



Jeff Maynard

How the Internet works

# Jeff Maynard

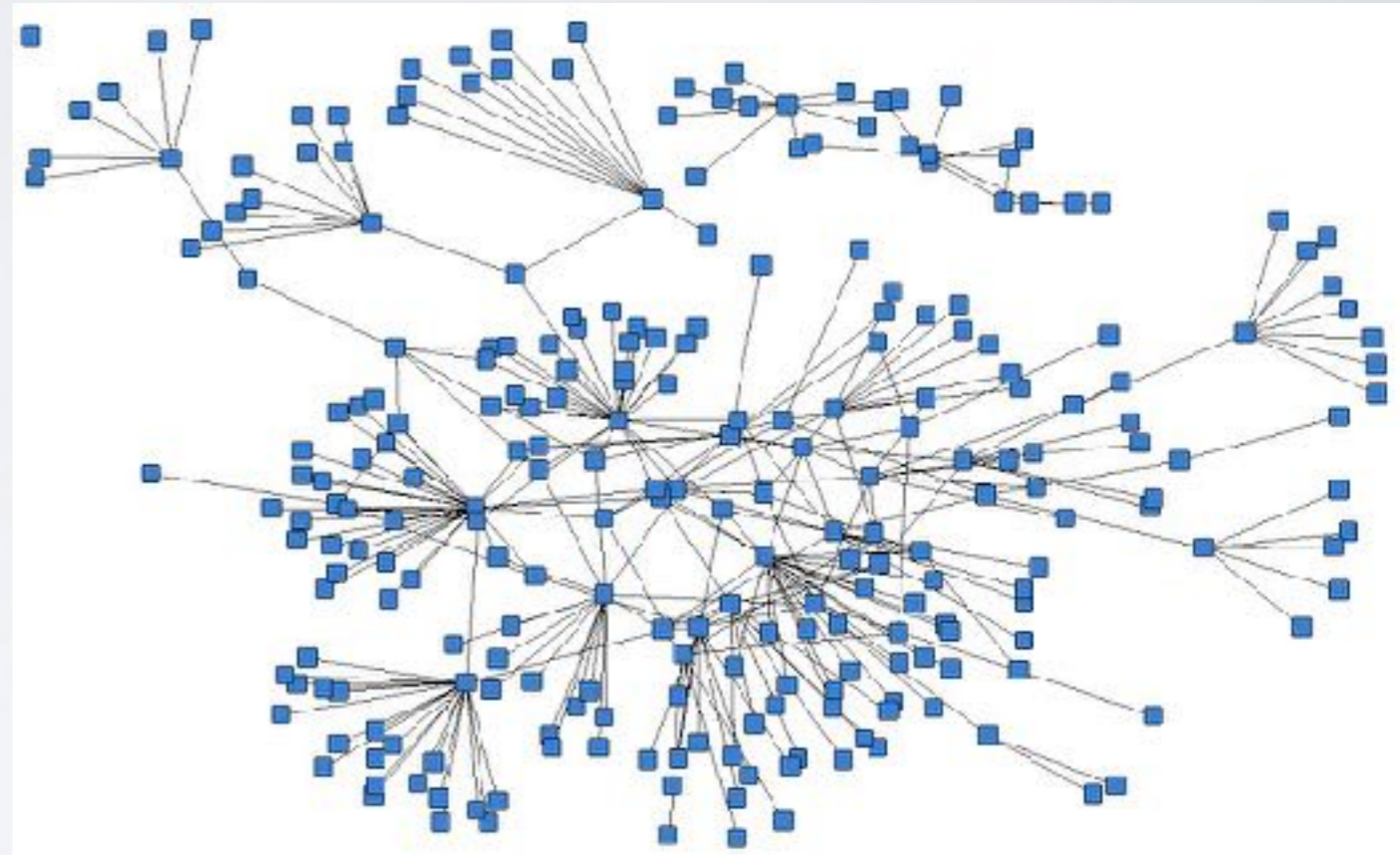


- Started in computing in September, 1965
- Ran British Airways' global comms and computers
- Migrated C&W from analogue to digital networking
- IT Entrepreneur Of The Year, 2000
- Floated three IT companies (OTC, LSE, AIM)
- Writes iPhone/Android Apps as a hobby
- Advisor to Thames Valley Police on cyber crime

# What Is The Internet?



- Technical answer:
  - A network of networks
    - All interconnected
    - Configuration constantly changing
    - Acting as one single network



# How Does Data Flow?



- Data/information/instructions/routing etc:
  - Controlled by a series of 'protocols' (167 in total!)
  - A 'protocol' is just a set of universally agreed rules

