2019/5/8

Security Level:

CABLE TYPES, VLAN, TCP/IP MODEL STP, DHCP

Huawei Turkey Enterprise & Openlab

www.huawei.com

TRAINER: AHMET KAYHAN ŞEKER / 00263551

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential

Contents

VLAN	17
VLAN Advantages	18
VLAN Packets (IEEE 802.1Q)	19
VLAN Port Types	20
STP	21
DHCP	42

HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 3　HUAWEI
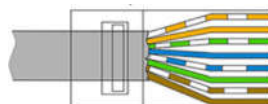
Cable Types

1990	1995	1999
Ethernet	Fast Ethernet	Gigabit Ethernet
10 mbps	100 mbps	1000 mbps
10 Base-T	100 Base-T	1000 Base-T ,1000 Base-LX, 1000 Base-SX
IEE 802.3	IEE 802.3u	IEE 802.3ab, IEE 802.3z
Cooper	Cooper	Cooper,Fiber
100 meters	100 meters	100 meters-cooper, 550 meters- SX, 5 Km-LX

Coaxial Cable

Twisted-Pair Cable

Fiber Cable

Thinnet :185m
Thicknet :500m

UTP (Unshielded Twisted-Pair) :100m
STP (Shielded Twisted-Pair) :100m

MM: 1000m- 40000m
SM:1000m-40000m

HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 4　HUAWEI

4-5: Pair1

1-2: Pair3

7-8: Pair4

3-6: Pair2

I send on Pair 3
I receive on Pair 2

Pair 3

Pair 2

I send on Pair 2
I receive on Pair 3

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 5
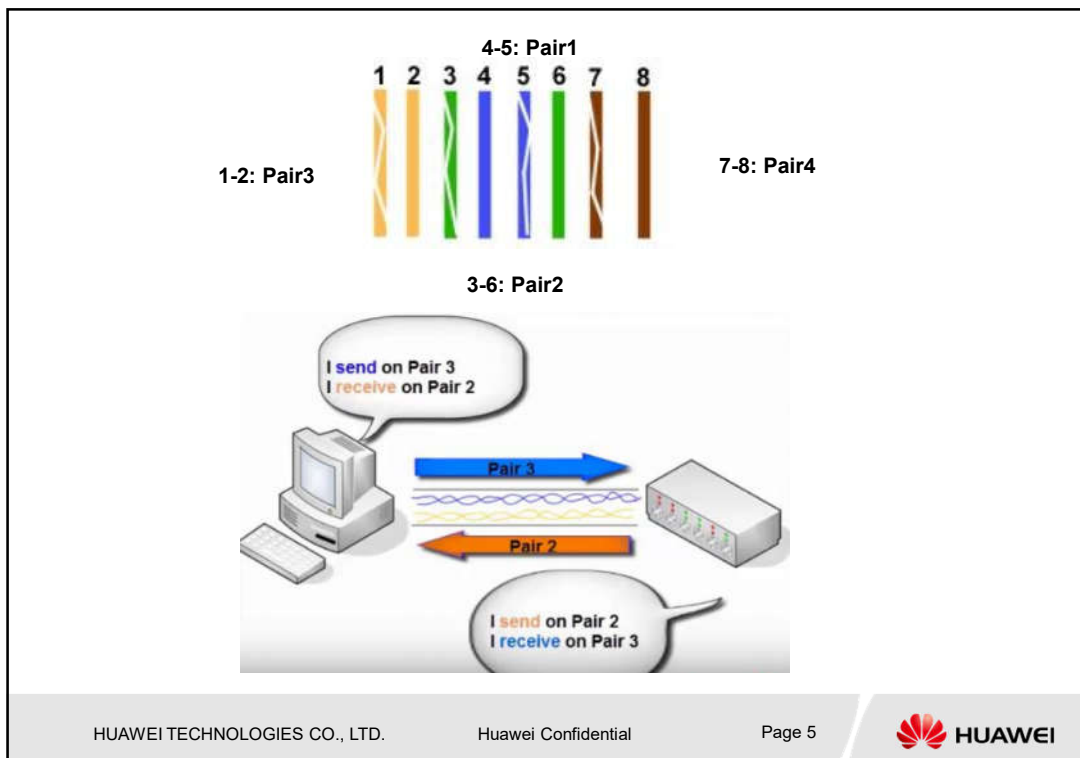
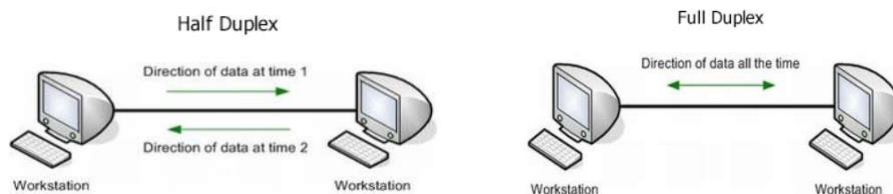
CSMA/CD

- Networks that use Ethernet technology determine which machine will be used at a given moment by means of a technique called CSR (Carrier Sense Multiple Access / Collision Detection). In this technique, the transmission line is controlled by the machine before the packets are sent. If the line is empty and is not currently used by someone else, it starts sending the packet. If the line is full, it waits for a while and continues to listen to the line. If two machines attempt to use the same line at the same time, a collision called collision occurs and both machines cannot transmit their packets.

