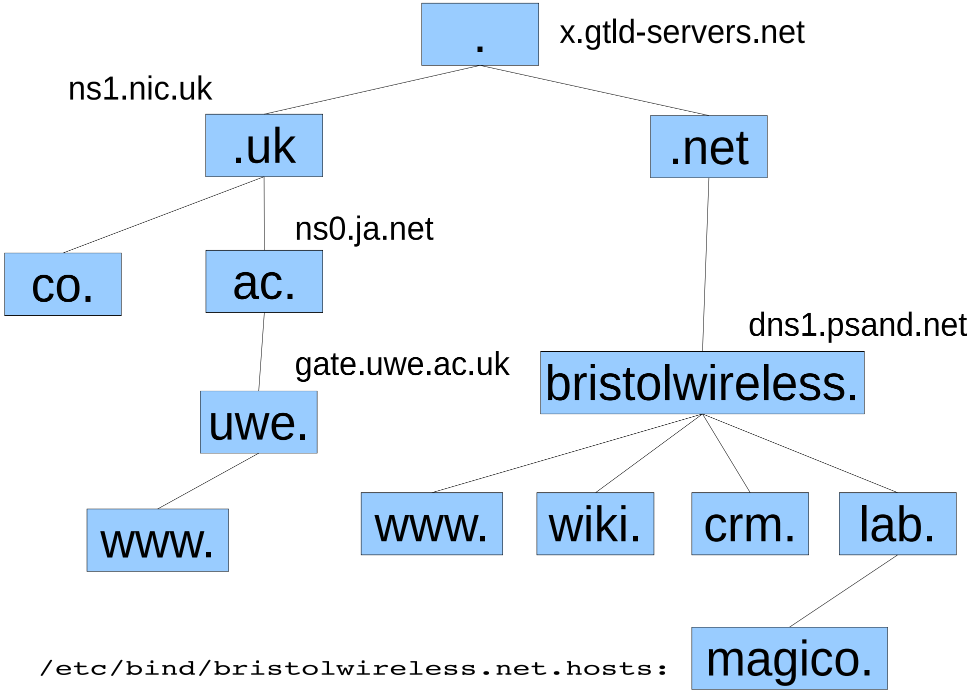
- arp
- iwconfig
- ifconfig
- nmap
- route
- nestat
- ping & traceroute

Scanning & Monitoring tools

- nload
- smokeping
- mrtg
- cacti
- nagios
- nessus
- nc

Domain Name Service (DNS)

- Application layer protocol connecting to UDP port 53
- Hierarchical tree structure.
- Special servers called root servers manage the top of the tree.
- Each subsequent level DNS is controlled by authoritative server.
- Under BIND, a DNS record is just a flat (hosts) file.
- Common record types are NS, MX, A, TXT and PTR.
- Useful tools: whois, ping & dig



```
/etc/bind/bristolwireless.net.hosts:

$ttl 38400
bristolwireless.net.  IN    SOA  dns1.psand.net
hostmaster.psand.net. (
                2009101601
                10800
                3600
                604800
                38400 )

           IN   NS    dns1.psand.net.
           IN   NS    dns2.psand.net
           IN   MX    10   mango.psand.net.
            IN    MX   20  chutney.psand.net.

ns                         IN   CNAME strummer
www                        IN   A     194.164.9
wiki                       IN   A     194.164.9
```

Secure Shell (ssh)

- Secure shell gives command line (console) access over a secure (encrypted) connexion to a remote system.
- It is a replacement for telnet, uses TCP port 22 and is an Application Layer protocol.
- Uses several methods of authentication, password and public key. We use both of these.
- Switch **-A** does authentication forwarding.
- Switch **-X** does X11 forwarding.
- Switch **-L** does port forwarding.
- Variants of the command include 'scp' and 'sftp'

Common network files under Unix

- /etc/host.conf
- /etc/hosts
- /etc/resolv.conf
- /etc/named.conf & /var/named/*
- /etc/dhcp/*
- /etc/sysconfig/network & /etc/sysconfig/networking/*
- /etc/sshd/sshd_config & ssh_config
- ~/.ssh/*

Thank You

07811 671 893

mike.harris@leanbytes.co.uk
http://leanbytes.co.uk
https://mbharris.co.uk
http://uk.linkedin.com/in/mbharris
https://github.com/mikebharris/

Lean Bytes