SSL vs TLS

Secured Sockets Layer:

Ensure security on the internet.

Uses public key encryption to secure data.

Working:

When a computer connects to a website using SSL.

The computer asks the website to identify itself

A copy of SSL certificate will be passed.

Browser will check to ensure.

Encrypted data will follow.

TLS

Transport layer security – Successor to SSL.

Authenticates the server, client and encrypts the data.

Command Lines

IFCONFIG

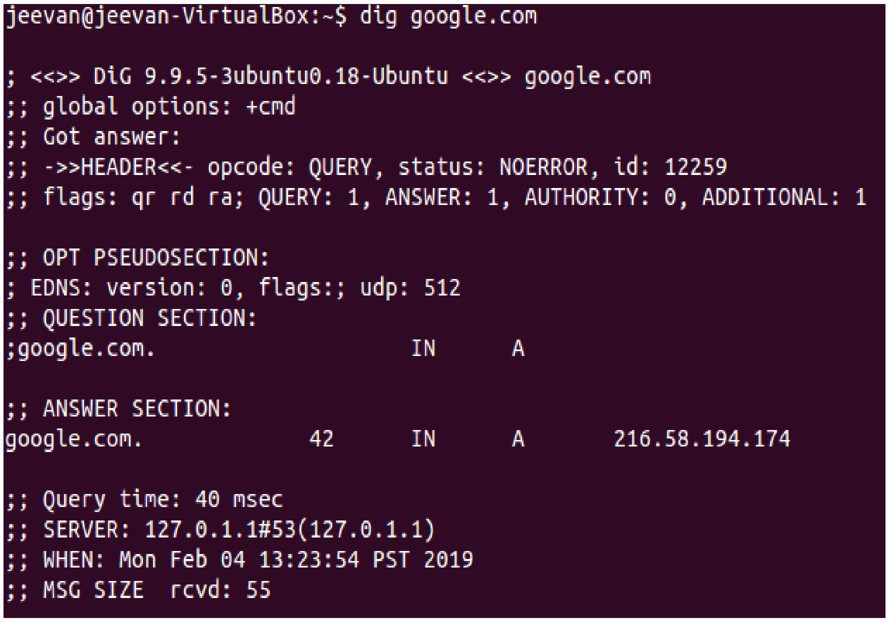
Check the ip address and configuration assigned to the system.

Traceroute

Displays the routers the packet passes on its path to the destination.

DIG command

Returns the answers returned by DNS records



```
jeevan@jeevan-VirtualBox:~$ dig google.com

; <<>> DiG 9.9.5-3ubuntu0.18-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             42      IN      A       216.58.194.174

;; Query time: 40 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 04 13:23:54 PST 2019
;; MSG SIZE  rcvd: 55
```

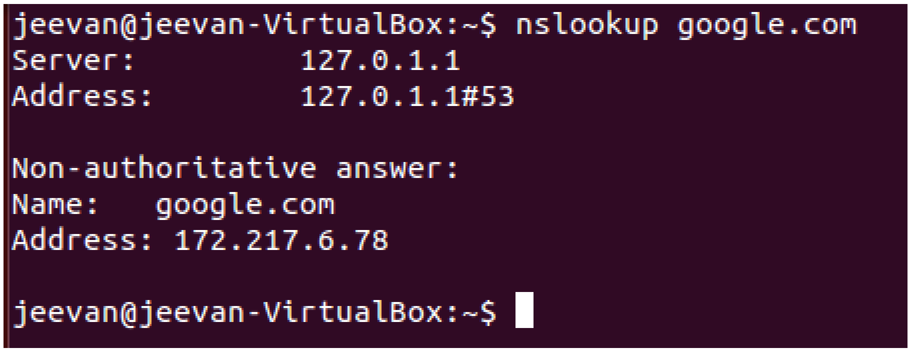
Telnet

To check connectivity between two hosts.

