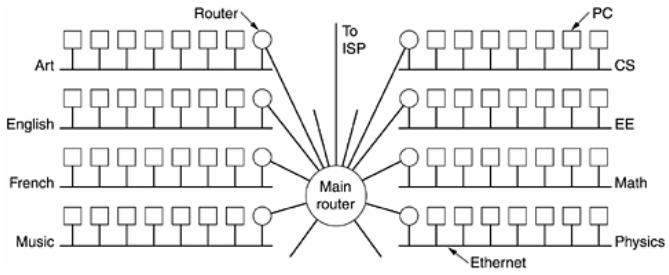
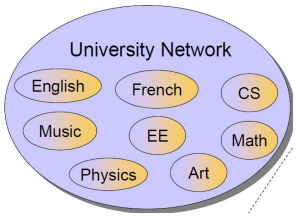
Вариант 0 / Вариант 9/

0. Какво представляват корпоративните мрежи? Дайте пример за реализация на корпоративна мрежа.



Университетска (корпоративна) мрежа разделена на подмрежи

При създаване на Internet корпоративна мрежа се използва протоколния стек TCP/IP. Тези мрежи използват транспортните услуги на Internet и хипертекстовите технологии WWW. При корпоративните мрежи защитата е възложена на системните администратори. С помощта на специални средства проверяват всеки входящ и изходяш файл за вируси.



‘Subneting’ се използва за идентифициране на подмрежите в корпоративните (университетските) мрежи, като отвън се виждат като една мрежа с общ IP адрес(128.143.0.0). Във вътрешното пространство част от полето на хостовете се използва за адресиране на подмрежите.

С цел улесняване на администрирането в големите мрежи (корпоративни, университетски и т.н.), които всяка година се разширяват с нови хостове и нови мрежови приложения се препоръчва разделянето им на подмрежи. В подмрежите се групират компютри с еднотипни приложения, адмистративни и бизнес функции и т.н.

1.Управление на явлението задръстване при TCP протоколите.

Когато голямото количество трафик преминаващо през дадена връзка, създаде задръстване, част от пакетите биват задържани (в опашки) за известно време или биват отхвърлени. Това от своя страна води до повторно предаване на отхвърлените, увеличаване на забавянията и в крайна сметка до лоша производителност. Технологията за регулиране скоростта на предаване по TCP протокол, реагира преди да е настъпило задръстване като по този начин действително намалява до минимум появата на големи забавяния. С контролиране на потвържденията към изпращача и управляване на анонсираните размери на "прозореца", механизма за регулиране скоростта на предаване по TCP протокол диктува на изпращащия компютър с каква скорост да предава данните за да бъдат предотвратени образуванията на задръствания (респ. намалени забавянията, породени от задържане на пакетите в опашките на маршрутизаторите). Всичко това води до намаляване на забавянията по мрежата и ускоряване работата на всички приложения.

Лекции: Поради ограничения размер на опашката в маршрутизатора настъпва задръстване, в следствие на повторно изпратените сегменти (timeout за сегменти на хоста A). Това ще доведе до нови time outs и задълбочаване на задръстването.

Управление на явлението задръстване посредством времето за изчакване на ACK (**Retransmission Timer**) със “Slow Start/Congestion Avoidance”.

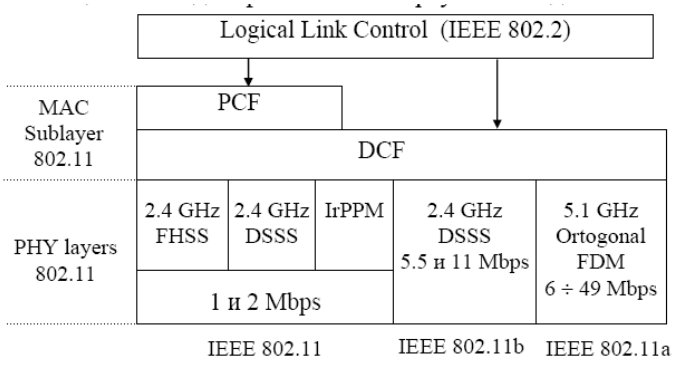
2.Опишете какви кадри се използват при MAC подслоя на IEEE 802.11/??????????????????????

Комплексно решение на проблема за управление на достъпа до безжични съобщителни среди при двете основни топологии предлага стандарта IEEE 802.11. MAC протокола при 802.11 е проектиран да работи с три вида съобщителни среди - два радио-канала в ISM диапазони 2.4 GHz(FHSS със скорости 1 и 2 Mbps и DSSS с 1, 2, 5.5 и 11 Mbps) и 5.1 GHz и третата съобщителна среда е дифузен инфрачервен канал с позиционно-импулсна модулация IrPPM (infrared pulse-position) и скорости от 1 и 2 Mbps.

IEEE 802.11 MAC протокола реализира две взаимно свързани функции на механизма на достъп:

разпределена координираща функция DCF (distributed coordination function) и функция реализираща сканиране PCF (point coordination function).

Разпределената координираща фукнкция се реализира с механизма CSMA/CA и е достъпна за‘Ad hoc’ и структурираните WLAN. За разлика от кабелните мрежи, където всички станции са свързани (могат да се “чуват” една с друга) и следенето на носещата с цел откриването на конфликти се реализира от предаващата станция, то при безжичните мрежи това е невъзможно поради ограничената свързваемост (ограничената излъчвана мощност) и ефекта скрит терминал (предаващата станция би “чувала” само собственото си предаване). Затова тук MAC протокола е полудуплексен и механизма на следене на носещата с цел откриване на зает канал и избягване на конфликт се реализира по два допълващи се метода - физическо и виртуално следене.



Виртуалното следене на носещата се реализира от MAC подслоя и се базира на вектора за определяне състоянието на мрежата NAV (network allocation vector), поддържан от всяка мобилна и базова станция, и съдържащ информация за времето през което съобщителния канал ще бъде зает. Времената в NAV се задават от полетата 'продължителност на обмена' в служебните кадри RTS/CTS, използвани за резервиране на канала преди предаването на данните - фигура 8. По такъв начин се предотвратява явлението скрит терминал, като всички станции 'чуващи' предаващата (MH1) или отговора на приемащата (MH2) станция актуализират своят NAV отлагайки достъпа до общия съобщителен канал (Defer access). Появата на конфликт е най-вероятна по-времето на състезателният период (CW) при размяната на RTS кадри (конфликтите възникват в приемащата станция). Предаващата станция установява конфликта, по липсата на CTS кадър или ACK (опознаване) при конфликт на кадри с данни.

3.Определете същността на QoS (Quality of Service).

Необходимост от QoS (Quality of Service) - Формиране на опашки при маршрутизатори и комутатори. Гарантиране на изпращането на пакетите – основна цел на QoS.

- Двумерен контрол по четност (Блоков контрол по четност) - При този метод предаваният кадър от *d* бита се рзделя на *i* реда и *j* стълба, като за всеки от тях се прави контрол по четност. Това позволява при възникване на грешка по време на предването, сгрешеният бит да се открие и след неговото инвертиране се коригира.

Осигуряване на допълнителен клас обслужване QOS (Quality of Service – качество на услугите) – даващ възможност на потребителите да определят приоритет на своите клетки чрез установяване на специален бит <CLP> (Cell Loss Priority) в заглавната част;

Когато се използва QoS, различните мрежови приложения могат да съществуват в една и съща мрежа, без да поглъщат честотната си лента една на друга.

Определение: Терминът Quality of Service се отнася към множество технологии, за да гарантира качеството на различните услуги на мрежата. Качеството се отразява например в постоянното ниво на честотната лента, ниската латентност, липсата на загуба на пакети от данни и прочие. Основните ползи от QoS оптимизирана мрежа могат да бъдат обобщени така:

- Способност за приоритизиране на трафика – позволява критичните потоци от информация да бъдат пренасяни преди тези, които са с по-малка приоритетност.
- По-голяма сигурност в мрежата, благодарение на контролирането на количеството честотна лента, което всяко приложение може да използва, и нивата на честотната лента между различните приложения.

При препълване на опашката има загуба на пакети. В зависимост от политиката на QoS се отхвърлят най-дълго чакалите или новопристигналите.

QoS–средства използвани при съвременните мрежи

- Classification and marking tools
- Policing and shaping tools
- Congestion-avoidance (selective dropping) tools
- Congestion-management (queuing) tools
- Link-specific tools

Вариант 1

1.Сравнете линейното кодиране RZ и NRZ?

Преобразуването на цифрово съобщение в цифров сигнал се нарича кодиране в комуникационната линия (линейно кодиране). При него се използва специален линеен код за кодиране на цифровото съобщение в цифров сигнал. Под линиен код се разбират правилата, установяващи съответствие между поредицата битове на съобщението (кадъра на каналния слой) и символите, с които те се представят за предаване по комуникационната линия. Линийният код се избира по такъв начин, че параметрите на резултантния сигнал, както и честотният му спектър, да са подходящи за предаване по съответната физическа среда. Най-обикновения и най-простия начин да се предават цифрови сигнали е да се използват две различни нива на напрежение (U) за двете двоични цифри. Обикновено отрицателно напрежение се използва да представи "1" и положително напрежение да представи "0". Този код е известен като NRZ-L (Non return to-Zero - Level – без връщане към нула). Означава че сигнала никога не се връща в "0" значение на напрежението, и значение по време на "продължителността" на всеки бит време е някакво значение (ниво) на напрежението, тоест

сигналът никога не се възстановява. Недостатъците за този код са наличие на постоянна съставна в предавания сигнал и голяма вероятност за загуба на синхронизация при дълги последователности от 1 и 0.
При RZ (Return to-Zero – с връщане към нула) сигналът се възстановява, тоест връща се в положение „0".RZ - три стойности: положителна, отрицателна и нула
-1 - преход от положително към нулево напрежение
-0 - преход от отрицателно към нулево напрежение.
//Кодът от типа без връщане към нула NRZ (Non Return to Zero) намира приложение при цифровите логически схеми.
Кодът от типа връщане към нула RZ (Return to Zero) се получава като всеки символ се разделя на две части. Първата част на символа показва неговата двоична стойност, а остатъкът от символа винаги е нула. Поради съкращаването на импулса наполовина, в спектъра на сигнала се появяват много по-силни съставки с тактовата честота и с нейните хармоници, но сигнала не е лишен от постоянна съставяща и има относително широка честотна лента.

2.Опишете MAC подслоя 802.5?
Това е стандарта за кръгова топология с управляващ маркер. Основните характеристики са:
-Всички станции се свързват една след друга, като предават данни само в една посока. Предаващата двойка на всяко устройство се свързва към приемащата двойка на следващото устройство в кръга.
-Всяка станция се свързва директно във физическа звездообразна стуктура към централни концентратори (MSAU). Целта на MSAU е да запази функционалността на кръга чрез електрическо игнориране на неработещото устойство (когато станцията е изключена или блокирала). Станциите при Token Ring са директно свързани към MSAU, които от своя страна могат да се свържат заедно в един голям кръг.
-Всяка мрежова карта на станция работи като напълно функционален повторител (еднопосочен) като регенерира сигнала и извършва побитово повторение.
-Работи на скорост от 16 Mbps или 4 Mbps, но не и на двете едновременно (зависи от конфигурацията/типа на мрежовата карта. Всички устройства трябва да са съгласни със скоростта на кръга (ако всички станции в кръга могат/са конфигурирани да работят на скорост от 16 mbps тогава това е скоростта на кръга, ако дори само една карта не може или не конфигурирана за тази скорост, то кръга работи на 4 Mbps).
В MAC – подслоя на стандарта се използва протокола Token Ring . Управлението на достъпа става с маркер. Маркерът се генерира при инициализиране на мрежата, след което той циркулира по кръга само в една посока. Притежанието на маркера дава право за предаване на данни. Ако станцията получила маркера няма информация за предаване, предава маркера на следващата станция в потока, като всяка станция може да задържи маркера за определен период от време. Станция получила маркера и имаща информация за трансфер, го задържа и променя един бит в него, като го превръща в начало на кадър с данни, добавя информацията която трябва да се предаде и изпраща кадъра към следващата станция по кръга. Докато информациония кадър се предвижва по кръга няма маркер в мрежата (освен ако не се използва ранно освобождаване на маркера), което означава че останалите станции имащи данни за предаване изчакват до освобождаване на маркера. Информационният кадър обикаля по кръга докато достигне станцията местоназначение, която го копира за обработка. Кадърът продължава да се движи по кръга докато достигне до станцията, която го е изпратила. Тя проверява завръщащият се кадър, за да разбере дали станцията местоназначение го е видяла и в последствие копирала, след което го премахва и освобождава нов маркер. Ако се поддържа ранно освобождаване на маркера, след предаването на информационния кадър излъчващата станция освобождава нов маркер който "гони" кадърът с информация. Така или иначе във даден момент има само един маркер по кръга.
Протоколът Token Ring има предварително зададено максимално време за закъснение на кадъра, поради което е удобен за работа в реално време.

