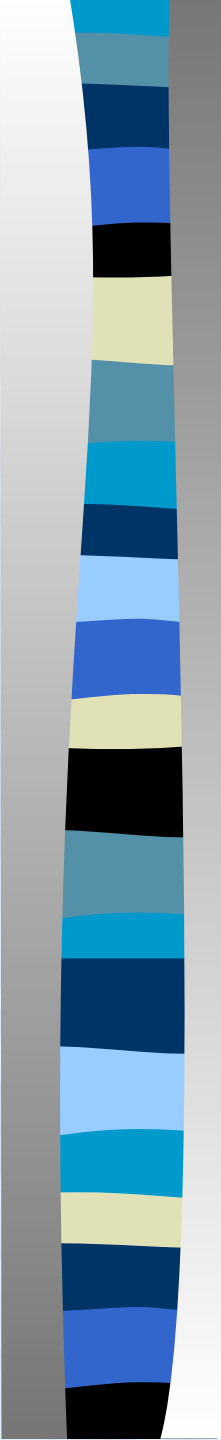


Тема 11. Нижние уровни стека TCP/IP

- Взаимодействие сетей IP с сетями других технологий
- Инкапсуляция IP-пакетов в кадры Ethernet, Token Ring и FDDI
- Протокол последовательного канала SLIP
- Протокол PPP
- Базовый формат кадра PPP
- Протокол LCP
- Аутентификация по протоколам PAP и CHAP
- Протоколы NCP и LQM



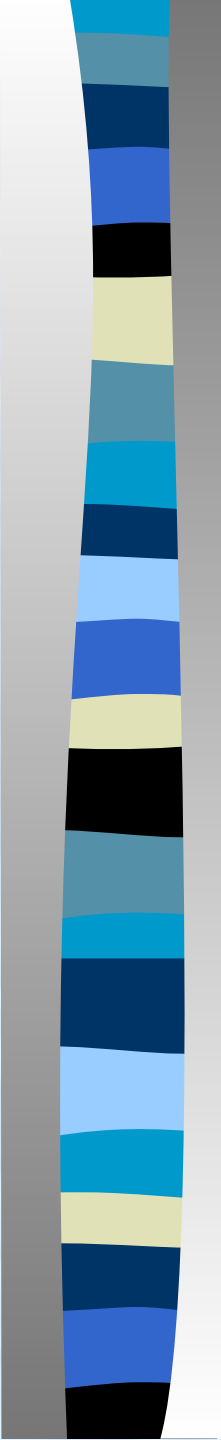
Задачи протокола IP при взаимодействии с протоколами нижних уровней

1. Правила инкапсуляции IP-пакета в кадры
 - В какой тип кадра, если их несколько (Ethernet)
 - Как заполняются служебные поля кадра
2. Правила работы ARP
 - Broadcast - просто
 - Non-Broadcast with Multiple Access – как?
 - Point-to-point – нужен?
3. Работа с логическими подсетями (VLAN, FR, ATM)



Три типа сетей нижнего уровня

1. Широковещательные (broadcast)
Локальные сети: Ethernet, Token Ring, FDDI
2. Точка-точка (Point-to-Point)
PPP, HDLC
3. Нешироковещательные сети с множественным доступом
X.25, frame relay, ATM – сети с предварительным образованием виртуальных каналов

- 
1. Широковещательные (broadcast)
Локальные сети: Ethernet, Token Ring, FDDI

Спецификации инкапсуляции IP-пакетов в кадры Ethernet, Token Ring и FDDI

1. Инкапсуляция пакетов IP в кадры Ethernet

⇒ Ethernet DIX (Ethernet II)

```
ETHERNET: Destination address : 484C00054699
ETHERNET: Source address : 008048EB814C
ETHERNET: Ethernet Type : 0x0800 (IP: DOD Internet Protocol)
IP: ID = 0x654E; Proto = TCP; Len: 40
```

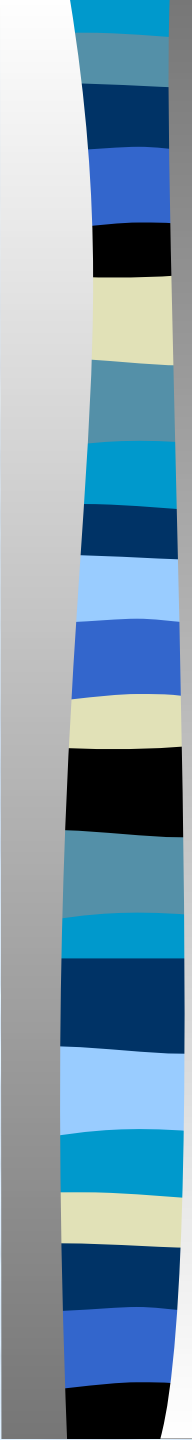
⇒ Ethernet LLC/SNAP

```
ETHERNET: Destination address : 01000CCCCCCC
ETHERNET: Source address : 00E0F77F1920
ETHERNET: Frame Length : 303 (0x012F)
```

```
LLC: DSAP = 0xAA : INDIVIDUAL : Sub-Network Access Protocol (SNAP)
LLC: SSAP = 0xAA: COMMAND : Sub-Network Access Protocol (SNAP)
LLC: Frame Category: Unnumbered Frame
LLC: Command = UI
LLC: LLC Data: Number of data bytes remaining = 286 (0x011E)
SNAP: ETYPE = 0x0800 (IP: DOD Internet Protocol)
IP: ID = 0x654E; Proto = TCP; Len: 40
```

2. Инкапсуляция пакетов IP в кадры Token Ring и FDDI -

формат LLC/SNAP



2. Протоколы точка-точка (Point-to-Point)

PPP, HDLC

Протоколы "точка-точка"

Протокол SLIP (Serial Line IP) -

надежность

очень простая схема кадрирования, невысокая

Протокол HDLC (High-level Data Link Control)

