## Systems and Devices 2 (Network) Lec 2b: Application Layer

#### Before we get started ...

- We considered the top level view of two file transfer protocols: HTTP, FTP and looked at SMTP.
  - How did your research into SMTP go?
    - Not expecting you to be an expert, more of an exercise to see if you start to understand the ideas, the structure of a protocol.
- We now need to consider how the Internet is organised e.g. how we identify different machines
  - Domain Name System (DNS): mapping domain names to IP
  - DNS servers: Berkeley Internet Name Domain (BIND)
  - DNS tools: Domain Information Groper (DIG)
- Then consider how IP addresses are allocated
  - Static or dynamic IP.
  - Dynamic Host Configuration Protocol (DHCP)

University of York : M Freeman 2024

#### Internet protocol stack

#### Application layer

Application

Transport

Network

Link

Physical

 Need to consider house keeping protocols e.g. to identify and allocate network addresses, or simply operate the

computer.

- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Network Time Protocol (NTP)
- Transport
- Network
- Link
- Physical

#### Host and domain names

 mike@mike-Aspire /etc

 File
 Edit View Search Terminal Help

 127.0.0.1
 localhost

 127.0.1.1
 mike-Aspire

 192.168.0.254
 raspberrypi

 144.32.50.115
 pi-time

 144.32.50.6
 bug-press



pi1.desk85.lan .com .org .net .int .edu .gov .mil .uk .fr .be .de .ca .us .aq ... .bank .airforce .eurovision ... https://www.iana.org/domains/root/db

#### osts" 14 lines, 301 characters

- The internet's phone box
  - How do we organise it?
    - Broken down into domains based on the location (organisational / geographical) of the computer.
    - People identify hosts by their hostnames and domains, networks use IP addresses. Need a way to map between the two.
  - One solution is to maintain a single, centralized host table e.g. /etc/hosts, mapping hostnames to IP an address. This works, but by the early 1980s this approach was becoming unmanageable. University of York : M Freeman 2024

## Host and domain names

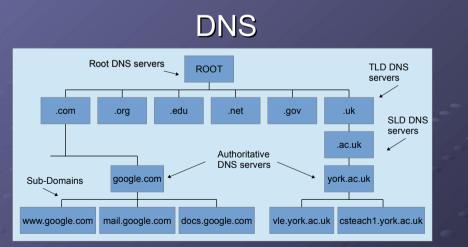


- The Internet Assigned Numbers Authority (IANA) oversees global allocation of IP and AS numbers to Regional Internet Registries (RiR)
- Also maintains the top-level domain name servers in association with Internet Corporation for Assigned Names and Numbers (ICANN)

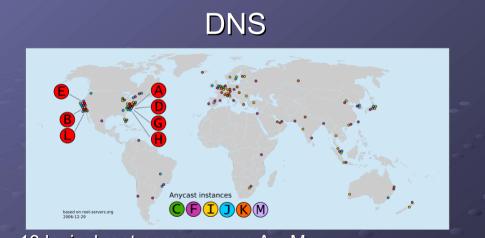
University of York : M Freeman 2024

#### DNS

- Domain Name System Protocol
  - RFC 1035: https://tools.ietf.org/html/rfc1035
  - Domain Name System (DNS) protocol created in 1983
    - Distributed database, replicated servers
      - Improves reliability (SPF), reduces network load (quires), reduces delays (location) and processing load (updates)
  - Client-Server model, default port 53.
  - Communicates across UDP links
  - Used extensively by other application layer protocols
     Uniform Resource Locator (URL), or web address
  - Organised as:
    - Root DNS servers
    - Top-level domain (TLD) DNS servers
    - Authoritative DNS servers
    - Local DNS server University of York : M Freeman 2024



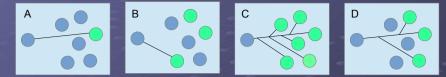
- TLD and Authoritative servers: vle.york.ac.uk
  - https://www.iana.org/domains/root/db
    - SOA: Start of authority records for specific zones
       University of York : M Freeman 2024



#### 13 logical root name servers A – M

- a.root-servers.net m.root-servers.net ( https://root-servers.org )
- Have to start somewhere, top level uses "well know" ip addresses.
   If changes need to be made you still have 12 more until updated

#### Quick Quizzz



- Q : match the above pictures to connection types below.
  - Unicast : one-to-one association between hosts
  - Broadcast : one-to-all association, packet routed to all possible hosts on network
  - Multicast : one-to-many-of-many, packet routed to select hosts.
  - Anycast : one-to-one-of-many association, packet routed to any single host of a group of potential hosts.
- Q : how are connections to the root DNS servers managed? As of Aug 2024: 1865 actual root DNS servers?