# TCP/IP

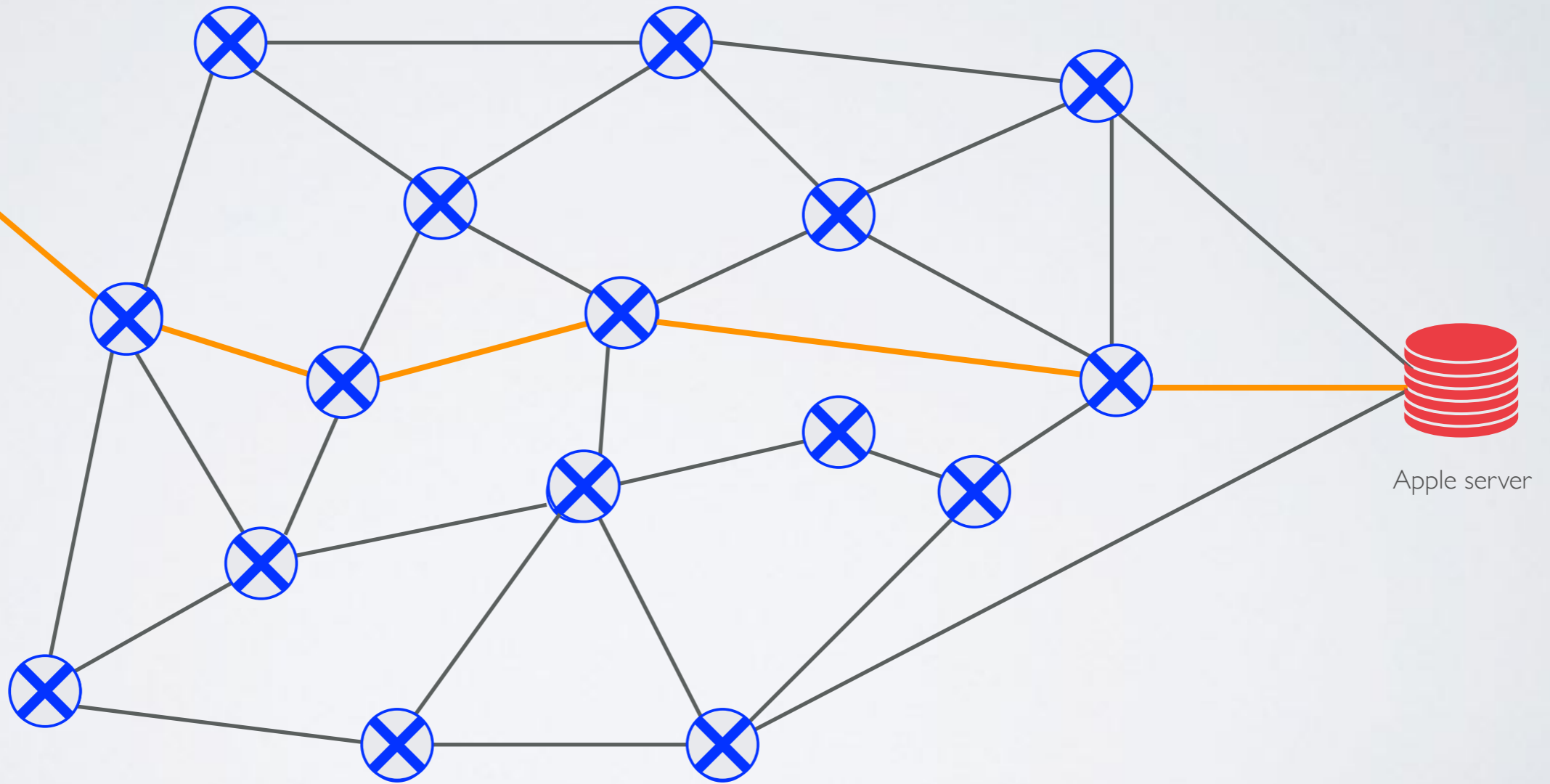


- Internet traffic flow is managed by two protocols:
  - TCP breaks data into packets
  - IP transmits (routes) packets from source to destination
  - TCP reassembles packets into message



