Configuration and Management of Networks

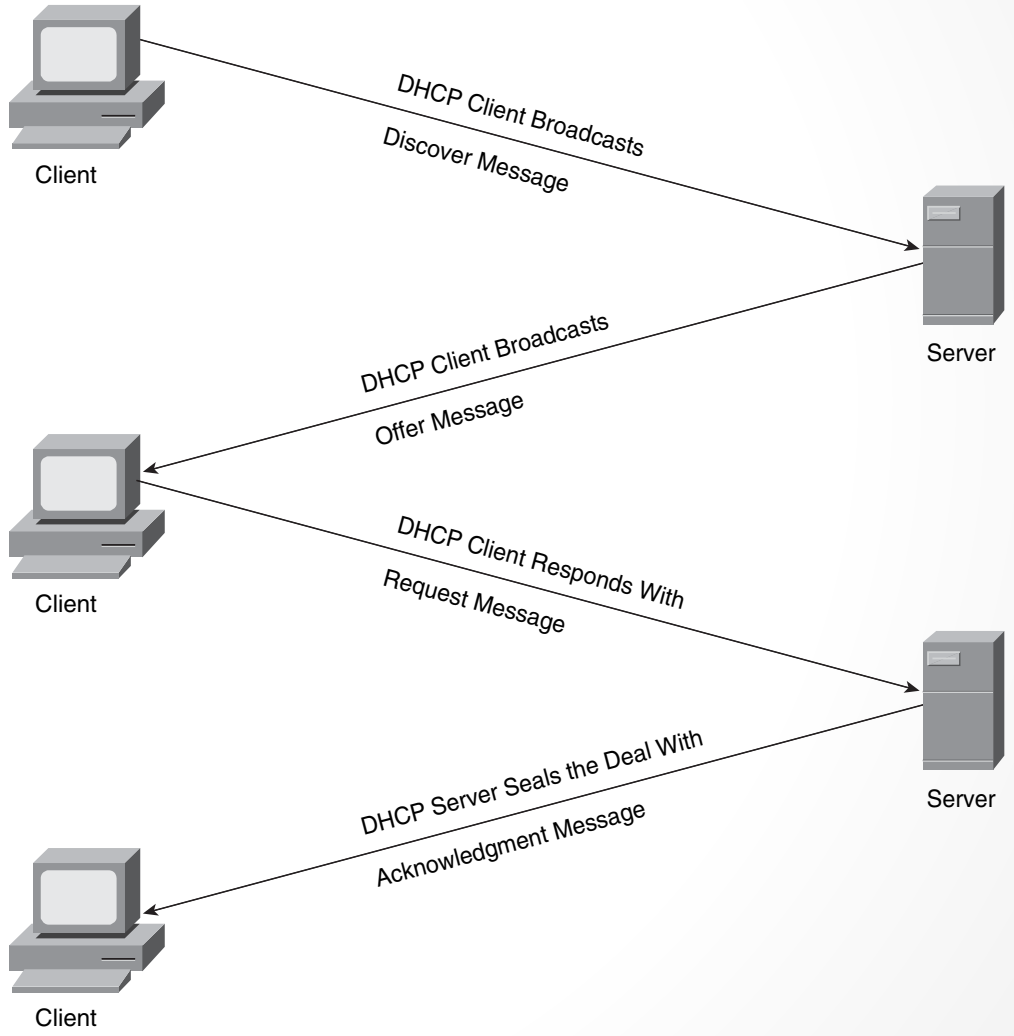
Pedro Amaral

2023

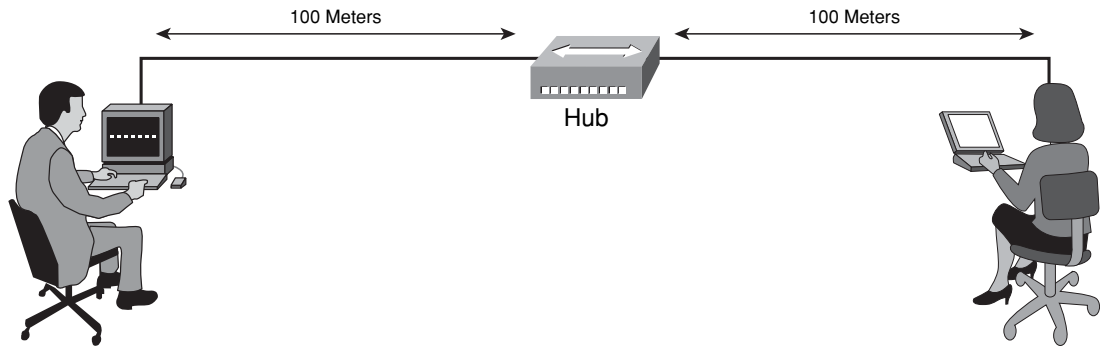
IP addressing – Dynamic Host Configuration Protocol DHCP

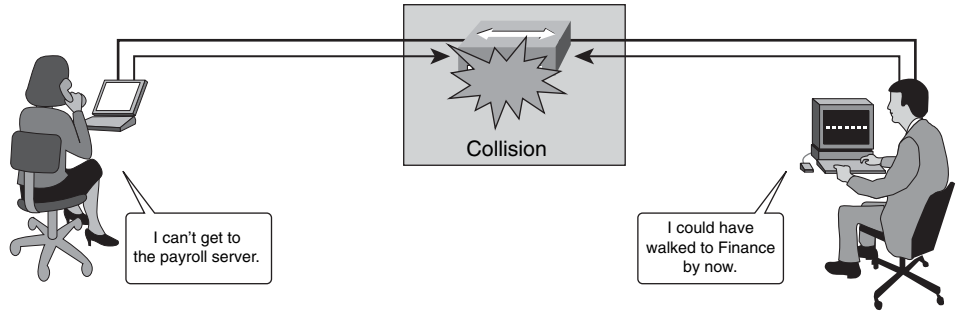
DHCP is a protocol used to assign IP addresses automatically and to set TCP/IP stack configuration parameters, such as the subnet mask, default router, and Domain Name System (DNS) servers for a host.

Address is only "leased" to the host, so the host periodically contacts the DHCP server to extend the lease.

