

Локалне мреже

У овом поглављу сазнаћемо:

- које су основне карактеристике локалних мрежа,
- о мрежним оперативним системима који се користе у локалним мрежама,
- које су стандардне врсте етернет мрежа,
- које су карактеристике бежичних локалних мрежа,
- какве су Bluetooth и ZigBee технологије,
- каква је разлика између радио и инфрацрвених LAN-ова,
- о заштити података на мрежи,
- шта су то проху-сервер, mail-сервер и web-сервер.

9.1. УВОД

Локалном мрежом назива се свака рачунарска мрежа која ради на другом OSI слоју, тј. у слоју везе. Према овој дефиницији WAN мреже су мреже које раде на трећем OSI слоју, тј. у слоју мреже.

Основне карактеристике локалних рачунарских мрежа су следеће:

- у локалној мрежи ниједан рачунар не може присилно да покрене, заустави или управља другим рачунаром, тј. не постоји однос надређени/подређени.
- све умрежене станице готово су увек повезане на заједнички медијум што значи да све станице деле укупни пропусни опсег медијума. Много ређе се локалне мреже пројектују на принципу преноса од тачке до тачке. Тада локална мрежа личи на минијатурни WAN,
- брзине рада локалних мрежа су велике, данас обично од неколико десетина Mb/s до више Gb/s,
- због најчешће релативно малог растојања између станица кашњење и број грешака су мали,
- постоји могућност мултикастинга и бродкастинга.
- локалне мреже никад нису јавне, већ су у власништву неке установе, предузећа или појединца.

Број станица у LAN мрежама обично варира од неколико до неколико стотина.

Пошто су локалне рачунарске мреже готово увек пакетске дифузне мреже, то мора да постоји неки механизам који станицама додељује пропусни опсег медијума тако да свака станица може да приступи медијуму током неког разумног периода времена, а да се при том обезбеди да неискоришћеност медијума буде минимална. Механизми приступа медијуму реализују се путем протокола који се налазе у слоју везе. Постоји много протокола од којих сваки има и добрих и лоших страна.

Природу локалне мреже одређују три фактора:

- медијум кроз који се обавља пренос,
- топологија мреже,
- протокол за приступ медијуму.

Медијум и топологија мреже у великој мери одређују брзину и ефикасност комуницирања.

Локалне мреже могу да буду жичне и бежичне, односно могу да раде у основном и у транспонованом опсегу учестаности. Зато се у локалним мрежама могу користити све врсте медијума.

У жичним локалним мрежама најчешће се користи упредена парица због ниске цене и лаког инсталирања.

Коаксијални кабл је знатно скупљи, али има знатно боље перформансе од упредене парице. Пре свега, има већи капацитет што омогућава већи проток података, затим дозвољава да се у мрежу повеже већи број станица и омогућава пренос на већа растојања. Коаксијални кабл омогућава пренос у основном опсегу (енгл.: *baseband*) и у транспонованом, односно како се често каже, у широкопојасном опсегу (енгл.: *broadband*).

Локалне мреже које раде у основном опсегу јефтиније су и у техничком погледу једноставније од мрежа које раде у транспонованом опсегу, али имају мањи пречник и мањи је број станица које се могу укључити у мрежу. Широкопојасне локалне мреже технички су сложеније и теже се инсталирају и одржавају зато што кроз њих може да се одвија разноврстан саобраћај по много канала. Просечно кашњење услед коначне брзине простирања сигнала је у широкопојасним мрежама у *просеку* два пута веће но у мрежама које раде у основном опсегу зато што сигнал од изворишта до одредишта прелази у *просеку* два пута дужи пут.

Када су потребне врло велике брзине преноса, користи се оптичко влакно јер има далеко већи капацитет од коаксијалног кабла. Оптичко влакно најчешће се користи у везама типа *од тачке до тачке* и као *окосница* (енгл.: *backbone*) за повезивање брзих LAN-ова, али се све више користи и у локалним мрежама и поред одређених техничких проблема при инсталирању због чега су и трошкови постављања још увек велики.

Последњих година све више се користи бежична локална мрежа. Како је растао број портабл рачунара, тако су расли и захтеви за њиховим повезивањем са осталим рачунарима и комуникационим уређајима. Први портабл уређаји нису имали ову способност, али су уз помоћ модема могли да се повежу у мрежу са фиксним рачунарима. Дакле, да би портабл рачунари били повезани, морала је постојати жична веза до фиксне мреже. Тако ови рачунари јесу били *портабл*, али нису били *мобилни*. Стварна мобилност портабл рачунара постиже се само ако се комуникација обавља помоћу радио или инфрацрвених сигнала.

9.1.1. МРЕЖНИ ОПЕРАТИВНИ СИСТЕМИ

Овде ћемо рећи нешто више о мрежним оперативним системима у локалним мрежама.

Мрежни оперативни системи (МОС) могу се поделити у две основне групе, и то на:

- мрежне оперативне системе који се користе у равноправним мрежама (енгл.: *peer-to-peer network operating systems*) и
- клијент-серверске мрежне оперативне системе (енгл.: *client-server network operating systems*).

Зависно од тога који се тип мрежног оперативног система користи локалне мреже могу бити:

- локалне мреже равноправних рачунара,
- клијент/сервер локалне мреже.

9.1.1.1. Равноправне локалне мреже

Peer-to-eer мрежа омогућава да два или више РС-ја обједине своје ресурсе (податке, програме, штампаче и др.) тако да постану доступни сваком РС-ју. Информације су, дакле, децентрализоване, па сваки РС може да ради и као клијент (тражи информације) и као сервер (пружа информације). На пример, ако је у оваквој мрежи само на једном рачунару инсталиран неки програмски пакет, нпр., Windows Word, овај програм могу да користе све остале умрежене станице. Ова конфигурација погодна је за употребу у малим предузећима и организацијама, као и у кући.

