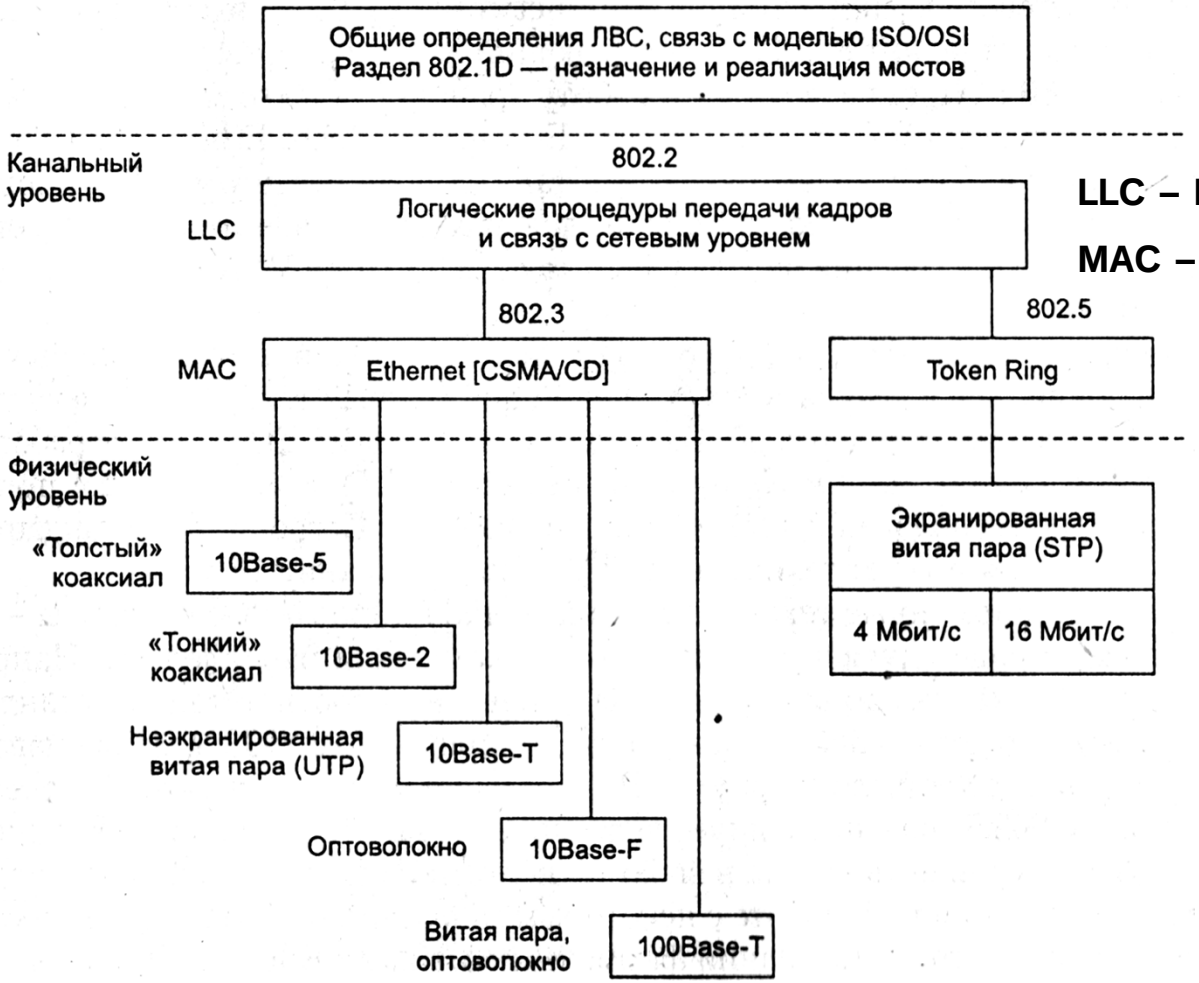
Технологии 2 уровня

комитеты IEEE 802.x и соответствующие стандарты

IEEE – Institute of Electrical and Electronics Engineers, институт инженеров по э/тех. и э. (США)

- 802.1 — Internetworking — объединение сетей;
- 802.2 — Logical Link Control, LLC — управление логической передачей данных;
- 802.3 — Ethernet с методом доступа CSMA/CD;
- 802.4 — Token Bus LAN — локальные сети с методом доступа Token Bus;
- 802.5 — Token Ring LAN — локальные сети с методом доступа Token Ring;
- 802.6 — Metropolitan Area Network, MAN — сети мегаполисов;
- 802.7 — Broadband Technical Advisory Group — техническая консультационная группа по широкополосной передаче;
- 802.8 — Fiber Optic Technical Advisory Group — техническая консультационная группа по волоконно-оптическим сетям;
- 802.9 — Integrated Voice and data Networks — интегрированные сети передачи голоса и данных;
- 802.10 — Network Security — сетевая безопасность;
- 802.11 — Wireless Networks — беспроводные сети;
- 802.12 — Demand Priority Access LAN, 100VG-AnyLAN
- 802.15 — WPAN Task Group 6 (TG6) Body Area Networks
- 802.16 — WirelessMAN
- 802.20 — Mobile Broadband Wireless Access
- 802.22 — WRAN
- ISO/IEC 8802-x – соответствующие международные стандарты ISO

Модель IEEE начальных уровней LAN и распределение стандартов по уровням



LLC – Logical Link Control

MAC – Media Access Control

Кадры стандартов 802

Заголовок Ethernet	Кадр LLC

Кадр 802.3/LLC

6	6	2	1	1	1(2)	46–1497 (1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр Raw 802.3/Novell 802.3

6	6	2	46–1500	4
DA	SA	L	Data	FCS

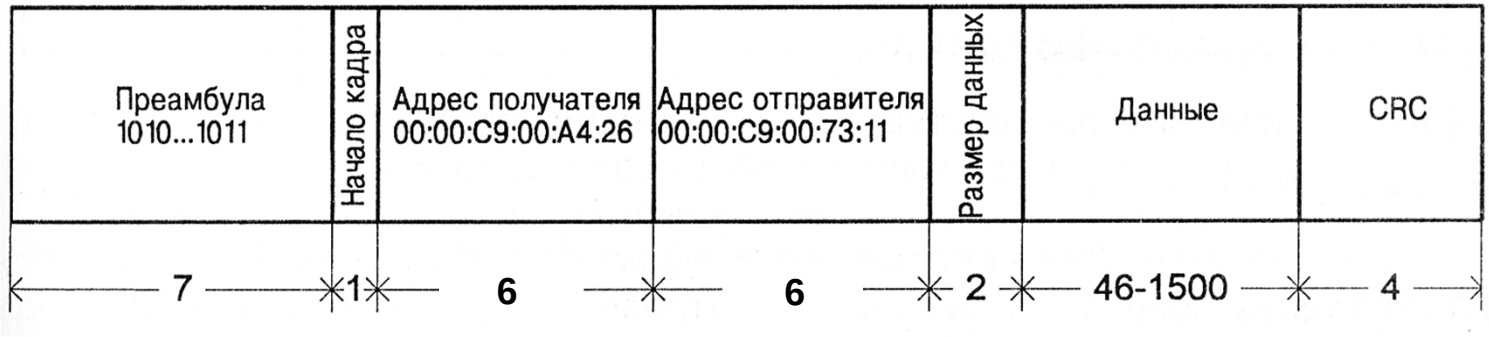
Кадр Ethernet DIX (II)

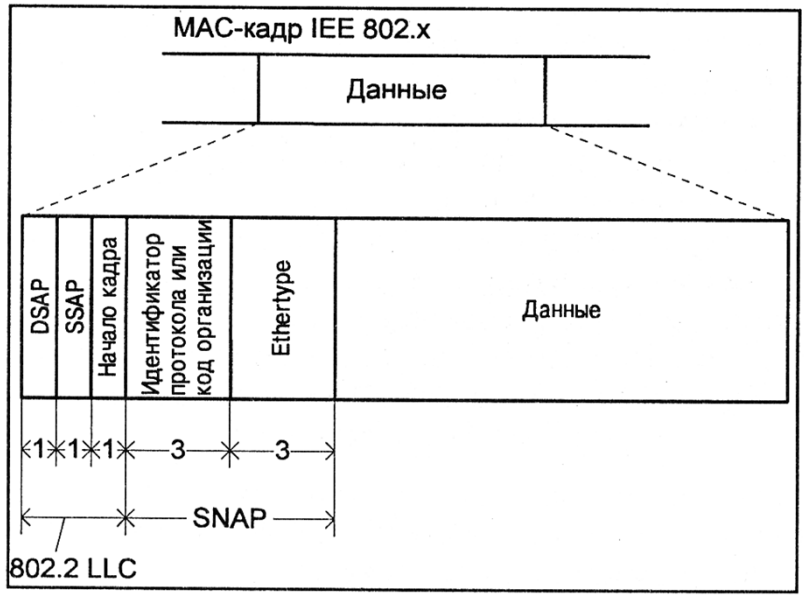
6	6	2	46–1500	4
DA	SA	T	Data	FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46–1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

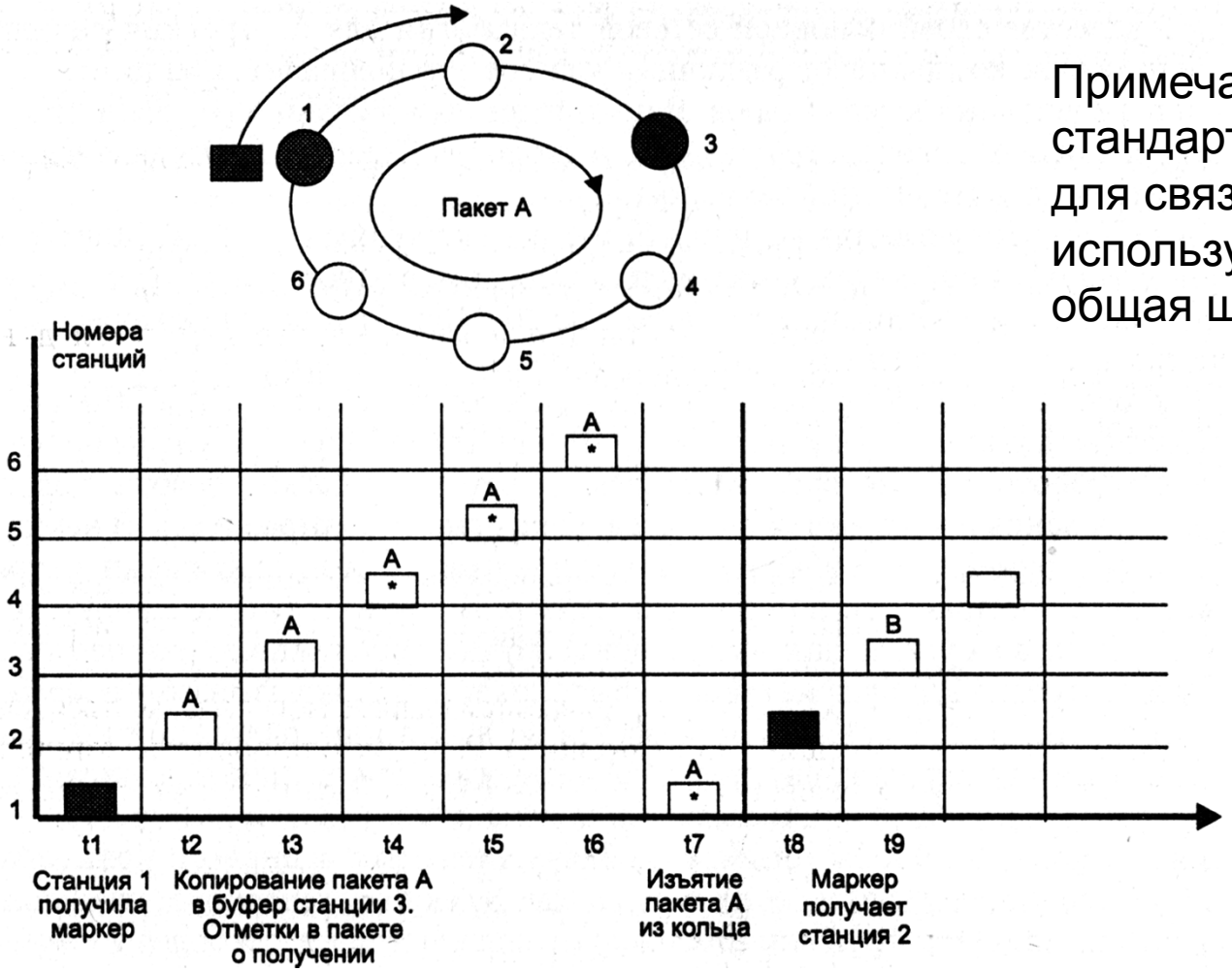
Форматы кадров 802.3 и LLC





Каждый производитель Ethernet устройств использует свои диапазоны MAC адресов, которые покупает у IEEE. Идентификатор производителя (OUI - Organizationally Unique Identifier) занимает первые 3 байта MAC-адреса устройства Ethernet. Например, MAC-адрес 00:11:95:bf:57:26 - оборудование фирмы D-Link/Тайвань (OUI=00:11:95)

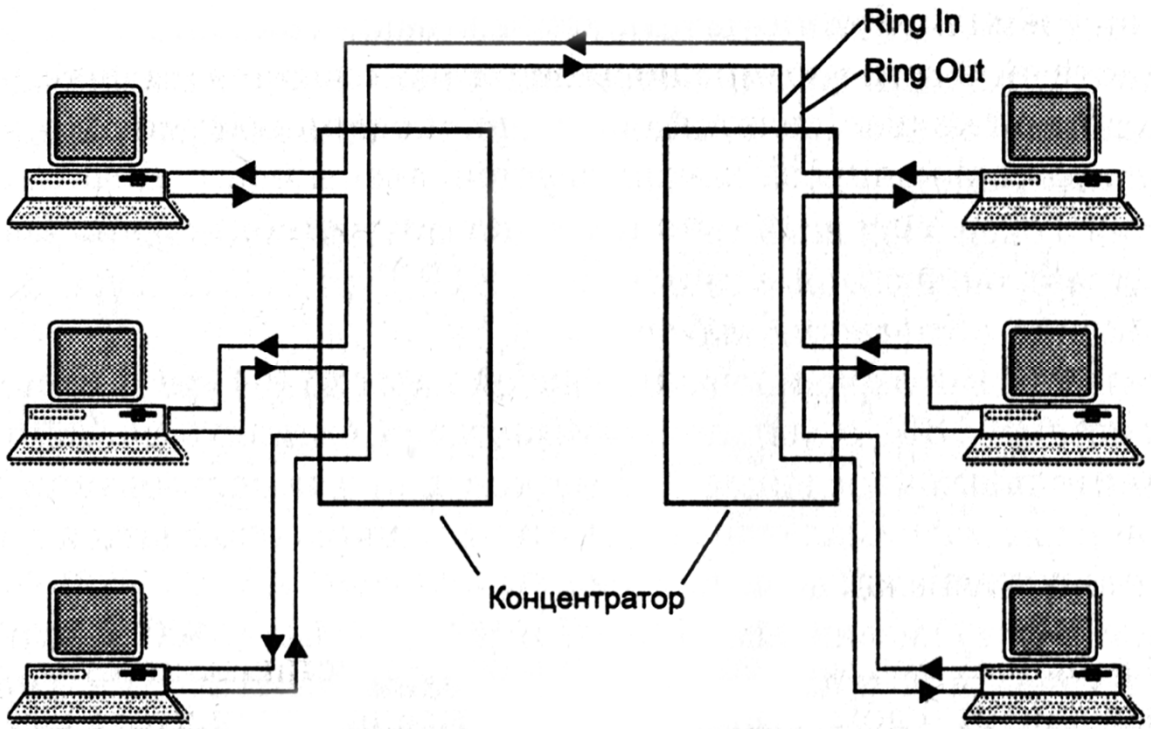
Маркерный метод управления каналом (802.4, 802.5, FDDI и т.п.)



