# HCIA Cheatsheet

## Contents

Take me to:



> TODO: SDN, OpenFlow

## Basics + Routing & switching

- **Switch FLOODS (not discards) if MAC not found**
- **Switch discards if next port MAC = Source MAC**

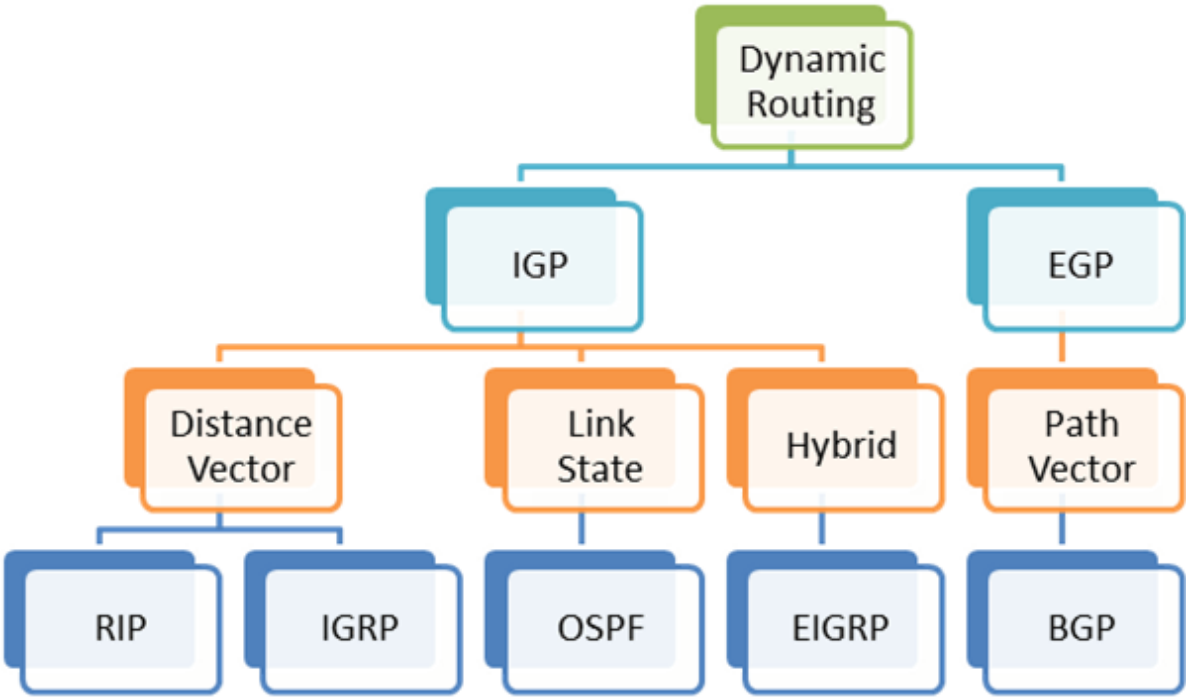
> Routes: direct (link layer protos), static (handmade), dynamic (ospf, is-is, etc.)

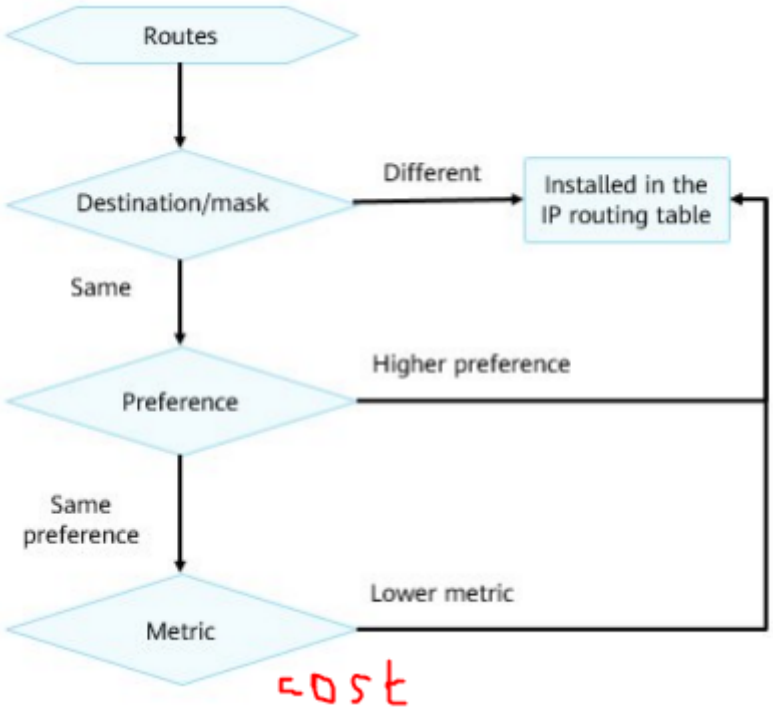
- **Switch = isolate collision domains, join 1 broadcast domain**
- **Router = isolate broadcast & collision domains**

**TYPE CODES**: TCP-6, UDP-17, ICMP-1

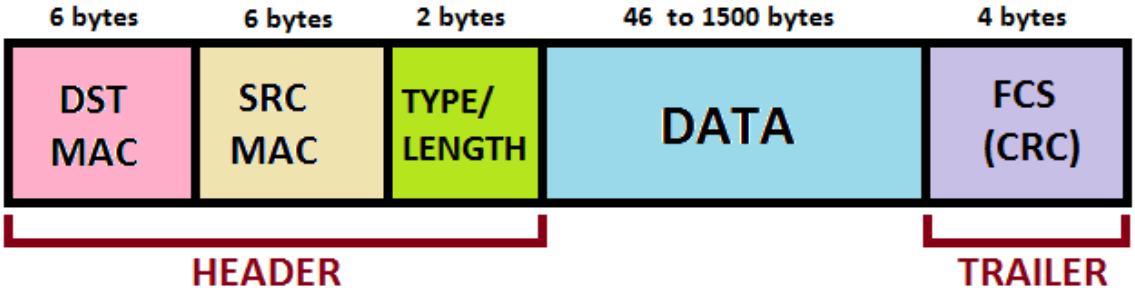
**Ports:**

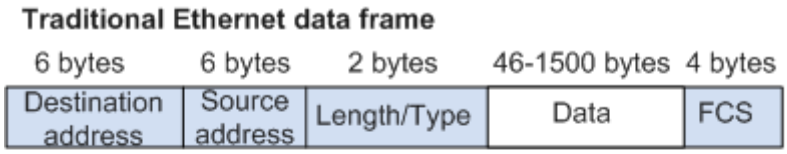
> SNMP uses UDP/161, UDP/162
>
> TFTP uses UDP/69
>
> FTP uses TCP/21 (commands), TCP/20 (data)
>
> SFTP uses SSH+TCP/22
>
> CAPWAP uses UDP ports 5246 (control channel) and 5247 (data channel)

