04.05.2022

----------

Networking

Communication between two or more devices is called Networking

What is Communication?

Exchange of Information between two devices (Sender / Reciever)

Communication Terminology

Simplex - One way Communication (Radio / TV)

Duplex (Half / Full) - Two Way

Half Duplex - Communication Bidrectional (one at a time) - Walkie talki (Signalling)

Full Duplex - Communication Bidrectional (Both at a time) -

Telephone

Communication Speed : bits / sec - baud

Parity - Error Detection bit (used for flow control) - Checksum

Networking

----------

LAN / WAN - Local Area Network / Wide Area Network

LAN is limited to within a building or campus

WAN can communicte beyond campus / city/ State / Country

Networking Devices

------------------

Switch - A device which interconnects within your network (LAN)

Router

When a node wants to talk with other node it places a request called as ARP (Address Resolution Protocol)

Protocol - Set of communication Rules

Functions of Switch: 1) Address Learning (MAC Address)2) Packet forwarding / Filtering

Router - Interconnects 2 or more networks

Functions of Router - 1. Packet Filtering 2) Packet Forwarding

3) Internetworking 4) Path Definition

NIC - Network Interface Card - Every Node / system has NIC

MAC Address - Hardware Address - Physical Address - Ethernet Address

assigned by Manufacturer ( 12 bit Hexa decimal Number)

05.05.2022

----------

Hub - Old version of Switch - Totally outdated (lot of collisions)

Switch - speeds

Ethernet - 10Mbps (Ethernet), 1994-98

Fast Ethernet 100Mbps 2000

Giga Ethernet 1000Mbps or 1Gbps 2005

10G Ethernet 10G 2015

Bridge - Old version of Switch (Totally Obsolete)

LAN

WLAN - wireless Lan

Topology - Study of Networks

1. Client Server Model or STAR Topology

2. Peer to Peer or Bus Topology

3. Mesh Topology

4. Hybrid Toplogy

Open Systems Interconnection (OSI) model - ISO (Data Communications)

----------------------------------------------

Communication Protcol - (Rules)

7 - Application Layer - File, Message, database, print, email

6 - Presentation Layer - suite, browser,

5 - Session Layer - Interaction - handshake, Authentication

4 - Transport Layer - Path of packet flow / data flow, encapsulation, Acknowledments,

3 - Network Layer - Serivce Provider - Logical Addressing, ARP (Internet / Intranet), Routing

2 - Data Link Layer - Establishes connection to Network Layer (LLC), PHysical Identity/Addressing (MAC)

1 - Physical Layer - Devices, cables, connectors, topology

MAC - Media Access Control - Physical Identity ( 12 digit Hexa Number)

LLC - Logical Link Control

Physical Address / MAC Address / Ethernet Address / Hardware Address - 48 bit Binary or 12 digit Hexa

Logical Addressing / IP Addressing

ARP Address Resolution Protocol

Routing - Path Definition

Connection Oriented Protocol Connectionless Protocol

------------------------------------------------------------------------

More Reliability Less Reliability

Acknowledgement NO acknowledgments

Costly Less Cost

TCP UDP (User Datagram Protocol)

Internet - TCP/ IP Model Communication (4 layers)

7 - Application Layer

6 - Presentation Layer

5 - Session Layer - Application Layer

4 - Transport Layer - Host to Host Layer

3 - Network Layer - Internet Layer

2 - Data Link Layer - Access Layer

1 - Physical Layer

C:>\ipconfig - Report the IP configured

Ip Assignment can be done in 2 methods - Static / Dynamic

Static is manual and assigning IP from Router is dynamic

IANA - Internet Assigned Numbers Authority

IP Address Space - IP Addressing 1) IPv4 2) IPv6

IPv4 - 32 bits - 11111111.11111111.11111111.11111111 (8.8.8.8) 2^32 4Billion - 400Crores

255.255.255.255

IPv6 - 128Bits - 2^128

1. ARIN - American Region

2. APNIC - Asia Pacific

3. RIPE - Europe

4. LACNIC - Latin America

5. AFRINIC - AFrica

IP Addressing - Internet (from browser) / Intranet (Command Prompt)

Intranet / Private Networking

-----------------------------

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

06.05.2022

----------

Network

Classification of IP Addressing

-------------------------------

255.255.255.255 (32 Bits - 8.8.8.8)

