PCS3-NW

Autorë: Roland Bauch, Martin Dausch, Michael Raith

Botimi I në Gusht 2007

Internet: www.herdt.com

Projekt:
• Arsimimi i të Rriturve në Shqipëri
• Adult Education in Albania
• Erwachsenenbildung in Albanien

Rr. "Bogdani", P.7/5A, P.O.BOX 8153
Tiranë, Shqipëri (Albania)
Tel: +355-4-257477; 259494
Fax: +355-4-257476
Email: office@parsh.org.al
Internet: www.parsh.org.al

Përkthyes: Dipl.Ing. Thoma Kero

Redaktimi letrar: Irena Nasi

Përshtatja grafike: Dipl.Ing. Thoma Kero

Faqosja: Elvira Çiraku

Shtypi: Shtëpia Botuese Vernon Publishing

Administrimi dhe mirëmbajtja e sistemeve dhe rrjeteve kompjuterike

Teknologjitë e rrjeteve dhe Internetit

PCS3-NW

Mbështetur me mjete financiare të Delegacionit të Komisionit Evropian

ISBN: 978-99943-55-30-3

1 Rrjetet e kompjuterave - Bazat

Në këtë kapitull do të lexoni:

→ Ç'kuptohet me rrjet kompjuterash?

→ Ç'lloje rrjetesh ekzistojnë?

Parakusht:

✓ Njohuri të përgjithshme mbi kompjuterin.

1.1 Nga se dallohet një rrjet kompjuterash?

Ç'është një rrjet kompjuterik?

Në përgjithësi, një rrjet paraqet një grup sistemesh të lidhur me njëritjetrin, të cilët mund të komunikojnë ndërmjet tyre. Themi se kemi të bëjmë me një rrjet kompjuterik, në qoftë se minimumi 2 kompjutera janë lidhur në mënyrë të tillë që të mundësojnë shkëmbimin e të dhënave ndërmjet tyre.

Dy kompjutera të lidhur me një kabëll

Ekzistojnë këto lloje rrjetesh kompjuterike:

Rrjetet lokale (LAN - Local Area Network)

Një LAN dallohet nga dy karakteristikave bazë: Shtrirja e tij gjeografike është e kufizuar, dhe kjo shtrirje nuk e kalon kufirin e sipërfaqes ku është vendosur firma. I gjithë hardware-i gjendet plotësisht në zonën e juridiksionit dhe nën mbikqyrjen e një përdoruesi, respektivisht të një firme.

Në rrjetet lokale transferimi i të dhënave, në shumicën e rasteve, kryhet përmes kabllit. **Karta e rrjetit** administron transferimin e të dhënave nga kompjuteri në kabëll dhe anasjelltas. Ajo vendoset në të ashtuquajturin *extention slot* në motherboard. Çdo kartë rrjeti ka një numër (adresë), i cili është unik dhe i pandryshueshëm në të gjithë botën (MAC-Address). MAC-Address-a shërben për identifikimin e qartë të stacionit të punës brenda rrjetit.

Rrjetet lokale pa kabëll (WLAN - Wireless Local Area Network)

Wireless Local Area Network (rrjeti lokal pa kabëll) është një variant i LAN-it dhe dallohet nga ky i fundit nga media që përdor për transmetimin e të dhënave. Për transferimin e të dhënave në këtë rast, në vend të kabllit përdoret teknologjia e radiopërhapjes. Për shembull, njëri nga standardet që përdoret mjaft kohët e fundit për transmetimin e të dhënave (në një zonë rrethuese prej afro 10 metrash) është Bluetooth-i.

Përsa i përket aspektit të **sigurisë** tek WLAN-i ka shumë elemente për t'u marrë në konsideratë, elemente të cilat sjellin për pasojë një harxhim më të madh kohe për konfigurim.

☑ WLAN-i duhet të ketë një emër të koduar (përzierje gërmash, shifrash dhe karakteresh te veçanta). I ashtuquajturi SSID (Service Set Identifier) duhet „fshehur". Në këtë mënyrë pengohet që WLAN-i t'u njoftojë emrin e tij me transmetim në grup (broadcast) klientëve potencialë, si dhe nga ana tjetër arrihet që klienti duhet të japë saktësisht emrin e WLAN-it në mënyrë që të lidhet me të.

☑ WLAN-in lejohen ta aksesojnë vetëm klientët, adresa e kartave të rrjetit të të cilëve është e regjistruar në listen e aksesit të krijuar për këtë qëllim.

☑ Transferimi i të dhënave në WLAN duhet të bëhet vetëm i koduar.

Krahasimi LAN/WAN

Tradicionalisht i rëndësishëm në LAN është transferimi i të dhënave, në WAN shtohen edhe elemente të tjerë si transmetimi i zërit (rrjeti telefonik) dhe i figurave lëvizëse (rrjeti i televizionit kabllor).

Një karakteristikë kryesore e LAN-it është që të gjithë përbërësit e rrjetit zotërohen nga firma përkatëse. Karakteristikë kryesore e WAN-it është që trafiku i të dhënave, të paktën në pjesë të caktuara, kalon edhe në linja të cilat nuk janë në pronësi të firmës, që në një formë, apo një tjetër, duhen „marrë me qira".

	LAN	WAN
Koncepti	Transferimi i të dhënave në një zonë të kufizuar	Transferimi i zërit, i të dhënave dhe videove në largësi të mëdha.
Shkalla e transmetimit	10 Mbps deri 10 Gbps	64 Kbps deri 622 Mbps, respektivisht 10 Gbps
Pronësia	Në zotërim të përdoruesit	Në zotërim të një kompanie publike apo private

Ndërtimi i një WAN-i në pronësi të vetë firmës ka kuptim dhe është rentabël vetëm në shumë pak ndërmarrje, apo organizata. Kostot respektive, për shembull për kabllin, mirëmbajtjen, apo mbikqyrjen e rrjetit, do të sillnin shpesh vlera amortizimi të shtrira në afate kohore mjaft të gjata.

Në këtë ndërvarësi duhen përmendur termat Internet, Intranet dhe Extranet, meqë ato e bëjnë të qartë ndryshimin, prej termave klasike LAN dhe WAN.

MAN - Metropolitan Area Network

Shtrirja e MAN-it kufizohet në hapësirën e një qyteti, ose një qendre industriale dhe përfshin largësi prej rreth 100 km.

WAN - Wide Area Network

WAN-i, i quajtur ndryshe dhe rrjet me shtrirje të gjerë, nuk kufizohet në shtrirjen e tij gjeografike. Në formën e tij klasike ai sherbente per lidhjen e pajisjeve kompjuterike në distanca të largëta. Të dhënat, në shumicën e rasteve, transferohen nëpërmjet linjave publike, për shfrytëzimin e të cilave ka tarifa të caktuara. Firmat mund ta shfrytëzojnë WAN-in si lidhje të LAN-eve të veçanta të tyre.

GAN - Global Area Network

Termi GAN përshkruan shtrirjen e një WAN-i në një dimension global. Në një rrjet global largësitë ndërmjet kompjuterave që komunikojnë mund t'i kalojnë mijëra kilometrat. Të dhënat kalojnë në rrugën e tyre nga dërguesi tek marrësi, shumë stacione ndërmjetëse (routera). Distanca kalohet jo si një e tërë, por e ndarë në shumë segmente.

Interneti

Interneti është sot për sot GAN-i më i madh që egziston. Kompjutera të panumërt në mbarë botën mund të lidhen me njëri-tjetrin në rrugë nga më të ndryshmet dhe të shkëmbejnë informacione.

Meqë gjithnjë e më shumë fusha të zinxhirit të prodhimit ekonomik po ndryshojnë në varësi të Internetit, flitet tashmë për një „revolucion ekonomik" me pëmasa të ngjashme me industrializimin.

Intraneti

Intranet-i është një LAN, që është ndërtuar duke përdorur teknikat e Internetit. Krahas përdorimit të TCP/IP-së si protokoll standard, vihet re përdorimi i Web-Serverave, te cilët mbështesin komunikimin e punonjësve bazuar në të ashtuquajturën „browser technologies". Intranet-i shfrytëzon lidhjet në rrjet të vetë firmës për shkëmbimin në gjithë firmën e të dhënave në formë teksti, grafikësh dhe videosh.

Ekstraneti

Extranet-i është bashkimi i kontrolluar i lidhjeve të intraneteve të firmave të ndryshme. Ai është hapja me jashtë e intranetit të vetë firmave për aksesime të ligjshme nga interneti, apo për çiftimin me intranete të tjera.

Përparësitë e rrjeteve lokale

- ☑ **Komunikim i shpejtë:** Në një rrjet lokal dy apo më shumë stacione pune lidhen me njëri-tjetrin nëpërmjet një kablli. Nëpërmjet këtij kablli dërgohen të dhënat nga njëri kompjuter në tjetrin. Rrjeti kompjuterik përdoret për transmetimin e njoftimeve dhe paraqet në këtë mënyrë një mjet komunikimi. Njoftimet për punonjësit dërgohen në formën e postës elektronike (e-mail). Edhe në rastin kur në një moment të caktuar, i adresuari, nuk është duke punuar në kompjuterin e tij, informacioni nuk humbet. Ai memorizohet dhe punonjësi e merr atë sapo ky i fundit ndez kompjuterin dhe bën identifikimin (log on) në rrjet.
- ☑ **Shfrytëzim i përbashkët i të dhënave:** Të dhënat, të cilat shfrytëzohen nga disa persona, memorizohen në rrjet vetëm në një vend të caktuar. Të gjithë punonjësit, nga vendi i tyre i punës (kompjuteri i tyre) kanë akses nëpërmjet rrjetit mbi këto të dhëna të përbashkëta. Në këtë mënyrë, punonjësit përdorin gjithmonë të dhënat aktuale. Gabimet, të cilat shkaktoheshin nga të dhëna jo uniforme dhe të memorizuara në disa vende (kompjutera), nuk ndodhin më.
- ☑ **Sigurimi qendror i të dhënave:** Përmes ruajtjes së të dhënave në një kompjuter në rrjet, krijohet mundësia e sigurimit (backup-it) në mënyrë qendrore të të dhënave të rëndësishme. Krahasuar me sigurimin e të dhënave në kompjutera të veçantë, kjo sjell në një masë të madhe lehtësimin e punës së administratorit të rrjetit.
- ☑ **Shfrytëzimi i përbashkët i mjeteve të punës:** Pajisje të kushtueshme, si printera me ngjyra, apo plloteta, mund të shfrytëzohen nga gjithë punonjësit nëpërmjet rrjetit. Kjo zvogëlon kostot për investime.
- ☑ **Shfrytëzim i përbashkët i Software-ve:** Shumë programe aplikative ekzistojnë në version për rrjet. Këto programe instalohen në një kompjuter qendror në rrjet, në të ashtuquajturin server rrjeti, dhe mund të kërkohen nga disa stacione pune (të ashtuquajturit klientë, apo stacione pune). Programi, pasi kërkohet nga klienti nëpërmjet rrjetit, ngarkohet në memorien operative të stacionit të punës së klientit. Në këtë mënyrë kursehet vend në memorien e diskut të ngurtë të klientit. Sektori i TI*-së mund të punojë në mënyrë më efektive, në rast se bën të mundur që programet e rishikuara dhe përmirësuara të mos instalohen veçmas në çdo kompjuter. Përveç kësaj, shfrytëzimi i përbashkët i softwareve çon në thjeshtëzimin e administrimit të të drejtave të licensave (inventarizim softwaresh), si dhe mundëson zgjidhje më ekonomike për softwaret speciale, të cilat nuk mund të vihen në dispozicion njëkohësisht për të gjitha sistemet.
- ☑ **Administrim qendror:** Ky lejon përcaktimin e përbashkët të elemetëve të sigurisë për klientët.

1.2 Klienti dhe Serveri

Roli i kompjuterave të veçantë në shkëmbimin e të dhënave

Në një rrjet shkëmbehen të dhëna ndërmjet kompjuterave të ndryshëm. Gjatë shkëmbimit të të dhënave, kompjuterat e angazhuar në këtë proces marrin përsipër secili nga një rol të veçantë.

Çdo shkëmbim të dhënash kryhet sipas të njëjtit parim: kompjuteri **klient**, dërgon një kërkesë tek një kompjuter tjetër **(serveri)**. Serveri i dërgon më pas klientit shërbimin e kërkuar.

Sistemet operative të rrjeteve dhe serverave

Si sistem operativ rrjeti mund të përdoret çdo sistem operativ, i cili mundëson komunikimin midis kompjuterave të lidhur ne rrjet. Po të marrim si shembull produktet e kompanisë së prodhimit të software-ve Microsoft, të gjitha sistemet operative që nga Windows 3.11 bëjnë të mundur komunikimin në rrjet.

Me *sistem operativ për server* kuptohet ai sistem operativ i konceptuar në mënyrë të tillë që, t'i ketë të integruara të gjitha funksionet bazë të rrjetit, të nevojshme për komunikimin klient dhe server, si dhe të jetë i optimizuar për aksesim nga shumë klientë njëherazi.

Si rregull sistemi operativ i serverit përbëhet nga dy komponente: prej software-it për server dhe për klient.

Në çdo kompjuter të lidhur në rrjet, punon në sfond i ashtuquajturi Client-Software (programi klient). Ai administron kërkesat e përdoruesit (p. sh. hapjen e një skedari në server) dhe e dërgon këtë informacion më tej në server. Përveç kësaj Client-Software-i merr të gjitha të dhënat dhe ia ve ato në dispozicion përdoruesit.

*TI – Teknologjia e informacionit

Pjesa tjetër e software-it të rrjetit (Server-Software - programi server) punon në Server. Programi administron të gjitha kërkesat që vijnë, kryen përpunimet e duhura dhe i jep dërguesit të kërkesës (klientit) informacionin përkatës.

Sistemet që përdoren sot si sisteme operative për servera janë p.sh. Windows 2000 (Advanced) Server dhe Windows 2003 (Advanced) Server. Këto sisteme operative komunikojnë me ato të klientëve, respektivisht në versionet Windows 2000 Professional dhe Windows XP Professional, të cilat mund të përdoren edhe të vetme (të pavarura) si sisteme operative të instaluara në një stacion pune.

Lejimi i shfrytëzimit të pajisjeve të punës në rrjet

Në mënyrë që punonjësit të shfytëzojnë nëpërmjet rrjetit të dhënat dhe pajisjet e kompjuterave të tjerë, duhet që këto këto pajisje pune të lejohen për t'u përdorur në rrjet.

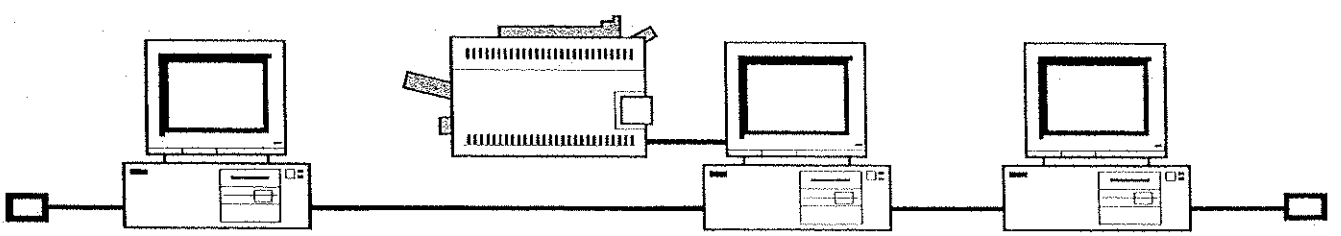
Mundësia për të vënë në dispozicion burimet – resurset - (printer, pajisje, disqe të ngurtë) e një kompjuteri për t'u shfytëzuar në rrjet, është një karakteristikë e veçantë pune e sistemit operativ.

1.3 Rrjetet Peer-to-Peer (kokë-më-kokë)

Ndërtimi i një rrjeti Peer-to-Peer

Në një rrjet Peer-to-Peer janë të lidhur me njëri-tjetrin disa kompjutera të barazvlershëm. Kompjuterat kanë të njëjtat të drejta ndaj njëri-tjetrit. Ata të gjithë përmbushin të njëjtat detyra.

- ☑ Çdo kompjuter shërben pikësëpari si stacion pune për një punonjës.
- ☑ Përveç kësaj çdo kompjuter mund të kryejë detyra të caktuara për një kompjuter tjetër.
- ☑ Çdo kompjuter në një rrjet Peer-to-Peer mund të shërbejë si server dhe si klient.



Rrjeti Peer-to-Peer

Rrjeti Peer-to-Peer është i përshtatshëm veçanërisht në rastet, kur vetëm pak kompjutera janë lidhur me njëri- tjetrin. Rrjeti është i „tejdukshëm" dhe i strukturuar thjesht.

Windows-i 3.11 for Workgroups, Windows-i 9x dhe Windows NT, respektivisht 2000 ose XP, ofrojnë funksionalitetet e rrjetit, si p.sh. vënien në dispozicion të shërbim-pajisjeve (resources) për përdorues të tjerë në rrjet.

Nga pikëpamja e sigurisë nuk këshillohet përdorimi i sistemeve operative të vjetëruara si Windows 3.11 for Workgroups dhe Windows 9x .

Probleme gjatë përdorimit të një rrjeti Peer-to-Peer

Problem kryesor për një rrjet Peer-to-Peer është që një kompjuter, krahas punës së tij normale për përdoruesin lokal, duhet të përpunojë dhe kërkesat për shërbim që i vijnë nëpërmjet rrjetit. Kjo gjë mund të sjellë humbje të shpejtësisë së përpunimit të të dhënave.

Kompjuterat, shërbim-pajisjet e të cilëve (printer, hapësirë për ruajtje të dhënash) vihen në dispozicion të pjesës tjetër të rrjetit, duhet të jetë vazhdimisht në punë dhe mund të shfrytëzohen maksimalisht nga 10 klientë njëkohësisht.

Në këtë strukturë rrjeti ndikon negativisht fakti që çdo përdorues është vetë përgjegjës për administrimin e kompjuterit të tij dhe për sigurinë e të dhënave. Kjo zvogëlon kohën e administrimit qendror, por nga ana tjetër kërkon përdorues me përvojë në punën me kompjuter dhe në rrjet.

Organizimi i përdoruesve dhe grupeve të tyre duhet të bëhet lokalisht në çdo kompjuter, gjë që do të thotë se në një kompjuter duhet të hapet llogari për çdo përdorues në rrjet, i cili duhet të punojë në rrjet në kompjuterin në fjalë. Kjo rrit ndjeshëm kohën e administrimit.

Fushat e zbatimit

Përsa i përket performancës rrjetet Peer-to-Peer rradhiten nga fundi. Megjithatë këto rrjete përshtaten mjaft mirë, kur bëhet fjalë për një numër të kufizuar përdoruesish, që duan p.sh. të shfrytëzojnë bashkërisht një printer, apo të aksesojnë herë pas here të dhënat e përbashkëta

1.4 Serveri

Përparësitë dhe detyrat e serverit

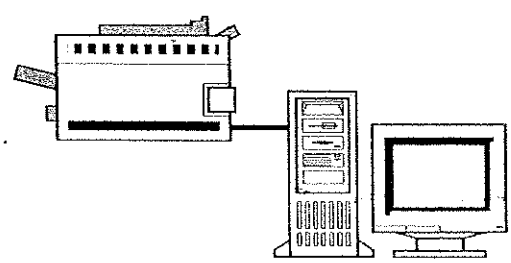
Për sasi të mëdha të dhënash ia vlen të parashikohet një kompjuter i veçantë, në të cilin do të ruhen të dhënat e përbashkëta dhe do të kryhen shërbime të tjera.
Ruajtja qendrore e të dhënave në një kompjuter sjell përparësitë e mëposhtme:

- ☑ Të dhënat mund të sigurohen (backup) pa problem në intervale të rregullta kohore.
- ☑ Përdoruesit e dinë gjithmonë me saktësi se ku duhët ta kërkojnë informacionin e dëshiruar. Atyre nuk u duhet të mbajnë mend, apo të shënojnë se në cilin kompjuter është memorizuar p.sh. lista e inventarit, apo një tabelë e caktuar.
- ☑ Të dhënat për identifikim në rrjet mund të memorizohen në server. Kjo lehtëson administrimin e përdoruesve.
- ☑ Në server kontrollohen në mënyrë qendrore të drejtat per akses në rrjet, të drejtat për akses të përdoruesve mbi resurset e rrjetit (p.sh. të dhënat dhe printerat), si dhe konfigurimi i elementeve të sigurisë.

Detyra e vetme e serverit konsiston në dërgimin e të dhënave tek klientët nëpërmjet rrjetit, kur këta të fundit i kërkojnë ato. Nga ana tjetër, serveri memorizon në diskun e tij të ngurtë të dhënat e krijuara në një kompjuter tjetër në rrjet.

Llojet e serverave

Sipas llojit të shërbimit që ofrojnë, serverat marrin dhe emrat përkatës.



File-Server dhe Print-Server

- ☑ File-Server (Sever Skedarësh)
- ☑ Print Server (Server Shtypi)
- ☑ E-Mail-Server (Server Poste Elektronike)
- ☑ Fax-Server (Server Faksi)
- ☑ Web-Server (Server Shërbimesh Web)
- ☑ Server për administrimin e përdoruesve (domain controller, NetWare- respektivisht. SAMBA-Server)
- ☑ Application-Server (Server Aplikacionesh/Programesh) etj.

Serverat dallohen më së shumti për performancën e lartë. Ata pajisen me disa disqe të ngurtë (harddisks) me kapacitete të larta për mbajtje informacioni, kohë të ulët të aksesimit të te dhënave dhe me memorie operative të madhe. Një vlerë të veçantë ka besueshmëria, pasi në rast mosfunksionimi të serverit, rrjeti paralizohet dhe klientët nuk mund të aksesojnë më të dhënat e përbashkësuara dhe printerin/at.

Në rrjetet e vogla shpesh serveri merr përsipër disa shërbime. Në rrjetet e mëdha, me shumë përdorues dhe shumë detyra për t'u kryer nëpërmjet rrjetit, shpesh instalohen dhe integrohen servera të specializuar, të cilët marrin përsipër shërbime të caktuara.

Aksesi në Server

Kur punoni në rrjet zor se dalloni ndonjë ndryshim nga puna në një kompjuter të veçantë. Ndryshimet paraqiten hollësisht më poshtë.

- ☑ Duhet të identifikoheni me një emër përdoruesi dhe fjalëkalim, me qëllim që të aksesoni të dhënat tuaja në Server.
- ☑ Krahas drive-it A: (disketa) dhe C: (disku i ngurtë) keni akses dhe mbi drive të tjerë, të cilët identifikohen me germa shtesë. Bëhet fjalë për direktori apo drive të përbashkësuara (shared) në server.
- ☑ Kur filloni printimin, të dhënat për t'u printuar kalojnë direkt në printerin e rrjetit .

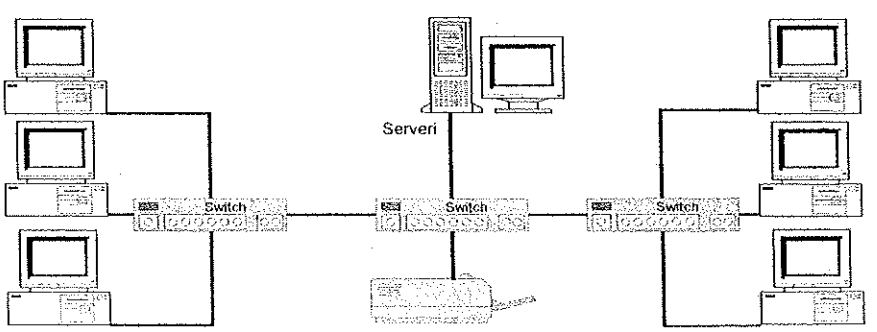
1.5 Rrjetet e strukturuara

Ndërtimi i një rrjeti të strukturuar

Në një firmë me shumë departamente dhe punonjës është i nevojshëm strukturimi i rrjetit. Në shumicën e rasteve struktura e rrjetit pasqyron strukturën e ndërmarrjes.

Në një rrjet të strukturuar është e mundur që punonjësit të grupohen në grupe, të cilat psh. u korrespondojnë departamenteve të veçanta të ndërmarrjes.

Me qëllim që të mund të ndërtohet një rrjet i strukturuar, nevojitet një sistem operativ efektiv për rrjetin. Ky sistem operativ për rrjete mundëson administrimin qëndror dhe klasifikimin e punonjësve, sasisë së të dhënave dhe mjeteve të punës.



- ☑ **Administratori i rrjetit:** Në çdo rrjet ka të paktën një administrator. Ai kujdeset për serverin, e administron atë dhe stacionet e punës, si dhe është i gatshëm t'u përgjigjet pyetjeve që mund të kenë përdoruesit.
- ☑ **Llogaritë e përdoruesve dhe identifikimi:** Me qëllim që një punonjës, gjatë punës, të mund të shfrytezojë burimet e rrjetit, ai duhet të identifikohet në rrjet. Për këtë qëllim atij i hapet nje llogari (konto) në rrjet (server). Llogaria ka emrin e përdoruesit dhe fjalëkalimin përkatës. Fjalëkalimin (password-in) në rastin ideal duhet ta dijë vetëm punonjësi në fjalë. Kjo do të pengonte, që një person i panjohur të identifikohej në rrjet dhe si rrjedhim të kishte akses mbi të dhëna te konfidenciale.
- ☑ **Grupet e përdoruesve:** Punonjësit, të cilët kryejnë të njëjtën detyrë ose detyra të ngjashme, apo i përkasin të njëjtit departament, grupohen në grupe përdoruesish (users groups). Sipas grupeve të përdoruesve administratori mund të caktojë ndër të tjera, cilat pajisje dhe të dhëna lejohet të perdorin gjatë punës punonjës (përdorues) të caktuar.

2. Topologjitë

Në këtë kapitull do të lexoni:
- → ndryshimin midis topologjive fizike dhe logjike
- → cilat topologji bazë mund të përdoren
- → cilat avantazhe dhe disavantazhe paraqet secila topologji
- → cilat topologji vlejnë në fusha zbatimi të caktuara

Kusht paraprak
- ✓ Njohuri bazë për arsyet dhe qëllimet e një lidhjeje në rrjet

2.1 Termi "Topologji"

Përcaktimi i topologjive fizike dhe logjike

Përmes rrjeteve të kompjuterave kalon trafik të dhënash dhe ashtu si në llojet e tjera të trafikut, edhe në fushën e IT-së ndryshojnë rrugët dhe rregullat e trafikut.

Topologjitë fizike

Topologjia fizike e një rrjeti lidhet me rrugët e trafikut. Këtu do të përshkruhet ndërtimi fizik i një rrjeti më fjalë të tjera, në cilën strukture janë lidhur me njëri-tjetrin komponentët individualë të rrjetit, ose e thënë më thjesht, në cilën formë p.sh. do të shtrihet kablli, apo ku do të vendosen antenat në rastin e transferimit të të dhënave pa kabëll.

Topologjia fizike është e krahasueshme me një hartë, në të cilën janë shënuar rrugët e trafikut. Ky kapitull përshkruan format më të rëndësishme bazë të topologjive fizike:

☑ Bus	☑ Star (Yll)	☑ Ring (Unazë)

Topologjitë logjike

Topologjia logjike e një rrjeti përshkruan rregullat bazë të trafikut, të cilat vlejnë në rrugët e trafikut. Këtu bëhet fjalë ndër të tjera edhe se kush ka të drejtë të aksesojë mediumin e transmetimit.

Ndërvarësitë

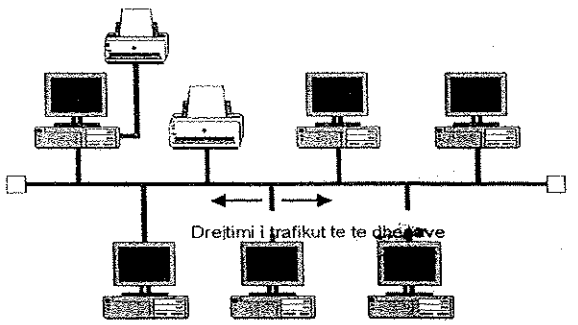
Në praktikë ekziston një varësi e ngushtë midis dy termave, kështu që në një rast normal një topologji fizike e caktuar sjell me vete nje topologji logjike të caktuar. Topologjitë fizike dhe logjike nuk duhet të jenë identike me njëra-tjetrën.

Gjithsesi, zgjedhja e topologjisë fizike është shumë e rëndësishme, pasi pasojat që sjell me vete kjo zgjedhje ndikojnë tek faktorë të tillë si p.sh. ç'lloj kablli do të përdoret, apo sa elastik është rrjeti në rast se del nevoja e zgjerimit me përdorues të tjerë. Përveç kësaj, me zgjedhjen e topologjisë lidhen ngushtë dhe varen aspekte si siguria nga defektet, shpejtësia e komunikimit, gjerësia e bandës në dispozicion, pa neglizhuar kostot përkatëse që lidhen me aplikimin e topologjisë së zgjedhur.

2.2 Bus

Të gjitha pajisjet shfrytëzojnë të njëjtin kabëll

Topologjia bus dallohet nga përdorimi i një kablli qendror të vetëm, i cili përshkruhet si Bus. Me këtë kabëll lidhen të gjitha pajisjet, të cilat duhet ta ndajnë mes tyre këtë medium (sha-red media). Topologjia bus citohet edhe si rrjet pajisjesh në linjë/ rradhë.



Topologjia Bus

Topologjia bus eshte topologji pasive gjë që do të thotë se kompjuterat e lidhur në këtë rrjet nuk e rishpërndajnë sinjalin më tej. Ato kapin sinjalet që vijnë përmes kabllit, ose dërgojnë sinjale në kabël, sinjale të cilat përhapen në të dyja drejtimet. Këtu flitet për një rrjet difuziv.Në rrugën përgjatë kabllit sinjalet humbin, dhe/ose dobësohen, kështu që gjatësia e busit është e kufizuar. Nëpërmjet përdorimit të përforcuesve të sinjalit (repeater-at) mundësohet që gjatësia e lejuar të shtrihet më tej.

Fundet e buseve duhen mbyllur me rezistenca terminatore, përndryshe sinjalet reflektohen dhe rikthehen sërish në kabël. Duke kaluar sërish nëpër kabël, sinjalet përplasen me sinjale të tjera duke shkaktuar dëmtimin e të dhënave që ato përmbajnë. Prandaj lidhësit e kabllit tek pajisjet e veçanta mbahen sa më të shkurtra që të jetë e mundur (më e mira një lidhës në formë T-je në kartën e rrjetit), pasi përndryshe do të kishte reflektime.

Përparësitë e topologjisë Bus

- ☑ Kosto relativisht të ulta, meqë nevojitet pak kabël për të bërë lidhjen.
- ☑ Mosfunksionimi i një kompjuteri nuk shkakton probleme në rrjet.

Përparësia e dytë vlen, sigurisht vetëm për rastin, kur funksionimi jo i mirë nje kompjuteri nuk çon në krijimin dhe dërgimin në rrjet të sinjaleve të pakoordinuara. Ne një rast të tillë duhet të marrim parasysh interferenca të vogla që mund të shfaqen.

Disavantazhet e topologjisë Bus

- ☑ Të gjitha të dhënat transferohen nëpërmjet një kablli të vetëm.
- ☑ Gjithmonë vetëm një kompjuter mund të dërgojë të dhëna në rrjet. Gjatë dërgimit të të dhënave nga ky kompjuter, të gjithë të tjerët janë të bllokuar.
- ☑ Një interferencë, në një vend të caktuar të bus-it, në mediumin e transmetimit (kabël me defekt, lidhje e lirë tek bashkuesit, kompjuteri është konfiguruar gabim) bllokon të gjithë rrjetin dhe çon në një proces të mundimshëm për gjetjen e defektit.

Performanca në topologjinë bus varet nga numri i kompjuterave, të cilët njëkohësisht tentojnë të dërgojnë të dhëna. Në rast se ndodh që të dergojnë të dhëna, njëkohësisht ndodh procesi i përplasjes (kolisionit) dhe dërgesat automatikisht ripërsëriten në periudha të caktuara kohore. Sa më shpesh të ndodhë kjo gjë, aq më e ulët do të jetë performanca dhe efektiviteti i dergimit të të dhënave në rrjet .

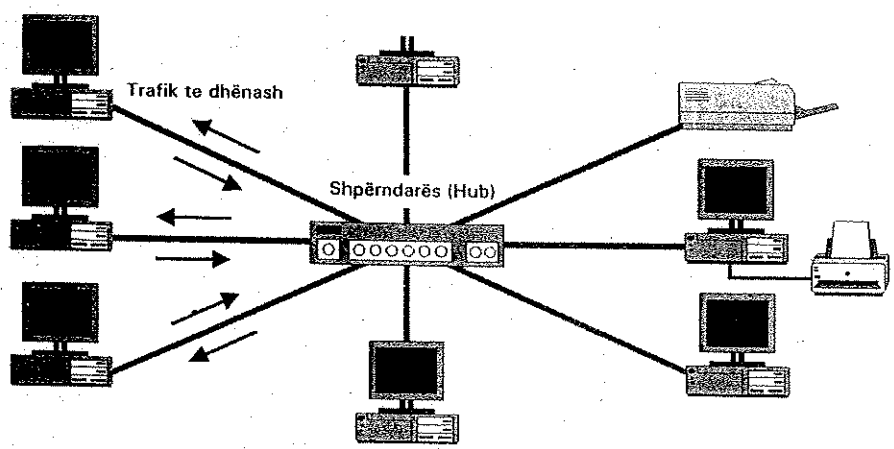
Fusha e zbatimit

Megjithë disavantazhet, topologjia bus ishte njëra nga më të përdorshmet në rrjetet e vogla lokale dhe e lidhur ngushtë me termin Ethernet në standardet 10Base5 dhe 10Base2. Sot ky lloj kabëllzimi nuk luan më ndonjë rol të ndjeshëm. Kjo topologji është zëvendësuar gjërësisht nga struktura fizike yll. Tek rrjetet pa kabël (WLAN) mund të gjenden ende ngjashmëri me topologjinë bus, si p.sh. kur një kompjuter dërgon të dhënat e veta në të gjitha drejtimet e mundshme.

2.3 Star

Çdo pajisje përdor kabllin e vet

Në topologjinë star secili kompjuter lidhet me shpërndarësin qendror nëpërmjet një kablli. Ekziston pra, një lidhje kokë më kokë (point-to-point) midis shpërndarësit qëndror dhe secilës paisje të lidhur veças me të.



Topologjia Star

Hub-i

Shpërndarësi qendror përgjithësisht përcaktohet si **Hub**. Përcaktime të tjera për të si përqendrues kabllosh, apo shpërndarës në formë ylli, thjesht qartësojnë se detyra bazë e kësaj pajisjeje është vënia në dispozicion e një pajisjeje qendrore me shumë mundësi lidhjeje për pajisjet e tjera.

Përparësitë e topologjisë Star

- ☑ Mosfunksionimi i një stacioni pune, apo defekti i një kablli nuk ka asnjë ndikim për pjesën tjetër të rrjetit.
- ☑ Shpërndarësit aktivë shërbejnë njëkohësisht edhe si përforcues sinjali.
- ☑ Gjatë një mënyre funksionimi të caktuar të shpërndarësit, dy stacione pune mund të shfrytëzojnë për komunikimin mes tyre të gjithë gjerësinë e bandës që ofron media transmetuese, pa penguar ndërkohë stacionet e tjera të punës. Në këtë mënyrë kjo topologji fizike lejon në total një shkallë më të lartë të transferimit të të dhënave.
- ☑ Stacione të tjera pune dhe/ose shpërndarës të tjerë mund të lidhen pa problem më pas.

Disavantazhet e topologjise Star

- ☑ Kërkon përdorimin e një sasie të madhe kabllosh
- ☑ Mosfunksionimi i shpërndarësit nxjerr jashtë loje të gjithë rrjetin, pra nuk ka më trafik të dhënash.

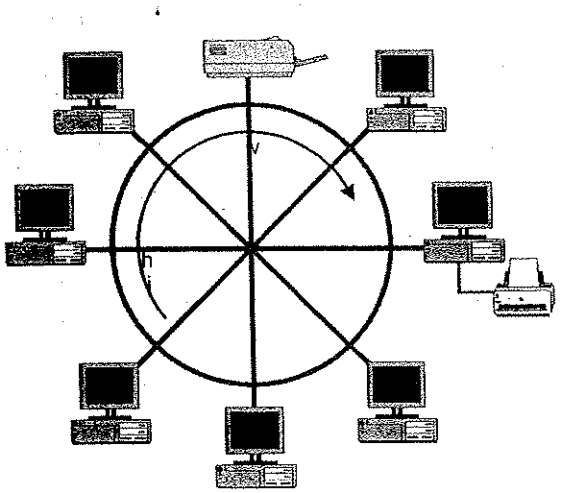
Topologjitë fizike star shpesh punojnë logjikisht si topologji bus. Shpërndarësi dërgon një sinjal marrës tek te gjitha komponentët e lidhur në rrjet. Rruga, në të cilën kalojnë të dhënat nga dërguesi te marrësi, ndikohet nga konfigurimi i shpërndarësit (switch-it, hub-it, etj).

Fusha e zbatimit

Topologjia star përdorimin praktik e gjen në rrjetet lokale në variantet moderne te Ethernetit (Fast Ethernet, Gigabit Ethernet). Kjo formë kabllimi përdoret sot gjerësisht në instalimet e reja në nivel kati, apo godine.

2.4 Ring

Çdo pajisje lidhet me dy pajisje fqinje



Topologjia Ring

Tek topologjia ring kabllot e përdorura formojnë një formë të mbyllur unaze. Nuk ka fillim, apo fund kablli.

Të gjitha stacionet e punës lidhen në „unazë" (ring), si elemente të cilat përpunojnë dhe përforcojnë sinjalet që kalojnë në kabëll dhe i dërgojnë ato më tej.

Këtu qëndron edhe disavantazhi më i madh, pasi defekti i një kompjuteri, apo i një pjese të kabllit paralizon punën në të gjithë rrjetin.

Flitet për një rrjet të pjesshëm, dhe bëhet fjalë për një lidhje Point-to-Point midis kompjuterave fqinjë.

Çdo kompjuter kja nje pararendës dhe një pasardhës. Trafiku i të dhënave kryhet vetëm në një drejtim.

Ky layout rrjeti ndeshet rrallë si topologji fizike në rrjetet e sotme lokale, meqë kostot e shtrirjes së kabllit janë relativisht të larta.

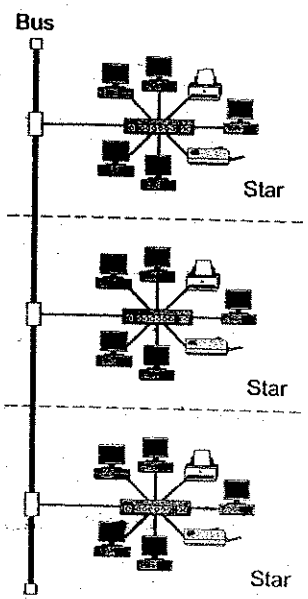
Si topologji logjike në praktikë kjo po gjen zbatim dhe realizohet shpesh nëpërmjet një pajisjeje qendore (shpërndarës ring). Fizikisht ndërtohet si një topologji yll (star), por mënyra se si të dhënat do të administrohen nga shpërndarësi, kryhet logjikisht sipas rregullave të një topologjie ring. Në praktikë njihet p.sh. si "Token Ring". Sigurisht ky lloj rrjetëzimi nuk përdoret më.

Shënime

2.5 Format mikse

Kombinimet e topologjive Bus, Star dhe Ring

Në praktikë, kryesisht në rrjetet e mëdha, gjejmë raste të kombinimit të topologjive të sipërpërmendura, p.sh. atëherë kur rrjete (apo pjesë rrjetesh) ekzistuese bashkohen në ndërtimin e të ashtuquajturës Backbone.



Rrjeti Star-Bus

Backbone

Me Backbone kuptohet lidhja fizike e shumë rrjeteve me njëri-tjetrin. Bëhet fjalë për një rrjet në sfond që mundëson p.sh. lidhjen e ndërtesave të ndryshme dhe rrjeteve të tyre individuale respektive.

Rrjeti Star-Bus

Një rrjet star-bus formohet kur Hub-e të ndryshëm, respektivisht qendra e yllit të formuar prej lidhjes së tyre, lidhen me njëri-tjetrin me nje kabëll bus.

Po japim një shembull të thjeshtë për ta qartësuar si ide. Në një ndërtesë trikatëshe çdo kat është li lidhur në rrjet duke përdorur topologjinë star. Të tria katet, ose më saktë Hub-et, lidhen me njëri-tjetrin përmes një kablli bus.

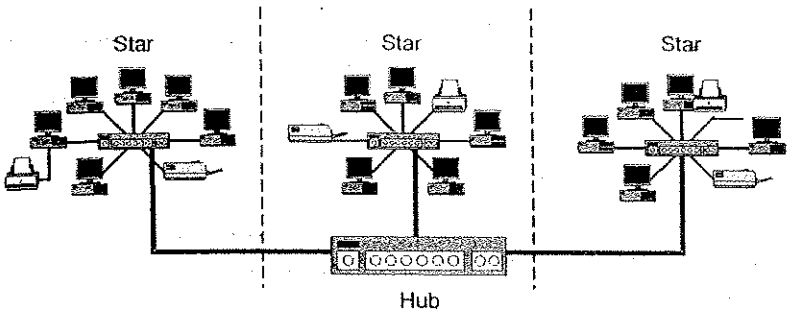
Në qoftë se kablli bus ka defekt, katet nuk mund të komunikojnë më me njëri-tjetrin. Në rast se bie Hub-i, ndërpritet komunikimi në rrjet brenda katit dhe njëkohësisht mes këtij kati dhe kateve të tjera.

Rrjeti Star-Star

Një rrjet Star-Star formohet, kur Hub-e të ndryshëm krijojnë respektivisht qendrën e një ylli dhe më tej këto Hub-e lidhen përmes një kablli me një Hub kryesor. Në këtë Hub kryesor, në praktikë, shpesh lidhen direkt edhe servera të rëndësishëm.

Po japim një shembull të thjeshtë: Në një ndërtesë trikatëshe me zyra, secili kat është lidhur në rrjet me kabëll duke përdorur teknologjinë star. Të tria katet, ose më saktë Hub-et me njëri-tjetrin, lidhen përmes një kablli me një Hub kryesor.

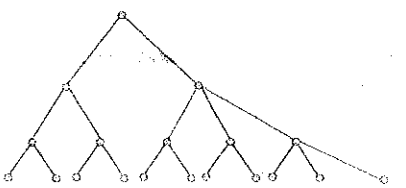
Në rast mosfunksionimi të Hub-it qendror, komunikimi brenda çdo kati është ende i mundur. Për arsye sigurie Hub-i qendror mund të jetë rendundant (i dubluar), gjë që do të thotë se një Hub i dytë qëndon në stand by modus dhe futet menjëherë në punë në rast mosfunksionimi të të parit. Ne rast se kablli, që kalon nga Hub-i qendror tek njëri nga Hub et e kateve ka defekt, atëherë ky kat nuk do të jetë në gjendje të komunikojë me katet e tjera.



Rrjeti Star-Star

Struktura në formë Peme

Topologjia pemë është ndërtuar në formë të tillë që nga një rrënjë dalin një sasi e madhe degëzimesh që lidhen me pika të tjera shpërndarje. Bëhet fjalë për zgjerimin e një rrjeti star-star (yll-yll) në një rrjet me shumë nivele.

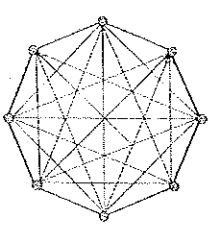


Topologjia Peme

Struktura në formë peme përshtatet mirë për rrjetizimin e mjediseve të një firme, në të cilën ndërtesat e ndryshme lidhen nëpërmjet një qendre llogaritëse, apo përdorimi i kësaj strukture në rrjetet e shpërndarjes së sinjalit televiziv me kabëll që përdorin televizionet kabllore.

Rrjeti Mesh

Në një rrjet të tillë ekzistojnë shumë nyja ndërmjet nyjave individuale të rrjetit.



Rrjeti Mesh

Kuptimi i ndërtimit të një rrjeti të tillë është se në rast mosfunksionimi të një lidhjeje, sistemi mundëson aksesimin e një lidhjeje të dytë rezervë (redundant). Shpesh këtë lloj lidhjeje e gjejmë tek rrjetet WAN.

Më tej mund të dallojmë nëse linjat rezervë që do të përdoren janë aktive (load sharing, me ndarje të ngarkesës), apo pasive (standby).

Shënime

3 Modelet e rrjeteve

Në këtë kapitull do të lexoni:

→ çfarë janë modelet e rrjeteve
→ si mund të punoni me modelet e rrjeteve
→ çfarë është modeli OSI
→ çfarë është modeli DoD

Parakusht

✓ njohuri të përgjithshme mbi kompjuterin

3.1 Vështrim i përgjithshëm

Hyrje

Supozoni se një klient X, nëpërmjet kompjuterit të tij, dëshiron të aksesojë faqen HTML të një prodhuesi hardware-sh, me qëllim që të shkarkojë prej andej driver-in e kartës grafike të tij, duke përdorur shërbimin FTP.

Për këtë qëllim, klienti X mund të përdorë një sistem operativ, i cili ndryshon dukshëm nga ai që përdor prodhuesi i hardware-ve. Mundet që ai e akseson Internetin nëpërmjet një LAN-i, por ndoshta edhe nëpërmjet një modemi. Edhe Browser-i, të cilin ai përdor, mund të jetë bërë nga prodhues software-sh të ndryshëm.

Në Internet, kërkesa e tij transmetohet deri tek kompjuteri i prodhuesit të hardware-it nëpërmjet linjave ATM, lidhjeve Frame-Relay ose linjave ISDN, ku sipas rrethanave hyjnë në përdorim protokolle të ndryshme si TCP/IP, IPX/SPX, apo SNA.

Ju vini re gjithashtu, që për shkak të shumëllojshmërisë së komponetëve hard- dhe software pjesëmarrës, nevojitet një strukturim i qartë i komunikimit nëpërmjet rrjetit. Vetëm në këtë mënyrë mund të garantohet, që produktet e ndryshme të jenë në gjendje të komunikojnë me njëri-tjetrin në ndërfaqet midis hardware-ve të rrjetit, protokolleve të komunikimit dhe software-ve.

Shtresat

Me qëllim që këto ndërfaqe midis komponentëve të komunikimit të standardizohen, nevojitet një model, i cili u cakton shtresave të caktuara komponentë dhe detyra të veçanta, të cilat të paraqesin ndërfaqe të standardizuara për shtresat fqinje. Në raste të veçanta mund të bashkohen paketa nga shtresa të caktuara, vetëm nëse kjo funksionon nga pikëpamja e hardware-ve, apo kur plotëson kërkesat e aplikacioneve të software-eve, kështu që për arsye kompatibiliteti, është e nevojshme të përdoret një model i përgjithshëm për standardizim.

Sot, për paraqitjen e komunikimit në rrjet, përdoren tri modele. Ato ndryshojnë nga njëra-tjetra para së gjithash nga sakstësia me të cilën përcaktohen shtresat e veçanta. Perveç kësaj, ekzistojnë ndryshime edhe në përgjithësimin e modeleve. Këtu vlen përcaktimi: sa më i vlefshëm përgjithësisht të jetë një model, aq më saktësisht duhet përshkruar çdo funksion i veçantë, i cili bën pjesë në një shtresë të caktuar.

Tri modelet më të fundit janë:

☑ modeli ISO/OSI
☑ modeli DoD
☑ modeli TCP

3.2 Modeli OSI

Historik i shkurtër

Modeli ISO/OSI u zhvillua në vitin 1984 nga Organizata Ndërkombëtare e Standardeve - ISO (International Standards Organisation), në vijim të përvojës së krijuar nga ARPANet, për të krijuar një model teorik, i cili do të shërbente si standard per të plotësuar kërkesat për paraqitjen e komunikimit në rrjet. Meqë modeli nuk i përket ndonjë familjeje të caktuar protokollesh, ai quhet ndryshe Open-System-Interaction-Model (Modeli – OSI).

Përshkrimi

Modeli përbëhet nga shtatë shtresa, të cilat duhet të përshkojnë dy herë rrugën ndërmjet dy sistemeve. Ky model lejon me metoda të thjeshta të paraqesë një model komunikimi.

Më poshtë, komponentët e veçantë të modelit OSI do të trajtohen në mënyrë shumë të detajuar. Sa më mirë ta kuptoni se çfarë ndodh në shtresat e veçanta, aq më të lehtë do ta keni në praktikë, nëse iu bie rasti të identifikoni shkaqet e problemeve të mundshme që shfaqen në rrjet. Edhe pse modeli OSI është model teorik, atë duhet ta përvetësoni sa më mirë, me qëllim që protokollet dhe shërbimet e dëshiruara të mund t'i vendosni sipas shtresave përkatëse.

Shembull

Supozojmë se një punonjës A i një firme gjendet me shërbim jashtë firmës. Ai duhet t'i japë një klienti informacione në lidhje me një produkt, përshkrimi i të cilit gjendet në një dokument mbi tavolinën e tij të punës. Ai i telefonon kolegut të tij B në zyrat qendrore, i cili i lexon atij informacionin e kërkuar. Në këtë mënyrë punonjësi A mund ta vazhdojë më tej bisedën me klientin në lidhje me produktin.

Por cilat janë hapat e veçanta, të nevojshme për t'u ndërmarrë, me qëllim që punonjësi me shërbim jashtë firmës të marrë informacionin e kërkuar?

Shtresa fizike (Physical Layer)

Së pari punonjësi A duhet të ketë akses mbi një media, e cila gjithashtu është në dispozicion edhe të punonjësit B. Në këtë rast media është telefoni. Në rast se A, në vend të telefonit merr një radio me valë, atëhere komunikimi do dështonte. Duhet gjithashtu që mediat të jenë kompatibël në nivelin fizik të transmetimit.

Shtresa e lidhjes (Data Link Layer)

Punonjësi A duhet t'i bjerë numrit të duhur të telefonit me qëllim që rrjeti i telekomit ta lidhë me abonentin e dëshiruar (në rastin e shembullit tonë me zyrat qendrore të firmës). Vetëm në rast se NTBC-ja e duhur merr një sinjal, atëhere mund të kryhet një lidhje. Edhe në shtresën e lidhjes duhet të kryhet një adresim i saktë.

Shtresa e rrjetit (Network Layer)

Brenda rrjetit të firmës, nëpërmjet centralit telefonik të vetë firmës, kryhet një nëndarje logjike. Kjo nëndarje nuk varet nga Telekomi, por i shërben dhe ndjek kryesisht strukturimin logjik të rrjetit të firmës. Kështu p.sh. mund të identifikohen më 1xx kati i parë dhe me 2xx kati i dytë. Tek shtresa e rrjetit në këtë rast i referohemi lidhjes (linjës) përkatëse.

Shtresa e transportit (Transport Layer)

Informacionet nga A-ja tek B-ja duhet të vijnë në formë të kuptueshme. Për këtë të dy partnerët në komunikim duhet të flasin të njëjtën gjuhë dhe të ruajnë të njëjtat konvencione të përcaktuara gjatë komunikimit. Nëse A-ja flet me zë të ulët, shumë shpejt, apo ka kërcitje që degjohen në linjë, B-së i duhet të pyesë për se bëhej fjalë. Në shtresën e transportit gjithashtu sigurohet, që të gjitha informacionet kanë mbëritur në mënyrë korrekte dhe janë procesuar në të njëjtën mënyrë, nga të dy anët.

Shtresa e sesionit (Session Layer)

Në qoftë se A-ja fillon të flasë, ende pa ngritur receptorin B-ja, komunikimi nuk do të kishte sukses. Nëse paraprakisht është kryer krijimi dhe kontrolli i lidhjes nëpërmjet përshëndetjes, vetëm atëhere A-ja mund t'i japë B-së instruksione çfarë duhet të bëjë. A-ja fillimisht duhet edhe të identifikohet tek B-ja. Kjo pasi B-ja nuk nuk mund t'i japë informacionet, që gjenden në tavolinën e A-së çdo personi që merr në telefon. Në këtë shtresë kontrollohen gjithashtu rregullat e përgatitjes së aksesit dhe komunikimit.

Shtresa e prezantimeve (Presentation Layer)

Sipas shembullit të mësipërm, A-ja nuk ka mundësi t'i lexojë vetë informacionet e kërkuara; edhe në rastin kur këto informacione ia lexon B-ja, ai nuk mund t'i përdorë ato. Vetëm kur B-ja e jep sërish me zë të lartë informacionin, atëhere A-ja mund ta marrë atë. Informacioni duhet përgatitur për t'u "transportuar" nëpërmjet telefonit. Në këtë shtresë ndodh gati një ndryshim i rrugëzimit të procesit të "leximit", i cili nuk është i përshtatshëm për rrjetin, në procesin e "të folurit", i cili është i përshtatshëm për transportin.

Shtresa e aplikacioneve (Application Layer)

Me qëllim që përfundimisht të mund të realizohet aksesi tek informacionet e kërkuara, B-ja duhet të dijë se në cilat dokumenta gjenden të dhënat e nevojshme, duhet të marrë syzet, të hapë dokumentat, e kështu me rradhë. Vetëm pasi të kryhen veprimet e mësipërme, ai mund të fillojë me leximin e informacioneve. Në shtresën e aplikacioneve parapërgatitet gjithashtu mjedisi për veprimin e „leximit".

Aplikacionet

Veprimi i leximit në vetvete nuk është pjesë e modelit të komunikimit. Ai mund të bëhet edhe pa telefon dhe si rrjedhim nuk luan asnjë rol në procesin e komunikimit. Kësisoj ai nuk do të merret parasysh në model.

Modeli OSI

Në tabelën e mëposhtme do të gjeni të vendosura karshi njëra-tjetrës shtresat që i korrespondojnë shembullit të mësipërm me ato të nomenklaturës së modelit OSI:

	Shembull	Modeli OSI (Shqip)	Modeli OSI (Anglisht)
Shtresa 7	Zgjedhja e informacionit	Shtresa e aplikacioneve	Application Layer
Shtresa 6	Leximi/Të folurit	Shtresa e paraqitjes	Presentation Layer
Shtresa 5	Përshëndetja/Identifikimi	Shtresa e komunikimit, shtresa e sesionit	Session Layer
Shtresa 4	Kontrolli i të kuptuarit	Shtresa e transportit	Session Layer
Shtresa 3	Zgjedhja e numrit	Shtresa e rrjetit, shtresa e shkëmbimit të të dhënave	Network Layer
Shtresa 2	Numri i lidhjes	Shtresa e sigurimit të të dhënave, shtresa e lidhjes	Data Link Layer
Shtresa 1	Zgjedhja e medias së transmetimit	Shtresa fizike e transmetimit të Bit-eve	Physical Layer

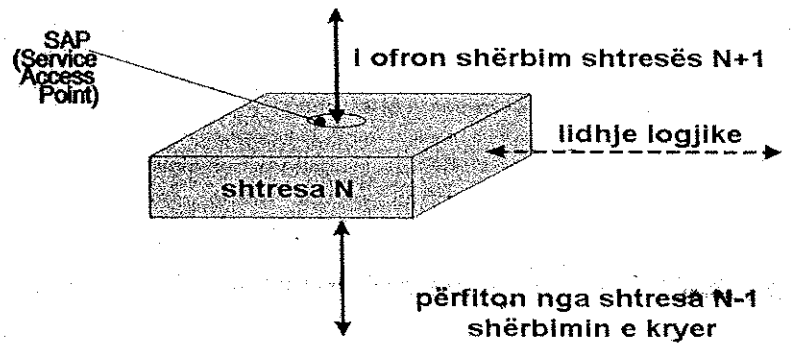
Është e nevojshme të mësohen termat anglisht të shtresave, pasi në literaturën profesionale në shqip mund të gjenden përkthime të ndryshme për të njëjtin term. Gjithsesi, termat anglisht jepen gjithmonë në kllapa krahas atyre të përkthyera.

Parimi i funksionimit të modelit referues OSI

Parimi bazë i modelit OSI është komunikimi midis shtresave të ndryshme të tij.

☑ Çdo shtresë siguron një grup shërbimesh (services) për shtresën e mësipërme me anë të një ndërfaqeje të përcaktuar mirë, e ashtuquajtura **Service Access Point (SAP)**. Këto shërbime sigurojnë akses tek strukturat e të dhënave.

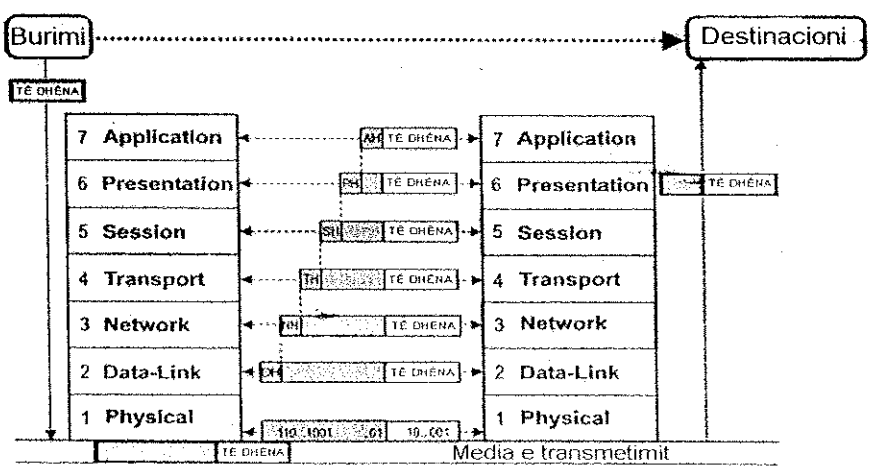
- ☑ Sa më e lartë shtresa, aq më komplekse janë detyrat që ajo përmbush. Funksionaliteti i çdo shtrese bazohet mbi standardet e shtresës së mëposhtme.
- ☑ Gjatë trafikut të të dhënave, secila nga shtresat individuale të nyjeve (nodes) të rrjetit të përfshira në komunikim, reagon sikur të komunikonte me shtresën korresponduese (peer layer) të node-it partner (komunikim horizontal përmes një lidhje logjike). Në fakt, të gjitha të dhënat kalojnë përmes të gjitha shtresave (komunikim vertikal ose ndërshtresor).
- ☑ Ndërveprimi ndodh gjithmonë midis shtresave fqinje, pra me fjalë të tjera shtresa të veçanta nuk mund të kapërcehen.



Kommunikimi ndërmjet shtresave

Të dhënat midis shtresave quhen njësi të dhënash protokolli (**PDU - Protocol Data Unit**). Ato bashkohen me njëra-tjetrën në një të ashtuquajtur **Header** (kokë), në të cilën gjenden informacionet e kontrollit të protokollit (**PCI - Protocol Control Information**) të shtresave përkatëse, si dhe „ngarkesa" përkatëse me të dhëna të shfrytëzueshme (**SDU - Service Data Unit**).

Kur të dhënat kalohen përmes shtresave, çdo shtresë individuale e stacionit dërgues që transmeton të dhëna i bashkëngjit një header të dhënave të marra, i cili interpretohet dhe hiqet përsëri nga shtresa respektive e stacionit marrës.



Modeli me shtresa

Përparësitë e konceptit me shtresa

Megjithëse modeli me shtresa është shumë abstrakt, ai iu jep prodhuesve dhe zhvilluesve disa përparësi.

Pavarësia reciproke e shtresave nga njëra-tjetra

Zbatimi aktual në përmbajtjen e një shtrese është i parëndësishëm. Të rëndësishme janë vetëm shërbimet, të cilat ofrohen tek ndërfaqet. Kështu, shtresa të veçanta mund të zhvillohen të pavarura nga njëra-tjetra p.sh. nga kompani, apo institucione të ndryshme.

Fleksibiliteti

Ndryshimet në shtresat e veçanta nuk ndikojnë në shtresat e mëposhtme, apo të mësipërme të tyre, përsa kohë që ndërfaqet e përcaktuara mbeten siç janë.

Ndarja fizike e shtresave

Çdo shtresë, sipas funksionit që kryen, mund të përshtatet më mirë si zgjidhje soft- apo hardware.

Standardizimi i thjeshtuar

Përcaktimi i saktë i funksionit të secilës shtrese lejon zhvillimin e shtresave standarde.

Mirëmbajtja dhe zbatimi i thjeshtë

Zhvillimi i sistemeve komplekse thjeshtohet nëpërmjet modularitetit dhe ndërfaqeve të përcaktuara mirë.

Disavantazhet

Disavantazhi i një koncepti me shtresa qëndron në sasinë e jashtëzakonshme të informacioneve të kontrollit (çdo shtresë shkruan headerin e vet), për shkak të së cilës vonohet transmetimi i të dhënave.

3.3 Shtatë shtresat e modelit OSI

1. Shtresa e transmetimit të bit-eve (Physical Layer)

Shtresa fizike përcakton gjithë specifikimet e nevojshme për dërgimin dhe marrjen e Bit-eve individuale respektivisht nga apo tek një media transmetimi.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

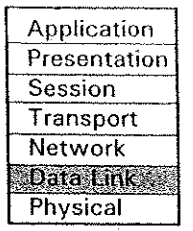
Në pjesën **mekanike** specifikohen elementët e nevojshëm për sigurimin e një lidhjeje fizike (konektorët, lloji i medias së transmetimit, etj.).

Në pjesën **elektrike** përcaktohen p.sh. nivelet e tensionit të përdorur, rezistenca e kabllit, intervalet kohore për sinjalet dhe ndryshimet e tensionit, procedurat e përdorura të kodimit (si duhet të paraqitet një Bit?).
Këto specifikime përcaktojnë fluksin maksimal të arritshëm të transmetimit të të dhënave.

Specifikimet **funksionale** kanë të bëjnë me funksionin e linjave të përfshira si p.sh. me ndryshimin midis linjave të të dhënave me ato të kontrollit, frekuencën (clock rate), apo caktimin e PIN-it.

Specifikimet **procedurale** përcaktojnë p.sh. mënyrat e transmetimit (half-, fullduplex), apo për sa kohë një nivel i përcaktuar tensioni duhet të aplikohet, për t'u identifikuar si 1 dhe 0 logjik.

2. Shtresa e sigurimit të të dhënave (Data Link Layer)



Kjo shtresë paketon të dhënat e marra nga shtresa e rrjetit (network layer) në formën e të ashtuquajturave frames (data-frames të një madhësie fikse) dhe i kalon më tej tek shtresa fizike (physical layer). Nëse kërkohet, paketat e mëdha me të dhëna ndahen në paketa më të vogla. Copëzimi i frame-ve në Bit-e të veçanta për t'u dërguar më pas në shtresën fizike të transmetimit dhe procesi i kundërt, pra mbledhja sërish e Bit-eve individuale për krijimin e frame-ve (nga shtresa 1) bën pjesë gjithashtu në detyrat e shtresës Data Link .

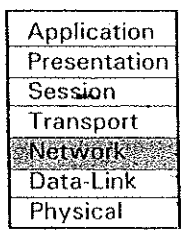
Një frame i thjeshtë përbëhet prej një të ashtuquajturi **Header** (siguron adresat e burimit dhe të destinacionit, si dhe informacione kontrolli), **Të dhënat** aktuale, si dhe një **Trailer** bashkëngjitur (FCS - Frame Check Sequence), për të identifikuar nëse të dhënat janë transmetuar pa gabime. Për llogaritjen e shumës së kontrollit të frame-it (Frame Checksum) si rregull përdoret algoritmi CRC (Cyclic Redundancy Check).

Nga kontrolli i FCS-së marrësi mund të gjykojë, nëse të dhënat janë ndryshuar gjatë transportit. Pro-to-kollet e Data Link Layer-it zotërojnë procedura të dedektimit të gabimeve duke siguruar ritransmetimin e frame-ve të humbura, apo të dëmtuara.

Funksioni i fundit i Data Link layer është kontrolli i fluksit të të dhënave (**flow control**). Ky funksion ka për qëllim që të pengojë një transmetues të shpejtësisë së lartë të "përmbytë" me të dhëna një marrës të shpejtësisë së ulët.

Dedektimi i gabimeve dhe kontrolli i fluksit të të dhënave implementohen shpesh, në mënyrë të tillë që transmetuesi pret derisa të marrë një konfirmim për frame-in e dërguar. Frame-t, marrja e të cilave është e pakonfirmuar, do të ritransmetohen.

3. Shtresa e rrjetit (Network Layer)

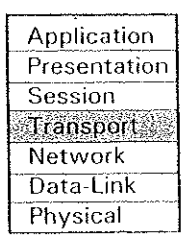


Shtresa e rrjetit përcakton rrugëkalimin më të mirë të mundshëm përmes rrjetit. Ajo realizon një lidhje end-to-end midis dy stacioneve që komunikojnë me njëri-tjetrin, përmes nyjeve (nodes) të ndryshme të rrjetit.

Këtu hyjnë adresimi dhe interpretimi i adresave, përcaktimi i rrugës së transmetimit (routing), si dhe ndërlidhja e rrjeteve të ndryshme të transportit.

Në qoftë se një router nuk është në gjendje të dërgojë më tej (forward) të dhëna në madhësinë që kanë ardhur në shresën e rrjetit, atëherë të dhënat copëzohen më tej në paketa më të vogla (fragmentation).

4. Shtresa e transportit (Transport Layer)



Shtresa e transportit realizon një lidhje "fikse" midis dy proceseve, duke iu ofruar shtresave të mësipërme një kanal transparent.

Shtresa e transportit punon si shtresë ndërmjetëse midis shtresave të orientuara nga aplikacionet (7. - 5.) dhe shtresave të orientuara nga transporti (3. - 1.) duke përgatitur të dhënat respektive. Meqë protokolle të ndryshme transmetojnë të dhëna në madhësi të ndryshme, të dhënat ndahen në paketa korresponduese dhe markohen me numra të njëpasnjëshëm (sekuencial). Marrja e secilës paketë konfirmohet.

Në këtë shtresë kryhen sërish funksionet e kontrollit të fluksit të të dhënave dhe dedektimit të gabimeve. Këtu kontrollohet nëse paketat arrijnë të plota, të padëmtuara, sipas rradhës së duhur dhe pa dublikata.

5. Kontrolli i komunikimit-/Shtresa e sesionit (Session Layer)

Kjo shtresë konrollon të ashtuquajturat sesione. Ajo është përgjegjëse për realizimin, menaxhimin dhe përfundimin e komunikimit midis burimeve të rrjetit. Këtu hyjnë dhe „name resolution" i burimeve të rrjetit, si dhe negocimi i parametrave të kontrollit të fluksit të të dhënave (kur një stacion lejohet të transmetojë, çfarë sasie të dhënash, në cilat intervale kohe e kështu me rradhë). Session Layer-i përfaqëson një shërbim transporti universal në komunikimin ndër procesual (procss-to-process communication).

Application
Presentation
Session
Transport
Network
Data-Link
Physical

Menaxhimi i sesionit, para së gjithash përfshin edhe sinkronizimin. Kur ndodh një rënie e papritur e rrjetit, duhet të mundësohet ritransmetimi i të dhënave të humbura. Për ta garantuar këtë gjë shtohen elementë kontrolli (checkpoints) tek të dhënat. Kur ndërpritet fluksi i transmetimit të të dhënave, atëhere duhen ritransmetuar vetëm të dhënat pas kontrollit të fundit.

6. Shtresa e prezantimit (Presentation Layer)

Shtresa e prezantimit konverton të dhënat në një format standard të përgjithshëm (ASN.1 Abstract Syntax Notation One), për të cilin është rënë dakord dhe që është i kuptueshëm nga kompjuterat e përfshirë në komunikim. Kjo është e nevojshme, meqë prezantimi i brendshëm i të dhënave mund të trajtohet në mënyra të ndryshme (p. sh. në kodet e karaktereve ASCII, ANSI, EBCDIC) nga sistemet individuale të përdorura.

Application
Presentation
Session
Transport
Network
Data-Link
Physical

Detyra të tjera që kryen kjo shtresë janë transformimi i protokolleve, kodimi i të dhënave, si dhe komprimimi i të dhënave për reduktimin e trafikut në rrjet.

I ashtuquajturi *redirector*, i cili kryen administrimin e operacioneve të hyrjes dhe daljes së informacionit (input/output) midis disqeve të ngurtë lokalë dhe burimeve të përbashkësuara të rrjetit, punon gjithashtu në këtë shtresë.

7. Shtresa e aplikacioneve (Application Layer)

Shtresa e aplikacioneve paraqet ndërfaqen midis aplikacioneve (programeve dhe përdoruesve) dhe shërbimeve të rrjetit. Këtu trajtohet aksesi në rrjet, kontrolli i fluksit të të dhënave, eliminimi i gabimeve, si dhe shërbimeve të aplikacioneve (services) si p.sh. transferimi i skedarëve (files), aksesi në bazat e të dhënave, e mail-i apo përbashkësimi i resurseve për akses në rrjet (sharing).

Application
Presentation
Session
Transport
Network
Data-Link
Physical

Kotrolli i shumfishtë

Mekanizma të ndryshme, si p.sh. mekanizmi i kontrollit të fluksit të të dhënave apo gabimeve, aplikohen në mënyrë të përsëritur në më shumë se një shtresë. Çdo shtresë rregullon pjesën "e vet" të kontrollit. Nëse kjo shtresë nuk mund të vazhdojë më tej me mekanizmat e veta të kontrollit, atëhere dërgohet një raport "më lart", në shtresën më të afërt. Atje veprojnë mekanizma të tjera për ta eliminuar problemin.

Frazat

Dy frazat e mëposhtme kanë për qëllim të lehtësojnë mbajtjen mend te shtresave sipas rradhës:

Nga shtresa 1 deri tek 7: PLEASE DO NOT THROW SAUSAGE PIZZA AWAY
Nga shtresa 7 deri tek 1: ALL PEOPLE SEEM TO NEED DATA PROCESSING

Vështrim i përgjithshëm në lidhje me detyrat

Tabela e mëposhtme jep një përmbledhje të shkurtër të paraqitjes së një modeli të pastër OSI.:

Nr.	Shtresat e modelit OSI	Detyrat
7	Application	Aplikacionet
6	Presentation	Formatet e të dhënave, informacionet në lidhje me prezantimin dhe kodimin
5	Session	Lidhjet, kontrolli i rrjedhës -fluksit (parametrat e komunikimit), pikat e kontrollit të fluksit të të dhënave
4	Transport	Paketat, kontrolli i rrjedhës (fluksit), trajtimi gabimeve dhe konfirmimi i marrjes
3	Network	Informacionet e adresave, routing
2	Data Link	Frames, trajtimi i gabimeve
1	Physical	Përcaktimi i vlerave fizike

Grupet e shtresave

Shpesh shtresat përmblidhen në dy grupe, meqë ato janë formuar nga karakteristika përgjithësisht të ndryshme.

Grupet e shtresave	Nr.	Shtresat sipas modelit OSI	Shembuj		
			Protokollet e aplikacioneve	Sherbimet specifike të sistemit	Protokollet e rrjetit
Shtresat e aplikacioneve	7	Application	Transmetitmi i file-eve, Post, WWW		
	6	Presentation	FTP, SMTP, HTTP		
	5	Session		SMB, WinSocket	
Shtresat e rrjetit	4	Transport			TCP, UDP, SPX
	3	Network			IP, IPX, ARP
	2	Data Link			MAC
	1	Physical			ETHO, TokenRing

Nga njëra anë janë shtresat 1 deri në 4, të cilat merren me detyrat specifike për rrjetin që kanë të bëjnë me komunikimin. Nga ana tjetër janë shtresat 5 deri në 7, në të cilat sigurohen shërbime specifike për sistemin operativ, përpunohen të dhëna dhe sigurohet mbështetja për aplikacionet.

