Gmail **Aravindh Seeneevasan <aravindh.sp@gmail.com>**

FW: Network

7 messages

aravindh.seeneevasan@accenture.com <aravindh.seeneevasan@accenture.com>
To: aravindh.seeneevasan@accenture.com, aravindh.sp@gmail.com
Cc: aravindh.sp@gmail.com, aravindh.seeneevasan@accenture.com

V2

Thanks & Regards

Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery

P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 11:58 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: RE: Network

V1

Thanks & Regards

Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery

P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 8:34 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Cc: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: Network

networks

connecting two or more devices to share the information and services

Protocols

is the rules that governs how devices should be communicate with each other

Network Reference Model

OSI-open system interconnection

DOD -Dept of Defense(TCP/IP)

Network types

Lan -Under a single administration or the infrastructure for connecting the resources inside a building

WAN -Two or more Lans connecting together to form a WAN or Two different adminstration

MAN - Connecting different locations or geographic area

SAN (Storage area network)- Provide high-speed , lossless connectivity to the data

VPN - (Virtual Private Network) - used to send data securely in an unsecure or public network

Term Internetwork:

Multiple networks connecting together. INTERNET is the larget internetwork.

Network Artitechture

Host -A device that is connected in the network can provide resources to the node of the network and also assigned with a valid address.

Client- Request data

Server- Send data to client

-disadv-Single point of failure(can be avoided using redundancy in the server layer)

Peer- Send and Request data

-Pose security problems since the data are spread across devices

Mainframe/termminal

-thin client protocols are

-RDP(remote desktop protocol) and ICA(Independent Computer Architecture)

WAN Connection Types

WANs are generally grouped into three separate **connection types**:

• Point-to-Point technologies

• Circuit-switched technologies

• Packet-switched technologies

\	Circuit Swithcing	Message switch	Packet switch
Approach	no store and forward	Store and forward	Store and forward
Connection	Connection	connectionless	may b connected or connectionless
Path	dedicated path	no dedicated	no dedicated
data rate	Constant	variable	Variable
following path	same path for entire transmission	diff route for diff packets	same path for VCI and independent path for Datagram approach
Bandwidth	fixed	fixed	Dynamic

Examples of Packet switched technology

Frame-Relay

• X25

OSI MODEL:1984

Interoperating b/wn products of diff manufacturers pose chalenge

Why are we going for layered approach

Proven standard

Switching:

Circuit switching

Message switching

Packet switching

UpperLayer are 765

App layer :7

- provides Interface between the user ,application and the network
- eg : web browser, email client
- =the user interact with application which in turn converted into a protocol and serves the specific functionality
- Eg: FTP,http,pop3,smtp
- Varity of functions:\
  - identifies communication partners
  - Determines the resource availability
  - Synchronizes communication.
- It wont interact with any other layer above but the below presentation layer

Presentation Layer:6

- Controls the formatting and syntax of the user application.
- ensures Data from the sending application understood by the receiving application.
- Eg:img,audios,videos and text
- If two devices doesnt support the same formatting ,presentation layer provides the converstion or translation functionality
- Additionally, it provides encryption and decryption

Session layer:5

- Establish,maintaining and terminating the connection
- Session communication/Transmission modes
  - Simplex
  - Half duplex
  - Full duplex

Lower Layer:4321

Transport that are happening in this layer is responsible for end-to-end communication

Transport Layer:4

End to END

-reliable transfer of data

Ensuring data receiving in the destination is error free and in order

Segmentation and sequencing

Acknowledgements

Flow control(Windowing) –Data transfer rate is negotiated to prevent congestion

Two Categories

Connection oriented -TCP

More reliable

Upon data lost , data can be resent

Connection is established after a 3 way handshake

Connection less oriented –UDP

TCP/UDP – Sliding window mechanism

Network Layer:3

Responsibl for Sending data to dissimilar network / send data across network

Responsible for

Logical addressing

-provides a unique address that identifies both the host, and the network that host exists on.

Routing

-determines the best path to a particular destination network, and then routes data accordingly

Protocols are :IP and IPX

IPV4,IPV6

-X.25 -1.56kbbs

Hop to hop

in computer **networking**, a **hop** is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways on the way. Each time packets are passe

TTL Is used for loop avoidance.

 The main purpose of the router are

– Route selection

– Packet forwarding

– Packet filtering

Data Link Layer :2

Responsible to send data within a same network

2 sublayers

LLc(Logical Link control)

Serves as an intermediary between physical link and all higher layer protocols

responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.

Additionally Error control and flow control

MAC(Media acess control)

Control the access to physical medium

CSMA/CD

-Higher layer data into frames, this is called framing or encapsulation.

- hardware addresses contain no mechanism for differentiating one network from another, and can only identify a host within a network.

-Frame relay-1.54mbps

-ATM

-Ethernet

-FDDI

The three main functions of Switch

1. Address learning – Learns the MAC address from the frame source MAC field

2. Forward/filter decisions – Make the decision based on the learned MAC address

3. Loop avoidance – Switch redundant path make unavoidable loop. Spanning Tree protocol

is the key to avoid the Loop in redundant path.

Node to Node delivery

Node:

In communication **networks**, a **node** (Latin nodus, 'knot') is either a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment). The definition of a **no**

Physical layer :1

Controls signaling and transferring of raw bits into the physical medium

- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the network topology as bus, mesh, or ring being some of the most common.

-NIC card

Network Devices

Hubs and repeaters(Layer 1)

Switches and Bridges(Layer 2)

Routers(layer 3)

Encapsulation

: As data is passed from the user application down the virtual layers of the OSI model, each layer adds a header (and sometimes a trailer) containing protocol information specific to that layer encapsulation.

Network Topology

• Bus • Star • Ring • Full or partial mesh

Network Devices

Hubs and repeaters(Layer 1) – 1 broadcast domain and 1 collision domain

A **collision domain** is simply defined as any physical segment where a collision can occur

A **broadcast domain** is a logical segmentation of a network, dictating how far a broadcast (or multicast) frame can propagate.

Hubs provide no intelligent forwarding

hubs will always forward every frame out every port, excluding the port originating the frame.

Switches and Bridges(Layer 2) – each port has 1 collision domain and by whole has 1 broadcast domain

- High port density for switches than bridges
- A switch behaves much like a hub when first powered on. The switch will flood every frame, including unicasts, out every port but the originating port. The switch will then build the MAC-a
- A switch is in a perpetual state of learning. However, as the MAC address table becomes populated, the flooding of frames will decrease, allowing the switch to perform more efficient fon
- ASIC(Application specific integrated circuits) for making intelligent forwarding decisions

Multilayer switch(referring to any switch that forwards traffic at layers higher than Layer-2**) &Routers(layer 3)**

Routers build routing tables to perform forwarding decisions, which contain the following:

• The destination network and subnet mask

• The next hop router to get to the destination network

• Routing metrics and Administrative Distance

The routing table is concerned with two types of Layer-3 protocols:

• Routed protocols - assigns logical addressing to devices, and routes packets between networks. Examples include IP and IPX.

• Routing protocols - dynamically builds the information in routing tables. Examples include RIP, EIGRP, and OSPF.

Each individual interface on a router belongs to its own collision domain. Thus, like switches, routers create more collision domains, which results in fewer collisions.

As a rule, a router will never forward broadcasts from one network to another network (unless, of course, you explicitly configure it to).

Traditionally, a router was required to copy each individual packet to its buffers, and perform a route-table lookup. Each packet consumed CPU cycles as it was forwarded by the router, result

switching functions were typically performed in hardware, and routing functions were typically performed in software.

Consider the above diagram. Remember that:

• Routers separate broadcast and collision domains. • Switches separate collision domains. • Hubs belong to only one collision domain. • Switches and hubs both only belong to one broadcas

TCP and UDP

The combination of the IP address and port number (identifying both the host and service) is referred to as a socket, and is written out as follows:

192.168.60.125:443

0-1023-Well known ports

1024 – 49151- Registrered Ports

49152-65535- dynamic ports- A client initiating a connection will randomly choose a port in this range as its source port (for some operating systems, the dynamic range starts at 1024 and hig

TCP establish connetion

Sys A send **Syn to** SYS B

Sys b replies **Syn+ACK to** sys A

Sys A send back **ACK to** sys b to establish the connection

TCP connection Establishment states:

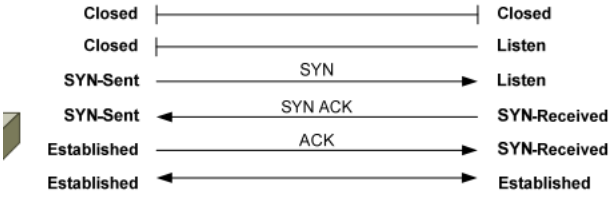
Closed

Listen

Syn-sent

Syn-received

Established



TCP connection Terminiation states:

Established

Fina-wait 1

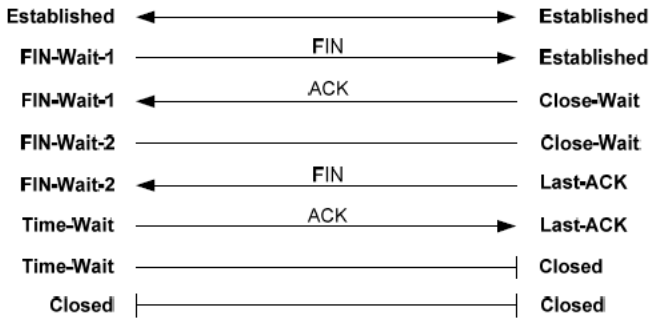
Close-wait

Fin-wait 2

Last_ack

Time_wait

Closed



Connections are identified by the sockets of both the source and destination host, and data specific to each connection is maintained in a Transmission Control Block (TCB)

TCP employs a sliding window mechanism.

Bytes in a sliding window fall into one of four categories:

• Bytes that have already been sent and acknowledged.

• Bytes that have been sent, but not acknowledged.

• Bytes that have not yet been sent, but the receiving host is ready for.

• Bytes that have not yet been sent, and the receiving host is not ready for.

TCP header flags

PSH –push and URG –Urgent flag

Eventhough the TCP window cant handle the data both of the above flags used to prioritize the data

RST – Reset Flag

TCP utilizes the Reset message, using the RST flag, to address half-open connections.

• URG (Urgent) – prioritizes specified traffic.

• ACK (Acknowledgment) – acknowledges a SYN or receipt of data.

• PSH (Push) – forces an immediate send even if window is not full.

• RST (Reset) – forcefully terminates an improper connection.

• SYN (Synchronize) – initiates a connection.

• FIN (Finish) – gracefully terminates a connection when there is further data to send.

Congestion

Network congestion in data **networking** and queueing theory is the reduced quality of service that occurs when a **network** node is carrying more data than it can handle. Typical effects incl

UDP

UDP, above all, is simple. It provides no three-way handshake, no flow control, no sequencing, and no acknowledgment of data receipt. UDP essentially forwards the segment and takes no fu

-connectionless

Less latency compared to TCP

latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the **latency**.

The following provides a quick comparison of TCP and UDP:

TCP	*UDP*
Connection-oriented	Connectionless
Guarantees delivery	Does *not* guarantee delivery
Sends acknowledgments	Does *not* send acknowledgments
Reliable, but slower than UDP	Unreliable, but faster than TCP
Segments and sequences data	Does *not* provide sequencing
Resends dropped segments	Does *not* resend dropped segments
Provides flow control	Does *not* provide flow control
Performs CRC on data	Also performs CRC on data
Uses port numbers	Also uses port numbers

Router Components

CCNA Study Guide v2.71 – Aaron Balchunas 152

Router Memory, Quick Reference

The following table details each of the basic types of **router memory**:

Memory	*Writable?*	*Volatile?*	*Function*
ROM	No	No	*Stores bootstrap*
Flash	Yes	No	*Stores IOS*
NVRAM	Yes	No	*Stores startup-config*
RAM	Yes	Yes	*Stores running-config*

DNS: Domain Name system :port 53

Conversion / Translation of IP address to human readable names and vice versa

How dns works

When request on google.com

It search in the local host cache

If the local host cache doesn't have a entry, it will be forwarded to local host file.

If the local host file doesn't have a entry., it will be forwarded to dns root server

Dns root server then will follow the hierarchy of domain resolution and reply back to the request.

DNS uses TCP for Zone Transfer over Port: 53

It is necessary to maintain a consistent DNS database between DNS Servers.

The connection is established between the DNS Server to transfer the zone data and Source and Destination DNS Servers

DNS uses UDP for DNS Queries over Port: 53

A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it must re-transmit the DNS Query using the TCP after 3-5 s

Dns

Resolving the human readable name into IP and vice versa.

There are two common methods for implementing name resolution:

• A **static file** on each host on the network, containing all the name-toaddress translations (examples include the HOSTS/LMHOSTS files).

• A **centralized server** that all hosts on the network connect to for name resolution.

Dynamic DNS allows DNS to be integrated with Dynamic Host Configuration Protocol (DHCP). When DHCP hands out an IP address lease, it will automatically update the DNS entry for that host on the DNS server.

DHCP(Dynamic host control protocol) :port 67 Server and Port 68 for client and for Port 69 is for TFTp

DORA Process

DHCP servers **lease** out IP addresses to DHCP clients, for a specific period of time. There are four steps to this DHCP process:

• When a DHCP client first boots up, it broadcasts a **DHCPDiscover** message, searching for a DHCP server.

• If a DHCP server exists on the local segment, it will respond with a **DHCPOffer,** containing the "offered" IP address, subnet mask, etc.

• Once the client receives the offer, it will respond with a **DHCPRequest**, indicating that it will accept the offered protocol information.

• Finally, the server responds with a **DHCPACK**, acknowledging the clients acceptance of offered protocol information.

By default, DHCP leases an address for **8 days**. Once 50% of the lease expires, the client will try to renew the lease with the *same* DHCP server.

SNMP Port 161(TCP) and port 162(SNMP trap for both tcp and udp)

161-polling

162-traps

Used to retrival of metrics-

Eg: whats my cpu usage, how much is my ram occupied,

Polling(requesting for the information) - Once in a while server request router for the information of devics to a router and router send backs the information

Polling happens using OID(object ids)

MIB-Management information base , basically a DNS for OIDs

Trap – on a unfortunate event in the router it is having an option of sending a trap.

Router saying server hey something happened in me. Kindly check – its based on the security level

Syntax: snmp-server community cisco ro(read only)or rw(read/wirte)

Snmp enable traps

Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol for collecting and organizing information about managed devices on IPnetworks and for modif servers, workstations, printers, modem racks and more.[1]

Syslog:

Useful for Event management

Controls on an unfortunate event occurs based on the log level it will capture the logs and can b further used for troubleshooting purpose.

Ports 514-used for system logging(UDP)

Port 601-reliable syslog service(TCP)

Port 6514 – reliable syslog over TLS(TCP)

Port 10514- TLS enabled syslog (TCP/UDP)

Severity Level	Name	Description
0	Emergencies	Severe conditions that render a system unusable
1	Alerts	Conditions that require immediate attention
2	Critical	Conditions that should be addressed to prevent an interruption in service, but less severe than an Alert condition
3	Errors	An error condition that does not render the system unusable
4	Warnings	A condition where an operation failed to successfully complete
5	Notifications	An administrative notification about a change to the system
6	Informational	Information about a normal system operation
7	Debugging	Very detailed information about system operation, typically used for troubleshooting

Configuring syslogs

>Config terminal

>logging 192.168.1.2(server address where the syslog gets captured)

>logging trap 5(log level) or >logging trap notificational(in words)

SMTP:

PoRT 25 FOR BOTH TCP AND UDP

Arcsight:

https://youtu.be/_Fvx_nI6E4c

IP addressing

Class A : 1.0.0.0 to 127.255.255.255

Class b :128 to 191

Class c: 192 to 223 -

Class d: 224 to 239 – Multicast purpose or group address

Class e: 240 to 255 –Experimental use

Binary to decimal -2^0 to 2^7

Decimal to binary –

Divide the number by 2 and have the reminders has binary number, - L divide method

Network address is the first address in the block – it defines itself to the rest of the internet

Last address of the block is called broadcast address of that block

NetIds=All 1's

Host Id's =All 0's

Default mask:

All net id will be 0 and all host id will be 1

Default mask will be given based on the class

Masking concept:

Identify the first address of the block or network address

An address in the block with AND operation gives the first address of the block

Eg

23.56.7.91

255.0.0.0

_____

23.0.0.0(first address/network address)

Limited broadcast address

255.255.255.255

Router blocks the limited broadcast packet

Subnetting

Well utilization of address space

Subnet mask:

All net ids and subnet ids will be 1 and host id will be 0

Security information and event management

In the field of computer security, **security information and event management** (**SIEM**) software products and services combine security information management (SIM) and se
hardware and applications.