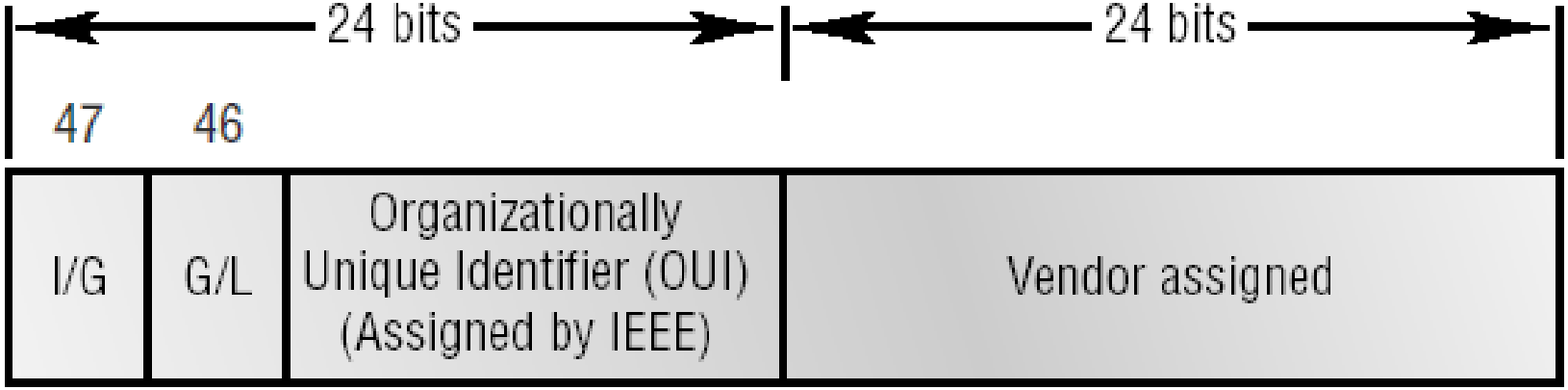
Примечание: в стандарте 802.4 для связи узлов используется общая шина

Реализация Token Ring (IBM)

- Token Ring – 16 Mbps;
- High-Speed Token Ring (HSTR) – 100/155 Mbps;
- среды: STP1, UTP3, UTP6, MMF, SMF
- ограничение на максимальную длину кольца – 4000м (не жесткое)



Ethernet адресация



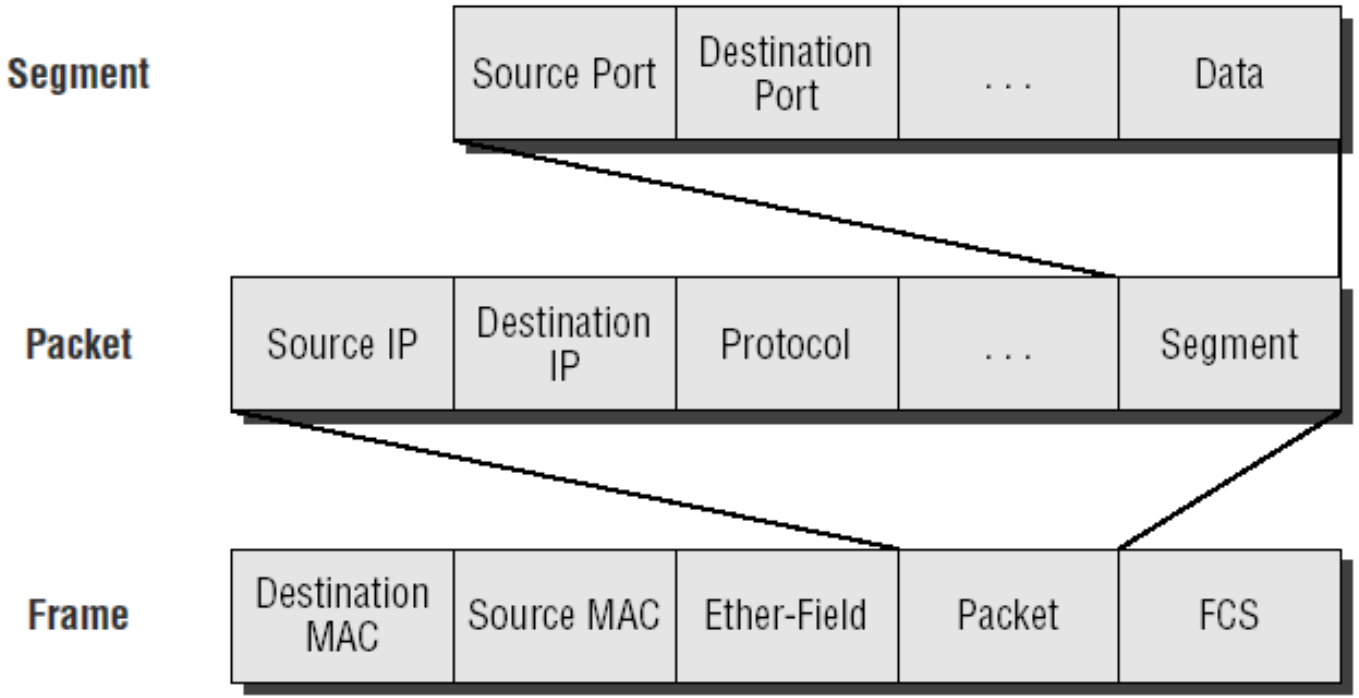
OUI - organizationally unique identifier

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.

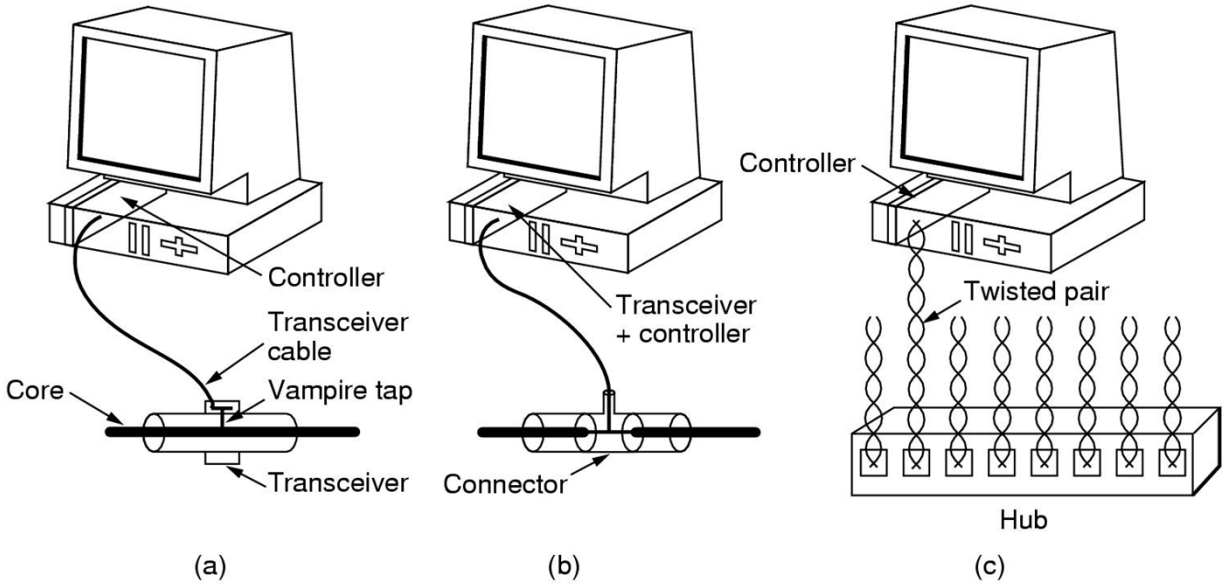
Ethernet (IEEE 802.3) standards

- 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

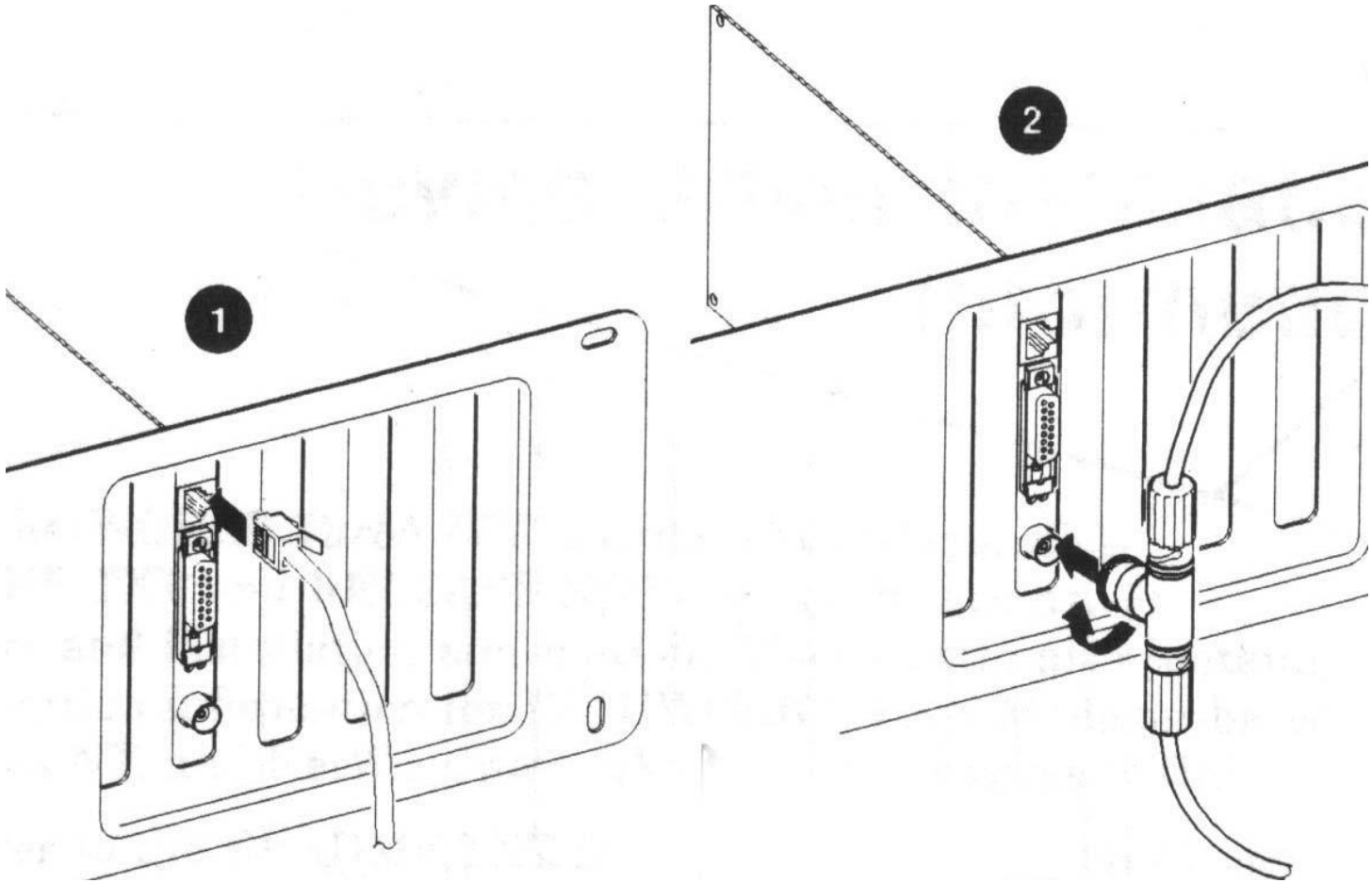
Реализация Ethernet



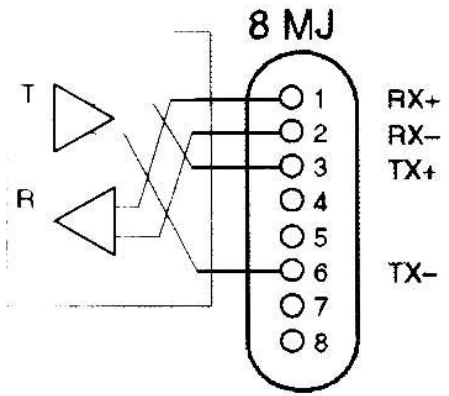
- a – 10Base-5
- b – 10Base-2
- c – 10Base-T, 100Base-T, 1000Base-T, 10GBase-T (кат. 6a и 7), 100GBase (возможна витая пара, 10м!)

Среды: витая пара (UTP3-7; STP1,2), оптика (MMF, SMF)

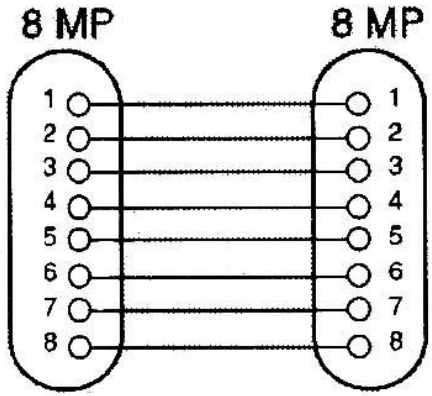
Витая пара (TP), рис. 1 и коаксиальный кабель, рис. 2

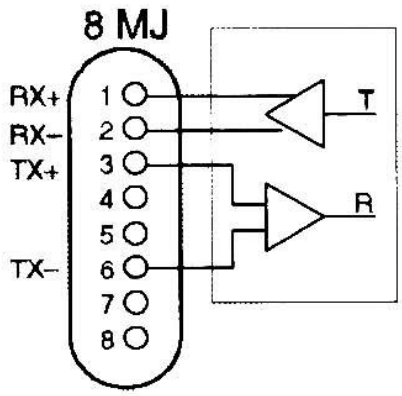


Коннекторы и патч-кабели для среды витая пара (Twisted Pair, TP)

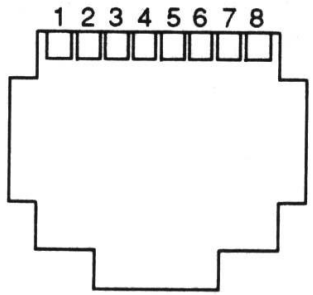


DECrepeater 900TM





MAU



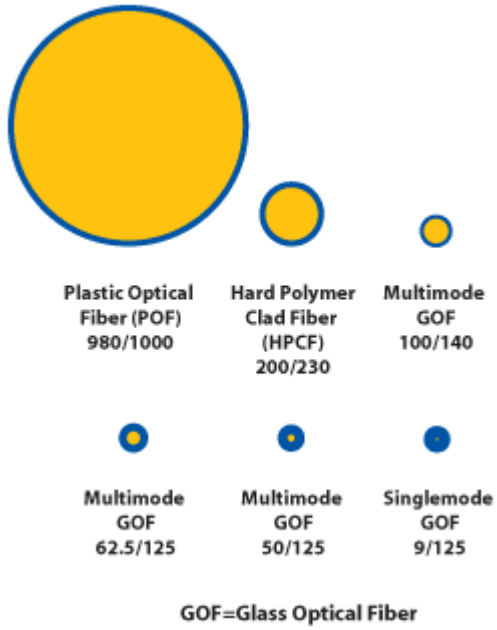
гнездо RJ-45

Стандарты TIA/EIA-568A/B, ISO11801

- TIA/EIA-568A и -568B - два стандарта на установку коннекторов на витую пару 3 и 5 категорий. Оба стандарта подходят и для высокоскоростных соединений, однако 568B обычно применяют в постоянных соединениях, а 568A - для коротких соединителей (патчей). Единственное отличие этих стандартов - порядок, в котором соединяются контакты разъема с парами (оранжевой и зеленой). На обоих концах кабелей должны быть одинаковые запрессовки: либо 568A, либо 568B.
- Если держать разъем так, как при подключении к розетке на стене (защелкой вниз, а контактами вверх), то контакты нумеруются 1-8 слева направо. В таблице приводятся соответствия между номерами контактов и цветом проводников пар.

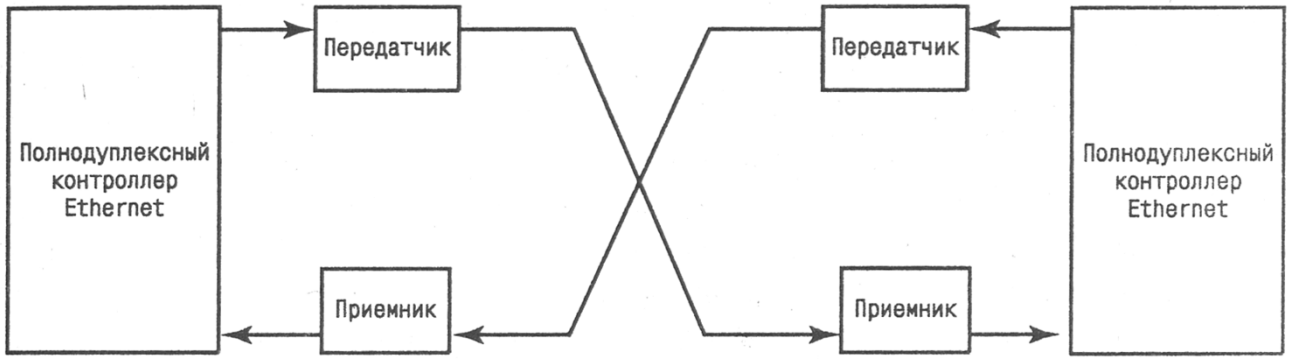
EIA/TIA-568A			**EIA/TIA-568B**
контакт	цвет		цвет
1	бел./зел.		бел./оранж.
2	зеленый		оранжевый
3	бел./оранж.		бел./зел
4	голубой		голубой
5	бел./голуб.		бел./голуб.
6	оранжевый		зеленый
7	бел./корич.		бел./корич.
8	коричневый		коричневый

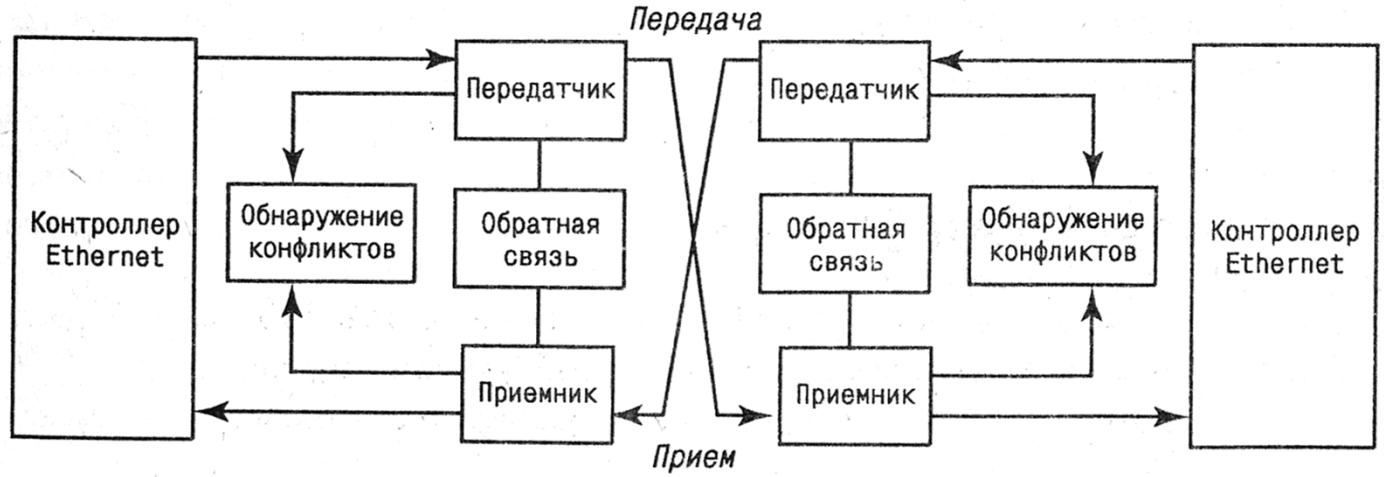
Коннекторы для оптоволокна (ST, FC, CS). Диаметры пластиковых и стеклянных кабелей.