Nënshtresat e shtresës së dytë te modelit OSI (Data Link Layer)

Praktika ka treguar, se është e nevojshme një nëndarje e mëtejshme teorike e shresës Data Link Layer, meqë ajo merr përsipër të kryejë dy funksione shumë të ndryshme nga njëra-tjetra.

Nënshtresat e shtresës Data Link	Detyrat
Logical Link Control (LLC)	**SAP-et** LLC-ja vë në dispozicion të nënshtresës MAC SAP-në, me qëllim që të dhënat nga nënshtresa MAC të mund të dërgohen tek shërbimet e duhura në shtresën 3 (p. sh. një paketë ICMP procesohet ndryshe nga një paketë ARP).
	Ndarja nga rrjeti dhe protokolli LLC-ja mundëson funksionimin e pavarur nga lloji i rrjetit të protokolleve të shtresave më të larta. Kështu p.sh. IP-ja mund të zëvendësohet nga IPX-i ose Eth0 nga TokenRing-ut, pa patur ndonjë ndikim respektiv.
	Kontrolli i fluksit të të dhënave Kontrollon shpejtësinë me të cilën, të dhënat arrijnë në shtresat e larta. Në këtë mënyrë pengohet „përmbytja" e një hosti me të dhëna.
	Sekuencat e Frame-eve Në LLC frame-t, të cilat merren nga karta e rrjetit, vendosen sërish sipas rradhës së duhur.
Media Access Control (MAC)	**Adresimi fizik** Nëpërmjet adresës MAC çdo kartë rrjeti është qartësisht e identifikueshme në të gjithë botën. Adresa MAC bashkon në vetvete adresën unike Unique ID (UID) të prodhuesit dhe adresat specifike të tij. Të dyja janë vlera hexadecimale që paraqiten me 6 karaktere. Kur një frame merret nga shresa fizike, shtresa MAC kontrollon, nëse ajo është përcaktuar për kartën e rrjetit, dhe nëse është e nevojshme fillon procesimin.
	Framing Paketat, të cilat procesohen nga shtresa e rrjetit, transportohen përmes rrjetit në formën e frame-ve. Për këtë arsye administrohet Header-i dhe Trailer-i, si dhe kryhet një kontroll për gabime.

Modeli OSI në praktikë

Me modelin OSI u arrit një përcaktim i karakteristikave të komunikimit, i cili mund të shfrytëzohet nga institucionet (si p.sh. IEEE), për përcaktimin e standardeve, të cilat mbulojnë një, ose më shumë shtresa të modelit.

Duke marrë parasysh vlefshmërinë e përgjithshme të modelit OSI, ai gjithsesi mbetet jashtëzakonisht kompleks. Në rast se në fusha të caktuara ky kompleksitet nuk nevojitet, shpesh përdoren modele të tjera më të thjeshta, të cilat – në fushën ku përdoren – kufizojnë faktorë thelbësorë të teorisë së rrjetit. Më të përdorshmet janë modelet DoD dhe TCP.

Këto modele nuk mund ta zëvendësojnë asnjëherë modelin OSI, pasi njohuritë e mira mbi modelin OSI shërbejnë për një vlerësim të saktë të problemeve, apo si bazë për gjetjen e zgjidhjeve në fushën e komunikimit në rrjet.

3.4 Modeli DoD

Origjina

Ministria e Mbrojtjes e SHBA-së (Department of Defence = DoD) ka luajtur nje rol vendimtar në shumë zhvillime që i përkasin fushës së rrjeteve. Dhe nuk është për t'u çuditur, që nga DoD-ja u zhvillua një model rrjeti vetjak mbi bazën e modelit OSI. Vëmendja më e madhe në këtë model i kushtohet përshkrimit të komunikimit në Internet, dhe më pak vëmendje i kushtohet rrjeteve lokale. Si rezultat, në formën e vet standarde, modeli i kushton pak rëndësi ndryshimeve midis shtresave te modelit OSI në nivel aplikacionesh. Këto të fundit janë integruar si shërbime të Internetit në shtresën në fjalë.

Krahasimi midis modelit OSI dhe DoD

Modeli DoD-Modell përmbledh shtatë shtresat e modelit OSI në një model standard me katër shresa. Në disa burime përshkruhet një formë e veçantë e modelit DoD. Të përmendura shkurt në përmbledhje, duke marrë parasysh dhe përhapjen e pakët të tyre, nuk po i trajtojmë më tej, meqë kuptimi i tyre qartësohet nga përcaktimi i shtresave te modelit OSI.

Shtresat tek modeli OSI	Modeli OSI	Modeli DoD (Standard)	Forme modeli e veçantë	Shresat tek modeli DoD
7	Application Layer	Application Layer	Process Layer	4
6	Presentation Layer			
5	Session Layer		Application	
4	Transport Layer	Host-to-Host Layer	Host-to-Host Layer	3
3	Network Layer	Internet Layer	Internet Layer	2
2	Data Link Layer	Network Access Layer	Lokal Network Layer	1
1	Physical Layer		Network Access Layer	

3.5 Modeli TCP

Përqendrimi tek protokolli i Internet-it

Në mënyrë të ngjashme si modeli DoD, modeli TCP provon një thjeshtim të logjikës së ndërtimit, me qëllim që të mund t'i përshtatet më mirë praktikës së komunikimit. Sot, TCP/IP është pa dyshim familja më e përhapur e protokolleve. Komponentët qendrorë janë vendosur në shtresat 3 dhe 4 të modelit OSI. Ajo që ndodh në shtresat më poshtë dhe më sipër, fillimisht luan një rol të dorës së dytë.

Si rezultat, një model, që përdoret për përshkrimin e komunikimit përmes TCP/IP-së, nuk ka nevojë të përshkruajë çfarë ndodh në shtresat e aplikacioneve, apo në shtresat e aksesimit të rrjetit. Më poshtë paraqitet një model prej katër shtresash, që në parim korrespondon me modelin DOD dhe ndryshon nga ai vetëm në detaje të nomenklaturës.

Modeli OSI	Modeli TCP
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer, Host-to-Host-Layer
Network Layer	Network Layer, Internet Layer
Data Link Layer	Network Interface Layer
Physical Layer	

3.6 Paketimi dhe ç'paketimi

Paketimi

Kur të dhënat arrijnë nga shtresat më të larta në ato më të ulta, me të dhënat ndodhin dy fenomene. Nga njëra anë të dhënat copëzohen në paketa gjithnjë e më të vogla, me qëllim që në rast nevoje një paketë e vogël të mund të ritransmetohet sërish. Nga ana tjetër të dhënave u bashkëngjiten informacione kontrolli, me qëllim që nëpërmjet tyre të sigurohen informacione në lidhje me rradhën dhe integritetin e të dhënave.

Ky proces quhet paketim (kapsulim-capsulation) dhe gjatë ç'paketimit me të dhënat duhet të ndodhë procesi i kundërt. Tabela e mëposhtme tregon, se si ky proces i ndan të dhënat prej shtresës së aplikacioneve. Shtresat e larta konsiderohen si një shtresë e vetme, pasi nuk ndryshojnë dhe nuk luajnë asnjë rol në paketimin dhe ç'paketimin e të dhënave.

Sistemi 1		Sistemi 2
Application	Datagram: Të dhëna	**Application**
Presentation		**Presentation**
Session		**Session**
Transport	Segment: Header Të dhëna	**Transport**
Network	Packet: Header Të dhëna	**Network**
Data Link	Frame: Header Të dhëna	**Data Link**
Physical	Bits: Të dhëna	**Physical**

Nga këndvështrimi i një shtrese të nënrenditur bëhet fjalë, tek header-i i shtresave më të larta, për të dhëna të cilat nuk ndryshojnë nga pesha që zënë realisht. Kjo bëhet e qartë nga fakti që informacionet e header-it mund të vlerësohen vetëm nga shtresat që i kanë vendosur.

Përmes bashkimit të të dhënave dhe header-ave mund të jetë e nevojshme, që një segment të ndahet në dy paketa, meqë madhësia maksimale e njësisë së transmetimit (Maximal Transmission Unit, MTU) nuk lejohet të kapërcehet.

Ç'paketimi

Nëse marrësit i lejohet që të bëjë një ndryshim të informacioneve, atëherë procesi duhet të përsëritet në mënyrë të anasjelltë:

- ☑ Vlerësohen informacionet e header-it dhe të trailer-it .
- ☑ Header-i dhe trailer-i hiqen nga paketa.
- ☑ Nëse është e nevojshme segmentet grumbullohen dhe mblidhen sërish së bashku.
- ☑ Të dhënat dërgohen më tej tek shtresa më e lartë e afërt.
- ☑ Atje procesohen në mënyrën e duhur.

4 Mediat e transmetimit me kabëll

Në këtë kapitull do të lexoni:

- → si klasifikohen mediat e transmetimit prej bakri
- → si janë ndërtuar përcjellësit metalikë dhe jometalikë
- → si mund të përdoret në mënyrë efektive kablli prej bakri
- → si janë ndërtuar kabllot me fibra optike
- → si kryhet lidhja e kabllove me fibra optike

Parakusht

- ✓ Njohuri bazë mbi rrjetet

4.1 Karakteristikat dhe të dhënat teknike të transmetimit të sinjalit

Cilësia e transmetimit të sinjalit

Cilësia e transmetimit të sinjalit nëpërmjet kabllove prej bakri varet nga shumë faktorë. Bashkëveprimi i këtyre faktorëve përcakton karakteristikat e transmetimit të kabllove prej bakri, si p.sh. shpejtësinë e transmetimit, distancën e transmetimit dhe gjerësinë e bandës.

Të dhënat tekniko-fizike, të cilat luajnë një rol përcaktues në përkeqësimin e karakteristikave të transmetimit, rradhiten më poshtë sipas rëndësisë:

Faktorët	
Rezistenca e përcjellësit	Rezistenca e përcjellësit përcaktohet nga cilësia e bakrit të përdorur (përcjellshmëri specifike), nga seksioni tërthor dhe nga gjatësia e përcjellësit.
Rezistenca e valëve	Rezistenca e valëve përbëhet nga bashkësia e rezistencës, kapacitetit, përcjelljes dhe induktivitetit. Ajo përbën një karakteristikë teknike shumë të rëndësishme në një qark transmetimi.
Humbjet në kabëll	Çdo linjë transmetimi ndikohet nga humbjet. Shkak për këtë janë karakteristikat e kufizuara përçuese dhe humbjet dielektrike. Amplituda e një sinjali që kalon përgjatë kabllit bie.
Rezistenca e çiftimit (lidhjes)	Rezistenca e çiftimit është masë për cilësinë skermimit të kabllit. Ajo përcaktohet si raport i tensionit përgjatë skermos së kabllit të sistemit të interferuar me rrymën e sistemit interferues.
Humbjet në kthim të sinjalit	Humbjet në kthim të sinjalit janë ajo masë e sinjaleve të reflektuara në raport me sinjalin e dërguar që mund të shfrytëzohet. Sinjalet e reflektuara krijohen nga ndryshimet (variacionet) në strukturën e kabllit. Humbjet në kthim janë një matës shumë i mirë i cilësisë së një kablli prej bakri.
PSNEXT (Powersum NEXT)	Powersum NEXT përmban shumën e të gjitha sinjaleve interferuese, të cilat krijohen në një çift përcjellësish.
Vonesat e sinjalit	Me kohëzgjatje do të kuptojmë kohën që i duhet sinjalit të kalojë nga njëra pikë e medias së transmetimit në tjetrën. Ajo varet nga media e përdorur e transmetimit dhe i korrespondon shpejtësisë së dritës (tek transmetimet satelitore), ose më pak (tek transmetimet në kabllot prej bakri).
Deformimi i sinjalit	Sinjalet elektrike, në varësi të kapacitetit elektrik të vetë kabllit, deformohen në krahun fundor të sinjalit katror. Deformime të tilla mund të balancohen me ndihmën e përforcuesve (repeaters).

4.2 Teknika e kabllit prej bakri

Klasifikimi i kabllove prej bakri

Në thelb, mediat e transmetimit prej përcjellësish metalikë, klasifikohen në tre grupe sipas formës së ndërtimit:

- ☑ Kabëll koaksial
- ☑ Kabëll simetrik
- ☑ Kabëll josimetrik

Tek kabllot e grupit të fundit, fijet përbërëse janë të thurura në të gjithë gjatësinë e kabllit. Fusha e përdorimit të kabllove të tilla kufizohet në teknikën e drejtim-rregullimit, si dhe në prodhimin e makinerive. Në fushën e transmetimit të të dhënave, përdorimi i këtij kablli është i kufizuar. Kabllot me ndërtim josimetrik janë të përshtatshme vetëm për transmetimet në gjerësi bande në diapazonin e ngushtë prej disa mijëra Herz. Në teknikën e transmetimit të të dhënave përdoren kryesisht frekuenca më të larta transmetimi.

Kablli koaksial është një formë ndërtimi e veçantë e kabllit josimetrik. Sipas rezistencës së valëve këto kabllo përdoren në fusha të ndryshme p.sh. për rrjetet shpërndarëse me bandë të gjerë (televizionet kabllore), ose rrjetet lokale.

Ndërtimi i kabllove prej bakri

Karakteristikat më të rëndësishme të përcjellësve elektrik, që përdoren për transmetimin e të dhënave, janë karakteristikat mekanike dhe elektrike, si:

- ☑ Ndërtimi i përcjellësit
- ☑ Veshja
- ☑ Materialet izoluese të kabllit
- ☑ Thurja e fijeve
- ☑ Skermimi (Mbrojtja)
- ☑ Sjelljet në transmetim (p. sh. humbjet, vonesa e sinjalit)

Ndërtimi i përcjellësve

Kabllot me përcjellës metalik përbëhen prej një, apo më shumë fijesh. Nga ana e tyre këto të fundit mund të përmbajnë disa përcjellës më të hollë, ose një përcjellës të vetëm masiv me një prerje tërthore të caktuar.

Përdorimi i llojeve të përcjellësve varet nga kërkesat që paraqiten për kabllin. Kështu, kabllot masive përdoren aty ku gjatë shtrimit kërkohet qëndrueshmëri dhe janë më të përshtatshme se kabllot me shumë fije. Kabllot masive kanë disavantazhin, që për shkak të karakteristikave të tyre, janë më pak të përkulshme dhe nuk janë fleksibël. Por sidoqoftë, ato kanë karakteristika elektrike më të mira se kabllot me fije të holla. Kabllot me fije të holla janë më të përshtatshme si kabllo të parakonfiguruara (patchkabëll), apo si kabllo lidhëse fundore për pc-të dhe pajisjet periferike, meqë janë më fleksibël dhe manovrohen më lehtë.

Mediat e transmetimit me përcjellës metalik mund të përbëhen prej materialesh të ndryshme. Më shpesh si përçues elektrik përdoret bakri. Mund të përdoren edhe materiale të tjera bazë, por përdorimi i tyre në shumicën e rasteve kushtëzohet nga kostot e blerjes dhe përpunimit të lëndës së parë.

Materiali	Aftësia përcjellëse	Karakteristikat e ngjitjes (saldimit)	Karakteristikat në përkulje	Kostot
Bakër	Shumë e mirë	Të mira	Shumë të mira	Të ulta
Bakër me zink	Shumë e mirë	Shumë të mira	Të mira	Të ulta
Bakër me argjend	Shumë e mirë	Shumë të mira	Të mira	Shumë të larta
Bakër me nikel	E mirë	Të mjaftueshme	Të kënaqshme	Mesatare
Nikel	E kënaqshme	Nuk ka	Të mjaftueshme	Të larta
Alumin	E mirë	Të këqia	Shumë të mira	Të ulta

Veshjet e kabllove

Krahas karakteristikave mekanike dhe elektrike të përcjellësve, veshja e kabllit është një karakteristikë e rëndësishme tek mediat e transmetimit me kabëll. Veshja e kabllit mbron përcjellësit ndaj faktorëve të jashtëm si tërheqja, shtypja, përdredhja, por edhe nga lagështira, efektet kimike dhe zjarri. Në zgjedhjen e veshjes së përshtatshme të kabllit një rol të rëndësishëm luan edhe vendi ku ai do të përdoret. Për kabllimet brenda godinës vlejnë rregulla të tjera krahasuar me kabllimet në mjediset e jashtme.

Një vend të rëndësishëm zënë fushat e përdorimit në industri, meqë këtu mbizotërojnë mjediset me temperatura të larta dhe me shumë lagështirë dhe në situata të caktuara ndodhin dhe procese kimike. Materiali i veshjes së jashtme të kabllit për një mjedis të tillë duhet përcaktuar saktë që më parë në bashkëpunim të ngushtë me prodhuesin e kabllit.

Në mjediset e jashtme kabllot duhen veshur me materiale që i mbrojnë nga brejtësit dhe lagështia.

Materiale tipike për izolim dhe veshje

Materiali	Shkurtimi	Standardi DIN/VDE
Chloropren-Kauçuk	CR	5G
Kauçuk natyral / Styrol -Butadien-Gomë	NR/SBR	G
Polivinilklorid	PVC	Y
Kauçuk silikoni	SIR	2G
Etilen-Vinilacetat	EVA	4G
Poliurethan	PUR	11Y
Përzierje pa halogjen rezistente ndaj zjarrit	FRNC	
Cell-Polietilen	Zell-PE	2Y
Polietilen i rrjetëzuar	VPE	2X
Polietilen	PE	
Teflon	FEP	6Y
Polipropilen	PP	9Y

Kur të përdorni në kompaninë tuaj kabllo për transmetim të dhënash kujdesuni të përdorni kabllo kundër zjarrit dhe pa halogjen. Në terminologjinë ndërkombëtare materialet e sipërpërmendura quhen si më poshtë:

- ☑ Flame Retardant = FR
- ☑ Non Corrosive = NC
- ☑ Low Smoke Zero Halogene = LSOH

Materialet veshëse dhe izoluese pa halogjen dhe kundër zjarrit shpërbëhen vetë në rast zjarri. Përdorimi i një kabllit të tillë rekomandohet veçanërisht në mjedise zyre. Një strukturë në formë ylli, për shkak të trashësisë së trankut kabllor, në vende të caktuara mund të krijojë premisa për rritjen e intensitetit të zjarrit. Gjatë djegies PVC-ja lëshon gaze helmuese, të cilat në bashkëveprim me ujin krijojnë acide agresive dhe shkatërruese.

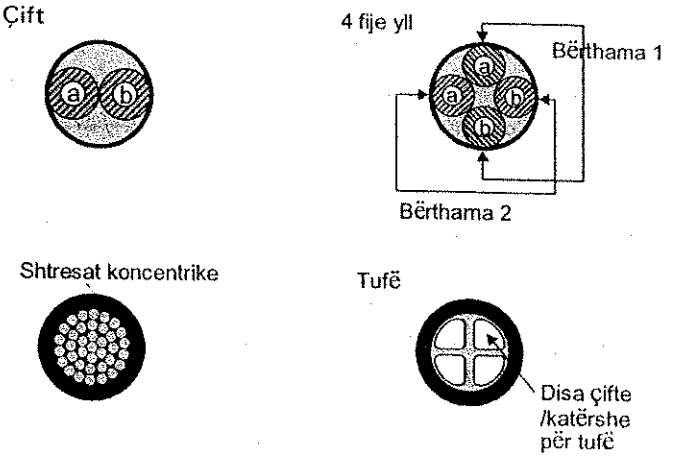
Para shtrirjes së kabllit kontrolloni nëse është pa halogjen. Të dhëna për këtë qëllim do të gjeni në katalogjet e prodhuesit përkatës, ose direkt mbi kabëll, p. sh. S/STP 4x2xAWG23 4P *H*.

Një përparësi tjetër e kabllove me përzierje materiali pa halogjen dhe kundër zjarrit është fakti se në rast djegieje ato nuk lëshojnë dioksine. Dioksina lëshohet p.sh. gjatë djegies së PVC-së, apo materialeve të ngjashëm që përmbajnë klor.

Thurja dhe grupimi i fijeve

Thurja është përdredhja njëra me tjetrën e fijeve të izoluara që përbëjnë kabllin. Me qëllim që të pengohen interferencat e ndërsjellta të fijeve përbërëse të kabllove simetrike, ato thuren me njëra-tjetrën sipas një skeme të përcaktuar. Tipike është thurja e dy ose katër fijeve në një çift fijesh apo katërshe fijesh.Tek një thurje fijet përbërëse renditen në bllok apo në tufë koncentrike. Në varësi të mënyrës se si është kryer thurja, dallojmë midis thurjes bllok dhe asaj tufë.

Numri i përdredhjeve për metër përbën një masë konstruktive për uljen e interferencave të kryqëzuara (cross-talk) tek kabllot simetrikë. Disa prodhues kabllosh përdorin teknikat e tyre të veçanta të thurjes për të zvogëluar sa më shumë interferencat.



Llojet e thurjeve; majtas poshtë: thurje bllok, në krah: thurje tufë

Skermimi (mbrojtja)

Për të mbrojtur fijet që përcjellin sinjalin nga interferencat e jashtme, kabllot për transmetimin e të dhënave janë të skermuara. Skermimi zvogëlon rrezatimin e valëve elektromagnetike. Tek skermimi dallojmë foliet (fletët) mbrojtëse dhe skermon reflektuese. Një kombinim i të dyjave është gjithashtu i mundur. Numri i elementeve të kabllit, të cilat përdorin një skermo të përbashkët, jepet si më poshtë:

- ☑ 1 fije në folien mbrojtëse
- ☑ Çift fijesh në folien mbrojtëse
- ☑ Tre fije në folien mbrojtëse
- ☑ Katërfijësh në folien mbrojtëse
- ☑ Tufë fijesh në folien mbrojtëse

Si material për folien mbrojtëse përdoret poliesteri. Skermoja reflektuese përbëhet prej një rrjete të hollë bakri .

Marrëdhëniet e transmetimit

Me qëllim që të mund të kryhet një transmetim të dhënash pa probleme, percjellësve elektrikë iu vihen kërkesa të ndryshme përsa i përket karakteristikave. Krahas vlerave standarde, si prerja tërthore e përcjellësit, aftësitë përçuese të tij, respektivisht rezistenca, kontribuojnë në cilësinë e përcjellësit të transmetimit edhe parametra të tillë si rezistenca e izolimit dhe rezistenca e valëve.

Rezistenca e valëve është një madhësi, e cila është shumatore e rezistencës së përcjellësit, rezistencës së izoluesit, kapacitetit dhe induktivitetit në punë. Gjatë përshtatjes së gabuar të përcjellësit me rezistencën e valëve mund të rezultojnë pasqyrime (reflektime).

Çiftimi i sinjaleve nga një përcjellës në tjetrin ndikon negativisht në mënyrën e transmetimit. Kjo interferencë e kryqëzuar e sinjaleve varet nga frekuenca. Përmes një ndryshimi mekanik të ndërtimit të thurjes së fijeve përbërëse të kabllit ndryshojnë karakteristikat e tij. Tensionimet e mëdha mekanike gjatë instalimit, përkeqësojnë interferencat tërthore. Forca të larta në tërheqje dhe shtypje gjatë instalimit shkaktojnë ndryshimin e seksionit tërthor të kabllit (rrjedhje në të ftohtë).Rezultati është një vlerë shumë e lartë humbjesh.

Për përdorimin e kabllit prej bakri për transmetimin e të dhënave vlejnë kërkesat e mëposhtme:

- ☑ Humbje të vogla
- ☑ Shpejtësi të larta transmetimi
- ☑ Distanca të mëdha
- ☑ Interferenca të vogla

4.3 Specifikimet

Kablli koaksial

Kabllot koaksiale paraqisnin deri para pak kohësh llojin më të përhapur të kabllimit në lidhjet në rrjet.. Arsyet kryesore për këtë ishin çmimi relativisht i ulët dhe ndikimi i vogël i interferencave të ndryshme. Kabllot koaksiale (të njohur ndryshe edhe si kabllo BNC) përdoren për topologjitë e rrjetit të tipit „autobuz" (Bus-Topolgy). Kapaciteti maksimal i transmetimit arrin në 10 MBit/s.

- ☑ Përcjellësi i brendshëm (bakri) mbështillet me një shtresë izoluese (dielektrike).
- ☑ Skermimi prej rrjete metalike apo prej flete alumini mbron të dhënat që transmetohen nga humbjet e sinjaleve elekronike që lëvizin nga një vend në tjetrin, të cilat quhen ndryshe edhe zhurma, në mënyrë që këto të mos ndikojnë negativisht mbi kabëll dhe të dhënat të mos deformohen gjatë transmetimit.
- ☑ Mbështjellja e jashtme e mbron kabllin nga influencat e drejtpërdrejta mbi të si, papastërtitë, nxehtësia dhe tërheqja.

Për kushte ekstreme të mjedisit, p. sh. mjedise me rrezatim të lartë zhurmues, kabllot koaksiale prodhohen me skermo katërfishe. Skermoja e katërfishtë përbëhet prej dy shtresash me fletë izoluese dhe prej dy shtresave skermo prej rrjete metalike.

Përcjellësi i brendshëm

Përcjellësi i brendshëm i një kablli koaksial transmeton sinjale elektronike, të cilat mbartin me vete të dhëna. Ky përcjellës mund të jetë një i tërë ose i thurur. Nëse fija e kabllit përbëhet prej një materiali të plotë, atëhere ai në shumicën e rasteve është prej bakri.

Përcjellësi i brendshëm rrethohet nga një shtresë e trashë jo përcjellëse, e cila e ndan atë nga rrjeta e hollë metalike dhe e stabilizon deri diku mekanikisht. Rrjeta e hollë metalike shërben për tokëzim duke e mbrojtur në këtë mënyrë përcjellësin e brendshëm nga interferencat elektrike dhe interferencat e kabllove fqinjë.

Përcjellësi i brendshëm dhe rrjeta metalike duhen të jenë të ndara nga njëra-tjetra, pasi në rast të kundërt në kabëll do të ndodhte një qark i shkurtër. Kjo sjell si pasojë, që interferencat elektrike të transmetohen në kabllin prej bakri.

Kabllot koaksiale, janë më pak të ndjeshme se kabllot me çifte të përdredhura (Twisted-Pair), përsa i përket humbjeve (zvogëlimit të fuqisë së sinjalit gjatë rrugës së tij nëpër kabëll) dhe interferncave të tjera.

Kryesisht dallojmë dy lloje kabllosh koaksiale:

- ☑ I hollë - Thinnet
- ☑ I trashë - Thicknet

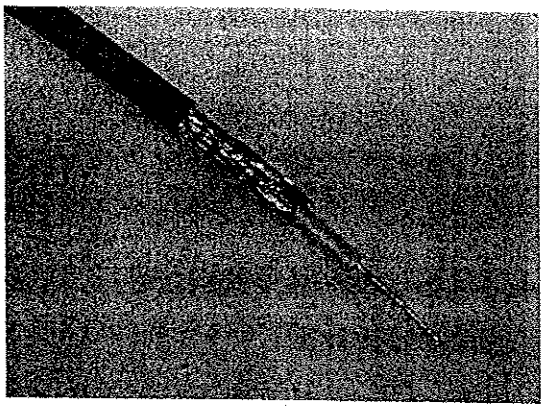
Se cili kabëll do të përdoret, kjo varet nga kërkesat e rrjetit përkatës.

Kablli Thinnet

Ky lloj kablli koaksial është mjaft i përkulshëm dhe i përshtatshëm gati për të gjitha instalimet e rrjeteve. Ai ka një diametër prej rreth 0,64 centimetrash (0,25 Inch).

Nëpërmjet këtij kablli mund të transmetohen sinjale deri në një largësi prej 185 metrash pa pasur humbje të konsiderueshme të sinjalit.

Kablli Thinnet i përket grupit të kabllove RG-58. Ai paraqet një rezistencë prej 50 Ohm (Impedanca përshkruan rezistencën (matur në Ohm) ndaj rrymës alternative, e cila kalon përmes përcjellësit të brendshëm). Veçoria kryesore e një kablli RG-58 është, që fija e brendshme e tij është prej bakri.



Kabëll koaksial RG-58 me fijen kryesore të thurur

Tabela: Llojet dhe përshkrimi i kabllove koaksiale

Kabllo	Përshkrimi
RG-58 /U	Përcjellësi i brendshëm prej teli masiv bakri, Thinnet, 10Base2 (53.3 Ohm)
RG-58 A/U	Përcjellësi i brendshëm i thurur, Thinnet, 10Base2 (50 Ohm)
RG-58 C/U	Specifikimi sipas standartit ushtarak i RG-58 A/U
RG-59	Transmetim me bandë të gjerë, p. sh. tek televizionet kabllore (75 Ohm)
RG-62	Arc-Networks dhe SNA (93 Ohm)
RG-8 A/U	Thicknet, 10Base5 (50 Ohm)

Kablli Thicknet

Kabllot Thicknet janë krahasimisht më të ngurtë dhe kanë një diametër prej rreth 1,27 centimetra (0,5 Inch). Këto kabllo përshkruhen nganjëherë edhe si kabëll i verdhë "Yellow Cable", apo kabëll standard Ethernet-i, pasi ky ishte kablli i parë, i cili u përdor në arkitekturën gjerësisht të përhapur të rrjetit Ethernet.

Bazuar në diametrin e trashë, nëpërmjet këtij lloj kablli mund të të transmetohen të dhëna në largësi më të mëdha se nëpërmjet kablit Thinnet. Largësia maksimale është rreth 500 metra. Për shkak të vështirësive në shtrim, përdorimi i kabllove thicknet ka qenë i kufizuar.

Kablli katërfijësh yll

Në rastin e një kablli katërfijësh yll bëhet fjalë për një kabëll telefoni të përmirësuar, brenda të cilit janë thurur katër fije të izoluara me njëra-tjetrën. Fusha kryesore e përdorimit të një kablli të tillë është telefonia. Karakteristikë e veçantë e këtij kablli është konstruksioni i tij. Kabllot katërfijësh yll janë thurur në mënyrë kaq stabël, saqë edhe në shtrimet me kërkesa shumë të larta për kabllot fijet nuk lëvizin. Variantet e sotme të kablit katërfijësh yll janë:

- ☑ JYY 2 x 2 x 0.6 = dy fije dyshe
- ☑ JYY 4 x 2 x 0.6 = katër fije dyshe
- ☑ JYY 6 x 2 x 0.6 = gjashtë fije dyshe
- ☑ JYY 10 x 2 x 0.6 = dhjetë fije dyshe
- ☑ JYY 20 x 2 x 0.6 = njëzet fije dyshe
- ☑ JYY 50 x 2 x 0.6 = pesëdhjetë fije dyshe
- ☑ JYY 100 x 2 x 0.6 = njëqind fije dyshe

Kabllot katërfijësh yll ekzistojnë për mjedise të jashtme dhe të brendshme. Kabllot e jashtme i gjejmë kryesisht si 200 x, 500 x, apo si 1000 x 2 x 0.6 në formën e kabllove lidhës të shtruar për tek vendshpërndarja (exchange point).

Kabllot katërfijësh yll kanë përparësinë e madhe, që i kanë përmasat më të vogla se kabllot Twisted-Pair. Kjo përparësi është veçanërisht e rëndësishme në rastet kur vendet ku kalon kablli janë të ngushta dhe me kthesa.

Twisted-Pair-Kabël

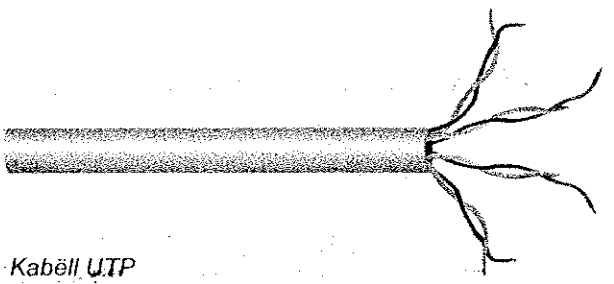
Një formë e veçantë e kabllit të bakrit simetrik është kablli Twisted-Pair. Në teknikën e lidhjes në rrjet ky lloj kablli përdoret gjerësisht. Nëpërmjet ndërtimit me thurje të dy fijeve të izoluara arrihen karakteristika të mira transmetimi me kosto të ulta. Çifti i përdredhur (twisted pair) krijon qëndresë ndaj interferencave të jashtme. Kabllin Twisted-Pair e gjejmë në forma të ndryshme si:

- ☑ kabël Twisted-Pair të paskermuar (unshielded) = UTP
- ☑ kabël Twisted-Pair të skermuar (shielded) = STP
- ☑ kabël Twisted-Pair me skermim të plotë = S/UTP
- ☑ kabël Twisted-Pair me skermim të plotë dhe çift fijesh të skermuara = S/STP
- ☑ kabël Twisted-Pair me skermo me fletë = FTP

Për shkak të karakteristikave të mira që paraqesin, kabllot Twisted-Pair përdoren gjerësisht në ndërtimin e rrjeteve të reja. Nëpërmjet këtij kablli arrihen flukse transmetimi deri në 100 MBit/s e më shumë. Kablli Twisted-Pair është një media transmetimi, e cila mbulon shërbimet më të rëndësishme në rrjet. Standardi i kabllove TP është me dy dhe katër çifte.

Kabllot Unshielded Twisted-Pair (UTP)

Unshielded (i paskermuar) do të thotë, që çiftet e veçanta të përdredhura nuk kanë skermim në çift. Ky lloj ndërtimi i bën kabllot UTP shumë të ndjeshme ndaj interferencave të jashtme, kështu p. sh. ndaj interferencës së sinjaleve të çifteve fqinjë ose nga impulset me frekuencë të lartë të çelsave elektrik. Në rast se kabllot UTP janë shtrirë në një mjedis industrial, atëhere makineritë nëpërmjet qarqeve të rrymave dhe tensioneve të larta mund të krijojnë zhurma në transmetim. Këto ndikojnë negativisht në transmetitmin e të dhënave.



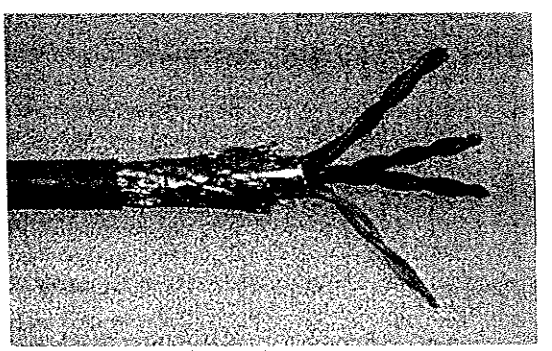
Kabël UTP

Kabllot Shielded Twisted-Pair (STP)

Shielded (i skermuar) do të thotë, që çiftet e përdredhura kanë mbrojtje (skermim) në çift. Ky lloj kablli është i pandjeshëm ndaj interferencave të jashtme. Nëpërmjet fletës mbrojtëse çiftet e fijeve janë pothuaj të izoluara ndaj ndikimeve nga kabllot fqinje. Edhe rrezatimet që ato vetë lëshojnë janë nën kontroll përmes kësaj veshjeje mbrojtëse. Transmetimi i sinjalit nëpërmjet kabllove STP është dukshëm më i mirë përkundrejt kabllove UTP. Në këtë mënyrë, kabllot STP lejojnë transmetime të dhënash në distanca më të mëdha dhe me fluks më të lartë.

Nëpërmjet një skermim të përgjithshëm shtesë prej rrjete bakri përmirësohen efektet e interferencave – si të brendshme ashtu dhe të jashtme - për të gjithë sistemin.

Duke pasur parasysh karakteristikat e EMV-së (qëndrueshmëria elektromanjetike) mënyra e ndërtimit të këtij kablli është plotësisht domethënëse. Të ashtuquajturat kabllo S/STP janë sot standardi për kabllimin e strukturuar të ndërtesave.



Kabël STP

4.4 Fushat e përdorimit

Kabllot koaksiale

Kabllot koaksiale përdoren në fushën e rrjeteve kompjuterike, ekskluzivisht tek topologjitë bus. Krahasuar me kabllimet që përdorin kabllo twisted-pair apo fibra optike, zgjidhja me kabllo koaksiale është shumë e leverdisshme përsa i përket kostove, por sidoqoftë sot pothuaj nuk përdoren më, pasi fluksi i transmetimit prej 10Mbps që ato lejojnë të transmetohet është mjaft i ulët për t'u marrë në konsideratë

Kabllot Thinnet

Diametri i vogël prej 0,64 centimetrash e bën këtë kabëll shumë mirë të manovrueshëm. Ai është elastik dhe mund të shtrohet mirë në kanale apo kuti kabllosh. Ky lloj kablli nuk është i përshtatshëm për instalime të jashtme.

Kabllot Thicknet

Diametri prej 1,27 centimetrash e bën kabllin thicknet shumë të ngurtë dhe joelastik. Si rezultat, ai nuk është i përshtatshëm p.sh. për kabllimin e ambjenteve të brendshme të zyrave. Duke pasur parasysh distancën e lejuar prej 500 m, ky kabëll përdoret rëndom si backone për të lidhur me njëra-tjetrën p.sh. dy ndërtesa. Ai është i përshtatshëm për instalime të jashtme.

Kabllot me çifte të përdredhura të paskermuara (Unshielded Twisted-Pair - UTP)

Ky lloj kablli përdoret gjerësisht në SH.B.A. Ai shërben si kabëll komunikimi për transmetimin e zërit dhe të dhënave. Për shkak të disavantazheve që ai paraqet, sidomos në lidhje me ndjeshmërinë ndaj interferencave, ky lloj kablli nuk rekomandohet. Avantazh i këtij kablli janë përmasat e vogla, meqë i mungon veshja mbrojtëse.

Kabllot UTP përshtaten mirë për telefoninë (analoge dhe dixhitale), Token Ring me 4 dhe 16 Mbps, Ethernet, shërbimet për transferimin e të dhënave dhe rrjetet terminale.

Kabllot me çifte të përdredhura të skermuara (Shielded Twisted-Pair - STP)

Kabllot STP përdoren gjerësisht në kabllimet e reja dhe zgjerimet e kapaciteteve të rrjeteve ekzistuese brenda godinave. Ky lloj kablli përdoret si alternativë e leverdisshme e kabllove me fibra optike për kabllimin brenda ndërtesave. Meqë fluksi i transmetimit që lejon kablli STP është 100 Mbps, ai është i përshtatshëm edhe për lidhjen e posteve të punës që përdorin CAD-in apo CAM-in. Ai përdoret edhe për transmetimin e të dhënave të mëdha multimediale. Për shkak të karakteristikave më të mira që paraqesin kabllot STP, ato janë të preferueshme. Në rastin e zgjedhjes së një kablli UTP mund të ndodhë që gjatë transmetimit në lidhjet me performanca të larta të ketë zhurma interference të padëshiruara.

4.5 Kategoritë

Ndarja e kategorive sipas ISO/IEC

Meqë tashmë ekziston një shumëllojshmëri kabllosh simetrike prej bakri me përdorim të shumëanshëm, lind nevoja e kategorizimit dhe klasifikimit të tyre. Baza për një klasifikim të kabllove prej bakri për transmetimin e sinjaleve janë normat ISO-s (International Standard Organization) dhe IEC-së (International Electronical Commission). P.sh një normë me emërtimin ISO/IEC DIS 11801 vendos standardet e kabllit për të cilat qëllime do të përdoret kablli i bakrit. Standardi Evropian EN 50173 bazohet në standardin ndërkombëtar ISO/IEC 11801.

Për të pasur një ide më të qartë në lidhje më llojet e ndryshme të kabllove, ato janë ndarë në kategori të ndryshme. Këto kategori marrin parasysh vlerat e standardeve të mësipërme për fushat përkatëse të përdorimit.

Kategoria	Klasa	Brezi i frekuencave	Aplikimi/Shërbimi
Kategoria 1	Klasa A	Deri 100 KHz	Telefoni, Modem Dial Up
Kategoria 2	Klasa B	Deri 1 MHz	ISDN, kabllim IBM lloji 3
Kategoria 3	Klasa C	4 deri 16 MHz	Token Ring, Ethernet
Kategoria 4		Deri 20 MHz	Nuk përdoret
Kategoria 5	Klasa D	Deri 100 MHz	TPDDI, Fast Ethernet
Kategoria 6	Klasa E	Deri 250 MHz	Fast Ethernet, Gigabit Ethernet
Kategoria 7	Klasa F	Deri 700 MHz	Gigabit Ethernet, CATV
Kategoria 8	Klasa G	Deri 1200 MHz	Përdorime në të ardhmen

Si kategori ndërmjetëse midis kategorisë 5 dhe 6 eziston kategoria 5e (enhanced – e përmirësuar) ose ndryshe 5+. Kjo kategori bazohet në kategorinë 5, por sidoqoftë ka vlera kufi të ndryshme. Këto vlera janë më të larta se tek kategoria 5, por sidoqoftë ato mbeten poshtë vlerave që kërkon kategoria 6. Diapazoni matës për kategorinë 5e është njëlloj si tek kategoria 5 me 100 MHz.

Në ndarjen sipas kategorive merren parasysh vetëm komponente të veçantë, si kablli apo teknika e lidhjes. Në ndarjen sipas klasave merret parasysh i gjithë kanali i transmetimit.

Kategoria 7

Propozimi i sotëm i standardit për kategorinë 7, klasa F, duhet të gjejë përdorim në transferimin e të dhënave në diapazonin deri 1 GHz. Aplikacione, të cilat kërkojnë këto flukse të larta transferimi, për momentin nuk kërkohen apo janë ende në zhvillim. Meqë prodhuesit e komponentëve të shpejtësive të larta, komponentë të cilët nga ana tjetër transmetojnë të dhëna me shpejtësi 1 Gbps (ATM me 2,4 Gbps), favorizojnë më tepër përdorimin e fibrave optike, atëhere në të ardhmen nuk do t'ia vlejë përdorimi i kabllove të kategorisë 7.

4.6 Përcjellësit e valëve të dritës

Të përgjithshme

Përcjellësit e valëve të dritës i përkasin mediave të transmetimit me përcjellës jometalik. Sipas materialit të përdorur, përcjellësit e valëve të dritës (LWC) ndahen në fibra optike ose fibra plastike. Ndërtimi mekanik dhe përhapja e sinjaleve janë identike tek të dy llojet e fibrave.

Fibrat optike

Tek kabllot prej fibrash optike si bërthama ashtu edhe veshja (cladding) përbëhen nga kuarc i pastërtisë së lartë (SiO_2) me tregues të ndryshëm thyerjeje.

Bazuar në karakteristikat që paraqesin, kabllot me fibra optike janë të përshtatshme veçanërisht për transmetimin e sinjaleve në distanca të largëta, p. sh. për ndërtesa të tëra ose distancat midis kateve. Në teknikën e transmetimit të të dhënave përdoret ekskluzivisht ky lloj përcjellësi i valëve të dritës (LWC – Light Wave Conductor). Duhet pasur kujdes, që në përgjithësi kur flasim për një kabëll LWC gjithmonë bëhet fjalë për një kabëll me fibra optike.

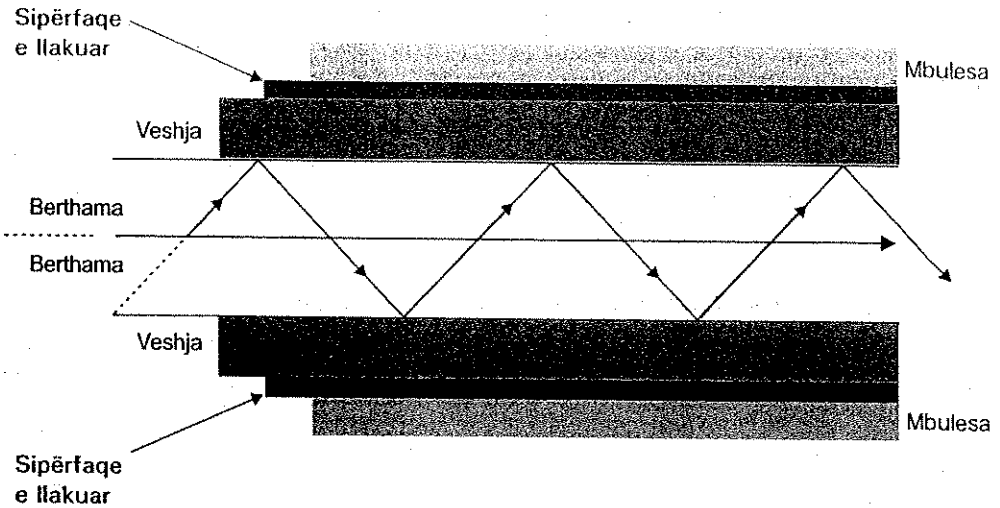
Fibrat plastike

Një variant tjetër i LWC-ve është i ashtuquajturi fibër plastike (plastic fiber). Tek fibrat plastike për transmetimin e sinjalit përdoret një përçues plastik drite. Fibrat plastike janë më të leverdisshme dhe më të lehta për shtrim, por ato kanë disavantazhin se kanë karakteristika transmetimi shumë më të këqija se fibrat optike. Për shkak të vlerave të larta të humbjeve dhe si rezultat i distancave të shkurtra të transmetimit, ky lloj kablli nuk përdoret në fushën e rrjeteve kompjuterike. Ai përdoret në fushën e industrisë së automobilave, ose për efekte drite në kushtet e shtëpisë.

4.7 Veçoritë e kabllove me fibra optike

Ndërtimi

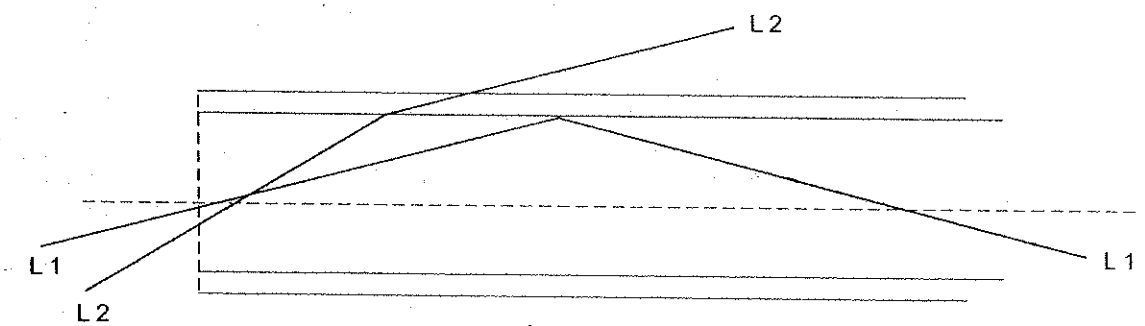
Përçuesit e valëve të dritës, në ndërtimin e tyre bazë, përbëhen nga një bërthamë (core) dhe një veshje, e ashtuquajtura cladding. Bërthama dhe veshja rrethohen edhe nga një mbulesë shtesë (primary coating) për mbrojtjen nga dëmtimet mekanike. Drejtimi i një impulsi drite bëhet në bërthamë dhe veshje (Light impuls). Mbulesa shtesë është vetëm një mbrojtje nga dëmtimet mekanike. Midis Cladding dhe Primary Coating gjendet edhe një shtresë llaku me trashësi 2 deri 5 μm. Ajo shërben për të mbrojtur fibrën nga depërtimi i lagështirës.



Fibër optike me rreze drite përshkuese

Transmetimi i sinjalit

Në një përcjellës valësh drite sinjalet transmetohen në formën e impulseve të dritës. Transmetimi kryhet vetëm në një drejtim (unidirectional), prandaj për transmetim janë të nevojshme dy fibra. Përhapja e sinjaleve të dritës (light impulses) në përcjellës bazohet në parimin e pasqyrimit të plotë (reflektimit total). Drita përthyhet gjatë kalimit nga një mjedis optikisht më pak i dendur në një mjedis optikisht më të dendur. Ky efekt shfrytëzohet gjatë transmetimit të impulseve të dritës në fibrat optike.



Parimi i pasqyrimit të plotë

Rrezja e dritës L2 përthyhet nën një kënd të madh rënieje (kënd pranueshmërie). Ajo përthyhet në kufirin e shtresës që ndan bërthamën nga veshja dhe del jashtë fibrës. Për transmetimin e informacioneve një rreze drite e këtij lloji është e papërshtatshme. Më e përshtatshme për këtë qëllim është rrezja e dritës L1. Për shkak të këndit të saj të favorshëm, rrezja e dritës L1 pasqyrohet plotësisht në kufirin e shtresës që ndan bërthamën nga veshja dhe qëndron brenda përcjellësit të valëve të dritës.

Përgjithësisht kemi që: Një rreze drite gjatë kalimit nga një mjedis optikisht më pak i dendur, (p.sh. ajri) në një mjedis optikisht më të dendur (p. sh. kuarci), përthyhet me një kënd me të ngushtë me pingulen se këndi fillestar. Gjatë kalimit nga një mjedis optikisht më i dendur në një mjedis optikisht më pak të dendur, rrezja e dritës përthyhet në një kënd më të gjërë me pingulen se këndi fillestar.

Avantazhet	Disavantazhet
Flukse të larta transmetimi	Përpunimi është i kushtueshëm
Humbje të vogla në transmetim	Kosto lidhjeje më të larta krahasuar me teknikat me kabllot prej bakri
Nuk ka interferenca nga fijet/fibrat fqinje	Pajisje dhe komponentë aktivë të shtrenjtë
Nuk ndikohet nga interferencat e fushave elektrike nga jashtë	Pikë e dobët teknologjia e kokave lidhëse
Nuk ka zhvendosje potencialesh	E ndjeshme ndaj ngarkesave mekanike
Mbrojtje më e madhe e investimit	Kosto të larta riparimi
Shtrimi në zona të rrezikuara nga shpërthimi	Kosto më të larta pas instalimi
E sigurt ndaj përgjimit	
Formë ndërtimi kompakte	
Nuk kërkohen masa shtesë për ta ruajtur nga mbitensioni	

Humbjet

Karakteristikat e transmetimit të fibrave optike varen shumë nga humbjet e sinjaleve optike, gjatësitë e valëve dhe lloji i përdorur i fibrës. Humbjet në kabllin me fibra optike duhet të jenë sa më të vogla që të jetë e mundur. Tek një kabëll transmetimi, e cila mbulon një distancë të caktuar, humbjet totale janë shumatorja e humbjeve që shkaktojnë shkaqet e veçanta.

Shkaqet më të rëndësishme të humbjeve të sinjaleve optike janë:

- ☑ Gjatësia totale e një linje kabllore
- ☑ Defektet tek fibrat optike
- ☑ Koka e kabllit shumë e papastër
- ☑ Gabime në shtrirjen e kabllit
- ☑ Ngjitje e keqe
- ☑ Numri i lidhjeve
- ☑ Rreze bërthame të ndryshme dhe profilet e thyerjeve
- ☑ Defekte në bashkim
- ☑ Sipërfaqja e kokave e pastruar keq
- ☑ Papastërti tek pajisjet optike dërguese/marrëse

Produkti gjerësi bande x gjatësi

Produkti gjerësi bande-gjatësi (gjerësia e bandës në MHz, gjatësia në km) është parametri vendimtar për përcaktimin e transmetueshmërisë së gjerësisë së bandës dhe distancës së mbuluar. Produkti gjerësi bande-gjatësi mund të jepet si për mjediset metalike të transmetimit, ashtu edhe për ato optike. Produkti gjerësi bande - gjatësi jepet në lidhje me një përcjellës valësh drite të caktuar. Produkti gjerësi bande - gjatësi varet nga faktorë të ndryshëm si p. sh. lloji i fibrës dhe gjatësia e valëve.

Tek një produkt me gjerësi bande prej 800 MHz x km mund të

- ☑ punojë në gjatësi 500 m me një gjerësi bande prej 1,6 GHz
- ☑ punojë në gjatësi 1 km me një gjerësi bande prej 800 MHz
- ☑ punojë në gjatësi 2 km me një gjerësi bande prej 400 MHz

Produkti gjerësi bande gjatësi jepet në dokumentat shoqëruese të prodhuesit. Kini parasysh në zgjedhjen e të dhënave se çʼllój fibre, pra gjatësie valësh përdoret në kompaninë tuaj.

Shënime

Shembull për karakteristikat optike të një kablli me fibra optike multimode:

Lloji fibrës [µm]	50 µm / 125	62,5 µm / 125	E9, 10 µm / 125
Humbja [dB/km] në 850 nm	2,7	2,8	--
Humbja [dB/km] në 1300 nm	0,7	0,8	0,34
Humbja [dB/km] në 1550 nm	--	--	0,21
Raporti gjerësi bande-gjatësi [MHz/km]			
850 nm	>400	>200	--
1300 nm	>800	>500	--

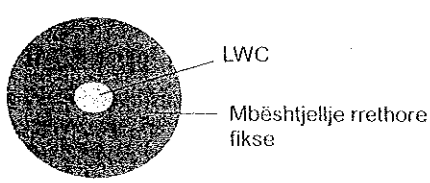
☑ Dispersion modal
☑ Dispersion profili
☑ Dispersion materiali
☑ Dispersion valësh

Dispersioni ka një ndikim të madh mbi gjerësinë e bandës së transmetimit dhe si pasojë me raportin gjerësi bande-gjatësi.

4.8 Ndërtimi i fibrave

Fibër fikse

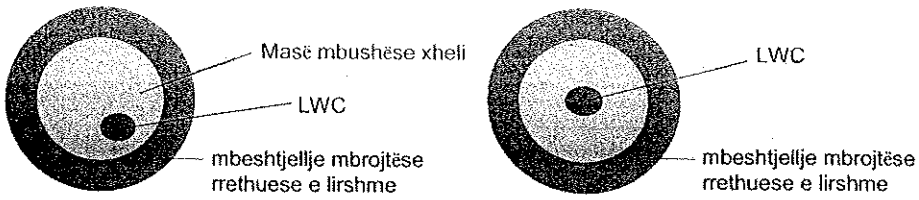
Fibrat fikse përbëhen prej një fibre të vetme, e cila rrethohet nga një mbështjellje fikse. Bazuar në cilësitë që paraqesin fibrat fikse janë më elastike (fleksibël) se fibrat me zemër boshe për shembull. Distanca e vogël midis fibrës së vetme dhe mbështjelljes rrethore i bën fibrat fikse shumë të ndjeshme ndaj ngarkesave mekanike.



Prerje tërthore e një fibre fikse

Fibër me zemër boshe

Fibrat me zemër boshe i gjejmë në dy variante; të mbushura dhe të pambushura. Të mbushurat përbëhen prej një fibre dhe një mbështjelljeje mbrojtëse rrethuese të lirshme. Hapësira ndërmjetëse midis fibrës dhe mbështjellës rrethore është mbushur me xhel të papërshkueshëm nga uji. Përmasat e kësaj fibre janë pak më të mëdha po ajo zotëron karakteristika më të mira përsa i përket qëndrueshmërisë mekanike. Tek varianti i fibrave të pambushura hapësira midis fibrës dhe mbështjellës rrethuese është pa material mbushës.

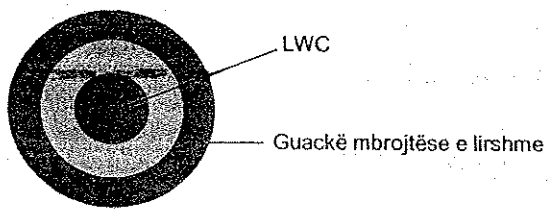


Prerje tërthore e një fibre me zemër boshe me mbushje dhe pa mbushje

Nga të dyja variantet, varianti i parë (i mbushur me xhel) për shkak të karakteristikave të mira mekanike, përdoret më shpesh.

Fibër kompakte

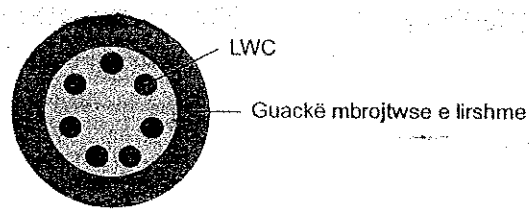
Fibra kompakte, përsa i përket ndërtimit, është një formë e modifikuar e fibrës fikse. Ndryshimi i vetëm me këtë të fundit është një distancë më e vogël midis fibrës dhe veshjes mbrojtëse. Kjo lloj fibre nga ndërtimi është më kompakte se fibra me zemër boshe dhe ka karakteristika mekanike të përmirësuara ndaj fibrës fikse.



Prerje tërthore e një kablli me fibër kompakte

Tufë fibrash

Tek modeli me tufë fibrash, disa fibra rrethohen nga një guaskë mbrojtëse e përbashkët. Hapësira midis fibrave dhe guaskës mbrojtëse mbushet me xhel të papërshkueshëm nga uji. Numri i fibrave në një tufë, si rregull, varion nga 2 deri 12 fibra.



Prerje tërthore e një kablli me tufë fibrash

4.9 Specifikimet e kabllove me fibra optike

Specifikimi sipas DIN VDE 0888

Para përdorimit të kabllove me fibra optike së pari duhen testuar në vend rrethanat e ambjentit ku do të shtrihen kabllot, meqë kabllo me fibra optike ka si për instalime në ambjentet e brendshme, ashtu edhe në ambjentet e jashtme. Kritere të mundshme për zgjedhje janë:

- ☑ Shtrirje në tokë ose në mjedise të jashtme
- ☑ Shtrirje në mjedise me lagështirë dhe të lagura
- ☑ Shtrirje në mjedise të thata dhe të brendshme
- ☑ Shtrirje në tuba dhe vendosje ne panele
- ☑ Shtrirje në mjedise të pambrojtura mekanike
- ☑ Shtrirje me varje të lirë

Në varësi të rrethanave të mjedisit në të cilin ndodhet ndërmarrja, duhet testuar kabli me fibra optike që do të përdoret. Në standardin DIN VDE 0888 do të gjeni sqarime për llojet përkatëse të kabllove.

DIN - VDE 0888, Pjesa 4: kabëll simplex

Position	Kodi i kabllit
1	J = Kabëll i brendshëm
2	V = Fibër fikse e plotë / H = Fibër me zemër boshe, e pambushur / W = Fibër me zemër boshe e mbushur
3	Y = Veshje PVC / H = Veshje prej materiali pa halogjen
4	Numri i fibrave
5	G = Fibër gradient / E = Fibër monomodë
6	Diametri i bërthamës në μm
7	Diametri i veshjes në μm
8	Koeficenti i humbjes në [dB/km]
9	Gjatësia e valëve B = 850 nm / F = 1300 nm / H = 1550 nm
10	Gjerësia e bandës [MHz x km]

Shembull: J-VH 2G50/125

DIN - VDE 0888, Pjesa 5: Kabëllthyerje

Position	Kodi i kabllit
1	AT = Kabëll i jashtëm i ndarë
2	V = Fibër fikse e plotë / W = Fibër me zemër boshe, e mbushur / D = Tufë fibrash të mbushura
3	(ZN) = Elemente çtensionuese jo metalike
4	Veshja e elementëve bazë: Y = veshje PVC / H = Veshje prej materiali pa halogjen
5	Y = Veshje PVC / H = Veshje prej materiali pa halogjen
6	Numri i elementëve bazë (fibra)
7	G = Fibër gradient / E = Fibër njëmodale
8	Diametri i bërthamës në μm
9	Diametri i veshjes në μm
10	Koeficenti i humbjes në [dB/km]
11	Gjerësia e bandës B = 850 nm / F = 1300 nm / H = 1550 nm
12	Gjerësia e bandës [MHz x km]
13	LG = Thurje në gjatësi

Shembull: AT-V(ZN)Y 8G62,5/125

DIN - VDE 0888, Pjesa 3: Kabëll i jashtëm

Pozicioni	Kodi i kabllit
1	A = Kabëll i jashtëm
2	B = fije tufë, e pambushur / D = fijet tufë, e mbushur / W = Fibër me zemër boshe, e mbushur / H = Fibër me zemër boshe, e pambushur
3	S = element metalik në zemrën e kabllit
4	F = Masë mbushëse për mbushjen e hapësirave boshe në zemrën e kabllit
5	2Y = Veshje PE / (L)2Y = Veshje me shtresa / (ZN)2Y = PE-Veshje me ç'tensionim jometalik
6	B2Y = Riforcim me mbështjellje mbrojtëse PE / BY = Riforcim me mbështjellje mbrojtëse PVC
7	Numri i elementëve bazë (fibra)
8	G = Fibër gradient / E = Fibër monomodë
9	Diametri i bërthamës në μm
10	Diametri i veshjes në μm
11	Koeficenti i humbjes në [dB/km]
12	Gjatësia e valëve B = 850 nm / F = 1300 nm / H = 1550 nm
13	Gjerësia e bandës [MHz x km]
14	LG = Thurje në shtresa

Shembull: A - DQ(ZN)B2Y 24G50/125

4.10 Fushat e përdorimit të kabllove me fibra optike

Fushat e përdorimit të kabllove me fibra optike

Bazuar në karakteristikat e mira të transmetimit, kabllot me fibra optike përdoren në rjete ku kërkohet shkëmbimi i sasive të mëdha të të dhënave. Ato shërbejnë si High-End-Backbone për grupe serverash (server farms), ose për lidhjen e ndërtesave të firmave. Për shkak të zvoglimit të kostove të përgjithshme, sot fibrat optike po shtrihen edhe brenda ndërtesave deri në vendin e punës (Fiber-to-the-Desk).

Përdorimi i fibrave multimodë

Fibrat me indeksim me disa nivele për shkak të kohëzgjatjeve shumë të ndryshme të sinjaleve dhe shpërhapjes së fuqishme të impulsit të dritës, janë të papërshtatshme për përdorim praktik për distanca të shkurtra (deri rreth 1 km) dhe gjerësi bandash të ulta (deri 100 MHz).

Fibrat me indeksim me gradient janë përkundrazi të përshtatshme për distanca mesatare (deri rreth 25 km) dhe gjerësi bande deri në 1 GHz, sidomos për lidhjet midis ndërtesave dhe lidhjet e ashtuquajtura Fiber-to-the-Desk-brenda ndërtesave. Për shkak të karakteristikave më të mira optike të fibrave me indeksim me gradientë ato, ndryshe nga fibrat me indeksim me nivele, preferohen edhe për distancat e shkurtra.

Përdorimi i fibrave monomodë

Fibrat monomode janë të përshtatshme për distancat e gjata (WAN) deri në rreth 55 km. Ato paraqesin një produkt gjerësi bande – gjatësi për më shumë se 10 GHz / km.

Kabllot përçuese të valëve të dritës për përdorim industrial

Gjatë përdorimit të këtyre kabllove në industri duhen pasur parasysh disa kritere shtesë. Faktorë, të cilët shfaqen në mjediset industriale, janë:

- ☑ Temperatura
- ☑ Lagështira
- ☑ Pluhuri
- ☑ Vibracionet

Me qëllim që të përmbushen këto kërkesa të larta, cilësitë e kabllove për përdorim zyre u zgjeruan më tej.

Dy variante shtesë janë:

- ☑ **Fibër plastiko optike. Plastic Optical Fiber (POF)**
- ☑ **Silikon me veshje të përforcuar. High Cladded Silicia (HCS)**

Karakteristikat e tyre të veçanta, si qëndrueshmëria e lartë termike dhe qendrueshmëria më e mirë ndaj tensionimeve mekanike, i bëjnë këto lloj kabllosh mjaft të përshtatshme për përdorim në mjediset industriale. Një avantazh tjetër qëndron tek konfeksionimi më i mirë në vend. Këto kabllo, krahas llojeve të tjera të fibrave optike, kanë parametra dukshëm më të lartë përsa i përket humbjeve dhe për këtë arsye mund të përdoren vetëm për transmetimet në distanca të shkurtra.

Përshkrimi	10 MBit/s	100 MBit/s	Fusha e përdorimit
POF	**50 Metra**	**35 Metra**	Automjetet, sistemet audio dhe video, teknikat e automatizimit, qarqet e kompjuterave
HCS	**Deri në 300 Metra**		Sensorët, teknologjinë mjeksore, teknikat e të dhënave industriale

Plastic Optical Fiber (POF)

Fibra POF është një fibër e pastër plastike dhe përbëhet prej një bërthame transparente prej polymethyl-methacrylat-i (PMMA) ose polycarbonat-i (PC). Kjo bërthamë ka një diametër prej 980 μm. Veshja e një fibre POF përbëhet prej polyethylen-i (PE), ose edhe prej polyamid-i (PA). Diametri i bërthamës së një fibre POF është 980 μm.

Silikon me Veshje të Përforcuar (High Cladded Silicia (HCS))

Tek fibra HCS-bërthama përbëhet nga kuarc (SiO_2) dhe ka një diametër prej 50 μm deri në 1000 μm. Veshja e një fibre HCS-përbëhet prej një materiali plastik special. Madhësia tipike për një fibër standard me diametër të vogël bërthame janë 125 μm (bërthama), 140 μm (cladding) dhe 250 μm (veshja mbrojtëse).

4.11 Teknikat e bashkimit të kabllove me fibra optike

Bazat e teknikës së bashkimit të kabllove me fibra optike

Qëllim i teknikës së bashkimit të kabllove optike është që këto të fundit të bashkohen me njëra-tjetrën në mënyrë të pandashme, ose të ndashme. Lidhja e pandashme quhet ndryshe dhe ngjitje optike. Ndërsa kur lidhja është e ndashme, atëhere bëhet fjalë për një lidhje me prizë-kokë bashkuese. Në praktikë kërkohet një mënyrë bashkimi e thjeshtë dhe humbje të vogla fikse. Për shkak të ndjeshmërisë që paraqesin kabllot me fibra optike ndaj papastërtive, pastërtia e lidhjeve të ndashme është shumë e rëndësishme. Elementët lidhës dhe sipërfaqja e fibrave duhen pastruar me kujdes.

Përgatitja

Për krijimin e një lidhjeje me fibra kërkohet kujdes dhe pastërti e lartë. Për krijimin e një lidhjeje me fibra, koha që nevojitet gjatë fazës së parapërgatitjes është periudha e kohës që harxhohet më shumë në totalin e kohës së konsumuar për këtë qëllim. Përgatitja e lidhjes është pothuaj e njëjtë, si tek lidhjet me bashkim ashtu edhe tek lidhjet me koka bashkuese. Meqënëse fibra optike nuk është e zbuluar duhet fillimisht të zhvishet nga mbulesa. Në varësi të ndërtimit të fibrës optike duhet të hiqen shtresat e jashtme. Pasi zbulohet fibra, duhet të arrihet një sipërfaqe e sheshtë duke e gërvishtur dhe thyer fibrën. Kjo sipërfaqe e sheshtë fundore është tregues për cilësinë e lidhjes. Në rast krisjesh, rrumbullakosjesh, parregullsish sipërfaqsore apo këndi të gabuar prerjeje, është e garantuar një lidhje e keqe.

Bashkimet e kabllove me fibra optike

Lidhjet e pandashme të kabllove me fibra optike përdoren kryesisht për lidhjet e përhershme, ose për lidhjet me kabllo lidhëse të parakonfeksionuara (pigtails). Dallojmë llojet e mëposhtme:

- ☑ Bashkim termik
- ☑ Bashkim me ngjitje
- ☑ Bashkim mekanik

Bashkimet me ngjitje përdoren për lidhjet afatgjata dhe duhet të ofrojnë lidhje stabël dhe humbje të vogla.

Bashkimi termik

Gjatë bashkimit termik, fundet e fibrave optike ngjiten me njëra-tjetrën me ndihmën e një aparati ngjitës me hark drite. Gjatë nxehjes, nëpërmjet një motori elektrik me hapa (motor steper), afrohen sipërfaqet ballore të fibrave me kujdes njëra me tjetrën. Tensionet sipërfaqësore gjatë procesit të shkrirjes ndikojnë në krijimin e një efekti vetëqendërzimi tek fibrat. Për shkak të temperaturave të larta, të dyja fundet e fibrave shkrihen në një lidhje, e cila pas këtij procesi bashkimi testohet në tërheqje mekanike. Pas lidhjes së suksesshme të fundeve të fibrave nevojitet mbrojtja e bashkimit nga mbingarkesat mekanike nëpërmjet një mbulese mbrojtëse.

Bashkimi me ngjitje

Gjatë bashkimit me ngjitje, fibra drejtohet në një të çarë, një tub apo një manikote dhe ngjitet. Materiali ngjitës siguron krahas stabilitetit mekanik të lidhjes, edhe përshtatjen e **numrit të thyerjes**. Vlerat tipike të humbjeve variojnë nga 0,1 deri 0,2 dB.

Bashkimi mekanik

Gjatë bashkimit mekanik mbajtësja përkatëse siguron një lidhje fikse dhe me stabilitet afatgjatë. Fundet e fibrave që do të lidhen vendosen në një të çarë në formë V-je dhe bashkohen me kapse. Tek ky lloj bashkimi, në rast lidhjeje të parregullt, mund të shkaktohen humbje të mëdha. Vlerat tipike të humbjeve variojnë nga 0,2 deri 0,5 dB. Për përgatitjen e fibrave monomode vlejnë të njëjtat parakushte si për fibrat multimodë, sidoqoftë kërkesat për fibrat monomodë janë shumë më të larta.

Lidhjet për kabllot me fibra optike

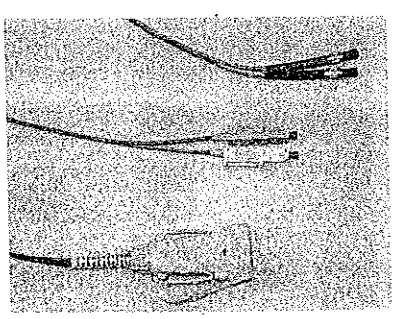
Në lidhjet e kabllove me fibra optike përdoren koka të ndryshme lidhëse. Format e sotme të ndërtimit të tyre janë E-2000, SC, F-SMA dhe ST. Nga këto tipe përdoren para së gjithash tipet SC dhe ST. Kokat e modeleve më të vjetra F-SMA-nuk përdoren më në kabllimet e reja.

Përshkrimi	Kapja/fiksimi	Lidhja	Fusha e përdorimit	Lloji i fibrës
SC	push/pull	Sustë	LAN, Teknikë matjeje	Gradient-Fibër monomodë
ST	Bajonetë	Sustë	LAN, Teknikë matjeje	Gradient- Fibër monomodë
SMA	Bulon	Vidhosje	Automatizim, LAN	Gradient fibër
DIN	Bulon	vidhosje	Teknikë matjeje	Gradient - Fibër monomodë
FC / PC	Bulon	sustë	Teknikë matjeje	Gradient - Fibër monomodë

Lidhjet me koka ST- dhe SC, për shkak të thjeshtësisë që ofrojnë përbëjnë sot lidhjet më të favorizuara. Nëpërmjet lidhjes bajonetë, e cila përdoret tek kokat ST, procesi i lidhjes lehtësohet dhe lidhja nuk shkëputet lehtë për shkak të vibrimeve.

Kabllot lidhëse dhe patchkabllot kanë përparësi për shkak të lidhjes dhe shkëputjes së shpejtë që lejojnë me prizat e rrjetit, apo me portat përkatese të switch-it, hub-it etj.

Një fushë e veçantë përdorimi për lidhjen F-SMA është transmetimi i të dhënave audio. Lidhja ofron një shtrëngim të mirë me vidhosje, e cila nuk shkëputet nga vibrimet e shkaktuara nga sinjali audio bas.