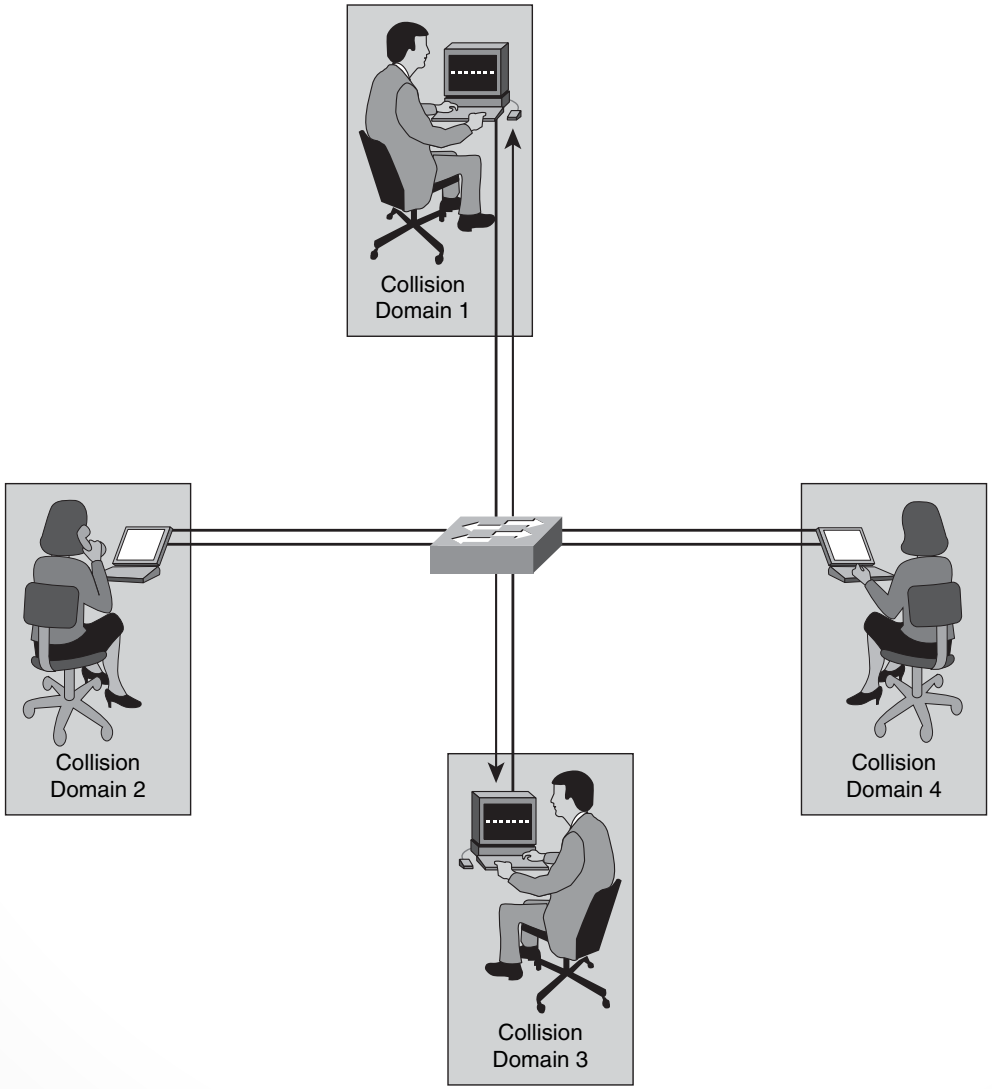


LAN design – Extending a LAN

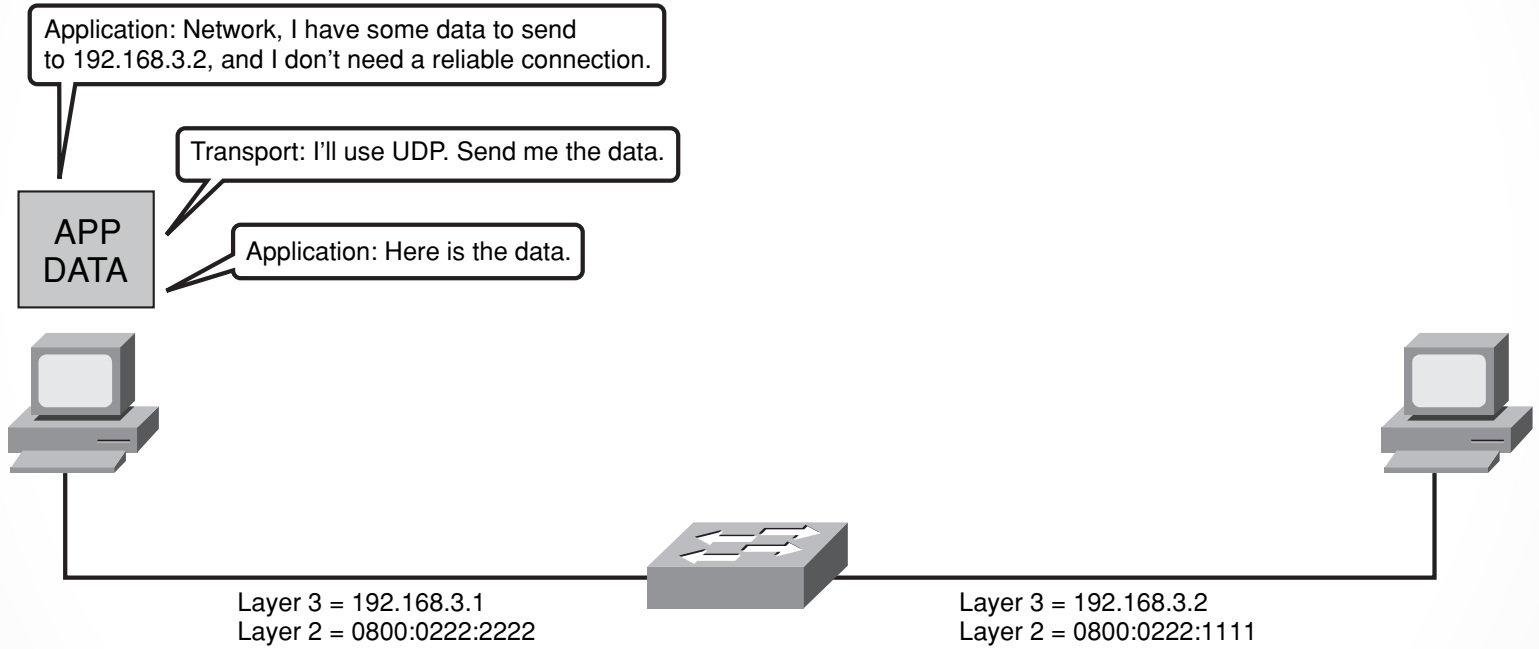




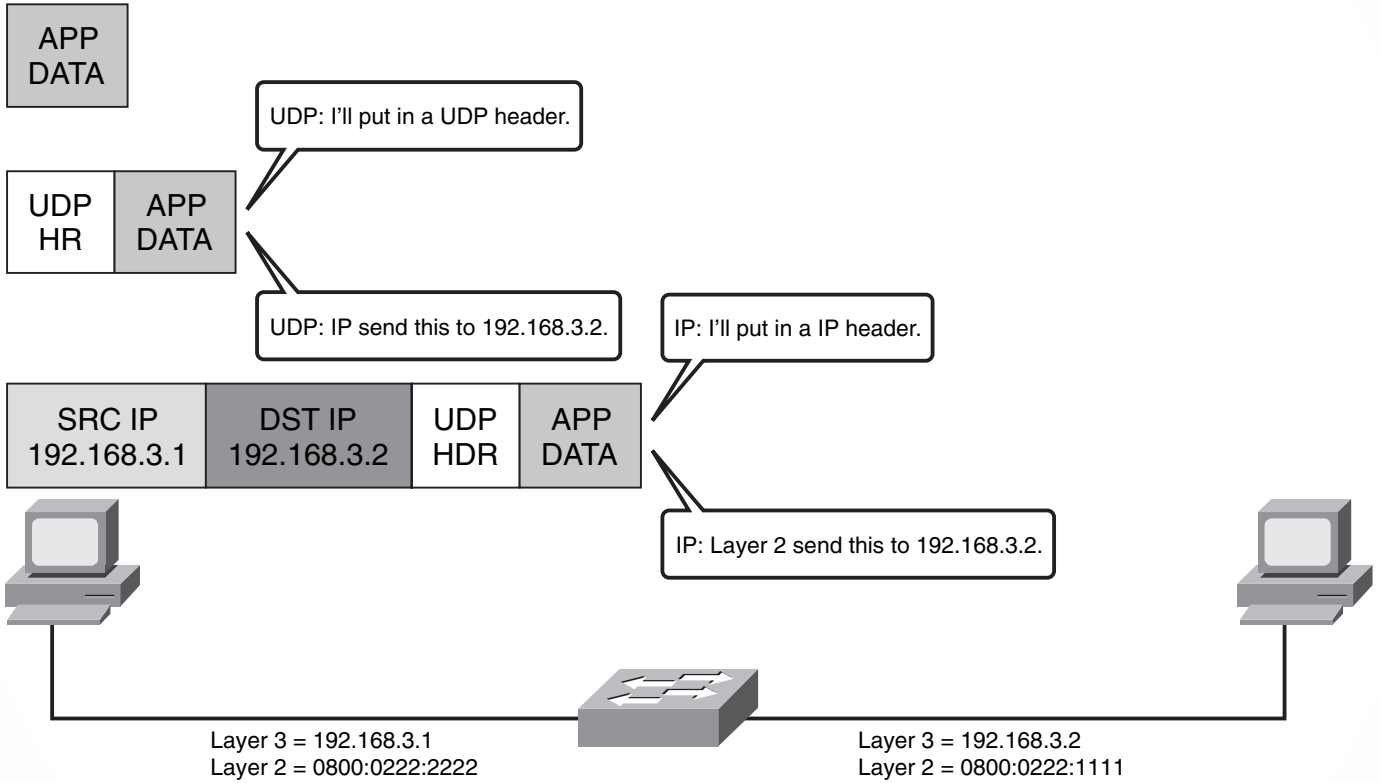
LAN design – Creating multiple collision domains