CS-дуплекс

Полу- и полнодуплексные режимы





Метод управления каналом CSMA/CD (802.3)

CSMA/CD - Carrier Sense Multiple Access with Collision Detection, протокол множественного доступа с прослушиванием несущей и обнаружением коллизий

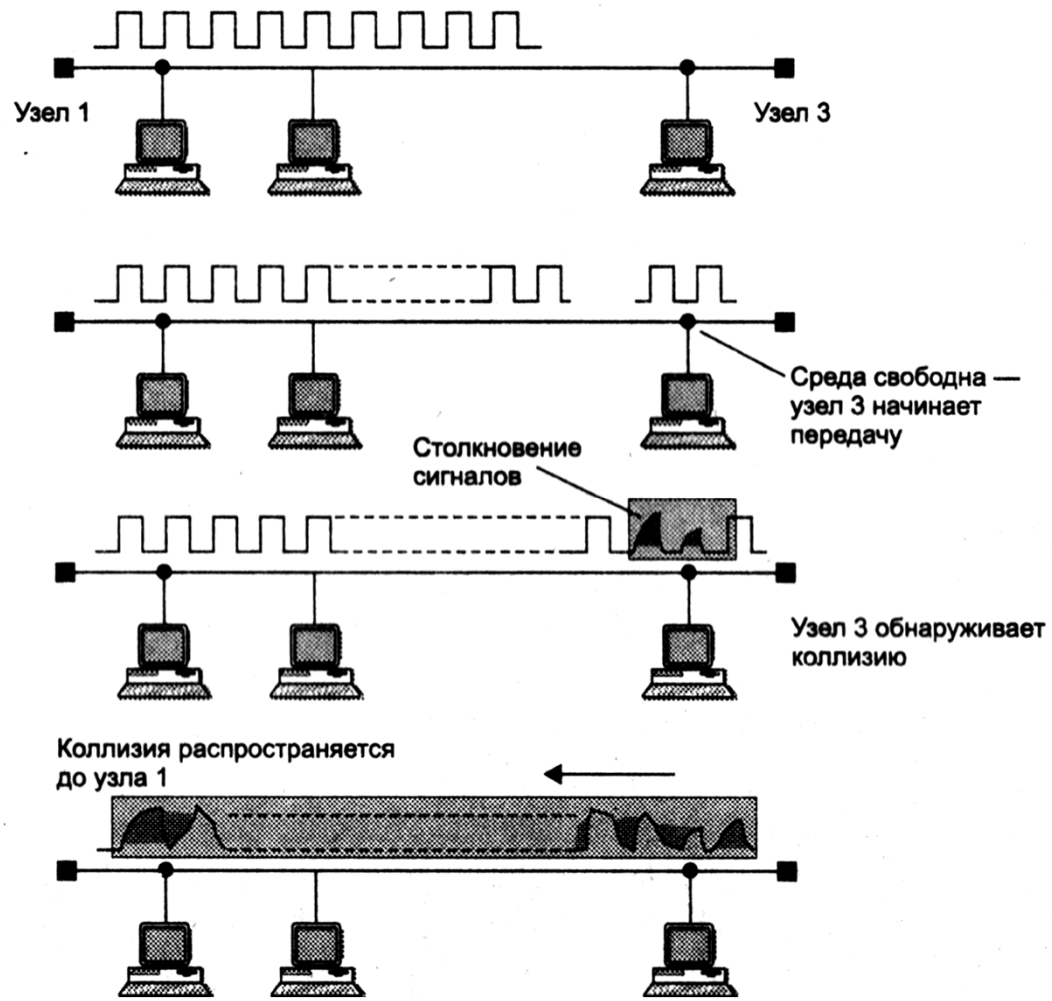
Обнаружение коллизий

Время двойного оборота:

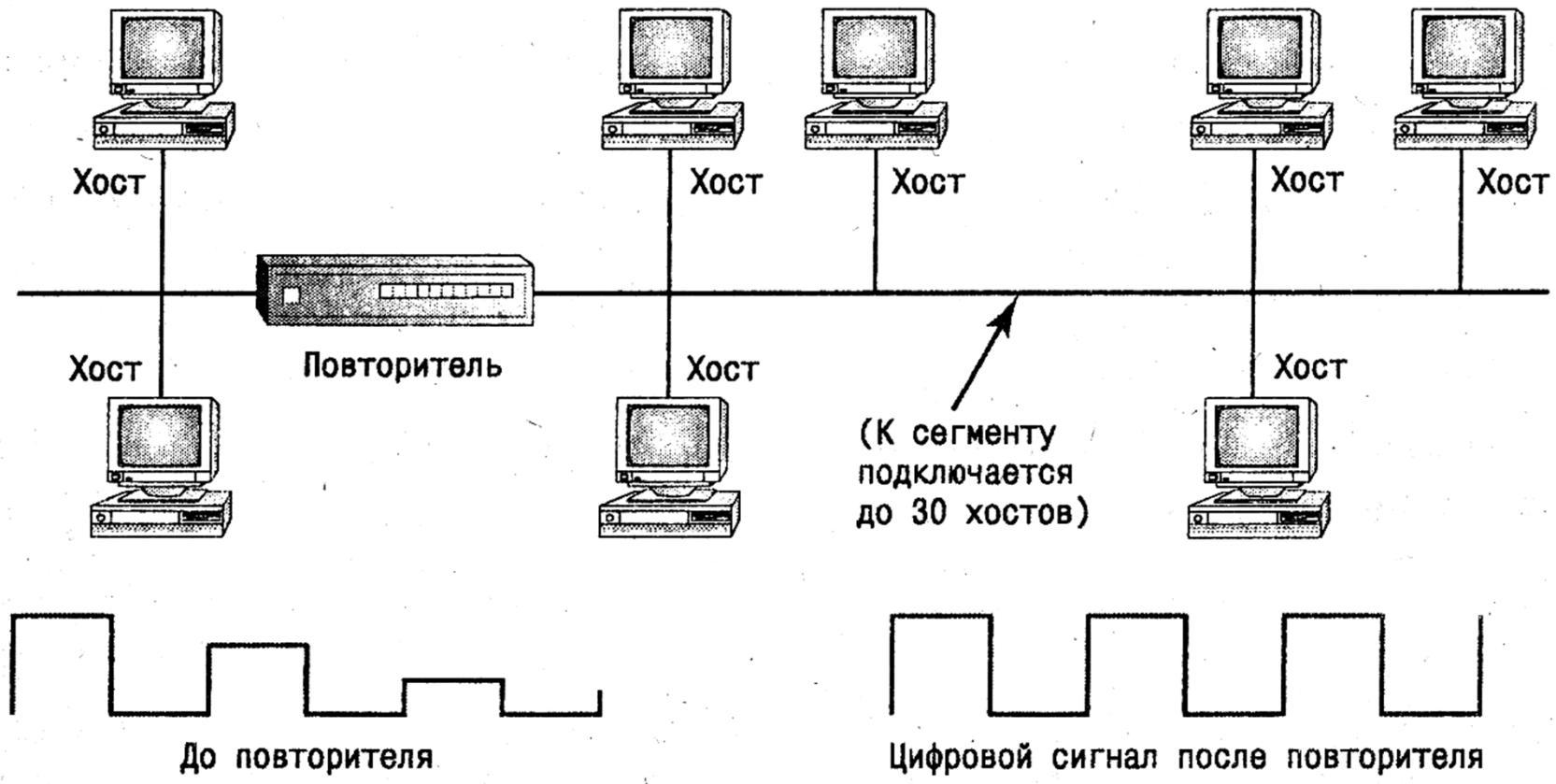
Тд.о.=2*L/c*k

L - длина линии

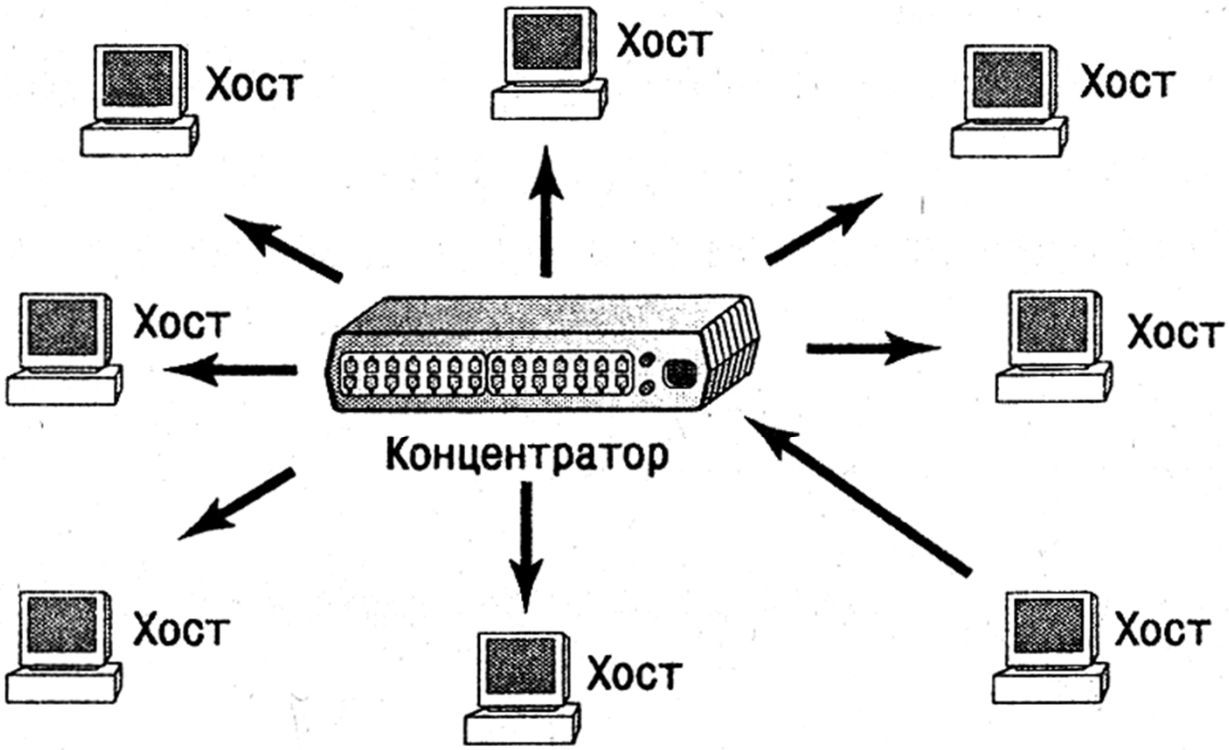
k – коэффициент замедления



Устройства LAN: повторитель



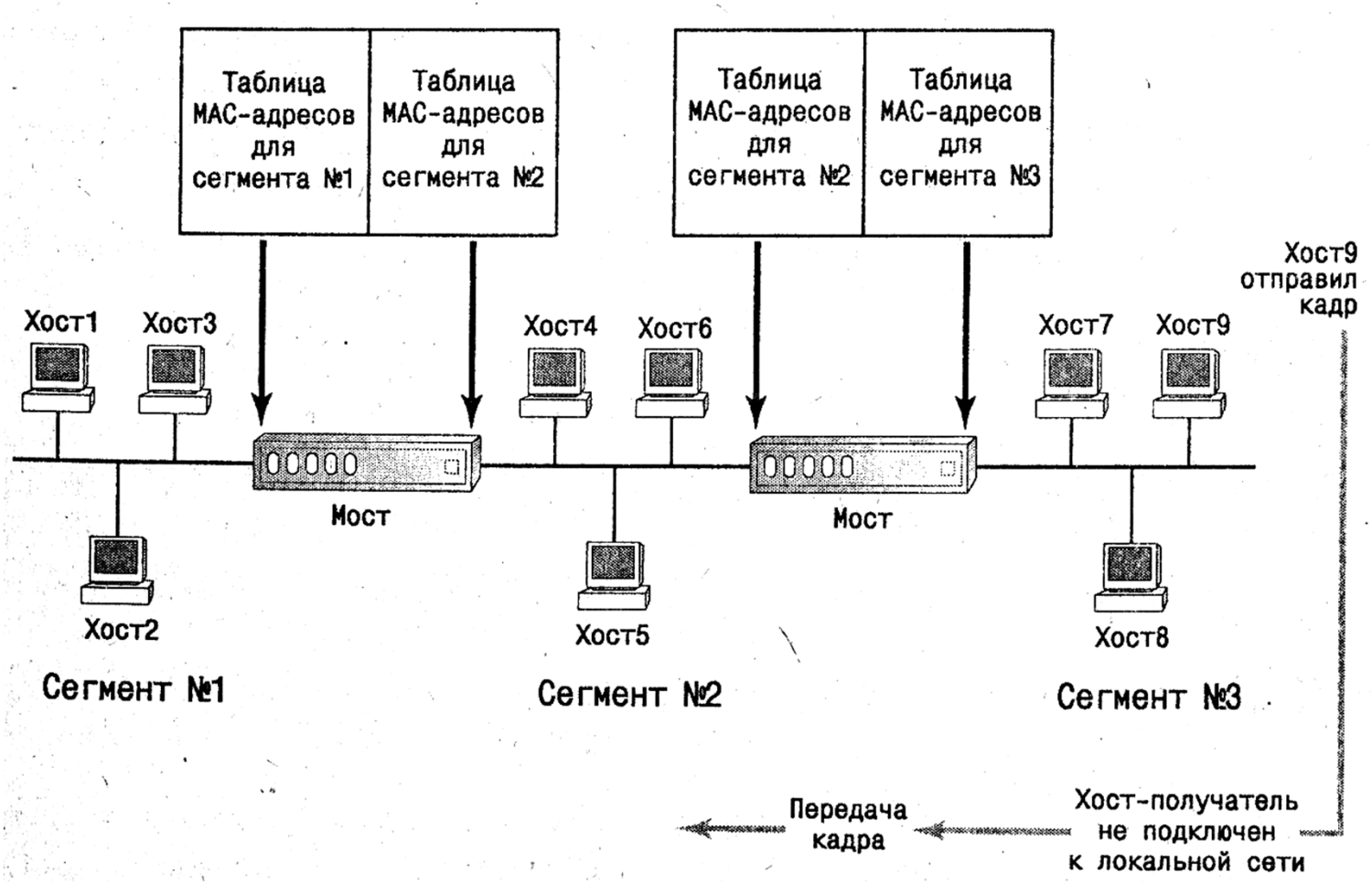
Устройства LAN: концентратор



Когда один хост ведет передачу, остальные хосты должны выполнять прослушивание

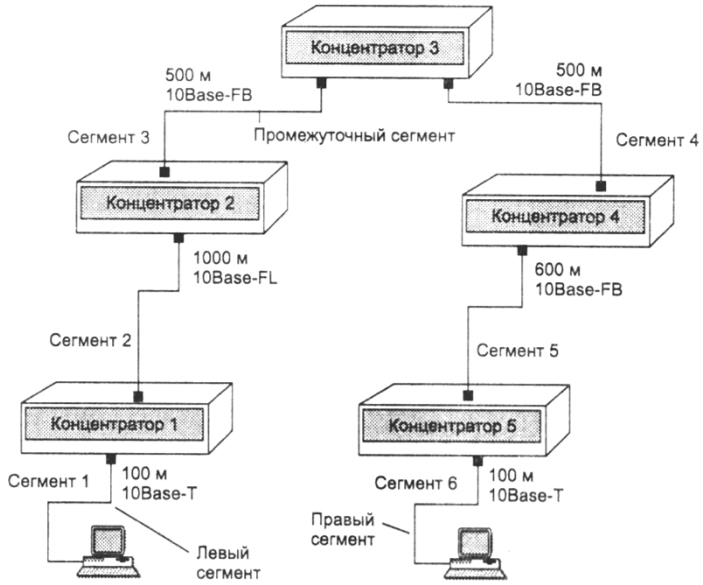
Концентратор в локальной сети

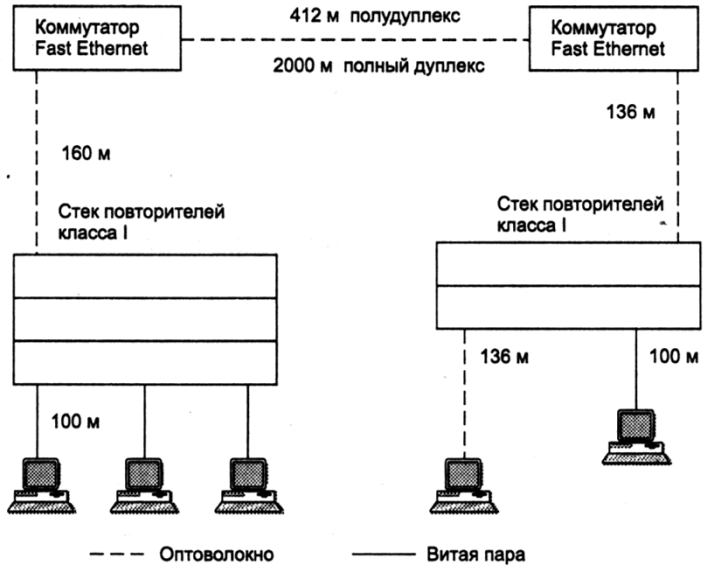
Устройства LAN: мост/коммутатор



Домен коллизий

- Домен коллизий (collision domain) – область сети Ethernet, распространяясь в которой, кадр может вызвать конфликт (коллизию).
- Коммутаторы (свичи), маршрутизаторы (роутеры) ограничивают распространение коллизий.





