# Network Lesson 1 31.08/2012

## Networking Components

Host = Any devices connected to a network

Peer-to-Peer = Is when two or more nodes provide or use a service without a centralised computer.

Intermediary Device = Centralised Device that interconnects end devices. These devices provide connectivity and work behind the scene to ensure the flow of data across the network.

Network Media = Network media refers to the communication channel used to interconnect nodes on a computer network. For example, Ethernet cables, copper coaxial cables, optical fibre, etc.

### Network Infrastructure Types:

LAN = Local Area Network is a collection of devices, connected together in one physical location, building, office, or home. A LAN can be small or large, but is limited by its geographical area.

WAN = Wide Area Network is a collection of local area networks or other network that communicate with one another. (Basically a network of networks).

### Internet, Intranet & Extranet

Intranet – Is a private network for sharing information and data with an organisation, with the exclusion of access by outsiders.

Extranet – Is a private section of a network, that provide access for different organisations. For example, Supplies, customers, or collaborators.

Internet – A internet is a connected network that connects vast amount of networks together, allowing for access across a massive geographical area.

Communication Fundamentals

* Message Source (Sender) Message sources are people or electronics devices that send a message to another individual or device
* Messages Destination (Receiver) Is the destination that is receiving the message/data.
* Channel – This consist of the media that provides the pathway over which the message travels from source to destination

Message Delivery Options

Unicast – Information is being transmitted to a single end-device. Other devices can hear the message, but only one device responds to it.

Multicast – Information that is intended for a selected amount of end devices. Other devices can hear the request, but only the specified target will respond.

Broadcast - Sending information to everyone on the network, doesn’t care who responds.

Protocol Suites

OSI Model

Is a 7 layer, networking model that describes how information is transferred from one networking component to another. It defines the protocols and device that are required for building a network as well as how networks communicate, operate and isolate troubleshooting network issues.

Allows for communication regardless of operating systems.

|  |  |  |
| --- | --- | --- |
| Layer | Definition | Protocol |
| 1. Physical Layer | Responsible for transmitting raw unstructured date bits across the network. | USB, RJ-45 Jack, Hub |
| 1. Data-Link | Responsible for the transmission of data from on NIC to NIC. Data is packed into frames. | MAC, Frame Relay, Ethernet |
| 1. Network | Responsible for receiving frames and delivering them based on the IP addresses, Routes data information between networks | IP, ARP, IPSec, ICMP, RIP |
| 1. Transport | Responsible for managing the delivery and error checking of data packets, deciding to used TCP or UDP to distribute them across the network. | UDP, TCP |
| 1. Session | Establishing and or terminating a connection between two or more applications or machines | PPTP, NetBIOS, PAP |
| 1. Presentation | Responsible for compressing data, so its receives correctly and encoding and encrypting data. | SSL, TLS, JPEG, PNG |
| 1. Application | Responsible for the interaction of web applications. Providing services to the user. | HTTP, SMTP, DHCP, FTP, SNMP, POP3 |

TCP/IP

|  |  |
| --- | --- |
| Application | Application  Presentation  Session |
| Transport | Transport |
| Network | Network |
| Data-Link | Data-Link  Physical |
|  |  |

Transmission Control Protocol/ Internet Protocol (TCP/IP)

A 4 Layer model of communication protocols, used to interconnect network devices on the internet. Seen as the core function of delivering packets of information from a source device to a target device.

Because IP doesn’t handle packet handling or error checking, such functionality requires another protocol, typically TCP.

Port Numbers are used to identify the transaction over a network by specifying both the host and the service. To differentiate between many different IP services.

* Port Numbers, reside on the Transport layer of the OSI/TCP/IP
* Destination port number is associated with the destination application on the server host.
* PC Host detects what port to use on the destination machine
* It will use the default ports unless changed by the destination host.

A server can offer more than one service simultaneously:

* SSH
* WEB
* FTP
* DNS, etc.

Transport Layer Addressing

Provides the user address which is specified as a station or port. It is accomplished by using TCP and UPD ports. Responsible for delivering messages between network host.

TCP is to ensure reliable transmission of packets. It solves problems that may arise from a packet-based messages, such as loss of packets, out of order packets, duplicate packets and corrupted packets. It does this by checking the host to make sure it has received the packets in the correct order, if not, the packet is drop and the transmission starts again.

UDP - User Datagram Protocol, is a lightweight protocol that can detect corrupt data but doesn’t attempt to solve problems like TCP. Because it doesn’t care about packet loss, it allows host to receive live data, without waiting for the packets to be checked.

Port Groups

|  |  |  |
| --- | --- | --- |
| Port Groups |  |  |
| Well-Known Ports | 0 – 1’023 | Used for common popular services |
| Registered Ports | 1’024 – 49’151 | Used for a specific purpose or application |
| Private/Dynamic(Ephemeral) Ports | 49’152 – 65’535 | Used when the OS will assign a random port when a connection between it and a service is made |
|  |  |  |

Client machine will use a random ephemeral port to connect to a well-known port on the server machine.