---

Class A - (0-127) Very Large 2^24 Hosts 16Million or 1.6Crores

Class B - (128-191) Medium 2^16 Hosts 64K or 65536Hosts

Class C - (192-223) Small 2^8 Hosts or 256 Hosts

Not used in Internet / Intranet (Special Purpose)

Class D - (224-239) Multicasting (Routers Communication)

Class E - (240-255) Research (Future Use)

For Every Network

-----------------

Starting is called as Network Address

Range or Valid IP

Ending is called as Broadcast Address

192.168.1.0 - Class C - Network Address

192.168.1.(1 - 254) Range

192.168.1.255 - BC BroadCast Address

172.16.0.0 - Class B - Network Address

172.16.(0.1 - 255.254) - Range

172.16.255.255 - BC

10.0.0.0 - Class A - Network Address

10.0.0.1 - 10.255.255.254 - Range

10.255.255.255 - BC

10.0.0.1 2 3 ....10.0.0.255

10.0.1.0 1 2 3 ... 10.0.1.255

10.0.2.0.............

10.0.255.0.......10.0.255.255

10.1.0.0..

Router is a device which can communication to other Network and this called gateway.

Address given to Router is also called as gateway address.

Decimal Hexadecimal Binary(0,1)

0 0 0

1 1 1

2 2 10

3 3 11

4 4 100

5 5 101

6 6 110

7 7 111

8 8 1000

9 9 1001

10 A 1010

11 B 1011

12 C 1100

13 D 1101

14 E 1110

15 F 1111

16 10 10000 ........

17 11 10001

18 12 10010

19 13 10011

20 14 10100

Decimal to Binary

-----------------

50 (decimal) 110010 (Binary) 32(Hexadecimal)

110010 - 2^5 + 2^4 +2^1 = 32 + 16 + 2 = 50 (Hence Verified)

543210

75 - 4B

245 - F5

192.168.10.15 - convert into Binary

11000000.10101000.1010.1111

10101100.00010000.00010100.00110111

172.16.20.55

11011000.1011.0011110.0111010 (Convert to Hexa)

d8.b.1e.3a

216.11.30.58

d8.b.1e.3a

Subnetting - Introduction

-------------------------

A Large Network dividing into Smaller Network is called subnetting

(----------------------------------TMF----------------------------------------------------)

(----ProjectA---) (--------Project B---)(----Project C-----)........................

Dept Requirement Block Network Range Broad Count subnet

Count Addr cast bits(Y) MasK(X)

Human Resouces 10 16 0 1-14 15 4 8.8.8.4 (255.255.255.240)

Sales 12 16 16 17-30 31 4 8.8.8.4 (255.255.255.240)

Personnel 20 32 32 33-62 63 5 8.8.8.3 (255.255.255.224)

Payroll 30 32 64 65-94 95 5 8.8.8.3 (255.255.255.224)

Stores 15 16 96 97-110 111 4 8.8.8.4 (255.255.255.240)

Finance 14 16 112 113-126 127 4 8.8.8.4 (255.255.255.240)

IT 80 128 128 127-254 255 7 8.8.8.1 (255.255.255.128)

--- -----

7 subnet 181 256

--- ------

Total Bits (TB) - 32

Network Bits(N) 24 + 8 Host(H) Bits

TB=H + N

TB = X+Y

Hosts = 2^y -2

Subnets - 2^X

192.168.1.0/24

Human Resources - 192.168.1.0 (1-14) BC - 192.168.1.15

SNM - 8.8.8.4 - 11111111.11111111.11111111.11110000 - 255.255.255.240

VLSM - Variable Length Subnet Masing

CIDR - Classless Inter domain Routing

Manufacturing Industry

----------------------

BlCount Y bits N VIP Br Ad SNM(X) SNM

Dept A 25 32 5 0 1-30 31 24.3 224

Dept B 14 16 4 32 33-46 47 24.4 240

Dept C 7 16 4 48 49-62 63 24.4 240

Dept D 30 32 5 64 64-94 95 24.3 224

Dept E 15 32 5 96 97-126 127 24.3 224

Dept F 5 8 3 128 129-134 135 24.5 248

---

136 136

---

Dept A - 192.168.1.0/27 (/27 - cidr )

Dept B - 192.168.1.32/28

Dept C - 192.168.1.48/28

Dept F - 192.168.1.128/29

10000000 - 128

11000000 - 192

11100000 - 224

11110000 - 240

11111000 - 248

11111100 - 252

11111110 - 254

11111111 - 255

Network

179.99.0.0

No. of Subnets 265 9sn +16 = 25 - X Y -7

255.255.255.128

VPC - Virtual Private Cloud

Intranet / Private Networking

-----------------------------

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

(--------------------------- VPC -10.0.0.0/16 (64K Hosts) -----------------------------------------)

(---sub1---) (---sub2....) (----Sub3---) (---sub4-----)...................