# Traffic Flows Router-To-Router

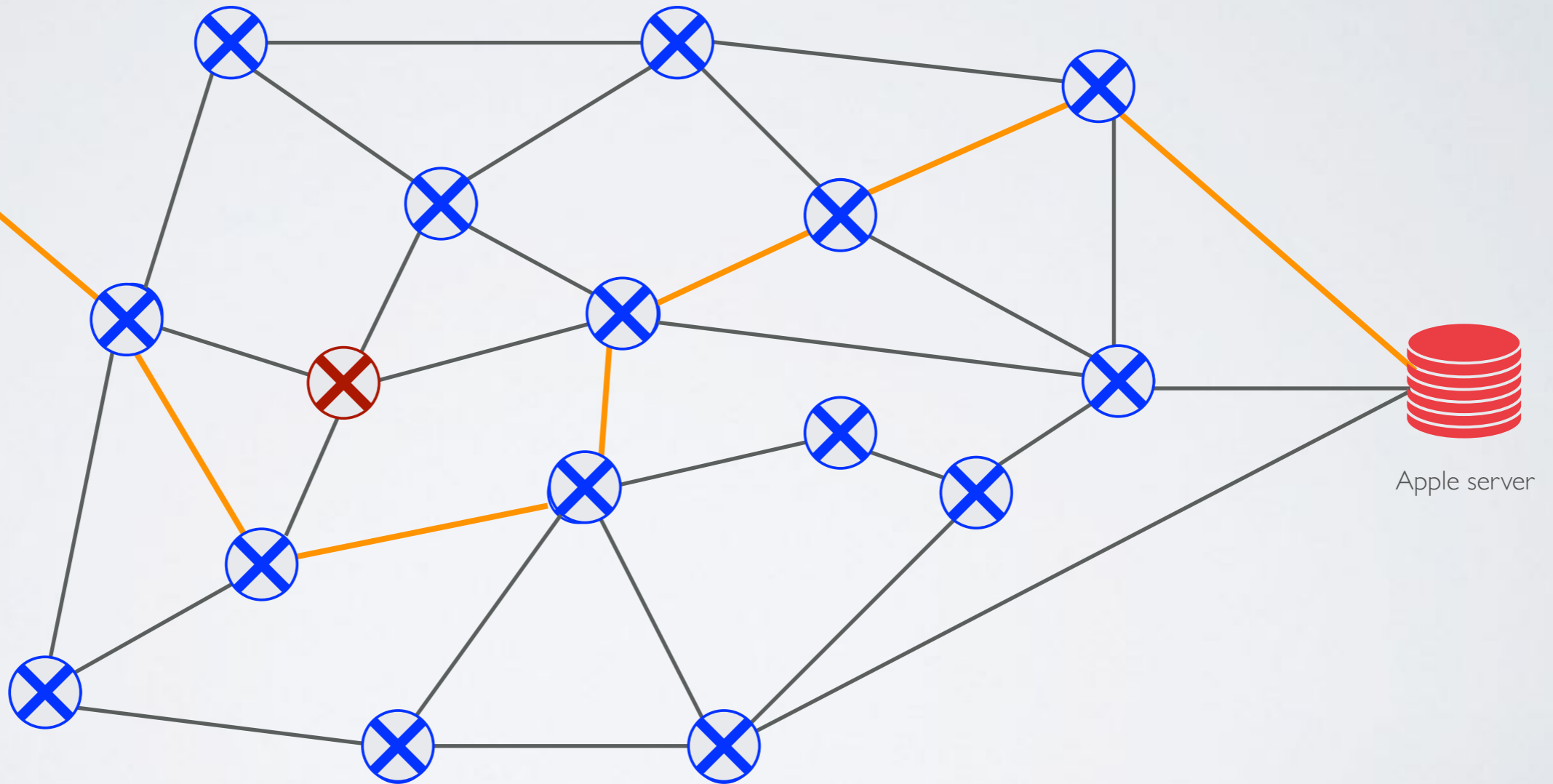
www.apple.com





# Traffic Flows Router-To-Router

www.apple.com



# Actual Trace Route

to phylliscourt.co.uk



tracert to phylliscourt.co.uk (79.170.44.210), 64 hops max, 72 byte packets

```
1 192.168.168.1 (192.168.168.1) 0.897 ms 0.513 ms 0.456 ms
2 31.55.185.184 (31.55.185.184) 6.017 ms 5.691 ms 5.999 ms
3 core1-hu0-17-0-5.colindale.ukcore.bt.net (195.99.127.150) 6.378 ms 6.572 ms 6.794 ms
4 peer1-hu0-19-0-0.slough.ukcore.bt.net (62.172.103.141) 6.410 ms 7.165 ms 7.007 ms
5 linx.edr1.lon1.ldn.uk.nsfocus.cloud (195.66.225.49) 8.270 ms 8.110 ms 8.243 ms
6 ae1.dr-master.ld5.core.heg.com (87.230.114.218) 14.524 ms 14.330 ms 14.445 ms
7 web210.extendcp.co.uk (79.170.44.210) 13.988 ms 13.995 ms *
```

## NOTE:

No mention of www.phylliscourt.co.uk

Addresses translated to numeric form

eg: 79.170.44.210



# Internet Addressing



- The Internet does not recognise the likes of *www.bbc.com*
- This needs translating (for BBC) to 212.58.244.66
- Translation is the role of D N S:
  - Domain Name Service
- Your ISP will automatically set up a DNS address for you
  - Although you can use Google: 8.8.8.8 and 8.8.4.4




# Internet Addressing

- IP addresses are four numbers separated by dots:
  - Each number is in range 0 to 255 ( $2^8$ )
    - Eg: 124.226.88.75 | 11.12.44.250 | 203.34.119.2
  - IP addresses beginning 192 or 172 or 10 are private
    - Eg: typical router is 192.168.1.1 or 10.0.0.254
  - Each connected device allocated IP: eg 192.168.168.22
    - Allocation by modem/router's DHCP



# Internet Addressing



The screenshot shows the iPad Settings app with the Wi-Fi settings for a network named 'Phyllis-Court'. The left sidebar shows the 'Settings' menu with 'Wi-Fi' selected. The main screen displays the following information:

- Unsecured Network:** Open networks provide no security and expose all network traffic. If this is your Wi-Fi network, configure the router to use WPA2 Personal (AES) security type. [Learn more about recommended settings for Wi-Fi...](#)
- Forget This Network:** A button to remove the network from the device.
- Auto-Join:** A toggle switch that is currently turned on.
- IPV4 ADDRESS:**
  - Configure IP:** Automatic >
  - IP Address:** 10.0.0.43
  - Subnet Mask:** 255.255.255.0
  - Router:** 10.0.0.254
- Renew Lease:** A button to refresh the IP address.
- DNS:**
  - Configure DNS:** Automatic >