3.Опишете процедурата при изграждане на сокет. Пример:
Сокетите са средство за локална и мрежова комуникация между два процеса. Използването на сокети се базира на архитектурата клиент/сървър. Единият сокет работи на станцията, изискваща някаква услуга, а другият – на станцията предлагаща услугата. За да се осъществи комуникацията, клиентът и сървърът трябва да използват един и същ протокол. Поради различните идеологии при поточните и дейтаграмните сокети, произтичащи от спецификите на използвания транспортен протокол, алгоритъма на работа на двата типа е различен. При поточните сокети има изграждане на връзката и функциите за изпращане и получаване на данни не съдържат адреса на отдалечения възел.
Клиентската станция извършва следните действия за осъществяване на комуникация:
1. Създаване на сокет и получаване на дескриптор от ОС.

2. Свързване на сокета към сървърен такъв.
3. Трансфер на данни.
4. Затваряне на сокета.
Сървърната станция извършва следните действия за осъществяване на комуникация:
1. Създаване на сокет и получаване на дескриптор от ОС
2. Обвързване на сокета с локален адрес и порт
3. “Слушане” за клиентски заявки и добавяне на заявките в опашка за обработване
4. Приемане на заявка от опашката. (Създава се нов сокет по време на обмена)
5. Трансфер на данни
6. Затваряне на сокета
За да адресираме един сокет ни е необходимо да зададем мрежов адрес, порт, домейн на адреса. Това се постига с използването на структура от данни.

```
struct in_addr {unsigned long s_addr;};
struct sockaddr_in{
short sin_family; //AF_UNIX | AF_INET
u_short sin_port; // port number
struct in_addr sin_addr; // address
char sin_zero[8]; // padding
};
```

Вариант 2

1.Защо се използва резервиране на канала при MAC протокола na WLAN 802.11. Пример. ??????????????

Комплексно решение на проблема за управление на достъпа до безжични съобщителни среди при двете основни топологии предлага стандарта IEEE 802.11. MAC протокола при 802.11 е проектиран да работи с три вида съобщителни среди - два радио-канала в ISM диапазони 2.4 GHz(FHSS със скорости 1 и 2 Mbps и DSSS с 1, 2, 5.5 и 11 Mbps) и 5.1 GHz и третата съобщителна среда е дифузен инфрачервен канал с позиционно-импулсна модулация IrPPM (infrared pulse-position) и скорости от 1 и 2 Mbps.

IEEE 802.11 MAC протокола реализира две взаимно свързани функции на механизма на достъп: разпределена координираща функция DCF (distributed coordination function) и функция реализираща сканиране PCF (point coordination function). Разпределената координираща фукнкция се реализира с механизма CSMA/CA и е достъпна за‘Ad hoc’ и структурираните WLAN. За разлика от кабелните мрежи, където всички станции са свързани (могат да се “чуват” една с друга) и следенето на носещата с цел откриването на конфликти се реализира от предаващата станция, то при безжичните мрежи това е невъзможно поради ограничената свързваемост (ограничената излъчвана мощност) и ефекта скрит терминал (предаващата станция би “чувала” само собственото си предаване). Затова тук MAC протокола е полудуплексен и механизма на следене на носещата с цел откриване на зает канал и избягване на конфликт се реализира по два допълващи се метода - физическо и виртуално следене. Виртуалното следене на носещата се реализира от MAC подслоя и се базира на вектора за определяне състоянието на мрежата NAV (network allocation vector), поддържан от всяка мобилна и базова станция, и съдържащ информация за времето през което съобщителния канал ще бъде зает. Времената в NAV се задават от полетата ‘продължителност на обмена’ в служебните кадри RTS/CTS, използвани за резервиране на канала преди предаването на данните - фигура 8. По такъв начин се предотвратява явлението скрит терминал, като всички станции ‘чуващи’ предаващата (MH1) или отговора на приемащата (MH2) станция актуализират своят NAV отлагайки достъпа до общия съобщителен канал (Defer access). Появата на конфликт е най-вероятна по-времето на състезателният период (CW) при размяната на RTS кадри (конфликтите възникват в приемащата станция). Предаващата станция установява конфликта, по липсата на CTS кадър или ACK (опознаване) при конфликт на кадри с данни.

2.Какви са предимставта на IPv6 пред IPv4?

IPv4 адресът е 32 битово шестнадесетично число, което за удобство е разделено на 4 осем битови десетични числа разделени с точка. Проблемът на IPv4 е че адресите, които предлага са вече на привършване. Има само един начин да се разшири областта на IP адресите. Числото да стане по-голямо. IP адресите от IPv6 са вече 128 битови числа!

Освен проблема с изчерпването на номерата, IPv6 предоставя и някои други предимства, включително опростяване на рутиращата съвкупност и автоматична конфигурация на адресите. Протоколът има и предимства във връзка с мобилността и сигурността, като например вградена възможност за криптиране.

протокол от мрежово ниво за комуникационни мрежи, основани на предаването на пакети.

Версия 6 на Интернет протокола е създадена с цел замяната на версия 4, тъй като решава голяма част от проблемите, възникнали след широката употреба на IPv4:

- Поддръжка на многократно повече IP адреси в сравнение с IPv4;
- Plug and Play настройване с или без DHCP;
- По-добро оползотворяване на честотната лента използвайки multicast и anycast без broadcast;
- По-добра поддръжка на нивото на качество за всички приложения;
- Подобрена поддръжка за разширения и възможности за по-добро маршрутизиране;
- Нативна информационa структура за безопасност както за пакети с данни така и за контролни пакети;
- Подобрена мобилност с бързо сменяне на каналите, машрутна оптимизация и йерархична мобилност.

3.Опишете явлението „задръстване" при TCP протокола и как се преодолява?

Когато голямото количество трафик преминаващо през дадена връзка, създаде задръстване, част от пакетите биват задържани (в опашки) за известно време или биват отхвърлени. Това от своя страна води до повторно предаване на отхвърлените, увеличаване на забавянията и в крайна сметка до лоша производителност. Технологията за регулиране скоростта на предаване по TCP протокол, реагира преди да е настъпило задръстване като по този начин действително намалява до минимум появата на големи забавяния.

С контролиране на потвържденията към изпращача и управляване на анонсираните размери на "прозореца", механизма за регулиране скоростта на предаване по TCP протокол диктува на изпращащия компютър с каква скорост да предава данните, за да бъдат предотвратени образуванията на задръствания (респ. намалени забавянията, породени от задържане на пакетите в опашките на маршрутизаторите). Всичко това води до намаляване на забавянията по мрежата и ускоряване работата на всички приложения.

Вариант 3

1.Пример за процедура за свързване на 2 GSM модема.??????????????????

GSM комуникацията сериозно се различава от стандартната телефония. Тя използва радио вълни за преносна среда, затова са запазени някои основни идеи от телефоните (напр управлението чрез AT комадни и сериен интерфейс за достъп до оборудването). Най-важната характеристика на GSM комуникацията е, че това е мрежа от клетки. GSM използва най-близката клекта за предаване на информацията. Основните елементи на GSM мрежата са: мобилна станция (MS), модул за идентификация на потребителя (SIM), базова трансийверна станция (BTS), контролер на базова станция (BSC), транскодер и адаптор (TRAU), център за превключване на мобилни услуги (MSC), домашен регистър (HLR), гост регистър (VLR), регистър за идентификация на оборудване (EIR), публична наземна мобилна мрежа (PLMN). MS е всяко устройство, което е краен клиент в GSM мрежата. SIM се използва за идентификация в системата, за определяне на права, таксуване. BTS се грижи за радиовръзката между мрежата и мобилните станции. BSC е централно устройство на група от съседни BTS и изпълнява контролиращи функции. Понятието BSS - базова подсистема - се отнася до BSC и прилежащите му BTS. TRAU за компресия на данните и управление на честотния спектър за предаване. MSC за маршрутизиране на информацията, пристигаща от множество BSC. HLR е голяма БД за потребителите на мрежата. VLR-да не се претоварва HLR. Тя съдържа и/ята за текущо вързаните потребители към мрежата. EIR е база от данни на идентификационните номера на телефоните, не на потребителите(при кражба на gsm).

2.Опишете основните елементи на протокола CSMA/CA

CSMA/CD – Carrier Sense Multiple Access Point

•PCF (Point Coordination Function) –централизиран, детерминиран достъп до съобщителната среда-стартира след PIFS; При PCF базовата станция сканира мобилните хостове за наличие на кадар за предаване (Beacon), след което станциите предават или получават кадър в зависимост от наличната заявка.

•DCF (Distributed Coordination Function) – осигурява разпределен състезателен достъп до съобщителната среда–стартира след DIFS.

DIFS (Distributed Inter Frame Space)–интервал от време между два периода на DCF;

(Carrier Sense Multiple Access with collision avoidance) - протокол, изискващ от устройствата предварително да проверяват средата за предаване на информация. Множествен достъп с откриване на носещата честота и разпознаване на конфликтите. Протоколът допуска, че всички мрежови възли са равноправни. Всички предават по общата комуникационна среда, като се състезават помежду си. Възлите в мрежата сами разпознават дали шината е заета или свободна. CA е Collision Avoidance, т.е. при тях механизма изключва едновременното предаване на два компютъра. Излъчването в ефира става със заявка и потвърждение, при което се избягват колизиите между отделните компютри.

3.Опишете протоколното въздействие на метода GET при HTTP

Протокола HTTP версия 1.1 поддържа общо 8 различни метода: GET, POST, HEAD, PUT, DELETE, OPTIONS, TRACE, CONNECT. Най-често използваните методи обаче са GET и POST. Също така те имат най-голямо отношение към

Web програмирането. GET методът представлява команда за извличане на ресурс, указан от зададено URI или релативен път в рамките на Web-сървъра. Всичко, което прави Web-сървърът за извличането на статичен ресурс чрез GET заявка е да го прочете от файловата система и да го върне на клиентите в подходящ HTTP отговор. При извличане на динамичен ресурс сървърът изпълнява програмния код, който генерира ресурса и връща резултата от него в HTTP отговор. Пример:

```
GET /InetJava-2002-program.html HTTP/1.1
Host: inetjava.sourceforge.net
Accept: */*
Accept-Language: bg
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0(compatible;MSIE 6.0; Windows NT 5.0)
Connection: Keep-Alive
Cache-Control: no-cache
```

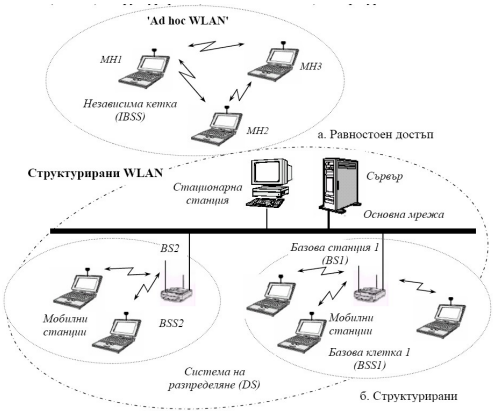
Тази заявка ще ви върне програмата на курса Интернет програмиране с Java. При HTTP GET заявката ако към искания ресурс трябва да се зададат параметри, това става като към URI-то се добави въпросителен знак, а след него двойки от вида <име на параметър>=<стойност>, като двойките от този вид се разделят една от друга със &. За избягването на някои непозволени символи се използва така нареченото URL-кодиране.

Вариант 5

1.Какви съобщителни среди се използват при WLAN. Дайте примери.?????????????

Комплексно решение на проблема за управление на достъпа до безжични съобщителни среди при двете основни топологии предлага стандарта IEEE 802.11. MAC протокола при 802.11 е проектиран да работи с три вида съобщителни среди - два радио-канала в ISM диапазони 2.4 GHz(FHSS със скорости 1 и 2 Mbps и DSSS с 1, 2, 5.5 и 11 Mbps) и 5.1 GHz и третата съобщителна среда е дифузен инфрачервен канал с позиционно-импулсна модулация IrPPM (infrared pulse-position) и скорости от 1 и 2 Mbps.

2.Каква е разликата в MAC протокола при Ad-hoc и структурирани WLAN при IEEE 802.11???????????????????



При безжичните локални мрежи са се наложили две основни топологии: мрежи с равностоен достъп (Ad Hoc) и структурирани (Infrastructure WLAN) – на фигурата.

Мрежите с равностоен достъп от типа “Ad Hoc” се използват в случаите на изграждане на временни WLAN, или когато в помещанието не съществува предварително изградена инфраструктурана кабелна LAN. Всяка станция в мрежата може да установява връзки от типа ‘peer-to-peer’ с другите станции, като използваните MAC протоколи реализират множествен достъп до съобщителната среда. Реализирането на надежден канал и напълно свързана мрежа при голями помещения (покриването на относително големи области) и голям брой мобилни станции (MH - mobile host) е трудно осъществимо без ретранслиране на излъчените пакети, поради ограниченията в излъчваната мощност. Това налага разделяне на мрежата на кетки (BSS - Basic service set) с принадлежащи MH, като към всяка клетка има базова станция (BS - точка за достъп), през която се реализира обмена с останалите клетки. Този принцип е в основата на топологията на структурираните мрежи. Връзката между отделните BS от една страна и съществуващите компютърни мрежи (ако има такива) от друга, се реализира посредством традиционните кабелни локални мрежи (наричани основна мрежа - Backbone Network), а връзката между BS и MH се реализира от безжична съобщителна среда. По този начин се постигат две цели: разширяване обхвата на безжичните мрежи в големи помещения и области, и интегрирането им към съществуващи инфаструктури на кабелни мрежи и интернет. Към всяка базова станция може да бъде асоциирана клетка или област от помещение, в която мобилните станции могат да поддържат комуникация зависима от базовата станция, като трафика предназначен за отдалечени MH принадлежащи на други базови станции се препредава от базовите станции по основната мрежа. При движение на мобилните станции, когато MH излезе от обхвата на текущата базова станция и попадне в обхвата на друга, трябва автоматично да се асоциира към новата клетка. Това явление е извесно като ‘roaming’ или ‘handoff’ (подобно на клетъчните комуникации).