University of York : M Freeman 2024

#### DNS

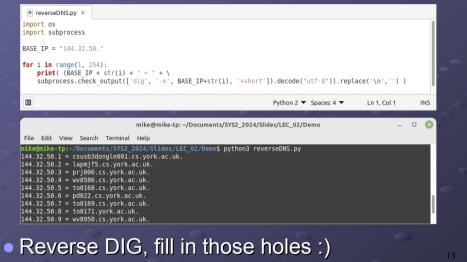
- A DNS query can contain up to 253 characters
  - A domain names consists of one or more labels
  - A label may contain 0 to 63 characters
     Root has 0 characters
  - In theory can contain up to 127 sub-domains i.e. single letter labels, but typical will be a lot less e.g. 3 to 4.
    - [char].[char].[char].[char]......
    - 63[char].63[char].63[char].61[char]
  - Fully qualified domain names: defines all levels from top to bottom e.g. "csteach0.york.ac.uk."
    - Trailing "." is for the root DNS server
- Can create an alias for a domain name i.e. map to a canonical name (CNAME)
  - Multiple domains sharing the same IP address. University of York : M Freeman 2024

			Demo	
orf Fuddations(fine) Beneficial States of the second additional States of the second Addate Sections: Addate Sections: Second Sections: Second Sections: Second Sections: Second Sections: Second Sections: Second Sections: Second Sections: Second Sections: Second Second Sections: Second Second Sections: Second Second	ttu «Co» KARY, status; KO HRY: 1, ANDYRT: 1, MDY: 2005 1,	00000, 14: 58479         30.           3), animatify 7, 8, 400115844.: 27         5           6         1.000158994971.001.           6         1.000158994971.001.           7         5.000158994971.001.           8         1.000158994971.001.           9         1.000158994971.001.           9         1.000158994971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.00015899971.001.           9         1.000158999771.001.	<pre>Indextbookdage:</pre>	<pre>Mitchinkagine + fig prime and i fig the metal set of the prime and i end of the metal set of the prime and i end of the set of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and interaction of the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime and the prime and the prime i figst grant of the prime i figst g</pre>
		ookups	.uk, dig york.ac.uk, dig w	