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 6
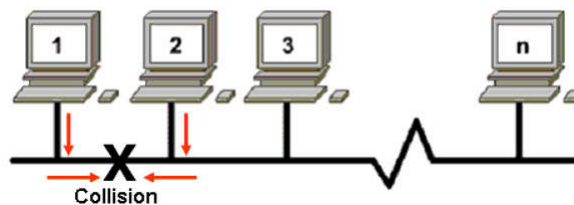
Half Duplex & Full Duplex

- **Half Duplex:** A station is a type of communication that allows the other station to receive only data while sending data. In half-duplex communication, devices can send and receive bi-directional data; but they cannot do this simultaneously. When more than one station tries to send data at the same time, the Ethernet protocol is activated to prevent conflicts. Walkie-talkie devices are good examples of half-duplex communication.
- **Full Duplex:** It is a type of communication that can perform data receiving and sending simultaneously. A station can send and receive data at the same time. In point-to-point, the 2nd Layer Data-Link layer determines whether the communication is half duplex or full duplex. In full-duplex communication, layer 2 defines the suitability of devices at both ends of the media for data transmission. There is no collision in full-duplex communication.

Half Duplex

Direction of data at time 1

Direction of data at time 2

Workstation   Workstation

Full Duplex

Direction of data all the time

Workstation   Workstation

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 7   HUAWEI

Unicast-Multicast-Broadcast

Unicast : It is the most secure connection form since it has a one to one connection with the IP to communicate.

UNICAST

Multicast : The way of contacting multiple groups with an IP is called Multicast. For example: There are a total of 7 machines on the network, you need to communicate with 4 of them. As a traffic 7 We can relieve the CPU by communicating with only 4 machines instead of sending data to the machine.

Subscriber

Subscriber

Hey? I do not want to receive it...

Broadcast

Nonsubscriber

Broadcast : It is necessary to use all the network communication. It has to be used very little because it uses more CPU usage, security vulnerabilities and time.

Subscriber

Subscriber

Do not Disturb. Thanks.

Multicast

Nonsubscriber
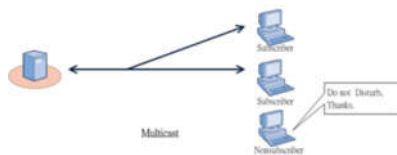
HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 8   HUAWEI

Collision Domain

- The collision domain, as its name suggests, is part of the 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 resend the packets; this also reduces network efficiency. Conflicts are usually in a hub environment, because each port in a hub is in the same collision area. Conversely, each port on the bridge, switch, or router is in a separate collision zone.
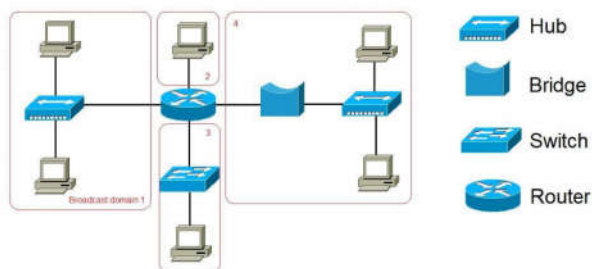
HUB	REPEATER	SWITCH	BRIDGE	ROUTER
Geçirir	Geçirir	Geçirmez	Geçirmez	Geçirmez

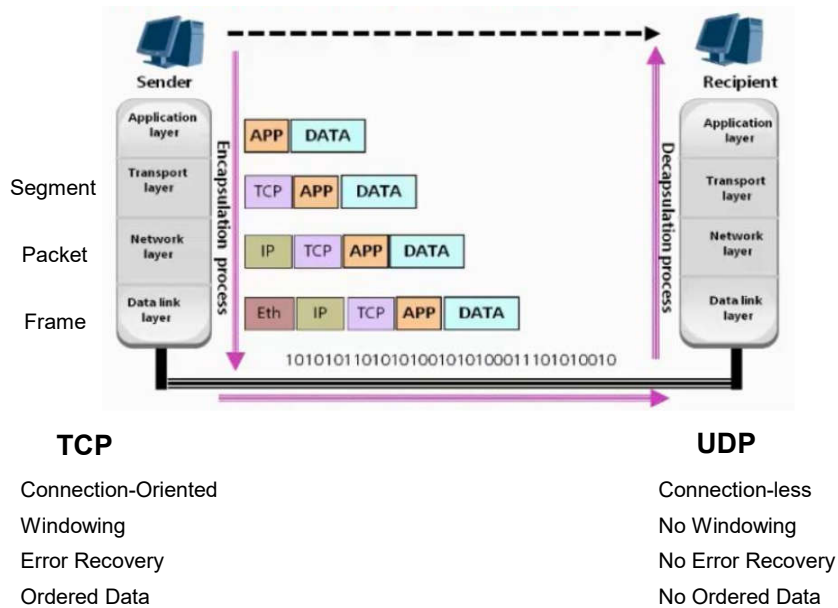HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 9　　HUAWEI
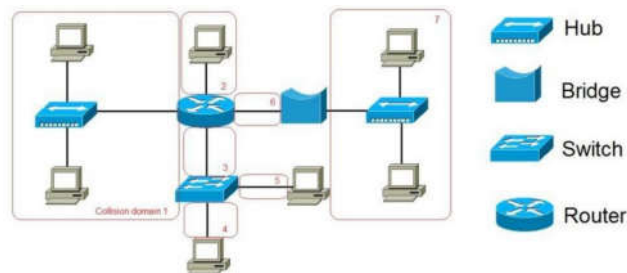
Broadcast Domain

- A broadcast domain is a domain name where the feed is transmitted. The broadcast domain contains all the devices that can access each other in the data link layer (OSI layer 2) using broadcast. All ports on a hub or switch are located by default in the same broadcast domain. All ports on a router are located in different broadcast areas, and routers do not redirect broadcasts from one broadcast area to another.

