# Security +
*Network Topography*

**Author:** Joseph Lee
**Email:** joseph@ripplesoftware.ca
**Mobile:** 778-725-3206

## General Terms

**PBX Private branch exchange**
- Is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines

**IP address / Internet Protocol Address**
- See RFC 1918 - Address Allocation for Private Internets https://tools.ietf.org/html/rfc1918
- **IPv4** (4 octets - 32 bits) and **IPv6** (128 bit hexadecimal)
- **Reserved IP address ranges:**
  - 10.x.y.z
  - 172.16.y.z - 172.31.y.z
  - 192.168.y.z

**DHCP Dynamic Host Configuration Protocol**
- Dynamically assigns an IP address to a host on the network
- **Network address allocation** can restrict how many IP addresses can be requested from a specific network segment, and should be used to prevent a DHCP starvation attack

**MAC Media Access Control**
- The identifier of your network interface representing the physical address
- Used in Data-link (Layer 2) communications by hosts when sending packets/data to other hosts

**MTU Maximum transmission unit**
- The largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based **network** such as the Internet

**Subnet**
- Logical subdivision of an IP network address space
- Divides the IP address space into:
  - **Network ID** - First x bits which represents the subnet
  - **Host ID** - Remaining x bits which represents each unique host
- **CIDR (Classless Inter Domain Routing)** is identified after the IP as: [1-31]
- Example: 192.168.1.1/**24**

    - The equation for the number of possible hosts is **2 ^ (32-CIDR ) - 2**
    - The - **2** is to remove one possible address for the **default gateway** and **broadcast address**
- **Subnet Mask**
    - RFC 1878
    - The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network by performing a bitwise AND operation between **another host's IP** and the **subnet mask**
    - The **subnet mask** is used for network interfaces to determine if a computer they are communicating with is on the same subnet or not, which determines how the host should address outgoing packets (i.e. using either the **gateway mac address** or **the other device's host address**)
- **Broadcast Address**
    - A network address at which **all devices** connected to a multiple-access communications network are **enabled to receive datagrams**
- **Network Gateway**
    - The IP address of the networks router / bridge for network data destined for other networks

**Screened subnet (triple-homed firewall)**

- A network architecture that uses a single firewall with three network interfaces
    - Interface 1 is the public interface and connects to the Internet
    - Interface 2 connects to a DMZ (demilitarized zone) to which hosted public services are attached
    - Interface 3 connects to an intranet for access to and from internal networks

**ACL Access Control List**

- Rules implemented on a router and firewalls to identify what traffic is allowed or denied

**Broadcast domain**

- Is a logical division of a computer network, in which all nodes can reach each other by broadcast at the **data link layer**
- A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments
- In terms of current popular technologies, any computer connected to the same Ethernet repeater or switch is a member of the same broadcast domain
- Further, any computer connected to the same set of inter-connected switches/repeaters is a member of the same broadcast domain
- Routers and other higher-layer devices form boundaries between broadcast domains
- **Traffic Types**
    - **Unicast -** peer to peer (one to one) traffic

    - **Broadcast -** one-to-all traffic using the subnet's broadcast address which is the highest value address in the subnet range (all 1 bits)
    - **Multicast -** one-to-many traffic

**CIDR - Classless Inter-domain Routing**

- Four major address classes, A through D
- Each of these classes allocates some portion of the 32-bit IP address format to identify a sub-network (called the network ID)
    - The first 8 bits for class A
    - The first 16 for class B
    - The first 24 for class C
    - Class D is experimental class
- The **default network gateway** and **broadcast address** can be determined by examining the CIDR
- The non-network portion of the address space is used to identify individual **hosts** on that network (called the Host ID)
- More than 16 million in class A, 65,535 in class B and 254 in class C

**Control Plane**

- The frame (packet) segments with routing information (hops, source and destination IP and ports)

**Data Plane**

- The data portion of the frame or packet

**Media Gateway**

- Translates network traffic from one type to another type
- For example, traditional analog voice phone line to VOIP

**Convergence time**

- A measure of how fast a group of routers reach the state of convergence
- It is one of the main design goals and an important performance indicator for routing protocols to implement a mechanism that allows all routers running this protocol to quickly and reliably converge
- A state of convergence is achieved once all routing protocol-specific information has been distributed to all routers participating in the routing protocol process

