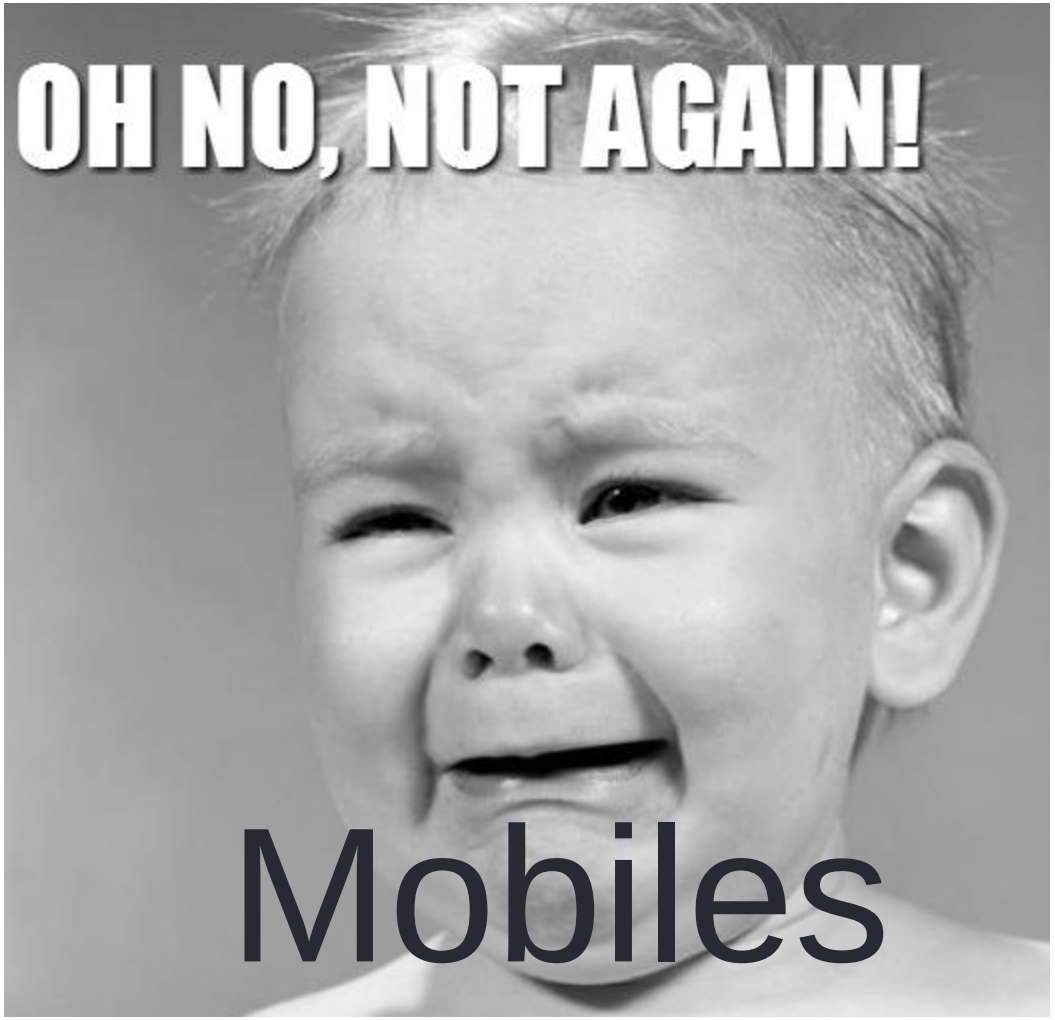
# UNIT 307: MOBILE AND OS

Outcome 2: Understand remote operation, deployment and secure integration of mobile devices

5/6/19

Swaraj Jeyasingh


OH NO, NOT AGAIN!
Mobiles

# Agenda for the day

- 9.00– 1000 – Intro and mobile connectivity
- 1000 – 1030 – Break
- 1030 – 1100 – Deployment & Security
- 1100 – 1200 – Remote Support
- 1200 – 1300 – Lunch

- Next week – Remote Management & Policies

# A+ 902 - Mobile Phones

- OS x 3
- Application – sources
- Sensors and Calibration
- OS features
- Connectivity and Email
- Airplane Mode
- Updates
- Mobile Data
- Mobile VPN
- Hotspots and Tethering
- Configuring Email = POP, IMAP, Exchange
- Mobile Synchronisation – Apple – Itunes, Icloud
- Android
- S/W Installation Reqts

Topics highlighted in yellow will be also mentioned in this Unit

# 307: Mobility in the Enterprise

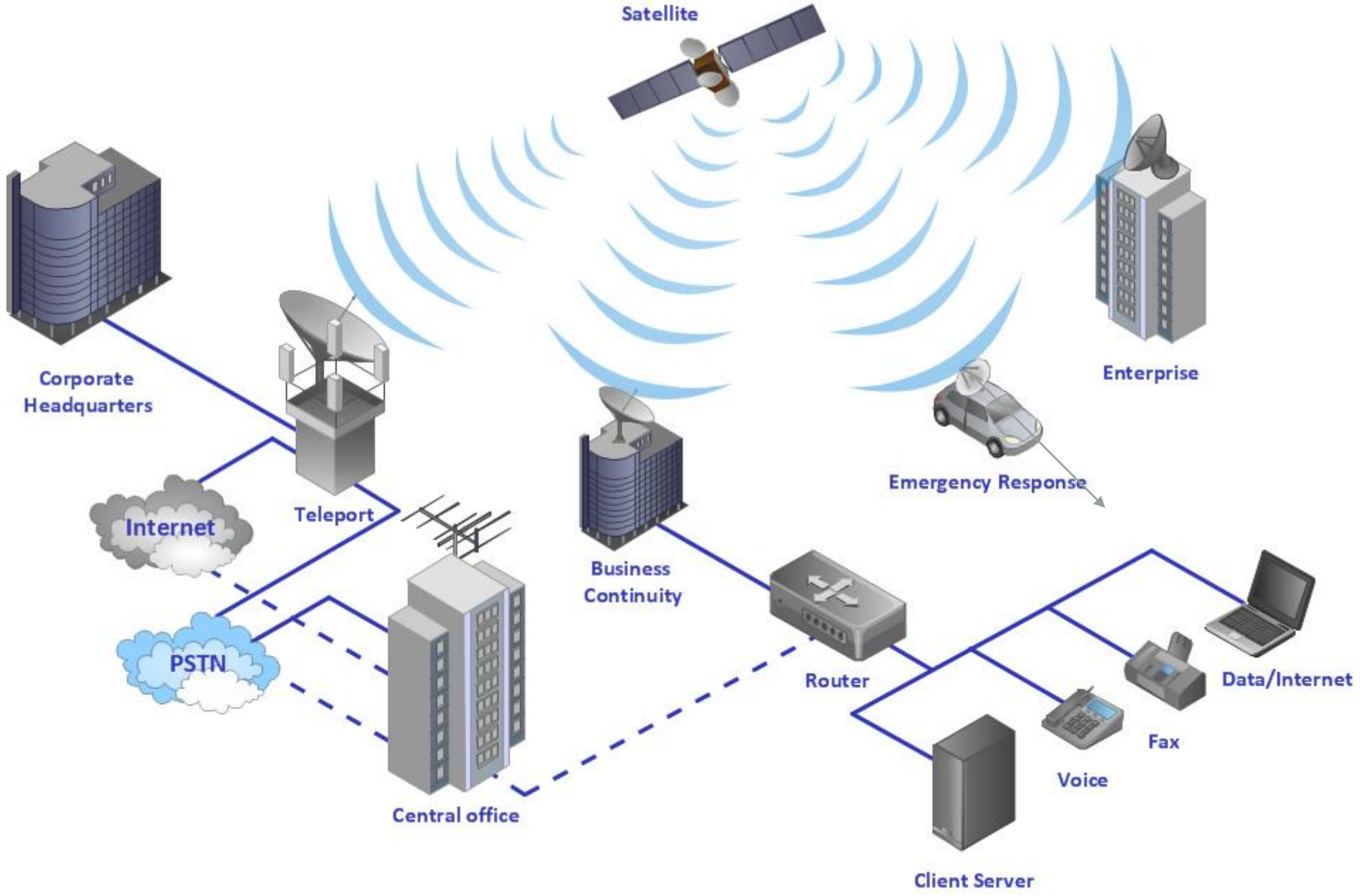
Outcome 2: Understand remote operation, deployment and secure integration of mobile devices.

Specifically,

- To Configure a mobile device to meet business specifications.
- To Maintain a mobile device by providing remote support

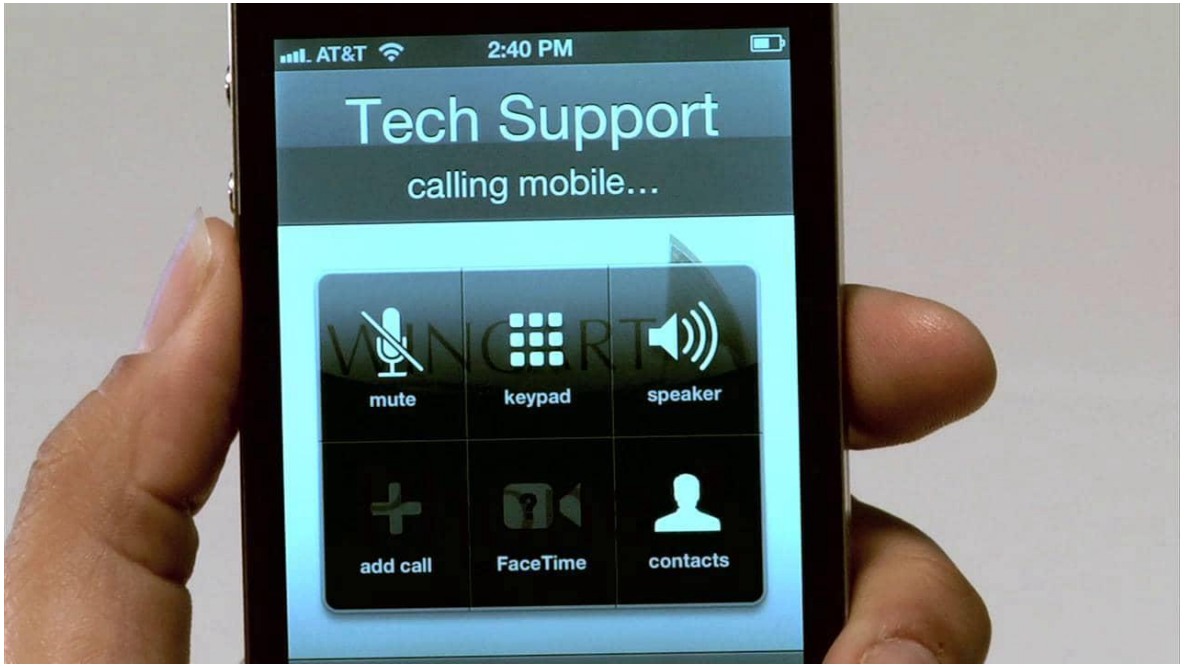
# Remote working


Thrane & Thrane


Satellite
Corporate Headquarters
Teleport
Internet
PSTN
Central office
Business Continuity
Emergency Response
Enterprise
Router
Data/Internet
Fax
Voice
Client Server