HUB	REPEATER	SWITCH	BRIDGE	ROUTER
Geçirir	Geçirir	Geçirir-Geçirmez	Geçirir	Geçirmez

HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 10　　HUAWEI

TCP/IP Model

TCP	UDP
Connection-Oriented	Connection-less
Windowing	No Windowing
Error Recovery	No Error Recovery
Ordered Data	No Ordered Data

TCP Connection 3-Way Handshake

SYN
SYN ACK
ACK

PC1   PC2
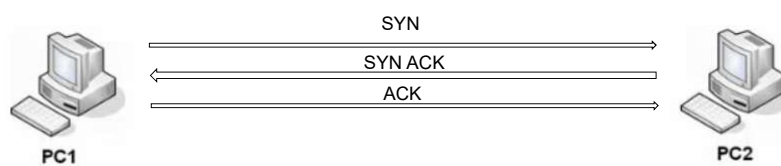
TCP Connection Termination

FIN
ACK
FIN
ACK

PC1   PC2

6
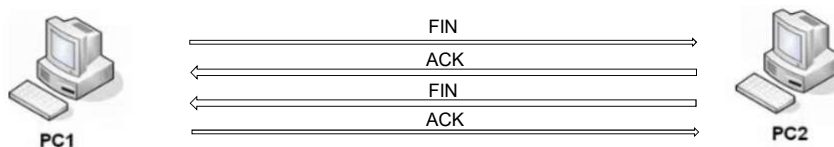
TCP Normal Data Transmission

Data 1

Data 2

ACK = 3

Data 3

PC1 / PC2

TCP Error Recovery

Data 1

Data 2

Data 3

ACK = 2

Data 2

ACK = 4

PC1 / PC2

HUAWEI

TCP Windowing

Window=2

1

2

ACK=3

3

4

ACK=5

PC1 / PC2

Window=1

1

ACK=2 , Window = 2

2

3

ACK=4

PC1 / PC2

HUAWEI
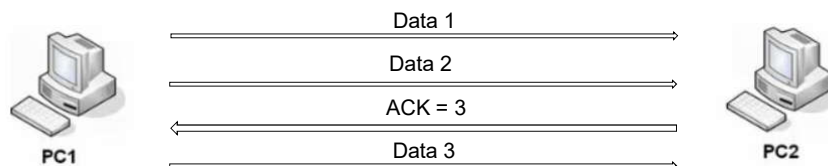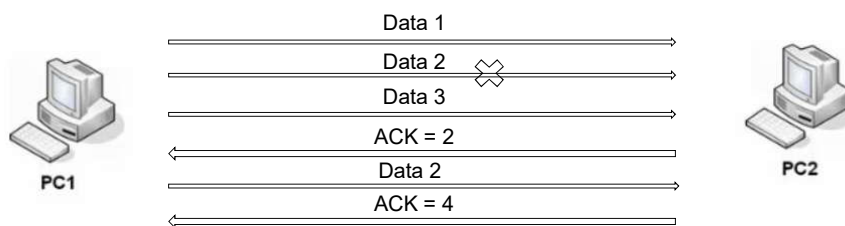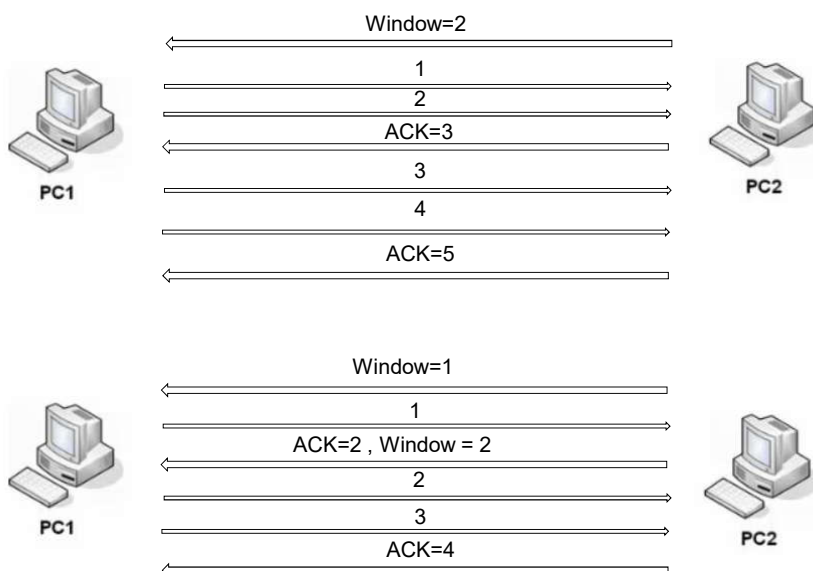
Ethernet II and IEEE 802.3 Packets

| | IP | 2048 (0x0800) |
| | ARP | 2054 (0x0806) |

bytes 8	6	6	2	46 - 1500	4
Preamble	Destination	Source	Type	Data Unit	CRC

DIX Ethernet Packet

bytes 7 1	6	6	2		46 - 1500		4
Preamble	Destination	Source	Length	LLC	Data Unit	Pad	FCS

Start of frame

IEEE 802.3 Frame

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 15   HUAWEI
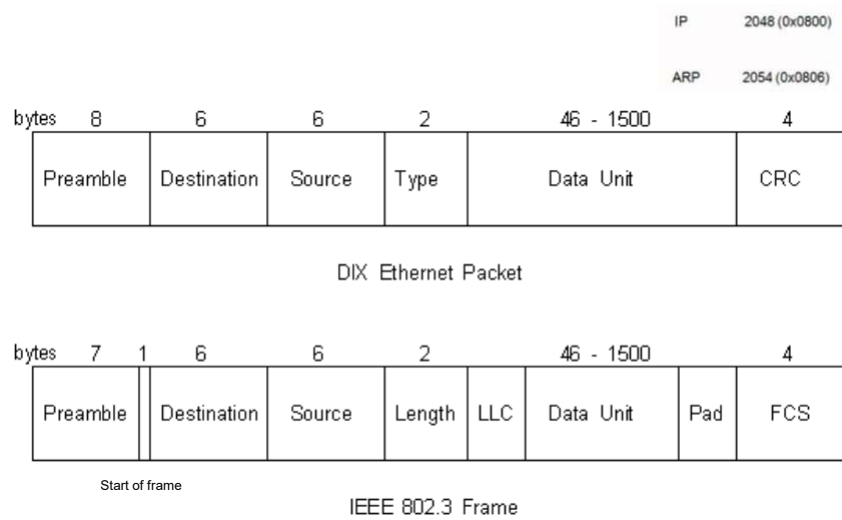
IP Package and Other Package Comparison

