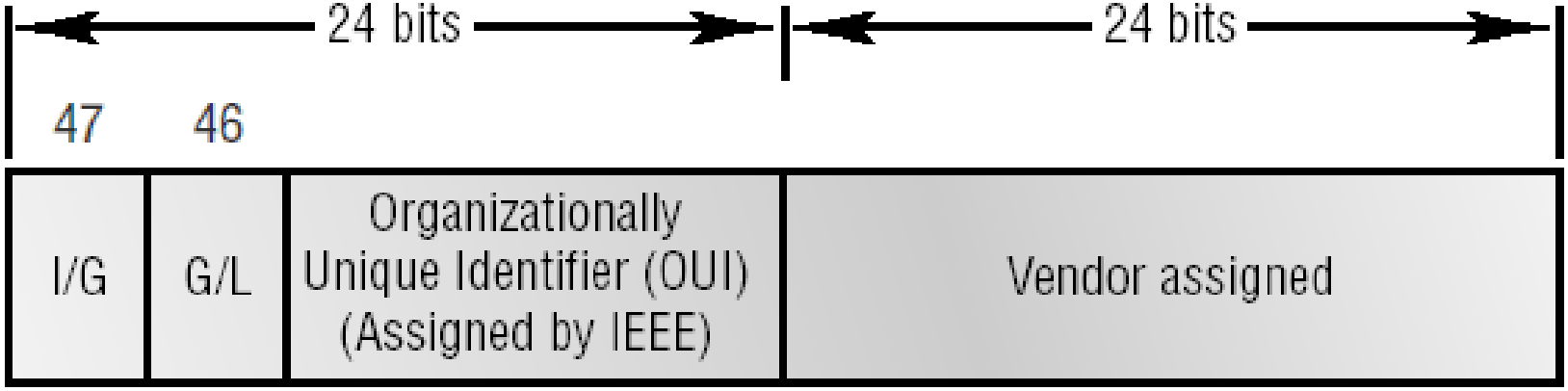
Технологии 2 уровня

Ethernet адресация



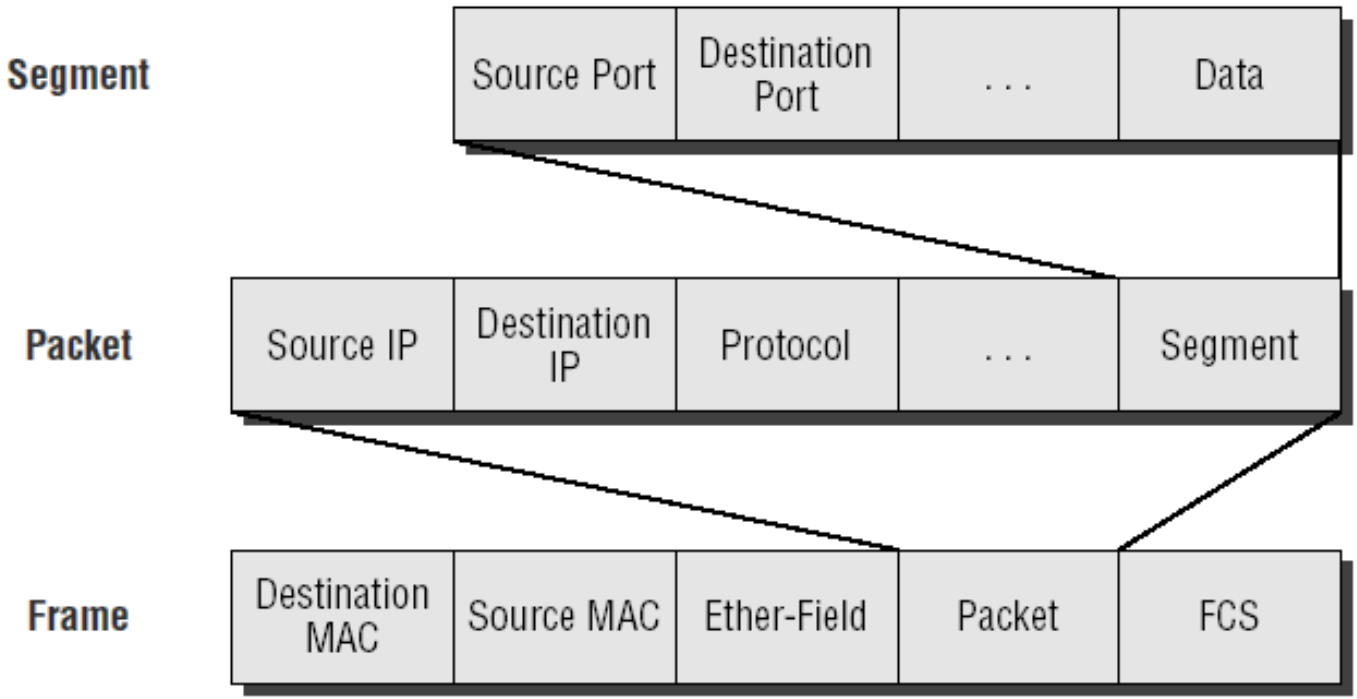
OUI - organizationally unique identifier

G/L(U/L) – Globally/Locally administered

I/G - Individual/Group

Vendor assigned – серийный номер карты

Инкапсуляция PDU



Ethernet (IEEE 802.3) standards

- IEEE 802.3 сигнальные стандарты:
- 10Base2, 10Base5, 10BaseT, 100BaseTX (IEEE 802.3u), 100BaseFX (IEEE 802.3u), 100VG-AnyLAN (IEEE 802.12)
- 1000BaseCX (IEEE 802.3z) twinax, до 25 meters.
- 1000BaseT (IEEE 802.3ab) Category 5, 4 парная UTP до 100 m.
- 1000BaseSX (IEEE 802.3z) MMF 62.5- и 50-micron core; 850 nm laser, до 220 m (62.5), 550 m (50).
- 1000BaseLX (IEE 802.3z) SMF 9-micron core 1300 nm laser, до 10 km.

