**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**

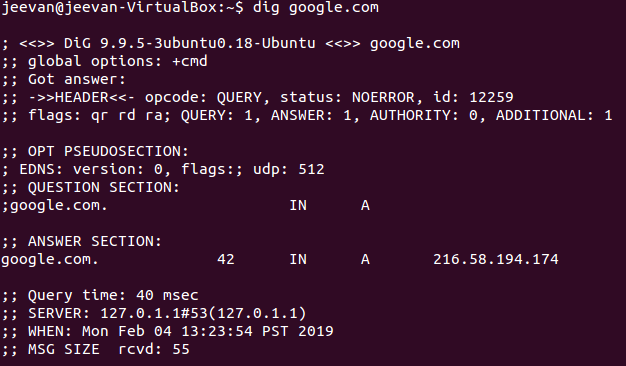
Check the ip address and configuration assigned to the system.

**Traceroute**

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

**DIG command**

Returns the answers returned by DNS records



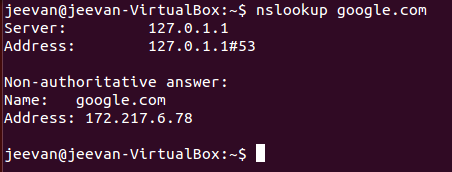
**Telnet**

To check connectivity between two hosts.

telnet hostname portno

**NSLOOKUP**

To find entries on the DNS servers

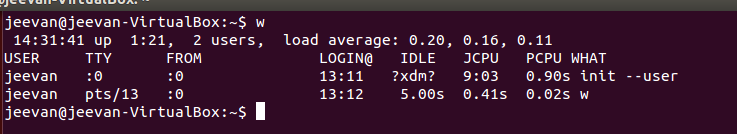


**NETSTAT**

Summary of all ports connected and their status

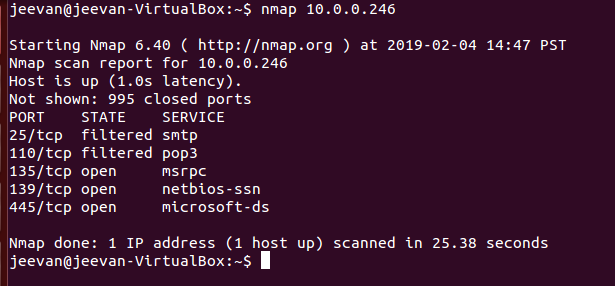
**W**

Summary of current activity on the host



**NMAP**

Checks the open ports on the server



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

**IFUP / IFDOWN**

To enable or disable a network interface.

Example

Ifup eth0

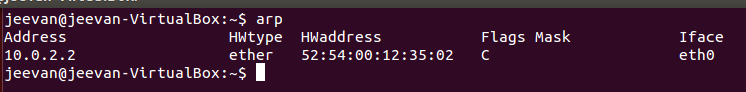
Ifdown eth0

**SCP**

Secure copy files from other hosts in the network

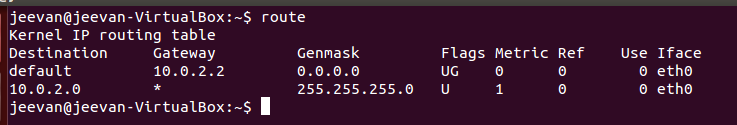
**ARP command**

ARP table on the host machine



**Route Command**

Routing table on the host machine



Adding a default gateway

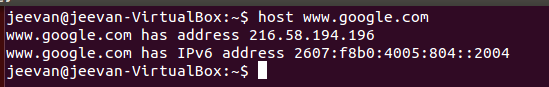
route add -net <ipaddress> gw <gateway ipaddress>