На пример, оперативни систем Windows 98 садржи у себи peer-to-peer мрежни оперативни систем што значи да Windows 98 омогућава формирање локалне мреже равноправних рачунара. Поред Windows 98 и 95, познати peer-to-peer мрежни оперативни системи су Windows for Workgroups, Artisoft LANtastic и NetWare Lite.

Peer-to-peer мрежа може се реализовати било у облику 10BaseT мреже или танког етернета. 10BaseT конфигурација је погодна за повезивање до шеснаест станица које нису много удаљене, при чему неке од њих могу бити портабл рачунари који повремено могу да напусте мрежу.

После инсталирања мрежног хардвера у сваки РС мора се унети peer-to-peer мрежни софтверски модул који, када корисници затраже, омогућава пренос информација између рачунара, хард дискова и осталих уређаја.

У већини peer-to-peer мрежних оперативних система корисници могу да одреде које своје ресурсе стављају на располагање осталим корисницима. Када се један кориснички диск конфигурише као „дељив“, он се код осталих корисника појављује као нови драјв. На пример, ако корисник А има на свом рачунару С драјв, а корисник В конфигурише свој С драјв као „дељив“, корисник А ће одједном имати С и **Д** драјв, при чему је **Д** драјв корисника А у ствари С драјв корисника В.

Peer-to-peer МОС има следеће предности у односу на клијент/сервер МОС: није потребан администратор мреже, подешавање и одржавање мреже је једноставно, па самим тим и јефтино, сваки рачунар може да направи резервну копију на другим рачунарима и да тако повећа сигурност података.

9.1.1.2. Клијент-сервер локалне мреже

У клијент-сервер мрежи клијенти (којих може бити неколико или неколико десетина, стотина, па и хиљада) могу да користе ресурсе које поседује сервер. У овој конфигурацији, за разлику од peer-to-peer конфигурације, информације су централизоване: све информације које се налазе на серверу, као и сви уређаји којима управља сервер, доступни су свим клијентима. На пример, ако су у серверу ускладиштени подаци и програми, реч је о *фајл серверу*, а сервер који управља једним штампачем или више штампача назива се *принтер сервер*.

Клијент-серверски МОС води рачуна да истом ресурсу (нпр., штампачу) не приступе истовремено два или више заинтересованих. Такође, администратор мреже може преко мрежног оперативног система да додели корисницима различите нивое приоритета при коришћењу ресурса: нпр., неки корисници могу само да прегледају, али не могу да мењају садржај фајлова, док се другима то дозвољава. Штавише, неким корисницима може се забранити приступ појединим мрежним ресурсима.

Клијент-серверски МОС треба да обезбеди поузданост, безбедност и флексибилност мрежног повезивања и да омогући брзо реконфигурисање како хардвера, тако и софтвера по могућности без прекида рада.

У оперативни систем Windows NT интегрисан је клијент-серверски мрежни оперативни

систем Microsoft Windows NT servers, што значи да се под оперативним системом Windows NT може формирати клијент/сервер LAN. Клијент-серверски МОС су, такође, Linux, NetWare, Solaris, Windows 2000 и Server 2003.

Клијент-серверски МОС идеалан је за велике организације којима је потребан брз мрежни приступ и операције над базама података, табелама, као и видео и мултимедијални приступ.

9.1.2. СЕРВЕРСКИ ПРОГРАМИ

Сервер и клијент могу бити било рачунар, било програм. Серверски програм је програм коме преко мреже клијент шаље захтев, а серверски програм поступа по захтеву и потом клијенту шаље одговор. Програми који се користе на сервер рачунарима специјално су развијени за клијент/сервер мрежне оперативне системе. На пример, серверски програми су DNS (Domain Name System) који се користи за пресликавање симболичких имена рачунара у IP адресе, затим DHCP (Dynamic Host Configuration Protocol) софтвер који се реализује у серверима и рутерима и који аутоматски додељује привремене IP адресе клијент-станицама у IP мрежи, mail сервер софтвер итд.

9.2. ЖИЧНЕ ЛОКАЛНЕ МРЕЖЕ

Жичне локалне мреже реализују се најчешће у облику звезде, а нешто ређе у облику магистрале или прстена. Мреже у облику магистрале и звезде (која је, као што је речено у глави 2, физички звезда, а логички магистрала) дефинисане су стандардом IEEE 802.3, док су мреже у којима се приступ каналу обезбеђује помоћу жетона покривене стандардима IEEE 802.4 (магистрала са жетоном) и IEEE 802.5 (прстен са жетоном).

Данас се далеко најчешће срећу етернет мреже, тј. мреже које дефинише IEEE 802.3 стандард.

9.2.1. СТАНДАРДНЕ ВРСТЕ ЕТЕРНЕТ МРЕЖА

IEEE 802.3 дефинише две основне врсте етернет мрежа:

- етернет у основном опсегу (baseband Ethernet) и
- широкопојасни етернет (broadband Ethernet).

IEEE 802.3 дефинише пет стандарда за етернет у основном опсегу (10Base5, 10Base2, 10Base-T, 1Base5 и 100Base-T) и само један стандард за широкопојасни етернет (10Broad36).

Први број у називу стандарда означава брзину преноса у Mb/s, а последњи број или слово означава максималну дужину кабла (у стотинама метара) или врсту кабла. Када се говори о максимално дозвољеној дужини кабла, мисли се на случај када се не користе регенератори или мостови.

У случају етернета у основном опсегу носећи сигнал је поворка правоугаоних импулса. У случају широкопојасног етернета носећи сигнал је простопериодични сигнал.