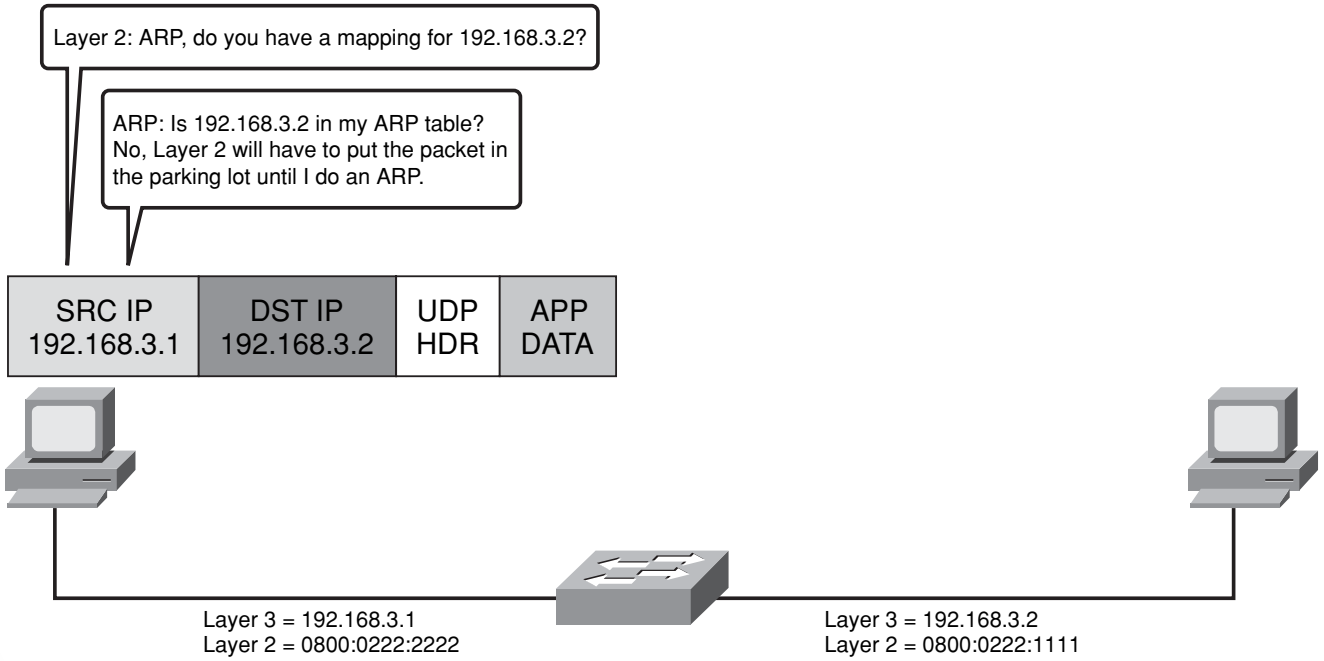
LAN design – Packet Delivery



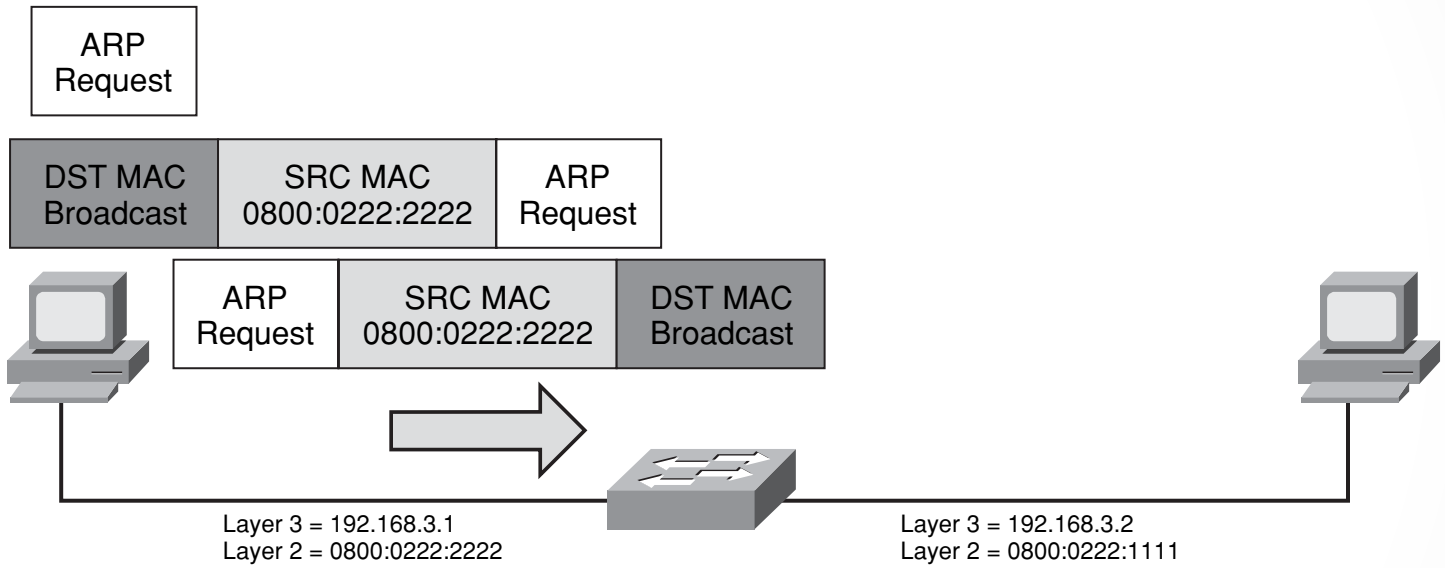
LAN design – Packet Delivery



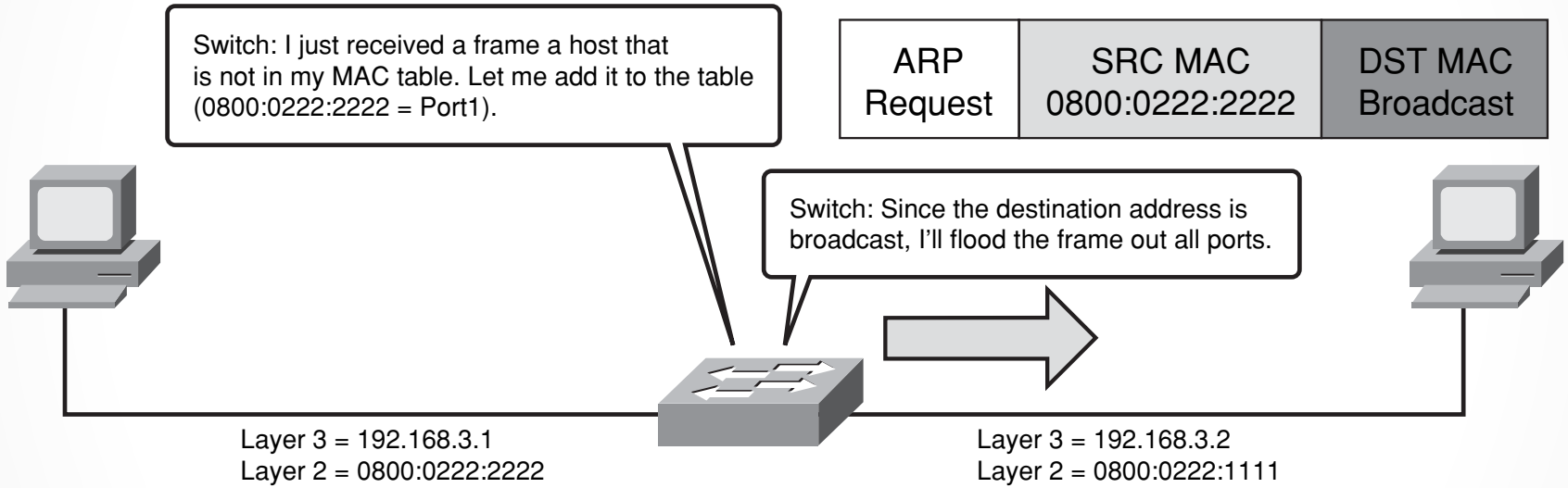
LAN design – Packet Delivery



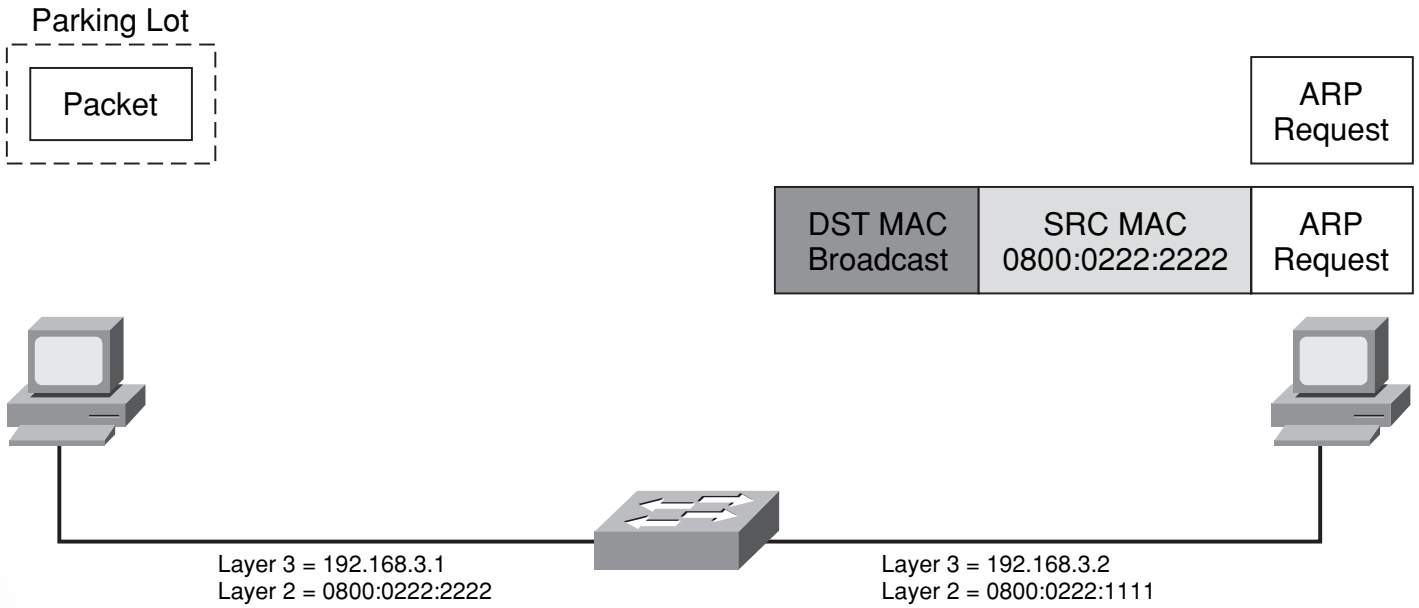
LAN design – Packet Delivery



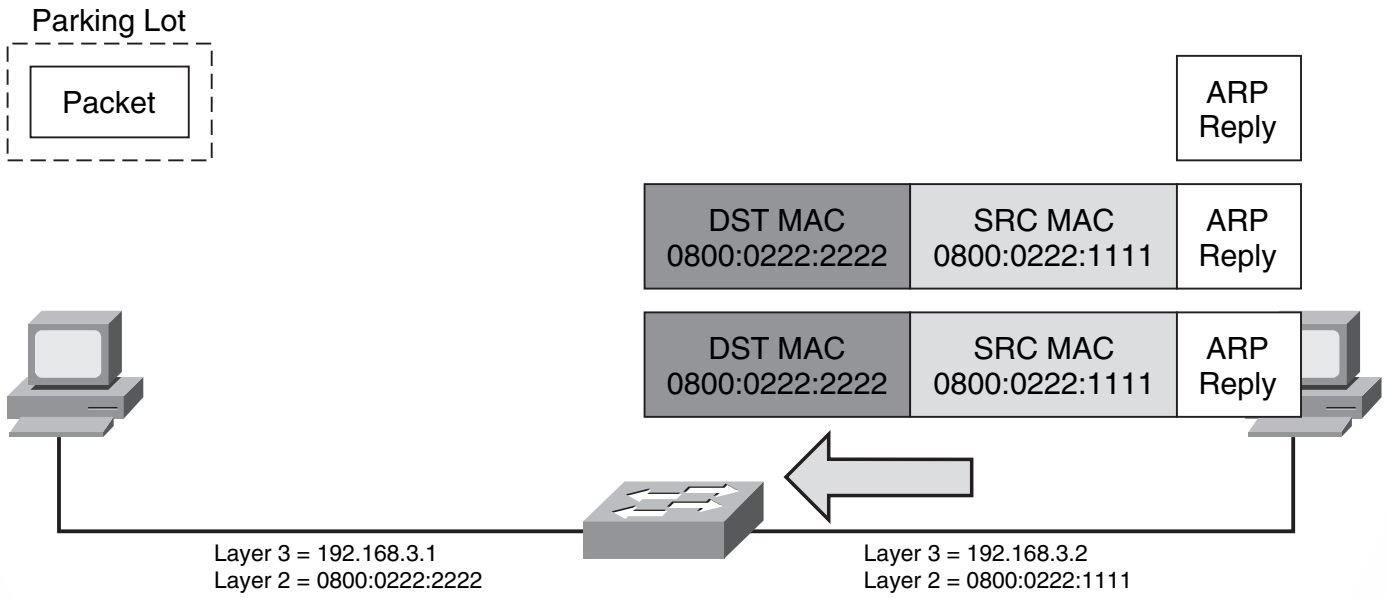
LAN design – Packet Delivery



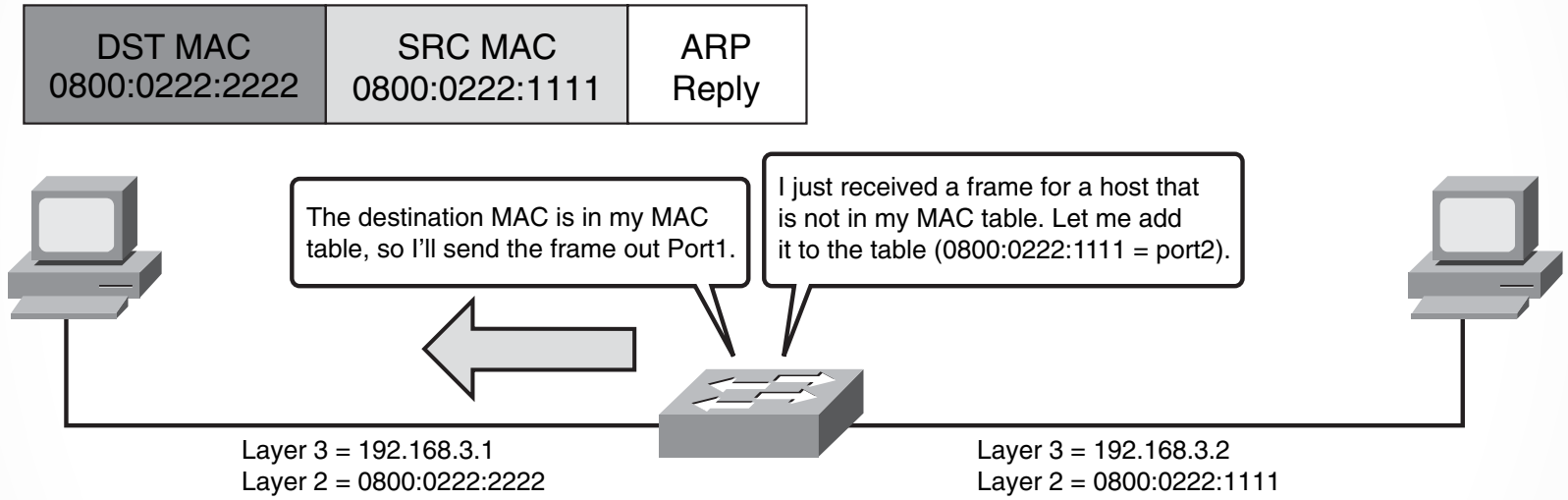
LAN design – Packet Delivery



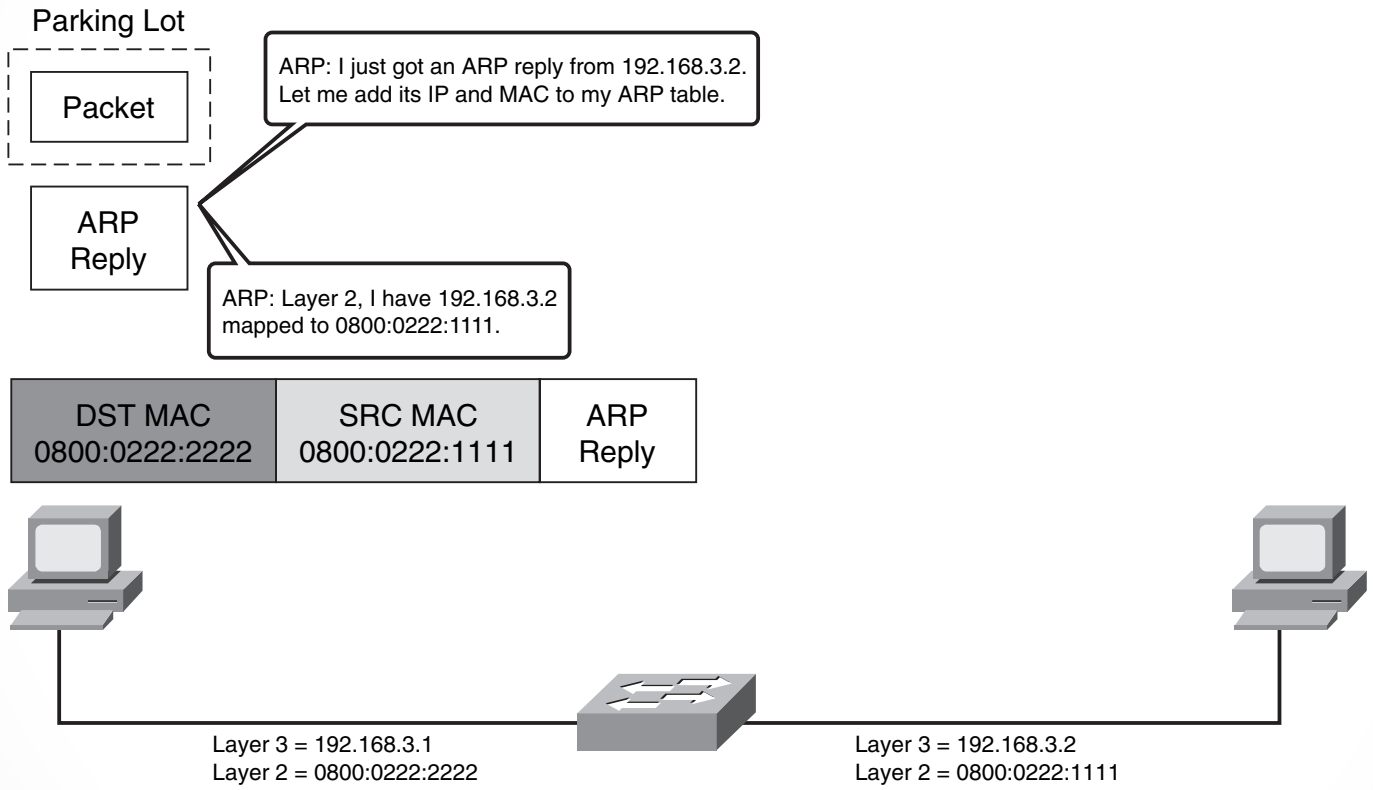
LAN design – Packet Delivery



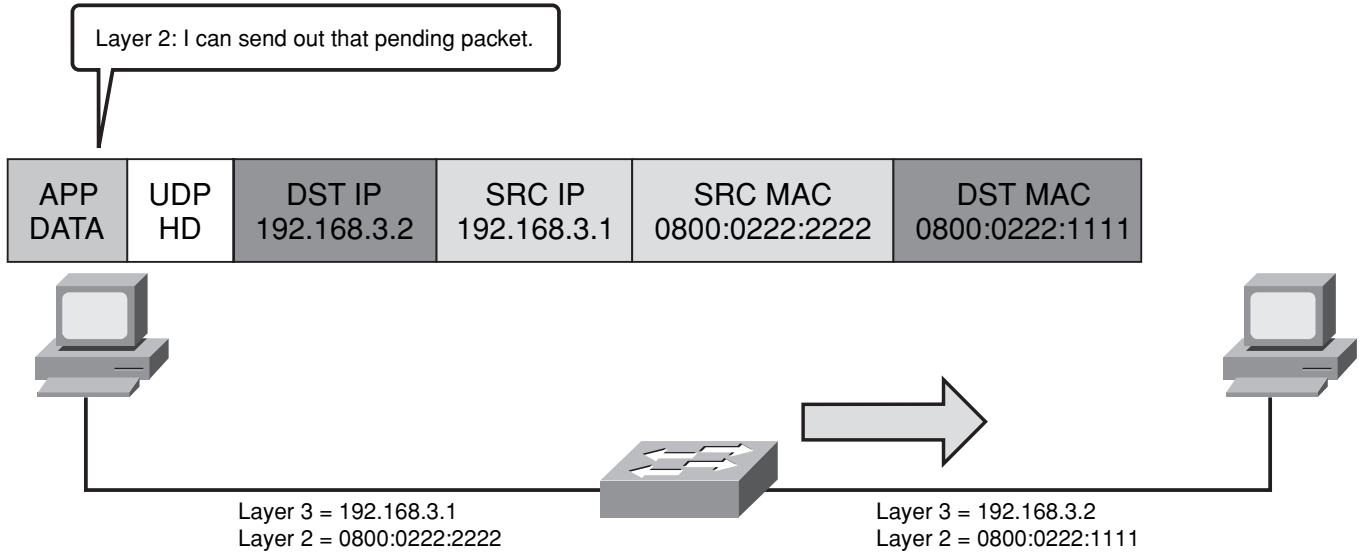
LAN design – Packet Delivery



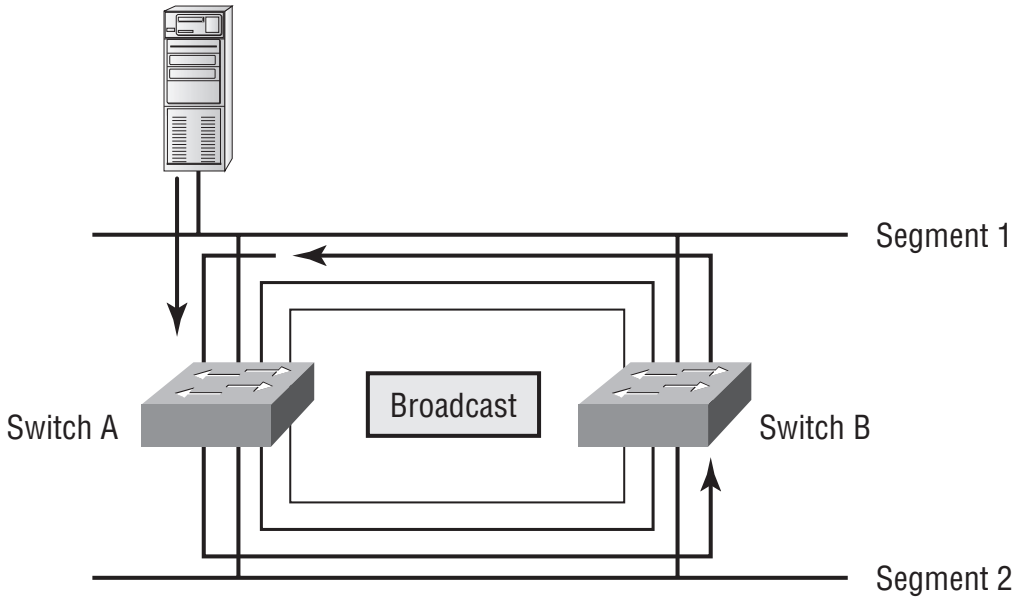
LAN design – Packet Delivery



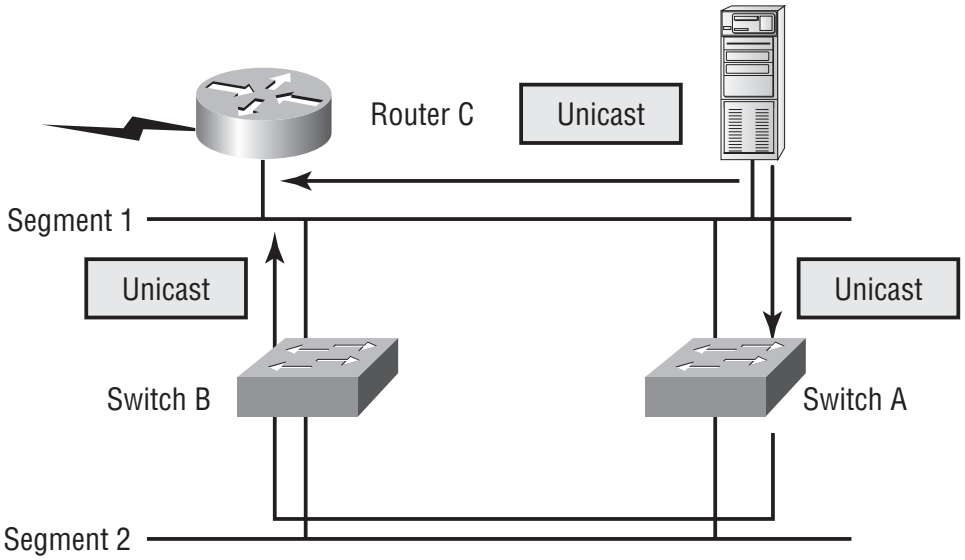