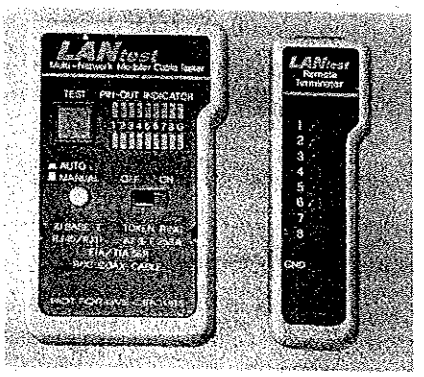


Elementë lidhës fibrash optik

4.12 Zgjedhja e pajisjeve matëse

Testues Mini-LAN-esh

Me anën e një testuesi Mini-LAN mund të kontrollohet nëse janë lidhur në mënyrë të saktë të gjitha Pin-et e një kablli nga patchpaneli deri tek priza e rrjetit. Dërguesi dhe marrësi i testuesit Mini-LAN është pajisur, për çdo Pin të fijeve të veçanta dhe për skermon mbrojtëse, me nga një LED (dritëz) të veçantë. Në rast se p.sh. Pin-i 3 është ndërprerë, për shkak të një dëmtimi të kabllit, atëhere LED-i 3 tek marrësi i Mini-LAN-it nuk ndriçon.



Testues Mini-LAN-esh

Multimetër dixhital

Krahas kontrollit të përshkueshmërisë të kablove prej bakri, me një multimetër dixhital mund të kryhen edhe matje të tensionit dhe të rezistencës. Tek kabllime BNC p.sh. mund të testohet montimi i saktë i kokës së kabllit. Ky testim kryhet duke matur rezistencën midis skermos mbrojtëse prej flete metalike dhe përcjellësit të brendshëm të kabllit. Në rast se rezultati i matjes është zero Ohm, atëhere gjatë montimit të kokës është krijuar një lidhje e shkurtër. Edhe tek kabllot twisted-pair multimetri dixhital gjen mjaft përdorim. Nëpërmjet tij identifikohen shpejt lidhjet e shkurtra midis fijeve përbërëse të kabllit dhe skermos prej flete të hollë metalike, por edhe portat me defekt në prizat e rrjetit dhe në patchpanel.

Pajisje për kërkimin e linjave kabllore

Në kompanitë e mëdha me densitet të lartë kabllosh, pajisja e kontrollit të linjave kabllore është shoqërues i pandashëm. Në rast se mungojnë etiketimet e prizave të rrjetit apo pattchpanelit, me anën e pajisjes për kërkimin e linjave mund të identifikohet shpejt porta që i përket kabllit të dëshiruar. Kjo gjë bëhet pa ndonjë mundim të madh, meqë dërguesi mund të lidhet direkt me prizën e rrjetit apo me patchpanelin. Marrësi dërgon një sinjal zanor, përsa kohë që ai është pranë kabllit përkatës. Patchpanelet dhe prizat e rrjetit nuk duhen hapur.

Pajisje për matjen e kabllit

Me anën e një pajisjeje për matjen e kabllit mund të maten karakteristikat elektrike të tij si kapaciteti, humbjet për shkak të fluksit të kthimit, rezistenca, tensioni etj., si dhe kabllimi i saktë i rrugës së transmetimit. Me anën e një grafiku që paraqitet në ekranin (display) e pajisjes, mund të dallohen menjëherë fijet e lidhura gabim, apo ndërprerjet në tërësinë e kabllit duke mundësuar në këtë mënyrë eliminimin e lehtë të tyre. Para së gjithash, me ndihmën e kësaj pajisjeje mund të identifikohen defekte të kabllit, të cilat nuk dallohen me sy të lirë.

4.13 Eliminimi i lidhjeve të shkurtra

Identifikimi i lidhjes së shkurtër

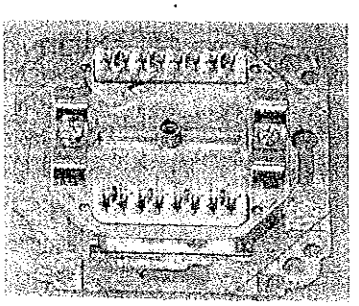
Gjatë kabllimit të ri të një zyre me kabëll të kategorisë 5, protokollohen matjet e kryera në disa prej rrugëkalimeve të kabllove.

Në njërën nga prizat pajisja matëse e kabllit tregon lidhje të shkurtër midis Pin-eve 1,2,3 dhe skermos mbrojtëse

Procedura e veprimit

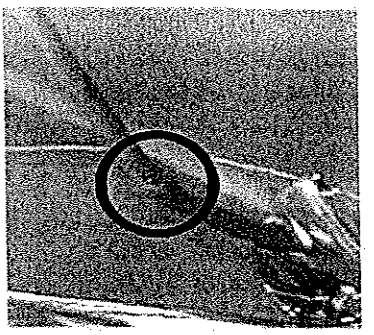
→ Hapni prizën përkatëse të rrjetit dhe patchpanelin, dhe testoni vendosjen korrekte të fijeve në foletë udhëzuese të lidhjes LSA+. A janë vendosur siç duhet fijet e veçanta në foletë udhëzuese të lidhjes LSA+?

→ Mbetje të fijeve α apo fletës mbrojtëse β mund të mblidhen në brendësi të prizës RJ45 dhe mund të shkaktojnë lidhje të shkurtër me elemente te prizës. Për këtë arsye këto mbetje duhen hequr.


Mbetjet e fijeve

⇒ Kontrolloni vendin ku duhet bërë zhveshja e kabllit. Prerjet e thella, me një thikë të mprehtë, mund të shkaktojnë dëmtimin e kabllit, si dhe të izolimit të fijeve të vecanta χ. Edhe kapëset e vendosura pa kujdes, apo më të shtrënguara se duhet, mund të shkaktojnë dëmtimin e izolimit të kabllit.

⇒ Kontrolloni portat RJ45 të prizës së rrjetit dhe patchpanelit. Masni me një testues përshkueshmërie kontaktet e vecanta në foletë RJ45 të lidhjes LSA + -. Mbetje të fijeve apo fletës mbrojtëse mund të mbllidhen në brendësi të prizës RJ45 dhe mund të shkaktojnë lidhje të shkurtër me elemente të prizës. Kjo veçanërisht në shumicën e rasteve, është i vështirë për t'u diagnostikuar. Provoni përmjet goditjeve të lehta, apo tërheqjes që t'i clirgoni këto mbetje.



Izolim fije i dëmtuar

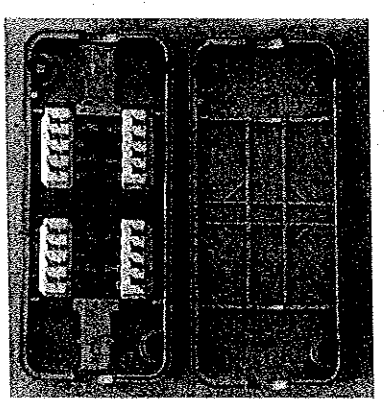
Kontrolloni vijueshmërinë e kabllit të të dhënave

⇒ Kontrolloni rrugën në të cilën kalon kabli i shtruar. A dallohen dëmtime të jashtme të kabllit? A ka kthina të "mprehta" në rrugën ku kalon kabli, para se gjithash tek distancat e gjata, të cilat mund ta kenë dëmtuar kabllin? Në këtë rast dëmtimi, ose jo i kabllit, mund të identifikohet me një multimetër.

⇒ Shkëputeni kabllin nga priza e rrjetit dhe nga patchpaneli dhe masni fijet e vecanta të tij ndaj mbulesës mbrojtëse (testi i përshkueshmërisë).

⇒ A e identifikuan vendin e „thyerjes" (palosjes) së kabllit?

⇒ Në rast se kabli është i dëmtuar, atëherë vendi i dëmtuar mund të shkëputet dhe të riparohet me një lidhës tunel δ. Megjithatë, çdo lidhje e tillë, do të thotë humbje në cilësi, rekomandohet që në këtë segment i gjithë kabli të shtrohet nga e para.



Lidhës tunel

4.14 Zvogëlimi i humbjeve të fluksit të rikthimit

Identifikimi i humbjeve të mëdha si pasojë e fluksit të rikthimit

Gjatë kabllimit të ri të një zyre me kabëll të kategorisë 6, protokollohen matjet e kryera në disa prej rrugëkalimeve të kabllove. Në njërën nga lidhjet pajisja matëse e kabllit tregon humbje të mëdha si pasojë e një fluksi të lartë të rikthimit.

Procedura e veprimit

⇒ Testoni paraprakisht gjendjen e baterive dhe fishave të pajisjes matëse. Kryeni një zerim të aparatit.

⇒ Përsëritni matjen.

⇒ Nëse defekti rishfaqet, kontrolloni gjatësinë e kabllit. Gjatësia maksimale prej 100m nuk duhet kaluar.

⇒ Hapni prizën përkatëse të rrjetit dhe patchpanelin dhe testoni vendosjen korrekte të fijeve në foletë udhëzuese të lidhjes LSA + -.

⇒ Shkaqe të shpeshta për humbje nga fluksi i rikthimit janë thurja dhe mbrojtja difektoze e fijeve përbërëse të kabllit në zonën ku është bërë lidhja. Fleta mbrojtëse dhe thurja e fijeve dyshe duhet të mbahen sa më pranë të jetë e mundur me foletë udhëzuese ne vendlidhjen LSA + -.

⇒ A është përdorur kabëll i cilësisë së lartë?

⇒ A janë vendosur fijet sipas standardit EIA/TIA 586B? Moszbatimi i këtij standardi mund të ndikojë negativisht në transmetimin e sinjalit.

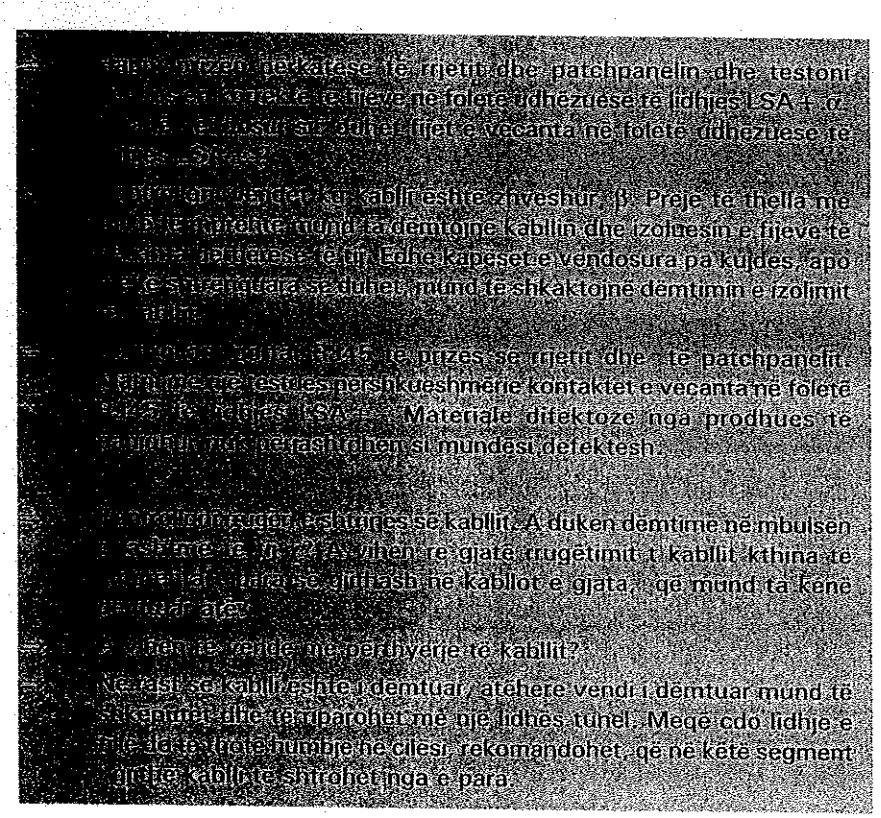
⇒ Tek patchpanelet/prizat modulare për testim duhen ndërruar elementet përbërëse.

4.15 Eliminimi i shkëputjeve tek pin-ët

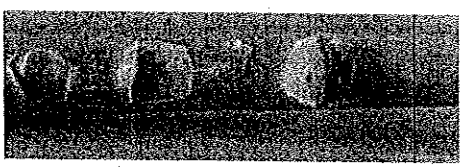
Identifikimi i shkëputjeve

Gjatë kabllimit të ri të një zyre me kabëll të kategorisë 6 lidhjet e veçanta testohen me pajisje matëse dhe rezultatet protokollohen. Gjatë matjes së lidhjeve të fijeve të një prize rrjeti, pajisja matëse e kabllit tregon një ndërprerje tek Pin-i 1.

Procedura e veprimit



Prizë rrjeti e lidhur në mënyrë jo profesionale



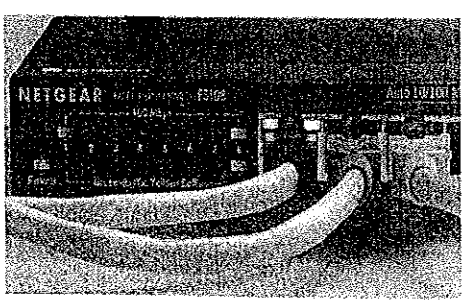
Veshje e dëmtuar e kabllit

4.16 Rivendosja e lidhjeve difektoze në rrjet

Kryerja e testimit të lidhjës

Në një firmë me një rrjet të kategorisë 5, 100-Mbit, përdoruesi nuk mund të identifikohet më në rrjet.

Procedura e veprimit



Treguesi i lidhjes (link LED) në një pajisje switch

→ A gjendet aty pranë një prizë tjetër rrjeti? Ne rast se po, lidheni kompjuterin me këtë prizë. Mos harroni, që duhet kontrolluar që kjo prizë të jetë e lidhur në HUB. A ndriçon LED-i i kartës së rrjetit?

→ Në qoftë se po, kontrolloni lidhjen me një testues Mini LAN. Nëse identifikohen ndërprerje procedoni si në shembullin 4.

→ Në qoftë se LED-i nuk ndriçon duke treguar linkun, ndërroni kartën e rrjetit.

→ Si mundesi e fundit defekti mbetet Hub-i. Përdorni një porte tjetër të tij. Në rast se prova nuk del me sukses, ndërroni Hub-in.

4.17 Burimet më të shpeshta të defekteve

Defektet dhe zgjidhjet

Përshkrimi i defektit	Zgjidhja e mundshme
Vendosje e gabuar e madhësisë së fijeve	Kontrolloni mbulimet e Pin-eve në prizat e rrjetit dhe në patchpanel, dhe kryeni korrigjimet përkatëse kur lind nevoja sipas EIA/TIA 586B
Lidhje e shtrirë nuds dy apo më shumë fijeve	Kontrolloni për mbetje fijesh kablli tek lidhjet LSA+- në prizën e rrjetit dhe në patchpanel Kontrolloni veshjen e kabllit për prerje (çarje), apo vende ku kablli tensionohet Kontrolloni për dëmtime në vendet, ku është shtrirë kablli
Ndërprerje tek një ose disa fije (e kabllit)	Hapni prizën përkatëse të rrjetit dhe patchpanelin dhe testoni vendosjen korrekte të fijeve në foletë udhëzuese të lidhjes LSA+-.α. Matni me testues përshkueshmërie kontaktet e lidhjes LSA+-
Humbje e madhe si pasojë e ndikimit të kthimit	Kabëll shumë i gjatë (maksimumi është 100 m) Fleta mbrojtëse e kabllit STP dhe thurja e cifteve të përdredhura duhet mbajtur sa më afër që të jetë e mundur lidhjeve të prizës LSA+- apo të kokës së kabllit. Ndërimi i elementëve me defekt tek sistemet modulare Mosrespektimi i kodit të ngjyrave sipas EIA/TIA 586B
LED-i i kartës së rrjetit nuk tregon lidhje (nuk ndriçon)	Patchkabëll me defekt Kartë rrjeti me defekt HUB me defekt Kontrolloni lidhjen me testues Mini-LAN-esh

5 Përbërësit aktivë të rrjetit

Në këtë kapitull do të lexoni

- → cilët përbërës aktivë të rrjetit ekzistojnë
- → cilët nga këto përbërës ka kuptim të përdoren nga kompania
- → ku mund të përdoren pajisje të caktuara
- → cilat pajisje mund të përdoren për kërkim të thjeshtë të defektit
- → si mund ta rivendosni përsëri në punë një lidhje të ndërprerë në rrjet

Kusht paraprak

- ✓ Njohuri mbi modelin referues ISO/OSI
- ✓ Njohuri mbi topologjitë e rrjeteve
- ✓ Njohuri mbi ndërtimin e kabllove të transmetimit të të dhënave

5.1 Përbërësit aktivë të rrjetit orientuar sipas modelit ISO/OSI

Njohuri bazë mbi përbërësit aktivë të rrjetit

Përbërësit aktivë të rrjetit shërbejnë për të lidhur rrjetet kompjuterike me njëri-tjetrin, ose për të kapërcyer kufizimet në gjatësi të së mediave lidhëse. Pjesërisht, ato kontribuojnë në lidhjen e rrjeteve që përdorin media transmetimi, protokolle, apo shpejtësi transmetimi të ndryshme.

Nëpërmjet përdorimit të saktë të përbërësve aktivë të rrjetit, mund të rritet fluksi i transmetimit të të dhënave në rrjet.

Referuar modelit ISO/OSI, përbërësve aktivë u caktohen shtresat përkatëse në të cilat ato punojnë. Tabela e mëposhtme tregon, shtresën në të cilën renditet pajisja respektive:

Shtresa e OSI	Përbërësi	Shënime
4 - 7	Gateway, Layer-7-Switch	Paketa e plotë e transformuar e të dhënave
3	Router, Layer-3-Switch	Punon në nivel protokolli
2	Bridge, Switch	Punon ne nivel MAC-u
1	Hub, Repeater, Media Converter	Rigjenerim sinjali, transformim sinjali

5.2 Hub-i

Mënyra e funksionimit

Një Hub shpesh përshkruhet si përqëndrues kabllosh, ose si shpërndarës yll, pasi ai përdoret si qendra e një rrjeti. Hub-et përdoren kryesisht kur ndërtohen rrjete logjike. Hub-et janë në gjendje të lidhin me njëri-tjetrin topologji të ndryshme rrjeti.

Hub-i punon në shtresën 1, referuar modelit OSI (Physical Layer – Shtresa Fizike). Në Hub sinjali vetëm rigjenerohet dhe dërgohet më tej tek të gjithë kompjuterat e lidhura me të.
Çdo transport të dhënash në rrjet përçohet në të gjitha portat. Parimisht Hub-et janë të ndërtuara në mënyrë të ngjashme me topologjinë bus, në të cilën e gjithë gjerësia e bandës ndahet midis pjesmarrësve të lidhur në rrjet.

Në një rrjet 10-Mbit-sh me 10 pjesmarrës, çdo pjesmarrësi i takon një gjerësi bande teorike prej 1Mbit, dhe nëse bëhen 20 pjeswmarrës në të njëjtin segment, do të kemi 0,5 Mbit për pjesmarrës.

Përplasjet e vazhdueshme të paketave me të dhëna janë të pashmangshme. Si pasojë, koha e pritjes gjatë së cilës ndodh shkëmbimi i të dhënave në rrjet rritet.

Hub-et, sipas fushës së përdorimit, ndahen në hub-e të nivelit të grupeve të punës, (workgroups), nivel kati /sektori (departmental) dhe nivel ndërmarrjeje (enterprise).

Hub-et për grupe pune (workgroup-hubs) përdoren për grupet e vogla të punës me pak pjesëmarrës (përdorues). Workgroup-Hubs përdoren kryesisht për lidhjen në rrjet të PC-ve dhe pajisjeve të tjera që janë në gjendje të punojnë në rrjet (printera) dhe përmblidhen në një grup pune. Në shumicën e rasteve ekziston një lidhje (Up-Link) midis kateve, ose e shprehur ndryshe e Hub-eve në nivel ndërmarrjeje.

Një shpërndarës Ethernet në formë ylli me 24 porta është shembulli tipik për një Hub kati.

Hub-et në nivel ndërmarrjeje formojnë kolonën vertebrore të strukturës së informacionit në një ndërmarrje. Bazuar në mënyrën e tyre modulare të ndërtimit, këto Hub-e janë në gjendje , të lidhin mes tyre topologji të ndryshme rrjeti. P.sh. me një Hub qendror në nivel ndërmarrjeje mundet të lidhen me njëri-tjetrin lloje të ndryshme rrjetesh si: Token Ring, Ethernet, Fast Ethernet dhe FDDI.

Hub-et modulare punojnë gjerësisht me sisteme bus-i të brendshme, specifike sipas prodhuesit (Backplane). Kapaciteti përcaktohet nëpërmjet procesit të aksesimit të Bus-it të brendshëm, p. sh. Token ose CSMA/CD.

Fushat e përdorimit

Para futjes në përdorim të Hub-eve në kompaninë tuaj duhet të qartësohet qëllimi i përdorimit dhe investimi për të ardhmen.

Gjatë planifikimit të blerjeve të reja duhet pasur parasysh të përdoret teknologjia switching, meqë këto pajisje nuk janë më të shtrenjta se Hub-et dhe për më tepër ofrojnë fluks transmetimi të dhënash më të lartë për shkak të parandalimit të përplasjeve - kollisionit (CSMA/CD) dhe Full-Duplex-Modus-it që ata përdorin gjatë transmetimit. Kur zgjidhet një prodhues, përveç kësaj duhet të kemi parasysh gjendjen e stokut të pajisjeve (moduleve) përkatëse.

Raste në të cilat mund të përdoret një HUB janë:

- ☑ Në rastin kur duhen lidhur 4 deri në 8 stacione pune për një periudhë të shkurtër (p. sh. provizorisht gjatë rinovimit të zyrës)
- ☑ Në rastin kur duhet lidhur grupi i punës, i cili punon në një segment me topologji bus (lidhje BNC) me grupin e punës që punon me topologjinë yll (star)
- ☑ Në rast se ngrihet një rrjet për qëllime demonstrimi

Variantet

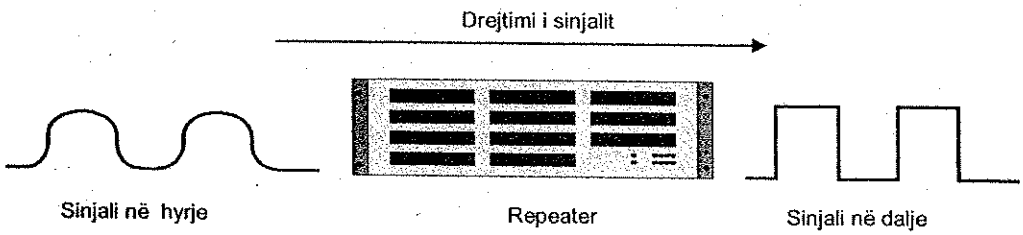
Hub-et në nivel grupi pune dhe sektori ekzistojnë në variante të ndryshme.Treguesi më dallues i tyre është numri i portave. Hub-et e grupeve të punës ofrojnë 4 deri në 8 mundësi lidhjeje. Hub-et e sektorëve janë me 8, 12 dhe 24 porta. Tregues të tjerë të rëndësishëm janë:

- ☑ Porta me 10 Mbit ose 100 Mbit
- ☑ Porta me 10 Mbit dhe 100 Mbit me identifikim automatik të shpejtësisë së komunikimit (autosensing)
- ☑ Hub kaskadë ose/edhe stackable
- ☑ Hub me mundësi zgjerimi të përbërësve (extention slot) (për fibër optik ose Up-Link)
- ☑ Hub me mundësi për segmentim
- ☑ Hub me portë BNC të integruar ose jo

5.3 Repeater-i (rigjeneruesi i sinjalit)

Mënyra e funksionimit

Meqë sinjalet elektrike, në varësi të veçorive të linjës së transmetimit, dobësohen në intensitet, shpesh del i nevojshëm rigjenerimi i tyre. Me ndihmën e repeaters-ave bëhet i mundur rrigjenerimi i plotë i rrjedhës së sinjalit të transmetimit. Për këtë, repeater-i, merr sinjalin e dërguar, e rigjeneron dhe e dërgon tek marrësi. Repeater-i punon totalisht transparent ndaj protokolleve dhe përdoret për kapërcimin e kufizimeve që shkaktojnë distancat e gjata në segmente të veçanta të kabllit.



Rigjenerimi i sinjalit përmes një repeater-i

Veçoritë rigjeneruese të repeaters-ave kanë përparësi, pasi sinjalet difektoze nuk i përçojnë tek segmenti tjetër. Në këtë mënyrë, me përdorimin e tyre, bëhet i mundur lokalizimi i defekteve në një zonë të caktuar të segmentit.

Forma të veçanta

Ekzistojnë forma të ndryshme rigjeneruesish:

- ☑ Remote Repeater
- ☑ Multiport Repeater
- ☑ Optical Repeater
- ☑ Buffered Repeater

Remote Repeater

Tek Remote Repeaters (rigjeneruesit për distanca të largëta) dy repeatera lidhen me njëri-tjetrin me kabëll me fibra optike, me qëllim që të kapërcehet një distancë më e madhe.

Multiport Repeater

Multiport Repeater-at (rigjeneruesit me shumë porta), siç e tregon edhe emri, kanë shumë porta. Kjo bën të mundur që të lidhen me njëri-tjetrin më shumë se dy segmente.

Optical Repeater

Optical repeater-at (rigjeneruesit optikë) përdoren për të balancuar humbjet dhe dobësimin e sinjaleve të dritës. Në distanca shumë të gjata, veçanërisht tek fibrat monomode, sinjali përforcohet dhe rigjenerohet, në intervale të caktuara, nga rigjeneruesit optikë. Rigjeneruesit optikë kryejnë të njëjtin funksion si ata tradicionalë. Dallimi i vetëm është, se rigjeneruesit optikë përdoren vetëm në rrjetet me fibra optike. Ndryshimi thelbësor me rigjeneruesit tradicionalë qëndron në faktin se rigjeneruesit optikë marrin sinjale drite, i transformojnë këto në sinjale elektrike dhe në fund sërish në sinjale optike për t'i përçuar tek marrësi.

Buffered Repeater

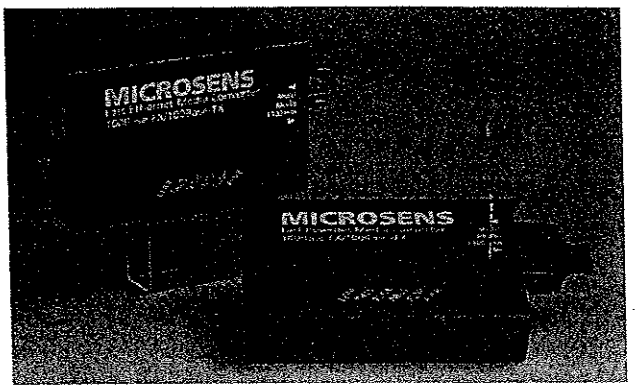
Një buffered repeater punon në shtresën e dytë të modelit OSI. Ndryshe nga rigjeneruesit standard, një buffered repeater merr vetëm paketat e plota me të dhëna. Buffered repeater-at punojnë në bazë të parimit store-and-forward (magazino dhe kaloje më tej). Në të njëjtën kohë, të dhënat e marra ruhen në një memorje ndërmjetëse, përpara se të përçohen më tej në rrjet për tek marrësi.

Rigjeneruesit janë të nevojshëm para së gjithash, atje ku kërkohet shtrirje e distancave të transmetimit. Ato shërbejnë për zgjatjen e distancave që mbulohen me fibra optike, shtrirjen më tej të një segmenti BNC, ose për përpunimin e sinjaleve, të cilat si rezultat i cilësive jo të mira të përcjellësit, nuk mund të dekodohen më tek marrësi.

5.4 Konvertuesit e mediave

Mënyra e funksionimit

Konvertuesit e mediave lidhin me njëri-tjetrin dy lloje të ndryshme kabllosh. P.sh. mund të lidhet kablli koaksial me kabllin twisted pair, ose me fibra optike. Një konvertues mediash ka dy ndërfaqe që varen nga standardi i kabllit, që do të përdoret në rrjetet lokale. Konvertuesit e mediave përdoren shpesh edhe për të kapërcyer kufizimet në distanca të mediave. P.sh. konvertuesi (twisted pair në fibra optike) mund të përdoret, nëse dëshironi të lidhni në rrjet një stacion pune të shkëputur në distancë.



Pamje e konvertuesve të mediave me bashkues LWC

Konvertuesit e mediave transformojnë sinjalet elektrike të një medie në sinjale përkatëse të një medie tjetër. Për këtë konvertuesit e mediave zotërojnë ndërfaqet me elementët përkatës, të cilat nevojiten për gjeometrinë e kabllit. Në rast të transformimit p.sh. nga kabëll bakri në fibra optike, sinjalet elektrike, nga dërguesi, transformohen në sinjale optike dhe tek marrësi sinjalet optike transformohen sërish në sinjale elektrike. Konvertuesit e mediave janë transparentë ndaj protokolleve të komunikimit dhe punojnë në shtresën fizike (physical layer) sipas modelit OSI.

Gjatë përdorimit të konvertuesve të mediave duhet patur parasysh sa më poshtë:

- ☑ Konvertimi është gjithmonë i mundur vetëm midis dy mediave (BNC në TP, BNC në LWC, TP në LWC).
- ☑ Konvertuesit e mediave nuk mbështesin autosensing - negocimin automatik të shpejtësisë së transmetimit (konvertimi ndodh vetën nga 10 Mbit në 10 Mbit ose 100 Mbit në 100 Mbit).
- ☑ Konvertuesit e mediave i kanë fikse të sintonizuara drejtimet e transmetimit (half duplex ose full duplex).
- ☑ Tek konvertuesit e medias për fibra optike ndërfaqja e lidhjes (ST, SC) duhet përcaktuar më parë.
- ☑ Konvertues të ndryshëm mediash kanë edhe një cross-over-port në anën TP.
- ☑ Është i mundur konvertimi i fibrës multimode në singlemode.

Shënime

Variantet

Konvertuesit e mediave disponohen në variante të ndryshme:

- ☑ Për instalime në kanelina, ose në dysheme (installation hub)☑
- ☑ Për instalime në module 19" (korniza modulesh)
- ☑ Për konvertues ethernet-i 19"

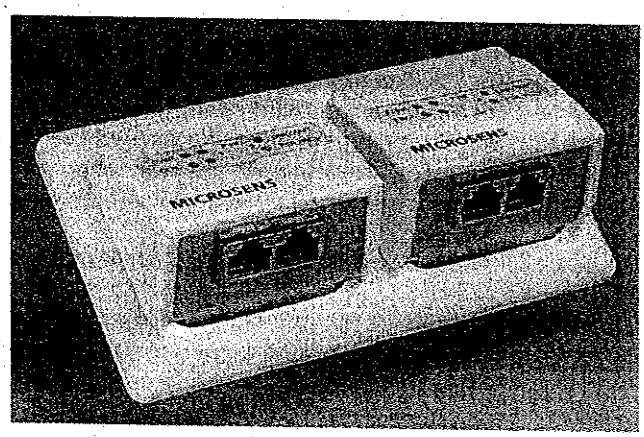
Instalimi në kanelina

Përdorimi i konvertuesve të medias gjatë instalimit ë kanelinave mundëson implementimin, thjesht dhe me kosto të leverdisshme, të koncepteve fiber-to-the-office. Me këto pajisje është e mundur, të arrihet lidhja e deri katër pajisjeve fundore nëpërmjet një bashkuesi shielded-twisted-pair (STP) tek pajisja qendrore, ku lidhen fibrat optike dhe kabllot. Furnizimi me rrymë, i këtij të ashtuquajturi "installation hub", kryhet nëpërmjet një sistemi ushqimi të integruar 230-V. Installation hubs disponohen për 10 Mbit ose për 100 Mbit. Lidhja përmes fibrave optike është e mundur për multimode (50 μm, 62,5 μm), ose për singlemode (9 μm).

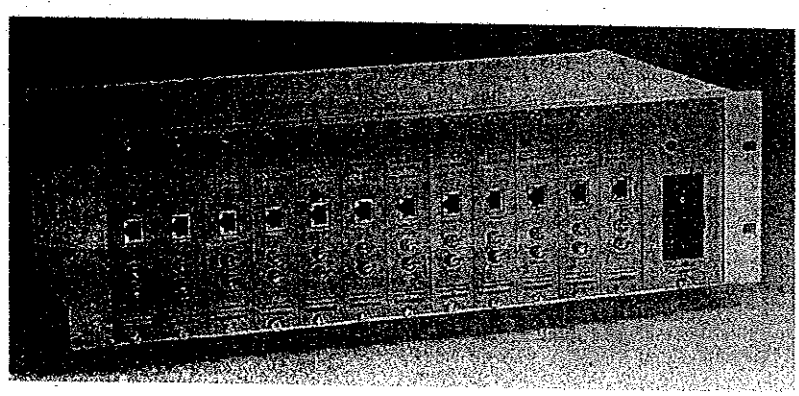
Montimi i sitemeve modulare19"

Në pajisjet qendrore të përpunimit të të dhënave del shpesh e nevojshme kërkesa për konvertimin e bashkuesve ekzistues në media të tjera. Me qëllim që të shmanget përdorimi i një numri të madh pajisjesh të veçanta (stand-alone) për konvertim, ekzistojnë të ashtuquajturat sisteme modulare 19". Këto sisteme modulare montohen pa problem në shpërndarës (rack) dhe u përshtaten me elasticitet kërkesave të vëna. Furnizimi i tyre me rrymë kryhet nëpërmjet një sistemi qëndror ushqimi, i cili mund të jetë edhe redundant (pajisur me sistem ushqimi rezervë).

Konvertuesit e medias janë në formën e kartave modulare 19". Në një sistem modular 19" mund të montohen deri në 12 karta konvertuese. Tek kartat konvertuese gjenden ndërfaqe të ndryshme konvertimi.



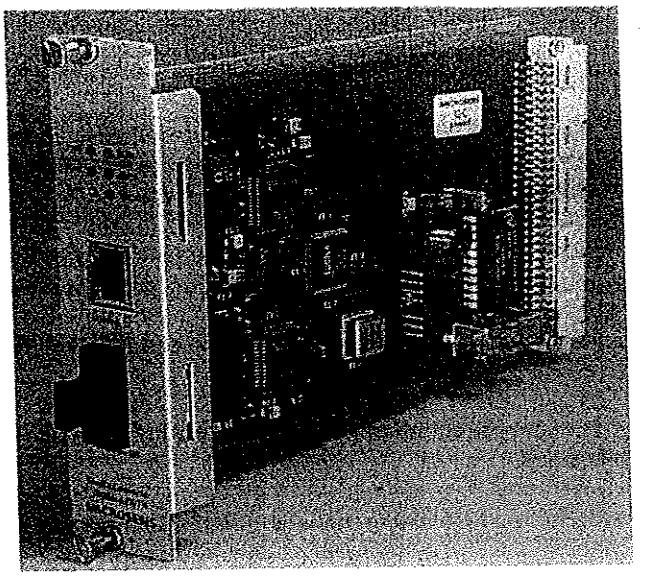
Hub prizash rrjeti për Ethernet të montuara në kanelinë (Installation's hub)



Sistem modular konvertues mediash 19" i pajisur me karta modulare

Në praktikën e punës ndeshen kartat e mëposhtme:

- ☑ Modul rrjeti 230-V
- ☑ Konvertues 10Base-FL në 10Base-T
- ☑ Konvertues 100Base-FX në 100Base-TX
- ☑ 10Base-FL në 10Base2
- ☑ 10Base-T në 10Base-2
- ☑ Token Ring në LWC
- ☑ LWL në modul Token Ring MAU
- ☑ RS-232 në LWC
- ☑ Konvertues mediash Multimode në Monomode
- ☑ Modul konvertues redundant (me elemente rezervë) LWC (1x100Base-TX në 2x100Base-FX)
- ☑ Modul konvertues redundant CU (2x100Base-TX në 1x100Base-FX)



Kartë modulare për sistem modular konvertimi mediash

Kartat modulare redundante (me elementë rezervë) janë konceptuar në mënyrë të tillë, që në rast defekti në njërën linjë, transmetimi i sinjalit transferohet në linjën tjetër. Aplikime të tilla janë veçanërisht të përshtatshme p.sh. për linja të sigurimit të të dhënave (back-up-i) për servera, ose switche.

Përdorni në kompaninë tuaj sisteme modulare 19", me qëllim që të kurseni vend në rack, si dhe të zotëroni një pamje të përgjithshme më të mirë tek ky i fundit. Sistemet modulare 19" janë më të shtrenja se pajisjet stand-alone, por ato kanë nevojë për më pak vend dhe më pak lidhje për furnizim me rrymë (çdo konvertues mediash ka nevojë për një lidhje 230V), kur vendosen në shpërndarës (rack).

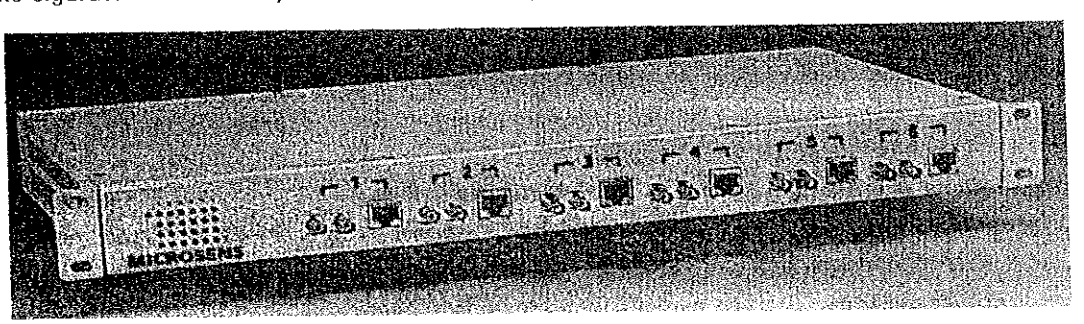
Konvertues etherneti 19"

Këta konvertues janë të ndërtuar në formë 19" me një lartësi 1 HU (High Unit ose Rack Unit). Karakteristika më e spikatur e këtyre konvertuesve, e cila i bën ata shumë të përdorshëm, është konvertimi me kosto të ulët i disa portave twisted pair në fibra optike. Përparësi e konvertuesve Ethernet 19" është, që ato lidhen fiks në një mbajtëse 19". Furnizimi me rrymë kryhet nëpërmjet një ushqyesi të integruar 230 V. Ethernet-Hubs 19"- i gjejmë në variantet me 6 ose me 12 porta.

- ☑ Konvertues mediash me 12 porta - nga 10Base-T në 10Base-FL
- ☑ Konvertues mediash me 6 porta – nga 100Base-TX në 100Base-FX
- ☑ Konvertues mediash me 12 porta – nga 100Base-TX në 100Base-FX
- ☑ Konvertues me 12 porta – nga 10Base-FL në një uplink 10Base-T

Konvertuesi me 12 porta 10Base-FL me një uplink 10Base-T, mundëson çiftimin e 12 segmenteve me fibra optike në një rrjet etherneti. Përmes uplink-ut shtesë 10BaseT mund të realizohet një lidhje me hub-e apo switch-e të tjera.

Forma e rrafshët (flat) e hub-eve 19" të ethernetit lejon vendosjen e disave syreshve në një pajisje mbajtëse shpërndarëse (rack), duke siguruar në këtë mënyrë dendësi të madhe portash.



Konvertues ethernet-i 19" me porta fikse

5.5 Switch-i

Mënyra e funksionimit

Me qëllim që të mund të përdoren me sukses, aplikacionet kritike kërkojnë gjerësi bande të konsiderueshme. Tek rrjetet që përdorin p.sh. Hub-e 10-Mbit- ose 100-Mbit, kjo kërkesë nuk plotësohet gjithmonë. Duke marrë shkas nga ky fakt u zhvilluan të ashtuquajturat switch-e.

Switchet punojnë në shtresën 2 (Data Link Layer) të modelit OSI. Switchi memorizon adresat MAC 48 Bit të gjata të kompjuterave të lidhura në të dhe të portave përkatëse në SAT (Source-Address-Table). Në këtë mënyrë sigurohet, që paketa e rrjetit (ndryshe nga Hub-i) transferohet vetëm tek porta e switchit, në të cilën është lidhur kompjuteri me adresën përkatëse. Në rast se adresa e destinacionit nuk gjendet në SAT, atëhere switchi e përçon më tej paketën tek të gjitha pajisjet e lidhura në rrjet.

Switchet prodhohen me 4 deri 48 porta dhe janë në gjendje, që të lidhin disa porta të pavarura nga njëra-tjetra (non-blocking).

Switchet elektronike, parimisht janë të ndërtuar në mënyrë të ngjashme si switchet mekanike, pra e gjithë gjerësia e bandës i kalohet përdoruesit respektiv të sapolidhur.

Në një rrjet me gjerësi bande 10 Mbit dhe 10 përdorues të lidhur në rrjet, çdo kompjuter ka në dispozicion një gjerësi bande prej 10 Mbit. Në qoftë se p.sh. në çdo portë switchi lidhet një workgroup-hub me 4 porta dhe si rrjedhim në të 10 portat e switchit operojnë gjithësej 40 stacione pune, atëhere çdo grup pune (workgroup) merr një gjerësi bande të dedikuar prej 10 Mbit. Tek një portë switchi 100 Mbit janë pra 100 Mbit për grup pune. Nëse në një nga portat 100 Mbit të switchit lidhet një kompjuter i vetëm, atëhere ky kompjuter ka në dispozicion të gjithë bandën.

Duke marrë parasysh çmimet e leverdishme, switchet nuk shërbejnë më për segmentimin e rrjeteve që përdorin Hub-e. Gjithmonë e më tepër switchet po provojnë se mund të lidhin shumë mirë, direkt me njëri-tjetrin në rrjet, routera, servera dhe kompjutera.

Fushat e përdorimit

Switchet mund të përdoren në kompaninë tuaj në fushat e mëposhtme:

Nëse dëshironi	
☑ të sillni informacionet e aplikacioneve intensive, që kërkojnë gjerësi bande të madhe, deri tek kompjuterat e përdoruesve	
☑ të segmentoni një rrjet me arkitekturë Hub-i	
☑ të zvogëloni kufizimet e rrjetit	
☑ të ndërtoni një lidhje backbone për lidhje serverash	Atëhere duhet të kaloni në Switching-Technology

Për kompaninë do t'ia vlente në çdo rast kalimi nga një sistem i bazuar ne Hub-e në një të bazuar në switche. Nëpërmjet pajisjeve si switchet, përmbushen kerkesat për performancë në rrjet të kompjuterave të sotëm. Aplikacionet e bazuara në rrjet punojnë dukshëm më mirë dhe transferimi i të dhënave bëhet dukshëm më shpejt. Në rast se në kompaninë tuaj lind nevoja për zgjerim apo për ngritjen e një infrastrukture të re, atëhere për këtë qëllim, si pajisje komunikimi në LAN duhen përdorur switchet.

Migrimi në teknologjinë switching

Në rast se dukuritë e mëposhtme vihen re në rrjetin tuaj, atëhere duhet marrë parasysh kalimi në teknologjinë switching:

- ☑ Transferimi i të dhënave është tepër i ngadaltë.
- ☑ Përdorimi në rritje i Internetit ngadalëson në kohë përgjigjet e rrjetit.
- ☑ Gjatë egzekutimit të aplikacioneve në rrjet ka vonesa të dukshme deri në ndërtimin e figurës së plotë.
- ☑ Printimet në rrjet vonohen gjithnjë e më tepër.
- ☑ Përdoruesit nuk identifikohen dot ose identifikohen me vonesë në rrjet.
- ☑ Transferimi i skedarëve të mëdhenj bllokon aksesin në rrjet.

Kriteret që duhen patur parasysh gjatë blerjes

Në qoftë se do të blini një switch, duhen marrë parasysh faktorët e mëposhtëm:

- ☑ Numri i portave
- ☑ I menaxhueshëm ose jo
- ☑ Standalone Switch
- ☑ Half-duplex- dhe/ose Full-duplex
- ☑ 10 Mbit Switch ose 10/100 Mbit Switch
- ☑ Layer-2- ose Layer-3-Switch
- ☑ Mundëson VLAN
- ☑ Kryen agregim portash

Switchet e menaxhueshme

Switchet e menaxhueshme mundësojnë kontroll në distancë mbi rrjet. Për këtë qëllim switch-it i caktohet një adresë IP-je, nëpërmjet të cilës ai mund komunikojë direkt. Pajisja mund të aksesohet me një instrument software-i të përshtatshëm, si p.sh. Telnet. Nëpërmjet SNMP-së (Simple Network Management Protocol) mund të kryhet mbikqyrja dhe nxjerrja e statistikave të rrjetit.

Switchet e menaxhueshme duhen përdorur në rrjetet e mëdha, në të cilat gjejnë përdorim edhe pajisje të tjera të menaxhueshme.

Switchet e pa menaxhueshme

Switchet e pamenaxhueshme kanë çmime të leverdisshme. Ato janë veçanërisht të përshtatshme për zyra, ose biznese të vogla.

Shënime

Portat e shpejtësive të larta (Highspeed Ports)

Tek shumica e switcheve ekziston mundësia e instalimit të një moduli të shpejtësisë së lartë (highspeed module). Me një LWC-Backbone midis switcheve rritet dukshëm largësia dhe shpejtësia e transmetimit. Në këto raste mund të instalohen module të përshtatshme për switchin me 100-Mbit-, ose edhe 1Gbit.

Ka module 100-Mbit-she si Single Port, pra me një vend lidhjeje, ose si Dual Port për dy vendlidhje LWL. Modulet Gigabit-she (GBIC) dallohen në 1000Base-SX-GBIC- dhe 1000Base-LX-GBIC. Modulet 1000Base-SX-GBIC, fibër multimode, janë menduar të përdoren për mbulimin e distancave prej rreth 500 metrash. Modulet 1000Base-LX-GBIC nga ana tjetër janë menduar për përdorim për fibrat monomode dhe mbulojnë një distancë prej deri në 3 kilometra.

Agregimi i portave (Port Aggregation)

Me këtë karakteristikë të switcheve bëhet i mundur bashkimi në një kanal logjik i disa portave të tyre. Nëpërmjet kësaj, mundet p.sh. të rritet fluksi i transmetimit të të dhënave gjatë një lidhjeje backbone midis switcheve. Me ndihmën e kësaj mundësie të krijuar, në disa raste, mund të kursehet lidhja LWC-Backbone. Mundësitë e agregimit të portave përdoren gjerësisht për lidhjet switch-to-switch- ose për lidhje të shpejtësive të larta **Server to Switch. Sidoqoftë, duhet treguar kujdes, që gjatë agregimit të portave maksimumi 4 porta mund të lidhen së bashku në një njësi. Në këtë mënyrë mundësohet një gjerësi bande deri në 800 Mbps (fullduplex) midis pajisjeve të lidhura.**

Funksioni VLAN (Virtual LAN)

Nëpërmjet LAN-eve virtuale (VLAN) stacionet e punës, të ndara fizikisht, bashkohen në një segment rrjeti logjik. Këto grupe logjike formojnë një të ashtuquajtur rrjet brenda rrjetit. Të gjitha paketat dërgohen vetëm brenda këtij segmenti logjik. Broadcastet në një VLAN nuk transmetohen më në të gjithë LAN-in. Në këtë mënyrë ngarkesa në rrjet bie.

5.6 Bridge-t (Urat)

Mënyra e funksionimit

Me ndihmën e urave (bridges) krijohet mundësia e zgjerimit më tej e kufijve të një rrjeti, respektivisht të numrit të kompjuterave në rrjet dhe gjatësisë fizike të lejueshme të tij. Nëpërmjet çiftimit të një rrjeti me anë të një ure, rrjeti ndahet në dy nënrrjete (subnets). Në bazë të nëndarjes më tej të rrjeteve krijohet mundësia, që në subnetet respektive, të rritet sërish në maksimum numri i stacioneve të lejuara pë punës. Një përparësi tjetër e kësaj nëndarjeje është që, kufizimi gjatësor në një subnet të tillë rikthehet në atë që i lejohet zgjerimit bazë të një rrjeti. Meqë paketat me të dhëna të urës, të cilat i takojnë rrjetit të vet, nuk transferohen më tej, atëhere ngarkesa lokale e rrjetit zvoglohet ndjeshëm. Edhe paketat me probleme nuk kalohen më tej në subnetet fqinjë.

Ura lexon paraprakisht kokën (header-in) e paketës dhe më pas krahason informacionet e adresës së burimit dhe destinacionit në një tabelë adresash. Këto tabela janë vende memorizimi me kohë aksesi të përcaktuar që shkon rreth 3 ns. Në rast se adresa përkatëse gjendet në tabelë, atëhere paketa dërgohet më tej tek kjo adresë. Në rast se adresa nuk gjendet në tabelën e adresave, atëhere dërguesi dhe marrësi i paketës me të dhëna gjenden në të njëjtin subnet. Me ndihmën e këtij funksioni filtrimi rrjetet mund të segmentohen më tej dhe dërgimi i broadcast-eve të kufizohet.

Për krijimin dhe mbarëvajtjen e këtyre tabelave të adresave ekzistojnë dy mundësi bazë:

- ☑ Tabela adresash statike
- ☑ Tabela adresash dinamike

Tek urat me tabela adresash statike, adresat parakonfigurohen nga administratori dhe të dhënat e hedhura nuk ndryshohen më gjatë punës. Bridget me tabela adresash dinamike i ndërtojnë automatikisht tabelat e adresave dhe i plotësojnë gjatë punës d.m.th. heqja, apo shtimi i një stacioni pune në subnetin përkatës fshin, apo shton një adresë të dhënë në tabelën e adresave.

Një tregues i rëndësishëm i urave është se ato krijojnë çiftim transparent ndaj protokolleve në rrjet të shtresave të larta. Kjo, për rastin e aplikacioneve do të thotë, që të gjitha protokollet e tjera përçohen transparent nga ura. Urat punojnë në shtresën 2 të modelit OSI.

Variantet

Sipas fushës së përdorimit urat ndahen në:

- ☑ Ura lokale (local bridge)
- ☑ Ura në largësi (remote bridge)
- ☑ Ura shumëportëshe (multiport bridge)

Ndërsa urat lokale lidhin me njëri-tjetrin vetëm rrjete të të njëjtit tip, urat në largësi mund të çiftojnë dy rrjete nëpërmjet një lidhje WAN-i.

Në ndryshim nga dy të parat, urat shumëportëshe janë në gjendje të lidhin rrjete të llojeve të ndryshme.

5.7 Router-i

Mënyra e funksionimit

Routerat janë përbërës aktiv të rrjetit, të cilët çiftojnë rrjete të ndryshme nga njëri-tjetri. Ky çiftim rrjetesh mund të kryhet nga LAN-i në LAN edhe nëpërmjet disa routerash.

Routerat punojnë referuar modelit OSI në shtresën e transportit (Shtresa 3) dhe varen nga protokolli i përdorur. Routeri duhet të jetë në gjendje t'i kuptojë protokollet me të cilat ai duhet të punojë. Meqë routeri duhet t''i ç'paketojë të gjitha paketat e ardhura me të dhëna, me qëllim që këto të fundit të mund të përpunohen më tej, ai është gjithashtu në gjendje të lidhë me njëra-tjetrën topologji të ndryshme si p.sh. Ethernet me FDDI.

Dallojme llojet e mëposhtme të routerave:

- ☑ Routera me një protokoll
- ☑ Routera shumëprotokollësh
- ☑ Routera hibridë

Routerat një protokollësh (single protocol)

Routerat me një protokoll përdoren për të lidhur rrjetet me njëri-tjetrin. Tregues i rëndësishëm tek këta routera është se ata mund të përdoren për lidhjen e dy rrjeteve me një protokoll rrjeti të vetëm. Në shumicën e rasteve routerat me një protokoll përdoren për lidhjen e rrjeteve me njëri-tjetrin (lidhja LAN-LAN), ose rrjete me një rrjet që ka lidhje me backbone-in (lidhja LAN-WAN).

Shënime

Routerat shumëprotokollsh (multiprotocol)

Routerat shumëprotokollësh janë në gjendje të lidhin rrjete me protokolle të ndryshme. Në rast se në një rrjet përdoren p.sh. protokolle si TCP/IP, IPX/SPX, DECNet, atëhere për secilin nga këta protokolle ekziston një protocol-stack në router. Protocol-stack do të thotë që, të gjitha paketat me të dhëna duke filluar nga shtresa 3 ç'paketohen, transferohen dhe si përfundim paketohen sërish në të njëjtën rradhë.

Nëpërmjet këtyre protocol-stacks, të cilat janë implemetuar në router, lidhen me njëri-tjetrin rrjete të ndryshme logjike.

Routerat hibridë

Routerat hibridë janë në gjendje që të gjitha paketat, të cilat nuk mund të routohen në një rrjet, t'i transferojë në një rrjet tjetër. Për këtë qëllim, tek një router hibrid, të gjitha të dhënat merren dhe vlerësohen. Pasi informacionet e kontrollit merren dhe vlerësohen, paketa me të dhëna, nëpërmjet ndërfaqes përkatëse, transferohet në një rrjet në largësi (remote network). Ky proces, sidoqoftë, lejon vetëm çiftimin e rrjeteve të njëllojta me njëri-tjetrin.

Kriteret e mëposhtme duhen mbajtur parasysh, në rast të përdorimit të një routeri në firmën tuaj:

- ☑ A është routeri modular 19" i montueshëm, apo duhet vendosur mbi një mbajtëse speciale?
- ☑ Për cilat shërbime duhet të jetë i përshtatshëm routeri (p.sh. vetëm Internet)?
- ☑ A duhet të lidhen me të degë të rrjetit të kompanisë?
- ☑ A do të kërkohet më vonë zgjerimi i rrjetit të firmës (modular router)?
- ☑ Cilat protokolle duhet të mbështesë routeri (multiprotocol-Router)?

Sipas performancës dhe fluksit të transmetimit të të dhënave routerat ndahen në klasa të ndryshme:

- ☑ High Performance Router
- ☑ Gigabit-Router
- ☑ Enterprise-Router
- ☑ Access-Router
- ☑ SoHo-Router

Ndërsa High Performance Router, Gigabit-Router dhe Enterprise-Router përdoren vetëm në rrjetet e mëdha, që kërkojnë performancë të lartë, Access-Router dhe SoHo-Router (SmallOffice, HomeOffice) janë konceptuar të përdoren në rrjete të madhësive mesatare. Me SoHo-Routerat realizohen më së shumti lidhjet në Internet, apo ndërmjet degëve. Access-Routerat shërbejnë si hyrje kryesore në administrimin qendror, nëpërmjet të cilit degët lidhen me njëra-tjetrën. Këto lloj routerash janë modulare dhe mund të pajisen sipas nevojës me modulet përkatëse (ISDN, S2M, ATM).

Routimi i adresave IP

Sot, për lidhjen e kompjuterave përdoren më së shumti switchet, të cilat punojnë vetëm në shtresat 1 dhe 2 sipas modelit OSI. Ato nuk mundësojnë nëndarjen logjike të shtresës 3 të medias së komunikimit.

Në rast se një hosti me një adresë i duhet të komunikojë me një rrjet tjetër, i duhet të përdorë një teknikë, e cila merr përsipër transportin e paketave në rrjetin tjetër. Kjo pajisje që zotvron këtë teknikë njeh rrugën (route) për tek rrjeti përkatës, dhe quhet router.

Me qëllim që një host të identifikojë, nëse duhet të komunikojë me një host tjetër në rrjetin e vet, apo me një host në një rrjet tjetër, atij i duhet të përdorë adresën e rrjetit dhe te subnetit të hostit .

5.8 Gateway

Mënyra e funksionimit të Gateway-it

Me Gateway kuptohet një sistem, me anë të të cilit rrjete të ndryshme lidhen me njëri-tjetrin, ose iu bashkohen rrjeteve të tjera nëpërmjet konvertimit të protokollit. Për këtë qëllim paketat me të dhëna paketohen sërish nga Gateway, me qëllim që ato t'i korrespondojnë kërkesave të sistemit të destinacionit. Gateway mund të kuptohet si një lloj konvertuesi protokolli.

Gateway punon në shtresën e aplikacioneve referuar modelit OSI (Shtresa 7 –Layer 7). Gateway i kupton plotësisht protokollet e konvertueshme dhe në rrjetet e kufizuara është një nyje e adresueshme rrjeti.

Gjatë konvertimit të protokolleve përkatëse të rrjetit, të gjitha informacionet e paketave me të dhëna, si p.sh. adresa e destinacionit dhe e burimit, përshtaten sipas formatit respektiv të rrjeteve të largëta (remote networks). Krahas përshtatjes së pastër të përmbajtjes së paketave me të dhëna kryhet konvertimi i kontrollit të rrjedhës së të dhënave, si dhe përshtatja e shpejtësisë së transmetimit me atë të rrjetit tjetër.

I vetmi disavantazh që paraqet përdorimi i një Gateway është se këto pajisje mund të përshtasin me njëri-tjetrin vetëm dy protokolle të ndryshme rrjeti. Mbi këtë bazë, në një rrjet heterogjen ku përdoren shumë protokolle kërkohet një numër korrespondues gateway-sh. Në këtë mënyrë rriten edhe kostot administrative në rrjetet e mëdha.

Meqë funksioni i Gateway-t ndahet sipas detyrës speciale që ai kryen, shpesh Gateway-t e marrin emrin sipas detyrës që kryejnë.

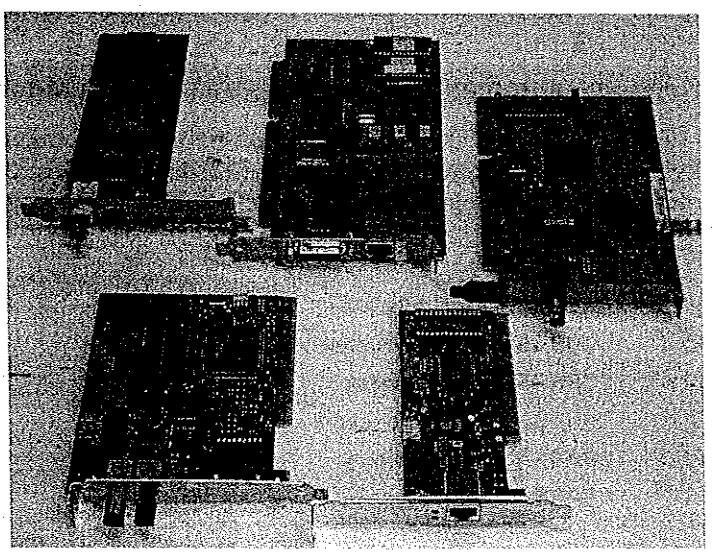
- ☑ një NOVELL-Gateway ka për detyrë, të përshtasë të dhënat nga një rrjet i caktuar në një rrjet Novell
- ☑ një Proxy-Gateway (Translating Proxy) transformon p.sh. protokollin HTTP, me qëllim që të mundësojë lidhjen me një server FTP
- ☑ një E-Mail-to-Fax-Gateway transformon E-Mail-in e dërguar në një faks
- ☑ një E-Mail-to-SMS-Gateway dërgon E-Mail-et si SMS tek një numër telefoni
- ☑ një Media-Gateway transformon informacionet dixhitale të koduara multimediale (p.sh. informacione zëri, figure, audio) në mënyrë të tillë që të jenë në gjendje për t'u transportuar në rrjet

5.9 Kartat e rrjetit

Ndërfaqet e kartave të rrjetit

Karta rrjeti dhe ndërfaqe të ndryshme të tyre
Network-Interface-Cards (NIC) janë karta për sisteme bus-i të caktuara, si ato që përdoren në pc. Kartat e rrjetit krijojnë atë që quhet ndërfaqja fizike e rrjetit. Për lidhje me mediat fizike të transmetimit, kartat e rrjetit janë pajisur me elementet lidhës respektivë. Tek kartat e rrjetit Ethernet dallojmë elementët lidhës të mëposhtëm:

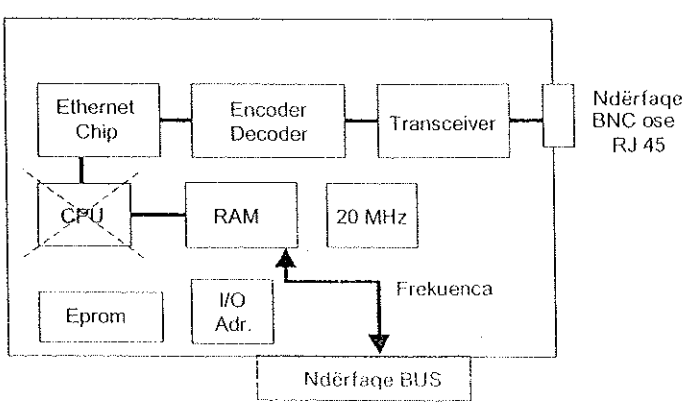
- ☑ Dalje 15-inch Sub-D për lidhjen AUI
- ☑ Portë RJ-45 për lidhjen në një rrjet 10BaseT- ose 100BaseT.
- ☑ Dalje BNC për rrjet 10Base2
- ☑ Dalje ST- ose SC për rrjetet me fibra optike (10BaseFL respektivisht. 100BaseFX)



Karta rrjeti dhe ndërfaqe të ndryshme të tyre

Njësitë funksionale të kartës së rrjetit

Grupet sipas funksioneve të një karte rrjeti
Me ndihmën e kartave të rrjetit, nëpërmjet medias respektive, kompjuterat janë në gjendje të komunikojnë me pajisje të tjera në rrjet (PC, printera). Ato formojnë një ndërfaqe midis një sistemi kompjuterik (PC) dhe medias specifike të transmetimit (bakër, fibra optike). Kështu, të dhënat e përdoruesit procesohen nëpërmjet kontrollerave të komunikimit, të integruar në kartën e rrjetit, të cilët janë të përshtatshëm për shkëmbimin e të dhënave.



Grupet sipas funksioneve të një karte rrjeti

Treguesit e performancës së kartave të rrjetit

Në rast se të dhënat nga PC-ja në rrjet dhe anasjelltas nuk transportohen aq shpejt sa duhet, atëhere i gjithë fluksi i transmetimit është i ngadaltë. Në një rrjet bus me proces CSMA/CD nuk mund të transmetohen të dhëna të tjera në rrjet përsa kohë që dërguesi i të dhënave të ketë mbaruar transmetimin e të dhënave të tij. Kjo e rrit në mënyrë drastike kohën e pritjes në rrjet.

Rritja e shpejtësisë së transmetimit tek kartat e rrjetit arrihet nëpërmjet karakteristikave të mëposhtme:

- ☑ **Busmaster** që mundëson këmbimin e të dhënave nëpërmjet DMA-së
- ☑ Memorje e kartës NIC që shfrytëzohet bashkërisht me atë të PC-së
- ☑ Memorizim i ndërmjetëm i të dhënave në një memorie Puffer
- ☑ Mikroprocesor onboard

Kartat e rrjetit, të cilat disponojnë në qarkun e tyre një mikroprocesor të vetin, nuk kanë nevojë për mbështetje nga CPU-ja e kompjuterit. Nëpërmjet tij rritet dukshëm shpejtësia e përpunimit të të dhënave në rrjet. Ky tip karte rrjeti quhet ndryshe edhe kartë rrjeti aktive. Kartat e rrjetit pa mikroprocesor të vetin onboard quhen ndryshe edhe karta rrjeti pasive.

Lloji i funksionimit - Promiscuous Mode

Parimisht, nga kartat e rrjetit pranohen vetëm paketa me të dhëna, të cilat transferohen tek adresat përkatëse të hardware-it. Paketat e marra transferohen më tej, nëpërmjet shtresës fizike, në shtresën më të afërt lart. Disa karta rrjeti janë në gjendje që të lexojnë të gjitha paketat me të dhëna në rrjet si dhe t'i transferojnë në shtresat më të larta. Kjo mënyrë funksionimi quhet "Promiscuous Mode". Promiscuous Mode përdoret gjerësisht nga softwaret e analizimit të rrjetit si dhe nga instrumenta të tjerë mbikqyrës që kryejnë protokollimin e paketave me të dhëna në rrjet.

Negocimi automatik i shpejtësisë së transmetimit (Auto Negotiation)

Negocimi automatik i shpejtësisë së transmetimit (Auto Negotiation) përcaktohet në standardin Ethernet IEEE 802.3. Ky proces ndodh në pak milisekonda gjatë krijimit të lidhjes. Gjatë negocimit automatik, dy pajisjet që komunikojnë në rrjet negociojnë shpejtësinë më të mirë të mundshme të komunikimit. Rradha e zgjedhjes automatike të shpejtësisë është si vijon:

- ☑ 1000BASE-TX Full duplex
- ☑ 1000BASE-TX Half duplex
- ☑ 100BASE-TX Full duplex
- ☑ 100BASE-TX Half duplex
- ☑ 10BASE-T Full duplex
- ☑ 10BASE-T Half duplex

Transferimi paralel i të dhënave (Parallel Tasking)

Në teknologjinë parallel-tasking bëhet fjalë për një variant specifik sipas prodhuesit në shkëmbimin e të dhënave midis kartës së rrjetit dhe host-it. Gjatë përdorimit të kësaj teknologjie kalimi i fluksit të të dhënave kryhet përmes transmetimit të njëkohshëm të tyre në të dy drejtimet (dërgimit dhe marrjes). Në këtë mënyrë optimizohet shkëmbimi i të dhënave, si dhe rritet shpejtësia e komunikimit në rrjet.

Me anë të kësaj teknologjie paketat me të dhëna transmetohen në rrjet direkt sapo merren. Ndryshe nga teknologjia tradicionale, tek e cila pritet, derisa paketat me të dhëna arrijnë të gjitha në memorjen puffer, teknologjia parallel-tasking rrit ndjeshëm fluksin e të dhënave të transmetuara.

Një zhvillim i mëtejshëm i teknologjisë parallel - tasking është teknika e quajtur parallel – tasking II. Kjo e fundit bazohet në teknologjinë e mëparshme, por në ndryshim nga ajo rrit akoma më shumë fluksin e të dhënave nga karta e rrjetit për në host. Risia thelbësore në teknologjinë parallel – tasking II është shfrytëzimi i komandave speciale për chipet e PCI-së.

Kartat e rrjetit Gigabit-Ethernet për lidhjet me kabëll prej bakri

Përparësia më e madhe e arritjes së shpejtësisë Gigabit në kabllot prej bakri është, se në këtë rast mund të shfrytëzohet struktura e lidhjes kabllore ekzistuese (konvencionale) e ngritur me kabëll të kategorisë 5. Tek kabllot e bakrit në përdorim duhet mbajtur parasysh, që një transmetim standard 1000Base-T kryhet përmes katër çifteve të përdredhura që përbëjnë kabllin (twisted pairs). Prizat modulare ekzistuese të rrjetit me dy dalje, që përdorin dy çifte të përdredhura

të kabllit për çdo dalje (cable sharing), çojnë në impas. Para përdorimit të kartave Gigabit-she të rrjetit këto gjëra duhen mbajtur parasysh patjetër. Kartat Gigabit-Ethernet janë kompatibël me pararendëset e tyre (backward compatibility), kartat Fast-Ethernet me 10/100 MBit/s, si dhe mbështesin negocimin automatik të shpejtësisë së transmetimit (Auto Negotiation).

Fluksi i të dhënave prej 1 GBit/s arrihet përmes transmetimit të njëkohshëm të 250 MBit/s për çift kablli të përdredhur. Nga katër çiftet e përdredhura rezulton shuma prej 1 GBit/s. Këtu transmetimi kryhet në mënyrë të ngjashme si tek 100 MBit/s, me një frekuencë prej 125 MHz. Sidoqoftë, në këtë rast përdoret një proces kodimi dhe dekodimi më i mirë se tek 100 MBit/s. Në krahasim me 100 MBit/s – këtu transmetohet 1-Bit-Symbol me 125 MHz (=125 MBit/s) – për 1 GBit/s transmetohen 2 Bits me 125 MHz (250 MBit/s).

Në bazë të procesit të kodifikimit të përdorur për 100 Mbit - 4-Bit-të dhëna do të transmetohen si informacion 5-Bit-sh – në një frekuencë 125 MHz ato japin një fluks të dhënash 100 MBit/s.

6 Protokollet e sotme të komunikimit

Në këtë kapitull do të lexoni
→ çfarë janë protokollet
→ çfarë janë shërbimet
→ si përdoren protokollet dhe shërbimet

Parakusht
✓ Njohuri bazë mbi rrjetet

6.1 Detyrat e protokolleve dhe shërbimeve

Protokollet dhe shërbimet

Protokollet shërbejnë për të garantuar transportin e të dhënave. Ato paraqesin në vetvete „gjuhët", me të cilat sisteme të ndryshme komunikojnë me njëri-tjetrin. Sigurisht në çdo proces komunikimi marrin pjesë disa protokolle.

Shërbimet u vënë në dispozicion protokolleve një mjedis në të cilin detyra si konfigurimi i informacioneve të rrjetit, ose përgatitja e të dhënave në sisteme në largësi, të mund të përputhen me njëra-tjetrën. Të gjesh vijën ndarëse midis shërbimeve dhe protokolleve nuk është gjithmonë aq e lehtë. Kështu, shërbimi i Internetit bazohet në një protokoll të vetin (HTTP), ndërsa shërbimi i rezolucionit të emrit DNS (Domain Name Service) përdor protokollin DNS.

Përgjithësisht thuhet se asnjë shërbim nuk mund t'i përmbushë detyrat pa një protokoll të përshtatshëm. Kjo pasi çdo komunikim bazohet në PED në një shumllojshmëri mundësish të ndryshme, të cilat sidoqoftë kërkojnë një përshtatje të saktë të mjedisit për këtë qëllim. Këto përshtatje përshkruhen si rregulla të sakta për detyrat e protokolleve të planifikuara.

Protokollet për transmetimin fizik të të dhënave

Një grup protokollesh përshkruan procedurën si duhet të transportohen të dhënat nëpërmjet një mediumi të caktuar. Kështu në protokollin e Ethernet-it përcaktohet lloji i aksesit në median transportuese (CSMA/CD = Carrier Sense, Multiple Access with Collision Detection), si dhe përcaktimet e flukseve, mbulimi i fishave, tensioni, paraqitja e njëshave dhe zerove, etj.

Protokolle të tjera shërbejnë për lidhjen e të dhënave të një rrjeti me të dhënat e një lidhjeje telefonike, me qëllim që të mundësohet transporti midis rrjeteve. Përcaktimet si rasti i lidhjeve me telefon përfshihen sigurisht në zonën kufi të protokolleve të rrjetit. Në fakt sot ISDN-ja nuk mendohet më si shërbim jashtë rrjetit, por realisht bëhet fjalë për shfrytëzimin e një shërbimi jashtë rrjetit.

Në këtë kapitull nuk do të thellohemi në përshkrimin e protokolleve më pranë hardware-ve. Përdorimi i tyre do të përcaktohet nëpërmjet hardware-ve të përdorura dhe nuk lë vend për përshtatje individuale.

Protokolle për gjetjen e rrugës së paketave dhe për transportin e tyre

Një grup tjetër protokollesh ka për detyrë të garantojë transportin e paketave me të dhëna midis rrjeteve. Këto protokolle përmblidhen në dy grupe:

☑ Protokolle që shërbejnë për gjetjen e rrugëve të mundshme të transportit të të dhënave midis rrjeteve (Routing protocols)

☑ Protokolle që shërbejnë për transportin e paketave midis rrjeteve (Routed protocols)

Protokolle për transport të dhënash

Sot, pa përjashtim, konsiderohet normale që disa aplikacione në një kompjuter të kërkojnë njëkohësisht shërbime të rrjetit. Midis këtyre aplikacioneve dhe rrjetit duhen përdorur protokolle ndërmjetëse, të cilat i ndajnë të dhënat në segmente të transportueshme dhe më pas i bashkojnë për t'i transferuar tek aplikacionet përkatëse. Segmentet me të dhëna, të cilat nga protokollet e transportit transferohen më tej tek protokollet e rrjetit, përshkruhen si datagrame.

Meqë datagramet mund të transportohen në rrugë të ndryshme përmes rrjetit, duhet patur kujdes, që ato më pas të mblidhen në rradhën e duhur dhe të transferohen më tej në shtresën e aplikacioneve.

