Badji Mokhtar University Annaba
Electronics Department

Lecture 3

Contact:
seifallah.nasri@univ-annaba.org

June 03, 2019 Annaba, Algeria

Review

Ethernet is the most used networking technology for LANs today. It defines wiring and signaling for the Physical layer of the OSI model. For the Data Link layer, it defines frame formats and protocols.

Ethernet is described as **IEEE 802.3** standard. It uses **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** access method and supports speeds up to 100 Gbps.
It can use coaxial, twisted pair and fiber optic cables.

.

The term **Ethernet LAN** refers to a combination of computers, switches, and different kinds of cables that use the Ethernet standard to communicate over the network. It is by far the most popular LAN technology today

Review

Preamble	SFD	Destination MAC	Source MAC	Type	Data and Pad	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

Preamble – informs the receiving system that a frame is starting and enables synchronisation.

SFD (Start Frame Delimiter) – signifies that the Destination MAC Address field begins with the next byte.

Destination MAC – identifies the receiving system.

Source MAC – identifies the sending system.

Type – defines the type of protocol inside the frame, for example IPv4 or IPv6.

Data and Pad – contains the payload data. Padding data is added to meet the minimum length requirement for this field (46 bytes).

FCS (Frame Check Sequence) – contains a 32-bit Cyclic Redundancy Check (CRC) which allows detection of corrupted data.

Review

Preamble	SFD	Destination MAC	Source MAC	Type	Data and Pad	FCS
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN
0x22F3	IETF TRILL Protocol
0x22EA	Stream Reservation Protocol
0x6002	DEC MOP RC
0x6003	DECnet Phase IV, DNA Routing
0x8035	Reverse Address Resolution Protocol (RARP)
0x809B	AppleTalk (Ethertalk)
0x80F3	AppleTalk Address Resolution Protocol (AARP)
0x8100	VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq with NNI compatibility
0x8102	Simple Loop Prevention Protocol (SLPP)
0x8137	IPX
0x8204	QNX Qnet
0x86DD	Internet Protocol Version 6 (IPv6)

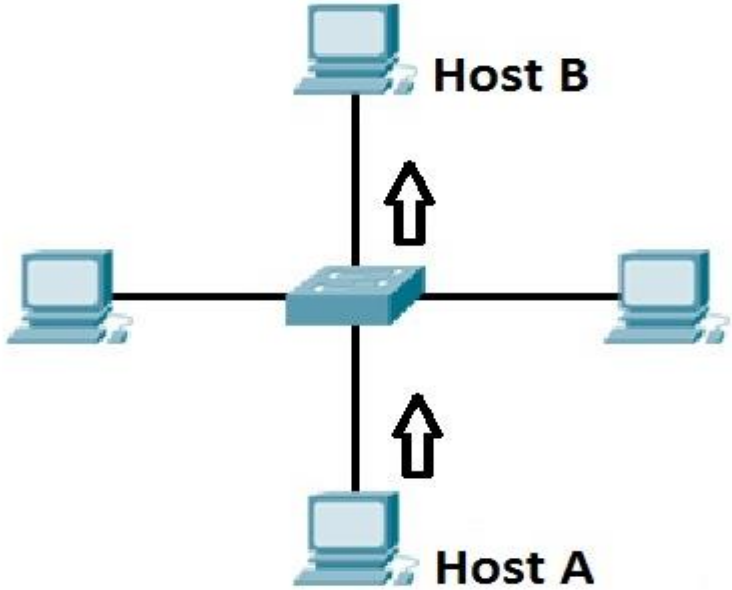
Review

- A hub serves as a central point to which all of the hosts in a network connect to.
- A Hub is an OSI Layer 1 device and has no concept of Ethernet frames or addressing.
- It simply receives a signal from one port and sends it out to all other ports

Review

- Switch is an OSI Layer 2 device, which means that it can inspect received traffic and make forwarding decisions.
- Each port on a switch is a separate collision domain and can run in a full duplex mode

Review



Host A is trying to communicate with Host B and sends a packet.