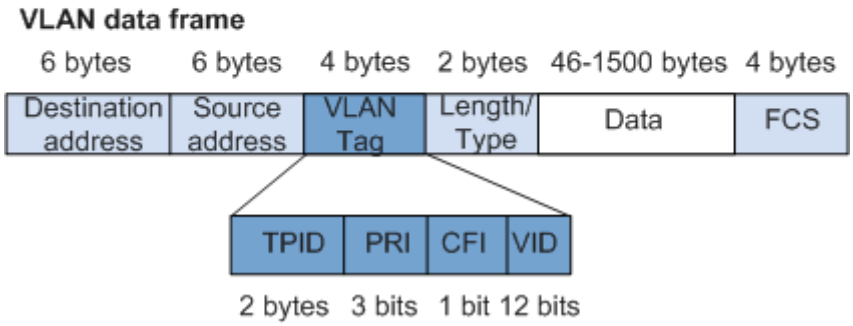



## ETHERNET II (DIX) FRAME






> - *Tag Protocol Identifier* (TPID, идентификатор протокола тегирования). Размер поля — 16 бит. Указывает какой протокол используется для тегирования. Для 802.1Q используется значение 0x8100.
> - Tag control information (TCI). Также 16 бит. Состоит из следующих полей:
>   - *Priority code point (PCP)*. Размер поля — 3 бита. Используется стандартом IEEE 802.1p для задания приоритета передаваемого трафика (class of service).
>   - *Drop eligible indicator (DEI). Размер поля — 1 бит.* (Прежде *Canonical Format Indicator*) *Индикатор допустимости удаления*. Может использоваться отдельно или совместно с *PCP* для указания кадров, которые могут быть отброшены при наличии перегрузки.
>   - *VLAN Identifier* (VID, идентификатор VLAN). Размер поля — 12 бит. Указывает какому VLAN принадлежит кадр. Диапазон возможных значений от 0 до 4095.
>
> При использовании стандарта Ethernet II, 802.1Q вставляет тег перед полем «Тип протокола». Так как фрейм изменился, пересчитывается контрольная сумма.

# OSI

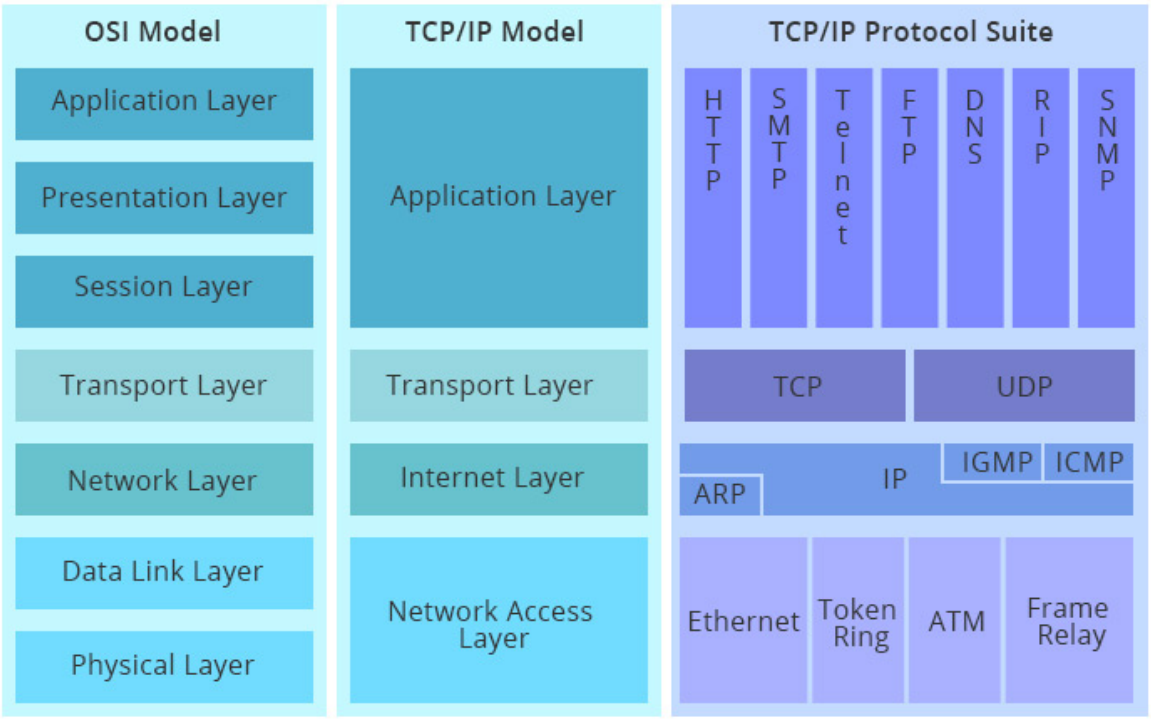
## 1.4 Network Reference Model and Standard Protocols

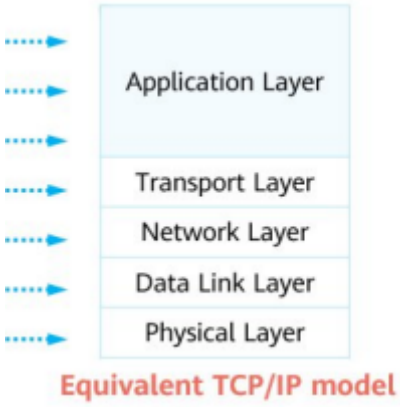
### 1.4.1 OSI Reference Model

The Open Systems Interconnection Model (OSI) was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.

The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:

- Physical layer: transmits bit flows between devices and defines physical specifications such as electrical levels, speeds, and cable pins.
- Data link layer: encapsulates bits into octets and octets into frames, uses MAC addresses to access media, and implements error checking.
- Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
- Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error checking before retransmission.
- Session layer: establishes, manages, and terminates sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between applications on different devices.
- Presentation layer: provides data encoding and conversion so that data sent by the application layer of one system can be identified by the application layer of another system.