# Understand Remote Operation, Deployment and Secure Integration of Mobile Devices

- 2.1 Deployment
- 2.2 Remote Support
- 2.3 Remote Management



# 2.1 Deploy remote mobile comms

- Setting up a mobile device network/connection
  - Devices
  - Physical Connectivity
  - Frequency Bands
  - Antenna placements
  - Channels
  - Standards
  - Networks
  - Security

# Platforms and Devices Integration

- Choosing the right device: smartphone, tablet
- Choosing OS: Android, IOS
- Applications: productivity, specialist,
- Getting everything to work together seamlessly from any device or platform and from anywhere.
- Managed centrally


Wireless Router Network Diagram
Internet
MP3 Player
HDD
Cable Modem
WEB Camera
Printer
Wireless router
Desktop PC
Media PC
IP Camera
Digital Camera
Wireless Media Player
Smartphone
Laptop
Entertainment

# Physical Connectivity

Different ways of connecting to a network wirelessly using different frequencies/technologies:

- Satellite - global, expensive, niche
- WiFi – best experience, more data=> big files, streaming, updates, apps, WhatsApp – mostly within buildings and some urban
- Mobile phone signal/cellular/2G– voice and text/SMS; almost nationwide
- Mobile With DATA enabled - 3G/4G/5G – internet, files, VOIP,
- Bluetooth – some file transfer
- NFC - Near Field Communications - no file transfer

Choice depend on location, convenience, cost, device capability

# Antenna

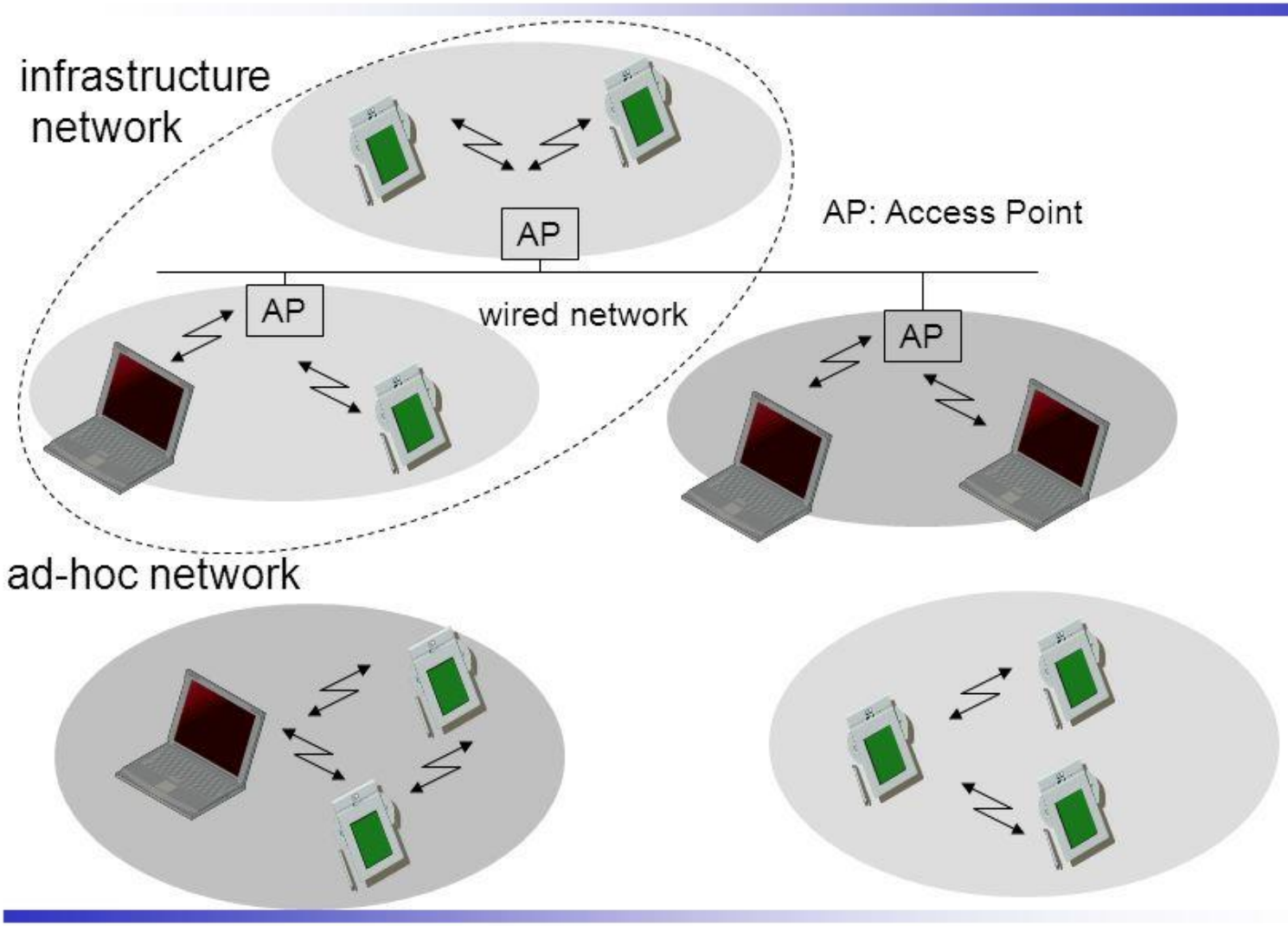



# Implementation

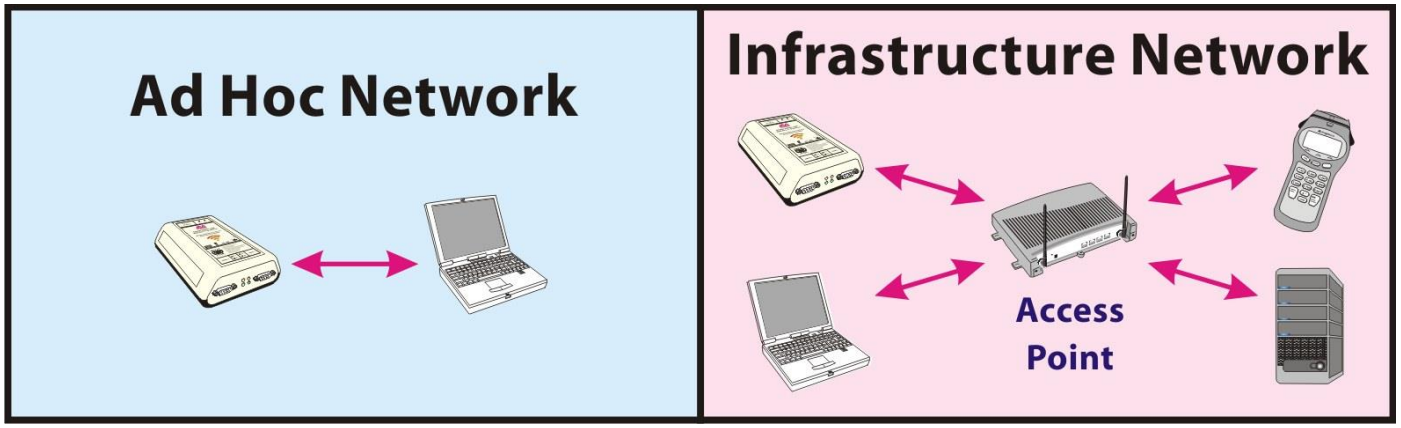
- Dial up – hardly used now
- ATM and Frame Relay (connection oriented) typically Carrier based (e.g. BT)
- IP and MPLS over ADSL (connectionless) – Internet VPN – cheapest but least performance and security

- To prevent disclosure of private information, VPNs typically allow only authenticated remote access using tunnelling protocols and encryption techniques.