telnet hostname portno

NSLOOKUP

To find entries on the DNS servers



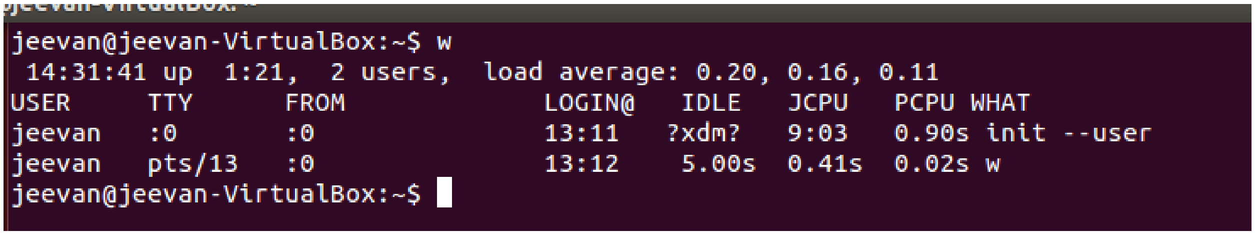
```
jeevan@jeevan-VirtualBox:~$ nslookup google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.6.78

jeevan@jeevan-VirtualBox:~$
```

NETSTAT

Summary of all ports connected and their status

W

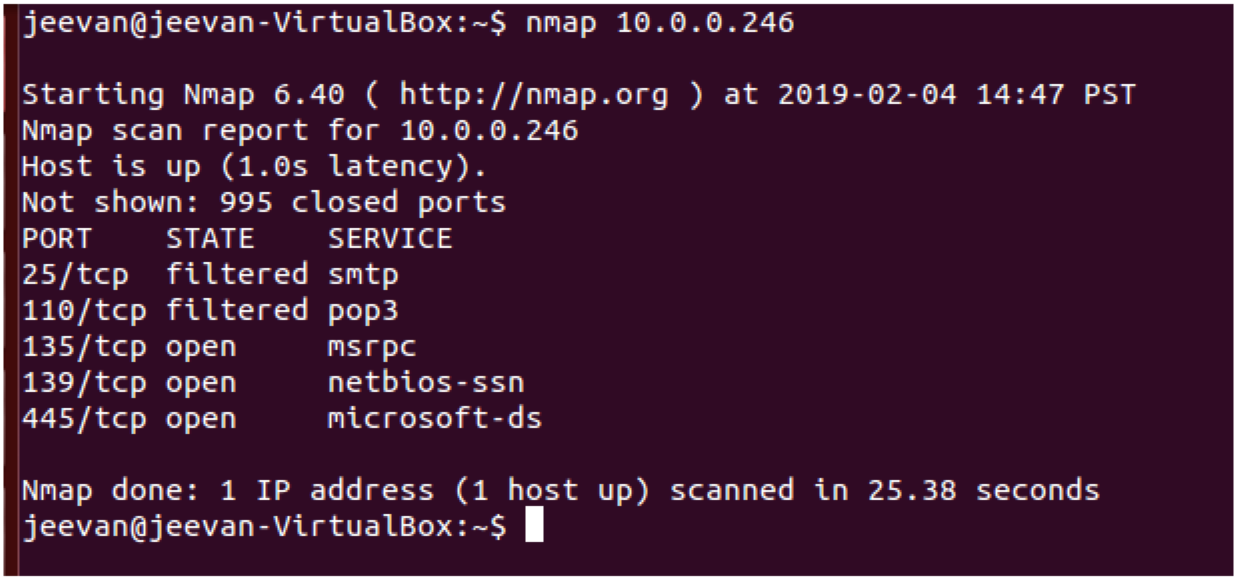
Summary of current activity on the host



```
jeevan@jeevan-VirtualBox:~$ w
 14:31:41 up  1:21,  2 users,  load average: 0.20, 0.16, 0.11
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
jeevan   :0       :0               13:11   ?xdm?   9:03   0.90s init --user
jeevan   pts/13   :0               13:12    5.00s  0.41s  0.02s w
jeevan@jeevan-VirtualBox:~$
```

NMAP

Checks the open ports on the server



```
jeevan@jeevan-VirtualBox:~$ nmap 10.0.0.246

Starting Nmap 6.40 ( http://nmap.org ) at 2019-02-04 14:47 PST
Nmap scan report for 10.0.0.246
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
25/tcp  filtered smtp
110/tcp filtered pop3
135/tcp open     msrpc
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 25.38 seconds
jeevan@jeevan-VirtualBox:~$
```

https://www.tecmint.com/nmap-command-examples/

IFUP / IFDOWN

To enable or disable a network interface.