9.2.1.1. 10Base5

Најстарији 802.3 стандард је 10Base5. Често се назива **дебели етернет** или **стандардни етернет**. Користи топологију у облику магистрале која се реализује помоћу коаксијалног кабла пречника око 1 cm (одакле и потиче назив *дебели*), којим се до удаљености од 500 метара без регенерисања преносе сигнали брзином од 10 Mb/s. Стандард дозвољава да се, због проблема са колизијама, регенераторима повезује највише пет сегмената, па зато 10Base5 мрежа може бити дугачка максимално 2,5 километара, док растојање између суседних станица не сме бити мање од 2,5 метра (слика 9.1). Зато се на један сегмент може да повеже највише 200 станица.



Слика 9.1. – Пример етернет мреже 10Base5 максималне дужине

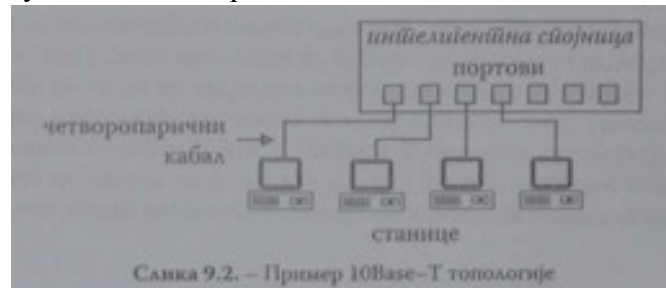
9.2.1.2. 10Base2

Као и 10Base5, тако и 10Base2 стандард користи топологију у облику магистрале и омогућава брзину преноса (проток) од 10 Mb/s. Назива се и **танки етернет** или **чипернет** (енгл.: *chipernet*). Сам назив *чипернет* (енгл.: *chip* = јефтин) указује да је ова мрежа јефтинија од 10Base5 мреже јер се користи тањи кабл (пречника око 0,5 cm). Због тога је инсталирање танког етернета лакше и јефтиније. Наравно, због мањег пресека кабла краће је растојање на које се сигнал може пренети без регенерисања: оно у овом случају износи 200 метара.

Зашто 802.3 стандард прописује да дужина сегмента не сме да буде већа од 500 метара у случају 10Base5 инсталације, односно од 200 метара у случају 10Base2 инсталације? Максимална дозвољена дужина сегмента везана је за могућност откривања колизије. Раније смо видели да станица утврђује да је дошло до колизије тако што открива да је снага сигнала на њеном прикључку на кабл већа од максималне снаге сигнала који она може да емитује. Зато станица стално испитује колика је снага сигнала на њеном прикључку и када снага пређе одређени, унапред утврђени праг, станица закључује да је дошло до колизије. Међутим, пошто сигнал слаби током простирања кроз медијум, када су две станице, станице *A* и *B*, сувише удаљене, сигнал који стиже из станице *A* до прикључка станице *B* толико је ослабљен да и када се суперпонира са управо емитованим сигналом из станице *B*, резултантни сигнал не прелази вредност прага. Пошто је слабљење утолико мање уколико је пресек проводника већи, стандард 802.3 ограничио је дужине сегмената дебелог и танког етернета на наведене вредности јер на овим растојањима при датим условима неће ни у случају најудаљенијих станица сигнал толико ослабити да у случају колизије резултантни сигнал не пређе унапред задати праг.

9.2.1.3. 10Base-T

Најчешћа етернет конфигурација је у облику звезде (слика 9.2). Стандард 10Base-T (Т - twisted-pair Ethernet = етернет са упреденом парицом) покрива локалне мреже које су физички реализоване у облику звезде и у којима се користе упредене парице одакле и потиче назив овог стандарда. Омогућава брзине преноса од 10 Mb/s, а максимално растојање између спојнице (хаба) и станице је 100 m. Користи се интелигентна спојница у коју се свака станица (тачније, њена мрежна картица) прикључује преко посебног порта помоћу четворопаричног кабла који се са обе стране завршава мушким конектором.



На слици 9.2 се види да је укључивање станица у мрежу и излажење из мреже веома једноставно.

С обзиром на то да физичка топологија 10Base-T инсталације има облик звезде, колизија се открива другачије но у случају топологије у облику магистрале. Наиме, чим спојница утврди да је на два или више портова присутан сигнал, она закључује да је дошло до колизије и зато генерише сигнал *присутна колизија* који прослеђује свим станицама.

Основни недостатак хаба је што пристигли рам из станице реемитује по свим својим портovima тако да они стижу до свих умрежених станица. Иако рам прихвата само она станица на коју је он адресован, при сваком преносу ангажован је цео капацитет мреже, свих 10 Mb/s. Пошто се капацитет мреже дели између станица, што се више станица повеже у мрежу утолико свака станица има на располагању, статистички посматрано, мањи део капацитета канала. Хаб можемо замислити као вишесмерну раскрсницу испред које свако возило мора да се заустави. Ако више возила истовремено стигне пред раскрсницу, свако возило мора да сачека свој ред да продужи пут. Лако је закључити шта се дешава када број путева који се уливају у раскрсницу расте: са порастом броја путева који се укрштају расту како време чекања на право проласка кроз раскрсницу, тако и вероватноћа судара (колизије).

Зато се хаб у данашњим 10Base-T мрежама готово не користи, већ се замењује свичом. Свич омогућава да се у мрежи истовремено одвија више сесија (разговора). Овакве мреже називају се *свичовани етернет*.

9.2.1.3.1. Свичовани етернет

Свич је „паметнији“ од хаба (зато, наравно, и скупљи): он препознаје адресу одредишта, па пристигли рам не упућује на све своје портове, већ само на порт на који је повезана одредишна станица. Тако свич омогућава различитим станицама у мрежи да међусобно директно комуницирају. Сада више корисника могу да у исто време шаљу информације по мрежи, а да при томе не успоравају једни друге јер свич може истовремено да прима рамове из више (теоријски из свих) умрежених станица и да их прослеђује у њихова одредишта, а да не дође до колизије.