3.Опишете методите за разпределяне на съдържанието при WWW / 3. HTTP, методи и взаимодействия на протоколния стек.??????????????????????????????????????

http (hyper text transfer protocol) е стандартен протокол на приложно ниво, позволяващ работа със структурирани разпределени данни. Той е създаден за да обслужи хипермедийна информация (хипертексови документи, образи, звук и специални ефекти) в световната мрежа за хиперизация WWW. Актуалната стандартна версия на протокола е HTTP 1.1. Това е обектно-ориентиран протокол, работещ на принципа клиент-сървър. Той се състои от методи за достъп (команди на прокола), които се използват като индикатор за типа на заявката за обслужване, подадена от клиента към сървера. Обслужването на заявките в протокола за трансфер на хипертекст става по дисциплина за обслужване известна като Унифициран Идентификатор на Ресурсите-URI(uniform resource identifier). Тя осъществява достъп до обекта по неговия адрес, определен чрез съответен URL(uniform resource locator) или достъп до ресурса по име чрез унифицирано име на ресурса-URN(uniform resource name). Обменяните съобщения м/у клиента и сървера чрез протокола HTTP във формат MIME(multiple internet mail extension). Всеки диалог в протокола за трансфер на хипертекст се състои от заявка на клиента към сървъра и отговор от сървъра. При предаване на т.н. пълна заявка (full-request) и съответен пълен отговор(full response) се използва формат на съобщението определен от докумунтите RFC 822.

Разпределяне наресурсите при WWW - Често при достъпа до изходния Web сървър отговора се забавя поради следните причини: •по пътя между клиента и сървъра има ниско скоростна линия;

•на пътя между клиента и сървъра има претоварен възел;

•Изходния Web сървър е претоварен.

За решаване на проблема едни и същи ресурси се разполагат на различни сървъри, като заявките се пренасочват към бързо достъпния.

HTTP протоколът поддържа различни методи за заявка от страна на клиента. Методът на заявка служи, за да укаже на сървъра какво действие трябва да извърши над заявения ресурс. По-важните методи са:

- ***GET*** – заявка за получаване на ресурс,
- ***POST*** – заявка за предаване на данни към даден ресурс,
- ***PUT*** – заявка за поставяне на ресурс на даден URI,
- ***DELETE*** – заявка за изтриване на ресурс.

Структурата на заявката включва:

- заглавна част (header)
  - о поддържани типове (MIME),
  - о поддържани кодирания (encoding),
  - о поддържани кодови таблици (charset),
  - о дата и час,
  - о идентификация на потребителя,
- тяло на съобщението (body)

Вариант 6

1.Какво негативно явление се избягва при размяната RTS/CTS на при WLAN. Дайте пример. ??????????????????

От лекции: С размяна на служебните кадри RTS и CTS се резервира канала за предаване на кадър с данни от A към B и връщане на AKN от B към A. Това се реализира чрез отмяна на предаването на съседите на A(C) и B(D) за интервал от време NAV-RTS за A и NAV-CTC за B.

Заявка за предаване на данни – RTS (Request to Send) Състояние ”логическа 1” на тази шина показва, че DTE е готово да предава данни към DCE. Състояние „логическа нула” указва, че DTE няма готовност да предаде данни.

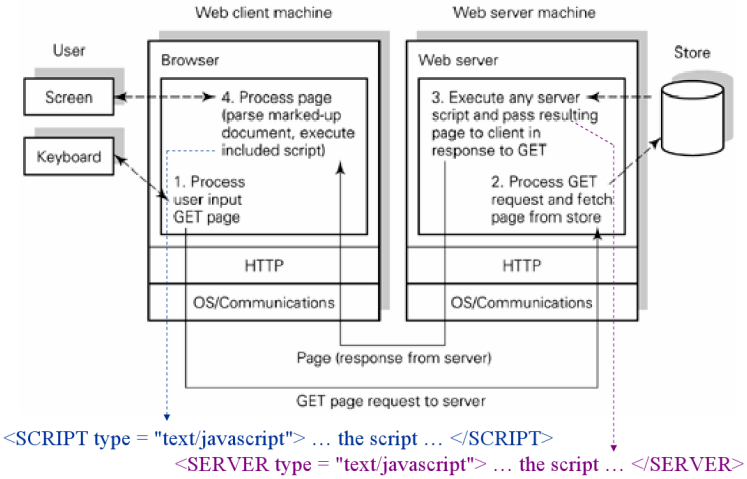
Готовност за приемане на данни – CTS (Clear to Send) Състояние ”логическа 1” на тази шина показва на DTE, че DCE е готово да приема данни. Този сигнал се изпраща в отговор на заявката за предаване на данни.

MAC протокола е полудуплексен и механизма на следене на носещата с цел откриване на зает канал и избягване на конфликт се реализира по два допълващи се метода - физическо и виртуално следене.

Виртуалното следене на носещата се реализира от MAC подслоя и се базира на вектора за определяне състоянието на мрежата NAV (network allocation vector), поддържан от всяка мобилна и базова станция, и съдържащ информация за времето през което съобщителния канал ще бъде зает. Времената в NAV се задават от полетата ‘продължителност на обмена’ в служебните кадри RTS/CTS, използвани за резервиране на канала преди предаването на данните - фигура 8. По такъв начин се предотвратява явлението скрит терминал, като всички станции ‘чуващи’ предаващата (MH1) или отговора на приемащата (MH2) станция актуализират своят NAV отлагайки достъпа до общия съобщителен канал (Defer access). Появата на конфликт е най-вероятна по-времето на състезателният период (CW) при размяната на RTS кадри (конфликтите възникват в приемащата станция).Предаващата станция установява конфликта, по липсата на CTS кадър или ACK (опознаване) при конфликт на кадри с данни.

2.Клиент/Сървър взаимодействие, включващо script processing

Клиент –сървър взаимодействие включващо 'script processing'.



Взъимодествието между клиент и сървър включващо изпълнението на скрипт протича по следният начин:

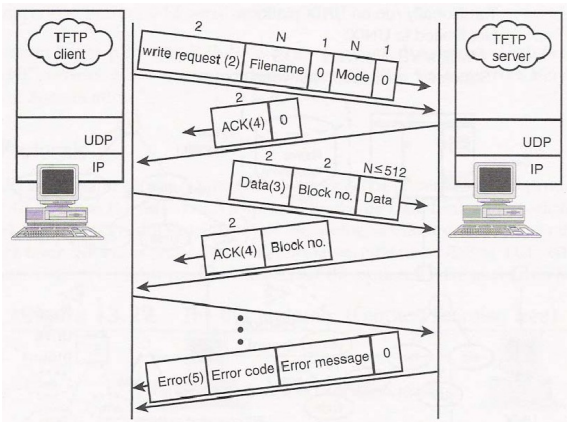
1.Клентът отправя заявака за определена страница (чрез GET) към сървъра.

2.Сървърът приема заявката и съответно проверява страницата за наличието на скрипт, който трябва да се изпълни.

3.Скриптът се изпълнява от сървърът и резултат се изпраща до клиента като отговор на неговата GET заявка.

4. Клиентът приема изпратената от сървъра страница, включваща резултата от изпълнението на скрипта.

3.Интернет приложение TFTP. Пример



TFTP (Trivial File Transfer Protocol – тривиален протокол за прехвърляне на файлове) използва се за прехвърляне на файлове, най-често когато в мрежата имаме хостове без налично на тях дисково пространство, им се дава възможност да се заредят операционна система от друга машина изтегляйки файловете през TFTP.

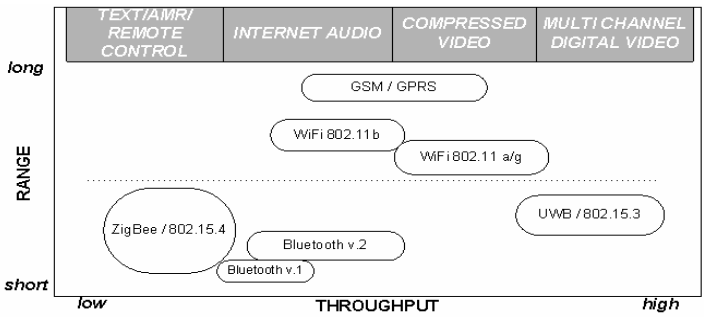
TFTP е много прост протокол за предаване на данни. TFTP подпомага четенето и записването на данни. Не са налични много функции на по-разпространеното FTP, като приблизително безполезните chmod, съобщаването на налични данни или потребителска дейност. TFTP е приложен мрежов протокол, позволяващ двустранен трансфер на файлове. Тъй като е опростен (не поддържа работа с директории и някои други възможности на FTP), се използва предимно за съхранение или възстановяване и актуализиране на операционните системи на рутерите и други управляеми мрежови устройства. Протоколът TFTP е опростен вариант на FTP – използват се транспортните услуги на протокола UDP с приложение на собствен метод за доставка на данните. TPTP – разделя файла на равни блокове с размери 512 байта и използва старт-стопен режим на предаване блок по блок с получаване на положителна квитанция за правилно приемане.

Мотивацията за развитието на TFTP беше края на потребителските системи или конфигурирането през мрежата. В TFTP се съдържа:

- Пакетно ориентиран протокол
- Всеки пакет се потвърждава
- Четене и запис на данни на сървър
- Не е подредено в списъци съдържанието
- Не е достоверна, компресирана и кодирана
- Максималната големина на данните е 32 MBytes (16 MBytes при някои изпълнения)

Вариант 7

1.Каква е разликата при WLAN базирани на инфрачервен канал LOS и дифузен канал??????????????????



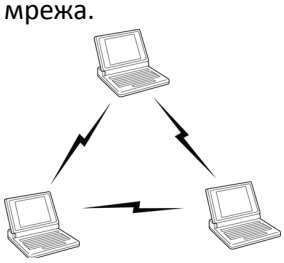
WLAN – безжични локални мрежи

Когато се налага използването на висока пропускателна способност при изискване за мрежова свързаност между устройствата в относително малки пространства и площи, тогава се използва WLAN по стандарта IEEE 802.11. На фигура 2.1 е показана зависимостта на пропускателната способност, която се изисква (нанесена по абсцисата) и обхвата на

действие на дадената технология (по ординатата). Засичането дава обсега на действие на различните системи за безжичен достъп, които са актуални в момента.

2. Опишете MAC подслоя използвайки Ad-hoc (IEEE 802.11).??????????????????????

Възможни са няколко режима на работа на крайните устройства, всеки от които се характеризира с определена функционалност и настройка на параметрите, за да може да бъде настроена една безжична мрежа.



AD-HOC (всеки с всеки)

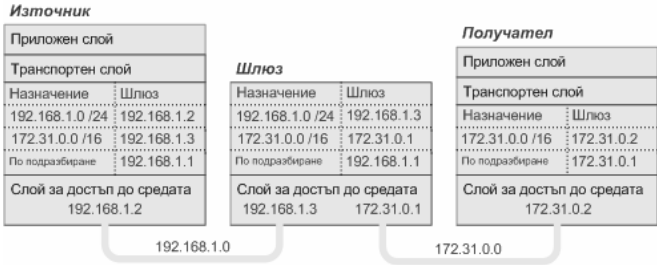
В този режим, който е най-често срещан при връзка на мобилни устройства помежду си (laptop, palmtop и др.), не е необходимо определено безжично устройство в мрежата да синхронизира достъпа до канала. Това не е често срещан режим на работа поради ниската производителност и възможността за колизии.

'Ad hoc' топологията реализира равностоен достъп до мобилните хостове MH при липса на инфраструктура. Мрежите с равностоен достъп от типа "Ad Hoc" се използват в случаите на изграждане на временни WLAN, или когато в помещанието не съществува предварително изградена инфраструктурана кабелна LAN. Всяка станция в мрежата може да установява връзки от типа 'peer-to-peer' с другите станции, като използваните MAC протоколи реализират множествен достъп до съобщителната среда.

3. Какво означава таблица на маршрутизиране? Дайте пример при автономни системи.

Основният принцип на мрежовият слой е доставянето на пакетите от техният източник, до местонахождението им. При това предвижване пакетите могат да минат през няколко на брой междинни маршруизароти. Като всеки един от тези маршрутизатори трябва да избере следваща стъпка за предаването на пакета, въз основа на записана в него "маршрутизираща таблица". Тази таблица сдържа две основни полета "Destination" и "Gateway". Полето "Destination" определя адресът от който пристига пакета, а полето "Gateway" адреса на където той следва да бъде препратен. Като освен това могат да се отчитат и раличните интерфейси. В общият случай при приситгането на пакет, рутера започва да претърсва своята рутираща таблца от нейното начало, като се претърсва по следният алгоритъм: Първо се търси съвпадение на "Destination" адреса с този от който пристига пакета, ако няма пълно съвпадение се търси за мрежата от която пристига пакета. След това се проверява за Gateway съвпадаща с адреса на получателя на пакета, и ако няма съвпадение, се търси (в таблицата) за мрежата на получателя на пакета. Ако се открие някой от търсените записи в таблицата, пакета се препраща към съответният следващ рутер към самият хост (ако той фигурира в таблицата). Ако няма съвпадения се проверява дали в таблицата има указан Gateway по подразбиране, към който да се изпращат пакети чийто адрес на източник или на получарел не са известни, ако няма такъв, то пакета се връща.