# Instructions To Network



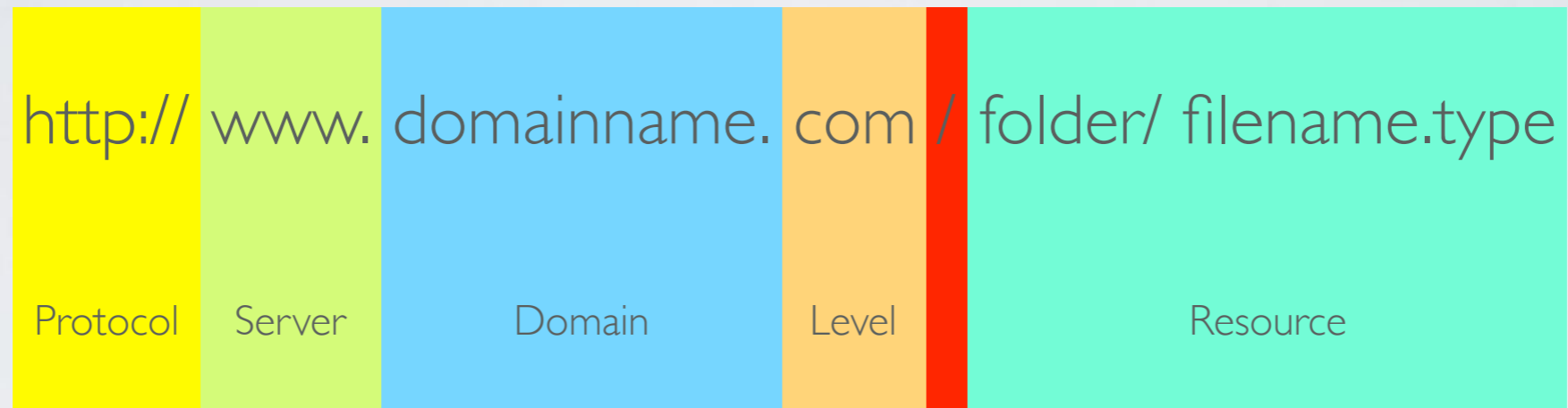
- A URL (Uniform Resource Locator)
  - Says 'what from where'
  - HTTP is the most common type of URL
  - Others include FTP HTTPS WHOIS IRC
    - 'MAILTO' opens local email client -
      - POP3, IMAP and SMTP are email send/receive protocols

# The HTTP Protocol

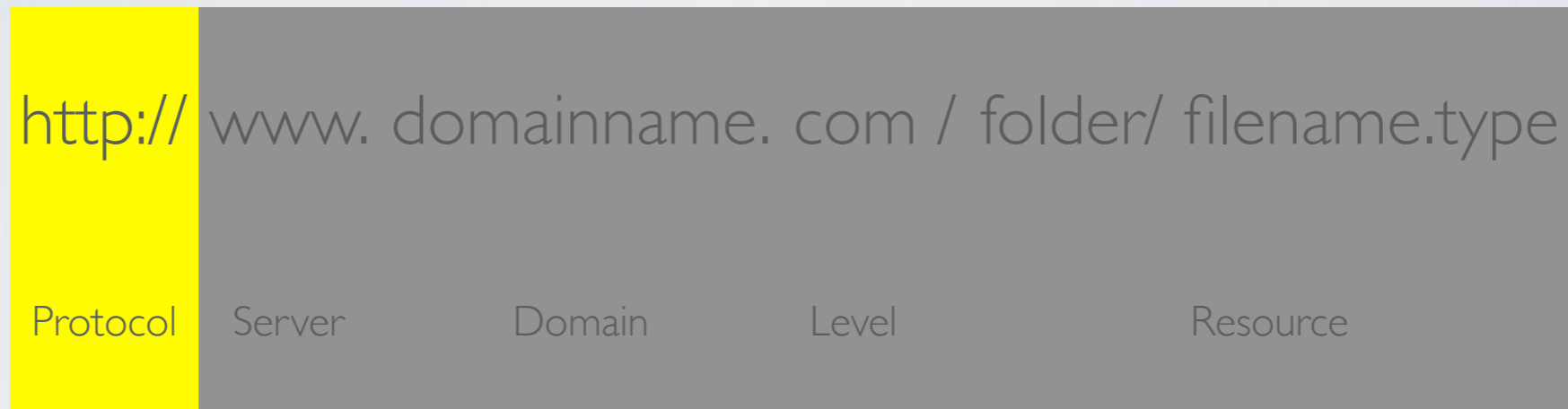


- Lets the network know we want to view a web page
- HTTP:// no longer typed *but is inserted automatically by browser*
- Follows a standard layout (as defined in the protocol)

# The URL Components

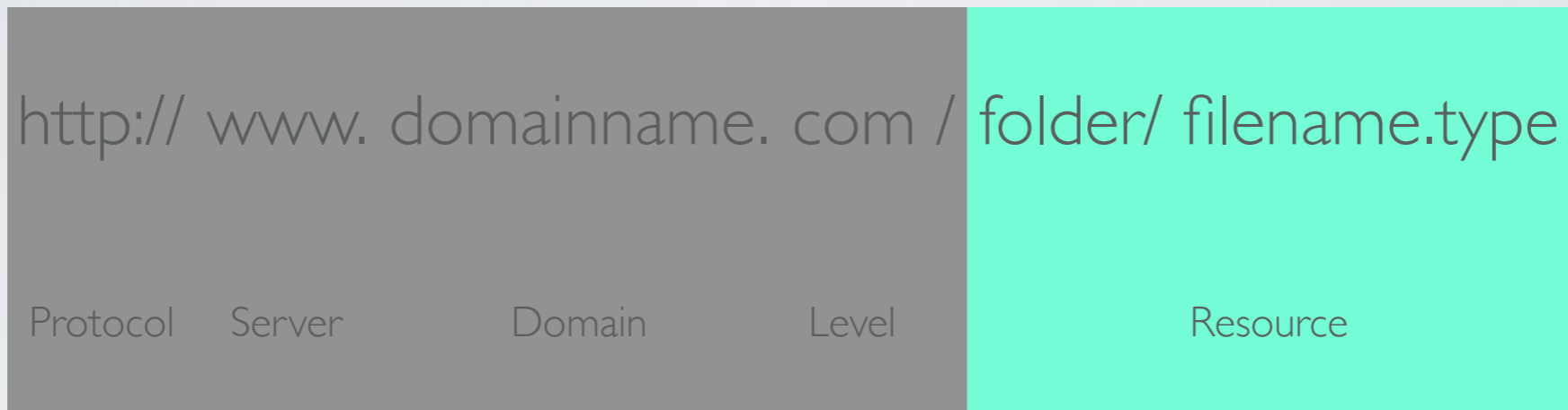


# The URL Components



http:// indicates this is a request for a web page and is not usually typed but IS required