Оновну разлику између хаба и свича илустроваћемо следећим примером.

Посматрајмо мрежу капацитета 10 Mb/s која повезује пет станица, при чему свих пет станица желе да емитују. У случају коришћења хаба свака станица може у овом случају да користи само петину укупног капацитета мреже, тј. 2 Mb/s. Ако се уместо хаба користи свич, онда свака станица (без обзира на то што и остале четири станице емитују) има на располагању целокупан капацитет мреже, тј. свих 10 Mb/s.

Наставимо малопређашњу аналогију са друмским саобраћајем. У друмском саобраћају право решење представља изградња раскрсница у више нивоа тако да један аутопут прелази преко другог аутопута, а прелаз са једног на други аутопут обавља се преко улазне и излазне траке. Тако свако возило прелази са једног на други аутопут без заустављања и чекања на раскрсници. У мрежном саобраћају свич управо обавља функцију раскрснице са више нивоа која омогућава да се пакетски саобраћај одвија без застоја при преласку са једне на другу путању.

Пошто свич омогућава да се у мрежи истовремено одвија више сесија (разговора), то је у оваквим мрежама омогућен дуплексни рад: информација може истовремено да путује од станице до свича и од свича до станице. Пре увођења свича етернет је био полудуплексни.

У свичованим мрежама користи се или упредена парица или оптички кабл. У оба случаја се за слање и за пријем података користе засебни проводници. У оваквим условима етернет станице могу се одређи процеса откривања колизија јер за саобраћај у сваком смеру постоји засебна путања.

У свичованој мрежи свич ради у другом OSI слоју, што значи да користи физичке адресе.

9.2.1.4. 1Base5

Стандард 1Base5 предвиђен је за примену у топологији у облику звезде, али се практично више и не користи због данашње потребе мале брзине преноса података.

9.2.1.5. 100Base-T

Брзина преноса података у стандардним етернет мрежама од 10 Mb/s није довољна при обради звука и слике у реалном времену. У стандарду 100Base-T, иначе познатијем као *брзи етернет* (енгл.: *Fast Ethernet*), користи се физичка топологија у облику звезде, као и у стандарду 10Base-T, а брзина рада је 100 Mb/s.

У етернет мрежама, ако брзина мреже расте, онда се сразмерно порасту брзине мора или повећати минимална дужина рама или смањити максимална дужина кабла. Пошто је брзина преноса у брзом етернету десет пута већа од брзине преноса у стандардном етернету и с обзиром на то да се задржава стандардни формат етернет рама, то се максимално дозвољено растојање између станица мора смањити десет пута те сада износи највише 250 m. У 100Base-T мрежама станице су обично удаљене од свича до неколико десетина метара, па ово смањење максимално дозвољеног растојања нема практичних последица на изградњу оваквих мрежа.

9.2.2. ГИГАБИТСКИ ЕТЕРНЕТ

Гигабитски етернет је новија технологија која, коришћењем ласерске технике и оптичког влакна, омогућава пренос брзинама реда Gb/s. И у овом етернету MAC подслој и начин приступа медијуму остају непромењени, али се мења физички слој, тј. преносни медијум и систем кодовања. Иако протоколи за гигабитски етернет дозвољавају употребу упредене парице и оптичког влакна, практично се користе оптички каблови. Гигабитски етернет се обично користи као *окосница* за повезивање мрежа са брзим етернетом.

9.3. БЕЖИЧНЕ ЛОКАЛНЕ МРЕЖЕ

Бежичне локалне мреже (WLAN - Wireless LAN) састоје се од фиксних и/или портабл рачунара који међусобно комуницирају невођеним ЕМТ, дакле, без коришћења физичких проводника. Бежични LAN-ови имају донекле различите особине од жичних LAN-ова, те зато захтевају посебне протоколе у MAC подслоју.

Сви уређаји повезани бежичним медијумом називају се *станице*. У свакој станици налази се *бежична мрежна интерфејс картица* (WNIC). Бежичне станице деле се у две групе: *тачке приступа* и *клијенте*. Тачке приступа су базне станице за бежичне мреже. Оне емитују и примају радио-сигнале како би се омогућило комуницирање бежичних уређаја. Бежични клијенти су мобилни уређаји као што су лаптопови, IP телефони, PDA или су то фиксни уређаји (као што су стони рачунари и радне станице) опремљени бежичним мрежним интерфејсом.

За пренос се користе невођени ЕМТ у фреквенцијском опсегу од 2,4 до 2,484 GHz за који није потребна дозвола за рад. У САД и Канади је поред овог опсега на располагању и опсег од 5,725 до 5,850 GHz. Ови опсези се користе за различите намене: поред већ споменуте примене у WLAN-овима, у овом опсегу раде бежични телефони, бежични звучници, системи за отварање гаражних врата и сл.

Бежични LAN-ови се све чешће формирају у пословним зградама. Унутар објекта се плански распоређују *базне станице* које су међусобно повезане бакарним или оптичким линијама. Ако је емисиона снага базних станица и фиксних и портабл рачунара подешена да има домет од 3 до 4 метра, тада свака просторија постаје једна ћелија, а цела зграда представља велики *целуларни* (ћелијски) систем као у случају мобилних телефонских система. Међутим, за разлику од мобилне телефоније, овде свака ћелија има само један канал који покрива цео расположиви опсег. Бежичне базне станице су жично везане са етернет мрежом и могу да имају домет од више десетина метара без обзира на евентуално постојање неметалних препрека, нпр. зидова. У принципу, између предајника и пријемника не мора да постоји оптичка видљивост. Корисници који се крећу могу да прелазе из домета једне у домет друге базне станице без раскидања везе, као и у системима мобилне телефоније.