Ethernet (IEEE 802.3) standards

- 10G Ethernet:
- 10GBASE-L
  - SMF, 1310 нм – 10 км
- 10GBASE-E
  - SMF, 1550 нм – 40 км
- 10GBASE-S
  - MMF, 850 нм – 26 .. 300 метров
- 10GBASE-T (проект до 2006 г.)
  - 802.3an, TP Cat.6a, Cat.7, (Cat.6 – 50м.)

100G Ethernet (IEEE Higher Speed Study Group)

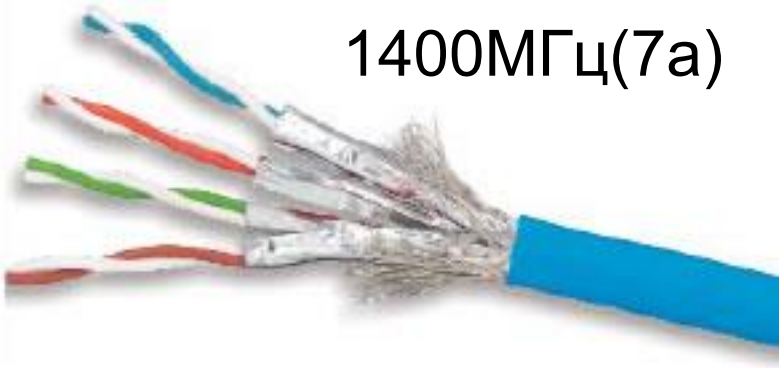
- 07.2007 IEEE 802.3 Higher Speed Study Group (HSSG) инициировала запрос на разработку 100G Ethernet с целями:
- 100Gbps;
- 100m MMF;
- 10km SMF;
- 40km SMF;
- Только дуплекс;
- поддержка кадра 802.3 ;
- BER>10^{-12}.
- См.:
- http://grouper.ieee.org/groups/802/3/hssg/public/index.html

Новые и будущие виды TP

Cat 6/Class E
250/500(6a) МГц

RJ-45

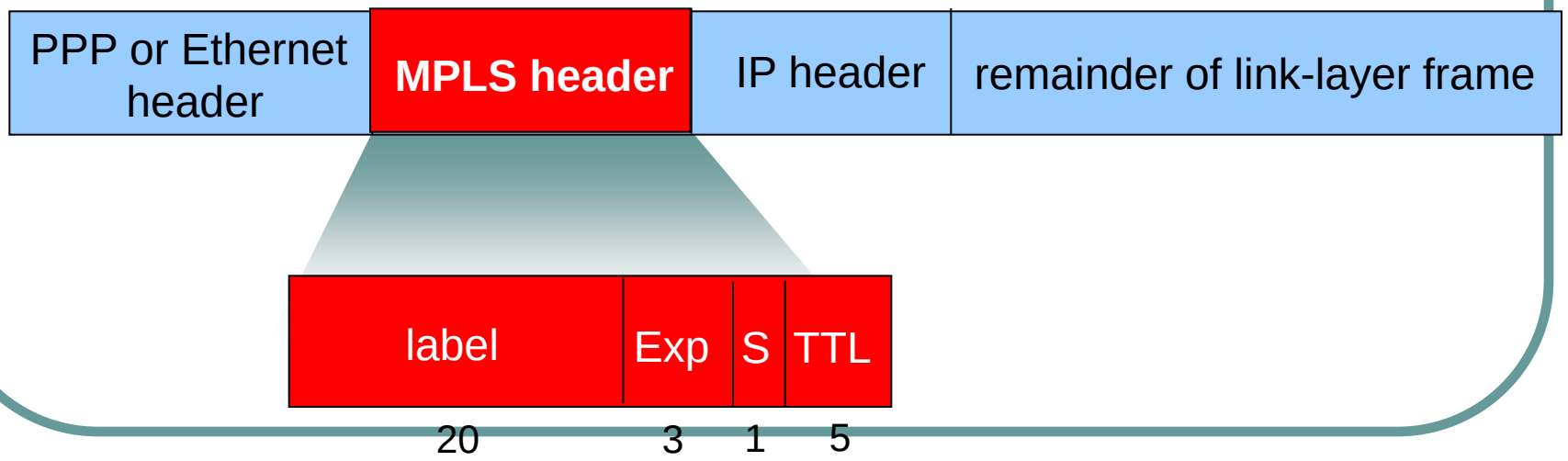
Cat 7/Class F, полоса 700 МГц / 1400МГц(7a)