# The URL Components



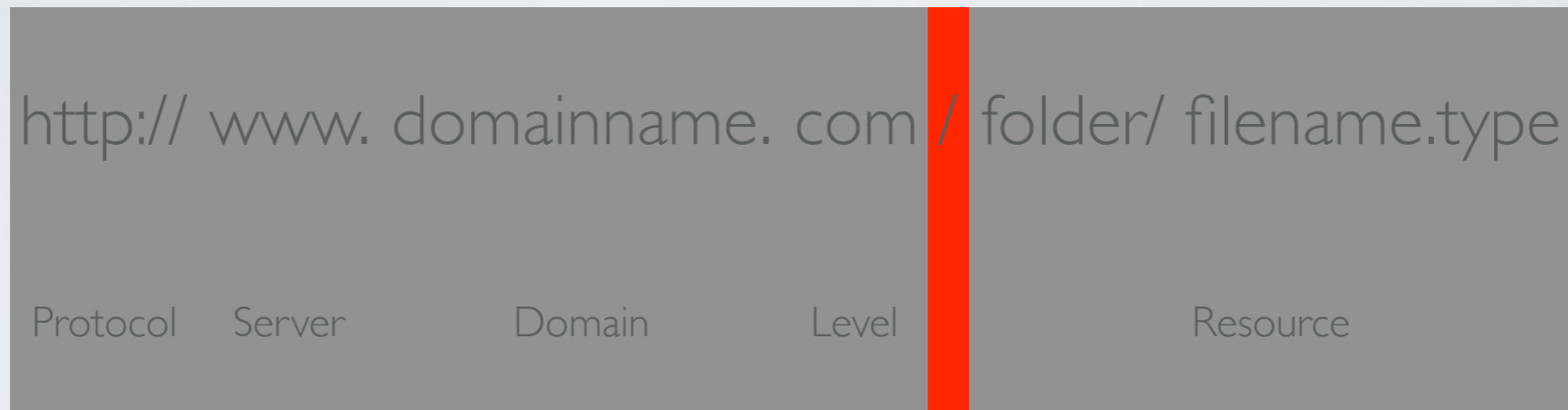
Specifies the location and type of the resource required  
if omitted then *index.html* is assumed.