- ♦ Сложный протокол, работающий на основе алгоритмов установления соединения и скользящего окна
- ♦ Он использует 12 различных типов кадров и обеспечивает снижение вероятности искажения бита с 10^{-3} до 10^{-9} .
- ♦ Обеспечивается управление потоком данных за счет механизма окна и специальных кадров, приостанавливающих на время передачу данных от источника
- ♦ Протокол рассчитан на полнодуплексные соединения
- ♦ В семейство HDLC входят протоколы LAP-B, LAP-D, LAP-M, LAP-L, LAP-N, LAP-Q, LAP-R, LAP-S, LAP-T, LAP-U, LAP-V, LAP-W, LAP-X, LAP-Y, LAP-Z, LAP-AA, LAP-AB, LAP-AC, LAP-AD, LAP-AE, LAP-AF, LAP-AG, LAP-AH, LAP-AI, LAP-AJ, LAP-AL, LAP-AM, LAP-AN, LAP-AO, LAP-AP, LAP-AQ, LAP-AR, LAP-AS, LAP-AT, LAP-AU, LAP-AV, LAP-AW, LAP-AX, LAP-AY, LAP-AZ, LAP-BA, LAP-BB, LAP-BC, LAP-BD, LAP-BE, LAP-BF, LAP-BG, LAP-BH, LAP-BI, LAP-BJ, LAP-BL, LAP-BM, LAP-BN, LAP-BO, LAP-BP, LAP-BQ, LAP-BR, LAP-BS, LAP-BT, LAP-BU, LAP-BV, LAP-BW, LAP-BX, LAP-By, LAP-BZ, LAP-CA, LAP-CB, LAP-CC, LAP-CD, LAP-CE, LAP-CF, LAP-CG, LAP-CH, LAP-CI, LAP-CJ, LAP-CL, LAP-CM, LAP-CN, LAP-CP, LAP-CQ, LAP-CR, LAP-CS, LAP-CT, LAP-CU, LAP-CV, LAP-CW, LAP-CX, LAP-Cy, LAP-CZ, LAP-DA, LAP-DB, LAP-DC, LAP-DD, LAP-DE, LAP-DF, LAP-DG, LAP-DH, LAP-DI, LAP-DJ, LAP-DL, LAP-DM, LAP-DN, LAP-DO, LAP-DP, LAP-DQ, LAP-DR, LAP-DS, LAP-DT, LAP-DU, LAP-DV, LAP-DW, LAP-DX, LAP-Dy, LAP-DZ, LAP-EA, LAP-EB, LAP-EC, LAP-ED, LAP-EE, LAP-EF, LAP-EG, LAP-EH, LAP-EI, LAP-EJ, LAP-EL, LAP-EM, LAP-EN, LAP-EO, LAP-EP, LAP-EQ, LAP-ER, LAP-ES, LAP-ET, LAP-EU, LAP-EV, LAP-EW, LAP-EX, LAP-Ey, LAP-EZ, LAP-FA, LAP-FB, LAP-FC, LAP-FD, LAP-FE, LAP-FF, LAP-FG, LAP-FH, LAP-FI, LAP-FJ, LAP-FL, LAP-FM, LAP-FN, LAP-FO, LAP-FP, LAP-FQ, LAP-FR, LAP-FS, LAP-FT, LAP-FU, LAP-FV, LAP-FW, LAP-FX, LAP-Fy, LAP-FZ, LAP-GA, LAP-GB, LAP-GC, LAP-GD, LAP-GE, LAP-GF, LAP-GG, LAP-GH, LAP-GI, LAP-GJ, LAP-GL, LAP-GM, LAP-GN, LAP-GO, LAP-GP, LAP-GQ, LAP-GR, LAP-GS, LAP-GT, LAP-GU, LAP-GV, LAP-GW, LAP-GX, LAP-Gy, LAP-GZ, LAP-HA, LAP-HB, LAP-HC, LAP-HD, LAP-HE, LAP-HF, LAP-HG, LAP-HH, LAP-HI, LAP-HJ, LAP-HL, LAP-HM, LAP-HN, LAP-HO, LAP-HP, LAP-HQ, LAP-HR, LAP-HS, LAP-HT, LAP-HU, LAP-HV, LAP-HW, LAP-HX, LAP-Hy, LAP-HZ, LAP-IA, LAP-IB, LAP-IC, LAP-ID, LAP-IE, LAP-IF, LAP-IG, LAP-IH, LAP-II, LAP-IJ, LAP-IL, LAP-IM, LAP-IN, LAP-IO, LAP-IP, LAP-IQ, LAP-IR, LAP-IS, LAP-IT, LAP-IU, LAP-IV, LAP-IW, LAP-IX, LAP-Iy, LAP-IZ, LAP-JA, LAP-JB, LAP-JC, LAP-JD, LAP-JE, LAP-JF, LAP-JG, LAP-JH, LAP-JI, LAP-JJ, LAP-JL, LAP-JM, LAP-JN, LAP-JO, LAP-JP, LAP-JQ, LAP-JR, LAP-JS, LAP-JT, LAP-JU, LAP-JV, LAP-JW, LAP-JX, LAP-Jy, LAP-JZ, LAP-KA, LAP-KB, LAP-KC, LAP-KD, LAP-KE, LAP-KF, LAP-KG, LAP-KH, LAP-KI, LAP-KJ, LAP-KL, LAP-KM, LAP-KN, LAP-KO, LAP-KP, LAP-KQ, LAP-KR, LAP-KS, LAP-KT, LAP-KU, LAP-KV, LAP-KW, LAP-KX, LAP-Ky, LAP-KZ, LAP-LA, LAP-LB, LAP-LC, LAP-LD, LAP-LE, LAP-LF, LAP-LG, LAP-LH, LAP-LI, LAP-LJ, LAP-LK, LAP-LM, LAP-LN, LAP-LO, LAP-LP, LAP-LQ, LAP-LR, LAP-LS, LAP-LT, LAP-LU, LAP-LV, LAP-LW, LAP-LX, LAP-Ly, LAP-LZ, LAP-MA, LAP-MB, LAP-MC, LAP-MD, LAP-ME, LAP-MF, LAP-MG, LAP-MH, LAP-MI, LAP-MJ, LAP-MK, LAP-ML, LAP-MN, LAP-MO, LAP-MP, LAP-MQ, LAP-MR, LAP-MS, LAP-MT, LAP-MU, LAP-MV, LAP-MW, LAP-MX, LAP-My, LAP-MZ, LAP-NA, LAP-NB, LAP-NC, LAP-ND, LAP-NE, LAP-NF, LAP-NG, LAP-NH, LAP-NI, LAP-NJ, LAP-NK, LAP-NL, LAP-NM, LAP-NO, LAP-NP, LAP-NQ, LAP-NR, LAP-NS, LAP-NT, LAP-NU, LAP-NV, LAP-NW, LAP-NX, LAP-Ny, LAP-NZ, LAP-OA, LAP-OB, LAP-OC, LAP-OD, LAP-OE, LAP-OF, LAP-OG, LAP-OH, LAP-OI, LAP-OJ, LAP-OK, LAP-OL, LAP-OM, LAP-ON, LAP-OO, LAP-OP, LAP-OQ, LAP-OR, LAP-OS, LAP-OT, LAP-OU, LAP-OV, LAP-OW, LAP-OX, LAP-Oy, LAP-OZ, LAP-PA, LAP-PB, LAP-PC, LAP-PD, LAP-PE, LAP-PF, LAP-PG, LAP-PH, LAP-PI, LAP-PJ, LAP-PK, LAP-PL, LAP-PM, LAP-PN, LAP-PO, LAP-PP, LAP-PQ, LAP-PR, LAP-PS, LAP-PT, LAP-PU, LAP-PV, LAP-PW, LAP-PX, LAP-Py, LAP-PZ, LAP-QA, LAP-QB, LAP-QC, LAP-QD, LAP-QE, LAP-QF, LAP-QG, LAP-QH, LAP-QI, LAP-QJ, LAP-QK, LAP-QL, LAP-QM, LAP-QN, LAP-QO, LAP-QP, LAP-QL, LAP-QM, LAP-QN, LAP-QO, LAP-QP, LAP-QQ, LAP-QR, LAP-QS, LAP-QT, LAP-QU, LAP-QV, LAP-QW, LAP-QX, LAP-Qy, LAP-QZ, LAP-RA, LAP-RB, LAP-RC, LAP-RD, LAP-RE, LAP-RF, LAP-RG, LAP-RH, LAP-RI, LAP-RJ, LAP-RK, LAP-RL, LAP-RM, LAP-RN, LAP-RO, LAP-RR, LAP-RS, LAP-RT, LAP-RU, LAP-RV, LAP-RW, LAP-RX, LAP-Ry, LAP-RZ, LAP-SA, LAP-SB, LAP-SC, LAP-SD, LAP-SE, LAP-SF, LAP-SG, LAP-SH, LAP-SI, LAP-SJ, LAP-SK, LAP-SL, LAP-SM, LAP-SN, LAP-SO, LAP-SS, LAP-ST, LAP-SU, LAP-SV, LAP-SW, LAP-SX, LAP-Sy, LAP-SZ, LAP-TA, LAP-TB, LAP-TC, LAP-TD, LAP-TE, LAP-TF, LAP-TG, LAP-TH, LAP-TI, LAP-TJ, LAP-TK, LAP-TL, LAP-TM, LAP-TN, LAP-TO, LAP-TT, LAP-TU, LAP-TV, LAP-TW, LAP-TX, LAP-Ty, LAP-TZ, LAP-UA, LAP-UB, LAP-UC, LAP-UD, LAP-UE, LAP-UF, LAP-UG, LAP-UH, LAP-UI, LAP-UJ, LAP-UK, LAP-UL, LAP-UM, LAP-UN, LAP-UO, LAP-UR, LAP-US, LAP-UT, LAP-UU, LAP-UV, LAP-UW, LAP-UX, LAP-Uy, LAP-UZ, LAP-VA, LAP-VB, LAP-VC, LAP-VD, LAP-VE, LAP-VF, LAP-VG, LAP-VH, LAP-VI, LAP-VJ, LAP-VK, LAP-VL, LAP-VM, LAP-VN, LAP-VO, LAP-VR, LAP-VS, LAP-VT, LAP-VU, LAP-VV, LAP-VW, LAP-VX, LAP-Vy, LAP-VZ, LAP-WA, LAP-WB, LAP-WC, LAP-WD, LAP-WE, LAP-WF, LAP-WG, LAP-WH, LAP-WI, LAP-WJ, LAP-WK, LAP-WL, LAP-WM, LAP-WN, LAP-WO, LAP-WR, LAP-WS, LAP-WT, LAP-WU, LAP-WV, LAP-WW, LAP-WX, LAP-Wy, LAP-WZ, LAP-XA, LAP-XB, LAP-XC, LAP-XD, LAP-XE, LAP-XF, LAP-XG, LAP-XH, LAP-XI, LAP-XJ, LAP-XK, LAP-XL, LAP-XM, LAP-XN, LAP-XO, LAP-XR, LAP-XS, LAP-XT, LAP-XU, LAP-XV, LAP-XW, LAP-XX, LAP-Xy, LAP-XZ, LAP-YA, LAP-YB, LAP-YC, LAP-YD, LAP-YE, LAP-YF, LAP-YG, LAP-YH, LAP-YI, LAP-YJ, LAP-YK, LAP-YL, LAP-YM, LAP-YN, LAP-YO, LAP-YR, LAP-YS, LAP-YT, LAP-YU, LAP-YV, LAP-YW, LAP-YX, LAP-Yy, LAP-YZ, LAP-ZA, LAP-ZB, LAP-ZC, LAP-ZD, LAP-ZE, LAP-ZF, LAP-ZG, LAP-ZH, LAP-ZI, LAP-ZJ, LAP-ZK, LAP-ZL, LAP-ZM, LAP-ZN, LAP-ZO, LAP-ZR, LAP-ZS, LAP-ZT, LAP-ZU, LAP-ZV, LAP-ZW, LAP-ZX, LAP-Zy, LAP-ZZ

Протокол PPP (Point-to-Point Protocol) -

Internet Engineering

Task Force

старейшего протокола PPP

разработан группой

- ♦ Протокол PPP взамен у выделенных каналов в цифровой сети стал фактическим стандартом для глобальных линий связи на
- ♦ Протокол PPP первоначально использовал формат кадров HDLC собственными полями - поля протокола PPP и дополнил их HDLC вложены в поле данных кадра

Протокол LAP-B:

Структура кадра LAP-B

Флаг	Управление на уровне канала	Данные (X.25) кадр	Циклический код (CRC)	Флаг
------	-----------------------------	--------------------	-----------------------	------

01111110

Адрес	Управление
-------	------------

1 2 3 4 5 6 7 8

ООД : 11000000

Комм.: 10000000

0	N(S)	P/F	N(R)	Информационный кадр
10	S	P/F	N(R)	Супервизорный кадр
11	M	P/F	M	Ненумерованный кадр

N(S). N(R) -

Типы кадров LAR-V

(1) *Информационный* -
данные X.25
Супервизорные

(2) **Готовность к приему**

(3) **Неготовность к приему**

(4) **Отказ**

(5) **Селективный отказ**

Ненумерованные

(6) **Установить режим нормальных ответов**

(7) **Установить режим асинхронных ответов**

(8) **Разъединить**

(9) **Запрос передачи**

(10) **Сброс**

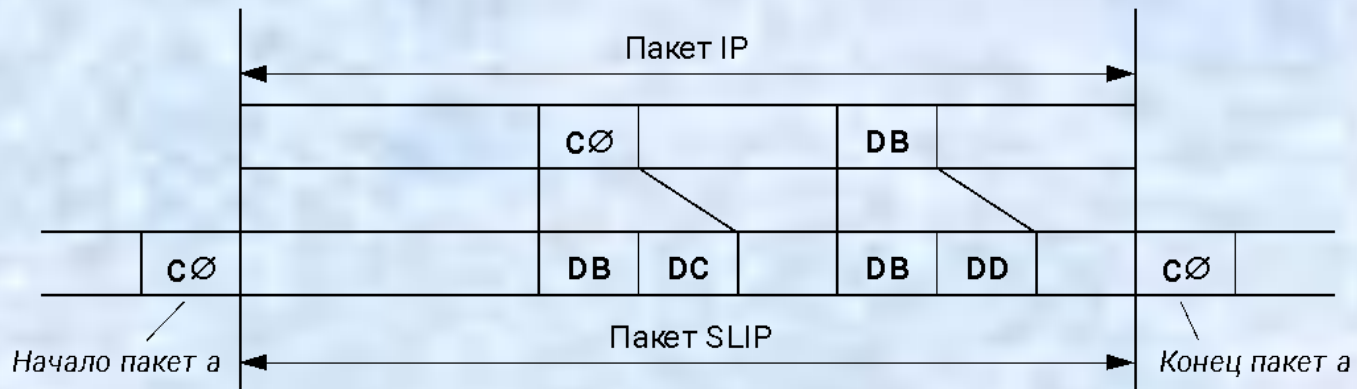
(11) **Отказ от кадра**

(12) **Подтверждение**



Протокол последовательного канала SLIP

- ♦ SLIP (Serial Line IP) - позволяет устройствам, соединенным последовательной линией связи, работать по протоколам TCP/IP
- ♦ В 1984 г. был встроен в операционную систему 4.2 Berkley Unix
- ♦ Дает возможность подключаться к сети Internet стандартного порта RS232 посредством
- ♦ Выполняет работу по выделению из последовательности передаваемых по последовательному каналу бит границ пакета IP
- ♦ Большинство реализаций протокола SLIP поддерживают спецификацию Compressed SLIP (CSLIP)