**Packet switching**

- The method of grouping data into packets for transmission through a network

**SOHO Style Topography**

- Small Office / Home Office networks

## Network Connection States

- **ESTABLISHED -** Normal state

- **LISTEN -** Waiting for a connection request
- **CLOSE_WAIT -** System is waiting for a closed connection termination request
- **TIME_WAIT -** Waiting for response to handshake
- **SYN_SENT -** System has sent a handshake initialization request (SYN packet) to the remote host
- **SYN_RECEIVED -** System has sent SYN-ACK and is waiting for ACK

## ISDN Integrated Services Digital Network

- A set of **communication standards** for **simultaneous** digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network
- **ISDN standards** define several kinds of access interfaces, such as:
  - **Basic Rate Interface (BRI)**
  - **Primary Rate Interface (PRI)**
  - **Narrowband ISDN (N-ISDN)**
  - **Broadband ISDN (B-ISDN)**
- Employed as the **network, data-link and physical layers** in the context of the **OSI model**
- **ISDN** is connection oriented and uses explicit signalling to manage call state

## DNS Domain Name Server

- Hosts data in zones (like a database) with records such as:
  - **A (IPv4 Host record)**
    - Domain name to IP address translation
  - **AAAA (IPv6 Host record)**
    - Similar to A record, but for IPv6
  - **PTR (Pointer record)**
    - Opposite of an A record
    - Clients can send queries for the IP address and the domain is returned
  - **MX (Mail exchange record)**
    - Identifies the domain name for the mail server.
  - **CNAME (canonical name record / alias)**
    - Maps one domain name (an alias) to another (the canonical name) to allow routing of subdomains to the same or different domains
  - **SOA Start of Authority**
    - Has TTL (time to live) settings and other settings
  - **TXT**
    - Provides the ability to associate arbitrary text with a host or other name, such as human readable information about a server, network, data center, or other accounting information
- Most DNS servers on the internet run **BIND (Berkley Internet Name Domain)** software and run on **Linux or Unix**
- Microsoft networks use Microsoft DNS software

- **Zone transfers** use **TCP port 53** while NS resolution use **UDP port 53**

**DNSSEC Domain Name System Security Extensions**

- RFC 4033, RFC 4034, RFC 4035, RFC 4470, RFC 4641, RFC 6781, RFC 5155, RFC 6014, RFC 4398
- Encrypts and uses digital signatures to each record for data integrity
- Produces RRSIG records on the host that is using DNSSEC
- Holds a DNSSEC signature for a record set (one or more DNS records with the same name and type)
- Resolvers can verify the signature with a public key stored in a DNSKEY-record
- Helps prevent DNS poisoning and DNS cache poisoning

## NAT Network Address Translation

- NAT translates a public IP to a private IP address and vice versa
- Prevents LAN IP addresses from being publicly known

**PAT Port Address Translation**

- An **extension to network address translation (NAT)** that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address
- The goal of PAT is to conserve IP addresses due to the word-wide-web popularity and IPv4 limitations
- Most home networks use PAT
- In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router

**Static NAT**

- Creates a persistent mapping of public IP address to a private one
- Should only be used when needed because creates a security issues

## Zones and Topographies

**Intranet**

- Internal network accessible to an organization and sometimes its partners
- Includes LAN technologies such as switches and may include WAN technologies if the intranet includes site-to-site networking

**Extranet**

- Part of an internal network that is accessible from outside of the network
- Usually extranet resources are in the DMZ
- Resources can often also be accessed from the intranet
- An older term referring to what is currently known as VPN network topography

**Network Perimeter**

- Between the intranet and the internet

**DMZ Demilitarized Zone**

- A buffered zone in between a private network and the internet which provides a layer of protection for the internal network from attackers
- The DMZ may also contain firewalls and internet-facing application servers such as web servers, mail servers, certificate servers, database servers, RDP servers, FTP servers, etc.