# Comparison: infrastructure vs. ad-hoc networks



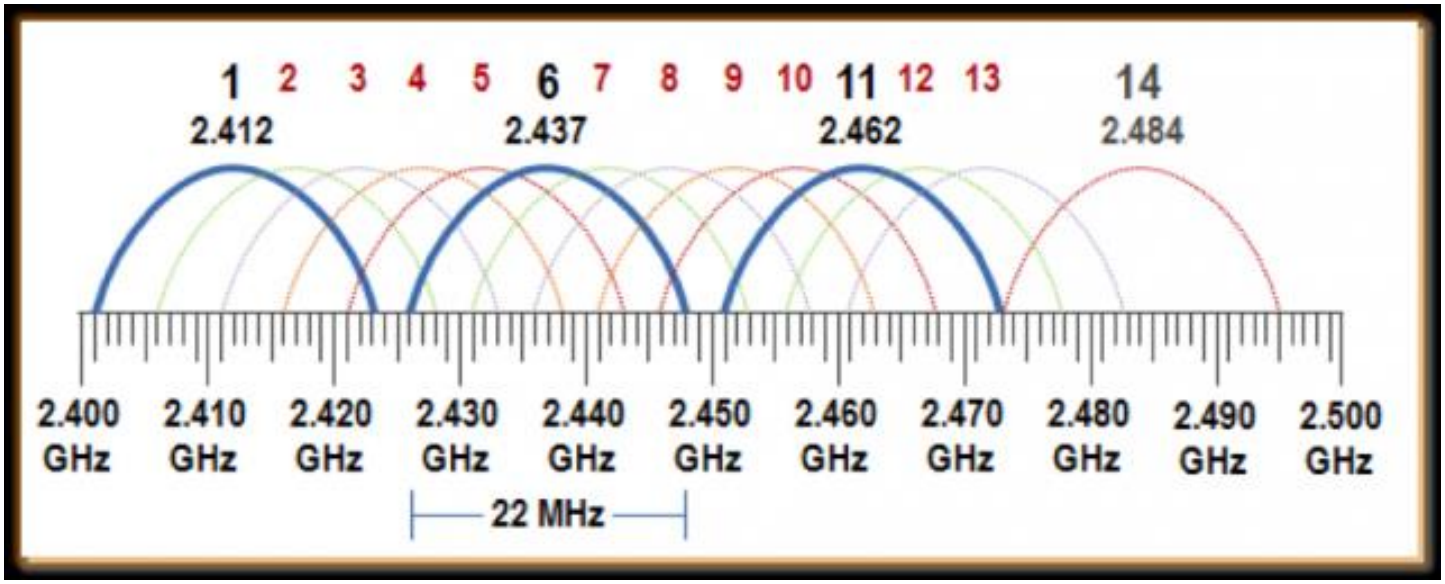
# Ad Hoc / Infrastructure Connection




- No central admin
- Each node can act as router
- Quick to set up/take down but not efficient

# Wi-Fi – 2.4 Ghz Band Channels

- The 2.4ghz band starts at 2.4ghz and ends just short of 2.5ghz.
- This gives it a total of 0.1ghz or 100mhz of bandwidth.
- This space is then split up into different *channels*, each 22mhz wide (only 20mhz is used).
- Each channel overlaps with other channels



## Is 5 Ghz Better than 2.4GHz?

More available channels

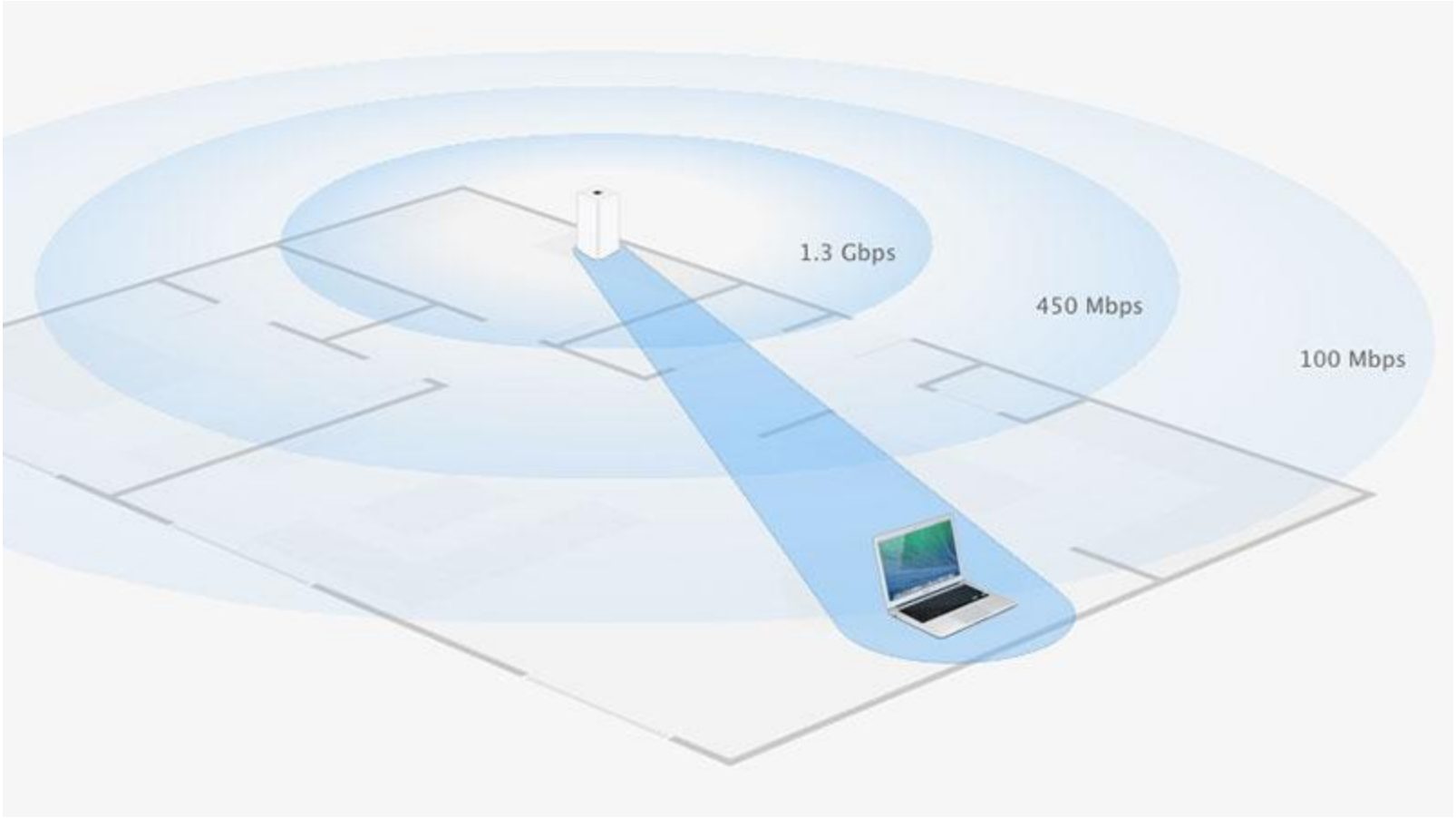
Non-overlapping channels

Less crowded

Reduced range

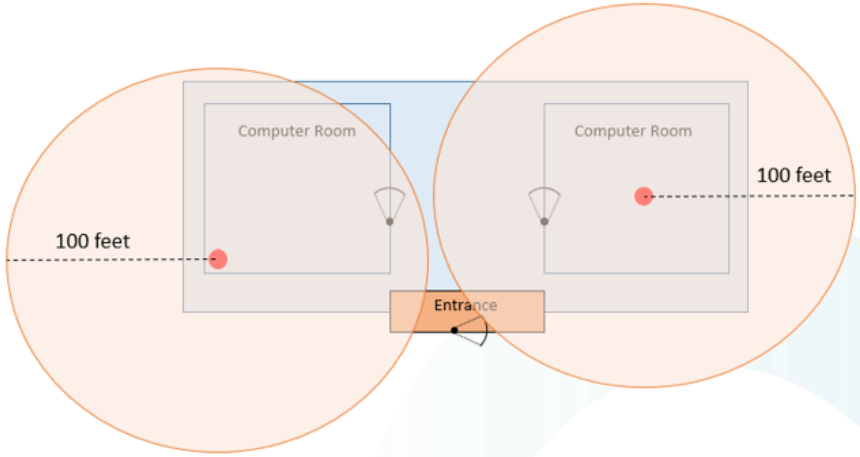
Worse attenuation through solid objects

# WiFi Range



# Antenna Placement

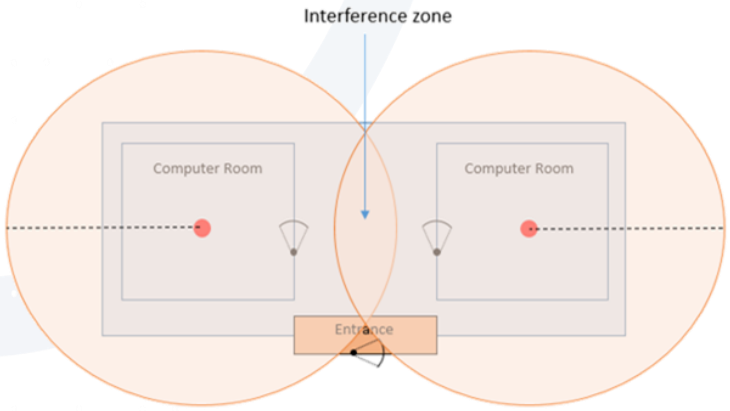
- Wi-Fi typically has a maximum indoor range of 30m / 100 feet.
- The weaker the signal, the lower the data rate.
- Signals pass through solid objects but are weakened in doing so
- Other radio devices can cause interference
- **What issues can you identify with the pictured setup?**

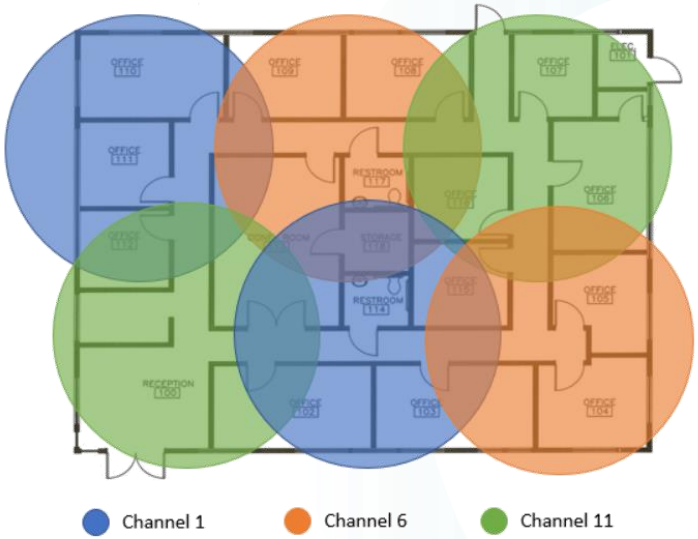



- In this example, both APs are causing a potential security risk as the signal extends well beyond the building
    - Lower device power or alter device placement
- Areas with poor coverage
    - Alter device placement or use additional access points

# Antenna Placement

- APs with overlapping coverage can cause interference
- At 2.4 Ghz, use non-overlapping channels, e.g. 1, 6, 11
- At 5 Ghz, use any two different channels
- Alternatively, use 2.4 Ghz on one AP and 5 Ghz on the other



# Hotspot

- Hotspot – for enabling several WiFi capable device to connect to a single data enabled phone

# Tethering

Tethering - For situations when no wifi is available but mobile data is available;  connect a laptop to a mobile network  via a mobile phone using a USB cable. Laptop can now access the internet.