Ограничения протокола SLIP

- ◆ размер инкапсулируемого пакета IP не должен превышать 1006 байтов
- ◆ нет механизмов, дающих возможность обмениваться адресной информацией. Это ограничение не позволяет использовать SLIP для некоторых видов сетевого сервиса
- ◆ можно передавать трафик лишь одного сетевого протокола
- ◆ не предусмотрены процедуры обнаружения и коррекции ошибок



Протокол PPP (Point-to-Point Protocol)

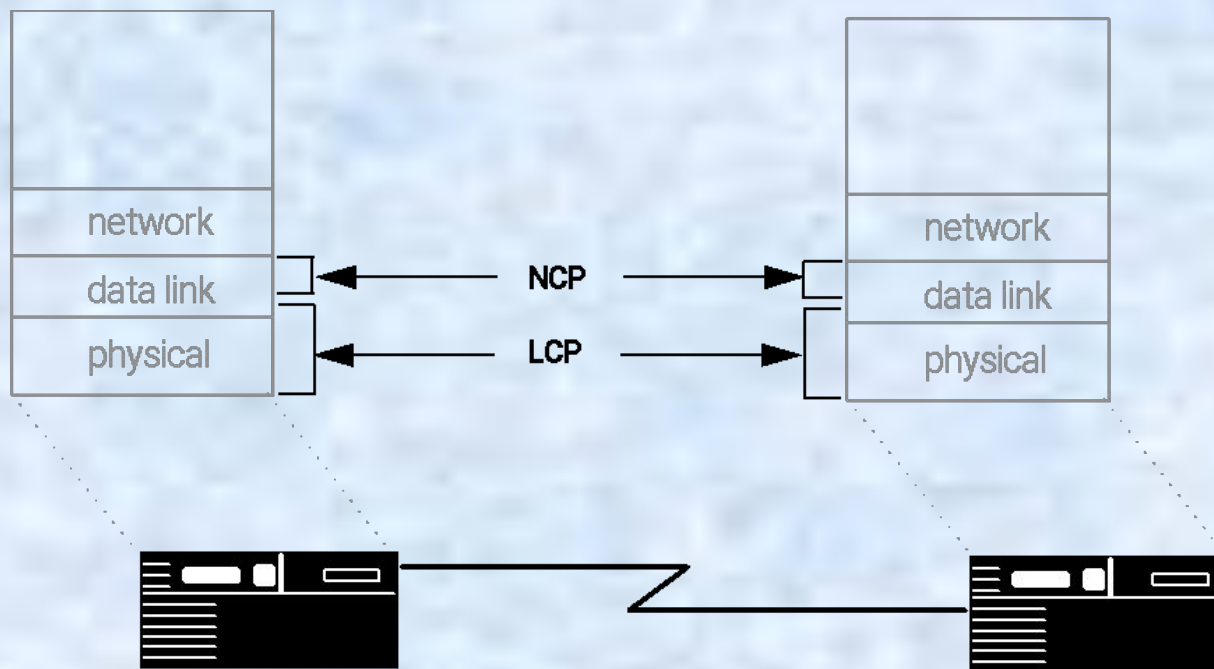
Основное назначение - организация одновременной передачи по одному логическому каналу "точка-точка" нескольких протоколов сетевого уровня

Поддерживаются протоколы:

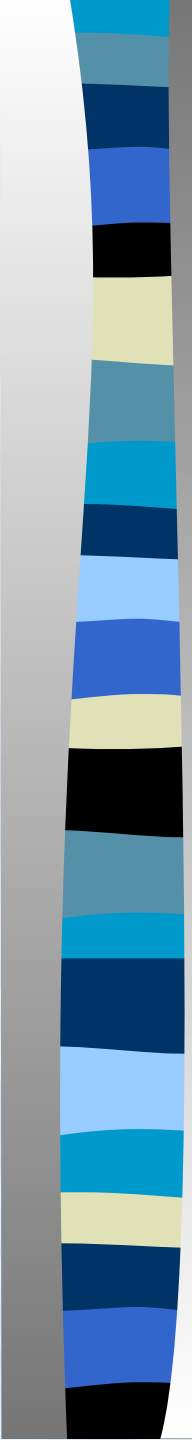
- ⇒ AppleTalk
- ⇒ DECnet phase IV
- ⇒ IPX
- ⇒ IP
- ⇒ OSI
- ⇒ XNS
- ⇒ Banyan VINES
- ⇒ NetBEUI (проект стандарта)

PPP может использоваться для инкапсуляции других протоколов канального уровня, например, Ethernet, обработки по алгоритму моста для их

Компоненты протокола PPP

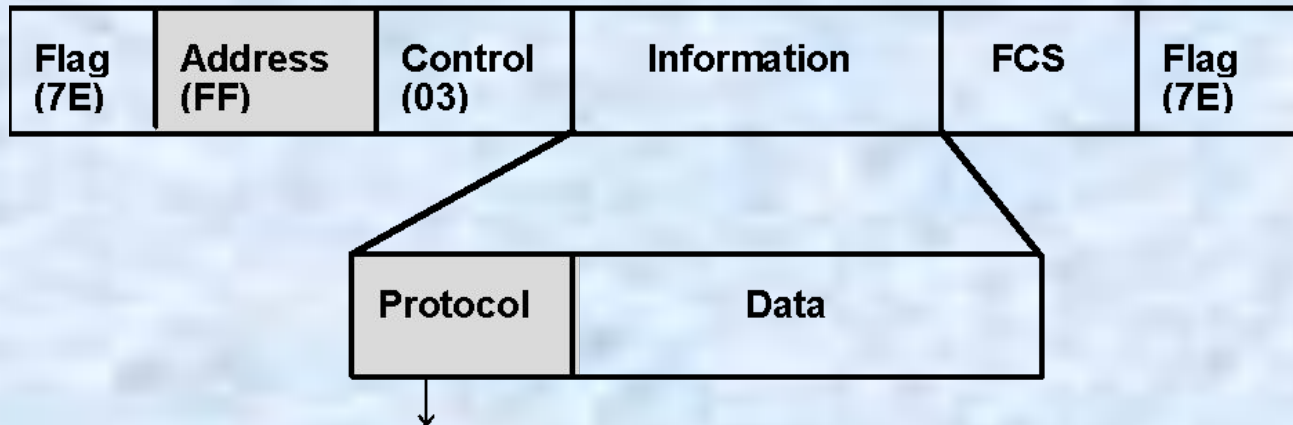


- ◆ При установлении сессии сначала работает протокол LCP,
- ◆ а затем протокол NCP
- ◆ Протокол LCP организует переговорный процесс о параметрах канала, например, о максимальном размере кадра. Протокол LCP также и завершает PPP-соединение между узлами

- 
- ◆ Протокол NCP позволяет договориться о том:
 - ⇒ какие сетевые протоколы будут передаваться в данной сессии PPP
 - ⇒ каковы из параметры, например, IP-адрес клиента
 - ◆ LCP о-
после открытия сессии работает все время в фон
вом режиме до завершения связи
 - ◆ При организации сессии с помощью протокола LCP стороны могут договориться об использовании некоторых необязательных протоколов:
 - ⇒ протокола Link Quality Monitoring (LQM), который используется для слежения за качеством канала связи
 - ⇒ протокола аутентификации Password Authentication Protocol (PAP)
 - ⇒ протокола аутентификации Challenge Handshake Authentication Protocol (CHAP)

Базовый формат кадра PPP

RFC1549 "PPP in HDLC Framing"



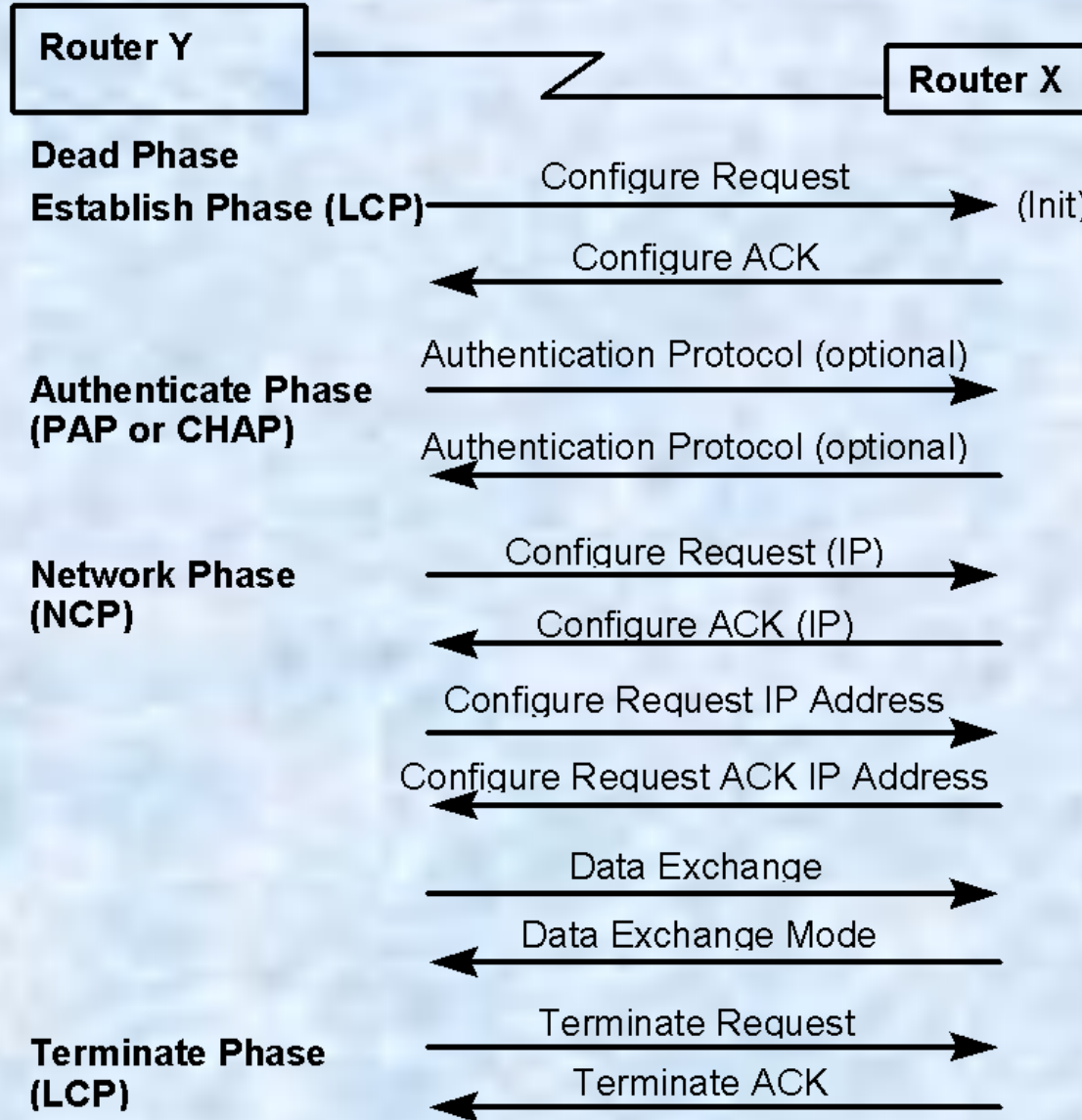
Указывает тип передаваемых данных : LCP, NCP, или протокол сетевого уровня:

Cxxx = LCP

8xxx = NCP

0xxx = Протокол сетевого уровня

Фазы работы протокола PPP





- ◆ **Dead Phase** -

случае успешной инициализации физического уровня. Канал переходит в Establish Phase

- ◆ **Establish Phase** -

канала связи. Когда оба взаимодействующих узла получают сообщение Configure ACK, канал считается открытым и переходит в обязательную фазу аутентификации Authenticate Phase

- ◆ **Authenticate Phase** (

необязательная фаза) аутентифицируются обе точки, используя протоколы Password Authentication Protocol (PAP) Challenge Handshake Authentication Protocol (CHAP).

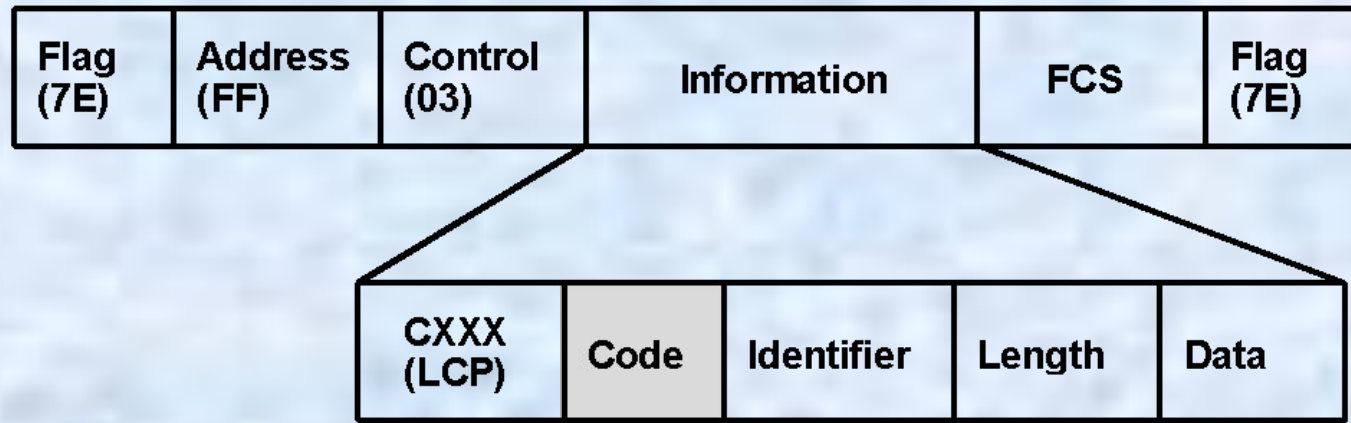
Network Phase Канал не переходит в фазу икации до завершения успешной аутентиф

- ◆ **Network Phase** -

любых из поддерживаемых протоколов сетевого уровня, используя соответствующий протокол NCP. После открытия сессии NCP, PPP канал начинает передавать пользовательские данные

- ◆ **Terminate Phase**—

Структура пакета протокола LCP

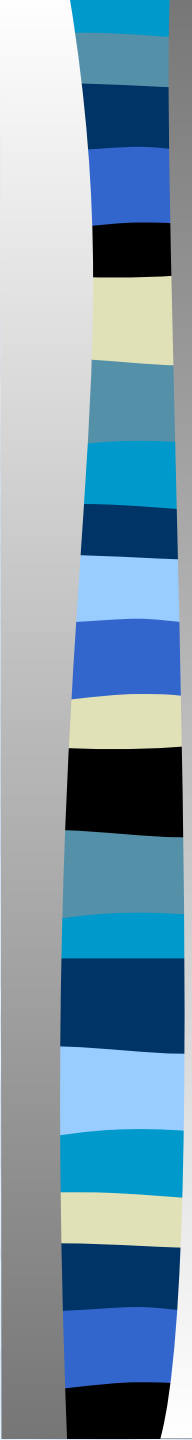


Указывает тип LCP сообщения:

- Config Req (code=1)
- Config Ack (code=2)
- Config Nak (code=3)
- Config Rej (code=4)

Длина LCP пакета (code, ID, и data)

Ставит в соответствие LCP запросы и ответы

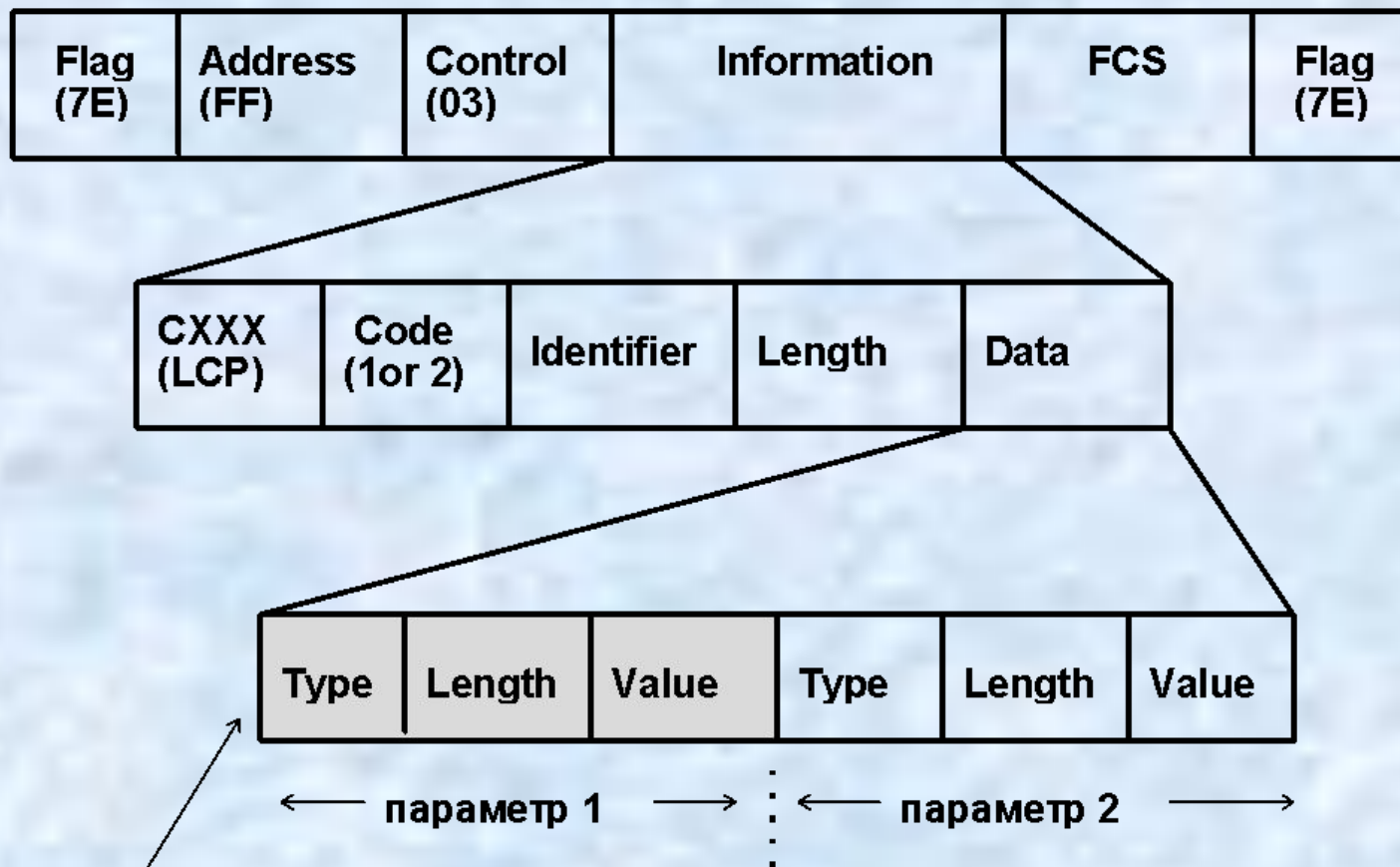


Примеры LCP пакетов, соответствующие различным кодам сообщений:

- ◆ **Configure Request (code=1)**
 - ⇒ Открытие соединения
 - ⇒ Обмен параметрами конфигурации
 - ⇒ Прием оговоренных параметров от другой стороны
- ◆ **Configure Ack (code=2)**
 - ⇒ Ответ на запрос Configure Request
 - ⇒ Указание на то, что значения параметров, полученных в Configure Request корректны
 - ⇒ Сигнализирует, что канал должен быть открыт по прибытию пакета
- ◆ **Configure Nak (code=3)**
 - ⇒ Показывает, что значения параметров неприемлемы
- ◆ **Configure Reject (code=4)**
 - ⇒ Указывает, что некоторые из параметров неприемлемы
 - ⇒ Шлет новый пакет Configure Request, не содержащий неприемлемые параметры, найденные в отвергнутом пакете

Поле Identifier идентифицирует LCP- запросы и LCP-ответы, помечая ответ на определенный запрос тем же идентификатором, что и запрос