Një nga arsyet, se përse të dhënat transportohen në segmente dhe jo si një tërësi është, se në rast dëmtimi nuk ka nevojë të dërgohet sërish e gjithë paketa me të dhëna, por vetëm segmenti i dëmtuar. Prandaj, për çdo proces përpunimi shtesë, protokolli i angazhuar ndërmerr edhe një nëndarje të mëtejshme të të dhënave në copëza më të vogla. Në rast dëmtimi apo humbjeje të të dhënave, shumë protokolle reagojnë në mënyrë të përshtatshme duke kryer ritransmetimin e tyre. Protokolle të tjera e lenë në dorë të protokolleve apo shërbimeve të specializuara, që të merren me sigurimin e integritetit të të dhënave.

Në përgjithësi, çdo funksion shtesë gjatë transportit të të dhënave ka nevojë për gjerësi bande të rrjetit dhe kapacitet përpunimi të CPU-së. Për këtë arsye duhet të gjendet gjithmonë një kompromis midis sigurisë së transmetimit dhe dhe efektivitetit të shfrytëzimit të të dhënave.

Shërbimet

Shërbimet e përhapura në kohën e sotme përfshijnë një numër mjaft të madh detyrash të ndryshme. Shumë nga këto detyra garantohen nga më shumë se një protokoll, por mbulohen nëpërmjet disa shërbimeve të ndryshme. Kjo pjesërisht çon në një performancë të ndryshme të rrjeteve, sistemeve operative, përdoruesve dhe aplikacioneve, e pjesërisht bëhet fjalë për shërbime alternative për produkte të prodhuesve të ndryshëm.

Shërbimet në rrjete ndahen në tre grupe të mëdha:

- ☑ Shërbimet për punën në rrjet
- ☑ Shërbimet për sistemet operative
- ☑ Shërbimet për përdoruesit dhe aplikacionet

Shënime

Shërbimet për punën në rrjet

Një grup shërbimesh ka për detyrë të sigurojë punë pa probleme në rrjet dhe ta bëjë atë sa më të lehtë për përdoruesit (user friendly). Ato marrin përsipër të kryejnë shërbime të tilla si rezolucioni i adresës, caktimi i adresës, sinkronizimi i kohës, filtrim sigurie i të dhënave dhe paketave, vënien në dispozicion te informacioneve të ruajtura në memorjen ndërmjetëse për lehtwsimin nga ngarkesa të lidhjeve WAN.

Një kufi ndarës fiks me grupin tjetër të shërbimeve të rrjetit mund të vendoset vetëm pjesërisht. Kështu p.sh. mund të përdoret sinkronizimi i kohës, si i komponentëve të rrjetit, ashtu edhe i sistemeve operative, apo i përdoruesve.

Shërbimet për sistemet operative

Egzistojnë një sërë shërbimesh, të cilat përmbushin detyra specifike të sistemit operativ. Në vijim do të gjeni një pamje të përgjithshme të detyrave të sotme të sistemit operativ, të cilat garantohen nga shërbimet e rrjetit:

- ☑ **Autentifikimi i përdoruesve:** Në rrjetet e sotme, identifikimi i përdoruesve nuk behen nga sistemet lokale, por administrohen në një bazë qëndrore të dhënash që shërben për të gjithë rrjetin.
- ☑ **Përgatitja e shërbimeve të shpërndarjes (distribution services):** Me qëllim që resurset e sistemit të shfrytëzohen në mënyrë efikase, sot p.sh. bazat e të dhënave mund të shpërndahen në disa kompjutera (servera). Edhe aplikacionet nuk egzekutohen më gjithmonë në sistemet lokale, por gjithnjë e më shumë egzekutohen në të ashtuquajturit servera aplikacionesh (application servers). Kjo ndër të tjera ofron mundësinë që të kursehen potenciale në hardëare, licensa, si dhe të zvogëlohet dukshëm koha e administrimit dhe e mirëmbajtjes së rrjetit.
- ☑ **Siguria ndaj rënies së sitemit:** Nëpërmjet sistemit të shpërndarjes së skedarëve (distribution file system) krijohet mundesia e ruajtjes së dokumentave në disa servera në rrjet, gjë që bën të mundur, që edhe në rast të rënies së një sistemi të tërë, rrjeti të mbetet sërish në punë. Nëpërmjet shpërndarjes gjeografike të sistemeve parandalohen humbjet e të dhënave si pasojë e katastrofave të shkaktuara nga tërmetet, zjarret, përmbytjet etj.duke qenë se cluster-at janë të lidhura nëpërmjet linjave të WAN-it.
- ☑ **Shpërndarja e ngarkesës:** Krahas sigurisë që ofrojnë për mosrënien e sistemit, cluster-at ofrojnë edhe avantazhin e rritjes së përformancës së sistemeve. Në qoftë se në një sistem operojnë shërbime të cilat e aksesojnë intensivisht diskun e ngurtë (harddrive) gjatë kohës që një sistem tjetër kryen detyra të cilat e ngarkojnë shumë procesorin, atëhere ka plotësisht kuptim, që këto dy shërbime të shperndahen në të dyja sistemet, me qëllim që të parandalohen ngadalësimet (bottlenecks) apo ngecjet e punës.

Shërbimet për përdorues dhe aplikacione

Grupi i shërbimeve të rrjetit u vë në dispozicion përdoruesve dhe aplikacioneve funksione të rrjetit. Zor se gjendet njeri sot që nuk përdor shërbime të tilla si World Wide Web-i, News-groups-et apo E-Mail-et. Në rrjetet e firmave aksesi i printerave në distancë (remote printers) apo ruajtja e të dhënave në file servera në distancë nuk është më imagjinatë.

Një grup i tërë shërbimesh të tjera përdoret nga përdoruesit, pa qënë gjithmonë të ndërgjegjshëm këta të fundit që po i përdorin. Kështu p.sh. gjatë blerjeve në Internet informacionet kodohen, me qëllim që klienti të mbrohet nga aksesi i padëshiruar i të dhënave nga të tretët. Thjesht vetëm me një akses në një website, krahas HTTP-së aktivizohen p.sh. edhe cookies, scripte, Active-X-e etj., të cilat në pjesën më të madhe i riaksesojnë sërish shërbimet e tyre të rrjetit.

Kështu pra, në një akses të vetëm marrin pjesë dhe aktivizohen një duzinë protokollesh dhe shërbimesh të ndryshme.

6.2 Protokollet në rrjetet lokale

Protokollet e rrjetit

Më poshtë do të paraqiten shkurtimisht një sërë protokollesh, të cilat në ditët e sotme gjejnë përdorim në rrjetet lokale. Për t'u kuptuar më mirë ato ndahen në grupet e mëposhtme:

- ☑ Protokollet e transmetimit
- ☑ Protokollet e transferimit

Grupi i protokolleve të transmetimit merret me transmetimin fizik të të dhënave dhe vepron më tepër në fushën e hardware-ve.

Ndryshe nga sa më sipër, protokollet e transferimit merren me dërgimin e saktë të të dhënave përmes rrjetit. Ato garantojnë, që të dhënat të merren nga marrësi i duhur, që përpunimi i mëtejshëm në sistem të kryhet pa probleme dhe në mënyrë efikase, si dhe që të dhënat e dëmtuara, apo të humbura të ritransmetohen sërish.

Protokollet e transmetimit

Grupi i protokolleve të transmetimit, i cili përdoret sot në rrjetet moderne, nuk është aq i madh siç qe rasti i para pak viteve. Sot, përveç Ethernet-it, zor se mund të gjejë përdorim ndonjë protokoll tjetër i bazuar në lidhjet kabllore. Pas ndalimit të prodhimit, në fillim të vitit 2002 nga IBM, të komponenteve për rrjetet Token Ring, parashikohet që këto produkte të zhduken shpejt nga tregu.

Protokolle të tilla si VG-AnyLAN zor se gjenden në ndonjë rrjet në ditët tona. Arsye për këtë është, krahas kostove, tendenca e tregut për standardizim. Në këtë mënyrë, që një procedurë të pranohet në treg duhet që të jetë patjetër më e mira. Rëndësi më të madhe këtu merr edhe mbështetja nga prodhuesi.

Ethernet-i

Familja e protokolleve Ethernet në rrjetet lokale sot është më e përhapura. Për saktësim duhet përmendur se tek Ethernet-i nuk bëhet fjalë për një protokoll të vetëm, por për një sërë protokollesh të cilët merren me zbatime të ndryshme të procesit të aksesit të rrjetit : Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Nomenklatura e Ethernet-it

Në Ethernet sot përdoren materiale të ndryshme për transport, shpejtësi transmetimi të ndryshme dhe mënyra transmetimi të ndryshme të të dhënave. Në tabelën e mëposhtme paraqiten zbatimet më të rëndësishme të Ethernet-it me të dhënat përkatëse që i shoqërojnë ato. Shpejtësitë e transmetimit në Megabit për sekondë jepen me numrin që vendoset para fjalës BASE. Fjala BASE do të thotë banda bazë (angl.: baseband) dhe i referohet teknikës me anë të së cilës i gjithë mediumi i transmetimit përdoret përjashtimisht vetëm për Ethernet-in. Në rast se media e transmetimit përdoret dhe për të dhëna të tjera, atëhere bëhet fjalë për transmetime me broadband. Këtë rast, në lidhje me Ethernet-in, e gjejmë të përdoret vetëm për 10BROAD-36, një procedurë e vjetëruar, tek e cila mbi tre kanale për drejtim kapërcejnë distanca prej 3,6 kilometrash (lidhjet me kabell të televizioneve kabllore).

Specifikimi i Ethernet-it	Emri ndryshe (Koment)	Lloji i kabllit	Gjatesia maksimale e segmentit
1Base5	StarLAN	Unshielded Twisted Pair (UTP) 1 cift fijesh	500 Metra deri tek Hub-i
10Base-2	CheaperNET, BNC	Kabëll koaksial i hollë 50 Ω	185 Metra
10Base-5	Thicknet, Yellow Cable	Kabëll koaksial i trashë 50 Ω	500 Metra
10Base-T	Twisted Pair	2 çifte UTP Kategoria 3 ose më të mirë	100 Metra deri tek Hub-i
10Base-F	----	Familja e fibrave	
10Base-FL	----	2 LWC Multimode me HUB aktiv asinkron	2 Kilometra deri tek Hub-i
10Base-FP	----	2 LWC Multimode me HUB pasiv asinkron	500 Metra deri tek Hub-i
10Base-FB	----	2 Multimode LWC me HUB aktiv sinkron	2 Kilometra deri tek Hub-i
100Base-T4	----	4 çifte UTP Kategoria 3 ose më të mirë	100 Metra deri tek Hub-i
100Base-TX	----	2 çifte UTP Kategoria 5 ose më të mirë	100 Metra deri tek Hub-i

100Base-FX	----	2 Multimode LWC	2 Kilometra deri tek Hub-i
	(Shumë rrallë)	2 çifte UTP Kategoria 3 ose më të mirë	100 Metra deri tek Hub-i
	Gigabit Ethernet	Përshkrimi i familjes	
		4 çifte UTP Kategoria 5 ose më të mirë	100 Metra deri tek Hub-i
		2 çifte 150 Ω Balanced Shielded Cable	25 Metra deri tek Hub-i
		2 LWL Multimode 850 nm	270 Metra për 62,5 μ, 550 Metra për 50 μ
		2 Mono- ose LWC Multimode 1300 nm	440 Metra për 62,5 μ Multimode, 550 Metra për 50 μ Multimode, 3 Kilometra për 9 μ Monomode

Protokollet e transmetimit

Protokollet e transmetimit kanë për detyrë të sigurojnë, që të dhënat transmetohen në një rrugë të përshtatshme nga dërguesi tek marrësi. Në përgjithësi dallohen dy grupe:

☑ Protokollet që mundësojnë route-imin
☑ Protokollet që nuk e mundësojnë route-imin

Protokollet që mundësojnë route-imin përmbajnë informacione mbi strukturat logjike të rrjeteve. Këto struktura ndërtohen në formën e rrjeteve dhe nënrrjeteve (subnets), të cilat vendosin lidhje me njëra-tjetrën nëpërmjet router-it. Ato shërbejnë për implementimin e hierarkisë në rrjet dhe mund të segmentojnë të ashtuquajturat broadcast domains. Në rast se të dhënat transmetohen brenda një rrjeti logjik, hierarkia nuk luan asnjë rol, por në rast se trafiku i të dhënave do t'i kapërcejë kufijtë e rrjetit, atëhere në protokollin që mundëson route-imin duhet të përmbahet informacion në lidhje me rrjetin destinacion, i cili u lejon pajisjeve ndërmjetëse (routerave) të zgjedhin rrugën më të përshtatshme për transmetim.

Protokollet që mundësojnë routimin janë:

☑ **Internet Protocol (IP)**
☑ Internet Packet Exchange (IPX)
☑ AppleTalk

NetBEUI si protokoll që nuk e mundëson routimin

Protokollet që nuk e mundësojnë routimin nuk luajnë asnjë rol në trafikun e të dhënave midis rrjeteve. Ato nuk mbështesin nëndarjet në rrjete logjike, por mundësojnë komunikimin e të gjithë nyjeve (knots) fizike përkatëse të një rrjeti, të cilat gjenden në të njëjtën lidhje logjike. Në këtë mënyrë ato nuk mund të përdoren për të mundësuar trafikun e të dhënave midis rrjeteve.

Por nga ana tjetër kjo bën që koha e konfigurimit të protokollit dhe ngarkesa (overhead-i) e tij (pjesa shtesë e informaconeve të protokollit për t'u transmetuar) janë dukshëm më të vogla, se sa në rastin kur në një header do të duhej të përmbahej dallimi i nyjeve dhe rrjeteve.

I vetmi protokoll që nuk e mundëson route-imin dhe që përdoret ende sot në mënyrë shumë të kufizuar, është NetBEUI. Bëhet fjalë për një protokoll proprietar të Microsoft-it, i cili nuk bën dallim midis transferimit të paketave dhe protokollit të transportit, si dhe që jo çdo formë e konfigurimit kryhet nëpërmjet administratorit. Përveç kësaj, ai përdor një numër të madh broadcastesh, duke qenë se fusha e tij e përdorimit kufizohet në rrjete të vogla me pak nyje.

6.3 Shërbimet e rezolucionit të emrit (name resolution)

Emrat e kompjuterave dhe domain-et

Sa më i madh të jetë rrjeti, aq më e rëndësishme është, që sistemet të mund të adresohen nga përdoruesit në një mënyrë sa më të kuptueshme. Për këtë arsye një nomenklaturë (rregullat e dhënies së emrave) e saktë merr një rol domethënës.

Puna për përdoruesit dhe administratorët e rrjetit bëhet më e lehtë, në qoftë se përdoren emra apo shkurtime emrash domethënës, si p.sh TR-AQ-PrSrv1, për emrin e print-server-it të administratës qendrore të institucionit në Tiranë, sesa po të përdorej po për këtë pajisje një emër i tillë si 24Bv27Ssr254. Në mënyrë të ngjashme në të gjithë rrjetin duhen vendosur rregulla të sakta. Sipas mundësive këto rregulla duhen hedhur në një manual të detyrueshëm për zbatim, i cili duhet të gjendet si informacion i dokumentuar dhe i aksesueshëm publikisht në rrjet nga përdoruesit.

Nëse rrjeti bëhet gjithnjë e më i madh, ku përfshihen mbase disa shtete, apo firma të një konsorciumi, atëherë si pjesë përbërëse e mëtejshme e emrave futet domain-i. Domain-et u vënë në dispozicion grupeve të kompjuterave dhe të përdoruesve instanca qendrore autentifikimi. Kështu informacioni i vendndodhjes TIRANE mund të përmbahet si nëndomain i emrit FIRMA. Ndërsa print-server-it të administratës qendrore të firmës mund t'i jepet një emër si *AQ-PrSrv01.Tirana.Firma.al*.

Protokollet e rezolucionit të emrit

Rëndësia e emrave për përdoruesit në rrjet merr kuptim edhe më domethënës, kur bëhet fjalë për transferimin e informacioneve midis rrjeteve logjike. Adresimi i sistemeve kryhet nëpërmjet adresave të qarta, të cilat përbëhen nga adresat e rrjetit dhe të nyjeve të rrjetit. Me qëllim që rrjeti të jetë në gjendje, që për të përmbushur një kërkesë të një përdoruesi për transferim të dhënash nga *elektrike-wks215.tirana.uni.al* (wks këtu do të thotë work-station – kompjuter, stacion pune) tek *prodhimi-02.tirana.firma.al*, duhet që sistemi t'i caktojë emrave nga një adresë.

Shënime

Kjo në përgjithësi mund të kryhet në disa mënyra. Llojet e rezolucionit të emrave varen nga njëra anë nga protokolli i përdorur i rrjetit, dhe nga ana tjetër nga sistemi operativ. Renditja e mëposhtme jep një pamje të përgjithshme në lidhje me mënyrat e sotme të rezolucionit të emrave:

- ☑ Broadcast-et me kërkesë për rezolucion emri
- ☑ Broadcast-et e publikimit të emrave
- ☑ Caktimi i emrave nëpërmjet skedarëve (file-ve)
- ☑ Bazat e të dhënave statike ose dinamike në servera

Publikimi i shërbimeve

Krahas emrave, rrjeteve i nevojiten edhe informacione në lidhje me disponueshmërinë e shërbimeve. Edhe këto informacione publikohen nëpërmjet mekanizmave të rezolucionit të emrave dhe nuk duhet të konsiderohen të ndara, pasi në parim ato paraqesin vetëm një formë të veçantë të rezolucionit të emrave.

Broadcastet me kërkesë për rezolucion emri (Name Resolution Broadcast)

Brenda rrjeteve të vogla është e mundur, që rezolucioni i emrave të rregullohet nëpërmjet broadcast-eve. Në rast se përdoruesi, ose një aplikacion i dërgon një sistemi kërkesën për inicializimin e një transferimi të dhënash me një sistem tjetër, atëhere sistemi i dërgon si fillim një kërkesë në të gjitha sistemet e tjera, në të cilën kërkohet që marrësi të bëjë të njohur adresën e tij.

Ky lloj rezolucioni i emrit nga njëra anë rrit ngarkesën në rrjet, meqë e gjithë gjerësia e bandës në dispozicion nuk mund të shfrytëzohet më për transferimin e të dhënave dhe nga ana tjetër bën që të gjitha kartat e rrjetit të ngarkohen me vlerësimin e paketave, të cilat vetëm në raste të rralla janë për to përcaktuese. Broadcast-et mund të përdoren edhe vetëm brenda rrjeteve logjike apo subneteve, meqë këto nuk mund të routohen më tej. Përndryshe ekziston rreziku, që të gjitha rrjetet të vërshohen nga broadcastet. Kjo përshkruhet ndryshe edhe si broadcast-storm (stuhi broadcast-esh).

Broadcast-et për rezolucionin e emrit përdoren nga NetBIOS-i, një shërbim proprietar i Microsoft për këtë qëllim. Broadcastet, krahas rrjeteve të routueshme, të cilat nuk i suportojnë, nuk mbështesin asnjë koncept hierarkik domainesh, dhe për këtë arsye po përdoren gjithnjë e më pak.

Broadcastet e publikimit të emrave (Name Publication Broadcast)

Një metodë tjetër për rezolucionin e emrave në rrjete bazohet në atë që sistemet, të cilat vënë në dispozicion shërbime të caktuara për rrjetin, të dërgojnë si broadcasts të ashtuquajturat publikime shërbimesh. Ky sistem e ngarkon rrjetin dukshëm më pak.

Në një rrjet, si rregull disa stacione pune adresohen në pak servera. Rasti që stacionet e punës të adresohen tek njëri-tjetri është më shumë një përjashtim dhe në shumicën e rasteve aspak i dëshirueshëm (kjo gjë p.sh. vështirëson administrimin e një strukture sigurimi tv dhvnash (backup-i), tek e cila të dhënat do të siguroheshin vetëm në servera). Kur stacionet e punës dërgojnë broadcast-e, me qëllim që të gjejnë shërbime të serverit, ngarkesa në rrjet është dukshëm më e lartë, se në rastin kur serveri, në intervale të caktuara, informon se cilat shërbime janë të disponueshme në rrjet. Kjo pasi në shumicën e rrjeteve ka shumë më tepër stacione pune sesa servera.

Një sistem, të cilit i nevojitet një shërbim i caktuar, mund ose ta aksesojë direkt informacionin, ose „pyet" tek një server i dedikuar, se cili shërbim ofrohet dhe nga cilët servera. Listat e publikimit të shërbimeve mund të shkëmbehen midis router-ave dhe mund të arrihen në rrjetet e largëta, nëpërmjet shërbimeve të broadcast-it, pa shkaktuar ngarkesë shtesë në rrjet.

Familja e protokolleve IPX/SPX e Novell-it përdor Service Advertisement Protocol (SAP), me qëllim që të publikohet disponueshmëria e shërbimeve në rrjet. Në rast se një klient nuk e di ende adresën e një serveri për një shërbim që i nevojitet, ai dërgon një kërkesë GNS (GNS-request) si broadcast (Get Nearest Server). Kësaj kërkese i përgjigjet, duke dërguar informacionin përkatës, një server ose një router.

Meqë numri i SAP-eve mund të gjenerojë një ngarkesë të konsiderueshme në rrjet (si standard ato dërgohen çdo 60 sekonda). Protokollet IPX/SPX e ngarkojnë mjaft rrjetin.

Caktimi i emrave nëpërmjet file-ve (skedarëve)

Një mundësi tjetër për çiftimin e emrave të kompjuterave apo shërbimeve me adresa IP-je është përdorimi i skedarëve (files) të parakonfiguruar, të cilët përmbajnë të dhënat e çifteve të tilla (entries). Duke i patur në dispozicion lokalisht këto informacione të rrjetit gjerësia e bandës lehtësohet dukshëm, por nga ana tjetër rriten kostot administrative të përsonelit dhe të punës për mirëmbajtje. Prandaj, puna me këto skedarë ofrohet vetëm atëhere kur resurse të veçanta në largësi duhet të adresohen në një mjedis të routueshëm, ku mund të kryhet rezolucioni i emrave në emra kompjuterash lokalë nëpërmjet broadcasteve. Një fushë tjetër përdorimi e skedarëve për rezolucionin e emrave është kur përdoren shërbime si DNS (Domain Name System), të cilat nuk i suportojnë broadcastet.

Skedarët tekst (Text-files) *Hosts* dhe *LMHosts*

Informacionet ruhen në formën e çifteve adresë-emër në skedarë tekst dhe mund të vlerësohen nga sistemi, vetëm kur ato janë memorizuar me një emër fiks në vënde të caktuara të sistemit të skedarëve (file system). Ky emër për informacionet e NetBIOS-it është *LMHosts* dhe për informacionet e DNS-së *Hosts*. Vendi ku memorizohen varet nga sistemi operativ i përdorur. Tek sistemet operative Microsoft-NT dhe UNIX si rregull është direktoria *etc/*, ndërsa në sistemet Windows-9x-është direkt nën *%systemroot%*.

Bazat e të dhënave statike ose dinamike në servera

Në rrjetet e mëdha informacionet në lidhje me çiftet emër-adresë administrohen vetëm atëhere, kur ato vihen në dispozicion për të gjithë rrjetin në një qendër të caktuar për këtë qëllim. Këto baza të dhënash mund të aktualizohen në mënyrë dinamike nga sistemet operative, nga shërbimet e rrjetit, ose duhet të hidhen në mënyrë manuale nga operatorët e serverit si hyrje statike.

Domain Name System (DNS)

Sistemi i përhapur në të gjithë botën për rezolucionin e emrit në adresë IP-je dhe anasjelltas është i ashtuquajturi **Domain Name System**. Serverat DNS mbështesin një sistem hierearkik emrash, që bazohet në top-level-domain-e, domain-e dhe nëndomain-e. Në shembullin e mëposhtëm

serv.qrpd.uni-tirana.al

kompjuteri (serveri) *serv* është vëndosur në nëndomain-in *qrpd* (Qendra Rajonale e Përpunimit të të Dhënave) të domain-it *uni-tirana* në top-level domain-in *al* .

Adresat në DNS mund të shfrytëzohen nga sistemet lokale, ose mund të jenë të lidhura me Internetin dhe të përdoren për rezolucionin e emrave (name resolution). Në Internet, poshtë rrënjës ROOT, vendosen top-level-domain-et e shteteve dhe organizatave (të cilat dallohen tek emrat DNS ngaqë tek ato vendoset pika e fundit në grupin e pikave që dallojnë domain-et, nëndomain-et etj. nga njëra-tjetra). Këto adresa administrohen në mbarë botën nga InterNIC (International Network Information Center), ose nga nënorganizatat kombëtare (p.sh. ERT për Shqipërinë, ose DeNIC për Gjermaninë). Tek këto organizata firmat apo përsonat privatë mund të aplikojnë për emra domain-esh, për administrimin e të cilave janë vetë përgjegjëse.

DNS-ja bazohet mbi një bazë statike adresash, në të cilën krijohen zonat për hapësirat përkatëse të emrave të domain-eve. Këto përmbajnë të dhëna (entries) të nënrenditura për emrat e kompjuterave, shërbimeve dhe nëndomain-eve. Sot ekzistojnë gjithësej 19 lloje të dhënash (entries), të cilat mbështeten nga sistemi. Krahas emrave mund të përdoren p.sh. edhe të dhëna (entries) mbi shërbimet (SRV), të cilat tregojnë se cili server duhet të verë në dispozicion të rrjetit shërbime të caktuara.

Shënime

Një veçori tjetër e DNS-së është, që ajo mund ta replikojë bazën e vet të të dhënave në një server tjetër. Në këtë mënyrë egziston mundësia që në rrjetet me disa vendndodhje rezolucioni i emrave të kryhet lokalisht, duke lehtësuar nga ngarkesa lidhjet WAN. Sigurisht, në shumicën e zbatimeve të DNS-së nuk është e mundur që të kryhen ndryshime nga serverat replikues. Këto zona sekondare janë kopje të pastra të zonës primare, e cila përfaqëson bazën aktive të të dhënave. Këtu bëhet fjalë për një konfigurim të tipit master/slave.

Zhvillimet e reja lejojnë edhe krijimin e zonave sipas modelit multi-master, tek të cilat disa servera aktivë DNS mund të aktualizojnë me njëri-tjetrin informacionet e konfigurimit në një zonë të vetme, si dhe të mund të kryejnë ndryshimet e zonës në secilin nga serverat pjesmarrës.

DNS-ja dinamike (D-DNS)

Megjithëse DNS-ja bazohet mbi baza statike të dhënash, ekzistojnë zbatime të reja, të cilat mbështesin hyrjet dinamike të të dhënave. Për më tepër, një server DNS dinamik mund të marrë nga një server DHCP informacione në lidhje me shpërndarjen dinamike të adresave të IP-së tek klientët, të cilët vetë nuk e mbështesin DDNS-në (Dynamic DNS). Në këtë mënyrë zvogëlohet dukshëm koha e nevojshme për administrimin e DNS-së. Aktualisht D-DNS-ja mbështetet vetëm nga sistemet operative Windows 2000, XP si dhe nga versionet e reja të LINUX-it.

Windows Internet Name Service (WINS)

Windows Internet Name Service shërben, për të vënë në dispozicion të klientëve emrat NetBIOS dhe shërbimet në rrjet, ku çiftimi dhe caktimi emra-adresa mbahet në një bazë qendrore të dhënash. Çdo klient WINS i caktohet një serveri WINS primar, i cili gjatë startimit të kartës së rrjetit informon për adresën e tij të IP-së, emrat e sistemit, si dhe një numër informacionesh të tjera që i përkasin NetBIOS-it.

Serverat WINS mbështesin, krahas aktualizimit dinamik të hyrjeve të përshkruar më lart edhe atë statik (static entries). Në rast se në rrjet gjenden edhe p.sh. servera UNIX, për to nevojiten hyrje statike, pasi UNIX-i nuk e mbështet NetBIOS-in si protokoll.

Serverat WINS përdorin replikimin me servera të tjerë WINS, rast ky që gjithashtu i përket replikimit Multi-Master. Në secilin server pjesmarrës në replikim mund të kryhen ndryshime. Përdorimi i serverave WINS në rrjetet e mëdha të shpërndara nuk mund të rregullohet, meqë klientët do të përdorin serverin WINS më të afërt si server primar. Sigurisht që WINS-i nuk mbështet koncepte hierarkike, kështu që përdorimi i tij është i përshtatshëm vetëm për sisteme shumë të mëdha.

6.4 Protokollet e WAN-it (Wide Area Network)

Vështrim i përgjithshëm

Në fushën e komunikimit në WAN, parimisht ekzistojnë rregulla të tjera në komunikimin në rrjet krahasuar me rrjetet lokale - LAN. Kjo para së gjithash ka të bëjë me faktin, që në WAN del në pah kryesisht komunikimi i orientuar nga lidhja (connection oriented), i cili ndryshon dukshëm nga komunikimi në mediat e transmetimit të rrjeteve lokale. Si rezultat ka kërkesa të tjera ndaj protokolleve WAN në krahasim me protokollet LAN.

Në rrafshin logjik komunikimi në WAN i ngjan komunikimit në mjediset komplekse të LAN-it. Edhe në WAN zakonisht duhet të transmetohen të dhëna midis rrjeteve të ndryshme. Në këtë mënyrë lind nevoja e përdorimit të protokolleve të njohura të rrjetit si IP dhe IPX.

Më poshtë do të paraqiten shkurt vetëm shërbimet WAN. Në këtë mënyrë do të jepet vetëm një vështrim i përgjithshëm i tyre. Listimi i protokolleve të veçanta, të cilat përmbushin detyra të ndryshme në sfond, e kapërcen kornizën e këtij vështrimi të përgjithshëm.

Familjet e sotme të protokolleve WAN

Protokolli	Përshkrimi
Asynchronous Transfer Mode (ATM)	Me ATM bëhet fjalë për një shërbim të shpejtësisë së lartë në transmetimin e të dhënave, i cili përdoret në fushën e LAN-Backbone, në rrjetet e telefonisë, në Internet, si dhe tek lidhjet e dedikuara. Në rrjetin ATM krijohet një lidhje virtuale midis sistemeve fundore, nëpërmjet një fluksi konstant prej 53 Byte „big cells" të mund të transmetohen të dhëna nga aplikacione të ndryshme. Në këtë mënyrë përdoren shpejtësi të ndryshme transmetimi.
Frame Relay	Frame Relay u zhvillua si shërbim për ISDN-në dhe përbën gjithashtu një shërbim të shpejtësisë së lartë në transmetimin e të dhënave në fushën e WAN-eve. Ai është një proces "packet-switching", gjë që do të thotë se të dhënat transmetohen nëpërmjet linjave virtuale sipas adresës së destinacionit. Madhësia e të dhënave të transmetuara është e ndryshme.
Integrated Services Digital Network (ISDN)	Shërbimi telefonik dixhital ISDN luan edhe në rrjete një rol domethënës për lidhjet WAN. Këtu krahas linjave për dial-up futen edhe linjat fikse. Ndryshe nga shërbimet e përmendura më parë këtu përballohen vetëm shpejtësi të ulta. ISDN-ja, të paktën në Gjermani, është shërbimi WAN më i përhapur. Të dhënat, të cilat do të transmetohen përmes shërbimit ISDN, si rregull duhet të kapsulohen. Ky proces kryhet nëpërmjet protokolleve të ndryshme si p.sh. PPP, L2TP ose PPTP.
Digital Subscriber Line (DSL)	DSL-ja po gëzon një popullaritet në rritje. Ky popullaritet para së gjithash është në rritje për lidhjet e Internetit në shtëpi (për konsumatorët privatë). Këtu më shumë përdoret shërbimi Asymetric DSL (ADSL), i cili ofron përkundrejt një fluksi të lartë download-imi (download-rate) një fluks të ulët upload-imi (upload-rate). Në rrjetet e firmave përdoret kryesisht shërbimi Symetric DSL (SDSL). Një nga arsyet kryesore për përhapjen e gjerë të shërbimit DSL është, se DSL mundëson të shfrytëzohet kabllimi i rrjeteve ekzistuese për transmetime të dhënash me shpejtësi të larta dukę mbajtur për kalimin në këtë shërbim kosto relativisht të ulta. Bashkë me DSL-në shpesh ndeshim një emërtim të gabuar, kur bëhet fjalë për modemat DSL. Në të vërtetë bëhet fjalë për një modem DSL zakonisht me një ATM-Bridge.

Shënime

6.5 Protokolle të reja në kufijtë midis WAN-it dhe LAN-it

Nevoja në rritje për gjerësi bande në LAN

Me rritjen konstante të nevojës për gjerësi bande në rrjetet lokale gjithmonë e më shumë teknika të zbatuara në fushën e WAN-it po zbatohen atë të LAN-it. Kjo shkakton disa probleme, pasi komunikimi midis rrjeteve shfaq përgjithësisht një sjellje tjetër krahasuar me komunikimin në LAN. Arsyeja për nevojat në rritje për gjerësi bande janë para së gjithash sasitë gjithnjë e më të mëdha të të dhënave, që përdoren nga aplikacionet e sotme dhe veçanërisht tendenca për "zbukurimet" multimediale të dokumentave. Për ta ilustruar këtë fakt mjafton të krahasojmë madhësinë e një dokumenti në Power Point me një dokument thjesht tekst, gjë që qartëson idenë se përse sot shpejtësitë e transmetimit në rrjet prej 10 Mbit/s nuk janë më të mjaftueshme.

LANE

Një nga teknikat që po gjen zbatim gjithmonë e më shumë tek LAN-et është ATM-LAN-Emulation (ATM-LANE). Bëhet fjalë për simulimin qarkullimin pothuajse pa lidhje dhe strategjitë e rezolucionit të emrave të rrjeteve lokale në një media të orientuar nga lidhja (connection oriented media).

Zbatimi i kësaj teknike kërkon funksionalitete plotësisht të reja rrjeti, të cilat pasqyrojnë veçoritë e LAN-it në rrjetin ATM. Këtu futen teknologjitë e reja për serverat, si p.sh. broadcast-emulators over ATM.

Nevoja në rritje për adresa

Një aspekt tjetër, i cili ka të bëjë si me fushën e LAN-it, ashtu edhe me atë të WAN-it (e veçanërisht me Internet-in), është nevoja në rritje e adresave të vlefshme të IP-së, nevojë e cila duhet të plotësohet nëpërmjet kalimit nga Ipv4 në Ipv6. Nëpërmjet transformimit të adresave nga 32 Bit (Ipv4) në 128 Bit (Ipv6) ky problem duhet të zgjidhet.

Në rast se para pak vitesh në shumicën e firmave kishte vetëm një duzinë kompjuterash në punë, shumë prej të cilëve pa lidhje në rrjet, sot zor se mund të gjendet një zyrë, në të cilën të mos nevojitet një rrjet i pajisur me servera, lidhje në Internet, mail-server dhe dial-in server.

Kjo gjë çon pashmangshmërisht në implementimin e Ipv6-ës dhe kërkon sërish rritjen e gjerësisë së bandës, pasi Header-i i Ipv6ës është shumëfish më i madh se ai i Ipv4-ës.

Nevoja për siguri

Në botën e sotme të biznesit përpunimi elektronik i të dhënave përbën një mjet të rëndësishëm në infrastrukturën e informacionit dhe në një masë gjithmonë e më të madhe luan një rol të fuqishëm në proceset private të komunikimit. Kur të dhënat kritike të firmave aksesohen nëpërmjet lidhjeve WAN, si dhe një pjesë e madhe e korrespondencës së saj bëhet nëpërmjet e-mail-it, tema e sigurisë merr një kuptim gjithnjë e më domethënës.

Në rast se para pak vitesh zor se gjeje ndonjë kompjuter të pajisur me antivirus, sot madje dhe individët privatë duhet të merren me konfigurimin e firewall-it, filtrave të spam-it dhe të software-ve të tjera mbrojtëse. Në fushën e kontrollit të aksesit përmes lidhjeve WAN po gjejnë gjithmonë e më shumë përdorim mekanizma autentifikimi si RADIUS-i të lidhura me certifikata dhe gjeneratorë fjalëkalimesh të njëhershme. Me përhapjen e shpejtë të WLAN-it kodimi i të dhënave, si dhe transmetimi i mbrojtur dhe i sigurtë i tyre po fitojnë gjithnjë e më shumë terren. Mënyrat e kodimit zor se mund të jenë të qarta për përdoruesit e thjeshtë për shkak të një numri të madh faktorësh – si p.sh. gjatësitë e çelsave, algoritmet e përdorura dhe jetëgjatësia e çelsave. Në të njëjtën kohë edhe metodat e sulmeve bëhen gjithmonë e më të sofistikuara, gjë që çon në një lloj "gare armatimi".

Fusha e sigurisë së rrjetit, preket pak në këtë libër, por sidoqoftë çdo specialist i IT-së duhet të jetë i ndërgjegjshëm për mprehtësinë e çështjes, si dhe të ndërgjegjësojë kolegët e punës dhe të njohurit në lidhje me këtë temë. Mbrojtja e e-mail-eve nëpërmjet Private Key Infrastructure nuk përbën më luks, por është guri bazë i një sjelljeje të përgjegjshme dhe të ndërgjegjshme në punën me kompjuter. Kush dërgon të dhënat e kartës së tij të kreditit përmes linjave të pasigurta, duket sikur kërkon vetë keqpërdorimin e këtij informacioni. Kundërmasa, në këtë rast kodimi (p.sh. nëpërmjet IPSec), e rrit sigurinë dhe detyron përdoruesin, ashtu si në fusha të tjera, që krahas kërkesave të sistemit të marrë në konsideratë edhe kornizat ligjore respektive.

Transmetimi i sinjaleve nëpërmjet valëve

Në LAN-et e sotme gjejmë gjithmonë e më shpesh format mikse të përdorimit të teknikave të transmetimit me dhe pa kabëll. Deri para pak vitesh, lidhjet valore përdoreshin para së gjithash për lidhjen në rrjet të ndërtesave, ndërsa sot për arsye konfortabiliteti dhe mobiliteti, edhe laptop-ët (notebooks) janë pajisur me karta rrjeti wireless (W-LAN adapter). Nga ana tjetër, përdorimi i Bluetooth-i po gjen gjithnjë e më tepër përhapje.

Meqë gjithmonë e më shumë pajisje mobile – si p.sh. telefonat celularë dhe organizer-at – po sinkronizohen me kompjuterat, është e pritshme që kjo tendencë për komunikim valor të forcohet edhe më shumë. Meqë bandat e frekuencave, të cilat mund të përdoren për transmetimin e të dhënave janë të kufizuara, parashikohen konflikte ndërmjet pajisjeve. Në firmat e mëdha vihet re që rrjetet pa kabëll (valore) janë shpesh të mbingarkuara dhe mund të ndodhë që gjatë orarit të punës, përdoruesit të mos indentifikohen dot në rrjet (nuk logohen dot).

Epilog

Implementimi i IP-ve në rrjetet lokale, apo i DNS-së në Intranet, është importim i teknikave të WAN-it nga Interneti në rrjetet lokale duke bërë në këtë mënyrë që teknikat klasike të LAN-it si NetBEUI, ose NetBIOS, të cilat ishin dukshëm më efikase në rrjetet e vogla, të spostohen.
Kjo tendencë do të forcohet në të ardhmen, dhe është vetëm çështje kohe, kur rrjetet e pa orientuara nga lidhja (not connection oriented) të zëvendësohen komplet nëpërmjet linjave virtuale të dedikuara të orientuara nga lidhja (connection oriented) . Një shembull konkret për këtë tendencë është përdorimi i Layer3-Switches, tek të cilat çdo porte i caktohet një adresë IP-je statike.

Shënime

7 Procedurat e aksesimit të LAN-it

Në këtë kapitull do të lexoni

→ si përcaktohet teknologjia Ethernet
→ si përcaktohet Gigabit-Ethernet-i
→ si është ndërtuar një modul Gigabit Interface Converter (GBIC)
→ si është ndërtuar procedura e aksesit në rrjetet Token-Ring

Kusht paraprak

✓ Njohuri mbi modelin ISO/OSI

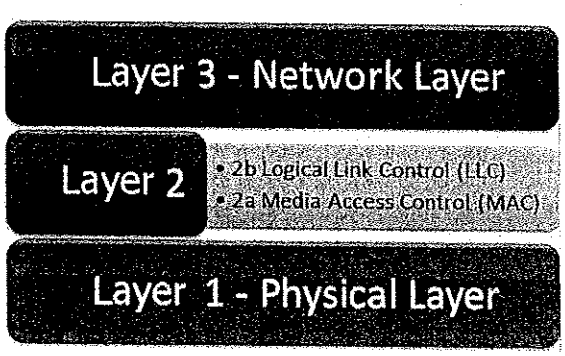
7.1 Teknologjia Ethernet

Vështrim historik

Parimi bazë i Ethernetit e ka zanafillën në një projekt të Universitetit të Hawait në fillimin e viteve 70. Krahas sistemeve të radiopërhapjes ALOHA u zhvilluan parimet e reja të transmetimit, të cilat më vonë morën kuptim të rëndësishëm edhe për Ethernetin: menaxhimi i përplasjeve (collisions) dhe transmetimi i paketave me të dhëna (frames). Këtu kuptohet transmetimi i të dhënave, të disa stacioneve në rrjet, nëpërmjet një kanali të përbashkët transmetimi.

Në vitin 1972 Xerox filloi me vënien në punë të një sistemi eksperimental Ethernet-i. Shtatë vjet më vonë DIX-Group (DEC, Intel dhe Xerox) zhvilloi një konfigurim të standardizueshëm Ethernet-i, 10MBit/s-. Ky u publikua nga IEEE në vitin 1982, i quajtur ndryshe si standardi 802.3 për 10Base5. Njohja në mbarë botën e standardeve të Ethernetit u bë në vitin 1985. Rreth dy vjet më vonë dolën në treg produktet e para Twisted–Pair dhe Multiprotocol-Router. Standardizimi i Ethernetit për kabllot Twisted-Pair (10BaseT) u bë në vitin 1991. Vetëm një vit më vonë u publikua standardi Ethernet për fibrat optike.

Arkitektura e specifikuar nga seksioni 802 i IEEE-së, për standardin e Ethernetit (10Base5), bazohet në caktimin e funksioneve të dy shtresave të poshtme të modelit të referencës OSI.



Për Ethernetin janë domethënës paragrafët 802.1, 802.2 dhe 802.3. Në specifikimin sipas 802.1 dhe 802.2 gjenden përcaktime të përgjithshme të arkitekturës së LAN-it dhe Logical Link Control (LLC).

Në specifikimin 802.3 përcaktohet aksesi në median fizike (Media Access Control = Shtresa MAC) për rrjetet bus me CSMA/CD (Carrier Sense Multiple Access with Collision Detect). Standardi Ethernet, sipas këtij specifikimi, është përcaktuar si rrjet Bus, i cili punon sipas procedurës CSMA/CD.

IEEE 802.2 (= LLC [Logical Link Control] - pjesë e shtresës 2)

Pjesa LLC e shtresës Data Link Layer (Shresa 2) përbën pjesën e sipërme të saj në modelin OSI, e cila kontrollon transmetimin e të dhënave tek shtresa 3. Ajo përmbledh proceset e adresimit të sistemit dhe kontrollit të gabimeve si dhe përshkruan specifikimet e pjesmarrësit, ndërfaqen MAC të protokollit LLC.

LLC përcakton seksionin logjik (SAP = Service Access Points) dhe kujdeset për krijimin e lidhjes midis dy stacioneve në rrjet (LAN). Standardi 802.2 përcakton klasat e ndryshme LLC:

☑ Lloji I (shërbim i pakonfirmuar pa lidhje)

Informacioni dërgohet nga Data Link Layer-i (Shtresa 2) tek marrësi, pa e informuar dërguesin. Në rast se të dhënat nuk do të mund të arrijnë tek marrësi, atëherë duhet që në shtresat më të larta, p.sh. Application Layer, të gjenerohet një njoftim për dërguesin.

☑ Lloji II (shërbim i orientuar nga lidhja)

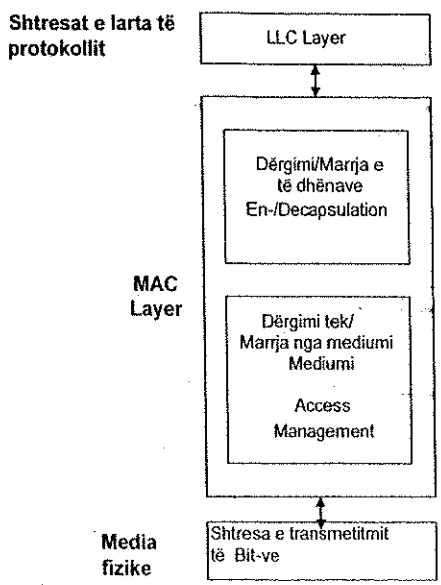
Paketat e transmetuara me të dhëna konfirmohen nga dërguesi dhe në rast gabimi transmetohen sërish.

☑ Lloji III (shërbim i konfirmuar pa lidhje)

Të gjitha datagramet duhen konfirmuar nga marrësi.

Pjesa e shtresës MAC (Media Access Control)

Pjesa MAC e shtresës komunikon direkt me kartën e rrjetit dhe është përgjegjëse për transmetimin pa gabime të të dhënave midis kompjuterit dhe rrjetit.



Pjesa MAC e shtresës

Ajo formon një vend tranzitimi midis protokolleve më të larta dhe shtresës fizike të transmetimit të Biteve. Ajo kryen shërbimet e mëposhtme:

☑ Përgatitja e frame-ve për dërgim / marrje

☑ "Dorëzimi" i frame-ve në medium për dërgim me rregullim të aksesit (Access Management)

Përgatitja e Frame-ve

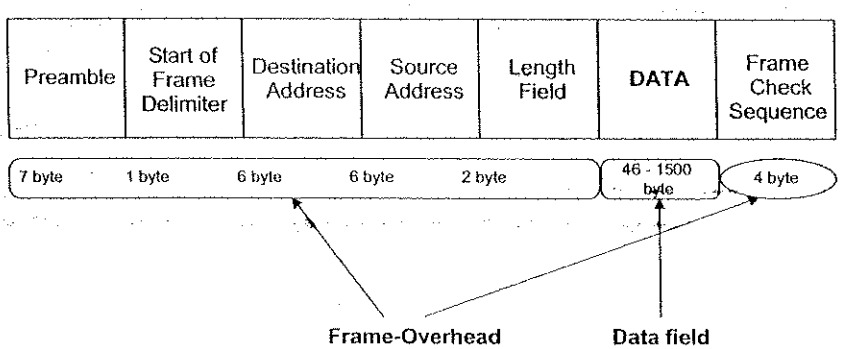
Për dërgim (Data Encapsulation)

☑ Nga shtresa LLC merret një datagram.

☑ Përmes krijimit të një Frame-I, formohet një paketë e përshtatshme.

☑ Nga paketa e formuar krijohet një shumë kontrolli (checksum).

☑ Paketa me të dhëna tranferohet tek moduli i dërgimit të MAC-ut, në të cilin ai e transformon atë në një fluks të dhënash të njëpasnjëshme për dërgim në shtresën fizike (physical layer).



Ndërtimi i Frame-eve

Për marrje (Data Decapsulation)

Tek Ethernet-i paketat me të dhëna dërgohen në të gjitha stacionet e punës në rrjet në formë broadcasti. Në varësi të adresës së marrësit, çdo stacion përcakton vetë, nëse paketa e marrë me të dhëna i përket atij apo jo. Vetëm paketa të tilla me të dhëna do të përpunohen më tej nga stacioni i punës.

☑ Në varësi nga shuma e kontrollit, provohet nëse paketa e marrë me të dhëna ka arritur e plotë apo jo.

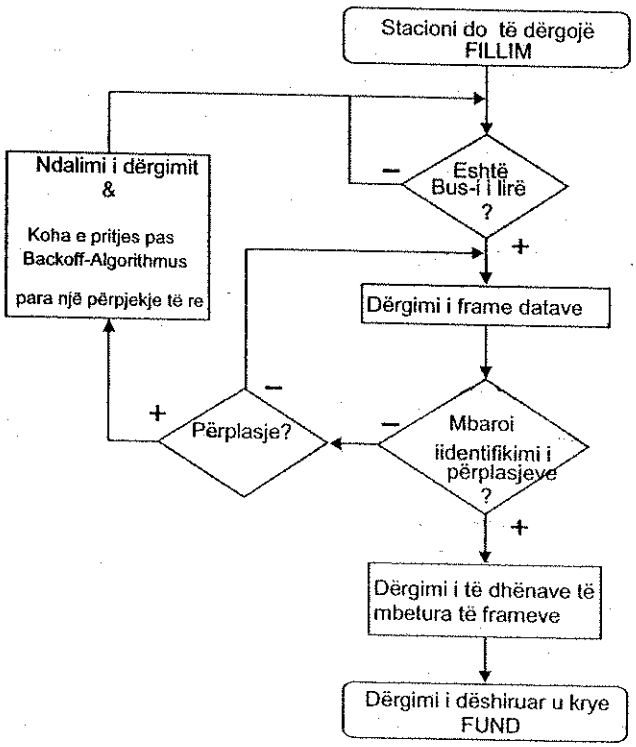
☑ Nëpërmjet një pakete të vlefshme, filtrohen të dhënat e shfrytëzueshme nga data-frame-t.

☑ Fusha me të dhënat e shfrytëzueshme duhet të jetë midis 46 dhe 1500 Bytes e gjatë. Më tej, sasia e të dhënave duhet të jetë shumëfish i 8 Bit-shit. Në rast se gjenden gabime, paketa fshihet.

☑ Një fushë të dhënash pa gabime transferohet tek shtresa LLC.

Transferimi i paketave me të dhëna në shtresën fizike (medium) me CSMA/CD

Ethernet-i emërtohet ndryshe edhe si shared-media, apo shared-bandwidth-architecture. Të gjitha stacionet e punës janë të lidhura në të njëjtin Bus dhe shfrytëzojnë bashkërisht gjerësinë ekzistuese te bandës së transmetimit. Shtresa e protokollit Medium Access Control (MAC) është përgjegjëse, që të parandalojë që disa stacione të tentojnë njëkohësisht të transferojnë të dhëna në media. Për këtë qëllim, nga Ethernet-i përdoret procesi i aksesimit i quajtur Carrier Sense Multiple Access with Collision Detection (CSMA/CD).



Bllok – skema e rrjedhës së procesit CSMA/CD

Stacioni fillimisht kontrollon, nëse Bus-i është i lirë, apo po përdoret ndërkohë nga një stacion tjetër. (Carrier Sense). Në rast se në Bus po kryhet një transmetim të dhënash, atëherë kontrolli do të kryhet sërish pak kohë më pas.

Në rast se Bus-i është i lirë, stacioni fillon të dërgojë të dhënat e veta. Megjithatë, nuk mund të përjashtohen përplasjet gjatë dërgimit të njëkohshëm të dy stacioneve, p.sh. në rastet e mëposhtme:

- ☑ Të dy stacionet kanë marrë pothuaj në të njëjtën kohë një kërkesë për dërgim. Në këtë mënyrë ata kontrollojnë në të njëjtën kohë, nëse Bus-i është i lirë. Marrim rastin që Bus-i është i lirë, kështu që të dy stacionet fillojnë të dërgojnë të dhëna në të njëjtën kohë, gjë që çon në përplasje (collision).
- ☑ Stacionet kanë largësi të madhe nga njëri-tjetri referuar gjatësisë totale të Bus-it. Duke konsideruar kohën që i duhet sinjalit për të lëvizur në kabëll (tek kabllot e bakrit rreth. 200.000 km/s) duket sikur Bus-i është i lirë. Në të vërtetë, në fundin tjetër të busit, një tjetër stacion sapo ka filluar të dërgojë të dhëna.

Në raste të tilla disa stacione dërgojnë njëkohësisht të dhëna në median e transmetimit që shfrytëzohet bashkërisht (Multiple Access). Kjo gjë çon në përplasje (collisions). Stacionet e veçanta duhet t'i zbulojnë përplasje të tilla dhe të testojnë dërgesat e tyre. Në rast së ndodhin përplasje, procesi i dërgimit ndërpritet menjëherë (collision detect). Pas një kohe pritje të caktuar, stacioni provon sërish t'i dërgojë të dhënat.

Mekanizmi i identifikimit të përplasjeve nuk përdoret gjatë gjithë kohës së transmetimit. Tek rrjetet 10/100-MBit/s-ky kontroll kryhet vetëm për transferimin e 576 Biteve të para. Këtu bëhet fjalë për 576 bit-time. Kjo vlerë llogaritet nga framet më të vogla të mundshme me madhësi 64 Byte = 512 Bit duke shtuar këtu edhe një kohë bllokimi transmetimi për identifikimin e përplasjeve. Tek rrjetet 1-GBit/s kjo vlerë nuk është më e vlefshme. Për këtë qëllim, vlera minimale e frame-it rritet në 512 Byte. Gjatë kohës që një stacion kryen identifikim përplasje, atëhere periudha kohore e dërgimit zgjatet.

Sipas identifikimit të përplasjeve të përshkruar më lart, stacioni mund t'i dërgojë të dhënat e mbetura në formë frame-sh pa kontroll të mëtejshëm. Të gjitha stacionet në rrjet e kanë identifikuar që bus-i është i zënë. Në rast të kundërt, duke qenë se:

- ☑ shtrirja maksimale e busit është shumë e madhe
- ☑ janë bashkuar shumë segmente rrjeti me njëra-tjetrën nëpërmjet Repeaterave/Hubeve

atëhere sërish do të kemi përplasje, të ashtuquajturat Late Collisions (përplasjet e vona). Këto përplasje nuk identifikohen më nga stacioni dërgues dhe mund të korrigjohen vetëm nga nivetet e larta të protokolleve (p. sh. shtresa 4 e një protokolli të orientuar nga lidhja).

7.2 Specifikimi Gigabit

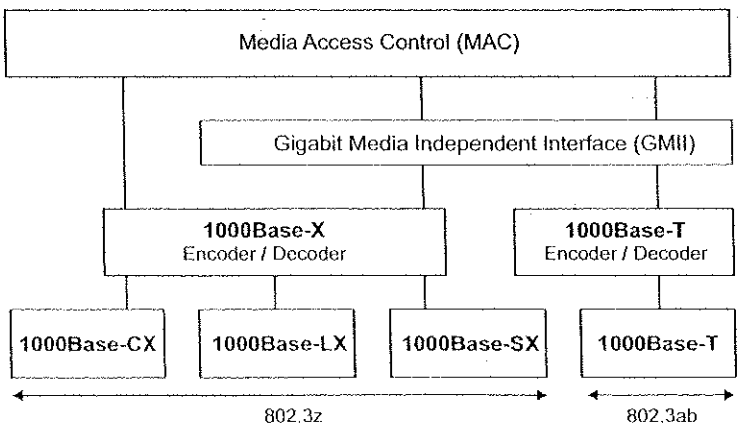
Aspekti historik i Gigabit-Ethernet-it

Gigabit-Ethernet-i mundëson dhjetëfishimin e fluksit të të dhënave të teknologjisë Fast-Ethernet me shpejtësi transmetimi prej 1 GBit/s. Për këtë qëllim, në vitin 1995, u ngritën dy grupe pune speciale (802.3z dhe 802.3ab). Përdorimi i kësaj teknologjie është veçanërisht interesant tek LAN-Backbones.

Gigabit-Ethernet-i është kompatibël me formatin ekzistues Ethernet 802.3 si dhe është në gjendje, që të përdorë procesin e aksesimit CSMA/CD. Format e frame-ve sipas 802.3 dhe kufizimet e gjatësisë së frame-ve midis 64 Byte dhe 1.518 Byte mbeten ato ekzistueset. Gigabit-Ethernet-i mbështet topologjinë yll me të gjitha rekomandimet për mediat e transmetimit që jepen në standardet e kabllimit ISO 11801. Kështu, grupi i punës 802.3z zhvilloi standardet për fibrat monomode, fibrat multimode dhe kabllin STP. Grupi i punës 802.3ab u përqëndrua në standardizimin e Gigabit-Ethernet-it tek kabllot UTP në fushën e realizimit të lidhjeve.

Kategoria 5 e kabllit UTP, përdoret në rastet që e kanë gjatësinë e lejuar të lidhjes deri në 100 m. Kabllot e kategorive 6 dhe 7 nuk janë parashikuar në standard, por sidoqoftë rekomandohen. Normat për arkitekturën Gigabit-Ethernet përshkruajnë standardin bazë dhe ndryshimet në proceset CSMA/CD. Ndryshimet i referohen vetëm shpejtësive të mëdha. Në parim dallojmë katër teknologji:

- ☑ 1000Base-LX
- ☑ 1000Base-SX
- ☑ 1000Base-CX
- ☑ 1000Base-T



Arkitektura e Gigabit-Ethernet-it

1000Base-LX

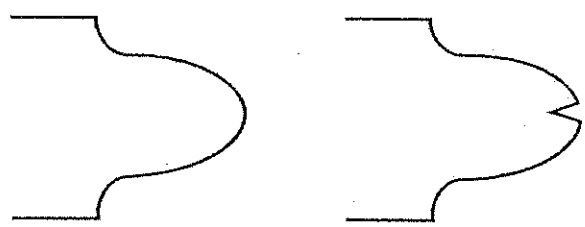
1000Base-LX është një variant i Gigabit-Ethernet, i cili përdoret tek kabllot me fibra optike me një gjatësi vale të gjatë. Këtu gërma L i korrespondon Long Wavelength. Në këtë rast përdoret një lazer me gjatësi vale mesatare prej 1300 nm (nga 1270 nm deri 1355 nm). Gjithashtu, këtu mund të përdoren si fibrat multimode, ashtu edhe ato monomode (singlemode). Rrezet e distancave që mbulojnë ndryshojnë. Me fibrat multimode 62,5 μm dhe 50 μm kapërcehet një distancë prej 550 m. Tek fibrat monomode rrezja e mbullimit arrin 3 km. Këtu duhet marrë parasysh, që bëhet fjalë për lidhjet Point-to-Point në Full-Duplex pa CSMA/CD. Të specifikuara më tej janë performancat e transmetimit optik me -3 dBm, performancat minimale të transmetimit optik me -11,5 dBm dhe performancën në marrje -3 dBm. Si adaptor, në të gjitha variantet, përdoret Duplex-SC.

1000Base-SX

Ky variant i Gigabit-Ethernet-it i ngjan variantit LX. Sidoqoftë, këtu përdoret një lazer me gjatësi vale të shkurtër (short wavelength). Me lazer 850-nm, në praktikë në varësi nga diametri i fibrave optikë multimode, arrihen distanca nga 270 m (62,5 μm) në 550 m (50 μm). Në distanca të tilla duhet marrë parasysh, së bëhet fjalë për një lidhje Point-to-Point me Full-Duplex pa CSMA/CD, si në rastin e 1000Base-LX. Performanca mesatare e transmetimit optik është specifikuar me 0 dBm, në mënyrë të ngjashme me performancën mesatare marrëse. 1000Base-SX përdor si adaptor Duplex-SC-në.

Probleme tek 1000Base-LX dhe 1000Base-SX

Gjatë përdorimit të kabllove LWC me kabllo me fibra multimode mund të ndeshen gabime gjatë transmetimit. Tek disa fibra multimode mbizotërojnë grupe të caktuara variantesh, në rastet kur si burim drite përdoret rrezja lazer. Çdo fibër optike mund të drejtojë vetëm një numër të kufizuar variantesh. Në varësi nga këndi, në të cilin rrezja e dritës pasqyrohet në fibër, ekzistojnë ndryshime në kohëzgjatje në transmetim midis varianteve të veçanta. Me qëllim që të balancohen këto ndryshime, fibrat përdoren me profil këndor. Indeksi refraktar i profilit këndor zvogëlohet duke filluar nga qendra deri tek mbështjella e fibrës.



Profil refraktar me indeks këndor ideal dhe me çarje

Në kushte ideale, fibra ka një profil refraktar të "lëmuar", nëpërmjet së cilës balancohen ndryshimet e kohëzgjatjes së transmetimit. Në rast se profili ka një çarje, kjo mund të çojë në deformime të impulseve.

Nëpërmjet "conditional launching – lëshimit të kushtëzuar" mundësohet një stimulim i balancuar për të gjitha variantet e fibrave optike. Modulet kompensuese (mode conditioner) përdoren tek 1000Base-SX (transceivers) dhe nga jashtë (extern) tek 1000Base-LX (patch cords).

1000Base-CX

Varianti CX është standardizuar me 150 Ohm për Gigabit-Ethernet me (over) Twinax-Cable. Varianti 1000Base-CX është i përshtatshëm për lidhjen e pajisjeve fundore në një largësi prej 25 metrash. Për shkak të rrezes relativisht të shkurtër të mbulimit, përdorimi i Gigabit-Ethernet-it me kabëll bakri përfaqëson vetëm një zgjidhje të përkohshme.

1000Base-T

1000Base-T paraqet standardizimin e teknologjisë Gigabit-Ethernet me kabëll bakri të kategorisë 5 (CAT 5) me mundësi lidhjeje me një gjatësi 100 m. Shtresa e MAC-ut qëndron e pandryshuar deri në shpejtësitë më të larta, perkundrejt varianteve klasike të Ethernet-it 10-Mbit/s dhe 100-Mbit/s (Fast-Ethernet). Parimet bazë të 1000Base-T e kanë origjinën në teknikën 100Base-T2 - 100 MBit/s (me kabllot e kategorisë 3 (CAT 3) punohet me dy çifte të përdredhura të kabllit). Tek teknika 1000Base-T punohet me të katra çiftet e përdredhura të kabllit.

Për transmetimin e 1 Gbit/s në Fullduplex-Modus është e nevojshmë, që çdo çift i përdredhur të transmetojë në çdo drejtim 250 Mbit/s. Sipas specifikimeve, kjo shpejtësi për kabllot e kategorisë 5 është tepër e lartë. Standardi përshkruan një gjerësi bande prej 100 MHz. Këto shpejtësi të larta transmetimi kanë efekt negativ duke shkaktuar të ashtuquajturin „cross talk" (interferencë në transmetim) midis çifteve të përdredhura të përcjellësve. Standardi 1000Base-T i merr parasysh këto kufizime dhe parashikon një Forward Error Correction (procedurë të korrigjimit të gabimit).

Me qëllim që të zgjidhet problemi i trunkimit (trunking - lidhja paralele e disa ethernet-links), integrohet një Link-Aggregation-Layer – Shtresa e Agregimit të Lidhjes (Link-Bundling). Kjo shtresë futet midis niveleve të larta të protokolleve ose të LLC-së. Nëpërmjet saj mundësohet, që të punohet paralelisht me disa kolona MAC-u. Në këtë mënyrë arrihet një redundancë e mirë linje, pasi në rast se bie një linjë atëhere mund të vazhdohet puna me linjën rezervë, megjithëse me kapacitet më të ulët. Me këtë funksion arrihet një shkallëzim i trashë i gjerësisë së bandës.

Kufizimet në transmetimin e fluksit maksimal të të dhënave

Faktor frenues për arritjen e fluksit maksimal të të dhënve prej 1 GBit/s përbëjnë karakteristikat elektrike të kabllove TP (twisted pair). Nuk është e mundur që në një kabëll TP të transmetohen të dhëna me një fluks infinit. Një nga kriteret më të rëndësishme të deritanishme që përcaktojnë cilësinë është humbja, ku dallojmë humbjet nga interferencat në afërsi dhe largësi (close cross talk-- dhe remote cross talk).

Meqë tek 1000Base-T të dhënat transmetohen njëkohësisht tek të gjitha çiftet e përdredhura, çdo çift ka fqinjë tri çifte të tjera. Këto shkaktojnë interferencë të sinjalit. Parregullsitë në kabëll sjellin me vete (p. sh. rritje të rezitencave në transmetim) reflektime, të cilat i mbivendosen sinjalit. Shkak për këtë mund të jetë konfeksionimi i keq i kabllit, ose përdorimi i elementeve lidhës me cilësi të dobët. Si kriter vlerësimi merret fluksi i kthimit të humbjeve, i cili ndikon ndaj reflektimit. Sa më i lartë të jetë ky fluks, aq më i mirë është kablli. Një shkallë më e lartë e kthimit të fluksit të humbjeve bën që sinjali i reflektuar të jetë më i dobët.

Konfeksionimi i keq i kabllit (p. sh. heqja e përdredhjes së fijeve tek priza lidhëse), mund të ndikojë shumë negativisht në karakteristikat elektrike të kabllit.

Procedura e kodimit

Tek Gigabit-Ethernet-i çdo 8 ns (125 MHz), shtresës fizike-Physical Layer (PHY), nëpërmjet GMII-së (Gigabit Media Independent Interface-Ndërfaqja e Pavarur Gigabitshe e Medias), i transferohet një e dhënë me gjatësi 8 Bit. Kjo e fundit, presupozon $2^8 = 256$ kombinime të ndryshme bitesh. Me qëllim që të mund të transmetohen pa humbje të gjitha kombinimet, duhet përdorur një procedurë kodimi, e cila ofron minimumi 256 kombinime simbolesh të ndryshme.

Një kodim në tri nivele, si tek 100Base-TX, do të mundësonte në të katër çiftet vetëm $3^4 = 81$ kombinime simbolesh të transmetueshme. Ndërsa në rastin e një procedure kodimi në katër nivele do të ishin vetëm $4^4 = 256$ kombinime simbolesh, të cilat do të mjaftonin për transmetimin e të dhënave, por jo për transmetimin e informacioneve të kontrollit. Procedura e kodimit me pesë nivele (PAM5), e cila u zhvillua enkas për 1000Base-T, mundëson 625 kombinime simbolesh, nga të cilat 113 përdoren për kontrollin dhe identifikimin e gabimeve.

Për çdo periode 125-MHz GMII transferon 8 Bite, të cilat i përkasin një kombinimi të mundshëm prej 256 Bitesh. Kodimi PAM5 krijon nga kjo një kombinim simbolesh, të cilat transferohen gjatë periodës në fjalë nëpërmjet të katër çifteve të përdredhura të kabllit. Në këtë mënyrë, për çdo çift transmetohen dy bite. Referuar fluksit të të dhënave, në rastin e përdorimit të katër çifteve të përdredura dhe transmetimit të 2 Biteve për periodë, rezulton një faktor ndarës 4 x 2 = 8. Kjo çon në një fluks të dhënash prej 1000 MBit/s për një fluks transmetimi 125 MBit/s për çift, i cili i korrespondon 100Base-TX.

Shënime

7.3 Gigabit Interface Converter (GBIC)

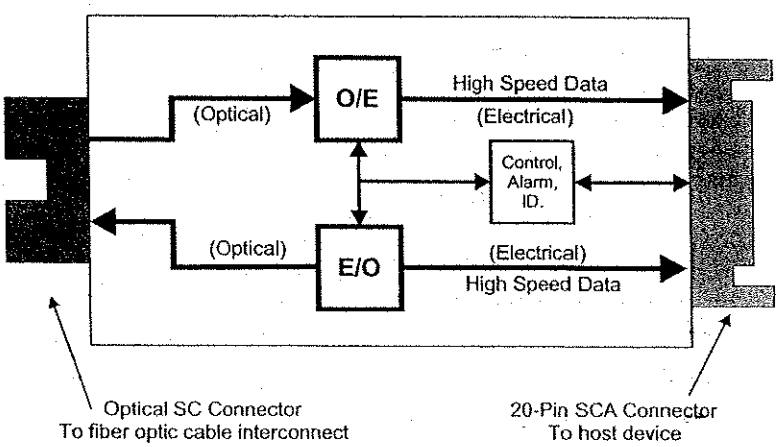
Moduli GBIC (Moduli Konvertues i Ndërfaqes Gigabitshe)

Përfshirja e shtresës fizike të Fibre Channel (FC-PH), si pjesë e specifikimit (IEEE 802.3z) të Gigabit-Ethernet-it (GE), ka kontribuar dukshëm në përhapjen e protokolleve të Fibre-Channel (teknika e transmetimit në shpejtësi të mëdha). Si FC-ja ashtu edhe GE-ja lejojnë përdorimin e mediave të ndryshme fizike si kablli UTP apo fibrat optike. Me qëllim që të thjeshtohej zhvillimi dhe implementimi i pajisjeve të sistemeve FC dhe GE, nga komiteti i Small-Form-Factor (SFF) u përcaktua një standard, i cili njihet si moduli Gigabit Interface Converter (GBIC) – moduli Konvertues i Ndërfaqes Gigabitshe.

Në nivelin më të thjeshtë moduli GBIC është një Fullduplex-Data-Transceiver (dërgues dhe marrës) me dy porta të dhënash.

Njëra nga portat është parashikuar për të dhënat që transferohen në mënyrë optike dhe mund të implementohet si konektor (lidhës) Duplex-SC. Porta tjetër shërben për rezervimin e sinjaleve elektrike dhe është implementuar si konektor 20-Pin-SCA. Kjo anë e modulit GBIC lidhet me pajisjen Host dhe përpunon sinjalet elektrike si kontrolli, alarmi, identifikimi i modulit dhe të dhënat seriale në formë impulsesh të shpejta elektrike. Me përdorimin e këtyre dy portave, GBIC konverton njëkohësisht të dhënat nga forma elektrike në optike (E/O) dhe anasjelltas, nga optike në elektrike (O/E).

Moduli GBIC



Modul GBIC

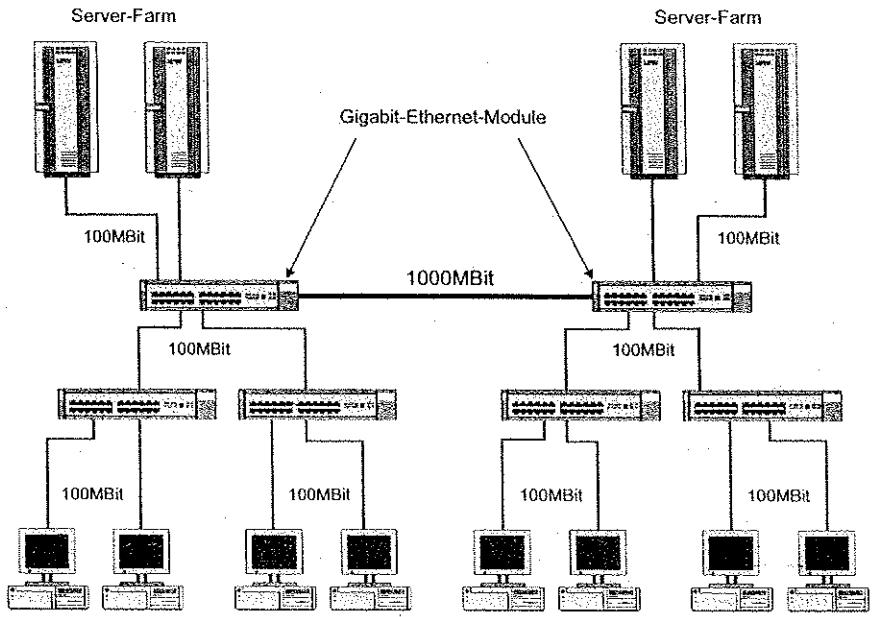
Duke marrë parasysh konformitetin e FC-PH për modulet GBIC, këto të fundit janë të përshtatshme jo vetëm për sistemet FC, por edhe për sistemet GE, si dhe për aplikacione të tjera të vetë firmave, të cilat kanë nevojë për linja transmetimi seriale me gjerësi bande të madhe.