Example

Ifup eth0

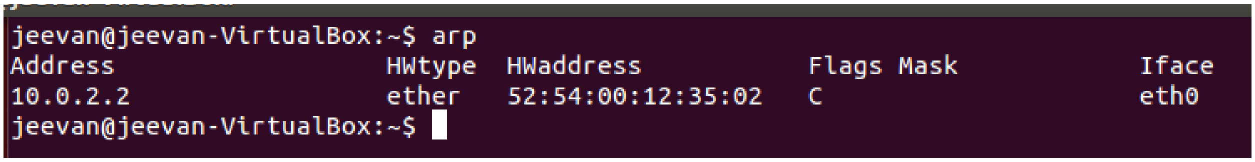
Ifdown eth0

SCP

Secure copy files from other hosts in the network

ARP command

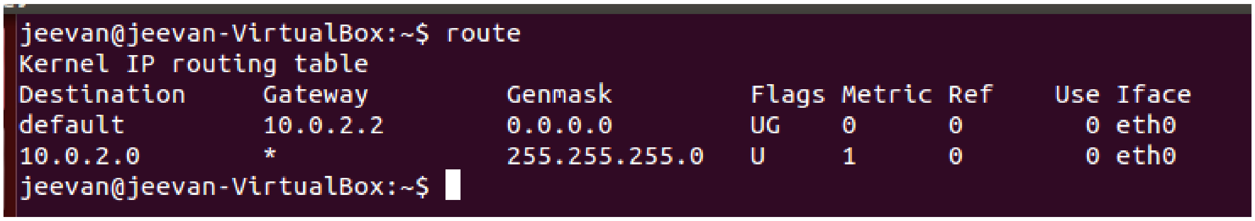
ARP table on the host machine



```
jeevan@jeevan-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.2.2                 ether   52:54:00:12:35:02   C                     eth0
jeevan@jeevan-VirtualBox:~$ 
```

Route Command

Routing table on the host machine



```
jeevan@jeevan-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.2        0.0.0.0         UG    0      0        0 eth0
10.0.2.0        *               255.255.255.0   U     1      0        0 eth0
jeevan@jeevan-VirtualBox:~$ 
```

Adding a default gateway

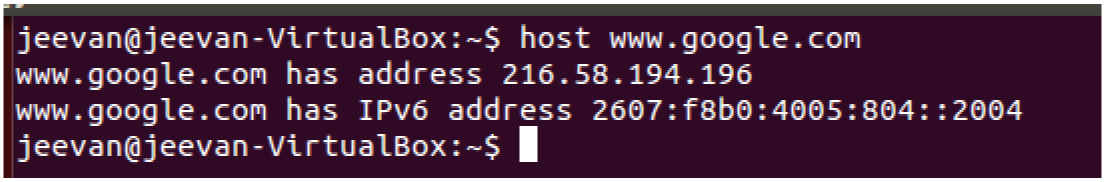
route add -net <ipaddress> gw <gateway ipaddress>

