

TCP

- Well known ports=Assigned for Standard Server Processes

Port	Protocol	Description
1	Telnet	Remote terminal connection to the server
2	FTP	File Transfer Protocol (control connection)
3	FTP	File Transfer Protocol (data connection)
4	SMTP	Simple Mail Transfer Protocol
5	POP3	Post Office Protocol version 3
6	SSH	Secure Shell
7	HTTP	Hypertext Transfer Protocol
8	HTTPS	Secure Hypertext Transfer Protocol
9	IMAP	Internet Message Access Protocol
10	LDAP	Lightweight Directory Access Protocol
11	SMTP	Simple Mail Transfer Protocol
12	POP3	Post Office Protocol version 3
13	SSH	Secure Shell
14	HTTP	Hypertext Transfer Protocol
15	HTTPS	Secure Hypertext Transfer Protocol
16	IMAP	Internet Message Access Protocol
17	LDAP	Lightweight Directory Access Protocol
18	SMTP	Simple Mail Transfer Protocol
19	POP3	Post Office Protocol version 3
20	SSH	Secure Shell
21	HTTP	Hypertext Transfer Protocol
22	HTTPS	Secure Hypertext Transfer Protocol
23	IMAP	Internet Message Access Protocol
24	LDAP	Lightweight Directory Access Protocol
25	SMTP	Simple Mail Transfer Protocol
26	POP3	Post Office Protocol version 3
27	SSH	Secure Shell
28	HTTP	Hypertext Transfer Protocol
29	HTTPS	Secure Hypertext Transfer Protocol
30	IMAP	Internet Message Access Protocol
31	LDAP	Lightweight Directory Access Protocol
32	SMTP	Simple Mail Transfer Protocol
33	POP3	Post Office Protocol version 3
34	SSH	Secure Shell
35	HTTP	Hypertext Transfer Protocol
36	HTTPS	Secure Hypertext Transfer Protocol
37	IMAP	Internet Message Access Protocol
38	LDAP	Lightweight Directory Access Protocol
39	SMTP	Simple Mail Transfer Protocol
40	POP3	Post Office Protocol version 3
41	SSH	Secure Shell
42	HTTP	Hypertext Transfer Protocol
43	HTTPS	Secure Hypertext Transfer Protocol
44	IMAP	Internet Message Access Protocol
45	LDAP	Lightweight Directory Access Protocol
46	SMTP	Simple Mail Transfer Protocol
47	POP3	Post Office Protocol version 3
48	SSH	Secure Shell
49	HTTP	Hypertext Transfer Protocol
50	HTTPS	Secure Hypertext Transfer Protocol
51	IMAP	Internet Message Access Protocol
52	LDAP	Lightweight Directory Access Protocol
53	SMTP	Simple Mail Transfer Protocol
54	POP3	Post Office Protocol version 3
55	SSH	Secure Shell
56	HTTP	Hypertext Transfer Protocol
57	HTTPS	Secure Hypertext Transfer Protocol
58	IMAP	Internet Message Access Protocol
59	LDAP	Lightweight Directory Access Protocol
60	SMTP	Simple Mail Transfer Protocol
61	POP3	Post Office Protocol version 3
62	SSH	Secure Shell
63	HTTP	Hypertext Transfer Protocol
64	HTTPS	Secure Hypertext Transfer Protocol
65	IMAP	Internet Message Access Protocol
66	LDAP	Lightweight Directory Access Protocol
67	SMTP	Simple Mail Transfer Protocol
68	POP3	Post Office Protocol version 3
69	SSH	Secure Shell
70	HTTP	Hypertext Transfer Protocol
71	HTTPS	Secure Hypertext Transfer Protocol
72	IMAP	Internet Message Access Protocol
73	LDAP	Lightweight Directory Access Protocol
74	SMTP	Simple Mail Transfer Protocol
75	POP3	Post Office Protocol version 3
76	SSH	Secure Shell
77	HTTP	Hypertext Transfer Protocol
78	HTTPS	Secure Hypertext Transfer Protocol
79	IMAP	Internet Message Access Protocol
80	LDAP	Lightweight Directory Access Protocol
81	SMTP	Simple Mail Transfer Protocol
82	POP3	Post Office Protocol version 3
83	SSH	Secure Shell
84	HTTP	Hypertext Transfer Protocol
85	HTTPS	Secure Hypertext Transfer Protocol
86	IMAP	Internet Message Access Protocol
87	LDAP	Lightweight Directory Access Protocol
88	SMTP	Simple Mail Transfer Protocol
89	POP3	Post Office Protocol version 3
90	SSH	Secure Shell
91	HTTP	Hypertext Transfer Protocol
92	HTTPS	Secure Hypertext Transfer Protocol
93	IMAP	Internet Message Access Protocol
94	LDAP	Lightweight Directory Access Protocol
95	SMTP	Simple Mail Transfer Protocol
96	POP3	Post Office Protocol version 3
97	SSH	Secure Shell
98	HTTP	Hypertext Transfer Protocol
99	HTTPS	Secure Hypertext Transfer Protocol
100	IMAP	Internet Message Access Protocol