- ✓ A packet arrives at the switch, which looks at the destination MAC address.
- ✓ The switch then searches that address in its MAC address table.
- ✓ If the MAC address is found, the switch then forwards the packet only to the port that connected to the frame's destination.
- ✓ If the MAC address is not found, the switch will flood the frame out all other ports.
- ✓ To learn which MAC address is associated with which port, switches examine the source MAC addresses of the receiving packet and store that MAC addresses in their MAC address table

Review

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0030.f2e4.35d3    DYNAMIC     Fa0/1
   1    00e0.a38d.640b    DYNAMIC     Fa0/2
```

A MAC address table lists which MAC address is connected to which port. It is used by switches to make forwarding decisions.

The table is populated by examining the source MAC address of the incoming packet.

If the source MAC address of a packet is not present in the table, the switch adds an entry to it’s MAC address table.

Review

A router is a device that routes packets from one network to another. A router is most commonly an OSI Layer 3 device.

Routers divide broadcast domains and have traffic filtering capabilities.

A router uses IP addresses to figure out where to send packets. If two hosts from different networks want to communicate, they will need a router between them to route packets

Review

```
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    10.0.0.0/8 is directly connected, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/0
```

A routing table lists a route for every network that a router can reach. It can be statically configured (using IOS commands) or dynamically learned (using a routing protocol).

It is used by routers when deciding where to forward packets.

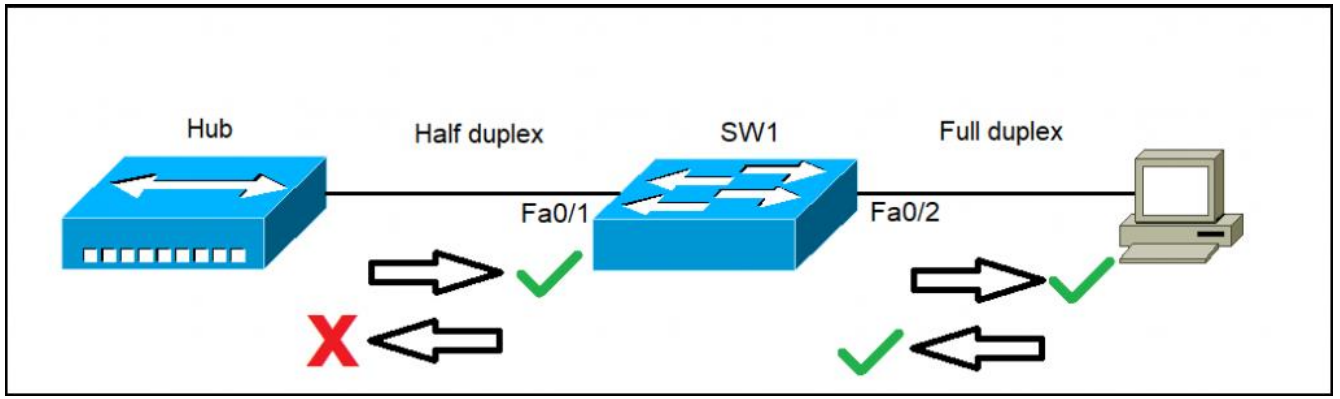
The command to display an IP routing table is ***show ip route***. In the picture above, you can see that this router has two directly connected subnets

