Chapter 3

Exploring network technologies and tools

horizontal line

# Basic network concepts

# Basic networking protocols

**TCP**: Transmission control protocol. Provides connection oriented traffic using 3 way handshake, providing guaranteed delivery

1. Client sends SYN packet
2. Server responds with SYN/ACK
3. Client completes handshake by sending ACK to establish connection

**UDP**: User Datagram Protocol. Provides connectionless sessions without three way traffic, without using extra traffic. Used by ICMP, and DoS attacks.

**IP**: Internet protocol, identifies hosts in TCP/IP network and delivers traffic between hosts using IP addresses

**ICMP**: Internet Control Message Protocol. Used for testing basic connectivity and includes ping and netstat commands. Can be blocked to prevent DoS

**ARP**: Address Resolution Protocol. Resolves IP addresses to MAC addresses. Required once a packet reaches destination. ARP poisoning use ARP packets to give clients false MAC address updates and disrupt/redirect internet attacks.

**NDP**: Neighbor Discovery Protocol, performs similar functions to ARP, and can also discover other IP addresses on network.

# Protocols for use cases

**Voice/Video**: Uses UDP. SRTP (Secure Real time transport Protocol) delivers audio/video over IP networks with security to protect integrity, and protect against replay attacks

**File transfer:**

* **FTP**: File Transfer Protocol. Uploads and downloads from large files to and from FTP server, but in cleartext. Uses TCP port 21 for control signals and port 20 for data. FTP Passive mode uses random TCP port for data. FTP random data is often blocked by a fire wall, so it is better to disable PASV in FTP clients.
* **TFTP**: Trivial File Transfer Protocol. Uses UDP port 69, and is used for transferring small amounts of data. Is not important so is usually disabled.

**Encryption protocols:**

* SSH: Secure Shell. Encrypts traffic in transit and can be used to encrypt other protocols such as FTP. Telnet is used in Linux to administer remote systems, but this transfers data in cleartext, so SSH is prefered. SCP (Secure Copy) is based on SSH. TCP port 3389.
* SSL: Secure Sockets Layer. Primary method to encrypt HTTP as HTTPS, but it has been compromised.
* TLS: Transport Layer Security. Replacement for SSL, and used with STARTTLS, which is a command to upgrade a connection to be encrypted.
* IPSec: IP security. Encrypts IP traffic and uses tunnel mode to protect VPN traffic. Uses:
  + AH: Authentication header, identified by protocol ID number 51
  + IKE: Internet key Exchange over UDP port 500 to create security association for VPN
* SFTP: Secure FTP. Extension of SSH, using port 22
* FTPS: FTP Secure. Extension of FTP, using TLS to encrypt traffic.

# Email and Web

SMTP: Simple Mail transfer Protocol. Transfers email between clients and servers, using TCP port 25. Used with SMARTTLS for security

POP3(TCP port 110) AND Secure POP (TLS on port 995): Transfers emails from servers to clients.

IMAP4: Internet Message Access Protocol stores email on server using port 143

HTTPS: HTTP Secure. Encrypts web traffic using port 80 and 443 for encrypted, and TLS/SSL

# Remote access

RDP (Remote desktop protocol) is used to connect to other systems remotely, using TCP port and SSH to encrypt.

# Time synchronisation

Kerberos requires all systems to be synchronised. NTP (Network Time Protocol) is used for synchronisation in windows. Simple NTP is less accurate.

# Network address allocation

Using DHCP (Dynamic host configuration protocol) dynamically assigns IP addresses to hosts, and also assigns other TCP/IP info.

**IPv4**: 32bit ip addresses. ISPs purchase IP addresses and assign them to customers. Private networks have private IP addresses which are formally defined in RFC 1918.

**IPv6**: 128 bit. 8 groups of 4 hex chars. Only allocated within private networks and not assigned to systems on the internet.

# Domain name resolution

DNS is for domain name resolution. URLs are queried to a DNS server for the mapped IP address of the URL. Uses UDP port 53. DNS is a hierarchy of servers, and queries are kept in a cache so it doesn't have to query again. DNS servers host data in zones:

* A: Host record, holding host name and IPv4 address. DNS client queries DNS with the name, and forward lookup takes place, giving IPv4 address.
* AAAA: Host name and IPv6 address.
* PTR: Pointer record. DNS client queries with IP address, and DNS responds with hostname → opposite of A.
* MX: Mail exchange. Identifies mail server, linked to A/AAAA record.
* CNAME: Canonical name, allowing system to have multiple names associated with single IP address.
* SOA: Start of Authority. Includes info about DNS zone and its settings, e.g. TTL, time to live, which is how long system will keep a result in its cache for.