32 bits

Version	IHL	Type-of-Service	Total Length	
Identification			Flags	Fragmentation offset
Time-to-live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options (+ padding)				
Data (variable)				

Ethernet Packet: Receiver MAC-address | Sender MAC-address | Number of bytes | Data

IP Packet: V | IHL | ToS | L | ID | FL | fO | ttl | Prot | CHs | Sender IP-address | Receiver IP-address | Data

TCP Packet: Sender Port number | Receiver Port number | S# | Ack# | Fl | CHs | Data

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 16   HUAWEI
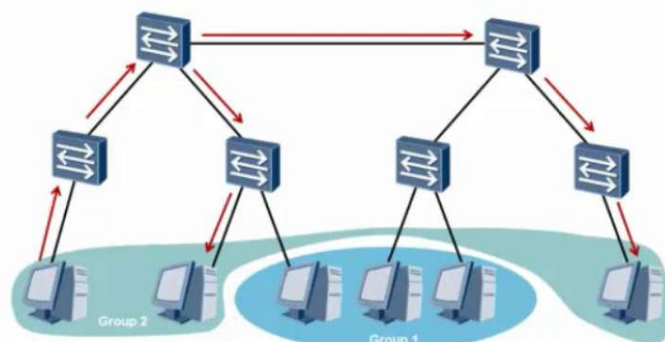
VLAN

VLans are virtual networks. Vlan's are used to distinguish keyed networks into segments. Vlan's provide a way to group devices within the LAN. Physical links take place instead of logical networks. There are 2 main purposes. They distinguish between safety and broadcasting.

HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 17　　**HUAWEI**
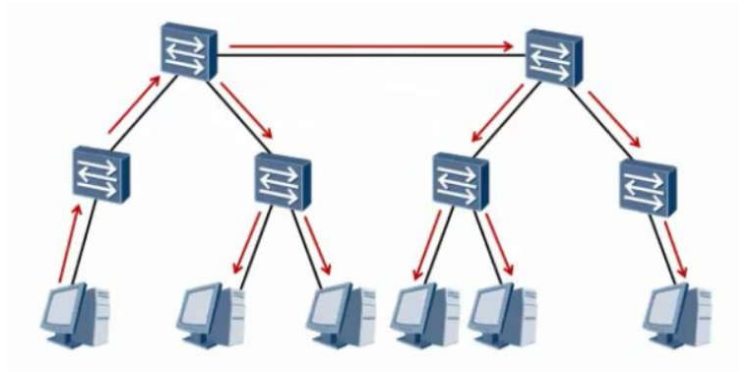
VLAN Advantages
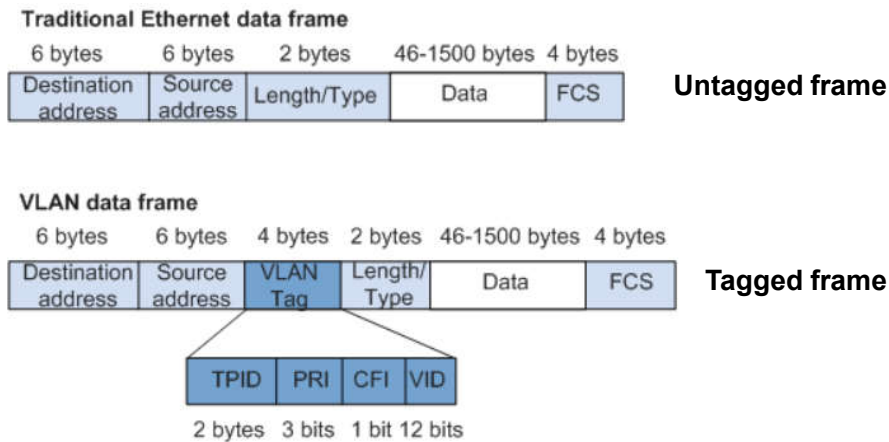
-Enhanced security　　　　-Decreasing cost　　　　-More smaller public broadcast switches

-Better performance　　　-BT efficiency　　　　-Management efficiency

● A VLAN enables logical isolation of traffic at the data link layer.

HUAWEI TECHNOLOGIES CO., LTD.　　Huawei Confidential　　Page 18　　**HUAWEI**

VLAN Packets (IEEE 802.1Q)

VLAN: 1- 4094

Traditional Ethernet data frame

Destination address	Source address	Length/Type	Data	FCS
6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Untagged frame

VLAN data frame

Destination address	Source address	VLAN Tag	Length/Type	Data	FCS
6 bytes	6 bytes	4 bytes	2 bytes	46-1500 bytes	4 bytes

Tagged frame

TPID	PRI	CFI	VID
2 bytes	3 bits	1 bit	12 bits

VLAN Port Types

| Port Type	UnTagged Frame Processing	Tagged Frame Processing	Frame Processing
Access port	Gets an untagged frame and adds a tag with the default VLAN ID to the frame.	If the VLAN ID of the frame matches the default VLAN ID, it accepts the tagged frame. If the VLAN ID of the frame differs from the default VLAN ID, it rejects the tagged.	After the PVID tag is removed, the frame is transmitted.
Trunk Port	Adds a tag to the untagged frame with the default VLAN ID and forwards the default VLAN ID if the interface is allowed. Adds a tag with the default VLAN ID to the unlabeled frame and then discards the default VLAN ID if it is rejected by the interface.	If the interface to the VLAN ID is allowed in the frame, it accepts a tagged frame. If the VLAN ID carried in the frame is rejected by the interface, it assigns a tagged frame.	If the VLAN ID of the frame matches the default VLAN ID and the interface permits the VLAN ID, the device removes the tag and transmits the frame. If the VLAN ID of the frame is different from the default VLAN ID, but the VLAN ID is still allowed by the interface, the device transmits the frame directly.