```
C    10.0.0.0/8 is directly connected, FastEthernet0/1
```

C means that the route is a directly connected route. The network in question is 10.0.0.0/8, and the router will forward each packet destined for that network out interface FastEthernet0/1.

In Windows, you can use the ***netstat -r*** command to display the routing table of your system.

Review



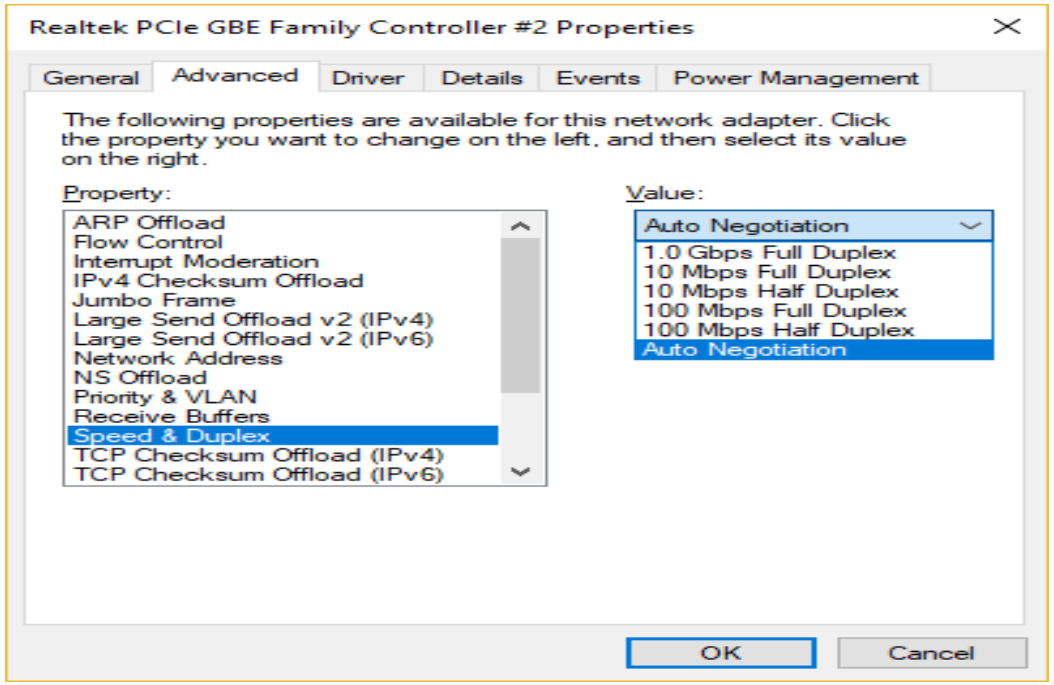
Half-duplex – a port can send data only when it is not receiving data. In other words, it cannot send and receive data at the same time. Network hubs run in half-duplex mode in order to prevent collisions. Since hubs are rare in modern LANs, the half-duplex system is not widely used in Ethernet networks anymore.

Full-duplex – all nodes can send and receive on their port at the same time. There are no collisions in full-duplex mode, but the host NIC and the switch port must support the full-duplex mode. Full-duplex Ethernet uses two pairs of wires at the same time instead of a single wire pair like half-duplex.

Review