Hp Arcsight

IBM Qradar

Jitter is defined as a variation in the delay of received packets.

VLan

a switch can be *logically* segmented

into separate broadcast domains, using **Virtual LANs** (or **VLANs**).

Each VLAN represents a unique broadcast domain:

• Traffic between devices within the *same* VLAN is switched.

• Traffic between devices in *different* VLANs requires a Layer-3

device to communicate.

Route command

>Enable –(to move to privilege mode)

>in privilege mode we can ran all show command

>config terminal(after reaching this mode we actually configure the device)

>show ip route(to display routing table)

>show ip access-list(to display access list)

>show xlate(to display the pat configuration)

NAT-Network Address Translation

The rapid growth of the Internet resulted in a shortage of available IPv4

addresses. In response, a specific subset of the IPv4 address space was

designated as *private,* to temporarily alleviate this problem.

A **public address** can be routed on the Internet. Thus, devices that must be

Internet-accessible must be configured with (or *reachable* by) public

addresses. Allocation of public addresses is governed by the Internet

Assigned Numbers Authority (IANA).

A **private address** is intended for internal use within a home or

organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses

NAT can also perform public-to-public address translation, as well as private-to-private address translation.

Private address range

class:

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

CISCO FIREWALL

four main administrative access modes:

Monitor mode :password recovery – to access this mode press break/esc

Unprivileged mode -

Privileged mode

Configure mode

Running Config – Volatile and stored in the RAM- to save the current running config, we need to type 'write memory' or copy run start

Startup config - non-volatile

Security levels

0-100

0- Outside

1-99- DMZ(Demilitarized Zone)

100-Inside

Highest Security level /interface can communicatge with lower security level and not vice versa.

Traffic from Higher Security Level to Lower Security Level

Allow all unless specified by a ACL

IF NAT is enabled, ther must be a **nat and global pair**

Traffic from Lower Security Level to Higher Security Level:

Drop all unless specified by an ACL.

IF NAT is enabled, ther must be a static-NAT between a higher to lower level.

Traffic between interfaces with same Security Level:

By default, don't allow,

Unless configured with **same-scurity-traffic-permit** command.

Firewall config:

STEP1: Configure a privileged level password

STEP2: Enable Command Line Management

1.)create a username and password

2.) ! Generate a 1024 bit RSA key pair for the firewall which is required for SSH

3.) Specify the hosts allowed to connect to the security appliance.

STEP3: **Configure a Firewall Hostname**

To create a route

ciscoasa(config)# route "*interface-name*" "*destination-ip-address*" "*netmask*" "*gateway*"

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1 ← Default Route

ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1 ← Static Route

Dynamic NAT :

From the pool of Ip address in the higher security interfafce as real ip maped with the pool of ip address in the mapped addrees pol for outbound communication.

Dynamic PAT:

Many to One:

The many real IP will be mapped to a single public IP with the request on each real IP will be assigned with the Port number for the request.

Static NAT

Bidirectional communication:

One-to-one address mapping between real and mapped ip

Lower level security interface can communicate with higher level inrerface with appropriate ACL configured.

the ASA firewall implements NAT in two ways:

"***Network object NAT***"

"***Twice NAT***"

NAT 0 or Identity Nat: Used for IPsec or VPN

ACL:

The Access Control List, as the name implies, is a List of statements (called Access Control Entries) that permit or deny traffic from a source to a destination.

Access control lists (ACLs) can be used for two purposes on Cisco devices:

to **filter** traffic, and to **identify** traffic

Each rule or line in

an access-list provides a condition, either **permit** or **deny**:

when filtering traffic, access lists are applied on interfaces.

Only one access list **per interface**, **per protocol**, **per direction** is allowed.

Two Golden Rules of Access Lists:

1. If a bit is set to **0** in a wild-card mask, the corresponding bit in the address must be **matched exactly.**
2. If a bit is set to **1** in a wild-card mask, the corresponding bit in the address can **match any number.** In other words, we "don't care" what number it matches.

Syntax:

The command format of an Access Control List is the following:

**ciscoasa(config)# access-list "*access_list_name"* [line *line_number*] [extended] {*deny* | *permit*} *protocol "source_address" "mask" [operator source_port] "dest_address" "mask*

Acess group

ciscoasa(config)# access-group "*access_list_name"* [in|out] interface "*interface_name*"

access-group "*access_list_name"* global

Access group used to bind the access list with the interface

There are four types of object groups:

Network: Used to group together hosts or subnets.

Service: Used to group TCP or UDP port numbers.

Protocol: Used to group protocols.

ICMP-type: Used to group ICMP message types.

_____

IDS firewall difference

Stateful/stateless firewall

Steless: Packet filtering or static filtering

It just allow or deny the traffic based on ACL.

It filters the traffic based on the below conditions.

Source Ip/Port

Destination Ip /Port

Protocol

Adv: easy to implement

Disadv : Noway to determine if the packet is part of an already existing connection.

Applications use random port numbers and these will trouble operating because of this.

IP spoofing attacks.

Statefull firewall: Dynamic filtering

IT monitors the connection state. Avoid TCP based attacks

Not only monitors the connection but also monitors the sequence numbers

Inside can start connect with outside and not vice versa.

All this will be accomplished by a session table called STATE table.

State table is dynamic, when the connection go quiet from inside, the outside cannot initiate the connection to the insider.

STATE table.

- Source and dest IPaddres/Port numbers
- TCP and UDP flag settings
- TCP sequence info.

TCP packets outside an expected will be dropped

Disadv: application layer attacks –Proxy server

Class A B C D - sub netting

Difference between router and switch

	Router	Switch
Used for	Connecting two or more networks	Connecting t
Function	Directs data in a network. Passes data between home computers, and between computers and the modem.	Allow to con
Used in (LAN, MAN, WAN)	LAN, WAN	LAN
Transmission Type	At Initial Level Broadcast then Uni-cast & Multicast	First broadca
Data Transmission form	Packet	Frame (L2 Sv
Layer	Network Layer (Layer 3 devices)	Data Link La
Ports	2/4/2008	Switch is mu
Device Type	Networking device	Active Devic
Table	Store IP address in Routing table and maintain address at its own.	Switches use
Transmission Mode	Full duplex	Half/Full du
Broadcast Domain	In Router, every port has its own Broadcast domain.	Switch has o

Definition	A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation.	A network s considered n
Device Category	Intelligent Device	Intelligent D
Bandwidth sharing	Bandwidth sharing is Dynamic (Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default percent-value is 0. The percent-value range is 1-96.)	There is no s
Speed	1-10 Mbps (Wireless); 100 Mbps (Wired)	10/100 Mbps
Routing Decision	Take faster routing decisions	Take more ti
NAT (Network Address Translation)	Routers can perform NAT	Switches can
Faster	In a different network environment (MAN/ WAN), a router is faster than an L3 switch.	In a LAN en
Features	Firewall VPN Dynamic hadling of Bandwidth	Priority rt ra
Examples	Linksys WRT54GL Juniper MX & EX series Cisco 3900, 2900, 1900	Alcatel's Om
Address used for data tramsmission	Uses IP address	Uses MAC a

Arp table and reverseARP

Arp request is broadcast and arp reply is unicast

ARP table maintains IP address corresponding mac address

RArp request is broadcast and Rarp reply is unicast

RARP request for corresponding mac address for a given IP address.

Inline/Passive in IDS

SSH vs TLS

Linux

Ip configuration in Linux

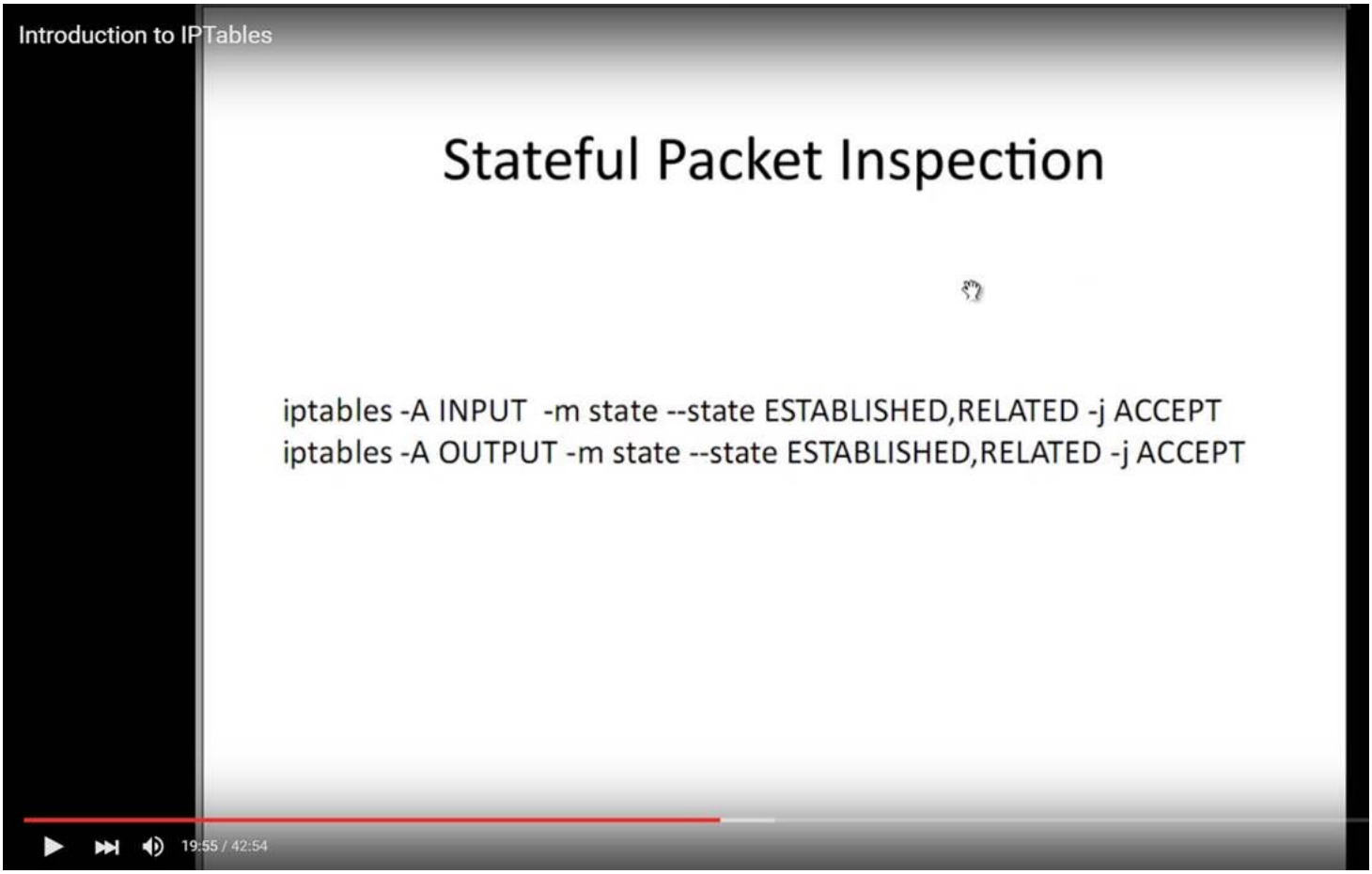
ifconfig interfacename netmask ip up/down

https://www.youtube.com/watch?v=SnACG4TDqJw

dns

iptables:

Packet filterting application in linux based os.



https://www.youtube.com/watch?v=XKfhOQWrUVw

check service status

netstat –a | grep ftp

packet capture -wireshark tcpdump

Project:

Challenges in Manet :

Energy centric,

Dynamic Topology,

Less computation power,

Attacks

Wormhole- advertise valid path and drop the packets

Greyhole- group of nodes advertises itself as a valid path and send the path to the destination after a long time. -> Batery consumption.

Blackhole- Advertises itself as a valid path and sends a fake information to the destination.

Model:

Trust proctor= Energy+direct trust+recommendation trust

Trust handler =Alarm table,friend table, trust evaluator

CA-Certificate authority

TCPdump :

_____

-h version checking

-d identify the available interface

-i interface

-c packet capture size

-s packet bytes size

-w to capture files

-r to read the captured files

-v verbose mode

-t time display

-q –quantity of content display

Capture the packets in the network and analyze the packet

Details abt the packet can either displayed on the screen or can be saved as a pcap file

Libpcap library used for packet filtering.

Version checking

Tcpdump –h

To identify the available interface like eth0 or eth1 like dat

Tcpdump –d

To capture packet using any option -I

Tcpdump –I any

Tcpdump wont stop capturing once start unles interpret by a user command - >ctrl+z

To capture specified number of packets use below -c

Tcpdump –I any –c 5

The above command will capture 5 packets

To display the ip address and port numbers in the result use below -n

Sudo tcpdump –I any –c 5 –n

Capture size of a packet can be altered by using –s

Sudo tcpdump –I any –c 5 –n –s 96 #capture 96 byte

Sudo tcpdump –I any –c 5 –n –s 0 #maximum size of 65535

To capture one direction of traffic:

Sudo tcpdump –I any –c 20 -n tcp and dst port 49952 –t

A single packet looks like the below:

IP sourceIP.port > destinationip.port flags[TCP] acq/seq , window , length

To save the capture for future analysis –w

Sudo tcpdump –I any –w capture.pcap

While capturing packet in the file , usually we cant see how many packets are captured in the CLI, to address this , we will use –v to display number of records got captured in the file

Sudo tcpdump –I any –w capture.pcap –v

To Read the capture files.

Sudo tcpdump –n –r capture.pcap

If the file is large, it will directly go the eof , to enable scrolling use | less

Sudo tcpdump –n –r capture.pcap |less (to scroll up and down)

TCPdump filters

Filters are used to isolate the traffic

To capture packet on particular host

Tcpdump –I eth1 –n host 10.0.0.1 –c 5

To see one direction traffic:

That s packet capture only from the sender src

Tcpdump –I eth1 –n src host 10.0.0.1 –c

Traffic between 2 ip ->source and destination – by using and operator

Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 –c 5

To capture packet only on specific port

Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 and port 80

Compound expression : to show traffic for port 80 or port 443 on the sending host

Tcpdump –I eth0 –n “host 192.168.1.1 \> and (port 80 or port 443)”

To capture ipv6 packets

Tcpdump –I etho 0 ip6

To ping ipv6 address

Ping6 IPV6

Verbose output

Tcpdump –I eth0 –v

Minimal quantity of output

Tcpdump –I eth0 –q

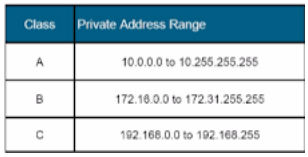
Timestamp

-t

-ttt

-ttttt

5 attachments



Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image004.png
22K

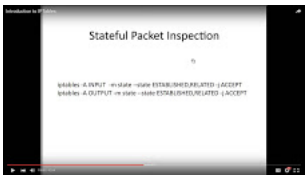


image008.jpg
43K

common_ports.pdf
20K

Cisco-ASA-Firewall-Fundamentals-2nd-Edition.pdf
2559K

printer.pdf
2751K

aravindh.seeneevasan@accenture.com <aravindh.seeneevasan@accenture.com>
To: aravindh.sp@gmail.com
Cc: aravindh.sp@gmail.com

From: Seeneevasan, Aravindh
Sent: Sunday, April 24, 2016 11:05 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>; aravindh.sp@gmail.com
Cc: aravindh.sp@gmail.com; Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: FW: Network

V2

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 11:58 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: RE: Network

V1

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 8:34 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Cc: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: Network

networks
connecting two or more devices to share the information and services
Protocols
is the rules that governs how devices should be communicate with each other

Network Reference Model
OSI-open system interconnection
DOD -Dept of Defense(TCP/IP)

Network types
Lan -Under a single administration or the infrastructure for connecting the resources inside a building
WAN -Two or more Lans connecting together to form a WAN or Two different adminstration
MAN - Connecting different locations or geographic area
SAN (Storage area network)- Provide high-speed , lossless connectivity to the data
VPN - (Virtual Private Network) - used to send data securely in an unsecure or public network

Term Internetwork:
Multiple networks connecting together. INTERNET is the larget internetwork.

Network Artitechture
Host -A device that is connected in the network can provide resources to the node of the network and also assigned with a valid address.