101	LDAP	Lightweight Directory Access Protocol
102	SMTP	Simple Mail Transfer Protocol
103	POP3	Post Office Protocol version 3
104	SSH	Secure Shell
105	HTTP	Hypertext Transfer Protocol
106	HTTPS	Secure Hypertext Transfer Protocol
107	IMAP	Internet Message Access Protocol
108	LDAP	Lightweight Directory Access Protocol
109	SMTP	Simple Mail Transfer Protocol
110	POP3	Post Office Protocol version 3
111	SSH	Secure Shell
112	HTTP	Hypertext Transfer Protocol
113	HTTPS	Secure Hypertext Transfer Protocol
114	IMAP	Internet Message Access Protocol
115	LDAP	Lightweight Directory Access Protocol
116	SMTP	Simple Mail Transfer Protocol
117	POP3	Post Office Protocol version 3
118	SSH	Secure Shell
119	HTTP	Hypertext Transfer Protocol
120	HTTPS	Secure Hypertext Transfer Protocol
121	IMAP	Internet Message Access Protocol
122	LDAP	Lightweight Directory Access Protocol
123	SMTP	Simple Mail Transfer Protocol
124	POP3	Post Office Protocol version 3
125	SSH	Secure Shell
126	HTTP	Hypertext Transfer Protocol
127	HTTPS	Secure Hypertext Transfer Protocol
128	IMAP	Internet Message Access Protocol
129	LDAP	Lightweight Directory Access Protocol
130	SMTP	Simple Mail Transfer Protocol
131	POP3	Post Office Protocol version 3
132	SSH	Secure Shell
133	HTTP	Hypertext Transfer Protocol
134	HTTPS	Secure Hypertext Transfer Protocol
135	IMAP	Internet Message Access Protocol
136	LDAP	Lightweight Directory Access Protocol
137	SMTP	Simple Mail Transfer Protocol
138	POP3	Post Office Protocol version 3
139	SSH	Secure Shell
140	HTTP	Hypertext Transfer Protocol
141	HTTPS	Secure Hypertext Transfer Protocol
142	IMAP	Internet Message Access Protocol
143	LDAP	Lightweight Directory Access Protocol
144	SMTP	Simple Mail Transfer Protocol
145	POP3	Post Office Protocol version 3
146	SSH	Secure Shell
147	HTTP	Hypertext Transfer Protocol
148	HTTPS	Secure Hypertext Transfer Protocol
149	IMAP	Internet Message Access Protocol
150	LDAP	Lightweight Directory Access Protocol
151	SMTP	Simple Mail Transfer Protocol
152	POP3	Post Office Protocol version 3
153	SSH	Secure Shell
154	HTTP	Hypertext Transfer Protocol
155	HTTPS	Secure Hypertext Transfer Protocol
156	IMAP	Internet Message Access Protocol
157	LDAP	Lightweight Directory Access Protocol
158	SMTP	Simple Mail Transfer Protocol
159	POP3	Post Office Protocol version 3
160	SSH	Secure Shell
161	HTTP	Hypertext Transfer Protocol
162	HTTPS	Secure Hypertext Transfer Protocol
163	IMAP	Internet Message Access Protocol
164	LDAP	Lightweight Directory Access Protocol
165	SMTP	Simple Mail Transfer Protocol
166	POP3	Post Office Protocol version 3
167	SSH	Secure Shell
168	HTTP	Hypertext Transfer Protocol
169	HTTPS	Secure Hypertext Transfer Protocol
170	IMAP	Internet Message Access Protocol
171	LDAP	Lightweight Directory Access Protocol
172	SMTP	Simple Mail Transfer Protocol
173	POP3	Post Office Protocol version 3
174	SSH	Secure Shell
175	HTTP	Hypertext Transfer Protocol
176	HTTPS	Secure Hypertext Transfer Protocol
177	IMAP	Internet Message Access Protocol
178	LDAP	Lightweight Directory Access Protocol
179	SMTP	Simple Mail Transfer Protocol
180	POP3	Post Office Protocol version 3
181	SSH	Secure Shell
182	HTTP	Hypertext Transfer Protocol
183	HTTPS	Secure Hypertext Transfer Protocol
184	IMAP	Internet Message Access Protocol
185	LDAP	Lightweight Directory Access Protocol
186	SMTP	Simple Mail Transfer Protocol
187	POP3	Post Office Protocol version 3
188	SSH	Secure Shell
189	HTTP	Hypertext Transfer Protocol
190	HTTPS	Secure Hypertext Transfer Protocol
191	IMAP	Internet Message Access Protocol
192	LDAP	Lightweight Directory Access Protocol
193	SMTP	Simple Mail Transfer Protocol
194	POP3	Post Office Protocol version 3
195	SSH	Secure Shell
196	HTTP	Hypertext Transfer Protocol
197	HTTPS	Secure Hypertext Transfer Protocol
198	IMAP	Internet Message Access Protocol
199	LDAP	Lightweight Directory Access Protocol
200	SMTP	Simple Mail Transfer Protocol