*Type is usually a web page (html, htm, shtml, php, asp, cgi...)*

*But can also be any file type (pdf, doc, img, mov, mp3...)*



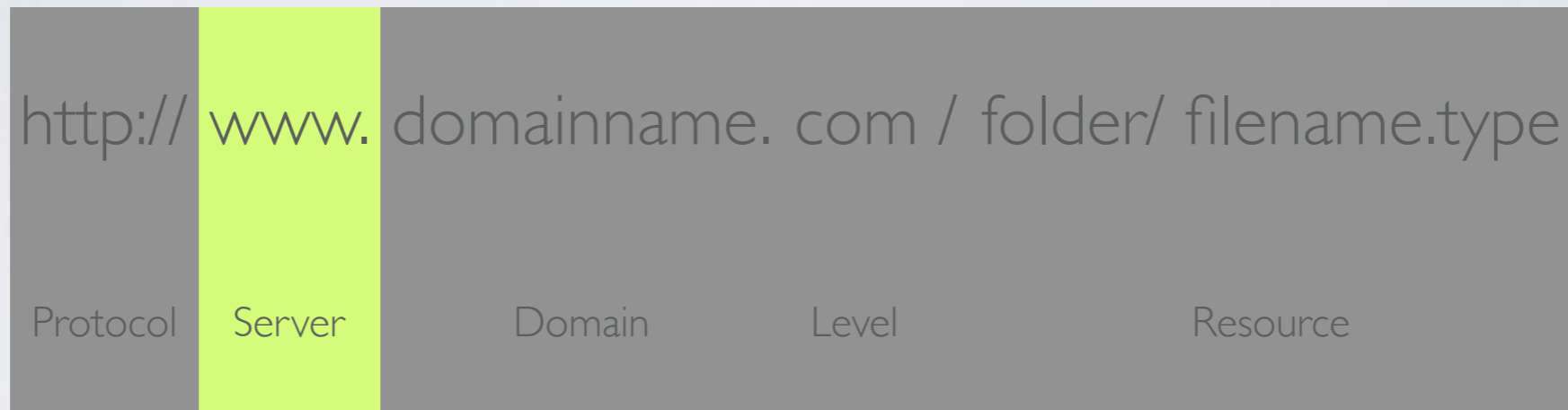
# The URL Components



The first slash *after* the `://` signifies the end of the domain id



# The URL Components

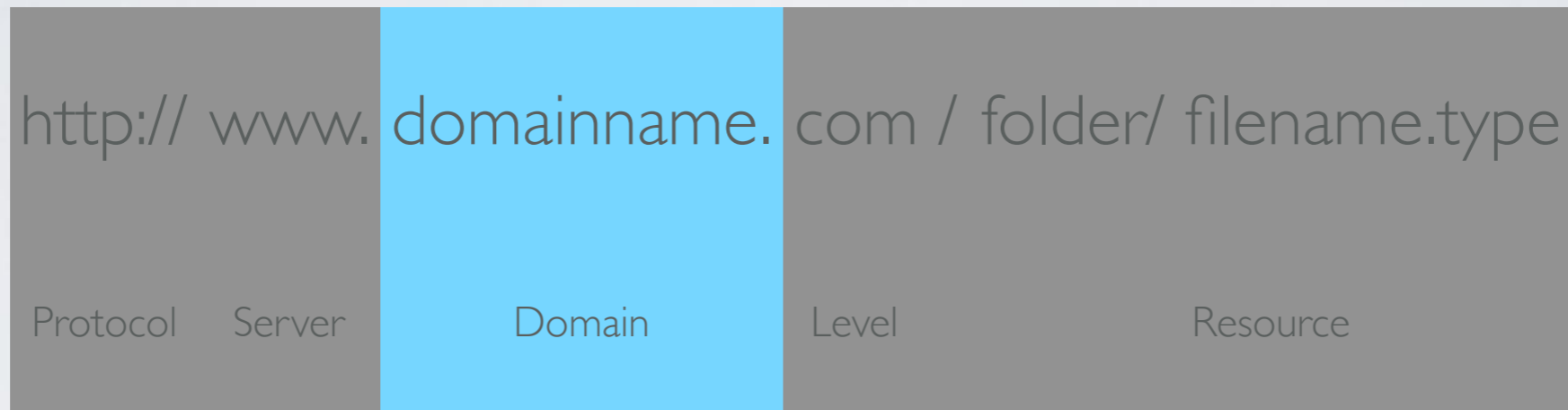


Contrary to popular belief, this does NOT indicate a web page request  
(http:// does that)

It is the name of the server providing the resource

Name can be anything the server builder chooses:  
www2.site.com | docs.resource.net | tickets.theatre.org | mail.messages.edu

# The URL Components



Officially: an identification string defining a realm of administrative autonomy, authority or control (*when tied to level*)

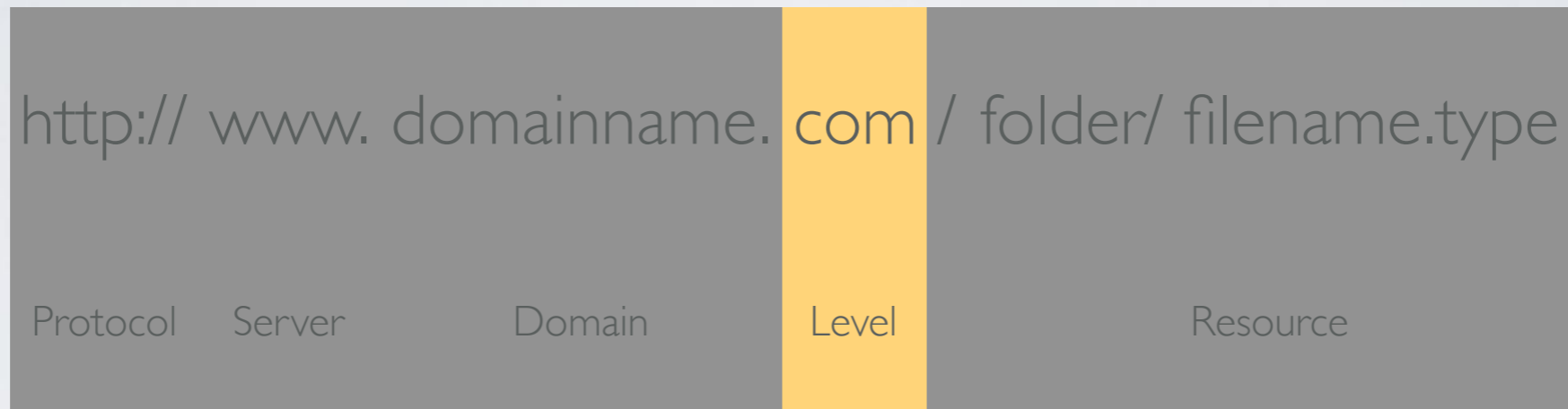
In practice: the company or organisation you are looking for

BUT

spelling.com is not the same as spelling.co.uk



# The URL Components



Originally intended to identify the nature of the domain owner  
Anyone can register an unused domain name

(registration is a *combination* of domain and level)

# Top Level Domains (TLDs)



- Original set:
  - .com commercial organisation (no longer restricted)
  - .net infrastructure provider (no longer restricted)
  - .edu university or school
  - .int organisations treaty-linked
  - .org non-profit organisation (no longer restricted)
  - .mil military (US only)
  - .gov government (US only)
- Hundreds recently added:
  - from .abc through .club .loan .photos .travel .work to .ventures

# Country Code TLDs



- 255 country codes from .ac to .ZW (St Helena & Zimbabwe)
- Seen alone::
  - hmrc.uk | www.gov.uk | hansard.parliament.uk | nic.ms
  - www.gov.gg | citi.cw | time.is | who.is | goo.gl | vlada.mk
  - правительство.рф | موقع.وزارة-الاتصالات.مصر

Montserrat; Guernsey; Curacao; Iceland; Gibraltar; Macedonia; Russia; Saudi Arabia

