Cloud Infrastructure Week#5

Emrah Mutlu

January 2024

AGENDA – WEEK#5

- Traditional Network
  - Today’s Network
  - OSI Reference Model & Encapsulation
  - Switches & L2 problems & ARP and types
  - TCP/IP & Transport Layer
  - IPv4 Addressing
  - VLANs and Trunks
  - Redundancy & HA (High-Availability) Solutions
  - Routing Protocols

Proprietary and Confidential

GENEL- PUBLIC

Orion Innovation

Today’s Network

Communication is almost as important to us as our reliance on air, water, food, and shelter. In today's world, with networks, we are connected like never before.

END DEVICES:

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.

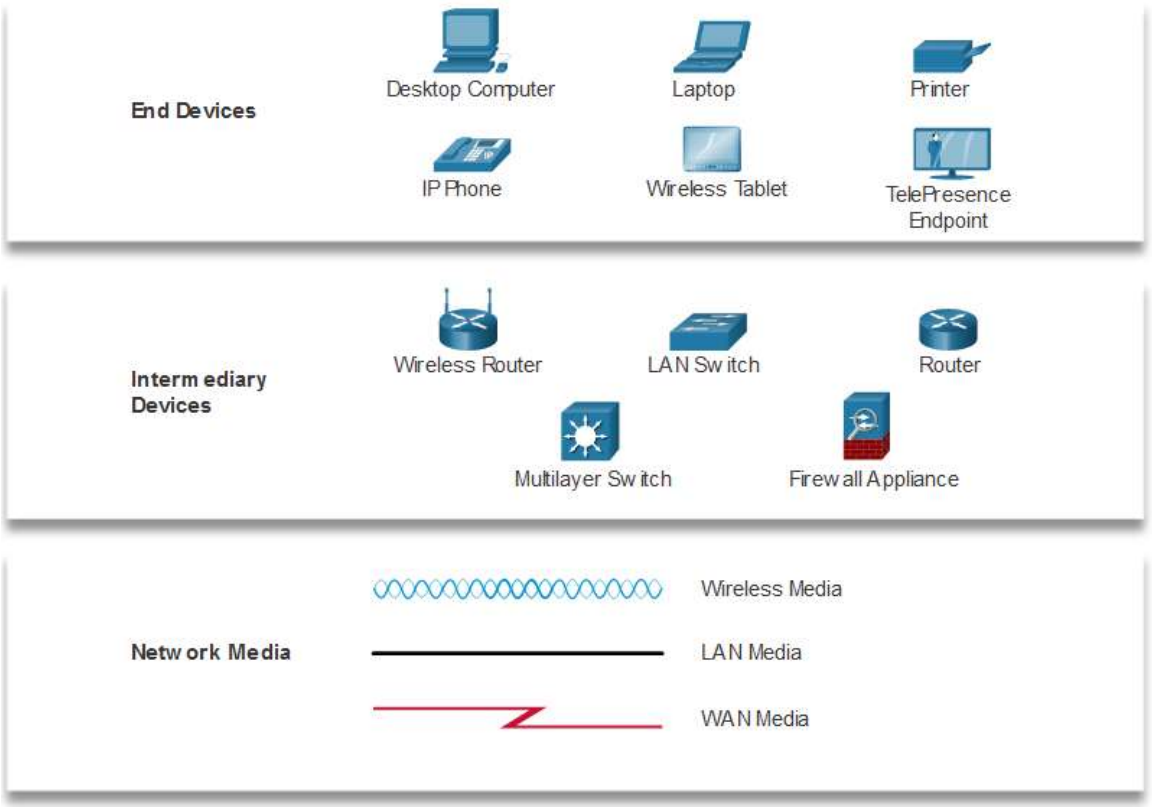
INTERMEDIARY NETWORK DEVICES:

An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.
Management of data as it flows through a network is also the role of an intermediary device, including:

- Regenerate and retransmit data signals.
- Maintain information about what pathways exist in the network.
- Notify other devices of errors and communication failures.

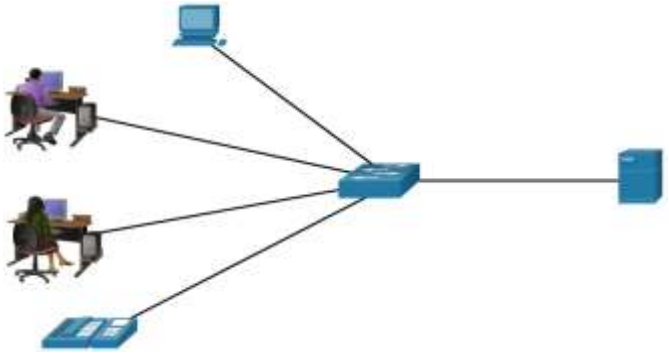
NETWORK MEDIA:

Communication across a network is carried through a medium which allows a message to travel from source to destination.

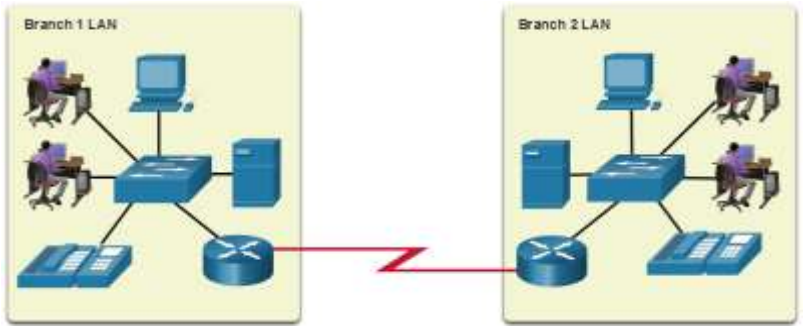


GENEL- PUBLIC

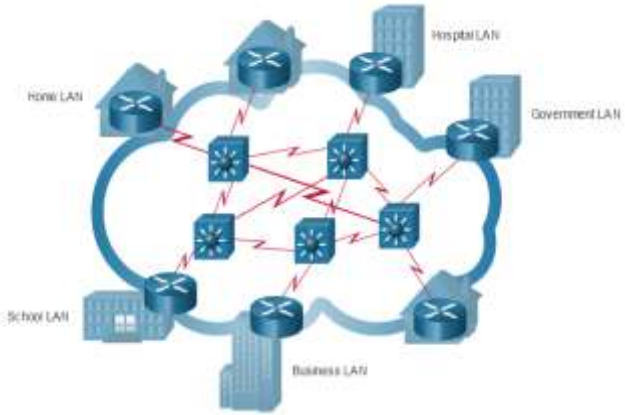
A **LAN** is a network infrastructure that spans a small geographical area.



A **WAN** is a network infrastructure that spans a wide geographical area.



The **internet** is a worldwide collection of interconnected LANs and WANs.



LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by one or more service providers.
Provide high-speed bandwidth to internal devices.	Typically provide slower speed links between LANs.

- What is the demarcation point?
- What is intranet, extranet and internet?

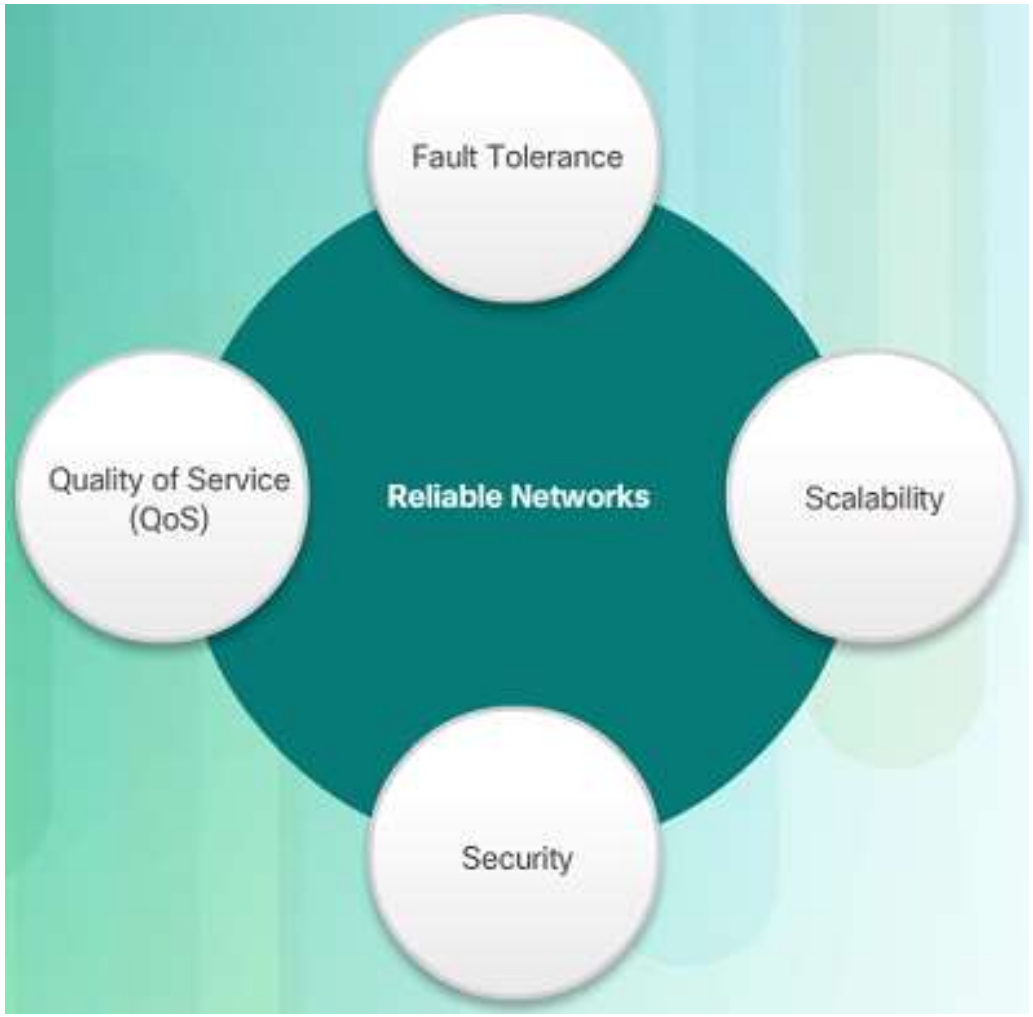
•**LANs** are connected to each other using WANs.
•**WANs** may use copper wires, fiber optic cables, and wireless transmissions.
The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:

- IETF
- ICANN
- IAB

Proprietary and Confidential
• GENEL- PUBLIC

NETWORK ARCHITECTURE: COMMON TERMS

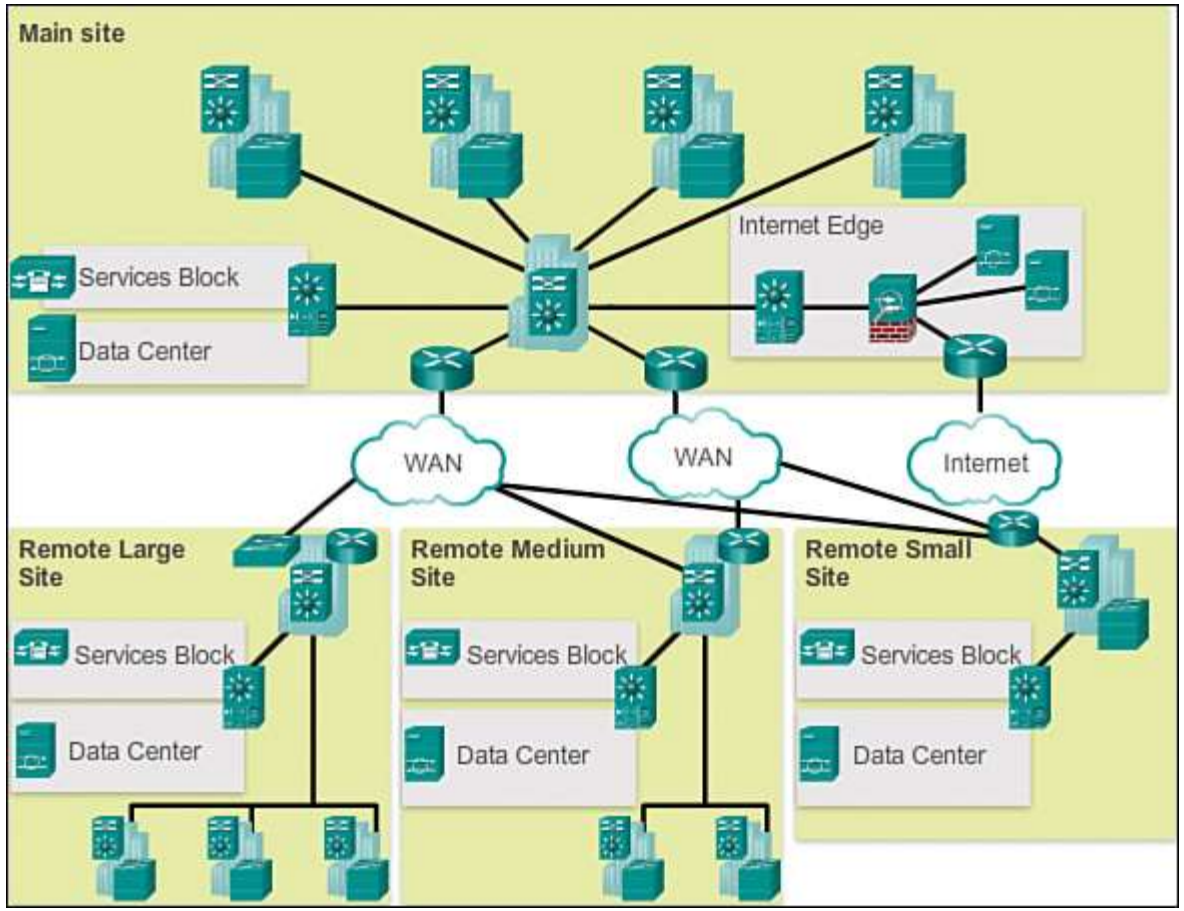
- **Fault Tolerance:** A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Redundancy is used for Fault-tolerant networks.
    - What is a single point of failure and what are the redundancy types?
- **Scalability:** A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users. Similarly, it needs to be shrunk when needed.
- **QoS:** Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
    - What are the packets in the network and how they are prioritized with QoS?
- **Network Security:** Huge concept, ideally, there are common terms in Network to secure the device physically and the data with encryption / network security devices.
    - What is encryption?
    - What are network security devices?

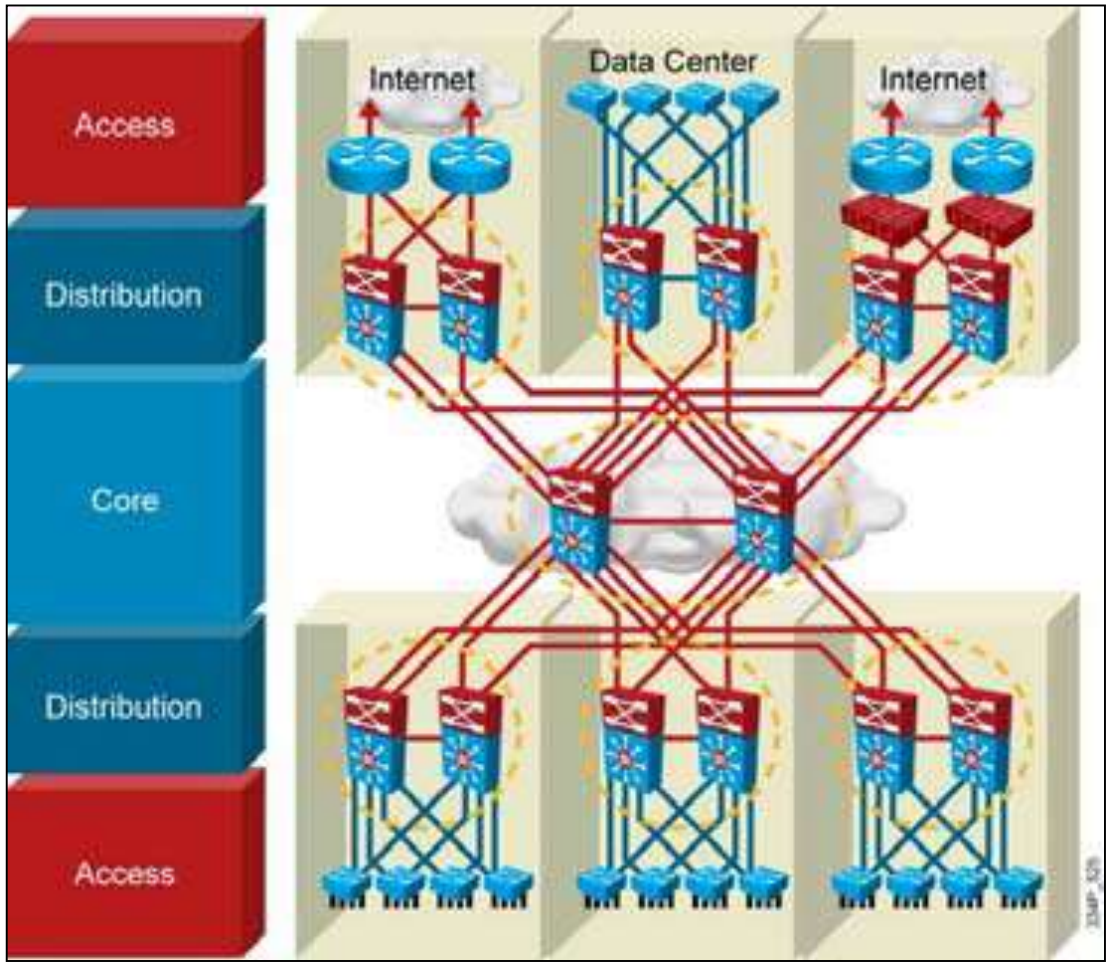


Proprietary and Confidential

GENEL- PUBLIC

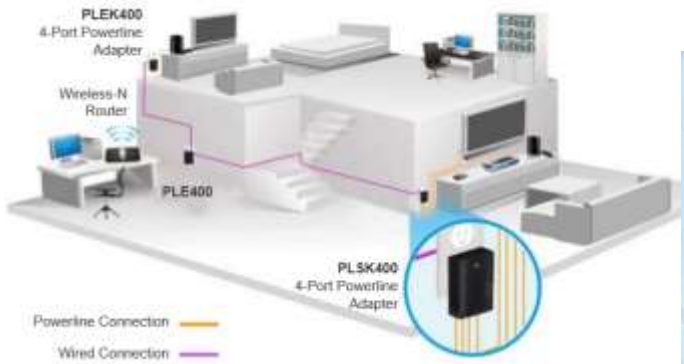
NETWORK ARCHITECTURE: HIERARCHICAL NETWORK MODEL





• GENEL- PUBLIC

- BYOD (Bring-Your-Own-Device)
- Online Collaboration
- Video Communication
- Cloud Computing
- Smart Home Technologies
- Powerline Networking
- Wireless Broadband Service



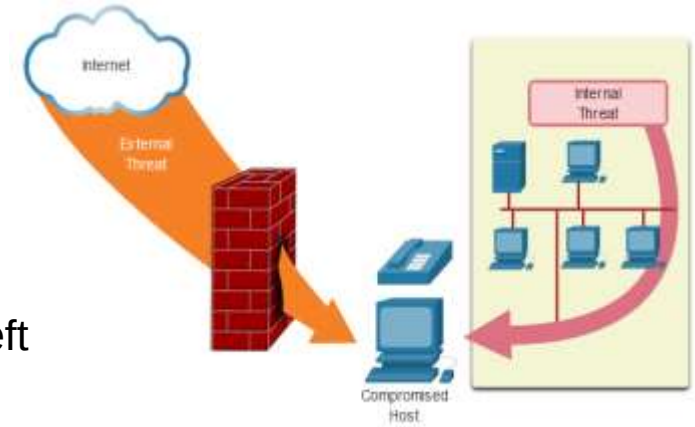
Proprietary and Confidential

GENEL- PUBLIC

Threats:

External Threats:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft



Internal Threats:

- lost or stolen devices
- accidental misuse by employees
- malicious employees

Solutions:

- Defense Strategies
  - Physical Security
  - Device Security
  - Network Security
  - Access Control
  - Permission Control
  - Encryption (Data)

- Antivirus / Antimalware / Antispyware
- Patching / Upgrades
- Firewall / ACLs (Access Control Lists)
- IDS & IPS Devices
- Proxies (DDoS Protection)
- VPNs (Virtual Private Networks)

Proprietary and Confidential

GENEL- PUBLIC

Orion Innovation

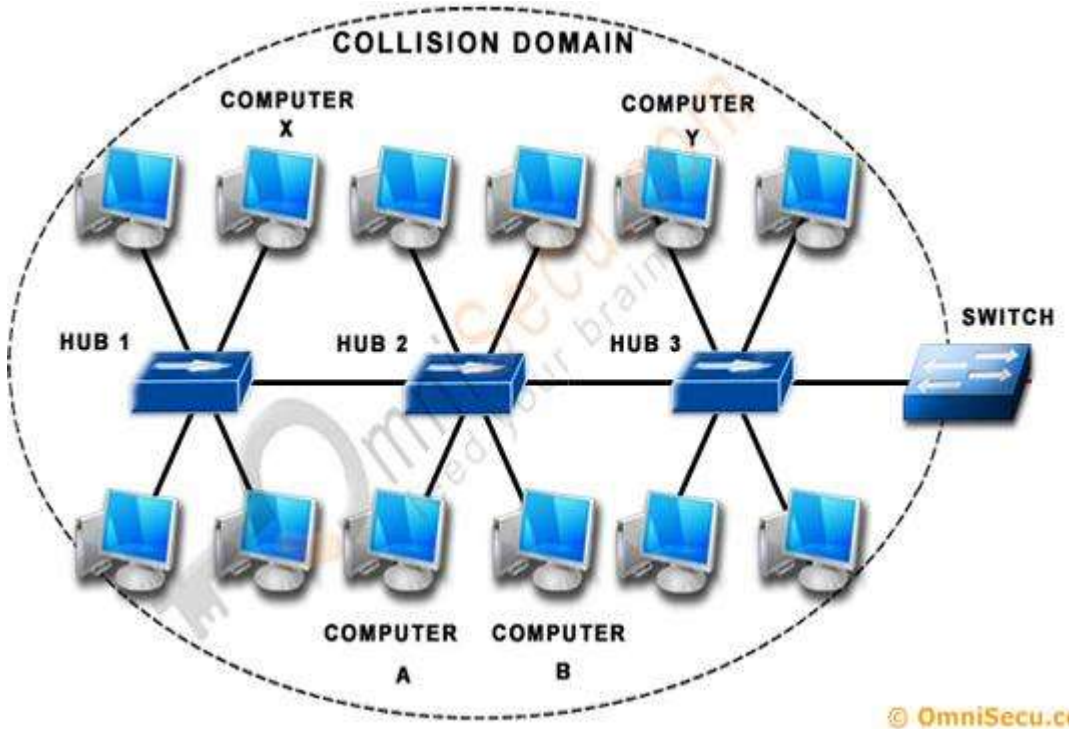
OSI Reference Model

COLLISION AND BROADCAST DOMAIN

A collision domain is a section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters, in particular, when using early versions of Ethernet.

- *A network collision occurs when more than one device attempts to send a packet on a network segment at the same time.*

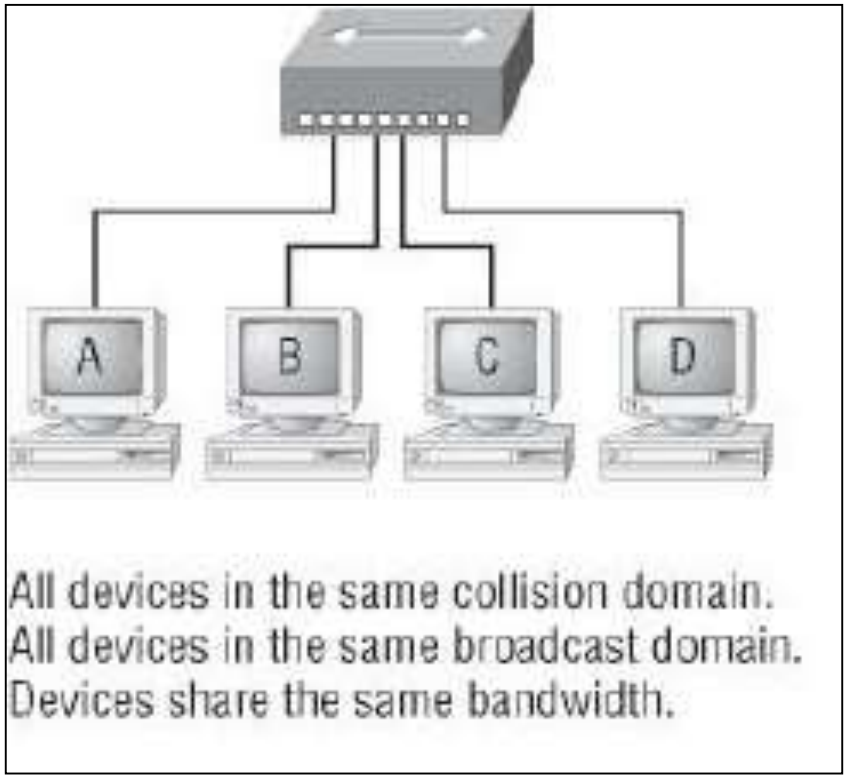
A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment, or it can be bridged to other LAN segments.



GENEL- PUBLIC

Jobs: Sends and receive ***bits***, provides connectivity
Devices: Hub, Repeater, Cable, Connectors (RJ-45, DB-9, etc)
The term Bandwidth is the capacity at which a medium can carry data.

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	Kbps	1 Kbps = 1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = 1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps – 1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = 1,000,000,000,000 bps = 10^{12} bps



Proprietary and Confidential

• GENEL- PUBLIC

Jobs:

Provides unique MAC address

Take bits and encapsulate a ***frame***

Devices: Switch, Bridge

Protocols:

LAN: IEEE's 802.2, 802.3, 802.5; ANSI's FDDI

WAN: ATM, FR (Frame-Relay), PPP, HDLC, SDLC, X.25

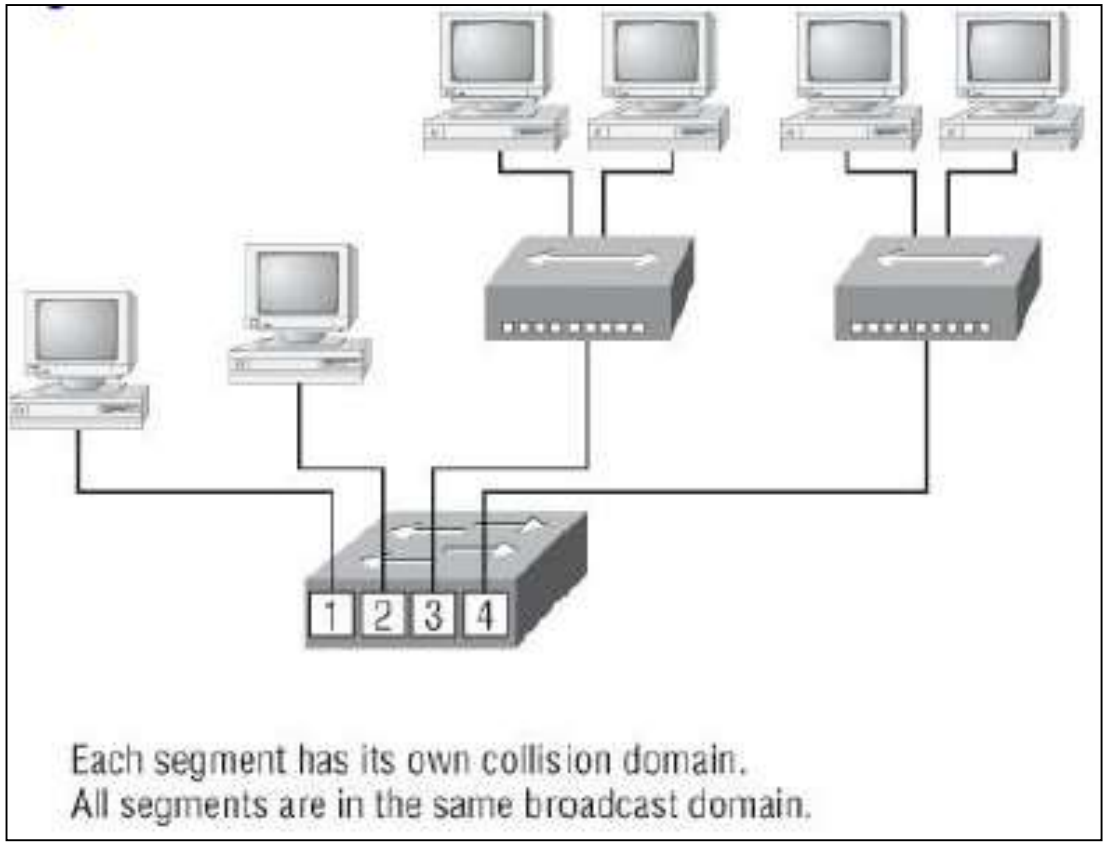
Address Types:

Broadcast: Every device on a segment

Multicast: A group of devices on a segment

Unicast: A single device on a segment

Troubleshoot: ARP, Address Tables, Protocol Analyzers



Proprietary and Confidential

GENEL- PUBLIC

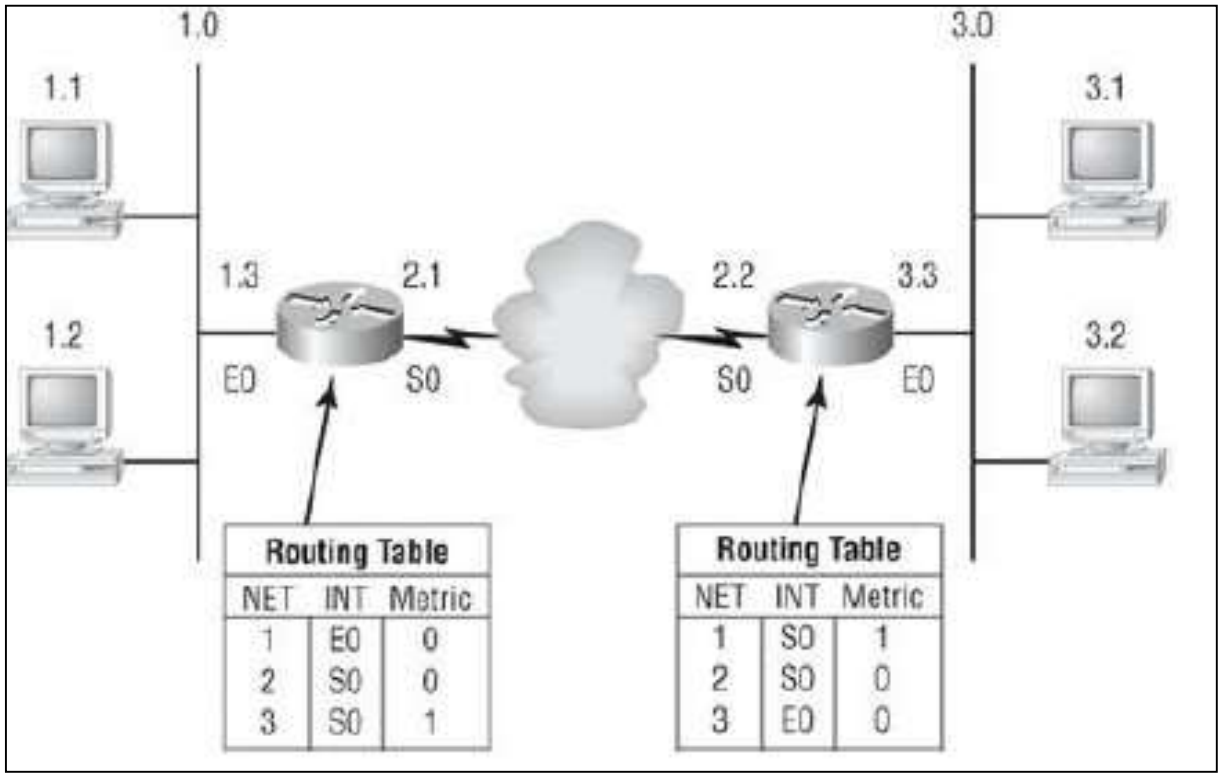
Jobs:

- Encapsulates a ***packet***
- Defines IP Addresses
- Find paths to destinations
- Creates broadcast domains
- Provides QoS, ACL, Encryption
- Connects different data link types together

Devices: Router, L3 Switch

Protocols: TCP/IP, IPX, AppleTalk

Troubleshoot: Traceroute, ping, ARP, Routing Table, Sniffing

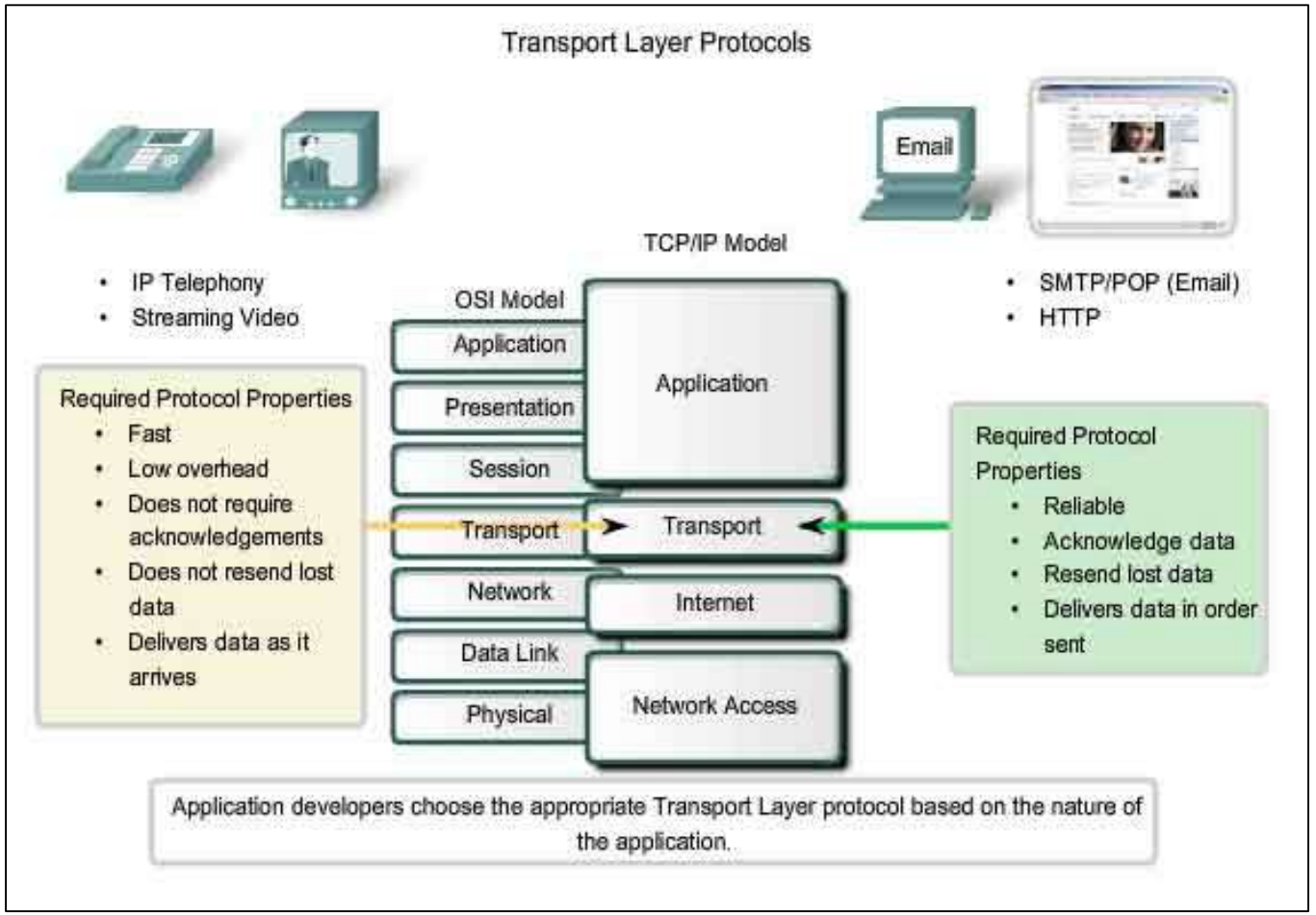


Jobs:

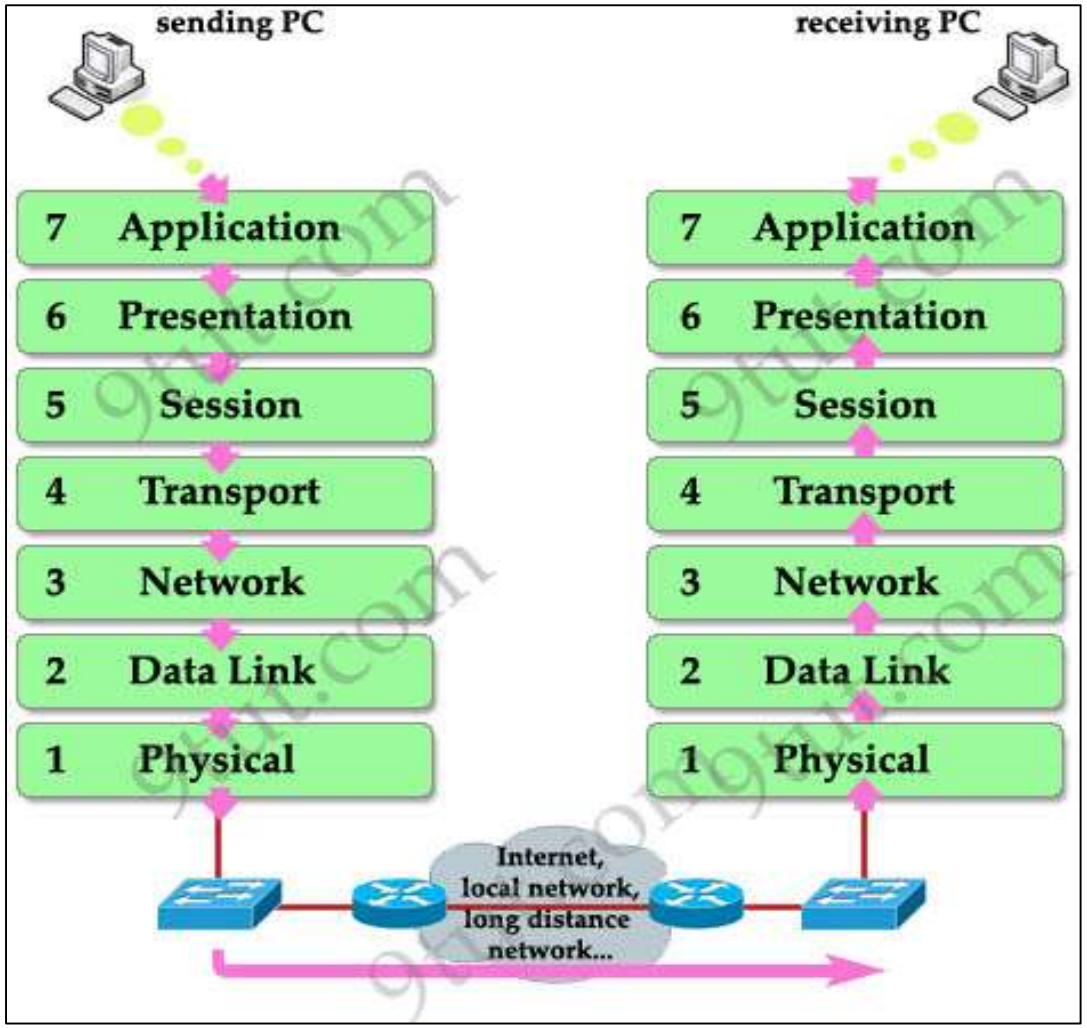
- Encapsulates a ***segment***
- Connection management (setup / tear down)
- Reliable / unreliable delivery of data
- Flow control (buffering, windowing, congestion avoidance)
- Multiplexing