Equivalent TCP/IP model

# MAC

IEEE - MAC 01-80-C2-xx-xx-xx (STP MULTICAST 8bit = 1, 7 - Local administrated addr)

48 bits

? Terminal host - not multicast ?

# IPv4

32 bits (24 mask as default)

> Types: Unicast, Multicast, Broadcast

OSPFv2

| Permanent Multicast Group Addresses | Description |
|---|---|
| 224.0.0.0 | Unassigned |
| 224.0.0.1 | All the hosts and routers on a network segment (similar to a broadcast address) |
| 224.0.0.2 | All multicast routers |
| 224.0.0.3 | Unassigned |

| Address Classes | RANGE | Bit Pattern of 1st byte | Decimal Range | Default Subnet Mask | Reserved for |
|---|---|---|---|---|---|
| | | | | webeasyinfo.com | |
| A | 1.0.0.0 to 126.255.255.255 | 0xxxxxxx | 1 to 127 | 255.0.0.0 | Governments |
| B | 128.0.0.0 to 191.255.255.255 | 10xxxxxx | 128-191 | 255.255.0.0 | Medium Companies |
| C | 192.0.0.0 to 223.255.255.255 | 110xxxxx | 192-223 | 255.255.255.0 | Small Companies |
| D | 224.0.0.0 to 239.255.255.255 | 1110xxxx | 224-239 | Not Applicable | Reserved for Multicasting |
| E | 240.0.0.0 to 255.255.255.255 | 11110xxx | 240-255 | Not Applicable | Experimental or future use |

# IPv6

Multicast addresses: https://support.huawei.com/enterprise/en/doc/EDOC1000177796/16e69f9c/multicast-addresses

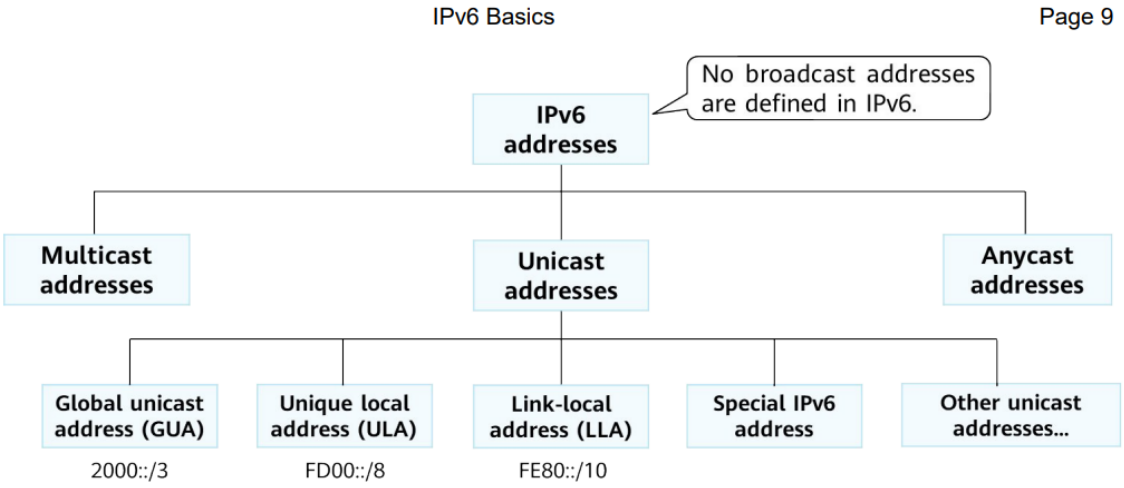
128 bits

> Types: Unicast, Multicast, Anycast

ospf v3

MULTICAST starts with FF

> ?Stages?
>
> - address configuration
> - duplicate address detection (DAD)
> - address resolution




An IPv6 packet has three parts: an IPv6 basic header, one or more IPv6 extension headers, and an upper-layer protocol data unit (PDU). An upper-layer PDU is composed of the upper-layer protocol header and its payload, which maybe an ICMPv6 packet, a TCP packet, or a UDP packet.

> Parts:
>
> - IPv6 basic header
> - one or more IPv6 extension headers
> - upper-layer protocol data unit (PDU)

| Comparison | IPv6 | IPv4 |
|---|---|---|
| Address length | 128 bits | 32 bits |
| Packet format | A fixed 40-byte basic packet header+variable-length extension headers | A basic header containing the Options field to support extended features |
| Address type | Unicast, multicast, and anycast | Unicast, multicast, and broadcast |
| Address configuration | Static, DHCP, and SLAAC | Static and DHCP |
| DAD | ICMPv6 | Gratuitous ARP |
| Address resolution | ICMPv6 | ARP |

| Range | IPv6 Multicast Addresses | Description |
|---|---|---|
| Node/Interface-local scope | FF01::1 | All node or interface addresses |
| | FF01::2 | All router addresses |
| Link-local scope | FF02::1 | All node addresses |
| | FF02::2 | All router addresses |
| | FF02::3 | Unassigned addresses |

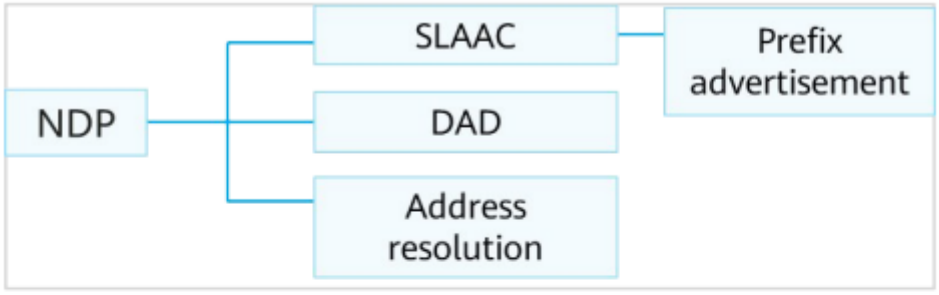



**Figure 1-25 NDP framework**

| ICMPv6 Type | Message Name |
|---|---|
| 133 | Router Solicitation (RS) |
| 134 | Router Advertisement (RA) |
| 135 | Neighbor Solicitation (NS) |
| 136 | Neighbor Advertisement (NA) |

# OSPF

fields: priority, router ID[no 0?] (**HIGHER** is best)

Default priority for an OSPF interface is **1**. The range is from 0 to 255. **0 means that the interface doesNOT** involve in the DR election.