COUNTING SECTION: 1 per k.w., IN         N         A           Amount SECTION: 1 per k.w., IN         IN         A         i; flags: gr rd rå; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1           Amount SECTION: 1 per k.w., IN         IN         A         iii.6 social-com.         iii.6 social-com.           Amount SECTION: 1 per k.w., IN         IN         A         iii.6 social-com.         iii.6 social-com.           Amount SECTION: 1 per k.w., IN         III. A         iii.6 social-com.         iii.6 social-com.         iii.6 social-com.           Amount SECTION: 1 per k.c.m., IN         III. A         iii.6 social-com.         iii.6 social-com.         iii.6 social-com.           Bit com., IN         III. A         III. Social-com.         III. A         iii.6 social-com.         iii.0 social-com.           Bit com., IN         III. Social-com.         III. Social-com.         GOO IN         A         109.201.135.65           Bit com., IN         A         216.239.32.18         iii. A         116.539.19.11         iii. A           Bit com., IN         A         216.239.32.18         iii. A         109.201.135.65           Bit com., IN         A         216.239.31.91.11         iii.         iii.         iii.           Bit com., IN         A         216.239.31.91.11         i	I	Demo
<pre>global options.tod ingering ard rg.google.com figs: g ard rg.google.com if get g ard rg.google.com if g ard rg ard rg.google.com if g ard rg ard r</pre>	Edt View Search Terminal Help egmike-Aspire ~ \$ dig mail.york.ac.uk	File Edit View Search Terminal Help
11. york actos.       yakar string.       yakar string.       yakar string.         yakar string.       yakar string.       yakar string.       yakar string. <tr< td=""><td>global options: «cmd doffannower, options: NERFICM, id: 11704 flags: gr aa rd ra; QUERY: 1, ANOMER: 2, AUTHONITY: 4, ADOITIONAL: 9 (flags: gr aa rd ra; QUERY: 1, ANOMER: 2, AUTHONITY: 4, ADOITIONAL: 9 (flags: gr absolute: 1, ADOITIONAL: 1, ADOITIONAL: 9 (flags: 1, ADOITION SECTION (flags: 1, ADOITION SECTION SECTION SECTION SECTION (flags: 1, ADOITION SECTION SECT</td><td>; &lt;&gt;&gt; DiG 9.10.3-P4-Ubuntu &lt;&gt;&gt; gooooooogle.com ;; global options: +cmd ;; Got answer: ;; -&gt;HEADER&lt;- opcode: QUERY, status: NOERROR, id: 28240</td></tr<>	global options: «cmd doffannower, options: NERFICM, id: 11704 flags: gr aa rd ra; QUERY: 1, ANOMER: 2, AUTHONITY: 4, ADOITIONAL: 9 (flags: gr aa rd ra; QUERY: 1, ANOMER: 2, AUTHONITY: 4, ADOITIONAL: 9 (flags: gr absolute: 1, ADOITIONAL: 1, ADOITIONAL: 9 (flags: 1, ADOITION SECTION (flags: 1, ADOITION SECTION SECTION SECTION SECTION (flags: 1, ADOITION SECTION SECT	; <>> DiG 9.10.3-P4-Ubuntu <>> gooooooogle.com ;; global options: +cmd ;; Got answer: ;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 28240
ADDITIONAL SECTION: 2003 IN A 216.239.23.18 provide com. Control Cont	ANDREE SECTOR: 1 prv 1 ac: A: geogle.com, 133 IM A 216.58.713.19 MIDENTY SECTOR: gle.com, 44073 IM M5 nr.1.google.com, gle.com, 44073 IM M5 nr.1.google.com,	;; OPT PSEUDOSECTION: ; EDMS: version:0, flags:; udp: 4096 ;; OUSTION SECTION: ;goococogle.com. IN A ;; ANSWER SECTION:
Overy time: 1 msec SerVer: 127.0.1.14551127.0.1.13 MHER: Tue Oct 13 17:04:53 BST 2020 ;; MSG SIZE rcvd: 106	_geogle.com, 62561 JN A 216.239.32.10 geogle.com, 62561 JN A 216.239.31.10 geogle.com, 62590 JN A 216.239.31.10 geogle.com, 62501 JN A 216.239.31.0 geogle.com, 62501 JN A 216.239.38.10 geogle.com, 62501 JN A 216.239.38.10 geogle.com, 62501 JN A 2801.4469.4802.331.10 geogle.com, 67725 JN AAAA 2801.4469.4802.331.10 GEOGLE.com, 67725 JN AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	;; AUTHORITY SECTION: gooocoogle.com. 86400 IN NS ns2.brainydns.com. gooocoogle.com. 86400 IN NS ns1.brainydns.com. ;; Query time: 30 msec ;; SERVER: 127.0.1.1#531127.0.1.1) ;; WHEN: Tue Oct 13.17.04535 827.2020

- Q: how many OOO's are there in Google?
  - Do not open these suspicious sites in a browser, especially if its a campus / department machine :)

#### Demo



University of York : M Freeman 2024

#### DNS

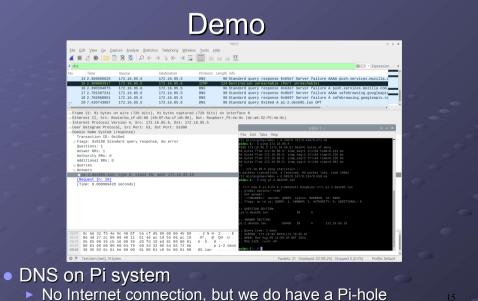
	0	0 8 15								0	8 1	5	
Header		ID									Name		
Question	QI	QR Opcode AA TC RD RA Z RCODE											
Answer		QDCount									Туре		
		•									Class		
Authority		ANCount									TTI.		
Additional		NSCount									TIL	Type Class TTL	
											RDLength		
General Format	ARCount										Rdata		
Header Format													
											Resource Record (RR) Format		