Devices: Firewall, Multilayer Switch

Protocols: TCP, UDP



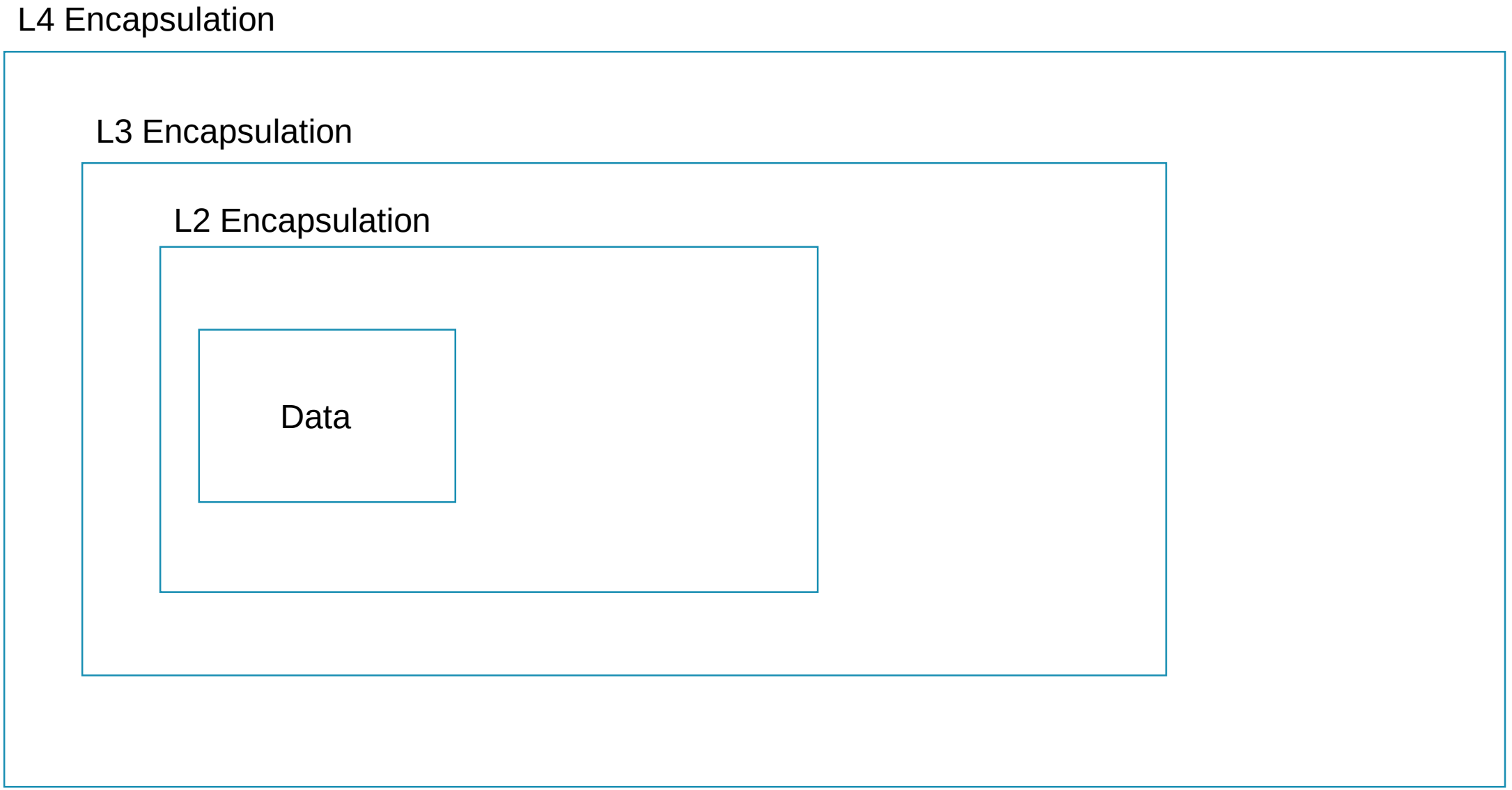
OSI REFERENCE MODEL AS A WHOLE



Application	• File, print, message, database, and application services
Presentation	• Data encryption, compression, and translation services
Session	• Dialog control
Transport	• End-to-end connection
Network	• Routing
Data Link	• Framing
Physical	• Physical topology

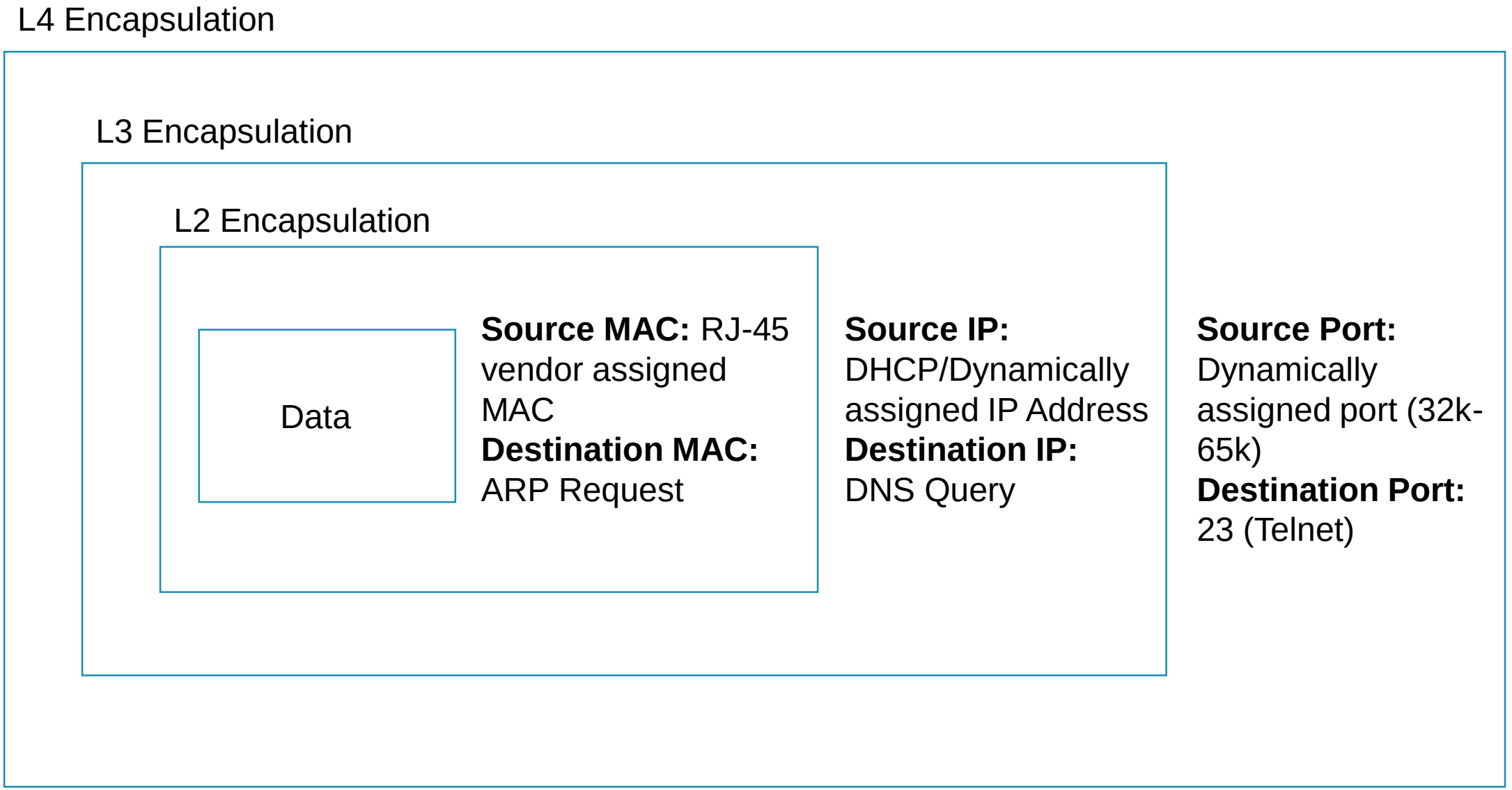
Proprietary and Confidential

• GENEL- PUBLIC



Proprietary and Confidential

GENEL- PUBLIC



Proprietary and Confidential

GENEL- PUBLIC

Orion Innovation

Switches & L2 Problems

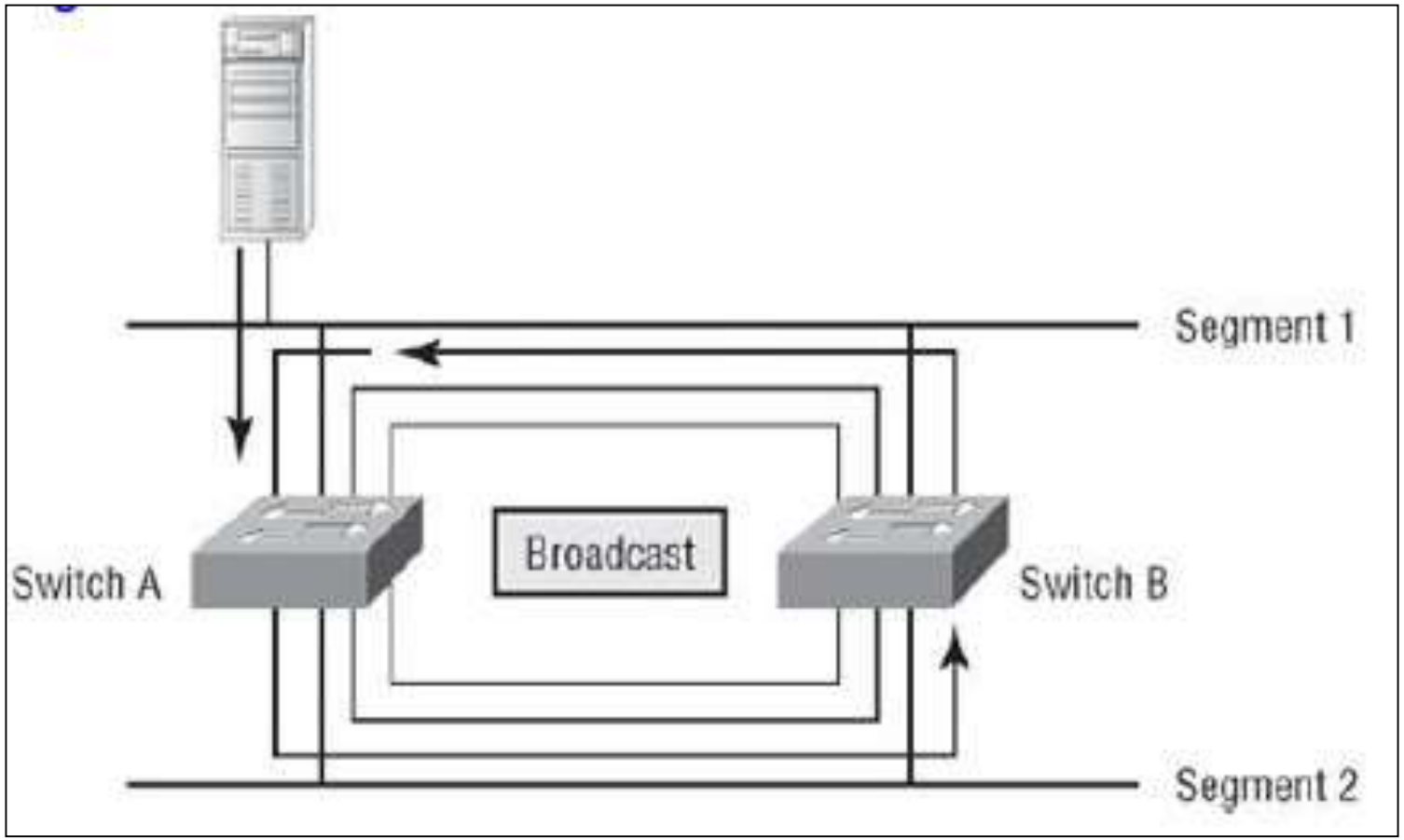
Uses (ASICs – Application Specific Integrated Circuits) **hardware switching** (Max. Speed 400M fps)
Supports **full-duplex**
Switching Methods are;

- Store and Forward: Put entire frame to buffer, check FCS via CRC, if passes forward, otherwise drop
- Cut-Through: Read first 14-bytes and start forwarding. Faster but may cause collisions
- Fragment-Free: Read first 64-bytes and start forwarding

Uses **STP** to overcome L2 loops

• GENEL- PUBLIC

- L2 loop is the main L2 problem
- The resolution is the STP

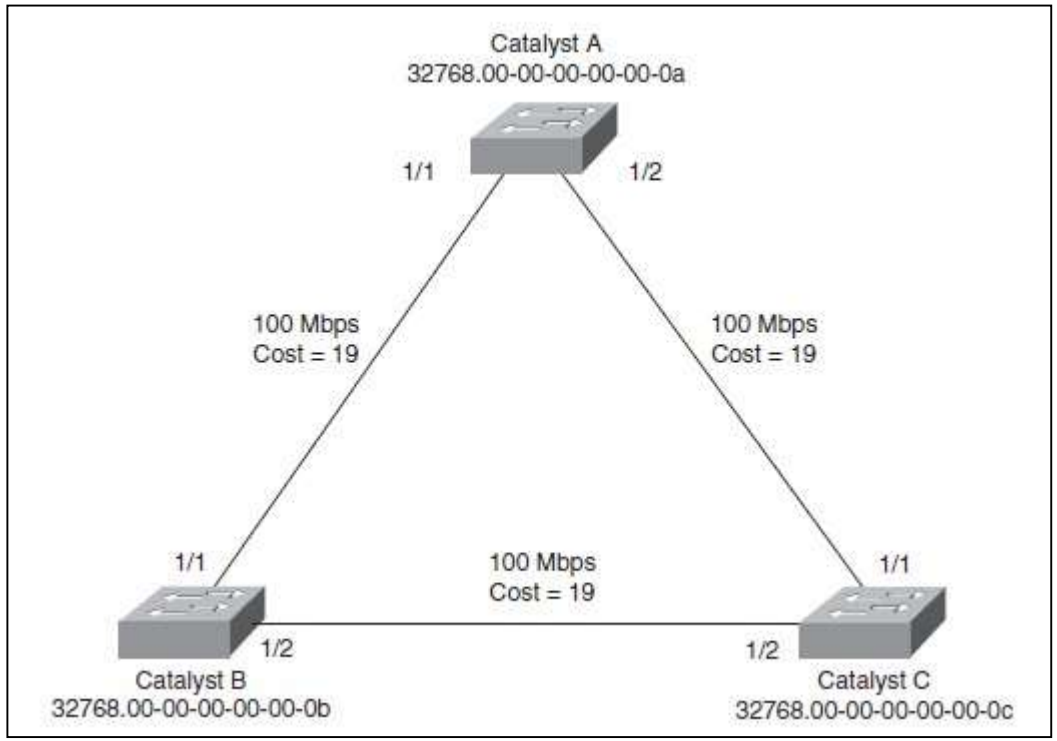


Proprietary and Confidential

GENEL- PUBLIC

STP is a L2 loop prevention method.
Rules;

1. Elect the root bridge (Lowest Priority, if equals, lowest MAC Address)
2. Determine Root bridge's ports as Designated Ports (FWD)
3. Determine Root Ports (FWD); other bridge's the nearest cost'ed ports to the Root Bridge
4. Remind that each segment should have one Designated Port (FWD)
5. Block the non-designated ports in each segment to prevent L2 loops



Link Bandwidth	Old STP Cost	New STP Cost
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

Proprietary and Confidential

• GENEL- PUBLIC

STP PORT STATES

- CST or Common STP (IEEE 802.1d) has 50 secs convergence time, which is not acceptable in today's networks. BPDU Hello Timer = 2secs.
- During calculation of the STP, all ports are disabled and the following port states are observed.
- If ports are access ports, then PortFast feature should be used for faster convergence.
- Only the root bridge can send the topology change information.

STP State	The Port Can...	The Port Cannot...	Duration
Disabled	N/A	Send or receive data	N/A
Blocking	Receive BPDUs	Send or receive data or learn MAC addresses	Indefinite if loop has been detected
Listening	Send and receive BPDUs	Send or receive data or learn MAC addresses	Forward Delay timer (15 seconds)
Learning	Send and receive BPDUs and learn MAC addresses	Send or receive data	Forward Delay timer (15 seconds)
Forwarding	Send and receive BPDUs, learn MAC addresses, and send and receive data		Indefinite as long as port is up and loop is not detected

Proprietary and Confidential

• GENEL- PUBLIC

STP ENHANCEMENTS; RSTP

Since STP convergence time is too long, new technologies are implemented as RSTP (Rapid STP) and MSTP (Multi-STP) for faster convergence and Per VLAN capabilities.

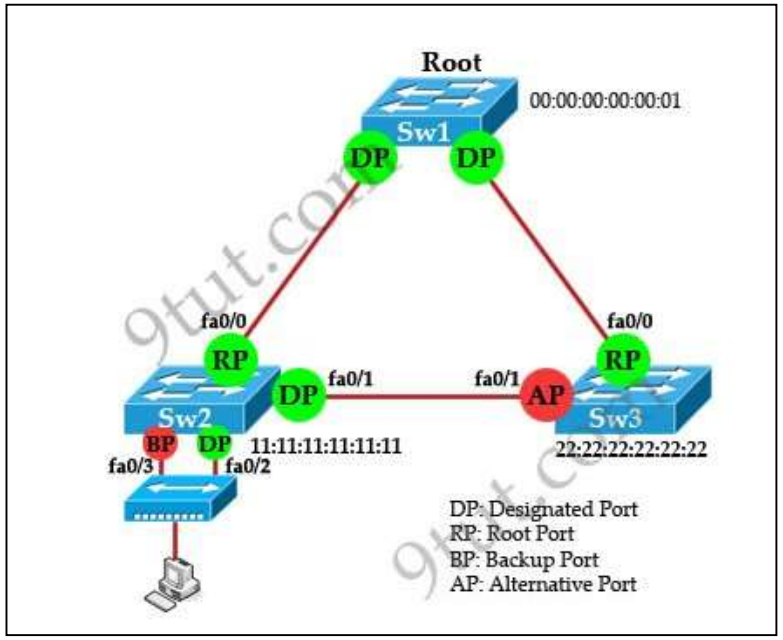
RSTP is an IEEE 802.1w protocol that speeds up the convergence time to 6 seconds only with the following new port states:

Discarding - Incoming frames simply are dropped; no MAC addresses are learned. (This state combines the 802.1D Disabled, Blocking, and Listening states because all three did not effectively forward anything. The Listening state is not needed because RSTP quickly can negotiate a state change without listening for BPDUs first.)

Learning - Incoming frames are dropped, but MAC addresses are learned.

Forwarding - Incoming frames are forwarded according to MAC addresses that have been (and are being) learned.