# Wireless Standards

- Wireless LAN – based on IEEE802 => 802.11
- Most important versions
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
  - 802.11ac
- Make sure equipment is compatible. Older router cannot support newer devices except at older speed levels.

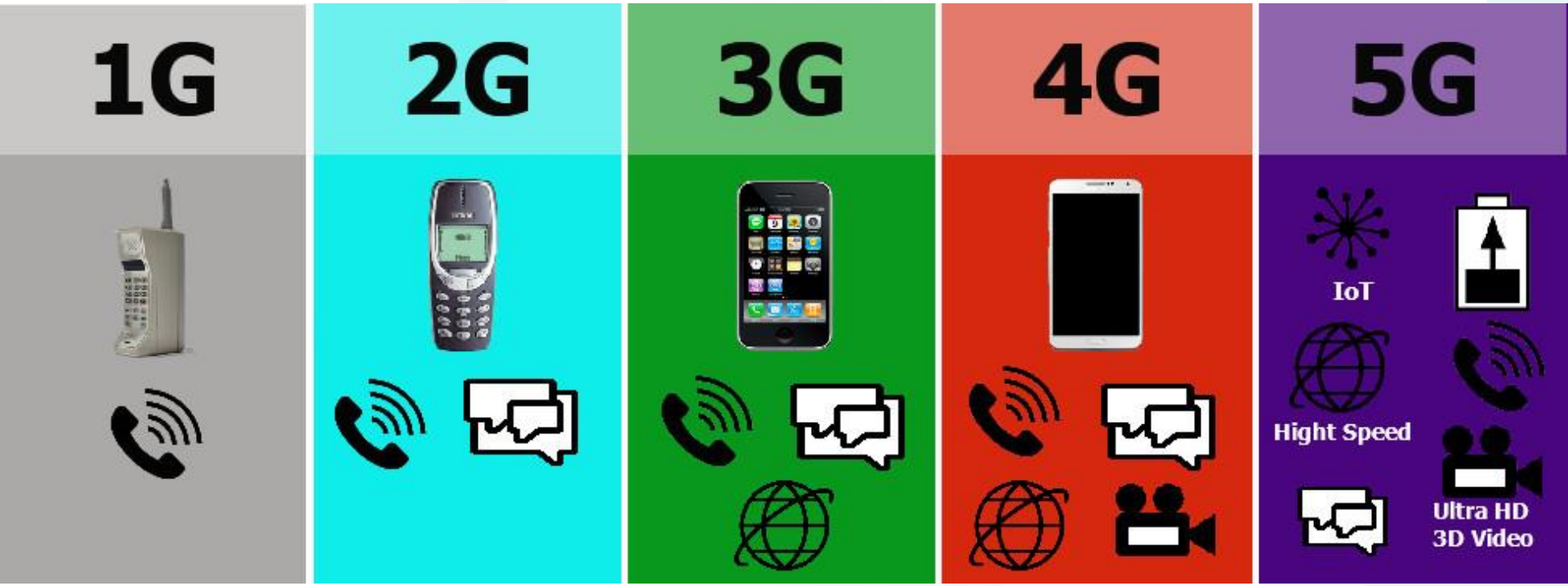
# WiFi Standards

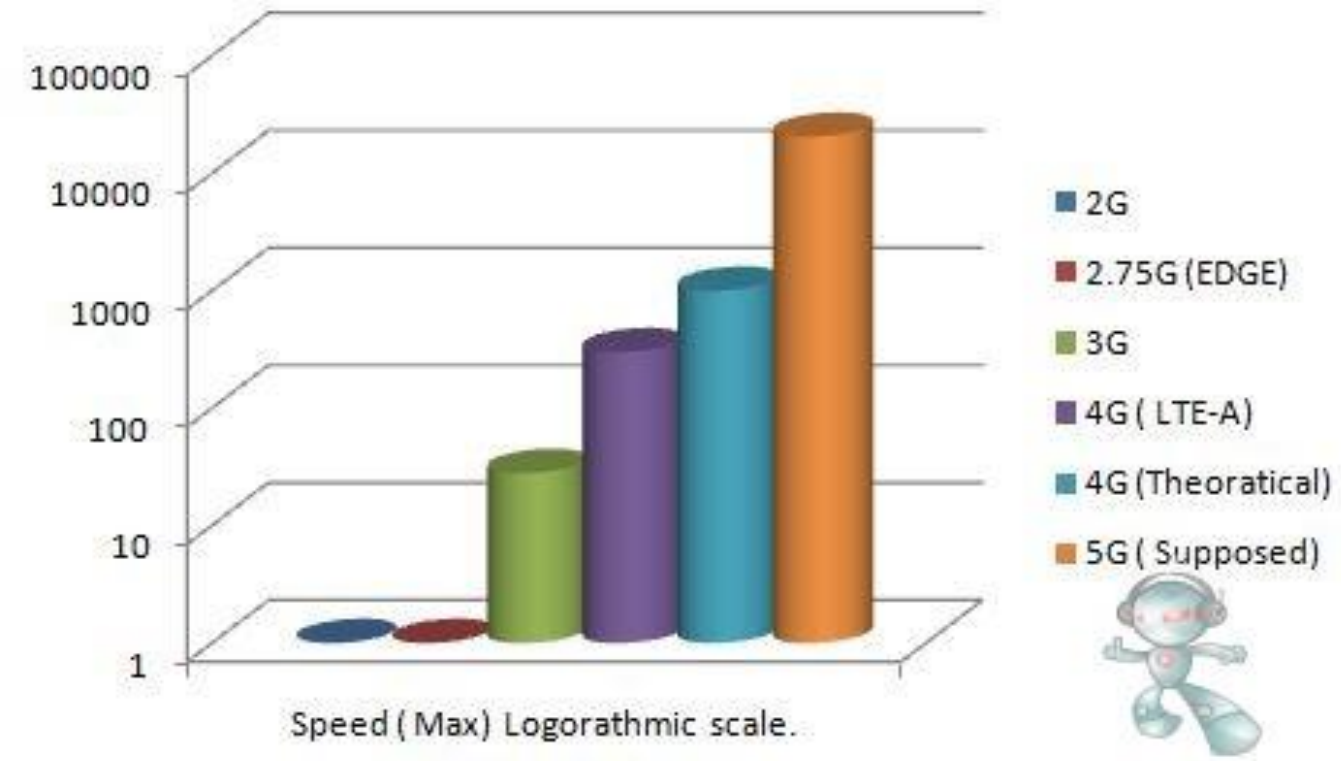
| Standard | Frequency | Max Streams | Bandwidth | Max Speed per Stream | Total Max Speed |
|---|---|---|---|---|---|
| 802.11a | 5 Ghz | 1 | 20 Mhz | 54 Mbps | 54 Mbps |
| 802.11b | 2.4 Ghz | 1 | 20 Mhz | 11 Mbps | 11 Mbps |
| 802.11g | 2.4 Ghz | 1 | 20 Mhz | 54 Mbps | 54 Mbps |
| 802.11n | 2.4 Ghz<br>5 Ghz | 4 | 20 or 40 Mhz | 150 | 600 Mbps |
| 802.11ac | 2.4GHz<br>5 Ghz | 8* | 20 Mhz | 86.7 | 693.6 Mbps |
| | | | 40 Mhz | 200 | 1600 Mbps |
| | | | 80 Mhz | 433 | 3464 Mbps |
| | | | 160 Mhz | 866.7 | 6933 Mbps |

802.11a was faster mainly because it used an encoding system called OFDM whilst 802.11b used DSSS. From 802.11g onwards, OFDM was adopted.

- For 802.11n, think of the possible speeds as multiples of ~72 and 150mbps depending on number of streams and channel bandwidth.
- For 802.11ac, think of it in terms of multiples of either 200 or 433 as 40mhz and 80mhz channels are most common. A typical maximum capacity on a SOHO router is 3 streams at 80mhz, which gives 1.3 Gbps.

# 5G Evolution




100000
10000
1000
100
10
1
2G
2.75G (EDGE)
3G
4G ( LTE-A)
4G (Theoratical)
5G ( Supposed)
Speed ( Max) Logorathmic scale.