**OSI Model**

- The following are the OSI protocols used in the seven layers of the OSI Model:
- **Layer 1 - The Physical Layer:**
  - This layer deals with the hardware of networks such as cabling. The major protocols used by this layer include Bluetooth, PON, OTN, DSL, IEEE.802.11, IEEE.802.3, L431 and TIA 449.
- **Layer 2- The Data Link Layer:**
  - This layer receives data from the physical layer and compiles it into a transform form called framing or frame. The protocols are used by the Data Link Layer include: ARP, CSLIP, HDLC, IEEE.802.3, PPP, X-25, SLIP, ATM, SDLS and PLIP.
- **Layer 3 - The Network Layer:**
  - This is the most important layer of the OSI model, which performs real time processing and transfers data from nodes to nodes. Routers and switches are the devices used for this layer. The network layer assists the following protocols: Internet Protocol (IPv4), Internet Protocol (IPv6), IPX, AppleTalk, ICMP, IPSec and IGMP.
- **Layer 4 - The Transport Layer:**
  - The transport layer works on two determined communication modes: Connection oriented and connectionless. This layer transmits data from source to destination node. It uses the most important protocols of OSI protocol family, which are: Transmission Control Protocol (TCP), UDP, SPX, DCCP and SCTP.
- **Layer 5 - The Session Layer:**
  - The session layer creates a session between the source and the destination nodes and terminates sessions on completion of the communication process. The protocols used are: PPTP, SAP, L2TP and NetBIOS.
- **Layer 6 - The Presentation Layer:**
  - The functions of encryption and decryption are defined on this layer. It converts data formats into a format readable by the application layer. The following are the presentation layer protocols: XDR, TLS, SSL and MIME.
- **Layer 7 - The Application Layer:**
  - This layer works at the user end to interact with user applications. QoS (quality of service), file transfer and email are the major popular services of the application layer. This layer uses following protocols: HTTP, SMTP,

DHCP, FTP, Telnet, SNMP and **SMPP.**

**SCADA Supervisory control and data acquisition / ICS Industrial Control System**

- A type of network used in process manufacturing computer systems
- Traditionally air-gapped for security reasons
- Inherently deserves high-level of security attention because SCADA networks control industrial systems can have an impact on human life

**SDN Software defined network**

- Using software application as a router or switch
- Useful when a single system hosts several virtual machine

**VLAN Virtual LAN**

- Although clients on different VLANs may be on the same switch, broadcast packets are not broadcast to clients on other VLANs
- **MAC based VLAN -** Uses a set list of **MAC addresses** to determine the **subnet** that the client will be assigned to
- **Port based VLAN -** Uses the physical switch port that the client is plugged into to determine the subnet the client will be assigned to
- Switches can be configured to route traffic between separate VLANs using **inter-VLAN routing**

## Network Hardware

**DOCSIS Data over Cable service interface specifications**

- An international telecommunications standard that permits the addition of high-bandwidth data transfer to an existing cable television (CATV) system
- It is used by many cable television operators to provide Internet access (see cable Internet) over their existing hybrid fiber-coaxial (HFC) infrastructure
-

**Switch**

- Learns which computers (MAC addresses) are attached to each physical port
- Facilitates communication between them by translating an IP address to physical ports on the switch
- Switches reduce network efficiency compared to hubs because hubs broadcast all traffic to all hosts instead of directing it only to the intended recipient host
- Switches can be configured to increase **port security** to use **persistent MAC** or **sticky MAC** addressing which binds a particular MAC address to a physical switch port preventing other devices from being able to access the port on the switch
- **Loop prevention**
  - Using **STP (spanning tree protocol)** or **RSTP (rapid spanning tree protocol)** prevents plugging in a cable that loops back to the same switch and then creates a loop
- **Layer 2 switch**

    - Work at the **data-link layer** and route packets by destination IP and MAC address on its physical ports
- **Layer 3 switch**
    - Use **ASIC (Application specific integrated circuit)** chip that gives them capability to do anything a router can do with lower latency than a traditional router
    - **ASIC (Application specific integrated circuit)**
        - A CPU that is not a general purpose CPU but is a CPU for making switching decisions very quickly
    - **Layer 3 switches** can separately route VLAN traffic by acting as a router between VLANs **(inter-VLAN routing)**
- **Aggregation switch / backbone switch**
    - Consolidates all traffic across the network to and provides access to the gateway (router)
- **Port Mirror / Switch Port Analyzer or SPAN**
    - Is a special port on managed switch configured to listen to all data going in and out of the switch

**Router**

- Connects multiple network segments (broadcast domains) together and directs traffic based on IP address
- If a network has too many devices on it, broadcasts can result in excessive collisions and reduce network performance
- May also have a capability to connect to non ethernet network such as DOCSIS, or DSL modems
- Operates at the **network layer** of the OSI model

**SSL / TLS Accelerators**

- Hardware devices to handle TLS traffic
- Traditionally placed close the web-server internal network
- Not placed on the network periphery

**SSL Decrypter**

- A system in the DMZ used to man-in-the-middle any outgoing network connections and analyze traffic

**Bridge**

- A network bridge connects multiple networks and can be used instead of a router
- A bridge is a network device mainly operating at the **data link layer** of the OSI model with **filtering and forwarding** capabilities
- A bridge is **transparent** to the adjacent end station or nodes and **merely forwards frames** instead of creating them as a router does
- Can act as a repeater as well