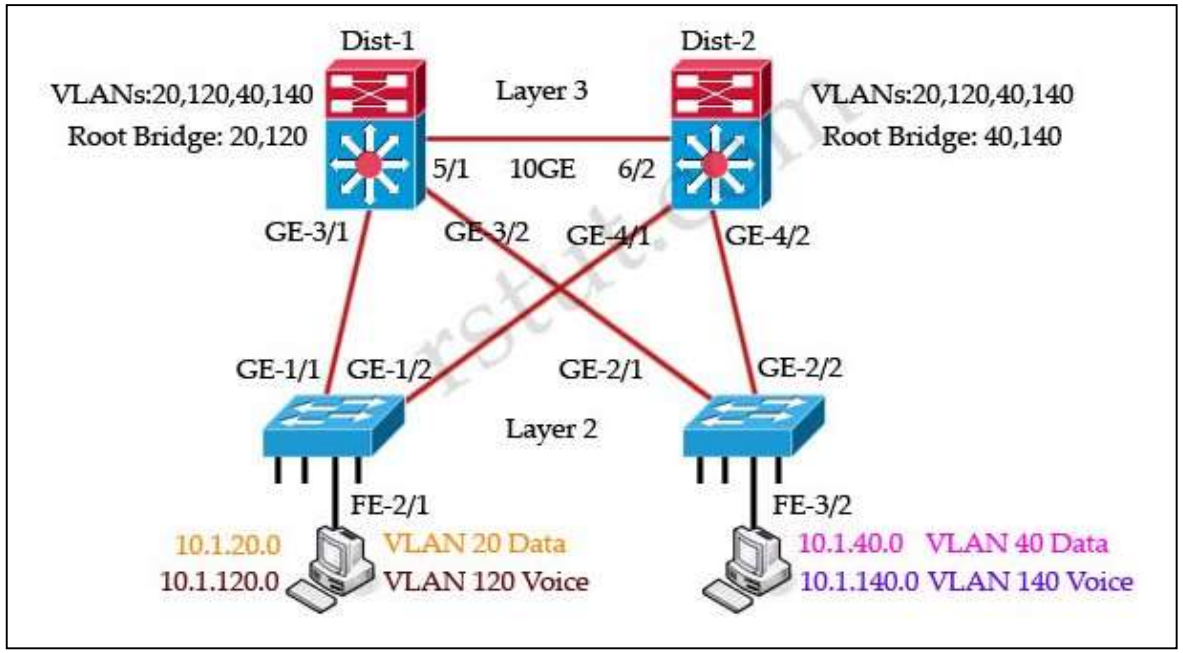
EdgePort term is replaced with PortFast for RSTP. Full-duplex switch-to-switch ports are defined as “Point-to-Point Port”.



• GENEL- PUBLIC

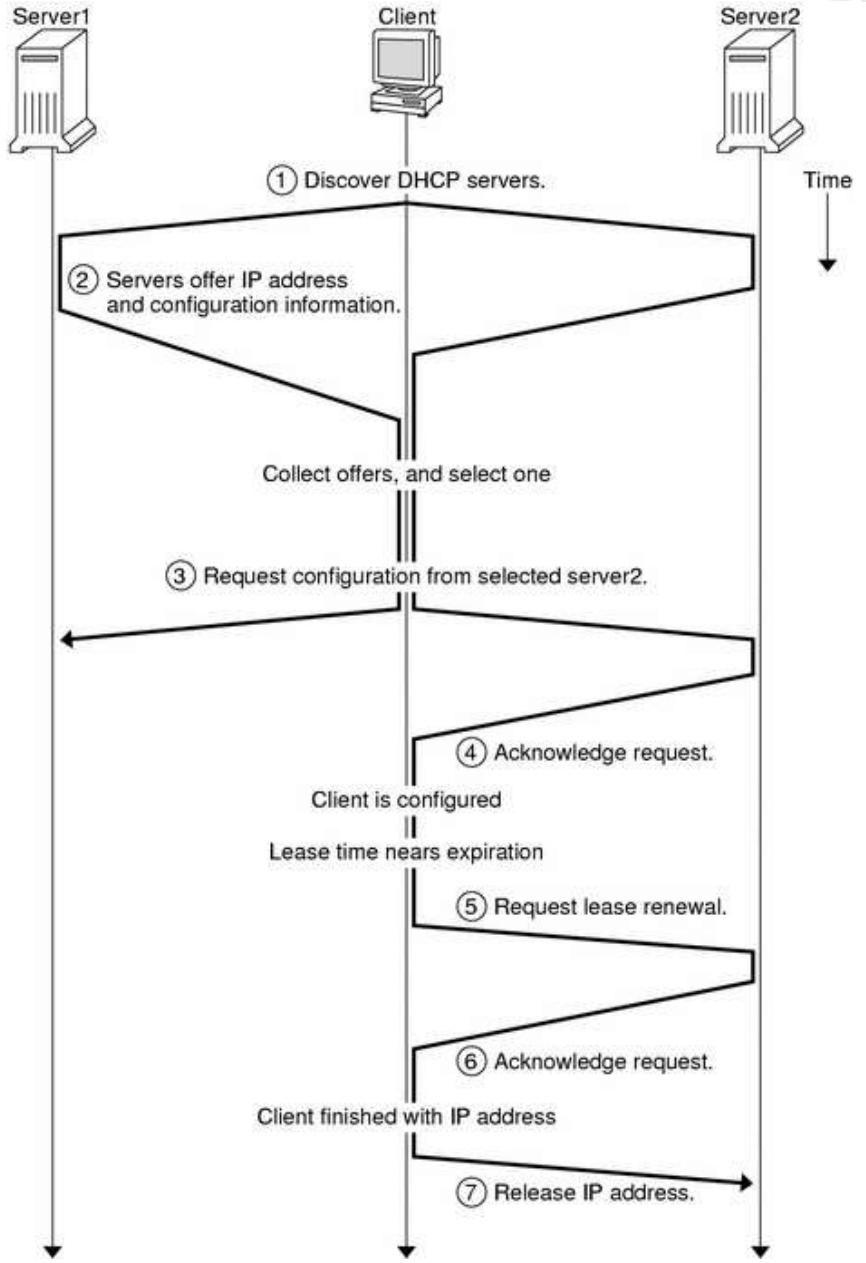
MST (IEEE 802.1s) is built on the concept of mapping one or more VLANs to a single STP instance. Multiple instances of STP can be used (hence the name MST), with each instance supporting a different group of VLANs.
MST is working with regions. If two switches have the same set of attributes, they belong to the same MST region. If not, they belong to two independent regions.

- MST configuration name (32 characters)
- MST configuration revision number (0 to 65535)
- MST instance-to-VLAN mapping table (4096 entries)



DHCP follows the below sequence:

1. Client generates DHCPDISCOVER (multicast)
2. All DHCP Servers send DHCPOFFER (unicast) with the following information;
   - IP Address
   - Subnet Mask
   - Default Gateway IP Address
3. Client accepts the first arrived offer with DHCPREQUEST (DHCPDECLINE)
4. Server responds DHCPACK (DHCPNACK)

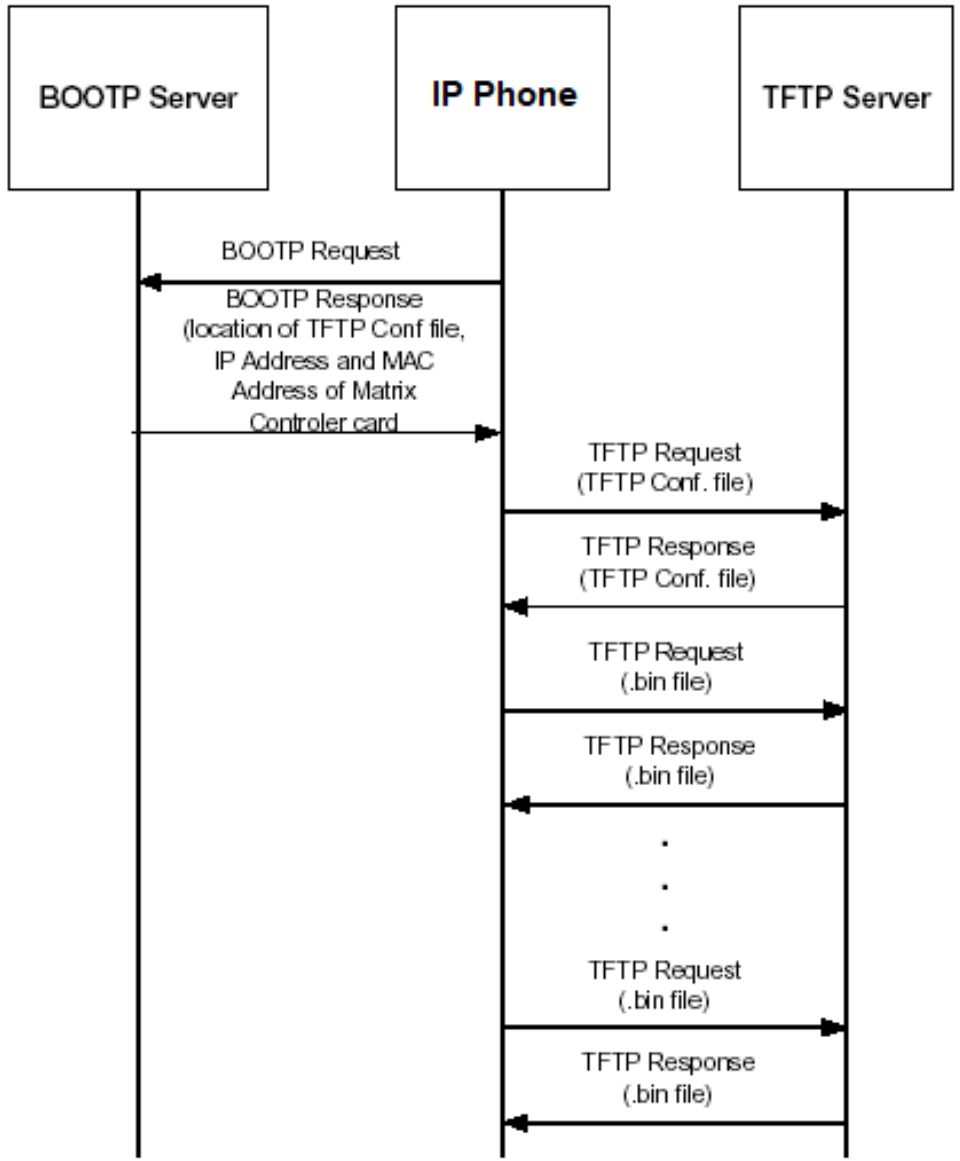


Proprietary and Confidential

GENEL- PUBLIC

BootP follows the below sequence:

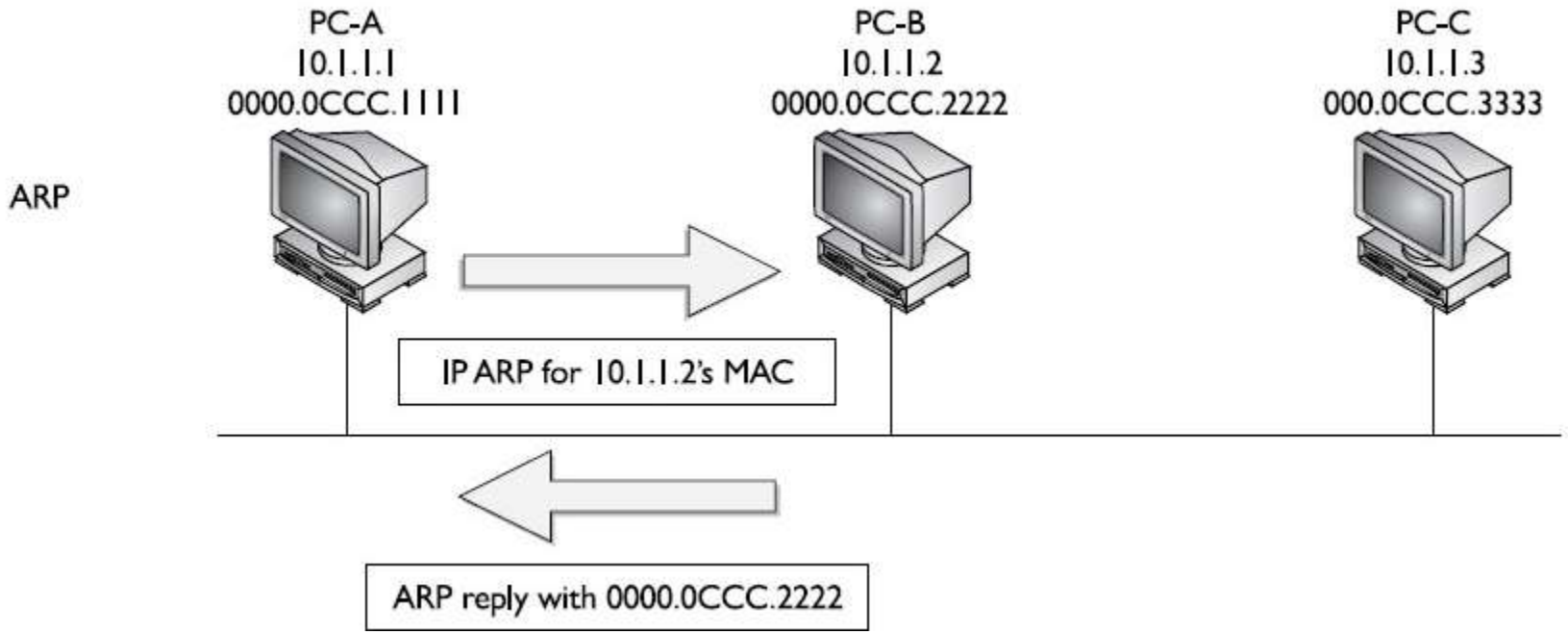
1. Client generates BootP_Request (Source IP: 0.0.0.0, Destination IP: 255.255.255.255, UDP Port: 67)
2. If Client and Server are not in the same subnet, then router performs BootP_Relay task between subnets and increments TTL
3. Server returns BootP_Reply (via ARP, UDP Port: 68) with the following information;
   - IP Address
   - Subnet Mask
   - Default Gateway Address
   - TFTP Server IP Address
   - The load path in the TFTP Server
4. Client requests boot file via TFTP (FTP over UDP)
5. Server provides boot file via TFTP
6. Client install the boot file and starts running



Proprietary and Confidential

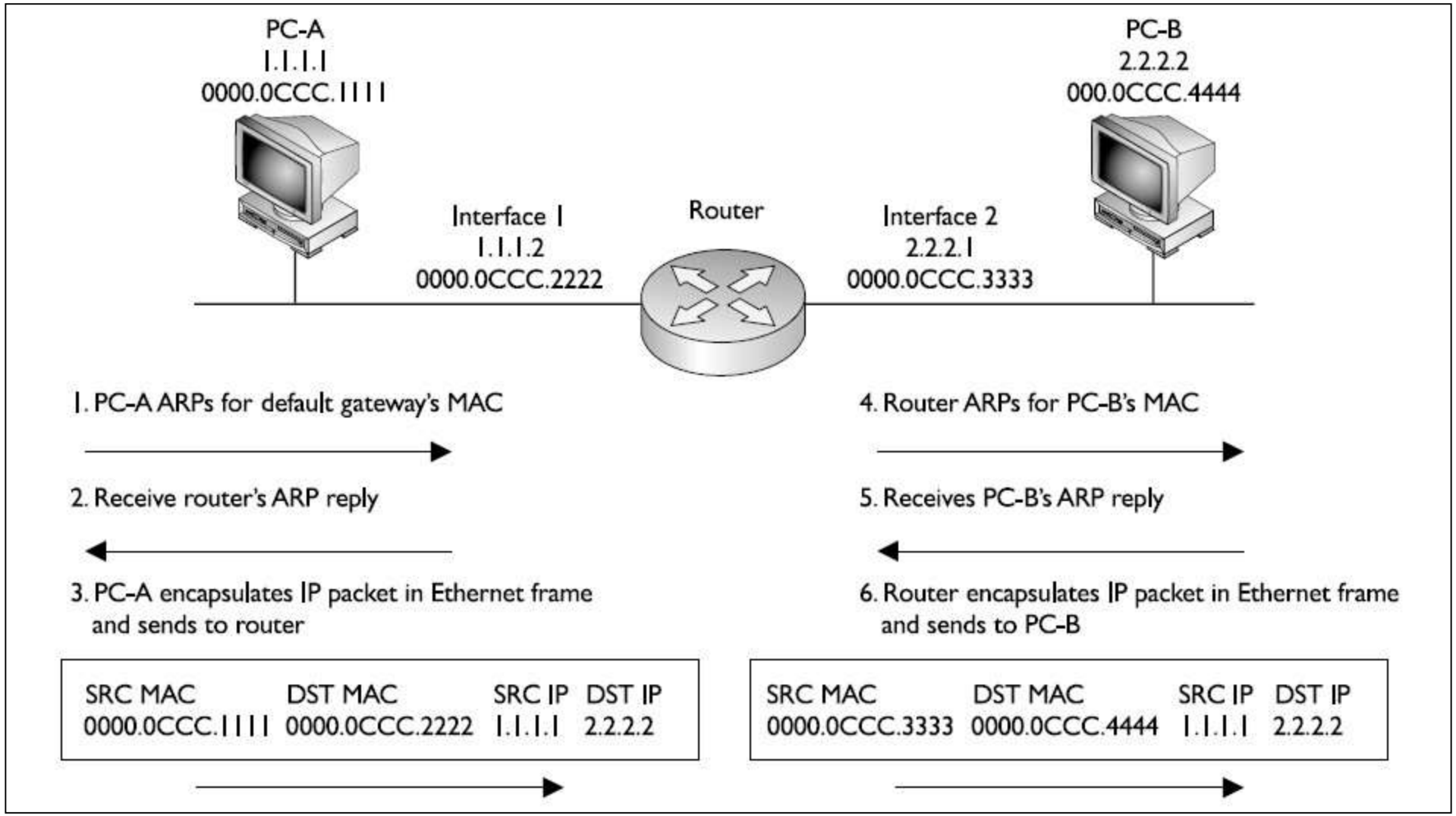
GENEL- PUBLIC

ARP is a Layer-2 protocol, which is used to learn a device's MAC address.