Процесът на придвижването на пакет информация от един физически мрежови сегмент към друг се нарича маршрутизиране (routing). Маршрутизирането управлява процеса на препращане на логически адресирани пакети информация от техния източник до крайната им цел посредством междинни устройства, наречени маршрутизатори. Маршрутизаторът е интелигентно устройство. То взима решения на базата на т.нар. маршрутизираща таблица, за да избере най-добрия маршрут за дейтаграмата по пътя й до крайния получател. Поради тази причина конструирането на маршрутизиращата таблица е важен етап за ефикасността на маршрутизирането.



В маршрутизиращата таблица се поддържа списък на най-добрите пътища до различни мрежи. За определянето на понятието най-добър маршрут се използват т.нар. мерни единици (metrics). Мерните единици представляват или оценка, или стойност на даден параметър на мрежовата връзка. Най-често използваните в маршрутизиращите протоколи мерни единици са:

• **Hop count** (брой преходи). Това е най-разпространената мерна единица. Тя измерва броя маршрутизатори, през които преминават пакетите от мрежата източник до режата получател.

• **Delay** (закъснение). Тази единица измерва времето, необходимо за придвижване на пакет от мрежата източник до мрежата получател. Факторите, определящи закъснението, могат да включват пропускателна способност, брой заявки, обслужвани от всеки маршрутизатор, мрежови задръствания и разстоянието между двете мрежи.

• **Bandwidth** (пропускателна способност). Тази единица измерва наличния капацитет на мрежовата връзка. Например, 10Mbps Ethernet връзката е за предпочитане пред 64K връзка.

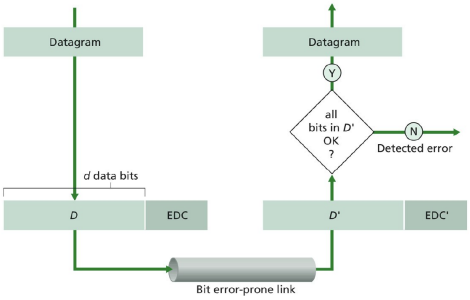
• **Reliability** (надеждност). Тази единица осигурява оценка на надеждността на мрежовите връзки. Някои връзки излизат от строя по-често, отколкото други, така че се предпочитат по-надеждните връзки. Друг параметър на надеждността е времето, необходимо за възстановяване на повредена връзка.
• **Communication cost** (цена на комуникацията). Понякога доставянето на информация за най-краткото възможно време не е основната цел. Често целта е минимизиране цената на мрежовия транспорт.

Автономни системи

Автономните системи (AS) представляват група от IP мрежи и маршрутизатори под контрола на една или няколко организации, придържащи се към единни, ясно дефинирани правила за маршрутизиране в интернет (RFC-1930). Обикновено организациите, които контролират AS, са доставчиците на интернет услуги (ISP). Всяка автономна област притежава уникален AS номер, който се отпуска от организацията IANA. Автономните области се разделят на три групи:
• ***Multihomed AS*** – това са автономни системи, които имат връзка към повече от един доставчик (ISP). По този начин автономната система остава свързана дори при напълно отпадане на някой от доставчиците.
• ***Stub AS*** – това са автономни системи, поддържащи връзка към един - единствен доставчик (ISP).
• ***Transit AS*** – този тип автономни системи осигуряват връзка между мрежи, свързани към тях. Доставчиците на интернет услуги (ISP) са винаги автономни системи от този тип.

Вариант 8

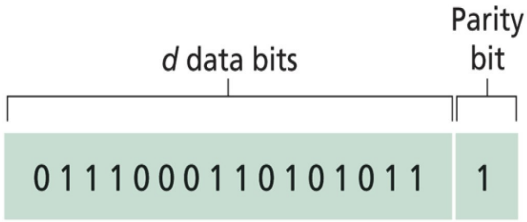
1.Какви методи за откриване и коригиране на грешки се използват в КМ ??

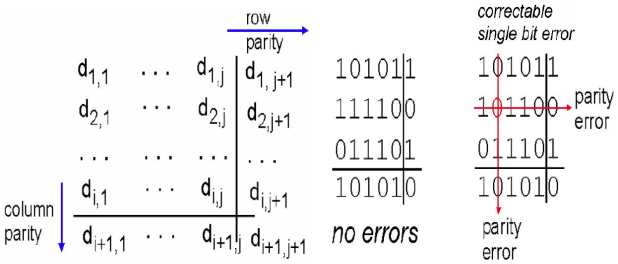


С добавяне на *EDC (Error Detection and Correction)* в предаващия хост се цели откриване или окриване и коригиране на грешки. Дължината на EDC зависи от BER на съобщителния канал.

Методи:

- Контрол по четност: При този метод има добавен един бит *EDC*. При предаване се добавя един бит равен на сумата по модул 2 на всички предавани бита d. В приемащия хост се изчислява сумата по модул 2 на всички приети d'бита и се сравнява с d'+1 бит, ако те не съвпадат има грешка в един бит. При грешка в два бита обаче контрола по четност няма да я открие.





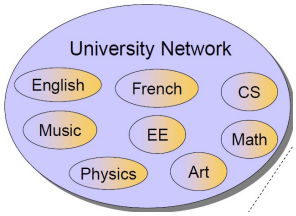
- Двумерен контрол по четност (Блоков контрол по четност): При този метод предаваният кадър от *d* бита се разделя на *i* реда и *j* стълба, като за всеки от тях се прави контрол по четност. Това позволява при възникване на грешка по време на предването, сгрешения бит да се открие и след неговото инвертиране се коригира.

- *Посредством **Retransmission Timer** TCP управлява **error control and congestion control** (приема се че грешките са вследствие на задръстване в опашките на маршрутизаторите);

2.Защо се използват мрежовите маски? Дайте пример за използване на мрежова маска при корпоративни мрежи.

Освен разделянето на адресите на класове е предвидено и друго средство за по-нататъшно разделяне на всяка мрежа на подмрежи. Това се осъществява чрез маска - subnet mask. Маската е 32-битово число, което се състои от последователност от единици, последвана от последователност от нули. Полето с единици започва от най-старшия бит. Винаги поредиците от единици и от нули са непрекъснати и тази от нули следва тази от единици. (Не може да има единици след започване на нулите. Например "11111100000" е част от валидна маска, "1110000110" – не). Например, за мрежа от клас B маската може да има вида 11111111 11111111 11111111 00000000 или представена за удобство 255.255.255.0. Полето с единици определя мрежовата част на IP адрес, към който се прилага маската, а полето с нули - адреса на хоста. Чрез мрежова маска се извършва

преместване на разделителната линия между двете части на адреса, дефинирана от съответния адресен клас A, B или C. Чрез прилагане на побитово "И" между адреса и маската се отделя мрежовата част. Така можем, притежавайки мрежа от даден клас, да я разделим на няколко мрежи. Разделянето на подмрежи подпомага работата на мрежовото оборудване и ограничава broadcast домейните.



'Subneting' се използва за идентифициране на подмрежите в корпоративните (университетските) мрежи, като отвън се виждат като една мрежа с общ IP адрес(128.143.0.0). Във вътрешното пространство част от полето на хостовете се използва за адресиране на подмрежите.

С цел улесняване на администрирането в големите мрежи (корпоративни, университетски и т.н.), които всяка година се разширяват с нови хостове и нови мрежови приложения се препоръчва разделянето им на подмрежи. В подмрежите се групират компютри с еднотипни приложения, адмистративни и бизнес функции и т.н.

Пример:

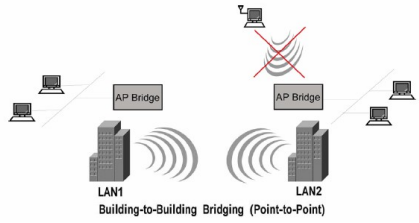
128.143.137.144 е IP адреса на хоста(144) от подмрежата 137

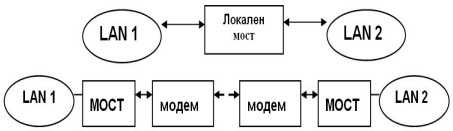
255.255.255.0 (или ffffff00) мрежовата маска

3.QoS – същност и методи ? Вариант 0/9

Варинат 10

1. Какви функции изпълнява устройството мост (bridge) между две LAN. Дайте пример.





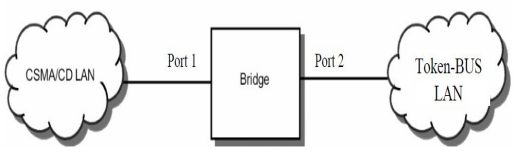
Bridge е предназначен за прозрачно свързване на 2 мрежови сегмента, като по този начин могат да се свържат безжично локалните мрежи на отдалечени офиси. Безжична връзка е възможна само между двете устройства, които работят в режим "AP Bridge", като по този начин те прехвърлят прозрачно всеки пакет от единия локален LAN сегмент към отдалечения.

Мостът предоставя основно управление на предаването на данни, като определя дали данните трябва да се прехвърлят в другия сегмент на мрежата или не. Съставя т.н. мостови таблици (bridge table) с физическите адреси на устройствата в мрежата, като ги научават при получаването на фрейм от съответното мрежово устройство.

Когато даден мост получи фрейм (формата на данните на вторият OSI слой), той преглежда физическия (MAC) адрес на получаващото устройство, проверява го в мостовата таблица и решава дали да го изпрати в другия сегмент или не. Процедурата е:

- Ако получаващото устройство е в същия сегмент, от където идва фрейма, моста няма да го изпрати в другия сегмент. Това се нарича филтриране.
- Ако получаващото устройство е в другия сегмент, а не в този от където е получен фрейма, то фрейма ще бъде изпратен към точния сегмент.
- Ако получаващото устройство е непознато (т.е. няма запис за него в мостовата таблица), фрейма ще бъде изпратен към другия сегмент.

Той комуникира на каналния слой като изолира физическия слой. Чрез него само добре формираните пакети се транспортират от един етернет сегмент до друг. Изолират се пакетни грешки. Не се транслират пакети ако не се знае дестинацията им. Основни видове са: 1)прозрачно свързване(transparent bridging) - използва се в етернет ЛМ. 2)свързване с маршрутизация от източника (source-route bridging) - маршрутът се определя от абоната в изходния пункт. Ползва се при token ring ЛМ. 3)свързване с преобразуване (translation bridging) - ползва се когато е необходимо да се преобразуват различаващи се формати на пакетите при предаване на данни по различни съобщителни среди (м/у етернет и token ring).



от лекции:

- Изолиране на трафик;
- Протоколни трансформации

2.Формат на HTTP заявка

HTTP – Hyper Text Transfer Protocol. HTTP представлява прост текстов протокол, който се използва за пренос на практически всякакъв вид данни, наричани събирателно **ресурси.** Обикновено HTTP протокола работи през

TCP/IP. Стандартния порт на HTTP е 80, но може да се използва всеки друг свободен TCP порт. HTTP се състои от:
- заявка (request) – съобщение от клиента към сървъра
- отговор (response) – отговор на сървъра на съобщението от клиента.
Формата на HTTP заявката е следният:
<метод> <URI> HTTP/1.1
<headers>
<empty line>
Има 3 основни елемента на HTTP заявката: **метод**, **URI** и **header** полета.
Метод на заявката - Метода описва вида на заявката, изпратена от клиента. Най-често използваните методи са GET и POST. Чрез GET метода клиента изисква някакъв ресурс от Web сървъра. POST метода служи за предаване на данни към сървъра. Имената на методите в HTTP заявките се изписват винаги с главни букви.
URI (Unique Resource Identifier) – Уникалния идентификатор еднозначно определя ресурса, над който ще оперира метода на заявката. Това е частта от URL, която стои след името на хост-а (сървъра) в URL.
HTTP/1.1 –версията на HTTP протокола, която ще бъде използвана за осъществяването на тази HTTP сесия.
Header полета - Полетата от заглавната част на заявката носят допълнителна информация, касаеща заявката и определяща изисквания относно ресурса, който се очаква да бъде върнат от сървъра.
Празен ред - всяка HTTP заявка завършва с празен ред.
Пример:
Ако искаме да заредим началната страница от сайта www.dir.bg, това може да стане със следната HTTP заявка:
GET / HTTP/1.1
Host: www.dir.bg
□

3.Кое позволява на два хоста да използват един и същи порт? (Кой механизъм позволява два хоста да използват един и същ порт на приемника при изграждане на TCP сесия към WEB сървър?)????????????

