

CO1507 Introduction To Networking

Domain Name Service (DNS)

Jonathan Edwards 2024

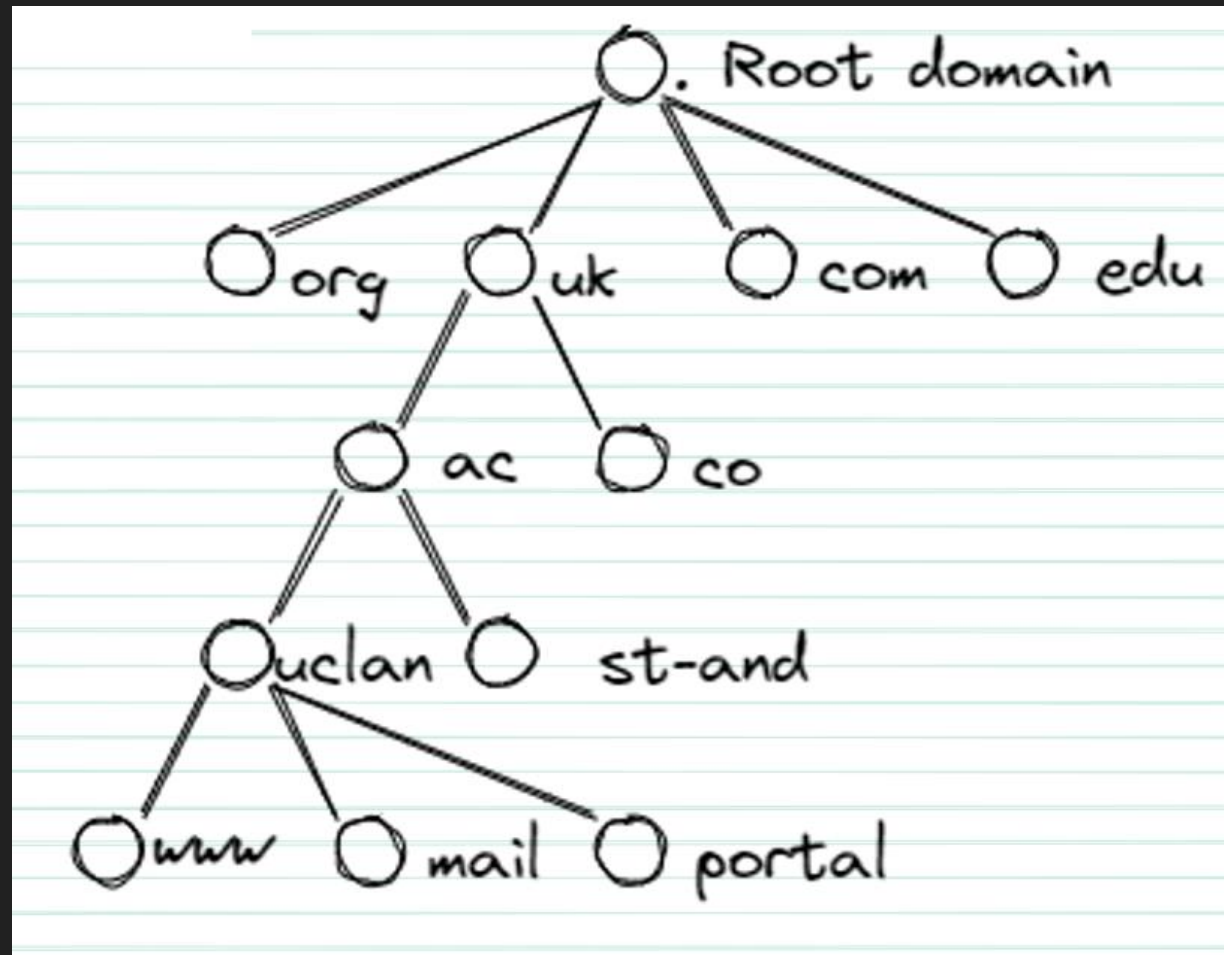
What is DNS and Why Do We Need It?

- People prefer easy to remember names rather than addresses
- Computers can only use the addresses
- Imagine remembering the IPs instead of the hostnames
 - 173.194.66.147
 - 193.61.253.9
 - 173.252.110.27
- DNS is Internet wide and provides a distributed database
 - Names to IPs
 - IP to names
 - Services to IP address

DNS Server

- **DNS** stands for **Domain Name Service** and is run on servers across the internet
- A DNS servers' role is to translate from human **readable** and **memorable** '*domain names*' into IP addresses of the corresponding server on the internet
- Imagine we are visiting www.example.com so we type the URL into the browser
- There is in fact another hidden dot at the end of this address i.e. www.example.com. 

Name Hierarchy



Domain Names

- Hosts and DNS names are based on the location in the tree
- Each part of the names is separated by a full stop (.)
- Examples:
 - `www.uclan.ac.uk`
 - `www.facebook.com`
- Labels:
 - Can be up to 63 characters long
 - Can contain textual, numeric characters as well as dash
 - Are not case-sensitive

Top level domains

Five types of top-level domain:

- Infrastructure top level domain (ARPA)
in-addr.arpa
- Generic top-level domain (gTLD)
com, org, net
- Country-code top level domain (ccTLD)
uk, fr, us
- Sponsored top level domain (sTLD)
gov, edu, mobi
- Test top level domain (tTLD)
test

DNS server

- The last (hidden) dot represents the root domain of the **internet namespace**
- First the browser may check its cache but assuming it doesn't hold the record in it asks the Operating System *'do you know where www.example.com'* is
 - E.g. In LINUX, the OS holds DNS records within /etc/resolv.conf
- If it is cached etc. this is okay.. However, chances are it is not
- If the OS does **not** have a DNS record stored, it must be forwarded onto a **DNS server** for resolution

DNS

- The computer having decided it doesn't know where www.example.com. is must consult a **resolving name server**
- The resolving name sever may or may not know this either
- But it *will* know how to find the **root name servers**
- The Root name server may also not know, but it can forward you to the **TLD name-server**
- In this case we need the **.com name-servers** (or .net .co.uk .org .ac.uk etc...)