Client- Request data
Server- Send data to client
-disadv-Single point of failure(can be avoided using redundancy in the server layer)
Peer- Send and Request data
-Pose security problems since the data are spread across devices
Mainframe/termminal
-thin client protocols are
-RDP(remote desktop protocol) and ICA(Independent Computer Architecture)

WAN Connection Types

WANs are generally grouped into three separate **connection types**:
• Point-to-Point technologies
• Circuit-switched technologies
• Packet-switched technologies

\	Circuit Swithcing	Message switch	Packet switch
Approach	no store and forward	Store and forward	Store and forward
Connection	Connection	connectionless	may b connected or connectionless
Path	dedicated path	no dedicated	no dedicated
data rate	Constant	variable	Variable
following path	same path for entire transmission	diff route for diff packets	same path for VCI and independent path for Datagram approach
Bandwidth	fixed	fixed	Dynamic

Examples of Packet switched technology
Frame-Relay
• X25

OSI MODEL:1984
Interoperating b/wn products of diff manufacturers pose chalenge
Why are we going for layered approach
Proven standard
A STANDARDIZED ARCHITECTURE DEFINING N/W COMMUNICATION.
A STANDARD TO CREATE STANDARD.

Switching:
Circuit switching
Message switching
Packet switching

UpperLayer are 765
App layer :7
- provides Interface between the user ,application and the network
- eg : web browser, email client
- =the user interact with application which in turn converted into a protocol and serves the specific functionality
- Eg: FTP,http,pop3,smtp
- Varity of functions:\

- identifies communication partners
- Determines the resource availability
- Synchronizes communication.
- It wont interact with any other layer above but the below presentation layer

Presentation Layer:6

- Controls the formatting and syntax of the user application.
- ensures Data from the sending application understood by the receiving application.
- Eg:img,audios,videos and text
- If two devices doesnt support the same formatting ,presentation layer provides the converstion or translation functionality
- Additionally, it provides encryption and decryption

Session layer:5

- Establish,maintaining and terminating the connection
- Session communication/Transmission modes
- Simplex
- Half duplex
- Full duplex

Lower Layer:4321

Transport that are happening in this layer is responsible for end-to-end communication

Transport Layer:4

End to END

-reliable transfer of data

Ensuring data receiving in the destination is error free and in order

Segmentation and sequencing

Acknowledgements

Flow control(Windowing) –Data transfer rate is negotiated to prevent congestion

Application separation via PORTS

Two Categories

Connection oriented -TCP

More reliable

Upon data lost , data can be resent

Connection is established after a 3 way handshake

Connection less oriented –UDP

TCP/UDP – Sliding window mechanism

Network Layer:3

Responsibl for Sending data to dissimilar network / send data across network

Responsible for

Logical addressing

-provides a unique address that identifies both the host, and the network that host exists on.

Routing

-determines the best path to a particular destination network, and then routes data accordingly

Protocols are :IP and IPX

IPV4,IPV6

-X.25 -1.56kbbs

Hop to hop

in computer **networking**, a **hop** is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways on the way. Each t

TTL Is used for loop avoidance.

 The main purpose of the router are

– Route selection

– Packet forwarding

– Packet filtering

Data Link Layer :2

Responsible to send data within a same network

2 sublayers

LLc(Logical Link control)

Serves as an intermediary between physical link and all higher layer protocols

responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.

Additionally Error control and flow control

MAC(Media acess control)

Control the access to physical medium

CSMA/CD

-Higher layer data into frames, this is called framing or encapsulation.

- hardware addresses contain no mechanism for differentiating one network from another, and can only identify a host within a network.

-Frame relay-1.54mbps

-ATM

-Ethernet

-FDDI

The three main functions of Switch

1. Address learning – Learns the MAC address from the frame source MAC field
2. Forward/filter decisions – Make the decision based on the learned MAC address
3. Loop avoidance – Switch redundant path make unavoidable loop. Spanning Tree protocol

is the key to avoid the Loop in redundant path.

Node to Node delivery
Node:
In communication **networks**, a **node** (Latin nodus, 'knot') is either a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment).

Physical layer :1
Controls signaling and transferring of raw bits into the physical medium

- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the network topology as bus, mesh, or ring being some of the most common.

-NIC card

Network Devices
Hubs and repeaters(Layer 1)
Switches and Bridges(Layer 2)
Routers(layer 3)

Encapsulation
: As data is passed from the user application down the virtual layers of the OSI model, each layer adds a header (and sometimes a trailer) containing protocol information specific to tha
encapsulation.

Network Topology

• Bus • Star • Ring • Full or partial mesh

Network Devices
Hubs and repeaters(Layer 1) – 1 broadcast domain and 1 collision domain
A **collision domain** is simply defined as any physical segment where a collision can occur
A **broadcast domain** is a logical segmentation of a network, dictating how far a broadcast (or multicast) frame can propagate.
Hubs provide no intelligent forwarding
hubs will always forward every frame out every port, excluding the port originating the frame.
Switches and Bridges(Layer 2) – each port has 1 collision domain and by whole has 1 broadcast domain

- High port density for switches than bridges
- A switch behaves much like a hub when first powered on. The switch will flood every frame, including unicasts, out every port but the originating port. The switch will then
- A switch is in a perpetual state of learning. However, as the MAC address table becomes populated, the flooding of frames will decrease, allowing the switch to perform mc
- ASIC(Application specific integrated circuits) for making intelligent forwarding decisions

Multilayer switch(referring to any switch that forwards traffic at layers higher than Layer-2**) &Routers(layer 3)**
Routers build routing tables to perform forwarding decisions, which contain the following:
• The destination network and subnet mask
• The next hop router to get to the destination network
• Routing metrics and Administrative Distance

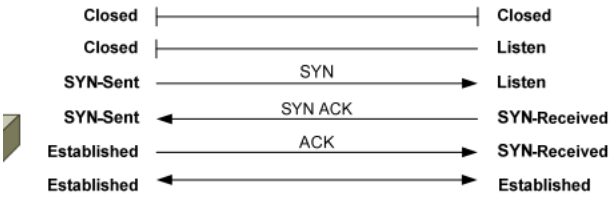
The routing table is concerned with two types of Layer-3 protocols:
• Routed protocols - assigns logical addressing to devices, and routes packets between networks. Examples include IP and IPX.
• Routing protocols - dynamically builds the information in routing tables. Examples include RIP, EIGRP, and OSPF.
Each individual interface on a router belongs to its own collision domain. Thus, like switches, routers create more collision domains, which results in fewer collisions.
As a rule, a router will never forward broadcasts from one network to another network (unless, of course, you explicitly configure it to).
Traditionally, a router was required to copy each individual packet to its buffers, and perform a route-table lookup. Each packet consumed CPU cycles as it was forwarded by the router,
switching functions were typically performed in hardware, and routing functions were typically performed in software.

Consider the above diagram. Remember that:
• Routers separate broadcast and collision domains. • Switches separate collision domains. • Hubs belong to only one collision domain. • Switches and hubs both only belong to one br

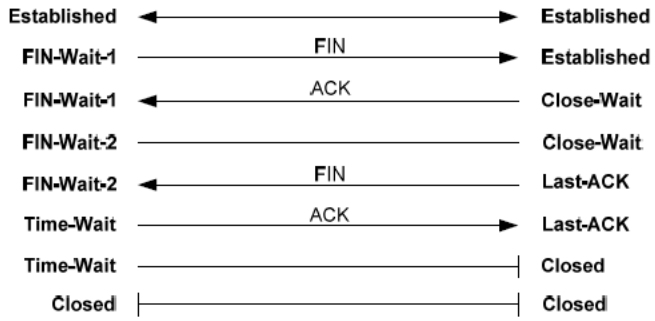
TCP and UDP
The combination of the IP address and port number (identifying both the host and service) is referred to as a socket, and is written out as follows:
192.168.60.125:443
0-1023-Well known ports
1024 – 49151- Registrered Ports
49152-65535- dynamic ports- A client initiating a connection will randomly choose a port in this range as its source port (for some operating systems, the dynamic range starts at 1024 a

TCP establish connetion
Sys A send **Syn to** SYS B
Sys b replies **Syn+ACK to** sys A
Sys A send back **ACK to** sys b to establish the connection

TCP connection Establishment states:
Closed
Listen
Syn-sent
Syn-received
Established



TCP connection Terminiation states:
Established
Fina-wait 1
Close-wait
Fin-wait 2
Last_ack
Time_wait
Closed



Connections are identified by the sockets of both the source and destination host, and data specific to each connection is maintained in a Transmission Control Block (TCB)

TCP employs a sliding window mechanism.
Bytes in a sliding window fall into one of four categories:
• Bytes that have already been sent and acknowledged.
• Bytes that have been sent, but not acknowledged.
• Bytes that have not yet been sent, but the receiving host is ready for.
• Bytes that have not yet been sent, and the receiving host is not ready for.

TCP header flags
PSH –push and URG –Urgent flag
Eventhough the TCP window cant handle the data both of the above flags used to prioritize the data
RST – Reset Flag
TCP utilizes the Reset message, using the RST flag, to address half-open connections.
• URG (Urgent) – prioritizes specified traffic.
• ACK (Acknowledgment) – acknowledges a SYN or receipt of data.
• PSH (Push) – forces an immediate send even if window is not full.
• RST (Reset) – forcefully terminates an improper connection.
• SYN (Synchronize) – initiates a connection.
• FIN (Finish) – gracefully terminates a connection when there is further data to send.

Congestion
Network congestion in data **networking** and queueing theory is the reduced quality of service that occurs when a **network** node is carrying more data than it can hand

UDP

UDP, above all, is simple. It provides no three-way handshake, no flow control, no sequencing, and no acknowledgment of data receipt. UDP essentially forwards the segment and takes
-connectionless
Less latency compared to TCP
latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the **latency**.

The following provides a quick comparison of TCP and UDP:

TCP	*UDP*
Connection-oriented	Connectionless
Guarantees delivery	Does *not* guarantee delivery
Sends acknowledgments	Does *not* send acknowledgments
Reliable, but slower than UDP	Unreliable, but faster than TCP
Segments and sequences data	Does *not* provide sequencing
Resends dropped segments	Does *not* resend dropped segments
Provides flow control	Does *not* provide flow control
Performs CRC on data	Also performs CRC on data
Uses port numbers	Also uses port numbers

Router Components

Router Memory, Quick Reference

The following table details each of the basic types of **router memory**:

Memory	*Writable?*	*Volatile?*	*Function*
ROM	No	No	*Stores bootstrap*
Flash	Yes	No	*Stores IOS*
NVRAM	Yes	No	*Stores startup-config*
RAM	Yes	Yes	*Stores running-config*

DNS: Domain Name system :port 53
Conversion / Translation of IP address to human readable names and vice versa

How dns works
When request on google.com

It search in the local host cache
If the local host cache doesn't have a entry, it will be forwarded to local host file.
If the local host file doesn't have a entry., it will be forwarded to dns root server
Dns root server then will follow the hierarchy of domain resolution and reply back to the request.

DNS uses TCP for Zone Transfer over Port: 53
It is necessary to maintain a consistent DNS database between DNS Servers.
The connection is established between the DNS Server to transfer the zone data and Source and Destination DNS Servers

DNS uses UDP for DNS Queries over Port: 53
A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it must re-transmit the DNS Query using the TCP after 3-5 s

Dns

Resolving the human readable name into IP and vice versa.

There are two common methods for implementing name resolution:
• A **static file** on each host on the network, containing all the name-toaddress translations (examples include the HOSTS/LMHOSTS files).
• A **centralized server** that all hosts on the network connect to for name resolution.

Dynamic DNS allows DNS to be integrated with Dynamic Host Configuration Protocol (DHCP). When DHCP hands out an IP address lease, it will automatically update the DNS entry for that host on the DNS server.

DHCP(Dynamic host control protocol) :port 67 Server and Port 68 for client and for Port 69 is for TFTp

DORA Process

DHCP servers **lease** out IP addresses to DHCP clients, for a specific period

of time. There are four steps to this DHCP process:
• When a DHCP client first boots up, it broadcasts a **DHCPDiscover** message, searching for a DHCP server.
• If a DHCP server exists on the local segment, it will respond with a **DHCPOffer,** containing the "offered" IP address, subnet mask, etc.
• Once the client receives the offer, it will respond with a **DHCPRequest**, indicating that it will accept the offered protocol information.
• Finally, the server responds with a **DHCPACK**, acknowledging the clients acceptance of offered protocol information.

By default, DHCP leases an address for **8 days**. Once 50% of the lease expires, the client will try to renew the lease with the *same* DHCP server.

SNMP Port 161(TCP) and port 162(SNMP trap for both tcp and udp)

161-polling
162-traps

Used to retrival of metrics-
Eg: whats my cpu usage, how much is my ram occupied,

Polling(requesting for the information) - Once in a while server request router for the information of devics to a router and router send backs the information
Polling happens using OID(object ids)
MIB-Management information base , basically a DNS for OIDs

Trap – on a unfortunate event in the router it is having an option of sending a trap.
Router saying server hey something happened in me. Kindly check – its based on the security level

Syntax: snmp-server community cisco ro(read only)or rw(read/wirte)
Snmp enable traps

Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol for collecting and organizing information about managed devices on IPnetworks and for modify servers, workstations, printers, modem racks and more.[1]

Syslog:
Useful for Event management
Controls on an unfortunate event occurs based on the log level it will capture the logs and can b further used for troubleshooting purpose.

Ports 514-used for system logging(UDP)
Port 601-reliable syslog service(TCP)
Port 6514 – reliable syslog over TLS(TCP)
Port 10514- TLS enabled syslog (TCP/UDP)

Severity Level	Name	Description
0	Emergencies	Severe conditions that render a system unusable
1	Alerts	Conditions that require immediate attention
2	Critical	Conditions that should be addressed to prevent an interruption in service, but less severe than an Alert condition
3	Errors	An error condition that does not render the system unusable
4	Warnings	A condition where an operation failed to successfully complete
5	Notifications	An administrative notification about a change to the system
6	Informational	Information about a normal system operation
7	Debugging	Very detailed information about system operation, typically used for troubleshooting

Configuring syslogs
>Config terminal
>logging 192.168.1.2(server address where the syslog gets captured)
>logging trap 5(log level) or >logging trap notificational(in words)

SMTP:
PoRT 25 FOR BOTH TCP AND UDP

Arcsight:
https://youtu.be/_Fvx_nI6E4c

IP addressing
Class A : 1.0.0.0 to 127.255.255.255
Class b :128 to 191
Class c: 192 to 223 -
Class d: 224 to 239 – Multicast purpose or group address
Class e: 240 to 255 –Experimental use

Binary to decimal -2^0 to 2^7
Decimal to binary –
Divide the number by 2 and have the reminders has binary number, - L divide method

Network address is the first address in the block – it defines itself to the rest of the internet
Last address of the block is called broadcast address of that block
NetIds=All 1's
Host Id's =All 0's

Default mask:
All net id will be 0 and all host id will be 1
Default mask will be given based on the class

Masking concept:
Identify the first address of the block or network address
An address in the block with AND operation gives the first address of the block

Eg
23.56.7.91
255.0.0.0
_____
23.0.0.0(first address/network address)

Limited broadcast address
255.255.255.255
Router blocks the limited broadcast packet

Subnetting
Well utilization of address space

Subnet mask:
All net ids and subnet ids will be 1 and host id will be 0

Security information and event management

In the field of computer security, **security information and event management** (**SIEM**) software products and services combine security information management (SIM) and se hardware and applications.

Hp Arcsight
IBM Qradar

Jitter is defined as a variation in the delay of received packets.

VLan
a switch can be *logically* segmented
into separate broadcast domains, using **Virtual LANs** (or **VLANs**).

Each VLAN represents a unique broadcast domain:
• Traffic between devices within the *same* VLAN is switched.
• Traffic between devices in *different* VLANs requires a Layer-3
device to communicate.

Route command
>Enable –(to move to privilege mode)

>in privilege mode we can ran all show command
>config terminal(after reaching this mode we actually configure the device)
>show ip route(to display routing table)
>show ip access-list(to display access list)
>show xlate(to display the pat configuration)

NAT-Network Address Translation

The rapid growth of the Internet resulted in a shortage of available IPv4 addresses. In response, a specific subset of the IPv4 address space was designated as *private,* to temporarily alleviate this problem.
A **public address** can be routed on the Internet. Thus, devices that must be Internet-accessible must be configured with (or *reachable* by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).
A **private address** is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses

NAT can also perform public-to-public
address translation, as well as private-to-private address translation.