STP

Broadcast Storms
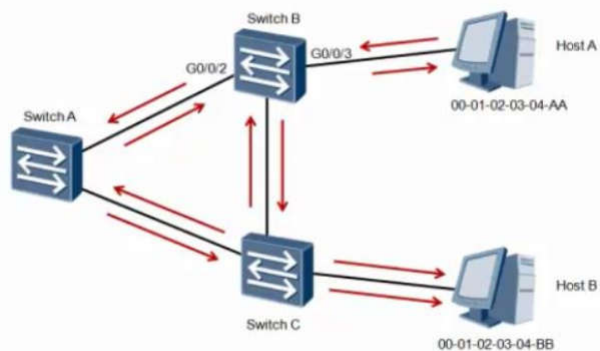
- Switching loops allow for broadcast storms to occur and duplication of frames to be received by end stations.
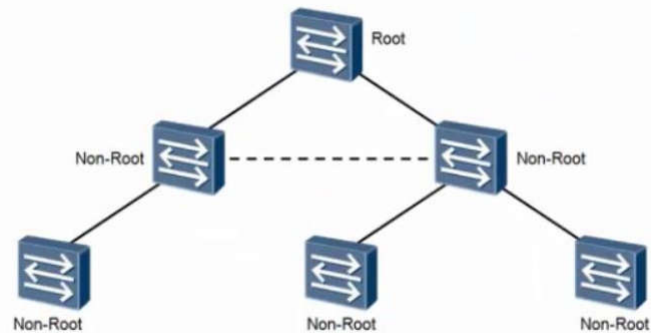
STP-2

Resolving Layer 2 Redundancy Issues
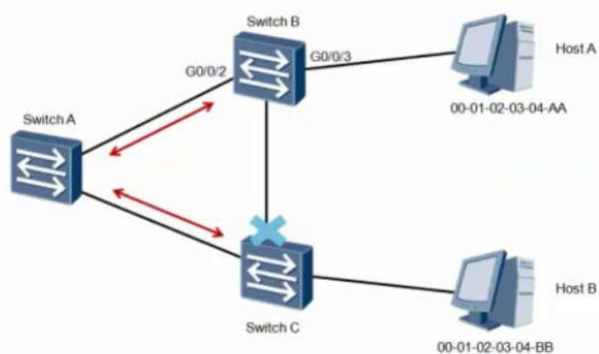
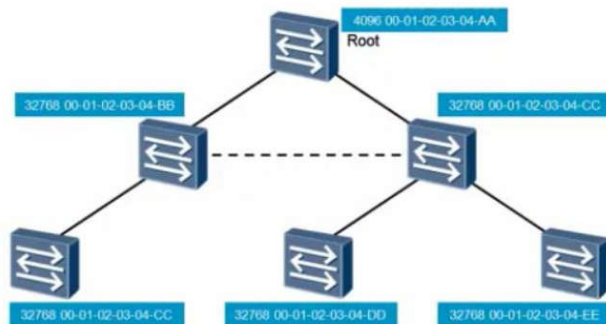- Loops are eliminated by restricting traffic flow over redundant paths.

STP-3

The Spanning Tree Root Bridge

- An inverted tree architecture is created as a result of STP.
- The root bridge represents the base of the spanning tree.

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 23   HUAWEI
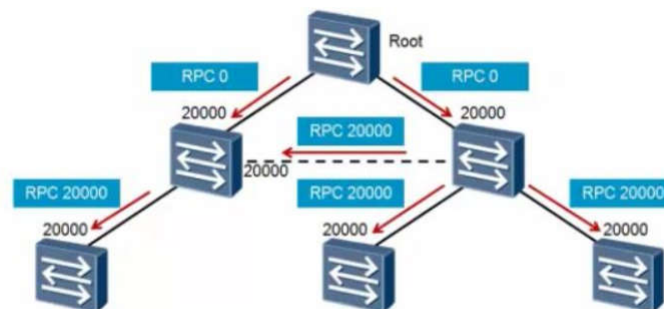
Metrics for STP Calculation

Bridge ID

- Bridge Identifiers are used to elect the root bridge.
- The bridge priority can be manipulated to force root selection.

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 24   HUAWEI

Metrics for STP Calculation-2

Path Cost

- Root path cost is carried in the BPDU and used to determine the shortest path to the root.

STP-7

Path Cost Standards

Port Speed	802.1D	802.1t	Path Cost Legacy
10 Mbps	99	1999999	1999
100 Mbps	18	199999	199
1 Gbps	4	20000	20
10 Gbps	2	2000	2

- STP supports various path cost standards
- The 802.1t is the default standard used by Huawei switches