**Aggregation switch**

- Connects multiple switches together in a network

**Repeaters**

- Used to amplify a signal so that you could use a longer segment of cable without degradation or attenuation of the signal

**ICS Industrial Control Systems**

- Collective term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes

**MFD Multi-functional Devices**

- A machine that can print, copy and scan
- Secure print and follow-me printing are two of the key features of newer MFD devices
- Lower costs, save space, and can handle larger loads of work
- Security considerations include:
  - **Default access credentials** are **publicly available**
  - MFDs contain **embedded operating systems** and so attackers can launch sophisticated attacks from them once they have been compromised
  - May have unneeded services enabled which increase the attack surface
  - Do not overlook updates and patches to MFD devices
  - Denial of services attacks such as using up printer resources with bogus print jobs, attacking the network address with packet floods, etc.
  - If the MFD is using old authentication protocol or service then credentials and/or data may be sent in cleartext allowing an attacker with network access to pivot to the device

## Network Security

**Port Security**

- Is a layer two traffic control
- Disabling all unused ports to precent someone from plugging in a laptop or computer to that ethernet wall jack or directly into the switch
- Helps **secure** the **network** by preventing unknown devices from forwarding packets
- Packets that have a matching MAC address (secure packets) are forwarded; all other packets (insecure packets) are restricted
- Limit the number of MAC addresses on a given **port**
- Enables an administrator configure individual switch **ports** to allow only a specified number of source MAC

**Anti-spoofing**

- Anti-spoofing can be implemented on a router to use ACL to prevent IP addresses from being faked
- Especially important is to prevent traffic from the internet / WAN to come into the network and spoof a LAN IP address

**Network Segregation**

- Separating network into sections such as with sub-netting (ranges of IP addresses) or VLAN (grouping physical ports on a switch)

**Layer 2 (OSI model) switch**

- Uses **ARP tables**, while a **layer 3 switch** operates like a **router** using **destination IP addresses to route rather than MAC**
- VLANs can be used to isolate network traffic based on department, job function or other administrative needs

**Network Segmentation**

- Partition a single network in to two or more networks
- This improves efficiency by reducing the size of the broadcast domain
- Network segmentation can be categorized into **physical segmentation** and **logical segmentation**

**Network Isolation / Airgap**

- Prevents direct communication on the network by **physically isolating** the networks
- **Classified** and **unclassified** networks are not physically connected to each other

## Proxy Servers

- Proxy servers can **improve performance** by:
  - Caching content
  - Limiting access to unwanted websites by filtering content and or request URI
- Proxy servers are on the **edge of the network** between the internet and intranet (DMZ)
- **Application proxies**
  - Forward requests for applications or services such as:
    - HTTP from a client through another server
    - Email
    - FTP
  - Filter DMZ traffic for specific applications such as:
    - Database
    - Web-server
    - RDP
    - Proxy to another extranet resource (such as to another companies API server)
- **SSL/TLS proxy**
  - Handles encryption layer of a connection and can be installed on the edge of a web-server-farm
- **Transparent Proxy**
  - Accepts and forwards requests without modifying them
- **Non-transparent proxy**
  - Can modify or filter requests for purposes of content filtering, virus

scanning, DLP, etc.

- **Reverse proxy server**
  - Accepts requests from the internet and acts as a cache proxy for some web pages such as static pages, or a load balancer for a server farm of multiple servers
- **Forward proxy**
  - Between the client and the main server or internet and will modify / log or scan traffic before forwarding the request / file to the server
  - May also filter blocked URLs, and enforce ACL such as time-of-day, etc.

**SSL/TLS Accelerators & decryptors**

- Hardware devices on the network perimeter for managing TLS layer for internet connections
- Accelerators benefit web-servers to mange TLS connections with clients and decryptors assist a UTM appliance to detect malware entering the intranet from the internet by decrypting it and inspecting it

**Embedded Systems**

- Device with dedicated functionality and OS to perform the function
- Printers, fax, wireless AP, photo-booths, security cameras, safes, digital locks, smart-tv, medical devices, smart-watches, refrigerator, stove, AC units, microwaves, alarm-systems, wearables, IoT, HVAC, UAV
- Change the default configuration because that information is widely available
- Check for regular updates to firmware, software
- Physical / Wifi access to the system should be considered / monitored
- EULA can allow collected data from IO such as audio or video to be saved and monitored by the vendors