Согласование параметров канала с помощью протокола LCP



У LCP восемь параметров конфигурации

Типы согласуемых по LCP параметров

Параметр	Описание	Тип	Длина	Значение
Maximum Receive Unit	Для согласования максимальных размеров пакетов (только для одного направления).	1	4	По умолчанию = 1500
Async-Control Character-Map	Согласует использование управляющих символов для асинхронных линий.	2	6	По умолчанию = FFFFFFFF
Authentication-Protocol	Используется для соглашения о используемом протоколе аутентификации. В некоторых реализациях допускается использование более одного протокола аутентификации.	3	≥ 4	C023 = Password Authentication Protocol C223 = Challenge/Response Authentication Protocol
Quality-Protocol	Определяет, когда и как часто в канале теряются данные	4	≥ 4	По умолчанию = нет C025 = Link Quality Report
Magic-Number	Для определения закольцованного канала и других аномалий на канальном уровне.	5	6	По умолчанию = нет
RESERVED				
Protocol-Field-Compressed	Согласует протокол сжатия на втором уровне.	7	2	По умолчанию = Запрещено
Address-and-Control Field-Compressed	Согласует сжатие полей address control (и значения фиксированные	8	2	По умолчанию = Не сжимать
FCS-Alternatives	Согласует длину поля контрольной суммы (32 или 16 бит).	9	2	По умолчанию = 16-бит FCS

Пример диалога между двумя узлами по протоколу LCP:

DLC: Frame 12 arrived at 11:59:42.4901; frame size is 18 (0012 hex) bytes

PPP:

PPP: Protocol = C021 (Link Control)

PPP: Code = 01 (Configure Request)

PPP: Identifier = 1

PPP: Length = 14 bytes

PPP: Type = 01 (Maximum Receive Unit)

PPP: Length = 4 bytes

PPP: Value = 1594 bytes

PPP: Type = 05 (Magic Number)

PPP: Length = 6 bytes

PPP: Value = 129D7DC8

PPP:

DLC: Frame 13 arrived at 11:59:42.5031; frame size is 18 (0012 hex) bytes

PPP:

PPP: Protocol = C021 (Link Control)

PPP: Code = 02 (Configure Ack)

PPP: Identifier = 1

PPP: Length = 14 bytes

PPP: Type = 01 (Maximum Receive Unit)

PPP: Length = 4 bytes

PPP: Value = 1594 bytes

PPP: Type = 05 (Magic Number)

PPP: Length = 6 bytes

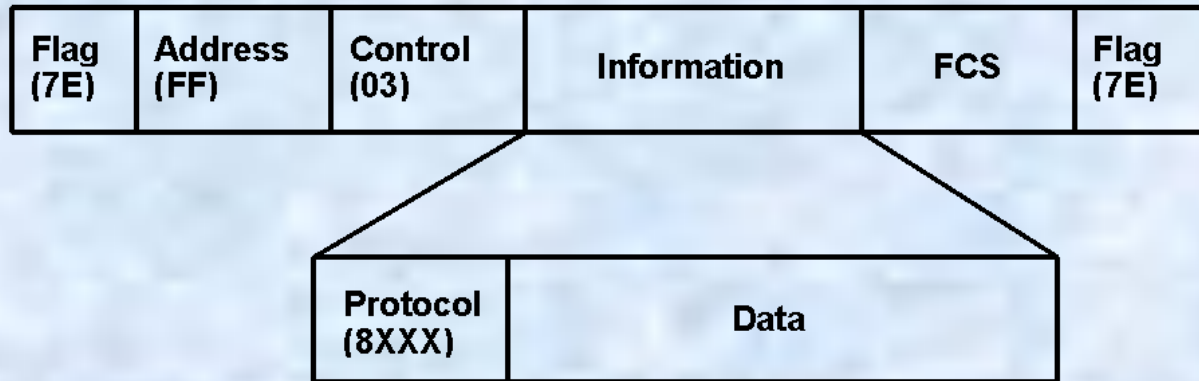
PPP: Value = 129D7DC8

PPP:

Протокол NCP

- ◆ Переговорный процесс, проводимый NCP, определяет, пакеты каких протоколов сетевого уровня будут передаваться в пакетах PPP в рамках данной сессии
- ◆ Для каждого протокола сетевого уровня, который поддерживается NCP, существует соответствующий стандарт RFC, определяющий способ инкапсуляции его пакетов в PPP пакет, а также параметры, подлежащие принятию в результате переговоров
- ◆ Например, для протокола IP существует спецификация RFC1332 "The PPP Internet Protocol Control Protocol (IPCP)"
- ◆ Аналогичные спецификации имеются для протоколов IPX (IPXCP), DECnet (DNCP) и других
- ◆ Отдельного протокола NCP не существует, а имеется семейство NCP-уровня протоколов, по одному для каждого протокола сетевого уровня
- ◆ Протоколы семейства NCP используют тот же формат кадра, что и протокол LCP

Формат кадра протокола NCP:



Указывает на тип NCP:

- 8021 - IP
- 8029 - AT
- 8025 - XNS, VINES
- 8031 - Bridge
- 8027 - DECnet
- 8023 - OSI

Пример процедуры согласования параметров протокола IP с помощью протокола IPCP

Согласуется IP-адрес

DLC: Frame 34 arrived at 12:00:09.4456; frame size is 14 (000E hex) bytes

PPP:

PPP: Protocol = 8021 (Internet Protocol Control)

PPP: Code = 01 (Configure Request)

PPP: Identifier = 9

PPP: Length = 10 bytes

PPP: Type = 03 (IP Address)

PPP: Length = 6 bytes

PPP: IP address = [200.5.5.1]

PPP:

DLC: Frame 35 arrived at 12:00:09.4626; frame size is 14 (000E hex) bytes

PPP:

PPP: Protocol = 8021 (Internet Protocol Control)

PPP: Code = 02 (Configure Ack)

PPP: Identifier = 9

PPP: Length = 10 bytes

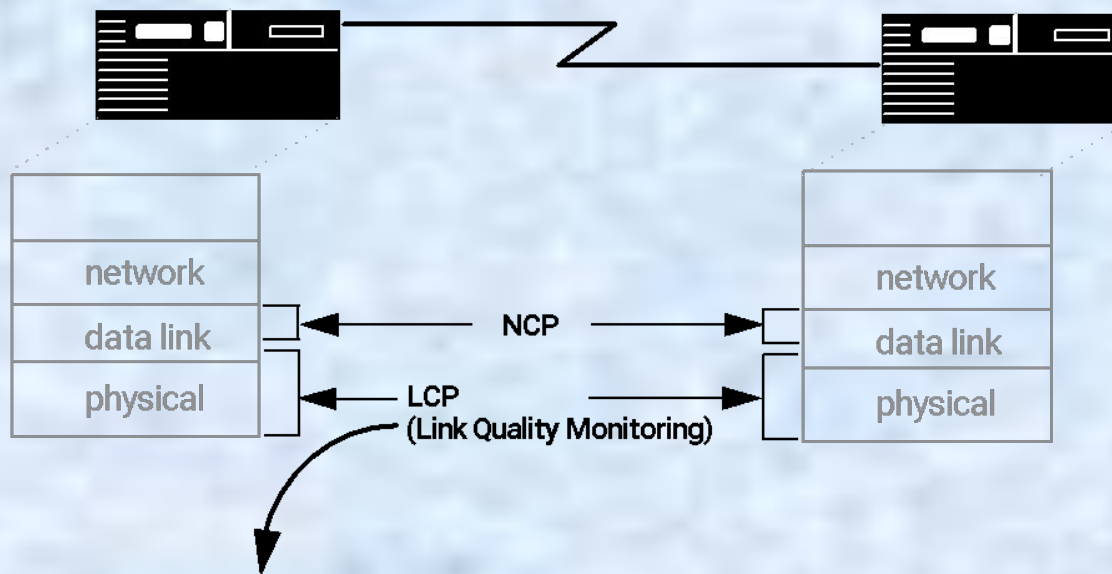
PPP: Type = 03 (IP Address)

PPP: Length = 6 bytes

PPP: IP address = [200.5.5.1]

PPP:

Протокол Link Quality Monitoring (LQM)



Протокол LQM использует для слежения два типа процедур:

- ♦ Link Quality Report (LQR)—
определяет качество линии связи, основываясь на проценте успешно переданных пакетов
- ♦ Echo Request/Reply -
определяет качество линии с помощью передачи служебных пакетов



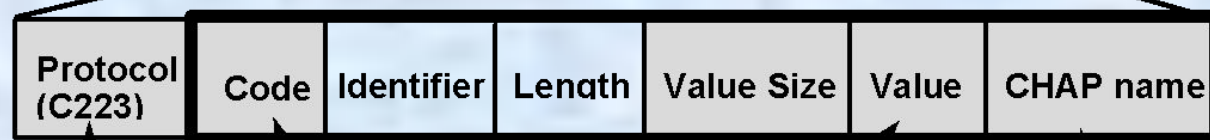
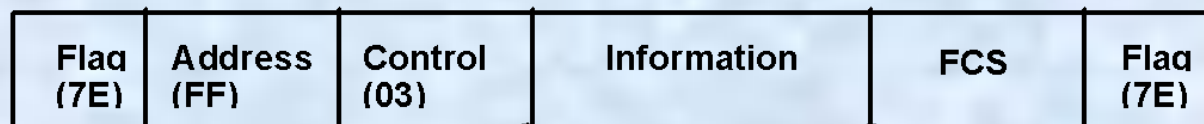
Протоколы аутентификации PAP и CHAP

- ◆ Описаны в RFC 1334
- ◆ В этом стандарте определено два протокола:
 - ⇒ Password Authentication Protocol (PAP)
 - ⇒ Challenge Handshake Authentication Protocol (CHAP)
- ◆ **Протокол PAP**
 - ⇒ Использует при аутентификации передачу идентификатора партнера и его пароля по глобальному каналу в виде открытого текста
 - ⇒ Если аутентификатор обнаруживает совпадение идентификатора и пароля с записью, имеющейся у него в базе легальных пользователей, то процесс аутентификации считается успешно завершённым

◆ Протокол SHAR

- ⇒ **Ключ** (*secret*) имеется как у аутентификатора, так и у партнера
- ⇒ **Слово-вызов** (*challenge*)
и передается в виде пакета генерируется аутентификатором типа Challenge партнеру
- ⇒ Партнер, получив слово-вызов, зашифровывает его с помощью односторонней хэш-функции MD5
- ⇒ Результат работы хэш-функции возвращается аутентификатору в виде пакета типа Response
- ⇒ Аутентификатор сравнивает этот ответ с тем значением, которое он получил, локально применив хэш-функцию к слову-вызову
- ⇒ Если результаты совпадают, то аутентификация считается успешной и партнеру посылается пакет типа Success - успех
- ⇒ Для защиты от перехвата ответа аутентификатор должен использовать различные значения последовательности символов при каждой последовательной аутентификации

Формат пакетов протокола CHAP



1 байт 2 байта 1 байт

Указывает на CHAP

CHAP код:
1 = challenge
2 = response
3 = success
4 = failure

Hash Value (secret)