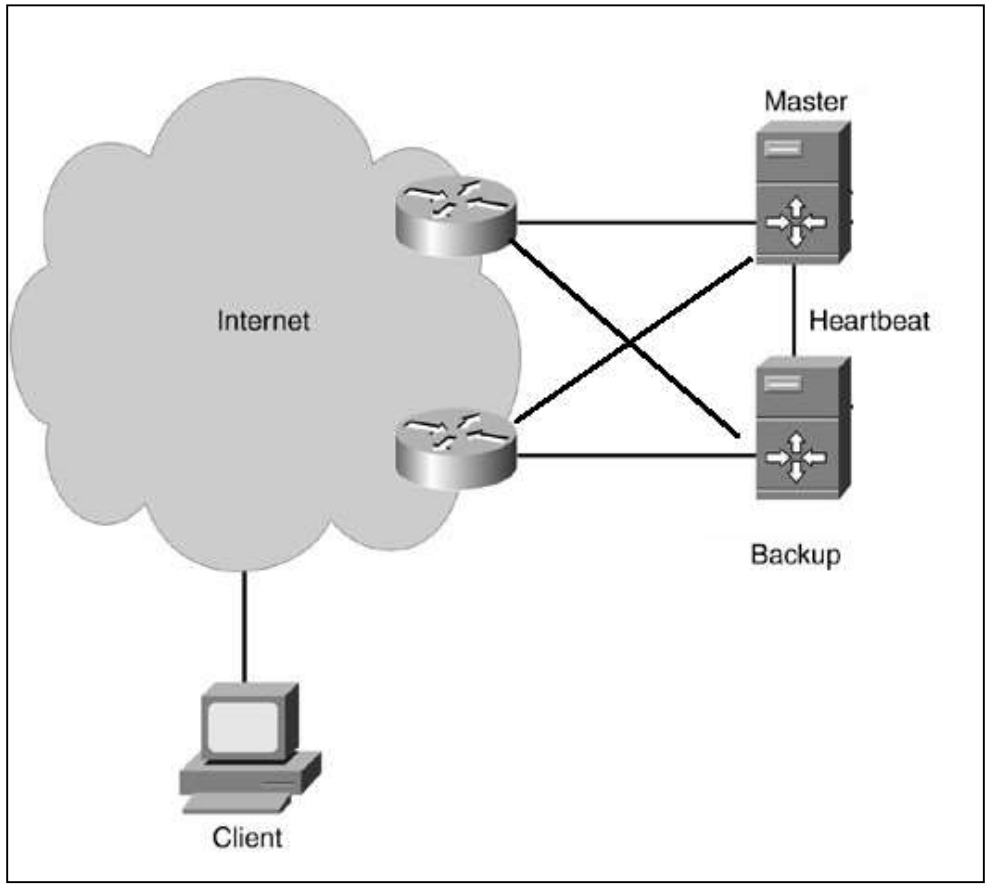
• GENEL- PUBLIC

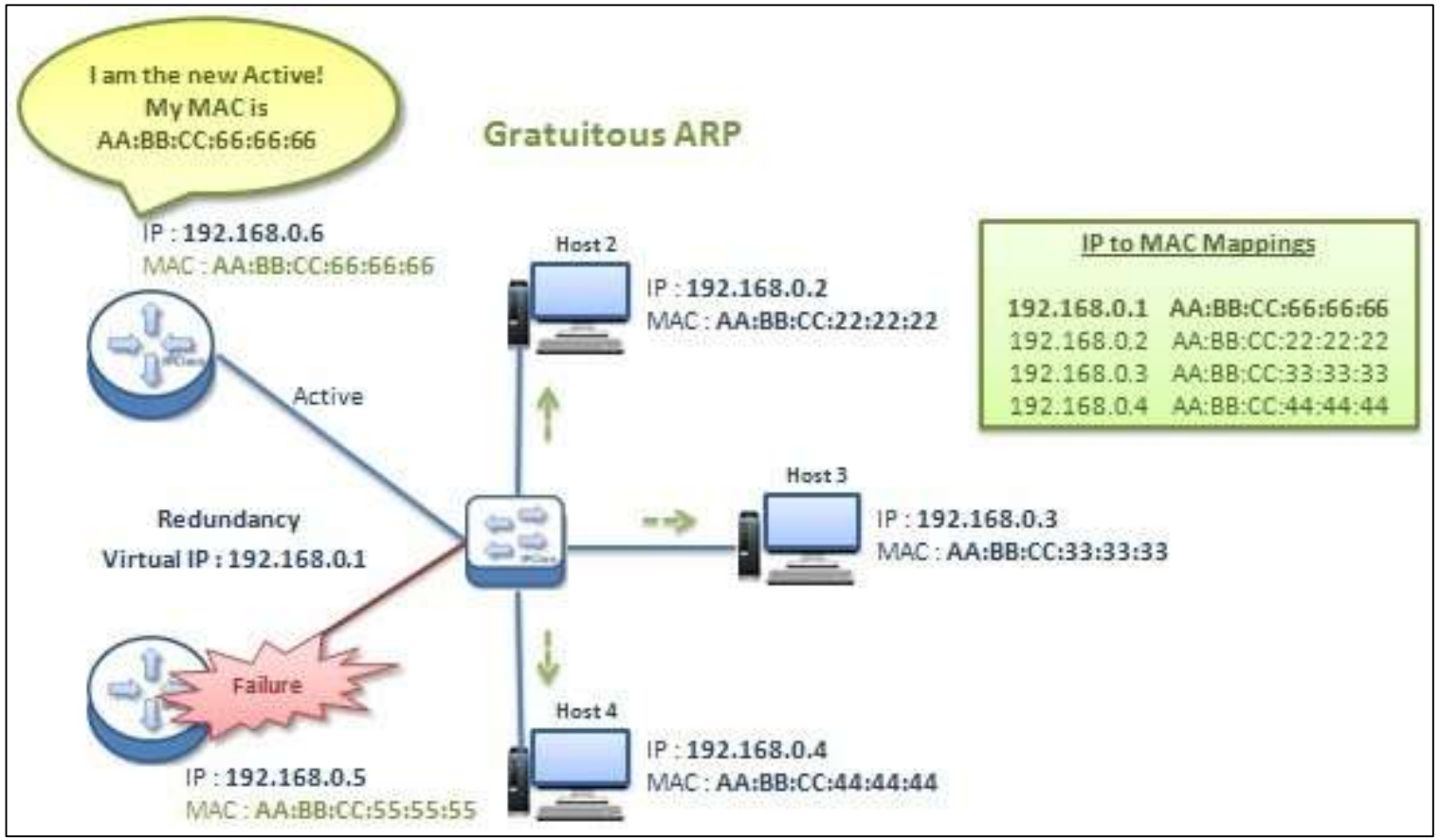
ARP DETAILED



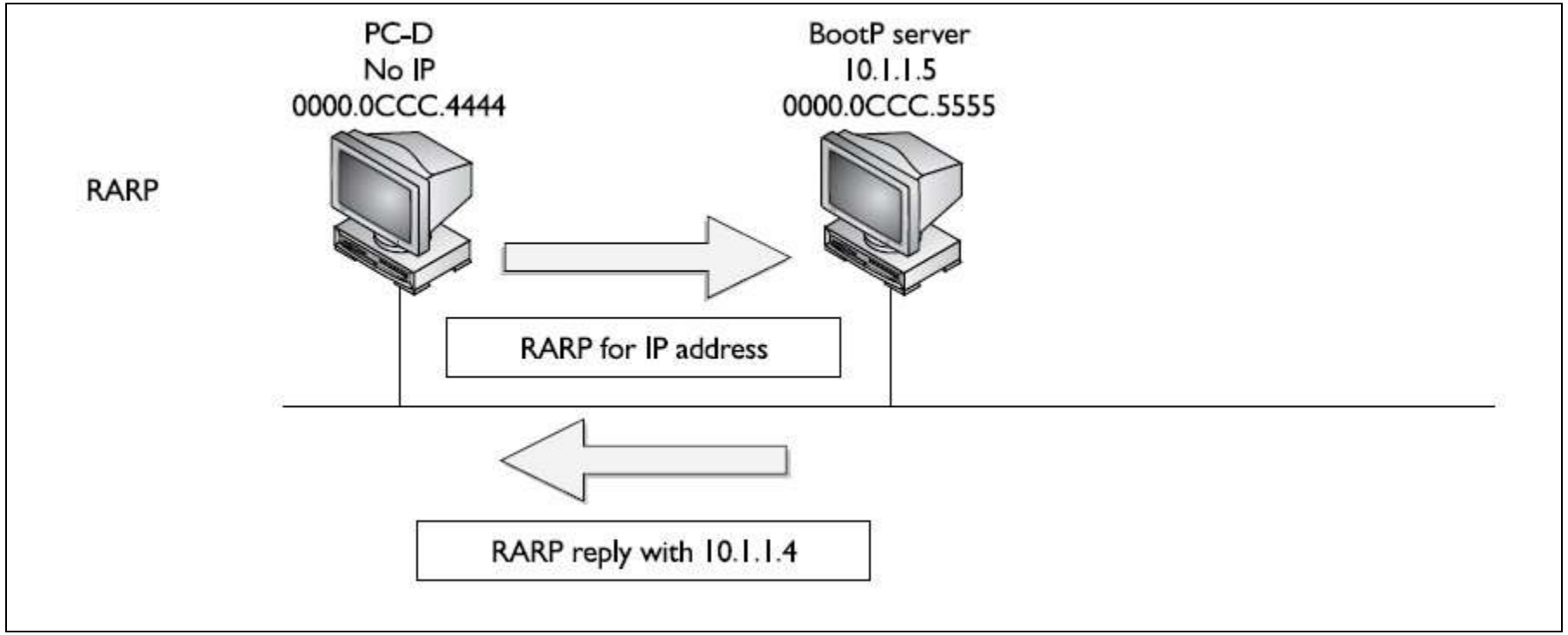
• GENEL- PUBLIC

Gratuitous ARP is a kind of ARP reply without asking of ARP request.





Reverse ARP is used to learn the IP Address during DHCP / BootP operations



GENEL- PUBLIC

ICMP is used to send error and control information between TCP/IP devices at the Internet layer (RFC 792)

Message types; Address Reply, Address Request, Destination Unreachable, Echo, Echo Reply, Information Reply, Information Request, Parameter Problem, Redirect, Subnet Mask Request, Time Exceeded, Timestamp, and Timestamp Reply.

```
C:\Users\emutlu>arp -a

Interface: 10.254.127.20 --- 0x9 - WI-FI
  Internet Address      Physical Address      Type
  10.254.127.1          00-00-0c-07-ac-7f     dynamic
  10.254.127.127        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.254.116.38 --- 0xb -- ETHERNET
  Internet Address      Physical Address      Type
  10.254.116.1          b4-0c-25-e0-40-16     dynamic
  10.254.116.23         30-e1-71-83-ca-b6     dynamic
  10.254.116.24         f8-b4-6a-96-bc-ca     dynamic
  10.254.116.29         48-ba-4e-f7-48-43     dynamic
  10.254.116.35         bc-e9-2f-cc-10-ab     dynamic
  10.254.116.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

```
C:\Users\emutlu>ping ribboncommunications.com
Pinging ribboncommunications.com [23.185.0.4] with 32 bytes of data:
Reply from 23.185.0.4: bytes=32 time=45ms TTL=54
Reply from 23.185.0.4: bytes=32 time=45ms TTL=54
Reply from 23.185.0.4: bytes=32 time=45ms TTL=54
Reply from 23.185.0.4: bytes=32 time=45ms TTL=54