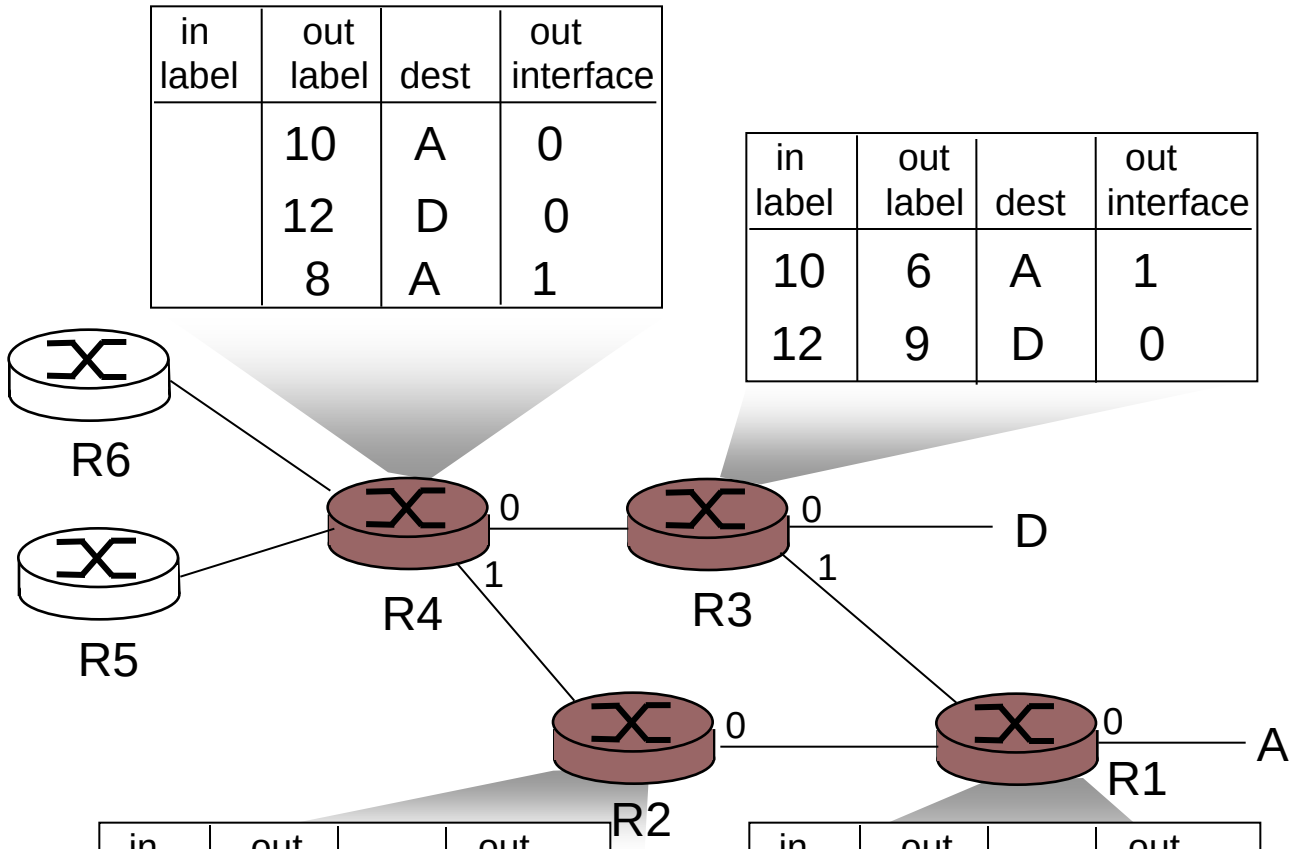
RF-45

Multi-Protocol Label Switching (MPLS)

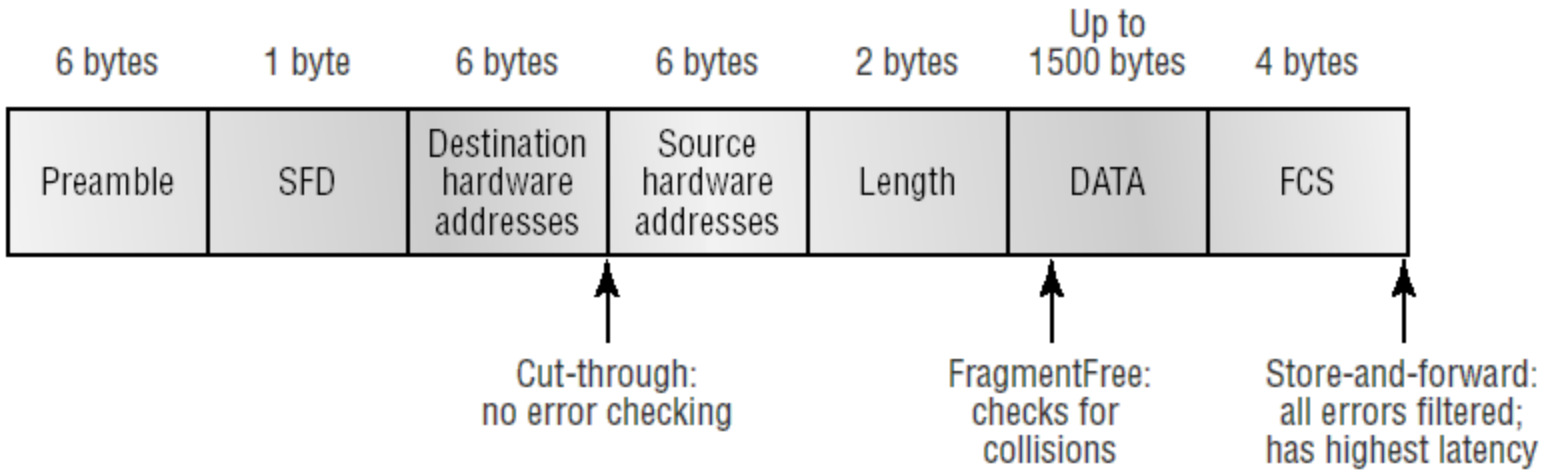
- Цель: ускорить IP доставку используя метки вместо IP адресов
  - идея Virtual Circuit (VC)
  - тем не менее, дейтаграмма содержит IP адрес