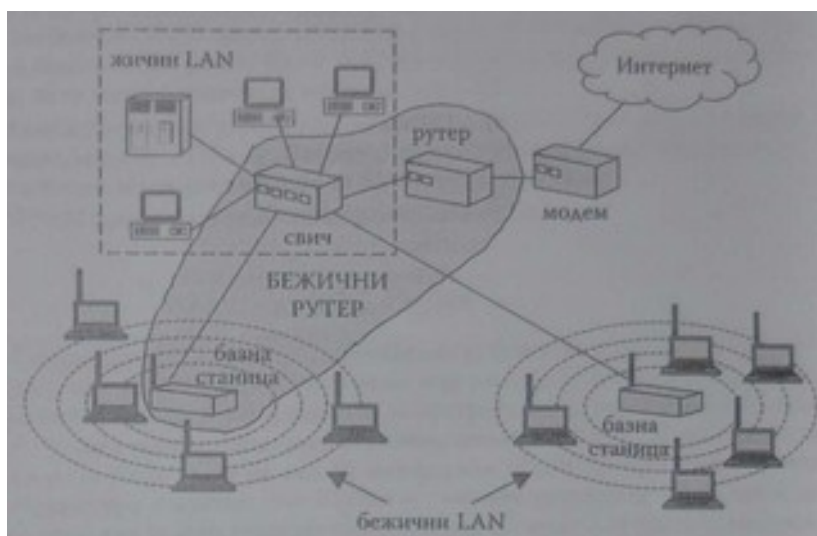
Функционисање бежичног LAN-а базира се на IEEE 802.11 стандарду који се обично назива Wi-Fi. Новији лаптопови се испоручују са уграђеним бежичним Wi-Fi адаптерима (примопредајницима), а у старије моделе се Wi-Fi адаптери прикључују преко USB порта или PC картичног слота. IEEE 802.11 спецификација дефинише физички слој и MAC подслој слоја везе OSI модела.

Wi-Fi базне станице обично су смештене у широкопојасне рутере и обезбеђују и жичну и бежичну комуникацију (слика 9.3).

Као што се на слици 9.3 види, бежични рутер садржи рутер, LAN свич и базну станицу.

У WLAN-овима се користи техника проширеног спектра или ортогонално фреквенцијско мултиплексовање (OFDM).

Бежични LAN-ови се лако повезују са другим мрежама и мрежним компонентама, а трошкови формирања су нижи но у случају LAN-ова са физичким линијама. WLAN-ови су постали популарни јер пружају следеће предности:



Слика 9.3. — Бежични LAN. Бежични LAN-ови раде као и системи мобилне телефоније: свака базна станица је тачка приступа која омогућава пријем унутар круга одређеног пречника. Корисници могу да се крећу између базних станица без раскидања везе. Бежични рутер обједињује у једном уређају LAN свич, рутер и једну базну станицу

- корисници могу да приступе мрежним ресурсима са сваког њима погодног места,
- корисници могу да приступе Интернету чак и када се не налазе у свом уобичајеном радном окружењу,
- корисници повезани у бежичну мрежу могу да остану готово стално повезани са својим послом и када путују,
- у бежичним мрежама број корисника лако се повећава за разлику од жичних мрежа у којима повећање броја корисника захтева да се обави инсталирање додатних линкова,
- иако је цена хардвера за бежичне мреже нешто већа од хардвера за жичне мреже, уштеда се остварује на основу цене каблова и трошкова њиховог постављања.

WLAN технологија има и својих недостатака:

- безбедност, јер се на бежичним мрежним картицама обично, ради уштеде, користе јефтине антене. Због тога је за неовлашћено прислушкивање довољно набавити квалитетнију антену, чиме се омогућава „хватање“ пакете и са раздаљине чак неколико стотина пута веће од пречника унутар кога обичан корисник прима саобраћа),
- домет - типичан домет WLAN-а са стандардном опремом је до неколико десетина метара. То је обично довољно за мреже у оквиру неке зграде или објекта, али је недовољно ако се ради о већим површинама, па се морају поставити репетитори или додатне базне станице што по већава трошкове,
- поузданост - радио-таласи и сигнали у бежичним мрежама подложни су интерференцији због чега долази до појаве вишеструких путања емитованог сигнала, што у одредишту може да доведе до делимичног или потпуног ишчезавања сигнала. Зато се важни мрежни ресурси, нпр., сервери, ретко бежично повезују,
- брзина - у већини WLAN-ова брзина преноса података је знатно мања но у ожиченим LAN-овима. Уобичајене брзине WLAN-ова се налазе у интервалу од 1 до 108 Mb/s, а брзине ожичених LAN-ова крећу се од 100 Mb/s до неколико Gb/s.

Паралелно са Wi-Fi техником преноса развијене су још две технике преноса у микроталасном подручју, такође на фреквенцији од 2,4 GHz, за који није потребна дозвола за рад. Користе се за комуникацију на веома кратким растојањима реда неколико метара или неколико десетина метара: Bluetooth и ZigBee.