- Registered ports

Ports ranging from 1024 - 49,151
Used for proprietary server processors or any client process

Normally not used

- Dynamic ports/ Ephemeral ports

From 49,152 to 65,535

Used by client processes temporarily

Source port address

For client TCP header this is a dynamic port number

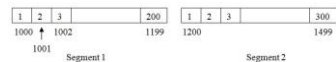
For server TCP header this is a well-known port number

Fields in the TCP Header That

Ensure Reliability

Sequence Number (4 bytes)

Ensures **data is delivered in order** and detects **loss**.



Acknowledgment Number (4 bytes)

Enables **positive acknowledgment**, confirming which data has been received.

Checksum (2 bytes)

Detects **data corruption** during transmission.

Flags (6 bits within 2 bytes)

SYN: Used to establish connections.

ACK: Acknowledges received data.

FIN: Used to terminate connections.

RST: Resets (Destroy / Terminate) the connection.

PSH: Pushes data to the application layer immediately.

URG: Urgent pointer field is significant.

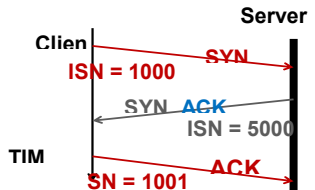
Header length (HLEN)

Header length in bytes = HLEN x 4

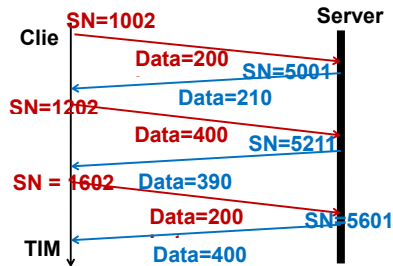
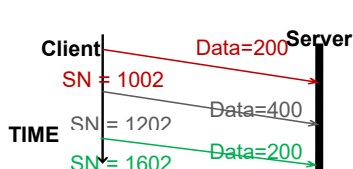
Sequence number