Because hubs can only operate in half duplex, the switch and hub will negotiate to use half-duplex, which means that only one device can send data at the time. The workstation on the right supports full duplex, so the link between the switch and the workstation will use full duplex, with both devices sending data simultaneously.

Each NIC and switch port has a duplex setting. For all links between hosts and switches, or between switches, the full-duplex mode should be used. However, for all links connected to a LAN hub, the half-duplex mode should be used in order to prevent a duplex mismatch that could decrease network performance.
In Windows, you can set up duplex settings in the **Properties** window of your network adapter:



Collision & broadcast domain

Collision domain

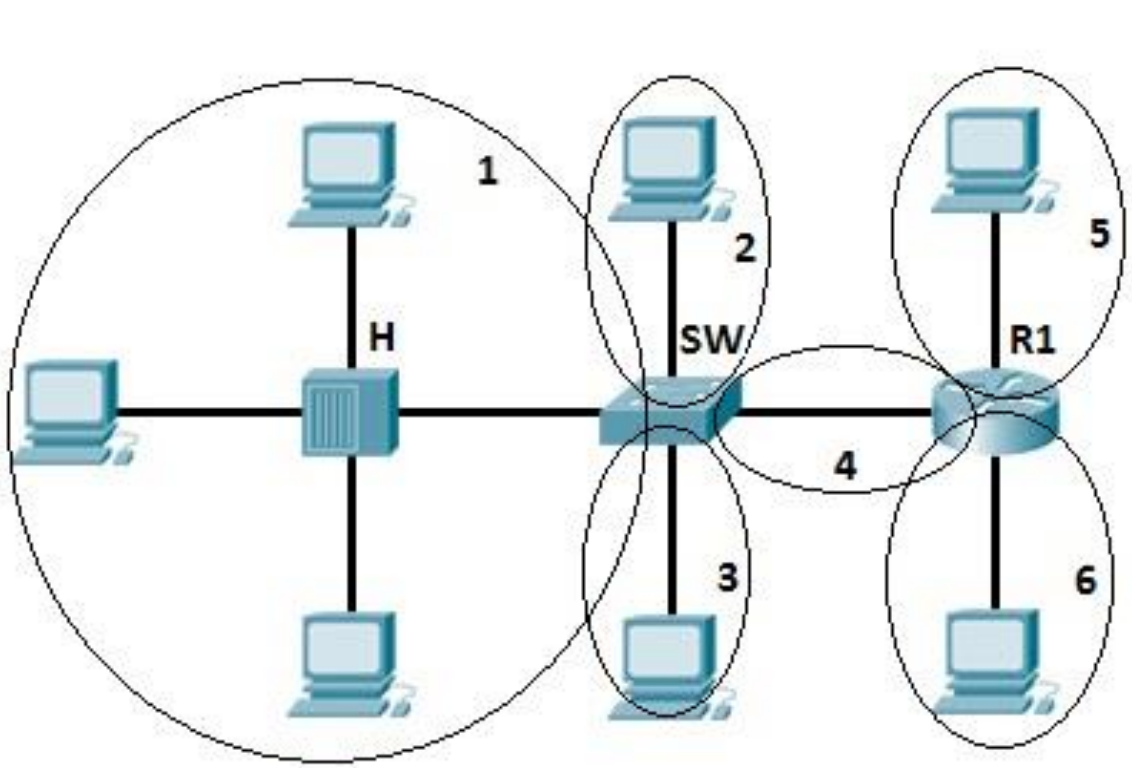
A collision domain is, as the name implies, the part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency. Collisions are often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain.

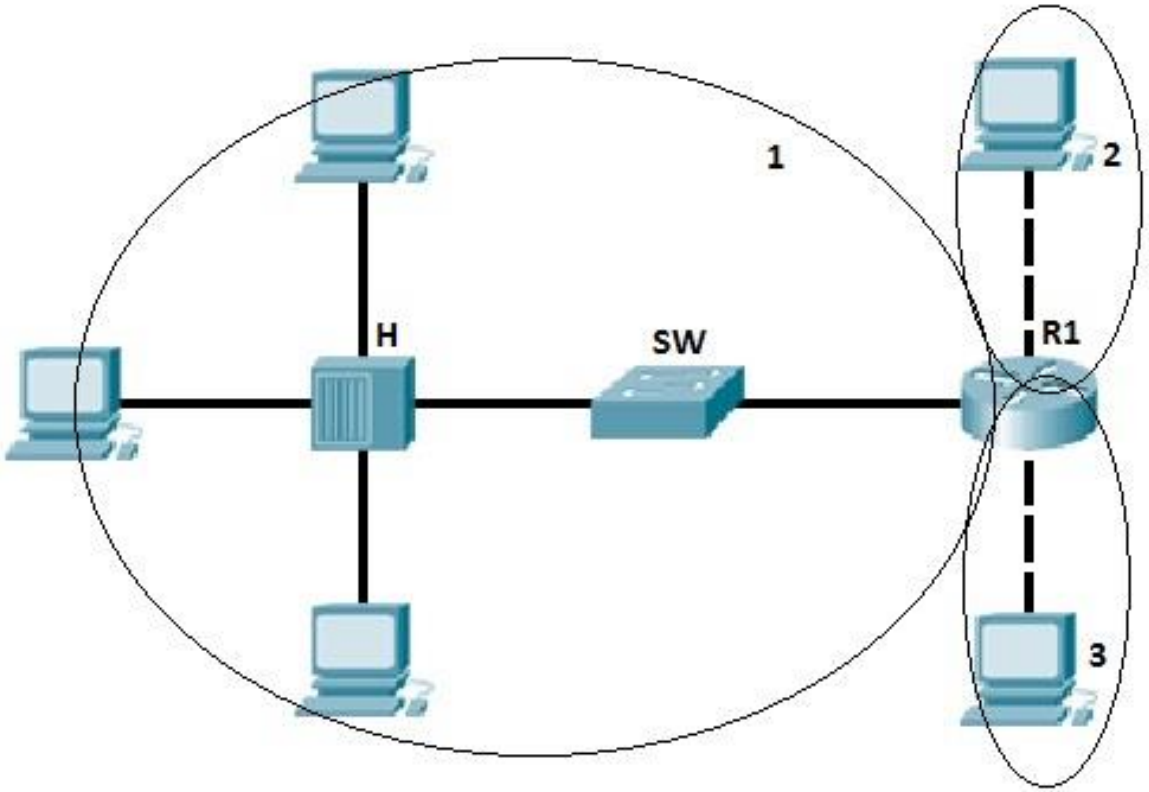
Broadcast domain