Data Link Layer Importance

* Prepares network data for the physical network,
* Only considered with the NIC-to-NIC communication
* Ethernet is a type of protocol

Ethernet Family

The common LAN is Ethernet:

* Half-Duplex: Either sends data or receives it, but can’t do both at the same time
* Full-Duplex: Capable of sending and receiving data at the same time.

Layer 2 (L2) Switch

* Switch is made up of integrated circuits and accompanying software to control data paths.
* Each Port Connects to an end device or intermediary device
* Forwards frames (BASED on MAC) to destination port
* Switch stores MAC address in cache table
* If Switch doesn’t know MAC address, it will broadcast the frames to every port (Except the one it’s from)
* Every Port has its own MAC address.

ARP (Address Resolution Protocol)

Maps MAC address to IP address

Networking Layer

* Switch forwards traffic based on destination MAC Address connected on the same data link standard(Ethernet)
  + Routers forward traffic based on IP address (Regardless of data link standards; 4G, 3G, Ethernet etc.)
* Routers don’t broadcast frames
* Switch has one broadcast domain
  + Router splits the broadcast domain into multiple broadcast domains
* Switch connects PC that share the same Network ID
* Router connects networks with different Network IDs
* Default Gateway
  + All Pc’s on some network share the same gateway, done on the router interface.

# Networking Lesson 3

Directly connected networks are networks directly connected to a router.

Routers don’t broadcast, instead for every interface, the router creates a broadcast domain

* Router-to-Switch = Broadcast domain
* Router-to-router = Broadcast domain

Static Routing – Is the process of configuring the routing path & IP address and not expecting or wanting said IP address to change.

* Static routing is configured and added manually to a router

Dynamic Routing - Routing provides the most optimal data routing paths.

* Selects path according to real-time network changes.
* Uses Routing Information Protocol or Open Shortest Path First

Next Hop - The next closest router a packet can go through

Metric Hop – How many routers it needs to pass through to get to destination IP Address.

Dynamic Host Configuration Protocol (DHCP)

* -Automates the assignment of IP address, subnet Mask, gateways and other networking parameters.
* DHCP server choosing a IP address from its address pool and leases it to a host for a configured pool of time.
* DHCP Server can be installed on:
  + Router
  + Wireless Access Point
  + Dedicated DHCP Computer
  + Personal Computer
* DHCP is a broadcast protocol, it assigns IP address on it’s own broadcast domain
* Resides on UDP 67 server & UDP 68 client

|  |  |  |
| --- | --- | --- |
| BORADCASTING | DHCP DISCOVER | DHCP client is new, so it broadcast discover message to make it’s self-known to a DHCP server |
| DHCP OFFER | DHCP server offers a IP address lease, and lets other DHCP server know. Its chosen a DHCP server |
| DHCP REQUEST | Client accepts the first offer received, by broadcasting a DHCP request message for the offered IP address. |
| DHCP ACKNOWLEDGMENT | Server accepts request by the client a DHCP Acknowledgment message |

Host PC can’t unicast without IP address.

If Host can’t get IP, it will self-Assign APIPA address (Automatic Private IP Addressing)

Hypertext Transfer Protocol(HTTP)

* -HTTP is application-layer protocol for transmitting hypermedia documents, such as HTML
* Used for Commutation between web browser & web server, but can be used for other needs
* HTTP is a client-server model, client opening a request and waiting for the server to respond
* HTTP uses port TCP 80 by default but can work on other ports
* HTTPS uses SSL/TLS for encryption and authentication
* HTTPS uses port 443
* SSL – Secure Socket Layer/ TLS – Transfer Layer Security

File Transfer Protocol

* Standard protocol for sending files between computers of TCP connections
* FTP uses port 21 TCP & sometimes port 20 TCP if running in active mode
* FTP isn’t secure but other protocols offer security
  + FTPS (FTP-TLS) Port 21/TCP
  + SFTP (SSH-FTP) Port 22/TCP
    - Port 22 because SSH runs on same port

Domain Name System (DNS)

* Translates human readable names to machine readable IP address
* Designed for Humans not computers
* New Addresses are linked to a domain name and connectivity is maintained.

DNS Hierarchy

* **Root Level Domain** -
  + **Top Level Domain** (.com, .net, .co etc.) -->
    - **Second Level Domain** (Cisco.com) -->
      * **Third Level Domain** (ftp.cisico.com, mail.cisco.com)

Simple Mail Transfer Protocol

* Client-Server used to send emails,
* Listens on port 25 /TCP (Port 465 or 587 for encryption)

Post Office Protocol (POP)

* Used to receive emails
* Used on Port 110 /TCP

Internet Message Access Protocol (IMAP)

* Open standard that describe how to access messages in an email mailbox. It deals with managing and receiving email messages from server.
* Difference between POP3 and IMAP, is:
  + POP3 will download email from a server to a single computer and then delete the email from server
  + IMAP stores the message on a server and synchronises the messages across multiple devise

Access Control List (ACL)

* ACL grants/Denys access to a certain resource (files, computer, server, network, system etc.)
* Tells devices which type of traffic can access the network & which activity is allowed or denied.
* It works by:
  + Getting the destination and Source address from the packets
  + Compares rule in ACL that matches the source & destination address/ports
    - If Deny: Drops packet
    - If Allow: Allows packet to pass
    - If No –Match: Drops packet immediately
* ALC are common in security devices.