Private address range

class:

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

CISCO FIREWALL

four main administrative access modes:

Monitor mode :password recovery – to access this mode press break/esc
Unprivileged mode -
Privileged mode
Configure mode

Running Config – Volatile and stored in the RAM- to save the current running config, we need to type 'write memory' or copy run start
Startup config - non-volatile

Security levels
0-100

0- Outside
1-99- DMZ(Demilitarized Zone)
100-Inside

Highest Security level /interface can communicatge with lower security level and not vice versa.

Traffic from Higher Security Level to Lower Security Level
Allow all unless specified by a ACL
IF NAT is enabled, ther must be a **nat and global pair**

Traffic from Lower Security Level to Higher Security Level:
Drop all unless specified by an ACL.
IF NAT is enabled, ther must be a static-NAT between a higher to lower level.

Traffic between interfaces with same Security Level:
By default, don't allow,
Unless configured with **same-scurity-traffic-permit** command.

Firewall config:

STEP1: Configure a privileged level password
STEP2: Enable Command Line Management
1.)create a username and password
2.) ! Generate a 1024 bit RSA key pair for the firewall which is required for SSH
3.) Specify the hosts allowed to connect to the security appliance.
STEP3: **Configure a Firewall Hostname**

To create a route

ciscoasa(config)# route "*interface-name*" "*destination-ip-address*" "*netmask*" "*gateway*"

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1 ← Default Route
ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1 ← Static Route

Dynamic NAT :
From the pool of Ip address in the higher security interfafce as real ip maped with the pool of ip address in the mapped addrees pol for outbound communication.

Dynamic PAT:
Many to One:

The many real IP will be mapped to a single public IP with the request on each real IP will be assigned with the Port number for the request.

Static NAT
Bidirectional communication:
One-to-one address mapping between real and mapped ip

Lower level security interface can communicate with higher level inrerface with appropriate ACL configured.

the ASA firewall implements NAT in two ways:
"***Network object NAT***"
"***Twice NAT***"

NAT 0 or Identity Nat: Used for IPsec or VPN

ACL:

The Access Control List, as the name implies, is a List of statements (called Access Control Entries) that permit or deny traffic from a source to a destination.

Access control lists (ACLs) can be used for two purposes on Cisco devices:
to **filter** traffic, and to **identify** traffic

Each rule or line in
an access-list provides a condition, either **permit** or **deny**:

when filtering traffic, access lists are applied on interfaces.

Only one access list **per interface**, **per protocol**, **per direction** is allowed.

Two Golden Rules of Access Lists:
1. If a bit is set to **0** in a wild-card mask, the corresponding bit in the address must be **matched exactly.**
2. If a bit is set to **1** in a wild-card mask, the corresponding bit in the address can **match any number.** In other words, we "don't care" what number it matches.

Syntax:

The command format of an Access Control List is the following:
ciscoasa(config)# access-list "*access_list_name*" [line *line_number*] [extended] {*deny | permit*} *protocol "source_address" "mask" [operator source_port] "dest_address" "mask" [op*

Acess group
ciscoasa(config)# access-group "*access_list_name*" [in|out] interface "*interface_name*"
access-group "*access_list_name*" global
Access group used to bind the access list with the interface

There are four types of object groups:
Network: Used to group together hosts or subnets.
Service: Used to group TCP or UDP port numbers.
Protocol: Used to group protocols.
ICMP-type: Used to group ICMP message types.

_____

IDS firewall difference

Stateful/stateless firewall
Steless: Packet filtering or static filtering
It just allow or deny the traffic based on ACL.
It filters the traffic based on the below conditions.
Source Ip/Port
Destination Ip /Port
Protocol

Adv: easy to implement
Disadv : Noway to determine if the packet is part of an already existing connection.
Applications use random port numbers and these will trouble operating because of this.
IP spoofing attacks.

Statefull firewall: Dynamic filtering
IT monitors the connection state. Avoid TCP based attacks
Not only monitors the connection but also monitors the sequence numbers
Inside can start connect with outside and not vice versa.
All this will be accomplished by a session table called STATE table.
State table is dynamic, when the connection go quiet from inside, the outside cannot initiate the connection to the insider.

STATE table.
- Source and dest IPaddres/Port numbers
- TCP and UDP flag settings
- TCP sequence info.

TCP packets outside an expected will be dropped

Disadv: application layer attacks –Proxy server

Class A B C D - sub netting

Difference between router and switch

	Router	Switch
Used for	Connecting two or more networks	Connecting
Function	Directs data in a network. Passes data between home computers, and between computers and the modem.	Allow to co
Used in (LAN, MAN, WAN)	LAN, WAN	LAN
Transmission Type	At Initial Level Broadcast then Uni-cast & Multicast	First broad
Data Transmission form	Packet	Frame (L2 S
Layer	Network Layer (Layer 3 devices)	Data Link l
Ports	2/4/2008	Switch is m
Device Type	Networking device	Active Dev
Table	Store IP address in Routing table and maintain address at its own.	Switches us integrated
Transmission Mode	Full duplex	Half/Full d
Broadcast Domain	In Router, every port has its own Broadcast domain.	Switch has

Definition	A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation.	A network network. A request it
Device Category	Intelligent Device	Intelligent
Bandwidth sharing	Bandwidth sharing is Dynamic (Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default percent-value is 0. The percent-value range is 1-96.)	There is no
Speed	1-10 Mbps (Wireless); 100 Mbps (Wired)	10/100 Mbp
Routing Decision	Take faster routing decisions	Take more
NAT (Network Address Translation)	Routers can perform NAT	Switches ca
Faster	In a different network environment (MAN/ WAN), a router is faster than an L3 switch.	In a LAN e
Features	Firewall VPN Dynamic hadling of Bandwidth	Priority rt r
Examples	Linksys WRT54GL Juniper MX & EX series Cisco 3900, 2900, 1900	Alcatel's O
Address used for data tramsmission	Uses IP address	Uses MAC

Arp table and reverseARP
Arp request is broadcast and arp reply is unicast
ARP table maintains IP address corresponding mac address
RArp request is broadcast and Rarp reply is unicast
RARP request for corresponding mac address for a given IP address.

Inline/Passive in IDS

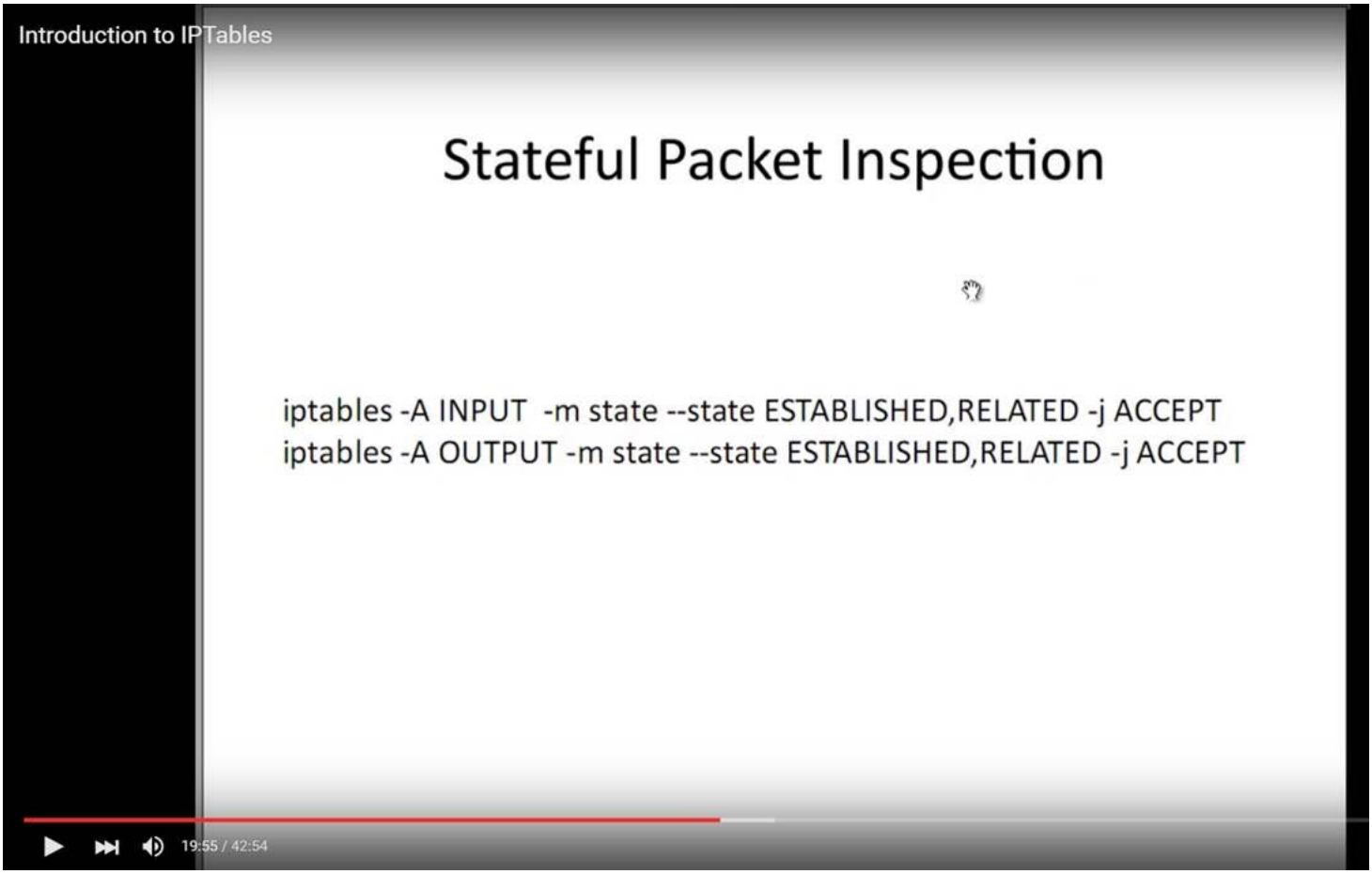
SSH vs TLS

Linux

Ip configuration in Linux
ifconfig interfacename netmask ip up/down
https://www.youtube.com/watch?v=SnACG4TDqJw

dns

iptables:
Packet filterting application in linux based os.



https://www.youtube.com/watch?v=XKfhOQWrUVw

check service status
netstat –a | grep ftp

packet capture -wireshark tcpdump

Project:

Challenges in Manet :
Energy centric,
Dynamic Topology,
Less computation power,

Attacks
Wormhole- advertise valid path and drop the packets
Greyhole- group of nodes advertises itself as a valid path and send the path to the destination after a long time. -> Batery consumption.
Blackhole- Advertises itself as a valid path and sends a fake information to the destination.

Model:
Trust proctor= Energy+direct trust+recommendation trust
Trust handler =Alarm table,friend table, trust evaluator
CA-Certificate authority

TCPdump :

_____
-h version checking
-d identify the available interface
-i interface
-c packet capture size
-s packet bytes size
-w to capture files
-r to read the captured files
-v verbose mode
-t time display
-q –quantity of content display

Capture the packets in the network and analyze the packet
Details abt the packet can either displayed on the screen or can be saved as a pcap file
Libpcap library used for packet filtering.

Version checking
Tcpdump –h

To identify the available interface like eth0 or eth1 like dat
Tcpdump –d

To capture packet using any option -l
Tcpdump –l any

Tcpdump wont stop capturing once start unles interpret by a user command - >ctrl+z

To capture specified number of packets use below -c
Tcpdump –l any –c 5
The above command will capture 5 packets

To display the ip address and port numbers in the result use below -n
Sudo tcpdump –l any –c 5 –n

Capture size of a packet can be altered by using –s
Sudo tcpdump –l any –c 5 –n –s 96 #capture 96 byte
Sudo tcpdump –l any –c 5 –n –s 0 #maximum size of 65535

To capture one direction of traffic:

Sudo tcpdump –l any –c 20 -n tcp and dst port 49952 –t

A single packet looks like the below:
IP sourceIP.port > destinationip.port flags[TCP] acq/seq , window , length

To save the capture for future analysis –w
Sudo tcpdump –l any –w capture.pcap

While capturing packet in the file , usually we cant see how many packets are captured in the CLI, to address this , we will use –v to display number of records got captured in the file
Sudo tcpdump –l any –w capture.pcap –v

To Read the capture files.
Sudo tcpdump –n –r capture.pcap

If the file is large, it will directly go the eof , to enable scrolling use | less
Sudo tcpdump –n –r capture.pcap |less (to scroll up and down)

TCPdump filters
Filters are used to isolate the traffic

To capture packet on particular host
Tcpdump –l eth1 –n host 10.0.0.1 –c 5

To see one direction traffic:
That s packet capture only from the sender src
Tcpdump –l eth1 –n src host 10.0.0.1 –c

Traffic between 2 ip ->source and destination – by using and operator

Tcpdump –l eth1 –n src host 10.0.0.1 and host 10.0.0.3 –c 5

To capture packet only on specific port
Tcpdump –l eth1 –n src host 10.0.0.1 and host 10.0.0.3 and port 80

Compound expression : to show traffic for port 80 or port 443 on the sending host

Tcpdump –l eth0 –n “host 192.168.1.1 \> and (port 80 or port 443)”

To capture ipv6 packets
Tcpdump –l etho 0 ip6

To ping ipv6 address
Ping6 IPV6

Verbose output
Tcpdump –l eth0 –v

Minimal quantity of output
Tcpdump –I eth0 –q

Timestamp
-t
-ttt
-ttttt

IOS- INTERNETWORKING OPERATING SYSTEM

---

3 attachments

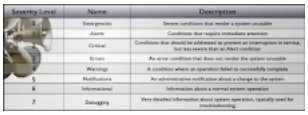


image007.png
94K

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image009.png
22K

image010.jpg
43K

---

aravindh.seeneevasan@accenture.com <aravindh.seeneevasan@accenture.com> Sat, Dec 3, 2016 at 10:36 PM
To: aravindh.sp@gmail.com

Encryption private and public key
TCp header ip header icmp flags

Crux2001@@!
promiscuous mode

TCP/IP – OSI Layer
TcP vs udp

Port and protocols

HTTPs port , port 8080

TLS vs SSL

Diff IPS and firewall

NIds vs HIDS

Tcpdump – switches

AJ

SOC Arcitecture

End device to analysis

LOGS PORT

Rsip SERVER - IIMPORTER

SiX MONTHS TO SIX MONTHS

Why Symantec

Marwan

Experience\\\\

Why this job??

Diff between an ACL – IPS/IDS

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

---

aravindh.seeneevasan@accenture.com <aravindh.seeneevasan@accenture.com> Sat, Dec 3, 2016 at 10:37 PM
To: aravindh.sp@gmail.com

OSI Layer - Deep

IDS firewall difference

Common port numbers yes
Stateful/stateless firewall
Class A B C D - sub netting

Difference between router and switch
Arp table
reverse arp

Inline/Passive in IDS

SSH vs TLS

Linux

Ip config
dns
iptables
check service status
packet capture -wireshark tcpdump

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

[Quoted text hidden]

---

aravindh.seeneevasan@accenture.com <aravindh.seeneevasan@accenture.com>
To: aravindh.seeneevasan@accenture.com, aravindh.sp@gmail.com

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery

P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Sunday, April 24, 2016 11:05 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>; aravindh.sp@gmail.com
Cc: aravindh.sp@gmail.com; Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: FW: Network

V2

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 11:58 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: RE: Network

V1

Thanks & Regards
Aravindh Seeneevasan - SE Analyst
Telstra | Products | PCR Delivery
P +91 44 434**6 2721**
M 9677986743
E aravindh.seeneevasan@accenture.com
W www.accenture.com

From: Seeneevasan, Aravindh
Sent: Wednesday, April 20, 2016 8:34 PM
To: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Cc: Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
Subject: Network

networks
connecting two or more devices to share the information and services
Protocols
is the rules that governs how devices should be communicate with each other

Network Reference Model
OSI-open system interconnection
DOD -Dept of Defense(TCP/IP)

Network types
Lan -Under a single administration or the infrastructure for connecting the resources inside a building
WAN -Two or more Lans connecting together to form a WAN or Two different adminstration
MAN - Connecting different locations or geographic area
SAN (Storage area network)- Provide high-speed , lossless connectivity to the data
VPN - (Virtual Private Network) - used to send data securely in an unsecure or public network

Term Internetwork:
Multiple networks connecting together. INTERNET is the larget internetwork.

Network Artitechture
Host -A device that is connected in the network can provide resources to the node of the network and also assigned with a valid address.

