Network is divided into few sections

-Physical part – cable RJ45 , fiber optics , hub , switches , router,

-Logical part – IP ADDRESS

TCP CONTAINS

{

TCP HEADER CONTAINS CONTAIN TCP PROTOCOL BLA BLA BLA .

IP HEADER source ip and dest ip

}

OSI

Please do not trust salesman post always

OSI is reference model (Understand how the network work , understand which session to look to troubleshoot )

PHYSICAL -> Cables , Access points , dump devices , hub , [data in bits ]

DATA LINK -> ONLY understand MAC ADDRESS (is a physical address , which is permanent which also contain source MAC and destination MAC )

[ARP (Address resolution protocol) ] – Translate IP ADDRESS TO MAC ADDRESS [Data is call frames , Packet is convert to bits ]

LLC (error correction , we cannot add another layer , therefore we convert into bit , after convert into bits , it become Frames )

NETWORK -> Router [ when we merge more and more segment , and it become fragment] , sometimes we can found switch in layer 3 because of Vlan using ip address to create .

TRANSPORT -> Which method to transfer (TCP/IP Transmission control protocol OR UDP (user datagram protocol)) [ IF THE DATA IS LARGE , THEN IT PERFORM SEGMENTATION LIKE 100KG PEOPLE BUT LIFT ONLY ABLE TO HOLD 20KG PEOPLE , THEREFORE IT PERFORM SEGMENTATION] . Data is now call SEGMENTS

SESSION - > establish , maintain , terminate [data still remain formatted data ]

PRESENTATION - > format , encryption , compression ,maybe format is kind of let the computer know the info [now it have become formatted data]

APPLICATION - > maybe emails or browser user data

Media layer = 1-3 , Host layer = 4-7

TCP/IP MODEL versus OSI

Application Layer = Application , Presentation and session layer (FTP,NFP , TELNET,RLOGIN)

Transport Layer = Transport Layer (TCP , UDP)

Internet Layer = Network Layer (How you reach the location , IP , ICMP , ARP, RARP(MAC TO IP \*\*REVERSE \*\*))

Network access = data link layer , physical layer

Type of Networks

WAN

LAN

MAN

Personal Area Network = bluetooth

Campus area network = workplace or campus coverage

Global Area Network = ??

Network Topologies

BLABLABLA RING , LINEAR BLA BLA

HUB AND SWITCHES

Broadcast Domains – where you sending (Hub only able have 1 broadcast domains , if you want 2 domains you want to do 2 domains ) , router let say it’s 4 ports then it’s 4 broadcast domains .

Collusion Domains – how many domains

Hub – It can forward the message or packets to other people , let say user a connect to hub , user b connect to hub , and hub connect to router .

Let say user a connect to fb , it hub will send all this packets to other users including itself user a and forward to router , and router will forward the packet back to user a and user b as well (other user that is connected to the hub )

It’s only contain 1 Collision Domain in the hub

Switches

Let say 4 port router it’s contain of 4 Collision Domains

It’s manageable , it forward back the packets base on mac address

IANA – GOD FATHER OF INTERNET ( INTERNET ASSIGNED NUMBERS AUTHORITY / ASSIGN IP ADDRESS )

RIR – REGIONAL INTERNET REGISTRA

-APNIC (Asia pacific , MALAYSIA (MYNIC) (SERVICE PROVIDER LEASE FROM MYNIC ), Taiwan(TWNIC))

-ARIN

-ICANN

-LACNIC

-AFRNIC

-RIPE-NCC

TCP/IP Protocol STACK

Process of translating private to public ip is known as

* NAT(Network Address Translation)
* PAT (Port Address Translation)

May Done by router or Firewall

NAT = 192.168.0.2 ----🡪 201.42.24.102

PAT = map multiple private ip to 1 public ip

201.42.24.102:20 (SPECIFIC PC MAYBE USER A)

201.42.24.102:70 (SPECIFIC PC MAYBE USER B)

DIFFERENCE PORT TO SPECIFY SPECIFIC USER

Root server is .

. is managed by RIR

But they know it’s from .com therefore it will goto .com server and it goto fb.com dns and it go into DNS cache (router maybe 15minutes , 1days , days or how many months ).

FB.com server is (Authoritative) , and router (cache is call non authoritative )

Assume the cache is 15minutes , after 15minutes , router will straight away as for fb.com (because it know where is the location)

Nsloopup

Set type =aaaa //ipv6

Set type =a //ipv4

Set type =mx //mail exchange server

Set type = cname // another name for the domains

Set type =

TCP HEADER IS ALWAYS =20 BYTES (contain flag 16bits ,window size 16 bits , sequence no 32bits , source port 16 bits , destination 16bits )

Tcp

Reliable – because it perform 3 ways handshake and it contain acknowledgement number

Packet no 1 goto computer b

Computer b will respond to ack 2 (mean it receive packet 1 and please send packet number 2 )

And computer a send Ack 2(packet 2 )

And computer b respond Ack 3

4 way handshake in TCP =Bye and Ok

Computer A send Bye

Computer B send ok && Computer B send Bye

Computer A send Ok

Secure

Encryption

Flag in TCP

Syn = Can I talk to you ?