# Break!

# Wireless Security

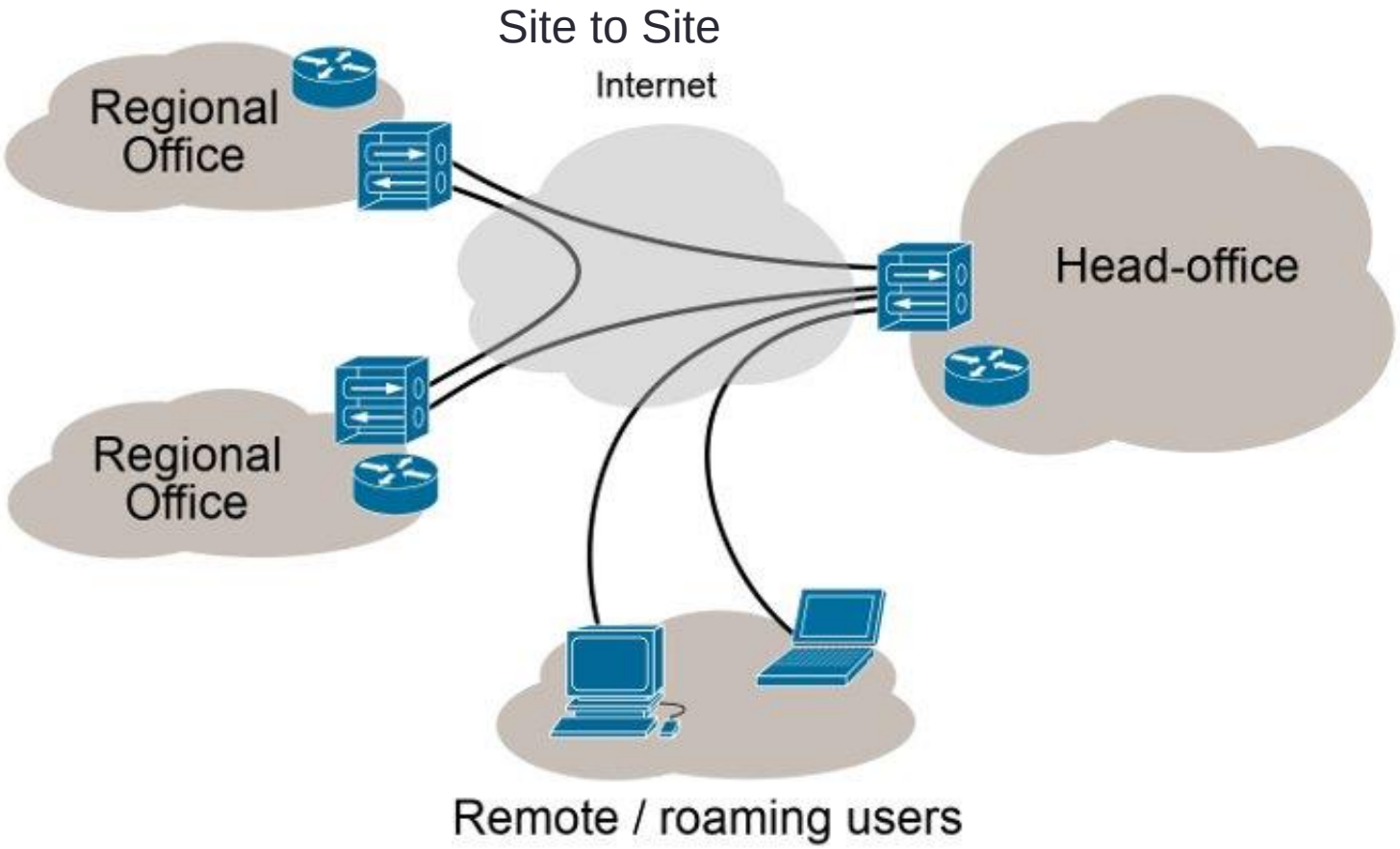
- SSID – can be hidden, guest network,
- Encryption: WEP, WPA, WPA2 – use WPA2
- Time limit on network key
- Limit access (time) using IP address or MAC address
- Power control - no need to blast the whole world
- Link to active directory in enterprise working - name and password instead of pre-shared key (PSK)
- Physical security of Wireless Access Point

# VPN – Virtual Private Network

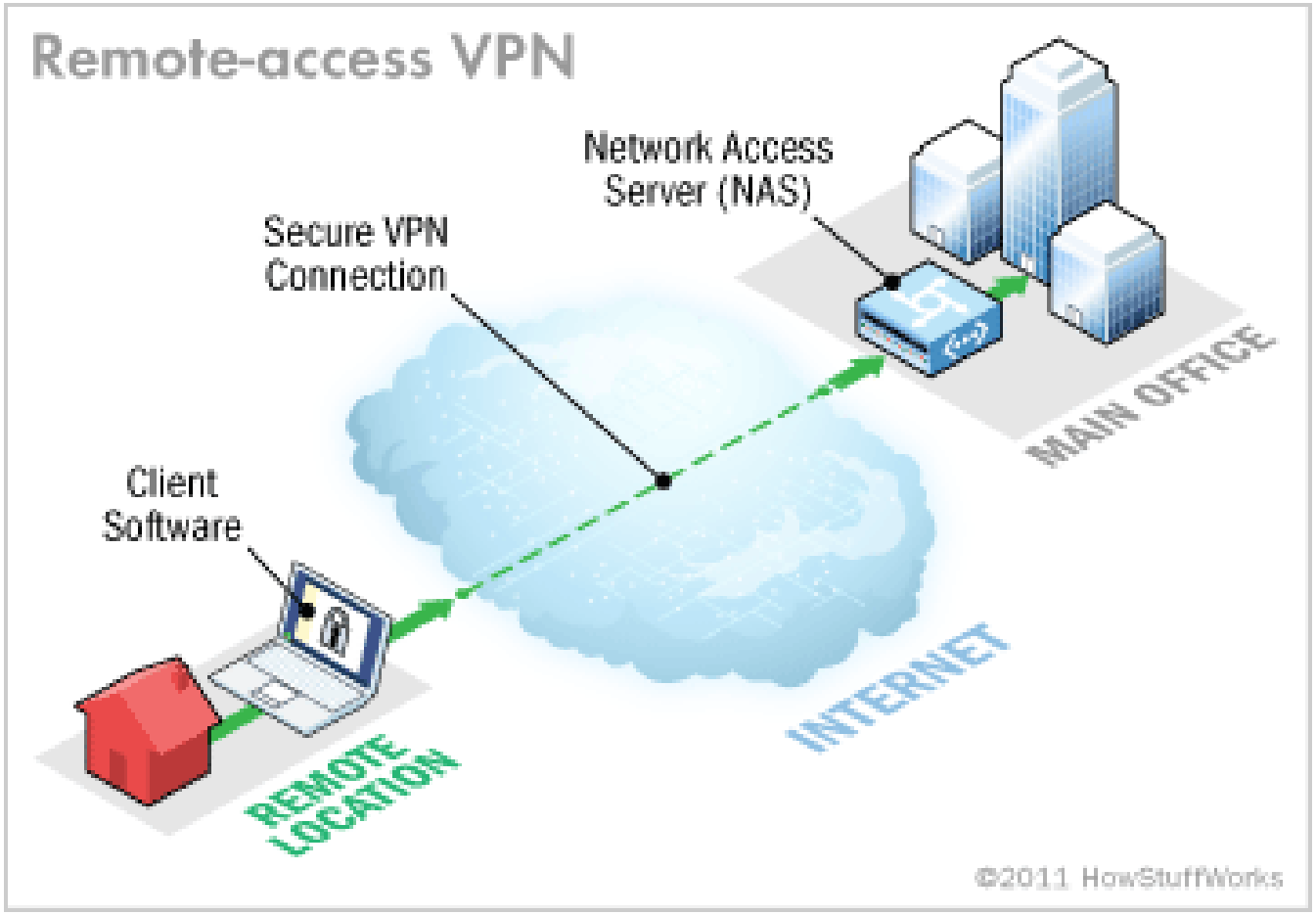
- Virtually private i.e not really but almost!
- It is a private network across a public network
  - Private taxi using the public roads
  - Private anything (cars, jet, boat)  is expensive
  - Private connection (road, river, connection) even more!
  - Private dedicated line or leased line is £££££
- This is a compromise
- Files and folders in remote office appears “locally”
- Keeps content private while using public highways
- Can carry both voice and data
- Paid and free service providers

# Protecting privacy while using public roads

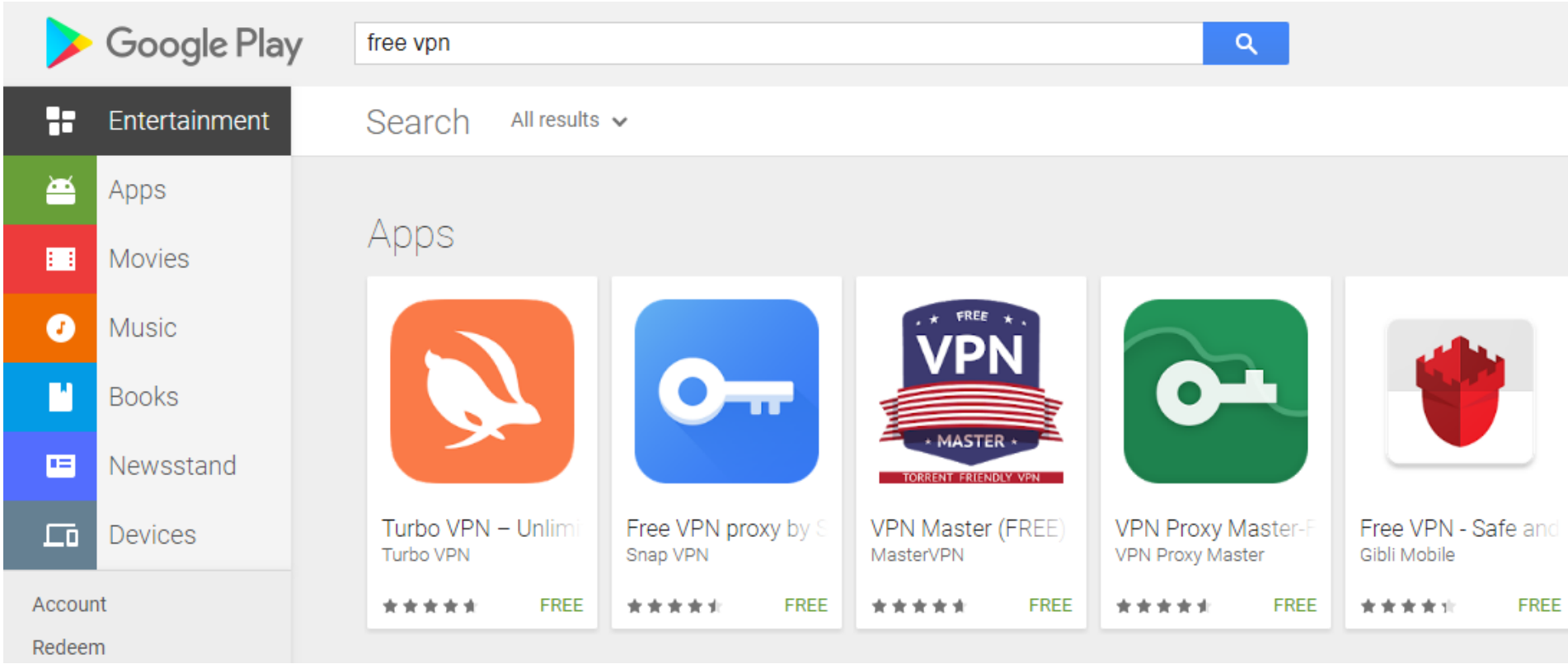
# Internet VPN



# Remote Access VPN



# VPN Client for Mobiles



# mVPN

Can maintain connection even if switching networks, connection points etc – more robust that conventional VPNs