default gateway

route add default gw <gateway ip address>

HOST Command

Name to ip and Ip to name



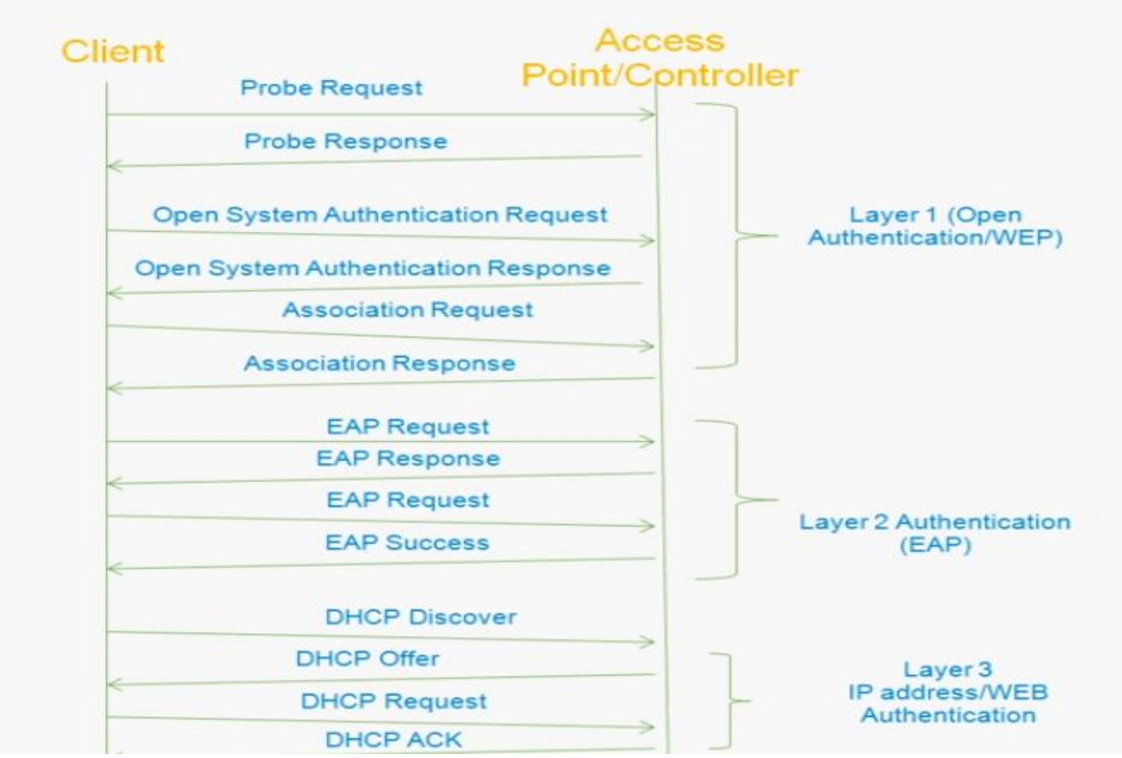
```
jeevan@jeevan-VirtualBox:~$ host www.google.com
www.google.com has address 216.58.194.196
www.google.com has IPv6 address 2607:f8b0:4005:804::2004
jeevan@jeevan-VirtualBox:~$ 
```

Checking Network Connectivity Issues

1. Check LAN and WAN connections
2. Verify wireless adapter
3. Verify AP and router settings.
    a. Verify SSID details (network parameters)
    b. Identify the subnet and whether the client has the ip address.
    c. Verify if the ip address of your desktop is assigned by the router.
4. Verify TCP/IP setting in the desktop.
5. Use ping to verify connectivity.
6. Check wireless specifications issue whether standards.

Client Connectivity Issues

Normal Connection Procedure



Layer 1 Authentication: To find all the available SSIDs or Available wireless networks over the air. After the response. Association request is sent. Agreeing to IEEE formats 802.1 or any.

Layer 2 Authentication: Authentication over data link layer.

Possible problems:

Wrong EAP authentication,

Layer 3: To get an IP address.

Possible problems:

DHCP proxy enable or disable

SSID mismatch

Troubleshooting Client:

3 commands:

1. debug client <MAC address>

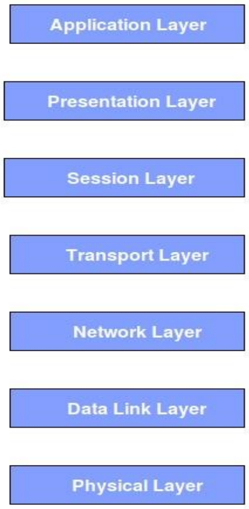
2. show debug → Policy manager state important one that gives status