DNS Query / reply packet format

Question : Name, Type and Class

Answer, Authority and Additions : use RR format

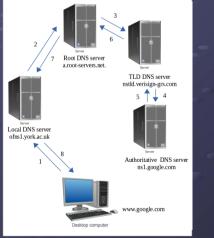
University of York : M Freeman 2024



Internet connection, but we do have a F University of York : M Freeman 2024

# Iterative or recursive query Flag in header Round-robin DNS Responses contain a list of

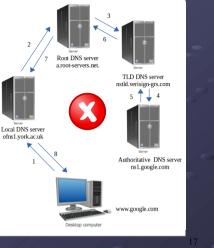
- potential servers (IP) that host identical services
  - Load balancing
- To minimise communication overheads previous DNS lookups are cached in the local DNS server
  - Time To Live (TTL)



#### DNS

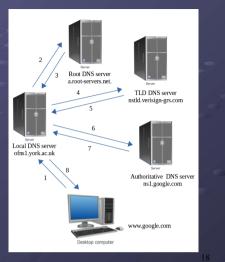
- Iterative or recursive query
  - Flag in header
- Round-robin DNS
  - Responses contain a list of potential servers (IP) that host identical services
    - Load balancing
- To minimise communication overheads previous DNS lookups are cached in the local DNS server
  - Time To Live (TTL)

University of York : M Freeman 2024



#### DNS

- Iterative or recursive query
  - Flag in header
- Round-robin DNS
  - Responses contain a list of potential servers (IP) that host identical services
    - Load balancing
- To minimise communication overheads previous DNS lookups are cached in the local DNS server
   Time To Live (TTL)

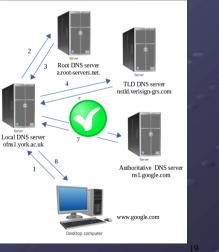


University of York : M Freeman 2024

#### DNS

- Iterative or recursive query
  - Flag in header
- Round-robin DNS
  - Responses contain a list of potential servers (IP) that host identical services
    - Load balancing
- To minimise communication overheads previous DNS lookups are cached in the local DNS server
  - ► Time To Live (TTL)





## Pause to consider ...

- We are starting to get a picture of how our network is working
  - Application layer protocols for transferring data
     HTTP, FTP, SMTP ...
  - To help organise and identify machines on our network we can use domain names. My office test machine
    - csestudentdev01.cs.york.ac.uk
  - We can translate domain names to an IP address using a DNS query (or reverse dig -x), but to do any of this our machine must first be connected to the network.
- Q : how do we get an IP address from the network when we don't have an IP address.
  - A chicken and egg situation :) University of York : M Freeman 2024

#### How to get a network address

auto lo iface lo inet loopback

auto eth0 iface eth0 inet static address 192.168.0.254



 One solution is to define this manually, on the Pi this is in: /etc/network/interfaces (file can vary). For each network interface controller (NIC) present we can assign it a static IP address.

- Advantage : simple for small networks that do not change.
- Disadvantage : becomes difficult to manage, especially if machines leave and then return to a network.

University of York : M Freeman 2024

#### DHCP

- Dynamic Host Configuration Protocol
  - RFC 1541: https://tools.ietf.org/html/rfc1541
  - DHCP created in 1993 (BOOTP 1985, RFC 951)
  - Client-Server model, default port 67 (server) and 68 (client)
  - Connectionless communicates across UDP links
    - Broadcast IP address 255.255.255.255 port 67
    - Host IP uses "unknown" address 0.0.0.0 port 68
      - Special local network and broadcast address, non-routable
  - IP address leased from server for specific time.
    - 600 sec (10 min), 7200 sec (2 hours), 86400 sec (one day)
    - Client tries to renew when 50% of lease elapses
  - If DHCP fails client assigned an IP address 169.254.0.0/16
    - RFC 5735: https://tools.ietf.org/html/rfc5735

