**Module 2 Technologies & Tools**

**2.1 Network Components P1 – Networking Devices**

**Router**

* Connects computer networks
* Operate at Layer 3 (Network Layer)
* Stores information about network destinations (Routing table)
* Border Router – outside connection of LAN to WAN

**Router Security**

* Access Control Lists (ACLs) – filtering packets by source address, destination address, protocol or port
* Zones – segmenting networks based on functionality/security
* Anti-spoofing – creating set of access lists that deny access to private IP addresses & local host ranges from internet

**Switch**

* Connects devices with computer network by using packet switching to receive, process & forward data to destination device
* Either Layer 2 (Data Link) or Layer 3 (Network)
* Packet-forwarding decisions based on Media Access Control (MAC) addresses

**Switch Security**

* Virtual LANs (VLANs) – segment networks & limit broadcast traffic
* Port Security – Layer 2 feature

1. Enable/disable individual switch ports based on MAC address
2. Can take 1 of following actions when detecting violation
3. Default shutdown mode
4. Protect mode
5. Restrict mode
6. Vulnerable to MAC address spoofing

* Loop Prevention

1. When data units travel from 1st LAN segment to 2nd LAN segment through more than 1 path (Can happen on switches/bridges)
2. Solution – Spanning Tree Protocol (STP), a link-management protocol that provides path redundancy while preventing undesirable loops in network

* Flood Guard – detect & prevent malicious traffic (normally associated with DoS attacks)

**Bridge**

* Connect 2 different physical networks
* Layer 2 (Data Link)
* Replaced by switches
* Bridge Loops (like switch loops)

**Network Address Translation (NAT)**

* Method of remapping 1 IP address space into another by modifying network address information in IP header of packets while they’re in transit across traffic routing device
* All devices in network share same public IP address (so there won’t be a lack of public IP)

**Proxy**

* Boundary device between internal & external networks
* Any device that acts on behalf of other(s) (Provide security, logging & caching)
* Proxy Server – blocks known malicious websites
* Forward Proxy – retrieves data on behalf of client
* Reverse Proxy – protects access to server on internal network
* Transparent Proxy (AKA intercepting/inline/forced proxy) – caching server that redirects client requests w/o modifying them to reduce bandwidth usage

**Load Balancer**

* Shifting burden from 1 device to another
* Benefits

1. Reduces response time
2. Maximises throughput
3. Allows better allocation of resource

* Scheduling – distributing load

1. Round-Robin – taking turns using circular pattern
2. Affinity (AKA Sticky Session) – requests sent to specific app
3. Least connections
4. Random

* Active/active – servers work together
* Active/passive – all traffic sent to active server
* Virtual IPs (VIPs) – at least 1 physical server assigned, but more than 1 virtual IP address assigned (Doesn’t correspond to a physical network interface)

**Access Points**

* Typically wireless (WAP)
* Layer 2 (Data Link) of OSI model
* Can operate as bridge connecting standard wired network to wireless devices/router passing data transmissions from 1 access point to another
* Consist of transmitter & receiver (transceiver) device used to create wireless LAN (WLAN)
* Centralised access controller (AC) capable of providing management, configuration, encryption & policy settings for WLAN access points

**Access Controllers**

* Fat – intelligent access points
* Fit – scaled Fat
* Thin – intelligent antennas (only transmit/receive)
* Controller-based vs. standalone

**Wireless Management & Security**

* SSID (Service Set Identifier)

1. Broadcast
2. Cloaked

* MAC Filtering
* Signal Strength
* Band selection/width
* Antenna types & placement

1. Omnidirectional
2. Directional