Sequence numbers of three-way handshake

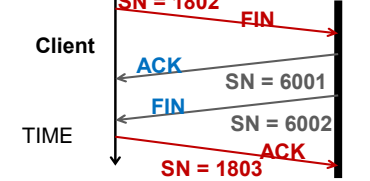
SYN and ACK: 1 byte each



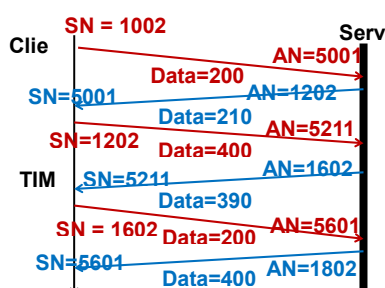
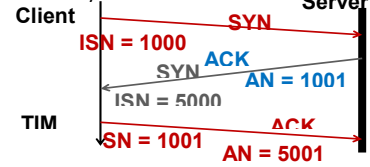
Sequence numbers of data segments



Sequence numbers of connection termination



Acknowledgement numbers of three-way handshake



Control (Fields)

RST - Reset

*Request for an unidentified port

Client or server has a problem

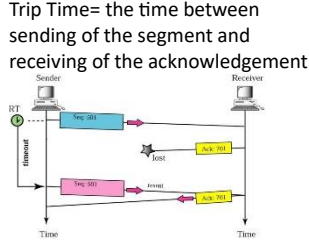
*The connection has been established

*The other side TCP is idle for a long time

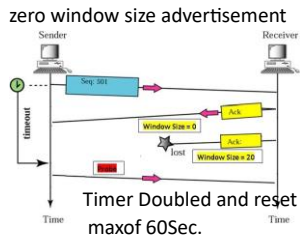
Timers

Retransmission-error control

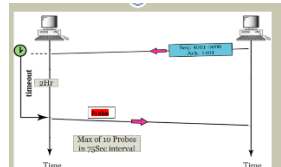
Retransmission time = 2 x Round Trip Time = the time between sending of the segment and receiving of the acknowledgement



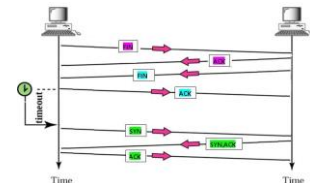
Persistence- To avoid problems of zero window size advertisement



Timer Doubled and reset max of 60Sec.
Threshold - 60 Sec



Time- waited- To avoid problems with delayed FIN segments



Error control

TCP uses the backward error control. If the receiver detects errors, it will discard that segment

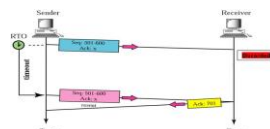
Errors in the received segment (corrupted segments)

Segment is lost on the way before reaching the receiver (last segment)

Duplicate received segments

Out of order segments (the segment numbers are not received in order)

Lost an acknowledgement on the way



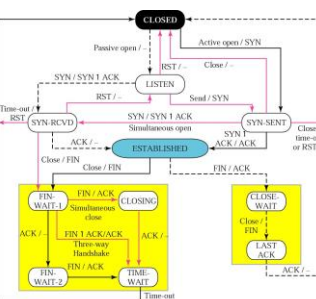
Window size

Receiver TCP buffer can be overflowed due to two reasons

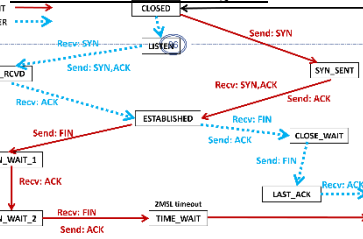
- The receiver TCP buffer receives data very fast

- The receiver application consumes data very slowly

Receiver TCP should inform the sender TCP how much bytes of data it can accommodate