A broadcast domain is the domain in which a broadcast is forwarded. A broadcast domain contains all devices that can reach each other at the data link layer (OSI layer 2) by using broadcast. All ports on a hub or a switch are by default in the same broadcast domain. All ports on a router are in the different broadcast domains and routers don’t forward broadcasts from one broadcast domain to another.

Review

Collision & broadcast domain





Review

IEEE Ethernet standards

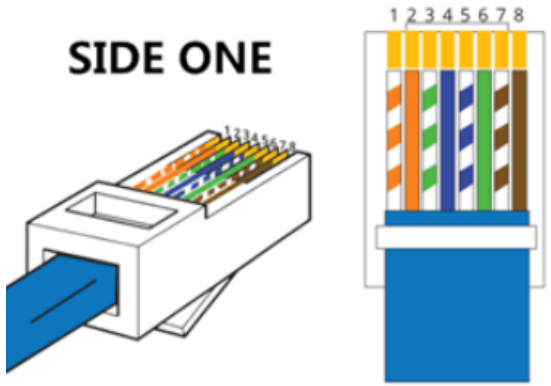
Ethernet is defined in a number of IEEE 802.3 standards. These standards define the physical and data-link layer specifications for Ethernet. The most important 802.3 standards are:

- **10Base-T (IEEE 802.3)** – 10 Mbps with category 3 unshielded twisted pair (UTP) wiring, up to 100 meters long.
- **100Base-TX (IEEE 802.3u)** – known as Fast Ethernet, uses category 5, 5E, or 6 UTP wiring, up to 100 meters long.
- **100Base-FX (IEEE 802.3u)** – a version of Fast Ethernet that uses multi-mode optical fiber. Up to 412 meters long.
- **1000Base-CX (IEEE 802.3z)** – uses copper twisted-pair cabling. Up to 25 meters long.
- **1000Base-T (IEEE 802.3ab)** – Gigabit Ethernet that uses Category 5 UTP wiring. Up to 100 meters long.