Useful  for travelling/field workers

Fixed VPNs also available

Good security features

Support for Mobile Management

# VPN Types

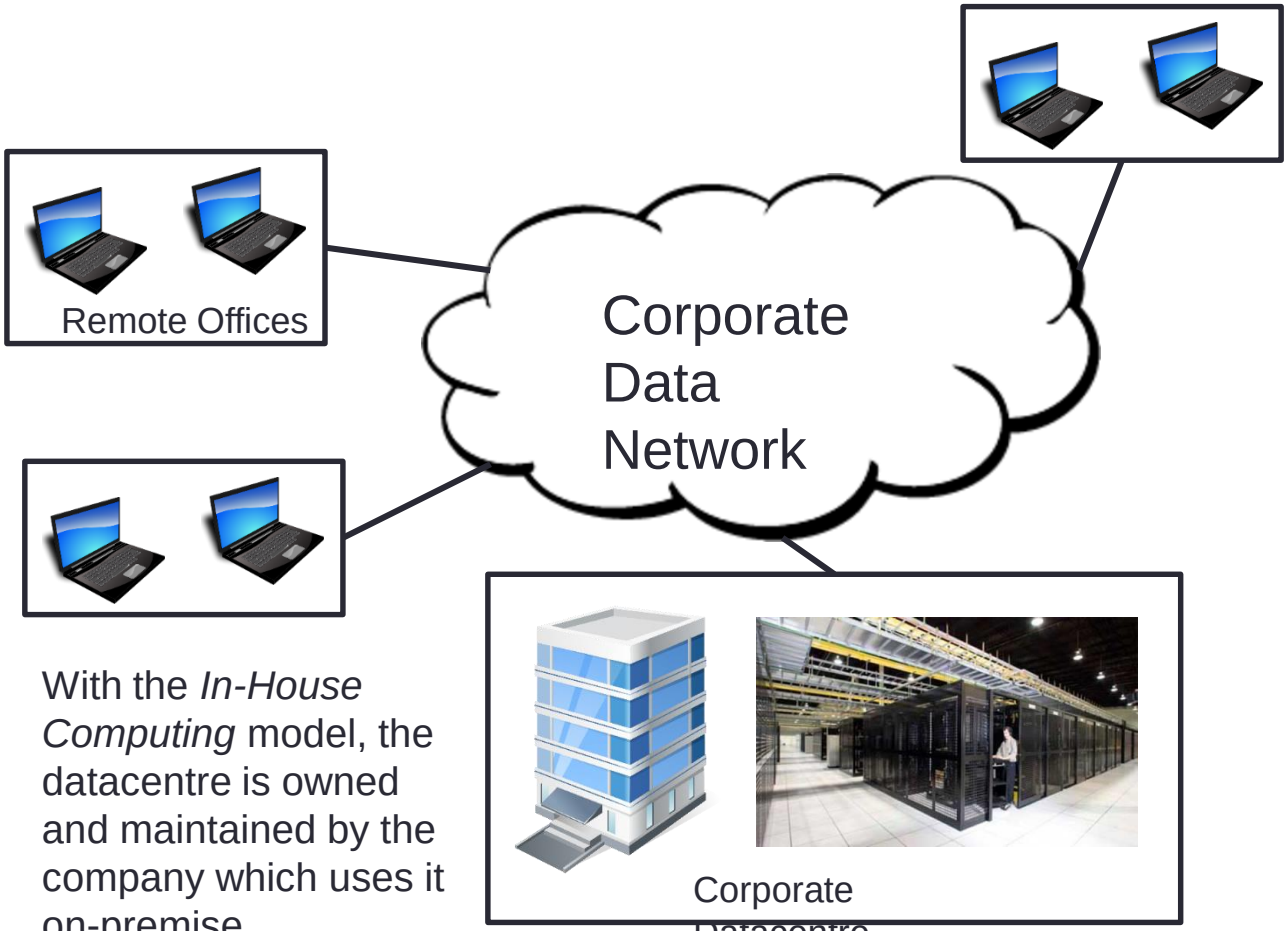
- VPN systems may be classified by:
  - the tunnelling protocol used to tunnel the traffic (GRE, L2TP, IPSec)
  - the tunnel's termination point location, e.g., on the customer edge or network-provider edge (Remote site/Inter site)
  - the type of topology of connections, such as site-to-site or network-to-network
  - the levels of security provided (Transport mode or Tunnel mode)
  - the OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
  - the number of simultaneous connections.

# Tunneling

- Allows a network user to access or provide a network service that the underlying network does not support or provide directly
- Analgous to Channel Tunnel (vehicle inside carriage)
- E.g, running IPv6 over IPv4, between two LANs over a WAN
- tunneling involves repackaging the traffic data into a different form (encapsulation)
- Encryption often as standard
- to hide the nature of the traffic that is run through the tunnels.
- works by using the data portion of a packet (the payload) to carry the packets that actually provide the service
- Ignores the layering when using the payload to carry a service not normally provided by the network

# Alternatives to VPN

- Cloud based services - More flexible, more secure
- TeamViewer, Dropbox, etc




With the *In-House Computing* model, the datacentre is owned and maintained by the company which uses it on-premise.

# O2: Understand Remote Operation, Deployment and Secure Integration of Mobile Devices

- 2.1 Deployment
- 2.2 Remote Support
- 2.3 Remote Management

# 2.2 Delivering Remote Support: Access and Security

Topics to cover:

- Authentication – you are who you say you are - HOW
- Authorisation – you are allowed to do something
- Access Control – limit who can access and what
- Auditing – who has accessed and what and when
- Remote Wipe – when phone is withdrawn or lost
- Auto-Wipe – after specified actions (5 failed logins)
- Remote Desktop – Alternative to VPN for the user
- Manage BYOD – Convenience versus Security

# Authentication

- NOT the same as identification
- Authentication often involves verifying the validity of at least one form of identification.
  - Something you know (BEEN TOLD) (password, PIN, response)
  - Something about you (inherited) – DNA, Fingerprint
  - Something you physically have (token, ID card, device)
- Authentication type
  - Single factor - password
  - Two factor – e,g. card and PIN
  - Multiple Factor – e.g. token, Bio and  day code
- Strong authentication
- Continuous authentication

  - Having 5 passwords doesnt make it multifactor!

# Protocols

A communications protocol specifically designed for transfer of authentication data between two entities. Both need to authenticate each other and observe the following

- A Protocol has to involve two or more parties and everyone involved in the protocol must know the protocol in advance.
- All the included parties have to follow the protocol
- A protocol has to be unambiguous - each step must be defined precisely.
- A protocol must be complete - must include a specified action for every possible situation

# Authentication Protocols

Common Protocols used

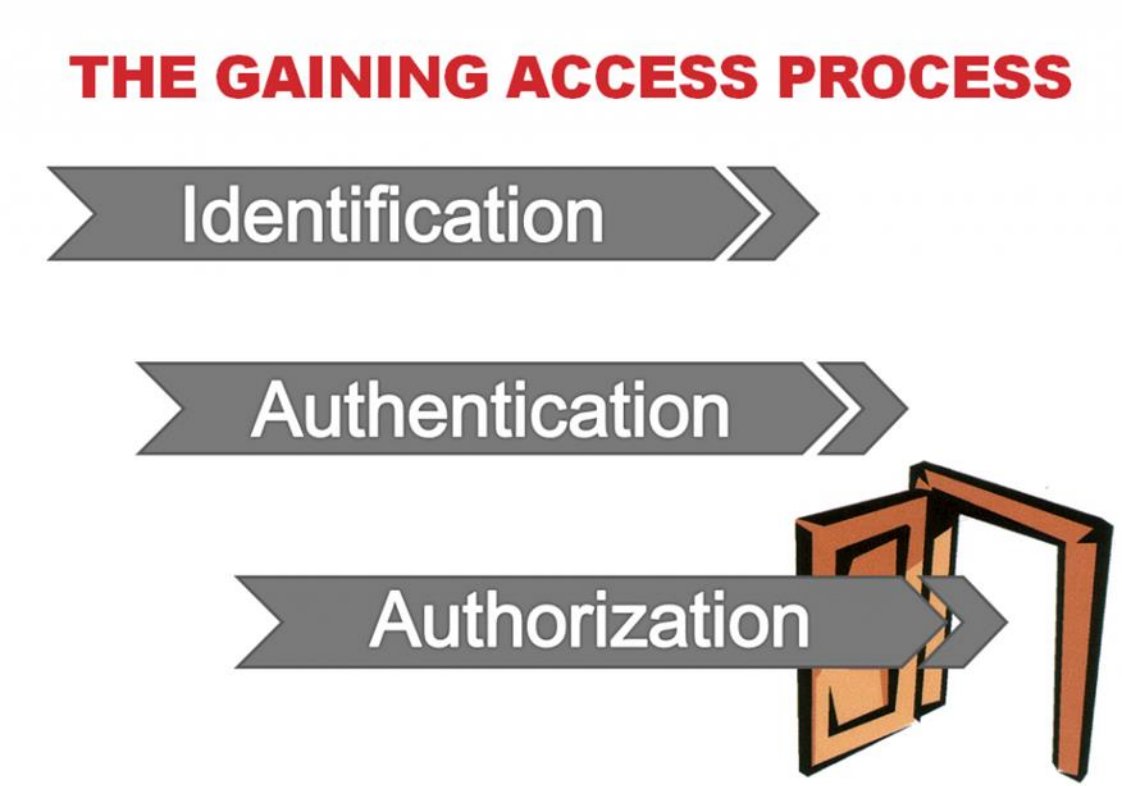
- PAP – Password Authentication Protocol – Old and insecure as password is open text
- CHAPS – Challenge-handshake authentication protocol – uses hash function
- EAP - Extensible Authentication Protocol – widely used and in many forms - a framework for methods such as
  - EAP-MD5
  - EAP-TLS
  - EAP-TTLS
  - EAP-FAST
  - EAP-PEAP – Protected EAP, - MOST SECURE
- AAA – Authentication, Authorization and Accounting Protocols – e.g. RADIUS
- NTLM NT Lan Manager - suite of security and integrity protocols from MS
- KerberosV4 – widely used authentication protocol – replaced NTLM