Расчет максимальной производительности Ethernet

- Определим скорость передачи данных пользователя для случая, когда размер кадра минимальный – по стандарту 46 байт:
  - преамбула кадра – 8 байт;
  - адреса источника и приемника – 6+6=12 байт;
  - поле длины кадра – 2 байта;
  - поле данных – 46 байт;
  - поле контрольной суммы (CRC-32) – 4 байта;
  - всего – 72 байта = 576 бит
  - передача такого кадра займет 57.6 мкс.
  - Добавляя техпаузу 9.6 мкс, получим 67.2 мкс или 14880 кадр/с
  - Пропускная способность т.о. равна 14880 x 46 x 8 = 5.48 Мбит/с
- Определим скорость передачи теперь для кадров максимального размера – по стандарту 1500 байт:
  - Период кадра 1526 x 8 x 0,1 мкс + 9.6 мкс = 1230,4 мкс
  - Скорость - 812,7 кадр/с или 812,7 x 1500 x 8 Мбит/с = 9,75 Мбит/с

Обработка коллизий в 802.3

- Алгоритм Binary Backoff (экспоненциальный откат)
  - После i коллизий, число пропускаемых временных слотов выбирается в диапазоне 0 .. 2^i-1
  - После 10 коллизий интервал фиксируется в диапазоне 0 .. 1024 слотов
  - BB алгоритм – компромисс для конфигураций с малым и большим количеством узлов, т.е. с большой и малой интенсивностью коллизий

Производительность 802.3

- Вероятность получения канала определяется как $A=kp(1-p)^{k-1}$, где p – вероятность передачи каждой станции в течении занятого слота
- A – максимально, когда p=1/k, при этом A-> 1/e, с увеличением k
- Вероятность того, что длительность конфликта j слотов – $A(1-A)^{j-1}$
- тогда среднее число слотов конфликтного периода:

$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}$$

Производительность 802.3

- Если слот имеет длительность t, средний интервал конфликта w=t/A, где A – вероятность передачи в слот для одной из k станций: $A = kp(1-p)^{k-1}$, p – вероятность передачи каждой станции в течении интервала конфликта.

  Тогда, для кадра длительностью T_{frame} сек.:

$$Эффективность = \frac{T_{frame}}{T_{frame} + t / A}$$

- Для сети с пропускной способностью B, размером кадра F, длиной кабеля L и скоростью распространения сигнала c:

$$Эффективность = \frac{1}{1 + 2BLe / cF}$$

Методика расчета 10Мб Ethernet

- Необходимо выполнение 4-х условий:
  - количество станций не более 1024;
  - длина сегмента не более определенной в стандарте для данной среды;
  - PDV (Path Delay Value) – не более 575bt;
  - сокращение межкадрового интервала за счет PVV (Path Variability Value) не более 49bt. Т.о., техпауза: 96 – 49 = 47bt.

Данные для расчета PDV 10Мб

Тип сегмента	База левого сегмента, bt	База промежуточного сегмента, bt	База правого сегмента, bt	Задержка среды на 1м, bt	Максимальная длина сегмента, м
10Base-5	11,8	46,5	169,5	0,0866	500
10Base-2	11,8	46,5	469,5	0,1026	185
10Base-T	15,3	42,0	165,0	0,113	100
10Base-FB	-	24	-	0,1	2000
10Base-FL	12,3	33,5	156,5	0,1	2000

Прим1.: комитет 802.3 в таблицах определяет сразу удвоенные задержки, не разделяя сеть на сегменты.

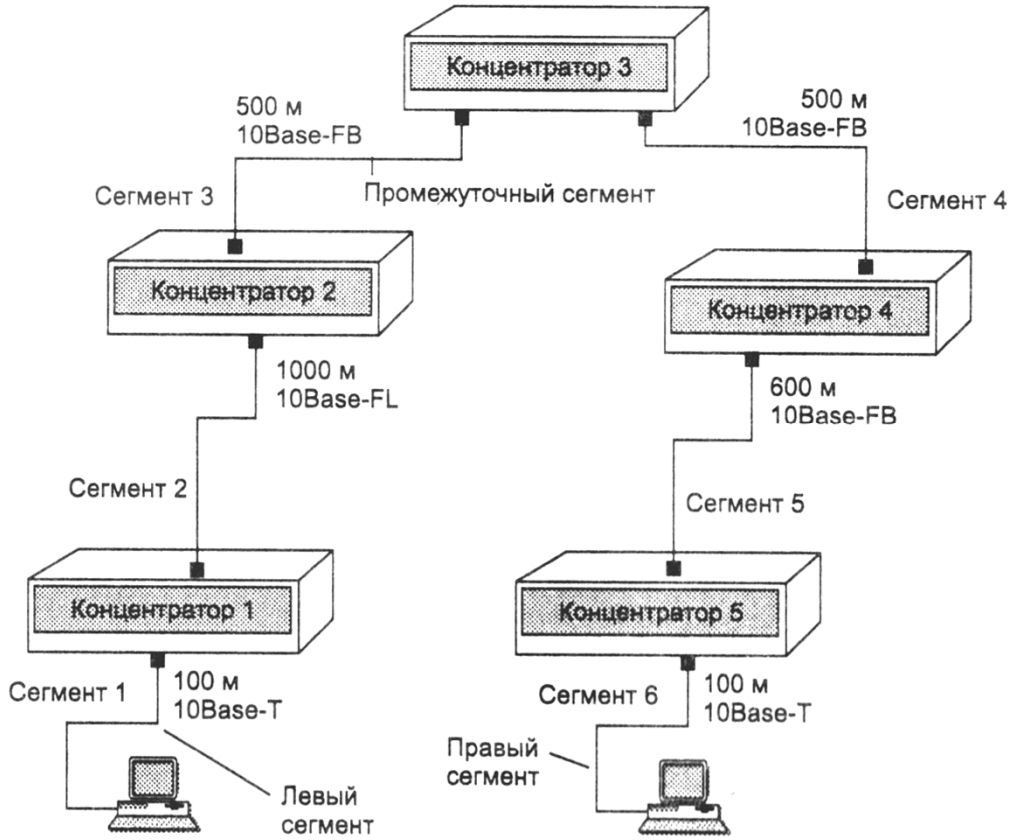
Правило (5-4-3): 5 сегментов - 4 повторителя - 3 нагруженных сегмента

Правило (для сетей 10Base-T): не более 4 хабов между любыми двумя станциями сети

Данные для расчета PVV 10Мб

Тип сегмента	Передающий сегмент	Промежуточный сегмент
10Base-5, 10Base-2	16	11
10Base-FB	-	2
10Base-FL	10	8
10Base-T	10,5	8

Расчетная конфигурация 10Мб



Данные для расчета 100Мб сетей

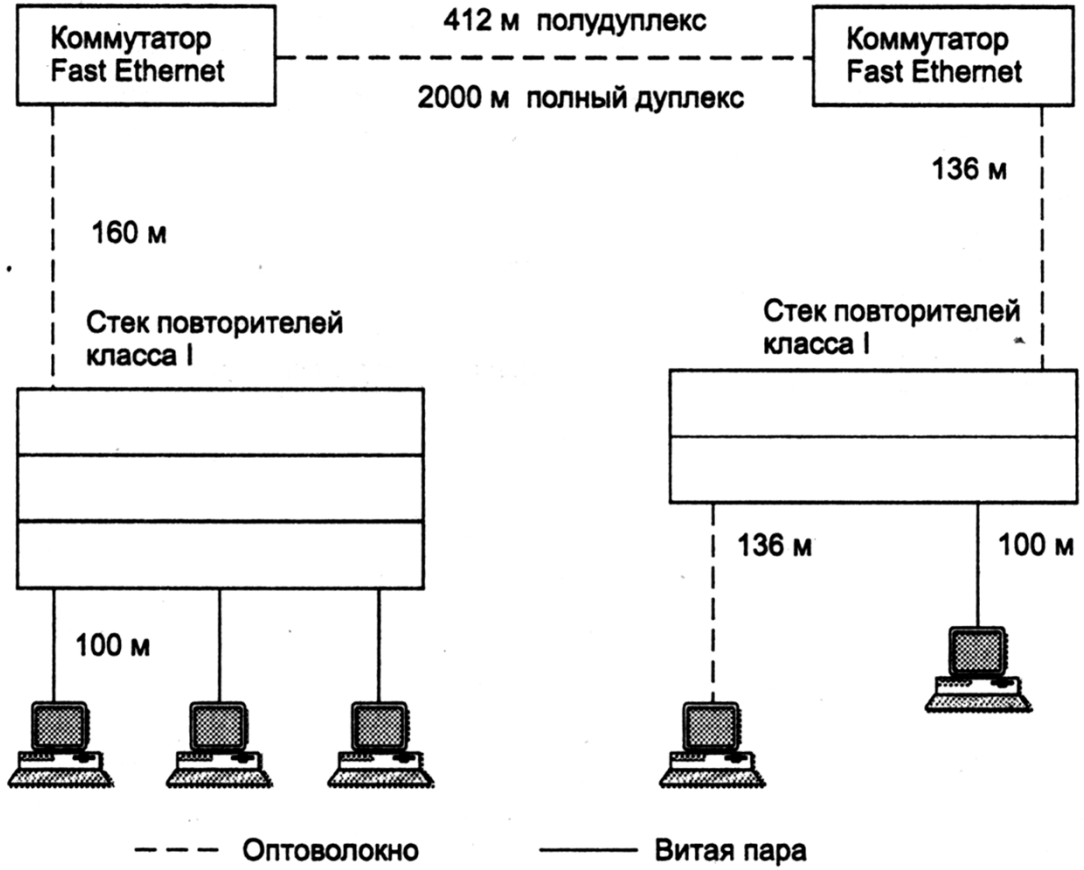
Тип кабеля	Удвоенная задержка на 1 м	Удвоенная задержка кабелем максимальной длины
UTP Cat 3	1,14 bt	114 bt (100 м)
UTP Cat 4	1,14 bt	114 bt (100 м)
UTP Cat 5	1,112 bt	111,2 bt (100 м)
STP	1,112 bt	111,2 bt (100 м)
оптоволокно	1,0 bt	412 bt (412 м)

Тип сетевого устройства	Максимальная задержка при двойном обороте
Два адаптера TX/F	100 bt
Два адаптера T4	138 bt
Один адаптер TX/FX и один T4	127 bt
Повторитель класса I	140bt
Повторитель класса II	92bt , 67bt (T4)

Прим1.: в задержках учитываются преамбулы кадров, поэтому PDV сравнивают с 512bt, а не 575bt.

Прим.2: комитет 802.3 в таблицах определяет сразу удвоенные задержки, не разделяя сеть на сегменты.

Расчетная конфигурация 100Мб



Правила:

-1 репитер I класса (4B/5B -> 8B/6T)

-2 репитера класса II, кабель < 5 м

Прим.: кодирование 8B/6T со скоростью передачи 33 Мбит/с по каждой из 3-х пар используется в технологии **HP VG-AnyLAN.** Четвертая пара применяется для CS/CD