Ack = Ok

Rst = no , I don’t want to talk

Urg = Urgent (eg POP protocol will use urg)

Psh = Push (eg POP protocol will use psh)

Fin = Finish

Tcp Window Size = How many bytes can you carry , 64 bytes , 128 bytes

UDP = Plaintext protocol && no security , no acknowledgement (DNS what is the ip address of the url )

IP HEADER

IP VERSION 4 OR 6 (ELSE SOMEONE IS MANUPULATING THE PACKET HEADER )

TOTAL LENGTH(16 BITS CONTAIN R , DF , MF )

TTL(how long the packet will leave the communication )

Mtu (maximum transfer unit) = 10bytes (each packet can only 10bytes , if more than 10 bytes then packet is drop )

Ipv6 occur because lack of ip in ipv4

Allow each devices contain a ip address

ICMP protocol (Internet control message protocol )

Ping (Echo request && Echo reply )

Ping [www.google.com](http://www.google.com) == Echo request

Result = echo reply

Arp-a show all ip to mac

Ethernet (Layer 2)

Cable determine how fast

10-Base T

100 – Base – T

Gigabit Ethicat

FDDI

Single mode =

Multi Mode = service provider use multimode to transfer longer place

Token ring is in occur in ring topology

IPv4

Always 32bits = 4bytes

8 bits = 1 bytes

xxx.xxx.xxx.xxx = 4 octet

xxx=8 bits

Class A = 0 – 126

Class b = 128- 191

Class C – 192- 191

Class d – 240 -255

Class e – 224 – 239

Private IP

Class a = 10.0.0.0 – 10.255.255.255

Class b = 172.16.0.0 – 172.31.255.255

Class c = 192.168.0.0 – 192.168.255.255

Subnet mask let us know which network we are in

A=255.0.0.0

B=255.255.0.0

C=255.255.255.0

10.0.2.5 /8 = CIDR (Classless Inter Domain Routing)

172.16.25.3 /16

192.168.25.3 /24

10.10.23.25 / 16 (10.10 is network cannot be change)

First ip = network address(can be known as id , to show the network)

Last ip = Broadcast (if ping all device will known)

Subnetting == perform subnetting

Supernetting == slightly different from subnetting

IPv6

0:0:0:0:0:0:0:0

IPSec = Ipv4 optional , Ipv6 built in

IPv6 = 2000:0020:0000:0000:F460:0000:0000:0010

Simply leading zero

2000:20:0:0:F460:0:0:10

Advanced simplify when 0 zeroes occur

2000:20::F460:0:0:10

Computer Network Defense

Detection , Response , Protection

IDS = REACTIVE

IPS = RE

After detect , incident handle (Response , what suppose should we do ) and perform protect from attacks

CIA

Confidentiality

Integrity

Availability

\*to prove your organization is secured\*

But to achieve these 3 , we must put in efforts

IAAA (triple A)

\*Identification (Who are you )

\*Authentication (MFA )

\*Authorization (What can I do , after I perform authentication (Roles base access control ) )

\*\*Auditing\*\* (Check above 3 is performing correctly or not)

Non – Repudiation – Stronger Authentication strong Non repudiation (let say fingerprint , cannot say that the finger got cut by attackers )

Blue Teaming

Defender

Red Teaming

Attackers

Defense in depth (DID)

Inorder to get the asset how many procedure to get (how many protection layer to access the data )

CND PROCESS

1. Protection
2. Monitor
3. Detection
4. Analyzing
5. Response

Most common factor Network security concerns Arise

1.Hardware or software misconfiguration

2.Insecure or poor Design of the networks (Range)

3.Inherent technology weakness (Teach you how to cook in school , but didn’t teach how to cook securely )

4.Careless approach of end users

5. Intentional acts from end users

Internal thread – Internet employee

External thread – External hacker

Unstructure thread – Unskilled hacker

Structure thread – Highly hacker

Type of vulnerability

TCP/IP PROTOCOL VULNERABLITY – HTTP , FTP . ICMP , SNMP ,SMTP , RLOGIN ,TELNET

OS Vulnerability – OS zero days

Network Device Vulnerablities – router , idp , ips (insecure routing protocol) default password, firmware vulnerabilities

Information Gathering

Passive Scan = Everywhere from google.com or whois

Active Scan = ??

Scanning

open port

identify port services and version

identify OS

Vulnerability (Open bias , kuali or quali )

Gaining Access

Password cracking

Dictionary attack

brute force attk

password sniffing

Social Engineering

Session Hijacking

Known exploit / Vulnerability (Remote exploit , Local exploit )

Local exploit is you need to infront of the pc

Privilege escalation

Maintaining Access

Install malware

Backdoor

Create new UA(User account )

Covering Tracks

Clear logs

Inteltechniques.com/menu.html (OSINT FRAMEWORK)

[www.Sploitus.com](http://www.Sploitus.com)

Piggybacking – Ask someone for helps to open the door

Tailgating – wear fake identify

SPIM – Chat messenger SPAM (SPAM MESSAGE over communication)

Cyber Squatting – domains name , eg : we buy [www.tehwinsam.tw](http://www.tehwinsam.tw) but it bought , and now resell much more expensive

Typo squatting – Microsoft.com = rnicrosoft.com

Replay Attack is capture/sniff the token , and replace the token to session hijacking

ARP Spoffing

Sniffing Tools

Bettercap

Wireshark

Ettercap

DHCP STARVATION

ATTACKERS CREATE ROUGE DHCP SERVER TO ACCEPT CLIENT REQUEST

COUNTERMEASURE

DHCP SNOOPING – Allow specific port to send DHCP PACKETS ONLY

Denial Of Service

1. Volumetric (Bandwidth consumption)
2. TCP State Exhausation Attack (TCP STATE)
3. Flooding (ICMP , TCP , UDP)
4. Application (Buffer Overflow , Social Engineering update firmware )