# Authentication & Authorization

- Authentication
  - The process of verifying the digital identity of the sender of a communication, such as a request to log in
  - Establish a trust relationship between a provider of services and a consumer of services
- Authorization
  - Permissions granted to an authenticated user
- Authorization *follows* Authentication

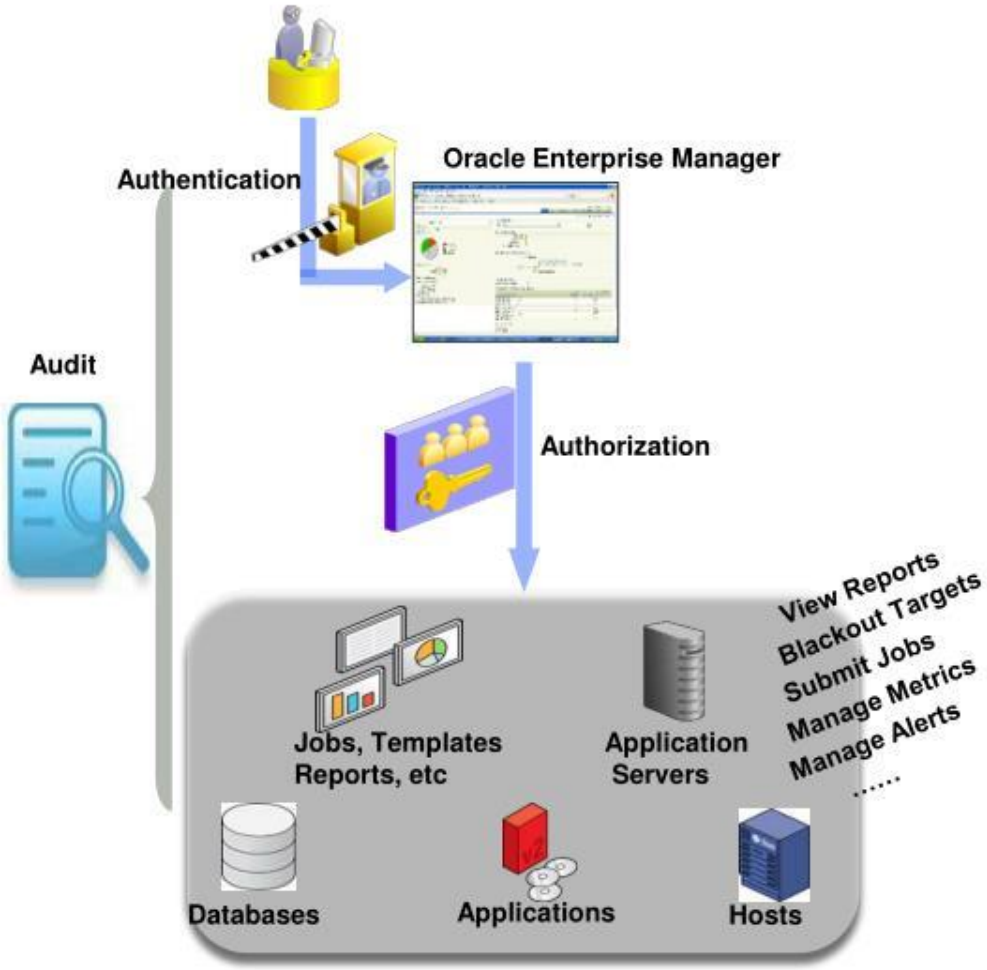
http://en.wikipedia.org/wiki/Authentication

# I, A, A


THE GAINING ACCESS PROCESS
Identification
Authentication
Authorization

# Authentication, Authorization and Auditing

## The Three A's

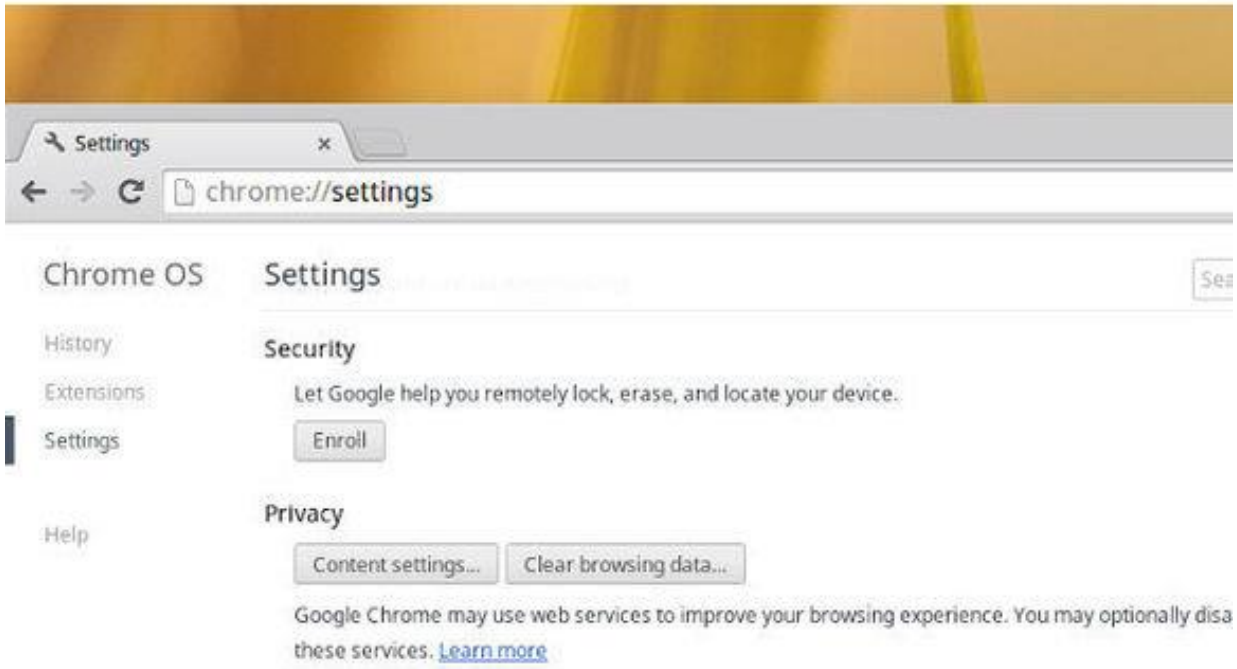



- Authentication
  - Determines whether someone is in fact who it is declared to be while accessing Enterprise Manager Grid Control
- Authorization
  - Provides access control to secure resources and functionalities within Enterprise Manager such as targets, jobs, templates, reports, etc.
- Audit
  - Keeps track of the actions happened within Enterprise Manager to prevent repudiation

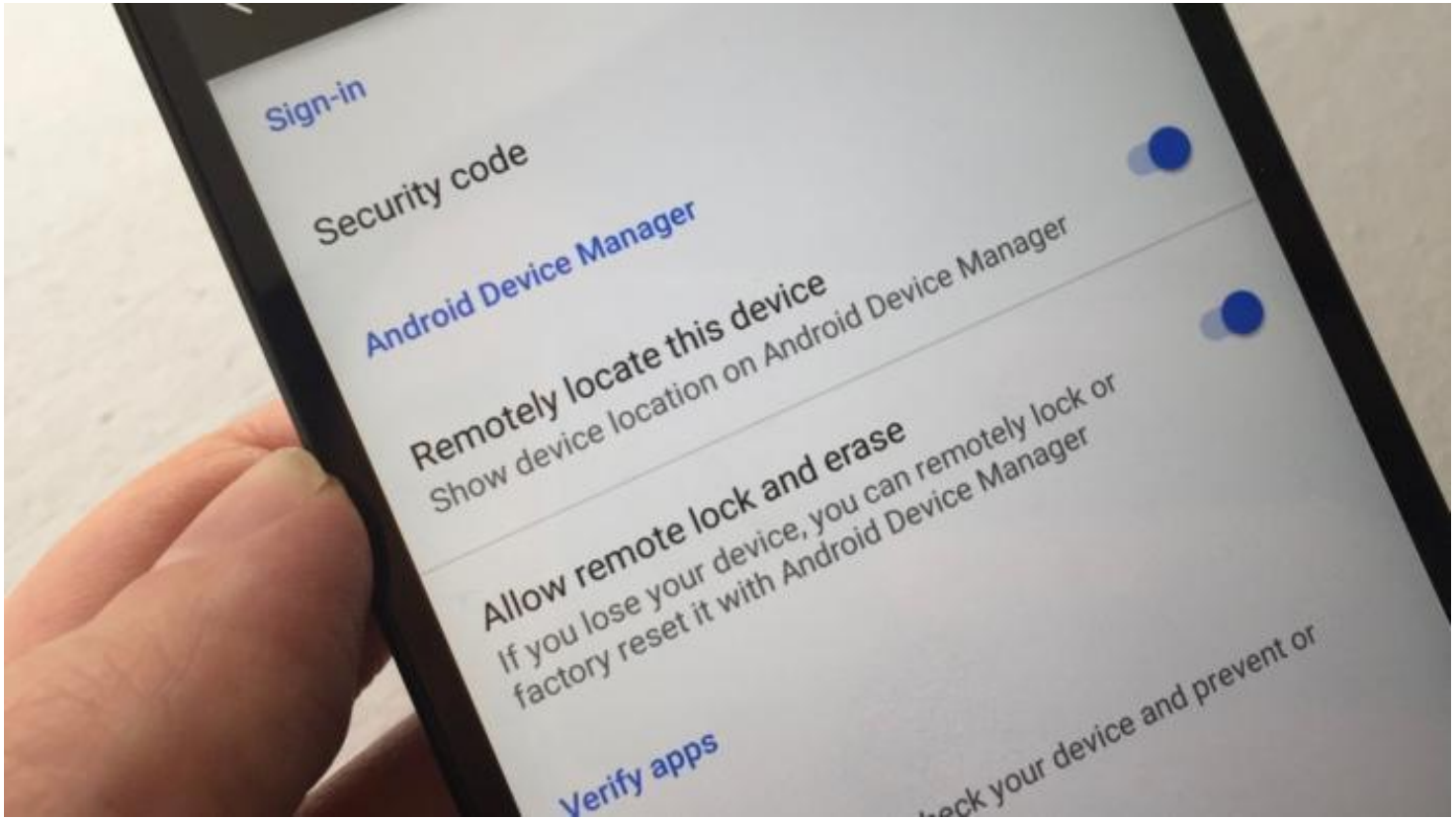
# Remote wipe

- Deleting all data on device if device is lost or stolen or just missing
- Typically when employee has left unexpectedly with phone.
- Only works if phone is connected to network
- Can be built in (Iphone) or additional download/app (Android) and needs setting up first.
- From another phone or web based
- Alternative is to lock up, factory reset, stop certain actions
- Auto wipe – to prevent fraudulent use

