6.Управление в канала - HDLC формати. Протоколи PPP и PPPoE

High-Level Data Link Control

Първият протокол на канално ниво, който се използва в IBM е**SDLC** (synchronous data link control).По-късно организацията по стандартизация ISO разработва на базата на SDLC протокола **HDLC** (high-level data link control). И двата протокола са битово-ориентирани и използват вмъкване на битове за правилно идентифициране на кадрите. Форматът на кадъра в HDLC е следния:



В началото и в края на кадъра са флаговете за маркиране награниците на кадъра. Полето *Address* се използва при многоточкови канали (multipoint) и чрез него се идентифицира получателя на кадъра. Полето *Control* се използва за номериране на кадрите, за потвърждения и за други цели. Полето *Data* съдържа данните на кадъра. По принцип има неограничена дължина. Полето *Checksum* е контролната сума на кадъра (използват се циклични кодове). Минималната дължина на кадъра, без да се включват флаговете за начало и край е 32 бита

High-Level Data Link Control

Кадрите са три вида - **information**, **supervisory** и **unnumbered.**

Полето Control в:

(a) information frame.

(b) supervisory frame.

(c) unnumbered frame.

- Полето *Control* за information-кадрите

В протокола се използва прозорци с 3-битови номера. Полето *Seq* е поредния номер на кадъра в прозореца на предавателя. Полето *Next* е прикачено потвърждение за насрещния поток – то съдържа номерът на следващия кадър, който се очаква в получателя. Битът *P/F* се използва при изпращане на кадри към терминали. Ако той е 1, предавателят указва на терминала да предава. Всички кадри, които терминалът изпраща освен последния имат стойност 1 за този бит. За последния изпратен кадър *P/F* е 0. Понякога битът *P/F* се използва за да се укаже на получателя да изпрати моментално потвърждение, а не да го прикачва към насрещния трафик.

- Полето *Control* за supervisory-кадрите

Полето *Type* определя типа на кадъра:

- тип 0 (RECEIVE READY) - кадър за потвърждение, в полето *Next* се указва номерът на следващия очакван кадър;

- тип 1 (REJECT) - кадър за негативно потвърждение, в полето *Next* се указва номерът на първия неполучен кадър, предавателят трябва да изпрати наново всички кадри, започвайки от *Next* (това отговаря на стратегията go back n);

- тип 2 (RECEIVE NOT READY) - кадър за потвърждение, подобен на RECEIVE READY, но указващ на предавателя да спре да изпраща кадри;

- тип 3 (SELECTIVE REJECT) - кадър за негативно потвърждение, в полето *Next* се указва номер на неполучен кадър,предавателят трябва да изпрати наново само кадърът с номер *Next* (това отговаря на стратегията selective repeat)

- Полето *Control* за unnumbered-кадрите

Тези кадри са служебни и касаят поддържането на съединението, наричат се още **команди**. Някои от командите са:

- DISC (DISConnect) - команда за разпадане на съединение;

- SNRM (Set Normal Response Mode) - команда за установяване на режим, в който едната машина управлява, а другата изпълнява;

- SABM (Set Asynchronous Balanced Mode) - команда за установяване на режим, в който двете машини имат еднакво влияние върху съединението;

- SNRME, SABME (Extended) - аналогични команди на SNRM и SABME, но номерацията на кадрите при тях е 7-битова (полетата *Seq* и *Next* се разширяват с по 4 бита);

- FRMR (FRaMe Reject) - команда, която указва за кадър с погрешна семантика - например, кадър с дължина по-малка от 32 бита или кадър за потвърждение на неполучен кадър.

- Полето *Control* за unnumbered -кадрите

Специален unnumbered кадър UA (unnumbered acknowledgement) за потвърждаване на получена команда.

След изпращането на всяка команда се изчаквасъответно потвърждение преди да се изпрати друга команда.