TCP state Transition Diagram

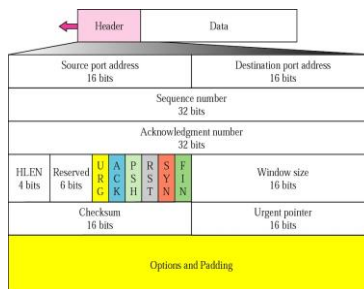
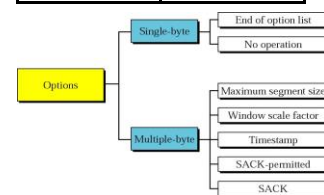


User Datagram Protocol (UDP)

*UDP does not have a connection establishment process
UDP does not have a connection termination process
UDP does not have error control, flow control and congestion control mechanisms
UDP header has only 8 bytes (TCP 20 bytes)

*Since UDP does not get any feedback from the receiver, there is no guarantee of delivering data to the receiver by UDP
Therefore UDP is an unreliable simple protocol
Because of its simplicity it is used for specific applications especially the broadcast type applications

Port NO	Application
69	TFTP
53	DNS
161	SNMP
520	RIP



HeaderSize = HLEN x 4

OptionField = HeaderSize - Standard Header Size

Both URG & ACK flags are set. URG flag set means, this contains urgent data that should read 1st. ACK flag is set means reader get acknowledgement

Distance Vector Protocol &

Distance Vector Protocol	Link State Routing protocol
Routers share their entire routing table with neighbors periodically.	Routers share information about the status of their own links with all routers in the network.
Periodic	Event-driven
Slower	Faster
Less scalable	More scalable
Simple	Complex
Ex: RIP (Routing Information Protocol)	Ex: OSPF (Open Shortest Path First), IS-IS

Link State Routing protocol

TCP	UDP
Connection-oriented	Connectionless
Reliable (ensures delivery, retransmissions)	Unreliable (no retransmission)
Email, Web browsing	Video streaming

Redundant Links & Spanning Tree Protocol (STP)

Why Redundant Links Are Needed

To keep the network running if one link fails (fault tolerance).

helps prevent downtime in business-critical networks.

Problems with Redundant Links (Without STP)

- ☑ Loops cause broadcast storms (infinite frame circulation).
- ☑ Multiple **frame copies** can confuse devices.
- ☑ **MAC table instability**: Switches get wrong info about device locations.

What is STP?

Spanning Tree Protocol (STP) is used to prevent loops in Layer 2 (Ethernet) networks. It **blocks redundant paths** temporarily to create a **loop-free** topology.

How STP Works (Spanning Tree Algorithm Steps)

Elect a Root Bridge – the switch with the lowest Bridge ID. Assigned manually or by the manufacturer. Sometimes can be MAC addr.

Elect Root Ports – The port with the least cost path to the root is root port.

Elect Designated Bridges-designated bridge is the bridge with least cost to root.

Elect Designated Port-designated port is the bridge with least cost to LAN segment.

Advantages of STP

Prevents Infinite Loops. Ensure there is only **one logical path** between any two switches
Prevents Infinite Loops. STP keeps the network **stable** and **usable**, even with redundancy.

Disadvantages of STP

Wasted Redundant Links:

*Some backup links are **active but blocked**, so they **don't carry any data**. ***Suboptimal Paths**: STP may **block shorter paths** and use **longer ones**, making the network **less efficient**.

BPDUs – Bridge Protocol Data Unit

Special message used by STP to share information about Bridge IDs & root path cost between switches (Bridge ID, cost, etc.).

◆ STP Port States

- ☑ Blocking – no data forwarded; prevents loops.
- ☑ Listening – processes BPDUs, no MAC learning.
- ☑ Learning – learns MAC addresses, no data forwarding.
- ☑ Forwarding – sends and receives data.
- ☑ Disabled – admin or failure shuts down the port.