University of York : M Freeman 2024

#### DHCP

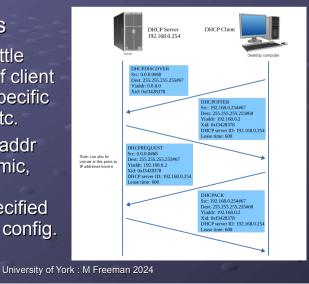
- DHCP packet format
  - Based on the Bootstrap protocol (BOOTP)
- Fields
  - Op: 1=request, 2=reply
  - Xid: transaction id (random) used to link request / reply
  - Ciaddr: client address (requested)
  - Yiaddr: current address
  - Options: DHCP phase, DNS server address and other network information (varies with phase) University of York : M Freeman 2024

0 15 31											
op htype hlen hops											
xid											
secs ops											
ciaddr											
	yi	addr									
siaddr											
giaddr											
chaddr											
sname											
file											
	ор	tions									
	1		23	;							

#### • DHCP phases

- May vary a little from shown if client requests a specific IP address etc.
- Assigned IP addr can be dynamic, automatic or manually specified in the server config.

#### DHCP



#### Demo

mike@mike_Aspire /var/lib/dbcp = + X	*enplot - + ×
mike@mike-Aspire /var/lib/dhcp – + ×	File Edit Wew Go Capture Analyze Statistics Telephony Tools Internals Help
File Edit View Search Terminal Help	🖉 🛛 🗃 🗶 🔁 🗋 🗶 ० ९ + + न ह ह 🗐 🗟 ९ ९ ९ -
mike@mike-Aspire /var/lib/dhcp \$ sudo dhclient -r -v	Filter: bootp   Filter: bootp Save
Killed old client process	No. Time Source Destination Protocol Length Info
Internet Systems Consortium DHCP Client 4.3.3	23 11.70683983 0.0.0.0 255.255.255 DHCP 342 DHCP Request
Copyright 2004-2015 Internet Systems Consortium.	24 11.70840418 192.168.0.254 192.168.0.2 DHCP 342 DHCP ACK 45 19.33381060 192.168.0.100 192.168.0.254 DHCP 342 DHCP Release
All rights reserved.	68 24:56316613: 0.0.0.0 255:255:255 DHCP 342 DHCP D1scover
For info, please visit https://www.isc.org/software/dhcp/	61 24.56467273 192.168.0.254 192.168.0.2 DHCP 342 DHCP Offer
,	62 24.56477365: 0.0.0.0 255.255.255.255 DHCP 342 DHCP Request 63 24.57352812-192.168.0.254 192.168.0.2 DHCP 342 DHCP ACK
Listening on LPF/wlp7s0/ac:e0:10:06:74:5d	000 101.1400028 192.168.0.2 192.168.0.254 DHCP 342 DHCP Request
Sending on LPF/WLp750/ac:e0:10:06:74:5d	010 103.5062010 102.168.0.2 102.168.0.254 DHCP 342 DHCP Request 015 310 5205561 302 160 0 2 102 160 0 254 DHCP 342 DHCP Bernard
Listening on LFF/eng890/30:65:ec:82:4c:bd	
Sending on LPF/enp8s0/30:65:ec:82:4c:bd	Frame 60: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0 Ethernet II, Src: WistronC 02:4c:bd (30:65:ec:02:4c:bd), 0st: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
	▶ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Sending on Socket/fallback	▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
DHCPRELEASE on enp8s0 to 192.168.0.254 port 67 (xid=0x39203aa9)	<ul> <li>Bootstrap Protocol (Discover)</li> <li>Missiae type: Boot Request (1)</li> </ul>
mike@mike-Aspire /var/lib/dhcp \$ sudo dhclient -v	Hardware type: Ethernet (0x01)
Internet Systems Consortium DHCP Client 4.3.3	Hardware address length: 6 Hoos: 0
Copyright 2004-2015 Internet Systems Consortium.	Transaction ID: 0xf3428378
All rights reserved.	Seconds elapsed: 0
For info, please visit https://www.isc.org/software/dhcp/	Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0
	Your (client) IP address: 0.0.0.0
Listening on LPF/wlp7s0/ac:e0:10:06:74:5d	Next server IP address: 0.0.0.0
Sending on LPF/wlp7s0/ac:e0:10:06:74:5d	Relay agent IP address: 0.0.0.0 Client MAC address: WistronG 02:4c:bd (30:05:ec:02:4c:bd)
Listening on LPF/enp8s0/30:65:ec:82:4c:bd	Client hardware address padding: 00000000000000000
Sending on LPF/enp8s0/30:65:ec:82:4c:bd	Server host name not given
Sending on Socket/fallback	Boot file name not given Magic cookie: DHCP
DHCPDISCOVER on wlp780 to 255.255.255.255 port 67 interval 3 (xid=0xb179a179)	Option: (53) DHCP Hessage Type (Discover)
DHCPDISCOVER on enp8s0 to 255.255.255.255 port 67 interval 3 (xid=0x0179a179)	Option: (50) Requested IP Address     Option: (12) Host Name
DHCPREQUEST of 192.168.0.2 on enp8s0 to 255.255.255.255 port 67 (xid=0x754263/6/	Option: (55) Parameter Request List
DHCPOFFER of 192.168.0.2 from 192.168.0.254	> Option: (255) End
	0000 ff ff ff ff ff ff 30 65 ec 82 4c bd 08 00 45 100eLE.
DHCPACK of 192.168.0.2 from 192.168.0.254	0010 01 48 00 00 00 88 11 39 56 00 00 00 01 ff . H 9 0020 ff ff 00 44 00 43 01 54 49 5a 01 01 06 00 f3 420.C.4 IB
bound to 192.168.0.2 renewal in 236 seconds.	0030 83 78 00 00 00 00 00 00 00 00 00 00 00 00 00
mike@mike-Aspire /var/lib/dhcp \$	0040 00 00 00 00 00 00 30 63 ec 82 4c bd 00 00 00 00
	🔾 💆 File: "Ampheireshark_enp8x0_202010 Packets: 13008 - Displayed: 45 (0.3%) - Dro Profile: Default
DHCD phases : discovery request	offer and acknowledge
<ul> <li>DHCP phases : discovery, request,</li> </ul>	Uner and acknowledge