# Country Code TLDs



- 255 country codes from .ac to .ZW (St Helena & Zimbabwe)
- Seen with modifier:
  - [www.amazon.co.uk](http://www.amazon.co.uk) | [www.naenara.com.kp](http://www.naenara.com.kp)
  - [webmail.tel.net.ba](http://webmail.tel.net.ba) | [jamaicapost.gov.jm](http://jamaicapost.gov.jm)
  - [www.cnc.asso.nc](http://www.cnc.asso.nc) | [www.cdp.ossrom.va](http://www.cdp.ossrom.va) | [www.fs.fed.us](http://www.fs.fed.us)

N Korea; Bosnia & Herzegovina; Jamaica; New Caledonia; Vatican; US

# Country Code TLDs



- Every US and Canadian state has two-letter modifier:
  - miami.fl.us - www.state.nj.us - webmail.nm.us
  - state.ab.ca - heritage.nf.ca - pcparty.ns.ca
- Other two letter domains used for marketing reasons:
  - magic.fm | del.icio.us | itun.es | cryp.to | sil.ly | porsche.ag

Fed States of Micronesia; US; Spain; Tonga; Libya; Antigua



# Summary So Far



- Type or click a URL
  - Typically: HTTP, HTTPS, FTP, (mail)
  - DNS translates the domain to IP address
  - Data broken into numbered packets
  - Data sent/received by routers based on protocol

# Search Engines

The Google logo, consisting of the word "Google" in its characteristic multi-colored font.The Bing logo, featuring a yellow chevron-like shape followed by the word "bing" in a lowercase, sans-serif font.The DuckDuckGo logo, which includes a stylized duck head in a red circle and the text "DuckDuckGo" in a grey, sans-serif font.The Yahoo! logo, featuring the word "YAHOO!" in a white, serif font on a purple rectangular background.

- Web crawler finds home page
  - Follows every link
  - Copies page and indexes
  - PageRank and update frequency

# Cloud Services



- Large on-line storage services
- Useful for sharing data
- Not a backup solution
- Most offer some free storage

# Some Internet Tools



- Whois
- Ping
- Tracert
- Port Scan

# Some Internet Tools



- Whois
- Ping
- Tracert
- Port Scan

## RAW WHOIS DATA

```
Domain name:
  phylliscourt.co.uk

Registrant:
  Phyllis Court Members Club Limited

Registrant type:
  UK Limited Company, (Company number: 88274)

Registrant's address:
  Marlow Road
  Henley On Thames
  Oxfordshire
  RG9 2HT
  United Kingdom

Data validation:
  Nominet was able to match the registrant's name and address against a 3rd
  party data source on 10-Dec-2012

Registrar:
  Invictanet Ltd t/a Invictanet Limited [Tag = INVICTAWIZ]
  URL: http://www.invicta.net

Relevant dates:
  Registered on: 30-Oct-1997
  Expiry date: 30-Oct-2019
  Last updated: 02-Oct-2017

Registration status:
  Registered until expiry date.

Name servers:
  ns1.invictawiz.com
  ns2.invictawiz.com
```

# Some Internet Tools



Ping has started...

```
PING phylliscourt.co.uk (79.170.44.210): 56 data bytes
64 bytes from 79.170.44.210: icmp_seq=0 ttl=52 time=14.518 ms
64 bytes from 79.170.44.210: icmp_seq=1 ttl=52 time=14.130 ms
64 bytes from 79.170.44.210: icmp_seq=2 ttl=52 time=14.441 ms
64 bytes from 79.170.44.210: icmp_seq=3 ttl=52 time=14.406 ms
64 bytes from 79.170.44.210: icmp_seq=4 ttl=52 time=14.620 ms
64 bytes from 79.170.44.210: icmp_seq=5 ttl=52 time=14.557 ms
64 bytes from 79.170.44.210: icmp_seq=6 ttl=52 time=14.105 ms
64 bytes from 79.170.44.210: icmp_seq=7 ttl=52 time=14.139 ms
64 bytes from 79.170.44.210: icmp_seq=8 ttl=52 time=14.274 ms
64 bytes from 79.170.44.210: icmp_seq=9 ttl=52 time=14.180 ms
```

--- phylliscourt.co.uk ping statistics ---

```
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.105/14.337/14.620/0.185 ms
```

- Whois
- Ping
- Tracert
- Port Scan



# Some Internet Tools

Port Scanning host: 79.170.44.210

- Whois

- Ping

- Tracert

- Port Scan

```
Open TCP Port: 7          echo
Open TCP Port: 25         smtp
Open TCP Port: 80         http
Open TCP Port: 110        pop3
Open TCP Port: 143        imap
Open TCP Port: 162        snmptrap
Open TCP Port: 443        https
Open TCP Port: 993        imaps
Open TCP Port: 995        pop3s
Open TCP Port: 3306       mysql
Open TCP Port: 10050      zabbix-agent
Open TCP Port: 31008
```

Port Scan has completed...