Modulet GBIC specifikohen si komponentë "hot plug". Kjo do të thotë, që modulet mund të vendosen, apo të hiqen nga një pajisje Host, pa qenë nevoja që pajisja të fiket. Kjo karakteristikë është e rëndësishme veçanërisht tek pajisje si hubet, apo switchet në rrjet, shkëputja nga puna e të cilave (down-time) nuk është aspak e dëshirueshme. Karakteri "hot plug" i moduleve GBIC thjeshtëzon upgrade-t dhe mirëmbajtjen pa shkëputje nga puna të pajisjes.

7.4 Shembuj konfigurimi

Upgrade-i i lidhjeve Switch-to-Switch

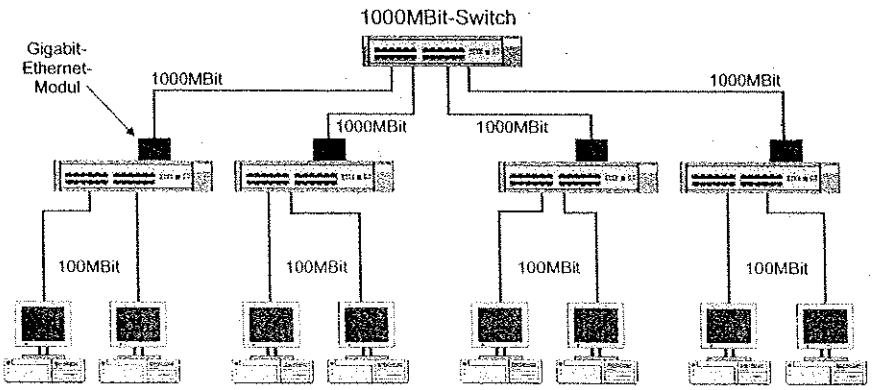
Nëpërmjet përdorimit të teknologjisë Gigabit-Ethernet, shpejtësia e lidhjes së switcheve 100-MBits rritet 10 herë. Gjerësia e bandës në dispozicion të lidhjes switch-to-switch mundëson komunikimin me njëri-tjetrin, nëpërmjet Backbone-it, të një numri dukshëm më të madh pajisjesh fundore, pa kufizim performance.



Lidhja Switch-to-Switch me Gigabit Ethernet

Upgrade-i i një Fast-Ethernet-Backbone

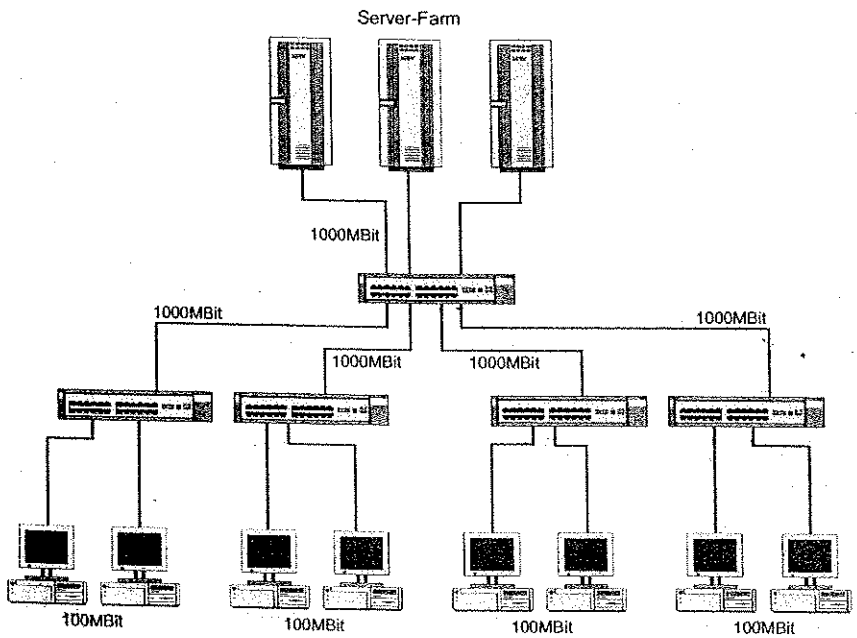
Switchet 10/100-Ethernet, të lidhura me Backbone-in, zëvendësohen me switche Gigabit-Ethernet. Sistemet modulare mund të pajisen më mirë dhe pa probleme nëpërmjet përdorimit të moduleve përkatëse Gigabitshe.



Upgrade-i i një Fast-Ethernet-Backbone

Zgjidhja komplete me Gigabit Ethernet

Nëpërmjet përdorimit të përshtatësve (adaptorëve) Gigabit-Ethernet-i mund të shfrytëzohet fluksi i të dhënave prej 1000 MBit në të gjithë rrjetin. Aplikacionet e së nesërmes në rrjet, që i përkasin fushës multimediale, (p. sh. videot) dhe që kanë fluks të lartë transferimi të dhënash, kanë nevojë për gjerësi të madhe bande, me qëllim që të mundësohet një vijueshmëri e qetë dhe pa pengesa e punës.



Zgjidhja komplete me Gigabit Ethernet

7.5 Token Passing

Procedura e aksesimit të rrjeteve Token-Ring

Ideja bazë e kësaj procedure aksesi është, që secilit stacion, në një interval të caktuar dhe të përllogaritur kohe, i jepet një herë mundësia të dërgojë të dhëna. Kjo procedurë mund të quhet si përcaktuese. Motoja këtu është: "secili në kohën e vet".

Nga anglishtja, "Token" mund të përkthehej me termat "kupon, copëz kujtese, kujtesë". Çdo stacion pune në rrjet, herë pas here, merr një "kupon" për një dërgim të dhënash që ka kryer. Në kuptimin figurativ, procesi i kalimit të "kuponit" nga një stacion në tjetrin ngjan me garën e stafetës në atletikë.

Token

Termi "Token" përshkruan një paketë me një shabllon bit-i special, e cila xhiron në rrjet dhe gjatë kohës që përshkruan këtë rrugë kalon tek të gjithë stacionet në rrjet, pra kalon nga njëri stacion tek tjetri (passing). Me qëllim që kjo të mund të realizohet, është parakusht ekzistenca e topologjisë logjike ring (unazë).

Në këtë rast nuk është e rëndësishme, nëse bëhet fjalë për një ring fizik apo nëse ring-u imitohet në formën e një shpërndarësi qëndror me qarqe, në formë ylli, apo nëpërmjet një kabëllzimi në formë peme.

Në rastin e një ring-u logjik, të dhënat nga stacioni dërgues në median transmetuese nuk dërgohen në të dyja drejtimet, por vetëm në një drejtim të përcaktuar.

Dërgimi/Marrja

Në qoftë se një stacion pune në rrjet dëshiron të dërgojë të dhëna, ai duhet të presë, derisa të marrë "kuponin-Token" që xhiron në ring. Brenda shabllonit të bit-it të një Token-i, është përcaktuar një vend, i cili jep informacion nëse Token në atë moment është i lirë apo i zënë.

Në rast se një stacion merr një "Free-Token – Token i lirë", atëhere informacioni i këtij të fundit ndryshon në "i zënë".Po kështu, jepen informacione për adresën burim dhe destinacion, si dhe për të dhënat bashkëngjitur. Paketa e plotë dërgohet si frame në stacionin tjetër, i cili konrollon para së gjithash adresën e marrësit.
Në rast se informacioni nuk është për stacionin në fjalë, ai transferohet në stacionin tjetër të rradhës. Kur informacioni arrin në stacionin për të cilin destinohet, atëhere ai kopjohet atje. Stacioni destincion konfirmon marrjen duke (kuotuar) shtuar një informacion në frame dhe e dërgon paketën e ndryshuar në stacionin e rradhës.

Pasi paketa e kuotuar arrin në fund (kryen xhiron e plotë në unaze-ring) dhe kthehet sërish tek dërguesi fillestar, ky i fundit, nga kuotimi, identifikon, që informacioni është transmetuar. Ndërkaq, ky stacion zëvendëson frame-n nëpërmjet një free-token, të cilën e dërgon tek stacioni më i afërt i rradhës.

Rregullat e aksesit

Krahas këtij ndërtimi bazë tek Token-Ring-u ekzistojnë edhe rregulla të tjera, të cilat duhet të sigurojnë transmetimin e të dhënave. Kështu, në çdo ring, një stacion merr përsipër rolin e "monitoruesit aktiv". Në përgjithësi ky është stacioni i parë, i cili bëhet aktiv në ring. Në qoftë se ky stacion fiket, këtë rol e merr, sipas një procedure të përcaktuar, një stacion tjetër (procedura token-claiming).

Ky monitorues aktiv ndër të tjera siguron, që një Token apo një frame i vlefshëm (= Token + të dhëna) të ekzistojnë gjithmonë në ring.

NAUN (nearest active upstream neighbour)

Përveç kësaj, stacioni i cili bën rolin e monitoruesit aktiv, gjatë dërgimit bën të njohur fqinjin dhe i kërkon atij, që të identifikojë sërish fqinjin gjatë dërgimit të rradhës së fluksit të të dhënave (upstream) .

Pasi çdo stacion pune ka dërguar më lart fluksin e të dhënave (upstream), si dhe ka bërë të njohur fqinjin e vet, ky i fundit do të quhet "fqinji aktiv i rradhës për dërgimin më tej të fluksit të të dhënave", shkurt NAUN (angl.nearest active up-stream neighbour).

Meqë ky proces ndodh gjithmonë, mund të gjendet relativisht shpejt, se në cilin prej stacioneve ka mundësi të jetë shfaqur problemi.

Avantazhet

- ☑ **Koha e një dërgimi mund të "llogaritet", çka do të thotë se mund të përcaktohet një kohë maksimale vonese për transmetimin.**
- ☑ Kjo procedurë është e përshtatshme veçanarisht për aplikacionet tek të cilat elementi kohë është kritik.

Disavantazhet

- ☑ Disavantazhi kryesor janë kostot mjaft të larta. Këto krijohen nga njëra anë si rezultat i kompleksitetit të madh të trafikut në rrjet, rregullimi i të cilit kërkon adaptorë të shtrenjtë, dhe nga ana tjetër për shkak të numrit të vogël të tyre në praktikë, gjë që bën që çmimi për njësi të rritet.
- ☑ Një stacion pune në rrjet, i cili dëshiron dë dërgojë të dhëna, nuk mund ta bëjë këtë mënjëherë, por duhet të presë për një "free-token". Në rastet kur asnjëri nga stacionet në rrjet nuk dëshiron të dërgojë, atëhere pothuajse menjëherë stacionit në fjalë i vihet në dispozicion një "free token".

8 Bashkësia e protokolleve TCP/IP

Në këtë kapitull do të lexoni

→ cilat protokolle i përkasin bashkësisë së protokolleve TCP/IP

→ cilat detyra bazë përmbushin protokollet

→ cilat shtresa u përkasin protokolleve të veçanta

Kusht paraprak

✓ Kuptimi i modeleve të sotme të rrjeteve

8.1 Protokollet dhe detyrat e tyre

Bashkësia e protokolleve TCP/IP (TCP/IP-Protocol-Stack)

TCP/IP-Protocol-Stack përfshin një gamë protokollesh, të cilat përmbushin detyra të ndryshme në rrjet. Emëruesi i përbashkët i këtyre protokolleve është që për transportimin e të dhënave të gjitha përdorin protokollin e Internetit (IP), i cili i përket shtresës së rrjetit (Network Layer) të modelit OSI. Tabela e mëposhtme na jep një pamje të përgjithshme mbi protokollet më të rëndësishme të bashkësisë së protokolleve (protocol stack).

Application Layer	Telnet, FTP, TFTP, HTTP, LDAP, DHCP, BOOTP, DNS, NFS, NETBIOS, SMTP ...	
Host-to-Host Layer	TCP	UDP
Internet Layer	IP	ICMP
Network-Interface-Layer	ARP, RARP	

Akostimi (caktimi) i ICMP-së në shtresën e Internetit është rezultat i detyrave të protokolleve. Edhe nëse ICMP-ja adresohet në një IP-SAP të vetin, ajo gjendet gjithsesi në shtresën e Internetit. Klasifikimi i ARP/RARP si pjesë e modelit me shtresa nuk është aq i thjeshtë, pasi protokollet kryejnë një klasifikim të informacioneve të Network Layer me informacionet e Data Link Layer. Ato quhen si nënprotokolle të LLC-së dhe në këtë mënyrë janë vendosur në shtresën Network-Interface-Layer.

Protokolli i Internetit (IP)

Application Layer	
Presentation Layer	
Session Layer	
Transportation layer	
Network Layer	IP
Data Link Layer	
Physical Layer	

Protokolli më i rëndësishëm i familjes së protokolleve TCP/IP është protokolli i Internetit (Internet Protocol). Ai është përgjegjës për transmetimin e datagrameve të TCP-së ose UDP-së në paketa (packet switching), si dhe kujdeset për gjetjen/përcaktimin e rrugëkalimit (path-it) në rrjet. Bazuar në pjesën që përcakton rrjetin në adresën e IP-së gjendet rruga më e mirë për transmetimin e paketave nga rrjeti dërgues për tek rrjeti marrës (destinacion). Brenda rrjetit destinacioni arrihet nëpërmjet adresës së hostit.

ARP/RARP

Application Layer	
Presentation Layer	
Session Layer	
Transportation layer	
Network Layer	
Data Link Layer	ARP/RARP
Physical Layer	

Address Resolution Protocol (ARP) shërben për gjetjen e adresës së hardware-it të një hosti të njohur IP, ndërsa me Reverse ARP(RARP) një adrese të njohur hardware-i i caktohet adresa korresponduese e IP-së.

Për këtë qëllim sistemi dërgon një MAC broadcast në shtresën Data Link Layer dhe një kërkesë (ARP-request) në shtresën e rrjetit (Network Layer). Kërkesa ARP (ARP Request) është një transmetim drejt e në adresën e IP-së së hostit destinacion, adresës MAC të të cilit duhet t'i bëhet rezolucioni (address resolution). Në këtë rast sistemi, me adresën e IP-së në fjalë, kërkon te informojë sistemin të cilit i është bërë kërkesa për adresën MAC të tij.

ICMP

Application Layer	
Presentation Layer	
Session Layer	
Transportation layer	
Network Layer	ICMP
Data Link Layer	
Physical Layer	

Internet Control Message Protocol (ICMP) shërben për përcaktimin e gabimeve, të cilat ndeshen gjatë transmetimit të paketave të IP-së. Në këtë rast, në sistemin destinacion dërgohet një e ashtuquajtur Echo Request. Në këtë rast bëhet fjalë për një Header 8 Byte të gjatë me informacione në lidhje me llojin e ICMP-së (1 Byte), Kodi ICMP (1 Byte), një shumë kontrolli (2 Byte) dhe një fushë operacionale (4 Byte), e cila sipas llojit të ICMP-së mund të marrë informacione të ndryshme, si statusi i gabimit (error status), apo vula kohore (time stamp) e paketës. Si payload ICMP-ja përdor një sasi të caktuar gërmash nga A tek E. Aplikimi më i njohur, i cili akseson ICMP-në, është komanda PING.

Transmission Control Protocol (TCP)

Application Layer	
Presentation Layer	
Session Layer	
Transportation layer	TCP
Network Layer	
Data Link Layer	
Physical Layer	

Transmission Control Protocol (TCP) shërben si protokoll i orientuar nga lidhja për transportin në rrjet të të dhënave. Ai kontrollon ndër të tjera krijimin dhe shkëputjen e sesionit të komunikimit, të ashtuquajturin multiplexing midis aplikacioneve të ndryshme të shtresave të larta, si dhe kontrollin e gabimeve për segmentet marrëse.

Në qoftë se rradha e marrjes së datagrameve ndryshon, kjo rradhë korrigjohet sërish p.sh. sipas sekuencës së numrave. Në rast se për datagramet e dërguara nuk merret një konfirmim marrjeje, atëhere ato dërgohen sërish.

User Datagram Protocol (UDP)

	UDP

Edhe User Datagram Protocol (UDP) është përgjegjës për transportin e të dhënave, por sigurisht ai është një protokoll i pa orientuar nga lidhja dhe si rezultat nuk kryen kontroll të mbërritjes (marrjes) së të dhënave. Për këtë arsye, ai nuk përdoret shpesh për transmetimin e sasive të mëdha të të dhënave, por përdoret para së gjithash me shërbime, të cilat përmes marrjes apo jo të një informacioni (mesazhi), kryejnë vetë një kontroll gabimi. Shembuj për këtë janë Domain Name Service (DNS) apo Dynamic Host Configuration Protocol (DHCP).

Në këtë mënyrë, ky protokoll mund përdoret për transportin e shpejtë dhe të thjeshtë të të dhënave në mjedise që kërkojnë siguri të lartë transmetimi. TFTP (Trivial File Transfer Protocol) mbështetet nga mekanizmat e kontrollit të shtresave të tjera dhe nëpërmjet UDP-së arrin shpejtësi transmetimi dukshëm më të larta se FTP-ja. Përdorimi i TFTP në fushën e WAN-it nuk është i përshtatshëm.

Protokollet e shtresave më të larta

Application Layer	HTTP, FTP, TFTP, POP, SMTP ...
Presentation Layer	JPEG, MIDI, ASCII, MPEG ...
Session Layer	NFS, NetBIOS, DNS ...
Transportation layer	
Network Layer	
Data link Layer	
Physical Layer	

Në shtresën e aplikacioneve të modelit TCP gjendet një seri protokollesh dhe shërbimesh me detyra të ndryshme. Meqë familja e protokolleve TCP/IP përdoret në të gjitha zbatimet e sotme në rrjet, duhet që për të gjitha aplikacionet e sotme të vihen në dispozicion protokollet përkatëse.

Protokollet e shtresës së sesionit (Session Layer)

TCP/IP mbështet një sërë protokollesh dhe shërbimesh të Session Layer. Disa nga këto përmbushin detyra të përgjithshme në rrjete, si rezolucioni i emrit (name resolution), ndërsa shërbime të tjera specifike ndaj sistemit operativ sigurojnë në rrjet autentifikimin e përdoruesve, apo aksesin mbi skedarë (files).

Shembuj për këtë janë DNS dhe WINS, NetBIOS, NIS dhe Kerberos ose NFS dhe CIFS.

Protokollet e shtresës së prezantimit (Presentation Layer)

Formate të ndryshme të dhënash, të cilat mbështeten p.sh. në shtresën e prezantimit, nuk jepen të detajuara për shkak të mungesës së lidhjes me praktikën. Përmendet vetëm që në disa raste të veçanta format e zbatimit (ASCII tek sitemet UNIX dhe Microsoft) ndryshojnë dhe kërkojnë një përshtatje të detajuar.

Tabela e mëposhtme synon të japë, nëpërmjet disa shembujve, një pamje të përgjithshme në lidhje me protokollet në shtresën 7. Sidoqoftë ajo nuk mund t'i paraqesë këtu të gjithë protokollet që punojnë në shtresën 7.

Tekst të dhëna	ASCII, EBCDIC, Unicode
[illegible]	MIDI, Wave
[illegible]	JPEG, GIF, PICT, TIFF
Video	MPEG, DivX, QuickTime

Të dhënat e këtyre protokolleve të ndryshme procesohen nga shtresa e prezantimit (Presentation Layer) për transport të mëtejshëm nëpërmjet rrjetit. Për këtë kryhet komprimimi i të dhënave, kontrolli i sesionit dhe kodimi. Mënyra e procesimit nuk varet nga sistemi operativ. Në këtë mënyrë mund të gjejnë përdorim karakteret 8-Bit-ASCII ose 16-Bit-ASCII.

Protokollet e shtresës së aplikacioneve (Application Layer)

Protokollet e shtresës së aplikacioneve, të cilat janë të integruara në familien TCP/IP, kanë për detyrë të sigurojnë shërbimet për programe të ndryshme. Kështu nëpërmjet FTP-së transmetohen të dhënat në rrjet, ndërsa SMTP-ja është përgjegjëse për transmetimin e mail-eve. Në tabelën e mëposhtme tregohen disa nga protokollet dhe shërbimet e sotme, të cilat egzekutohen nga shtresa e aplikacioneve dhe që mund të adresohen nga TCP/IP-ja.

Transmetimi i të dhënave	FTP, TFTP
E-Mail	SMTP, POP2, POP3
Remote sessions	Telnet, Rlogin
WWW	HTTP, HTTPS
Shërbimet e rrjetit	DHCP, WINS, DNS

Në këtë mënyrë, nuk nevojiten të gjiitha shërbimet e përmendura të rrjetit për aplikacionet jashtë tij, por ato janë shërbime që nuk përputhen me detyrat e shtresave më të ulta dhe për këtë (përsa kohë janë të integrueshme në një model rrjeti) duhet të klasifikohen nga shtresa e aplikacioneve.

Shënime

8.2 Ndërveprimi midis protokolleve dhe shërbimeve

Service Access Points

Çdo komunikim në rrjet ka nevojë për përdorimin e disa protokolleve, për të siguruar transportin pa gabime të të dhënave në rrjet. Me qëllim që të dhënat e një shtrese të kalojnë tek shërbimi i duhur i shtresës së mësipërme, ato duhet të adresohen sipas portave të përcaktuara për këtë qëllim. Këto quhen ndryshe edhe si Service Access Points (SAP).

Portat e shtresave 2 dhe 3 (Data Link Layer dhe Network Layer) nuk kanë ndonjë domethënie, kështu që nga administratorët e rrjetit nuk mund të kryhet ndonjë veprim nëpërmjet tyre. Në këtë mënyrë nuk luan ndonjë rol, në rast se TCP p. sh. e IP-së të adresohet tek porta 6, me përjashtim të rastit kur dëshirohet të lidhet/kanalizohet i gjithë trafiku i të dhënave me TCP-në. Në këtë rast shtrohet pyetja, përse duhet mbajtur në punë rrjeti.

Ndryshe paraqitet situata me portat e shtresës 4 (Transport Layer). Këtu njohja e saktë e portave është e nevojshme, nëse do të duhet të analizohet trafiku i të dhënave, ose nëse do të duhet të kryhet konfigurimi i një firewall-i për protokolle të caktuara.

Portat/Ports

Portat janë vende adresimi, të cilat përdoren tek protokollet e rrjetit, me qëllim që paketave me të dhëna t'u caktohen shërbimet përkatëse. Caktimi i portave kryhet nëpërmjet protokolleve TCP dhe UDP. Në qoftë se një protokolli i nevojiten shërbime të orientuara nga lidhja (si protokolli FTP në portën 21), ato mund të adresohen nëpërmjet TCP-së. Në të kundërt, në rast se një protokoll ka detyra të thjeshta, për të cilat nuk është i nevojshëm një komunikim i orientuar nga lidhja (si p.sh. protokolli DNS në portën 53), atëhere mund të përdoret protokolli UDP.

Portat e përdorshme numërohen si më poshtë:

- ☑ Portat **0** deri **1024** përshkruhen si porta të mirënjohura (wellknown ports).
- ☑ Portat **1024** deri **49151** përmblidhen si porta të regjistruara (registered ports) dhe rezervohen nëpërmjet aplikacioneve.
- ☑ Portat deri **65535** portat private ose dinamike (dynamic or private ports) nuk përdoren nga shërbimet standarde dhe mund të adresohen nga vetë përdoruesi.

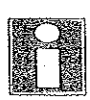


Tabela me informacion të mëtejshëm mbi portat do të gjeni në Internet (p. sh. tek *http://www.wikipedia.org/ në rast se kërkoni për portat dhe protokollet përkatëse).*

Skedari tekst *etc/services*

Caktimi i protokolleve për shërbimet regjistrohet në skedarin *etc/services*. Këtu, sipas nevojës, mund të kryhen ndryshime në rast se aplikacione të caktuara duan të caktojnë një protokoll në vend të atij që i korrespondon zakonisht asaj porte.

Formati i */etc/services* është përgjithësuar dhe nuk dallon në rastet e përdorimit të sistemeve operative si LINUX, apo Windows 2000/XP, edhe nëse porta të veçanta në sisteme të ndryshme nuk janë të përcaktuara. Kjo ndryshe do të thotë, që jo të gjitha shërbimet mund të përdoren në të gjitha sistemet operative. Caktimi i një porte nuk i krijon probleme punës së sistemit.

Emri i protokollit	Porta/Protokolli përkatës	Alias/Ndryshe	#Koment
www	80/tcp	http	# WorldWideWeb HTTP
www	80/udp		# Hyper Text Transfer Protocol

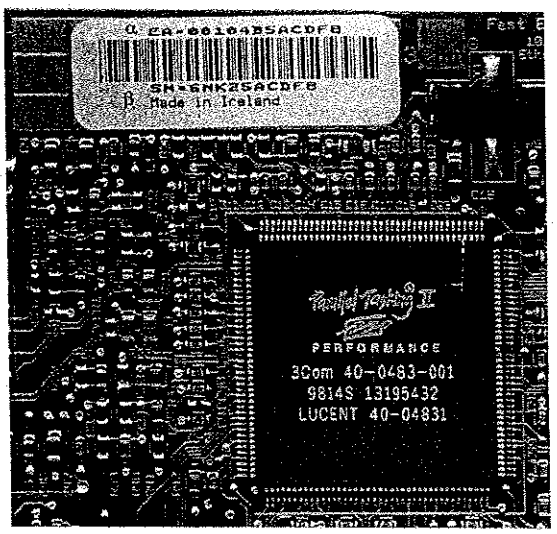
Siç duket qartë edhe nga shembulli, ka një hyrje informacioni për TCP-në dhe një tjetër, në të njëjtën portë, për UDP-në. Kjo i korrespondon RFC 1340, edhe nëse shumica e protokolleve nuk i suportojnë veprimet nëpërmjet UDP-së.

8.3 Adresat e IP-së dhe adresat MAC

Adresat në nivele të ndryshme

Adresa MAC e një karte rrjeti Ethernet

Procedura më e përdorshme e transmetimit në rrjetet lokale është Ethernet-i. Ethernet-i rregullon nëpërmjet frame-ve transmetimin e të dhënave në shtresat 1 dhe 2 të modelit OSI. Për këtë përdoren **adresa të cilat njihen si adresa Ethernet, adresa fizike,** ose **adresa MAC** α. MAC (Media Access Control) përbën një pjesë të shtresës 2 të modelit OSI. Adresa MAC vendoset si rregull, në varësi nga prodhuesi, krahas numrit serial të kartës së rrjetit dhe vetëm në raste të veçanta ndryshohet nga administratori i rrjetit.



Adresa MAC e një karte rrjeti Ethernet

Adresat e IP-së, në ndryshim nga adresat MAC, janë adresa logjike të ndryshueshme të hosteve. Ato jepen në shtresën e Internetit të modelit DARPA, shtresë e cila ka shtresën e vet korresponduese shtresën e rrjetit (Network Layer), apo ndryshe shtresën 3 të modelit OSI. Kjo shtresë në funksionin e vet është e pavarur nga shtresat e mëposhtme, si dhe të gjitha adresat dhe procedurat e transmetimit të përdorura nga ajo.

Me qëllim që të mundësohet në Ethernet shkëmbimi i të dhënave nëpërmjet TCP/IP-së, kërkohet krijimi i një lidhje midis adresës së IP-së dhe adresës MAC, e quajtur ndryshe **address resolution.** Për këtë qëllim përdoret **Address Resolution Protocol (ARP).**

ARP merr përsipër të kryejë detyrat e mëposhtme gjatë bashkëpunimit me procedurat e zakonshme të punës në LAN dhe WAN:

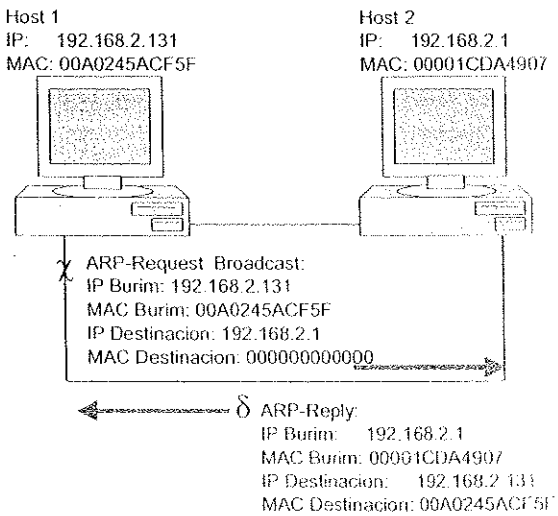
- ☑ Rezolucioni i adresës së IP-së tek adresa MAC nëpërmjet broadcast-it në rrjetet Ethernet dhe Token-Ring
- ☑ Memorizimi i ndërmjetëm në cache-në e ARP-së dhe përditësimi i ndryshimeve të adresave që kanë kryer rezolucionin
- ☑ Identifikimi dhe pengesat e konflikteve të adresave të IP-së

Në rastin e kundërt kur kërkohet përcaktimi i një adrese të njohur MAC, përdoret **Reverse ARP.** Për proceset e punës në rrjet si Frame Relay dhe ATM, të cilat nuk punojnë me broadcast, u zhvillua **Inverse ARP. InARP** përcakton në këto rrjete marrëdhënien midis adresave të IP-së së Host-eve dhe Virtual Circuit, përmes së cilit funksionon komunikimi respektiv.

Rezolucioni i adresave të IP-së në adresa MAC

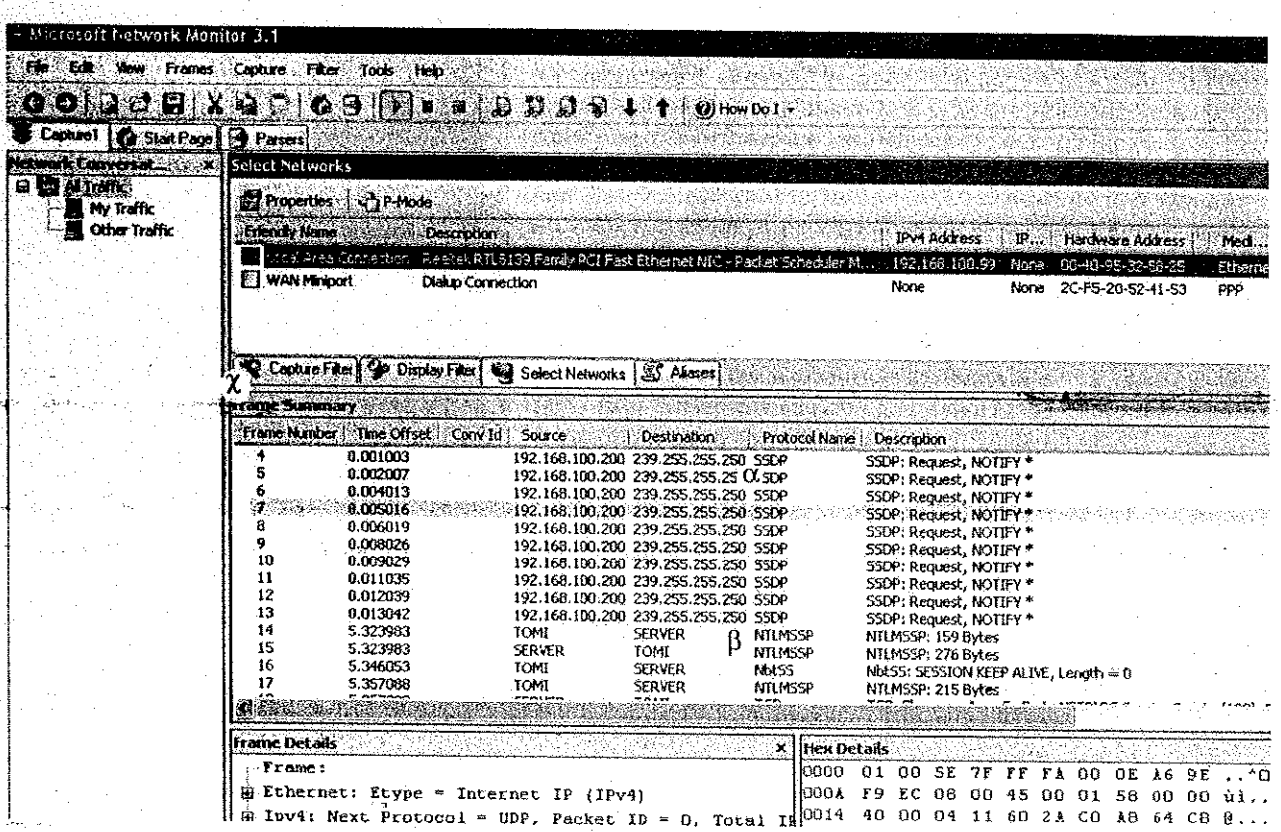
Adresa MAC nevojitet, me qëllim që të mund të transferohen direkt frame-t midis hosteve në komunikim, brenda një subnet-i të caktuar. Një host, i cili njeh vetëm adresën e IP-së të partnerit në komunikim, duhet të përcaktojë paraprakisht adresën MAC të tij. Ky proces kryhet si më poshtë:

Host-i 1 dërgon një **ARP-Request (kërkesë për address resolution protocol),** si broadcast, në subnet-in lokal χ me adresën MAC të destinacionit 00-00-00-00-00-00 dhe adresën e IP-së së partnerit të tij në komunikim - Host-i 2 (192.168.2.1). ARP-Request përmban si adresën burim, ashtu edhe adresën MAC dhe IP të Host-it 1. Ky broadcast merret dhe vlerësohet nga të gjithë klientët ethernet aktivë në rrjet. Host-i 2, me adresë IP 192.168.2.131, i përgjigjet Host-it 1 me një **ARP-Reply,** me anë të të cilës ai e informon këtë të fundit për adresën MAC të tij δ si adresë burim. Të dy partnerët në komunikim i njohin tashmë adresat respektive të njëri-tjetrit dhe mund të fillojnë procesin e komunikimit.



Rezolucioni i adresës nëpërmjet ARP-së

Ky shkëmbim të dhënash për rezolucionin e adresës mund të rikompozohet nga një software monitorues rrjeti, me anë të të cilit mund të regjistrohet dhe të paraqitet komunikimi që ndodh në rrjet. Komunikimi fillon me dërgimin e një ARP-Request-i α dhe më pas me marrjen e një përgjigje me ARP-Reply β, në të cilën përmbahet adresa MAC, deri tani e panjohur, si adresë burim χ.

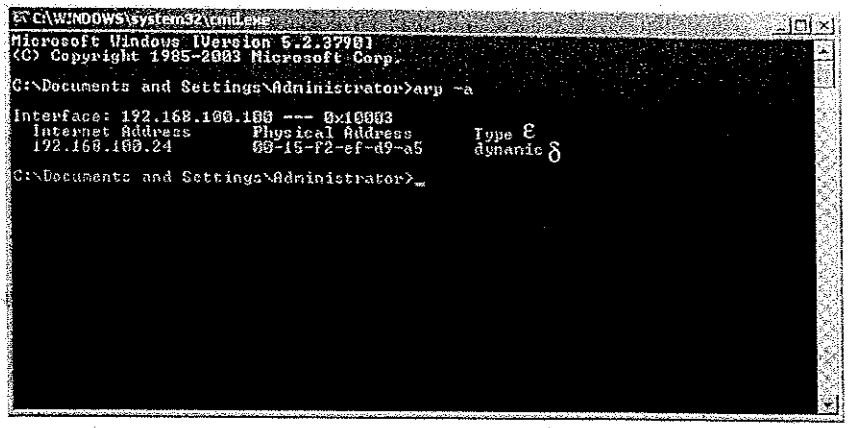


ARP-Request dhe ARP-Reply gjatë monitorimit të rrjetit

Duhet patur kujdes që një ARP-Request funksionon vetëm brenda një subnet-i IP-je, pasi broadcast-et nuk përçohen më tej nga routeri IP. Një rezolucion direkt i adresës me anë të ARP-së nëpërmjet router-it nuk është i nevojshëm. Hostet me anë të subnetmask-ës, përcaktojnë vetë nëse do t'ia dërgojnë apo jo router-it një paketë me të dhëna. Në këtë rast, nëpërmjet ARP-Request-it, hosti gjen adresën MAC të routerit fqinjë (standard gateway) dhe dërgon tek ai paketën me të dhëna për transferim të mëtejshëm. Në qoftë se nuk është konfiguruar një standard- gateway, hosti nuk ndërmerr asnjë tentativë komunikimi, kur si adresë destinacion ka një adresë IP-je jashtë subnet-it të vet.

Me qëllim që çdo shkëmbim të dhënash të mos fillojë me një broadcast për rezolucion adrese duke rritur në këtë mënyrë ngarkesën në rrjet, host-et memorizojnë për një farë kohe rezultatet e rezolucionit në memorjen e ndërmjetme - **ARP-Cache.** Procedurat e komunikimit që zhvillohen më pas, në vend të broadcast-it mund të riaksesojnë rezultatet e rezolucionit të memorizuara në memorien e ndërmjetme (ARP-Cache).

ARP-Cache



Në Windows ARP-Cache-ja ndërtohet nga një pjesë e RAM-it. Çdo rezolucion i plotë me ARP-Request dhe ARP-Reply çon në një regjistrim informacioni në ARP-Cache të adresës së IP-së δ dhe të adresës MAC korresponduese ε të hostit të dhënë. Në rast se në ARP-Cache nuk gjendet informacion mbi adresën e IP-së, ky informacion regjistrohet atje nga e para, dhe informacionet ekzistuese aktualizohen. Windows-i për çdo adresë lokale IP-je organizon një ARP-Cache të vetën.
Adresat MAC të cilat e kanë kryer një herë rezolucionin dhe informacioni i të cilave ka qëndruar për një kohë të gjatë në ARP-Cache, si dhe është përdorur gjatë kësaj kohe, mund të mbeten pa u vënë re dhe në mënyrë të padëshiruar për një kohë të gjatë pas mosfunksionimit, apo heqjes nga përdorimi të kartës së rrjetit: Një Host, i cili mund ta kryejë me sukses rezolucionin e një Ethernet-Frame-i në një adresë MAC, e konsideron si të suksesshëm procesin e komunikimit, pasi Ethernet-i nuk parashikon asnjë konfirmim. Për këtë arsye në Windows, kohëqëndrimi për informacionet e memorizuara në ARP-Cache është i kufizuar. Një regjistrim në ARP-Cache, i cili pas krijimit nuk përdoret më, fshihet pas 2 minutash. Në rast se brenda 2 minutave të para ai kërkohet sërish, qëndron i memorizuar edhe 2 minuta të tjera deri sa të kalojnë maksimumi 10 minuta. Më pas duhet dërguar një ARP-Request i ri.

Sipas nevojës, me ndihmën e konfigurimit të regjistrit (registry), mund të ndryshohen kohëqëndrimet e informacioneve në ARP-Cache, ose mund të shtohen informacione statike nëpërmjet komandës arp, të cilat nuk mund të fshihen automatikisht nga cache-ja.

Identifikimi dhe shmangia e konflikteve të adresave të IP-së

Kur dy hoste zotërojnë të njëjtën adresë IP-je, të dhënat nuk mund të transmetohen më në mënyrë të saktë. Për këtë ARP-ja në Windows përmban një procedurë për identifikimin e adresave të njëjta të IP-së në rrjet.

Gjatë startimit të sistemit dhe konfigurimit të TCP/IP-së një host dërgon disa herë një ARP-request për vetëtestim (Gratuitous ARP), i cili ka si adresë destinacion adresën e tij të IP-së. Përsa kohë që kjo adresë nuk përdoret nga një host tjetër në të njëjtin subnet, hosti që po starton nuk merr përgjigje për kërkesën e bërë (ARP-Requests). Kjo mund të presupozojë, që adresa e IP-së është e lirë dhe mund të aktivizohet për ndërfaqen e vet.

Në rast se kërkesës i përgjigjet një host tjetër, me po këtë adresë IP-je, nëpërmjet një ARP-Reply, sjellja e mëtejshme e host-it varet nga metoda me të cilën është konfiguruar adresa e tij e IP-së. Në qoftë se adresa e IP-së është konfiguruar në mënyrë manuale, hosti që po starton nuk e fillon procesin e konfigurimit të TCP/IP-së. Në vend të kësaj ai shfaq një mesazh gabimi dhe regjistron një ngjarje (event) në protokollin e sistemit, e cila mund të shihet tek Event Viewer. TCP/IP mund të ristartohet në këtë host vetëm pasi të bëhet një rikonfigurim i adresës së IP-së nga administratori. Kur adresat e IP-së jepen automatikisht nëpërmjet DHCP-së, host-i refuzon adresën IP të ofruar dhe kërkon një adresë tjetër.

Ky proces nuk mund të pengojë, që një host i konfiguruar për të punuar me dy adresa IP-je, ta përdorë adresën sërish, në qoftë se ai lidhet me vonë në një subnet tjetër. Këtu së pari identifikohet konflikti i adresave, në rastin kur njëri nga sistemet që kanë konflikt adresash dërgon një ARP-request. Sistemet respektive e përdorin më tej adresën ekzistuese të IP-së, por duke krijuar për çdo ARP-request një mesazh gabimi dhe regjistrimin përkatës në protokollin e sistemit.

Proxy ARP

Proxy ARP është një program, që u mundëson router-ave, t'u përgjigjen kërkesave për adresa MAC të bëra nëpërmjet ARP-request-it. Host-et në këtë rast gjenden në rrjete të ndryshme.
Kur kompjuteri A dërgon një ARP-request tek kompjuteri B, i cili ndodhet në një rrjet tjetër, përgjigjen në vend të kompjuterit B e jep router-i që ndodhet midis dy kompjuterave, i cili dërgon kompjuterit A si ARP-reply adresën e tij. Kompjuteri A dërgon një ARP-request në router, kërkesë e cila i dërgohet më pas kompjuterit B.

R-ARP (Reverse ARP)

Në rast se sistemi e njeh adresën MAC dhe i duhet të gjejë adresën respektive të IP-së, atëhere përdoret varianti i anasjelltë i ARP-së i quajtur Reverse Address Resolution Protocol (R-ARP).

Shënime

9 Protokolli i Internetit (IP)

Në këtë kapitull do të lexoni:

→ ku konsiston protokolli i Internetit
→ ku dallohen adresat e IP-së nga ato të rrjetit
→ si mund të llogariten adresat e IP-së dhe subnetmaskat

Kusht paraprak

✓ Njohuri bazë mbi mënyrën e llogaritjes së numrave binare

9.1 Pjesët përbërëse dhe detyrat e IP-së

Protokolli i Internetit

Protokolli i Internetit (IP) është sot protokolli më i përhapur **në shtresën 3 sipas modelit OSI**. Nga njëra anë ai luan rol **thelbësor në komunikimin në Internet**: pa IP nuk ka lidhje në Internet. Nga ana tjetër IP-ja është e rëndësishme edhe **për të gjitha rrjetet e tjera, pasi sot nuk ka më rrjete të izoluara, por rrjete që punojnë shpesh të lidhura me pjesë të tjera rrjetesh.**

Në të njëjtin rrjet gjithmonë e më tepër, nëpërmjet IP-së, punojnë shërbime të ndryshme.Transmetimi në rrjet i zërit dhe pamjeve të lëvizshme (videove) ndeshet sot gjithmonë e më shpesh. Gjithashtu, edhe video-kon-fe-ren-cat, apo transporti i sigurt i informacioneve për shërbime të tilla si online banking po preferohen gjithmonë e më tepër.

Tek të gjitha këto forma komunikimi e gjejmë sërish IP-në me karakteristikat e saj të shumëfishta. Për këtë arsye, më poshtë do të jepen të detajuara ndërtimi dhe përdorimi i adresave të IP-së, po ashtu dhe përpunimi i tyre në rrjet.

Funksioni dhe pjesët përbërëse të adresave të IP-së

Kërkesë kryesore për shkëmbimin e të dhënave në rrjet është që çdo kompjuter (host) dhe informacionet e dërguara tek ai të mund të identifikohen qartë. Ky identifikim mundësohet me ndihmën e një adrese. Në rast se rrjeti duhet të shtrihet globalisht, atëhere kërkohet një procedurë shtesë, e cila mundëson lokalizimin e një hosti brenda gjithë rrjetit.

Në suitën e protokolleve TCP/IP, protokolli i internetit (IP) është përgjegjës për adresimin e hosteve dhe për shkëmbimin e paketave me të dhëna mes tyre. Në këtë mënyrë të gjithë hostet marrin një adresë IP-je (IP-address), e cila përbëhet nga një bashkësi shifrash 32 bit e gjatë, gjithashtu një rradhë 32 shifrash binare me 0 dhe 1-sha, p.sh.:

11000000101010000000000111111110

Për përdoruesin, paraqitja e adresave të IP-së në sistemin dhjetor (decimal) është më i lehtë për t'u kuptuar edhe për t'u mbajtur mend, sesa paraqitja në sistemin binar. Për këtë arsye, adresat e IP-së ndahen në katër blloqe të quajtura ndryshe oktete, ku secilit i korrespondon 1 Byte (respektivisht 8 Bit). Secili nga këto blloqe përfaqëson $2^8 = 256$ kombinime të mundshme të 8 shifrave binare, që i korrespondojnë një vlere decimale nga 0...255. Të katër oktetet shkruhen njëra pas tjetrës dhe ndahen me pika:

11000000 10101000 00000001 11111110 = 192.168.1.254

Këtu vlejnë rregullat e zakonshme të konvertimit të numrave binarë në decimalë. Një proces i thjeshtë konvertimi jepet më poshtë:

→ Vini re se për çdo shifër binare të një okteti ka një vlerë korresponduese decimale.									
Shifrat binare	1	0	1	0	1	0	0	0	
Vlera decimale	128	64	32	16	8	4	2	1	
	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)	
→ Për shembull, të gjitha vlerave decimale, shifra binare e të cilave është "1". Rezultati është vlera decimale përkatëse e oktetit.									
	128	+	32	+	8				= 168

Adresat e IP-së, në mënyrën e funksionimit të tyre, ngjajnë me numrat e telefonit: Edhe lidhjet telefonike kryhen nëpërmjet numrave unikë dhe të identifikueshëm qartë në mbarë botën, nëpërmjet të cilëve këto numra mund të arrihen.

Pjesët përbërëse të një adrese IP-je

Adresat e IP-së ndahen në disa pjesë, si numrat e telefonit në prefiks dhe numrin lokal, dhe secila nga këto pjesë përmbush një detyrë të caktuar. Në këtë mënyrë është e mundur, që një host të lokalizohet njëlloj si në Internet edhe në një rrjet global IP-je. Bazat ligjore të administrimit, si dhe teknikat e transmetimit, kërkojnë gjithashtu ndarjen e rrjeteve globale në **segmente ose subnete (nënrrjete)** të veçanta, të pavarura nga njëra-tjetra. Kështu çdo adresë IP-je ka respektivisht dy pjesë përbërëse:

☑ Një **adresë rrjeti**, e cila jep segmentin përkatës të rrjetit, në të cilin ndodhet një host
☑ Një **adresë hosti**, e cila dallon hostet (kompjuterat) e veçanta brenda një segmenti

Adresa e rrjetit mund të ndahet nga ana e saj në një adresë identifikuese të rrjetit në Internet dhe në një adresë identifikuese subneti vetëm brenda një segmenti rrjeti. Ky identifikim subneti mund të përdoret me qëllim që të ndahen më tej subnetet e mëdha për të përdorur adresat ekzistuese të hosteve.

Sipas përcaktimit të bërë, adresa e IP-së fillon me pjesën e adresës së rrjetit dhe mbaron pjesën e adresave të hosteve (leximi nga e majta në të djathtë). Në njërën nga shifrat ndodh kthimi i adresës së rrjetit në adresa hostesh. Në përcaktimin klasik të IP-së këto shifra fiksohen me ndihmën e një klase **adresash.**

Në fushën e adresave të hosteve duhen marrë parasysh edhe dy raste të veçanta:

☑ Një adresë hosti, e cila përbëhet nga shifra binare 0, p.sh. 192.168.1.**0**, është vetë adresa e rrjetit dhe nuk lejohet të përdoret si adresë e një hosti të caktuar.

☑ Në rast se të gjitha shifrat binare të një adrese hosti përbëhen nga 1-sha, psh. 192.168.1.**255**, këtu mund të flitet për një adresë broadcast-i të rrjetit respektiv. Nëpërmjet kësaj adrese u adresohemi bashkërisht të gjitha hosteve të një rrjeti. Kjo adresë nuk lejohet të përdoret për hoste të tjera të veçanta.

Klasat e adresave

Klasat e adresave ndajnë një adresë IP-je në pjesën që identifikon adresën e rrjetit dhe në pjesën që identifikon adresën e hostit. Klasat e adresave caktojnë numrin e shifrave binare (= Bits) për adresë rrjeti. Janë përcaktuar pesë klasa adresash, të cilat identifikohen nga mënyra si vazhdojnë të plotësohen katër bitet e para të një adrese të parapëlqyer:

Klasat e adresave	Bitet e adresës së rrjetit	Vazhdimi i katër biteve të para	Numri i adresave të hosteve për rrjet	Diapazoni i adresave të rrjetit
Klasa A	8 (1 Oktet)	0xxx	16. 777. 214 (= 2^{24}-2)	1.0.0.0 deri 127.0.0.0
Klasa B	16 (2 Oktete)	10xx	65.534 (= 2^{16}-2)	128.0.0.0 deri 191.255.0.0
Klasa C	24 (3 Oktete)	110x	254 (= 2^8-2)	192.0.0.0 deri 223.255.255.0
Klasa D	- (Multicastgroups)	1110	(nuk egziston)	224.0.0.0 deri 239.255.255.255
Klasa E	- (eksperimental)	1111	(nuk egziston)	240.0.0.0 deri 255.255.255.255

Për përdorim normal janë të vlefshme adresat e klasave nga A-ja deri tek C-ja.

Ndarja e ngurtë e adresave të IP-ve nëpërmjet klasave të adresave ka sjellë si pasojë rritjen e papritur të numrit të hosteve në Internet dhe zvogëlimin e shpejtë të adresave të IP-së në dispozicion. Në qoftë se për një subnet të përcaktuar të klasës C do të nevojitet një numër adresash hostesh mbi 254, atëherë kërkohet menjëherë kalimi në një rrjet të klasës B.

Adresat e pashfrytëzuara të rrjetit të klasës B nuk mund t'u jepen të interesuarve të tjerë, pasi çdo adresë rrjeti i lejohet të identifikojë vetëm një rrjet, përndryshe nuk do të mund të garantohej më uniciteti i adresave të rrjetit në Internet. Të gjitha adresat e panevojshme të hosteve dhurohen, pjesërisht dhjetëra mijëra adresa në një rrjet të vetëm të klasës B.

Administrimi i adresave të IP-së bazuar në klasa u plotësua me **diapazonet e adresave private** dhe eventualisht nëpërmjet **subnetmaskës** dhe një nëndarjeje tjetër në blloqe adresash CIDR (Classless Inter-Domain Routing).

Adresat private

Adresat private të IP-së janë në dispozicion të rrjeteve, të cilat ose nuk janë të lidhura në Internet, ose janë të lidhura vetëm nëpërmjet routerave special. Adresat private të mëposhtme nuk transferohen (routohen) më tej në Internet dhe lejohen të përdoren nga çdo përdorues i një rrjeti privat:

Përshkrimi	Diapazoni i adresave	Subnetmask	CIDR-Blloku i adresave	Adresa IP-je (Hostesh)
Klasa A adresa private	10.0.0.0 deri 10.255.255.255, i përkasin një rrjeti të klasës-A	255.0.0.0	10.0.0.0/8	2^{24} = 16.777.216
Klasa B adresa private	172.16.0.0 deri 172.31.255.255, i përkasin 16 rrjeteve të klasës-B	255.240.0.0	172.16.0.0/12	$16*2^{16}$ = 1.048.576
Klasa C adresa private	192.168.0.0 deri 192.168.255.255, i përkasin 255 rrjeteve të klasës-C	255.255.0.0	192.168.0.0/16	2^{16} = 65.536

Në versionet që do të vijnë pas IPv4, IPv6, parashikohet një zgjerim i adresës së IP-së në 128 Bit dhe me këtë rast do të zgjidhen shumë procedura që ndërmerren për shkak të numrit të kufizuar të adresave të IP-së.

Adresat e rezervuara

Sipas dokumentacionit teknik bazuar në RFC 3330 (Request for Comments), adresat e mëposhtme të rrjetit janë të rezervuara për qëllime speciale:

Diapazoni adresave	Qëllimi	Dokumenti
0.0.0.0/8	Adresa e rrjetit aktual	RFC 1700
10.0.0.0/8	Rrjet privat i klasës A	RFC 1918
14.0.0.0/8	Rrjet publik të dhënash	RFC 1700
39.0.0.0/8	Rezervuar	RFC 1797
127.0.0.0/8	Loopback (kompjuter lokal)	RFC 1700
128.0.0.0/16	Rezervuar	RFC 3330
169.254.0.0/16	Rrjet privat (link lokal), APIPA	RFC 3927
172.16.0.0/12	Rrjet privat i klasës B	RFC 1918
191.255.0.0/16	Rezervuar	RFC 3330

192.0.0.0/24	Rezervuar	RFC 3330
192.0.2.0/24	Rrjet testimi	RFC 3330
192.88.99.0/24	IPv6 to IPv4 Relay	RFC 3068
192.168.0.0/16	Rrjet privat i klasës C	RFC 1918
198.18.0.0/15	Rrjet-Benchmark-Testimi	RFC 2544
223.255.255.0/24	Rezervuar	RFC 3330
224.0.0.0/4	Multicasts (rrjet i klasës-D)	RFC 3171
240.0.0.0/4	Rezervuar (rrjet i Klasës-E)	RFC 1700
255.255.255.255	Broadcast	--

9.2 Caktimi i adresave të IP-së

Caktimi i adresave statike të IP-së

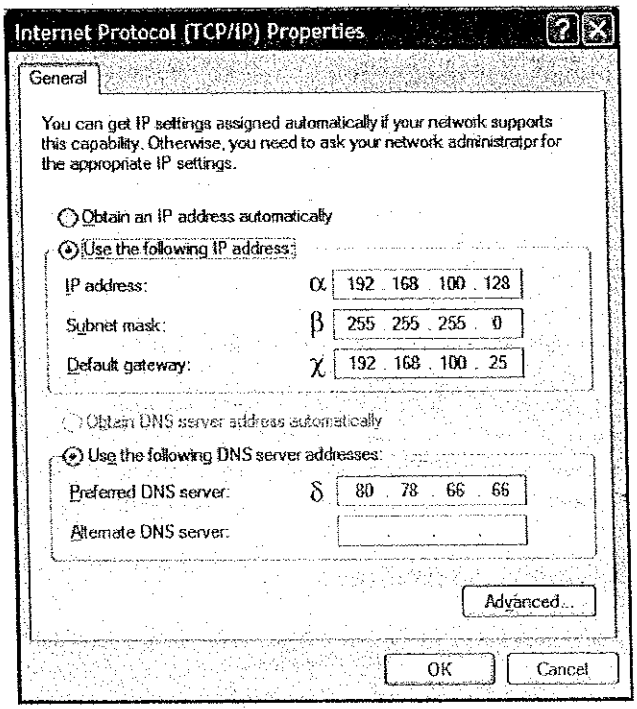
Gjatë konfigurimit standard Windows-i përdor procesin e konfigurimit automatik të adresës së IP-së dhe parametrave të tjera për TCP/IP-në (APIPA).

TCP/IP-ja mund të konfigurohet edhe manualisht. Pjesa më e madhe e elementëve të konfigurimit gjendet tek dritarja Local Area Connection Properties, e cila merret duke klikuar me butonin e djathtë të mausit mbi ikonën e lidhjes në rrjet. Më pas, zgjidhet Internet Protocol (TCP/IP) dhe butoni Properties.

Për TCP/IP-në kërkohet minimumi caktimi i një adrese IP-je α dhe një Subnet maske β .

Komunikimi me subnete të tjera ose në Internet kërkon akoma dhënien e një adrese për Default gateway χ dhe të paktën një adresë për serverin DNS δ.

DNS-ja nevojitet edhe për integrimin e një kompjuteri në një domain windows-i.



Konfigurimi manual i kartës së rrjetit

Bazat e DHCP-së

Konfigurimi manual i IP-ve të hosteve ka disa disavantazhe të rëndësishme, sidomos në rrjetet e mëdha:

- ☑ Përdorimi i adresave të IP-së duhet të dokumentohet saktësisht, me qëllim që të shmanget përdorimi dy herë i së njëjtës adresë dhe përdorimi i adresave dhe subnetmaskave të gabuara.
- ☑ Ndryshimet e adresës së IP-së në shërbimet kryesore si DNS, apo Default Gateway hapin shumë punë, pasi çdo Host që preket nga ky ndryshim duhet konfiguruar nga e para.
- ☑ Kompjuterat portabël, të cilat përdoren në subnete të ndryshme të kompanisë, duhet të rikonfigurohen pas çdo ndryshimi të subnetit.

Dynamic Host Configuration Protocol (DHCP - Protokolli i Konfigurimit Dinamik Automatik të Hosteve) mundëson konfigurimin automatik të TCP/IP-së së hosteve dhe pengon shfaqjen e problemeve të sipërpërmendura. Në këtë rast është e mundur të konfigurohen jo vetëm parametrat standard si adresa e IP-së dhe subnetmaska, por edhe një numër opsionesh shtesë të DHCP-së. Këtu futen p.sh. adresat e IP-ve për Default gateway-n dhe serverin DNS, ose një server për shërbimet e rrjetit si WINS.

DHCP është zgjerim i Bootstrap-Protokolls (BootP) dhe bazohet në modelin Klient-Server. Serveri DHCP disponon një **diapazon (pool)** adresash IP-je, të cilat mund t'ua japë klientëve. Çdo klient DHCP, gjatë startimit dhe në vazhdim, kërkon, në intervale të caktuara një server DHCP në rrjet. Kur e gjen dhe arrin të komunikojë me të, merr prej tij për një periudhe kohe të caktuar një adresë IP-je dhe të gjitha të dhënat e tjera të nevojshme për konfigurim. Ky proces njihet si **lease (huadhënie)**.

Caktimi i adresave të IP-së me DHCP

Gjatë caktimit të adresave të IP-së dallohen dy procese të ndryshme:

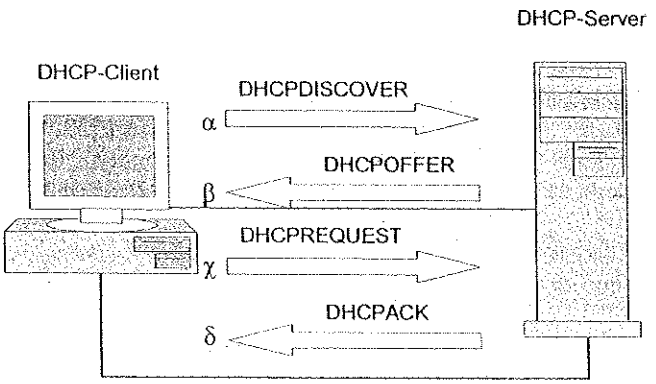
☑ Caktimi **automatik**, gjatë të cilit serveri DHCP i cakton klientit një adresë IP-je brenda një diapazoni të përcaktuar. Adresa është e lidhur me adresën MAC të klientit për një kohë të pacaktuar.

Në rast se nuk ka më adresa IP të lira, në diapazonin e caktuar në server për këtë qëllim, atëhere asnjë klient i ri nuk mund të identifikohet dhe shtohet në rrjet. Pas fshirjes së cache-së së DHCP-së në server, mund të fillojë sërish caktimi i adresave të reja të IP-së.

☑ Gjatë caktimit **dinamik** të IP-ve, adresat e dhëna memorizohen në një skedar konfigurimi. Klienti, gjatë një periudhe kohe të përcaktuar (**lease-time**) duhet ta konfirmojë adresën, përndryshe adresa mbetet e lirë dhe mund t'i caktohet një kompjuteri tjetër që identifikohet në rrjet.

Caktimi i adresave të IP-së nëpërmjet DHCP-së

Dhënia e sukseshme e një adrese IP-je, për një klient DHCP ende të pa konfiguruar, kryhet si më poshtë:



Dhënia e një konfigurimi të ri IP-je nëpërmjet DHCP-së

Klienti DHCP gjatë inicializimit të TCP/IP-së, dërgon një broadcast në subnetin lokal, me anë të të cilit kërkon dhënien e konfigurimit të IP-së. Ky mesazh i dërguar quhet **DHCPDISCOVER** α. Serveri DHCP, që është aktiv në rrjet, reagon ndaj kësaj kërkese me një ofertë **DHCPOFFER** β, e cila përmban një adresë IP-je dhe një subnetmaskë për klientin. Klienti e zgjedh ofertën në formë lease-i dhe e bën të njohur sërish në rrjetin lokal nëpërmjet një **DHCPREQUEST** χ. Në këtë mënyrë, të gjithë serverat DHCP e dinë tashmë cila ofertë u mor në përdorim dhe nga cili klient. Serveri DHCP, oferta e të cilit u zgjodh nga klienti, konfirmon përfundimisht zgjedhjen me dërgimin e një **DHCPACK** δ (acknowledge-njohje), e cila përmban të gjitha informacionet e mëtejshme që duhen për konfigurimin e TCP/IP-së së klientit.

Instalimi i serverit DHCP

Serveri DHCP ngrihet si shërbim në Windows Server 2003 ose në një kompjuter me sistem operativ Linux dhe duhet konfiguruar më pas. Parakusht për këtë është, që vetë serveri DHCP të ketë një adresë statike, e cila jepet nga administratori.

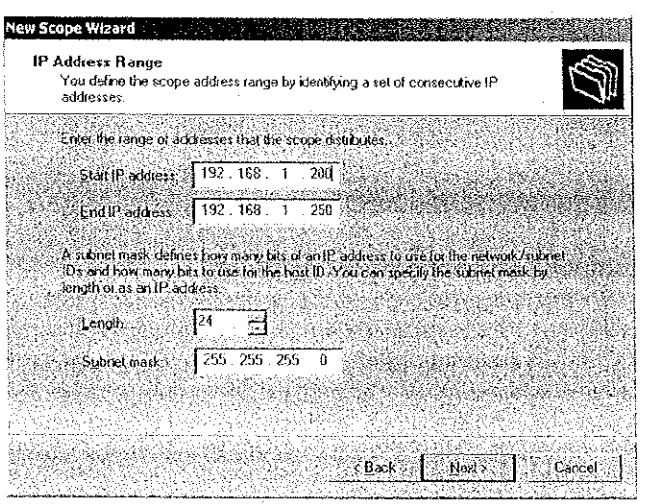
Pas instalimit duhen kryer konfigurimet e mëposhtme:

☑ Përcaktoni diapazonin e adresave duke dhënë adresat fundore (më të vogël dhe më të madhe – *Start IP address* dhe *End IP address*), brenda diapazonit të të cilave do të caktohen adresat.

☑ Më pas jepni adresën e Default gateway.

☑ Jepni adresën e IP-së të serverit përgjegjës DNS.

☑ Në fund duhet bërë identifikimi (autorizimi) i një serveri DHCP në rrjet, me qëllim që klientët të mund ta aksesojnë për marrjen e një adrese IP-je prej tij.



Caktimi i diapazonit të adresave të IP-së për shërbimin DHCP

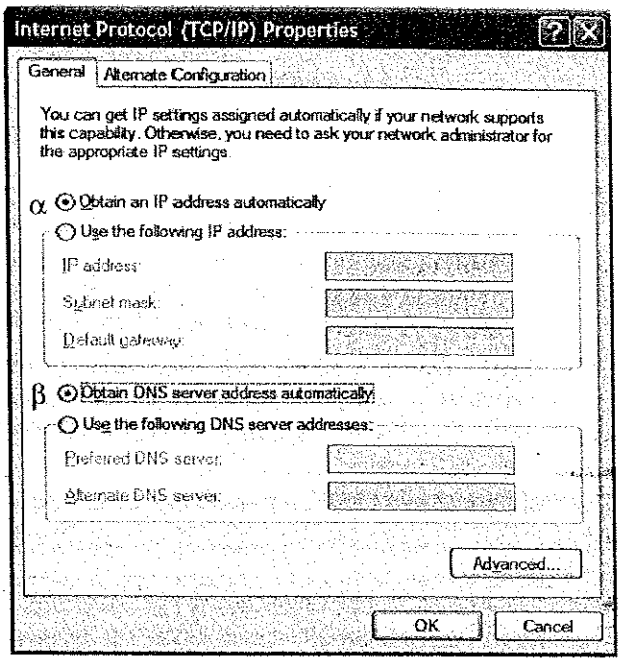
Në rrjetet e vogla, pa server, rolin e serverit DHCP e merr shpesh përsipër një router DSL. Ky i fundit jep në mënyrë dinamike adresat e IP-së. Në rast se në rrjet është aktiv edhe një server DHCP, atëhere router-i DSL duhet konfiguruar të punojë thjesht si modem i pastër.

Konfigurimi i klientëve për DHCP

Hostet në Windows 2000/XP/Vista, pas një instalimi standard të lidhjes në rrjet, janë konfiguruar automatikisht (by default) për përdorimin e DHCP-së. Gjatë çdo startimi të ri dhe në intervale të rregullta, nëpërmjet DHCPDISCOVER, kërkohet për një DHCP-Server dhe nga ky i fundit një adresë IP-je. Për këtë arsye, ndryshimi i konfigurimit nuk do të jetë më i nevojshëm.

Nëse do të duhet që adresat e IP-së të dhëna manualisht të merren nga një server DHCP, atëhere për hostet duhet zgjedhur dhënia automatike e adresave me opsionin *Obtain an IP address automatically* α.

Në të njëjtën dritare dialoguese mund të shkruani dhe adresën e serverit DNS- β (shih paragrafin pasardhës).



Caktimi automatik i adresës së IP-së nga Windows XP

Domain Name Service (DNS)

Domain Name Service (DNS) lejon që në vend të adresave numerike dhe të vështira për t'u mbajtur mend të IP-ve, një kompjuter të identifikohet me një host name (emër). Në këtë rast çdo adrese IP-je i vihet një emër i qartë. Kalimi nga adresë IP-je në emër kryhet nga serveri DNS, i cili me ndihmën e listave paraprake bën lidhjen e emrave me IP-të përkatëse. Po marrim si shembull emrin *www.herdt.com*, i cili i korrespondon adresës së IP-së 195.127.237.67.

Këto emra zgjidhen nga e djathta në të majtë. Ato fillojnë (djathtas) me të ashtuquajturin Top Level Domain, p. sh. *com* për organizatat tregtare, ose me një shkurtim dygërmësh për shtetet, p.sh. *al* për Shqipërinë, apo *de për Gjermaninë*.

Të ndarë nga një pikë, vijojnë njëri pas tjetrit një ose disa emra domain-esh (domain names). Në shembullin e mëposhtëm pjesa e fundit (majtas) i përket emrit të kompjuterit (host name). Një host mund të klasifikohet edhe nëpërmjet disa emrave. Ndërtimi i përgjithshëm i adresës është:

emri-kompjuterit.[subdomain.]domain.top-level-domain

Emrat e domaineve duhet të jenë unike, ashtu si dhe adresat e IP-ve. Për të marrë një emër të caktuar bëhet aplikimi (kërkesa) përkatëse dhe merret leja e duhur.

DNS-ja në rrjetin lokal

Instalimi dhe konfigurimi i DNS-së

DNS është parakusht absolut për punën në një domain Windowsi. Prandaj, DNS-ja duhet instaluar më së voni gjatë instalimit të një domain kontrolleri të Windows-it. Instalimi i një serveri DNS mund të mos kryhet në rrjetet e vogla, të cilat nuk përdorin domaine. Për akses në Internet të klientëve duhet një Proxy- Server i pajisur me të dhënat e një serveri të jashtëm DNS. Për përgatitjen e punës së DNS-së në një domain Windows-i ekzistojnë mundësitë e mëposhtme:

- ☑ Instalim i ri i DNS-së së Windows-it para ose gjatë instalimit të domain kontrollerit të parë të domain-it të Windows-it.
- ☑ Aktualizimi i një serveri ekzistues DNS në Windows Server 2003
- ☑ Mbajtja e një serveri DNS ekzistues me një sistem tjetër operativ, përsa kohë tek ky server DNS-je kryen hedhjet SRV (e detyrueshme) dhe bëhet përditësimi dinamik i zonave (opsionale).

Kryerja e konfigurimit të DNS-së për një lidhje në rrjet

Klientët kanë nevojë për DNS-në, me qëllim që të lokalizohen resurset brenda një domaini Windows-i, ndër të tjera dhe vetë domain kontrolleri. Pa deklarimin e një serveri DNS në domain-in respektiv, një klient nuk mund të shtohet në domain. Të dhënat e serverit DNS tek klientët mund të hidhen ose manualisht, ose mund të caktohen nga DHCP-ja si pjesë e konfigurimit të përgjithshëm të TCP/IP-së.

Proxy-Server-i

Në lidhje me trafikun në Internet shpesh përdoren Proxy-Servera për të kryer dy detyra. Nga njëra anë ato shërbejnë si cache, pra si memorie për ruajtjen e informacioneve (faqeve të internetit), të cilat duhet të jenë kërkuar dhe thirrur të paktën një herë në Internet.

Fusha tjetër e përdorimit ka si qëllim, daljen në internet të adresave të brendshme (private) të IP-së duke përdorur një adresë të vetme publike. Në këtë rast përdoret NAT-i (Network Address Translation), i cili përshkruhet ndryshe edhe si IP-Masquerading.

Në firmat e mëdha shpesh nuk është e mundur, ose nuk ka kuptim, pajisja e çdo klienti me një adresë publike IP-je. Prandaj, zakonisht konfigurohet një server me minimumi dy adresa IP-je: një private, e cila i përket rrjetit të firmës dhe një adresë publike të vlefshme në Internet.

Të gjithë klientët i dërgojnë kërkesat e tyre për Internet tek Proxy-Server-i, i cili ndryshon elementë të tyre dhe i kalon më tej në Internet. Proxy-Server-i zëvendëson dy elementë në paketën e IP-së që merr nga klientët: Adresën burim të IP-së së klientit, të cilën e zëvendëson me adresën e tij publike dhe portën burim të klientit të cilën e zëvendëson me një portë të papërdorur të proxy-t. Proxy-Server-i organizon për këtë një tabelë, në të cilin memorizohet, cili kombinim klient-IP dhe klient-portë i përket portës respektive në Proxy-Server.

Kompjuteri destinacion në Internet identifikon si adresë IP-je të dërguesit vetëm adresën e IP-së së proxy-t dhe në këtë mënyrë e dërgon përgjigjen e tij tek numri përkatës i portës së proxy-t. Në varësi të numrit të portës që merr si përgjigjë, proxy serveri kontrollon në tabelën e tij të brendshme, se cilës adresë IP-je dhe cilit numër porte, në rrjetin e brendshëm, i duhet dërguar përgjigja. Këto të dhëna ndryshohen në paketën e ardhur të IP-së.

Në këtë mënyrë bëhet e mundur që disa adresa të brendshme (intern) të dalin me një adresë të jashtme (extern) në Internet, gjë e cila mund të përdoret për anonimizimin e trafikut në Internet. Një përparësi e NAT-it që ka lidhje me sigurinë është, që kompjuteri në LAN nuk mund të aksesohet direkt nga jashtë rrjetit dhe në këtë mënyrë nuk mund të sulmohet direkt.

9.3 Subnetmaskat dhe subnetet

Subnetmaska

Gjatë vlerësimit të adresave të IP-së, nëpërmjet klasave të adresave, mjafton dhënia e një adrese IP-je, që të identifikohet pjesa e adresës së rrjetit dhe të hosteve. Subnetmaska (subnet mask) paraqet një alternativë për përdorimin e klasave të adresave. Përparësia kryesore është mundësia që gjatësia e adresës së rrjetit të shtrihet jo vetëm në nivelin e okteteve të plota, siç ndodh me adresat e klasave A deri C. Me ndihmën e caktimit të një subnetmaske të caktuar, së bashku me caktimin e një adrese IP-je, ekziston mundësia që adresa e rrjetit të mbarojë në çdo shifër të adresës së IP-së që ne preferojmë.