Most DNS servers run BIND (Berkeley internet name domain) software on Linux. Microsoft networks use Microsoft DNS software.

DNS servers share info with each other, known as zone transfers. Uses TCP port 53.

# DNSSEC: DNS Security extensions, prevents DNS cache poisoning. This is when attackers modify the DNS cache to change the IP addresses mapped to a hostname, so users can be redirected to the IP of a malicious website.

# DNSSEC provides validation for DNS responses, adding a digital signature to each record, providing integrity.

DNS zones include A records for IPv4 addresses, and AAAA for IPV6 addresses. DNS uses TCP 53 for zone transfers, and UDP 53 for name resolution.

NSlookup: verify that DNS can resolve specific names

Dig: verify that DNS is reachable, and can resolve names to IP addresses.

# Subscription services

Selling software such as MS etc. They usually use HTTP protocol for security. Databases have details of customers, and services they are renting. Connection between web and database servers should be secure and use HTTPS or TLS. End of subscription → SMTP to send emails.

# Ports

* Well known ports: 0-1023
* Registered ports: 1024-49,151.
* Dynamic and private ports: 49152-65535. Available for use by any application.

# IP addresses and ports

TCP/IP uses the IP address to get the packet to the computer, which then forwards it to the correct port so the correct protocol can process it.

# IP addresses are used to locate hosts

# Server ports

Packets with destination port 80 are sent to a web server app.

# Client ports

When you send a browser request, your system assigns a port to receive packets. The web server will send packets addressed to that port, and these packets are then sent to the web browser to be processed.

Packets are sent via an IP address, which gets the packet to the server. The server then looks at the port, e.g. 80, and then passes it onto the web server program servicing HTTP.

Packets are then sent back to the source IP and source port.

# Basic network devices

Methods that IPv4 uses when addressing TCP/IP traffic:

**Unicast**: One to one traffic. One host sends traffic to another host using IP

**Broadcast**: One to all. Host sends traffic to all other hosts on subnet. Switches pass broadcast traffic between their ports, but routers do not pass broadcast traffic.

# Switches

A switch can learn which computers are attached to each of its physical ports, and then uses this knowledge to create internal switched connections. Switches internally switch unicast traffic, but broadcast to all ports.

**Security benefits:** if an attacker installs a protocol analyser to a non-unicast port, he can’t capture traffic that does not reach the port.

However, if traffic was on a hub, it would go to all ports, so an attacker would be able to analyse packets. Therefore, switches reduce attacks, and increase efficiency, as packets do not need to be sent to all networks.

**Port security**: You can configure each port to accept traffic from certain MAC addresses.

Includes disabling unused ports and limiting no of MAC addresses per port.

**Physical security**: Console port is used to monitor all traffic in or out of a switch, useful for troubleshooting. Physical security protects a switch by keeping it in a secure area such as locked wiring close, preventing physical access.

**Loop prevention**: When a switch constantly sends and resends unicast transmissions through the switch. This disables and degrades a switch.

STP (Spanning tree protocol) prevents looping, and thus prevents slowing of network.

**Flood attacks**: MAC flood attack attempts to overload a switch with different spoofed MAC addresses associated with each port. The switch runs out of memory and enters a fail-open state, operating as a simple open hub, allowing a protocol analyser to be attached.

**Flood guard**: Limits amount of memory used to store MAC addresses, and if a switch starts receiving more requests to store more, it gives an alert, sending a Simple Network Management Protocol (SNMP) error msg, and disables port. Can also limit no of MAC addresses supported by port.

# Routers

Connects multiple network segments into a single network and routes traffic between segments. Segments separated by routers are referred to as broadcast domains.

Too many computers on a single network → excessive collisions and low network performances. Moving computers to different segment can improve performance.

# Routers and ACLs

ACLs are rules implemented on a router to identify what traffic is allowed and denied, providing rule-based management and basic packet filtering, based on:

* **IP addresses and networks**: Can block access from any single computer based on IP address, or subnet IDs.
* **Ports**: If you want to block HTTP traffic, you can block traffic from port 80. You can choose whether to block incoming or outcoming traffic.
* **Protocol numbers**: e.g. ICMP uses protocol number 1, so you can block all traffic with this protocol number.