Други варианти

1.Опишете MAC подслоя при 802.3
IEEE 802.3 е стандарт дефиниращ физически слой и MAC подслой от канален слой за жичен етернет. Това обикновено е LAN технология с някои MAN приложения. Физическите връзки се правят м/у възлите и/или инфраструктурни устройства (hub, switch, router) чрез различни типове медни или други кабели. В iso/iec ieee 802.3 стандартите фреймовете на MAC подслоя съдържат полетата: 1.destination address (адрес на получателя) 2.source address (адрес на източника) 3.lenght/type data 4.data 5.FCS. Встъпителната част на кадъра (Фиг.46) е от седем байта, всеки от които има стойност $(10101011)_2$ и заедно с <началния ограничител> $(10101011)_2$ се използват за синхронизация и определяне началото на кадъра. MAC – адресът на възела-подател се ползва от получателя, за да определи от кой възел идва съобщението. MAC – адресът на получателя определя за кой възел е съобщението. Ако първият бит е 0, то кадърът е за един получател. Ако първият бит е 1, то кадърът е предназначен за група получатели (multicast адресиране). Ако всички битове са 1 – кадърът е предназначен за всички възли в мрежата (broadcast адресиране). В полето <дължина> се посочва дължината на полето <данни>. То може да е от 0 до 1500 байта. Ако данните са с дължина, по-малка от 46 байта, се използва полето <PAD> за допълване на поле <данни> до 46 байта. Ограничението от минимална дължина на поле <данни> 46 байта се налага, за да има достатъчно време да се върне заглушаващият сигнал при конфликт. Полето <FSC> се използва за кодиране на данните (без първите две полета) с шумоустойчив код (CRC – 32), което дава възможност на възела-получател да установи дали кадърът е приет с грешки или коректно

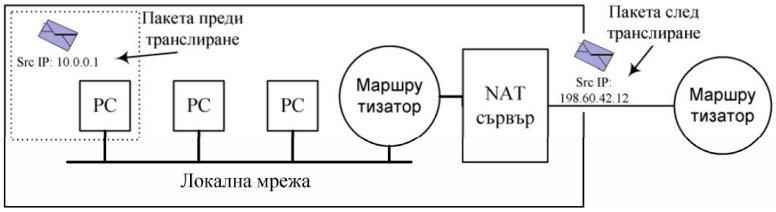
Встъпи-телна част	Начален ограни-чител (SFD)	MAC – адрес на В. по-лучател	MAC – адрес на възел-подател	Дължи-на	Данни LLC блок	PAD	Контрол но поле (FCS)
7	1	2 V 6	2 V 6	2	0 ÷1500	46/0	4 байта

Фиг. 46. Формат на кадър на MAC подслоя за протокол CSMA/CD.

В стандарта IEEE 802. 3. MAC - подслоя се управлява от протокол CSMA/CD – (Carrier Sense Multiple Access With Collision Detection) т. е. множествен достъп с откриване на носещата честота и разпознаване на конфликтите. Протоколът допуска, че всички мрежови възли са равноправни. Всички предават по общата комуникационна среда, като се състезават помежду си. Възлите в мрежата сами разпознават дали шината е заета или свободна.

2.Транслиране на адреси (NAT)

Когато даден пакет трябва да напусне мрежата на организацията, преди да бъде подаден към мрежата на доставчика на Интернет (ISP) се извършва транслиране на адреса. Механизмът на работа на NAT е показан на фигурата. В рамките на вътрешната мрежа всеки компютър има уникален адрес от вида 10.x.y.z. Когато пакет напуска мрежата на организацията той преминава през машина извършваща транслиране на адреси. Там частния IP адрес на източника (10.0.0.1) се заменя с реалния IP адрес отпуснат на организацията(198.60.42.12). Обикновено машината която извършва транслиране на адресите се комбинира заедно със защитна стена (firewall), а доста често това е и машината която извършва маршрутизирането навън.



След транслирането на адреса отговорът ще се получи не от истинския адресант, а от машината с IP адрес 198.60.42.12. Приетото решение на проблема е да се използва номерата за порт на източника. Всеки TCP или UDP пакет съдържа в себе си две 16 битови числа указващи номерата на портовете на източника и получателя. Машината която извършва NAT поддържа таблица с размер 65,536 реда, в която записва двойката (*source IP*, *source port*) за всеки изходящ пакет. След това се извършва замяна както на IP адреса така и на оригиналния порт номер на източника и пакета се пуска навън. Когато се получи отговора, порт номера на получателя ще се използва като индекс в NAT таблицата за да се извлече IP адреса и порт номера на компютъра от вътрешната мрежа до който е предназначен този отговор. Едно друго приложение на транслирането на адреси, което е открито в последствие е свързано с факта, че NAT скрива структурата на вътрешната мрежа и по този начин може да се използва за повишаване на сигурността. Въпреки, че NAT успява да намали натиска свързан с изразходването на IP адресите, това не е идеално решение и крие редица проблеми и недостатъци. Най-важните от тях са:

• Първо, транслирането на адреси нарушава архитектурния модел на IP, според който всеки IP адрес уникално идентифицира една единствена машина в интернет. Цялата софтуерна структура на Интернет се крепи на този факт. Посредством NAT, хиляди машини могат да използват адреса 10.0.0.1.

• Второ, NAT променя Интернет от безвръзково-ориентирана мрежа в единвид връзко-ориентирана. Проблема е свързан с това, че NAT поддържа информация за съответствието за всяка връзка преминала през него. Ако се получи срив в NAT машината, всички TCP връзки ще бъдат разрушени.

• Трето, NAT нарушава най-фундаменталното правило за разделянето на отделните слоеве. По този начин ако по-късно излезе нова версия на TCP която използва 32 битови номера на портове или бъде използван друг транспортен протокол, транслирането ще пропадне.

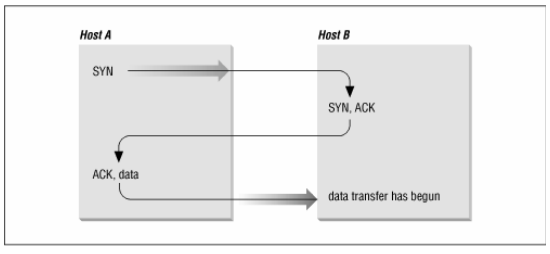
• Четвърто, някои приложения включват IP адресите в тялото на текста. Получателя извлича тези адреси и ги използва. Тъй като NAT няма никакви знания за съдържанието на пакетите не може да ги замени и всякакъв опит за връзка с отдалечения сайт ще пропадне. FTP е пример за такъв протокол и освен ако не се вземат допълнителни мерки няма да работи заедно с NAT.

• И последно, тъй като порт номерата са 16 битови, то най-много 65,536 машини могат да бъдат скрити зад един IP адрес. Реално те са по-малко тъй като част от порт номерата са резервирани. Решение на този проблем все пак е използването на повече от един реални IP адреси.

4.Как се реализира виртуален канал при TCP протокола?

Виртуалният канал се реализира чрез взаимодействието three-way-handshake.

При първоначално отваряне на връзката между два хоста е необходимо всеки един от тях да изпрати на другият началният номер (initial sequence number) на байтовата последователност, която ще изпраща и съответно да получи потвърждение за получаване на този номер. Процедурата за установяване на връзка се нарича Three Way Handshake, в нормалния случай е следната:



- Хостът, който отваря връзката, изпраща SYN сегмент. В същият сегмент клиентът задава номера на порта на сървъра, с който ще осъществява връзка и началният номер на потока байтове, който клиентът ще предаде към сървъра.
- Сървърът отговаря със собствен SYN сегмент, включващ началния номер на неговия поток байтове. В сегмента се съдържа и потвърждение ACK за SYN.
- Клиентът трябва да потвърди т.е. да прати сегмент с ACK за получаването на SYN.

За затваряне на връзката се използва процедура, при която прекратяването на връзка става по начин, предотвратяващ загубата на информация.

- Хостът, който затваря връзката, изпраща FIN сегмент.

- Другият потребител изпраща сегмент с потвърждение ACK и FIN.
Може връзката да бъде прекратена безусловно. Тогава се установява флаг RST, който в заглавната част идентифицира сегмет за прекратяване на връзката. Той се изпраща от протокола TCP, когато по връзката се получи некоректен сегмент, в който IP адреса и номерът на порта на изпращача или получателят не съвпадат с тези на съответната връзка.

5.Опишете функциите на firewall.

Това е компютърна система, която има не по малко от два интерфейса *(dual homed gateway)* и е специализирана да контролира информационния обмен между две обособени части от компютърната мрежа, имащи различни нива на сигурност**. Функциите й са**:
1)Анализ на изходящия и входящия информационен поток и вземане на решение кои негови части да бъде пропуснати или не;
2)Замяна на адресната информация във входящите и изходящите пакети, за да се осигури анонимност на хостовете от защитената група;
3)Водене на дневници за информационния поток със записи на събитията, които отговарят на критериите за повишен риск.
//Филтпипапе на пакетите *(Packet filtering firewalls)* е пропускането или не на даден пакет в зависимост от стойността на определени полета в заглавната му част. Най-често това са полетата за тип на протокола (TCP, UDP, ICMP и т. н.), за номер на порт на източника или на приемника, за мрежовия (IP) адрес на източника или на получателя (в случая много често става дума за група адреси) или за някаква комбинация от критерии за тези полета. Много често за подобно филтриране не е необходимо използването на специализирана система за защитна стена, а е възможно то да се извърши в маршрутизаторите дори без за това да се изисква закупуването на допълнителен софтуер.
Динамичен контрол **на** ***пакетите*** - анализира се състоянието на връзката между защитения и външния хост, т. е. контролът обхваща и част от транспортното ниво. Защитената мрежа е отворена за даден поток от пакети само през ограничени периоди от време.
Шлюзове на транспортно ниво-реализира контрол на транспортно ниво. При нея защитната стена проверява допълнително дали дадена връзка може да бъде отворена или не от гледна точка на мрежовите адреси на източника и приемника, номерата на портове на източника и приемника, типа на протокола, времето от деня, потребителя, паролата. Предимство на защитата чрез шлюз на транспортно ниво е нейната пълна прозрачност за приложните програми. Много трудно да се реализира пробив с фалшифициране на мрежов адрес.
Шлюзове на приложно ниво - всички заявки за ползване на външни ресурси се отправят към специализираната система, реализираща защитната стена. От своя страна тази система изпраща заявка към съответния външен ресурс и го доставя на клиента. Пример за шлюз на приложно ниво е така наречения proxy *server.* Предимствата на този подход са изолацията на потребителя от външните ресурси, възможност за идентифициране и определяне на правата за достъп на потребителя при свързването му към *прокси сървера,* възможност за водене на подробни дневници за информационния обмен. Недостатък на *прокси сървера* при използването му като защитна стена е необходимосгга в съответната приложна програма да е предвидено конфигуриране за работа в този режим.
Преобразуване на мрежовите адреси- във всички пакети от изходящия трафик към външния свят, като адрес на източника се използува един или няколко IP адреса на защитната стена. Това е едно много ефикасно средство за скриване на мрежовите адреси на защитените хостове, което силно затруднява атаките срещу тях. Преадресирането често е наложително и поради факта, че защитената мрежа използва адреси, резервирани за частни интернет мрежи (от 192.168.0.0 до 192.168.255.255), които в глобалната мрежа не се маршрутизират.
Преобразуване на номерата на портове - във всички пакети от изходящия трафик към външния свят реалният номер на порта на източника е заменен с друг номер. Прилага се предимно за номерата на портовете на източника от пакетите на защитения хост, когато той е клиент.

6. MAC модел 802.4

Този подслой използва протокола Token Bus. Достъпът се реализира чрез управляващ маркер. Това е специален кадър – щафета, който се предава от възел на възел.

Встъпи-телна част	Начален раздели-тел	Управ-ление	MAC – Подател	Адреси Получа-тел	Данни	Контрол -но поле FCS	Краен раздели-тел
1	1	1	2 или 6	2 или 6	0 ÷8182	4	1 байт

Само възелът, който притежва маркера има право да предава данни към останалите, като всеки възел знае адресите на съседите си. При инициализация на мрежата пръв има право да притежава маркера и да предава възелът с най-голям адрес.
Всеки възел владее маркера за определено време, след което го предава на съседа с по-малък адрес. За това време се предават кадрите (Фиг.), с данните към възела, за който са предназначени. Когато даден възел няма кадри за предаване, маркерът се предава на следващия възел. След като маркерът се изпрати към следващия възел се получава потвърждение за получаването му. Ако след второто изпращане на маркера не се получи потвърждение, се изпраща специален кадър "кой е следващият". Ако и тогава не се получи потвърждение, в шината се изпраща запитване "търся заместник". Очаква се произволен възел да се обади и да приеме маркера. По протоколът Token Bus може да се използва приоритетна схема. Някои възли могат да се изключат и да не получават право на маркер за предаване, а само да приемат. Недостатък на този протокол е, че локалната мрежа трудно се реконфигурира, защото трябва да се пренастройват и описват съседните възли.

8.Какви методи за модулация се използват при предаване на данни в WLAN??????????????

С утвърждаването си през 1997 година стандартът съдържа спецификации за поддръжката на скорости 1 и 2 Mb/s за инфрачервения канал, както и разширяващите по спектър FHSS и DSSS в радио обхвата 2,4 GHz на ISM.
През 1999 година излизат две допълнения към стандарта, които засягат нови методи на модулация позволяващи по-високи скорости на предаване. Тези допълнения са:
– IEEE 802.11a за ISM 5 GHz и скорости от 6, 9, 12, 18, 24, 36, 48, и 54 Mb/s
– IEEE 802.11b за ISM 2,4 GHz и скорости от 5,5 и 11 Mb/s при DSSS.