Новые и будущие виды TP

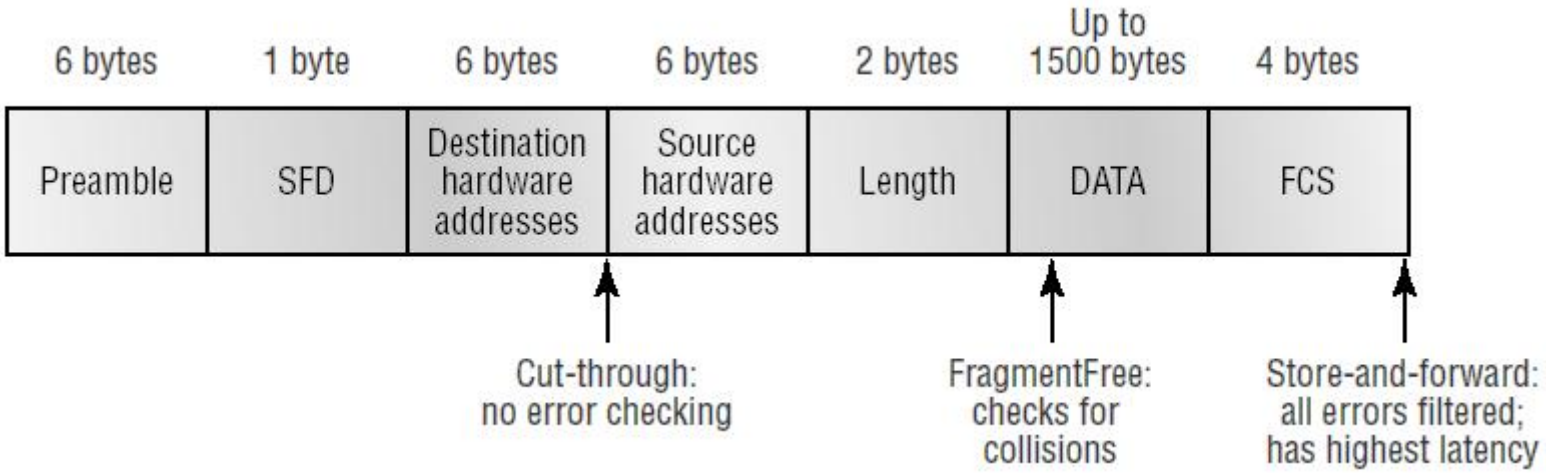
Cat 6/Class E

RJ-45

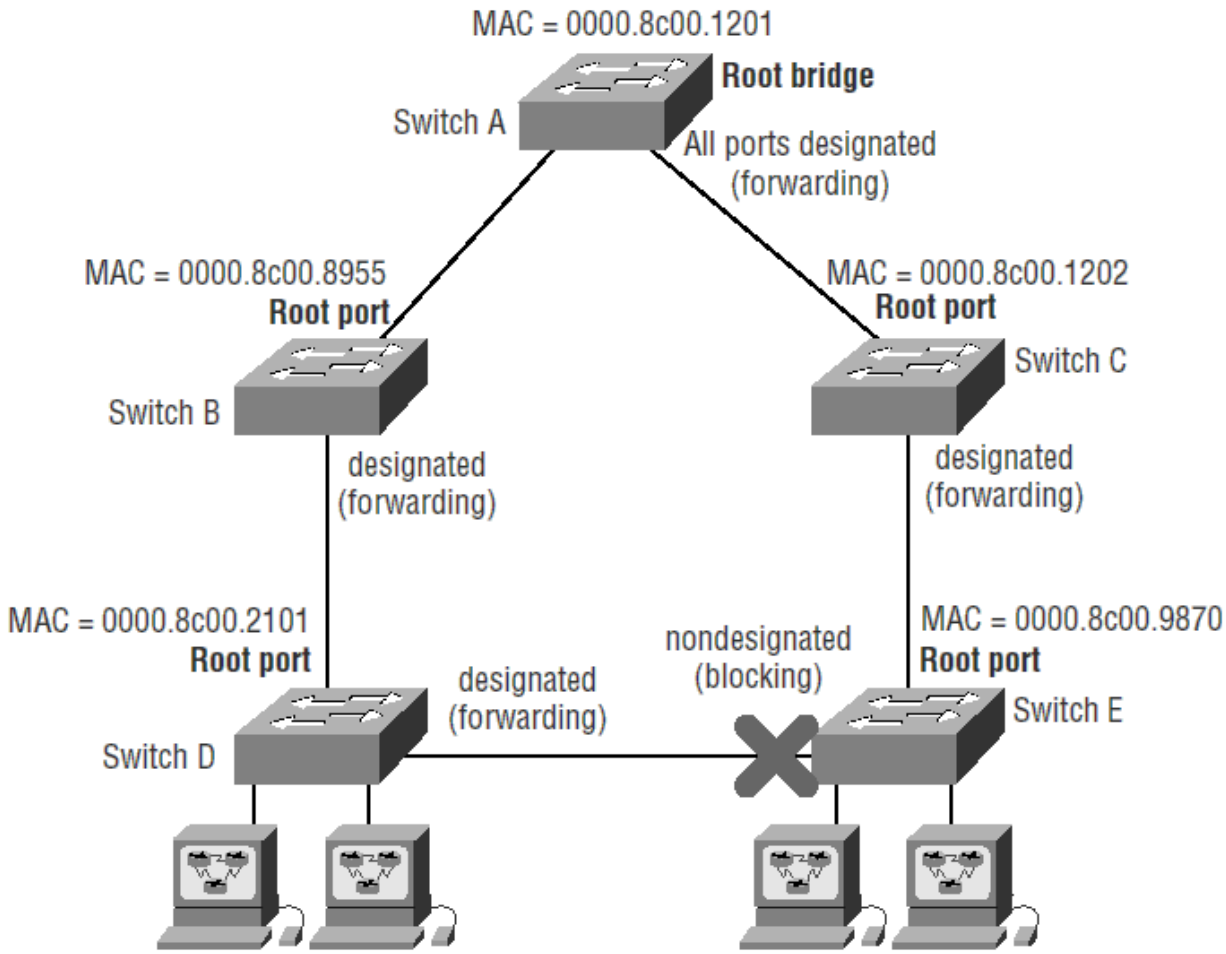
Cat 7 / Class F

RF-45

Типы коммутаторов



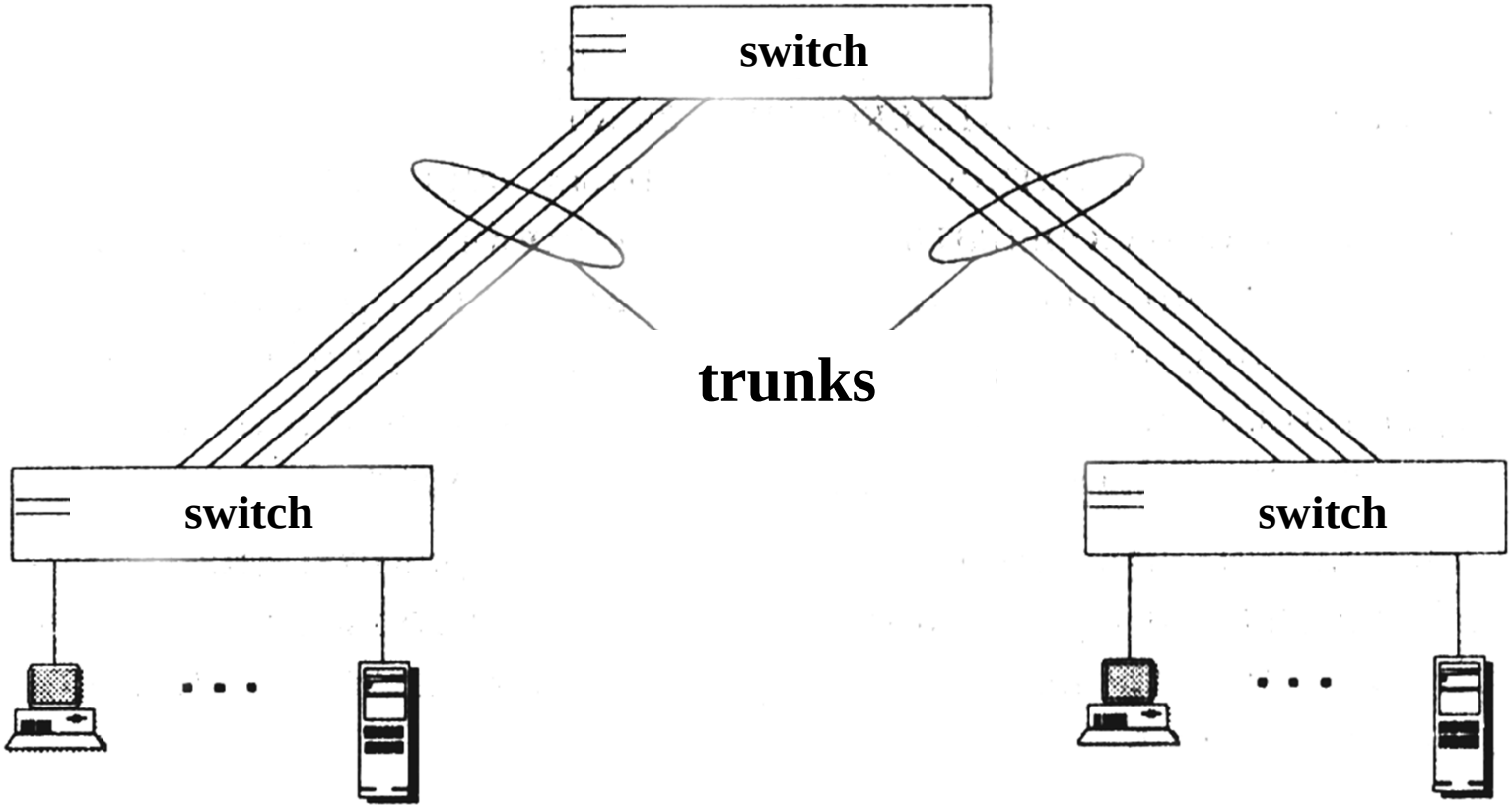
STP, 802.1D


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
designated
(forwarding)
nondesignated
(blocking)
MAC = 0000.8c00.9870
Root port
Switch D
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

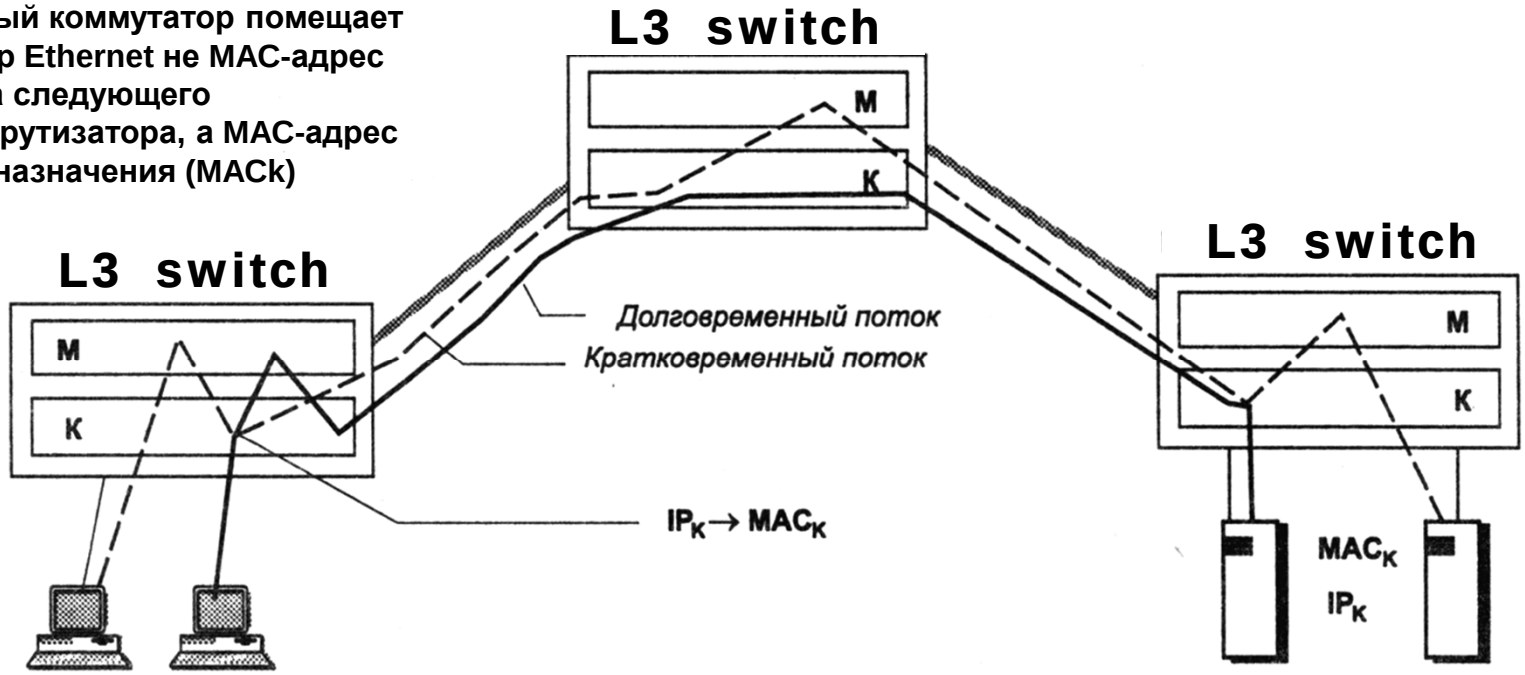
Агрегирование - Link aggregation (trunking)



IEEE 802.3ad, Link Aggregation Control Protocol (LACP)

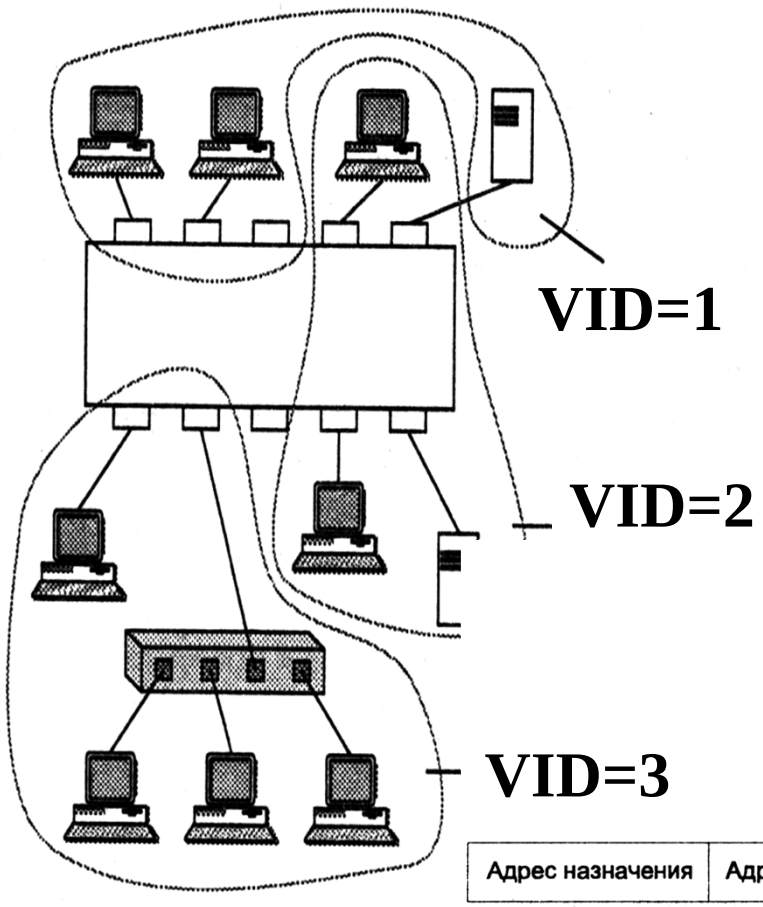
Layer3 коммутаторы

Первый коммутатор помещает в кадр Ethernet не MAC-адрес порта следующего маршрутизатора, а MAC-адрес узла назначения (MACk)



- **L3/4 switching – набор технологий вендоров оборудования**
- **ASICs – специализированные ИС**
- **IP адреса, UDP/TCP порты, TOS хешируются и запоминаются в конфигурациях портов на пути потока пакетов (NetFlow)**

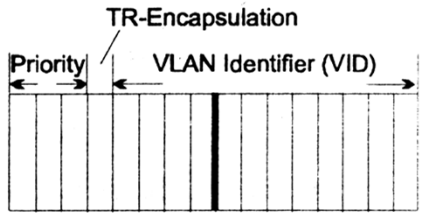
Virtual LANs (VLANs)



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

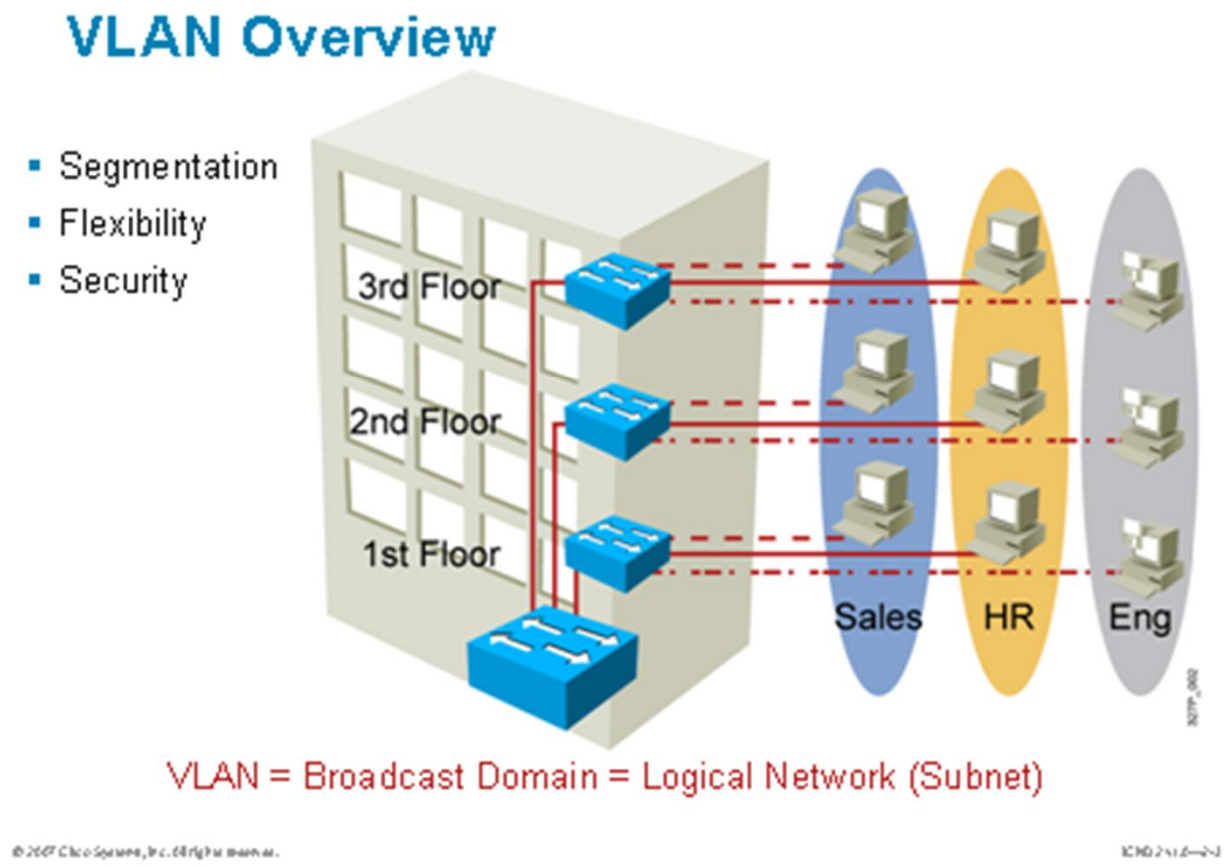
CISCO's proprietary (устарел) – ISL

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	

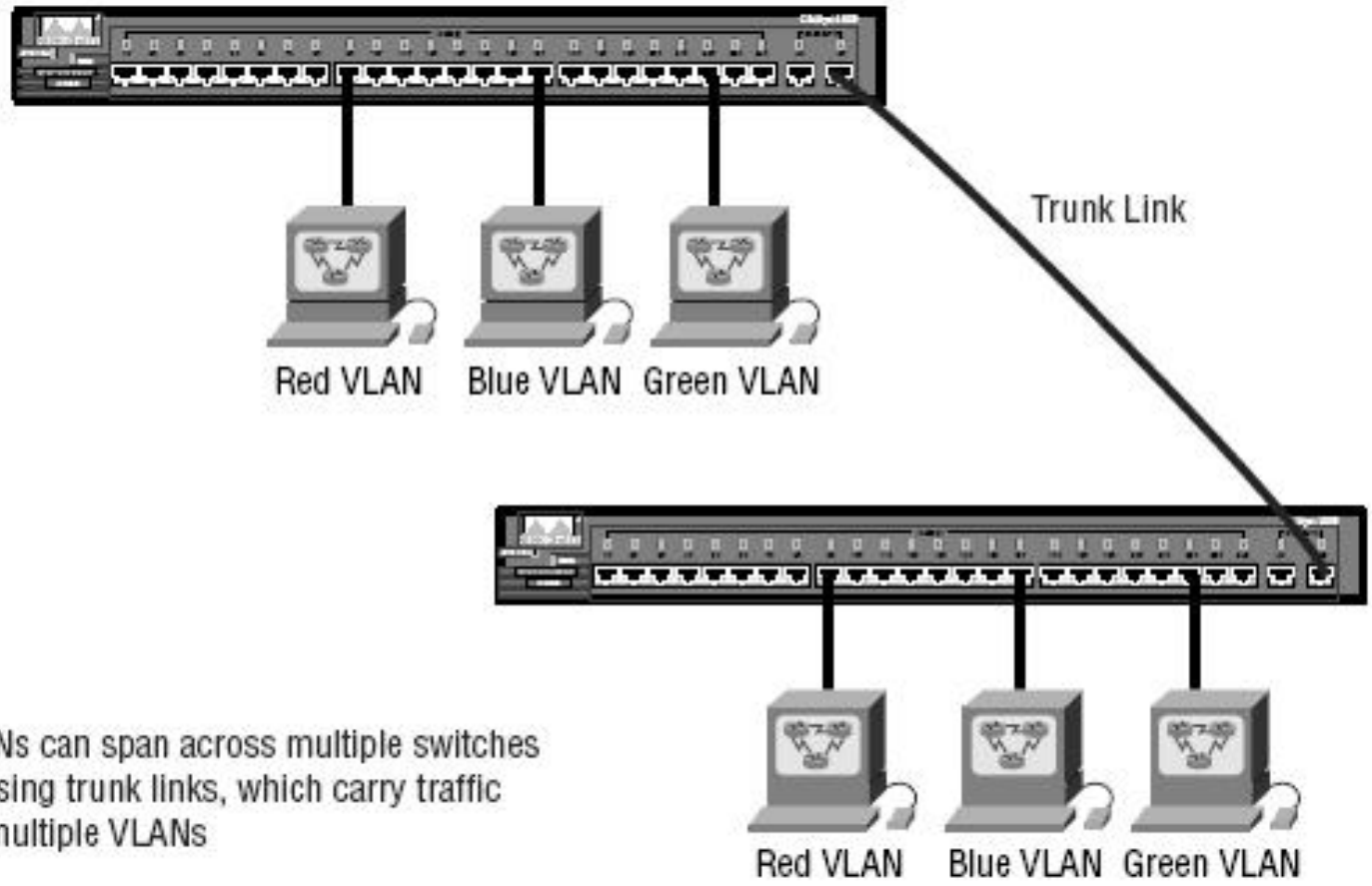
VLAN-ы устраняют физические ограничения



Типы VLAN

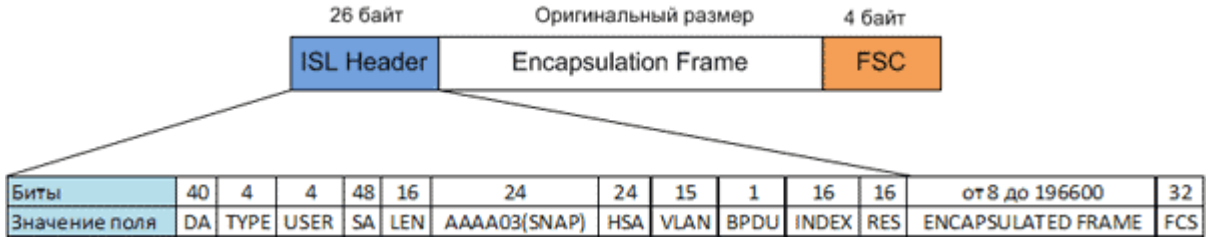
- Статические VLAN
  - Членство в VLAN конфигурируется администратором
- Динамические VLAN
  - Автоматическое определение членства в VLAN, основанное на MAC, протоколах, приложениях.
  - VLAN Management Policy Server (VMPS) у CISCO.