3. debug disable-all

Client details

Show client <Mac address>

OSI Model



Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

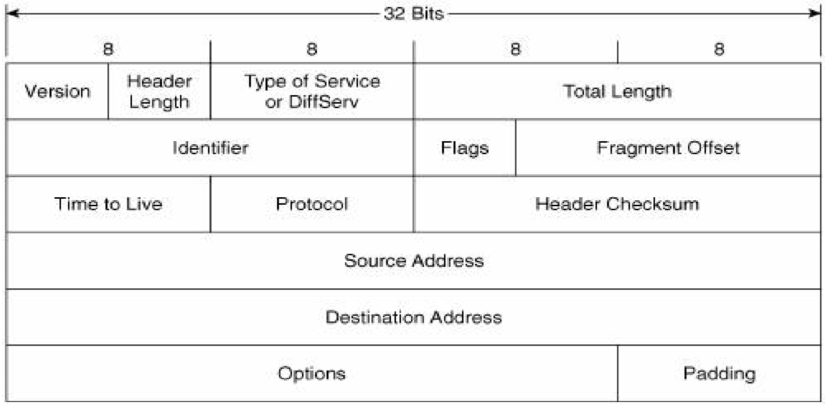
Application Layer: Data is first processed by one of the application as required. In the application layer. It specifies details how the data is encoded, encrypted and how sessions are managed.

Example: HTTP, HTTPS, DNS, SMTP.

Presentation Layer: Takes data from the application layer and converts it into a standard format. So that application layer in the receiver end can decode the data in the correct way.

Session Layer: Establish manage and ends connections between the devices.