FHSS в обхвата 2,4 GHz на ISM

Разширяването по спектър чрез скачаща честота (FHSS – Frequency-Hopping Spread Spectrum) се нарича метода по който сигнал, с относително тясна честотна лента, се предава по канал с няколко пъти по-широка честотна лента и разделен на подканили, като често се сменят под каналите на предаване (подскоци). Честотния обхват 2,400 – 2,485 GHz е разделен на 79 канала, като средата на първия канал се намира на 2,402 MHz, средата на всеки следващ канал се намира на 1 MHz отстояние от предходния, и така до последния канал, чиято среда се намира на 2,480 MHz. Номера на канала при всеки скок се избира по специална таблица, съгласно изискването за минимално отстояние от 6 MHz между отделните скокове. Стандартът е предвидил три такива таблици, чиито множества от стойности нямат съвпадения, позволявайки разполагането на три отделни FHSS канала в рамките на 2,4 GHz ISM обхват.

DSSS в обхвата 2,4 на ISM

Разширяване по спектър чрез пряка последователност (DSSS – Direct sequence spread spectrum)се нарича метода по който канал с относително ниска скорост на данните се смесва с канал с по-висока скорост на данните и предварително дефинирано съдържание. По високоскоростния канал с 11 пъти по-висока скорост се предава 11 битов шумоподобен (PNC – Pseudo Noise Code) код, наречен код на Баркър.

9.Какви протоколи се използват при приложение e-mail. Примери

Ел.поща е мрежова услуга, чрез която всеки потребител с компютър, свързан към глобалната компютърна мрежа, може да обменя съобщения с всички потребители на мрежата. Обикновено обменяната на информация е в текстов формат (известен като ASCII). Съществуват също така възможности за компресиране на предаваните файлове, което улеснява изпращането и получаването на големи по обем масиви от данни.
За обмен на данни чрез ел.поща се използват множество протоколи по-важните от които са:
*SMTP (Simple Mail Transfer Protokol) – този протокол осигурява обмен на писмата между програмите, предназначени за изпращане и получаване на ел.поща. Протоколът SMTP приема съобщение и използва протокола TCP, за да го предаде на SMTP модула на хоста – получател. Всяко съобщение се състои от две части:
- Заглавна част (header), съдържаща информация за доставката и обработка на съобщението;
- Тяло (body) – самото съобщение.
Заглавната част и съобщението са разделени с празен ред. Заглавната част съдържа полетата:
"Received", "Date", "From", "Subject", "Sender", "Reply to", "To", "Bcc", "Comment", "X Mailer".
*POP3 (post office protokol Version 3) – този протокол е предназначен за прехвърляне съдържанието на пощенската кутия на потребителя от пощенски сървър към персоналния компютър на потребителя.
*IMAP4 (Internet Message Access Protokol Version 4) – протоколът осигурява връзка между пощенски сървър и потребителски работни станции или персонални компютри чрез динамичен достъп до пощенскатанкутия на сървъра. Разликата с протокола POP3 е, че прочетените писма остават на съхранение в пощенския сървър, а не се прехвърлят в локалната система. Това позволява на потребителя да има достъп до пощенската си кутия от различни клиентски компютри.

*UUCP (Unix to Unix Copy) – опростен протокол за обмен на електронни съобщения между компютърни системи, работещи с Unix операционни системи.

10.Описание на каналния слой при 802.3??????????????????????????

ЛМ Етернет използва метода на достъп МДОН/РК. Нейната спецификация е обявена в средата на 70те. Американския институт на инженерите по електротехника и електроника (IEEE) спонсорира проекта 802, по която се изготвят стандарти за ЛМ. След няколко модификации за ЛМ е шинна топология на базата на МДОН/РК става известен като 802.3. той описва функциите на физическия и каналния слой от метода OSI.Формат на кадъра-преамбюл7/начало на разделителя на кадъра1/Адреси на получателя 2или6/Адрес на източника 2или6/Дължина на данните2/Данни 0-1500/PAD 0-46/Контролна сума4
Кадърът започва със синхронизиращи байтове, наричани още преамбюл-поредица от битове 10101010, началото на разделителя на кадъра е съставен от поредицата 10101011 и определя началото на кадъра, стандартът позволява 2 или 6 байтови адреса, но параметрите дефинирани в стандарта за скорост на предаване 10Мб/сек използват само 6 байтови адреси. Най-старшия бит на адр. на получателя е 0 за нормален адрес и 1 за групов адрес. Груповите адреси позволяват на множество станции да слушат предаването на една станция. Предаването за група от станции се нарича мултикаст. Адрес, който се състои само от единици се използва за бродкаст – предаване до всички станции в мрежата. Свойство на адресирането тук е използването на бит 46 (съседен на най-старшия бит) за различаване на локални от глобални адреси. Глобалните адреси използват 46 бита, което прави приблизително $7*10^{13}$ глобални адреса. Полето дължина на данните сочи броя байтове (от 0 до 1500) в следващото поле. Макар и дължина 0 да е допустима, тя създава проблеми. Когато приемо-предавателят разбере за конфликт, той престава да предава настоящия кадър, което означава, че част от кадъра ще се разпространява по мрежата. За да може да се прави разлика между невалидни части от кадри и валидни кадри, 802.3 дефинира валидните кадри да бъдат с дължина поне 64 байта от началото на адреса на получателя до края на контролната сума. Когато полето данни е по-малко от 46 байта се използва полето PAD за запълване на кадъра до минималната му дължина. Една много съществена причина за наличието на минимална дължина на кадъра е да се предотврати предаване на къс кадър, преди достигането на първия бати до края на кабела, където е възможен конфликт с друг кадър. Във време 0 станция А, разположена в единия каря на кабела, изпраща кадър. Нека времето за разпространение на този кадър до другия каря на кабела означим с *тау*. Нека точно преди пристигането на кадъра в другия край на кабела (във време *тау-епсилон*) най-отдалечената станция Б започне предаване. Тя скоро разбира за конфликта, прекратява предаването и генерира 48 битова поредица, наречена форсиране на конфликта, с което предупреждава всички станции за случилото се в мрежата. Във време 2*тау,* станция А приема информацията за конфликта и също прекратява своето предаване. Ако станцията се опита да предаде много къс кадър, конфликт е възможен отново, но предаването ще е завършило преди станцията да получи информация за конфликта във време 2*тау.* Това ще доведе до погрешното заключение от страна на изпращащата станция, че пакетът е изпратен успешно. За предотвратяване на това, изпращането на всеки кадър трябва да бъде за време повече от 2*тау*. За ЛМ със скорост на предаване 10Мб/с максимална дължина 2500м. и 4 повторителя, минималното време за предаване на кадъра трябва да е 51,2 микросек. Това време съответства на предаване на 64 байта. Кадри с по-малко байтове се допълват до 64 посредством полето PAD. Пропорционално с увеличаване на скоростта на мрежата минималната дължина на кадъра трябва да нарасне или пък максималната дължина на кабела да стане по-малка. За ЛМ с дължина 2500м работеща на 1Гб/с, минималният размер на пакета трябва да бъде 6400 байта. Друг вариант е минималният размер да бъде 640 байта, а максималното разстояние между всеки 2 станции да бъде 250м.
Последното поле в кадъра на 802,3 е контролната сума. В случай на грешки при предаване (например поради шум в кабела) предадената в кадъра контролна сума ще се различава от тази, която е генерирана в приемника, и ще бъде отчетена грешка при предаването.

11.RTS/CTS??????????????????????????????????

- заявка за предаване на данни – RTS (Requrest to Send) Състояние ”логическа 1” на тази шина показва, че DTE е готово да предава данни към DCE. Състояние „логическа нула” указва, че DTE няма готовност да предаде данни
- Готовност за приемане на данни – CTS (Clear to Send) Състояние ”логическа 1” на тази шина показва на DTE, че DCE е готово да приема данни. Този сигнал се изпраща в отговор на заявката за предаване на данни.

Позволява да се осъществи управление на потока от данни. За целта се използват сигналите „Заявка за предаване на данни” RTS и "Готовност за приемане на данни” CTS. Предаването се управлява от устройството-приемник чрез свързан към неговия вход CTS. Устройството-предавател изпраща данни само, когато неговия входен сигнал е в състояние лог. 1. Ако този сигнал премине в лог. 0, то преустановява предаването на данни.

Кабелът – нул модем се нар. Така, защото посредством него се имитира наличието на модеми между две крайни у-ва. Всяко от тях работи по интерфейса RS232, считайки че от другата страна на интерфейса е включен модем. Със схемата се реализира управление на потока от данни. С установяване в състояние лог.1 на сигнала RTS крайното у-во съобщава на у-вото за предаване на данни, че има готовност за предаване. Предаването започва когато устройството за предаване готово за това и установи в „лог.1” сигнала CTS. При схема на свързване г/ се осъществява пълно управление на обмена на данни по интрефейс RS232

<u>12.Опищете процеса на 3 диалоговото ръкостискане при изграждане на виртуален канал.</u>

При първоначално отваряне на връзката между два хоста е необходимо всеки един от тях да изпрати на другият началният номер (initial sequence number) на байтовата последователност, която ще изпраща, и съответно да получи потвърждение за получаване на този номер. Процедурата за установяване на връзка се нарича Three Way Handshake, в нормалния случай е следната:

- Хостът, който отваря връзката, изпраща SYN сегмент. В същият сегмент клиентът задава номера на порта на сървъра, с който ще осъществява връзка и началният номер на потока байтове, който клиентът ще предаде към сървъра.
- Сървърът отговаря със собствен SYN сегмент, включващ началния номер на неговия поток байтове. В сегмента се съдържа и потвърждение ACK за SYN.
- Клиентът трябва да потвърди т.е. да прати сегмент с ACK за получаването на SYN.

За затваряне на връзката се използва процедура, при която прекратяването на връзка става по начин, предотвъртяващ загубата на информация.

- Хостът, който затваря връзката, изпраща FIN сегмент.
- Другият потребител изпраща сегмент с потвърждение ACK и FIN.

Може връзката да бъде прекратена безусловно. Тогава се установява флаг RST, който в заглавната част идентифицира сегмет за прекратяване на връзката.Той се изпраща от протокола TCP, когато по връзката се получи некоректен сегмент, в който IP адреса и номерът на порта на изпращача или получателят не съвпадат с тези на съответната връзка.

- -

<u>Разни изватки</u>

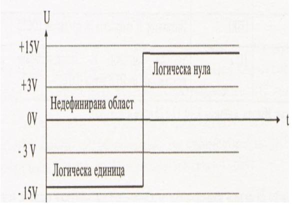
<u>1.Връзка м/у PC с хост ч/з взаимодеиствие м/у едноименни слоеве ч/з протоколите за обмен</u>

Схема за достъп от PC до приложна програма(пп) от хост,свързан към мрежа ч/з буферен процесор(бп). Връзката хост-бп е локална ,а PC-хост п/з 2 възела(ВК1 ВК2).Бу ферният процесор об служва и освобождава хоста от телекомуника ционни процедури.

Правилата за взаимо действие м/у слоевете се нарича интерфайс или м/услоев протокол.

Интерфейс RS232

Този интерфейс свързва край но у-во DTE(Data Terminal Equipment) и у-во за предаване на данни DCE(Data Cercuit-Termination Equipment). Предаването на данни по него може да се извърши по синхронен или асинхронен режим.



Основните групи от шини в интерфейс RS-232:

1. Информационни:
   - Предавани данни-TxD
   - Приемни данни-RxD.
2. Управляващи:
   *Заявка за предаване на данни-RTS(Request to send);
   *Готовност за работа на DTE-DTR(Data Terminal Request);
   *Готовност зо предаване на данни-CTS(Clear to send)
   *Готовност за работа на DCE-DSR(Data Set Ready);
   *Открита носеща честота-DCD(Data Carrier Detect).
3. Тактови:
   *Тактови импулси за синхро низиране на предавани те от DTE данни-TC-1(Transmit Clock);

*Тактови импулси за синхро низиране на приеманите от DTE данни-RC(Receive Clock)
*Тактови импулси за синхрони зиране на предаваните от DTE данни-TC-2(Transmit Clock).

Широко разпространение на цифровото предаване доведе до разработка на методи, които да позволяват в един канал с висока пропускателна способ ност да се мултиплекси рат няколко цифрови телефон ни канала.Един от тях е стондартът T1.В един канал със скорост на предаване 1.544 Mb/s се мултиплексират 24 цифрови телефонни канала. Отчетите се предават последо вателно на 24 кодека,като все

ки от 24-те кодека въвежда последователно 8 бита в изходящия цифров поток. Седем от тези бита представля ват данни, а осмият се използ ва за управление.Кадърът се състои от 193 бита-192 бита информация и 1бит за синхро низация на кадъра.Той се предава за 125μs и се постига общата скорост 1.544Mb/s. Съществува и интерфейса E1. При него кадърът е с дължина 256 бита, предава се за 125μs и скоростта е 2.048 Mb/s.Всеки кадър има 32 осембитови канала,като 30 от тях се използ ват за предаване на данни,а останалите 2 служат за преда ване на сигнална синхрони зираща информация. **Аналогови модеми** Аналоговите модеми за предаване на данни по обикновинни телефонни линни използват честот на лента,ненадвишаваща 3,3kHz.Аналоговите мо деми се включват към те лефонна линия и пре дават сигнали през теле фонната мрежа без изме нения,тъй като тази мрежа третира излъчва ните сигнали като преда ване на глас.**Високоскоростни модеми** Наличието на филтри в края на телефонната линия налага чес тотната лента да бъде ограни чена до 3,3kHz.Без тези филтри по усуканата двойка провод ници могат да се предават данни с много висока скорост. Висококоростните модеми се делят на няколко класа: *DSL(Digital Subscriber Line) модеми-осигуряват цифрова абонатна линия.*HDSL(High bit-rate Digital Subscriber Line) модеми-реализират висококо ростна цифрово абонатна линия.*ADSL(Asymmetric Digital Subscriber Line) модеми-служат за изграждане на асиметрична цифрова абонатна линия.