STP Path Cost vs Bandwidth

Higher **bandwidth** = **lower path cost**

ACL

Tell what types of data access or deny based on source address, destination address, protocol, upper layer port no.

Things ACL can do

- ☐ Prevent unwanted traffic
- ☐ Prevent hackers from penetrating the network
- ☐ Prevent employees from using systems in unauthorized manner
- ☐ Filter routing updates
- ☐ Match packets for prioritization
- ☐ Match packets for VPN tunneling
- ☐ Match packets for implementing quality of service features

How ACL works?

*ACL have many statements
*They operate in sequential, logical order

*If statement 1 is matched, router has to carry out the action defined in that statement

*Continue looping until a statement is matched
+Wildcard Mask = 1 means need not to check
+Wildcard Mask = 0 means need to check

Ex: 172.30.16.29 0.0.0.0 checks all the address bits.

(Host(172.30.16.29))

Accept any address: 198.10.0.1 255.255.255.255.

Abbreviate using the keyword **any**.

Standard ACL

Router (config) # access-list access-list-number {permit | deny} {Source address} {wildcard}

ACL No= 1-99

*Checks source address

***Standard ACLs** should be placed as close to the destination as possible

Permit my network only

access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 deny 0.0.0.0 255.255.255.255 /
access-list 1 deny any

Extended ACL

ACL No= 100-199

*Checks destination address

***Extended ACLs** should be placed as close to the Source as possible

Router (config) # access-list access-list-number {permit | deny} {protocol} {Source address} {wildcard mask} {destination address} {wildcard mask} {eq | lt | gt} {port number}

*Needs to restrict Internet access of 192.168.10.0 to allow only website browsing

192.168.10.0 0.0.255 any eq 80 80 OR **http**

R1 (Config) # access-list 103 permit tcp

Apply ACL to an interface

Router (config-if) # {protocol} access-group access-list-number {in | out}

Ex: R1 (config) # interface s0/0/0
R1 (config) # ip access-group 103 out

RAM - running configuration file

ROM-bootable IOS image & bootstrap program

NVRAM - startup configuration file - Retains content when router is powered down

Flash memory - fully functional IOS image. Is a type of electronically erasable, programmable ROM (EEPROM)

Router# copy startup-config running-config
Router#show startup-config

Classful Addressing - Subnet Mask

Net ID part: All 1's
Host ID part : All 0's

Default Gateway IP Address

120.0.0.0 - 120.0.0.50

Loopback address

Any address start with 127.

Public IP Addresses

Is any valid address that can be accessed over the Internet.

Private IP Addresses

Class	Private Network Address	# Net
A	10.0.0.0	1
B	172.16.0.0 to 172.31.0.0	16

C	192.168.0.0 to 192.168.255.0	256
---	------------------------------	-----

This host on this network

Net Id 0's

Host Id 0's

Specific host on this network

Net Id 0's

Host Id Specific

Limited Broadcast Address

Net Id 1's

Host Id 1's

No: of Sub Net= 2^n

(n= Extra bits get from host part)

No of total address= 2^{no: of host bits}

Remaining host bits

Usable IP addresses = 2^{no: of host bits} - 2

Dual Stack – IPv4 and IPv6 to coexist on the same network.

Tunneling- transporting IPv6 over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet

Translating- NAT64 can transfer IPv6 to IPv4

Rule 1 (Omitting Leading 0s)

Rule 2 (Omitting All 0 Segments)

× Unicast: One device send one device

× Multicast: 1 device sent many device

× Any cast: One device sent the nearest device and that nearest device sent another device

IPv6 Unicast Addresses

*Global unicast -Global unicast can be configured statically or assigned dynamically.