# Remote wipe of Chromebook



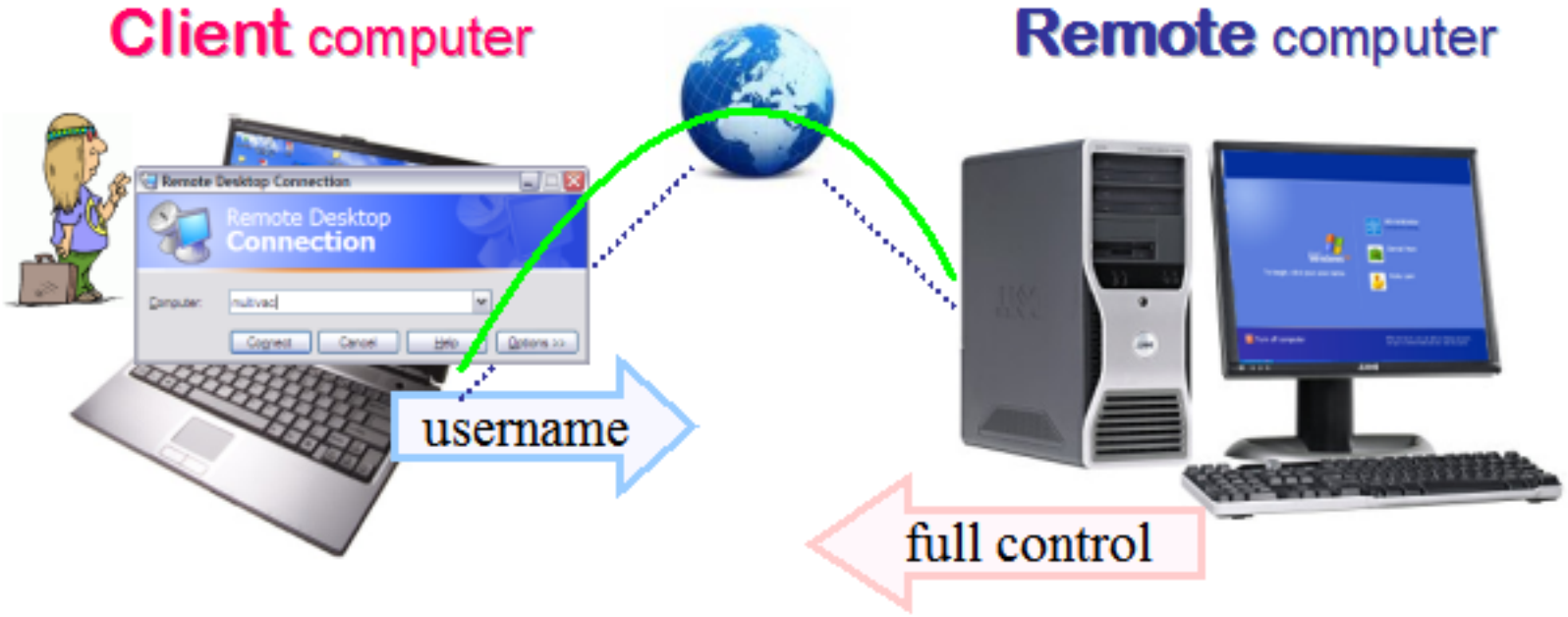
# Remote wipe - Android



# Remote Wipe


Info
OSXDaily.com
iPhone 4
Located 27 seconds ago.
Play Sound or Send Message
Remote Lock
Remote Wipe
Using remote wipe will prevent you from locating your iPhone.

# Remote Desktop – user aspect




Use this mouse/keyboard…

AKA Screen Sharing

…and this computer will do all the work, and send back a live image of the desktop

# Remote Desktop Requirements

- OS requirements – must support RDC
- Built in utility or installed application or  browser based
- Access authorisation/authentication method
- Open router or gateway port (e.g. 3389 for RDC but can be changed) Other apps may use other ports.
- Adequate bandwidth for desired performance/responsiveness
- Supporting Policies and procedures (covered later)
- Awareness of Computer Misuse Act – do you have permission to access their machine; And Data Protection Act – do you have access to any sensitive data.

# Remote Desktop Options

- Windows - Remote Desktop Connection/Services
- Linux – Remmina,
- MacOS – MS Remote desktop for Mac, Back to MyMac

Platform neutral

- VNC
- GoToMyPC
- LogMeIn
- NTR
- TeamView
- Skype screenshare
- Impero
- Other?

# Managed BYOD

- Why BYOD is popular
- Why is it a Risk
- Why does it need to be managed
- How can it be managed

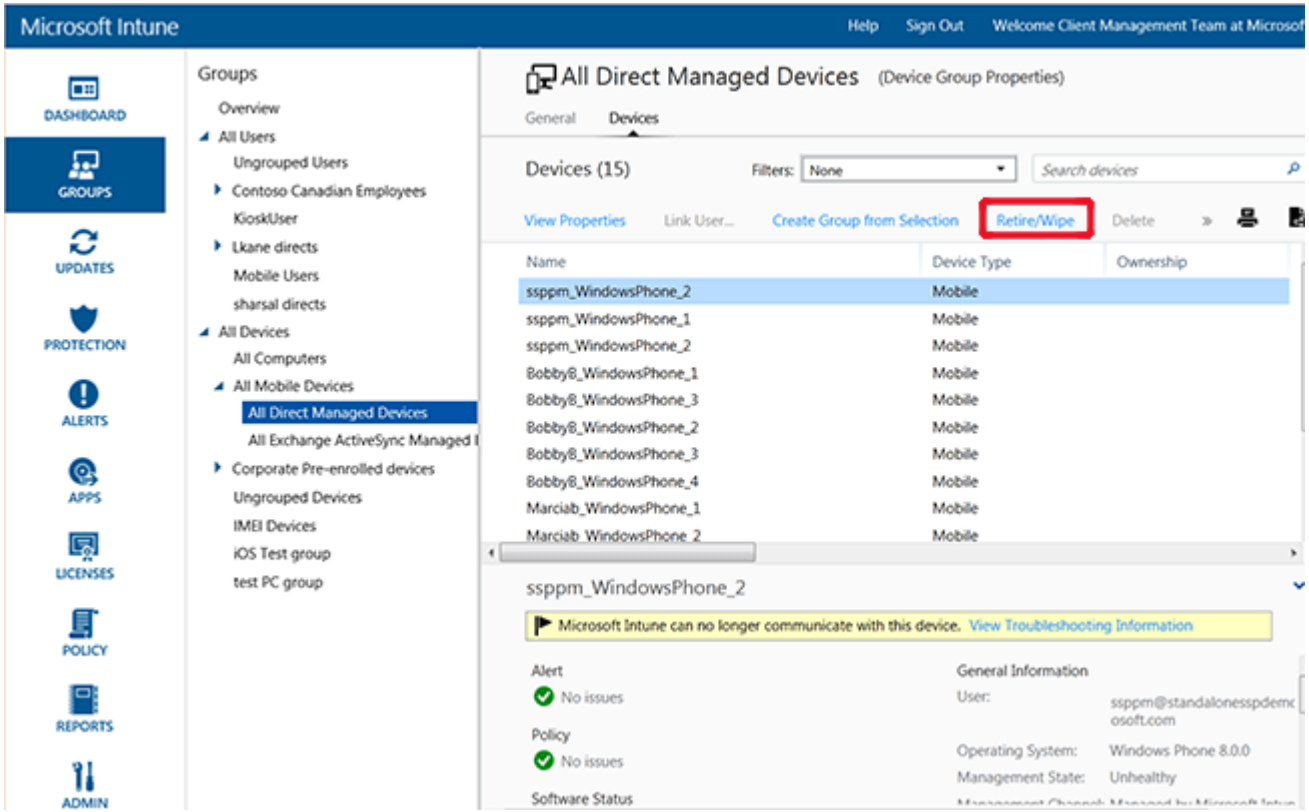
# Managed BYOD

- Why BYOD is popular – because people have individual tastes/pockets and don't want to carry two devices.
- Why is it a Risk – too many unknowns, contaminated at home and brought to work,
- Why does it need to be managed – to mitigate risk; to improve efficiency and business performance
- How can it be managed – by policies and procedures AND by specialist applications (management s/w)

# Enterprise Mobility Management (EMM)

- Mobility doesn't mean just using a smartphone
- But also laptops, netbooks, smartphones, tablets, iPads
- EMM allows organisations to manage data on their mobile devices
- Deploy, manage and withdraw from a central console
- Monitor usage, problems, trends
- Carry out remote audit and wipe (factory reset, lock up)
- Available for all devices: Android, IOS and Windows
- E.g SOTI, Microsoft InTune, Apple Device Enrolment Program, JAMF, Google Mobile Management (Gsuite)

# Example of EMM




That's all Folks!