default gateway

route add default gw <gateway ip address>

**HOST Command**

Name to ip and Ip to name

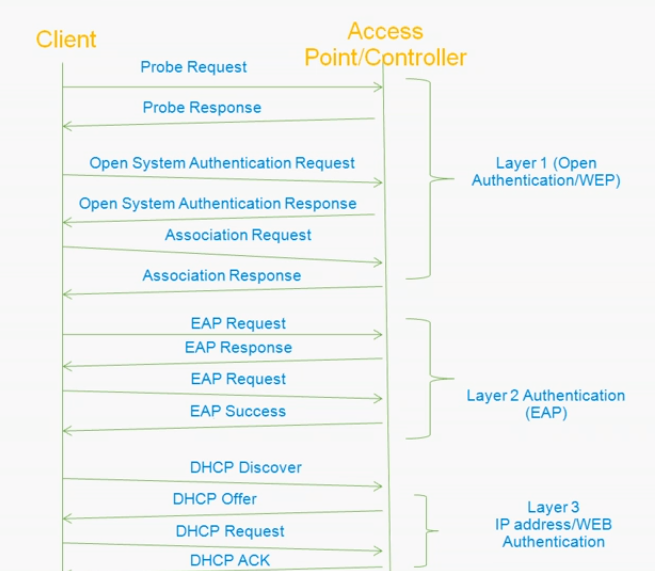


**Checking Network Connectivity Issues**

1. Check LAN and WAN connections
2. Verify wireless adapter
3. Verify AP and router settings.
   1. Verify SSID details (network parameters)
   2. Identify the subnet and whether the client has the ip address.
   3. 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:**

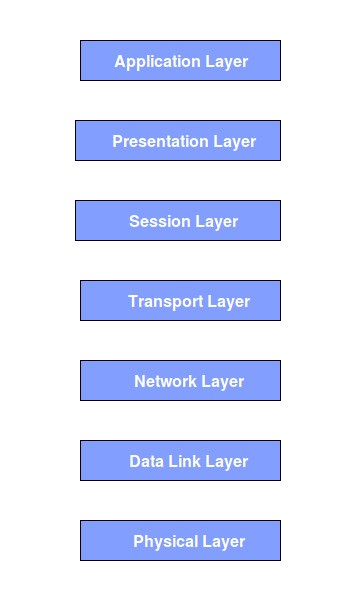
3 commands:

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**



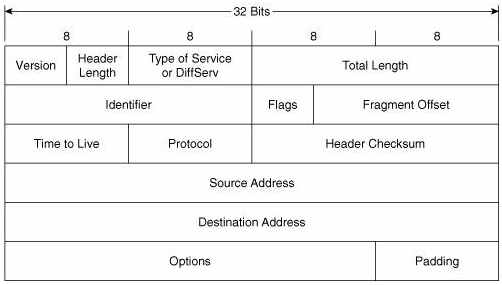
**Application Layer**: Data is first processed by one of the application as required. In the application layer. It specifies details how the data is encoded, encrypted and how sessions are managed.

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.

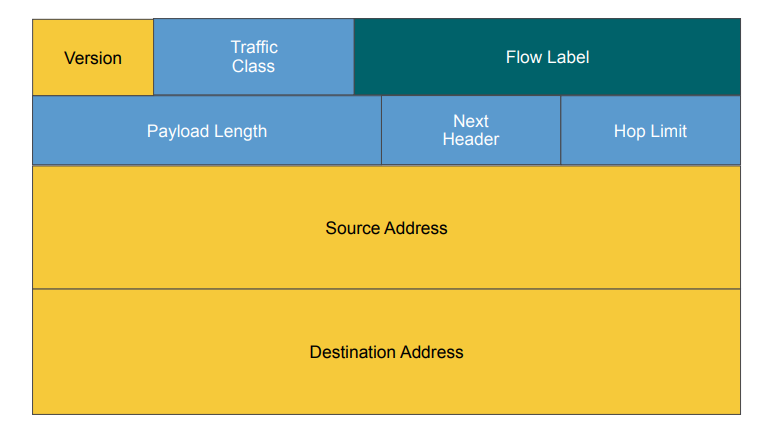
**IPv4 Header**



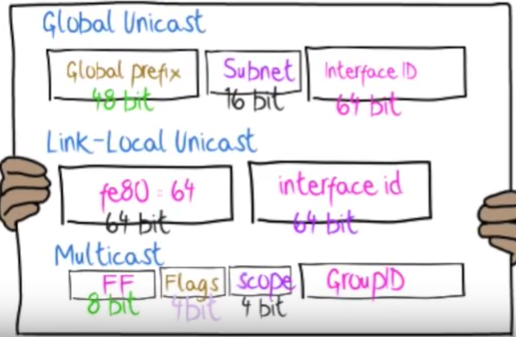
**Protocol field**: will indicate the transport layer protocol.