Client- Request data
Server- Send data to client
-disadv-Single point of failure(can be avoided using redundancy in the server layer)
Peer- Send and Request data
-Pose security problems since the data are spread across devices
Mainframe/termminal
-thin client protocols are
-RDP(remote desktop protocol) and ICA(Independent Computer Architecture)

WAN Connection Types

WANs are generally grouped into three separate **connection types**:

• Point-to-Point technologies

- Circuit-switched technologies
- Packet-switched technologies

\	Circuit Swithcing	Message switch	Packet switch
Approach	no store and forward	Store and forward	Store and forward
Connection	Connection	connectionless	may b connected or connectionless
Path	dedicated path	no dedicated	no dedicated
data rate	Constant	variable	Variable
following path	same path for entire transmission	diff route for diff packets	same path for VCI and independent path for Datagram approach
Bandwidth	fixed	fixed	Dynamic

Examples of Packet switched technology

Frame-Relay

- X25

OSI MODEL:1984

Interoperating b/wn products of diff manufacturers pose chalenge

Why are we going for layered approach

Proven standard

Switching:

Circuit switching

Message switching

Packet switching

A STANDARDIZED ARCHITECTURE DEFINING N/W COMMUNICATION.

A STANDARD TO CREATE STANDARD.

UpperLayer are 765

App layer :7

- provides Interface between the user ,application and the network
- eg : web browser, email client
- =the user interact with application which in turn converted into a protocol and serves the specific functionality
- Eg: FTP,http,pop3,smtp
- Varity of functions:
  - identifies communication partners
  - Determines the resource availability
  - Synchronizes communication.
- It wont interact with any other layer above but the below presentation layer

Presentation Layer:6

- Controls the formatting and syntax of the user application.
- ensures Data from the sending application understood by the receiving application.
- Eg:img,audios,videos and text
- If two devices doesnt support the same formatting ,presentation layer provides the converstion or translation functionality
- Additionally, it provides encryption and decryption

Session layer:5

- Establish,maintaining and terminating the connection
- Session communication/Transmission modes
  - Simplex
  - Half duplex
  - Full duplex

Lower Layer:4321

Transport that are happening in this layer is responsible for end-to-end communication

Transport Layer:4

End to END

-reliable transfer of data

Ensuring data receiving in the destination is error free and in order

Segmentation and sequencing

Acknowledgements

Flow control(Windowing) –Data transfer rate is negotiated to prevent congestion

Two Categories

Connection oriented -TCP

More reliable

Upon data lost , data can be resent

Connection is established after a 3 way handshake

Connection less oriented –UDP

TCP/UDP – Sliding window mechanism

Application separation via PORTS

Network Layer:3

Responsibl for Sending data to dissimilar network / send data across network

Responsible for

Logical addressing

-provides a unique address that identifies both the host, and the network that host exists on.
Routing
-determines the best path to a particular destination network, and then routes data accordingly
Protocols are :IP and IPX
IPV4,IPV6
-X.25 -1.56kbbs
Hop to hop
in computer **networking**, a **hop** is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways on the way. Each t
TTL Is used for loop avoidance.

 The main purpose of the router are
– Route selection
– Packet forwarding
– Packet filtering

Data Link Layer :2
Responsible to send data within a same network

2 sublayers
LLc(Logical Link control)
Serves as an intermediary between physical link and all higher layer protocols
responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.
Additionally Error control and flow control
MAC(Media acess control)
Control the access to physical medium
CSMA/CD
-Higher layer data into frames, this is called framing or encapsulation.
- hardware addresses contain no mechanism for differentiating one network from another, and can only identify a host within a network.
-Frame relay-1.54mbps
-ATM
-Ethernet
-FDDI

The three main functions of Switch

1. Address learning – Learns the MAC address from the frame source MAC field
2. Forward/filter decisions – Make the decision based on the learned MAC address
3. Loop avoidance – Switch redundant path make unavoidable loop. Spanning Tree protocol
is the key to avoid the Loop in redundant path.

Node to Node delivery
Node:
In communication **networks**, a **node** (Latin nodus, 'knot') is either a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment).

Physical layer :1
Controls signaling and transferring of raw bits into the physical medium
- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the network topology as bus, mesh, or ring being some of the most common.

-NIC card

Network Devices
Hubs and repeaters(Layer 1)
Switches and Bridges(Layer 2)
Routers(layer 3)

Encapsulation
: As data is passed from the user application down the virtual layers of the OSI model, each layer adds a header (and sometimes a trailer) containing protocol information specific to tha
encapsulation.

Network Topology

• Bus • Star • Ring • Full or partial mesh

Network Devices
Hubs and repeaters(Layer 1) – 1 broadcast domain and 1 collision domain
A **collision domain** is simply defined as any physical segment where a collision can occur
A **broadcast domain** is a logical segmentation of a network, dictating how far a broadcast (or multicast) frame can propagate.
Hubs provide no intelligent forwarding
hubs will always forward every frame out every port, excluding the port originating the frame.
Switches and Bridges(Layer 2) – each port has 1 collision domain and by whole has 1 broadcast domain
- High port density for switches than bridges
- A switch behaves much like a hub when first powered on. The switch will flood every frame, including unicasts, out every port but the originating port. The switch will then
- A switch is in a perpetual state of learning. However, as the MAC address table becomes populated, the flooding of frames will decrease, allowing the switch to perform mc
- ASIC(Application specific integrated circuits) for making intelligent forwarding decisions

Multilayer switch(referring to any switch that forwards traffic at layers higher than Layer-2**) &Routers(layer 3)**
Routers build routing tables to perform forwarding decisions, which contain the following:
• The destination network and subnet mask
• The next hop router to get to the destination network

• Routing metrics and Administrative Distance

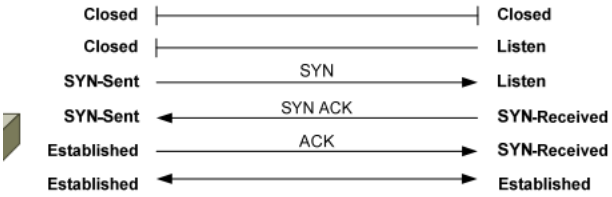
The routing table is concerned with two types of Layer-3 protocols:
• Routed protocols - assigns logical addressing to devices, and routes packets between networks. Examples include IP and IPX.
• Routing protocols - dynamically builds the information in routing tables. Examples include RIP, EIGRP, and OSPF.
Each individual interface on a router belongs to its own collision domain. Thus, like switches, routers create more collision domains, which results in fewer collisions.
As a rule, a router will never forward broadcasts from one network to another network (unless, of course, you explicitly configure it to).
Traditionally, a router was required to copy each individual packet to its buffers, and perform a route-table lookup. Each packet consumed CPU cycles as it was forwarded by the router, switching functions were typically performed in hardware, and routing functions were typically performed in software.

Consider the above diagram. Remember that:
• Routers separate broadcast and collision domains. • Switches separate collision domains. • Hubs belong to only one collision domain. • Switches and hubs both only belong to one br

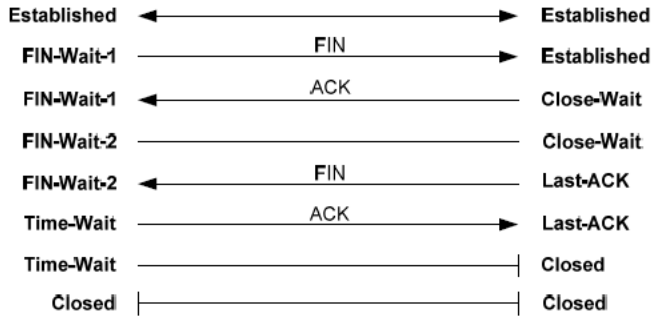
TCP and UDP
The combination of the IP address and port number (identifying both the host and service) is referred to as a socket, and is written out as follows:
192.168.60.125:443
0-1023-Well known ports
1024 – 49151- Registrered Ports
49152-65535- dynamic ports- A client initiating a connection will randomly choose a port in this range as its source port (for some operating systems, the dynamic range starts at 1024 a

TCP establish connetion
Sys A send **Syn to** SYS B
Sys b replies **Syn+ACK to** sys A
Sys A send back **ACK to** sys b to establish the connection

TCP connection Establishment states:
Closed
Listen
Syn-sent
Syn-received
Established



TCP connection Terminiation states:
Established
Fina-wait 1
Close-wait
Fin-wait 2
Last_ack
Time_wait
Closed



Connections are identified by the sockets of both the source and destination host, and data specific to each connection is maintained in a Transmission Control Block (TCB)

TCP employs a sliding window mechanism.
Bytes in a sliding window fall into one of four categories:
• Bytes that have already been sent and acknowledged.
• Bytes that have been sent, but not acknowledged.
• Bytes that have not yet been sent, but the receiving host is ready for.
• Bytes that have not yet been sent, and the receiving host is not ready for.

TCP header flags
PSH –push and URG –Urgent flag
Eventhough the TCP window cant handle the data both of the above flags used to prioritize the data
RST – Reset Flag
TCP utilizes the Reset message, using the RST flag, to address half-open connections.
• URG (Urgent) – prioritizes specified traffic.

- ACK (Acknowledgment) – acknowledges a SYN or receipt of data.
- PSH (Push) – forces an immediate send even if window is not full.
- RST (Reset) – forcefully terminates an improper connection.
- SYN (Synchronize) – initiates a connection.
- FIN (Finish) – gracefully terminates a connection when there is further data to send.

Congestion

Network congestion in data **networking** and queueing theory is the reduced quality of service that occurs when a **network** node is carrying more data than it can hand

UDP

UDP, above all, is simple. It provides no three-way handshake, no flow control, no sequencing, and no acknowledgment of data receipt. UDP essentially forwards the segment and takes
-connectionless
Less latency compared to TCP

latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the **latency**.

The following provides a quick comparison of TCP and UDP:

TCP	*UDP*
Connection-oriented	Connectionless
Guarantees delivery	Does *not* guarantee delivery
Sends acknowledgments	Does *not* send acknowledgments
Reliable, but slower than UDP	Unreliable, but faster than TCP
Segments and sequences data	Does *not* provide sequencing
Resends dropped segments	Does *not* resend dropped segments
Provides flow control	Does *not* provide flow control
Performs CRC on data	Also performs CRC on data
Uses port numbers	Also uses port numbers

Router Components

Router Memory, Quick Reference

The following table details each of the basic types of **router memory**:

Memory	*Writable?*	*Volatile?*	*Function*
ROM	No	No	*Stores bootstrap*
Flash	Yes	No	*Stores IOS*
NVRAM	Yes	No	*Stores startup-config*
RAM	Yes	Yes	*Stores running-config*

DNS: Domain Name system :port 53
Conversion / Translation of IP address to human readable names and vice versa

How dns works
When request on google.com

It search in the local host cache
If the local host cache doesn't have a entry, it will be forwarded to local host file.
If the local host file doesn't have a entry., it will be forwarded to dns root server
Dns root server then will follow the hierarchy of domain resolution and reply back to the request.

DNS uses TCP for Zone Transfer over Port: 53
It is necessary to maintain a consistent DNS database between DNS Servers.
The connection is established between the DNS Server to transfer the zone data and Source and Destination DNS Servers

DNS uses UDP for DNS Queries over Port: 53
A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it must re-transmit the DNS Query using the TCP after 3-5 s

Dns

Resolving the human readable name into IP and vice versa.

There are two common methods for implementing name resolution:
• A **static file** on each host on the network, containing all the name-toaddress translations (examples include the HOSTS/LMHOSTS files).

• A **centralized server** that all hosts on the network connect to for name resolution.

Dynamic DNS allows DNS to be integrated with Dynamic Host Configuration Protocol (DHCP). When DHCP hands out an IP address lease, it will automatically update the DNS entry for that host on the DNS server.

DHCP(Dynamic host control protocol) :port 67 Server and Port 68 for client and for Port 69 is for TFTp

DORA Process

DHCP servers **lease** out IP addresses to DHCP clients, for a specific period of time. There are four steps to this DHCP process:
• When a DHCP client first boots up, it broadcasts a **DHCPDiscover** message, searching for a DHCP server.
• If a DHCP server exists on the local segment, it will respond with a **DHCPOffer,** containing the "offered" IP address, subnet mask, etc.
• Once the client receives the offer, it will respond with a **DHCPRequest**, indicating that it will accept the offered protocol information.
• Finally, the server responds with a **DHCPACK**, acknowledging the clients acceptance of offered protocol information.

By default, DHCP leases an address for **8 days**. Once 50% of the lease expires, the client will try to renew the lease with the *same* DHCP server.

SNMP Port 161(TCP) and port 162(SNMP trap for both tcp and udp)

161-polling
162-traps

Used to retrival of metrics-
Eg: whats my cpu usage, how much is my ram occupied,

Polling(requesting for the information) - Once in a while server request router for the information of devics to a router and router send backs the information
Polling happens using OID(object ids)
MIB-Management information base , basically a DNS for OIDs

Trap – on a unfortunate event in the router it is having an option of sending a trap.
Router saying server hey something happened in me. Kindly check – its based on the security level

Syntax: snmp-server community cisco ro(read only)or rw(read/wirte)
Snmp enable traps

Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol for collecting and organizing information about managed devices on IPnetworks and for modif servers, workstations, printers, modem racks and more.[1]

Syslog:
Useful for Event management
Controls on an unfortunate event occurs based on the log level it will capture the logs and can b further used for troubleshooting purpose.

Ports 514-used for system logging(UDP)
Port 601-reliable syslog service(TCP)
Port 6514 – reliable syslog over TLS(TCP)
Port 10514- TLS enabled syslog (TCP/UDP)

Severity Level	Name	Description
0	Emergencies	Severe conditions that render a system unusable
1	Alerts	Conditions that require immediate attention
2	Critical	Conditions that should be addressed to prevent an interruption in service, but less severe than an Alert condition
3	Errors	An error condition that does not render the system unusable
4	Warnings	A condition where an operation failed to successfully complete
5	Notifications	An administrative notification about a change to the system
6	Informational	Information about a normal system operation
7	Debugging	Very detailed information about system operation, typically used for troubleshooting

Configuring syslogs
>Config terminal
>logging 192.168.1.2(server address where the syslog gets captured)
>logging trap 5(log level) or >logging trap notificational(in words)

SMTP:
PoRT 25 FOR BOTH TCP AND UDP

Arcsight:
https://youtu.be/_Fvx_nI6E4c

IP addressing
Class A : 1.0.0.0 to 127.255.255.255
Class b :128 to 191
Class c: 192 to 223 -
Class d: 224 to 239 – Multicast purpose or group address
Class e: 240 to 255 –Experimental use

Binary to decimal -2^0 to 2^7
Decimal to binary –
Divide the number by 2 and have the reminders has binary number, - L divide method

Network address is the first address in the block – it defines itself to the rest of the internet
Last address of the block is called broadcast address of that block
NetIds=All 1's
Host Id's =All 0's

Default mask:
All net id will be 0 and all host id will be 1
Default mask will be given based on the class

Masking concept:
Identify the first address of the block or network address
An address in the block with AND operation gives the first address of the block

Eg
23.56.7.91
255.0.0.0
_____
23.0.0.0(first address/network address)

Limited broadcast address
255.255.255.255
Router blocks the limited broadcast packet

Subnetting
Well utilization of address space

Subnet mask:
All net ids and subnet ids will be 1 and host id will be 0

Security information and event management

In the field of computer security, **security information and event management** (**SIEM**) software products and services combine security information management (SIM) and se
hardware and applications.

Hp Arcsight
IBM Qradar

Jitter is defined as a variation in the delay of received packets.

VLan

a switch can be *logically* segmented
into separate broadcast domains, using **Virtual LANs** (or **VLANs**).

Each VLAN represents a unique broadcast domain:
• Traffic between devices within the *same* VLAN is switched.
• Traffic between devices in *different* VLANs requires a Layer-3
device to communicate.

Route command
>Enable –(to move to privilege mode)
>in privilege mode we can ran all show command
>config terminal(after reaching this mode we actually configure the device)
>show ip route(to display routing table)
>show ip access-list(to display access list)
>show xlate(to display the pat configuration)

NAT-Network Address Translation

The rapid growth of the Internet resulted in a shortage of available IPv4 addresses. In response, a specific subset of the IPv4 address space was designated as *private,* to temporarily alleviate this problem.
A **public address** can be routed on the Internet. Thus, devices that must be Internet-accessible must be configured with (or *reachable* by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).
A **private address** is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses

NAT can also perform public-to-public
address translation, as well as private-to-private address translation.

Private address range

class:

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

CISCO FIREWALL

four main administrative access modes:

Monitor mode :password recovery – to access this mode press break/esc
Unprivileged mode -
Privileged mode
Configure mode

Running Config – Volatile and stored in the RAM- to save the current running config, we need to type 'write memory' or copy run start
Startup config - non-volatile

Security levels
0-100

0- Outside
1-99- DMZ(Demilitarized Zone)
100-Inside

Highest Security level /interface can communicatge with lower security level and not vice versa.