*Link-local-communicate with other device in same local link

*Unique local-Similar to private address in IPV4

Adaptive Routing

• Each router maintains a routing table
• Routing table modifies itself according to the network changes
Advantages - Network traffic is minimized - Low latency - The best route will be selected most

Disadvantages - Router memory need to keep a routing table

Host Specific Routing

Each router keeps one record/entry for each
• Table entry has Host IP and the Interface

Disadvantages • Large number of records •Table updating is difficult and complex
Network Specific Routing

One record for one network) • Table entry has Network address and Interface

Advantages • Number of records are limited (Table updates are not for each host but for a network) •Update is easy
Static routing

Router (config) #ip route <destination network><desti. Network subnet mask><next hop address | exit interface | Both>

Default routing

B (config) #

B (config) #ip route 0.0.0.0 0.0.0.0 172.16.2.2

RIP

Router (config) #router rip
Router (config-router) #network<net address>

RIP V2

Router (config) #router rip
Router (config) #version 2

No auto-summary

Router (config-router) #network <net-address> (Directly connected)

EIGRP

Router (config) #router Eigrp AS
Router (config-router) #network<net- address>

Switch

Based on physical factor

1. Fixed config (Can't modify phy.)

2. Modular config (Ports can add or remove)

3. Stackable config (Sw connected. Kept one on other, Daisy wheel cabling stru.)

Business Considerations On Selecting switches • Cost • Speed and #of Interfaces

• Port Density • Power • Power access points, • 24/7 Continues access • Port Speed • Ethernet, Fast Ethernet, Gigabit Ethernet • Scalability • Network growth

Switch Functions

•Address learning (MAC address table)

• Forward/filter decisions(only forwarded out the specified destination port)

• Loop avoidance((STP is used to stop network)

Configuring Basic Switch Management Access with IPv4

S1#configure terminal
S1 (config) # interface vlan 99
S1 (config-if) # ip address 172.17.99.11 255.255.255.0
S1 (config-if) # no shutdown
S1 (config-if) # exit
S1 (config) # ip default-gateway 172.17.99.1
S1 (config) # end
S1# copy running-config startup-config

•Dynamic MAC addresses –MAC Add. Added dynamically

• Sticky MAC addresses –Learned dynamically & can save permanently
•Permanent MAC addresses –Manually assign specific port that unchanged

Permanent MAC addresses

Port Security-Limits #of valid MAC Addr.on a switch port (More Secure)
Restrict port 0/1 so that only 3 MAC addresses can be learned on port 0/1

Switch (config) #interface Ethernet 0/1
Switch (config-if) # switchport port-security maximum 3(default 1)

Port Security do in 2 modes

*Access Mode- End device Connection

Switch# interface E0/4
Switch (config-if) #switchport mode access
Switch (config-if) #switchport port-security
Switch (config-if) #switchport port-security mac-address 0200.1111.1111

*Disable Unused Ports using **shutdown**
*Use show **port-security interface** to verify max # MAC addresses

VLAN

*Trunk Mode- Connect Switch

S1# Configuration terminal
S1 (config) # interface FastEthernet0/1
S1 (config-if) # switchport mode trunk
S1 (config-if) # switchport trunk allowed vlan 10,20,30,99
S1 (config-if) # end

No switchport allowed vlan<vlan list> (**Disable**)
No switchport allowed native vlan (Default)

Inter-VLAN Routing Using Routers

S1 (config) # vlan 10
S1 (config-vlan) # vlan 30
S1 (config-vlan) # interface f0/5
S1 (config-if) # switchport mode trunk
S1 (config-if) # end
R1 (config) # interface g0/0.10(subintfce)
R1 (config-subif) # encapsulation dot1q 10
R1 (config-subif) # ip address 172.17.10.1 255.255.255.0
R1 (config-subif) #exit
S1 (config) # interfaceg0/0
S1 (config) # no shutdown
S1# config t
S1 (config) # vlan 10
S1 (config-vlan) # name student
S1 (config-vlan) # end
S1 (config) # interface f0/18
S1 (config-if) # switchport mode access
S1 (config-if) # switchport access vlan 20
S1 (config-if) # end

Configure Router-on-a-Stick: Switch
Configure Router-on-a-Stick: Router
Creating VLAN
Assigning ports