Ping statistics for 23.185.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 45ms, Average = 45ms
```

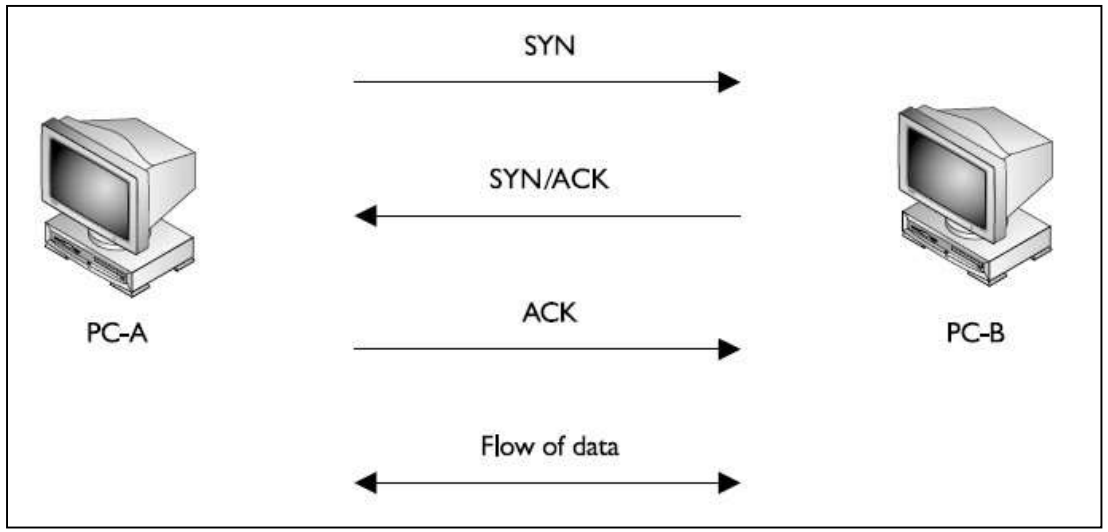
```
C:\Users\emutlu>tracert ribboncommunications.com
Tracing route to ribboncommunications.com [23.185.0.4]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.254.116.1
  2     1 ms     1 ms     1 ms  netasfw.netas.lab.nortel.com
[217.78.96.161]
  3     2 ms     1 ms     1 ms  intrtr1.netas.lab.nortel.com
[217.78.97.1]
  4     3 ms    16 ms     3 ms  host-213-74-185-
149.superonline.net [213.74.185.149]
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
```

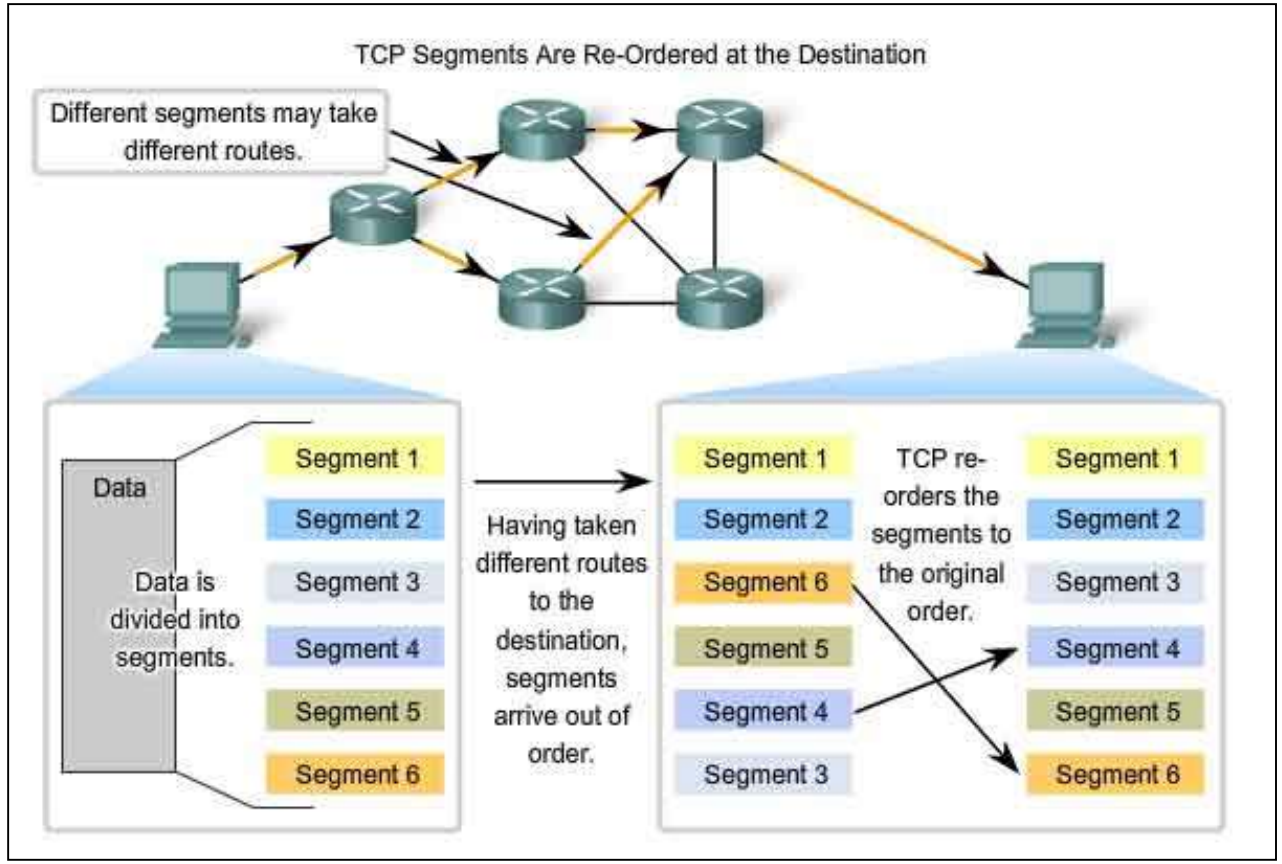
Proprietary and Confidential

Orion Innovation

TCP/IP and Transport Layer

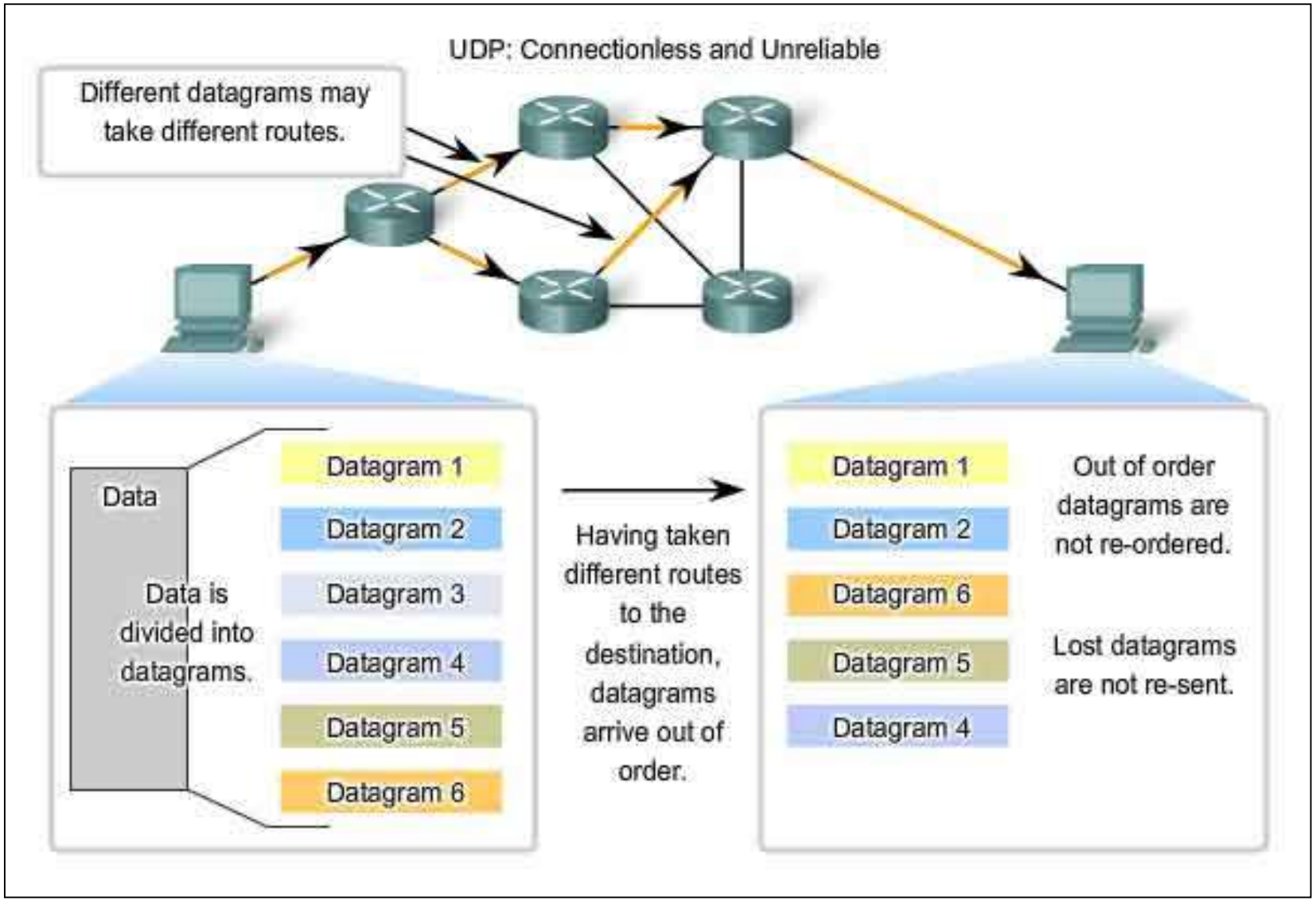
TCP (Transmission Control Protocol) is a connection-oriented, reliable protocol
Applications: FTP, HTTP, Telnet, SSH, SMTP, POP3 for TCP





Proprietary and Confidential
• GENEL- PUBLIC

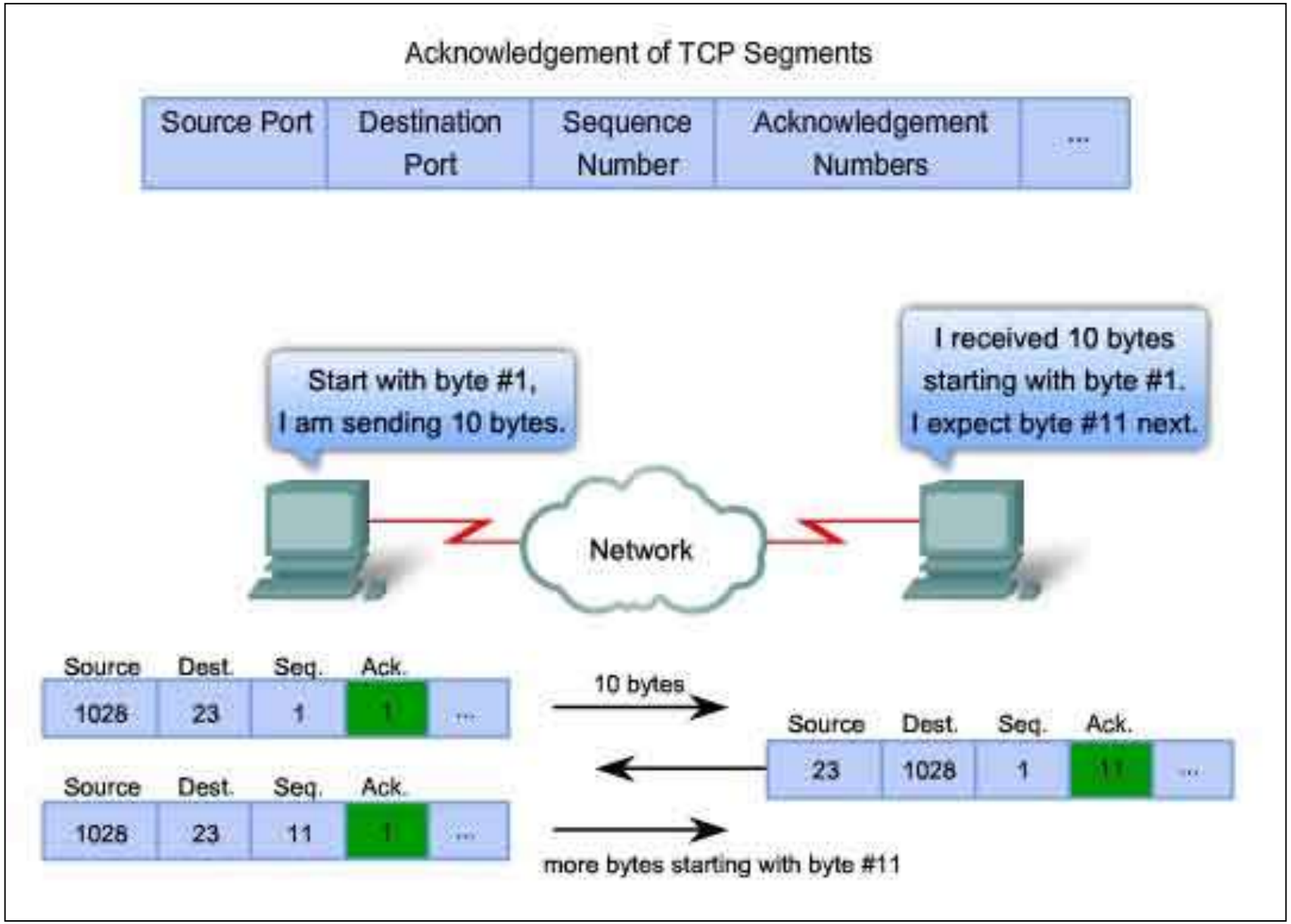
UDP (User Datagram Protocol) is a connectionless, unreliable protocol
Applications: DNS, TFTP, SNMP, RIP for UDP



Proprietary and Confidential

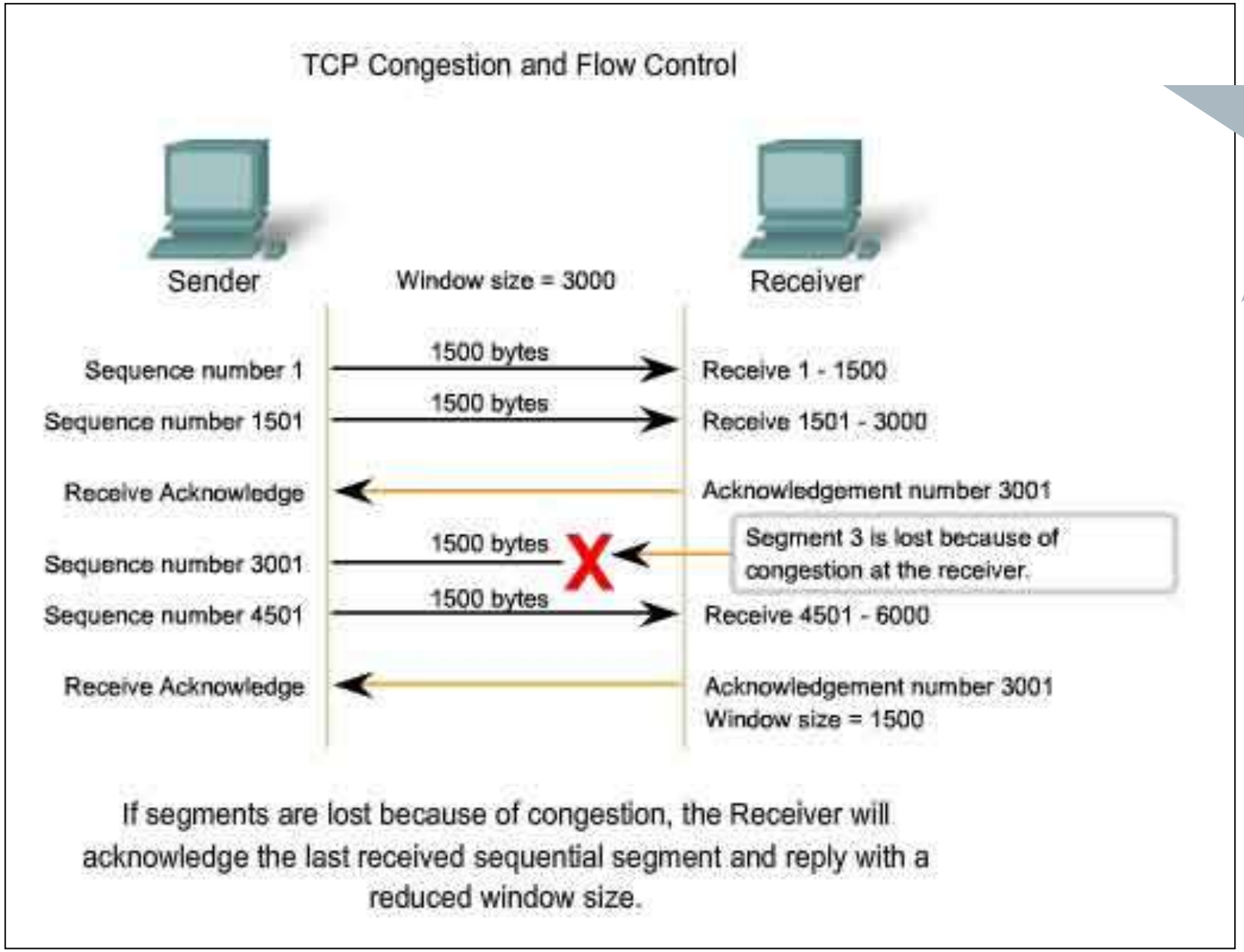
• GENEL- PUBLIC

TCP FRAGMENTATION



• GENEL- PUBLIC

TCP FLOW CONTROL



What is MTU?

COMMON PORT NUMBERS

- Total 65536 (16-bits) of ports are available
- 0-1023 are reserved by IANA
- 1024-49151 are assigned by IANA to applications
- Operating System can assign ports in range 49152-to-65535
- Well-known ports are; HTTP:80, POP3:110, SMTP:25, SNMP:161, DNS:53, RIP:520, TFTP:69, SSH:22, Telnet:23, FTP:21

7 Echo	**554** RTSP	**2745** Bagle.H	**6891-6901** Windows Live
19 Chargen	**546-547** DHCPv6	**2967** Symantec AV	**6970** Quicktime
20-21 FTP	**560** rmonitor	**3050** Interbase DB	**7212** GhostSurf
22 SSH/SCP	**563** NNTP over SSL	**3074** XBOX Live	**7648-7649** CU-SeeMe
23 Telnet	**587** SMTP	**3124** HTTP Proxy	**8000** Internet Radio
25 SMTP	**591** FileMaker	**3127** MyDoom	**8080** HTTP Proxy
42 WINS Replication	**593** Microsoft DCOM	**3128** HTTP Proxy	**8086-8087** Kaspersky AV
43 WHOIS	**631** Internet Printing	**3222** GLBP	**8118** Privoxy
49 TACACS	**636** LDAP over SSL	**3260** iSCSI Target	**8200** VMware Server
53 DNS	**639** MSDP (PIM)	**3306** MySQL	**8500** Adobe ColdFusion
67-68 DHCP/BOOTP	**646** LDP (MPLS)	**3389** Terminal Server	**8767** TeamSpeak
69 TFTP	**691** MS Exchange	**3689** iTunes	**8866** Bagle.B
70 Gopher	**860** iSCSI	**3690** Subversion	**9100** HP JetDirect
79 Finger	**873** rsync	**3724** World of Warcraft	**9101-9103** Bacula
80 HTTP	**902** VMware Server	**3784-3785** Ventrilo	**9119** MXit
88 Kerberos	**989-990** FTP over SSL	**4333** mSQL	**9800** WebDAV
102 MS Exchange	**993** IMAP4 over SSL	**4444** Blaster	**9898** Dabber
110 POP3	**995** POP3 over SSL	**4664** Google Desktop	**9988** Rbot/Spybot

Proprietary and Confidential

GENEL- PUBLIC

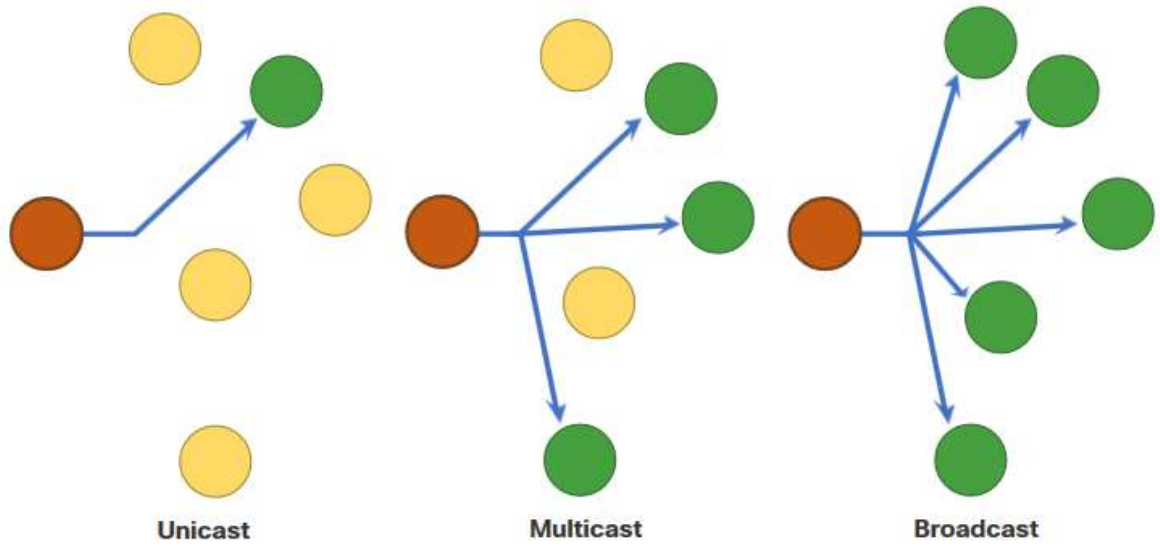
Orion Innovation

IPv4 Addressing

Class A: 8-bits network, 24-bits host number. 1 to 126, 0 means all, 127 is reserved for testing
Class B: 16-bits network, 16-bits host number. 128 to 191 (Binary: 1000 0000 - 1011 1111)
Class C: 24-bits network, 8-bits host number. 192 to 223 (Binary: 1100 0000 - 1110 1111)
Class D: Multicasting. 224 to 239 (Binary: 1110 0000 - 1110 1111)
Class E: Reserved. 240 to 254. 255 is reserved for broadcasting.

Private IP Addresses;
Class A: 10.0.0.0 - 10.255.255.255 (1 Class A Network)
Class B: 172.16.0.0 - 172.31.255.255 (16 Class B Network)
Class C: 192.168.0.0 - 192.168.255.255 (256 Class C Network)

IPv4 Address Types:
Reserved: Broadcast and Class D&E IPs.
Network ID: VLAN IP
Host ID: Host's IP
Directed Broadcast: Routable addresses by routers
Local Broadcast: 255.255.255.255 - router will not route
Loopback: 127.0.0.1
Auto-configured: DHCP assigned IPs
Public: Internet accessible IPs
Private: Local Network IPs.



Proprietary and Confidential

• GENEL- PUBLIC

IPV4 ADDRESS CLASSES & TYPES

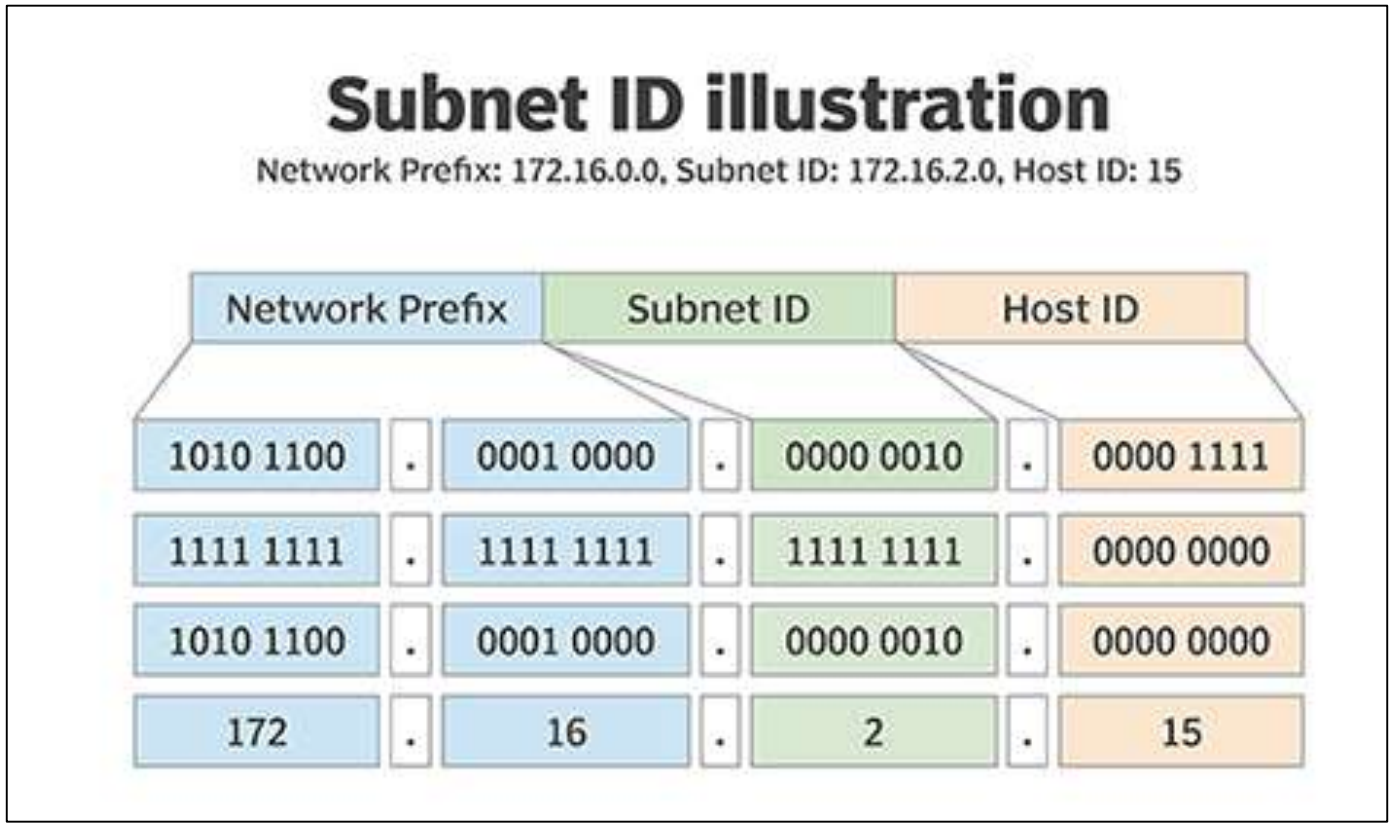
Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

Proprietary and Confidential

• GENEL- PUBLIC

Subnetting is to take some of “Higher order host bits” in a network number and use them to create more network. These networks are called as **subnets**.
Subnet mask is a 32-bits long number which decides the length of the network.
The 0’s and 1’s in the subnet mask should be contiguous.
Valid subnet masks are; 0, 128, 192, 224, 252, 254, 255.



Proprietary and Confidential

• GENEL- PUBLIC

1. Determine the network and host requirements (Max # of hosts required / exist, Max # of segments required / exist)
2. Satisfy Host and Network Requirements
(#_of_Networks: 2^S, where S=subnet bits, #_of_hosts=2^H-2, where H=host bits, Total_#_of_Host_Bits=S+H)
3. Determine the Subnet Mask (A=8, B=16, C=24 + S, e.g. for a C-Class Network 24+S)
4. Determine the Network Addresses
5. Determine the Directed Broadcast Addresses
6. Determine the Host Addresses

Examples:

1. You are given a Class C network (192.168.1.0) and you have four segments in your network, where the largest segment has 50 hosts. What subnet mask should you use and what is the layout of your addresses?
2. You are given a Class B network (172.16.0.0) and you have 490 segments in your network, where the largest segment needs 112 host addresses. What subnet mask should you use and what is the layout of your addresses?
3. You are given a Class A network (10.0.0.0) and you have 9000 segments in your network, where the largest segment needs 560 host addresses. What subnet mask should you use and what is the layout of your addresses?

SUBNETTING TABLE

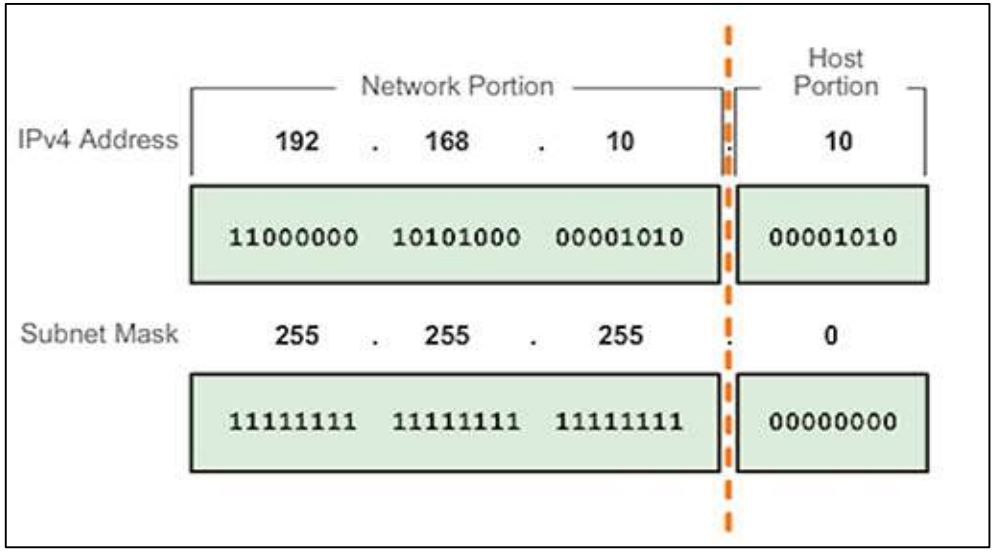
	128	64	32	16	8	4	2	1
Bits borrowed	1	2	3	4	5	6	7	8
Subnet Mask	128	192	224	240	248	252	n/a	n/a
/Mask	/25	/26	/27	/28	/29	/30	n/a	n/a
Wildcard Masks	.127	.63	.31	.15	.7	.3	n/a	n/a
Networks*	2	4	8	16	32	64	n/a	n/a
Hosts	126	62	30	14	6	2	n/a	n/a

Proprietary and Confidential

• GENEL- PUBLIC

DETERMINING IP ADDRESS COMPONENTS

1. An IP Address and Subnet Mask required
2. Examine the subnet mask and find interesting OCTET
3. Subtract the interesting OCTET from 256
4. Write down network addresses
5. Write down broadcast addresses
6. Write down host addresses



Examples:

Determine the network and address type:

1. 192.168.1.37/27
2. 172.16.5.0/23
3. 192.16.1.63/29

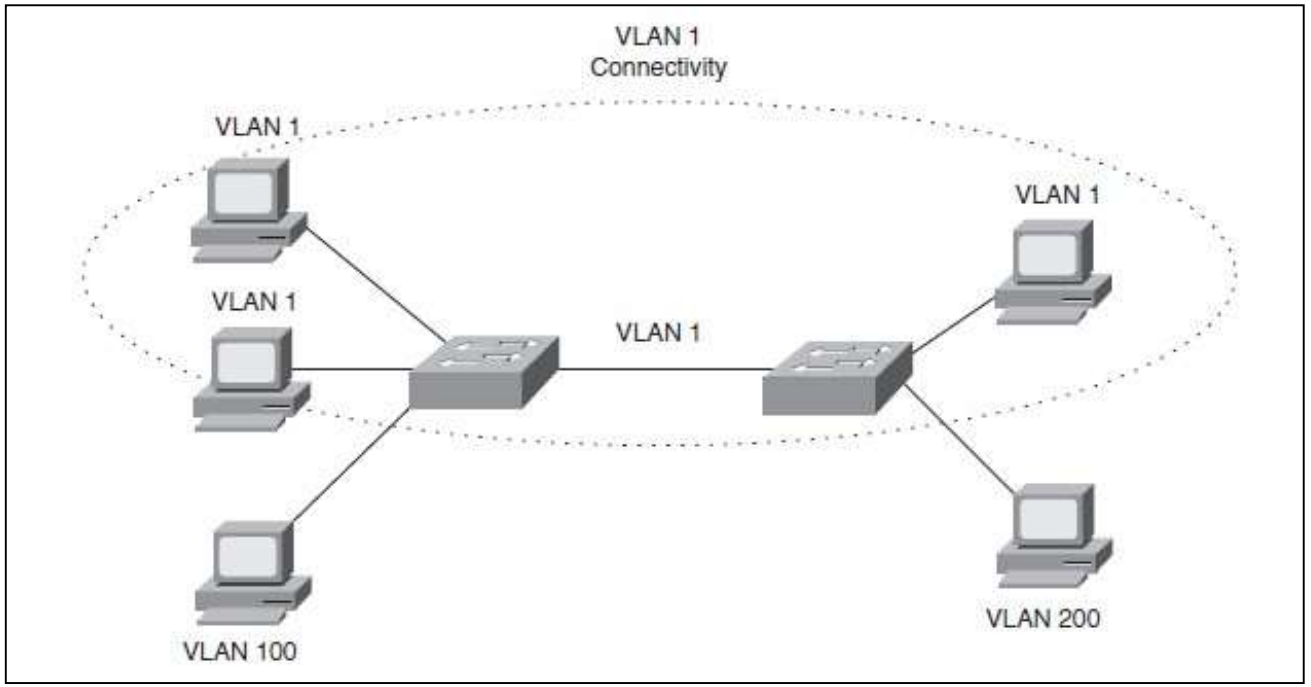
Proprietary and Confidential

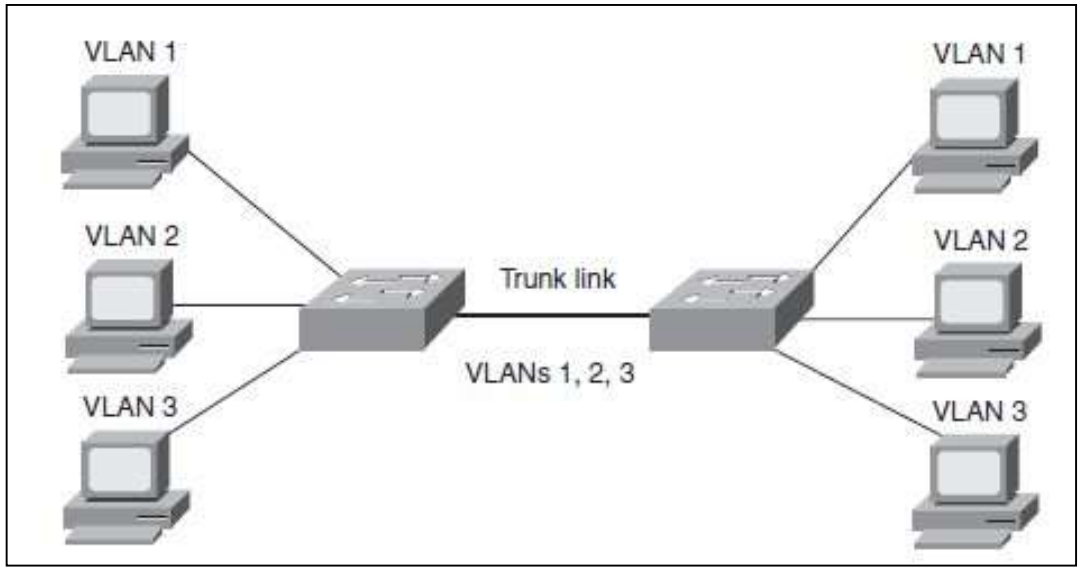
GENEL- PUBLIC

Orion Innovation

VLANs & Trunks

VLAN (Virtual LAN) is a logical separation, which is used to create broadcast domains in Layer-2.
Access Ports are assigned to hosts and allowed to pass only one VLAN.
Trunk Ports are interfaces between switches and can be configured to pass multiple VLANs.