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

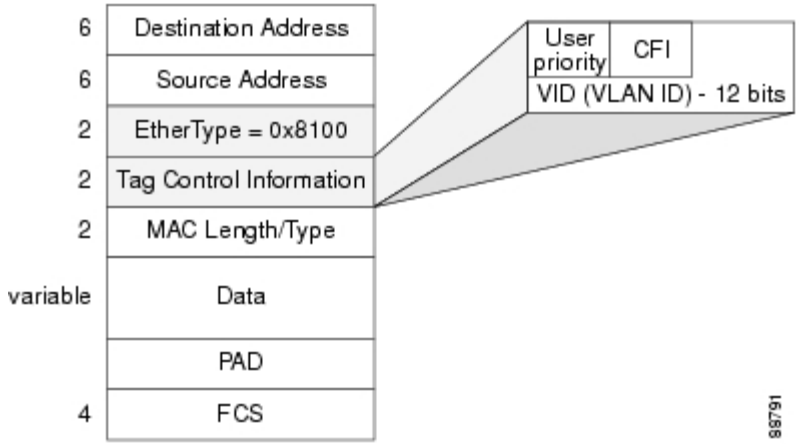


VLANs can span across multiple switches by using trunk links, which carry traffic for multiple VLANs

VLAN методы

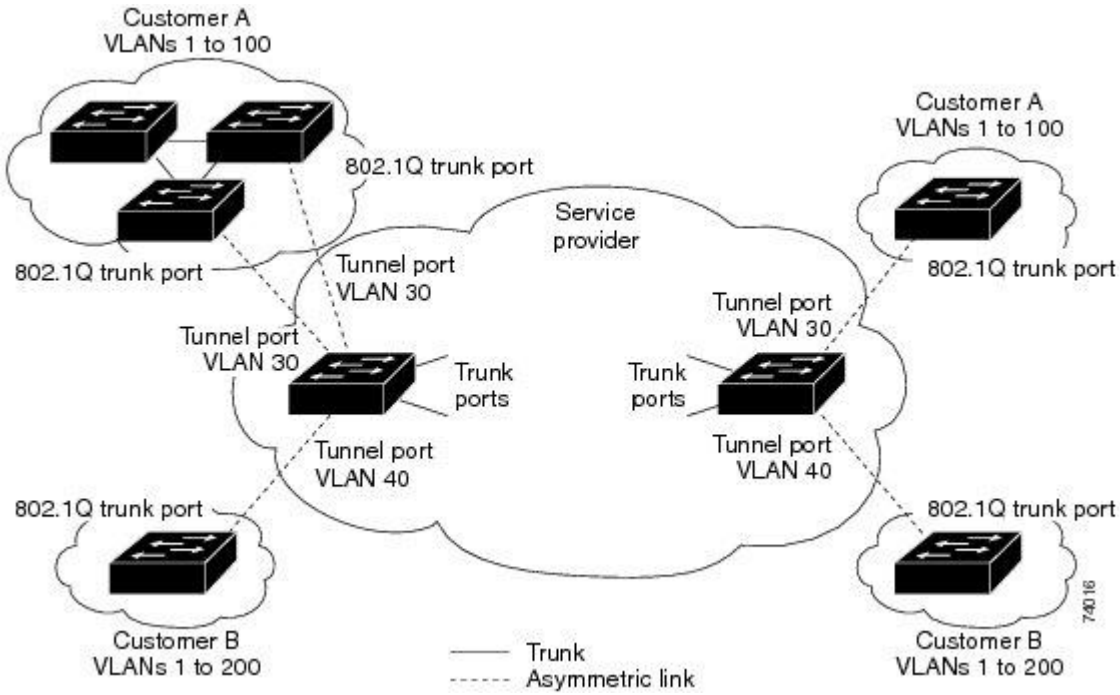


- Inter-Switch Link (ISL)
- IEEE 802.1Q
- VLAN Trunking Protocol (VTP)
  - Режимы: client, server, transparent



VLAN методы, развитие

- IEEE 802.1q
- IEEE 802.1QinQ (два тега)
- IEEE 802.1ad (стек тегов: внешний, внутренний, и набор промежуточных)
- IEEE 802.1aq – управление «Shortest Path Bridging», пока мало реализаций



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

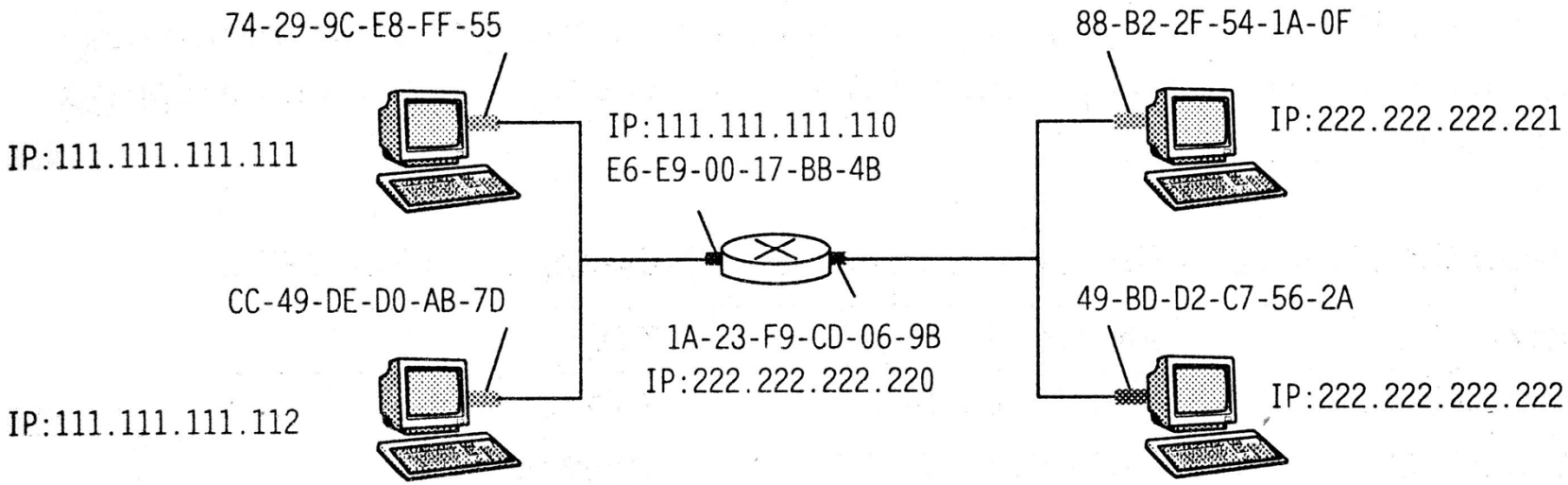
- Switch#config t
- Switch(config)#int f0/12
- Switch(config-if)#switchport mode trunk
- Switch(config-if)#switchport trunk encapsulation ?
  - **dot1q** Interface uses only 802.1q trunking encapsulation when trunking
  - **isl** Interface uses only ISL trunking encapsulation when trunking
  - **negotiate**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

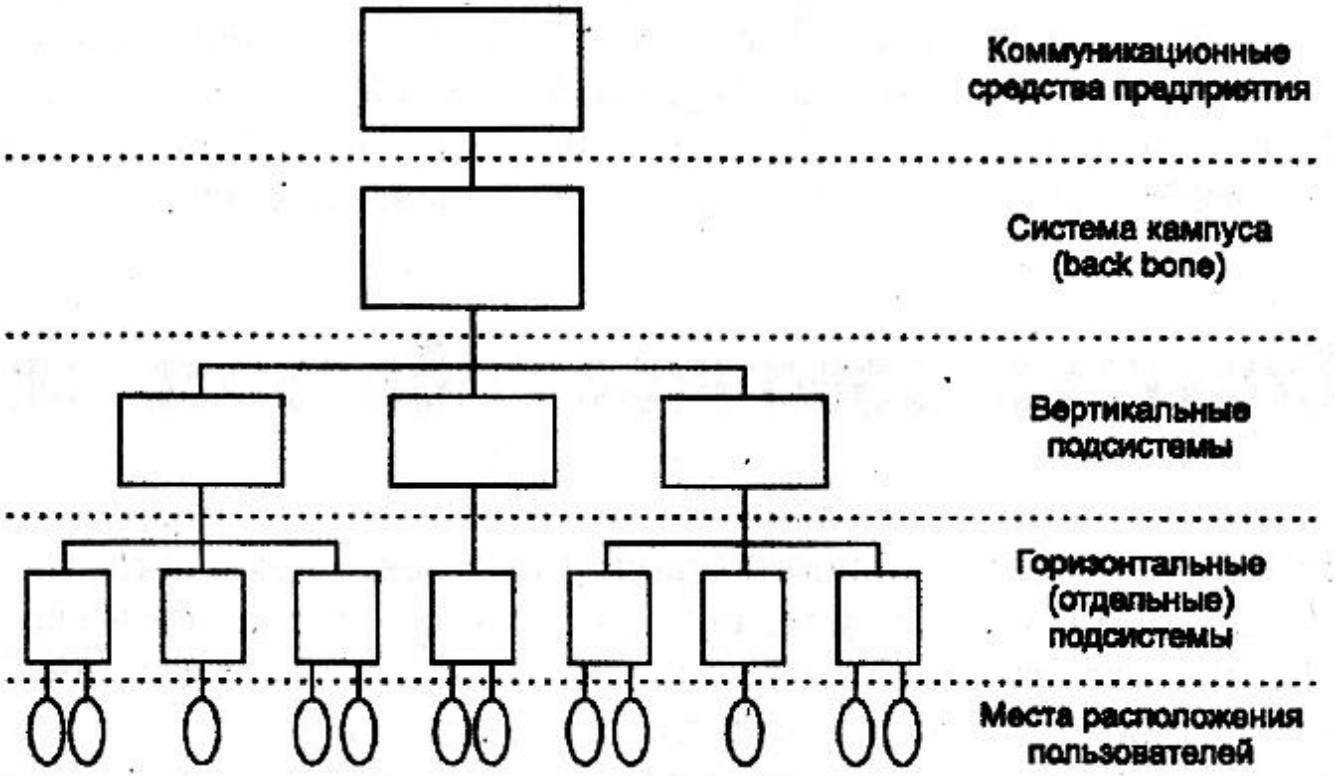
- MAC flooding [fl/\d…]
  - Потребление всей памяти коммутатора под MAC-таблицу для перевода его в failopen mode (hub-подобный)
  - Защита – привязка портов к MAC или ограничение кол-ва MAC на порт
- ARP(MAC)-spoofing, ARP-poisoning
  - ассоциация MAC аттакующего с IP другого узла (шлюза, сервера AAA) -> 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.

Структурированные кабельные системы (СКС)

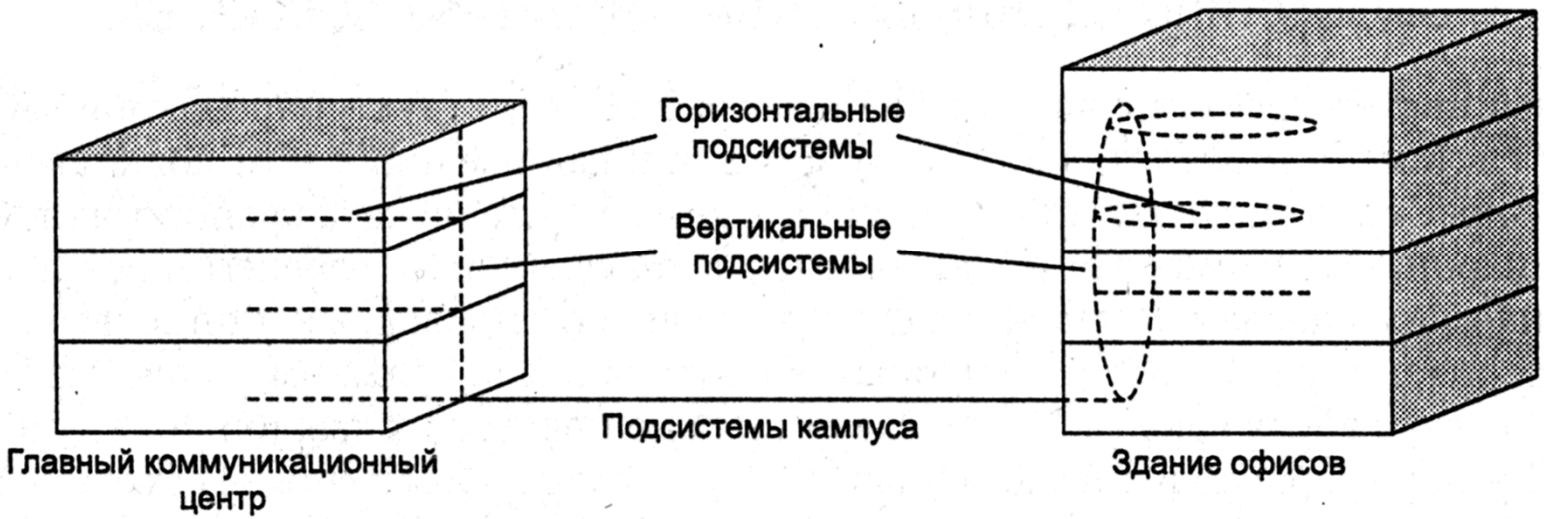
- SCS (Structured Cabling System) – набор соединительных элементов и методика их использования для создания регулярной структуры связей в ИС ISO/IEC 11801 (1995г.) и 15018 (2001г.)

- Преимущества:
  - универсальность
  - срок службы 10-15 лет
  - уменьшение стоимости подключения
  - возможность расширения сети
  - простота обслуживания
  - Надежность (совместимость компонентов)