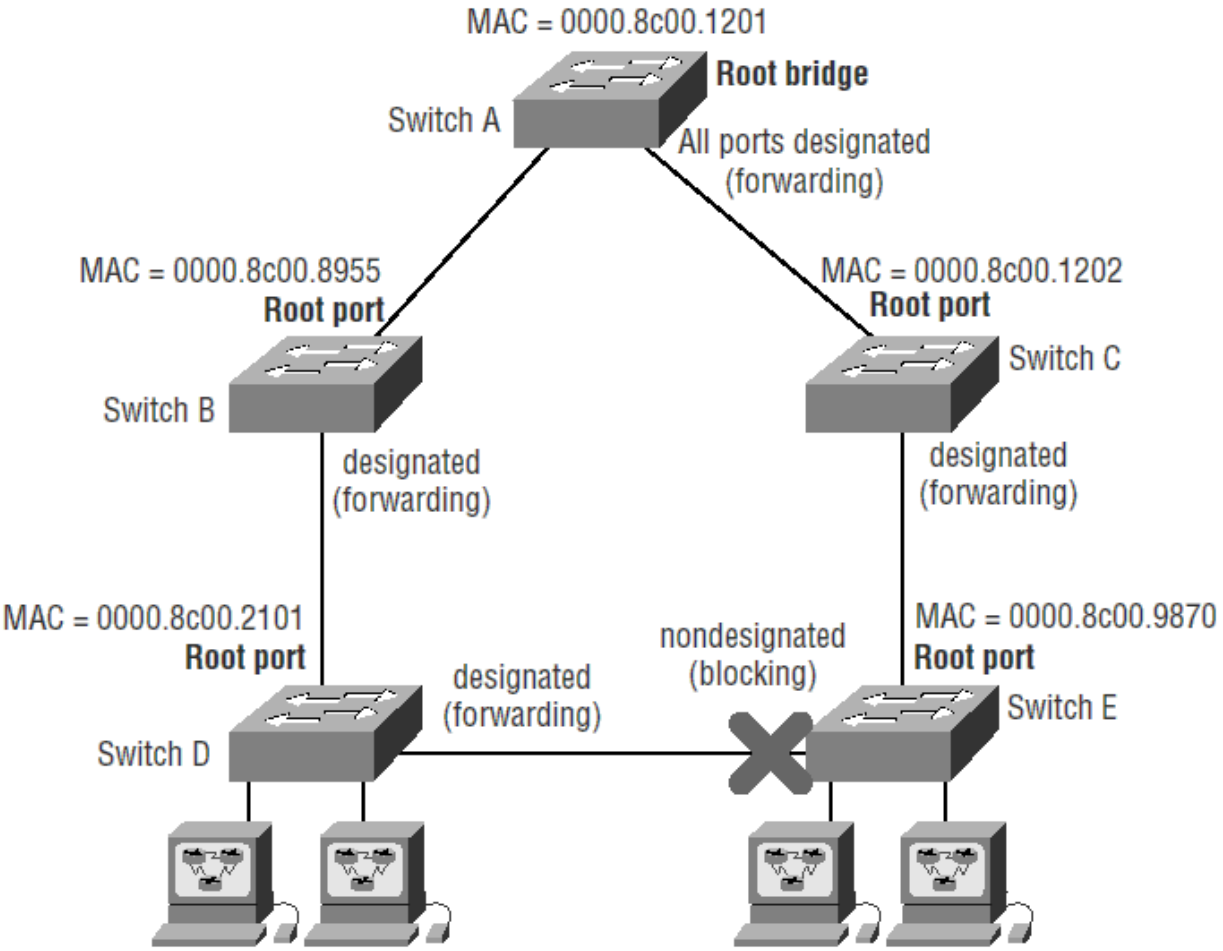
MPLS таблицы



Типы коммутаторов



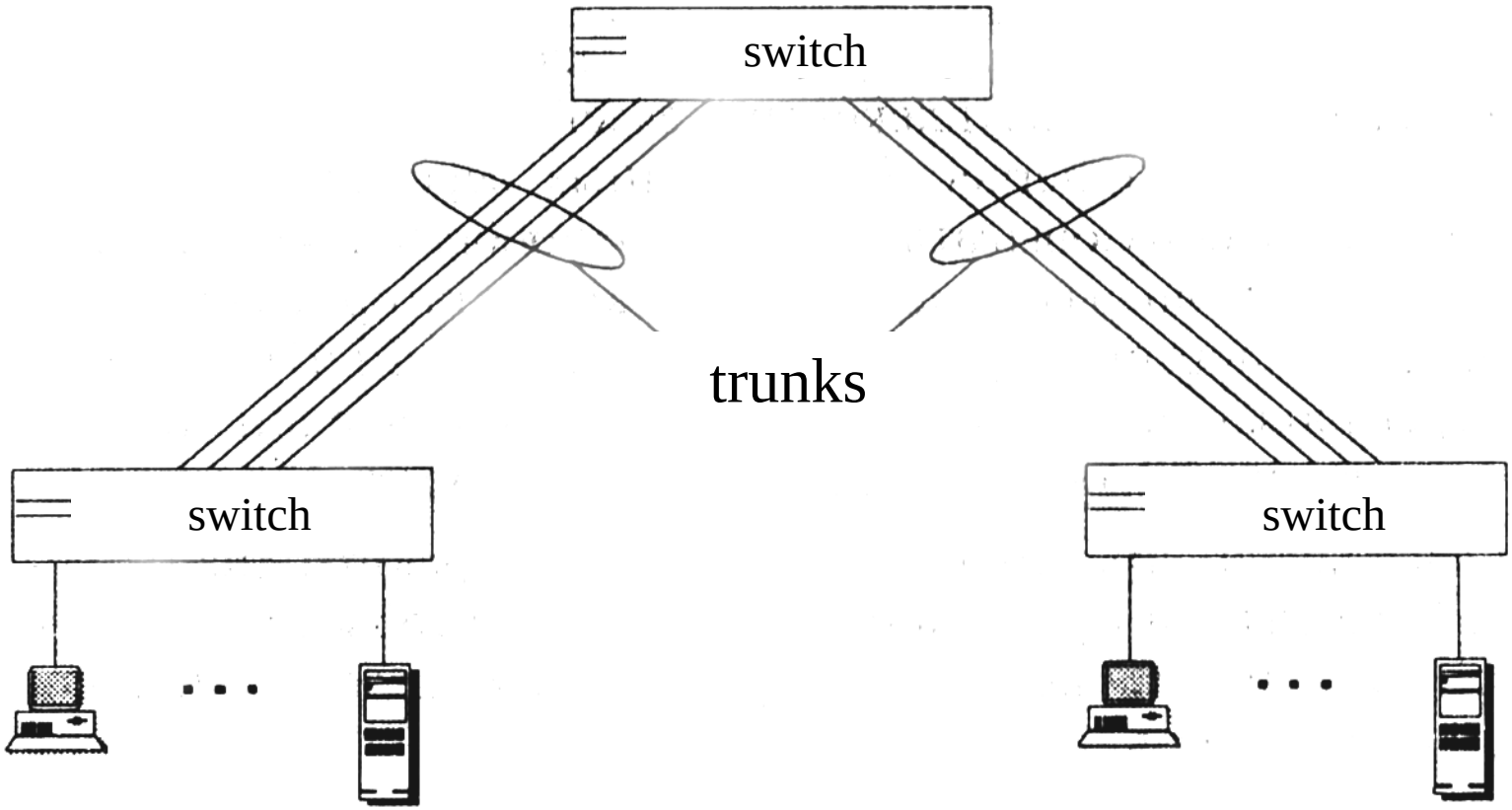
STP, 802.1D


MAC = 0000.8c00.1201
Root bridge
Switch A
All ports designated
(forwarding)
MAC = 0000.8c00.8955
Root port
Switch B
MAC = 0000.8c00.1202
Root port
Switch C
designated
(forwarding)
designated
(forwarding)
MAC = 0000.8c00.2101
Root port
Switch D
designated
(forwarding)
nondesignated
(blocking)
MAC = 0000.8c00.9870
Root port
Switch E