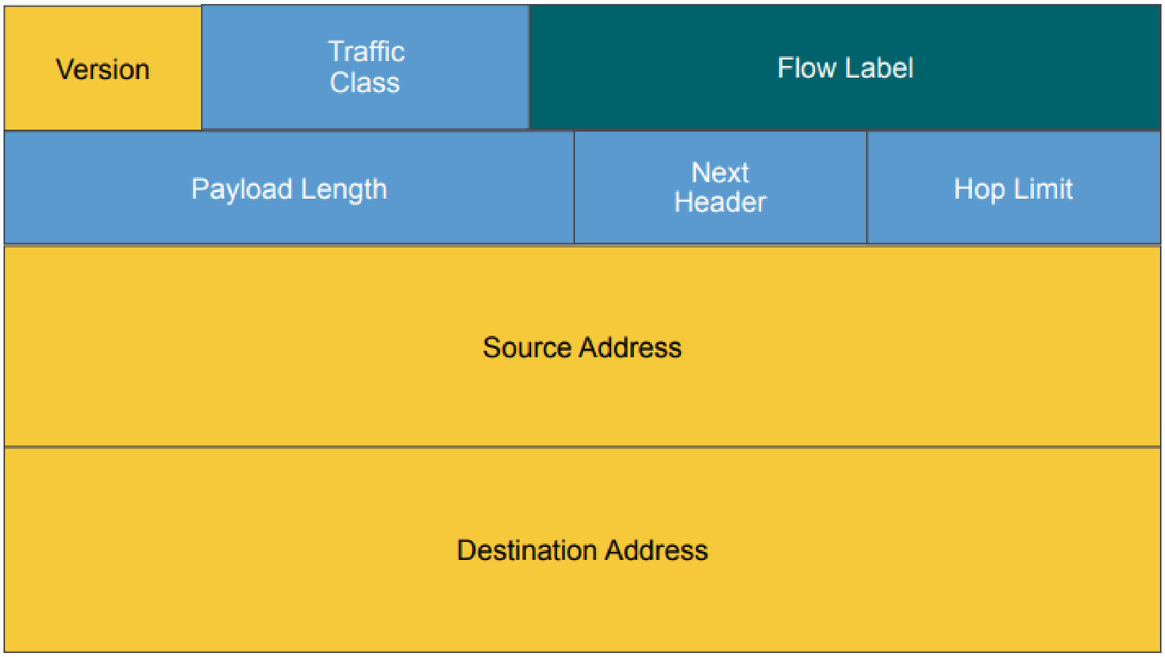
IPv4 Header



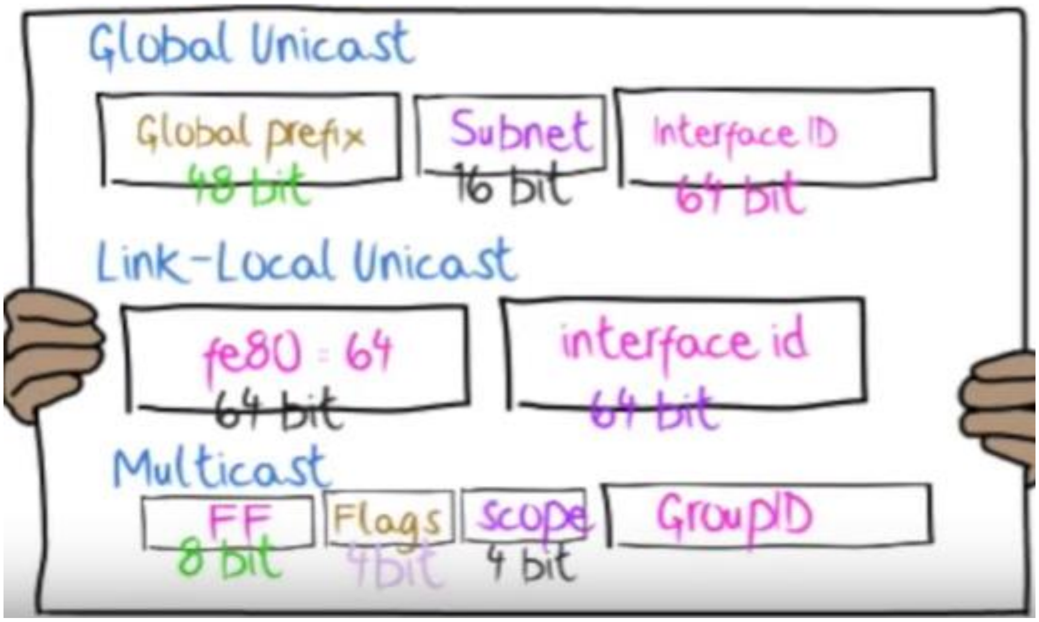
Protocol field: will indicate the transport layer protocol.

Type of service or Differential service: This field Is used to indicate the priority of the packet at the router.

IPV6



Flow label: Used for server load balancing.



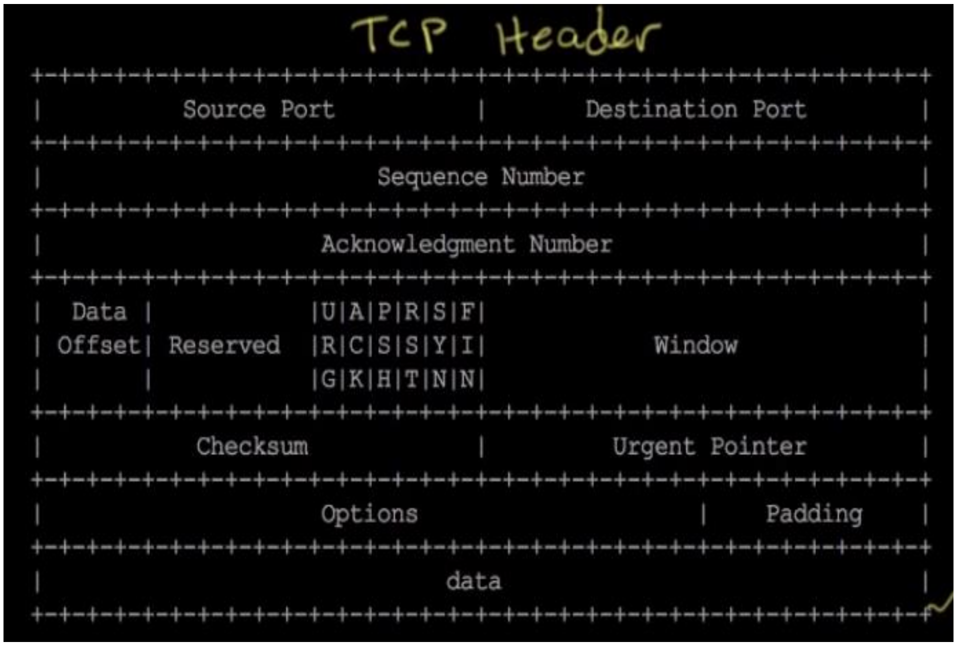
Advantages of IPv6 over IPv4

1. No need of NAT.
2. Reduces routing table size – no netmask and interface connected entries.
3. No need of IP header checksum to calculated
4. Supports multicast rather than broadcast.
5. IPsec provides security, confidentiality.