Subnetmaska përpunohet nga hosti, si çdo adresë IP-je e dhënë 32 bitshe e gjatë. Ajo nuk përbëhet nga një rradhë e cfarëdoshme numrash binarë, por fillon me një binar 1 dhe përmban maksimumi një ndryshim në binarin 0, p.sh.:

11111111 00000000 00000000 00000000 ose 255.0.0.0

Si rregull, shifrat binare të subnetmaskës, vlera e të cilave është 1, tregojnë adresën e rrjetit. Të gjitha shifrat binare të subnetmaskës, që e kanë vlerë 0, i përkasin adresës së hostit. Kjo gjë dallohet menjëherë shumë qartë në paraqitjen binare të adresës:

Adresa e IP-së	192.168.1.100 =	11000000	10101000	00000001	01100100	
Subnetmaska	255.255.255.0 =	11111111	11111111	11111111	00000000	
		Adresa e rrjetit			Adresa e Hostit	

Krahas mënyrës decimale të të shkruarit, ekziston edhe një mënyrë tjetër e thjeshtuar, e cila tregon numrin e shifrave që mbulojnë adresën e rrjetit, pas një adrese IP-je. P.sh. adresa e IP-së 192.168.1.100, me subnetmaskë me 24-shifra, 255.255.255.0, mund të shkruhet ndryshe edhe si 192.168.1.100/24.

Funksioni i subnetmaskës

Subnetmaska cakton, cilës pjesë të rrjetit i përket adresa e IP-së. Prandaj është e detyrueshme dhënia e një sub-netmaske së bashku me adresën e IP-së. Me anë të subnetmaskës, pjesa e adresës së rrjetit të kësaj adrese IP-je përcaktohet saktë dhe një ndryshim i subnetmaskës do të thotë një ndryshim në përkatësinë e pjesës së rrjetit.

Një host e përdor subnetmaskën, me qëllim që të përcaktojë se cila pjesë e adresës së vet të IP-së i përket adresës së rrjetit. Përfundimisht ai përcakton adresën e pjesës së rrjetit të partnerit të tij në komunikim dhe fikson se si do të transmetohen të dhënat. Për këtë ai përdor një operator logjik EDHE (AND), që mbledh adresen e IP-së me subnetmaskën e vet. Nëpërmjet kësaj **nëndarjeje**, çdo Bit i adresës së IP-së kombinohet me bit-in përkatës të subnetmaskës së vet. Sipas rregullave të mbledhjes së shifrave binare, operatori logjik AND jep në këtë mënyrë adresën e rrjetit, p.sh:

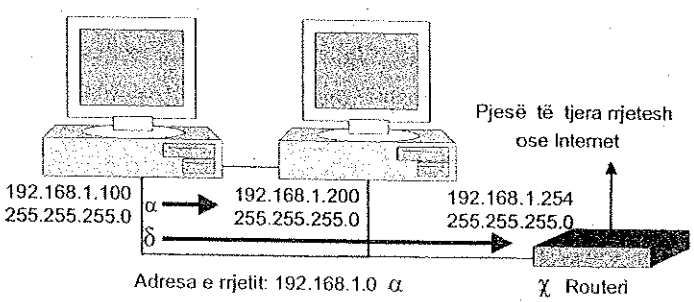
Adresa e IP-së	192.168.1.100 =	11000000	10101000	00000001	01100100	
Subnetmaska	255.255.255.0 =	11111111	11111111	11111111	00000000	
Mbledhja	192.168.1.0 =	11000000	10101000	00000001	00000000	Adresa e rrjetit

Në fund ky proces përsëritet me subnetmaskën e vet për adresën e IP-së së partnerit me të cilin komunikon (adresën e destinacionit), p.sh:

Adresa e destinacionit	192.168.1.200 =	11000000	10101000	00000001	11001000	
Subnetmaska	255.255.255.0 =	11111111	11111111	11111111	00000000	
Mbledhja	192.168.1.0 =	11000000	10101000	00000001	00000000	Adresa e rrjetit

Adresa e pjesës së rrjetit të hostit dhe e partnerit në komunikim në këtë rast janë të njëjta α. Prandaj, të dhënat sipas specifikimeve të IP-së, i dërgohen marrësit që ndodhet në të njëjtën pjesë të rrjetit β. Komunikimi i drejtpërdrejtë në këtë rast është i mundur.

Në rast se pas rezultatit të nëndarjes partneri në komunikim i një hosti nuk gjendet në të njëjtën pjesë të rrjetit me të, komunikimi bëhet i mundur vetëm nëse Hosti ka akses në një **router** χ (standard-gateway). Të dhënat dërgohen më pas në këtë router δ, i cili merr përsipër dërgimin më tej të tyre.



Komunikimi brenda dhe jashtë një segmenti rrjeti IP

Subnetmaskat standarde dhe jo standarde

Në vend të përcaktimit të klasave A, B dhe C mund të përdoren subnetmaskat e mëposhtme:

☑ 11111111 00000000 00000000 00000000 = 255.0.0.0 për ish rrjetet e klasës-A
☑ 11111111 11111111 00000000 00000000 = 255.255.0.0 për ish rrjetet e klasës-B
☑ 11111111 11111111 11111111 00000000 = 255.255.255.0 për ish rrjetet e klasës-C

Këto subnetmaska përshkruhen si **subnetmaska të natyrshme**, ose **subnet-maska standard** dhe ofrojnë të njëjtin funksionalitet si ato të klasave ekzistuese.

Në rast se duhet të realizohen subnete, të cilat devijojnë nga vlerat standarde, kërkohen **sub-net---maska jo standarde** të përshtatshme. Subnetmaskat e shtyjnë kufirin midis pjesës së adresës që i takon rrjetit dhe asaj që i takon hosteve një një vend të dëshiruar brenda adresës së IP-së. Subnetmaskat jostandarde janë konceptuar si më poshtë:

- ☑ 10000000 = 128
- ☑ 11000000 = 192
- ☑ 11100000 = 224
- ☑ 11110000 = 240
- ☑ 11111000 = 248
- ☑ 11111100 = 252
- ☑ 11111110 = 254

Në parim, secili oktet i subnetmaskës fikson kufirin midis adresës së pjesës së rrjetit dhe të pjesës së hosteve. Në praktikë, në varësi nga madhësia e rrjetit ekzistues, ndërtohen më shpesh subnete të klasave B dhe C.

Bëni kujdes, se përdorimi i subnetmaskës **255.255.255.254 nuk ka** kuptim, pasi në këtë rast mbetet vetëm një bit për adresat e hosteve. Ky bit përmbush detyrimisht njërin nga dy kushtet e papranueshme: "të gjitha Bitet = 0" ose "të gjitha Bitet = 1". Si pasojë nuk mund të adresohet asnjë host. Subnetmaska e parë që ka kuptim për rrjetet e klasës C është **255.255.255.252** me saktësisht dy adresa të vlefshme, të cilat mund të përdoren për lidhjen me dy routera.

Llogaritja dhe përdorimi i subnetmaskave jo standarde

Meqë përkatësia e një adrese IP-je fiksohet nëpërmjet biteve të ndryshueshme të subnetmaskës, është e mundur që të përshtatet saktësisht, sipas nevojës së një të interesuari, numri i adresave të hosteve në një pjesë të caktuar rrjeti. Për këtë ka dy mundësi:

- ☑ **Subnetting** për ndarjen e një rrjeti ekzistues në nënrrjete (subnete) të vogla me më pak adresa hostesh; të gjitha subnetet e përfituara nga kjo ndarje mund t'u jepen të interesuarve të ndryshëm, të cilët do të marrin sipas rastit adresat e rrjetit dhe subnetmaskën e saktë respektive.
- ☑ **Supernetting** për bashkimin e disa pjesëve të rrjeteve fqinjë për të interesuarit, të cilët kanë nevojë për më shumë adresa hostesh se ç'ofron p.sh. një rrjet i vetëm i klasës C.

Procesi i pëcaktimit të një subnetmaske të përshtatshme për një rrjet të dhënë mbetet njëlloj si për subnetting, ashtu edhe për supernetting.

Këshilla për përllogaritjen e subnetmaskës

Bazë për llogaritjen e një subnetmaske të përshtatshme është numri i nevojshëm i adresave të hosteve ose i nënrrjeteve që duhen krijuar. Subnetmaska duhet të zgjidhet në mënyrë të tillë që, për subnetet dhe hostet të krijohet numri i dëshiruar i shifrave për adresimin e tyre. Në rastin e mëposhtëm, pjesa e adresës së rrjetit të çdo nënrrjeti të krijuar nëpërmjet përdorimit të një subnetmaske jostandarde përbëhet nga 28 shifra binare. 24 nga këto shifra janë shifra binare të një subnetmaske normale **N** të klasës C, ndërsa 4 shifrat e tjera shtohen për identifikimin e **subnetit S** të adresës së rrjetit. Shifrat e mbetura **H** përfaqësojnë bitet egzistuese për adresimin e hosteve.

Subnetmaska	255.255.255.240 =	11111111	11111111	11111111	11110000	
Funksioni		NNNNNNNN	NNNNNNNN	NNNNNNNN	SSSSHHHH	

RFC 950, ashtu si edhe në rastin e adresave të hosteve, e ka ndaluar identifikimin e subneteve, prej vetëm 0 ose 1: Subnetet vetëm 0, në routimin e bazuar në klasa nuk marrin asnjë adresë të dallueshme në rrjet, si dhe adresa e broadcast-it me vetëm 1 subnete është njëlloj me adresën speciale të broadcast-it **all subnets directed broadcast**. Me daljen e routimit të adresave pa klasa, tek të cilat çdo adresë rrjeti qartësohet nëpërmjet një subnetmaske individuale, këto probleme janë zhdukur.

Për këtë arsye, me RFC 1812, u lejua sërish shrytëzimi i subneteve vetëm 0 dhe vetëm 1. Por kjo nuk do të thotë, që të gjithë routerat e kontrollojnë routimin në një rrjet pa klasa. Përpara se të ndryshoni të gjitha adresat ekzistuese në një rrjet nëpërmjet subnetting, duhet të siguroheni që routeri të mund t'u adresohet atyre në mënyrë korrekte. Windowsi në përputhje me standardin, është në gjendje ta bëjë këtë.

Në qoftë se përdorni ende routera të cilët nuk mund të punojnë me subnetet me vetëm 0 dhe vetëm 1-sha, atëhere një pjesë e madhe e subneteve dhe adresave ekzistuese të hosteve dalin jashtë loje. Përveç kësaj nuk lejohet përdorimi i subnetmaskës 128 bit-she. Ajo ofron vetëm një shifër për identifikimin e subnetit, shifër e cila krijon detyrimisht një subnet vetem 0 ose 1.

Përcaktimi i subnetmaskës për një numër të caktuar adresash hostesh

→ Përcaktoni numrin e shifrave binare, të cilat nevojiten për adresimin e numrit të dëshiruar **n** të hosteve.

→ Llogaritni **n + 2**, me qëllim që nga përdorimi i adresës së rrjetit dhe adresës për broadcast të balancohen 2 adresat e mundshme të hosteve.

→ Përcaktoni numrin me fuqinë të 2-shit, e cila është më e madhe ose baraz me (n + 2). Eksponenti jep numrin e shifrave të nevojshme të adresës së hostit.

Në rast se duhen adresuar p.sh. 370 hoste në një rrjet, nevojiten të paktën

n + 2 = 372

adresa. Numri tjetër i plotë, në të cilin duhet të ngrihet në fuqi 2-shi është

$2^9 = 512$,

nevojiten pra 9 shifra të adresës së IP-së për hostet. Ekziston gjithsesi një rezervë prej

512 - 370 = 142

adresash të mundshme, të cilat mbeten gjendje për adresimin në të ardhmen të hosteve.

→ Përcaktoni oktetin, që duhet të përmbajë subneti për t'u dalluar.

Për 9 shifrat e adresave të hosteve shembulli i mësipërm jep oktetin nr.3. Nga ky duhet hequr një shifër e adresës së rrjetit dhe t'i shtohet adresës së hostit.

Shifrat binare të subnetmaskës		11111111	11111111	11111110	00000000	
Funksioni		NNNNNNNN	NNNNNNNN	SSSSSSSH	**HHHHHHHH**	9 shifra H
Nr. oktetit		1.	2.	3.	4.	

→ Përcaktoni si përfundim subnetmaskën e duhur për shifrat e mbetura S të adresës së rrjetit.

Shifrat binare të subnetmaskës		11111111	11111111	**11111110**	00000000	
Mënyra e shkrimit të vlerave decimale		255	255	**254**	0	

Rezulton subnetmaska 255.255.254.0. Nominalisht ky është subnet i klasës B (subnetting), por ai mundet të ndërtohet nëpërmjet maskimit të adresave të dy diapazoneve fqinjë të adresave të klasës C (supernetting).

Përcaktimi i subnetmaskës për një numër të caktuar rrjetesh

→ Përcaktoni si më sipër numrin e shifrave binare për adresat e hosteve, të cilat nevojiten për dallimin e subnetit.

→ Përcaktoni nga numri i këtyre shifrave vlerën decimale përkatëse, në të cilën, duke filluar nga e majta e njw okteti shtoni shifrat e nevojshme pwr identifikimin e subnetit.

→ Zëvendësoni në subnetmaskën e natyrshme të rrjetit ekzistues oktetin e parë të adresave të hosteve nëpërmjet vlerës decimale të përcaktuar.

Në rast se p.sh. rrjeti ekzistues i klasës C 192.168.1.0 duhet ndarë në 2 subnete, jepni vlerat e mëposhtme:

Për adresimin e 2 rrjeteve të pjesshme nevojiten 2 subnete dalluese. Nga

$2 = 2^1$

rrjedh që për këtë nevojitet 1 shifër. Vlera përkatëse decimale është:

10000000 = 128

Meqë këtu nënndarja bazohet në një rrjet të klasës C, duhet që kjo vlerë e subnetmaskës të shfaqet në oktetin e fundit. Jepet

255.255.255.128

si subnetmaska e kërkuar.

Nëpërmjet kësaj subnetmaske krijohen 2 subnete të pavaruara me karakteristikat e mëposhtme:

Adresa e rrjetit 1	11000000	10101000	00000001	00000000	= 192.168.1.0/25
Adresa broadcast 1	11000000	10101000	00000001	01111111	= 192.168.1.127/25
Adresa e rrjetit 2	11000000	10101000	00000001	10000000	= 192.168.1.128/25
Adresa broadcast 2	11000000	10101000	00000001	11111111	= 192.168.1.255/25
Funksioni i shifrës	NNNNNNNN	NNNNNNNN	NNNNNNNN	SHHHHHHH	

Në të dyja rrjetet e pjesshme mund të adresohen respektivisht $2^7 - 2 = 126$ hoste.

Në subnetin 1 janë të shfrytëzueshme adresat 192.168.1.1.....192.168.1.126, në sub-netin 2 adresat 192.168.1.129.....192.168.1.254.

Efektet

Nëpërmjet ndarjes në subnete rezulton së pari një reduktim i numrit të adresave në dispozicion të hosteve. Në shembullin e mësipërm, numri i adresave të hosteve nga 254 zbret në 252. Kjo zbritje bëhet drastike, kur nuk mund të përdorni asnjë subnet tjetër veç atyre 0 dhe 1. Referuar shembullit të mësipërm, subnetmaska e kërkuar nuk do të ishte më 128, por 192. Në këtë mënyrë mbeten ende adresat e rrjetit 192.168.1.64 dhe 192.168.1.128 me respektivisht 62 hoste në dispozicion.

Një efekt tjetër i rëndësishëm i subnetting është që ndryshimet e adresës së IP-së së një klienti, në një oktet që i përket adresës së hostit, nuk kanë ndikim në përkatësinë e rrjetit: Ndërsa në rrjetin 192.168.1.0 me subnetmaskë 255.255.255.0 klientët që i përkasin oktetit të fundit të të njëjtit rrjet adresat marrin adresa midis 1 dhe 254, për subnetmaskën 255.255.255.128 nuk është më i përshtatshëm. Një host me adresë 192.168.1.100 gjendet në të njëjtën pjesë të rrjetit si hosti 192.168.1.150. Këto hoste mund të komunikojnë vetëm nëpërmjet një routeri, në qoftë se ato lidhen në të njëjtin rrjet fizik. Shumë shpesh, ky përbën burimin e gabimit në rrjetet me subnetmaska jo standarde.

Subnetting

Subnetting përdoret për nëndarjen në rrjete të pjesëshme logjike të rrjeteve të mëdha fizike.

Kështu p.sh, rrjeti me adresë **192**.168.1.0 dhe subnetmaskë 255.255.255.0 do të ndahet nëpërmjet subnet-maskës 255.255.255.192 në katër rrjete 192.168.1.0, 192.168.1.64, 192.168.1.128 dhe 192.168.1.192.

[illegible]	Adresat e hosteve			Adresat për broadcast
[illegible]	192.168.1.1	deri	192.168.1. 62	192.168.1. 63
[illegible]	192.168.1.65	deri	192.168.1.126	192.168.1.127
[illegible]	192.168.1.129	deri	192.168.1.190	192.168.1.191
[illegible]	192.168.1.193	deri	192.168.1. 254	192.168.1.255

Adresat e subneteve

Adresat e subnetit dallohen ngaqë të gjitha shifrat e saj, në diapazonin e hosteve, përbëhen vetëm nga shifra binare zero. Diapazoni i hosteve është diapazoni, i cili në subnetmaskë përbëhet vetëm nga zero binare. Më poshtë paraqitet subneti 192.168.1.0 me subnetmaskën 255.255.255.192:

Okteti i parë	Okteti i dytë	Okteti i tretë	Okteti i katërt
192	168	1	0
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0

Adresat për broadcast

Adresa për broadcast dallohet ngaqë në diapazonin e hosteve të gjitha bitet janë një. Nëpërmjet saj i adresohemi të gjitha sistemeve të rrjetit:

Okteti i parë	Okteti i dytë	Okteti i tretë	Okteti i katërt
192	168	1	63
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 1 1 1 1 1 1
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0

Adresa për broadcast e subnetit do të përdoret p.sh. për rezolucionin e emrave në emra të NetBIOS-it.

Diapazoni i hosteve

Diapazoni i hosteve përfshin të gjitha adresat, të cilat gjenden midis adresës së rrjetit (X. X. X. x x 0 0 0 0 0 0) dhe adresës për broadcast (X. X. X. x x 1 1 1 1 1 1), gjithashtu X. X. X. 1 deri X. X. X. 62.

Adresa e parë e hostit

Okteti i parë	Okteti i dytë	Okteti i tretë	Okteti i katërt
192	168	1	1
1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 1
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 0 0 0 0 0 0

Adresa e fundit e hostit

Okteti i parë	Okteti i dytë	Okteti i tretë	Okteti i katërt
192	168	1	62
1100 0000	1010 1000	0000 0001	0011 1110
1111 1111	1111 1111	1111 1111	1100 0000

Rrjetet pasuese

Në subnetet e të njëjtit rrjet vlejnë të njëjtat përcaktime për adresën e rrjetit, adresën për broadcast dhe diapazonin e hosteve. Gjithashtu, adresa specifike e rrjetit nuk lejohet të ndryshohet. Të vetmet që mund të ndryshohen, janë bit-et e subnetit; në shembullin e dhënë, biti i parë dhe i dytë i oktetit të katërt.

[illegible]	192. 168. 1. 00 x x x x x x
[illegible]	192. 168. 1. 01 x x x x x x
[illegible]	192. 168. 1. 10 x x x x x x
[illegible]	192. 168. 1. 11 x x x x x x

Adresat mund të interpretohen edhe sikur fiksojnë dy vlera decimale së bashku. Në të vërtetë, paraqitja e shifrave decimale nuk është shumë e „emrave" të vlerave të biteve.

Atëhere rrjeti i parë do të paraqitej si më poshtë:

Rrjeti:	192.	168.	1.	0 plus 0
Diapazoni i hosteve:	192.	168.	1.	0 plus 1 deri 62
Broadcast:	192.	168.	1.	0 plus 63

dhe rrjeti i dytë do të ishte:

Rrjeti:	192.	168.	1.	64 plus zero
Diapazoni i hosteve:	192.	168.	1.	64 plus 1 deri 62
Broadcast:	192.	168.	1.	64 plus 63

Këshilla për sjelljen me adresat e IP-së

Këshillat e mëposhtme nuk sjellin ndonjë gjë të re përsa i përket njohurive mbi IP-të, por ato mund të ndihmojnë në identifikimin e shpejtë të gabimeve në kompjuterat me adresa IP-je të konfiguruara. Kështu mund të dallohen rreth 50 % e të gjitha adresave të rrjetit të llogaritura gabim, meqë janë numra jo standard. Një numër jo standard tregon gjithmonë që biti i fundit është i fiksuar. Bit-i i fundit duhet të gjendet në diapazonin e hosteve.

- ☑ Një adresë rrjeti duhet të jetë gjithmonë fuqi e njëshit.
- ☑ Një adresë broadcast nuk është asnjëherë numër standard, i cili është 1 më i vogël se një fuqi e njëshit.
- ☑ Adresa më e lartë e rrjetit dhe subnetmaska në oktetin e hostit duhet të jenë identike p.sh. 165.34.224.0 me subnetmaskën 255.255.224.0.

Supernetting

Krahas mundësisë, që një rrjet i madh të nëndahet në njësi më të vogla, ekziston edhe mundësia, e bashkimit të disa rrjeteve nëpërmjet zgjerimit të diapazonit të hosteve.

Adresat e rrjetit	Subnetmaska	Adresat e hosteve	Adresat për broadcast
[illegible]	255.255.255.0	192.168.0. 1 deri 192.168.0. 254	192.168.0. 255
[illegible]	255.255.255.0	192.168.1. 1 deri 192.168.1. 254	192.168.1. 255
Termi profesional	Me subnetmaskë	Diapazoni i përbashkët i hosteve	Adresë e re broadcasti
[illegible]	255.255.254.0	192.168.0. 1 deri 192.168.1.254	192.168.1.255

Supernetting luan një rol të veçantë në bashkimin e rrugëzimeve (routes). Le të shqyrtojmë skenarin, sipas të cilit, një rrjet i një kompanie shtrihet në dy ndertesa, respektivisht dykatëshe secila. Në ndërtesën 1, në katin e parë, gjendet një kompjuter që i përket rrjetit 192.168.0.0 dhe në ndërtesën 2, në katin e dytë, një kompjuter që i përket rrjetit 192.168.1.0, Të dyja disponojnë një router për kat. Aksesi në ndërtesën 2 sigurohet nëpërmjet routerit të ndërtesës RN1. Routeri i ndërtesës 2, RN2, duhet t'i dërgojë tek RN1 të gjitha paketat që destinohen për rrjetet 192.168.0.0/24 dhe 192.168.1.0/24 pa u kujdesur për shpërndarjen e paketave të veçanta. Për të zvogëluar numrin e rrugëzimeve për arritjen e rrjetit 192.168.0.0/23, përdoret Gateway GN1. GN1 duhet të kujdeset pikësëpari për shpërndarjen e paketave në routerat e veçantë të kateve.

Termi profesional për bashkimin e rrugëzimeve është **route aggregation**. Ky proces është i mundur vetëm kur kthehemi tek interdomain routing pa klasa (Classless Interdomain Routing, CIDR).

9.4 Paketat IP

Mënyra e punës së protokollit IP

Në pjesën e parë të këtij kapitulli u shqyrtua ndërtimi dhe funksioni i adresave të IP-së. Në vazhdim do të trajtohet mënyra e punës së protokolleve. Këtu futet ndarja e të dhënave në paketa të përshtatshme dhe pajisja e këtyre paketave me një Header (Encapsulation).

Encapsulation

Të dhënat e një aplikacioni dërgohen nga shtresa e aplikacioneve (Application Layer) në shtresën që kryen transportin (Transportation Layer). Atje pajisen me nje TCP- ose UDP-Header dhe ndahen në Datagrame. Që këtu, shtresa e transportit i dërgon më tej datagramet në shtresën e rrjetit, ku ato ndahen në paketa dhe pajisen me Headers:

Application Layer: Data	Data
Transport Layer: Datagram	TCP-Header DATA
Network Layer: Packet	IP-Header TCP-HEADER DATA
Data Link Layer: Frame	Eth-Header IP-HEADER TCP-HEADER Trailer
Physical Layer: Bits	1 0 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 1 1 0 0 1.....

Paketa IP

Një paketë IP bashkon një Header me datagramin e segmentuar të shtresës së transportit. Madhësia maksimale teorike e një pakete IP-je është 64 Kilobyte, ndërsa në praktikë paketat e IP-së kufizohen në rreth 1500 Byte, meqë në të kundërt do të kapërcehej madhësia maksimale e Ethernet-Frames.

IPv4-Header

Header-i i një pakete IP tek versioni IPv4 ka si rregull një madhësi prej 20 Byte. Kjo sigurisht mund të variojë nga 20 Byte deri në 60 Byte. Tek IPv6 madhësia e Header-it arrin dyfishin e madhësisë.

Në tabelën e mëposhtme çdo rresht i përket një blloku 32-Bit-ësh.

1. Byte		2. Byte	3. Byte	4. Byte
Version	Header Length	Service type	Total length	
Identification number			Flags	Fragment Offset
TTL		Protocol-Port	Header-checksum	
Source address				
Destination address				
Options field				Fullbits
Data ...				

Versioni

Në fushën e versionit gjendet versioni i përdorur i protokollit IP. Si rregull, ai është ende IPv4. Sigurisht, supozohet se së shpejti IPv6 do të predominojë gjithmonë e më tepër.

Gjatësia e kreut (Header Length)

Gjatësia e kreut të paketës duhet dhënë, meqë IPv4 punon me një gjatësi kreu variabël, në varësi nga opsionet e përdorura. Dhënia kryhet në fjalë 32-Bit-she. Gjatësia maksimale e fushës prej katër bit përcakton vlerën maksimale prej gjashtëmbëdhjetë fjalë 32-Bit-she = 60 Byte.

Lloji i shërbimit

0	1	2	3	4	5	6	7
Prioriteti			D	T	R		

Në bazë të llojit të shërbimit përcaktohen përparësitë (precedence) nga 0 (normale) deri 7 (paketë kontrolli). Sipas kësaj mënyre paketat përpunohen në bazë të prioriteteve. Me treguesit-Flags D (Delay = Vonesa), T (Throughput = Fluksi) dhe R (Reliability = Besueshmëria) hosti mund të përcaktojë, se mbi cilën vlerë do ta vërë theksin më shumë gjatë transmetimit.

Një shembull për zgjedhjen e prioriteteve është transferimi i të dhënave gjatë sesionit të telnet-it. Normalisht grumbullohen të dhëna derisa paketa të arrijë një madhësi të pranueshme për shfrytëzimin efektiv të bandës. Në këtë rast sesioni i telnetit nuk mund të kryhet, pasi do të duhej të ndodhte dhënia e një numri tepër të madh karakteresh.Në vend të kësaj nevojitet, që transferimi i të dhënave të veçanta të kryhet menjëherë, edhe nëse do të duhet të transportohen më shumë të dhëna që i përkasin Header-it sesa të dhëna të shfrytëzueshme. Me qëllim që madhësia minimale e transmetimit (Minimum Transfer Unit) të mos bjerë poshtë minimumit të lejuar, paketat duhet të mbushen me të dhëna.

Gjatësia e përgjithshme (Total Length)

Në fushën e gjatësisë së përgjithshme përcaktohet, se cila mund të jetë madhësia maksimale e paketës. Meqë këtu mund të jepen maksimumi 65.535 Byte, si gjatësi e përgjithshme teorike e paketës së IP-së jepet 64 Kilobyte. Host-et sipas specifikimeve të (RFC 791) duhet të përpunojnë paketa IP-je me gjatësi minimumi 576 Byte, por si rregull përdoren paketa prej rreth 1500 Byte.

Identifikimi (Identification)

Të gjitha fragmentet e një datagrami tregojnë të njëjtin numër identifikimi (identification's number). Nëpërmjet tij sigurohet që fragmentet të mblidhen siç duhet së bashku, për të arritur më tej shtresat më të larta. Numri i identifikimit jepet nga dërguesi dhe interpretohet së bashku me adresën burim.

Flags

Flags (treguesit) shërbejnë për kontrollin e fragmenteve. Bit-i i parë nuk përdoret. Bit-i i dytë do të thotë DF (Don't Fragment = mos fragmento), dhe Bit-i i tretë do të thotë MF (More Fragments = Më shumë fragmente).

Fragment offset

Nga vlera e fushës për Fragment Offset përcaktohet, se në cilin vend një fragment është relativisht sa gjatësia e totale e datagramit. Gjatësia e fushës 13 Bit do të thotë, që një datagram mund të transferohet në maksimumi 8192 fragmente.

Time To Live (TTL)

TTL (Time To Live = kohëzgjatja maksimale e jetës së një pakete) përcakton kohëzgjatjen e pritshme të jetës së një pakete IP në 255 sekonda (UNIX, sipas RFC 791) ose 128 sekonda (sistemet operative të Microsoft). Në praktikë nuk ndërmerret ndonjë kufizim kohor, por reduktohet në një TTL-ja e çdo kompjuteri të përpunuar. Në qoftë se routeri duhet të memorizojë më gjatë një paketë në memorjen e tij ndërmjetëse, atëhere vlera e saj duhet të reduktohet herëpashere. Kur arrihet vlera zero, paketa hidhet poshtë (nuk pranohet). Në këtë mënyrë pengohet që paketat të qarkullojnë pafundësisht në rrjet.

Protocol port

Në fushën me portën e protokollit gjendet numri i Service Access Points (SAP) për shtresën e transportit. Këtu përcaktohet se cili protokoll i shtresave më të larta duhet të kryejë përpunimin e mëtejshëm të paketës. Flitet edhe për numra ULP (Upper-Layer-Protocol - Protokoll i Shtresave të Sipërme).

Numrat e shtresës së sipërme të protokollit (ULP) përcaktohen si më poshtë:

Identifik.	Numri	Emri	Përshkrimi
ip	0	IP	Internet-Protokoll, pseudoportë për vetëadresim
icmp	1	ICMP	Internet-Control-Message-Protocol
igmp	2	IGMP	Internet-Group-Multicast-Protocol
ggp	3	GGP	Gateway-to-Gateway- Protocol
tcp	6	TCP	Transport-Control- Protocol
egp	8	EGP	Exterior-Gateway- Protocol
pup	12	PUP	PARC-Universal-Packet- Protocol
udp	17	UDP	Universal-Datagram- Protocol
raw	255	RAW	RAW IP Interface

Header-Checksum

Header-checksum ka të bëjë me një shumë kontrolli për të gjithë IP-Header-in. Ajo përcaktohet si 16 Bit length parity dhe duhet llogaritur sërish nga çdo sistem përpunues, pasi TTL-ja ndryshon pas çdo përpunimi.

Source address, destination address

Këtu gjenden adresa e IP-së së burimit (Source Address), pra e dërguesit dhe adresa e IP-së së marrësit -destinacionit (Destina-tion Address) të paketës.

Opsionet

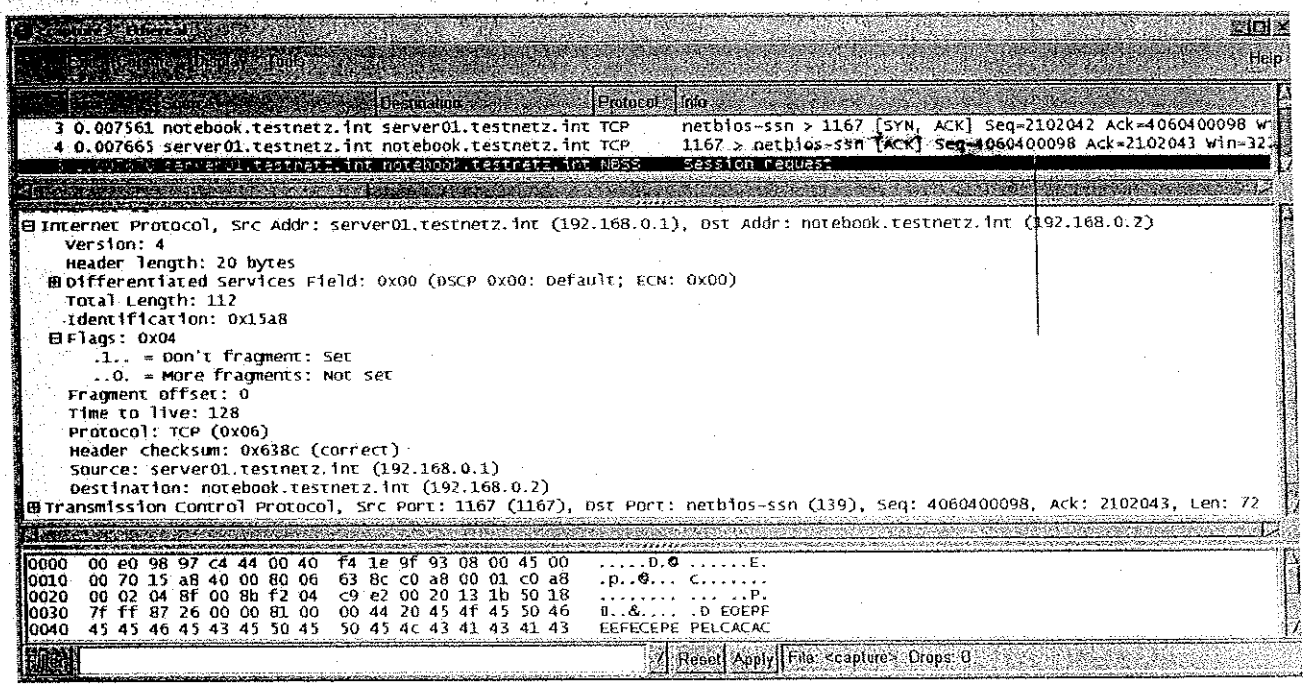
Ka një sërë informacionesh të dallueshme në kreun e paketës, të cilat shërbejnë për gjetjen e rrugëzimeve (routes) dhe eliminimin në shkallë të gjerë të gabimeve gjatë transmetimit. Këto elementë nuk janë objekt i trajtimit të këtij libri. Për t'u thelluar më tej në këtë temë lexoni RFC 791.

Fullbits

Me qëllim që informacioni mbi gjatësinë e paketës të vlerësohet saktë, paketa duhet të përbëhet nga një komplet 32 bit. Me fullbits (padding) bitet e munguara plotësohen më zero.

IP-Header-i në analizuesin e protokolleve

Në figurën e mëposhtme shihni screenshot-in e një analizuesi protokollesh, i cili ka kapur dhe po analizon një pakete të një adrese IP-je:

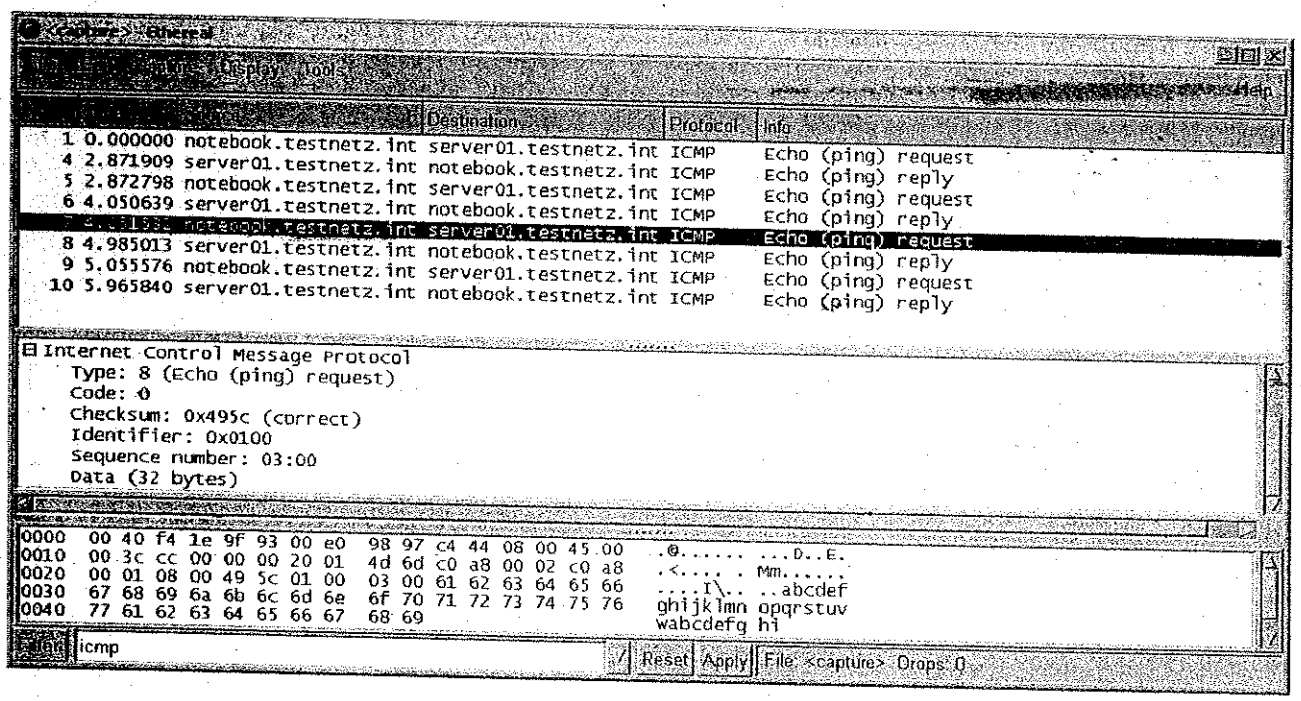


9.5 Internet-Control-Message-Protocol

ICMP

Internet-Control-Message-Protokoll (ICMP) shërben për shkëmbimin e raportimit të gabimeve dhe mesazheve të kontrollit midis pajisjeve në nivel IP-je. Ai thirret si protokoll i IP-së (ULP 1) dhe është protokoll i shtresës 3. Mesazhet ICMP transportohen si payload në fushën e të dhënave të paketave të IP-së.

Komanda më e rëndësishme e cila përdoret për kontrollin e ICMP-së, është komanda PING. Me PING dërgohet një ICMP-Echo-Request në një sistem, i cili nga ana e vet dërgon një ICMP-Echo-Reply. Një ICMP-Echo-Request i përket ICMP-Type 8, një ICMP-Echo-Reply i përket ICMP-Type 0. Në konfigurimin standard të PING-ut dërgohet një sekuencë prej katër kerkesash (requests) dhe përgjigjesh (replies).



Shënime

Një paketë ICMP përmban fushat e mëposhtme:

Type

Informacioni i tipit jep shpjegim, ç'lloj mesazhi ICMP do të dërgohet:

0 Echo Reply	Përgjigje ndaj një kërkese Ping-u nga një system në largësi (remote system)
3 Destination Unreachable	Destinacioni nuk mund të arrihet. Shkaku tregohet në fushën e kodit:0 = Rrjeti nuk mund të arrihet ☒☑ 1 = Hosti nuk mund të arrihet ☒☑ 2 = Protokolli nuk mund të arrihet ☒☑ 3 = Porta nuk mund të arrihet ☒☑ 4 = Nevojitet fragmentim ☒☑ 5 = Rrugëzimi i burimit (Sourceroute) në gjendje jo të mirë
4 Source Quench	Mbingopje e puffer-it; vijnë më shumë datagrame, sesa mund të përpunojë sistemi.
5 Redirect	Një Gateway informon sistemet që ekziston një rrugë më e mirë për në një destinacion të caktuar, si dhe dërgon adresën e IP-së së një Gateway-t të ri.
8 Echo request	Kërkesë për një Echo Reply
11 Time Exceeded for Datagram	Datagrami ka rënë. Shkaku tregohet në fushën e kodit: ☒☑ 0 = TTL është kaluar. ☒☑ 1 = Diapazoni maksimal kohor për bashkimin e fragmenteve është kaluar.
12 Parameter Problem on Datagram	IP-Header-i nuk mund të interpretohet. Në kod gjendet një referencë në lidhje me vendin përkatës ku gjendet Header-i.
13 Timestamp Request	Kërkesë për matje kohe në Milisekonda
14 Timestamp Reply	Përgjigje ndaj një kërkese për Timestamp
15 Information Request	Kërkesë për një Network-ID
16 Information Reply	Përgjigje ndaj një kërkese për Network-ID
17 Address Mask Request	Kërkesë për një Subnetmaskë
18 Address Mask Reply	Përgjigje ndaj një kërkese për Address Mask

Code

Këtu mund të merren hollësi në lidhje me llojin e mesazhit.

Checksum

Në fushën e checksum bëhet një shumë kontrolli për fushën e ICMP-së. Kjo është e nevojshme, meqë IP-ja teston vetëm Header-in e vet, por e le të paprekur përmbajtjen e pjesës së të dhënave.

Identifier ose Sequence Number

Kjo fushë vlerësohet, me qëllim që të kryhet klasifikimi pa probleme i një pakete gjatë një korde komunikimi. Gjatë paraqitjes shihet numri i sekuencës 3, meqë bëhet fjalë për kërkesën e tretë të një sekuence ping-u.

Data

Në fushën e të dhënave të paketës së ping-ut gjenden gërmat nga "a" deri tek "w".Nëpërmjet tyre arrihet të përcaktohet ngarkesa e të dhënave, me qëllim që të gjehen sa të jetë e mundur defektet e fragmentimit.

9.6 IPv6

Protokoll i Internetit - Versioni 6

Nëpërmjet protokollit të Internetit (IP), versioni 6 (IPv6, IP-Next Generation, IPnG) synohet të shmangen mungesat e adresave të IP-ve në Internet.Gjithashtu, aplikacionet e reja në fushën e multimedias kanë nevojë për flukse konstante të dhënash, të cilat në versionin IPv4 nuk mund të sigurohen. Gjatë transferimit të figurave të lëvizshme nuk mund të sigurohen shpejtësi transferimi konstante, kështu që lëvizjet nuk do të mund të paraqiten rrjedhshëm. Meqë IPv4 nuk përcakton cilësi shërbimi - Quality Of Service (QoS), atëhere lindi nevoja e përmirësimit të protokollit .

Karakteristikat e IPv6

[illegible]	Adresat IPv6 përbëhen jo më prej 32 Bit, por prej 128 Bit. Në këtë mënyrë disponohen rreth 3,4 herë 10 në fuqi 38 adresa.
[illegible]	Kreu (header) i IPv6 ka ndryshuar komplet. Në favor të adresave dukshëm më të gjata, u hoqën disa informacione të vjetra. Në vend të tyre mbështetet informacioni i klasave të trafikut të komunikimit dhe Header-ave të vjetër.
[illegible]	Me opsionet e reja që ofron IPv6 është pjesërisht e mundur që opsionet e vjetra të IPv4 të bashkë transportohen, ose të lihen mënjanë. Kjo lehtëson dhe thjeshtëzon përpunimin e paketave përmes routerave, të cilët mund t'i kapërcejnë opsionet përkatëse.
[illegible]	Me qëllim mbështetjen e aplikacioneve, të cilat e kanë kritik faktorin kohë, duhet përcaktuar cilësia e shërbimit.
[illegible]	IPv6 u zhvillua për përdorim në Internet dhe përmban mekanizma, të cilat garantojnë autenticitetin dhe integritetin e të dhënave gjatë transportit.
[illegible]	IPv6 u projektua dhe u zbatua që në fillim si një standard me mundësi zgjerimi në të ardhmen, me qëllim që të garantohej mundësia e përdorimit të saj duke marrë parasysh pretendimet e ndryshme.

Sistemet operative moderne, siç janë versionet aktuale të LINUX-it, Windows XP-së apo Windoss Server 2003 e mbështesin tashmë përdorimin e adresave IPv6. Por në fushën e LAN-eve përdoret ende si më parë versioni IPv4. Kalimi në IPv6 kërkon, krahas ndryshimeve të softëareve të rrjetit, edhe ndryshime masive në fushën e hardware-it. Kështu, pajisjet e përdorura deri më sot si kartat e rrjetit, router-at dhe switch-et që punojnë në shtresën e tretë (Layer 3) nuk janë në gjendje të përpunojnë adresa 128-Bit-she. Brenda kufijve të një LAN-i, në një konceptimi të arsyeshëm të tij, duhet të mjaftojnë rezervat e adresave që ofron IPv4.

Shënime

10 TCP dhe UDP

Në këtë kapitull do të lexoni:

→ si funksionojnë TCP-ja dhe UDP-ja
→ si është i ndërtuar Header-i
→ si funksionon një Three-Way-Handshake
→ si e shfrytëzon rrjetin në mënyrë më efikase TCP-ja me Sliding Window Size

Parakushte:

✓ Njohuri bazë mbi rrjetet
✓ TCP/IP-Protocol-Stack
✓ Protokolli i Internet-it

10.1 Funksioni dhe ndërtimi i TCP-së dhe UDP-së

Protokollet e transportit TCP dhe UDP

Megjithëse si Transport Control Protocol (TCP), ashtu edhe User Datagram Protocol (UDP) kanë për detyrë të garantojnë transportin e datagrameve, brenda familjes së protokolleve TCP/IP, të dyja protokollet punojnë në një mënyrë shumë të ndryshme.

TCP

Transport Control Protocol dallohet ndaj UDP-së nga një rradhë karakteristikash komplekse, të cilat nga njëra anë sigurojnë transportin e datagrameve, por nga ana tjetër ndikojnë dukshëm në rritjen e ngarkesës së protokollit (protocol-over-head). Për TCP-në, veçanërisht të rëndësishme janë karakteristikat e mëposhtme:

☑ Orientimi nga lidhja (connection oriented)
☑ Besueshmëria
☑ Fleksibiliteti në shfrytëzimin e gjerësisë së bandës

UDP

User Datagram Protocol, nga ana tjetër, është zhvilluar duke patur parasysh para së gjithash karakteristikat e mëposhtme:

☑ Shpejtësinë
☑ Ngarkesën më të vogël
☑ Eliminimin e kontrolleve të tepruara gjatë transportit

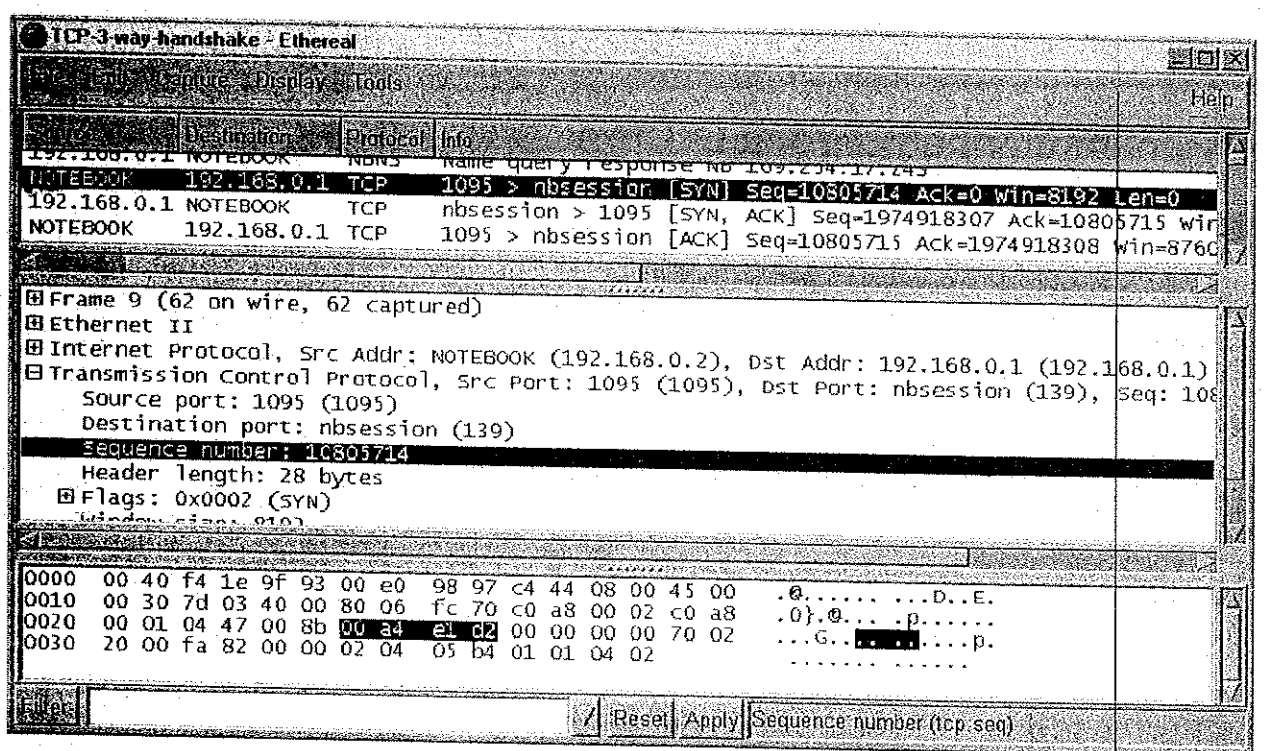
10.2 Mënyra e punës së TCP-së

Orientimi nga lidhja (connection oriented)

TCP-ja përdor Three-Way-Handshake për ndërtimin e lidhjes midis dy sistemeve në komunikim. Këtu bëhet fjalë për një proces, gjatë së cilit dy sisteme, në fillim të një sekuence shkëmbimi të dhënash kryejnë një sinkronizim të shërbimeve të TCP-së. Ky proces kalon tri hapa:

- ☑ Në hapin e parë, dërguesi transmeton një paketë me një kërkesë për sinkronizim (SYN) dhe me një numër sekuence "Seq = X".
- ☑ Në hapin e dytë, marrësi dërgon një konfirmim sinkronizimi (Acknowledgment, ACK). Përveç kësaj, numri i marrë i sinkronizimit rritet me 1 dhe dërgohet si "Ack = X + 1". Njëkohësisht, marrësi nga ana e tij kërkon një sinkronizim (SYN), i cili po ashtu përmban një numër sinkronizimi ("Seq = Y").
- ☑ Në hapin e tretë dhe të fundit dërguesi transmeton një konfirmim (ACK). Kjo paketë përmban numrin e vet të sinkronizimit ("Seq = X+1") dhe një numër konfirmimi ("Ack = Y+1").

Për ta qartësuar këtë proces, three-way-handshake ndiqet me ndihmën e një filtri paketash dhe paraqitet si në figurën e mëposhtme. Në dritaren e sipërme paraqiten tri paketat ndërmjet të cilave dërguesi (Notebook) dhe marrësi (192.168.0.1) replikojnë protokollin e komunikimit të shtresës TCP në komunikim, si dhe informacionin në lidhje me përmbajtjen e paketës. Dritarja e mesit tregon përmbajtjen e paketave të markuara më sipër dhe dritarja e poshtme paraqet përmbajtjen e paketës në formë oktetesh.



TCP-Three-Way-Handshake midis dy sistemeve

Puna me instrumentat e monitorimit dhe mbikqyrjes së rrjetit, siç janë analizuesit e paketave (të quajtura ndryshe edhe si "Network-Sniffers"), nuk është aq e thjeshtë dhe kërkon ushtrim dhe përvojë. Sigurisht ato përbëjnë një mjet mjaft të mirë, për ta kuptuar më thellë komunikimin në rrjet. Instrumenta të tillë ndihmojnë edhe për identifikimin e gabimeve dhe administrimin e burimeve.

Duhet pasur parasysh, se përdorimi i programeve të tilla, për shkak të problemeve që mund të shkaktohen në mbrojtjen e të dhënave, lejohet të përdoret vetëm pas miratimit nga drejtuesit dhe këshilli drejtues i kompanisë. Në rast se nuk jeni të sigurt pyesni gjithmonë një epror para përdorimit të instrumentave të tillë. Përdorimi i ndaluar i software-ve të „spiunimit të rrjetit" mund të ketë pasoja, si në aspektin e humbjes së vendit të punës, ashtu edhe në atë ligjor.

Kërkesat e sinkronizimit

Paketa me kërkesën për sinkronizim dërgohet nga porta 1095 tek session service NetBIOS (Porta 139, nbsessionservice) dhe ka numrin e sekuencës 10805714.

Flags-et e vendosura tregojnë, që bëhet fjalë për datagramin e parë të Hand-shake-ut. Përndryshe, edhe Header-i do të merrte një konfirmim (Acknoëledgement). Kështu vendoset vetëm i ashtuquajturi Syn-chro-nisa-tions-Flag.

Në rreshtat në vijim jepen Win-dow-Size (madhësia maksimale për paketë në Bit), Error Check-sum (shuma e kontrollit të gabimit), si dhe fusha e opsioneve.

```
Transmission Control Protocol, Src Port: 1095 (1095), Dst P
    Source port: 1095 (1095)
    Destination port: nbsession (139)
    Sequence number: 10805714
    Header length: 28 bytes
  Flags: 0x0002 (SYN)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 8192
    Checksum: 0xfa82 (correct)
  Options: (8 bytes)
```

Synchronisations-Flag

SYN-Request i një TCP-Three-Way-Handshake

Datagrami SYN/ACK

Në datagramin e mëposhtëm marrësi dërgon përgjigje për kërkesën për sinkronizim të dërguesit. Po kështu vendoset një Acknowledgement Flag dhe bëhet i njohur Acknowledgement Number. Ky numër i korrespondon numrit të sekuencës së rritur me vlerën 1 të datagramit të marrë më parë, si dhe është numri i sekuencës, i cili pritet në datagramin e rradhës. Në rast se ndodh që sistemi të identifikojë që datagramet nuk janë në rradhën e duhur, atëherë ai i sjell sërish në rradhën e duhur.

Në të njëjtën kohë një sinkronizim kryhet edhe nga marrësi. Në këtë mënyrë sigurohet, që të dy sistemet të mund të garantojnë një transmetim informacioni pa humbje.

```
Transmission Control Protocol, Src Port: nbsession (139), Ds
    Source port: nbsession (139)
    Destination port: 1095 (1095)
    Sequence number: 1974918307
    Acknowledgement number: 10805715
    Header length: 28 bytes
  Flags: 0x0012 (SYN, ACK)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...1 .... = Acknowledgment: Set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 32767
    Checksum: 0x4818 (correct)
  Options: (8 bytes)
```

Header-i TCP i datagramit të dytë të një Three-Way-Handshakes

Siguria ndaj humbjes së të dhënave

Me ndihmën e numrave të sekuencës datagramet mund të sillen në rradhën e duhur. Përveç kësaj, dërguesi mund të identifikojë, nëse brenda një kohe të caktuar nuk vjen asnjë konfirmim (acknowledgement) për një datagram të dërguar. Atëherë ky datagram dërgohet sërish, me qëllim që të eliminohen humbjet e të dhënave gjatë transmetimit.

Kontrolli i rrjedhës së të dhënave

Gjatë transferimit të informacionit mund të ndodhë që *Dërguesi* t'i transmetojë *Marrësit* më shumë të dhëna se sa ky i fundit mund të përpunojë në një moment kohe të caktuar. Në këtë rast, të dhënat memorizohen në një kujtesë të ndërmjetme të quajtur puffer. Meqë puffer-i ka një madhësi të kufizuar, mund të ndodhë mbingopja e puffer-it. Për ta parandaluar këtë, sistemi, puffer-i i të cilit është mbushur plot, dërgon një ECN-Echo (Explicit Congestion Notification Echo). Pas kësaj sistemi dërgues përgjysmon shpejtësinë e dërgimit të të dhënave, derisa sistemi marrës nëpërmjet një CWR-Flag (Congestion Window Reduced) sinjalizon, që transmetimi i të dhënave mund të vazhdojë sërish me shpejtësi normale.

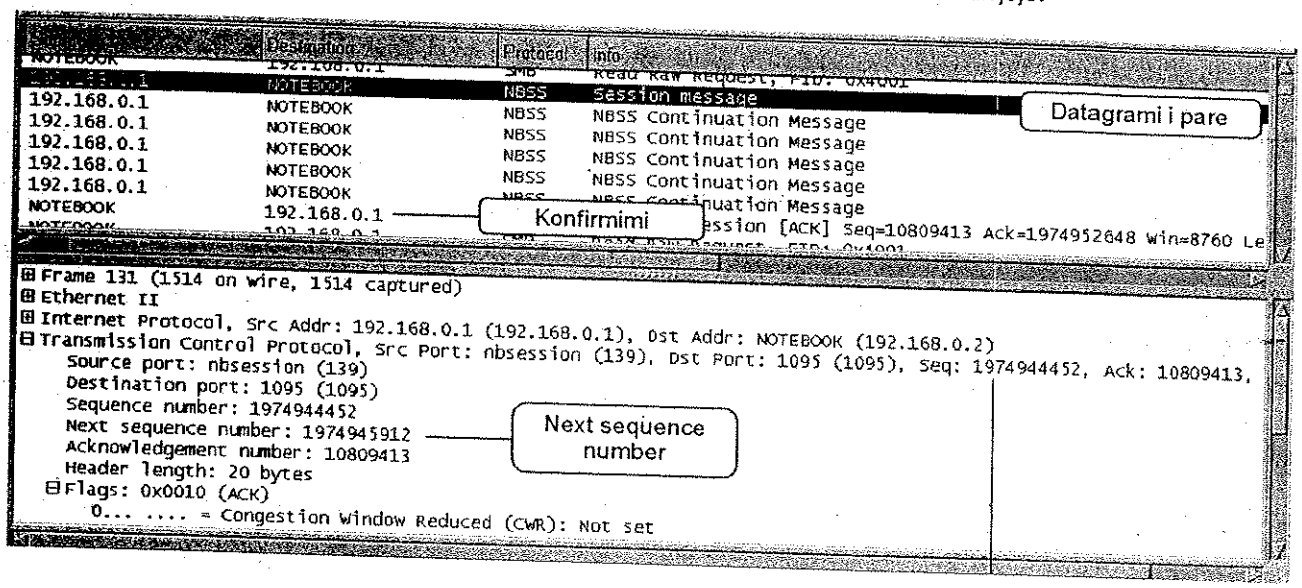
Sliding Window Size

Si rregull, në një rrjet TCP, për çdo datagram të dërguar transmetohet një konfirmim marrjeje (acknowledgement). Ky lloj relacioni midis të dhënave të shfrytëzueshme dhe jo të shfrytëzueshme, e ngarkon dukshëm gjerësinë e bandës së rrjetit. Nëpërmjet përdorimit të Sliding Window Size mund të transmetohen edhe më shumë datagrame, përpara se të bëhet konfirmimi i marrjes së tyre.

Zakonisht, direkt pas një numri sekuence (sequence number) vjen numri i pritshëm i konfirmimit (acknowledgement number). Në rast se janë dërguar disa datagrame njëri pas tjetrit, sistemi punon si përshkruhet më poshtë:

Pas numrit të sekuencës jepet numri tjetër i sekuencës i datagramit pasues, ndërkohë që numri i pritshëm i konfirmimit (Acknowledgement Number) mbetet njëlloj për të gjithë „zinxhirin" e datagramit. Vetëm kur marrësi merr të gjitha datagramet e „zinxhirit", ai dërgon paketën përkatëse të konfirmimit (Acknowledgment-Packet).

Në figurën e mëposhtme shihni një dërgesë prej 6 datagramesh dhe një konfirmim marrjeje.



Detyra të tjera

Krahas detyrave transportuese TCP-ja angazhohet edhe në administrimin e fluksit të të dhënave midis protokolleve të shtresës së aplikacioneve dhe shtresës së rrjetit. Këtu bëjnë pjesë segmentimi i fluksit të të dhënave të shtresës së aplikacioneve, i ashtuquajturi „puffering" i të dhënave, si dhe paralelizimi.

Segmentimi

Gjatë segmentimit të fluksit të të dhënave, të dhënat e shtresës së aplikacioneve (Application layer) grumbullohen dhe prej andej i bashkëngjiten për transmetim paketave, të cilat më pas pajisen me Header-in përkatës për t'u dërguar në shtresën e rrjetit (Network layer).

Puffering

Me qëllim që të dhënat e segmenteve të mund të mblidhen së bashku dhe pas kësaj të mund të dërgohen më tej në rradhën e duhur në shtresën e aplikacioneve, duhet që shtresa e transportit (Transport Layer) të ketë akses në një memorje të vetën (Puffer).

Paralelizimi

Në qoftë se një aplikacioni i nevojiten transferime më të shpejta të dhënash, se ato që mund të ofrohen nga i vetmi kanal në dispozicion, TCP-ja është në gjendje të shfrytëzojë disa lidhje njëkohësisht. Nëpërmjet kësaj bashkësie kanalesh mund të realizohet p. sh. dërgimi i njëkohshëm, nëpërmjet disa kanalesh ISDN, i të dhënave me afate kohore kritike.

Paralelizimi nuk është pjesë përbërëse fikse e TCP-së, por përbën një karakteristikë (feature) shtesë, e cila në sistemet operative moderne si UNIX, apo Windows 2000/XP dhe pasuesit e tyre, vihet në dispozicion nga vetë këto sisteme.

10.3 TCP-Header

Përshkrimi

Header-i (koka e protokollit) i një pakete TCP përmban informacionet e marra më parë, si dhe një rradhë fushash opsionale, të cilat sipas nevojës mund të përdoren për kontrollin e komunikimit. Informacionet e Header-t përmblidhen në blloqe 32 Bit-she (4 Byte). Edhe nëse Header-i do të bëhet më i gjatë, gjithmonë gjatësia do të jetë shumëfish i 4 Byte. Realisht informacionet e Header-it janë 20 Byte të gjata.

Më poshtë jepet një paraqitje skematike e Header-it.

1. Byte	2. Byte	3. Byte	4. Byte
Source Port		Destination Port	
Sequence Number			
Acknowledgement Number			
Header Length	Flags	Windows size	
Checksum		Urgent Flags	
Options	Mbushja me zero deri në arritjen e një shumëfishi të 32 Bit-shit		
Data			

Source Port (16 Bit)

Source Port (porta burim) jep, se nga cila portë në shtresën 5 e kanë origjinën të dhënat, të cilat duhet të transmetohen (të copëzuara në datagrame). Gjatësia maksimale prej 2 Byte i korrespondon vlerës më të lartë të një porte (65.535).

Destination Port (16 Bit)

Destination Port (porta destinacion) jep, se në cilën portë të shtresës 5 duhet të dërgohen të dhënat e rigrumbulluara nga datagramet.

Sequence Number (32 Bit)

Numri i sekuencës shërben po ashtu, që datagramet e marra t'i sjellë në rradhën e duhur, që të kontrollojë rrjedhën e komunikimit, si dhe të identifikojë ndonjë gabim të mundshëm.

Acknowledgment Number (32 Bit)

Acknowledgement Number (numri i konfirmimit) jep se cilin numër sekuence duhet të përdorë sistemi marrës për të konfirmuar marrjen pa probleme të datagramit.

Header Length (4 Bit)

Informacioni mbi gjatësinë e Header-it jep se sa fjalë 32-Bit-she përfshin ky i fundit. Kjo është e nevojshme, pasi gjatësia e Header-it mund të ndryshojë, p. sh. në qoftë se do të bihet dakort për opsione shtesë për kontrollin e rrjedhës së të dhënave.

Flags (12 Bit)

Edhe nëse në një moment të jenë përcaktuar 8 Bit = 8 Flags, sistemi është i parapërgatitur për zgjerim. Në këtë mënyrë forma të veçanta të TCP-së përmbajnë informacione speciale për transferimet satelitore të të dhënave, të cilat marrin parasysh ngadalësime të konsiderueshme tek transmetimet globale.

Windows size

Këtu caktohet sa Bit-e mund të marrë maksimalisht një pajisje njëherazi.

Checksum

Në varësi nga shuma e kontrollit (checksum) marrësi mund të përcaktojë, nëse të dhënat janë ndryshuar gjatë transportit.

Urgent Flags

Në qoftë se tek Flags ekziston një URGENT-Flags (tregues urgjence), të dhënat nuk vendosen në puffer, por fillohet menjëherë nga përpunimi i tyre. Treguesi i urgjencës i referohet në fund të dhënave që janë urgjente për t'u përpunuar. Kjo përdoret p.sh., në qoftë se në një sesion telnet-i do të duhet të transmetohen karaktere të veçantë tek partneri në komunikim.

Options

Këtu, në versionin standard të TCP-së, përcaktohet vetëm madhësia maksimale për segmentet TCP. Pjesa e mbetur e segmentit 32-Bit-sh duhet mbushur me zero, me qëllim që t'i korresopndojë informacionit mbi gjatësinë.

10.4 UDP

Përparësitë dhe fushat e përdorimit

User Datagram Protocol (UDP) përgatit në të njëjtën mënyrë shërbimet për shtresën e transportit, por pa pasur tolerancën e gabimit dhe orientimin nga lidhja të TCP-së. Prandaj protokolli UDP përdoret para së gjithash, në rastet kur shërbimet e shtresave të tjera marrin përsipër kontrollin e lidhjes dhe korrigjimin e gabimeve.

Përparësia e UDP-së ndaj TCP-së qëndron qartazi në mbingarkesën (overhead) e pakët. Kështu protocol-header-i i UDP-së rezulton me një madhësi prej 8 Byte dhe nga mungesa e dërgesave të konfirmimit (acknowledgement) të marrjes kursehet gjerësi bande shtesë.

UDP-ja është e përshtatshme para së gjithash për transmetimet, tek të cilat mendohet se do të ndodhin pak ose aspak humbje të dhënash. Kjo vlen veçanërisht për shërbimet e rrjetit. Pra, për një DNS-Request nuk është i nevojshëm kontrolli i rrjedhës së të dhënave. Në qoftë se serveri përgjigjet, atëhere informacioni përmbahet në një datagram të vetëm, në qoftë se serveri nuk përgjigjet, informacioni transmetohet sërish.

Një fushë tjetër përdorimi e UDP-së janë transmetimet e pastra të të dhënave. Kështu, nëpërmejt UDP-së kryhen transmetimet e të dhënave NFS (Network File System, një sistem organizimi file-sh (Distributed File System) nga SUN). Në rast se do të kishte humbje të dhënash, NFS nëpërmjet shtresës së aplikacioneve kryen sërish kërkimin e të dhënave. Këtu shpejtësia e transmetimit të të dhënave del në plan të parë.

Përballja e protokolleve TCP dhe UDP

Tabela e mëposhtme jep një pamje të përgjithshme të ndryshimeve midis protokolleve TCP dhe UDP.

Detyra	TCP	UDP
Metoda e transmetimit	Transmetim të dhënash i orientuar nga lidhja, three-way-handshake, konfirmimet e marrjes, numrat e sekuencës.	Sa më mirë të jetë e mundur ("As good as possible"), pa lidhje (connection less)
Madhësia e segmentit me të dhëna dhe e header-it	Madhësia e segmenteve me të dhëna trajtohet në mënyrë dinamike ndërmjet sistemeve, ndërsa header-i është midis 20 dhe 28 Byte i gjatë.	Header-i është gjithmonë 8 Byte i gjatë, ndërsa segmentet me të dhëna mund të kenë madhësi të ndryshme.
Kontrolli i rrjedhës së të dhënave	Administrimi i puffer-ave, Sliding Window Size	Nuk ka

Header-i UDP

Ndërtimi i një Header-i UDP:

1. Byte	2. Byte	3. Byte	4. Byte
Source Port		Destination Port	
UDP Header-Length information		Checksum	
Data			

Source Port

Adresa e shërbimit të një shtrese (layer-i) më të lartë, e cila i ka sjellë të dhënat në shtresën e transportit (Transport Layer), jepet në një numër porte 16 Bit e gjatë.

Destination Port

Adresa e shërbimit të një shtrese (layer-i) më të lartë, tek e cila duhet të arrijnë datagramet e shtresës së transportit, jepet në një numër porte 16 Bit e gjatë.

UDP Header-Length information

Këtu jepet që, header-i është 8 Byte i gjatë. Ky informacion në vetevete është i tepërt, por gjithsesi përfshihet bazuar mbi zgjerueshmërinë e protokollit.

Checksum

Në një informacion 16 Bit të gjatë përfshihet headeri dhe shuma e kontrollit (checksum) për të dhënat, me qëllim që të identifikohen ndryshimet e të dhënave gjatë transportit.

10.5 Testimi i lidhjeve të rrjetit

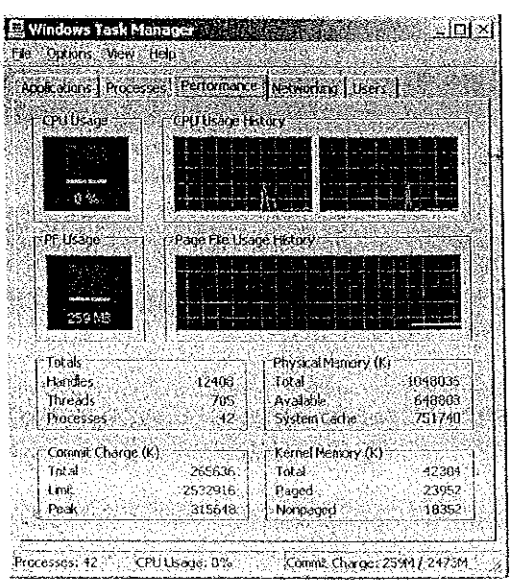
Mbikqyrja e serverit të rrjetit

Si komponentë bazë të një rrjeti, serverat kanë një ndikim të madh në mbarëvajtjen, funksionimin dhe performancën e shërbimeve të ofruara në rrjet. Për këtë arsye, gjendja e serverit, së paku në periudha të caktuara, duhet mbikqyrur (monitoruar) dhe rezultatet duhen protokolluar.

Shumë sisteme operative rrjeti vënë në dispozicion për këtë qëllim programet e tyre të monitorimit. Familja e Wndowsit ofron Task-Manager-in dhe System Monitor-in. Me anë të këtyre instrumentave mund të mbikqyren funksione bazë të serverit dhe rezultatet të paraqiten në formë grafike. Tek System Monitor, përveç kësaj të dhënat e performancës memorizohen si skedar protokolli.

Në funksionet e serverit, të cilat duhen monitoruar me të dyja instrumentat e sipërpërmendura, bëjnë pjesë ndër të tjera:

- ☑ Ngarkesa e procesorit
- ☑ Aktiviteti i diskut të ngurtë
- ☑ Ngarkesa e memorjes operative (RAM)
- ☑ Ngarkesa e rrjetit



Task-Manager-i i Windows XP dhe Server 2003

Në qoftë se në software-t aplikative të serverit është instaluar paketa Back-Office e Microsoft-it, atëhere në System Monitor shpesh mund të monitorohen edhe funksione specifike të programeve. Këtu bëjnë pjesë ndër të tjera aktiviteti i bazës së të dhanave të një Exchange-Server-i (Messaging), ose aktiviteti në rrjet i ISA-Server-it (Proxy dhe Firewall). Monitori i sistemit (System Monitor) do të përshkruhet në mënyrë të hollësishme në kapitullin 19.

Vini re, që në Task-Manager mund të vrojtohen funksionet e serverit, sidoqoftë nuk ekziston asnjë mundësi për memorizimin e të dhënave të performancës.

Shqyrtimi i aktiviteteve standarde

Gjatë punës pa probleme të serverit mund të regjistrohen të dhënat më të rëndësishme të performancës dhe si protokoll performance të memorizohet ngarkesa normale e serverit (aktiviteti standard). Kjo mundëson që më vonë të krahasohen të dhënat e performancës në ngarkesë normale me të dhënat e performancës të një rasti me probleme. Dallimet në ngarkesat e komponentëve të serverit janë lehtësisht të lexueshme.

Për shqyrtimin e aktivitetit standard, monitorit të sistemit i duhet një periudhë kohe e caktuar p.sh. 30 minuta ose një orë, që të protokollohet aktiviteti i serverit. Sidoqoftë, disa servera gjatë kohës së punës nuk janë njëlloj të ngarkuar. Serverat e identifikimit e kanë ngarkesën e punës veçanërisht në periudha speciale kohe, si p.sh. në fillim të punës apo gjatë ndryshimit të turneve. Këtu ofrohet regjistrimi i aktivitetit të serverit në këto periudha kohore speciale dhe një periudhë kohore tjetër gjatë aktivitetit normal të punës.