Други Data Link Layer протоколи

**Протокол PPP**

Протоколът PPP (Point-to-Point Protocol) е протокол за двуточкова връзка. Този протокол се използва за свързване на домашни компютри до доставчици на Интернет услуги по телефонна линия. Протоколът PPP е байтово-ориентиран и за идентифициране на кадрите се използва техниката вмъкване на байтове. Форматът на кадъра е наследен от HDLC:



При PPP няма индивидуални адреси на станциите, затова полето *Address* съдържа 11111111, което означава адресите на всички станции. Полето *Control* съдържа 00000011, което означава unnumbered-кадър. С други думи, PPP не осигурява надеждно предаване чрез номера на кадрите и потвърждения. Полето *Protocol* съдържа идентификатор на протокол, който указва как да се интерпретира полето *Payload*, в което се помества съответния пакет.Максималната дължина на *Payload* е 1500 байта.

Дължините на полетата *Protocol* и *Checksum* се договарят при установяването на съединение. След установяване на съединение, двете страни се договарят за мрежовите протоколи, които ще се използват. След това започват да се предават кадрите с данни, като полето *Protocol* съдържа идентификатор на един от уговорените мрежови протоколи, а *Payload* съдържа съответната дейтаграма.

PPP фази



Схема на установяване на връзката.

LCP

**Line Control Protocol** (**LCP**): автоматично конфигуриране на срещуположните интерфейси: дължина на кадъра, ESC символи; Проверка на линията за грешки с произволни числа (magic numbers). Ако линията е дадена накъсо, възелът получава LCP съобщение със своя си magic number, вместо да получи magic number на съседа; Компресия. Последвани евентуално от аутентикация.

Аутентикация

Съседите си обменят съобщения за аутентикация. Имаме два варианта:

Password Authentication Protocol (PAP) и Challenge Handshake Authentication Protocol (CHAP).

В безжичните мрежи се ползва EAP.

**PAP** предава пароли в явен ASCII текст по мрежата,затова е несигурен.

\* Клиент изпраща username и password

\* Сървърът връща: authentication-ack (ако е OK) или authentication-nak (в противен случай).

CHAP периодично проверява идентичността на клиента чрез **three-way handshake**. При установяване на сесията и през произволни интервали от време след това. Проверката се базира на споделена “тайна” (напр. Паролата на потребителя).

1. Сървърът изпраща **"challenge"** съобщение към клиента.

2. Клиентът отговаря с число, изчислено с помощта на еднопосочна хеш функция, напр. **MD5 checksum hash**.

3. Сървърът сравнява този хеш със своя. Ако съвпадат, с;едва acknowledge; в противен случай връзката се прекъсва.

4. През произволни интервали сървърът изпраща новопредизвикателство: стъпки 1-3 се повтарят.

Network Control Protocol (NCP) се стартира след LCP.Уговаря опции за протокола от мрежовия слой, надPPP. NCP са: Internet Protocol Control Protocol (**IPCP**) за IP,Internetwork Packet Exchange Control Protocol (**IPXCP**) за IPX и AppleTalk Control Protocol за AppleTalk и **IPv6 Control Protocol** (**IPV6CP**) за предаване на IPv6 пакети по PPP линии.

Развитие на PPP – PPPoE

**PPPoE**, **Point-to-Point Protocol over Ethernet** опакова PPP кадри вътре в Ethernet кадри. Използва се при свързвания към Интернет чрез ADSL или кабелни модеми, LANs, WLANs или Metro Ethernet мрежи. Разработена е от UUNET, Redback Networks и RouterWare, стандартизирана е в RFC (Request for Comment) 2516. Ethernet мрежите са с пакетна комутация, connectionless, нямат механизми за защита срещу IP и MAC конфликти и компрометирани DHCP сървъри. Чрез PPPoE потребителите виртуално “набират номера" на отдалечен сървър на провайдера през Ethernet и установяват“point to point” връзка.

PPPoE - стадии

PPPoE се установява на два точно определени стадия:

**PPPoE discovery** Традиционните PPP връзки се установяват между две крайни точки, които са предварително изградени. Но Ethernet мрежите са multi-access, така че преди обмен на PPP контролни пакети за установяване на връзката върху Ethernet, двете старни ще трябва да си научат MAC адресите, за да бъдат закодирани в контролните пакети. Също така се установява Session Id, която се използва при обмена на пакети.

**PPP session** След като са известни MAC адресите и е установена сесията, двете старни имат всичката информация за изграждане на “point-to-point” връзка по Ethernet и обмен на пакети.