9.3.1. BLUETOOTH

Bluetooth је техника бежичног преноса при чему се користе неусмерени ра дио-таласи који могу да пролазе кроз неметалне препреке, па није потребно да постоји оптичка видљивост између уређаја који су унутар домета сигнала. Ради у микроталасном подручју у опсегу учестаности од 2,4 GHz до 2,484 GHz (што значи да није потребна дозвола за рад) и користи технику проширеног спектра са фреквенцијским скакањем (фреквенција сигнала се мења 1.600 пута у секунди). Максимална брзина преноса је 720 kb/s. Максимална излазна снага, зависно од верзије, износи 1 mW, 2,5 mW и 100 mW. Користи се у тачка-тачка и вишетачкастим везама за пренос података и дигитализованог говорног сигнала на веома кратким растојањима (обично до 10 m) и не подржава роминг. Примењује се у WPAN, тј. у бежичним персоналним мрежама. Омогућава повезивање и размену информација између различитих дигиталних уређаја: мобилних телефона, персоналних рачунара, лаптопова, дигиталних камера, конзола за видео-игре, као и за комуникацију између рачунара и његових улазно-излазних јединица (тастатура, миш, штампач). Много се употребљава при коришћењу мобилног телефона када руке треба да буду слободне (нпр., током вожње аутомобила). Уз одређена побољшања домет може да се повећа и до 100 m (повећањем емисионе снаге), а брзина преноса до 3 Mb/s (одговарајућим начином кодовања).

Bluetooth и Wi-Fi раде на истој учестаности и користе технику преноса са проширеним спектром, али служе у различитим случајевима. Wi-Fi покрива већа растојања, омогућава брже успостављање везе, већу брзину преноса и већу безбедност, али је хардвер који се користи скупљи, а и потрошња енергије је већа. Wi-Fi замењује каблове само у LAN-овима и зато се често назива *бежични Етернет*. Bluetooth замењује физички медијум у низу случајева, па се може посматрати као бежични USB.

Bluetooth се данас уграђује и низ уређаја: мобилне телефоне, лаптопове, штампаче, модеме, PDA итд. Персонални рачунар мора да има Bluetooth адаптер да би могао да комуницира са Bluetooth уређајима.

WPAN мреже раде под стандардом IEEE 802.15.

9.3.2. ZigBee

Стандардом IEEE 802.15.4 дефинисана је бежична PAN мрежа (тачније физички слој и MAC подслој слоја везе) која ради на 2,4 GHz или у радио-опсегу на 868 MHz који је резервисан за индустрију, науку и медицину (тзв. ISM | опсег). Брзина преноса података је до максимално 250 kb/s. Пренос се може реализовати у пречнику од око 50 метара, али домет сигнала много зависи од температуре и влажности. ZigBee је спорији не само од Wi-Fi већ и од Bluetooth-a, али је зато економичнији јер има врло малу потрошњу енергије, што омогућава да батерије трају годинама.

ZigBee техника је једноставнија и јефтинија од Bluetooth-a. ZigBee мреже могу имати звездасту или непотпуно повезану топологију. Ове мреже обично се користе за контролу и управљање у индустрији или у великим зградама тако што периодично преносе мале пакете из сензора те се тако у неком објекту, нпр., регулише јачина осветљења, рад мотора и функционисање других уређаја. Такође се користе за прикупљање медицинских података (нпр., непрекидна контрола болесника који су под надзором).

9.3.3. ИНФРАЦРВЕНЕ МРЕЖЕ

У оквиру IEEE 802.11 стандарда постоји модул 802.11IR (IR - infrared = инфрацрвени) који, као што и сам назив показује, дефинише пренос података у инфрацрвеном делу спектра.

Основна разлика између бежичних инфрацрвених и радио LAN-ова јесте у фреквенцији преношених сигнала. Бежични LAN-ови раде на учестаностима које се налазе у опсезима око 2,4 GHz и око 5 GHz, док инфрацрвени системи користе фреквенције у терахерц опсегу. Инфрацрвени сигнали се налазе у области светлости која је невидљива за људско око и није под контролом Федералне комисије за комуникације (FCC).

IEEE 802.11 IR дефинише пренос података унутар само једне просторије (јер светлост не може да прође кроз зидове) брзином од 1 Mb/s и 2 Mb/s. Подаци се преносе у облику светлосних импулса који одговарају логичким јединицама м нулама.

Треба напоменути да се за сада не могу набавити системи који су потпуно сагласни са 802.11 IR стандардом, мада на тржишту има IR LAN-ова који су близу стандарда.

Инфрацрвени LAN има следеће карактеристике:

- велики степен безбедности — инфрацрвена светлост не пролази кроз зидове, па је готово немогуће да неовлашћена особа изван просторије у којој је IR LAN прислушкује саобраћај који се одвија унутар те просторије,
- нема интерференције са радио-фреквенцијама - пошто IR LAN-ови раде у опсегу учестаности светлости, не може да дође до интерференције са унутрашњим или спољашњим системима који користе радио-сигнале. IR LAN може да задовољи специфичне мобилне примене (нпр., оне које захтевају веома велики степен безбедности) у средини у којој функционише бежични радио LAN.
- ограничени домет — инфрацрвена светлост не пролази кроз зидове, па је неопходно да у свакој просторији постоји базна станица,
- непоштовање 802.11IR стандарда - како на тржишту за сада нема производа који су потпуно сагласни 802.11 IR стандарду, није могуће формирати IR LAN од елемената (базне станице и уређаја за конвертовање сигнала) различитих произвођача.

9.4. ЗАШТИТА ПОДАТАКА НА МРЕЖИ

Интернет безбедност или IS (Internet Security) је широк појам који се односи на разноврсне кораке које предузимају појединци и организације како би заштитили рачунаре и рачунарске мреже повезане на Интернет. *Системи за безбедност на Интернету* или ISS (Internet Security Systems) јесу уређаји и софтвер који су развијени и свакодневно се усавршавају како би се заштитили интереси корисника рачунарских мрежа од разних видова злоупотребе путем Интернета која у појединим случајевима добија облик сајбер криминала.

Термин *ISS сервер* је општи назив за разне врсте система који имају за циљ да обезбеде несметано функционисање мреже и може да означава било безбедносни софтвер, било рачунар у коме се реализује овај софтвер.