LAN design – Packet Delivery



LAN design – Loops – Broadcast Storm



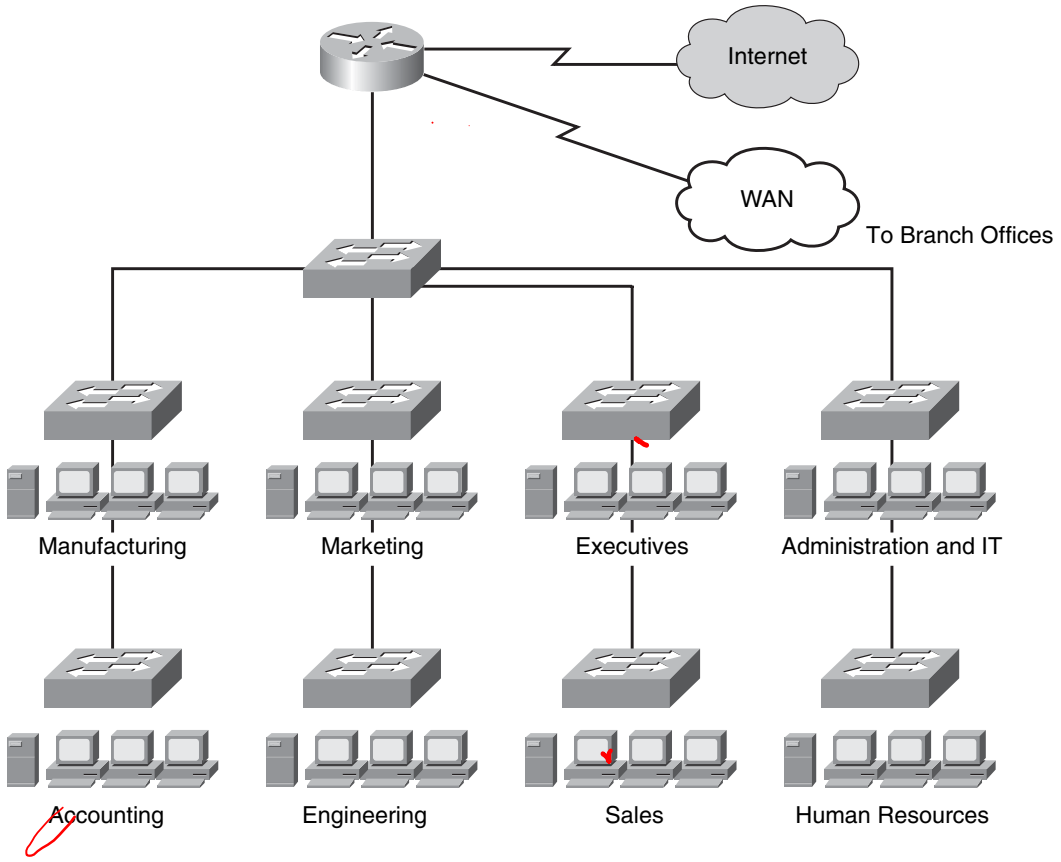
LAN design – Loops – Multiple Frame copies



Router C receives that unicast frame twice.

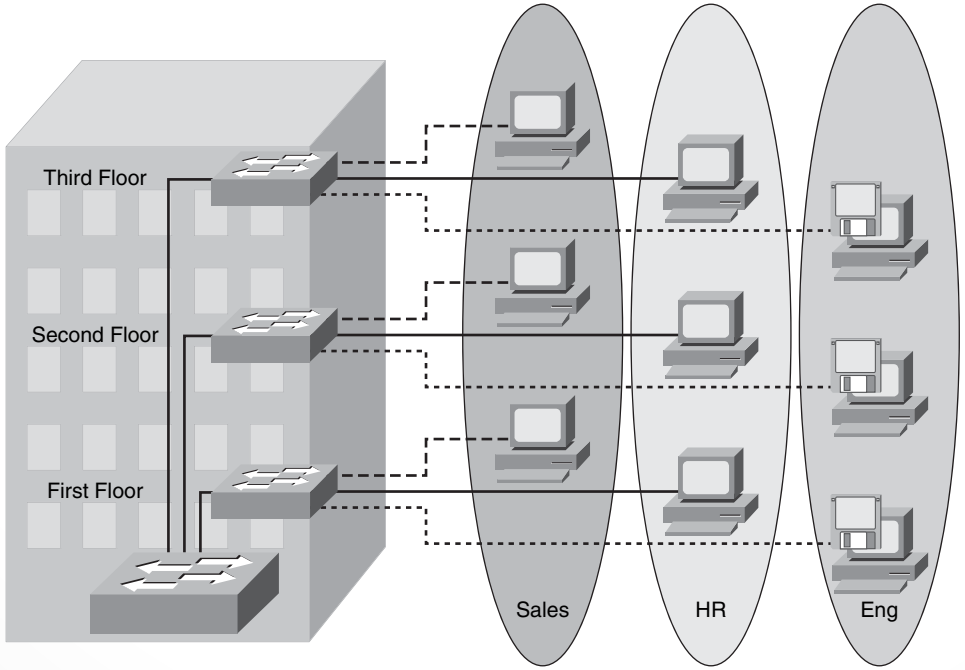
The switches can receive the frame from more than one link.

VLANs – Network with a single broadcast domain



VLANs – VLAN as a logical broadcast domain

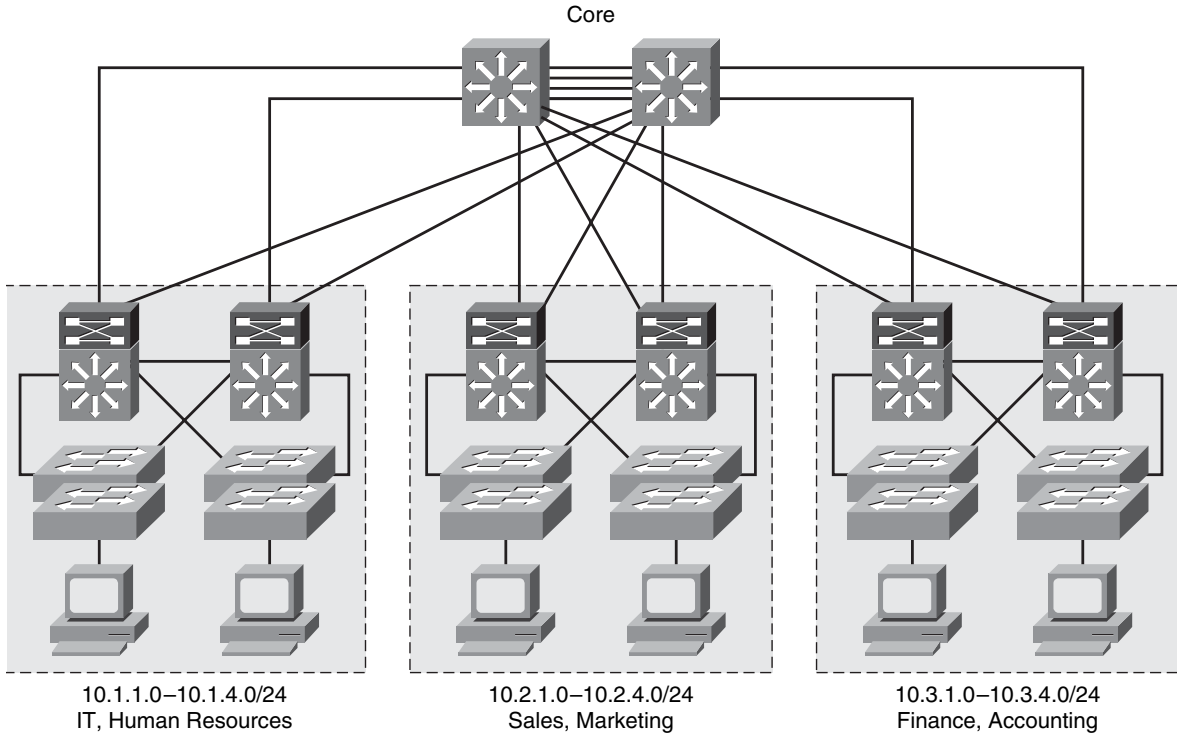
- A VLAN can span multiple physical LAN segments.
- Ports in a VLAN share broadcasts.
- Containing broadcasts in a VLAN improves the overall performance.
- A VLAN can exist on a single switch or span multiple switches.