> Network types
>
> - Point-to-point
> - Point-to-multipoint
> - Broadcast Multiaccess (BMA)
> - Virtual links
> - Nonbroadcast Multiaccess (NBMA)

**LSDB is same on DR and BDR (not DRO)**

> Authentification
>
> - area
> - interface

> display ospf lsdb

**IPv6** - OSPFv3

**IPv4** - OSPFv2

> ospf 1
>
> area 0 | 0.0.0.0
>
> // ? no enable ?

Area 0 - backbone

> DR is elected by all routers in segment

adjaency(full) DR/BDR + all > neighbour (2way) DRO+DRO

types: broadcast, nbma, p2mp, p2p

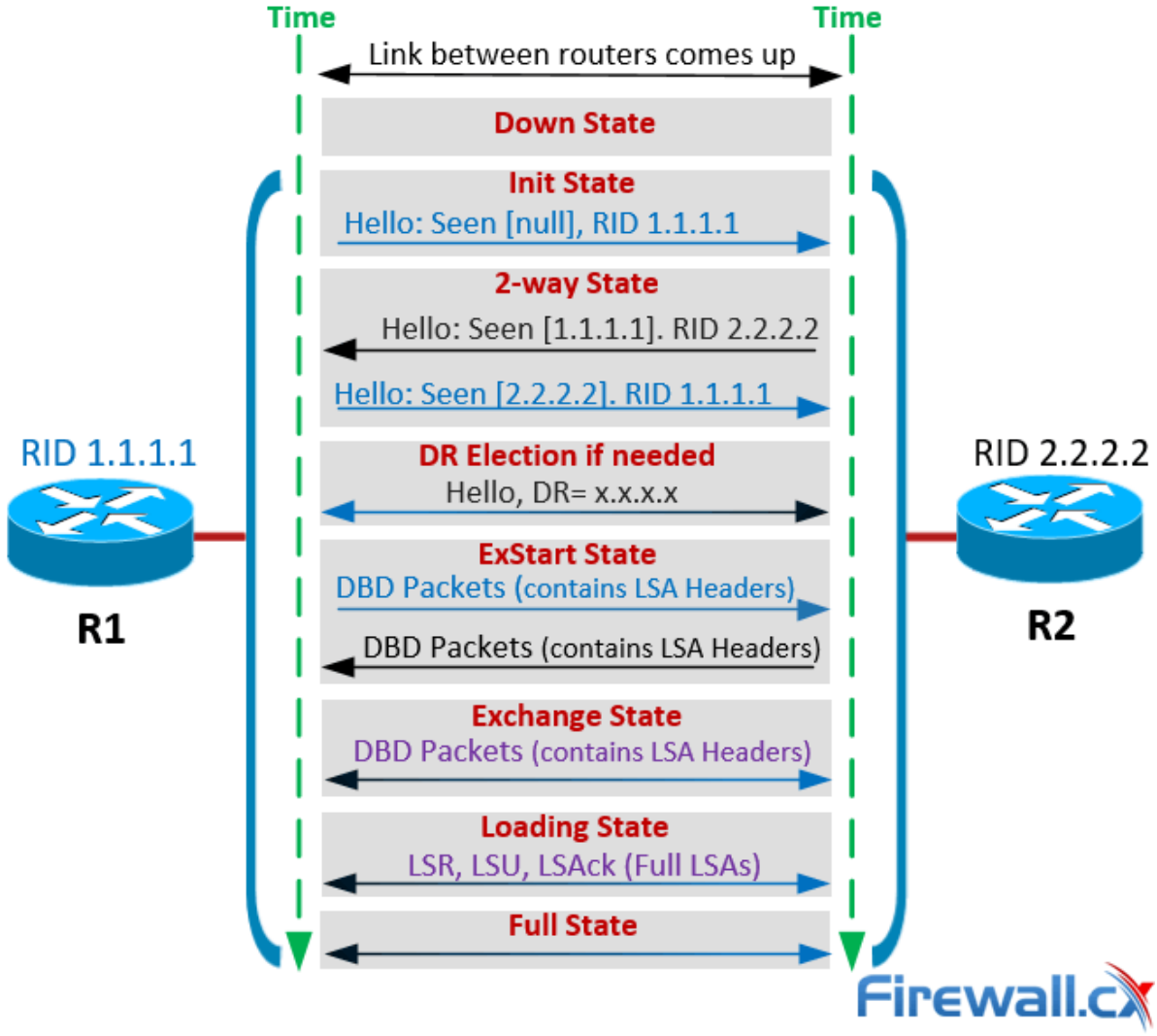
packets: Hello, DD, LSR, LSU, LSAack (LSA - not packet - link state advertise)

## 1.3.8 OSPF Packet Types

There are five types of OSPF protocol packets and implement different functions in interaction between OSPF routers.

**Table 1-1 OSPF Packet Types**

| Packet Name | Function |
|---|---|
| Hello | Is periodically sent to discover and maintain OSPF neighbor relationships. |
| Database Description | Describes the summary of the local LSDB, which is used to synchronize the LSDBs of two devices. |
| Link State Request | Requests a needed LSA from a neighbor. LSRs are sent only after DD packets have been successfully exchanged. |
| Link State Update | Is sent to advertise a requested LSA to a neighbor. |
| Link State ACK | Is used to acknowledge the receipt of an LSA. |