10.0.0.0/24 10.0.1.0/23 10.0.3.0/24 10.0.4.0/23

256H 512H 256H 512H

Terminology

VPC - Virtual Private Cloud

Subnet -

Gateway - Router

Internet Gateway - router

Route - Defining Path - 1) Attaching VPC with Igw 2) Communication between subnet and igw

3) From Subnet to internet using NAT

NAT - Network Address Translation - Address translation from Private to Public and vice Versa

#!/bin/bash

# Install Apache Web Server and PHP

yum install -y httpd mysql php

# Download Lab files

#wget https://aws-tc-largeobjects.s3.amazonaws.com/ILT-TF-100-TUFOUN-1/4-lab-vpc-web-server/lab-app.zip

wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-RESTRT-1/52-lab-NF-vpc-web-server/s3/lab-app.zip

unzip lab-app.zip -d /var/www/html/

# Turn on web server

chkconfig httpd on

service httpd start

10.05.2022

----------

Task -1

-------

VPC - Lab VPC

IPv4 - 10.0.0.0/16

Public Subnet 1 10.0.0.0/24

Private Subnet 1 10.0.1.0/24

Task -2

Public Subnet 2 - 10.0.2.0/24

Private Subnet 2 - 10.0.3.0/24

Go to Route Table

Task -3

Security Groups - Web Security Group

Task 4

public ip 34.218.48.241

private ip 10.0.2.84

Service - Port

FTP - 21

SSH - 22

Telnet - 23

SMTP - 25 (Simple Mail Transfer Protocol)

DNS - 53 (Domain Name System)

WWW or HTTP- 80

POP3 - 110 Post office Protocol (Mail delivery)

SNMP - 161 (Simple Network Management Protocol)

HTTPS - 443 Secure HTTP

RDP - 3389 (Remote Desktop Protocol)

TCP or Connection Oriented UDP or Connectionless Protocol

Networking diagnostics tool

Ping Tool - ICMP (Messaging Protocol)

Ping Performs the following

1) Verifies the remote IP / host / website is OK / Reply / alive

2) Traces the IP address of the URL

3) Also Display the Latency (Typically in ms)

DNS Managment Tool

nslookup

traceroute

C:\Users\star>tracert -4 www.google.com

Tracing route to www.google.com [142.250.195.68]

over a maximum of 30 hops:

1 <1 ms 6 ms 3 ms reliance.reliance [192.168.29.1]

2 2 ms 1 ms 2 ms 10.14.152.1

3 12 ms 10 ms 11 ms 172.31.2.18

4 11 ms 14 ms 11 ms 192.168.59.124

5 12 ms 9 ms 11 ms 172.26.74.70

6 11 ms 13 ms 12 ms 172.26.75.131

7 10 ms 12 ms 11 ms 192.168.60.226

8 13 ms 13 ms 11 ms 192.168.60.227

9 22 ms 22 ms 22 ms 172.31.2.63

10 26 ms 26 ms 25 ms 72.14.196.126

11 21 ms 24 ms 24 ms 209.85.251.159

12 23 ms 22 ms 28 ms 142.251.55.73

13 30 ms 23 ms 25 ms maa03s38-in-f4.1e100.net [142.250.195.68]

Trace complete.

Telnet

256 - 2 =254 (Network / Broadcast)

AWS Cloud subnet Minimum reserved IP (5) 256 -5 = 251 (Network / Broadcast /DNS / Router / Network Manangement)

11.05.2022

----------

Network Security

----------------

Security - Protection (No Dangers / risks / safety / no threats /)

Data Security - Confidentiality, Integrity & Availability

Confidentiality - Confidentiality, allows authorized users to access sensitive and protected data.