Развитие STP

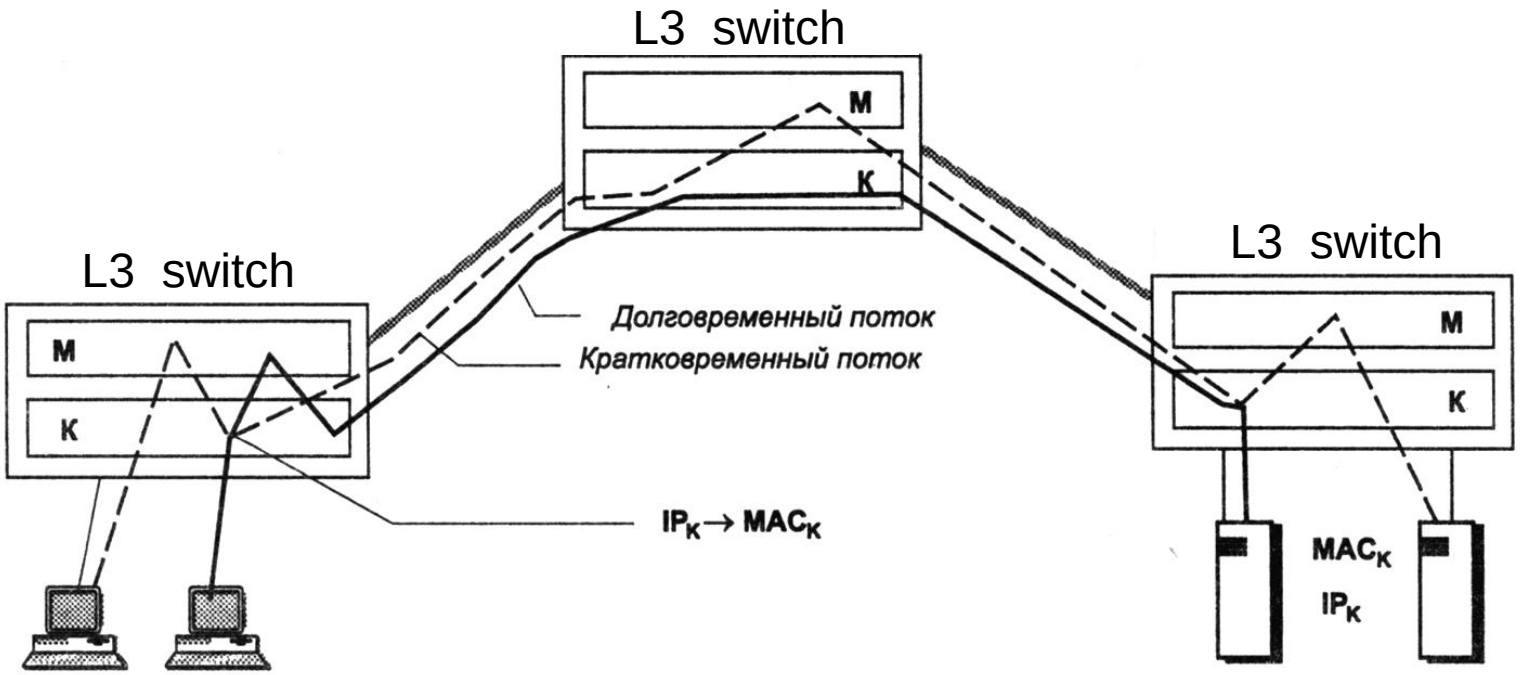
- Per-VLAN Spanning Tree (PVST, +, CISCO)
- Rapid Spanning Tree Protocol (RSTP), IEEE 802.1w
  - RSTP-мост может отвечать на BPDU, посланные с корневого моста
- Multiple Spanning Tree Protocol (MSTP), IEEE 802.1s, позже добавлен в IEEE 802.1Q-2003

Агрегирование - Link aggregation (trunking)



IEEE 802.3ad, Link Aggregation Control Protocol (LACP)