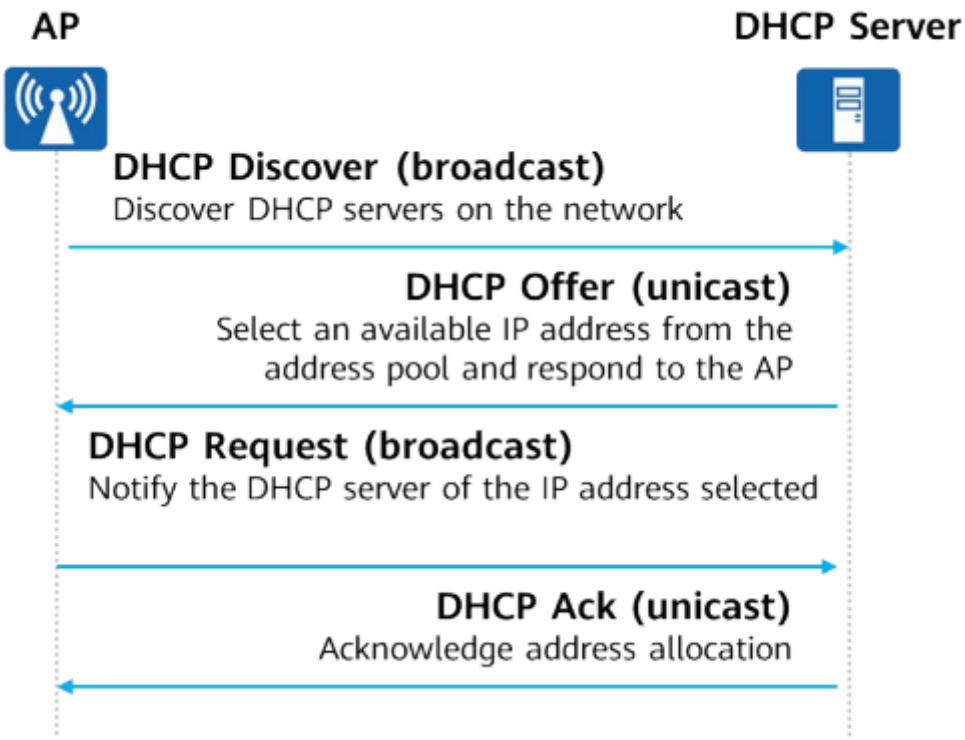



# DHCP

> addresses can be reused

> DHCPv6 devices are identified by DUIDs, and each DHCPv6 server or client can have only one DUID.

Packets (in time order): Discover-broadcast, offer-unicast, request-broadcast, ack-unicast




# VLAN (802.q1)

ID from 1 to 4095 (cisco)

**TPID** tag 0x8100 in TAG-ID .1q-frame (not Eth) **4 bytes tag**

> PVID - port vlan id, Vlan_ID - frame vlan id

Kinds:

- Interface-based
- Mac-based

> // enable command?

canNOT contain STP, RSTP (stp doNOTunderstand virtual networks, so works badly)

can - OSPF, ARP

by default all ports in default VLAN (can be manually deleted)

> ACCESS:
>
> Eth2 (no Vlan_ID) -> Vlan_ID := PVID
>
> Vlan_ID == PVID -> Eth2 (no Vlan_ID)
>
> Vlan_id != PVID -> X_discard_X
>
> TRUNK (inherits access):
>
> Eth2 -> Vlan_id -> check allow pass
>
> Vlan_id != PVID -> check allow pass
>
> Vlan_id == PVID -> Eth2
>
> Hybrid:

> The difference between a hybrid port and a trunk port is that a hybrid port allows the packets from multiple VLANs to be sent without tags, but a trunk port only allows the packets from the default VLAN to be sent without tags.
>
> For a hybrid interface, you need to configure not only a PVID but also two lists of VLAN IDs permitted by the interface: one untagged VLAN ID list and one tagged VLAN ID list.

# STP & RSTP

**LOWER** is best (0 - root)

> BID = bridge id (for picking root device)
>
> - Bridge priority 16 bits [0;65535], default **32768**, step 4096
> - MAC 48 bits

> PID = port id (picking port role)
>
> - port priority [0;240], default **128**, step 16
> - port number - 12 bits

*A root bridge does NOT have any root ports*. All ports on a root bridge are designated (*cisco*)

> RSTP ports roles:
>
> - root port
> - designated port - alternate on other side
> - (alternate/ non-designated?)

TCN - Topology Change Notification

doNOT work with vlan

Only 1 root port on non-root device

RSTP optimizes STP in many aspects, provides faster convergence, and is compatible with STP.

> RSTP = STP after conf BDPU

> In RSTP, a backup port can replace a faulty root port

Default Forward delay = **15 sec**

> RSTP ports roles:
>
> - root port
> - designated port
> - alternate port
> - backup port

## 1.4.10 STP Port State Transition

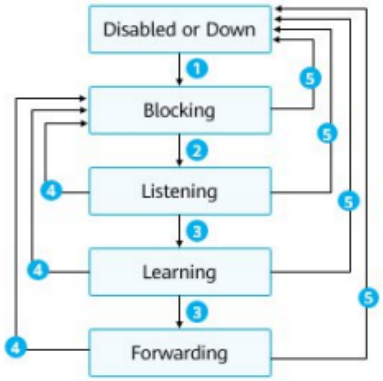



**Figure 1-29 STP Port State Transition**

1. When a port is initialized or activated, it automatically enters the blocking state.

Listening: A port in Listening state can forward BPDUs, but cannot forward user traffic.

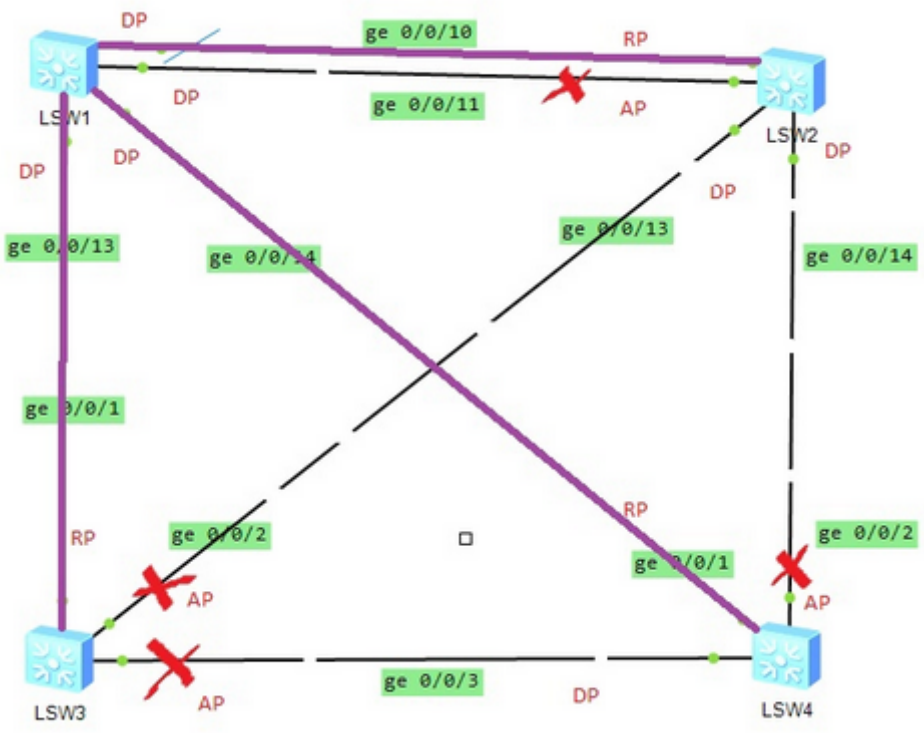
Blocking: A port in Blocking state can only receive and process BPDUs, but cannot forward BPDUs or user traffic. The alternate port is in Blocking state.