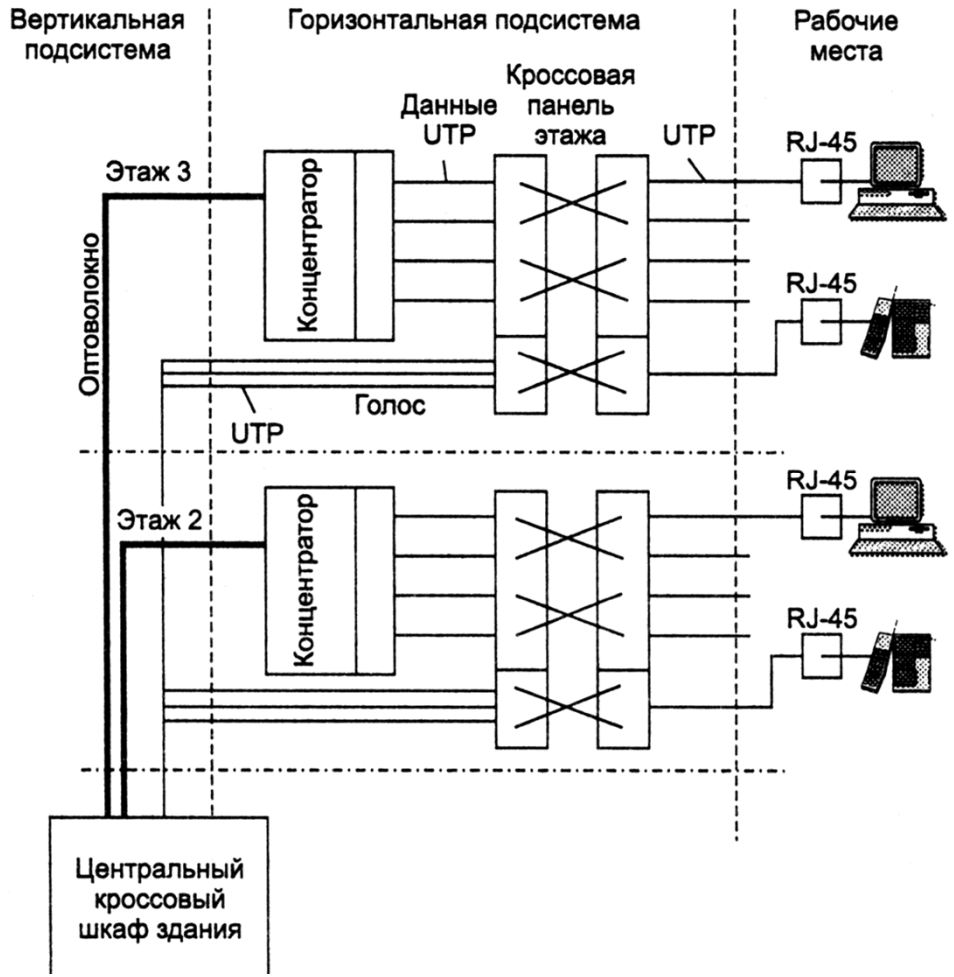
Иерархия СКС



Горизонтали и вертикали СКС

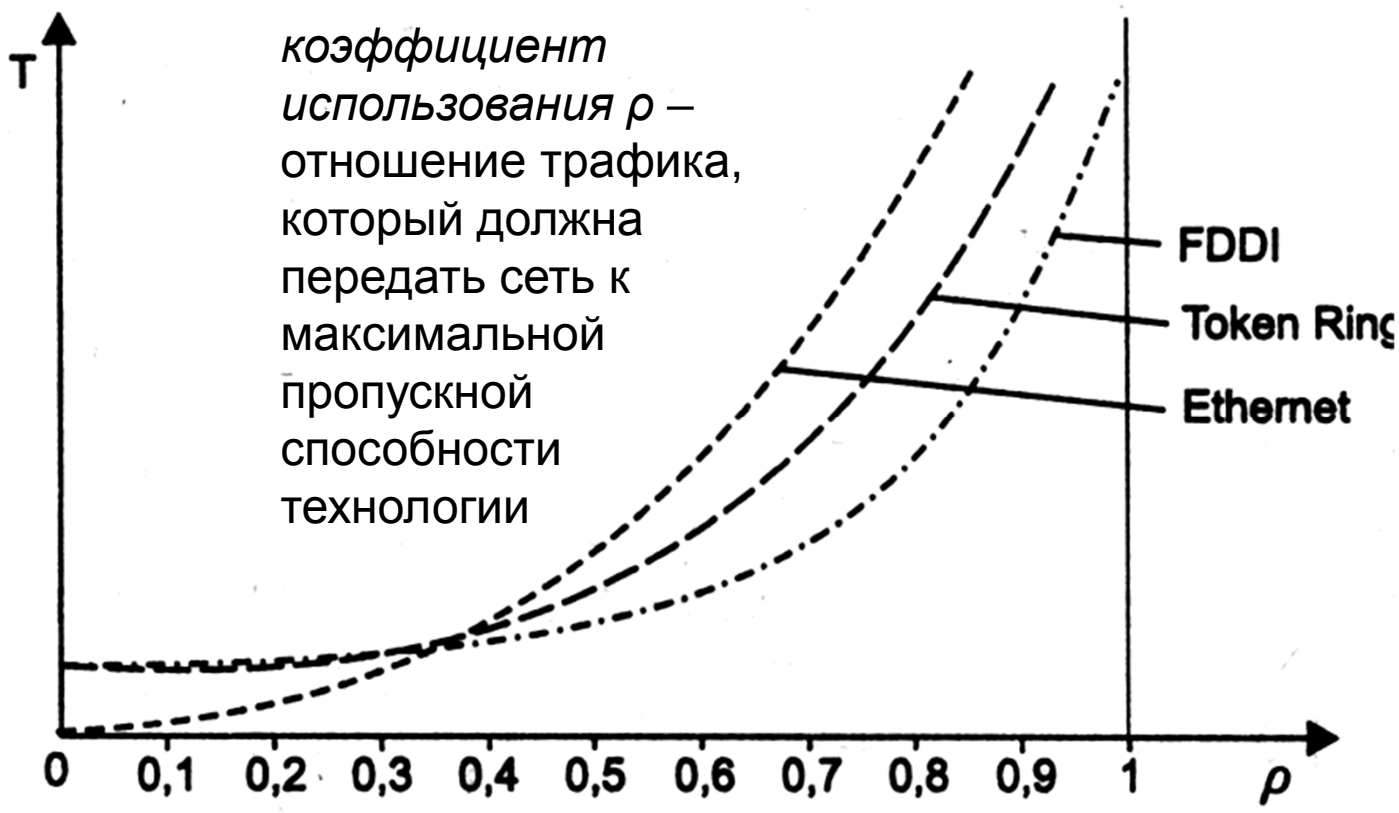


Элементы СКС



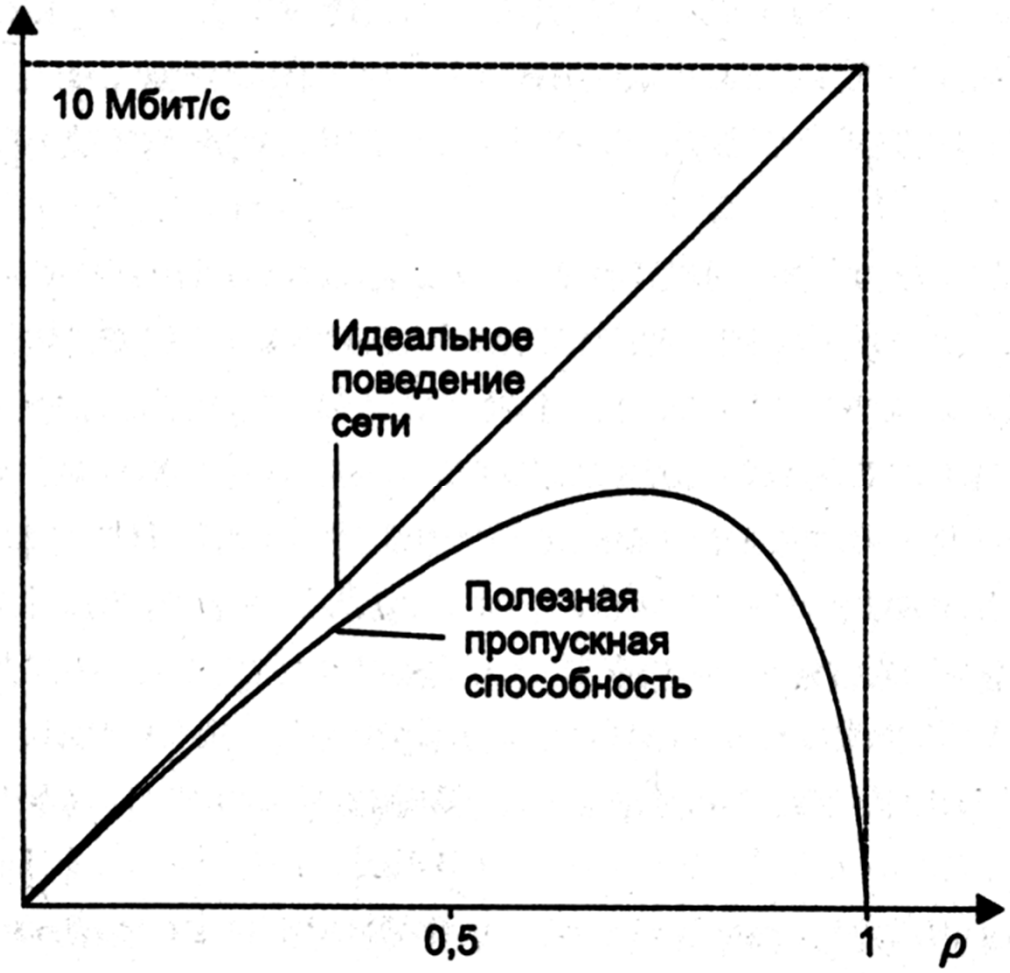
Задержки доступа к среде

коэффициент использования ρ – отношение трафика, который должна передать сеть к максимальной пропускной способности технологии

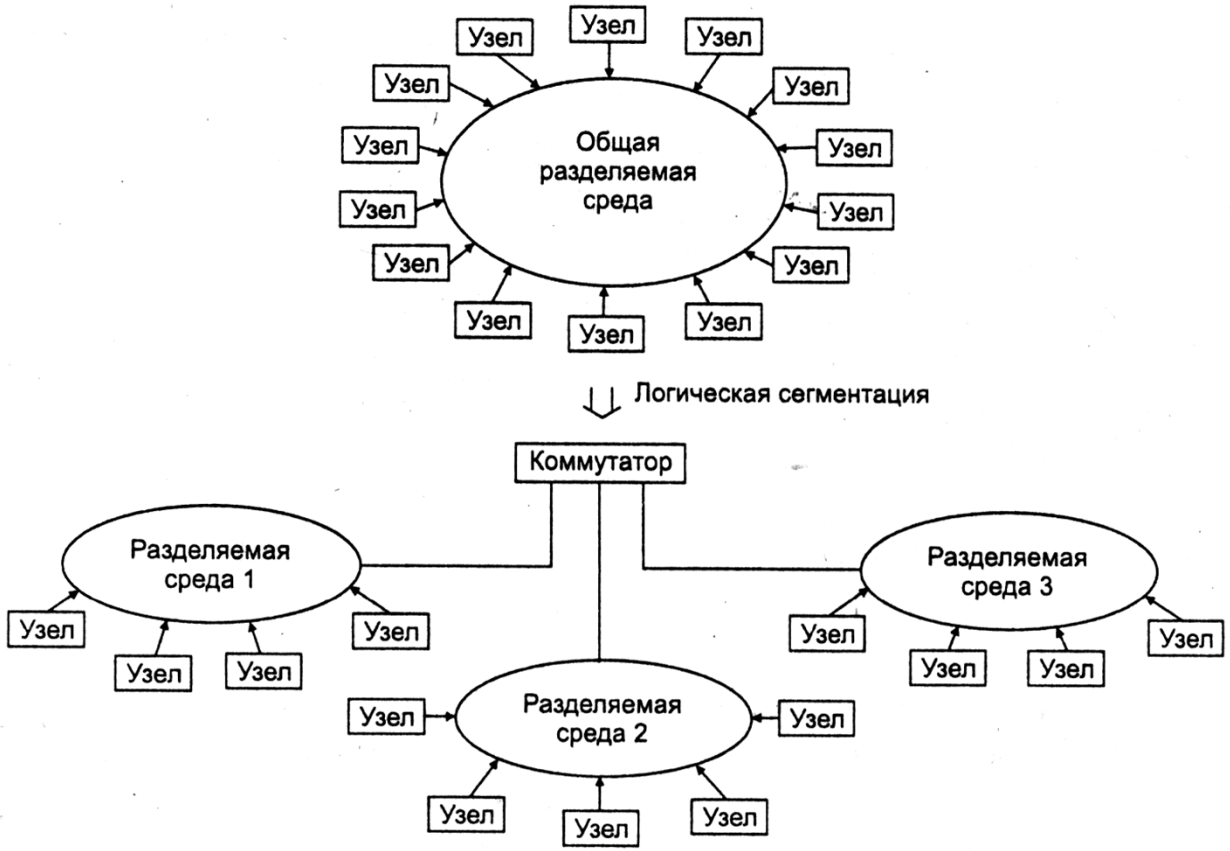


Зависимость пропускной способности сети от коэффициента использования

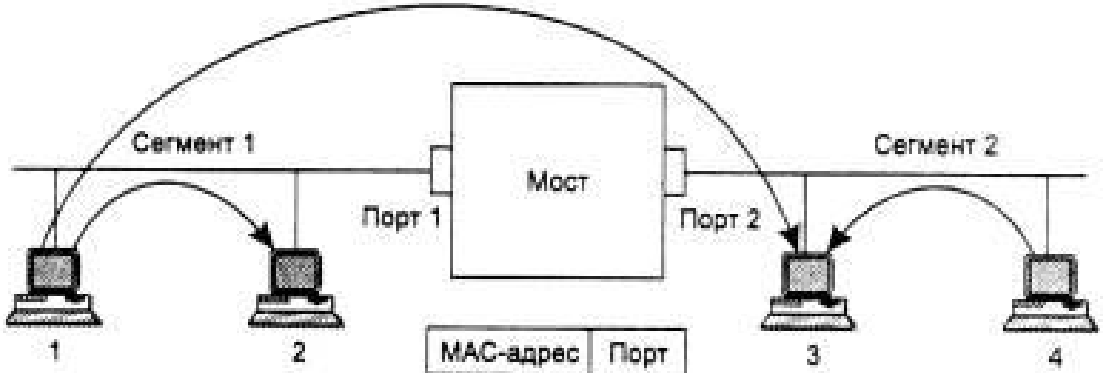
коэффициент использования ρ – отношение трафика, который должна передать сеть к максимальной пропускной способности технологии



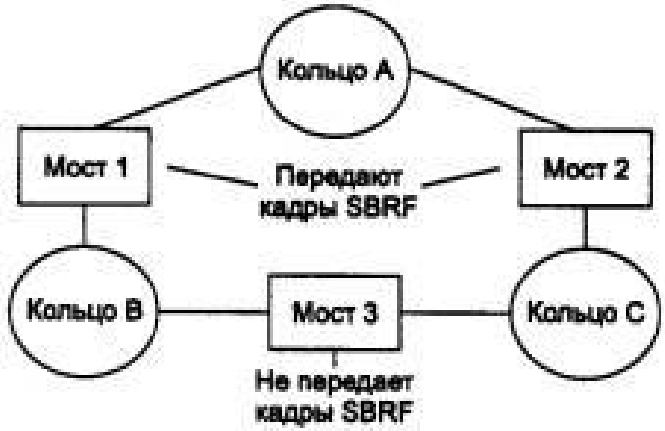
Структуризация сети



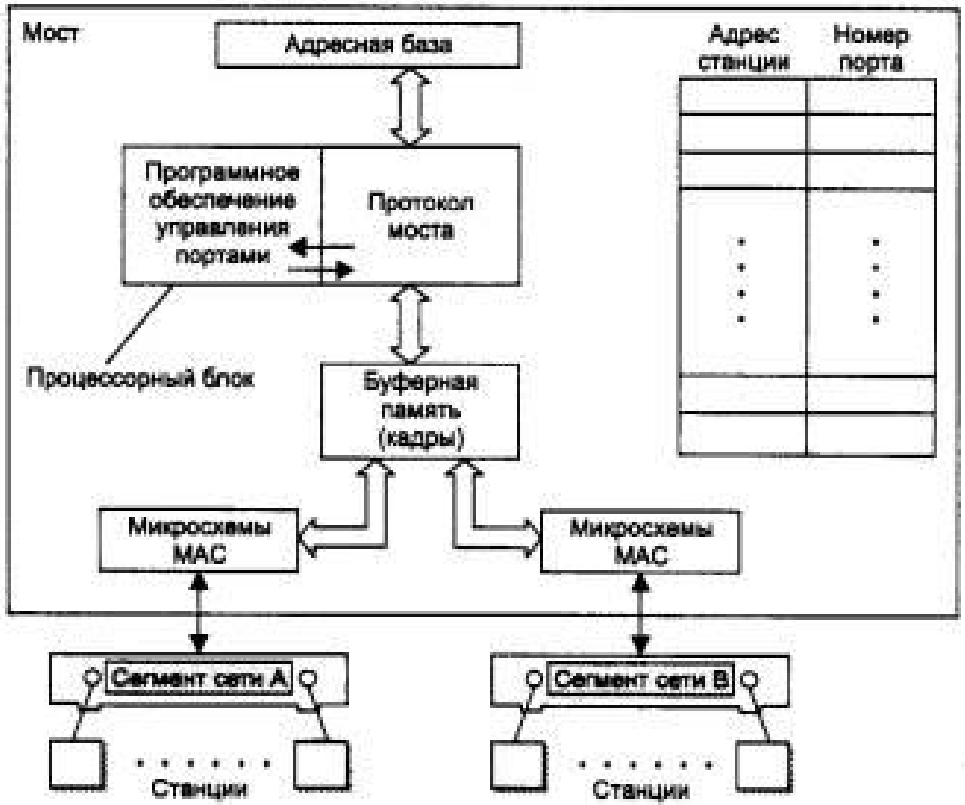
Transparent bridge (IEEE 802. 1D), Source routing