Traffic from Higher Security Level to Lower Security Level
Allow all unless specified by a ACL
IF NAT is enabled, ther must be a **nat and global pair**

Traffic from Lower Security Level to Higher Security Level:
Drop all unless specified by an ACL.
IF NAT is enabled, ther must be a static-NAT between a higher to lower level.

Traffic between interfaces with same Security Level:
By default, don't allow,
Unless configured with **same-scurity-traffic-permit** command.

Firewall config:

STEP1: Configure a privileged level password
STEP2: Enable Command Line Management
1.)create a username and password
2.) ! Generate a 1024 bit RSA key pair for the firewall which is required for SSH
3.) Specify the hosts allowed to connect to the security appliance.
STEP3: **Configure a Firewall Hostname**

To create a route

ciscoasa(config)# route "*interface-name*" "*destination-ip-address*" "*netmask*" "*gateway"*

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1 ← Default Route
ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1 ← Static Route

Dynamic NAT :
From the pool of Ip address in the higher security interfafce as real ip maped with the pool of ip address in the mapped addrees pol for outbound communication.

Dynamic PAT:
Many to One:

The many real IP will be mapped to a single public IP with the request on each real IP will be assigned with the Port number for the request.

Static NAT
Bidirectional communication:
One-to-one address mapping between real and mapped ip

Lower level security interface can communicate with higher level inrerface with appropriate ACL configured.

the ASA firewall implements NAT in two ways:
"***Network object NAT***"
"***Twice NAT***"

NAT 0 or Identity Nat: Used for IPsec or VPN

ACL:

The Access Control List, as the name implies, is a List of statements (called Access Control Entries) that permit or deny traffic from a source to a destination.

Access control lists (ACLs) can be used for two purposes on Cisco devices:
to **filter** traffic, and to **identify** traffic

Each rule or line in
an access-list provides a condition, either **permit** or **deny**:

when filtering traffic, access lists are applied on interfaces.

Only one access list **per interface**, **per protocol**, **per direction** is allowed.

Two Golden Rules of Access Lists:
1. If a bit is set to **0** in a wild-card mask, the corresponding bit in the address must be **matched exactly.**
2. If a bit is set to **1** in a wild-card mask, the corresponding bit in the address can **match any number.** In other words, we "don't care" what number it matches.

Syntax:

The command format of an Access Control List is the following:
**ciscoasa(config)# access-list "*access_list_name*" [line *line_number*] [extended] {*deny | permit*} *protocol "source_address" "mask" [operator source_port] "dest_address" "mask" [op*

Acess group
ciscoasa(config)# access-group "*access_list_name*" [in|out] interface "*interface_name*"
access-group "*access_list_name*" global
Access group used to bind the access list with the interface

There are four types of object groups:
Network: Used to group together hosts or subnets.
Service: Used to group TCP or UDP port numbers.
Protocol: Used to group protocols.
ICMP-type: Used to group ICMP message types.

_____

IDS firewall difference

Stateful/stateless firewall
Steless: Packet filtering or static filtering
It just allow or deny the traffic based on ACL.
It filters the traffic based on the below conditions.
Source Ip/Port
Destination Ip /Port
Protocol

Adv: easy to implement
Disadv : Noway to determine if the packet is part of an already existing connection.
Applications use random port numbers and these will trouble operating because of this.
IP spoofing attacks.

Statefull firewall: Dynamic filtering
IT monitors the connection state. Avoid TCP based attacks
Not only monitors the connection but also monitors the sequence numbers
Inside can start connect with outside and not vice versa.
All this will be accomplished by a session table called STATE table.
State table is dynamic, when the connection go quiet from inside, the outside cannot initiate the connection to the insider.

STATE table.
- Source and dest IPaddres/Port numbers
- TCP and UDP flag settings
- TCP sequence info.

TCP packets outside an expected will be dropped

Disadv: application layer attacks –Proxy server

Class A B C D - sub netting

Difference between router and switch

	Router	Switch
Used for	Connecting two or more networks	Connecting
Function	Directs data in a network. Passes data between home computers, and between computers and the modem.	Allow to cc
Used in (LAN, MAN, WAN)	LAN, WAN	LAN

Transmission Type	At Initial Level Broadcast then Uni-cast & Multicast	First broad
Data Transmission form	Packet	Frame (L2
Layer	Network Layer (Layer 3 devices)	Data Link
Ports	2/4/2008	Switch is m
Device Type	Networking device	Active Dev
Table	Store IP address in Routing table and maintain address at its own.	Switches u integrated
Transmission Mode	Full duplex	Half/Full d
Broadcast Domain	In Router, every port has its own Broadcast domain.	Switch has
Definition	A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation.	A network network. A request it
Device Category	Intelligent Device	Intelligent
Bandwidth sharing	Bandwidth sharing is Dynamic (Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default percent-value is 0. The percent-value range is 1-96.)	There is no
Speed	1-10 Mbps (Wireless); 100 Mbps (Wired)	10/100 Mbp
Routing Decision	Take faster routing decisions	Take more
NAT (Network Address Translation)	Routers can perform NAT	Switches ca
Faster	In a different network environment (MAN/ WAN), a router is faster than an L3 switch.	In a LAN e
Features	Firewall VPN Dynamic hadling of Bandwidth	Priority rt
Examples	Linksys WRT54GL Juniper MX & EX series Cisco 3900, 2900, 1900	Alcatel's O
Address used for data tramsmission	Uses IP address	Uses MAC

Arp table and reverseARP
Arp request is broadcast and arp reply is unicast
ARP table maintains IP address corresponding mac address
RArp request is broadcast and Rarp reply is unicast
RARP request for corresponding mac address for a given IP address.

Inline/Passive in IDS

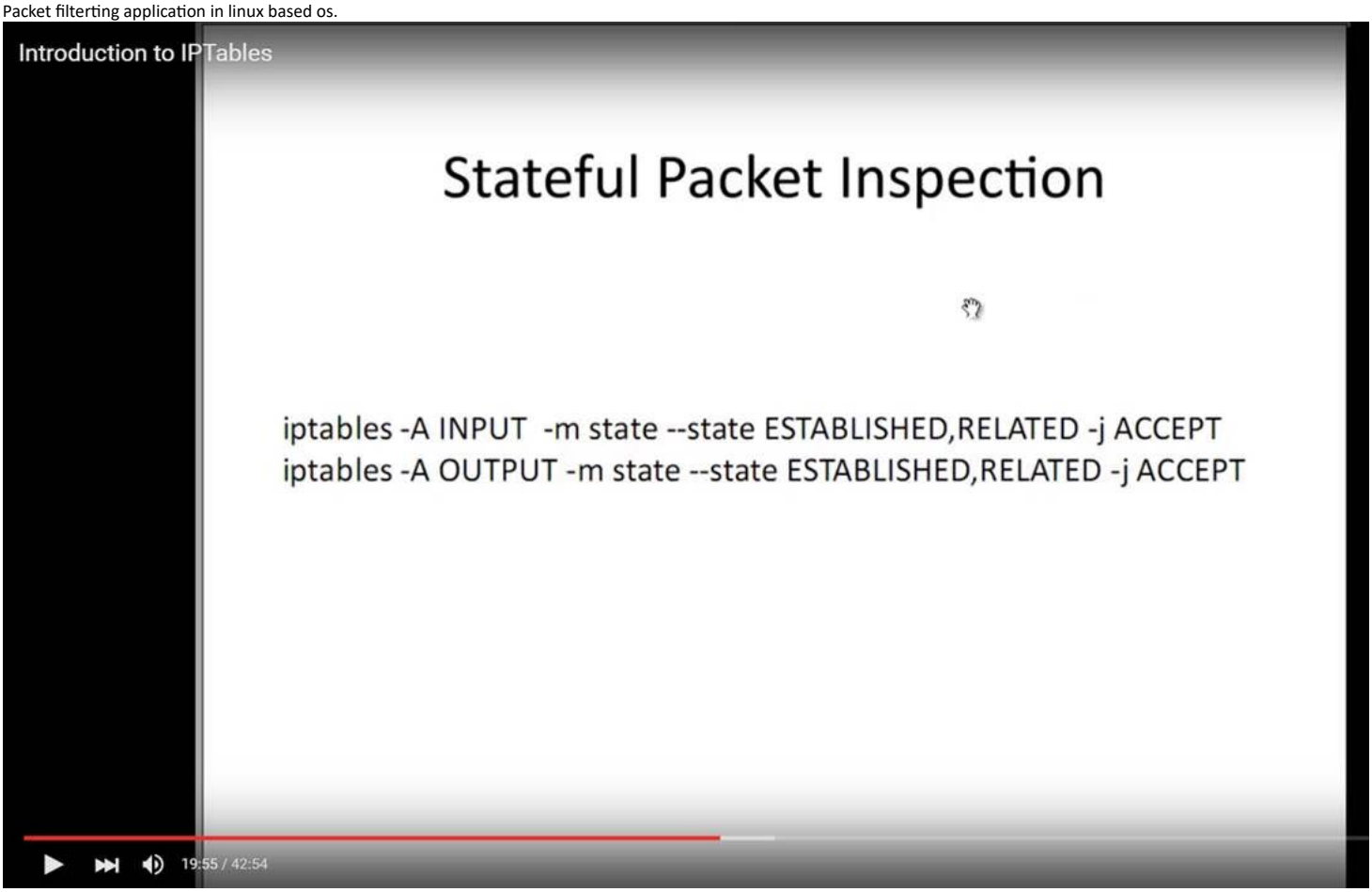
SSH vs TLS

Linux

Ip configuration in Linux
ifconfig interfacename netmask ip up/down
https://www.youtube.com/watch?v=SnACG4TDqJw

dns

iptables:
Packet filterting application in linux based os.



https://www.youtube.com/watch?v=XKfhOQWrUVw

check service status
netstat –a | grep ftp

packet capture -wireshark tcpdump

Project:

Challenges in Manet :
Energy centric,
Dynamic Topology,
Less computation power,

Attacks
Wormhole- advertise valid path and drop the packets
Greyhole- group of nodes advertises itself as a valid path and send the path to the destination after a long time. -> Batery consumption.
Blackhole- Advertises itself as a valid path and sends a fake information to the destination.

Model:
Trust proctor= Energy+direct trust+recommendation trust
Trust handler =Alarm table,friend table, trust evaluator
CA-Certificate authority

TCPdump :

_____
-h version checking
-d identify the available interface
-i interface
-c packet capture size

-s packet bytes size
-w to capture files
-r to read the captured files
-v verbose mode
-t time display
-q –quantity of content display

Capture the packets in the network and analyze the packet
Details abt the packet can either displayed on the screen or can be saved as a pcap file
Libpcap library used for packet filtering.

Version checking
Tcpdump –h

To identify the available interface like eth0 or eth1 like dat
Tcpdump –d

To capture packet using any option -l
Tcpdump –I any

Tcpdump wont stop capturing once start unles interpret by a user command - >ctrl+z

To capture specified number of packets use below -c
Tcpdump –I any –c 5
The above command will capture 5 packets

To display the ip address and port numbers in the result use below -n
Sudo tcpdump –I any –c 5 –n

Capture size of a packet can be altered by using –s
Sudo tcpdump –I any –c 5 –n –s 96 #capture 96 byte
Sudo tcpdump –I any –c 5 –n –s 0 #maximum size of 65535

To capture one direction of traffic:

Sudo tcpdump –I any –c 20 -n tcp and dst port 49952 –t

A single packet looks like the below:
IP sourceIP.port > destinationip.port flags[TCP] acq/seq , window , length

To save the capture for future analysis –w
Sudo tcpdump –I any –w capture.pcap

While capturing packet in the file , usually we cant see how many packets are captured in the CLI, to address this , we will use –v to display number of records got captured in the file
Sudo tcpdump –I any –w capture.pcap –v

To Read the capture files.
Sudo tcpdump –n –r capture.pcap

If the file is large, it will directly go the eof , to enable scrolling use | less
Sudo tcpdump –n –r capture.pcap |less (to scroll up and down)

TCPdump filters
Filters are used to isolate the traffic

To capture packet on particular host
Tcpdump –I eth1 –n host 10.0.0.1 –c 5

To see one direction traffic:
That s packet capture only from the sender src
Tcpdump –I eth1 –n src host 10.0.0.1 –c

Traffic between 2 ip ->source and destination – by using and operator

Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 –c 5

To capture packet only on specific port
Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 and port 80

Compound expression : to show traffic for port 80 or port 443 on the sending host

Tcpdump –I eth0 –n “host 192.168.1.1 \> and (port 80 or port 443)”

To capture ipv6 packets

Tcpdump –I etho 0 ip6

To ping ipv6 address
Ping6 IPV6

Verbose output
Tcpdump –I eth0 –v

Minimal quantity of output
Tcpdump –I eth0 –q

Timestamp
-t
-ttt
-ttttt

Hash
Is a number generated by a string of text.

Learn about RPM

IOS- INTERNETWORKING OPERATING SYSTEM

---

6 attachments

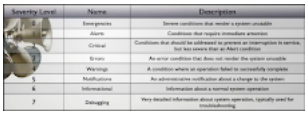


image001.png
94K

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image004.png
22K

image008.jpg
43K

common_ports.pdf
20K

Cisco-ASA-Firewall-Fundamentals-2nd-Edition.pdf
2559K

printer.pdf
2751K

Aravindh Seeneevasan <aravindh.sp@gmail.com> Fri, Sep 21, 2018 at 5:34 PM
To: sreemurali_g@symantec.com

[Quoted text hidden]
[Quoted text hidden]

organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses

NAT can also perform public-to-public

address translation, as well as private-to-private address translation.

Private address range

class:

cid:image004.png@01D19DB9.EBFBE6C0

<span style="font-size:14.0pt;font-family:Times-Roma

---

16 attachments

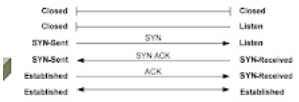


image002.png
15K

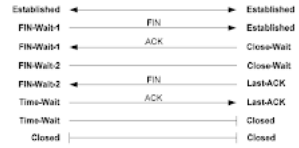


image005.png
18K

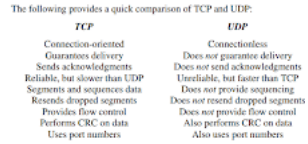


image006.png
49K

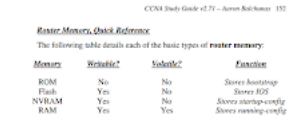


image007.png
43K

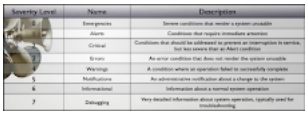


image001.png
94K

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image004.png
22K

image008.jpg
43K

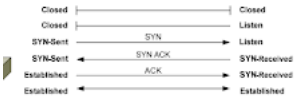


image002.png
15K

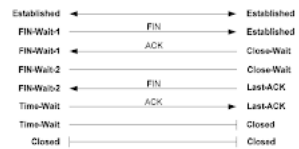


image005.png
18K

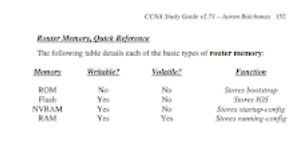
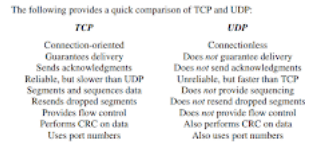


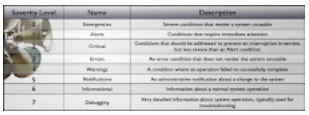
image007.png
43K

image006.png
49K



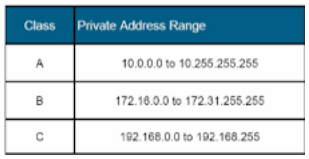
The following provides a quick comparison of TCP and UDP:

TCP	*UDP*
Connection-oriented	Connectionless
Guarantees delivery	Does *not* guarantee delivery
Sends acknowledgments	Does *not* send acknowledgments
Reliable, but slower than UDP	Unreliable, but faster than TCP
Segments and sequences data	Does *not* provide sequencing
Resends dropped segments	Does *not* resend dropped segments
Provides flow control	Does *not* provide flow control
Performs CRC on data	Also performs CRC on data
Uses port numbers	Also uses port numbers



Severity Level	Name	Description
	Emergencies	Severe conditions that render a system unusable
	Alerts	Conditions that require immediate attention
	Critical	Conditions that should be addressed to prevent an interruption in service, but less severe than an Alert condition
	Errors	An error condition that does not render the system unusable
	Warnings	A condition where an operation failed to successfully complete
5	Notifications	An administrative notification about a change to the system
6	Informational	Information about a normal system operation
7	Debugging	Very detailed information about system operation, typically used for troubleshooting

image001.png
94K



Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image004.png
22K

common_ports.pdf
20K

Cisco-ASA-Firewall-Fundamentals-2nd-Edition.pdf
2559K

printer.pdf
2751K

Aravindh Seeneevasan <aravindh.sp@gmail.com>
Draft To: aravindh.seeneevasan@accenture.com

https://www.cs.nmt.edu/~risk/TCP-UDP%20Pocket%20Guide.pdf

On Sun, Apr 24, 2016 at 11:06 PM <aravindh.seeneevasan@accenture.com> wrote:

> V2
>
> Thanks & Regards
>
> **Aravindh Seeneevasan** - SE Analyst
> Telstra | Products | PCR Delivery
>
> **P** +91 44 434**6 2721**
> **M** 9677986743
> **E** aravindh.seeneevasan@accenture.com
> **W** www.accenture.com
>
> ---
>
> **From:** Seeneevasan, Aravindh
> **Sent:** Wednesday, April 20, 2016 11:58 PM
> **To:** Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
> **Subject:** RE: Network
>
> V1
>
> Thanks & Regards
>
> **Aravindh Seeneevasan** - SE Analyst
> Telstra | Products | PCR Delivery
>
> **P** +91 44 434**6 2721**
> **M** 9677986743
> **E** aravindh.seeneevasan@accenture.com
> **W** www.accenture.com
>
> ---
>
> **From:** Seeneevasan, Aravindh
> **Sent:** Wednesday, April 20, 2016 8:34 PM
> **To:** Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
> **Cc:** Seeneevasan, Aravindh <aravindh.seeneevasan@accenture.com>
> **Subject:** Network
>
> **networks**

connecting two or more devices to share the information and services

Protocols

is the rules that governs how devices should be communicate with each other

Network Reference Model

OSI-open system interconnection

DOD -Dept of Defense(TCP/IP)

Network types

Lan -Under a single administration or the infrastructure for connecting the resources inside a building

WAN -Two or more Lans connecting together to form a WAN or Two different adminstration

MAN - Connecting different locations or geographic area

SAN (Storage area network)- Provide high-speed , lossless connectivity to the data

VPN - (Virtual Private Network) - used to send data securely in an unsecure or public network

Term Internetwork:

Multiple networks connecting together. INTERNET is the larget internetwork.