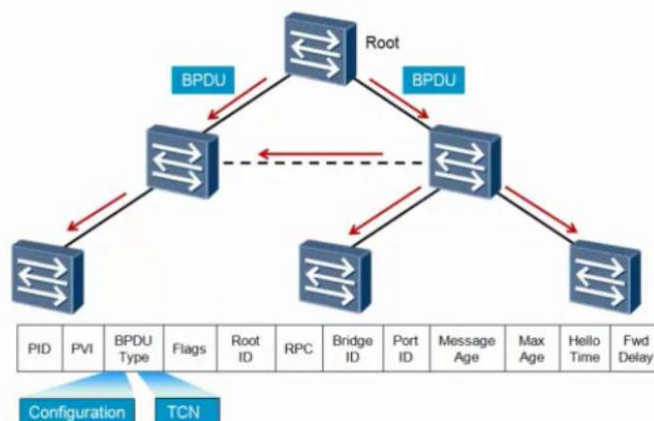## Metrics for STP Calculation-3

Port ID
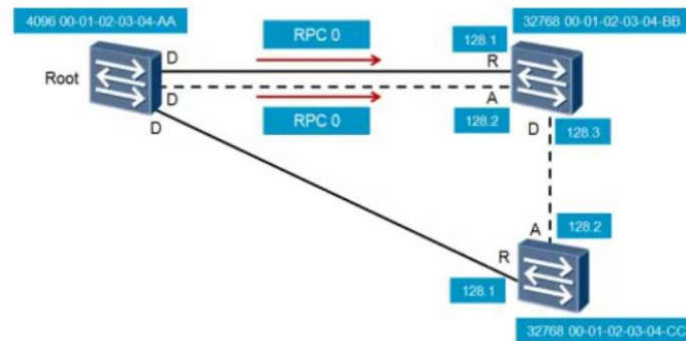
- Where the root path cost is equal, a port identifier is used to determine the active and alternate paths to the root.
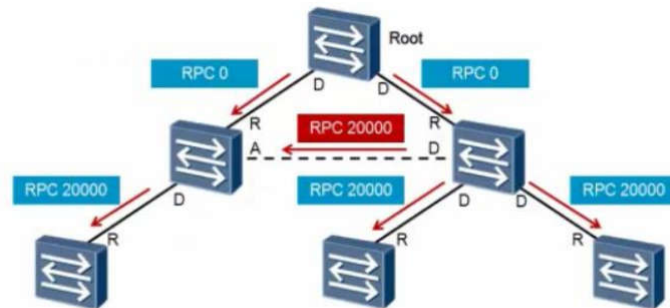
STP-4

Bridge Protocol Data Unit

PID	PVI	BPDU Type	Flags	Root ID	RPC	Bridge ID	Port ID	Message Age	Max Age	Hello Time	Fwd Delay

Configuration   TCN
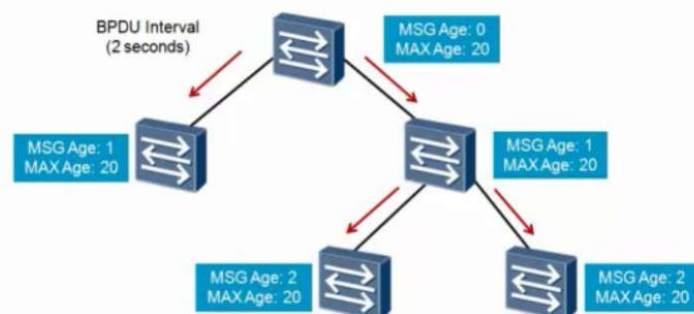
● **14**

STP-5

Spanning Tree Port Roles

- Spanning tree supports designated, root and alternate port roles.
- The root path cost enables port roles to be determined.
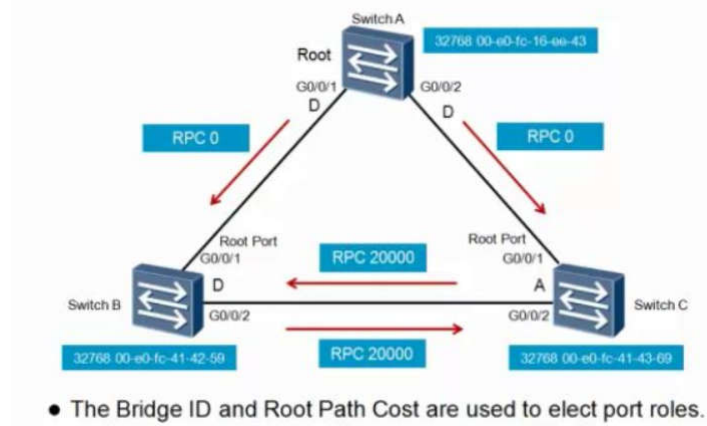
STP-6

Timers

- The MAX Age represents the aging timer of a BPDU.
- BPDU are discarded when Message Age exceeds MAX Age

STP-7

Port Role Establishment Process

- The Bridge ID and Root Path Cost are used to elect port roles.

STP-8

Table 14-3 STP port states

| Port State	Purpose	Description
Forwarding	A port in Forwarding state can forward user traffic and process BPDUs.	Only the root port and designated port can enter the Forwarding state.
Learning	When a port is in Learning state, the device creates MAC address entries based on user traffic received on the port but does not forward user traffic through the port.	This is a transitional state, which is designed to prevent temporary loops.
Listening	All ports are in Listening state before the root bridge, root port, and designated port are selected.	This is a transitional state.
Blocking	A port in Blocking state receives and processes only BPDUs, and does not forward user traffic.	This is the final state of a blocked port.
Disabled	A port in Disabled state does not process BPDUs or forward user traffic.	The port is Down.

STP-9

Root Failure
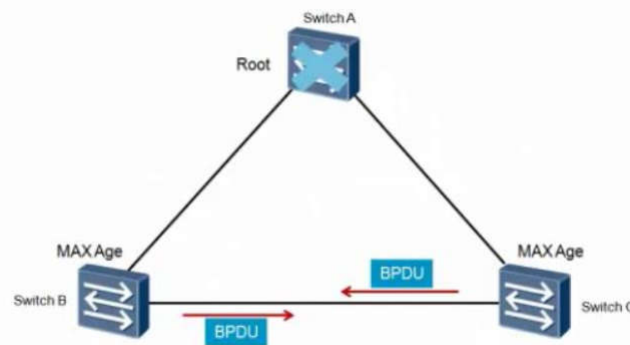
- Non root bridges wait for MAX Age before assuming loss of root
- Re-convergence is then initiated, beginning with root election.
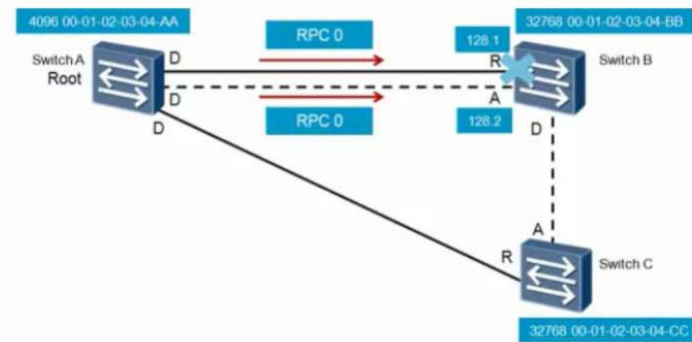
STP-10