FTP(File Transfer P.)ч/з него може да се прави обмен на фай лове м/у хостове,които използват различни файлови с-ми,при което файл.могат да бъдат с двоични или аски данни

*****П.за обмен на новини **NNTP** (Network News Transfer P.) деф.начина на обмен на съобщ.наречени “новини”

*****П. За ел. Поща

#SMTP(Simple Mail Transfer P.)опр.начина, по който пощата се доставя от из пращача до получателя и деф.вътрешният формат на пощ. Съобщ.

#**POP**(Post Office P.)прехвърля съдърж.на пощ.кутия на потре бителя от пощенският сървър към с-мата на потребителя.

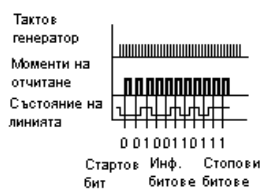
2.Сравнение м/у OSI и TCP/IP

И 2та модела се основават на концепцията за 1 стек от независими П. И в 2та модела слоевете от транспортния нагоре предоставят независимо от мрежата транспортно обслужване от край до край за процесите, които искат да комуникират. Слоевете над транспортния са приложно ориентирани и използват услугите на транспортния слой.

Св-ства на OSI модела: - Деф. На услуги. – Деф. на интерфейси. – Деф. на П. Предимства на OSI: Разграничение м/у тези 3 св-ства. Всеки слой изпълнява опр. Услуги и ги предоставя на слоя над него. Интерфейсите на слоевете съобщават на процесите над тях как да получат достъп до съответния слой. Двойките П. на едноименните слоеве извършват съответните услуги деф. за този слой. За TCP/IP модела няма точно разграничаване м/у услуги, интерфейси и П. Фактически само една реална услуга се предлага от интернет слоя и тя е изпращане на IP пакет и получаване на IP пакет. Като обобщение, П. в OSI модела са по добре обособени отколкото в TCP модела и могат да бъдат заменени относително по-лесно при промяна на технологията. При TCP/IP модела първо се разработват П. и моделът представлява реално описание на вече съществуващите П. OSI моделът има 7 слоя, а TCP/IP–4. И двата имат мрежов, транспортен и приложен слой, но др. слоеве са различни.

3.Сравнение м/у синхронно и асинхронно предаване.

При асинхронното предаване все ки символ се съпровожда от стар тов бит и 1 или 2 стопови битове. Стартовият бит е предназначен не само за синхронизиране на симво ла,но и за стартов сигнал на вътре шният тактов генератор, ч/з който се отделят битовете в рамките на символа.Тактовата честота на гене ратора превишава неколкократно честотата на следване на битовете ,като с нея се определят моменти те за отчитане стойностите на от делните битове.Моментите на стробиране се избират по средата на интервалите от време, предста вящи битовете, с цел евентуални те вариации в честотата на следва не на битовете да не доведат до грешно приемане на символите. Предаването на символа завършва с генериране на 1 или 2 стопови бита, чиято по-голяма продължи телност ги прави различими от информационните битове.Интерва лът от време м/у 2 последователно издадени символа се мени в широ ки граници, като в този период по линията продължава да се поддър жа съответното ниво “стоп”



При синхронното предаване информацията се представя като непрекъсната последователност от символи, обединени в отделни блокове от данни.Синхронизирането на битовете става или по външни сигнали,разпространявани по канала за връзка,или с помощта на методи за кодиране, при които фазата на информационния бит се съдържа в сигннала. В някои случаи синх

ронизирането е от синхронно работещи генератори, установени в приемната и предаващата част. Разпространен е също методът с периодично предаване на синхро низиращата последователност за съгласуване на работата на вътре шните тактови генератори.

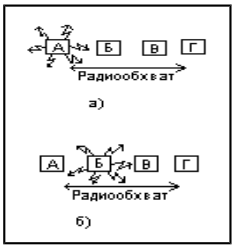
Предимството на синхронното предаване е най-вече в значително по-голямата скорост на обмен. При синхронното предаване може да се използват по-съвършени ме тоди за модулация.

Към недостатъците на синхронния метод за предаване трябва да се от несе преди всичко увеличаването на апаратурата.Възниква необхо димост от буферна памет, услож нява се обработващата логика, как то в приемната,така и в предавате лната част.

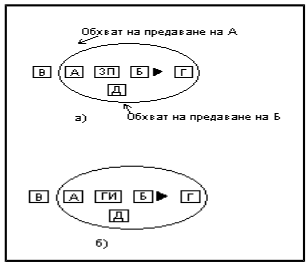
Приложение-Асинхронното преда ване е удобно за свързване на про ста, нискоскоростна терминална апаратура, докато синхронното предаване позволява по-големи скорости.

4.Безжични локални мрежи IEEE 802.11

За да се постигне пълна мобилност, компютрите трябва да използват радио или инфрачервени сигнали за комуникация. При такава комуникация потребителите могат да ползват електронна поща даже когато са на движещо превозно средство. Една с-ма от мобилни компютри,които приемат предават с радио вълни може да се разглежда като безжична локална мрежа. Тези ЛМ имат по различни св-ва от традиционните и изискват по специални протоколи на подниво за достъп до средата. 1 опростен подход за използване на безжична ЛМ е с CSMA метода – всяка станция само слуша за наличие на предаване и заема средата, ако никои друг не е направил това. За съжаление този протокол не е подходящ за такъв тип ЛМ, тъй като се получава интерференция при приемника, а не при предавателя. За да се изясни проблемът на фиг. е показан пример с 4 безжични станции.



В случая няма значение кои станции са базови и кои мобилни. Радиообхватът е такъв, че А и Б са в своите обхвати и може евентуално да интерферират при едновременно предаване една с друга. В също може да интерферира с Б и Г, но не и с А.



Нека станция А предава на Б. Ако В слуша ефира,т я няма да чуе А, защото е извън нейния обхват, поради което може погрешно да реши, че може да предава. Ако В започне предаване, интерферира в Б, унищожавайки кадъра от А. Проблемът на не може да открие потенциален потребител на ефира, защото твърде далеч. Това се нарича “проблем на скритата станция”(сигналът ще една станция е,че той понякога е hidden station problem). Случаят, когато Б предава на А, е показан на фиг.б. ако В разпознае това предаване в ефира, ще допусне неправилно, че не може да предава за Г. Всъщност едно такова предаване към Г би създало интерференция единствено в зоната м/у Б и В, където няма станции, за които е предназначено. Тази ситуация се нарича “ проблем на експонираната станция (“exposed station problem”). Проблемът се състои в това, че преди началото на предаването една станция трябва да знае дали има или няма активност около приемника. При методът CSMA се разбира единствено дали има или няма активност около станцията, която излъчва носещата. При използването на кабел, всичките сигнали се разпространяват към всички станции, така че само 1 предаване може да се осъществи по едно и също време в цялата с-ма. В с-ма, основана на късовълнови радиовълни, е възможно осъществяването на няколко предавания едновременно, ако те са с различни крайни получатели и тези получатели са извън обхвата си един на друг. Като пример може да се разгледа и една офис сграда, където всеки служител има безжичен мобилен компютър. Нека служителят А иска да прати съобщение на служителя Б. Компютъра на А слуша средата и, ако не разпознае активност, започва да предава. В този случай обаче е възможен конфликт при компютъра Б, защото трети служител Б може да изпраща в този момент съобщение на Б, а местонахожденията на А и Б отдалечени, при което те не могат да разберат, че единият от тях предава. Един протокол, разработен за безжични ЛМ е MACA (multiple access with collision avoidance). Той е в основата на IEEE 802.11 стандарта за безжични ЛМ. Основната идея е предаващата станция да стимулира приемащата да предаде къс кадър, така че наблизо стоящите станции да разберат за това предаване и да не излъчват сигнал по време на изпращания (голям) кадър с данни. Нека А трябва да предаде към Б фиг.2. А започва предаването с изпраща не на кадър на Б, съдържащ “Заявка за предаване”–ЗП. Този кратък кадър (30 байта) съдържа дължината на данните, които ще последват. Б изпраща кадър-отговор, наречен “Готовност за изпращане”-ГИ. Кадърът ГИ съдържа дължината на данните, копирани от ЗП. След получаване на кадъра ГИ от Б станция започва предаването. Реакциите на станциите, до които достигат кадрите ЗП и ГИ, са следните. Всяка станция, до която достигне ЗП, е в обхвата на А. Тя няма да предава за периода от време, през който се предава ГИ, за да може този пакет да се приеме обратно от А без да настъпи конфликт. Всяка станция, която приеме ГИ, е в обхвата на Б и не трябва да предава за период от време, съобразен със заявената в ЗП дължина на

предаваното съобщение. На Фиг.2. станция В е в обхвата на А, но не и в обхвата н Б. Следователно тя приема ЗП от А, но не приема ГИ от Б. До момента, в който тя не влиза в конфликт с кадъра ГИ, тя може да предава по времето на из пращането на кадъра с данни. Об ратно – станцията Г е в обхвата на Б, но не и на А. Тя не е приела ЗП, но е приела ГИ. Г разбира от ГИ, че е близо до станцията, която ще приеме данни, поради което тя се въздържа от каквото и да е предав ане,докато мине очакваното време за предаване на данните. Станция та Д приема и двата служебни ка дъра ЗП и ГИ и точно както Г трябва да се въздържа от предаване докато бъдат изпратени данните. Въпреки тези предпазни мерки е възможен конфликт на кадри. Нап ример Б и В могат да пратят едно временно ЗП за А. Тези кадри ще бъдат загубени. В случай на кон фликт неуспелия предавател(този, до който след определено време не достигне ГИ) изчаква случаен период от време и опитва отново да предава.

ISDN

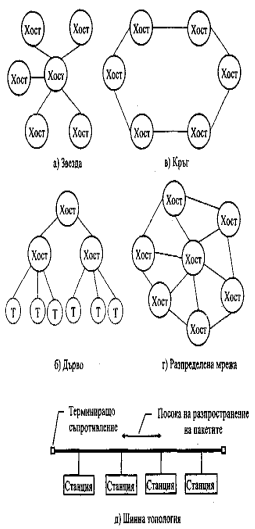
(Integrated Services Digital Network)

Предоставя набор услуги към крайните абонати на регионалните тел. компании, които включват цифрова телефония и пренос на данни. Крайните потребители, свързани към мрежата ISDN получават възможност да предават глас, данни, текст, графика, музика, изображения и информация от др. източници. Предаването на данните е цифрово.Най честото използване на ISDN в рамките на протоколния стек TCP/IP е за свързване на канално ниво на даден локален хост или маршрутизатора на неговата локална мрежа към друг отдалеч ен хост или респективно маршрут изатор през съществуващата тел. Мрежа

ATM

ATM пренася всички видове трафик-данни, глас, изображения и видеокартина, като използва клетки с един и същ формат.ATM мрежата включва ATM крайни у-ва и ATM комутатори.Крайните у-ва могат да бъдат маршрутизатори,работни станции,ключове на ЛМ и др.Всяко от тях трябва да включва в състава си ATM мрежов адаптер. ATM комутаторът получава клетки на входните си интерфейси от край но у-во или друг комутатор.Той анализира инф.в полето“заглавие”
на клетката и въз основа на този анализ предава клетката към изхо ден интерфейс, по който тя ще дос тигне до своя получател

5.Топология на мрежите



Топологията на мрежите определя геометричното свързване на физическите канали и възлите в мрежата.

При централизираните мрежи информацията се предава между главният хост и подчинените хостове. Подчинените хостове не могат помежду си да предават информация. *Централизираната (звездообразна) мрежа* изисква връзка на всички абонати с централния възел, който управлява цялата система (фиг. 1.7.а). Абонатите се свързват помежду си чрез централния хост.

Централизираната дървовидна структура (фиг. 1.7.6) е особено удобна за управляване на производствени процеси, тъй като чрез йерархичната си конфигурация може да обслужва няколко нива в цялостния производствен процес.

При мрежите с кръгова структура (фиг. 1.7.В.) хостове са разположени в кръг на определени разстояния един от друг и позволяват достъп до всеки компютър при прекъсване на физическия канал по обходен път. Най-често тази топология се използува при локалните мрежи.

Мрежите, на които хостове са частично или пълно свързани, имат най-голяма надеждност (фиг. 1.7.Г.). При тази топология може да се постигне значително по-голяма скорост на предаване. ***Шинната топологя*** представлява шина за данни, към която са свързани множество компютри. Използва се при LAN мрежите.