Network Artitechture

Host -A device that is connected in the network can provide resources to the node of the network and also assigned with a valid address.

Client- Request data

Server- Send data to client

-disadv-Single point of failure(can be avoided using redundancy in the server layer)

Peer- Send and Request data

-Pose security problems since the data are spread across devices

Mainframe/termminal

-thin client protocols are

-RDP(remote desktop protocol) and ICA(Independent Computer Architecture)

WAN Connection Types

WANs are generally grouped into three separate **connection types**:

• Point-to-Point technologies

• Circuit-switched technologies

• Packet-switched technologies

\	Circuit Swithcing	Message switch	Packet switch
Approach	no store and forward	Store and forward	Store and forward
Connection	Connection	connectionless	may b connected or connectionless
Path	dedicated path	no dedicated	no dedicated
data rate	Constant	variable	Variable
following path	same path for entire transmission	diff route for diff packets	same path for VCI and independent path for Datagram approach
Bandwidth	fixed	fixed	Dynamic

Examples of Packet switched technology

Frame-Relay

• X25

OSI MODEL:1984

Interoperating b/wn products of diff manufacturers pose chalenge

Why are we going for layered approach

Proven standard

Switching:

Circuit switching

Message switching

Packet switching

UpperLayer are 765

App layer :7

- provides Interface between the user ,application and the network
- eg : web browser, email client
- =the user interact with application which in turn converted into a protocol and serves the specific functionality
- Eg: FTP,http,pop3,smtp
- Varity of functions:\
  - identifies communication partners
  - Determines the resource availability
  - Synchronizes communication.
- It wont interact with any other layer above but the below presentation layer

Presentation Layer:6

- Controls the formatting and syntax of the user application.
- ensures Data from the sending application understood by the receiving application.
- Eg:img,audios,videos and text
- If two devices doesnt support the same formatting ,presentation layer provides the converstion or translation functionality
- Additionally, it provides encryption and decryption

Session layer:5

- Establish,maintaining and terminating the connection
- Session communication/Transmission modes
  - Simplex
  - Half duplex
  - Full duplex

Lower Layer:4321

Transport that are happening in this layer is responsible for end-to-end communication

Transport Layer:4

End to END

-reliable transfer of data

Ensuring data receiving in the destination is error free and in order

Segmentation and sequencing

Acknowledgements

Flow control(Windowing) –Data transfer rate is negotiated to prevent congestion

Two Categories

Connection oriented -TCP

More reliable

Upon data lost , data can be resent

Connection is established after a 3 way handshake

Connection less oriented –UDP

TCP/UDP – Sliding window mechanism

Network Layer:3

Responsibl for Sending data to dissimilar network / send data across network

Responsible for

Logical addressing

-provides a unique address that identifies both the host, and the network that host exists on.

Routing

-determines the best path to a particular destination network, and then routes data accordingly

Protocols are :IP and IPX

IPV4,IPV6

-X.25 -1.56kbbs

Hop to hop

in computer **networking**, a **hop** is one portion of the path between source and destination. Data packets pass through bridges, routers and gateways on the way. Each time packets are pa

TTL Is used for loop avoidance.

 The main purpose of the router are

– Route selection

– Packet forwarding

– Packet filtering

Data Link Layer :2

Responsible to send data within a same network

2 sublayers

LLc(Logical Link control)

Serves as an intermediary between physical link and all higher layer protocols

responsible for identifying Network layer protocols and then encapsulating them and controls error checking and frame synchronization.

Additionally Error control and flow control

MAC(Media acess control)

Control the access to physical medium

CSMA/CD

-Higher layer data into frames, this is called framing or encapsulation.

- hardware addresses contain no mechanism for differentiating one network from another, and can only identify a host within a network.

-Frame relay-1.54mbps

-ATM

-Ethernet

-FDDI

The three main functions of Switch

1. Address learning – Learns the MAC address from the frame source MAC field

2. Forward/filter decisions – Make the decision based on the learned MAC address

3. Loop avoidance – Switch redundant path make unavoidable loop. Spanning Tree protocol

is the key to avoid the Loop in redundant path.

Node to Node delivery

Node:

In communication **networks**, a **node** (Latin nodus, 'knot') is either a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment). The definition of a

Physical layer :1

Controls signaling and transferring of raw bits into the physical medium

- It defines transmission mode i.e. simplex, half duplex, full duplex.
- It defines the network topology as bus, mesh, or ring being some of the most common.

-NIC card

Network Devices

Hubs and repeaters(Layer 1)

Switches and Bridges(Layer 2)

Routers(layer 3)

Encapsulation

: As data is passed from the user application down the virtual layers of the OSI model, each layer adds a header (and sometimes a trailer) containing protocol information specific to that lay encapsulation.

Network Topology

• Bus • Star • Ring • Full or partial mesh

Network Devices

Hubs and repeaters(Layer 1) – 1 broadcast domain and 1 collision domain

A **collision domain** is simply defined as any physical segment where a collision can occur

A **broadcast domain** is a logical segmentation of a network, dictating how far a broadcast (or multicast) frame can propagate.

Hubs provide no intelligent forwarding

hubs will always forward every frame out every port, excluding the port originating the frame.

Switches and Bridges(Layer 2) – each port has 1 collision domain and by whole has 1 broadcast domain

- High port density for switches than bridges
- A switch behaves much like a hub when first powered on. The switch will flood every frame, including unicasts, out every port but the originating port. The switch will then build the MA
- A switch is in a perpetual state of learning. However, as the MAC address table becomes populated, the flooding of frames will decrease, allowing the switch to perform more efficient f
- ASIC(Application specific integrated circuits) for making intelligent forwarding decisions

Multilayer switch(referring to any switch that forwards traffic at layers higher than Layer-2**) &Routers(layer 3)**

Routers build routing tables to perform forwarding decisions, which contain the following:

• The destination network and subnet mask

• The next hop router to get to the destination network

• Routing metrics and Administrative Distance

The routing table is concerned with two types of Layer-3 protocols:

• Routed protocols - assigns logical addressing to devices, and routes packets between networks. Examples include IP and IPX.

• Routing protocols - dynamically builds the information in routing tables. Examples include RIP, EIGRP, and OSPF.

Each individual interface on a router belongs to its own collision domain. Thus, like switches, routers create more collision domains, which results in fewer collisions.

As a rule, a router will never forward broadcasts from one network to another network (unless, of course, you explicitly configure it to).

Traditionally, a router was required to copy each individual packet to its buffers, and perform a route-table lookup. Each packet consumed CPU cycles as it was forwarded by the router, res

switching functions were typically performed in hardware, and routing functions were typically performed in software.

Consider the above diagram. Remember that:

• Routers separate broadcast and collision domains. • Switches separate collision domains. • Hubs belong to only one collision domain. • Switches and hubs both only belong to one broadc

TCP and UDP

The combination of the IP address and port number (identifying both the host and service) is referred to as a socket, and is written out as follows:

192.168.60.125:443

0-1023-Well known ports

1024 – 49151- Registrered Ports

49152-65535- dynamic ports- A client initiating a connection will randomly choose a port in this range as its source port (for some operating systems, the dynamic range starts at 1024 and l

TCP establish connetion

Sys A send **Syn to** SYS B

Sys b replies **Syn+ACK to** sys A

Sys A send back **ACK to** sys b to establish the connection

TCP connection Establishment states:

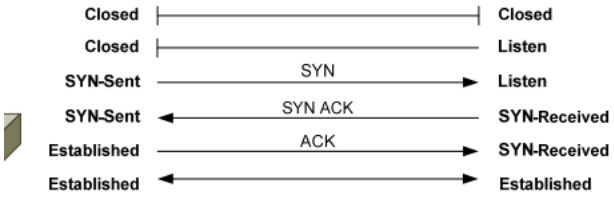
Closed

Listen

Syn-sent

Syn-received

Established



TCP connection Terminiation states:

Established

Fina-wait 1

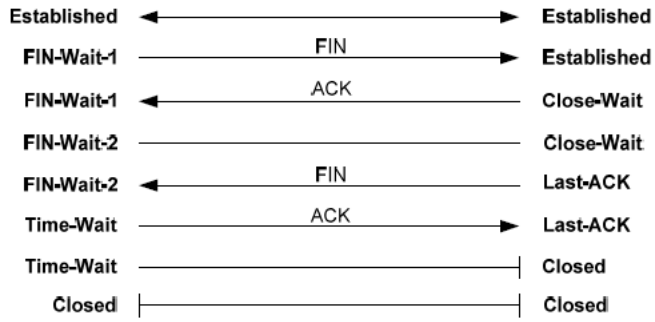
Close-wait

Fin-wait 2

Last_ack

Time_wait

Closed



Connections are identified by the sockets of both the source and destination host, and data specific to each connection is maintained in a Transmission Control Block (TCB)

TCP employs a sliding window mechanism.

Bytes in a sliding window fall into one of four categories:

• Bytes that have already been sent and acknowledged.

• Bytes that have been sent, but not acknowledged.

• Bytes that have not yet been sent, but the receiving host is ready for.

• Bytes that have not yet been sent, and the receiving host is not ready for.

TCP header flags

PSH –push and URG –Urgent flag

Eventhough the TCP window cant handle the data both of the above flags used to prioritize the data

RST – Reset Flag

TCP utilizes the Reset message, using the RST flag, to address half-open connections.

• URG (Urgent) – prioritizes specified traffic.

• ACK (Acknowledgment) – acknowledges a SYN or receipt of data.

• PSH (Push) – forces an immediate send even if window is not full.

• RST (Reset) – forcefully terminates an improper connection.

• SYN (Synchronize) – initiates a connection.

• FIN (Finish) – gracefully terminates a connection when there is further data to send.

Congestion

Network congestion in data **networking** and queueing theory is the reduced quality of service that occurs when a **network** node is carrying more data than it can handle. Typical effects ir

UDP

UDP, above all, is simple. It provides no three-way handshake, no flow control, no sequencing, and no acknowledgment of data receipt. UDP essentially forwards the segment and takes no

-connectionless

Less latency compared to TCP

latency is measured by sending a packet that is returned to the sender; the round-trip time is considered the **latency**.

The following provides a quick comparison of TCP and UDP:

TCP	*UDP*
Connection-oriented	Connectionless
Guarantees delivery	Does *not* guarantee delivery
Sends acknowledgments	Does *not* send acknowledgments
Reliable, but slower than UDP	Unreliable, but faster than TCP
Segments and sequences data	Does *not* provide sequencing
Resends dropped segments	Does *not* resend dropped segments
Provides flow control	Does *not* provide flow control
Performs CRC on data	Also performs CRC on data
Uses port numbers	Also uses port numbers

Router Components

Router Memory, Quick Reference

The following table details each of the basic types of **router memory**:

Memory	*Writable?*	*Volatile?*	*Function*
ROM	No	No	*Stores bootstrap*
Flash	Yes	No	*Stores IOS*
NVRAM	Yes	No	*Stores startup-config*
RAM	Yes	Yes	*Stores running-config*

DNS: Domain Name system :port 53

Conversion / Translation of IP address to human readable names and vice versa

How dns works

When request on google.com

It search in the local host cache

If the local host cache doesn't have a entry, it will be forwarded to local host file.

If the local host file doesn't have a entry., it will be forwarded to dns root server

Dns root server then will follow the hierarchy of domain resolution and reply back to the request.

DNS uses TCP for Zone Transfer over Port: 53

It is necessary to maintain a consistent DNS database between DNS Servers.

The connection is established between the DNS Server to transfer the zone data and Source and Destination DNS Servers

DNS uses UDP for DNS Queries over Port: 53

A client computer will always send a DNS Query using UDP Protocol over Port 53. If a client computer does not get response from a DNS Server, it must re-transmit the DNS Query using the TCP after 3-

Dns

Resolving the human readable name into IP and vice versa.

There are two common methods for implementing name resolution:

• A **static file** on each host on the network, containing all the name-toaddress translations (examples include the HOSTS/LMHOSTS files).

• A **centralized server** that all hosts on the network connect to for name resolution.

Dynamic DNS allows DNS to be integrated with Dynamic Host Configuration Protocol (DHCP). When DHCP hands out an IP address lease, it will automatically update the DNS entry for that host on the DNS server.

DHCP(Dynamic host control protocol) :port 67 Server and Port 68 for client and for Port 69 is for TFTp

DORA Process

DHCP servers **lease** out IP addresses to DHCP clients, for a specific period of time. There are four steps to this DHCP process:

• When a DHCP client first boots up, it broadcasts a **DHCPDiscover** message, searching for a DHCP server.

• If a DHCP server exists on the local segment, it will respond with a **DHCPOffer,** containing the "offered" IP address, subnet mask, etc.

• Once the client receives the offer, it will respond with a

DHCPRequest, indicating that it will accept the offered protocol information.

• Finally, the server responds with a **DHCPACK**, acknowledging the clients acceptance of offered protocol information.

By default, DHCP leases an address for **8 days**. Once 50% of the lease expires, the client will try to renew the lease with the *same* DHCP server.

SNMP Port 161(TCP) and port 162(SNMP trap for both tcp and udp)

161-polling

162-traps

Used to retrival of metrics-

Eg: whats my cpu usage, how much is my ram occupied,

Polling(requesting for the information) - Once in a while server request router for the information of devics to a router and router send backs the information

Polling happens using OID(object ids)

MIB-Management information base , basically a DNS for OIDs

Trap – on a unfortunate event in the router it is having an option of sending a trap.

Router saying server hey something happened in me. Kindly check – its based on the security level

Syntax: snmp-server community cisco ro(read only)or rw(read/wirte)

Snmp enable traps

Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol for collecting and organizing information about managed devices on IPnetworks and for moc servers, workstations, printers, modem racks and more.[1]

Syslog:

Useful for Event management

Controls on an unfortunate event occurs based on the log level it will capture the logs and can b further used for troubleshooting purpose.