Integrity - Integrity is the practice of showing a consistent and uncompromising adherence to original data

Availability -

Threats -

Malware - A Software which damages or destruction Security

Computer Virus, spyware, trojans, Ransomware, Worms, Bot, rootkits

Social Engineering - Phishing, Shoulder Surfing, Dumpster Diving, Tailgating,

Network Attacks - DOS Attack (Denial of Service)

Anti- Malware - Protection / Security - Stops / prevents your malicious programs with further attacks

Encryption - Plain Text data coverting to cipher text is called Encryption

(Cipher is algorithm based logic)

PT + Cipher = Cipher Text ----> Encryption

CT - Cipher = Plain Text ----> Decryption

Cryptography deals with Encryption / Decryption

Firewall - Protection your system by defining rules for data networking

Intrusion Detection System (IDS) - Network Montoring

Mitigation is a detection and protection policy that is adopted to safeguard networks.

Penetration testing and vulnerability scanning are also essential.

IDS - Alert (Monitoring)

IPS - Firewall (Block)

**How all layers works**

Now that you know the basics of how every

layer of out network model works, let's go through an exercise to look at how

everything works at every step of the way. Spoiler alert, things are about to

get a little geeky, in a good way. Imagine three networks, network A will

contain address space 10.1.1.0/24. Network B Will contain

address space 192.168.1.0/24, and network C will be 172.16.1.0/24. Router A sits between network A and

network B. With an interface configured with

an IP of 10.1.1.1 on network A, and an interface at

192.168.1.254 on network B. There's a second router, router B,

which connects networks B and C. It has an interface on network B

with an IP address of 192.168.1.1, and an interface on network C

with an IP address of 172.16.1.1. Now let's put a computer

on one of the networks. Imagine it's a desktop, sitting on

someone's desk at the workplace. It'll be our client in this scenario,

and we'll refer to it as computer 1. It's part of Network A and has been

assigned an IP address of 10.1.1.100. Now, let's put another computer

on one of our other networks. This one is a server in a data center,

it'll act as our server in this scenario, and we'll refer to it as computer 2. It's part of network C, and

has been assigned an IP address of 172.16.1.100, and

has a web server listening on port 80. An end user sitting at computer

1 opens up a web browser and enters 172.16.1.100 into the address bar,

let's see what happens. The web browser running on computer

1 knows it's been ordered to retrieve a web page from 172.16.1.100. The web browser communicates with the

local networking stack, which is the part of the operating system responsible for

handling networking functions. The web browser explains that

it's going to want to establish a TCP connection to 172.16.1.100, port 80. The networking stack will

now examine its own subnet. It sees that it lives on

the network 10.1.1.0/24, which means that the destination

172.16.1.100 is on another network. At this point, computer 1 knows that it'll

have to send any data to its gateway for routing to a remote network. And it's been configured

with a gateway of 10.1.1.1. Next, computer 1 looks at its ARP

table to determine what MAC address of 10.1.1.1 is, but

it doesn't find any corresponding entry. Uh-oh, it's okay,

computer A crafts an ARP request for an IP address of 10.1.1.1, which it sends to the hardware

broadcast address of all Fs. This ARP discovery request is sent

to every node on the local network. When router A receives this ARP message,

it sees that it's the computer currently assigned the IP

address of 10.1.1.1. So it responds to computer

1 to let it know about its own MAC address of 00:11:22:33:44:55. Computer 1 receives this response and now

knows the hardware address of its gateway. This means that it's ready to start

constructing the outbound packet. Computer 1 knows that it's being

asked by the web browser to form an outbound TCP connection, which

means it'll need an outbound TCP port. The operating system identifies

the ephemeral port of 50000 as being available, and opens a socket connecting

the web browser to this port. Since this is a TCP connection,

the networking stack knows that before it can actually transmit any of

the data the web browser wants it to, it'll need to establish a connection. The networking stack starts

to build a TCP segment. It fills in all the appropriate

fields in the header, including a source port of 50000 and

a destination port of 80. A sequence number is chosen and is used

to fill in the sequence number field. Finally, the SYN flag is set, and a

checksum for the segment is calculated and written to the checksum field. Our newly constructed TCP segment

is now passed along to the IP layer of the networking stack. This layer constructs an IP header. This header is filled in with