University of York : M Freeman 2024

#### Go and research

- Have a look at how the NTP functions
  - Can't just send time, need to compensate for network delays.
  - How is time represented i.e. what format, data types are used in the protocol?
  - How many stratum levels are there?
    - What are stratum level 0s?
  - Using the ntp query command: ntpq -p what are the fields: st, poll, reach, delay offset, jitter etc?

## NTP

CONTER	STATES	NATAL	CESERVATORY		ALTERNATE S	HASTER	CLOCK
			12 ( 122)				
				: 0	14 19 3 A gamman		
				G			

mike@mike-Aspire ~ Edit View Search Terminal Help											
e@mike-Aspire remote	~ \$ ntpq -p refid	st	t	when	poll	reach	delay	offset	jitter		
	.P00L. .P00L. .P00L. .GPS. .GPS. 92.21.53.217 85.199.214.102 193.204.114.232	16 16 16 16 1 1 2 2 2		- - 48 115 134 84 2	64 64 64 64 128 128 128 256	0 0 0 377 377 377 377 377 377	0.000 0.000 0.000 0.000 11.188 12.824 11.644 23.115 8.675	0.000 0.000 0.000 0.000 0.731 -0.186 -0.133 -0.213 0.345	0.000 0.000 0.000 0.000 0.000 0.000 0.094 0.045 0.074 0.065 0.254		

- Network Time Protocol
  - RFC 958 (5905): https://tools.ietf.org/html/rfc958
  - NTP created in 1985
  - Client-Server model, default port 123
  - Connectionless communicates across UDP links
  - Hierarchy of reference clocks and servers i.e. stratum levels
    - Typically millisecond accuracy achievable
       University of York : M Freeman 2024

#### Summary

- In addition to the headline protocols we need some glue to "bind" things together :)
- Note, we have only had a quick look at these protocols, there is a lot more detail behind the scenes e.g. how the distributed DNS database is maintained / updated etc.
- However, some unanswered questions
  - What are the TCP and UDP?
  - Why do we need two different protocols?
  - What is happening in the lower layers of the protocol stack?