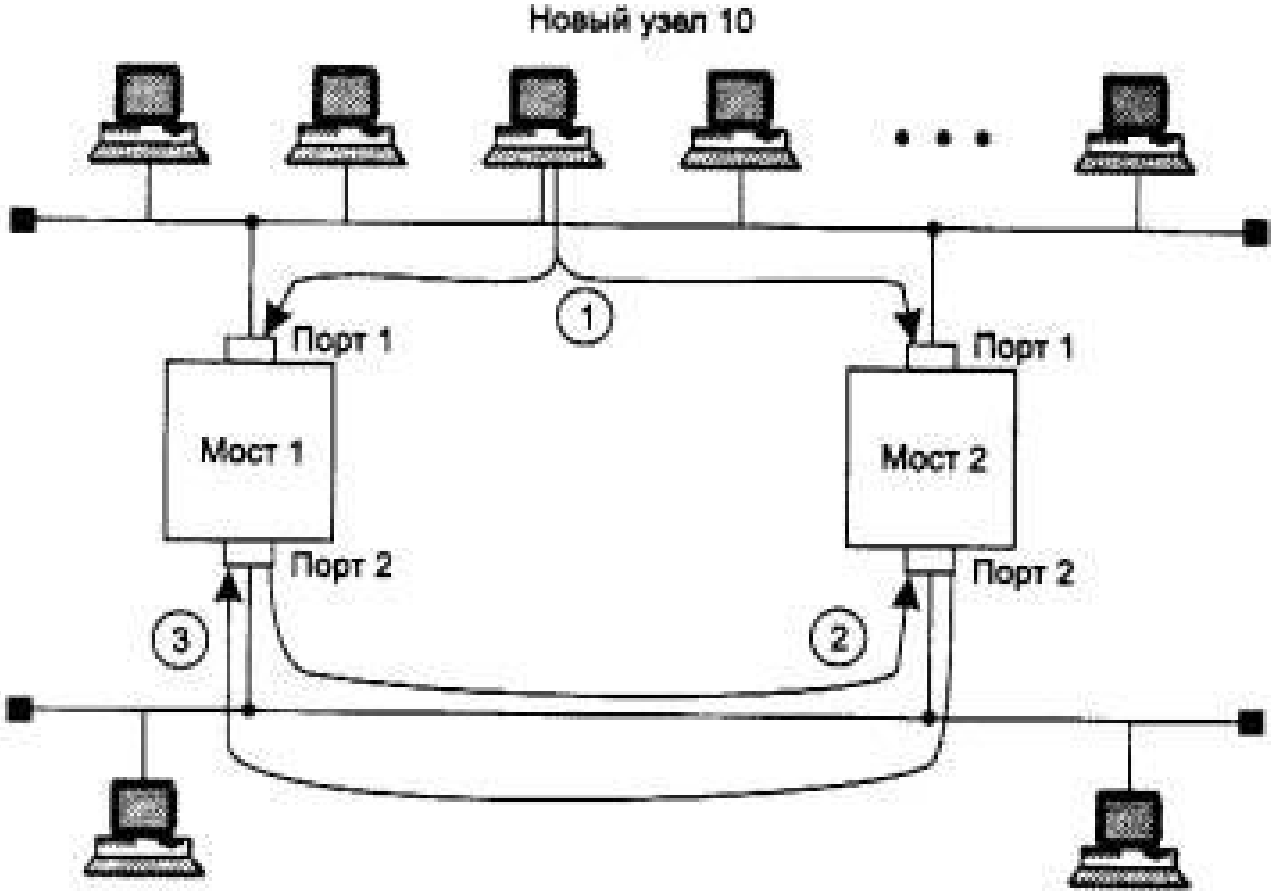
MAC-адрес	Порт
1	1
2	1
3	2
4	2



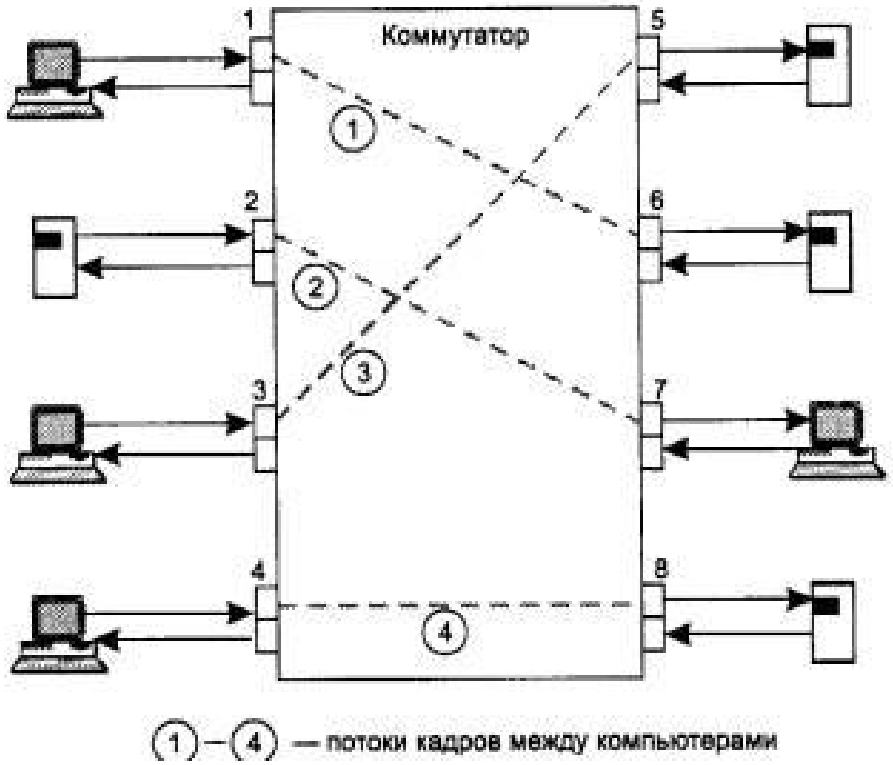
Структура моста



Петли и широковещательный шторм

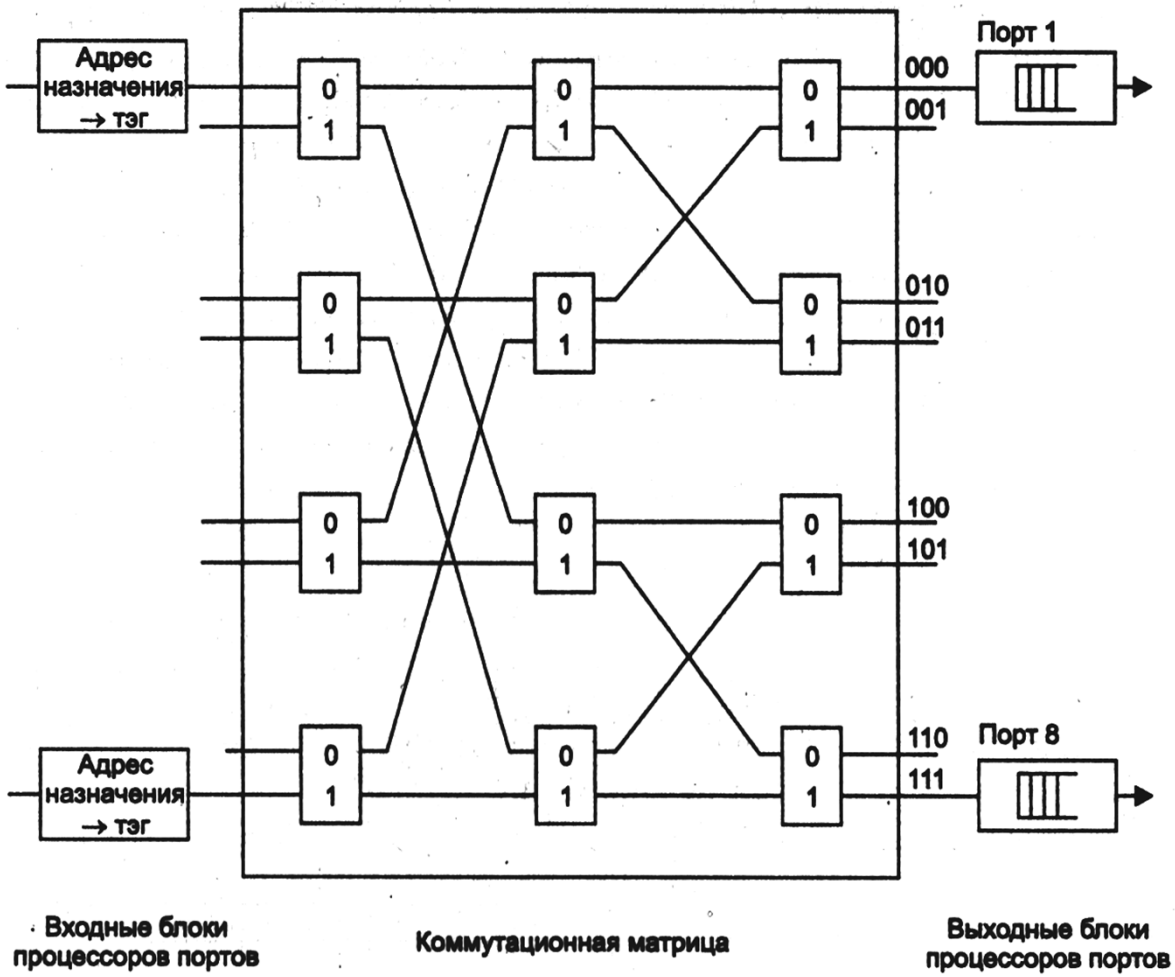


Работы коммутатора

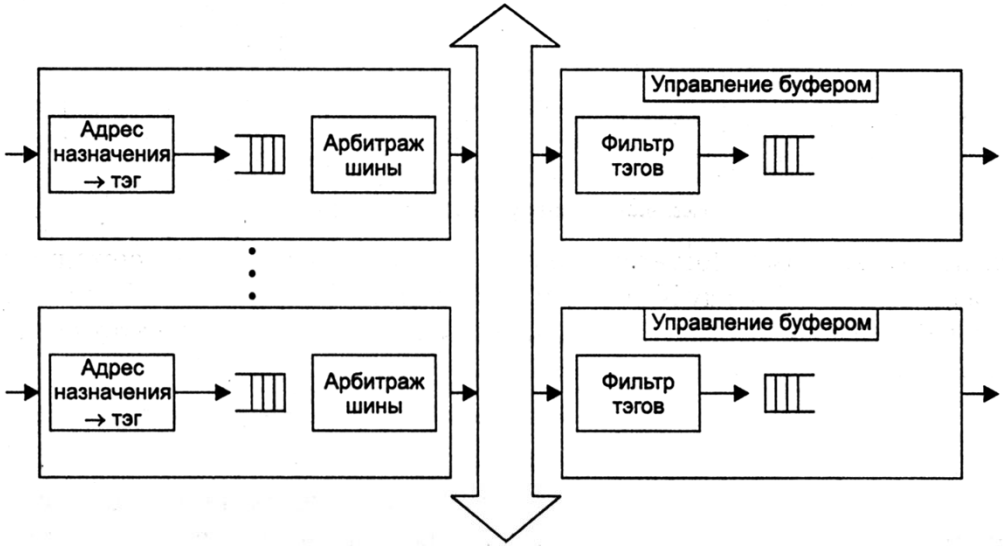


① – ④ — потоки кадров между компьютерами

Коммутаторы с управляемой матрицей соединений

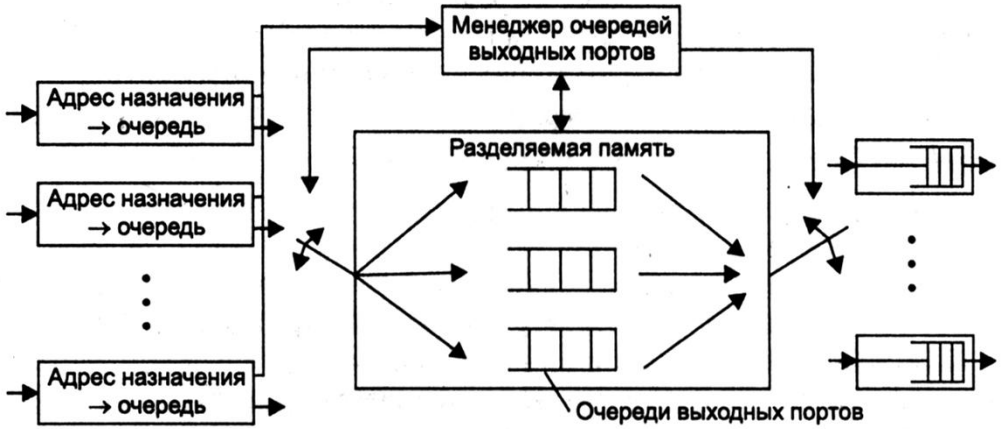


Коммутаторы с разделяемыми шиной и памятью

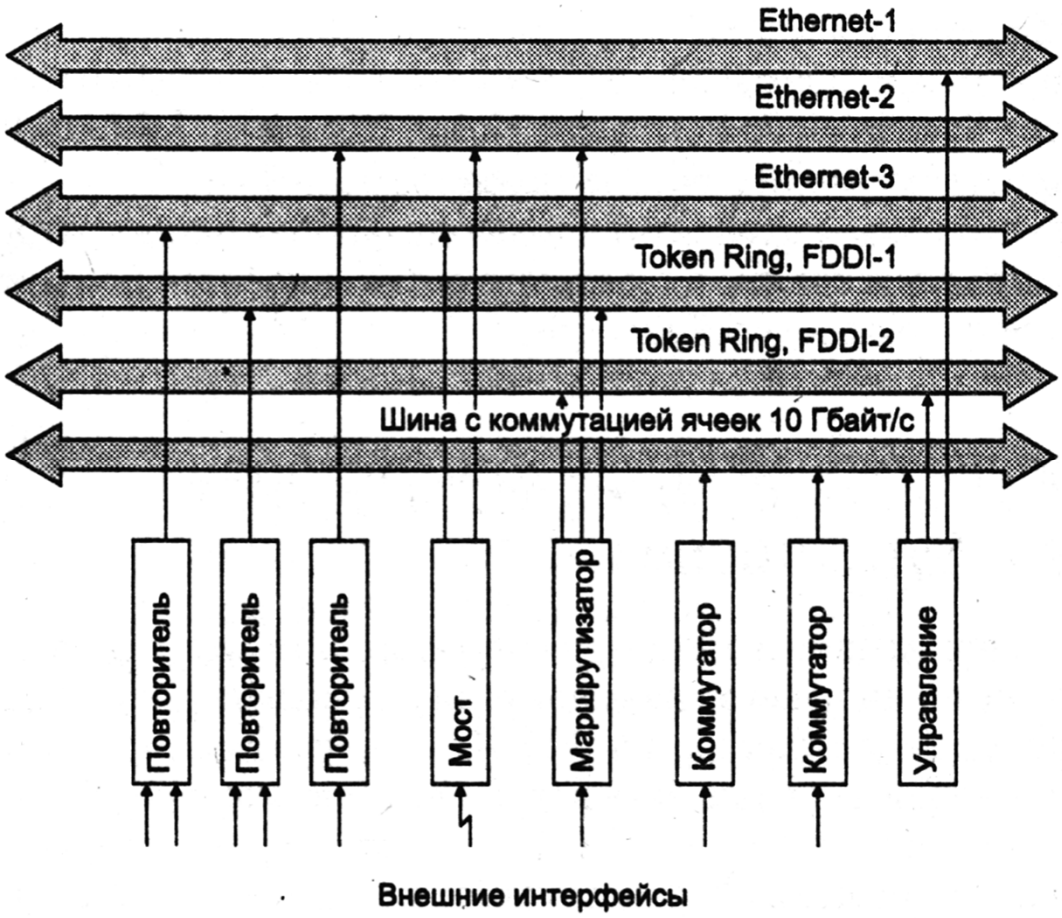


Коммутаторы с матрицей соединений называют cut-through

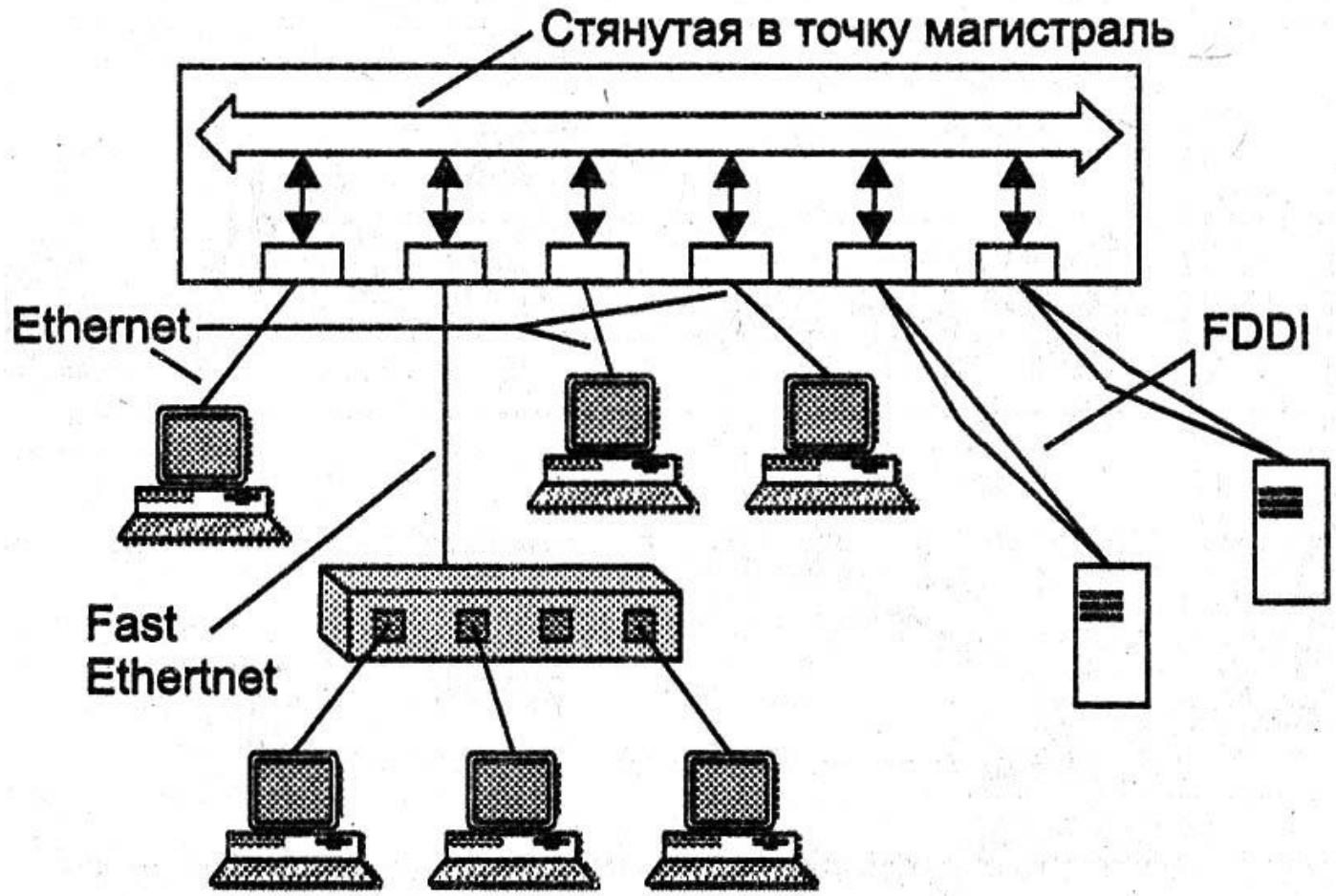
Коммутаторы с промежуточным хранением кадра – store and forward



Коммутаторы корпоративных сетей



Типовая схема применения коммутаторов «магистраль в точке» (collapsed backbone)



Типовая схема применения коммутаторов «распределенная магистраль» (distributed backbone)