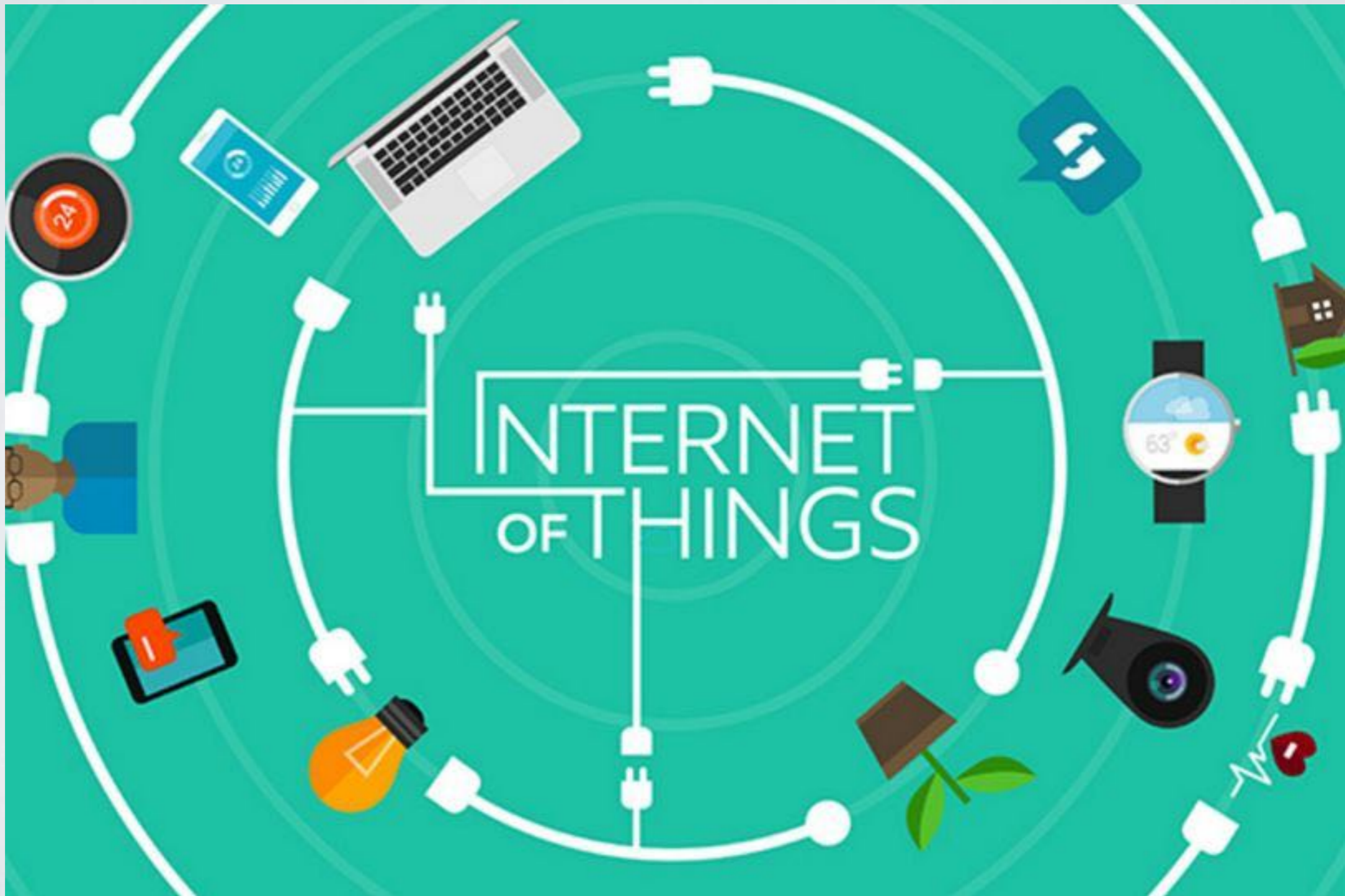
# Other Internet Stuff



- IoT
- Social Media
- V P N
- P2P
- Dark Web



# IOT - the Internet of Things



# IOT - the Internet of Things



- Anything and everything becomes connected:
  - Fridges, Home Heating, Home Security, Home Lighting, CCTV, Cars, Clothes, Training (Gym kit), Cameras, Drones, Farms, Ticket Barriers, Health Monitoring, Traffic Management
  - Augmented Reality



# Virtual Private Networks



- Simulates a direct connection but using the Internet
  - Very secure
  - Used to access company networks normally behind firewalls
  - Changes your apparent location
    - Access US Netflix from UK
    - Hides cyber criminals
  - Bypasses ISP DNS restrictions
    - Used for access to P2P sites

# Peer-To-Peer (P2P)



# Peer-To-Peer (P2P)



- BitTorrent used to transfer files from one PC to another
- Legitimate uses but also for file sharing:
  - The Pirate Bay (amongst others)
    - Shares *links* to copyright material
      - Music, Apps, Books, Films, Porn

# Peer-To-Peer (P2P)



- BitCoin
  - The P2P money system (totally anonymous)
  - BitCoins sent from one user to another
    - Details of every transaction sent to every blockchain
    - PK Cryptography and one-time addresses keep it secure

# The Dark Web



- A subset of the regular Internet but
  - Traffic and sites encrypted
  - Not visible to search engines or regular browsers
  - Need a special browser, TOR (The Onion Router)
  - Best avoided unless you are in great need of an AK47...



# The Deep Web



- Anything that cannot be 'seen' by search engines
- Mostly benign (and oft confused by the media!)
- Includes:
  - The Dark Web
  - Databases, PayWall material, Staging sites
  - Pages behind registration or login

# Internet Terms



- DDoS
- Bot
- Blog
- CSS
- Noob
- Troll

# Internet Governance



- NO central 'control room'
- NO overall governing body
- But various contributing agencies:
  - IETF
  - ICANN
  - IAB
  - IRTF
  - ...

# Staying Safe



- Don't use the Dark Web
- Use a VPN to access P2P sites
- Run an updated anti-virus program
- Maintain an off-site backup (of personal files)
- Don't change your modem/router firewall settings (except DNS)
- Take advantage!



# Jeff Maynard

How the Internet works