CHAP Local Name

- ♦ Поле **Code** определяет тип пакета
- ♦ Поле **Identifier** (Response) необходимо для отождествления ответов и вызовов (Challenge)
- ♦ Поле **Length** (Code Identifier) содержит длину пакета CHAP вместе с полями и
- ♦ Поле **Value Size** пакетах Challenge) определяет длину (слова-вызова (Ve) или хэш-значения (в пакетах Response))
- ♦ Поле **Value** или хэш-значения предназначено для передачи слова-вызова
- ♦ Поле **CHAP name** - аутентификатора или партнера, в зависимости от того, кто является отправителем пакета. Имя партнера нужно аутентификатору для того, чтобы знать, какой ключ нужно использовать при аутентификации

Пример аутентификации узла с именем chicago аутентификатора с именем paris: у

----- **Frame 24 (Challenge)** - -----

DLC: Frame 24 arrived at 12:50:02.1940; frame size is 18 (0012 hex) bytes

PPP: Protocol = C223 (Challenge Handshake Authentication)

ADDR	HEX	ID	
0000	FF 03 C2 23 01 02 00 0E	04 10 6C 02 F7 70 61 72	□.B#.....l.wpar
0010	69 73		14 is

----- **Frame 25 (Response)** -----

DLC: Frame 25 arrived at 12:50:02.2184; frame size is 32 (0020 hex) bytes

PPP: Protocol = C223 (Challenge Handshake Authentication)

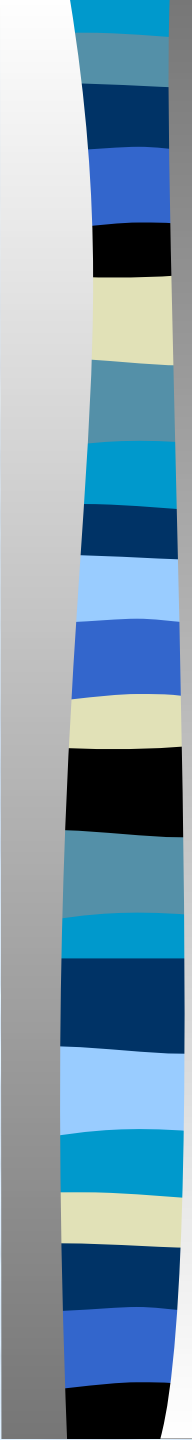
ADDR	HEX	ID	MD5 (
0000	FF 03 C2 23 02 02 00 1C	10 47 A4 0C 5D 45 4D EF	□.B#....G\$.]EMo
0010	5D 29 66 B2 13 17 1A F6 4B 63 68 69 63 61 67 6F]f2...vKchicago

----- **Frame 26 (Success)** - - -----

DLC: Frame 26 arrived at 12:50:02.2257; frame size is 8 (0008 hex) bytes

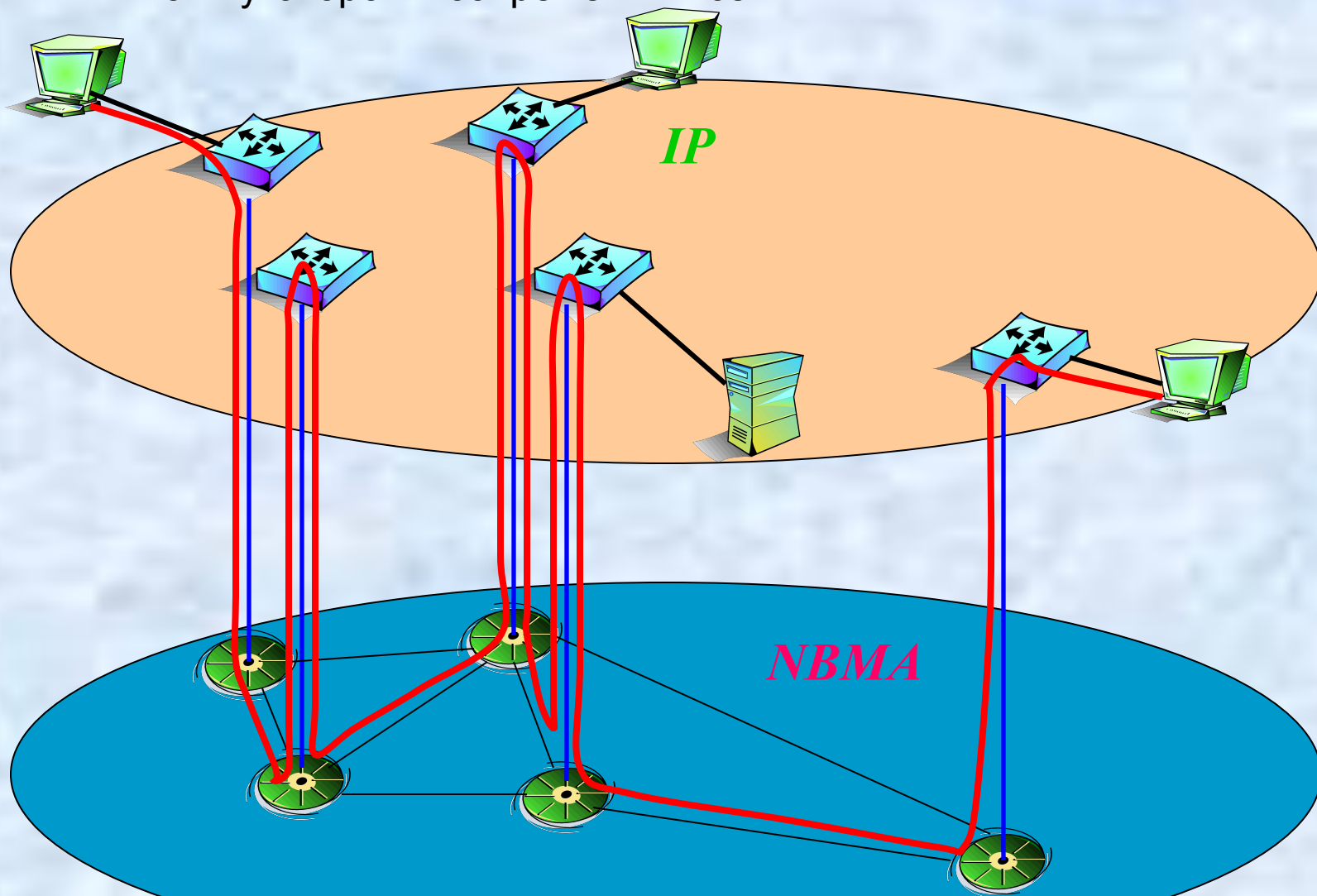
PPP: Protocol = C223 (Challenge Handshake Authentication)

ADDR	HEX	ASCII
0000	FF 03 C2 23 03 02 00 04	□.B#...



3. Нешироковещательные сети с множественным доступом – Non-Broadcast with Multiple Access, NBMA

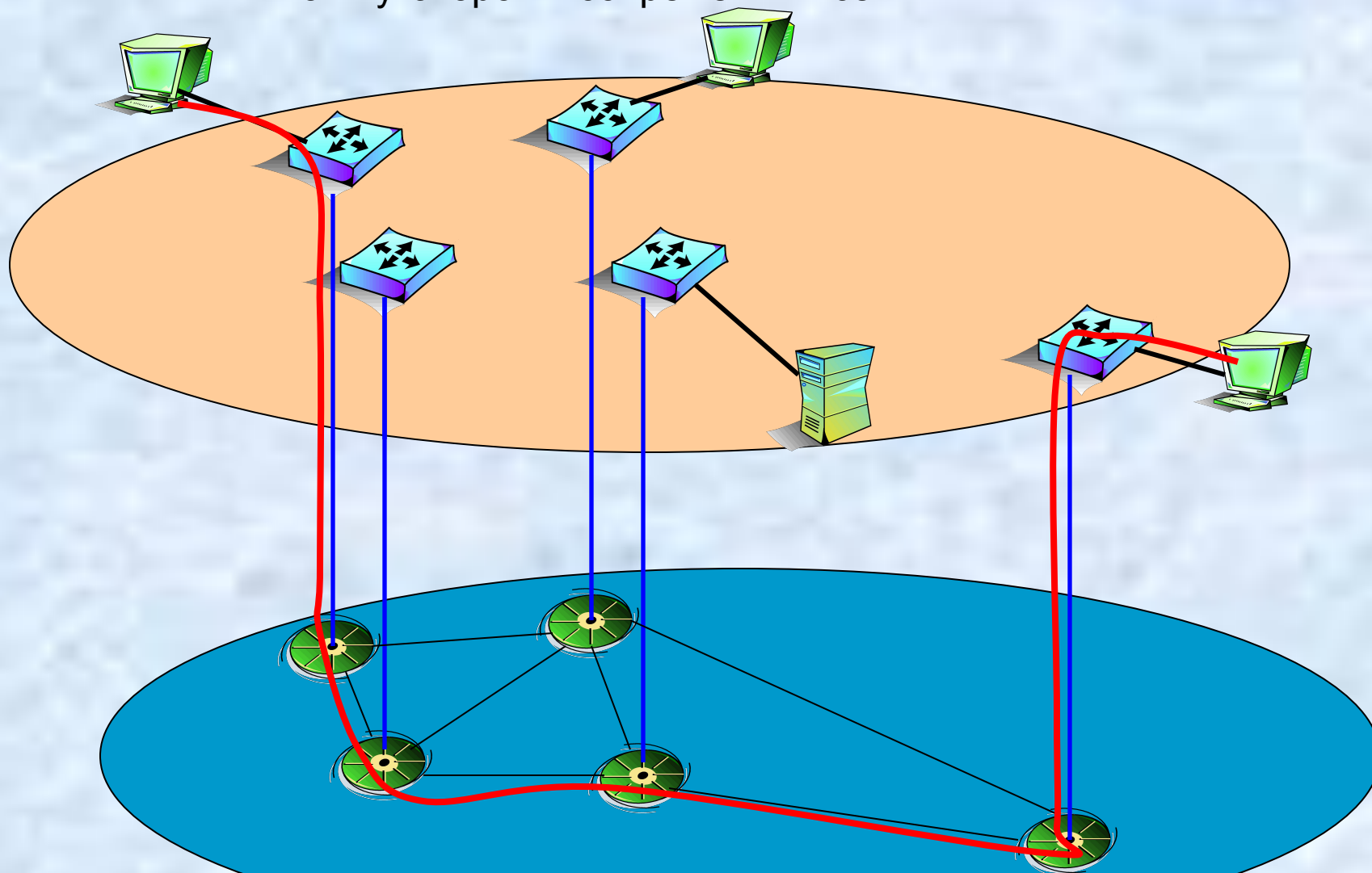
Взаимодействие слоев маршрутизаторов и коммутаторов в современных сетях