STP

**Table 1-1 Cost Calculation Methods**

| Port Rate | Port Mode | Recommended STP Cost | | |
|---|---|---|---|---|
| | | IEEE 802.1d-1998 | IEEE 802.1t | Huawei Legacy Standard |
| 100 Mbit/s | Half-duplex | 19 | 200,000 | 200 |
| | Full-duplex | 18 | 199,999 | 199 |
| | Aggregated link: two ports | 15 | 100,000 | 180 |
| 1000 Mbit/s | Full-duplex | 4 | 20,000 | 20 |
| | Aggregated link: two ports | 3 | 10,000 | 18 |
| 10 Gbit/s | Full-duplex | 2 | 2000 | 2 |
| | Aggregated link: two ports | 1 | 1000 | 1 |
| 40 Gbit/s | Full-duplex | 1 | 500 | 1 |
| | Aggregated link: two ports | 1 | 250 | 1 |
| 100 Gbit/s | Full-duplex | 1 | 200 | 1 |
| | Aggregated link: two ports | 1 | 100 | 1 |

| STP Port State | RSTP Port State | Port Role |
|---|---|---|
| Forwarding | Forwarding | Root port or designated port |
| Learning | Learning | Root port or designated port |
| Listening | Discarding | Root port or designated port |
| Blocking | Discarding | Alternate port or backup port |
| Disabled | Discarding | Disabled port |




# WLAN

AP upgrade modes: AC, FTP, SFTP *(no tftp)*

14 channels

**Authentication modes**: MAC, SN (serial number), no auth *(no password)*

DHCP + **option 43**

packet **Beacon** - AP **proactively** share SSID (**passive** STA scanning)

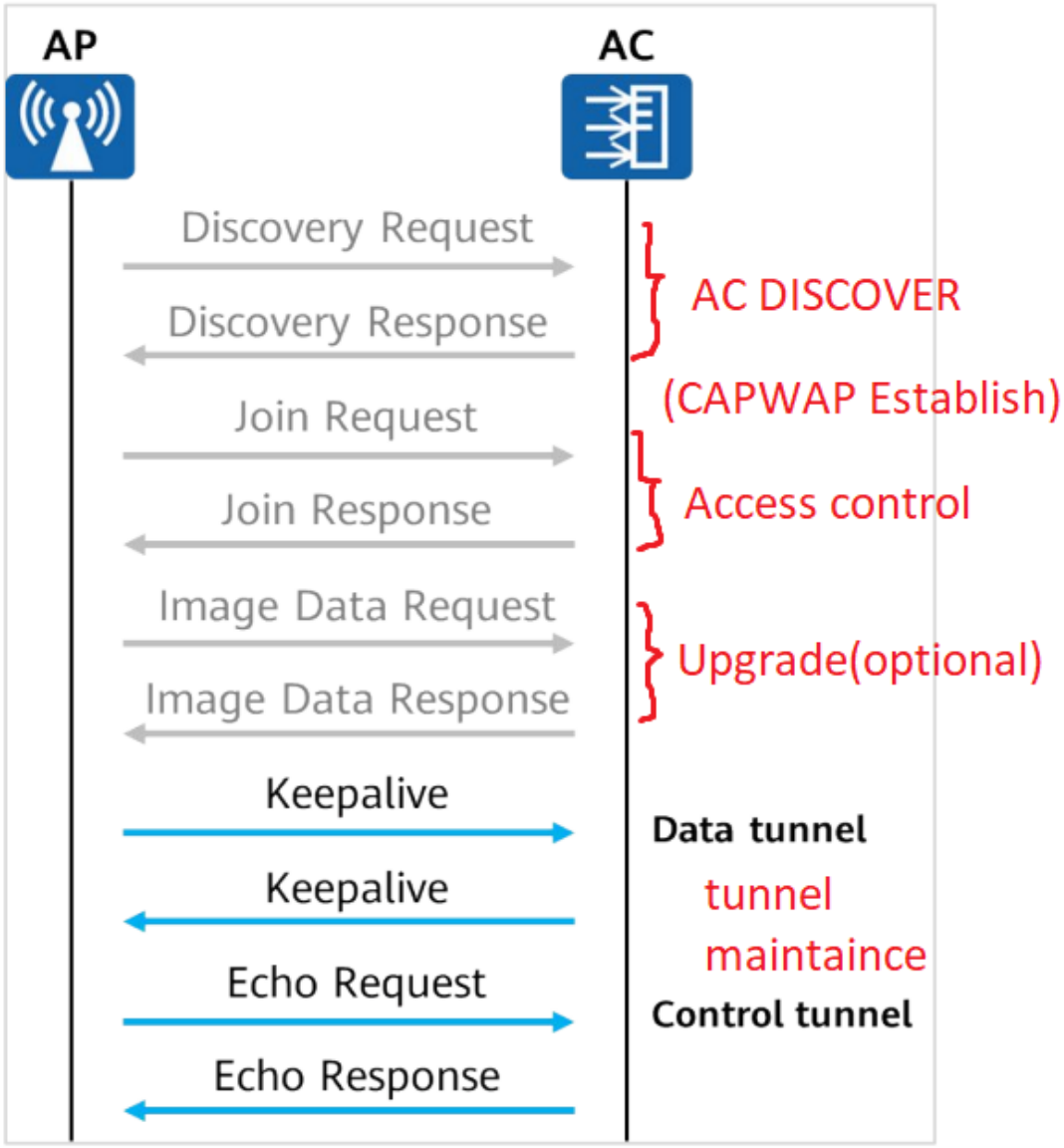
packet **Probe** - active STA scanning

> BSS - zone
>
> BSSID - AP zone id = func(APs MAC)
>
> SSID - wifi name

**BSSID** = func(APs MAC)

> Topologies:
>
> - in-path
> - off-path

- direct forwarding (local)
- **tunnel forwarding (centralized) - Data through AC**