Интернет по својој природи није безбедна средина јер је то отворена рачунарска мрежа која има за циљ да олакша размену информација. Подаци послати преко Интернета било да се ради о личној електронској пошти, било он-лајн куповини, путују кроз низ рачунара и линкова чији се број стално мења. Због тога злонамерници и хакери могу да пресретну и промене поруку.

Најпознатији проблем представљају *вируси*. Неки од њих у корисниковом рачунару модификују програме и тако их чине неупотребљивим, док други оштећују и уништавају

податке. Многи вируси се брзо шире и суптилно обављају свој деструктивни задатак тако да се не запажају све док не направе знатну штету.

Ради заштите од вируса развијено је много антивирусних програма и они се непрестано усавршавају. Данас се готово сви персонални рачунари продају са уграђеним антивирусним софтвером. Разни облици антивирусног софтвера користи се и у рачунарским мрежама. Корисници могу да преко Мреже непрекидно ажурирају своје антивирусне програме. Такође је корисно често правити резервне копије својих фајлова.

Хакери се најчешће труде да неовлашћено уђу у рачунарски систем и да онда изнутра мењају или краду информације. Један од начина на који хакери улазе у рачунарску мрежу јесте коришћење отвореног порта или конекције Интернета која је остала отворена и после завршетка сесије. Такође покушавају да дођу до *лозинке* (password) корисника тако што се труде да погоде лозинку или користе програме који лоцирају или хватају информацију о лозинци. Веома често хакери користе тзв. *e-mail њушкање*: овлашћеном кориснику рачунарске мреже стиже лажна електронска пошта која изгледа као да ју је послао неко кога корисник зна. Потом хакер покушава да превари корисника да му ода своју лозинку или неке друге пословне тајне.

Други веома чест начин који хакери примењују јесте да одређени систем споља преплаве информацијама и тако му онемогуће рад. То постижу тако што на жељени Интернет сајт шаљу енорман број порука, због чега долази до загушења система, па стварне поруке не могу да стигну у систем.

Посебан проблем представљају тзв. *spyware* или *шпијунски програми*. То је софтвер који се крадомице инсталира у корисников рачунар са циљем да неопажено, без знања власника рачунара, прикупља информације о кориснику било то особа или организација, било да преузме делимичну или потпуну контролу над радом рачунара. Шпијунски програми брзо се „угнезде“ у корисниковом рачунару, обично током „сурфовања“ по Мрежи и „скидања“ података са веб-сајтова. Потом неопажено, док корисник крстари Интернетом, шаљу информације „тамо где треба“.

У борби против spyware програма развијени су програми за њихову блокаду. Ови блокатори шпијунских програма постали су популарни готово као и антивирусни програми.

Проблеме корисницима Мреже чини и нежељена електронска пошта, тзв. *спам* (енгл.: spam). Обично су то рекламне поруке и разноврсне понуде, мада могу бити и поруке друштвене и политичке природе. Пошто се шаљу у огромним количинама и огромном броју корисника, спамови могу да доведу до загушења како појединих сегмената мреже, тако и рачунара корисника. У спамовима су релативно често, ненамерно или намерно, уграђени вируси. Зато је основно правило да се не отвара електронска пошта ако се не познаје пошиљалац. За борбу против спам порука развијен је *антиспам софтвер* који се обично уграђује у сервере и рутере, мада се може поставити и у рачунаре корисника. Овај софтвер филтрира, тј. одбацује све поруке за које утврди да представљају спам тако што их брише или их смешта у тзв. *спам фолдер*.

Има више начина да се спречи недозвољени приступ рачунарским системима. Најчешћа метода је провера (аутентикација) корисника путем лозинке. Пошто лозинка може да се украде или да се погоди, развијене су рафиниране методе провере да ли је особа која тражи приступ заиста овлашћени корисник (софтвер за препознавање гласа, системи за скенирање зенице и системи за препознавање рукописа). За аутентификацију банкарских и других докумената користи се *дигтални потпис*.

Један од најефикаснијих начина заштите рачунарске мреже која је повезана на Интернет од недозвољеног приступа споља представља *заштитни зид*, односно *мрежна баријера* (енгл.: *firewall*). То је хардверски безбедносни уређај који се поставља између рачунарске мреже и Интернета. Ради као веб-сервер: рутира саобраћај, али такође блокира приступ спољашњим

корисницима у унутрашњи рачунарски систем.

Наравно, мрежна баријера не може да заштити информације када оне напусте интерну мрежу. Општи начин спречавања неке неовлашћене особе да користи податке који путују кроз мрежу је да се подаци шифрују. Криптографски програми на отпреми модификују облик података тако да се не могу прочитати без одговарајућег кључа.

9.4.1. ЗАШТИТНИ ЗИД (Firewall)

Заштитни зид или *firewall* је рачунарски безбедносни систем који контролише проток података из једне мреже у другу мрежу. Његова главна намена јесте да заштити ресурсе приватне мреже тако што не дозвољава кориснику из спољашње мреже, посебно преко Интернета, да им приступи. И корисницима унутар приватне мреже може се онемогућити приступ рачунарима у другим мрежама. То се реализује тако што се целокупна комуникација одвија преко проху сервера који одлучује да ли се поруци или фајлу може дозволити улаз у локалну мрежу или излаз из ње.

Заштитни зид веома се много користи и представља основни безбедносни метод јер се, с једне стране, омогућава корисницима безбедан приступ Интернету, а с друге, одваја јавни веб сервер предузећа од његове интерне мреже. Заштитни зид се, такође, користи како би се сачувала безбедност сегмената интерне мреже (нпр., унутар неке компаније треба онемогућити да се сегменту мреже који припада финансијском одељењу неовлашћено приступа из неких других сегмената мреже).