Monitorimi i komponentëve aktivë të rrjetit

Edhe komponentët aktivë të rrjetit si hub-et, switch-et, apo router-at mund të kenë ndikim mjaft të madh në performancën e rrjetit. Si rrjedhim, duhet monitoruar edhe statusi i këtyre pajisjeve, me qëllim që në rast defekti të mund të reagohet shpejt.

Për këtë qëllim, familja e protokolleve TCP/IP ofron një protokoll të vetin, **Simple Network Mana-ge-ment Protocol (SNMP)**. Komponentët aktivë, të cilat kontrollojnë SNMP-në, zotërojnë një **agjent SNMP**. Ai mund të transmetojë informacione mbi statusin e pajisjeve tek një stacion pune i ngritur për qëllime menaxhimi, i ashtuquajturi **SNMP-Manager**. Transmetimi normalisht kërkohet në mënyrë të rregullt nga SNMP-Manager (Polling), por në rast gabimi mund të iniciohet edhe nga agjentët SNMP të pajisjes së monitoruar (Trap-Info). Tek çdo pajisje, që transmeton informacione mbi statusin nëpërmjet SNMP-së, administrohen disa të dhëna. Ato vendosen në Management Information Base (MIB) dhe janë më pranë për vlerësimin e informacioneve të statusit të pajisjes së monitoruar.

Problemet fillestare të sigurisë me SNMP-në si pasojë e mungesës së autentifikimit dhe kodimit janë eliminuar në versionin 2 të SNMP-së. Shumica e komponentëve aktiv të prodhueve me emër janë kompatibël me SNMP-në.

Monitorimi i trafikut në rrjet

Fluksi i të dhënave përcakton në të gjitha rrjetet, të cilat punojnë me Ethernet, kohën e reagimit gjatë aksesit mbi burimet e rrjetit (network resources). Rrjetet shumë të ngarkuara janë "të ngadalta", pasi çdo klient duhet të presë gjatë derisa të arrijnë paketat me të dhëna që i takojnë atij. Për këtë arsye, monitorimi i trafikut të rrjetit është një tregues i rëndësishëm për performancën e rrjetit.

Trafiku në rrjet në një server me WindoWs NT, WindoWs 2000/XP, apo Windows Server 2003 mund të monitorohet me ndihmën e monitoruesit të rrjetit të Microsoft-it. Novell-i për këtë qëllim ofron LANalyser-in i cili punon me sistemin operativ NetWare.

Monitoruesi i rrjetit i Microsoft-it grumbullon të gjitha të ashtuquajturat „data frames" nga serveri dhe i llogarit statistikisht. Përveç kësaj, ai vlerëson data frames-et dhe jep ndër të tjera informacione në lidhje me protokollin e përdorur dhe adresën e dërguesit. Sipas nevojës mund të tregohet edhe përmbajtja e të dhënave të transmetuara.

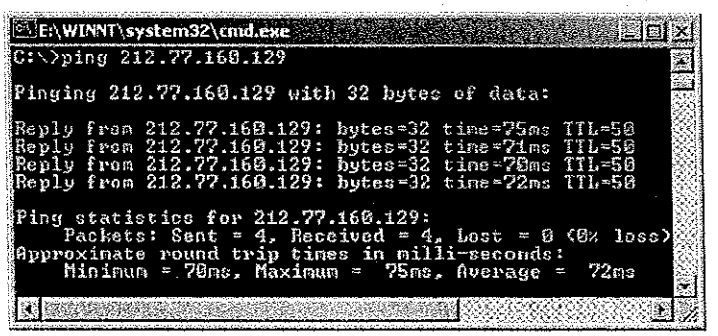
Përdorimi i Ping-ut

Komanda ping teston lidhjen midis dy kompjuterave, të cilët komunikojnë nëpërmjet protokolleve TCP/IP. Ping-u dërgon paketa me të dhëna tek një klient, i cili do të duhet të kthejë një përgjigje. Komanda quhet e ekzekutuar me sukses, kur tregon përgjigjen e klientit të paktën me adresën e tij të IP-së (Reply from - IP address). Nëse lidhja nuk krijohet nuk merret përgjigje (Request timeout).

Procedura e testimit të një lidhjeje me një klient rrjeti në largësi (remote client/host) nga një PC me Windows 2000/ XP është si më poshtë::

Klikoni mbi Start - RUN, dhe shkruani cmd. Hapet dritarja e command prompt-it C:\>.
Atje rrini komanden ping *IP Address*. Si *IP Address* jepni adresën e IP-së së klientit, me të cilin duhet të kontrollohet lidhja.
Windows-i do teston lidhjen me klientin në fjalë disa herë njëra pas tjetrës.

Në qoftë se komanda ping është e suksesshme, atëhere merret një përgjigje nga klienti. Përgjigja përmban ndër të tjera adresën e tij të IP-së, si dhe informacione në lidhje me kohëzgjatjen e transmetimit dhe numrin e Hop-eve të kërkuara.



Ping i suksesshëm tek një kompjuter klient në largësi (remote host)

Në qoftë se Ping-u dështon, atëhere në shumicën e rasteve kthehet si përgjigje **Request timeout**, kur klienti lidhja me të cilin po testohet nuk përgjigjet brenda një periudhe kohe të caktuar. Përsa kohë që nëpërmjet ping-ut jepet adresa e saktë e IP-së, ky njoftim (Request timeout) informon për një lidhje të gabuar, jo aktive, ose për një klient të konfiguruar në mënyrë jo të saktë.

Ping-u mund ta testojë lidhjen me klientin si nëpërmjet adresës së tij të IP-së, ashtu edhe nëpërmjet emrit të Host-it. Në rast se në vend të adresës së IP-së përdoret emri i host-it, atëhere kërkohet para së gjithash të kryhet një DNS-name resolution. Po qe se kjo nuk është e mundur, komanda ping dështon. Prandaj, një test i qartë i lidhjes mund të kryhet vetëm me ndihmën e adresës së IP-së. Në rast se kërkohet që ping-u të kryhet nëpërmjet emrit të host-it atëhere më parë duhet kryer një rezolucion i emrit (name resolution) përmes komandës nslookup, nga e cila del serveri DNS përgjegjës për rrjetin.

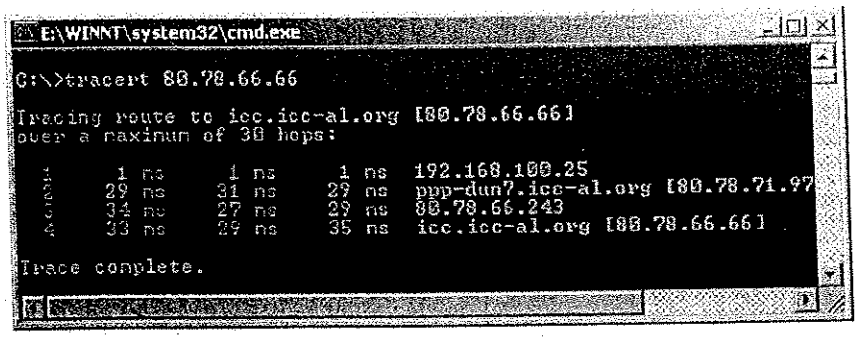
Krahas testit të një lidhjeje me një klient në largësi ping-u mund të përdoret gjithashtu, për të testuar instalimin lokal të TCP/IP-së dhe kartës lokale të rrjetit. Në rast se nga kompjuteri lokal nuk mund të krijohet një lidhje me një kompjuter tjetër të rrjetit, atëhere kompjuterin mund ta testoni si më poshtë:

Në command prompt C:\> jepni komanden ping 127.0.0.1. Kjo quhet ndryshe edhe **Loopback-Address** ose **adresa e vetetestimit** të cdo kompjuteri. Nëse kjo tentativë me ping dështon, atëhere ka problem në instalimin e bashkësisë së protokolleve TCP/IP (TCP/IP protocol stack) në kompjuterin lokal.
Në qoftë se vetetestimi kryhet me sukses, atëhere jepni në command prompt C:\> komanden ping me adresën lokale të IP-së. Në rast se tentativa e testimit me ping dështon, atëhere karta e rrjetit është me defekt.

Përdorimi i Tracert

Tracert teston gjithashtu lidhjen me një klient në largësi (remote client) në rrjetet TCP/IP, duke dhënë informacione shtesë mbi të gjithë router-at që gjenden midis router-it të rrjetit lokal dhe router-it të klientit në largesi, duke ndjekur si rrjedhim rrugën e një pakete me të dhëna deri tek klienti. Në këtë mënyrë ekziston mundësia, që të gjendet shkaku i një lidhjeje të ndërprerë.

Rezultati i komandës tracert tregon çdo router me emrin përkatës, adresën e IP-së dhe kohën e transmetimit.



Rezultati i komandës tracert për një server DNS

Në rast problemi në komunikim paraqitet router-i i fundit që funksionon dhe përgjigjet ende duke treguar në këtë mënyrë pjesën e rrjetit, në të cilën është ndërprerë komunikimi.

Në Linux (UNIX) përdoret komanda traceroute.

Paraqitja e lidhjeve në rrjet, tabelave të route-imit dhe informacioneve të tjera të lidhjes

Përdorimi i ipconfig

Përdoret në Windows për të paraqitur konfigurimin e Adresës së IP-së, Subnetmask-ës dhe Gateway-it të lidhjeve të instaluara të rrjetit (në Linux përdoret ifconfig).

Opsionet e ipconfig

p. sh:

Opsionet	Domethënia
/?	Kërkon ndihmë (Help) .
/all	Tregon të gjitha informacionet e konfigurimit të kartës së rrjetit.
/release	Çliron kartën e rrjetit nga adresa ekzistuese e IP-së.
/renew	Rinovon adresën e IP-së për kartën e dhënë të rrjetit.

netstat *opsionet*

Pa opsione, netstat tregon gjendjen e sockets-ave të hapura të të gjitha familjeve të adresave të konfiguruara. Opsionet e lejuara janë -a, -b, -e, -n, -o, -p, Protocol, -r, -s, -v, Interval

Opsionet	Domethënia
-a	Tregon të gjitha lidhjet dhe portat
-r	Tregon tabelën e route-imit të kernel-it
-v	Rrit saktësinë e informacioneve të dhëna
Interval	Ndikon, që netstat-i të përsëritë paraqitjen e informacioneve në intervale kohe që jepen me sekonda

Rezultati i komandës netstat paraqitet në formë tabelare. Kolonat e veçanta kanë kuptimin e mëposhtëm:

Protocol	Protokolli i përdorur
Local address	Adresa lokale dhe numri i portës
Remote address	Adresa dhe numri i portës i kompjuterit tjetër
Status	Gjendja e sockets

11 Protokollet e aplikacioneve dhe shërbimet e rrjetit

Në këtë kapitull do të lexoni

- → çfarë janë protokollet e aplikacioneve
- → si punon protokolli HTTP
- → ku mund ta përdorni protokollin FTP
- → çfarë e dallon protokollin TFTP
- → cilat Terminal Emulations ekzistojnë
- → cilat Protokolle të Terminal Emulations përdoren
- → si punon protokolli SMTP
- → si mund të përdoret SNMP-ja

Kusht paraprak

- ✓ Njohuri mbi bazat e rrjetit
- ✓ Bazat e TCP/IP-së
- ✓ Njohuri mbi shërbimet
- ✓ Njohuri mbi bazat e sistemit operativ
- ✓ Sistemet e shpërndara
- ✓ Njohuri mbi mënyrën e punës së TCP-së
- ✓ Njohuri mbi mënyrën e punës së DNS-së

11.1 Vështrim i përgjithshëm

Vështrim i përgjithshëm mbi protokollet e sotme të aplikacioneve dhe shërbimeve të rrjeteve në shtresat e sipërme të modelit OSI

Ekzistojnë një seri e gjatë protokollesh që punojnë në shtresat e sipërme të modelit OSI. Këto protokolle janë të lidhura pjesërisht me sisteme të vëçanta operative, ose mund të përdoren vetëm me bashkësi protokollesh (protocol-stacks) të caktuara. Të tjerat paraqesin standarde, të cilat janë adoptuar nga të gjithë prodhuesit lider në këtë fushë , me qëllim që të përdoren përgjithësisht nga platformat dhe sistemet operative.

Përgjithësisht, protokollet e paraqitura këtu kanë të përbashkët, që ato punojnë mbështetur mbi TCP/IP dhe aktivizohen përmes thirrjeve nga portat TCP dhe/ose UDP. Ato janë në dispozicion të të gjitha platformave të sotme të sistemeve operative dhe përdoren pjesërisht në rrjetin mbarëbotëror (WWW, Internet).

Shtresa në modelin OSI	Protokolli					
(7) Application Layer	HTTP	SMTP, POP, IMAP	NNTP	FTP	LDAP	DNS, DHCP
(6) Presentation Layer						
(5) Session Layer	Winsock.dll (tek sitemet e Windows-it)					
(4) Transport Layer	TCP					
(3) Network Layer	IP					
(2) Data Link Layer	PPP		SLIP		...	
(1) Physical Layer	Linjat telefonike, fibrat optike ...					

Familja e protokolleve TCP/IP

Për të kuptuar më mirë ndërvarësitë midis shërbimeve dhe protokolleve të ndryshme, më poshtë ndër të tjera, do të përshkruhet dhe shpjegohet sesioni HTTP nga DNS-resolution deri në transferimin e faqes HTML. Ndërtimi i lidhjes së mëparshme PPP nuk do të merret parasysh, pasi do ta rëndonte dhe do t'ia humbte qartësinë shpjegimit.

11.2 HyperText-Transport-Protocol

HTTP

Sot, protokolli HTTP është protokolli më i përhapur i shtresës së aplikacioneve. HTTP është protokoll pa status dhe i orientuar nga objektet (object oriented). Para së gjithash, ai shërben për transferimin e të dhënave në World Wide Web (WWW). Për këtë ai përdor një format të standardizuar të kërkimit të të dhënave në Web-Servera, formatin URL.

Uniform Resource Locator (URL)

HTTP përdor të ashtuquajturin Uniform Resource Locator (URL) për adresimin e host-eve:

p. sh. *http://www.todotango.com.ar/english/main.html*

Një adresë URL përbëhet nga:

- ☑ Identifikuesi i shërbimit (p.sh. *http://*)
- ☑ Adresa e DNS-së (p.sh. *www.todotango.com.ar/*)
- ☑ Rrugëkalimi (path-i) për në direktori (p.sh. *english/main.html*)

Rrugëkalimi që tregon URL-ja i referohet një direktorie logjike virtuale në Web-Server. Këto direktori janë vetëm rrugekalime të shkurtra (shortcuts) në strukturën e një website-i dhe mund të kërkohen nëpërmjet shërbimeve të ndryshme. Një faqe mund të jetë e vlefshme si faqe HTML, por mund të ruhet dhe në format PDF e të thirret nëpërmjet redirector-it të një aplikacioni, i cili mbështet këtë format. E gjithë kjo është jashtë përgjegjësisë së HTTP-së.

Protokolli HTTP është përgjegjës vetëm për ndertimin e sesionit dhe dërgimin e kërkesës për informacion. Përpunimi i mëtejshëm i informacionit ndodh jashtë modelit OSI në aplikacionet e veçanta, të cilat janë përgjegjëse për paraqitjen dhe vlerësimin e llojeve të të dhënave të marra.

Shënime

Ndërtimi i HTTP-së

HTTP-ja ekziston në variante të ndryshme që nga versioni 0.9. Ndryshimet e hollësishme ndërmjet versioneve të ndryshme nuk do të përshkruhen këtu. Bëhet fjalë për më tepër për dhënien e një kuptimi të përgjithshëm të Headers-ave dhe mënyrës së tyre të punës. Header-i i paraqitur pretendohet të kuptohet vetëm skematikisht. Ai nuk i përmban fushat e ndryshme opsionale, në të cilat përcaktohen gjuhët, protokollet e komprimimit, formatet e tekstit, versionet e Browser-it, programet e serverit etj.

Paketa kontrolluese e HTTP-së

Në fillim të një pakete kontrolli të HTTP-së është komanda HTTPI (si rregull GET). Gjatë një kërkese të thjeshtë (Simple Request) paraqitet vetëm komanda, ndërsa gjatë një kërkese të plotë (Full Request) (që nga Versioni HTTP 1.0) paraqitet numri i versionit HTTP.

Çdo rresht mbaron me një Carriage Return (\r, mbarim rreshti) dhe një Line Feed (\n, rresht i ri), meqë paketa HTTP përpunohet si skedar tekst.

Si pasojë, një URL mund të qëndrojë vetëm kur përcakton qëllimin. Më pas vijnë opsione të ndryshme të MIME-s diverse MIME dhe plotësime të komandave të specifikuara, në varësi nga komandat dhe versioni i protokollit.

11.3 Sesioni HTTP (http session)

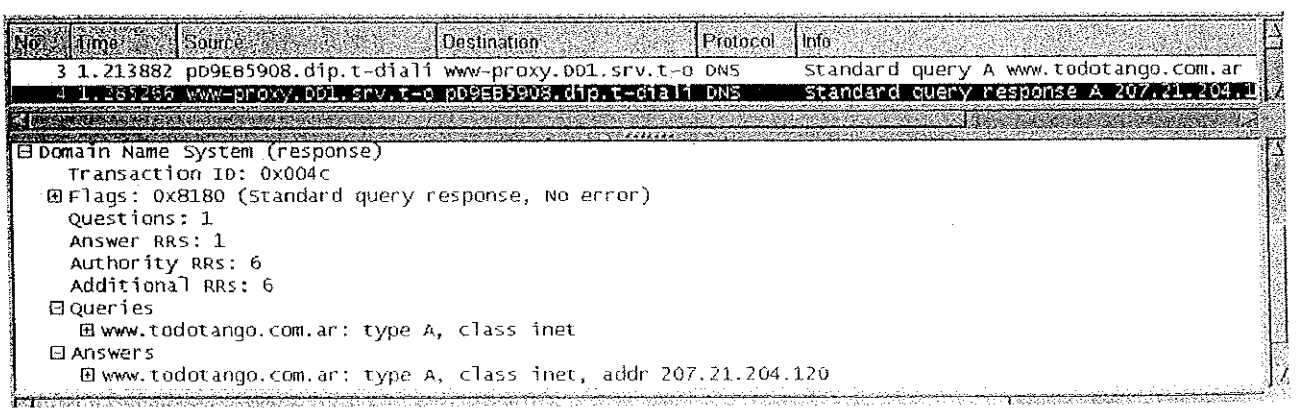
Ndjekja e hapave që kalon një sesion HTTP

Çdo akses në një faqe www paraqet një sesion të vetëm HTTP, i cili duhet të iniciohet ndarazi nga klienti. Për këtë përdoren struktura të thjeshta, të cilat fillojnë me një GET-Demand. Për ta shpjeguar këtë, do t'u duhet të ndiqni më poshtë ndërtimin e një sesioni HTTP.

URL-ja e kërkuar është: *www.todotango.com.ar*.

DNS-resolution

Si hap i parë duhet të bëhet rezolucioni i adresës DNS të URL-së. Meqë serveri DNS në Internet, që ka marrë kërkesën, e ka tashmë faqen e kërkuar në cache, përsëritja e procesit të rezolucionit nuk ndodh.



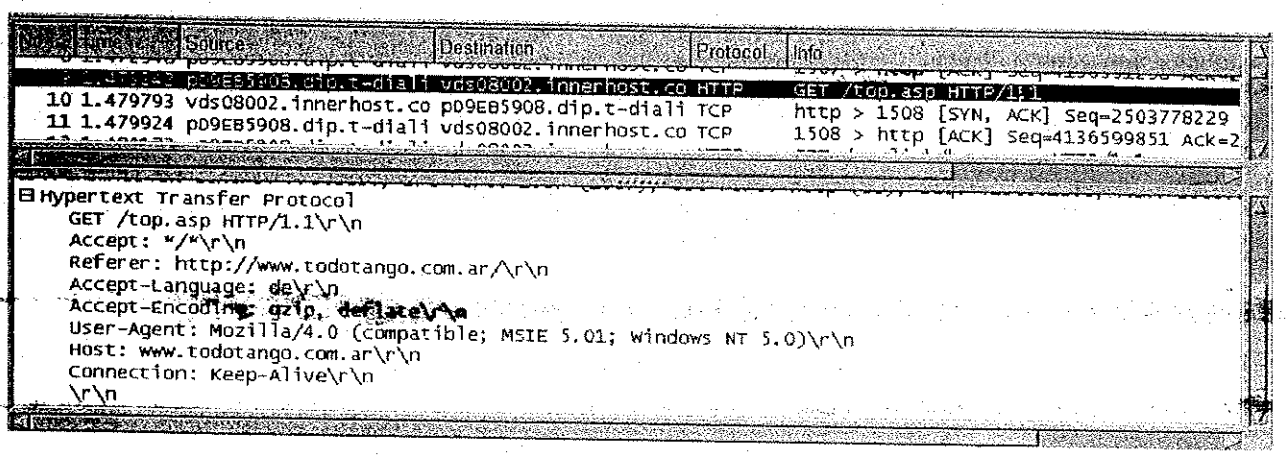
HTTP over TCP

HTTP përdor si protokoll transporti protokollin TCP, si dhe e mbështet kontrollin e rrjedhës së të dhënave dhe identifikimin e gabimeve në transmetim në mekanizmat e këtij protokolli. Kështu fillon një sesion komunikimi HTTP me një TCP-Three-Way-Handshake, i cili përbëhet nga një kërkesë për sinkronizim (synchronisation request) (SYN) (α), një kërkesë për sinkronizim dhe konfirmim njohjeje (SYN,ACK) (β) dhe së fundi një konfirmim njohjeje (ACK) (χ).

No.	Time	Source	Destination	Protocol	Info
6	1.291669	pD9EB5908.dip.t-diali	vds08002.innerhost.co	TCP	1508 > http [SYN] Seq=4136599850 Ack=0
7	1.472792	vds08002.innerhost.co	pD9EB5908.dip.t-diali	TCP	http > 1507 [SYN, ACK] Seq=2503739304
8	1.472948	pD9EB5908.dip.t-diali	vds08002.innerhost.co	TCP	1507 > http [ACK] Seq=4136551298 Ack=2

HTTP-GET-Demand

Pas „marrëveshjes" për parametrin e sesionit për TCP ndodh e ashtuquajtura GET-Demand nga HTTP.



Në kreun (Header-in) e HTTP-Get-Demand, ndër të tjera, mund të përmbahen informacione në lidhje më karakteret e suportueshme, programi i Browser-it, sistemi operativ dhe tipet e suportueshme të MIME-s. Gjithashtu, bëhet i njohur edhe lloji i komprimimit të të dhënave.

Transmetimi i të dhënave

Të dhënat transmetohen thjesht si tekst.Nëpërmjet llojeve të ndryshme të MIME-s mund të dërgohen tipe të ndryshme skedarësh. Kryesisht transmetimi ndodh si HTML-Text, i cili më pas vlerësohet nga interpretuesi i aplikacionit të Browser-it. Pasi ka mbaruar transmetimi, sesioni ndërpritet automatikisht. Për të aksesuar faqe të tjera duhet të iniciohet një sesion i ri.

HTTPS

HTTPS-ja konsiderohet si versioni "i sigurtë" i protokollit HTTP. Me anë të këtij protokolli konfirmohet autenticiteti i serverit përmes një certifikate dhe të dhënat gjatë transmetimit janë të koduara.

11.4 File-Transfer-Protocol

FTP

File-Transfer-Protokoll (Protokolli transferimit të skedarëve, FTP) është një shërbim që përdoret për transferimin e skedarëve (files) nga të gjithë sistemet operative. Me këtë rast hiqet barriera që ekzistonte më parë ndërmjet proceseve të aksesimit të skedarëve nga siteme të ndryshme operative. UNIX p.sh. përdor normalisht Network File System (NFS), OS/2 përdor High Performance File System (HPFS). Në rast se kompjutera me sisteme të ndryshme operative duan të aksesojnë të dhëna nëpërmjet rrjetit, me FTP bëhet e mundur të aksesohen të dhënat dhe të transportohen në kompjuterin lokal.

FTP-Session

Sesioni FTP bazohet në modelin Client/Server dhe ndahet në pesë faza:

Klienti starton një lidhje me serverin

Faza 1: **Krijimi i lidhjes**	Gjatë krijimit të lidhjes, nga klienti dërgohet në server një kërkesë për një sesion komunikimi. Serveri dërgon një kërkesë për identifikim (kërkesë opsionale). Nga klienti jepet emri i përdoruesit dhe fjalekalimi, dhe në këtë moment fillon sesioni.
Faza 2: [illegible]	Klienti nëpërmjet komandave mund të kërkojë transferimin e të dhënave. Në këtë moment fillon „negociimi" i parametrave të lidhjes për tramsferimin e të dhënave dhe parapërgatitet lidhja e të dhënave. Për këtë negociojnë portat e klientit dhe serverit.
Faza 3: [illegible]	Transferimi real i të dhënave përdor TCP-në për kontrollin e rrjedhës së të dhënave dhe korrigjimit të gabimeve.
[illegible]	Nëse të dhënat janë transferuar komplet dhe klienti dërgon një konfirmim për marrjen e të gjitha të dhënave, serveri dërgon komandën Close, me qëllim që të fillojë ndërprerja e lidhjes së të dhënave.
[illegible]	Pas marrjes së komandës Close, klienti fillon ndërprerjen e lidhjes së të dhënave.Transaksione të tjera mund të fillojnë nëpërmjet lidhjeve të reja të të dhënave.
[illegible] Ndërprerja e lidhjes	Nëse të gjitha lidhjet me të dhëna ndërpriten, nëpërmjet komandës QUIT, përdoruesi i klientit fillon ndërprerjen e lidhjes. Lidhja ndërpritet dhe si përfundim serveri dërgon një njoftim ndërprerjeje.

11.5 Protokollet SMTP, POP dhe IMAP

Protokollet për rregullimin e dërgimit dhe marrjes së E-Mail-eve

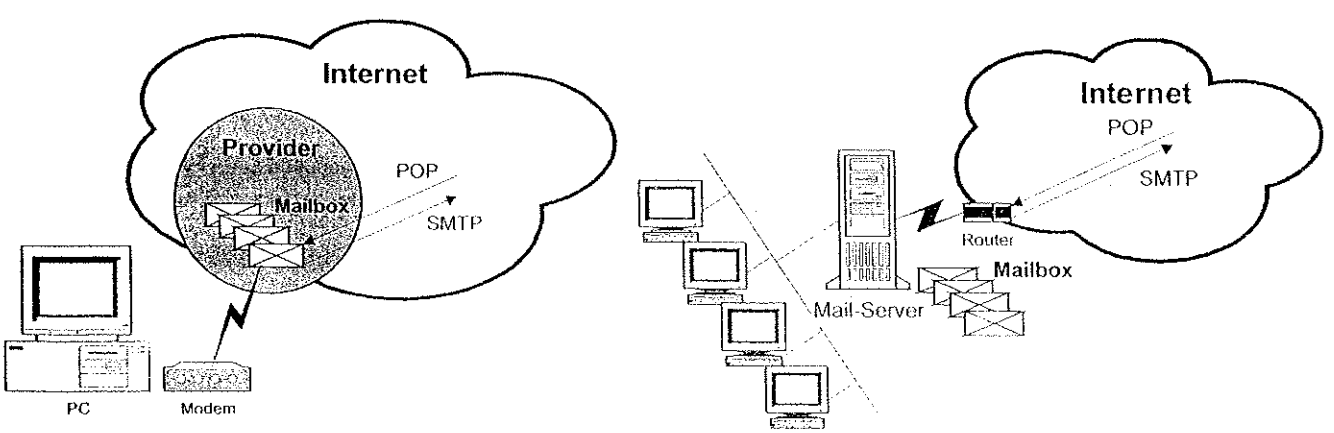
Dërgimi dhe marrja e një e-maili-i mund të krahasohet me dërgimin dhe marrjen e një letre: Letra hidhet në kutinë postare, e cila boshatiset në periudha të rregullta kohore, dhe të gjitha letrat magazinohen në një vend të caktuar grumbullimi. Në rast se marrësi nuk ndodhet në zonën që mbulon kjo pikë grumbullimi, letra nuk mund të dorëzohet dhe si pasojë dërgohet me tej në një pikë tjetër grumbullimi, deri sa më në fund vjen në kutinë postare të marrësit.

Internet-Provider-i, i cili mundëson lidhjen në Internet, administron ndër të tjera edhe një **E-Mail-Server**. E-Mail-Ser-ver-i rregullon dërgimin dhe marrjen e e-mail-eve dhe më së shumti punon me protokollet e mëposhtme:

☑ Dërgimi i E-Mail-eve: **Simple Mail Transfer Protocol** (SMTP)
☑ Marrja e E-Mail-eve: **Post Office Protocol** (POP)

Meqë një e-mail i dërgohet një personi të caktuar dhe jo nje kompjuteri, çdo përdorues ka nevojë për „kutinë e vet postare" **(Mailbox)**. Në mailbox grumbullohen dhe mund të tërhiqen të gjitha e-mail-et, të cilat drejtohen tek ju.

Në rast se lidhja në Internet kryhet nëpërmjet një provider-i, mailbox-i juaj do të gjendet tek provider-i. Si rregull, firmat e mëdha zotërojnë nje E-Mail-Server të vetin, në të cilin çdo punonjës ka një mailbox dhe i cili kryen dërgimin dhe shpërndarjen e e-mail-eve lokalisht, brenda rrjetit të firmës dhe nëpërmjet Internetit.

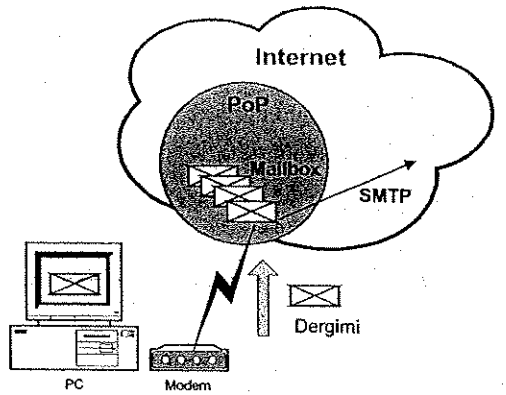


E-mail box-i tek provider-i dhe tek serveri i firmës

SMTP (Simple Mail Transfer Protocol)

Gjatë **dërgimit** të një E-Mail-i së pari shqyrtohet paketa e të **dhënave që përmban adresën e E-Mail-it** te dërguesit dhe të **marrësit. Më pas bëhet lidhja në Internet.Simple Mail Transfer Protocol** (SMTP) rregullon lidhjen me E-Mail-Ser-ver-in, pret për **konfirmim që E-Mail-Server-i** të marrë të dhënat dhe më pas t'i **dërgojë ato. Pas kësaj lidhja ndërpritet sërish.**

E-Mail-Server-i vendos, duke marrë parasysh adresën e marrësit, se cila rrugë transporti duhet përdorur. Transporti kryhet në shumicën e rasteve nëpërmjet disa kompjuterave ndërmjetës, të cilët e marrin e-mail-in dhe e dërgojnë një hap „më pranë" kompjuterit të destinacionit. Secili nga këta kompjutera përdor protokollin e transportit SMTP. Ju nuk ka nevojë të merreni me mënyrën e transportimit të E-Mail-eve.

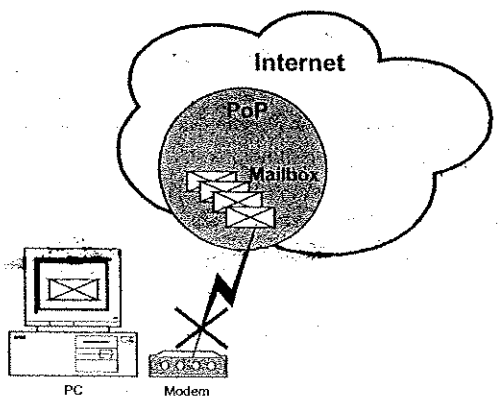


Dërgimi i E-Mail-eve

Shkrimi dhe përgjigjia e E-Mail-eve

Shkrimi dhe përgjigja e E-Mail-eve është një proces që kërkon kohë dhe gjatë të cilit nuk dërgohen të dhëna në Internet. Kjo do të thotë që gjatë fazës së shkrimit dhe përgjigjes së e-mail-eve, nuk ju nevojitet lidhje në Internet. Ju mund t'i shkruani e-mail-et "offline"; vetëm për dërgimin dhe marrjen e tyre duhet të jeni "online".

E-Mail-et e përgatitura vendosen në Outbox (kutia e postës në dalje). Atje ato qëndrojnë në pritje për t'u dërguar, p.sh. gjatë kohës kur tarifat janë më të ulta.



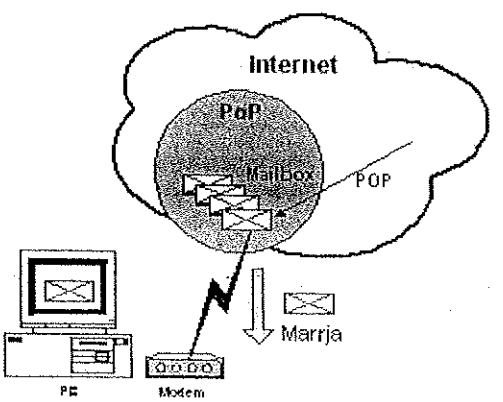
Përpunimi offline i E-mail-eve

POP (Post Office Protocol)

Për marrjen e E-Mail-eve, së pari nevojitet një lidhje në Internet dhe në vijim tërhiqen E-Mail-et e ardhura në mailbox-in tuaj. Më pas mund të shkëputet lidhja me Internetin dhe E-Mail-et e ardhura mund të lexohen dhe t'u kthehet përgjigje offline.

Aksesi në Mailbox i një përdoruesi rregullohet nga protokolli Post Office Protocol (POP). Ky protokoll lejon aksesin në një **mailbox të vetëm. Nëse keni më shumë se një mailbox (p.sh. në firmën ku punoni dhe privat), ju duhet që secilin mailbox ta kontrolloni veçantë.**

Protokolli POP njihet ndryshe edhe si POP3. Numri 3 tregon versionin aktual të protokollit.



Marrja e E-Mail-eve

IMAP (Interactive Mail Access Protocol)

Interactive Mail Access Protocol (IMAP) është një protokoll i ri për marrjen e E-Mail-eve. Ky proto-koll mundëson leximin dhe administrimin e E-Mail-eve në Mail-Server, si dhe kërkimin e Mailbox-it sipas kritereve të përcaktuara.

E-Mail-et qëndrojnë në Mail-Server dhe shkarkohen me komandën e përdoruesit. Kjo gjë bën të mundur që nga disa kompjutera te aksesohet i njëjti mailbox.

Protokolli IMAP njihet ndryshe edhe si IMAP4 (Versioni 4 është versioni aktual i protokollit).

NNTP (Net News Transfer Protocol)

Dërgimi dhe marrja e lajmeve (News) kryhet në mënyrë të ngjashme me marrjen e E-Mail-eve. News-et si rregull transferohen nëpërmjet protokollit **NetNews Transfer Protocol** (NNTP).

Ky protokoll rregullon mekanizmin e transportit që do të shërbejë për News-et (lajmet), me cilët kompjutera dhe në cilën mënyrë shkëmbehen News-et me njëri-tjetrin. NNTP bazohet ne tekst dhe funksionon nga alternimi i kërkesave të klientëve dhe përgjigjeve që japin serverat për këto kërkesa.

Në lidhjet me modem midis kompjuterave me UNIX, del si alternativë aplikacioni UUCP (Unix to Unix Copy Protocol).

11.6 SNMP (Simple-Network-Management-Protokol)

SNMP

Simple-Network-Management-Protocol (SNMP) u zhvillua në vitin 1989 nga Simple-Network-Gateway-Monitoring-Protocol (SGMP). Ky protokoll ekziston në dy versione: SNMPv1 dhe SNMPv2. SNMPv2 është një zhvillim i mëtejshëm i SNMPv1 dhe ka të integruara standarde të reja të ndryshme.

Detyrat e SNMP-së

SNMP shërben për mbikqyrjen dhe administrimin e qendërzuar të përbërësve aktivë të rrjetit si rou-tera, switche, bridge dhe Hube. Përbërësit e rrjetit që e kanë të mundësuar SNMP-në përshkruhen si agjentë, ndërsa kompjuteri që kryen administrimin quhet SNMP-Manager. Agjentë quhen të gjitha pajisjet, të cilat dërgojnë informacion mbi gjendjen e tyre. Manaxheri ka për detyrë grumbullimin e këtyre informacioneve (traps) të agjentëve.

Traps

Të dhënat që dërgon një agjent SNMP përshkruhen si traps. Në to përmbahen informacione në lidhje me gjendjen e punës së pajisjes dhe ngjarje të veçanta, apo probleme të saj gjatë punës.

Shembull si agjent SNMP-je është një router, i cili jep rregullisht informacione në lidhje me fluksin e të dhënave në portat e ndryshme të tij. Gjithashtu, ai transmeton çdo herë një informacion paralajmërues, në rast se nuk mund ta arrijë router-in fqinjë. Manaxheri i merr këto informacione dhe vlerëson statistikisht, si ecën trafiku në rrjet. Në rast se manaxheri merr informacion në lidhje me paarritshmërinë në rrjet të një routeri, ai dergon një lajmërim tek administratori.

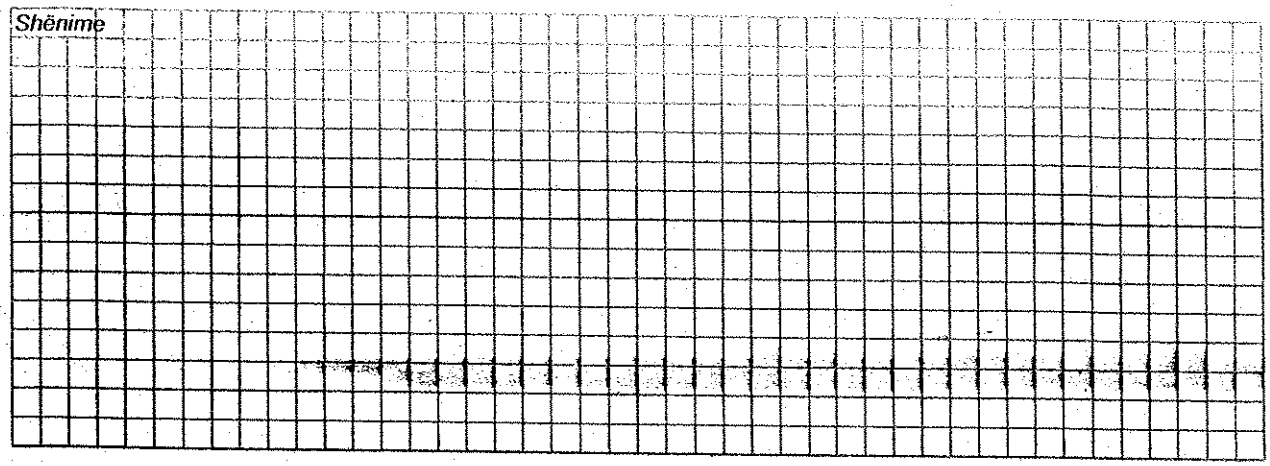
Monitori teston në periudha të rregullta kohore, nëse agjenti, nga i cili merr informacion, është ende në gjendje pune. Në rast se fillon të ketë probleme, ai dërgon një paralajmërim. Kjo është e nevojshme, pasi një pajisje nuk mund të njoftojë për mosfunksionimin e saj, pasi ka ndodhur defekti.

Community

Pajisjet e një njësie administrimi nën SNMP formojnë një komunitet (community). Një komunitet përbëhet minimumi nga një agjent dhe një manaxher, si dhe dallohet nga një emër i caktuar. Emri i komunitetit (community name) përmbahet në çdo dërgesë të një nyje (Knot) dhe vlerësohet nga një nyje, për të vendosur nëse ajo do ta interpretojë, apo jo nje informacion. Në rast se pajisjes nuk i jepet një community-name, ajo i përket të gjitha komuniteteve dhe interpreton të gjitha dërgesat e komuniteteve përkatëse të parapëlqyera.

SNMP-Proxy-Agent

Agjentët SNMP-Proxy shërbejnë për përfshirjen në mjedisin SNMP pajisje, të cilat vetë nuk mund të dalin si agjentë SNMP. Në këtë mënyrë mund të monitorohen me anë të SNMP-së pajisje si p.sh. telefona, modema apo printera. Agjenti SNMP-Proxy ka mundësi të grumbullojë informacione mbi gjendjen (statusin) direkt, p.sh. nëpërmjet komandave AT, ose indirekt nëpërmjet sensorëve.


Shënime

12 IPX/SPX

Në këtë kapitull do të lexoni:
- → Si është ndërtuar protokolli IPX/SPX
- → Çfarë duhet pasur parasysh në lidhje me protokollin IPX/SPX
- → Si duhet konfiguruar protokolli IPX/SPX
- → Cilat protokolle të shtresave të larta mbështeten nga IPX/SPX

Kusht paraprak
- ✓ Bazat e rrjeteve
- ✓ Modelet e rrjeteve

12.1 Fusha e përdorimit të IPX/SPX

Familia e protokolleve Netware

Ashtu sikurse Microsoft doli me familjen e vet të protokolleve NetBEUI, e cila u mendua të përdorej në rrjetet e vogla dhe të mesme, edhe firma firma Novell krijoi një familje protokollesh të vetën, e cila përshtatej me fushat speciale të përdorimit të sistemit operativ NetWare.

Që në fillimet e viteve 80, Novell-i, si pasues i XNS (Xerox Network System), filloi të zhvillonte të ashtuquajturin NetWare-Suit si NOS (Network Operating System). Si fushë përdorimi duhej të ishin lidhjet e rrjeteve të mëdha dhe të routeueshme LAN, pasi për mjedise të tilla rekomandohej veçanërisht përdorimi i strukturës me performancë të lartë të bazës së të dhënave të Novell-it.

Shërbimet, që duhet të ofroheshin ishin para së gjithash sigurimi aksesit në rrjet mbi skedarët, aplikimet në largësi (remote applications), si dhe aksesi mbi printerat e rrjetit dhe autentifikimi i përdoruesve në rrjet.

Novell-i pretendonte të ofronte një produkt dinamik dhe me performancë të lartë, siç qe rasti me IP-në dhe DNS-në. Kostot administrative për administrimin e bazës së të dhënave për DNS-në i bëjnë këto sisteme, në rastet me gjerësi bande të kufizuara dhe në rrjetet lokale dinamike, shumë të papërshtatshme. Përmes teknikave të reja si NetBIOS dhe WINS, në bashkëpunim me DHCP, TCP/IP u bë një produkt konkurues në fushën e LAN-it.

Grupi i protokolleve Netware

Tabela e mëposhtme klasifikon protokollet e familjes NetWare sipas modelit ISO/OSI:

Shtresat në modelin OSI	Netware-Protocols			
Application Layer	Applications		NCP	More
Presentation Layer	NetBIOS	NetWare Shell		
Session Layer				
Transport Layer	SPX			
Network Layer	IPX			
Data Link Layer	Ethernet 802.2	Ethernet 802.3	Token Ring	etj.
Physical Layer				

Shtresa e aplikacioneve (Application Layer)

Në shtresën e aplikacioneve nga Netware mbështeten një sërë aplikacioneh të zakonshme rrjeti. Këto nga njëra anë mbështeten nga një version i përshtatur i NetBIOS over IPX/SPX-Emulation, dhe nga ana tjetër mbështeten nga NetWare-Shell.

Server routines

Thirrjen e server routines në familjen e protokolleve NetWare e merr përsipër NCP, Netware Control Proto-col. Ky protokoll është i krahasueshëm me Server Message Blocks të Microsoft-it. Për kërkesa të veçanta në rrjet mund të angazhohen edhe protokolle të tjera. Kështu p.sh. mbështeten formate skedarësh në shtresën e prezantimeve (presentation layer). Këtu duhen përmendur vetëm protokollet speciale të Netware.

Shtresa e transportit (Transport Layer)

Në shtresën e transporteve Netware përdoret Sequenced Packet Exchange (SPX). Ky është i krahasueshëm me protokollin TCP, që garanton transport të besueshën dhe të orientuar nga lidhja të të dhënave. Në rast se kjo nuk nevojitet, ndryshe nga familja e protokolleve TCP/IP-e, cila përdor një protokoll të llojit UDP, NetWare përdor protokollin IPX për marrjen përsipër të së njëjtës detyrë.

Shtresa e rrjetit (Network Layer)

Përbërësi qendror i familjes së protokolleve Netware është protokolli Internet-Exchange (IPX). Në mënyrë të ngjashme si tek protokolli i Internetit (IP), këtu mbikqyret transmetimi i paketave ndërmjet rrjeteve. Transporti i paketave ndodh pa kontroll të transmetimit dhe lidhjes. Ndryshe nga IP, i ashtuquajturi protocol -over-head, është më i vogël, gjë që përmirëson shfrytëzimin e gjerësisë së bandës në dispozicion. Ky përmirësim shihet veçanërisht qartë, në rast se në shtresën 4 nuk nevojitet transport i orientuar nga lidhja. Më pas IPX mund të marrë përsipër funksionet e UDP-së dhe të përdoret për transportin e paketave dhe transmetimin e të dhënave.

Shtresat pranë hardware-it

Netware mbështet një sërë protokollesh që punojnë në shtresën e dytë - Data Link Layer. Krahas proceseve të sotme si Ethernet, me versionet e tij të ndryshme, mbështeten edhe Token Ring, FDDI, FrameRelay etj. Një domethënie të veçantë merr lloji i kapsulimit. Kështu për çdo kartë rrjeti duhet konfiguruar në mënyrë që të përcaktohet se cilës adrese rrjeti të kësaj karte i duhet caktuar, cili lloji frame-i. Klientët të cilët punojnë në një rrjet p.sh. me NetWare 3.1 dhe NetWare 4.x, si dhe që duhet të komunikojnë me të dy llojet e frame-ve, duhet të integrohen si me numrin e parë të rrjetit tek Ethernet II (802.2, versioni më i ri i llojeve të frame-it), ashtu edhe me një numër të dytë tek 802.3. Kjo bën që në kuadrin e versionit 802.3, në vend të informacionit për tipin, të paraqitet një informacion për gjatësinë dhe nga ana tjetër kuadri nuk mund të ndryshohet.

Shënime

Microsoft bën një njohje automatike të frametype-t në zbatimin e protokollit IPX/SPX, i cili njihet me emrin NWLink. Mos i besoni këtij automatizimi, pasi ai njeh „automatikisht" vetëm të ashtuquajturin frametype 802.2. Çfarë mund të vlerësohet automatikisht këtu është informacioni në lidhje më numrin e rrjetit për frames. Në rast se duhet të njihet automatikisht një frametype shtesë, ndryshe nga 802.2, konfigurimi duhet kryer në mënyrrë manule.

Ndërtimi i adresës

Ndërtimi i adresave IPX në krahasim me adresat e IP-së është i thjeshtë. Një adresë IPX ka dy pjesë përbërëse:

- ☑ Numri i rrjetit me deri në 32 Bit në vlera hexadecimale
- ☑ Adresa e kompjuterit (knot address) = adresën MAC të kartës së rrjetit

Parimisht numri i rrjetit mund të marrë çdo vlerë nga 1 deri FF:FF:FF:FE. Në këtë mënyrë disponohen më shumë rrjete se në të gjithë familjen TCP/IP. Për më tepër nëpërmjet dhënies së kufirit ndarës të adresës midis pjesës që tregon rrjetin dhe asaj që tregon hostet (knots), nuk del më e nevojshme dhënia e subnetmaskës. Një adresë MAC është gjithmonë 48 Bit e gjatë. Edhe këtu garantohet uniciteti në mbarë botën, për sa kohë prodhuesit e kartave të rrjetit do të vazhdojnë të ndalen në specifikimin e dhënies së adresave MAC.

Një shembull për adresën IPX do të ishte:

1B:00:A0:24:5A:CE:3F

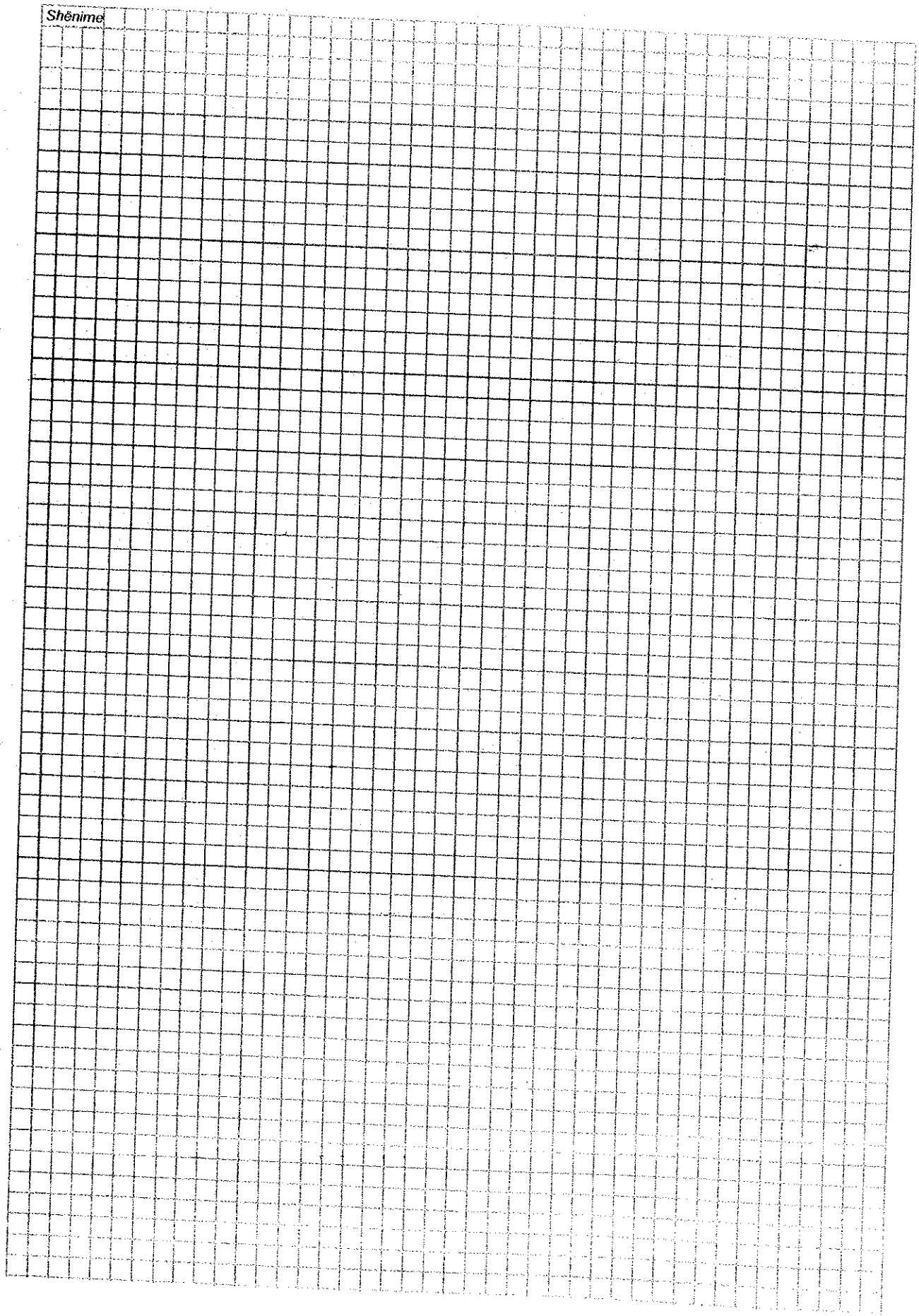
Ku 1B është numri i rrjetit (po të shprehej në formë decimale do të ishte 27), 00:A0:24 është kodi i prodhuesit (3Com) dhe 5A:CE:3F numri serial i kartës së rrjetit.

12.2 Përdorimi i adresës MAC për përshtatës të tjerë

Përshtatësi përdor adresë MAC

Në rast se në një pajisje përveç kartës së rrjetit, përdoren përshtatës të tjerë, të cilët e kryejnë komunikimin nëpërmjet IPX-it (p.sh. ndërfaqe seriale për FrameRelay), atëhere këtyre përshtatësve u caktohet një adresë MAC e një karte rrjeti ekzistuese në sistem. Për sa kohë që prodhuesi e ka dhënë adresën vetëm një herë, nuk paraqitet ndonjë problem: kombinimi i numrit të rrjetit dhe adresës MAC është unik në mbarë botën. Në të njëjtën mënyrë edhe adresat e të gjithë kompjuterave të lidhur brenda rrjetit (knots) duhet të jenë unike. Përndryshe nuk do të ishte i mundur routimi ndërmjet rrjeteve IPX.

Shênime



13 Teknikat e transmetimit të të dhënave pa kabëll

Në këtë kapitull do të lexoni

→ si përcaktohen nevojat për një WLAN
→ cilat parakushte duhen plotësuar
→ si mund të ngrihet një sistem WLAN-i

Kusht paraprak

✓ Njohuri mbi lidhjet me kabëll
✓ Njohuri mbi sistemet operative

13.1 WLAN-i

Wireless LAN - Avantazhet dhe disavantazhet

Tek rrjetet pa kabëll (WLAN-et) bëhet fjalë për rrjete, në të cilat në vend të mediave tradicionale, prej bakri apo fibrash optike, transmetimi i sinjaleve bëhet nëpërmjet valëve të radios. Kjo sjell me vete disa përparësi bazë:

☑ Brenda rrezes së mbulimit me sinjal, aksesi në rrjet mund të bëhet nga një vend i preferuar, i pakushtëzuar nga gjatësia e kabllit, apo vendndodhja e prizës së rrjetit.
☑ Për rrjetëzim nuk duhen parashikuar ndryshime në elementët e ndërtimit (p.sh. parashikimi i çarjes së kanaleve, shtrimit të kanelinave, vendosjes së prizave etj.)
☑ Teknologji fleksibel për zgjerim të mëtejshëm.
☑ Hapësirat publike (si rrugët, hapësirat ujore etj.) kapërcehen lehtë.

Këto përparësi kanë çuar në një rritje të shpejtë të preferecave për zgjidhjet që ofron WLAN-i. Kjo vlen sidomos për përdorimin e WLAN-it për lidhjen e kompjuterave portabël në rrjetet ekzistuese, ose për akses në Internet. Në këtë kuadër tashmë në treg gjenden routera DSL me përbërës WLAN-i të integruara.

Krahas përparësive, përdorimi i WAN-eve sjell me vete edhe një sërë problemesh, të cilat nuk ndeshen në procesin e transmetimit në rrjetet me kabëll:

☑ Interferencë e lartë
☑ Nuk ka siguri ndaj përgjimit
☑ Dendësi e vogël portash
☑ Në krahasim me LAN-in shpejtësi me e ulët transmetimi
☑ Në shtresën e dytë nevojitet proces kompleks identifikimi

Me qëllim që këto disavantazhe të balancohen gjatë ngritjes së WLAN-it duhet të merren në konsideratë faktorë shtesë. Kështu distancat midis dërguesit dhe marrësit duhen mbajtur të vogla, me qëllim që të kompensohen interferencat. Meqë sinjalet brenda një rrezeje të caktuar merren nga çdo marrës, i duhet kushtuar kujdes procesit të kodimit të sinjaleve të transmetuara. Me qëllim që të administrohet siç duhet denduria e portave, duhen përdorur zona më të mëdha frekuence dhe procese komplekse të modulimit të frekuencës. Për sinkronizimin e dërguesit me marrësin nevojiten disa protokolle.

Veçanërisht faktorët, të cilët lidhen me sigurinë e rrjetit, kanë nevojë për një planifikim të qendrueshëm para se të vihet në punë një WLAN. Në të njëjtën kohë, ka edhe faktorë shëndetsorë që duhen marrë parasysh, pasi ka mendime shumë të ndryshme në lidhje me dëmet që mund të sjellin rrezet elektromagnetike.

Topologjitë WLAN

Meqë në një WLAN aksesi në mediat e transmetimit nuk kufizohet në prizat e veçanta të rrjetit, ekziston mundësia e përdorimit të metodologjive të ndryshme. Me topologji kuptohet mënyra në të cilën është organizuar aksesi fizik në median e transmetimit. Dy topologjitë e sotme për WLAN-in janë:

- ☑ Rrjetet Ad-Hoc
- ☑ Rrjetet Infrastrukturë

Rrjetet Ad-Hoc

Në një rrjet Ad-Hoc, dy ose më shumë pajisje rrjeti komunikojnë direkt me njëri-tjetrin, përsa kohë gjenden brenda rrezes së mbulimit. Kjo e fundit do të quhet ndryshe si Basic Service Area (BSA). Në këtë rast bëhet fjalë për një rrjet Peer-to-Peer. Këtu të gjitha pajisjet janë partnerë të të njëjtit rang. Nëse pajisje të tjera gjenden brenda BSA-së , edhe këto mund të komunikojnë direkt. Nëse Host-i A gjendet vetëm në BSA-në e Host-it B, dhe Host-i B në BSA-në e Host-it C, A-ja dhe C-ja nuk mund të komunikojnë me njëri-tjetrin, pasi në një rrjet Ad-Hoc asnjë host nuk është ndërmjetës i të tjerëve.

Rrjetet Ad-Hoc përdoren në rradhë të parë në fushën private dhe në rrjetet e firmave shumë të vogla. Ato janë të thjeshta për t'u konfiguruar dhe lejojnë gjithashtu edhe përdoruesit me pak përvojë të ndërtojnë një mjedis WLAN. Kjo ndikon në zvogëlimin mundësive për zgjerimin e rrjetit dhe sigurinë e tij.

Rrjetet infrastrukturë

Një rrjet infrastrukturë është ndërtuar si një nyje qendrore aksesi. Kjo nyje do të quhet Access Point (AP) dhe paraqet ndërfaqen midis rrjetit me dhe pa kabëll. Të gjitha nyjet, të cilat dëshirojnë të marrin pjesë në komunikimin në rrjet duhet të identifikohen tek AP-ja, përpara se të mund të komunikojnë me pajisjet e tjera të rrjetit. Edhe në qoftë se Host-i A dhe Host-i B ndodhen në të njëjtin BSA, ato duhet patjetër të marrin kontakt me njëri-tjetrin nëpërmjet AP-së. Ato gjithashtu mund të komunikojnë më pajisje të tjera, të cilat nuk ndodhen brenda rrezes së tyre të komunikimit.

Rrjetet infrastrukturë, para së gjithash përdoren në rrjetet e mëdha, me qëllim që të shërbejnë si ndërfaqe midis rrjetit stacionar dhe pajisjeve të lëvizshme. Ato janë pak më të vështira për t'u konfiguruar se sa rrjetet Ad-Hoc, por lejojnë skalim të diferencuar të rrjetit.

Standardet dhe klasifikimi në modelin OSI

Application Layer	
Presentation Layer	
Session Layer	
Transport Layer	
Network Layer	
Data Link Layer	Familia e protokolleve 802.11
Physical Layer	

Protokollet, të cilat përcaktohen nga IEEE për standardet e rrjeteve pa kabëll, janë përmbledhur në standardin 802.11 që paraqitet në tabelën e mëposhtme.Ato përcaktojnë veprimet në shtresat një dhe dy të modelit OSI dhe përcaktojnë ndër të tjera shpejtësitë e transmetimit dhe procedurën e aksesimit.

802.11 b	Përcakton shpejtësinë e transmetimit deri në 11 Mbps në bandën 2,4-Ghz
802.11 a	Përcakton shpejtësinë e transmetimit deri në 54 Mbps në bandën 5-Ghz
802.11 g	Përcakton shpejtësi më të larta transmetimi deri në 54 Mbps në bandën 2,4-Ghz

13.2 Instalimi dhe testimi i sistemeve pa kabëll të lidhura me LAN-in

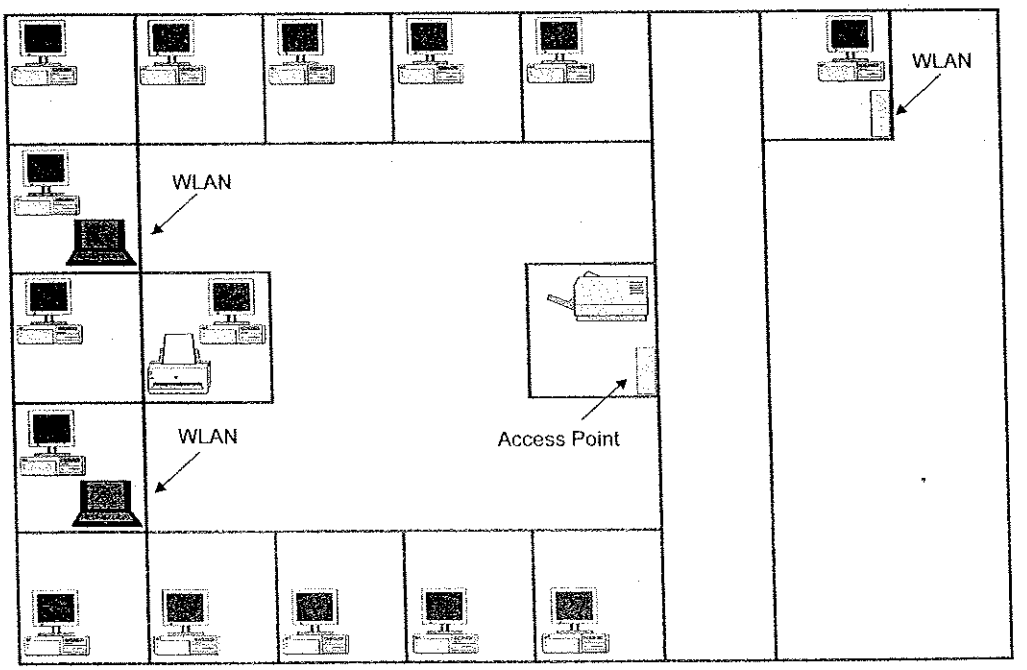
Veçori teknike tek sistemet WLAN

Sistemet Wireless-LAN janë duke avancuar dukshëm. Shpejtësitë e transmetimit të të dhënave janë standardizuar në nivelet 11, 22 dhe 54 Mbit/s. Ashtu si standard-i i Ethernet-it, i cili nga 10 Mbit/s është rritur në 1 Gbit/s, pritet gjithashtu një përmirësim i vazhdueshëm në fushën e WLAN-it.

Shpesh sistemet e WLAN-it janë të pajisura me një funksion IP/DSL-Router, i cili mbështet PPPoE-në (Point to Point Protocol over Ethernet). Access Point-et shërbejnë për lidhjen e klientëve të rrjetit wireless me njëri-tjetrin, gjithashtu ato pajisen me një akses në një pajisje DSL për lidhjen e të gjithë rrjetit me të. Tashmë nuk nevojitet më një DSL-Router që do të mundësonte akses të shpejtë në Internet. Në këtë rast duhet sqaruar patjetër nëse sistemi WAN i zgjedhur i suporton të dyja funksionet njëkohësisht. Ekzistojnë modele, të cilat i kanë të integruara të dyja funksionet, por të cilat nuk mund të shfrytëzohen njëkohësisht. Tek këto modele, gjatë konfigurimit të Access Point-it duhet përcaktuar, nëse Access Point-i duhet të shërbejë si router DSL, apo si akses i pastër në rrjet për klientët e WLAN-it.

Instalimi i sistemeve wireless

Gjatë një vizite në mjediset ku janë vendosur pajisjet e lidhura në rrjet, vemë re se atje gjendet një printer rrjeti. Ky printer është i vendosur në qendër dhe lidhet me rrjetin me anë të një prize rrjeti CAT-5 me dy dalje. Dalja e dytë e prizës së rrjetit është e lirë e si pasojë mund të përdoret për lidhjen e Access Point-it.



Skica e vendosjes së elementeve të një WLAN-i

Zyra e veçuar, që duket në të djathtë të figurës së mësipërme, ka një largësi rreth 20 m nga mjedisi i rrjetëzuar, dhe ndodhet brenda rrezes së mbulimit të Access Point-it të vendosur pranë printerit të rrjetit. Po ashtu, edhe zona e punës së laptop-ëve nuk e kapërcen kufirin e 30 metrave. Në këtë situatë nuk nevojitet vendosja e ndonjë Access Point-i shtesë.

Lidhja e Access Point-it në rrjet nëpërmjet një ndërfaqeje etherneti

Supozojmë se ne rack gjendet një switch 10/100 me 24 porta. Meqë në rrjet (switch) janë lidhur tashmë 14 kompjutera, 2 printera rrjeti dhe 2 laptopë, mbeten ende 6 porta të lira. Nëpërmjet njërës nga këto porta të lira, me anë të ndërfaqes Ethernet, mund të bëhet lidhja e Access Point-it me pjesën kabllore të rrjetit.

Instalimi fizik dhe i drajverave të kartës së WLAN-it në një Desktop-PC

Tashmë është bërë e mundur që kartat PCMCIA-WLAN për laptop dhe kartat PCI-WLAN për PC të instalohen pa problem. Meqë presupozohet që si sistem operativ i instaluar do të jetë Windows XP Professional, kartat do të njihen automatikisht nga sistemi si Plug & Play. Më pas duhet të instalohen driverat që prodhuesit e kartave i përfshijnë së bashku me kartat.

Meqë kompjuterat nuk kanë qenë të lidhur më parë në rrjet, nevojitet që protokollet e nevojshme të rrjetit (p. sh. TCP/IP, NetBEUI etj.) të instalohen dhe konfigurohen.

Konfigurimi i WLAN-it

Me softwaret e përfshira me kartat bëhet konfigurimi i lidhjes së WLAN-it. Softwaret e konfigurimit për Access Point-in preferohet të instalohen në server.

Së pari është e nevojshme të emërtohet Access Point-i. Nëpërmjet përdorimit të disa Access Point-eve është e mundur të krijohen grupe të ndryshme pune (workgroups) brenda WLAN-it. Kjo realizohet nëpërmjet emërtimit të grupeve. Në rast se do të integrohen disa Access Point-e (Roaming), atëhere duhet që emri i dhënë grupit të punës të jetë identik për të gjithë Access Point-et.

Çdo Access Point duhet të ketë një adresë IP-je. Kjo mund t'i jepet statike, ose dinamike nëpërmjet një serveri DHCP. Për klientët duhet instaluar një software, i cili cakton në cilin Access Point do të identifikohet klienti. Në këtë mënyrë ngarkesa e WLAN-it, ne rastet kur janë shumë klientë, do të shpërndahej në mënyrë optimale.

Si rregull Access Point-et integrohen në një grup, me qëllim që të mund të shfrytëzojnë "Roaming"-un. Nëpërmjet integrimit mundësohet mbulimi me sinjal i një sipërfaqeje më të madhe, si dhe rritet fluksi i transferimit të të dhënave. Klienti identifikohet automatikisht nga Access Point-i më i fuqishëm dhe e ndërron këtë Access Point atëhere, kur karakteristikat marrëse muk mjaftojnë për një transferim pa probleme të të dhënave.

13.3 WLAN-i si mënyrë lidhjeje pa kabëll në Internet

Zgjedhja e pajisjeve

Ashtu si tek lidhja WLAN/LAN, edhe në këtë rast rëndësi të veçantë ka zgjedhja e pajisjeve. Në varësi nga numri i klientëve të WLAN-it, duhet pasur kujdes që të sigurohet shpejtësia e nevojshme e transferimit të të dhënave nga Access Point-it tek klientët. P.sh, në rast se në mjediset e një shtëpie është i lidhur nëpërmjet WLAN-it vetëm një laptop në Internet, mjafton një Access Point me shpejtësi transferimi 11 MBit/s, respektivisht 22 MBit/s. Në rast se në rrezen e WLAN-it gjenden më shumë laptopë/PC, të cilët krijojnë një rrjet, duhet instaluar një Access Point me shpejtësi 54 MBit/s. Në këtë mënyrë mundësohet shkëmbimi i të dhënave të klientëve brenda rrjetit WLAN-it.

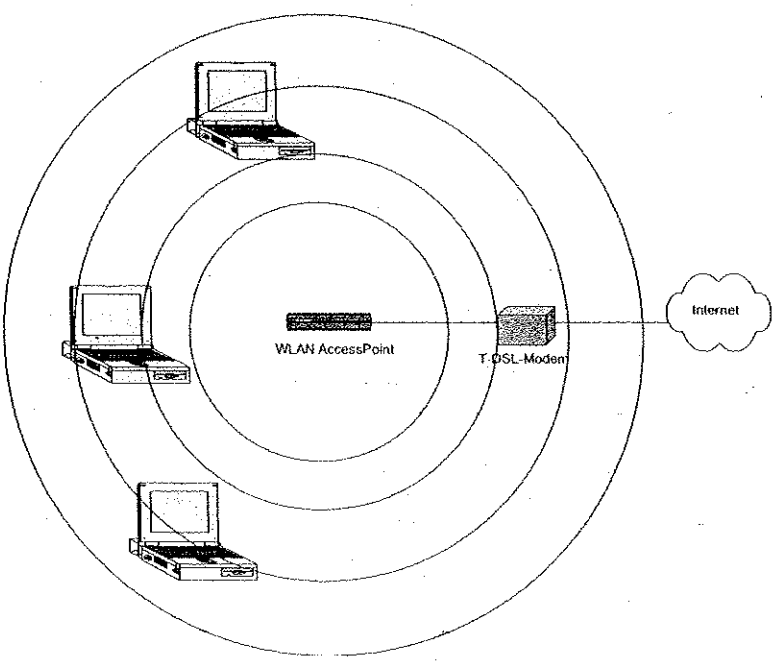
Shënime

Kartat WLAN për klientët janë si më poshtë:

- ☑ PCMCIA (për laptop)
- ☑ PCI (për PC)
- ☑ USB (për laptop/PC me lidhje me portë USB)

Kusht paraprak për WLAN-in, si akses pa kabëll në Internet, është një lidhje funksionale me DSL

Ndryshe nga lidhjet me kabëll WLAN-i mund të përdoret me të gjithë Internet-Provajderat e sotëm, meqë në çdo rast do të përdoret i njëjti protokoll për lidhje, protokolli PPPoE (PPP over Ethernet).



Pamje e përgjithshme e ndërtimit të WLAN-it

Instalimi dhe vënia në punë e Access Point-it

Pas lidhjes së Access Point-it me modemin DSL, ai është gati për punë. Access Point-et janë të konfiguruara në mënyrë të tillë që pa ndonjë konfigurim paraprak, të mund të krijojnë lidhje me një klient WLAN-i.

Instalimi dhe vënia në punë e klientëve

Me qëllim që të vihet në punë klienti në WLAN, duhen instaluar paraprakisht hardware-i (p. sh. WLAN PCMCIA-Karte) dhe software-i përkatës. Të dhëna të hollësishme mbi mënyrën e instalimit dhe përdorimit jepen nga prodhuesit e kartave.

Pas një instalimi pa probleme mund të krijohet një lidhje me WLAN-in, me qëllim konfigurimin e rrjetit. Kjo bëhet ose nëpërmjet software-it që vjen me kartën, ose nëpërmjet ndërfaqes web (Browser-it të Internetit).

Konfigurimi i Access Point-it

Konfigurimi i detajuar i Access Point-it varet nga prodhuesi. Sidoqoftë, konfigurimet më të rëndësishme janë njëlloj tek të gjithë prodhuesit.