TCP (Transmission Control Protocol)

Connection Oriented. Before sending any data, a connection has to be established.

TCP Header



TCP Header

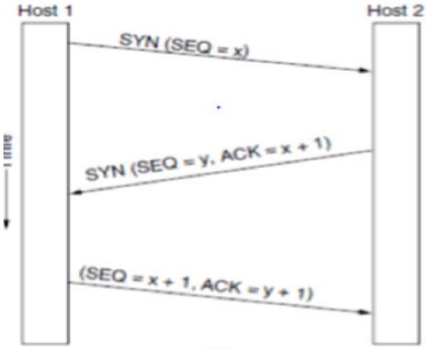
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

A combination of Ip address in layer 3 and Port number in Layer 4 identifies the connection.

Advantages:

1. Handles Packet Loss
2. Re-transmission
3. Reordering
4. Flow Control

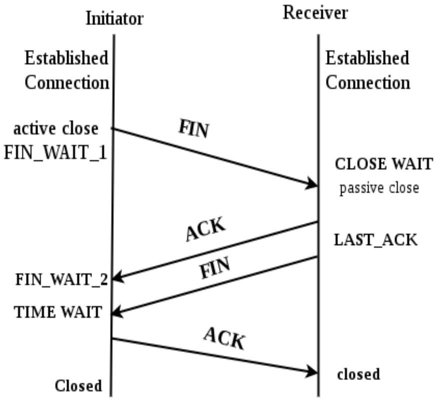
TCP Connection



(a)

Data Transmission

Closing Connection



When receiver needs to flow control:

It will alter the window size in the acknowledgement.

When cannot handle it sends a zero byte size window.

In such a case sender will send keep alive packets.

How to detect when a remote side has closed connection.

Have a timer and assume the remote side is down if acknowledgement is not received.

Keep alive messages on behalf of application stack.

Mobile Networks

3GPP is the organization releases the standards.

Two types of networkDis stitching exist

1. Voice call: Circuit switching
2. Data: Packet switching.

2G used GPRS

4G – connects to the voice call using IMS

5G

Use frequency between 6 and 30 GHz.

Disadvantages – High frequencies gets absorbed by tress and buildings.

Need more transmitting devices.

GSM (Global System for Mobile Communication)

CDMA (Code Division Multiple Access)

Several transmitters can send information simultaneously over a single communication channel.

Routing Protocols types

1. Interior gateway protocol
2. Exterior Gateway Protocol

Interior Gateway Protocol (IGP): A networking protocol designed and intended to use inside a single autonomous system. (EIGRP, OSPF)

Exterior Gateway Protocol (EGP): A routing protocol that was designed and designated to use between different autonomous systems. (BGP is the only EGP used now)

EIGRP: Advertise their routing table to all directly connected neighbors at regular frequent intervals using a lot of bandwidth and take time to converge.

OSPF: Advertise routing update only when changes occur.

1. All routers will determine its directly connected neighbors.
2. Every router will generate a LSA (Link State Advertisement) for its interfaces.
3. Once LSA are generated every router will flood the network with LSAs
4. All LSAs are used to build a network picture LSDB (Link State Database).
5. From LSDB find the Shortest Path First (SPF) Dijkstra to all nodes.
6. Place the best shortest paths in the routing table.

Network Security

Symmetric and Asymmetric:

Symmetric: If sender and receiver use the same key to decrypt.

Same key is used for both encryption and decryption.

Asymmetric: If entities use a different key.

One algorithm is used for encryption and a related algorithm for decryption. With a pair of keys.

AES (Advanced Encryption Standard)

It works on substitution permutation network.

AES has a fixed block size of 128 bits. Key sizes vary from 128, 192 and 256.

Package: PyCrypto

Mesh Network:

When bridges, routers and switches are non heirarchial.

Hub - sends packets to all other nodes except the received one.

works on layer 1.

Bridge -

will check the source address and looks at the destination address and decides whether or not to send the data.

Switch

send data to the interface it is connected to.

Layer 2

Full duplex

Each port has its own collision domain

Client Connectivity

https://community.cisco.com/t5/wireless-mobility-videos/troubleshooting-client-connection-issue-on-cisco-wireless/ba-p/3102725