# Implicit deny

Traffic that isn't explicitly allowed is implicitly denied. This rule is usually at the end of the ACL.

# Antispoofing

IP addresses can be spoofed. But they can be blocked by modifying the ACL to block IP addresses, e.g. private IP addresses

# Bridge

Connects multiple networks together and can be used instead of routers. Directs traffic based on destination MAC addresses.

Hardware bridge uses a learning method to learn where to redirect traffic, as it doesn’t know the MAC addresses of the network interfaces initially.

# Aggregation switch

Connects multiple switches together in a network. An aggregate switch can connect multiple switches, and then connect to the router. This reduces the number of ports used in router.

# Firewalls

**Host based firewalls**: Monitor traffic going through NIC, through rules configured in xtables (Linux). Provide protection for individual hosts, such as comp or server.

**Network-based firewalls**: Dedicated servers providing protection for a network.

**Application based vs network based firewalls**: App based firewall is a software running on a system, e.g. host-based firewalls. Network based is a dedicated system with additional software, and two or more NICs.

Stateless firewall rules: Use rules implemented as ACLs, and implicit deny strategy. The format is:

* Permission: PERMIT/ALLOW/DENY
* Protocol: TCP/UDP. If you want to block both, you can use IP.
* Source: You can identify IP addresses to block or allow traffic.
* Destination: You can identify destination IP addresses to block or allow traffic
* Port/protocol: Can block ports or protocols

Firewalls use DENY ANY ANY, DENY ANY, or DROP ALL at the end of an ACL to enforce implicit deny strategy.

Stateful vs stateless: Stateful firewall inspects traffic and makes decisions based on context/state of traffic, and blocks traffic that isn't part of a session, e.g. TCP traffic without a TCP handshake. Stateless firewalls use ACLs, can have misconfigured ACLs, not allowing the implicit deny rule, and allowing almost all traffic.

Web application firewall (WAF): To protect a web app and web server within the DMZ.

# Zones and topologies

Networks are divided into different zones with different topologies. Network perimeter provides a boundary between the intranet and internet.

DMZ: buffered zone between private network and internet, adding a layer of protection for the intranet. This is implemented by adding firewalls on the outside and inside of the DMZ, to control incoming and outgoing traffic.

# NAT and PAT

Network address translation (NAT) translates public IP addresses to private IP addresses, and vice versa, in internet-facing firewalls. It is commonly used in Port Address Translation (PAT)

* Public IP addresses don’t need to be purchased for all clients, as you can have multiple clients connected to one router running NAT.
* NAT hides internal computers from the internet: They aren’t easy to attack.

It is not compatible with IPSec

Static NAT: Uses a single public IP address in a one to one mapping, mapping private IP to public

Dynamic NAT: One to many mapping. Maps multiple public addresses to a single private one.

# Network separation

Physical isolation: Ensures that network isn't connected to any other network, e.g. SCADA (Supervisory control and data acquisition) systems. They provide protection against attacks, but not if attacker gains access via internal network. Airgap means a system is not connected to any other systems.

# Logical separation and segmentation

We can segment traffic between logical groups of users with a VLAN.

# Layer 2 vs Layer 3 switch

A traditional switch operates on layer 2 of the OSI model, and uses the destination MAC address to determine destination port. Routers operate on layer 3, and forward traffic based on IP addresses, blocking broadcast traffic.

A layer 3 switch mimics a router, and allows admins to create a VLAN. It forwards packets based on IP addresses, so is immune to ARP attacks.

# Isolating traffic with VLAN

It uses a switch to group several computers into a VN, isolating different networks.

A layer 3 switch can group machines based on logical needs, rather than physical.

You could separate 2 VLANs with a layer 3 switch, logically separating computers on that network

# Media Gateway

Converts data format between networks, e.g. voIP converts telephony traffic between phone lines and IP network.

Proxy servers: Located on edge of network bordering internet, and used to forward requests for services from clients. They can improve performance by caching content and can also filter content, like HTTP/S

# Caching content for performance

Increases performance by caching results, reducing bandwidth

# Transparent proxy vs non transparent proxy

Transparent proxy: Accepts and forwards requests without modifying them.

Non transparent proxy: Can modify or filter requests, used to restrict URL access.