the source IP, the destination IP, and a TTL of 64, which is a pretty

standard value for this field. Next, the TCP segment is inserted as

the data payload for the IP datagram. And a checksum is calculated for

the whole thing. Now that the IP datagram

has been constructed, computer 1 needs to get this to

its gateway, which it now knows has a MAC address of 00:11:22:33:44:55, so an Ethernet Datagram is constructed. All the relevant fields are filled in

with the appropriate data, most notably, the source and destination MAC addresses. Finally, the IP datagram is inserted as

the data payload of the Ethernet frame, and another checksum is calculated. Now we have an entire Ethernet frame ready

to be sent across the physical layer. The network interface connected to

computer 1 sends this binary data as modulations of the voltage of

an electrical current running across a CAT6 cable that's connected

between it and a network switch. This switch receives the frame and

inspects the destination MAC address. The switch knows which of its interfaces

this MAC address is attached to, and forwards the frame across only

the cable connected to this interface. At the other end of this link is router A,

which receives the frame and recognizes its own hardware

address as the destination. Router A knows that this

frame is intended for itself. So it now takes the entirety of the frame

and calculates a checksum against it. Router A compares this checksum with

the one in the Ethernet frame header and sees that they match. Meaning that all of the data

has made it in one piece. Next, Router A strips

away the Ethernet frame, leaving it with just the IP datagram. Again, it performs a checksum

calculation against the entire datagram. And again, it finds that it matches,

meaning all the data is correct. It inspects the destination IP address and performs a lookup of this

destination in its routing table. Router A sees that in order to get data to the 172.16.1.0/24 network,

the quickest path is one hop away via Router B, which has an IP of 192.168.1.1. Router A looks at all

the data in the IP datagram, decrements the TTL by 1,

calculates a new checksum reflecting that new TTL value, and

makes a new IP datagram with this data. Router A knows that it needs to

get this datagram to router B, which has an IP address of 192.168.1.1. It looks at its ARP table, and

sees that it has an entry for 192.168.1.1. Now router A can begin to

construct an Ethernet frame with the MAC address of its interface

on network B as the source. And the MAC address on router B's

interface on network B as the destination. Once the values for all fields in

this frame have been filled out, router A places the newly constructed IP

datagram into the data payload field. Calculates a checksum, and

places this checksum into place, and sends the frame out to network B. Just like before,

this frame makes it across network B, and is received by router B. Router B performs all the same checks,

removes the the Ethernet frame encapsulation, and performs

a checksum against the IP datagram. It then examines

the destination IP address. Looking at its routing table, router B sees that the destination

address of computer 2, or 172.16.1.100, is on

a locally connected network. So it decrements the TTL by 1 again,

calculates a new checksum, and creates a new IP datagram. This new IP datagram is again

encapsulated by a new Ethernet frame. This one with the source and destination

MAC address of router B and computer 2. And the whole process is

repeated one last time. The frame is sent out onto network C, a switch ensures it gets sent out of the

interface that computer 2 is connected to. Computer 2 receives the frame, identifies

its own MAC address as the destination, and knows that it's intended for itself. Computer 2 then strips away the Ethernet

frame, leaving it with the IP datagram. It performs a CRC and recognizes that

the data has been delivered intact. It then examines the destination IP

address and recognizes that as its own. Next, computer 2 strips

away the IP datagram, leaving it with just the TCP segment. Again, the checksum for this layer is

examined, and everything checks out. Next, computer 2 examines

the destination port, which is 80. The networking stack on computer 2

checks to ensure that there's an open socket on port 80, which there is. It's in the listen state, and

held open by a running Apache web server. Computer 2 then sees that this

packet has the SYN flag set. So it examines the sequence number and

stores that, since it'll need to put that sequence number in the acknowledgement

field once it crafts the response. After all of that,

all we've done is get a single TCP segment containing a SYN flag

from one computer to a second one. Everything would have to

happen all over again for computer 2 to send a SYN-ACK

response to computer 1. Then everything would have

to happen all over again for computer 1 to send an ACK back to

computer 2, and so on and so on. Looking at all of this end to end

hopefully helps show how all the different layers of our networking model have

to work together to get the job done. I hope it also gives you some perspective

in understanding how remarkable computer networking truly is. Even more remarkable than that, you

[LAUGH] for making it through this module. Now it's time to apply your new

knowledge to the next assessment. When you're done, I'll see in the next

video, but first, another quiz, you got this. But even if you don't, just review the material until you

get more comfortable with this stuff.