DNS

- The **TLD nameserver** also likely doesn't know, but it **will** know where the **.com Authoritative** nameserver is
- This is because it will be notified by the **Registrar** when new domains are purchased
- We can now be forwarded to the **Authoritative** nameserver. e.g. the 'example.com' name-server
- Finally, the authoritative name-server will be able to supply an IP address, send it back to the client computer which can then make a request to that IP address

DNS

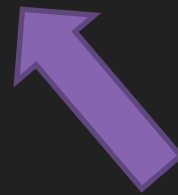
www.example.com.



example.com namespace
- **Authoritative** Name Server



.com **TLD** (Top Level Domain)
- **TLD** Name Server



Root namespace
- **Root** Name Server

Caching

- To reduce network load DNSs/resolvers cache responses
- Each entry in the DNS has a 'time-to-live' (TTL)
- Each entry can be cached upon the TTL expires
- Common to set TTL for days for weeks
- However, 0 is acceptable for some critical systems
- When an entry is cached, it is returned
- Marked as unauthoritative

DNS Fields

Each DNS entry can consist of multiple fields

- Doesn't have to have all of them - only need one
- There are many more than are included in this list
- Some of the more commonly used fields are

- A record
- AAAA Record
- CNAME

A Record

- An '*A record*' is the most frequently used DNS record field
- A Record is the name to an IP mapping
- Allows access to any service by its name
 - e.g. portal.uclan.ac.uk -> 192.61.255.211

Other DNS Fields

- CNAME = An alias to a host name
- AAAA = Gives the IPv6 information when a DNS query is performed
- NS = Delegates part of the domain to another DNS server
 - e.g. **mail**.uclan.ac.uk
- SOA = Start Of Authority; more information about the domain as a whole

DNS Security

- DNS is vulnerable to man-in-the-middle (MITM) attacks
- This is because it relies on transmitting unencrypted data over networks
- This makes it possible for an attacker to intercept and alter the data being transmitted between a client and a DNS server
- Effectively this means redirecting the client to a another, potentially malicious website
- e.g. The MITM attacker could modify the response from a DNS server to redirect a client to a fake website
 - The client thinks they are communicating with the legitimate website
 - This has the potential to compromise sensitive information such as passwords, financial data, etc...

DNS Config

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record

Address

Add Save Remove

No.	Name	Type	Detail
0	www.jonathan.com	A Record	192.168.10.1

DNS Cache

☐ Top

The Assessment will take place during the week 16 - 22 March

Practically this means either on **Tuesday 19th** or **Thursday 21st**

Assessment Information

The Assessment is worth 50% of the module grade whereas the exam at the end of April makes up the remaining 50%

Assessment Information

- Topics of the practical exercise (Packet Tracer task – 80% of the grade)
 - Routing (you must be able to configure a static recursive route)
 - DHCP server
 - Wireless Access Point
 - Custom Subnetting (e.g. /27 /28 /30)
 - Setup of router in the CLI

Assessment Information

- In addition to the task there will be a short multi-choice quiz (20% of the grade)
- Topics of quiz section:
 - All topics covered so far but especially since Christmas
 - i.e. the question may be on something we've done very recently, however may also rely on fundamental understanding of the concepts from way back in semester one
 - e.g. *'What is an IP address?'*
 - Make sure to do some revision!

RULES

- **Do not arrive late** on the day of the assessment as you will disturb other students working
- Disruption may mean you are not be allowed to sit the assessment
- You must come able to log in to **CISCO Packet Tracer**
- We cannot supply you with this information forgetting your password is nor a reasonable excuse as we've been using Packet Tracer ever week since week 1!
- If you require any special arrangements, please discuss these with the module leader ASAP.

Example multi choice questions

What is the correct subnet mask corresponding with CIDR notation /27

- a) 255.255.255.0
- b) 255.255.255.240
- c) 255.255.224.0
- d) 255.255.255.224

Example multi choice questions

If the default gateway is missing or configured incorrectly what is the outcome?

- a) Local area communication unaffected, wide area communication prevented
- b) Local area communication prevented; wide area communication prevented
- c) Wide area communication unaffected, local area communication prevented
- d) Local area communication unaffected, wide area communication unaffected

Example multi choice questions

What is the broadcast address for the network 192.168.10.0/24?

- a) 192.168.10.1
- b) 192.168.10.254
- c) 192.168.10.255
- d) 192.168.10.0

Example multi choice questions

At what layer of the OSI model does a router operate?

- a)Physical
- b)Data-Link
- c)Network
- d)Transport

Example multi choice questions

If the subnet mask is 255.255.255.240 how many valid host IP addresses are on the subnet?

- a)6
- b)14
- c)30
- d)62

This Week

- The upcoming few weeks labs we will prepare you for the assessment along with the past few
- Attendance to labs is very important in order give you the best chance of succeeding
- Please ask your lab tutor if there is any uncertainty over any of the topics covered in these labs
- It may end up costing **you** marks if you do not

Any Questions?