VLAN = Broadcast Domain = Logical Network (Subnet)

VLANs

Each VLAN in a switched network corresponds to an IP network.



VLANs – IP Addressing

Department	Number of Users	Location
IT	45	Building A
Human Resources	10	Building A
Sales	102	Building B
Marketing	29	Building B
Finance	18	Building C
Accounting	26	Building C

- Building A is allocated 10.1.0.0/16.
- Building B is allocated 10.2.0.0/16.
- Building C is allocated 10.3.0.0/16.

VLANs – IP Addressing

Building A

Department	VLAN	IP Subnet Address
IT	VLAN 11	10.1.1.0/24
Human Resources	VLAN 12	10.1.2.0/24
For future growth		10.1.3.0–10.1.255.0

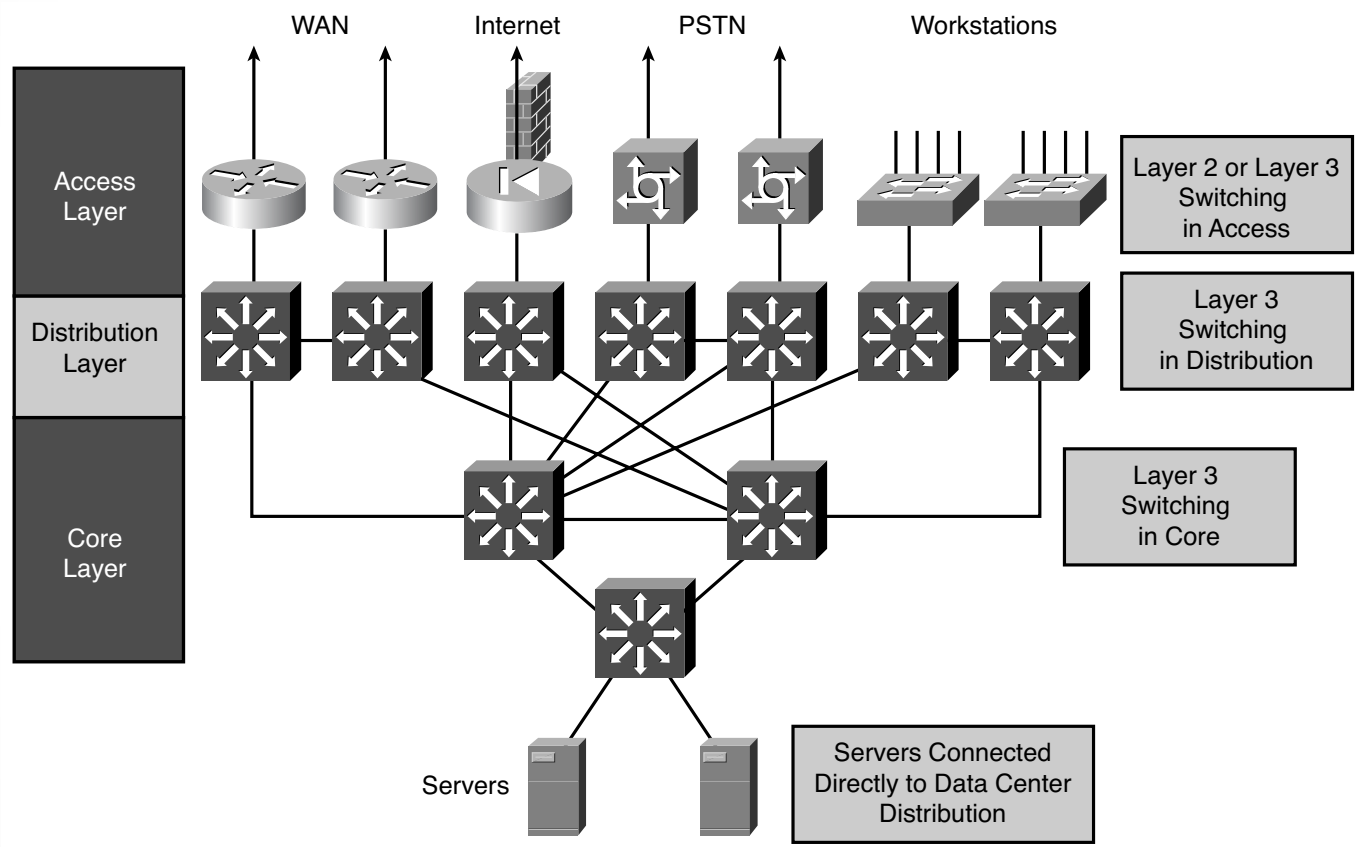
Building B

Department	VLAN	IP Subnet Address
Sales	VLAN 21	10.2.1.0/24
Marketing	VLAN 22	10.2.2.0/24
For future growth		10.2.3.0–10.2.255.0

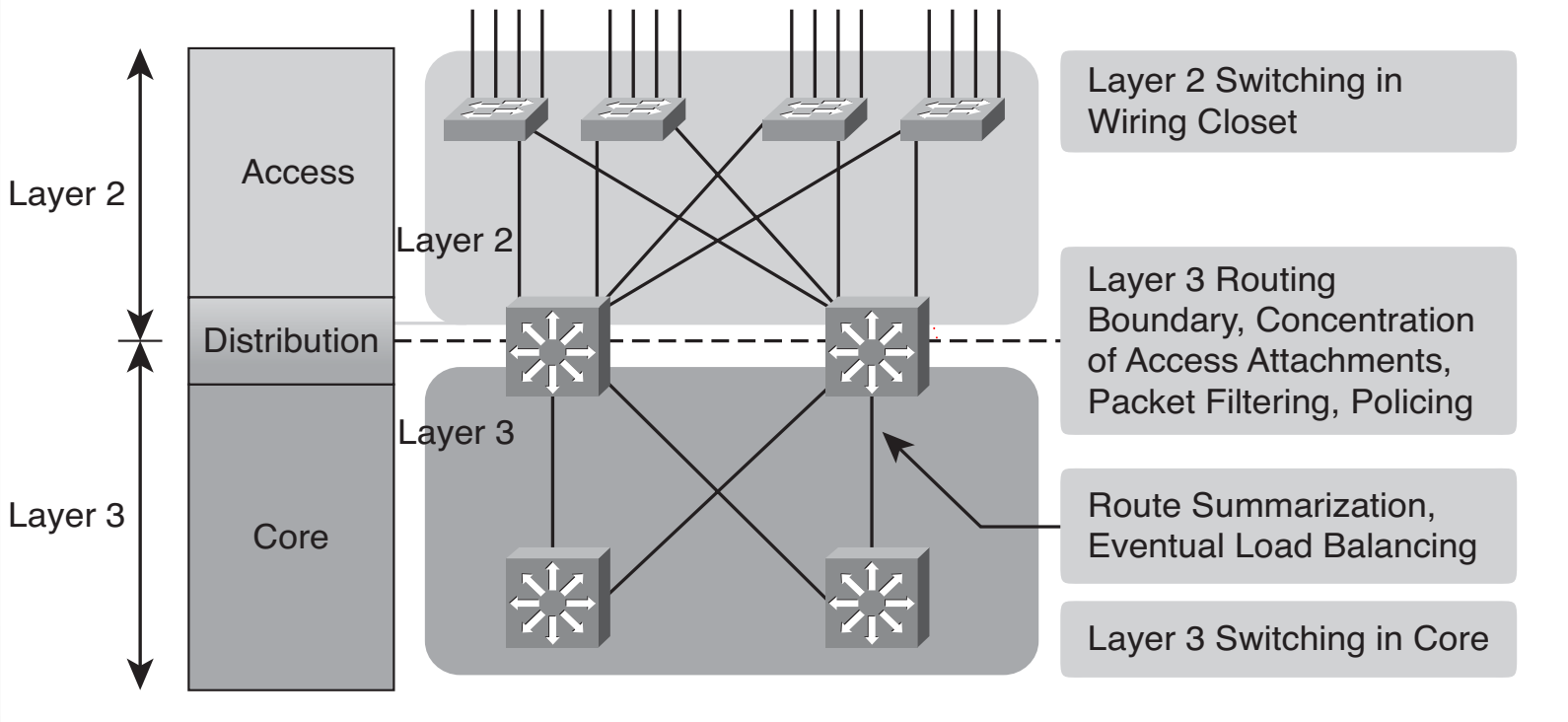
Building C

Department	VLAN	IP Subnet Address
Finance	VLAN 31	10.3.1.0/24
Accounting	VLAN 32	10.3.2.0/24
For future growth		10.3.3.0–10.3.255.0

VLANs – Campus Network Hierarchical Network



VLANs – Campus Network Hierarchical Network



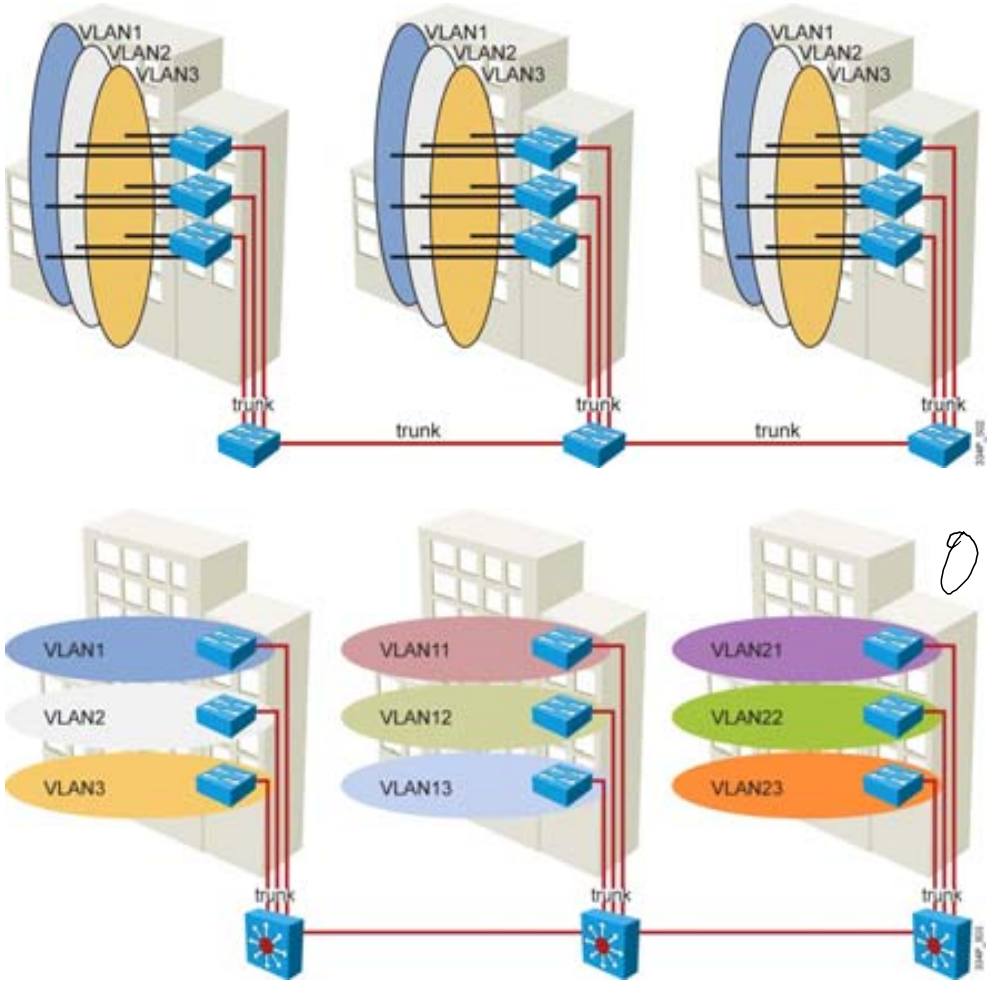
VLANs – End-to-end or local VLANs

End-to-End VLANs

- Users are grouped into VLANs independent of physical location.
- If users are moved within the campus, their VLAN membership remains the same.