Ports 514-used for system logging(UDP)

Port 601-reliable syslog service(TCP)

Port 6514 – reliable syslog over TLS(TCP)

Port 10514- TLS enabled syslog (TCP/UDP)

Severity Level	Name	Description
0	Emergencies	Severe conditions that render a system unusable
1	Alerts	Conditions that require immediate attention
2	Critical	Conditions that should be addressed to prevent an interruption in service, but less severe than an Alert condition
3	Errors	An error condition that does not render the system unusable
4	Warnings	A condition where an operation failed to successfully complete
5	Notifications	An administrative notification about a change to the system
6	Informational	Information about a normal system operation
7	Debugging	Very detailed information about system operation, typically used for troubleshooting

Configuring syslogs

>Config terminal

>logging 192.168.1.2(server address where the syslog gets captured)

>logging trap 5(log level) or >logging trap notificational(in words)

SMTP:

PoRT 25 FOR BOTH TCP AND UDP

Arcsight:

https://youtu.be/_Fvx_nI6E4c

IP addressing

Class A : 1.0.0.0 to 127.255.255.255

Class b :128 to 191

Class c: 192 to 223 -

Class d: 224 to 239 – Multicast purpose or group address

Class e: 240 to 255 –Experimental use

Binary to decimal -2^0 to 2^7

Decimal to binary –

Divide the number by 2 and have the reminders has binary number, - L divide method

Network address is the first address in the block – it defines itself to the rest of the internet

Last address of the block is called broadcast address of that block

NetIds=All 1's

Host Id's =All 0's

Default mask:

All net id will be 0 and all host id will be 1

Default mask will be given based on the class

Masking concept:

Identify the first address of the block or network address

An address in the block with AND operation gives the first address of the block

Eg

23.56.7.91

255.0.0.0

———

23.0.0.0(first address/network address)

Limited broadcast address

255.255.255.255

Router blocks the limited broadcast packet

Subnetting

Well utilization of address space

Subnet mask:

All net ids and subnet ids will be 1 and host id will be 0

Security information and event management

In the field of computer security, **security information and event management** (**SIEM**) software products and services combine security information management (SIM) and and applications.

Hp Arcsight

IBM Qradar

Jitter is defined as a variation in the delay of received packets.

VLan

a switch can be *logically* segmented

into separate broadcast domains, using **Virtual LANs** (or **VLANs**).

Each VLAN represents a unique broadcast domain:

• Traffic between devices within the *same* VLAN is switched.

• Traffic between devices in *different* VLANs requires a Layer-3

device to communicate.

Route command

>Enable –(to move to privilege mode)

>in privilege mode we can ran all show command

>config terminal(after reaching this mode we actually configure the device)

>show ip route(to display routing table)

>show ip access-list(to display access list)

>show xlate(to display the pat configuration)

NAT-Network Address Translation

The rapid growth of the Internet resulted in a shortage of available IPv4 addresses. In response, a specific subset of the IPv4 address space was designated as *private,* to temporarily alleviate this problem.

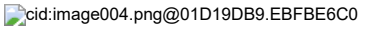
A **public address** can be routed on the Internet. Thus, devices that must be Internet-accessible must be configured with (or *reachable* by) public addresses. Allocation of public addresses is governed by the Internet Assigned Numbers Authority (IANA).

A **private address** is intended for internal use within a home or organization, and can be freely used by anyone. However, private addresses can *never be routed* on the Internet. In fact, Internet routers are configured to immediately drop traffic with private addresses

NAT can also perform public-to-public address translation, as well as private-to-private address translation.

Private address range

class:



CISCO FIREWALL

-

four main administrative access modes:

Monitor mode :password recovery – to access this mode press break/esc

Unprivileged mode -

Privileged mode

Configure mode

Running Config – Volatile and stored in the RAM- to save the current running config, we need to type ‘write memory’ or copy run start

Startup config - non-volatile

Security levels

0-100

0- Outside

1-99- DMZ(Demilitarized Zone)

100-Inside

Highest Security level /interface can communicatge with lower security level and not vice versa.

Traffic from Higher Security Level to Lower Security Level

Allow all unless specified by a ACL

IF NAT is enabled, ther must be a **nat and global pair**

Traffic from Lower Security Level to Higher Security Level:

Drop all unless specified by an ACL.

IF NAT is enabled, ther must be a static-NAT between a higher to lower level.

Traffic between interfaces with same Security Level:

By default, don't allow,

Unless configured with **same-scurity-traffic-permit** command.

Firewall config:

STEP1: Configure a privileged level password

STEP2: Enable Command Line Management

1.)create a username and password

2.) ! Generate a 1024 bit RSA key pair for the firewall which is required for SSH

3.) Specify the hosts allowed to connect to the security appliance.

STEP3: **Configure a Firewall Hostname**

To create a route

ciscoasa(config)# route "*interface-name*" "*destination-ip-address*" "*netmask*" "*gateway*"

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 100.1.1.1 ← Default Route

ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 192.168.1.1 ← Static Route

Dynamic NAT :

From the pool of Ip address in the higher security interfafce as real ip maped with the pool of ip address in the mapped addrees pol for outbound communication.

Dynamic PAT:

Many to One:

The many real IP will be mapped to a single public IP with the request on each real IP will be assigned with the Port number for the request.

Static NAT

Bidirectional communication:

One-to-one address mapping between real and mapped ip

Lower level security interface can communicate with higher level inrerface with appropriate ACL configured.

the ASA firewall implements NAT in two ways:

"***Network object NAT***"

"***Twice NAT***"

NAT 0 or Identity Nat: Used for IPsec or VPN

ACL:

The Access Control List, as the name implies, is a List of statements (called Access Control Entries) that permit or deny traffic from a source to a destination.

Access control lists (ACLs) can be used for two purposes on Cisco devices:

to **filter** traffic, and to **identify** traffic

Each rule or line in

an access-list provides a condition, either **permit** or **deny**:

when filtering traffic, access lists are applied on interfaces.

Only one access list **per interface**, **per protocol**, **per direction** is allowed.

Two Golden Rules of Access Lists:

1. If a bit is set to **0** in a wild-card mask, the corresponding bit in the

address must be **matched exactly.**

2. If a bit is set to **1** in a wild-card mask, the corresponding bit in the

address can **match any number.** In other words, we "don't care"

what number it matches.

Syntax:

The command format of an Access Control List is the following:

ciscoasa(config)# access-list "***access_list_name"*** **[line** ***line_number*****] [extended] {***deny* **|** ***permit*****} protocol "source_address" "mask" [operator source_port] "dest_address" "ma**

Acess group

ciscoasa(config)# access-group "***access_list_name"*** **[in|out] interface "*****interface_name*****"**

access-group "***access_list_name"*** **global**

Access group used to bind the access list with the interface

There are four types of object groups:

Network: Used to group together hosts or subnets.

Service: Used to group TCP or UDP port numbers.

Protocol: Used to group protocols.

ICMP-type: Used to group ICMP message types.

_____

IDS firewall difference

Stateful/stateless firewall

Steless: Packet filtering or static filtering

It just allow or deny the traffic based on ACL.

It filters the traffic based on the below conditions.

Source Ip/Port

Destination Ip /Port

Protocol

Adv: easy to implement

Disadv : Noway to determine if the packet is part of an already existing connection.

Applications use random port numbers and these will trouble operating because of this.

IP spoofing attacks.

Statefull firewall: Dynamic filtering

IT monitors the connection state. Avoid TCP based attacks

Not only monitors the connection but also monitors the sequence numbers

Inside can start connect with outside and not vice versa.

All this will be accomplished by a session table called STATE table.

State table is dynamic, when the connection go quiet from inside, the outside cannot initiate the connection to the insider.

STATE table.

- Source and dest IPaddres/Port numbers
- TCP and UDP flag settings
- TCP sequence info.

TCP packets outside an expected will be dropped

Disadv: application layer attacks –Proxy server

Class A B C D - sub netting

Difference between router and switch

	Router	Switch
Used for	Connecting two or more networks	Connectin
Function	Directs data in a network. Passes data between home computers, and between computers and the modem.	Allow to c
Used in (LAN, MAN, WAN)	LAN, WAN	LAN

Transmission Type	At Initial Level Broadcast then Uni-cast & Multicast	First broac
Data Transmission form	Packet	Frame (L2
Layer	Network Layer (Layer 3 devices)	Data Link
Ports	2/4/2008	Switch is r
Device Type	Networking device	Active Dev
Table	Store IP address in Routing table and maintain address at its own.	Switches u
Transmission Mode	Full duplex	Half/Full c
Broadcast Domain	In Router, every port has its own Broadcast domain.	Switch has
Definition	A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation.	A network considered
Device Category	Intelligent Device	Intelligent
Bandwidth sharing	Bandwidth sharing is Dynamic (Enables either static or dynamic bandwidth sharing for modular cable interfaces. The default percent-value is 0. The percent-value range is 1-96.)	There is no
Speed	1-10 Mbps (Wireless); 100 Mbps (Wired)	10/100 Mb
Routing Decision	Take faster routing decisions	Take more
NAT (Network Address Translation)	Routers can perform NAT	Switches c
Faster	In a different network environment (MAN/ WAN), a router is faster than an L3 switch.	In a LAN e
Features	Firewall VPN Dynamic hadling of Bandwidth	Priority rt
Examples	Linksys WRT54GL Juniper MX & EX series Cisco 3900, 2900, 1900	Alcatel's C
Address used for data tramsmission	Uses IP address	Uses MAC

Arp table and reverseARP

Arp request is broadcast and arp reply is unicast

ARP table maintains IP address corresponding mac address

RArp request is broadcast and Rarp reply is unicast

RARP request for corresponding mac address for a given IP address.

Inline/Passive in IDS

SSH vs TLS

Linux

Ip configuration in Linux

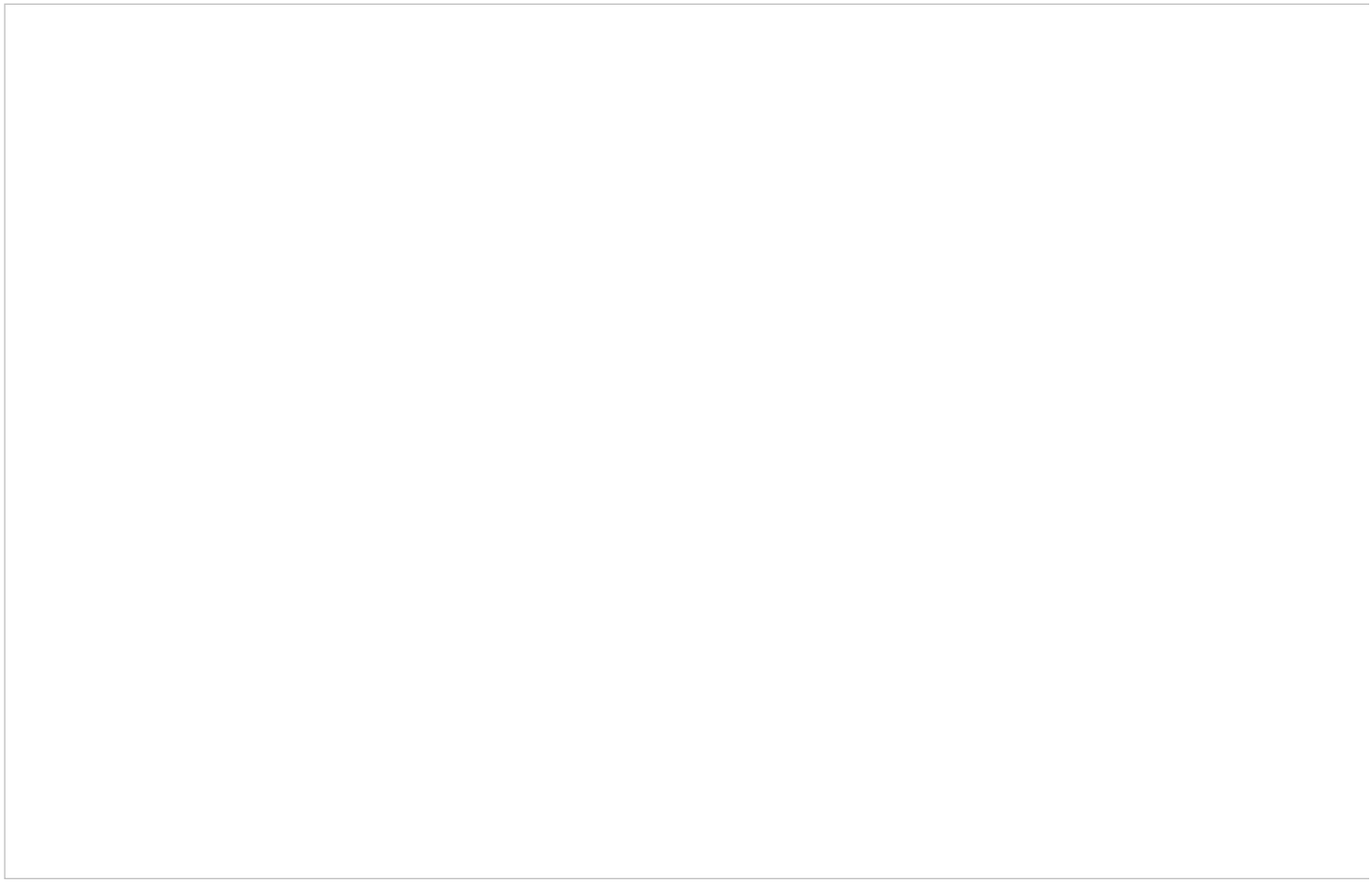
ifconfig interfacename netmask ip up/down

https://www.youtube.com/watch?v=SnACG4TDqJw

dns

iptables:

Packet filterting application in linux based os.



https://www.youtube.com/watch?v=XKfhOQWrUVw

check service status

netstat –a | grep ftp

packet capture -wireshark tcpdump

Project:

Challenges in Manet :

Energy centric,

Dynamic Topology,

Less computation power,

Attacks

Wormhole- advertise valid path and drop the packets

Greyhole- group of nodes advertises itself as a valid path and send the path to the destination after a long time. -> Batery consumption.

Blackhole- Advertises itself as a valid path and sends a fake information to the destination.

Model:

Trust proctor= Energy+direct trust+recommendation trust

Trust handler =Alarm table,friend table, trust evaluator

CA-Certificate authority

TCPdump :

_____

-h version checking

-d identify the available interface

-i interface

-c packet capture size

-s packet bytes size

-w to capture files

-r to read the captured files

-v verbose mode

-t time display

-q –quantity of content display

Capture the packets in the network and analyze the packet

Details abt the packet can either displayed on the screen or can be saved as a pcap file

Libpcap library used for packet filtering.

Version checking

Tcpdump –h

To identify the available interface like eth0 or eth1 like dat

Tcpdump –d

To capture packet using any option -I

Tcpdump –I any

Tcpdump wont stop capturing once start unles interpret by a user command - >ctrl+z

To capture specified number of packets use below -c

Tcpdump –I any –c 5

The above command will capture 5 packets

To display the ip address and port numbers in the result use below -n

Sudo tcpdump –I any –c 5 –n

Capture size of a packet can be altered by using –s

Sudo tcpdump –I any –c 5 –n –s 96 #capture 96 byte

Sudo tcpdump –I any –c 5 –n –s 0 #maximum size of 65535

To capture one direction of traffic:

Sudo tcpdump –I any –c 20 -n tcp and dst port 49952 –t

A single packet looks like the below:

IP sourceIP.port > destinationip.port flags[TCP] acq/seq , window , length

To save the capture for future analysis –w

Sudo tcpdump –I any –w capture.pcap

While capturing packet in the file , usually we cant see how many packets are captured in the CLI, to address this , we will use –v to display number of records got captured in the file

Sudo tcpdump –I any –w capture.pcap –v

To Read the capture files.

Sudo tcpdump –n –r capture.pcap

If the file is large, it will directly go the eof , to enable scrolling use | less

Sudo tcpdump –n –r capture.pcap |less (to scroll up and down)

TCPdump filters

Filters are used to isolate the traffic

To capture packet on particular host

Tcpdump –I eth1 –n host 10.0.0.1 –c 5

To see one direction traffic:

That s packet capture only from the sender src

Tcpdump –I eth1 –n src host 10.0.0.1 –c

Traffic between 2 ip ->source and destination – by using and operator

Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 –c 5

To capture packet only on specific port

Tcpdump –I eth1 –n src host 10.0.0.1 and host 10.0.0.3 and port 80

Compound expression : to show traffic for port 80 or port 443 on the sending host

Tcpdump –I eth0 –n “host 192.168.1.1 \> and (port 80 or port 443)”

To capture ipv6 packets

Tcpdump –I etho 0 ip6

To ping ipv6 address

Ping6 IPV6

Verbose output

Tcpdump –I eth0 –v

Minimal quantity of output

Tcpdump –I eth0 –q

Timestamp

-t

-ttt

-ttttt

2 attachments

image008.jpg
43K

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

image004.png
22K