**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.



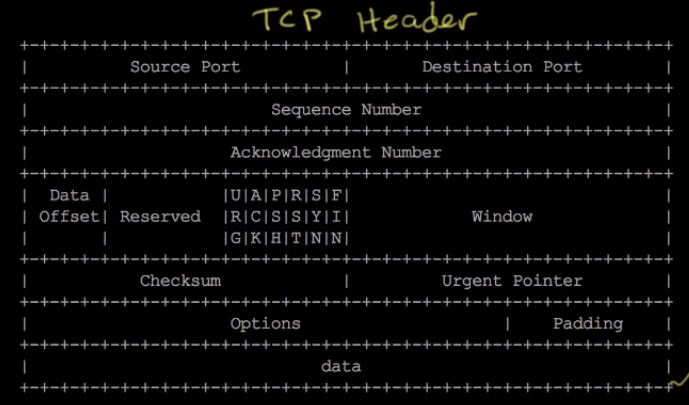
**Advantages of IPv6 over IPv4**

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
   1. Supports multicast rather than broadcast.
4. IPsec provides security, confidentiality.

**TCP (Transmission Control Protocol)**

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

**TCP Header**

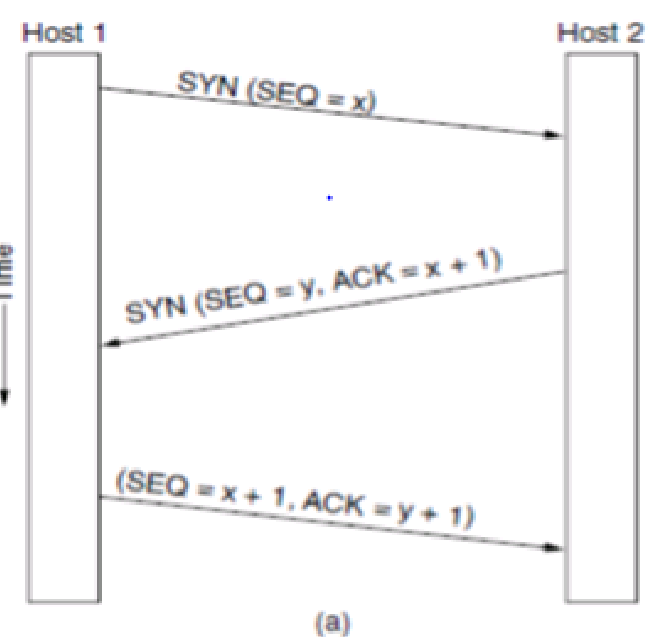


A combination of Ip address in layer 3 and Port number in Layer 4 identifies the connection.

Advantages:

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

**TCP Connection**



**Data Transmission**

**Closing Connection**

Image result for closing connection TCP

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-hierarchical.

**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

**DDoS (Distributed Denial of Service)**

When a attacker machine floods a server with dummy requests. (DoS)

When a attacker machine uses several other hosts to flood a server (DDoS)

How to safeguard:

F5 has a silverware platform

This has 2 ways to counter such attacks.

1. The silverware gets an idea of the average TPS (transaction per second) for a normal host. Shuts down host that do not fall in that range by sending a Javascript that only a user can handle not a bot
2. If the attacker maintains the TPS rate on Bots then, usually all bots use a HTTP post method to attack a server. The silverware prevents HTTPs post methods from the bots.

Kerberos Authentication

Authentication Protocol

HTTP in detail

<https://www.tutorialspoint.com/http/http_methods.htm>

**Client Connectivity**

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