Local VLANs

- This is the recommended solution in the Cisco Enterprise Campus Architecture.
- Users are grouped into VLANs depending on physical location.
- If users are moved within the campus, their VLAN membership changes.



VLANs – End-to-end or local VLANs

End-to-End VLANs

Pros:

- Geographically dispersed users appear on the same segment.
- Same policy (security, QoS) can be applied to the same group of users regardless of their physical location.

Cons

- All switches need to know all VLANs.
- Broadcast messages flood all switches.
- Troubleshooting may be challenging.

Local VLANs

Pros:

- Design is scalable.
- Troubleshooting is easy.
- Traffic flow is predictable.
- Redundant paths can be built easily.

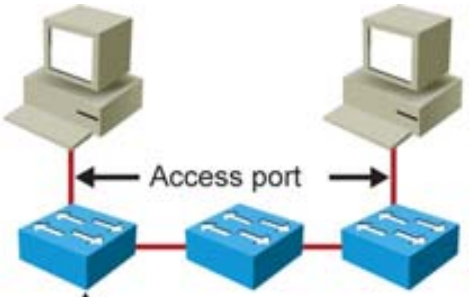
Cons

- More routing devices are required than in end-to-end models.
- Users belong to the same broadcast domain when they are at the same location.

The end-to-end VLANs design model was attractive when IP addressing was static and network traffic followed the 80/20 rule.

VLANs – VLAN configuration

- Configure VLANs on all switches.
- Configure access mode on port.
- Configure access VLAN on port.




```
switch(config)# vlan 3
switch(config-vlan)# name Accounting
switch(config-vlan)# exit
switch(config)# interface fa0/1
switch(config-if)# switchport mode access
switch(config-if)# switchport acces vlan 3
switch(config-if)# end
```

SW1(config)# vlan 99

SW1(config-vlan)# name Guests

SW1(config-vlan)# interface gi1/0/15

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan 99

SW1(config-if)# interface gi1/0/16

SW1(config-if)# switchport mode access

SW1(config-if)# switchport access vlan name Gues

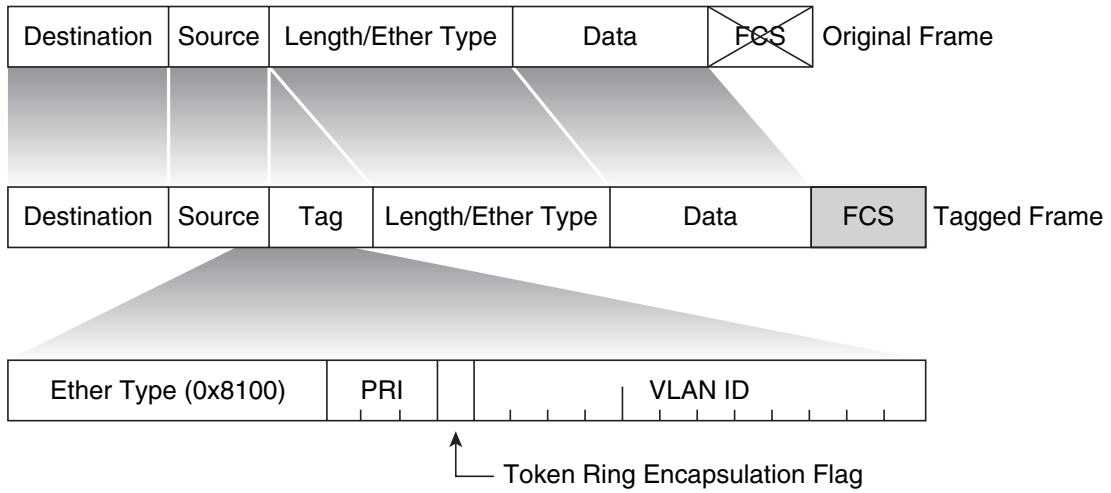
VLANs – VLAN verification

```
Switch# show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active
2    Marketing                           active    Fa0/2, Fa0/5
3    Accounting                          active    Fa0/1, Fa0/4
99   VLAN0099                            active
1002 fddi-default                        act/unsup
1003 token-ring-default                  act/unsup
1004 fddinet-default                     act/unsup
1005 trnet-default                       act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
99   enet  100003     1500  -      -      -        -    -        0      0
```

VLANs – Trunks

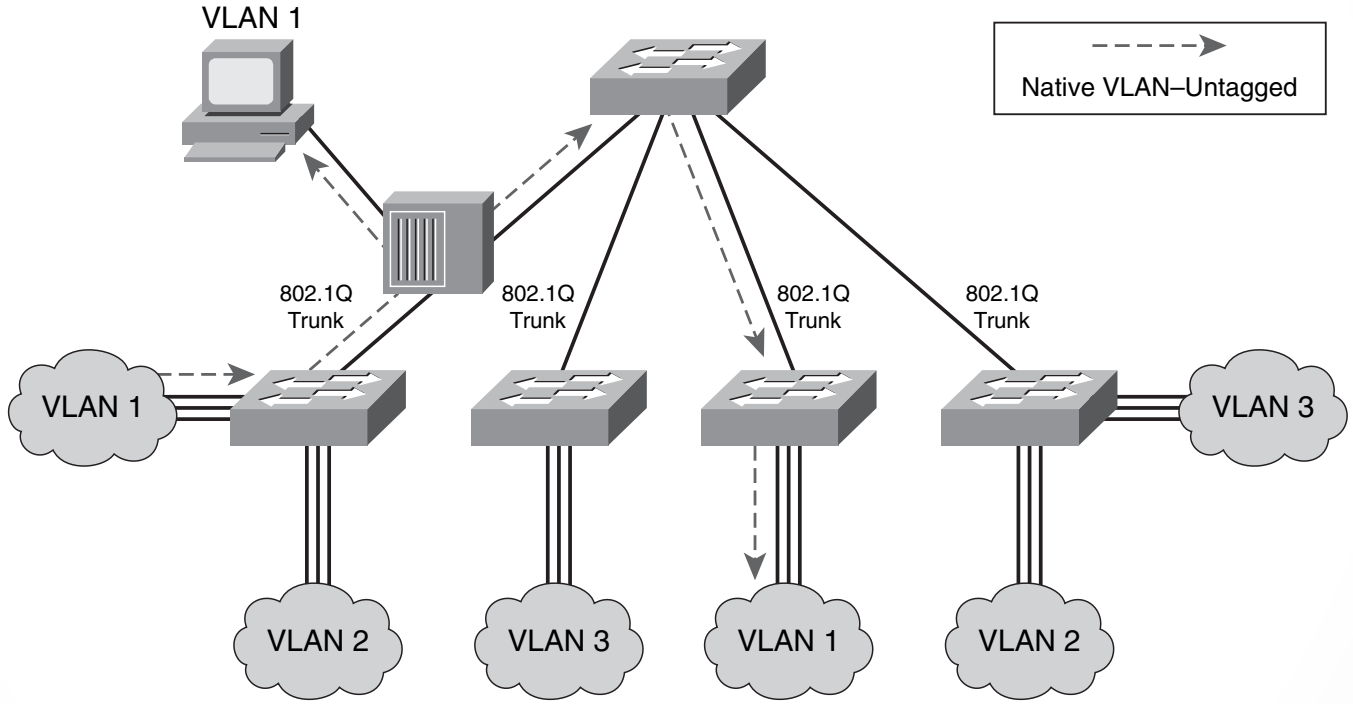
A *trunk* is a point-to-point link between one or more Ethernet switch interfaces that carries the traffic of multiple VLANs.

802.1Q Frame



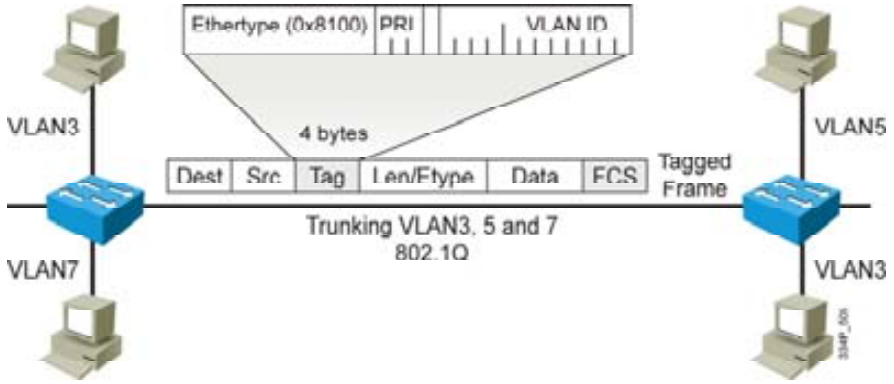
VLANs – Trunks

802.1Q does not tag frames for the native VLAN.



VLANs – Trunks configuration

- Configure VLANs.
- Disable trunk negotiation.
- Configure trunk mode.
- Set native VLAN to unused VLAN.
- Allow only required VLANs on trunks.




```
switch(config)# vlan 5,7-9
switch(config-vlan)# exit
switch(config)# interface fastethernet 0/1
switch(config-if)# shutdown
switch(config-if)# switchport trunk encapsulation dot1q
switch(config-if)# switchport nonegotiate
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 99
switch(config-if)# switchport trunk allowed vlan 3,5,8,99
switch(config-if)# no shutdown
```

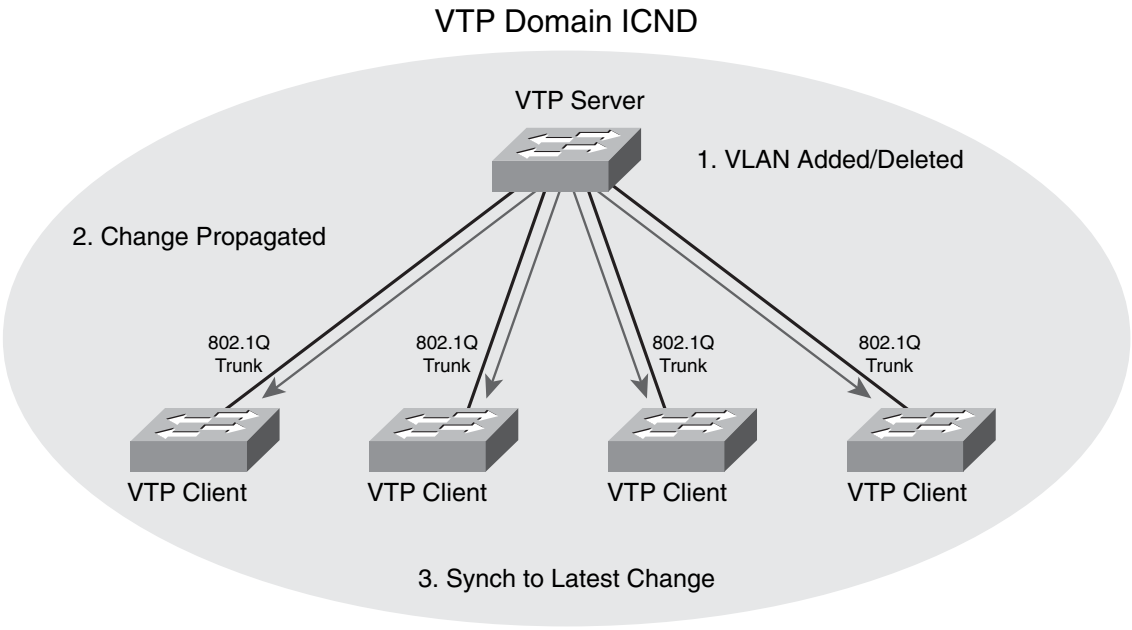
VLANs – Trunks configuration mode Interaction DTP (Dynamic Trunking Protocol)

- Configure the port as trunk or access on both switches.
- Disable negotiation and do not use dynamic (default).
- Manual configuration is recommended.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

VLANs – VLAN Trunking Protocol

(VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the additions, deletions, and name changes of VLANs across networks.