Layer3 коммутаторы

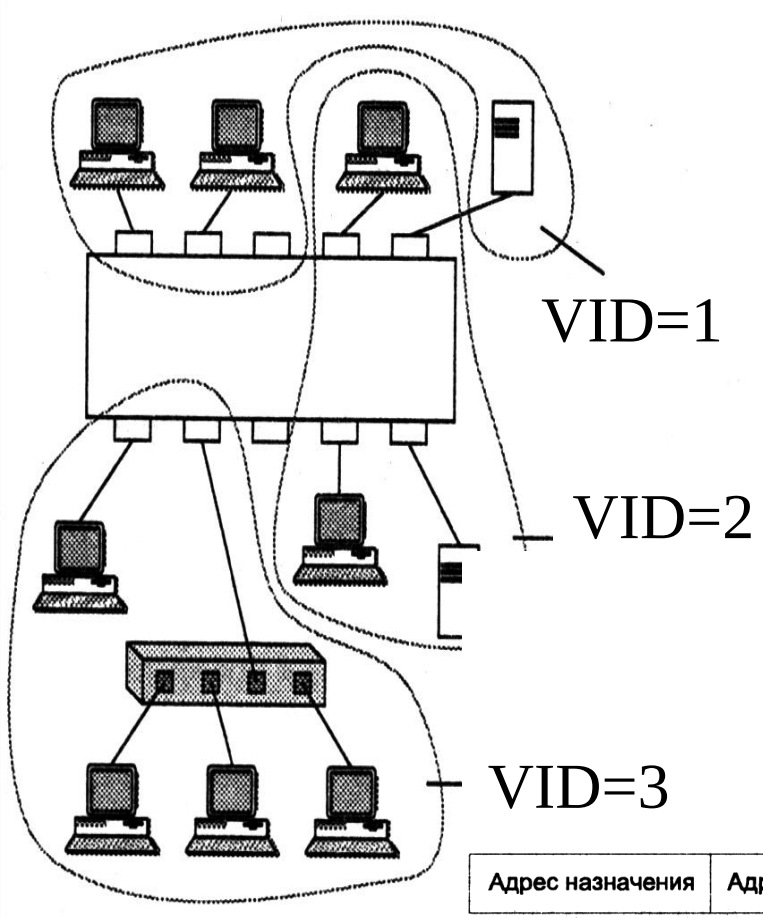


-L3/4 switching – several proprietary technologies

-ASICs

- IP addresses, UDP/TCP port, TOS хешируются и запоминаются в конфигурациях портов на пути потока пакетов (NetFlow)

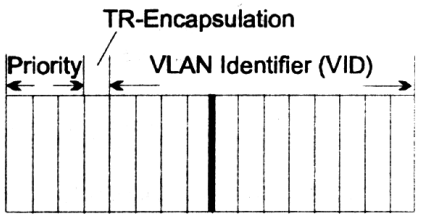
Virtual LANs (VLANs)



IEEE802.1p/Q defines additional field for VLAN ID (12 bits) and priority (3 bits)

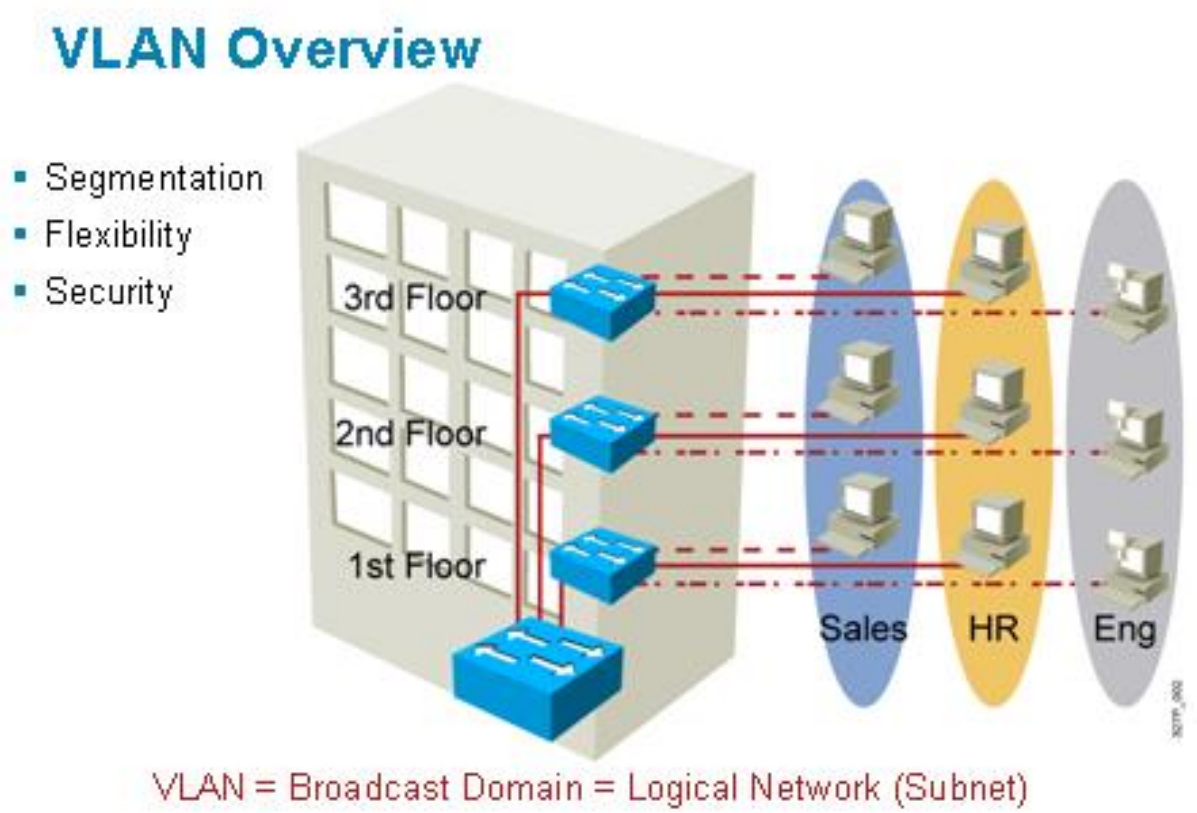
CISCO's proprietary (устарел) – ISL

VLAN – технология 2 уровня, но обычных реализациях требует оборудования 3 уровня.



Адрес назначения	Адрес источника	Tag Protocol Identifier	Метка VLAN	Ether Type	. . .
6 байт	6 байт	2 байта	2 байта	2 байта	