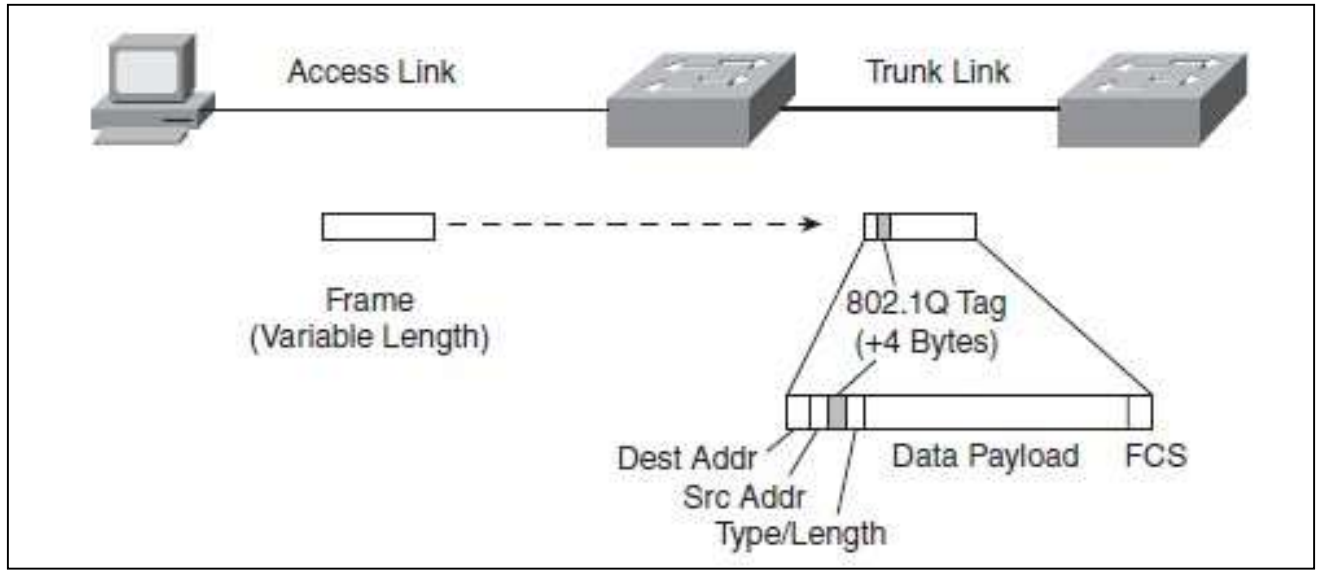
• GENEL- PUBLIC

802.1Q ENCAPSULATION

IEEE standard for marking packets (a.k.a frame identification).

If frames must be transported out another trunk link, the ***VLAN identifier*** is added back into the frame header. Otherwise, if frames are destined out an access (non-trunk) link, the switch removes the VLAN identifier before transmitting the frames to the end station. Therefore, all traces of VLAN association are hidden from the end station.

The first two bytes are used as a Tag Protocol Identifier (TPID) and always have a value of 0x8100 to signify an 802.1Q tag. The remaining two bytes are used as a Tag Control Information (TCI) field. The TCI information contains a three-bit Priority field, which is used to implement class-of-service (CoS) functions in the accompanying 802.1Q/802.1p prioritization standard. One bit of the TCI is a Canonical Format Indicator (CFI), flagging whether the MAC addresses are in Ethernet or Token Ring format. The last 12 bits are used as a VLAN identifier (VID) to indicate the source VLAN for the frame. The VID can have values from 0 to 4095, but VLANs 0, 1, and 4095 are reserved.

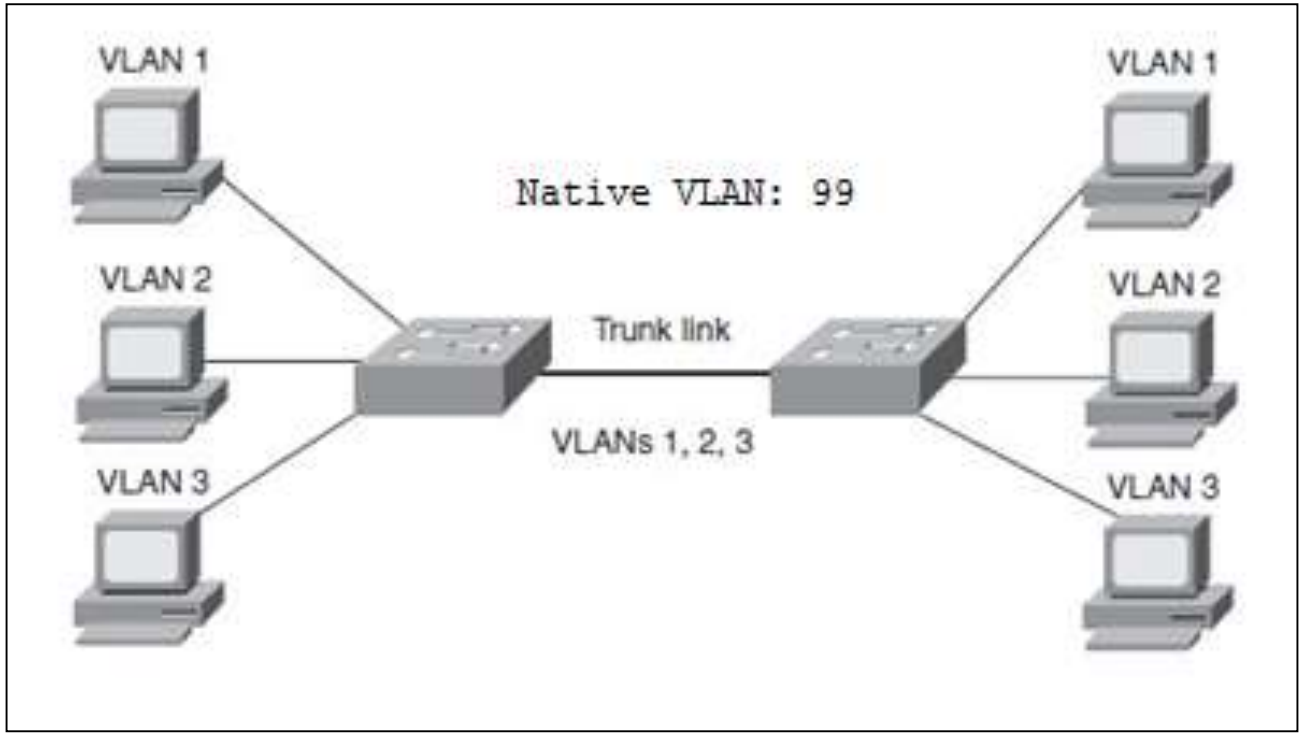


GENEL- PUBLIC

NATIVE VLAN

Frames belonging to **Native VLAN** are *not* encapsulated with any tagging information. If an end station is connected to an 802.1Q trunk link, the end station can receive and understand only the native VLAN frames. This provides a simple way to offer full trunk encapsulation to the devices that can understand it, while giving normal-access stations some inherent connectivity over the trunk.

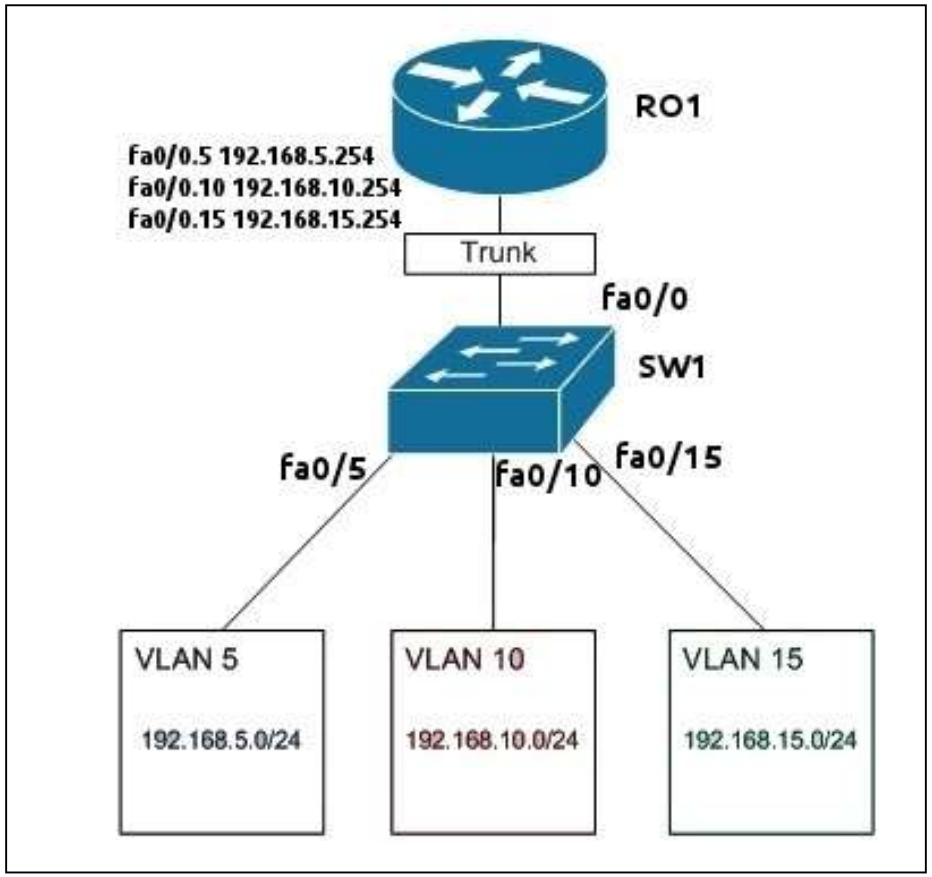
- If there is a Native VLAN mismatch between switches, then switch communication via BPDU may have problems!



VLANs require a **L3 device** such as Router or L3 switch to communicate with each other.

Router specific **sub-interface configuration** is called as “**router-on-a-stick**”.

If **L3 switches** are used, then an **SVI** needs to be defined for each VLAN.



Proprietary and Confidential

• GENEL- PUBLIC

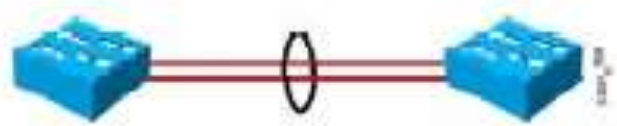
Orion Innovation

Redundancy & HA Solutions

Bundling **parallel links into a single, logical link** to increase the bandwidth and overcome STP.
Provides **redundancy** with several **bundled physical links**. If one of the links within the bundle fails, traffic sent through that link automatically is moved to an adjacent link. Failover occurs in less than a few milliseconds and is transparent to the end user.
Ports should be on the same Ethernet media type and speed as well as the same STP settings.
Generally, all bundled ports first must belong to the same VLAN. If used as a trunk, bundled ports must be in **trunking mode**, have the same native VLAN, and pass the same set of VLANs.
Load balancing method:

method Value	Hash Input	Hash Operation
src-ip	Source IP address	bits
dst-ip	Destination IP address	bits
src-dst-ip	Source and destination IP address	XOR
src-mac	Source MAC address	bits
dst-mac	Destination MAC address	bits
src-dst-mac	Source and destination MAC	XOR
src-port	Source port number	bits
dst-port	Destination port number	bits
src-dst-port	Source and destination port	XOR

- Same speed and duplex.
- Same mode (access or trunk).
- Same native and allowed VLANs on trunk ports.
- Same access VLAN on access ports.
- Configure these parameters on the port-channel interface.



Proprietary and Confidential

• GENEL- PUBLIC

LACP is an IEEE 802.3ad standard, **MLT control protocol**.
LACP packets are exchanged between switches over MLT-capable ports.
Ports are selected and become active according to their *port priority* value (a 2-byte priority followed by a 2-byte port number), where a low value indicates a higher priority.
The lowest port priorities as active MLT and the other links are placed in a standby state and will be enabled in the MLT if one of the active links goes down.

Mode	Negotiation Packets Sent?	Characteristics
LACP		
On	No	All ports channeling
Passive	Yes	Waits to channel until asked
Active	Yes	Actively asks to form a channel

Proprietary and Confidential

• GENEL- PUBLIC

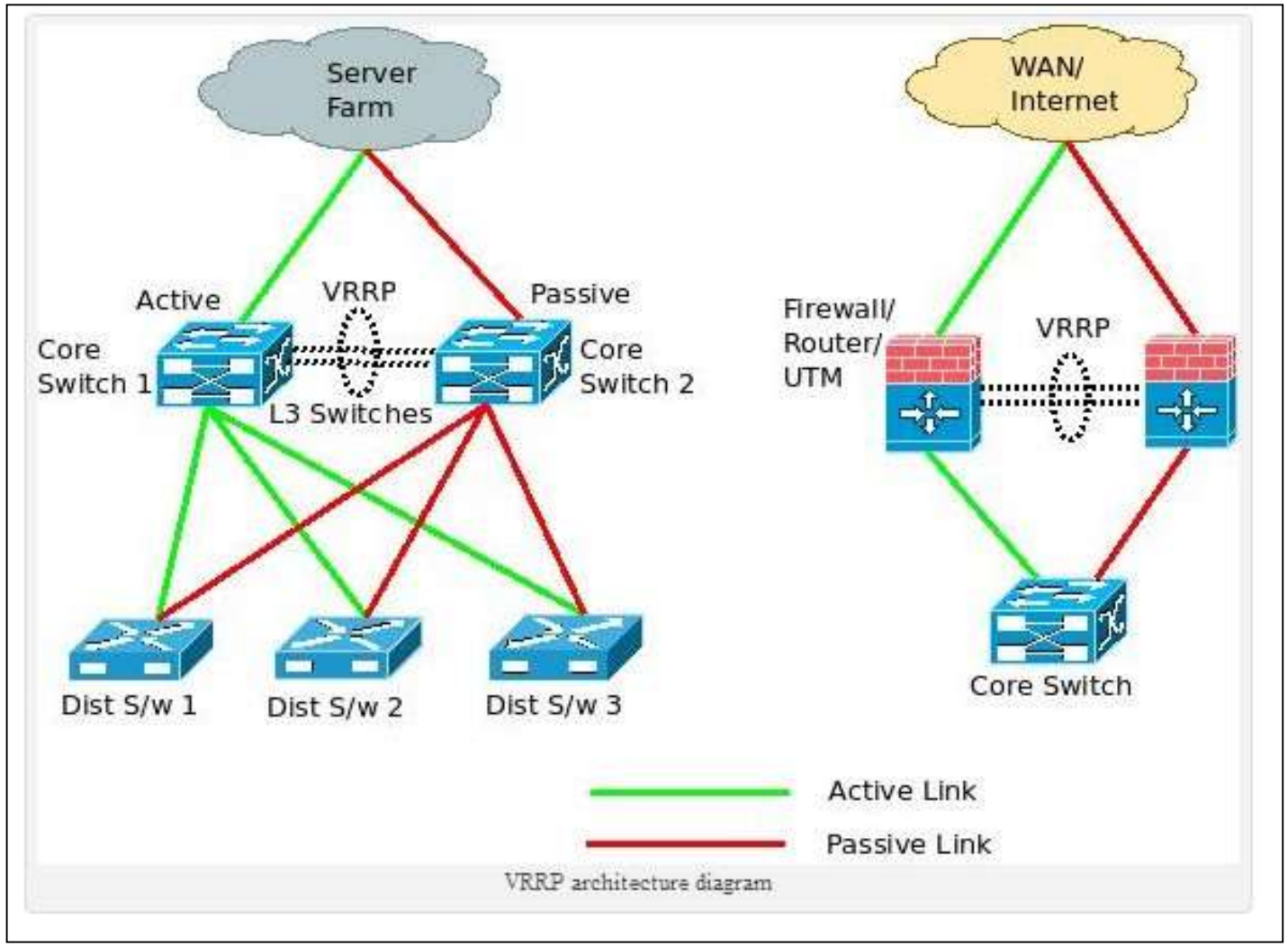
HIGH AVAILABILITY AND VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)

VRRP provides L3 redundancy on multilayer switches.
VRRP provides one redundant gateway address from a group of routers. The active router is called the *master router*, whereas all others are in the *backup state*.
The highest prioritized router becomes master, the default priority value is 100.
VRRP sends its advertisements to the multicast destination address 224.0.0.18 (All VRRP Routers), using IP protocol 112.
A virtual IP & MAC Address is created for each VRRP group. The virtual IP Address can be assigned to a VRRP Cluster.
Total 1000 IP Addresses can be defined as VRRP Virtual IP Address.
The virtual router MAC address is of the form 0000.5e00.01***xx***, where *xx* is a two-digit hex VRRP group number.
VRRP advertisements are sent at 1-second intervals. Backup routers optionally can learn the advertisement interval from the master router. The failover time is the 3 times of Adv. time.
By default, all VRRP routers are configured to preempt the current master router if their priorities are greater.
VRRP can *track objects* to determine if the critical paths still be reachable, otherwise performs a failover.
Load balancing can be performed per VRRP Group basis.
VRRP and STP should complete each other with design perspective.

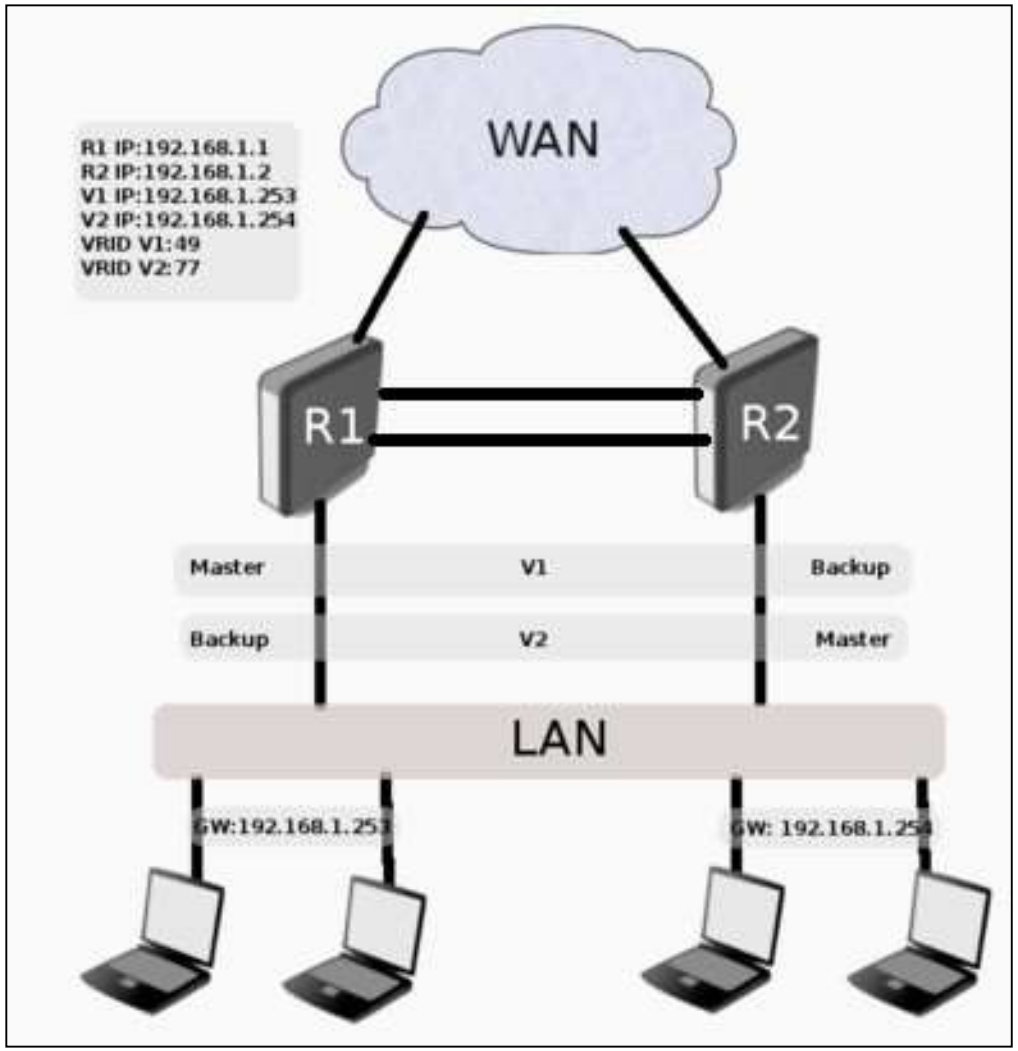
Proprietary and Confidential

• GENEL- PUBLIC

HIGH AVAILABILITY AND VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)



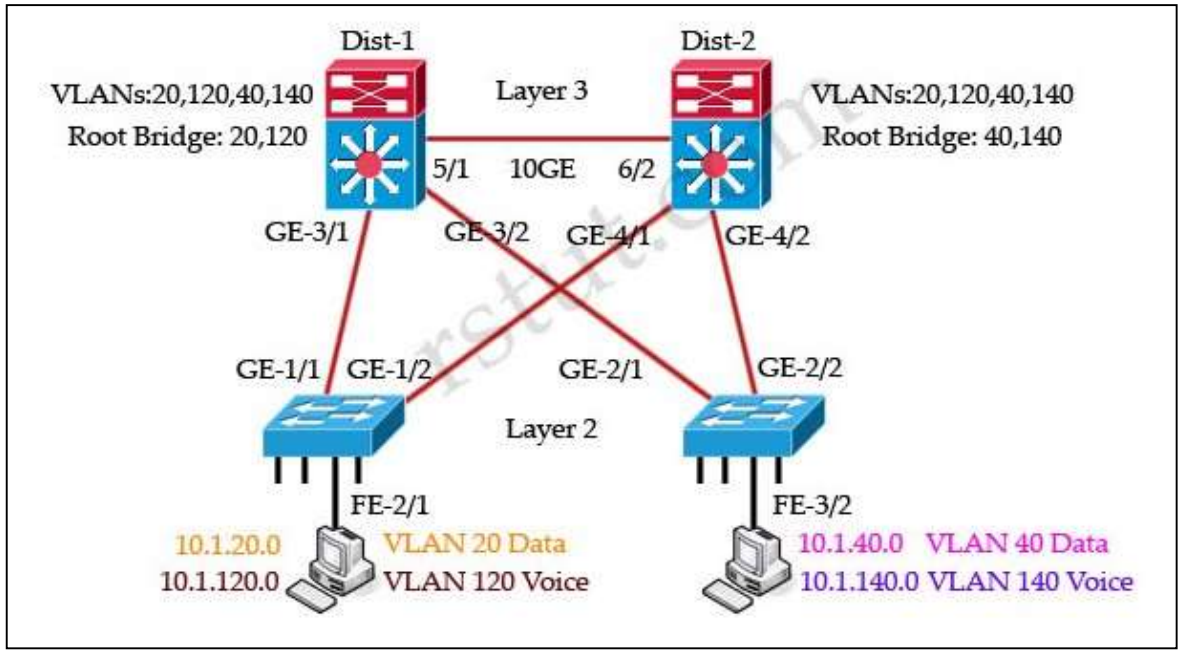
VRRP architecture diagram



• GENEL- PUBLIC

MST (IEEE 802.1s) is built on the concept of mapping one or more VLANs to a single STP instance. Multiple instances of STP can be used (hence the name MST), with each instance supporting a different group of VLANs.
MST is working with regions. If two switches have the same set of attributes, they belong to the same MST region. If not, they belong to two independent regions.

- MST configuration name (32 characters)
- MST configuration revision number (0 to 65535)
- MST instance-to-VLAN mapping table (4096 entries)



Orion Innovation

Routing Protocols

A static route is a manually configured route on your router. Static routes are typically used in smaller networks and when few networks or subnets exist, or with WAN links that have little available bandwidth.

With a network that has hundreds of routes, static routes are not scalable, since you would have to configure each route and any redundant paths for that route on each router.