Indirect Link Failure
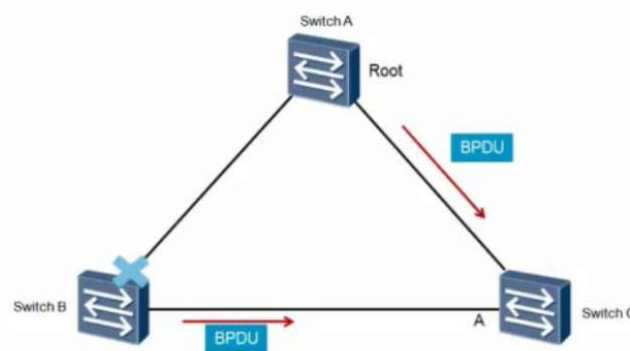
- Switch B begins root election, but BPDU is ignored by Switch C
- Root BDPU is propagated to switch B after MAX Age expires.
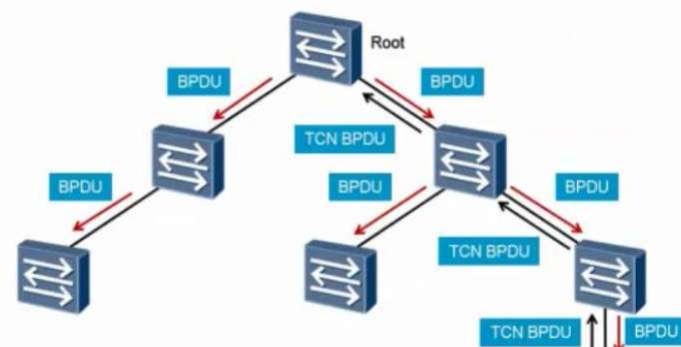
Max age: 20 sec in default

STP-11

Direct Link Failure

- Switch B detects failure and switches alternate port to root port.
- STP converges after 2x forward delay (30 seconds by default).
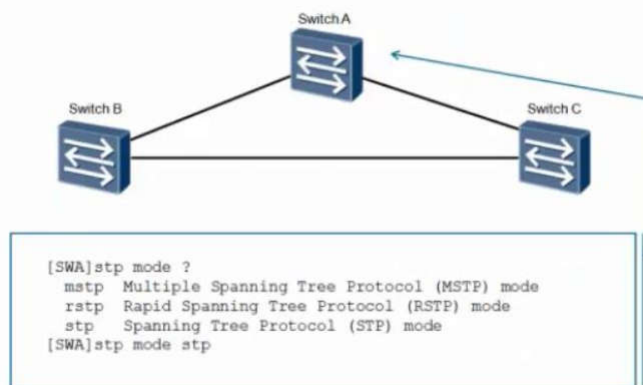
STP-12

Topology Change Process

- Topology Change Notification informs root of topology change.
- Root flushes MAC entries using BPDU with TC bit set.

STP-13

STP Modes


```
[SWA]stp mode ?
  mstp  Multiple Spanning Tree Protocol (MSTP) mode
  rstp  Rapid Spanning Tree Protocol (RSTP) mode
  stp   Spanning Tree Protocol (STP) mode
[SWA]stp mode stp
```

STP-14

Assigning The Root

Switch A — 4096 00-01-02-03-04-AA

Switch B — 32768 00-01-02-03-04-BB

Switch C — 32768 00-01-02-03-04-CC

```
[SWA] stp priority 4096
Apr 15 2013 16:15:33-08:00 SWA DS/4/DATASYNC_CFGCHANGE:OID
1.3.6.1.4.1.2011.5.25.191.3.1 configurations have been
changed. The current change number is 4, the change loop
count is 0, and the maximum number of records is 4095.
```
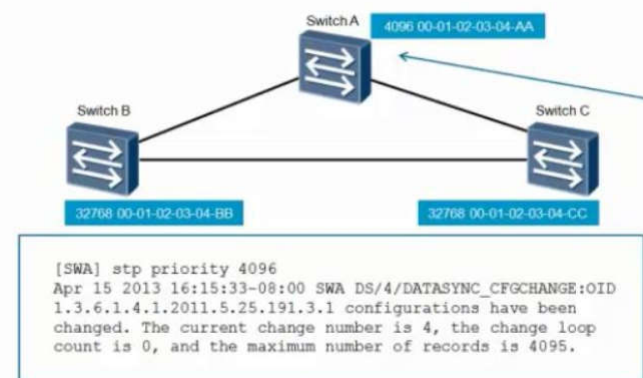
● Root can be set manually or by defining the switch as primary

STP-15

Assigning Path Cost


```
[SWC]stp pathcost-standard ?
  dot1d-1998   IEEE 802.1D-1998
  dot1t        IEEE 802.1T
  legacy       Legacy
[SWC]interface GigabitEthernet 0/0/1
[SWC-GigabitEthernet0/0/1]stp cost 2000
```

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 39   HUAWEI

STP-16

Root Protection


```
[SWA]interface GigabitEthernet 0/0/1
[SWA-GigabitEthernet0/0/1] stp root-protection
```

- Root protection prevents changes to the topology as a result of root bridge transition, caused by receiving higher priority BPDU.