VLANs – VLAN Trunking Protocol modes

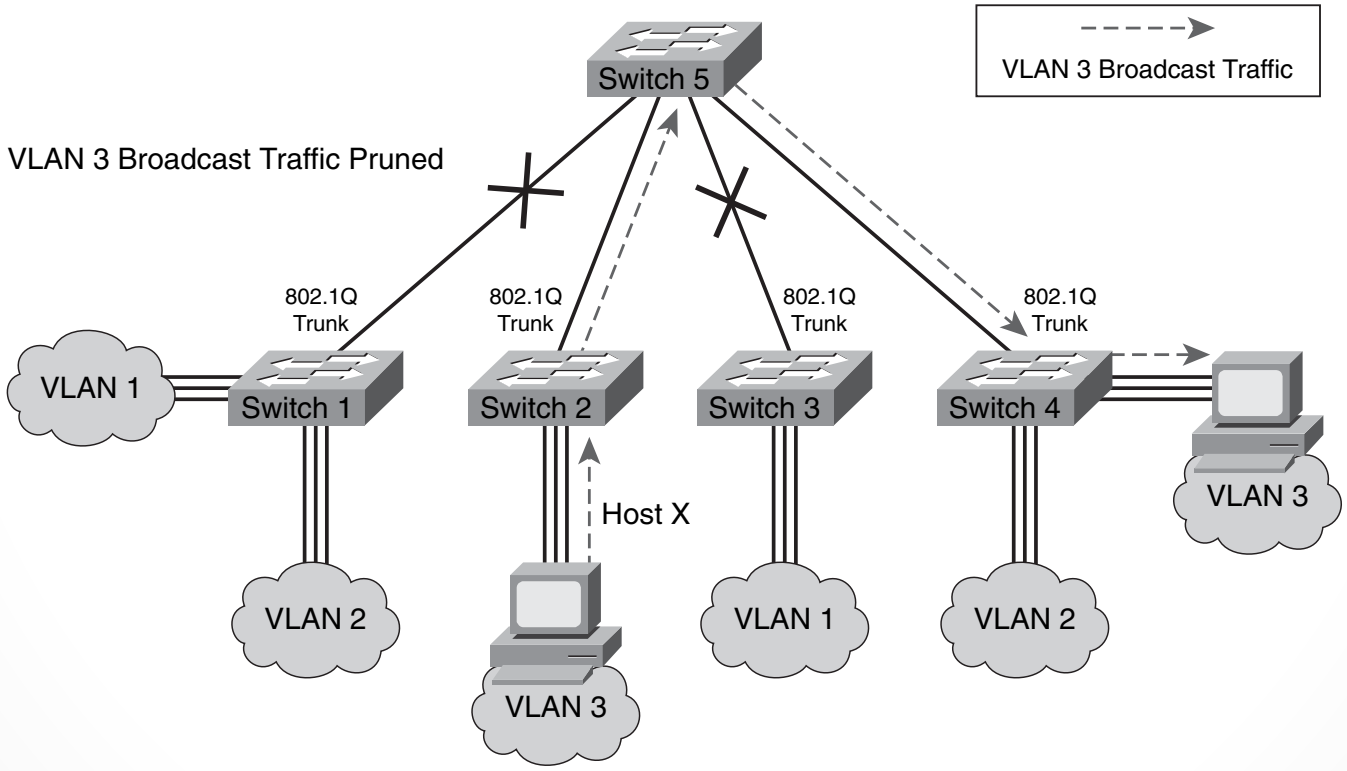
- **Server:** The default VTP mode is server mode, but VLANs are not propagated over the network until a management domain name is specified or learned.

- **Transparent:** When you change the VLAN configuration in VTP transparent mode, the change affects only the local switch and does not propagate to other switches in the VTP domain.

- **Client:** You cannot change the VLAN configuration when in VTP client mode; however, a VTP client can send any VLANs currently listed in its database to other VTP switches.

VLANs – VLAN Trunking Protocol (VTP) pruning

VTP pruning uses VLAN advertisements to determine when a trunk connection is flooding traffic needlessly.



VLANs –VTP configuration

- Configure VTP mode transparent (mode server is default).
- VLAN information is stored in switch configuration.
- No VTP advertisment to other switches.
- Recommended configuration.

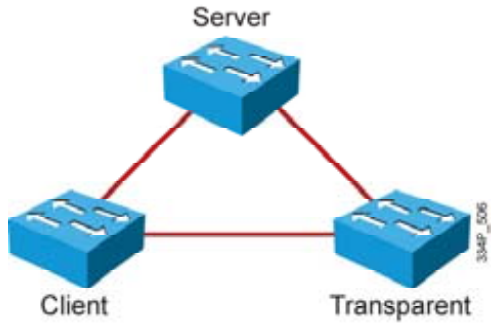
```
switch(config)# vtp mode transparent
switch(config)# vtp domain Cisco
switch(config)# vtp password xyz123
```