```
HQ#
HQ#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.2.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.0.2.0/24 is directly connected, GigabitEthernet0/2
L       10.0.2.1/32 is directly connected, GigabitEthernet0/2
C       10.0.3.0/24 is directly connected, GigabitEthernet0/0
L       10.0.3.1/32 is directly connected, GigabitEthernet0/0
C       10.10.0.0/24 is directly connected, Loopback0
L       10.10.0.1/32 is directly connected, Loopback0
S       10.11.0.0/24 [1/0] via 10.0.3.2
S*   0.0.0.0/0 [2/0] via 10.0.2.2

HQ#
```

Proprietary and Confidential

• GENEL- PUBLIC

RIPv1 uses **local broadcasts** (255.255.255.255) to share routing information.
These **updates are periodic** in nature, occurring, by default, every 30 seconds, with a hold-down period of 180 seconds.
RIP use ***hop count*** as a metric.
RIPv1 is a ***classful*** protocol.
RIP supports up to **six equal-cost paths** to a single destination, where all six paths can be placed in the routing table and the router can **load-balance** across them. The default is actually four paths, but this can be increased up to a maximum of six. RIP will not load-balance across *unequal*-cost paths.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 200.1.1.2, 00:00:15, FastEthernet0/1   LAN2
R    192.168.3.0/24 [120/1] via 200.1.1.3, 00:00:03, FastEthernet0/1   LAN3
C    200.1.1.0/24 is directly connected, FastEthernet0/1
```

Proprietary and Confidential

• GENEL- PUBLIC

Classless, hybrid
Uses **multicast** IP Address (224.0.0.9) for routing updates with triggered updates to speed up convergence
Metric is the "**hop-count**" with the maximum limit of 15
Auto-summarization is enabled by default
Supports **authentication** (Clear-text or hashed-key)
Supports **equal load balancing** as the same with RIPv1
Protocol Number: 17

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
C 172.30.1.0/24 is directly connected, FastEthernet 0/0
C 172.30.2.0/24 is directly connected, FastEthernet 0/1
R       172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
```

Proprietary and Confidential

• GENEL- PUBLIC

Open standard, **classless**, **link-state** protocol
Uses **SPF** (Dijkstra / Shortest Path First) algorithm for a **loop free** topology
Uses **incremental**, **triggered**, **multicast** [224.0.0.5 (OSPF All Routers), 224.0.0.6 (OSPF DRs)] LSAs to update the routing table
Uses **inverse of the bandwidth** as a cost value (10^8/BW where BW: 56Kbps Serial: 1785, 64Kpbs Serial: 1652, T1: 64, Ethernet: 10, Fast Eth.: 1, FDDI: 1)
Uses **load balancing** up to 16 equal-cost paths
AS (Automonous System) numbers are used to separate OSPF areas
Protocol Number: 89
Requires more memory, CPU. Complex to troubleshoot. Large network disadvantage (use BGP instead)

```
R1#show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 6 subnets
O       172.16.144.0 [110/2] via 10.1.124.4, 00:52:01, FastEthernet1/0
O       172.16.133.0 [110/65] via 10.1.13.3, 00:38:18, Serial0/1
O       172.16.104.0 [110/2] via 10.1.124.4, 00:52:01, FastEthernet1/0
C       172.16.101.0 is directly connected, Loopback0
O       172.16.102.0 [110/129] via 10.1.13.3, 00:38:18, Serial0/1
O       172.16.103.0 [110/65] via 10.1.13.3, 00:38:18, Serial0/1
     10.0.0.0/24 is subnetted, 3 subnets
C       10.1.13.0 is directly connected, Serial0/1
O       10.1.23.0 [110/128] via 10.1.13.3, 00:38:18, Serial0/1
C       10.1.124.0 is directly connected, FastEthernet1/0
S*   0.0.0.0/0 is directly connected, Serial0/1
R1#
```

Proprietary and Confidential

• GENEL- PUBLIC

Operation:

Unique Router ID: The active loopback with the highest IP address or the active physical interface with the highest IP address.

Neighboring: LSA Hello message sends every 10secs. Dead Time is 4 times of Hello (40 secs). If a router does not send Hello LSA within the dead time, then declared as dead.

The following should match for the routers to become neighbors:

- The area number
- Hello and Dead timer intervals
- OSPF password (if configured)
- Area Stub Flag
- MTU Size

During learning phase (exchange process), the following states are seen;

- Down State: Not exchanged any LSA with any router
- Init State: LSA Hello is received and added to neighbor database, unidirectional communication
- Two-way State: LSA Reply from the destination and update the neighbor database. DR / BDR election starts.

Proprietary and Confidential

• GENEL- PUBLIC

Operation:

DR / BDR Election: Client / Server implementation to OSPF

- The router with the highest Router ID becomes DR, second becomes BDR (Priority 0 means, not involve to election)
- DR + BDR called as DROTHERs. Each broadcast segment has the DROTHERs except WAN PPP.
- Routers send LSAs to DR directly (via multicast 224.0.0.6) and DR sends to all (via multicast 224.0.0.5). PPP sends to 224.0.0.5 only.

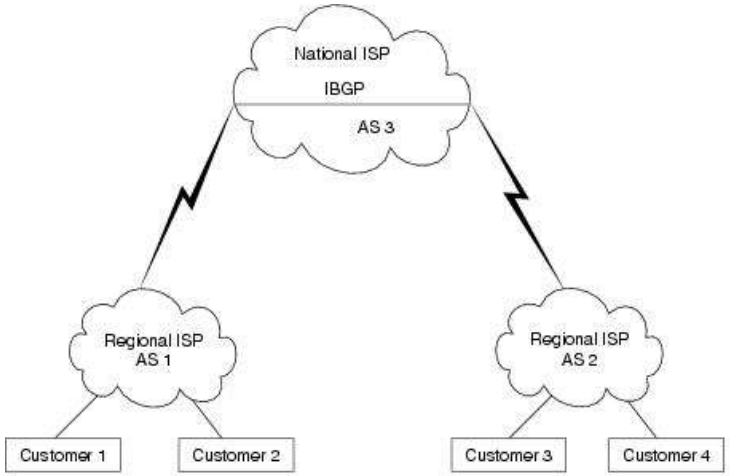
Routing Information Sharing: The following states are seen after the DR / BDR election:

- Exstart State: The DR is selected and started the exchange of routing database, others stays as slaves
- Exchange State: DR sends DBD/DDP (Database Description Packets) which contains the link state type, ID of advertising router, cost of advertising router and the sequence number of the link. Slave responds with LSACK and compares the DBD with its own database.
- Loading State: If the DR has more up-to-date database than slave, the slave will respond to DR's original DBD with a LSR (Link State Request). The DR sends a LSU (Link State Update) and slave generates LSACK again. If the slave has more up-to-date information, it'll repeat the exchange and loading states.
- Full State: DR and others are synch'ed.

Proprietary and Confidential

• GENEL- PUBLIC

BGP is an **exterior gateway protocol** (EGP), which means that it performs routing between multiple autonomous systems or domains and exchanges routing and reachability information with other BGP systems.
BGP uses 13-steps "**Best Path Selection**" algorithm to choose the best path.
Load balancing is supported but not recommended.
BGP is used on **Core layer routers**. Designed for **very-large scaled networks**, but convergence time is slower than OSPF.
BGP neighbors **exchange full routing information** when the TCP connection between neighbors is first established.
When changes to the routing table are detected, the BGP routers send to their neighbors **only those routes that have changed**. BGP routers **do not send periodic routing updates**, and BGP routing updates advertise only the optimal path to a destination network.
If a full BGP table is requested (not recommended for small routers), you can see the **whole internetwork**.
BGP is **controlled globally,** and you should confirm that the IP Address is a member of **YOUR** network, before you announce the network through BGP!
BGP is controlled by ISPs with **ACLs**.



BGP Best Path Selection Algorithm

COMPARISION OF ROUTING PROTOCOLS

Name	Type	Update	Metric	VLSM	Summary
RIPv1	DV	30 sec	Hops	No	Automatic
RIPv2	DV	30 sec	Hops	Yes	Automatic
IGRP	DV	90 sec	Composite	No	Automatic
EIGRP	Advanced. DV	triggered	Composite	Yes	Automatic + Manual
OSPF	LS	triggered	Cost	Yes	Manual
IS-IS	LS	triggered	Cost	Yes	Automatic
BGP	DV	triggered	N/A	N/A	Manual

Proprietary and Confidential

• GENEL- PUBLIC

- Provide an architectural view of an Enterprise Network that contains;
  - A server farm to host Web Servers, E-Mail servers, CRM and ERP data.
  - Office users (3 floors, 150 users in each floor) that will use a VoIP phone and a PC at their desks.
  - An approach to access from home to allow “Work from Home” concept.
  - A lab network to access lab area.
  - Customers could reach to Web Servers.
  - Key points:
    - Ensure that local redundancy is maintained and there is no single point of failure in design.
    - Ensure that the security focus is maintained.
    - Ensure that all activities are monitored and logged for data regulations.
    - Ensure that minimum cost rule is followed.
  - Provide your answers with drawings and explanations of key points.

Proprietary and Confidential

GENEL- PUBLIC

Thank You

orioninc.com

Disclaimer: This document is for informational purposes only and is subject to change without notice. This document and its content herein are believed to be accurate as of its date of publication. However, Orion Systems Integrators, LLC (herein referred as Orion) makes no guarantee, representations or warranties with regard to the enclosed information and specifically disclaims the implied warranties of fitness for a particular purpose and merchantability. As each user of Orion services is likely to be unique in their requirements in the use of such software solutions and their business processes, users of this document are always advised to discuss the content of this document with their Orion representatives.

Orion[SM] and Orion Innovation[SM] are service marks of Orion Systems Integrators, LLC.
All other trademarks acknowledged.

Copyright © 2020 Orion Systems Integrators, LLC.