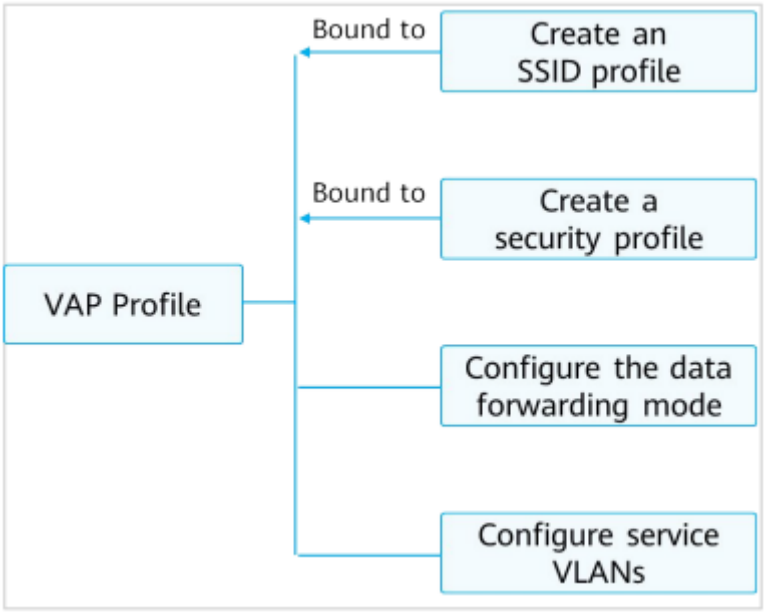



Config process

1 - AP obtains AC addr

2 - Establish CAPWAP

3 - AP access control



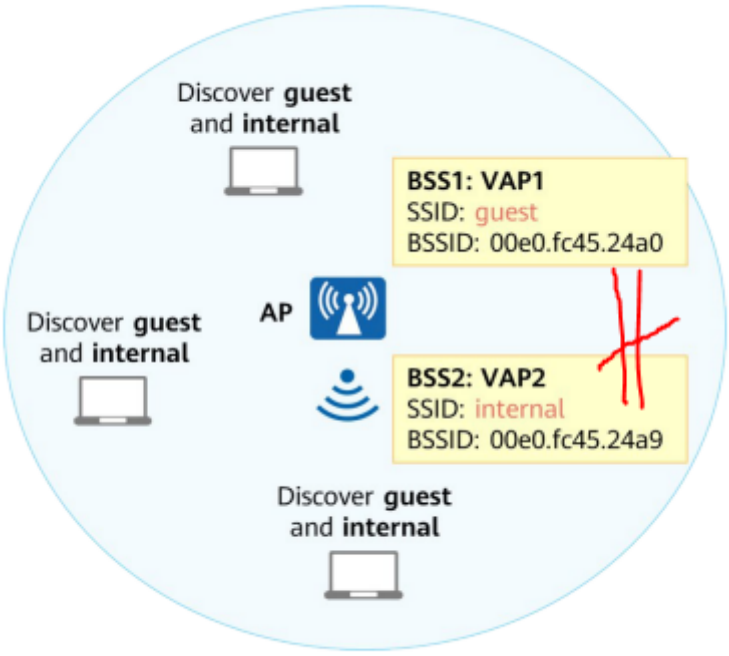
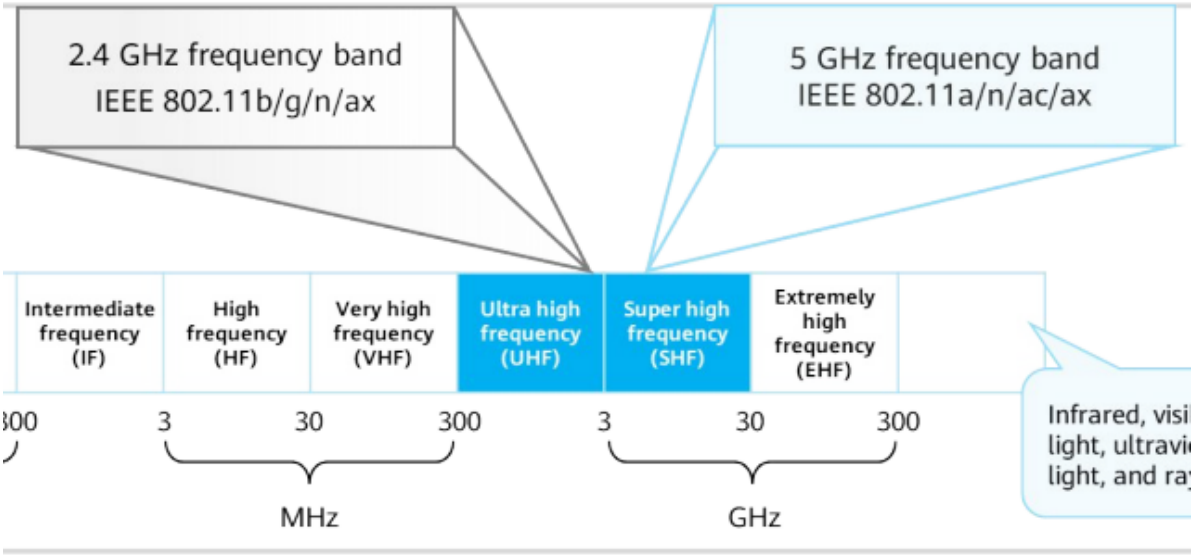




**Figure 1-16 VAP**

| Security Policy | Link Authentication | Access Authentication | Data Encryption | Description |
|---|---|---|---|---|
| **WEP** | Open system | N/A | No encryption or WEP | Insecure policy |
| | Shared-key Authentication | N/A | WEP | Insecure policy |
| **WPA/WPA2-802.1X** | Open system | 802.1X (EAP) | TKIP or CCMP | A more secure policy, applicable to large enterprises |
| **WPA/WPA2-PSK** | Open system | PSK | TKIP or CCMP | More secure policy, applicable to small- and medium-sized enterprises or household users |




# ACL

Default increment = 5 , CAN be changed

| ACL Type | ACL Number | Parameters |
|---|---|---|
| Basic ACL | 2000 to 2999 | Source IP Address |
| Advanced ACL | 3000 to 3999 | Source/Destination IP<br>Source/Destination Port |
| Layer 2 ACL | 4000 to 4999 | MAC Address |

# Eth-Trunk, iStack & CSS

Layer 2 and 3 both

> flow-based load balancing

LACP(DU) - link aggregation control protocol

LACP(DU): Device priority (default = **32768**), MAC, interface priority, port number

> LACP flags: synchronizing, collecting, distributing (111 - active, 000 - inactive)

Actor: **LOWER** system (device) priority, ? MAC ?