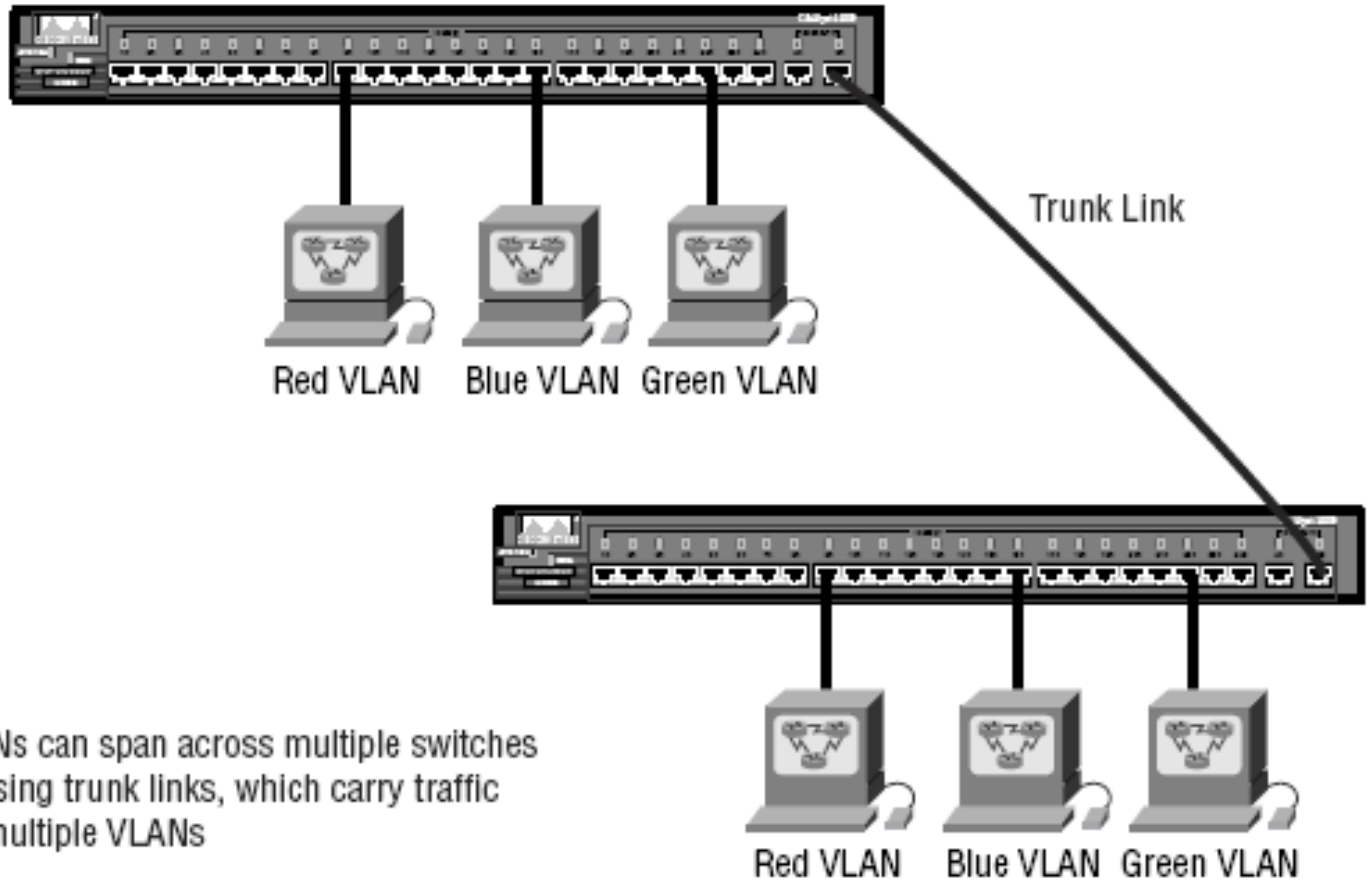
VLAN-ы устраняют физические ограничения



Типы VLAN

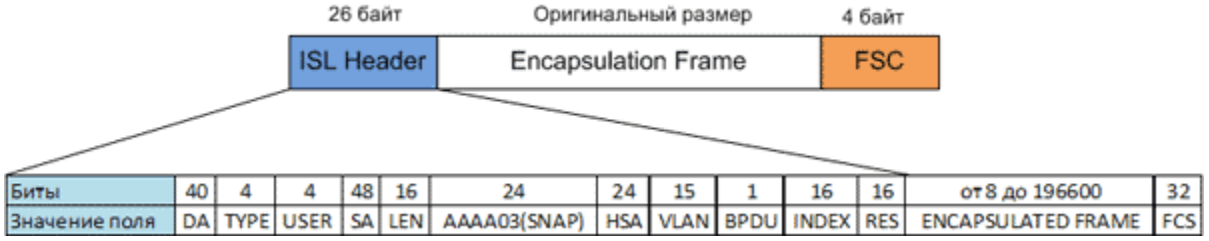
- Статические VLAN
  - Членство в VLAN конфигурируется администратором
- Динамические VLAN
  - Автоматическое определение членства в VLAN, основанное на MAC, протоколах, приложениях.
  - VLAN Management Policy Server (VMPS) у CISCO.

CISCO-транки. Режимы портов: access (untagged), trunk (tagged).



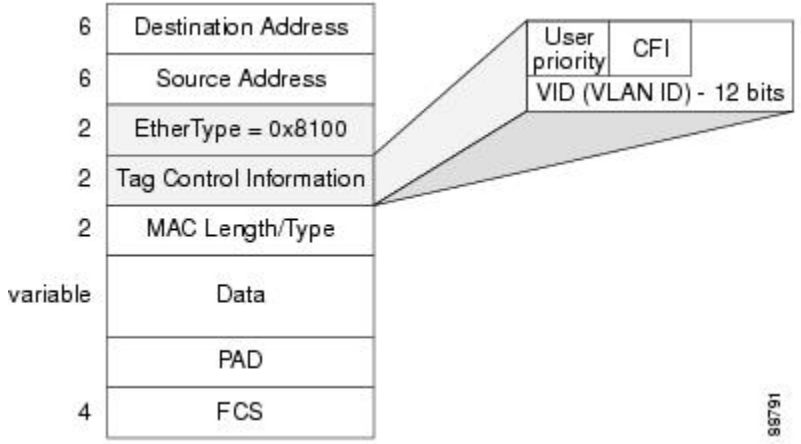
VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs

VLAN методы



Биты	40	4	4	48	16	24	24	15	1	16	16	от 8 до 196600	32
Значение поля	DA	TYPE	USER	SA	LEN	AAAA03(SNAP)	HSA	VLAN	BPDU	INDEX	RES	ENCAPSULATED FRAME	FCS

- Inter-Switch Link (ISL)
- IEEE 802.1Q
- VLAN Trunking Protocol (VTP)
  - Режимы: client, server, transparent



Настройка VLAN для 1900

- >en
- #config t
- (config)#hostname 1900
- 1900(config)#vlan 2 name sales
- 1900(config)#vlan 3 name marketing
- 1900(config)#vlan 4 name mis
- 1900(config)#exit
- 1900#sh vlan