Wildcards

Wildcards displayed the opposite of Subnet Mask

A Wildcard mash allows or denies all traffic from a network IP address, the wildcard mask tell the router which bits in the IP address needs to match the access control list and which do not.

* Subnet Mask 192.168.1.0 = 255.255.255.0
* Wildcard Mask 192.168.1.0 = 0.0.0.255

Firewall

Firewall is a system or group of systems that enforces an access control policy between networks, it monitors ingoing and outgoing traffic, based on the established security policies. It sits in-between a private and public network.

* Used to prevent exploitation of protocol flaws
* Blocks malicious data from Server & Clients
* Misconfigured firewalls can result in devastating consequences
* Used to reduce security management from administrators
* Network performance can affect a firewalls

Firewalls consist of Two Policy types:

Allow-list = Drops all packets except for specifically listed

Deny-list = Allows all packets except those specifically denied

Packet Filtering Firewall

* Filters packets on layer 3 and 4 of OSI model
* Filter packets based on assigned rules
* Auto denies if no rules is given to packet
  + Packets are mapped to criteria:
    - Source IP
    - Destination IP
    - Source Port
    - Destination Port
    - Packet Type
* Need to specify ingoing & outgoing rules

Stateful-Firewall

Constantly monitoring and detecting states of all traffic on a network to track and defend based on traffic patterns and flow.

Constantly analysing the complete context of traffic and data packets, seeking entry to a network.

Proxy Firewall

Security network system, that protects network resources by filtering messages at the application layer. Often deployed between network and internet.

Proxy protects a client’s machine by being an intermediary software/device

Web Application Firewall (WAF)

Helps protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. Operating on Layer 7 (Application Layer)

* Typically Protects against XSS & SQL injections

A type of reverse-proxy, that protects the server from exposure by having clients pass through the WAF before reaching the server.

Firewall Zones

A portion of a network that has specific security requirements. A name for a collection of systems that require the same access control policy.

Has 2 zones,

* Inside/Private trusted Zones (100%)
  + Inside your network/Organisation
* Outside/Public untrusted Zones (0%)
  + Internet/ other networks outside organisation

Firewall Zone – Demilitarized (DMZ)

A perimeter network that protects an organisation LAN and untrusted networks. Subnetwork that sits between the public internet and private network.

Inside Zone (100%) =

* Allows traffic to DMZ & Internet
* Blocks Traffic from DMZ & Internet

DMZ (50%) =

* Allows traffic to and from Internet
* Blocks traffic to the Inside Zone

Outside Zone (0%)

* Allows traffic from Inside Zone and DMZ
* Blocks traffic to the Inside Zone

IDS & IPS

Intrusion Detection System,

Monitors the network, and detects for any unusual activity. This differs from a firewall, as it allows or deny based on the set rules, regardless of unusual activity

* Host-Based IDS
* Network-Based IDS

Intrusion Prevention System

It will detect the unusual activity and attempt to prevent them from launching any known attacks by blocking attacker IP address or Port. It will also send a report of these events to the system admin. Combines the abilities of IDS and firewalls.

* Host-Based IPS
* Network-Based IPS

Network Address Translation(NAT)

To allow a device with a private IPv4 address to access device and resources outside of the local network, the local address must first be translated to a global address.

* This is done from the Router
* (Router give device a temporary global IP address)
* NAT see Local IP address packet; it will change the IP to a global one.
  + When the response comes back, it will change the global back to local.
  + Local Address to a Global address
    - Can be Private – Private
    - Or Private – Public

Types of NAT

Static NAT – Uses one-to-one mapping of local and global address.

* + - Fix Global Address

Dynamic NAT – Uses a pool of public address and assigns them on the a first-come, first-serve basis.

* + - Pool of IP Address, can’t assign any after Global IPs are all gone,

Port Address Translation (PAT) – Also known as a NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few address.

* + - IP address are translated to same IP address, but the Ports are kept to identify the connection. If multiple IPs send for same server, PAT will change ephemeral port.

# Networking Security Lesson 4

## VPN Virtual Private Network

Concept

Creates a secure network traffic between sites and uses

Creates end to end private network connection

A VPN is a virtual in that is carries private network but that information is actually transported

Benefits

|  |  |
| --- | --- |
|  |  |
| Cost Saving |  |
| Security | Provides highest level of security, with advance encryption and authentication protocols |
| Scalability | Allows organisation to use the internet. Makes it easy for add new user without adding significant infrastructure |
| Compatibility |  |

VPN Protocols

* Point-to-Point Tunnelling Protocol
* GRE
* L2TP
* SSH

Host to Host VPN

Host – to – Site VPN (Remote Access VPN)

For Host-to-site, we use a VPN gateway in front of the Site, to connect to the Hosts. Rather then a gateway on the router, we also use a gateway on the VPN.

This allows for connection for Host users that are running on slower, less powerful media.