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 40   HUAWEI

DHCP

DHCP Application In The Enterprise Network

Host A — Request IP Address → Switch ← Assign IP Address — DHCP Server (R)

Host B — Request IP Address →
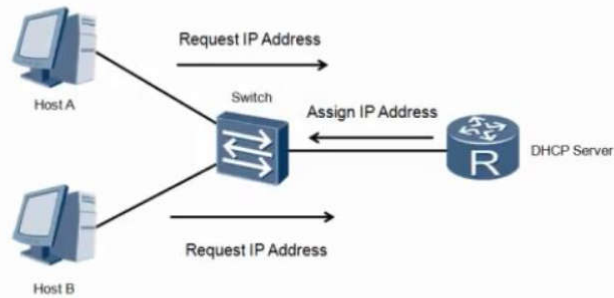
- Networks comprising of a large number of users requires a central management system for IP address allocation.

DHCP-2

DHCP Messages
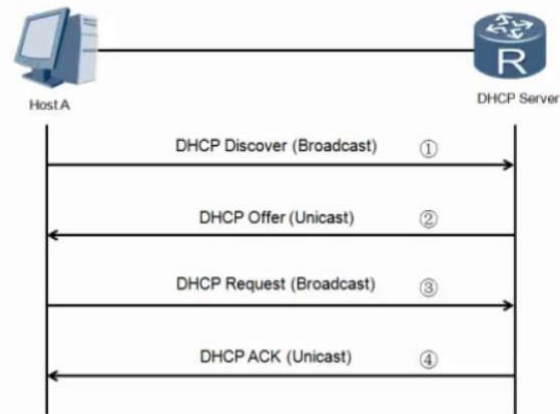
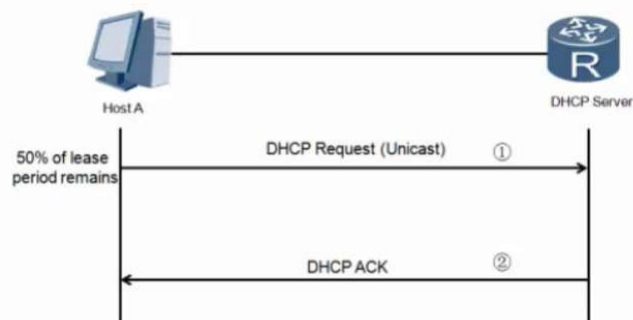| Message Types	Function
DHCP DISCOVER	Client broadcast used to locate available DHCP servers.
DHCP OFFER	Server responds to DHCPDISCOVER with an offer of configuration parameters
DHCP REQUEST	Client message to servers, either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming the correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.
DHCP ACK	Server confirmation sent to the client with configuration parameters, including committed network address.
DHCP NAK	Server indicates to the client that client's requested network address cannot be assigned.
DHCP RELEASE	Client relinquishes the network address to the server and cancels the remaining lease.

21

DHCP-3

DHCP Address Acquisition

Host A — DHCP Server

DHCP Discover (Broadcast) ①

DHCP Offer (Unicast) ②

DHCP Request (Broadcast) ③

DHCP ACK (Unicast) ④

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 43

DHCP-4

DHCP Lease Renewal

Host A — DHCP Server

50% of lease period remains

DHCP Request (Unicast) ①

DHCP ACK ②

- DHCP initiates an IP lease renewal process when a lease period of 50% remains.

HUAWEI TECHNOLOGIES CO., LTD.   Huawei Confidential   Page 44

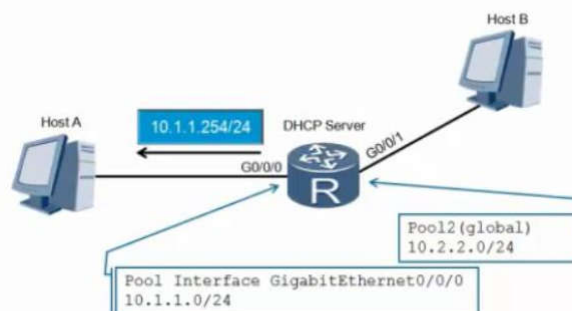## DHCP-5

IP Address Release

Host A — DHCP Server
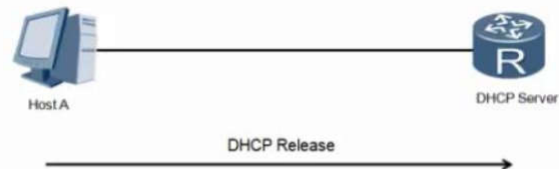
DHCP Release

- DHCP will result in the release of an IP address if the client fails to renew the IP address before the lease expiry.

DHCP-6

Address Pools

Host B

Host A　10.1.1.254/24　DHCP Server　G0/0/1

G0/0/0

Pool2(global)
10.2.2.0/24

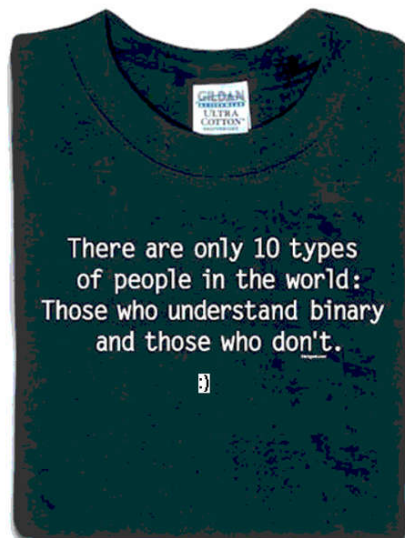Pool Interface GigabitEthernet0/0/0
10.1.1.0/24

- Address pools can be either global or interface based.

DHCP-7

DHCP Interface Pool Configuration


```
[Huawei]dhcp enable
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address
10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3
```

There are only 10 types
of people in the world:
Those who understand binary
and those who don't.

THANK YOU

www.huawei.com

HUAWEI