Традиционный способ - сеть коммутаторов используется для выполнения следующего хопа

Результат - медленное продвижение пакета - большое число хопов

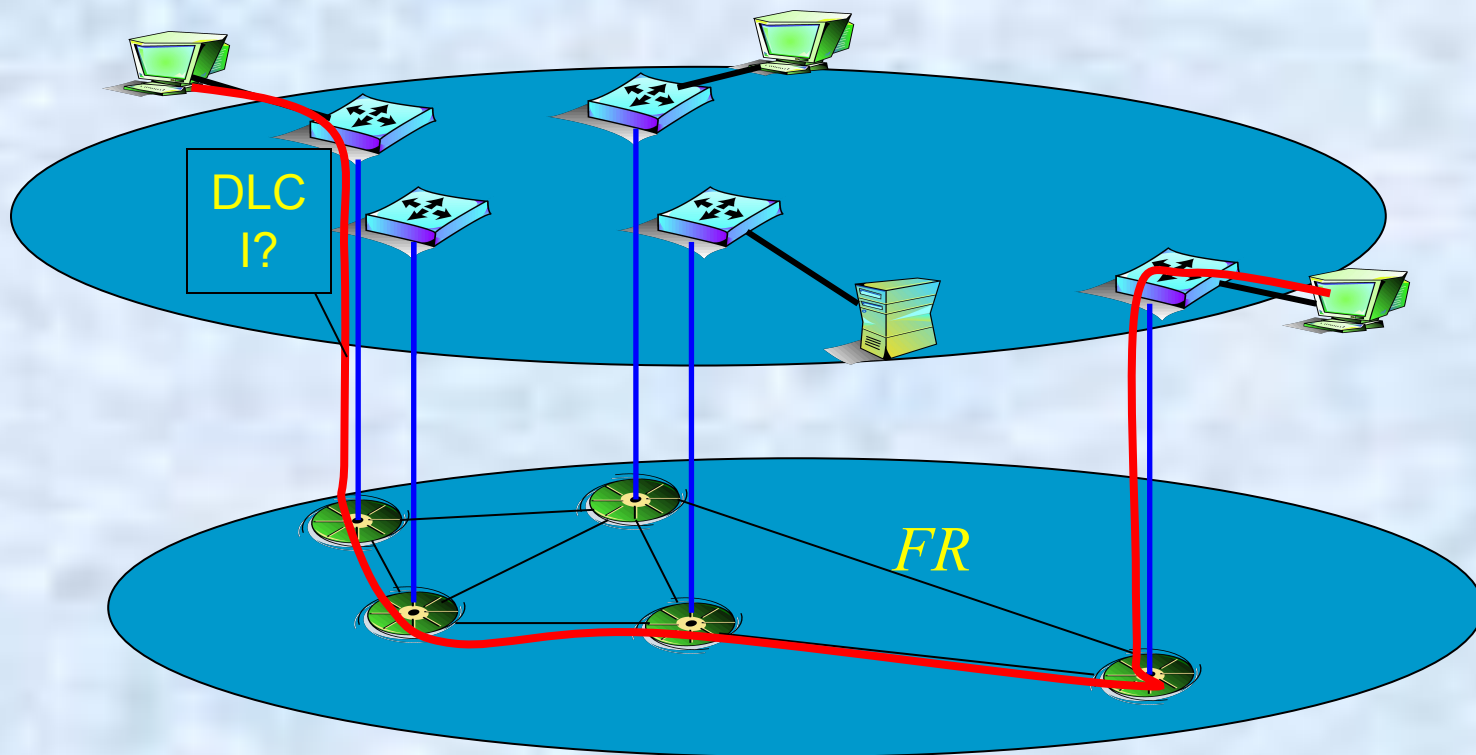
Взаимодействие слоев маршрутизаторов и коммутаторов в современных сетях



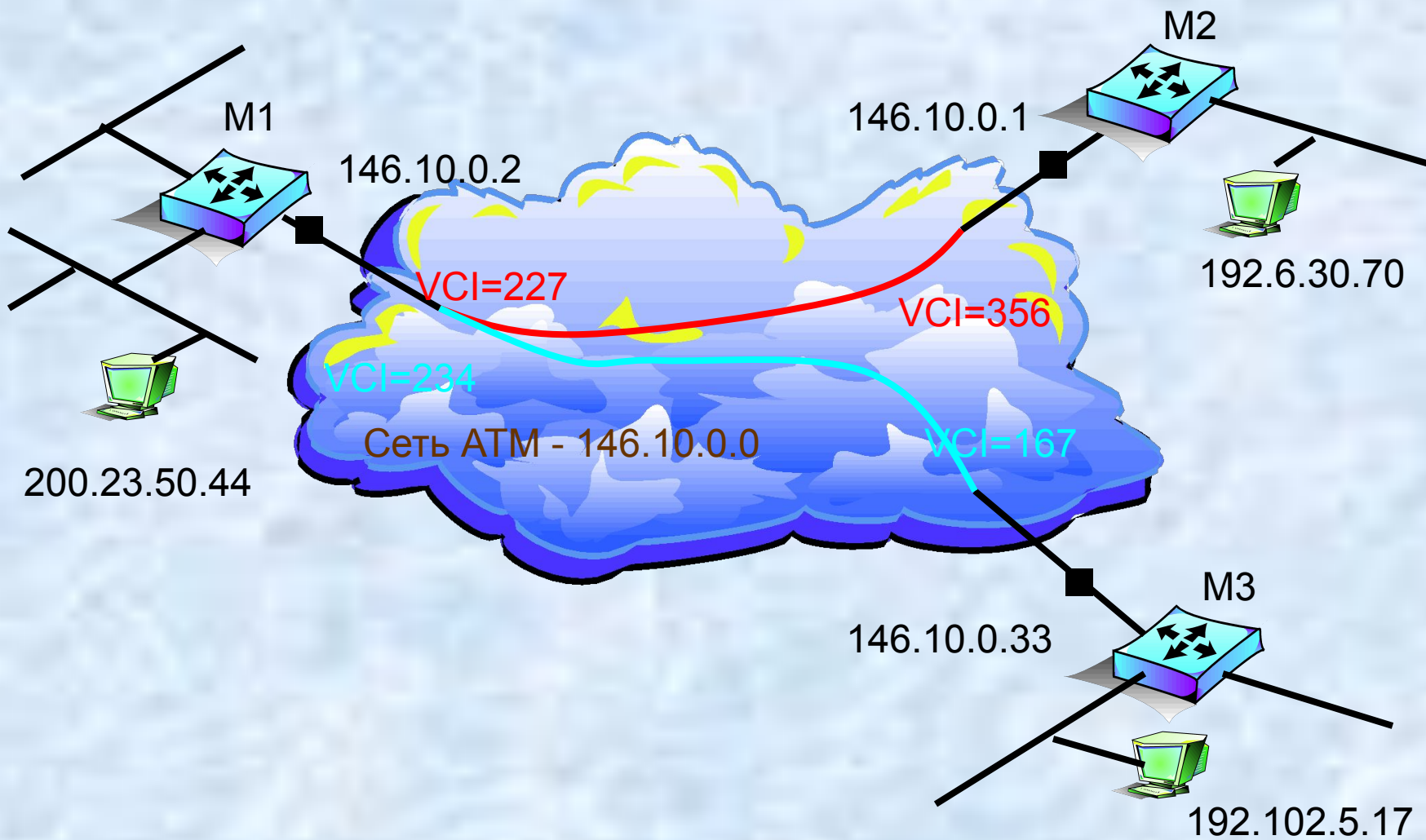
Ускоренная маршрутизация - пакет проходит сеть за два хопа

Происходит «прокол» сети коммутаторов до ближайшего к узлу назначения маршрутизатору

Основная проблема - как определить канальный адрес ближайшего маршрутизатора – как будет работать ARP ?



Традиционный вариант работы IP over NBMA



Ручное конфигурирование ARP-таблицы

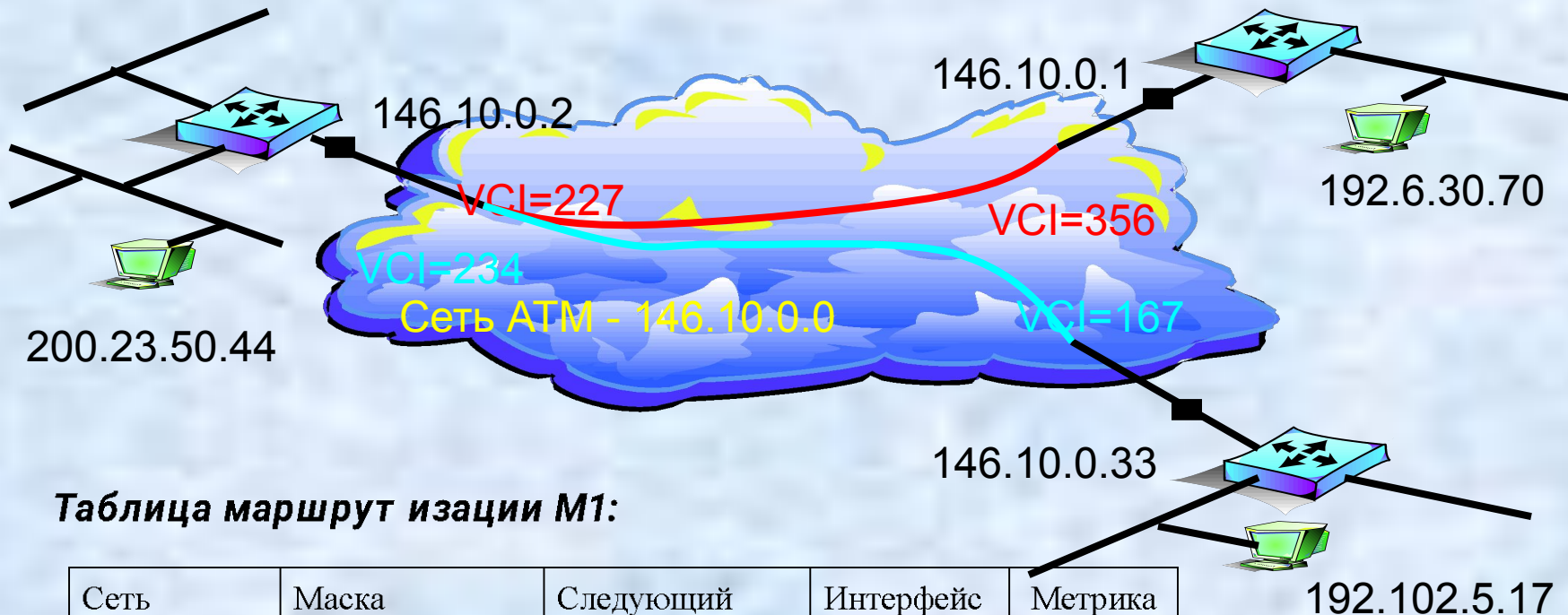


Таблица маршрут изации M1:

Сеть	Маска	Следующий маршрутизатор	Интерфейс	Метрика
146.10.0.0	255.255.0.0	146.10.0.2	146.10.0.2	1
200.23.50.0	255.255.255.0	146.10.0.2	146.10.0.2	1
192.6.30.0	255.255.255.0	146.10.0.1	146.10.0.2	2
195.102.5.0	255.255.255.0	146.10.0.33	146.10.0.2	2

ARP-таблица маршрутизатора 1:

146.10.0.1	227
146.10.0.33	234

Специальные команды конфигурирования маршрутизаторов Cisco для сетей NBMA

neighbor ip-address – задает соседа по NBMA

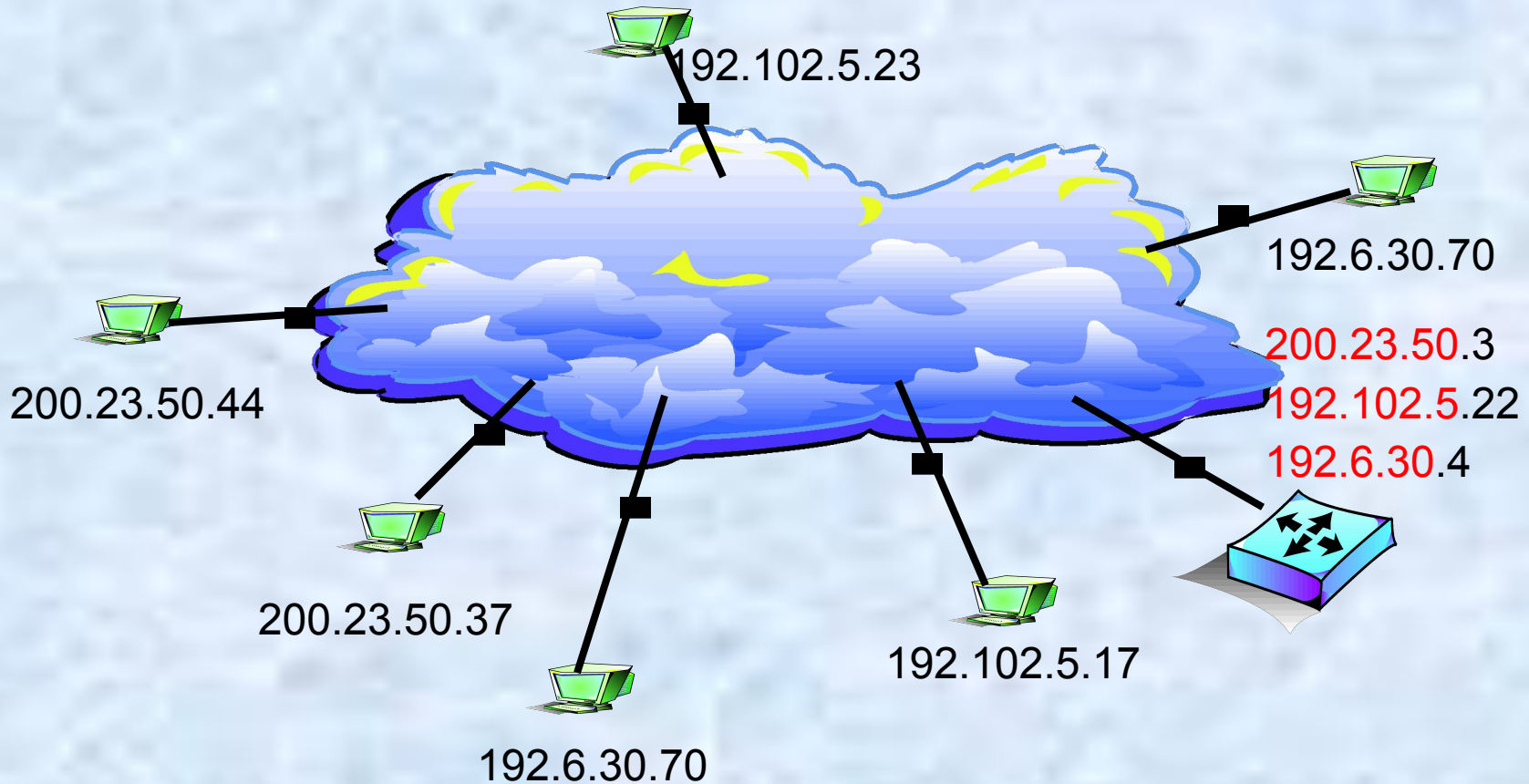
frame-relay map ip 194.12.200.5 201-

отображает IP-адрес 194.12.200.5 на номер PVC 201

no ip split-horizon

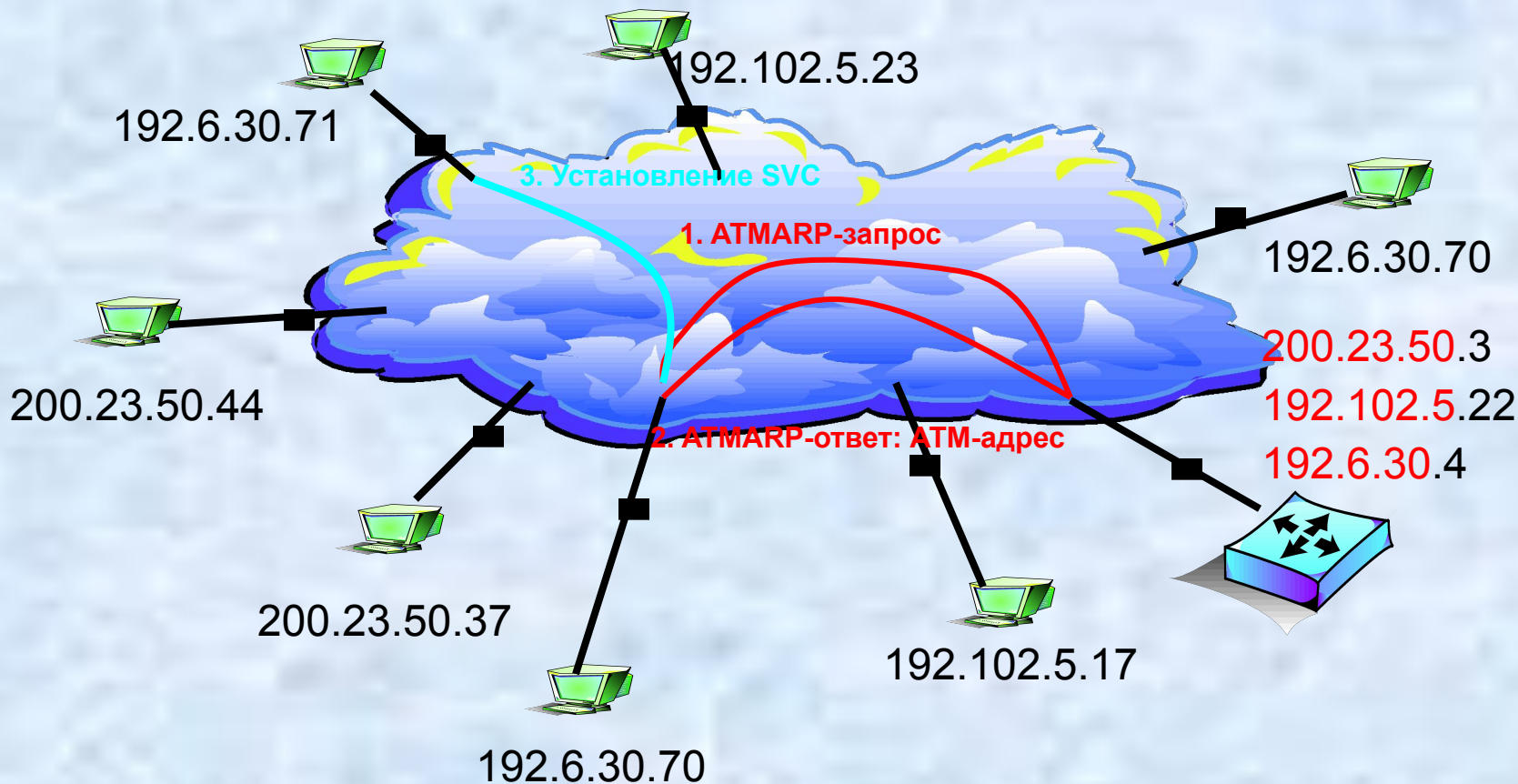
запрещает использование техники **split horizon** для интерфейсов с несколькими IP-адресами

Логические подсети - Logical IP Subnetwork



- Узлы различных IP-подсетей образуют логические IP подсети - LIS (Logical IP Subnetwork)
- Узлы различных LIS не могут взаимодействовать через сеть ATM непосредственно, только - через маршрутизатор
- Маршрутизатор присоединен ко всем LIS

Протокол Classical IP - поддержка LIS в ATM



- ◆ В каждой LIS должен быть свой ARP-сервер (обычно, это маршрутизатор)
- ◆ ATM-адрес ARP-сервера формируется в узлах вручную
- ◆ Каждый клиент должен установить соединение с ARP-сервером и зарегистрировать IP- и ATM-адреса
- ◆ Разрешение IP-адреса автоматическое, по стандартному ARP-запросу, направляемому ARP-серверу
- ◆ Взаимодействие между LIS – обычным способом, через маршрутизатор

NHRP - кратчайшая связь между LIS через «усеченные» маршрутизаторы

Сервер NHS

Клиент NHC - только IP forwarding

146.10.0.2
NBMA-5

NHRP-запрос прямого пути

146.10.0.1
158.27.0.1
NBMA-4

Прямой путь

200.23.50.44

Клиент NHC - только IP forwarding

146.10.0.14
NBMA-1

158.27.0.14
NBMA-2

158.27.0.2
NBMA-3

192.6.30.70

Нахождение прямого пути между сетями:

1. Клиент NHC - серверу NHS: Запрос (на следующий хоп к узлу 192.6.30.70 без маршрутизации, по протоколу NBMA)
2. Сервер NHS - клиенту NHC: Следующий хоп - адрес NBMA-3
3. Клиент устанавливает прямой путь к узлу NBMA-3 и передает ему пакет
4. Узел NBMA-3 – усеченный маршрутизатор. Он продвигает пакет узлу 192.6.30.70 обычным способом