Interfaces: **LOWER** interfaces priorities of actor, port number

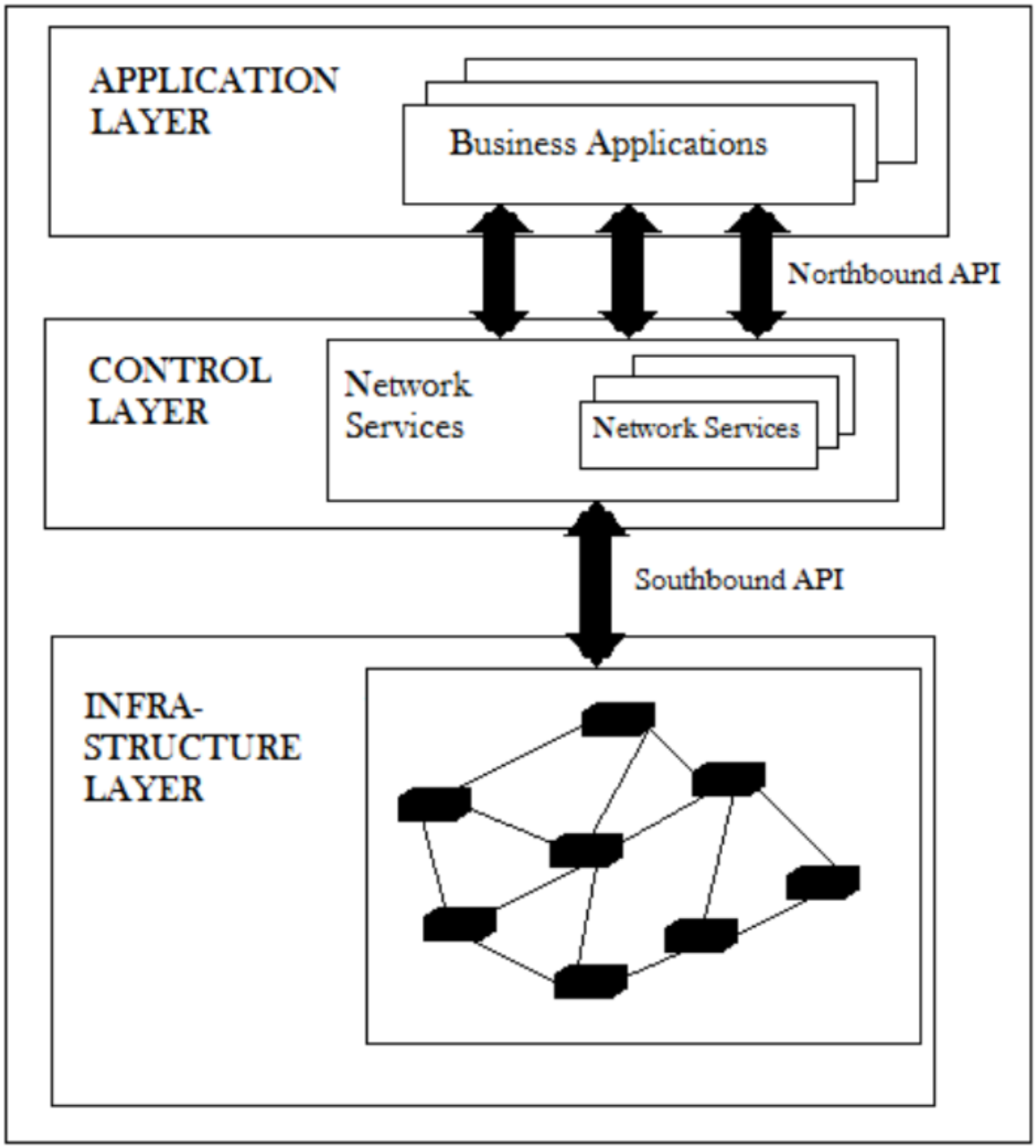
Same params on member interfaces: vlan, speed, duplex mode + load-balancing

---

iStack and CSS provide the same functions, despite their different names and implementation mechanisms.

# SDN

> Characteristics:
>
> - centralized control
> - forwarding-control separation
> - open programmable interfaces
> - (distributed forwarding)




# Other

MTU - Maximal transit unit (for interface)

Control plane: provides functions such as protocol processing, service processing, route calculation, forwarding control, service scheduling, traffic statistics collection, and system security. The control plane of a switch is used to control and manage the running of all network protocols. The control plane provides various network information and forwarding query entries required for data processing and forwarding on the data plane

forwarding equivalence class (FEC) is a term used in Multiprotocol Label Switching (MPLS) to describe a set of packets with similar or identical characteristics which may be forwarded the same way

> File extensions:
>
> cc - system softaware
>
> cfg, dat, zip - config
>
> pat - patch

> bin - PAF (features and resources)

> 44. ()The Point-to-Point Protocol (PPP) is a common data link layer protocol for wide area networks (WANs). Which of the following statements about PPP is false?
>
> - (FALSE) A. The establishment of a PPP link goes through three phases: link layer negotiation, network layer negotiation, and authentication.
> - B. PPP uses the Link Control Protocol (LCP) to negotiate link control layer parameters.
> - C. If PPP uses password authentication mode, negotiation packets are transmitted in plain text, which is insecure.
> - D. PPP supports the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

> (?) 52. ()The Network Configuration Protocol (NETCONF) provides a mechanism for managing network devices. Which of the following statements about NETCONF is false?
>
> - A. Yet Another Next Generation (YANG) is a data modeling language that standardizes NETCONF data content.
> - (FALSE) B. If YANG files are not integrated into a device, the device does not support NETCONF.
> - C. NETCONF messages are formatted using either JSON or XML.
> - D. NETCONF supports trial runs and rollback in case of errors.

In asynchronous transmission, data is transmitted byte by byte. Therefore, it is less efficient than synchronous transmission.

> IPv6 - OSPFv3
>
> IPv4 - OSPFv2

VRP - console, telnet, USB router conf *(no FTP)*

> simple switches doNOT isolate broadcast domains, but vlan or layer 3 can (usually routers do)

AAA - Authentication, Authorization, Accounting (Auth modes: hwtacacs | local (default) | radius)

FTP kinds: active, passive

Blackhole route / null route - key from routing loops

traceroute, ping - ICMP

Message Age of STP root conf msg = 0

RSTP = STP after conf BDPU

---