Anonymizers are sites that can be used to try to bypass these proxy servers, but can be blocked by them in response.

A subscription list is a list of banned websites, which can be loaded into a proxy server, blocking access to these sites

# Reverse proxy: Appears as a web server, but forwards traffic to the actual server. Protects web servers. When used with a web farm, it can act as a load balancer, forwarding requests to web servers using the load balancing algorithm

Application proxy: Used for specific applications, e.g. forward proxy used by HTTP. internet apps exchange data via APIs

Unified threat management (utm): Combines multiple security controls, e.g. firewall, antivirus and antispam etc. Content inspection monitors incoming data streams and blocks malicious content, and also specific types of transmissions. A DDoS mitigator attempts to detect and block DDoS attacks

UTMs can have a misconfigured content filter, blocking legitimate email or allowing spam, so sensitivity adjustment is needed.

They are placed at the network border, between inter and intranet.

# Mail gateways

Examine all incoming and outgoing email, and attempts to reduce risks associated with email by filtering spam, and DLP capabilities. DLP examines outgoing emails for sensitive info, and blocks them. It can do this by searching for keywords used in company confidential reports, blocking the email, and reporting it to admin.

Mail gateways can also support encryption, by encrypting outgoing mail to ensure confidentiality. We can also choose to encrypt certain emails. This can be done with vendor based or password based encryption.

# Summary

**Switches can do the following:**

* Preventing switch loops: Implementing STP or RSTP on switches
* Block flood attacks: Flood guards
* Unauthorised connection to unused ports: disable unused ports!
* Increased segmentation of computers: VLANs implemented on layer 3 switches

SNMPv3 (Simple network management protocol) monitors and manages network devices on UDP port 161. They send info back to an SNMP via notifications known as traps via UDP 162.

SNMPv1 passed passwords across networks as cleartext. V2 and v3 are more secure as they use authentication mechanisms.

**Routers can do the following:**

* Prevent IP spoofing: Antispoofing methods are implemented as rules within ACLs
* Provide secure management of routers: Using SNMPv3

**ACRONYMS**

**BASIC NETWORKING PROTOCOLS**

TCP: Transmission control protocol

UDP: User datagram protocol

ICMP: Internet control message protocol, used for testing connectivity

ARP: Address resolution protocol. Resolves IP to MAC

NDP: Neighbour discovery protocol, similar to ARP

SRTP: Secure real time transport protocol, delivers audio/video over IP

FTP: File transfer protocol, for transferring files

TFTP: Trivial file transfer protocol, transferring small amounts of data

SSH: Secure shell, encrypts traffic

SSL: Secure sockets layer, encrypts HTTP as HTTPS (compromised)

TLS: Transport layer security, replacement for SSL

IPSec: IP security. Encrypts IP traffic and uses tunnel mode for VPN traffic

* AH: Authentication header
* IKE: Internet key exchange, for VPN security

SFTP: Secure FTP, extension of SSH

FTPS: FTP Secure, extension of FTP using TLS

SMTP: Simple mail transfer protocol, transfers email between clients and servers

POP/POP3: Email from servers to clients

IMAP4: Internet message access protocol, stores email on server

RDP: remote access protocol, used to connect to other systems using TCP

NTP: Network time protocol, used for time sync in windows

DHCP: Dynamic host configuration protocol, assigns IPs to hosts

DNS: Domain name resolution, hierarchy of servers storing IP addresses of host names

DNS data zones:

* A: Host record, DNS → IPv4
* AAAA: IPv6 host record
* PTR: Pointer record, opposite of A.
* MX: Mail exchange, identifies mail server
* CNAME: Canonical name, allowing systems to have multiple names associated to IP address
* SOA: Start of authority, includes info about DNS zone and settings

DNSSec: DNS security extension. Prevents DNS cache poisoning, so users can be redirected to IP of malicious site

NSlookup: verifies that DNS can resolve specific names

DIG: Verifies DNS is reachable

**BASIC NETWORK DEVICES**

STP: Spanning tree protocol, prevents looping, and then slowing of network.

SNMP: Simple network management protocol, used for flood guard error msgs

WAF: web app firewall, protects web app and server in a DMZ

**ZONES AND TOPOLOGIES**

NAT: network address protocol, translates public IP to private and vice versa

PAT: Uses NAT. Port address translation

UTM: Unified threat management, combines multiple security controls, inc DDoS mitigator