7.IEEE стандарт 802.4 — маркерна шина

Локалните мрежи от типа "маркерна шина" са предпочитани в редица условия, където се работи в реално време. Използването на състезателните методи на достъп и базираните на тях протоколи не може да осигури гарантирано време за реакция при комуникация между определени системи. Стандартът IEEE 802.4 описва достъпа до средата за шинни мрежи с маркер. На станциите, които могат да предават данни се задават позиции, съответстващи на разположение в логически кръг. Възможно е дадена станция да е свързана към шината, но да не е в логическия кръг. В такъв случай, станцията може само да получава (не може да изпраща) пакети. Маркерът контролира достъпа до шината и се предава от станция на станция по реда, по който станциите са подредени в логическия кръг. Поради това всяка станция трябва да знае адреса на следващата станция от кръга. Когато една станция притежава маркера, тя има правото да предава пакети (за определен

период от време). Шинните локални мрежи с маркер се нуждаят от редица процедури за поддръжка - например за добавяне или изтриване на станция от кръга, инициализация на кръга, възстановяване на маркера и др. ЛМ от типа маркерна шина дефинира четири приоритети за трафик — 0, 2, 4, 6 (6 е най-високия). Всяка станция може да се разглежда като съставена от 4 подстанции — по една за всеки приоритет. Всяка подстанция поддържа опашка от пакети, които трябва да изпраги. При приемане на пакет се проверява неговия приоритет и пакета се насочва към подстанцията със съответния приоритет.

8.Стандартът 802.5

Стандартът описва локална компютърна мрежа с логическа топология тип "кръг". При нея сигналът обхожда в кръг последователно всички възли. Физическата топология може да е от друг тип, най-често "звезда".
Разстоянията, които се покриват са по-големи от тези при стандарти 802.3 и 802. 4, тъй като когато сигналът преминавайки през възелите се формира и усилва.
Използва се само режим "директно предаване". За комуникационните линии се използват се кабелите:
- Неекранирани усукани двойки (UTP) със съединители RJ – 45;
- Екранирана усукана двойка (STR) със съединители RJ – 45 или с MIC на IBM;
- Коаксиален кабел;
- Влакнесто – оптичен кабел.

Скоростта на предаване за стандарта е 16 Mb/s или 4 Mb/s. По кабел UTP се постига скорост до 4 Mb/s.
Крайните възли се свързват към кръга чрез специални съединителни устройства MAU (Multistation Access Unit). Чрез съединителите MAU може да се изключва повреден краен възел, с което се запазва целостта на мрежата. В една LAN по този стандарт може да има до 33 броя съединители тип MAU. Разстоянията между възела на мрежата и MAU – съединителя трябва да е минимално 2, 5 м. и максимално – до 100 м за кабел STP и 45 м за кабел UTP. Допуска се дължина на кабела между два съседни MAU – съединители до 150 м. и до 750 м. с използване на междинен усилвател (повторител).

MAC – подслой на стандарта IEEE 802. 5.

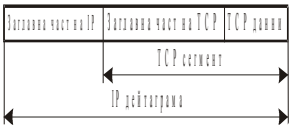
В MAC – подслоя на стандарта се използва протокола Token Ring . Управлението на достъпа става с маркер. Маркерът се генерира при инициализиране на мрежата, след което той циркулира по кръга само в една посока. Право на комуникационната среда има само възелът, който владее маркера. Когато един възел иска да владее маркера с цел предаване, в полето AC (Фиг.48.), в мркера се променя един бит, с което маркерът се превръща в начало на кадър на този възел. В този момент във възела се пуска таймер, с който се определя времето, за които възелът може да задържи маркера. Излъчените кадри преминава последователно през всички възли, но само възелът-получател ги копира в паметта си. Когато последния кадърът достигне до възела – подател, служебния маркер се освобождава и преминава към следващия възел. За правилното изпълнение на процедурите се грижи специална мониторна станция. За тази цел един от крайните възли на мрежата премахва „забравени кадри" и възстановява изгубени маркери.
Протоколът Token Ring има предварително зададено максимално време за закъснение на кадъра, поради което е удобен за работа в реално време.
В LAN с по-висока скорост (16 Mb/s) се използва методът на "предварително освобождаване на кадъра". Възелът – подател не чака последния кадър да "направи кръг", а щом го предаде в мрежата, веднага предава служебния маркер към следващия възел.

Начален ограни-чител (SD)	Управ-ление на достъпа (AC)	Управ-ление на кадъра (FC)	MAC – адрес на получа-теля (DA)	MAC-адрес на подате-ля (SA)	Дан ни	Кон-тролно поле (FCS)	Краен огранич-ител (ED)	Състоя-ние на кадъра (FS)
1 B	1	1	2 v 6	2 v 6	пром. дължина	4	1	1 байт

15.Управление на транспор тния слой. Протоколи

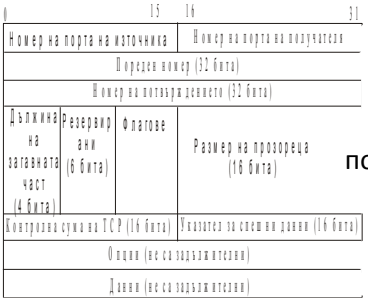
TCP и UDP са най-важните протоколи свързанни с транспор тния слой.CP осигурява надеж дното предаване на данните ме жду предавателя и приемника чрез установяване на връзка т.е. е гарантирано доставянето на предадената информация до получателя.UDP не е ориенти ран към установяване на връз ка т.е. е ненадежден протокол –не гарантира,че предаденото съобщение ще достигне до получателя си.TCP представля ва множество правила за осъществяване на надежден информационен обмен между приложните слоеве на два хоста.Тези функции се органи зират от програмен модул, който по принцип е част от ОС на съответния хост.Данните се обслужват и интерпретират ка то поток от байтове.TCP не вмъква автоматично разделите ли между лог. записи. Обменът се извършва посредством сег менти.При предаване TCP по лучава данни от по-горния слой,разделя ги на части,опако ва ги заедно с адреса на място назначението им в сегменти и ги праща

на IP протокола. След приемане разопакованите от IP дейтаграми,TCP сглобява и подрежда сегментите в съоб щения и ги подава на по-горни те слоеве такива,каквито са били получени.



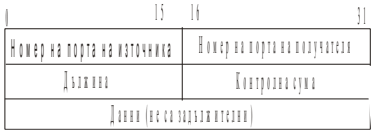
TCP осигурява на протоколите от по-горен слой възможността за двупосочно(дуплексно) пре даване на данните.Заглавна част на TCP сегмента включва задължителни полета с фикси ран размер от 20 байта (5 x 32 битови думи).Максимално до пустимата дължина на полето за данни е 2^{16} байта.

Номерът на потвърждението е номерът на първия байт данни, който се очаква да се получи със следващия сегмент.Заглав ната част на TCP има 6 флага: URG – Валиден е указателят за спешни данни (преустановява се работа за да се обработят по лучените спешни данни,указва позицията на първия байт на спешните данни спрямо начало то на полето за данни),ACK- валиден е номерът на потвърж дение,PSH-приемникът и полу чателят трябва незабавно да изпратят наличните си данни, RST-за прекратяване на връзка та безусловно,SYN-при устано вяване на връзка-указва нача лото на данните,FIN- изпраща чът прекратява изпращането на данни.



Контролната сума се изчислява в/у целия TCP сегмент, който се състои от заглавната част, данните и псевдо-заглавната част(включваща част от заглав ната част на IP дейтаграмата). TCP компенсира ненадеждност та на мрежовата среда и затова е необходимо да се запази дос товерността на данните при загуба на сегмент,дублиране на сегменти,при безусловно прекратяване на връз ката и др. При отваряне на връзка първо се изпраща началният номер на байтовата последователно ст, която ще се изпраща на сървъра.Това става чрез SYN сегмента и число x (начален номер).В последствие сървара отговаря също със SYN и нача лен номер y,както и номер на потвърждение ACK=x+1.В тре тата стъпка клиентът изпраща потвърждение ACK=y+1.Зараи тези три стъпки процедурата се нарича **диалог с три съобще ния** или three-way handshake.За пълно затваряне на връзката е необходим обмен на 4 сегмента.Използва се FIN,като този сигнал трябва да се изпра ти и от двете страни,за да се за твори изцяло връзката,в проти вен случай връзката остава полуотворена(2 сегмента) и след това да бъде потвърдено получаването му(другите 2 сег мента).Протоколът на плъзга щия прозорец служи за опре деляне на броя байтове,които могат да бъдат приети във все ки момент и се записва в по лето размер на прозореца. Уста новеният флаг RST е знак,че е получен некоректен сегмент, в който IP адреса и номера на по рта на изпращача или получа теля не съвпадат.Липсата на потвърждение или двукратно то потвърждение са индикация за загуба на сегмент.Двукратно то потвърждение се генерира при получен сегмент с разли чен от очаквания номер.Ако даден сегмент не бъде потвър ден за определено време се пре дполага,че има претоврване на мрежата и сегментът е загубен т.е.трябва да се предаде отно во.Времето на изчакване се нар. Таймер за препредаване.

Действието на UDP се основа ва на протокола IP.Процесът,из ползващ UDP,генерира една UDP дейтаграма за всяка изход на операция,която се изпраща посредством съответна IP дей таграма.UDP не осигурява на дежден транспорт.Дейтаграми те се изпращат от източника без да се контролира дали са достигнали до получателя.



Полето за дулжина задава в брой общата дължина на загла вната часта на данните в UDP дейтаграмата.Минималната стойност е 8-когато имаме са мо заглавна част.Контролната сума се изчислява върху псев до-заглавието,заглавната част и данните.

17.Интернет приложения. Обмен на файлове DNS, FTP, E-mail, WWW, DHCP: E-mail

E-mail

Ел.поща е мрежова услуга, чрез която всеки потребител с компютър, свързан към глобалната компютърна мрежа, може да обменя съобщения с всички потребители на мрежата. Обикновено обменяната информация е в текстов формат(известен като ASCII) . съществуват също така възможности за компресиране на предаваните файлове, което улеснява изпращането и получаването на големи по обем масиви от данни.

Основните понятие са:

***пощенски сървър**(mail server) – представлява програмна система, реализираща основните функции на ел.поща. за всеки домейн от глобалната мрежа е необходим поне един такъв сървър. Тази система включва следните компоненти:

-пощенска кутия(mail box) – специализиран файл, съхраняван в определена директория на сървъра. Всеки такъв файл носи името на съответния потребител и е предназначен да съхранява пристигащата за този потребител ел.поща.

-прехвърлящ хост (relay host) – програма, която управлява маршрутизирането и изпращането на ел.писма в рамките на глобалната мрежа. Тя изработва в последователен ред писмата, съхранявани в опашката за

изходящи писма на сървъра. При изпращането на маршрутизираното писмо се използва пощенския транспортен агент

-пощенски транспортен слой(mail transport agent – MTA) – програма, която приема и изпраща ел.писма. при приемане на дадено писмо тя анализира адреса на получателя. Ако получателят има пощенска кутия на сървъра, писмото се записва в нея. В противен случай то се записва в опашката за изходящи писма.

***пощенски клиент**(mail client) – програмна система, която изпраща/получава ел.писма към/от пощенски сървър.

***Шлюз**(gateway) – програмна система, която управлява обмена на ел.поща между различните видове комуникационни мрежи.

За да бъде в състояние даден хост да предлага услугата " Ел.поща" , е необходимо той да е част от глобалната мрежа. На него трябва да се инсталира пощенски сървър.

За обмен на данни чрез ел.поща се използват множество протоколи по-важните от които са:

***SMTP** (Simple Mail Transfer Protokol) – този протокол осигурява обмен на писмата между програмите, предназначени за изпращане и получаване на ел.поща.

***POP(** post office protokol) – този протокол е предназначен за прехвърляне съдържанието на пощенската кутия на потребителя от пощенски сървър към персоналния компютър на потребителя.

***IMAP**(Internet Message Access Protokol) – протоколът осигурява връзка между пощенски сървър и потребителски работни станции или персонални компютри чрез динамичен достъп до пощенскатанкутия на сървъра. Разликата с протокола POP е, че прочетените писма остават на съхранение в пощенския сървър,а не се прехвърлят в локалната система.. това позволява на потребителя д има достъп до пощенската си кутия от различни клиентски компютри.

***UUCP**(Unix to Unix Copy) – опростен протокол за обмен на електронни съобщения между компютърни системи, работещи с Unix операционни системи.

18.WWW

Основната цел при разработването на WWW мрежата е била създаването на универсално средство за достъп до различни по структура и характер данни, разпределени между голям брой компютърни системи.важно предимство при създаването и използването на WEB технологиите е възможността големи масиви от данни да бъдат разделяни на по-малки по обем документи, наречени WEB страници. Те от своя страна могат да се разполагат в локалния или в отдалечени WEB сървъри и при това да бъдат част от една и съща информационна система.

Основния принцип на работа на WWW информационната система се състои в това, че клиентът изпраща заявка в точно специфициран формат към сървъра, който я обработва и връща получения резултат обратно на клиента. Обменът на данни между клиента и сървъра обикновено се реализира по протокола HTTP, но има възможност да се използват и други комуникационни протоколи.