- 1900#config t
- 1900(config)#int e0/2
- 1900(config-if)#vlan-membership static 2
- 1900(config-if)#int e0/4
- 1900(config-if)#vlan-membership static 3
- 1900(config-if)#int e0/5
- 1900(config-if)#vlan-membership static 4
- 1900(config-if)#exit
- 1900(config)#exit

Настройка VLAN для 2950

- Switch>en
- Switch#config t
- Switch(config)#vlan 2
- Switch(config-vlan)#
- Switch(config-vlan)#vlan 3
- Switch(config-vlan)#name Sales
- Switch(config-vlan)#vlan 4
- Switch(config-vlan)#name Finance
- Switch(config-vlan)#^Z
- Switch#sh vlan brief

- Switch(config-if)#int f0/2
- Switch(config-if)#switchport access vlan 2
- Switch(config-if)#int f0/3
- Switch(config-if)#switchport access vlan 3
- Switch(config-if)#int f0/4
- Switch(config-if)#switchport access vlan 4
- Switch(config-if)#

Настройка транков 1900, 2950

- 1900#config t
- 1900(config)#int f0/26
- 1900(config-if)#trunk on

- Switch#config t
- Switch(config)#int f0/12
- Switch(config-if)#switchport mode trunk
- Switch(config-if)#^Z
- Switch#

Настройка транков для 3550

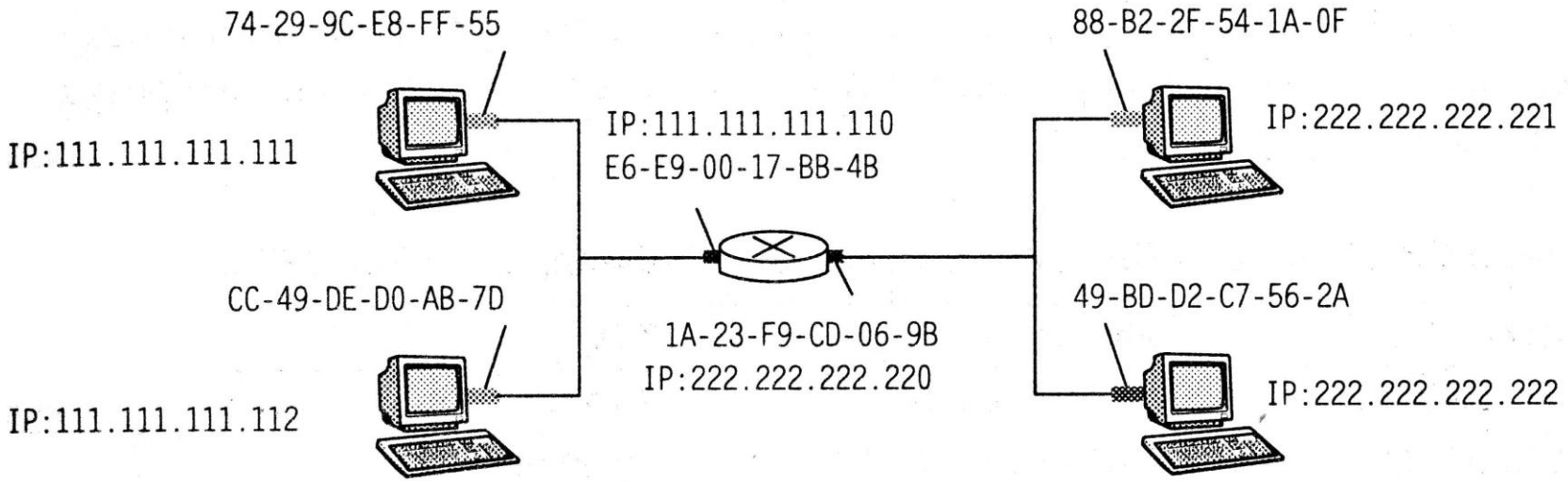
- Switch#config t
- Switch(config)#int f0/12
- Switch(config-if)#switchport mode trunk
- Switch(config-if)#switchport trunk encapsulation ?
  - **dot1q** Interface uses only 802.1q trunking encapsulation when trunking
  - **isl** Interface uses only ISL trunking encapsulation when trunking
  - **negotiate** Device will negotiate trunking encapsulation with peer on interface

Маршрутизация между VLAN

- 2600#config t
- 2600(config)#int f0/0.1
- 2600(config-subif)# encapsulation dot1q vlan#
- 2600(config-subif)# encapsulation dot1q 1
- 2600(config-subif)# ip address 192.168.10.129 255.255.255.240
- 2600(config-subif)# int f0/0.2
- 2600(config-subif)# encapsulation dot1q 2
- 2600(config-subif)# ip address 192.168.10.46 255.255.255.240

- 2600(config)#int f0/0.1
- 2600(config-subif)#encapsulation isl vlan#

Протокол ARP



Layer 2 атаки

- MAC flooding [fl/\d…]
  - Потребление всей памяти коммутатора под MAC-таблицу для перевода его в failopen mode (hub-подобный)
  - Защита – привязка портов к MAC или ограничение кол-ва MAC на порт
- ARP(MAC)-spoofing, ARP-poisoning
  - ассоциация MAC аттакующего с IP другого узла (шлюза, сервера AAA) -> DoS, пассивное сканирование or MiM атака
  - Защита: контроль ARP с помощью arpwatch , static ARP, dynamic ARP inspection (DAI), DHCP snooping
- VLAN Hopping
  - Эмуляция ПО атакующего коммутатора с trunk портом, поддерживающем ISL или 802.1q и Dynamic Trunking Protocol (DTP) signaling. Или теггирование кадров с двумя 802.1q заголовками.
  - Защита: установка всех пользовательских портов в non-trunking режим выключив DTP
- STP атака
  - Анонсирование системой атакующего моста с низким значением STP-приоритета. Постоянная конвергенция STP приведет к DoS.
  - Защита: корпоративные решения (например, CISCO's STP BPDU guard/root guard) используются для предопределения STP-топологии.