У кућним рачунарима персонални заштитни зид је обично инсталиран у корисниковом рачунару. Пример персоналног заштитног зида је Windows-ов заштитни зид који је уграђен у оперативне системе Windows XP, Windows

Server 2003 и Windows Vista. Заштитни зид прегледа пакете и пропушта само оне који представљају одговор на захтев који је поставио корисник. Тако се спречава да спољашњи корисник захтева податке ако није претходно добио дозволу за то.

У организацијама заштитни зид је самостални рачунар или софтвер у рутеру или у серверу. То може да буде једноставно рутер који филтрира, тј. одбацује нежељене пакете или може да обухвата комбинацију рутера и сервера при чему сваки од њих обавља одређену врсту заштитне обраде. Наиме, постоје различите методе заштите које се користе у заштитном зиду. Често се ради постизања веће безбедности користи комбинација неколико ових метода. Проху сервер је један од алата помоћу којих се формира ватрени зид.

9.4.2. PROXY SERVER

Прокси *Proxy сервер* или краће прокси има задатак да помогне у спречавању неовлашћеног упада у приватну мрежу. Проху сервер је рачунар или рутер који ради као прекидачка компонента између две мреже, односно између клијента и сервера тако што раскида везу између предајника и пријемника.

Као што и сам назив каже, прокси сервер ради по овалашћењу клијента и сервера. Сваки захтев клијента који је упућен серверу који се налази у интернету или у Интернету иде прво на прокси сервер. Прокси сервер га процењу је и ако је такав захтев допуштен, пропушта га на свој излазни порт ка интернету, односно Интернету. Исто тако, одговор или захтев који стиже са интернета или Интернета иду прво на процену у прокси сервер. И клијент и сервер имају утисак да директно комуницирају, а у ствари сваки од њих комуницира са прокси сервером.

Прокси сервер је, дакле, повезан у две мреже, па има две IP адресе (слика 9.4). Интернет види IP адресу са интернет стране проксија, док адреса станице која шаље захтев остаје скривена за спољни свет. Прокси сервери често се користе заједно са NAT софтвером (Network Address Translation) који скрива IP адресе клијент станице.

У енглеском реч „проху“ значи *радити у име*, односно *по овлашћењу*ца у унутрашњој мрежи. Прокси сервери могу, такође, да сместе веб-странице у своју кеш меморију, те се те странице могу испоручити знатно брже када неки други клијент захтева исте странице.



9.4.3. MAIL SERVER

Интернет систем електронске поште (SMTP - Simple Mail Transfer Protocol), такође, се заснива на принципу прокси сервера: електронска пошта не шаље се директно од пошиљаоца до примаоца, већ прво иде на mail сервер.

Mail или *поштански сервер* термин је који означава рачунар или софтвер који у мрежи обавља поштанске послове. У mail серверу се меморише пошта која стиже и потом се, ради даље дистрибуције примаоцима, прослеђује кроз одговарајући канал.

Два најпознатија стандардна интерфејса између e-mail клијента и mail сервера јесу POP3 (Post Office Protocol 3) и IMAP4 (Internet Message Access Protocol). Ове протоколе користе клијенти за комуникацију са mail сервером, тј. за слање своје електронске поште у mail сервер и за пријем електронске оште из mail сервера.

9.4.3. ВЕБ-СЕРВЕР

Термин веб-сервер означава рачунар или само софтвер који прихвата HTTP захтеве који стижу из клијената и враћа им HTTP одговоре у облику HTML докумената.

Када веб-сервер није јаван, већ се интерно користи, понекад се назива *Интранет сервер*.

Веб-сервери се не користе само за испоручивање веб-страница. веб-серверски софтвер се уграђује у много хардверских уређаја: било који мрежни уређај, нпр., рутер, тачка приступа или штампарски сервер може имати интерни веб-сервер (HTTP сервер) коме се приступа преко његове IP адресе исто као и веб-сајту.

Један рачунарски систем који би у неком мањем предузећу или установи пружао све Интернет услуге морао би, поред осталог, обавезно да садржи SMTP сервер (услуга електронске поште), FTP сервер („скидање“ фајлова), HTTP сервер (веб странице и фајлови) и NNTP сервер (дискусионе групе). Систем који би обезбеђивао све ове услуге представљао би веб-сервер. У великим системима свака услуга може се реализовати у засебном рачунару или групи рачунара. Тако велики јавни веб-сајт може да садржи велики број веб-сервера.

1. Набројте основне карактеристике локалних мрежа.
2. Који фактори одређују природу локалне мреже?
3. Које се врсте медијума користе у жичним LAN-овима и када?
4. Да ли је кашњење у просеку веће у широкопојасним мрежама или у мрежама које раде у основном опсегу? Покушајте да објасните зашто!
5. Које су особине peer-to-peer, а које клијент-серверских мрежних оперативних система?
6. Набројте стандардне врсте етернет мрежа и њихове карактеристике.
7. Каква је разлика између LAN-а у са хабом и LAN-а са свичом?
8. Шта је то WLAN? У којим случајевима се користи?
9. Који су недостаци бежичних LAN-ова?
10. Каква је то Bluetooth технологија? Када се користи?
11. Упоредити Bluetooth и ZigBee технологију.
12. Набројте најважније карактеристике инфрацрвених LAN-ова.
13. Због чега је неопходна заштита података на мрежи? Како се реализује?
14. Шта је то *заштитни зид*? Како функционише?
15. Шта је задатак прокси сервера?
16. Која је сличност између прокси сервера и поштанског сервера?
17. Да ли термин *веб-сервер* означава рачунар или софтвер? Каква је разлика између веб-сервера и интранет сервера?