VLANs –VTP verification

```
Switch# show vtp status
VTP Version                     : running VTP1 (VTP2 capable)
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 15
VTP Operating Mode              : Transparent
VTP Domain Name                 : XYZ
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x56 0x8B 0x47 0x72 0x63 0xE4 0x6B
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

VLANs –VTP problems

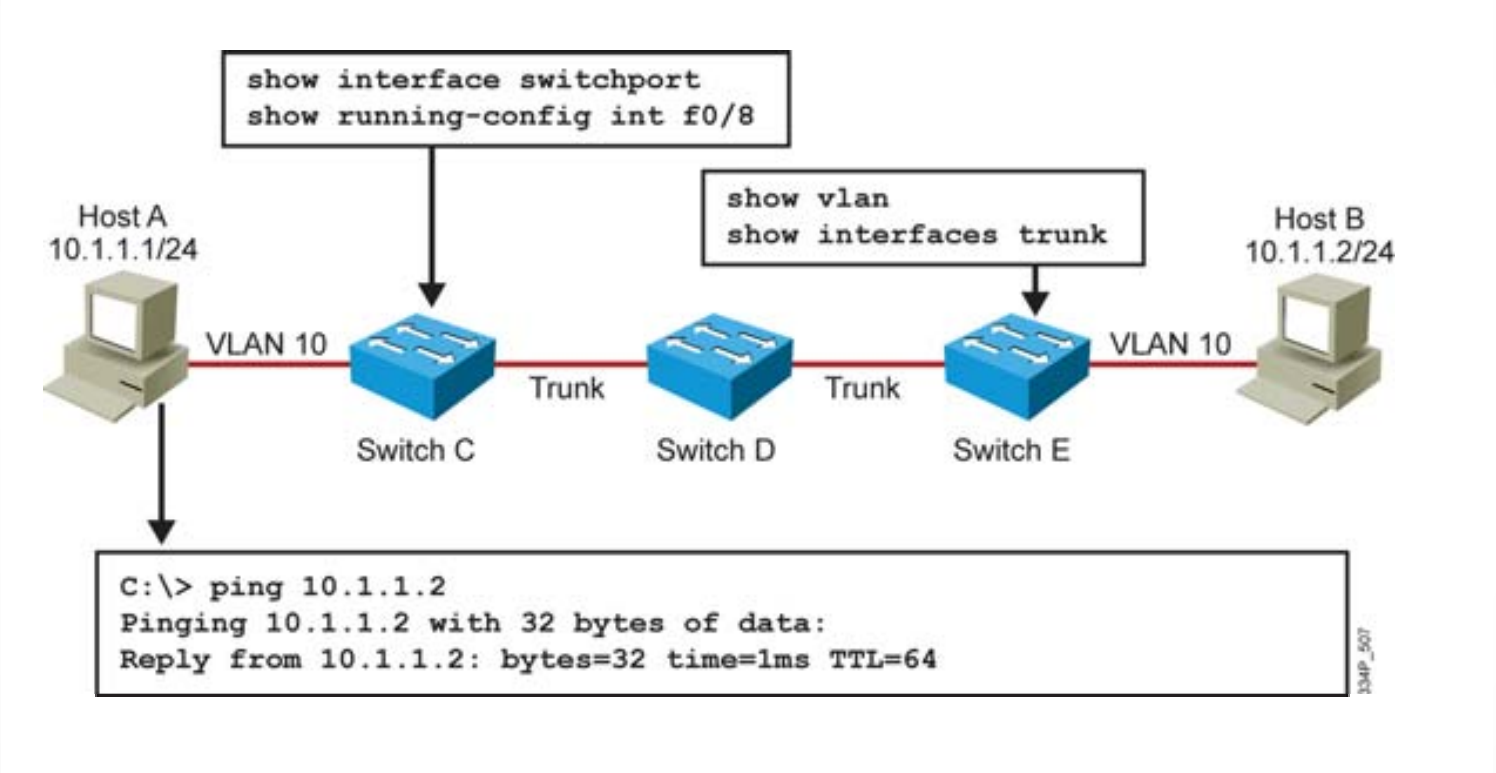
- Missing VLANs
  - Configuration has been overwritten by another VTP device.
- Updates not received as expected
  - VTP domain and password must match.
- Too many VLANs
  - Consider making VTP domain smaller.



VLANs – Trunks configuration recommendations

- Configure VLANs.
- Configure trunk mode.
- Disable trunk negotiation.
- Manually remove unnecessary VLANs from trunks.
- Configure native VLAN to unused VLAN.
- Disable trunking on host ports.
- Do not use VTP.

VLANs –Verification and Troubleshooting



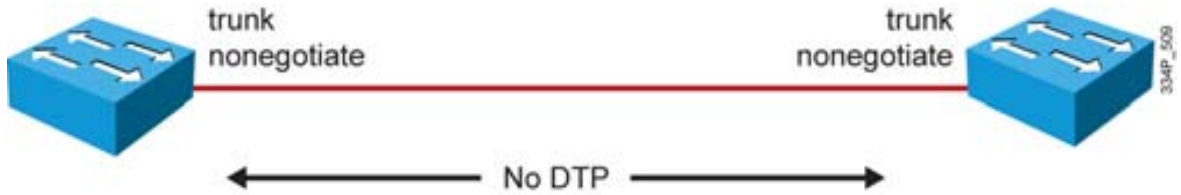
VLANs –Verification and Troubleshooting

Original implementation plan: Create new VLAN for new class of users.

- Create VLAN.
  - Was the VLAN added to all switches?
  - Is it manually pruned somewhere?
- Add new users to ports.
  - Is the correct VLAN configured on the port?
  - Is the port enabled?
  - Is it enabled as a switch port?
- Verify connectivity.
  - Are all links set to trunk?
  - Is the VLAN allowed on all trunks?
  - Is spanning tree blocking a link?

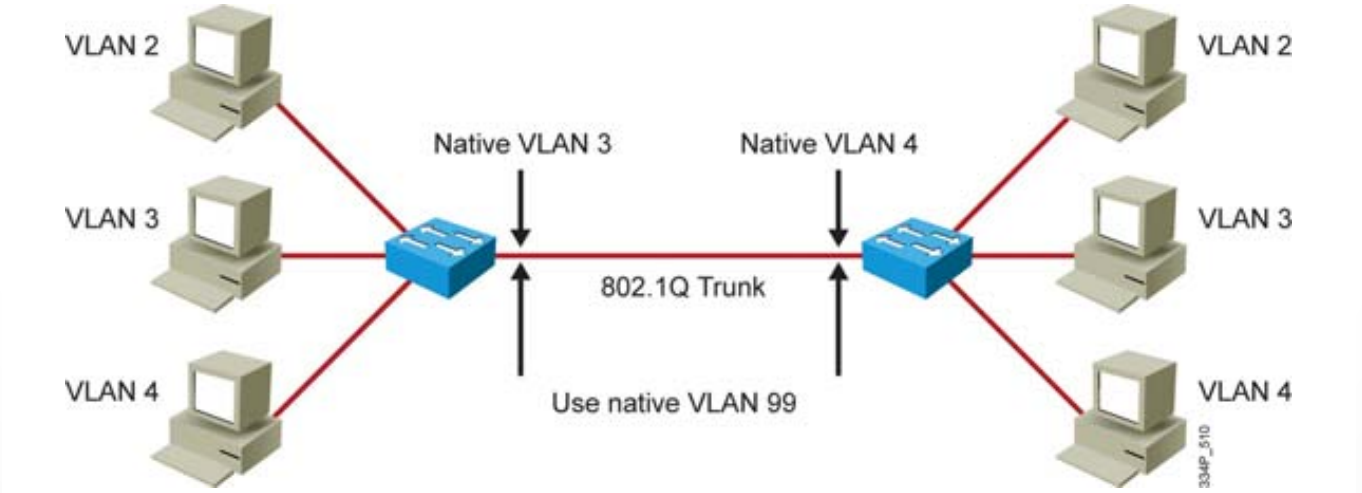
VLANs –Verification and Troubleshooting trunks

- When using DTP, ensure that both ends of the link are in the same VTP domain.
- Ensure that the trunk encapsulation type configured on both ends of the link is valid.
- On links where trunking is not required, DTP should be turned off.
- The best practice is to configure the trunk with **nonegotiate** where trunks are required.



VLANs –Verification and Troubleshooting trunks

- Native VLAN frames are carried over the trunk link untagged.
- Native VLAN must match at the ends of a trunk.
- A native VLAN mismatch will merge traffic between VLANs.
- Default native VLAN is VLAN 1.
- Configure an unused VLAN as native VLAN on trunks.

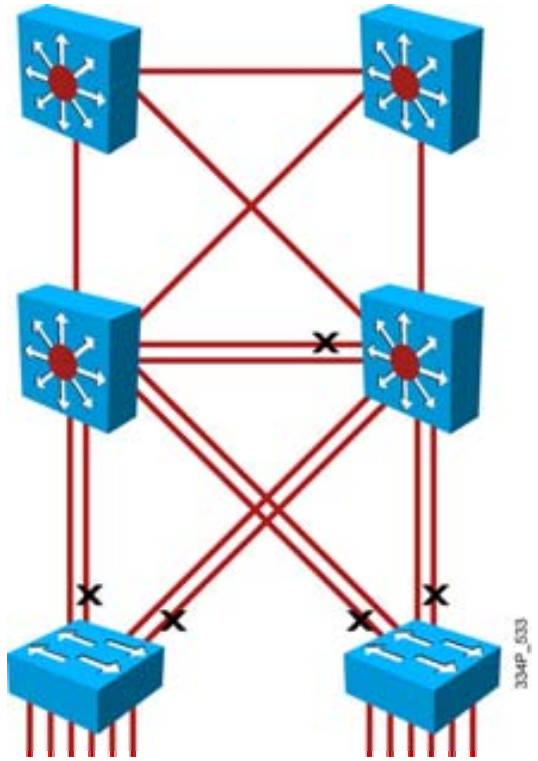


VLANs –Summary

- VLAN segmentation is based on traffic flow patterns.
- The creation of a VLAN implementation plan depends on the business and technical requirements.
- VLAN configuration includes creating the VLAN, configuring access ports, and configuring trunk ports.
- VTP configuration sometimes needs to be added to small network deployments, while VTP transparent mode is usually privileged for larger networks.
- When configuring VLANs over several switches, ensure that the configuration is compatible throughout switches in the same domain.

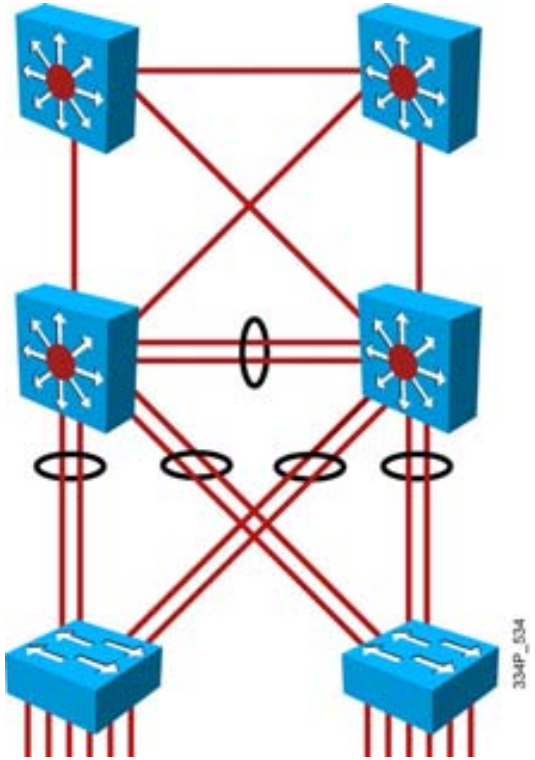
Link Aggregation

- When multiple links aggregate on a switch, congestion occurs.
- One solution is to increase uplink speed, but cannot scale indefinitely.
- Another solution is to multiply uplinks; loop prevention mechanisms disable some ports.



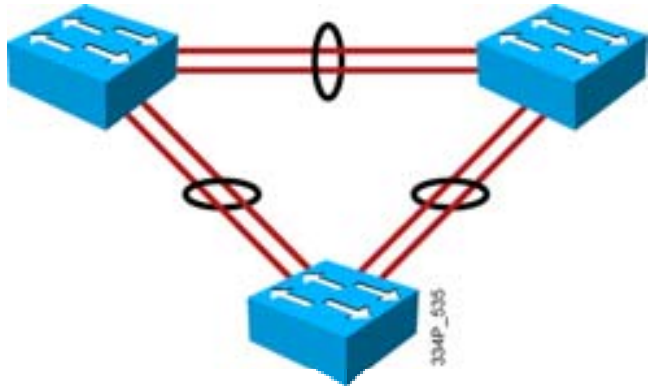
Link Aggregation

- Solution to provide more bandwidth
- Logical aggregation of similar links
- Viewed as one logical link
- Provides load balancing and redundancy
- Supported for switch ports (Layer 2) and routed ports (Layer 3)



Link Aggregation EtherChannel - PAgP and LACP

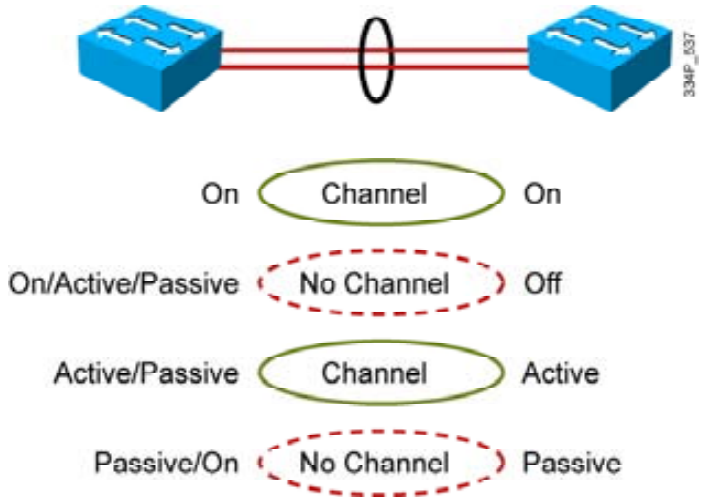
- Protocols to negotiate the EtherChannel link creation and maintenance.
- PAgP is a Cisco proprietary protocol.
- LACP is IEEE 802.3ad standard.
- Static EtherChannel configuration without protocol.



Link Aggregation EtherChannel - LACP standard

LACP negotiates EtherChannel formation and maintenance:

- On: channel member without negotiation (no protocol)
- Active: actively ask if the other side can/will
- Passive: passively wait for other side to ask
- Off: EtherChannel not configured on interface



Link Aggregation EtherChannel - Configuration

Basics tasks:

- Identify the ports to use on each switch.
- Configure channel group on interface.
  - Specify a channel group number.
  - Specify the mode (will set protocol)
    - On (no protocol needed)
    - Active / Passive
- Configure port-channel interface.
  - Access or trunk mode and other parameters.
- Verify connectivity.

Link Aggregation EtherChannel - Configuration

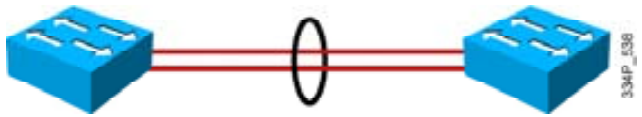
Port-channel interface configuration changes affect the EtherChannel.

The physical interface configuration changes affect the interface only.

EtherChannel cannot be used if SPAN is a destination port.

All interfaces within an EtherChannel must have same configuration.

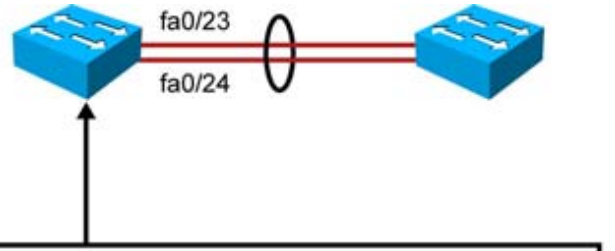
- Same speed and duplex.
- Same mode (access or trunk).
- Same native and allowed VLANs on trunk ports.
- Same access VLAN on access ports.
- Configure these parameters on the port-channel interface.



Link Aggregation EtherChannel – Configuration L2

- Channel group mode options:
  - On
  - Active or passive (LACP)

- The configuration on a port-channel interface is copied to member interfaces.




```
switch(config)# interface fastethernet 0/23
switch(config-if)# channel-group 1 mode active
switch(config)# interface fastethernet 0/24
switch(config-if)# channel-group 1 mode active
switch(config)# interface port-channel 1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 99
switch(config-if)# switchport trunk allowed vlan 2,3,99
```

Link Aggregation EtherChannel - Verification

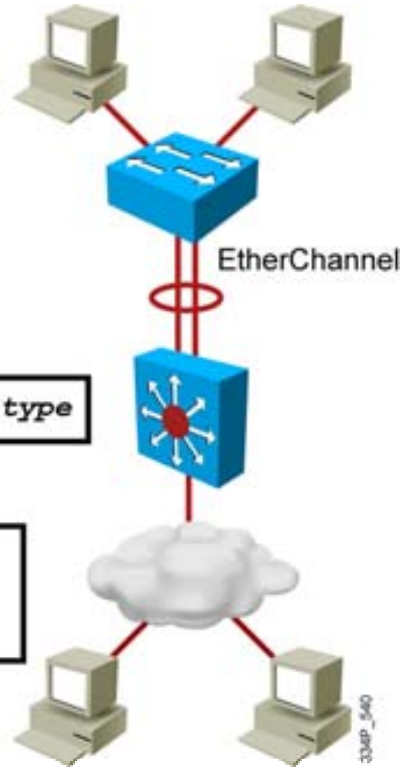
```
Switch#show interfaces f0/24 etherchannel
Port state    = Up Sngl-port-Bndl Mstr Not-in-Bndl
Channel group = 1     Mode = Active    Gcchange = -
Port-channel  = null  GC   =   -       Pseudo port-channel = Po1
Port index    = 0     Load = 0x00            Protocol =   LACP

Switch#show etherchannel 1 port-channel
                Port-channels in the group:
                ---------------------------
Port-channel: Po1    (Primary Aggregator)
Age of the Port-channel   = 195d:03h:10m:44s
Logical slot/port   = 0/1          Number of ports = 2
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+-----+------+------------------+-----------
  0     55     fa0/23    Active    4
  1     45     fa0/24    Active    4
```

Link Aggregation EtherChannel - Verification

```
switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------
2      Po1(SU)           -        Fa0/23(P)     Fa0/24(P)
```

Link Aggregation EtherChannel – Load Balancing

- EtherChannel load-balances traffic among port members of the same bundle.
- Load balancing can be based on MAC, port, or IP (source, destination, or both).
- Default: Source and destination IP address (**src-dst-ip**).




```
switch(config)# port-channel load-balance type
```

```
switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip
```

Link Aggregation EtherChannel – Summary

- EtherChannel increases bandwidth and provides redundancy by aggregating individual similar links between switches.
- EtherChannel can be dynamically configured between switches using either the Cisco proprietary PAgP or the IEEE 802.3ad LACP.
- EtherChannel is configured by assigning interfaces to the EtherChannel bundle and configuring the resulting port channel interface.
- EtherChannel load-balances traffic over all the links in the bundle. The method that is chosen directly impacts the efficiency of this load-balancing mechanism.