- **1000Base-SX (IEEE 802.3z)** – 1 Gigabit Ethernet running over multimode fiber-optic cable.
- **1000Base-LX (IEEE 802.3z)** – 1 Gigabit Ethernet running over single-mode fiber.
- **10GBase-T (802.3.an)** – 10 Gbps connections over category 5e, 6, and 7 UTP cables.

Review

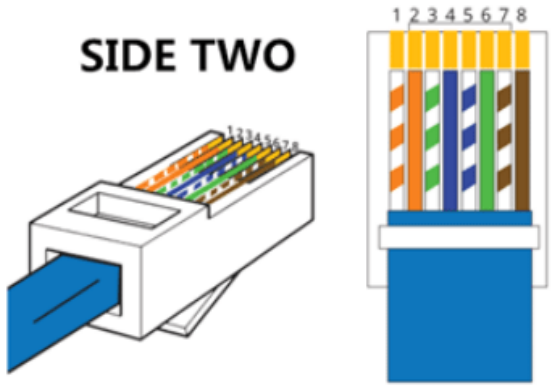
STRAIGHT-THROUGH

SIDE ONE



1. White Orange	5. White Blue
2. Orange	6. Green
3. White Green	7. White Brown
4. Blue	8. Brown

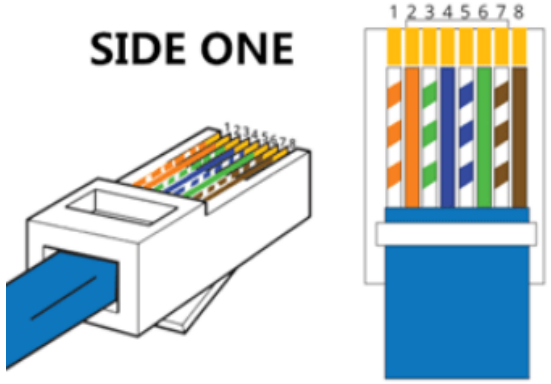
SIDE TWO



1. White Orange	5. White Blue
2. Orange	6. Green
3. White Green	7. White Brown
4. Blue	8. Brown

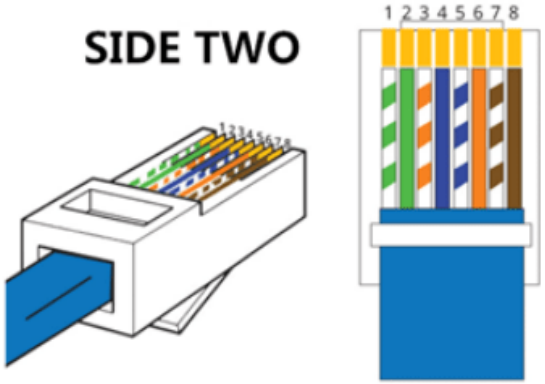
CROSSOVER

SIDE ONE

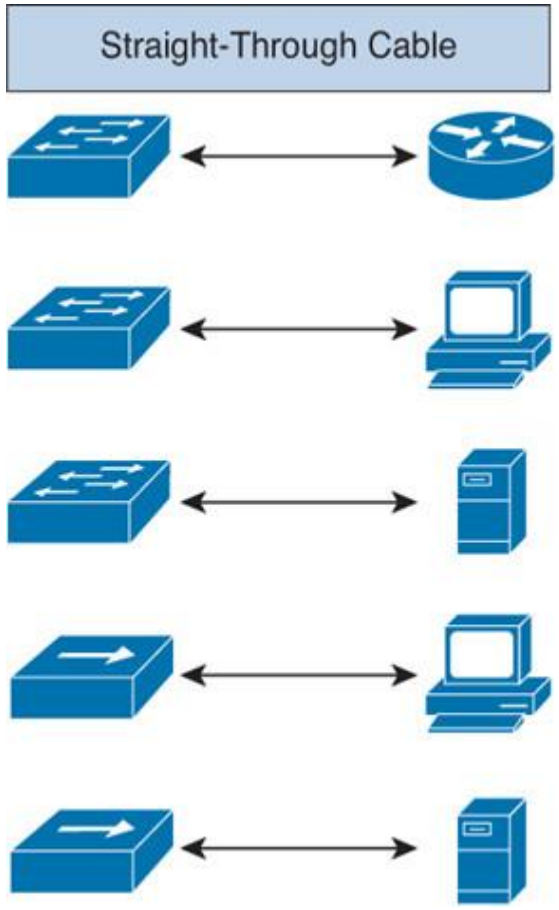


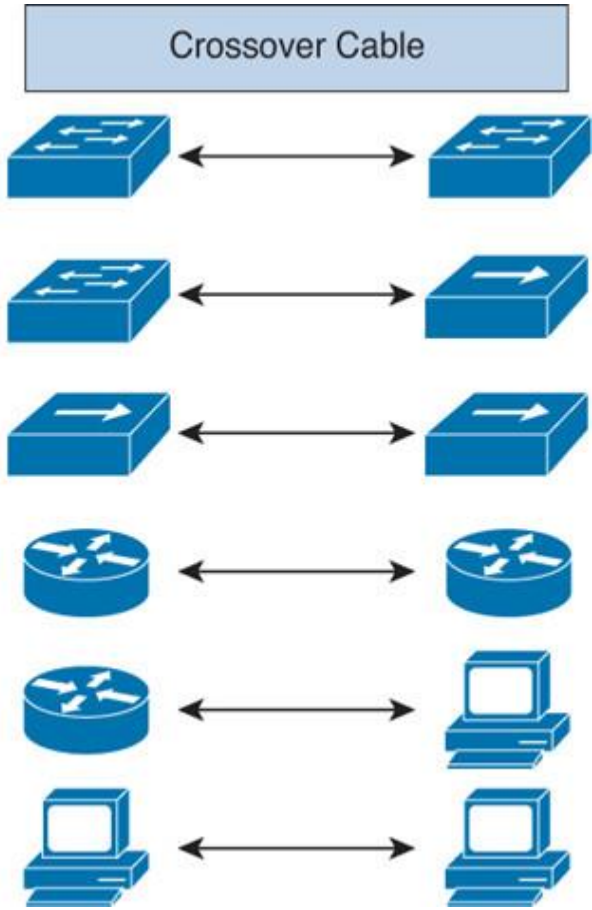
1. White Orange	5. White Blue
2. Orange	6. Green
3. White Green	7. White Brown
4. Blue	8. Brown

SIDE TWO



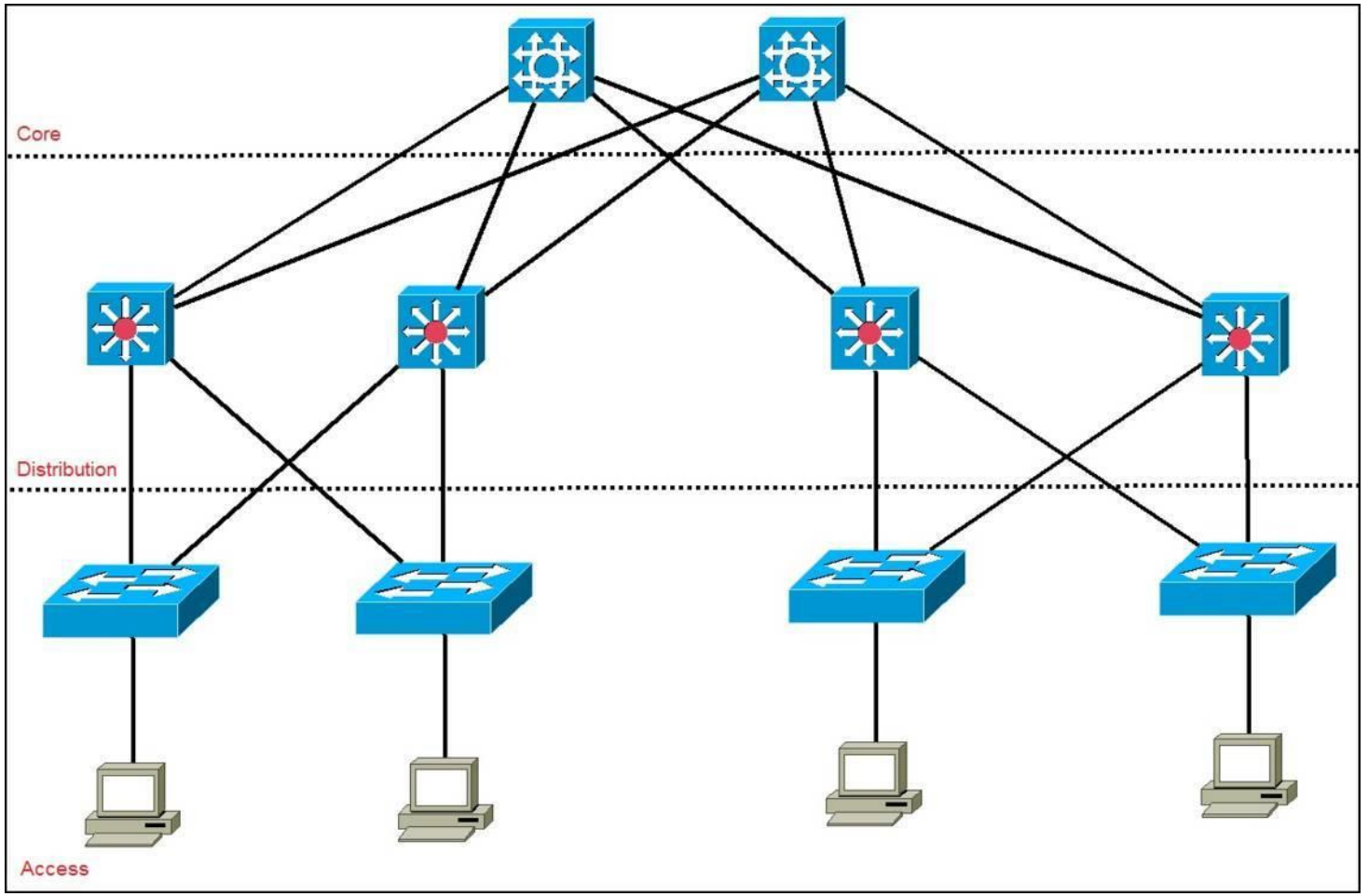
1. White Green	5. White Blue
2. Green	6. Orange
3. White Orange	7. White Brown
4. Blue	8. Brown





Review

Cisco three-layer hierarchical model



Access – controls user and workgroup access to the resources on the network.

This layer usually incorporates Layer 2 switches and access points that provide connectivity between workstations and servers.

You can manage access control and policy, create separate collision domains, and implement port security at this layer.

Review

•**Distribution** – serves as the communication point between the access layer and the core. Its primary functions are to provide routing, filtering, and WAN access and to determine how packets can access the core. This layer determines the fastest way that network service requests are accessed – for example, how a file request is forwarded to a server – and, if necessary, forwards the request to the core layer. This layer usually consists of routers and multilayer switches.

•**Core** – also referred to as the network backbone, this layer is responsible for transporting large amounts of traffic quickly. The core layer provides interconnectivity between distribution layer devices it usually consists of high speed devices, like high end routers and switches with redundant links.

Thank you for your attention