- ☑ Access Point-e të ndryshëm mund të funksionojnë si Router, ose si Bridge. Meqë në këtë rast duhet të krijohet një lidhje në Internet, duhet të zgjidhet IP-Router-Mode.
- ☑ Parametrat e TCP/IP-së duhen vendosur që të merren automatikisht me DHCP, me qëllim që gjatë lidhjes në Internet të mund të jepet një adresë IP-je nëpërmjet provider-it.

- ☑ Të dhënat që duhen për lidhjen PPPoE (emri i përdoruesit dhe fjalëkalimi) jepen nga provider-i. Në këtë rast tek Enable PPPoE duhet të jetë zgjedhur opsioni Yes.
- ☑ Connect on Demand do të thotë, që lidhja në Internet krijohet sipas nevojës (p. sh. nëse një klient thërret një faqe nëpërmjet Browser-it). Pasi kalon një kohë e caktuar, lidhja me Internetin shkëputet, në rast se brenda kësaj periudhe kohe nuk ndodh shkëmbim të dhënash me Internetin. Ky lloj konfigurimi është i rëndësishëm para së gjithash në rastet kur kemi tarifa që varen nga koha e qëndrimit në Internet.Në rastet kur kemi tarifë fikse (Flatrate) kjo vlerë mund të vendoset 0 ose mund të mos vendoset fare.
- ☑ Access Point-i ka një DHCP-Server të integruar. Kjo do të thotë që, tek klientët, gjatë konfigurimit, nuk është e nevojshme të behet manualisht hedhja e të dhënave të IP-ve. Adresat e IP-ve jepen automatikisht nga serveri DHCP. Diapazoni i adresave mund të ndryshohet në DHCP-Setup.

Testet e fundit kanë treguar, se një numër i madh WLAN-esh janë të pambrojtura. Kështu p.sh, dikush me një laptop mund të aksesojë rrjetin e një firme nga parkingu. Elementë të sigurisë se sistemit, që janë në dispozicion për mbrojtjen e tij, si kodimi WEP dhe filtri i adresave MAC, duhen aktivizuar patjetër.

Konfigurimi i klientëve

Pas përfundimit me sukses të instalimit, karta e WLAN-it integrohet në sistemin operativ, ashtu si dhe karta e rrjetit. Përmes Software-it që vjen me kartën kryhet konfigurimi i klientit. Ndër të tjera atje mund të shikohet fuqia dhe cilësia e marrjes së sinjalit, shpejtësia e transmetimit dhe adresa MAC.

Gjatë aktivizimit të kodimit WEP duhet pasur kujdes, që lloji i kodimit të jetë i njëjtë (40 Bit, 64 Bit apo 128 Bit) si ai i zgjedhur në Access Point. Çelësi (key) i dhënë duhet të korrespondojë me atë të Access Point-it.

Në rast se në Access Point është aktivizuar DHCP-ja, gjatë konfigurimit të karakteristikave të kartës së rrjetit, tek Properties e TCP/IP-së, duhet aktivizuar opsioni OBTAIN AN IP-ADDRESS AUTOMATICALLY. Në rast se përdoren adresa IP-je statike, një adresë e tillë i duhet dhënë në rrjet edhe Access Point-it.

Përdorimi i serverave DNS (Domain Name Service)

Me qëllim që të mund të vizitohen adresat në web (pra që të mund të hapen faqet e Internetit), duhet të dimë adresën e një serveri DNS. Për adresat e këtyre serverave pyetet Internet-Provider-i. Në varësi të prodhuesit të sistemit të WLAN-it, ekziston mundësia që të dhënat e DNS-Server-it të regjistrohen në Access Point. Tek modelet e vjetra duhej që të dhënat e DNS-Server-it të jepeshin manualisht tek dritarja Properties e TCP/IP-së.

Kërkimi i defektit në WLAN

Pamundësia nga klienti e krijimit i lidhjes me Internetin mund të ketë shkaqe të ndryshme:

- ☑ A ndodhet klienti në zonën e mbulimit të Access Point-it? (testoni fuqinë e sinjalit)
- ☑ A mund të arrihet Access Point-i me komandën ping ? (kontrolloni konfigurimin e rrjetit)
- ☑ A janë shkruar siç duhet në Access Point të dhënat e aksesit nga Internet provider-i? (Kontrolloni PPPoE -në)
- ☑ Në rastin kur është aktivizuar kodimi WEP, a është shkruar saktë çelësi (key) i përdorur si tek Access Point-I, ashtu edhe tek klienti?
- ☑ Në rastin kur filtri i adresave MAC është i aktivizuar duhet kontrolluar nëse janë shkruar saktë adresat e dhëna.

Me qëllim që të ngushtohet rrethi i defektit, mund të ç'aktivizohen kodimi WEP dhe filtrimi i adresave MAC-.

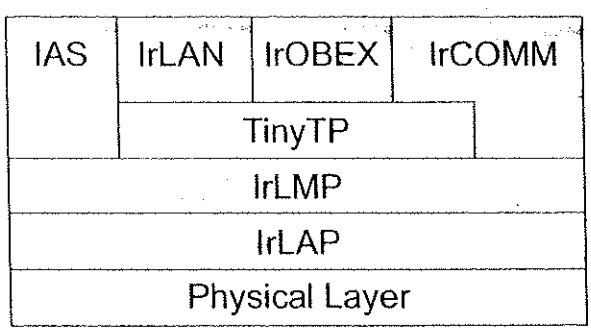
- ☑ Shumë prodhues të sistemeve WLAN integrojnë në sistemin e tyre një WLAN-Monitor ose Logfiles. Këto mund të jenë përcaktuese në gjetjen e problemit. Ndër të tjera është për t'u parë, nëse tashmë do të arrihet lidhja me provider-in, apo problemi qëndron gjatë identifikimit tek ky i fundit (të dhëna të sakta për aksesin).

13.4 Transmetimi i të dhënave me Infrared dhe Bluetooth

Teknika e transferimit me IrDA

Hardware-i i një ndërfaqeje IrDA (infra të kuqe) është ndërtuar si më poshtë: Si dërgues punon një diodë me rreze infra të kuqe me gjatësi vale midis 850 dhe 900 nm. Dioda marrëse mundëson një rreze komunikomi teorike prej rreth 1 metër. Problematik është fakti, që transmetimi është i ndjeshëm dhe reagon ndaj ndikimeve të jashtme si ndriçimi i mjedisit dhe objektet reflektuese. Transmetimi direkt nën dritën e diellit arrin një distancë komunikimi rreth 10 cm, ndërsa nën ndriçimin e një drite artificiale deri në 1 metër.

IrDA paraqet një ndërtim protokolli shumë voluminoz. Protokolli IrLAP (Infrared Link Access Protocol) mundëson krijimin e lidhjes ndërmjet pajisjeve. Në qoftë se ka më shumë se një pajisje, lidhjet krijohen nëpërmjet protokollit IrLMP-së (Infrared Link Management Protocol).



IrDA-Ndërtimi i protokollit

Krijimi i lidhjes bëhet si vijon: Pajisjet IrDA dërgojnë çdo dy sekonda një impuls drite, me qëllim që të sinjalizojnë praninë dhe gatishmërinë e tyre në marrje. Pajisja e parë IrDA, që merr impulsin, provon të krijojë një lidhje.

Pas krijimit të lidhjes, pajisjet nëpërmjet IAS-së transferojnë karakteristikat e tyre si emrin e pajisjes, klasën dhe aftësitë. Kështu bëhet e mundur për një notebook që të identifikojë që pajisja përkundrejt tij është një notebook tjetër, me të cilin mund të shkëmbehen skedarë. Për transmetimin e të dhënave në këtë rast është përgjegjës i ashtuquajturi TinyTP (Tiny Transport Protocol). Ky i fundit përmban në vetvete identifikimin dhe korrigjimin e gabimeve në transmetim.

Mbi këtë protokoll vendosen tri protokolle të nivelit të lartë High-Level-Protocols: IrLAN mundëson aksesin në rrjetet lokale. IrOBEX (Infrared Object Excange Protocol) është përgjegjës për shkëmbimin e skedarëve, por edhe të „kartëvizitave", ose njoftimeve të shkurtra. Ky protokoll është shumë i rëndësishëm për celularët. Protokolli IrCOMM është në gjendje të riprodhojë ndërfaqe seriale me infra të kuqe, ose ndërfaqe paralele. Kjo është vendimtare për aksesin mobil në Internet: Celulari simulon nje modem, që lidhet në rrjet dhe transferon të dhënat. Gjithashtu, përmes IrCOMM është i mundur printimi pa kabëll me printerin përkatës të pajisur me IrDA.

Teknika e transferimit me Bluetooth

Specifikimi i parë i Bluetooth-it u bë në Maj 1998 nga Bluetooth-SIG (Special Interest Group). Bluetooth-SIG u krijua nga firma Ericsson dhe u mbështet në fillimet e saj nga firmat IBM, Intel, Nokia dhe Toshiba. Në Korrik 1999 ky konsorcium paraqiti standardin Bluetooth në versionin 1.0, dhe firma të tjera iu bashkuan Buetooth-SIG-ut: Microsoft, 3COM, Lucent dhe Motorola.

Qëllimi i zhvillimit të Bluetooth-it ishte arritja e realizimit të një lidhjeje pa kabëll, me radiovalë, e cila të konsumonte pak energji dhe të mundësonte megjithatë fluks të lartë transmetimi.

Përparësia më e madhe e Bluetooth-it kundrejt IrDA-së qëndron tek fakti, se pajisjet fundore komunikojnë me njëra-tjetrën edhe pa pasur pamje të lirë, si dhe fluksi maksimal i transmetimit arrin 1 Mbit/s. Rrezja maksimale e komunikimit është rreth 10 metra. Frekuenca e punës është në zonën 2,4-GHz, e cila në të gjithe botën shfrytëzohet pa licensë dhe pa tarifë. Në vetvete, transferimi i të dhënave përmes muresh, çantash apo xhepash xhaketash nuk paraqet problem në këtë frekuencë. Me qëllim që të rritet rrezja e komunikimit, në të ardhmen do të përdoren përforcues 100 mW tek pjesa dërguese. Në këtë mënyrë është e mundur arritja e një rrezeje komunikimi prej 100 metrash.

Siguria me Frequency Hopping Spread Spectrum (FHSS)

Diapazoni i frekuencave në të cilat punon Bluetooth-i është nga 2,402 GHz deri 2,480 GHz. Brenda këtij diapazoni frekuencash punon FHSS-ja në 79 Hops per çdo interval frekuence 1 MHz. Në një sekondë ndodhin 1600 ndryshime frekuence.

Në një Piconet (mini-rrjet që formohet prej pajisjeve Bluetooth) mund të komunikojnë me njëri-tjetrin deri në maksimumi 8 pajisje fundore të pajisura me Bluetooth. Sapo dy apo me shumë pajisje me Bluetooth fillojnë të punojnë, ato identifikohen nëpërmjet një numri serial unik të gjatë 48 Bit. Pajisja e parë fundore që aktivizohet në një Piconet automatikisht bëhet dhe merr përsipër kontrollin e FHSS-së.

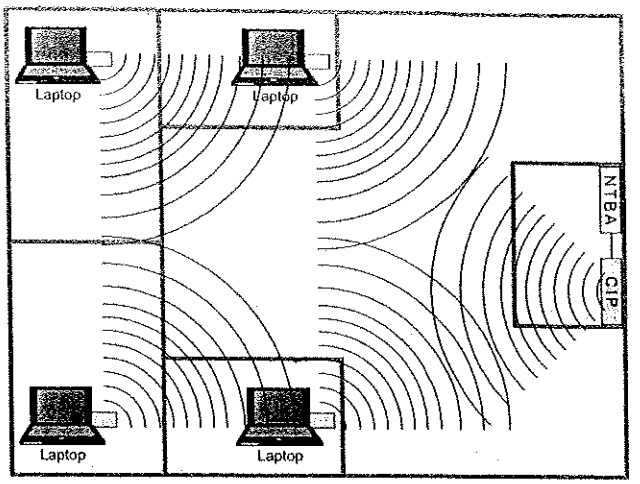
Fusha e zbatimit

Bluetooth-i është shumë i përhapur, për shkak të menaxhimit efikas të energjisë dhe fluksit të lartë të transmetimit, në fushën e telefonisë celulare. Pajisje si: Celularë, Organizera, PDAs, Notebooks etj., e kanë tashmë të integruar teknologjinë Bluetooth.

Një nga pajisjet e para Bluetooth është diktofoni portabël i firmës Ericsson. Pajisja peshon rreth 20 gram. Në një rreze prej rreth 10 metrash celulari mund të mbahet në xhep, në çantë apo të vendoset në dhomën fqinjë.

Shënime

Një veçori tjetër është që CIP-i (Common ISDN Access Profile), mundëson lidhjen ISDN over Bluetooth. Në këtë CIP janë në dispozicion pajisje fundore me Bluetooth të gjithë treguesit e performancës të ISDN-së në kanalin B dhe D. Si qendër shërben një Access Point ISDN, i cili është lidhur me ISDN-NTBC-në. Kjo mbështet pajisjet aktive fundore me Bluetooth në një rreze deri në 100 metra me karakteristikat e performancës së ISDN-së.



Common ISDN Access Profile (CIP)

Siguria në ambjente publike

Me qëllim që të parandalohen interferencat në mjedise publike, si spitale dhe aeroporte, ekziston mundësia që pajisjet me Bluetooth, si celularët dhe PDAs, të ç'aktivizohen që në portën e hyrjes. Sistemi i njeh automatikisht pajisjet me Bluetooth dhe i mbyll ato. Në ambjente më pak të rrezikuara, si p.sh. ne teatër, me këtë sistem mund të ç'aktivizohet zilja, ose t'i bëhet transferimi i thirrjes në sekretarinë telefonike të celularit.

13.5 Transferimi i të dhënave me radiovalë ose laserlink

Radiovalët për kapërcimin e distancave të shkurtra midis dy rrjeteve

Lidhja me radiovalë ofrohet si lidhje Point-to-Point midis dy rrjeteve (LAN-to-LAN)

- ☑ Në ndërtesa të ndryshme brenda kompleksit të firmës
- ☑ Midis dy ndërtesave të firmës, të cilat ndahen nga rruga
- ☑ Si broadband access në Internet nëpërmjet një Internet provider-i (Carrier) lokal

Meqë të gjitha lidhjet me kabëll përmes terreneve publike janë në përgjegjësi të Telekomit, shfrytëzimi i tyre shoqërohet me lejet dhe tarifat përkatëse. Si alternativë e sistemit të komunikimit me radio ofrohet një linjë fikse midis dy ndërtesave, shfrytëzimi i së cilës sjell me vete kosto të larta.

Avantazhet dhe disavantazhet e një lidhje me radiovalë

Avantazhe	Disavantazhe
Tarifë zero për shfrytëzimin e frekuencës 2,4-GHz (WLAN); Identifikimi i thjeshtë (në shumicën e rasteve merret përsipër nga firma që kryen instalimin)	Kur shfrytëzohet frekuenca 2,4-GHz e WLAN-it kufizimi është në 13 kanale dhe fuqia në dalje 100 Milliwatt Kur shfrytëzohet frekuenca 5-GHz fuqia në dalje shkon nga max. 200 Milliwatt deri në 1 Watt
Transferim i sigurtë i të dhënave nëpërmjet kodimit dhe filtrimit te adresave MAC (Access Control)	Kërkohet pamje e lirë midis stacioneve të radios
Rreze transmetimi deri 2 km	Fortësia e sinjalit dhe rrezja e mbulimit varen nga moti (shi, mjegull dhe dëborë)
Nuk ka rrezik për shëndetin nga rrezatimi, pasi fuqia në dalje është e ulët, 100 Milliwatt	Priret të ndikohet nga interferenca e radiove të privatëve dhe kompanive tregtare
Shpejtësi transmetimi 11, 22 ose 54 Mbit/s janë të mundura, në varësi te protokollit të përdorur	

Informacione të mëtejshme dhe rregulloret për shfrytëzimin për qëllime tregtare të lidhjeve me radiovalë mbi ndërtesat publike do t'i gjeni ne faqen *www.bundesnetzagentur.de*.

Free Space Optics (FSO)

Meqë sistemet që përdoren sot me radiovalë, punojnë me lidhjen Point-to-Point, më tej, për këto sisteme, do të përdoret termi *Free Space Optics* (FSO).

Sistemet tregtare FSO kapërcejnë largësi deri në disa kilometra dhe arrijnë shpejtësi transmetimi deri në 2,5 Gbit/s. Këto sisteme përdoren, gjithkund ku kërkohet fluks i lartë transmetimi dhe ku aplikimi i lidhjes me fibra optike është i pamundur, ose shumë i shtrenjtë.

Avantazhet dhe disavantazhet e një lidhje FSO

	Disavantazhe
Tarifë zero	Kosto të larta
Siguri e lartë në transmetimin e të dhënave, që realizohet përmes një rrezeje të ngushtë drite	Ndikohet negativisht nga tymi mjegulla dhe ndotja e ajrit
Fluks i lartë transmetimi	Ndikohet negativisht nga drita dhe hijet, gjithashtu edhe nga ndërprerjet nga pengesat fizike (zogjtë, vinçat, apo platformat e larta)
Ndikim i paktë nga shiu dhe bora	
Nuk ndikohet nga radiovalët tregtare apo private	

Informacione të mëtejshme do të gjeni ne faqen *www.freespaceoptics.org*.

Shënime

14 Krijimi i lidhjes në Internet

Në këtë kapitull do të lexoni:
- → çfarë është ISDN-ja
- → si punon ISDN-ja
- → si mund ta përdorni ISDN-në

Parakushte
- ✓ Njohuri bazë mbi rrjetet
- ✓ Njohuri bazë mbi konfigurimin e hardware-ve

14.1 Aksesi në rrjetet analoge

Modem-i

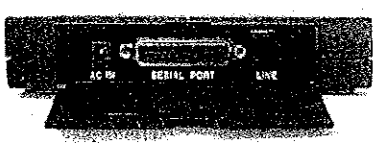
Gjatë proceseve analoge transmetohen sinjale me frekuenca dhe amplituda të ndryshme. Meqë kompjuteri punon me sinjale dixhitale, atëhere nevojitet një pajisje konvertuese: Modem-i.

Modem-i (Modulator/Demodulator) është në gjendje, që të dhënat dixhitale t'i modulojë në sinjale analoge (ton-) dhe sinjalet analoge t'i demodulojë në të dhëna dixhitale. Modemi lidhet në prizat e përshtatshme për kokat e standardit RJ11. Prizat TAE (Telefon-Anschluss-Einheit) – i takojnë standardit gjerman. Prizat trefishe të telefonit i përgjigjen kodit NFN që do të thotë: lidhja e mesit koduar si F i përket telefonit, ndërsa në dy lidhjet e tjera të koduara si N lidhen pajisje të tjera si modem, sekretari telefonike apo faks.

Modemat aktual punojnë me shpejtësi 57,6 Kbps në marrje (downstream) dhe 33,6 Kbps në dërgim (upstream), e cila i korrespondon afërsisht dërgimit të 2 faqeve tekst në sekondë. Performanca e këtyre modemave shpesh jepet nëpërmjet standardeve V.90 ose V.92. Shifrat më të ulta tek standardet V presupozojnë fluks transmetimi më të ulët.

Shumica e PC-ve sot shiten me modem të inkorporuar (internal). Figura e mëposhtme tregon pamjen e përparme dhe të pasme të një modemi të jashtëm (external).

Pjesa e përparme



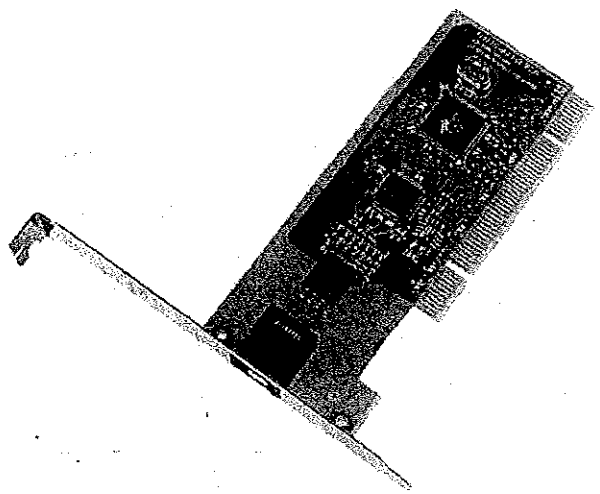
Pjesa e prapme me daljen për lidhjen e ushqimit me rrymë (AC IN), ndërfaqen seriale RS-232 (Serial Port), RJ-11-ndërfaqen e lidhjes së linjës së telefonit (Line)

Modem

14.2 Aksesi përmes ISDN-së në rrjetet dixhitale

Karta ISDN

ISDN (Integrated Services Digital Network) është një standard telekomunikacioni, i cili ofrohet nga telekomi si **T-ISDN**. Të dhënat (data) dhe të zëri (voice0 dixhitalizohen para transmetimit dhe më pas transmetohen në të njëjtin brez frekuencash si transmetimi analog i deritanishëm. Lidhjet ISDN disponohen në klasa performace të ndryshme. Lidhja më e thjeshtë ISDN është **lidhja bazë ISDN**, e cila përfshin tri kanale transmetimi të veçanta. Dy **Kanale B** ofrojnë respektivisht 64 KB/s dhe janë përgjegjëse realisht për transmetimin e të dhënave, ndërsa i treti, **Kanali D**, ofron shërbime shtesë dhe menaxhon krijimin e lidhjes.



Adaptor ISDN

Për të realizuar komunikimin nëpërmjet ISDN-së PC-së i nevojitet një kartë ISDN (adaptor ISDN). Kjo kartë lidhet me prizën ISDN me anën e një kabli me koka RJ-45. Karta ISDN merr përsipër funksione të ngjashme si një kartë rrjeti normale, por sidoqoftë me fluks më të ulët transmetimi.

Historiku dhe shfrytëzimi si shërbim

Integrated Services Digital Network (ISDN) është një formë dixhitale e transmetimit të informacionit, e cila punon në shtresat 1 dhe 3 të modelit OSI.

Qysh prej vitit 1993 ISDN-ja është vënë në dispozicion si shërbim në Gjermani me mbulim në të gjithë vendin. Para së gjithash ajo ofron fluks transmetimi informacioni më të lartë se rrjeti telefonik analog. Kjo çon në një përmirësim të cilësisë audio të telefonisë, para së gjithash në rastin e një gjerësie bande të madhe, e cila i vihet në dispozicion kompjuterave në lidhjet WAN. Për më tepër mund të ofrohen shërbime të ndryshme shtesë (p. sh. trokitja, transmetimi i numrit të thirrjes etj.).

Gjerësi të madhe bande sot ofrojnë edhe shërbime të tjera WAN, por ISDN-ja është i vetmi shërbim i shpejtësisë së lartë që ofron mundësinë e krijimit të lidhjeve me një partner të përcaktuar në komunikim.

Bazat e ISDN-së

Për ta përdorur në telefoni duhen dixhitalizuar sinjalet analoge që transmetojnë zërin. Kjo bëhet tek ISDN-ja me ndihmën e një pulse-code-modulation me rezolucion 12-Bit. Të dhënat që përmbahen atje konvertohen në paketa 8 Bit-she, me gjatësinë e një "fjale" për të dhënat analoge, të cilat transmetohen nëpërmjet ISDN-së.

Shënime

Kanalet e të dhënave

Kanalet janë linja virtuale transmetimi. Ato krijohen nëpërmjet ndërkyçjes (interlocking) periodike të transmetimit të paketave me të dhëna në një apo më shumë linja fizike transmetimi. Të dhënat e shfrytëzueshme transmetohen në kanalet B (bearer- ose basic channel). Çdo kanal B ka një kapacitet prej 64 kb/s. Tek lidhjet bazë (BRI = Basic Rate Interface) dhe teklidhjet e pajisjeve gjenden në dispozicion dy kanale B. Përveç kësaj, nevojitet edhe një kanal kontrolli (kanali D). Ai ka një kapacitet prej 16 kb/s. Në kanalin D, krahas sinjaleve të kontrollit (8 kb/s) mund të transmetohen edhe të dhëna të tjera (8kb/s) via X.25 ose Datex-P.

Kanalet e protokolleve

Për kanalin D sot, gati në gjithë Evropën, përdoret protokolli DSS1/Euro-ISDN (Digital Subscriber System Number 1), (në Francë VN5, VN6, i cili është kompatibël me DSS1). Gjatë përdorimit të protokolleve të vjetra si p.sh. 1TR6 (Gjermani), apo ISDN30 (Angli) sigurisht që është e mundur të komunikohet me pajisjet kompatibël me DSS1. Në SH.B.A janë protokollet ISDN-1, NI-1 (standard) ose ISDN-2, NI-2 (zhvilluar më tej).

Shtresat e ISDN-së

Bashkësia e protokolleve për kanalet B ndahet në tre shtresa: B1, B2 dhe B3.

Shtresa	Detyra	Protokolli (shembuj)
B1	Shtresa fizike e transmetimit të Bit-eve	**Karakteristika:** Bit transparent, transmeton të dhënat të ç'paketuara si rradhë e njëpasnjëshme Bit-esh **V.110** Barazon shpejtësitë e pajisjeve në komunikim nëpërmjet mbushjes me Bit-e (full bits)
B2	Korrigjimi i gabimeve nëpërmjet transmetimit të përsëritur të blloqeve të dëmtuara të të dhënave	**Karakteristika:** Bit transparent, që transmeton të pasiguruara në kanalin B, të folurit dhe të dhëna të tjera "analoge" **V.120** Kontrolli i rrjedhës së të dhënave tek lidhjet midis pajisjeve fundore me shpejtësi të ndryshme **HDLC (High Performance Data Link Control)** Përdoret në lidhjet në Internet me PPP, gjatësia e paketës maksimumi 512 Byte **X.75** Protokoll i sigurt me gjatësi pakete 2kByte, me opsion komprimimi
B3	Shtresa e negocimit, Renditja e paketave me të dhëna sipas aplikacioneve të ndryshme	**Karakteristika:** Transparent vetëm për një aplikacion, i cili shfrytëzon kanalin e të dhënave **T.70, T.90** Përmes Byte-it të drejtimit në kreun e paketës, paketa i bashkëngjitet aplikacionit përkatës **ISO 8208** Përdoret në transferimin e Euro-file-ve

Llojet e lidhjes

BRI (Basic Rate Interface; lidhja me disa pajisje)

Linja telefonike përfundon nëpërmjet të ashtuquajturës NTBC ("Network - Terminal – Basic – Connection"). Këtu fillon bus-i i brendshëm S0, me të cilin do të lidhen pajisjet e veçanta ISDN. Janë në dispozicion dy kanale B (64 kb/s) dhe një kanal D (16 kb/s). Zakonisht jepen tre numra thirrje (numra MSN), të cilat u caktohen pajisjeve ISDN. Në këtë mënyrë mund të kombinohen disa lidhje në të njëjtin numër thirrje, me qëllim që të kemi në dispozicion më shumë kanale B për të njëjtin numër thirrje.

Lidhja e pajisjeve

Tek NTBC-ja lidhet vetëm një pajisje ISDN (pajisje TK). Edhe këtu janë në dispozicion dy kanale B (64 kb/s) dhe një kanal D (16 kb/s). Caktohet një numër thirrjeje. Këtyre u jepen numrat 0 - 9 (tek pajisjet më të mëdha 0 - 99), me qëllim që me këto numra të brendshëm të identifikohen pajisjet e caktuara. Në mënyrë të ngjashme si tek lidhjet e integruara për shumë pajisje edhe në këtë rast është e mundur të kombinohen disa lidhje, me qëllim që të disponohen më shumë kanale B për të njëjtin bllok numrash thirrjeje.

Lidhja integruese

Në këtë rast bashkohen disa BRI dhe arrihen nga një numër thirrje i përbashkët. P.sh. për dy kanale B vihen në dispozicion katër lidhje.

Lidhja me multiplex primar

Nëse akumulohen sasi më të mëdha të dhënash, atëhere është e mundur që të integrohen disa kanale B. Primary Rate Interface (PRI) paraqet versionin evropian të një lidhje me multipleks primar.

- ☑ Tek lidhjet Evropiane me multiplex primar (PRI, E1 ose S2M) vihen në dispozicion 30 kanale B, një kanal D për kontrollin e sinjaleve, si dhe një kanal D për X.25 me respektivisht 64 kb/s për kanal. Kjo rezulton në një fluks transmetimi prej 1,92 Mb/s.
- ☑ Në Japoni dhe në Amerikën e Veriut përdoren lidhjet T1. Ato disponojnë 24 kanale me 64 kb/s për kanal, nga të cilat mund të përdoret njëri si kanal D ose sipas aplikacionit përkatës dhe tjetri si kanal B. Si rezultat, kemi një fluks maksimal transmetimi prej 1,56 Mb/s.

Bus-i S0

Lidhja e pajisjeve ISDN kryhet tek Bus-i S0 (quhet ndryshe S Zero). Ky është ndërtuar prej dy çifte fijesh, secila për drejtimin përkatës të transmetimit. Të tria kanalet (2B+1D) transmetojnë në një linjë të vetme me katër fije me një kapacitet transmetimi prej 144 kb/s. Bus-i fillon tek NTBC-ja dhe mbaron tek priza e fundit, ku është lidhur ISDN-ja. Në një gjatësi bus-i prej 200 m mund të lidhen deri në 12 priza IAE në një Bus S0. Me to mund të lidhen deri në tetë pajisje.

Tek vetëm katër priza lidhje, të cilat gjenden në 50 m e fundit të busit S0, është i mundur një gjatësi bus-i prej 500 m.

Meqë sinjalet e një thirrjeje vijnë tek të gjitha pajisjet e lidhura në bus, duhet që ato vetë të vendosin, nëse duhet të reagojnë apo jo, në bazë të objektivit MSN të bashkëdërguar.

Shënime

Veçoritë e shërbimit dhë shërbimet

Tek ISDN kemi mundësi të ndryshme zgjedhjeje në dispozicion për shërbimet dhe veçoritë e tyre.

Me ndihmën e veçorive të shërbimeve, nga të cilat disa kanë akses edhe në T-NET-in dixhital të telekomit, plotësohen funksione të ndryshme organizative.

Si shërbim përshkruhet lloji i të dhënave të transmetueshme. Ato identifikohen nëpërmjet numrash (portash) dhe duhet t'u caktohen pajisjeve ISDN. Një pajisje ISDN kontrollon më pas, nëse identifikimi i saj i shërbimit përputhet me atë të marrësit.

Veçori të shërbimit

Shkurtime	Shkurtimi i ...	Funksioni
AOCD	advice of charge during the call	Transmetimi i informacionit mbi tarifën e bisedës gjatë saj
AOCE	advice of charge at the end of call	Transmetimi i informacionit mbi tarifën e bisedës në fund të saj
CCBS	completion of calls to busy subscribers	Rithirrje automatike kur numri del "i zënë"
CFB	call forwarding busy	Transferimi i thirrjes kur numri del "i zënë"
CFNR	call forwarding no reply	Transferimi i thirrjes kur "nuk përgjigjet"
CFU	call forwarding unconditional	Transferimi i pakushtëzuar (i menjëhershëm) i thirrjes
CLIP	call line identification presentation	Identifikimi i numrit të thirrjes së marrësit nga pritësi i thirrjes
CLIR	call line identification restriction	Kufizim i identifikimit të numrit të thirrjes së marrësit nga pritësi i thirrjes
COLP	connected line identification presentation	Transferimi i numrit të thirrjes së marrësit nga pritësi i thirrjes
COLR	connected line identification restriction	Kufizimi i transferimit të numrit të thirrjes së marrësit nga pritësi i thirrjes
CË	call waiting	Pritje e thirrjes në linjë

Identifikimi i shërbimit tek CAPI 2.0 në Euro-ISDN

Numri ID	Identifikimi i shërbimit	Numri ID	Identifikimi i shërbimit
1	Voice	16	Digital voice
2	Data/Standard	17	Fax G2/3
3	Data/Limited	18	Fax G4-I
4	Voice 3,1 kHz	19	Fax G4-II/III
5, 26	Voice 7 kHz	20, 21, 23	Telex
6	Video	22	Videotext
7	Packet Mode	24	X400/eMail
8	Adaptor 56 kb/s	25	X200/OSI
9	Data and news	27, 28	Videotelefon

Meqë pajisjet, të cilat janë konfiguruar për një numër të përcaktuar MSN-je, gjatë një thirrjeje e cila u drejtohet atyre, reagojnë vetëm atëherë, kur shërbimi i vet i identifikimit përputhet me shërbimin e kërkuar, është e mundur që disa pajisje, të cilat kanë njohje shërbimi të ndryshme, t'i renditen të njëjtës MSN.

Përveç kësaj disa pajisje janë në gjendje ta identifikojnë vetë shërbimin. Para së gjithash kjo është e nevojshme, në rastet kur p.sh. një modem ISDN, duhet të zotërojë disa shërbime, në këtë rast p.sh. të dhëna, faks dhe telefon.

Drajver-i CAPI

Drajveri CAPI (Common-Application-Program-Interface driver) iu mundëson kartave ISDN për PC të komunikojnë në një rrjet ISDN-je, të identifikojnë shërbimet dhe të shfrytëzojnë veçoritë e tyre. Sot në Evropë si standard përdoret CAPI 2.0. CAPI paraqet në vetvete një bashkësi komandash, të cilat duhet integrohen në sistemin përkatës operativ, me qëllim që një aplikacion të mund të komunikojë nëpërmjet ISDN-së. Gabimet e transmetimit tregohen me ndihmën e një kodi katërshifror gabimi.

14.3 Fushat e përdorimit të ISDN-së

Telefonia

Bazuar mbi numrin e shërbimeve që mbështet, ISDN-ja mund të përdoret në shumë fusha në të cilat kërkohet transmetim informacioni.

- ☑ Pajisjet telefonike
- ☑ Call Center-at e drejtuara nga kompjuteri (karta ISDN e kompjuterit duhet të mbështesë shërbimet përkatëse)
- ☑ Konferencat telefonike
- ☑ Sekretaritë telefonike

Transmetimi i të dhënave

- ☑ Lidhja me dial-up në Internet nëpërmjet një provajderi (provider-ofrues shërbimi)
- ☑ VPN (Virtual Private Network): Me ndihmën e VPN-së mund të lidhemi nëpërmjet Internetit me një LAN në distancë (remote), pa qënë e domosdoshme të shtrihet një kabëll apo të merret me qera një linjë e shtrenjtë.
- ☑ Lidhja dial-in tek një partner i caktuar: Meqë lidhja me partnerin në komunikim bëhet nëpërmjet rrjetit telefonik dhe jo nëpërmjet Internetit, nuk është i mundur një sulm i hacker-ave.

14.4 ISDN-ja në praktikë

Llojet e kabllove/Lidhjet

Si lidhje për abonentët shtëpiak (për BRI-të dhe lidhjet e pajisjeve) mund të përdoret një kabëll katër fijesh, si ai që përdoret për lidhjet e zakonshme analoge. Në rast se lidhja gjendet në fund të bus-it ISDN të ofruesit të shërbimit, atëherë bus-i duhet terminuar në NBTC (100 Ω). Sigurisht, kjo e fundit duhet të lidhet në një vendshkëmbyes (central) dixhital, i cili lejohet të jetë në një largësi deri maksimumi 20 km.

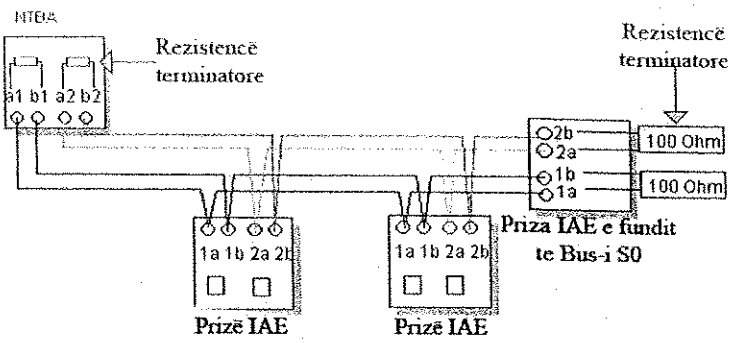
Lidhjen e NTBC-së tek linja e abonentit shtëpiak duhet ta kryejë ose një teknik i firmës ofruese të shërbimit, ose ky i fundit mund të ndryshojë NTBC-në. Firma disponon një kabëll lidhës me një kokë të zakonshme, e cila futet tek priza përkatëse (priza lidhëse, e cila bëhet gati nga ofruesi i shërbimit).

Për bus-in S0 duhet përdorur të paktën kabëll Twisted-Pair kategoria 2. Si rregull ato janë linja si ato që përdoren për rrjetet telefonike analoge të brendshme.

Në fundet e bus-eve çdo cift fijesh duhet të lidhet me një rezistencë (100 Ω) mbyllëse (terminator).

Bus-i S0 shfrytëzon të katër fijet e linjës si më poshtë:

Lidhjet tek prizat IAE përdorin një kokë standard RJ11 me katër kontakte si tek telefonat analogë. Gjithashtu, në vend të tyre mund të përdoren edhe prizat UAE8 me koka RJ45, nga tetë kontaktet e të cilave vetëm katër të mesit shfrytëzohen. Mbulimi i kabllove paraqitet si më poshtë:



NTBC	a1	b1	a2	b2
Kabell: katër fijesh, kodi i ngjyres	I kuq	I zi	I bardhë	I verdhë
Kabell: katër fijesh, kodi i unazës	Pa unazë	Unazë teke, hapësirë e gjërë	Unaza dyshe, hapësirë e gjërë	Unaza dyshe, hapësirë e ngushtë
Kabell: 12/16 fijesh	E bardhë	Blu	E bardhë	Kafe
Priza IAE	1a	1b	2a	2b
Priza UAE/RJ45	4	5	3	6

Lidhja e një PC-je

Me qëllim që një PC të lidhet me një bus S0, janë në dispozicion disa adaptorë:

- ☑ Për lidhjen tek portat seriale (COM)
- ☑ Për lidhjen tek ndërfaqet paralele (LPT)
- ☑ Për lidhjet tek portat USB
- ☑ Si karta PCI
- ☑ Tek bus-i PCMCIA për laptop-ë

Në qoftë se një aplikacion është programuar për përdorimin e modem-ave analogë, atëhere funksionet e nevojshme duhen emuluar nëpërmjet drajverave përkatës. Në parim për një sistem operativ të caktuar, duhen instaluar drajverat CAPI të përshtatshëm për të, me qëllim që të mund të shfrytëzohen veçoritë e shërbimit ISDN për PC-të.

Përdorimi nga telefonat analogë

Pajisje të përshtatshme telefonike, japin mundësinë që krahas një bus-i S0 të ketë mundësi lidhje edhe për telefona anlogë, modem-a, apo fakse. Në këtë rast pajisja telefonike merr përsipër konvertimin A/D të sinjaleve, njohjen e shërbimit dhe identifikimin e numrit MSN.

14.5 Zhvillime të reja

A do të zëvendësohet TAPI nga CAPI?

Nëpërmjet lidhjes së sistemeve kompjuterike në një rrjet ISDN krijohen një sërë mundësish, të cilat standardi CAPI nuk i mbështet, si p.sh. telefonat drejtuar nga software-t, video-konferen-cat, sistemet call center etj.
Meqë standardi amerikan TAPI i mbështet këto funksione (po ashtu edhe funksionet CAPI), atëhere prodhuesit e aplikacioneve për ISDN priren ta përdorin gjerësisht këtë standard. Kjo do të çojë me siguri, që në të ardhmen CAPI të zëvendësohet në mbarë botën nga TAPI.

14.6 Bazat e DSL-së

Zhvillimi i DSL-së

Në vitet 80, nevojat gjithnjë në rritje për gjerësi bande, në rrjetet WAN, çuan në përfundimin se duhej gjetur një mënyrë që rritja e gjerësisë së bandës të mund t'i ofrohej edhe masës së gjerë të përdoruesve në një kohë të shkurtër, me mbulim të gjerë dhe me kosto të ulët. Para së gjithash, lidhjet e abonentëve analogë tek rrjeti bazë konsiderohen si „bottleneck". DSL është shkurtimi i Digital Subscriber Line (Linjë abonimi për lidhje dixhitale) dhe paraqet dixhitalizimin e të ashtuquajturit „km i fundit" , pra shtrirja e kabllit të telefonit deri tek klientët fundor "last mile", Me ndihmën e teknologjive DSL është bërë i mundur shfrytëzimi dixhital i kabllove ekzistuese prej bakri të rrjetit telefonik.

Me POTS (Plain Old Telephone Service) përshkruhet rrjeti telefonik analog tradicional. Ai përfshin një diapazon frekuencash nga 300 Hz - 3,5k Hz në kabllot prej bakri dhe me anë të modemave mund të transmetojë një fluks bruto të dhënash deri në 56 kbit/s. ISDN-ja ishte teknika e parë DSL, e cila nëpërmjet një diapazoni frekuencash të përdorura nga 0 Hz - 50 kHz arrin një fluks bruto transmetimi të dhënash prej 160 kbit/s në të dy drejtimet dërgim dhe marrje (përdorimi i një BRI-e, Basic Rate Interface).

Gjithsesi, kapaciteti i transmetimit të fijeve dyshe të bakrit nuk mbaron këtu. Përdorimi i teknikave moderne të modulimit, si dhe një rritje e gjerësisë së bandës së përdorur deri në nivelin MHz, mundëson sot arritjen e transmetimit të një fluksi të dhënash deri në 52 Mbit/s.

Ndarja e teknologjive DSL

Teknologjitë e vecanta DSL përmblidhen nën termin xDSL dhe ndryshojnë nga njera tjetra, para së gjithash nga numri i cifteve të fijeve të përdorura, brezat e frekuencës dhe llojet e modulimit që përdorin:

Shkurtimi		Modulimi	Brezi i frekuencave	Fluksi i të dhënave	Distanca	Ciftet e fijeve
POTS	Plain Old Telephone Service		300 Hz - 3,5 kHz	56 bit/s		2
ISDN	Integrated Services Digital Network		0 Hz - 50/ 130 kHz	144 bit/s		1
HDSL	High Data Rate DSL	CAP	0 Hz - 292 kHz	2 Mbit/s	4 km	2 - 3
SDSL	Single Line DSL	PAM	0 Hz - 387 kHz	2 Mbit/s	3 km	1
ADSL up	Asymmetric DSL	CAP ose DMT	25 kHz - 138 kHz	640 kbit/s	5,5 km	1
ADSL down			138 kHz - 1,1 MHz	8 Mbit/s		
VDSL	Very High Data Rate DSL	CAP, DMT, DWMT dhe SLC	200 kHz - 30 Mhz	52 Mbit/s	1,5 km	1

Variante më pak të përhapura janë BDSL (Broadband DSL) dhe UDSL (Universal DSL).
T-DSL, M-DSL dhe Q-DSL janë emërtime produktesh të ADSL-së. Sky-DSL përfaqëson një lidhje abonenti nëpërmjet antenës satelitore (downstream) dhe një lidhje tradicionale me modem/ISDN (upstream).

Një veçori e ADSL-së është ndarja asimetrike e gjerësisë së bandës në dispozicion. Klientët privatë në përgjithësi marrin shumë më tepër të dhëna sesa dërgojnë. Për këtë arsye, fluksi i të dhënave të dërguara (upstream) kufizohet me qëllim të favorizimit të një fluksi më të madh të dhënash të marra (downstream).

Llojet e modulimit

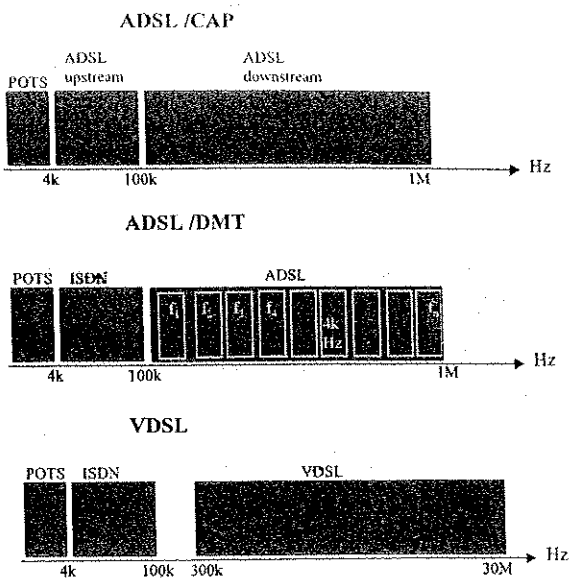
- ☑ **PAM:** Pulsed Amplitude Modulation
- ☑ **DMT:** Discrete Multitone Modulation
- ☑ **DWMT:** Discrete Wavelet Multitone Modulation, Variant i DMT
- ☑ **CAP:** Carrierless Amplitude/Phase Modulation, Variant i Quadratur Amplitude Modulation QAM
- ☑ **SLC:** Simple Line Code

Modulimi CAP krijon një sinjal, i cili nuk transporton të dhëna, dhe që tek i cili kryhen të ashtuquajturat up- dhe downstream në breza frekuence të ndara nga njëra-tjetra.

Modulimi DMT ndan bandën e përdorur të frekuencave në 32 kanale upstream- dhe 256 kanale downstream me respektivisht 4kHz gjerësi bande secila, cilësia e të cilave monitorohet. Gjatë interferencave në banda të veçanta frekuence, Bitrate-i mund të bjerë, ose mund të kalojë në kanale alternative. Modulimi DMT përdoret gjithnjë e më shpesh, para së gjithash nga ADSL-ja dhe duket se do të mbizotërojë për një kohë të gjatë.

VDSL-ja përdor lloje të ndryshme modulimi (shih tabelën në faqen pararendëse).

Distanca për t'u mbuluar për një fluks të dhënash të caktuar varet para së gjithash nga humbjet nga interferenca, dobësimi i sinjalit, seksioni tërthor dhe reflektimi i kabllit. Të ashtuquajturat sisteme të adaptueshme sipas fluksit të të dhënave mund të favorizojnë arritjen e një distance më të madhe mbullimi me uljen e fluksit të transmetimit.



Llojet e modulimit

POTS, ISDN dhe xDSL në një çift fijesh

Përdorimi i njëkohshëm i HDSL-së dhe POTS-it apo ISDN-së në të njëjtën linjë nuk është i mundur, pasi kjo teknikë DSL e përdor të gjithë brezin e frekuencave që ka në dispozicion. SDSL-të mund ta integrojnë POTS-in ose ISDN-në në DSL, si dhe të venë në dispozicion ndërfaqe lidhjesh analoge a/b ose ndërfaqe S_0. NTBC-ja në këtë rast do të ishte e tepërt.

Tek ADSL-ja është i mundur përdorimi i njëkohshëm i POTS-it nëpërmjet të ashtuquajturve POTS-Splitters (Emri nga Telekomi NTBBC, Network-Termination-Broad-Band-Connection). Këto splitter-a punojnë si një ç'kyçës (switch) frekuencash dhe vënë në dispozicion lidhje, si për DSL-në, ashtu edhe për telefoninë analoge. Referuar ISDN-së, ekzistojnë dy mundësi: Sipas ofruesit të lidhjes DSL, kufijtë e poshtëm të brezit të frekuencave që shfrytëzon DSL-ja mund të të jenë kaq të ulta, sa që të interferojnë me shërbimin ISDN. Shërbimet dixhitale ISDN duhet që paketat me të dhëna, të cilat transmetohen më pas nëpërmjet DSL-së, të paketohen (si tek SDSL-ja). Në qoftë se frekuenca (kufiri i poshtëm i saj) e bandës ADSL është aq sa duhet, atëhere sinjali ISDN nuk interferohet dhe me anën e një splitter-i ISDN (NTBBC) mund të ndahen nga sinjali ADSL.

Për POTS-in dhe ISDN-në, VDSL-ja kërkon një Splitter.

Norma dhe Standarde

Standardi	Komiteti/Instituti	Norma
HDSL	ETSI (European Telecommunications Standards Institute)	ETR152
ADSL	ANSI (American National Standards Institute)	T1.413
UDSL	UAWG (Universal ADSL Working Group) ITU (International Telecommunication Union)	G.Lite G.992.2
SDSL	ETSI, ITU	G.shdsl

14.7 DSL-ja në praktikë

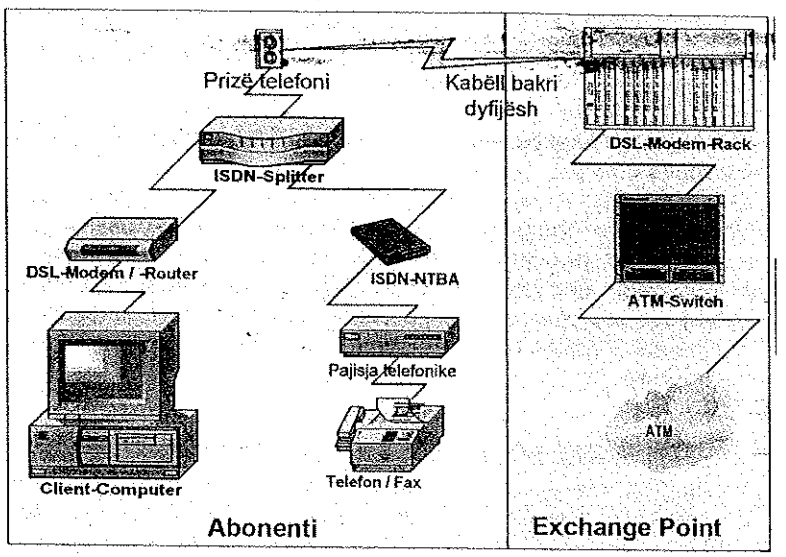
DSL-Hardware

Në vendshkëmbyesin e abonentit të linjës DSL, modem-at DSL dhe splitter-at POTS-/ISDN integrohen me anë të DSLAM-eve (DSL Access Multiplexer). Që këtej të dhënat, nëpërmjet një lidhje WAN (në shumicën e rasteve ATM) kalohen në një AC (Access Concentrator) dhe nga ky i fundit në POP-in (Point of Presence) e ISP-së (Internet Service Providers), pra të ofruesit të shërbimit të Internetit.

Sipas ofruesit të shërbimit ndryshojnë edhe pajisjet që duhen përdorur në anën e klientit (abonentit). Më poshtë jepet si shembull një lidhje ADSL nëpërmjet një linje telefonike, e cila shfrytëzohet njëkohësisht edhe nga ISDN-ja. Midis prizës së lidhjes së telefonit tek klienti dhe ISDN-NTBC-së lidhet një ISDN-Splitter. Lidhja kryhet nëpërmjet një kablli 4-fijesh (2 fije në përdorim –me koka RJ11). Për splitter-in nuk kërkohet furnizim me rrymë. Lidhja midis splitter-it ISDN dhe modem-it DSL kryhet nëpërmjet një kablli 2 fijësh me koka RJ45. Modem-i DSL furnizohet me rrymë nëpërmjet lidhjes me prizën e rrjetit elektrik dhe zakonisht ka një dalje për lidhje 10BaseT (sipas rastit edhe 100BaseT, ATM-25, USB ose IEEE1394 Firewire), e cila mundëson lidhjen me kompjuterin e klientit.

Në rast se dëshironi të lidhni klientë të tjerë tek lidhja DSL, atëhere duhet ose të shtohet një kartë rrjeti shtesë (NIC) në kompjuterin e lidhur me modem-in DSL dhe të konfiguroni shërbimet routing, ose proxy, ose përdorni një router DSL midis modem-it DSL dhe LAN-it. Router-at e rinj DSL pjesërisht kanë një modem DSL të integruar dhe në këtë mënyrë mund ta zëvendësojnë modem-in DSL.

Me emërtimin modem DSL jemi mësuar tashmë, por duke marrë parasysh transmetimet dixhitale që ai mundëson, ky emërtim rezulton i gabuar. Faktikisht, në këtë rast bëhet fjalë për një network-bridge (urë rrjeti) shumëprotokollëshe, e cila "përkthen" sinjalet e Ethernet-it, ose sinjalet seriale, në sinjale ATM. Termi Modem është futur nga kompanitë e telekomunikacionit, meqë ai ka hyrë tashmë për pajisjet WAN.

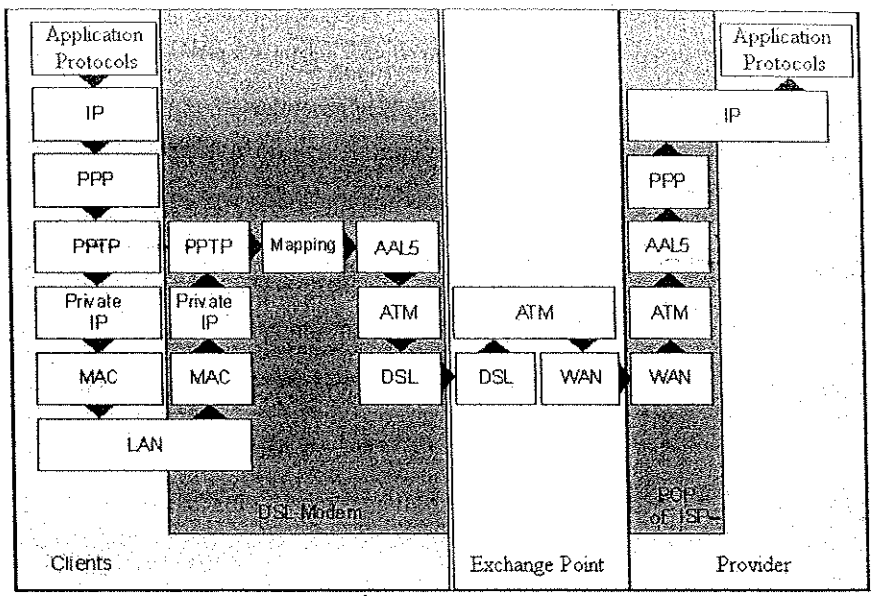


Përdorimi i hardware-ve për lidhjen DSL

Protokollet

Protokolli PPP përdoret midis klientit dhe ISP-së, me qëllim që të mundësohet konfigurimi i IP-së, autentifikimi i përdoruesve dhe ndërprerja e lidhjes me ISP-në. Prandaj, përdorimi i DSL-së është i ngjashëm me lidhjen klasike nëpërmjet modem-ave analogë, kështu që Internet Provider-at mund t'i përdorin edhe më pas lidhjet e tilla si p. sh. RRAS-in dhe RADIUS-in. Me qëllim që të mund të përdoren në LAN lidhjet PPP të klientëve është i nevojshëm një drajver për PPPoE (PPP over Ethernet) ose PPPoA (PPP over ATM).

Shënime



Bashkësia e protokolleve (protocol stack) midis klientit dhe serverit gjatë përdorimit të PPP-së dhe PPTP-së

Gjatë procesit të mapping-ut, në modem përfundon lidhja Point-to-Point-Tunneling dhe vazhdon më tej lidhja PPP në ATM nëpërmjet një qarku virtual (virtual circuit). Tek linjat fikse PPP-ja normalisht është e mbingarkuar dhe për këtë arsye më së shumti nuk përdoret. Në vend të protokollit IP mund të përdoren edhe protokollet NetBEUI ose IPX/SPX.

14.8 Zhvillime të reja

Pajisjet multifunksionale

Modem-at DSL i gjejmë edhe në formën e kartave PCI, aq të përdorshme në ndërtimin e PC-ve. Sipas rastit, në këto karta mund të gjejmë të integruar dhe një adaptor ISDN. Si zgjidhje të integruara ofrohen edhe pajisjet USB, të cilat i gjejmë të montuara brenda një kase: splitter, modem DSL dhe pajisje telefonike ISDN (tre linja analoge a/b, një ndërfaqe S_0, të konfigurueshme nga kompjuteri). Këto lidhen nëpërmjet portës USB me kompjuterin.

Disa routera DSL, me modem DSL të integruar, kanë si mundësi lidhje për ISDN. Në këtë mënyrë në LAN, nëpërmjet CAPI-t mund të ofrohen shërbime faksi ose dhe një lidhje automatike në Internet në rast të rënies së lidhjes DSL.

Shpesh ofrohen edhe routera DSL, të cilët formohen nga kombinimi i një ethernet-switch-i dhe një router-i me një ATM-Bridge. Shpesh në këto pajisje që quhen DSL-Router mund të gjejmë të përdorur një zgjidhje firewall-i të integruar.

Gjatë përdorimit të router-ave DSL duhet patur parasysh, që shumica e kontratave standarde (për individët privatë) nuk lejon përdorimin e lidhjes së Internetit më tej në një rrjet kompjuterash.

U-R2-Standardi i ndërfaqeve ADSL

Në vitin 2001 Telekomi Gjerman zhvilloi standardin e ri U-R2 për ndërfaqet ADSL. Në këtë standard janë saktësuar parametra të ndryshëm të standardeve të deritanishme ADSL, me qëllim që modem-at ADSL dhe DSLAM-et e prodhuesve të ndryshëm të jenë kompatibël me njëri-tjetrin. Teknologjitë e veçanta ADSL ndryshojnë kaq shumë, saqë pjesa më e madhe e modem-ave ADSL dhe Access-Multiplexer-ave funksionojnë me njëri-tjetrin vetëm kur janë prodhuar nga i njëjti prodhues.

U-R2, krahas DMT-së si procedurë modulimi dhe një frekuence ndarëse 130 kHz për splitter-in (ADSL over ISDN) standardizon edhe mbulimin me pin dhe formën e ndërtimit të kokave lidhëse të përdorura. Ecuria e procesit të handshakes gjatë krijimit të lidhjes, si dhe parametra të rëndësishëm të protokolleve të ATM-së gjithashtu specifikohen (formati i adresës së VCI-së dhe VPI-së, kontrolli i rrjedhës së të dhënave, etj.). Pajisjet që i korrespondojnë standardit U-R2 duhet të arrijnë, për një distancë minimumi 2800 m, një fluks bruto të dhënash prej minimumi 160 kBit/s upstream dhe 864 kBit/s downstream.

14.9 Mundësi të tjera lidhjesh

Rrjetet e televizioneve kabllore (Internet me cable modem)

Cable modem janë pajisje, të cilat transmetojnë të dhëna nëpërmjet rrjeteve të televizioneve kabllore. Cabel modem-i lidhet tek klientët me kabllin e televizorit, me rrjetin ose me portën USB të kompjuterit. Në këto lloj lidhjesh Cable Modem Termination System (CMTS) krijon lidhjen nga kablli i televizorit në Internet.

Aksesi në bandat me gjerësi të mëdha nëpërmjet televizioneve kabllore është shumë i përhapur në SH.B.A., Zvicër dhe Austri. Në R.F.GJ vetëm një pjesë e rrjeteve të televizioneve kabllore shfrytëzohen në të dyja drejtimet (bidirectional) dhe për më tepër, këto rrjete nuk janë të përshtatshme për transmetim të dhënash.

Shpejtësia e transmetimit varet shumë nga cilësia e kabllove të përdorur dhe numri i klientëve. Teorikisht, flukset e transmetimit mundësohen deri në 36 Mbit/s.

Rrjeti elektrik (Internet nga prizat elektrike)

Me Powerline Line Communication (PLC) përshkruhet mundësia e transmetimit të të dhënave nëpërmjet rrjetit elektrik.

Për shkak të problemeve nga interferencat e frekuencave dhe konkurencës së ashpër të ofruesve të shërbimit për akses në linjat e telefonit, në Gjermani, me përjashtime të rralla, të gjitha projektet janë pezulluar.

Si rrjet lokal, nën emërtimin PowerLAN, përdoret rrjet rrjeti elektrik, i cili si kabllo rrjeti përdor kabllot elektrike.

Satelitët (Internet nëpërmjet satelitit)

Për lidhjen në Internet nëpërmjet satelitit, për marrjen e të dhënave, përdoren satelitët gjeostacionarë (p.sh. ASTRA apo EUTELSAT). Këtu dallojmë llojet e mëposhtme të lidhjeve, që sigurojnë marrjen e sinjalit:

- ☑ Tek lidhjet satelitore dy-drejtimshe, sateliti përdoret shfrytëzohet në të dy drejtimet (down- dhe upstream). Flukset e transmetimit të ofruara janë midis 64 Kbit/s dhe 2048 Kbit/s.
- ☑ Tek lidhjet satelitore një-drejtimshe sateliti shfrytëzohet vetëm për shkarkime (downstream), pasi upstream-i kryhet nëpërmjet linjës telefonike. Flukset e transmetimit të ofruara janë midis 256 kbit/s dhe 2048 kbit/s.

Disavantazhe te lidhjes me satelit

- ☑ Shiu dhe mjegulla i krijojnë pengesa marrjes së sinjalit
- ☑ Shkëputje të gjata të sinjalit, deri në 0,24 sekonda, çojnë në uljen e shpejtësisë së transmetimit.
- ☑ Nevojitet një linjë telefonike për lidhjen satelitore të dyanshme (down- and upstream), e cila krijon kosto shtesë.

Shënime

15 Konfigurimi i Browser-it dhe një kontoje E-mail-i

Në këtë kapitull do të lexoni

→ Aksesimi i një adrese e-mail-i nëpërmjet Internetit
→ Krijimi i një kontoje e-mail-i në Outlook Express

Kusht paraprak

✓ Njohja e ndërfaqes së punës së Outlook Express-it

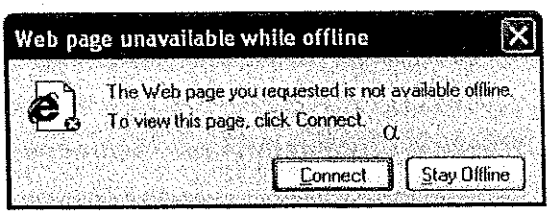
15.1 Krijimi i lidhjes në Internet

Puna me Internet në rrjetin e një firme

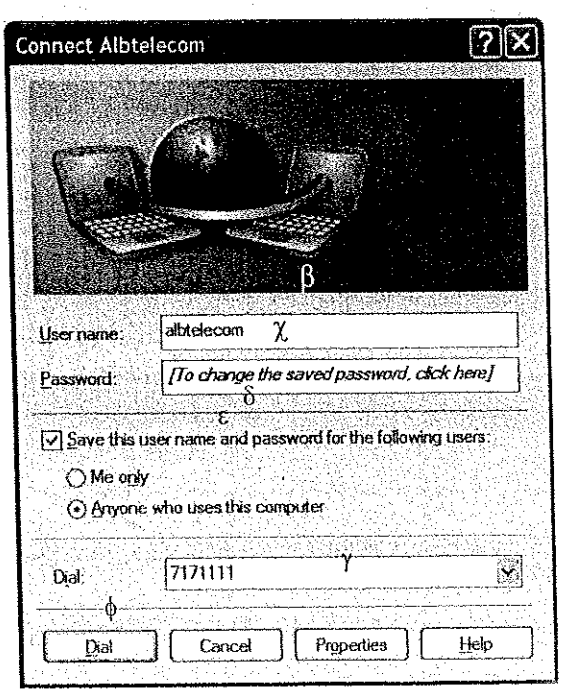
Në rast se punoni brenda rrjetit të një firme që ka akses të drejpërdrejtë në Internet , lidhjen dhe shkëputjen nga Interneti në këtë rast i rregullon një server rrjeti, gjë që do të thotë se pas startimit të Browser-it gjendeni automatikisht online.

Krijimi i një lidhje në Internet

Në qoftë se startoni Internet Explorer-in dhe ende nuk keni lidhje në Internet, automatikisht shfaqet dritarja dialoguese *Web page unavailable while offline*.

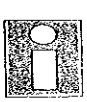


→ Klikoni mbi butonin Connect, α me qëllim që të aktivizohet dritarja dialoguese Dial-up connection.
→ Zgjidhni në listë lidhjen e krijuar β, me të cilën do të aksesoni Internetin.
→ Në fushën χ tregohet emri i përdoruesit (username) për lidhjen e zgjedhur.
→ Në rast se për lidhjen e zgjedhur e keni memorizuar fjalëkalimin ai do të tregohet i koduar.
→ Çaktivizoni fushëzën e kontrollit ε, në rast se nuk dëshironi të memorizoni fjalëkalimin.
→ Në këtë rast do t'ju duhet ta shkruani fjalëkalimin sa herë që do të provoni të lidheni.
→ Klikoni mbi butonin φ DIAL.



Kontrolli i të dhënave të lidhjes Dial-up

Pas klikimit mbi butonin DIAL për të bërë lidhjen, vijueshmëria e saj mund të ndiqet në dritaren dialoguese Dial-up Connection. Aty shikohet si krijohet lidhja me PoP-in e zgjedhur (Remote Computer). Në rreshtin e parë tregohet numri i PoP-it që thirret, nëpërmjet të cilit do të bëhet lidhja. Më pas tregohet procesi i lidhjes dhe kotrolli i emrit të përdoruesit dhe fjalëkalimit që janë dhënë për të bërë lidhjen Dial-up.

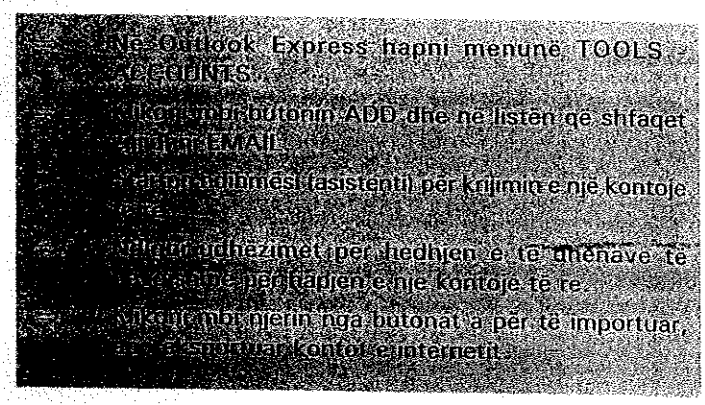


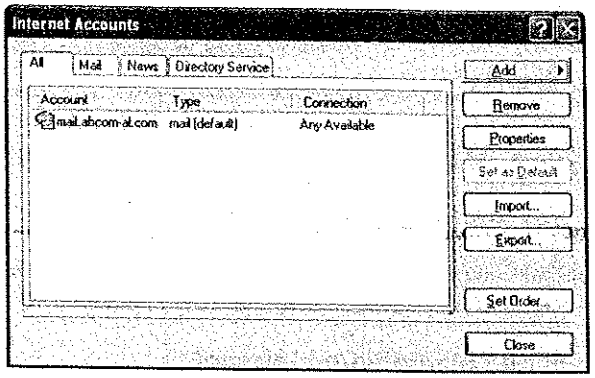
Në rast se nuk bëhet lidhja, apo të dhënat e emrit të përdoruesit ose fjalëkalimit janë gabim, atëhere shfaqet një dritare që njofton për gabimin.

15.2 Krijimi i një kontoje e-mail-i në Outlook Express

Krijimi i një kontoje e-mail-i

Në rast se keni një adresë e-maili me kontratë tek një provajder (ofrues shërbimi), prej tij do të merrni te dhënat për serverat që mundësojnë postën në hyrje dhe në dalje.(POP3 dhe SMTP). Ne rast se keni konto p.sh. ne www.gmail.com, atje mund të gjeni të dhënat e konfigurimit dhe emrat e serverave per POP3 dhe SMTP.

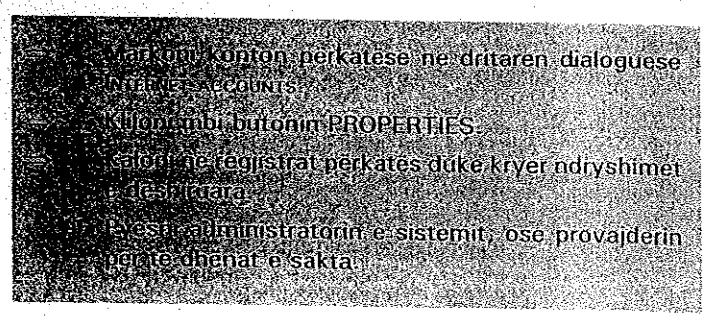


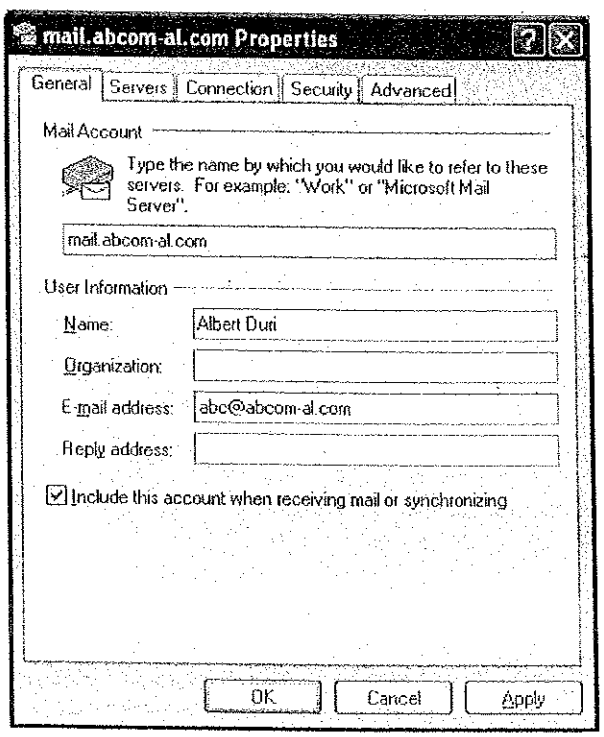


Hapja e kontove

Ndryshimi i karakteristikave të kontove

Karakteristikat e kontove të krijuara mund të ndryshohen me pas.





Ndryshimi i konfigurimit të nje kontoje e-mail-i

15.3 Konfigurimet për sigurinë gjatë shkëmbimit të e-mail-eve

Mbrojtja nga viruset

Në rast se një e-mail ka të bashkëngjitur një dokument dhe ky dokument hapet pa u kontrolluar më parë, ekziston rreziku i infektimit të kompjuterit nga viruset. "Viruse" është termi i përgjithshëm për programe, të cilat mund t'i shkaktojnë dëme kompjuterit.

Duhet kushtuar kujdes sidomos tek skedarët që u bashkëngjiten e-mail-eve (attachments), të cilat përmbajnë programe të ekzekutueshme, p.sh. Skedarët me prapashtesën **.exe*, **.bat* dhe **.com*, tek screensaver-at, p.sh.. **.scr*, dhe tek skriptet si **.vbs*.

Skedarë të krijuar me programet e Microsoft Office, p.sh. *.doc, *.xls ose *.ppt, mund të përmbajnë të ashtuquajturat viruse makrosh. Gjatë hapjes së një dokumenti ato ngarkohen automatikisht dhe mund të shkaktojnë fshirjen, apo dëmtimin e dokumentave ne diskun e ngurtë.

Ekzistojnë programe speciale antivirusi, me ndihmën e të cilave kontrollohet nëse një skedar përmban apo jo virus. Programet e antiviusit mund të gjenden p.sh. në Internet, në disa raste edhe pa pagesë.

- ☑ E-Mail-et që vijnë nga dërgues të panjohur duhen fshirë **pa i hapur.**
- ☑ Në fillim memorizoni në kòmpjuter skedarët bashkëngjitur e-mail-it, dhe kontrolloni për ç'lloj skedari bëhet fjalë. Për të parë prapashtesën e emrit të skedarit, në Windows-Explorer duhet të hapni menunë TOOLS – FOLDER OPTIONS, në regjistrin View hiqeni gremçin nga kutiza me opsionin HIDE EXTENTIONS FOR KNOWN FILE TYPES dhe vendoseni tek opsioni SHOW ALL FILES AND FOLDERS .
- ☑ Instaloni një program antivirusi aktual dhe mos harroni ta përditësoni, me qëllim që të jeni të mbrojtur edhe nga viruset më të reja. Kontrolloni për viruse, me ndihmën e programit të antivirusit, skedarin bashkëngjitur e-mail-it **përpara se ta hapni.**

Edhe nëse programi i antivirusit është instaluar dhe përditësuar, edhe nëse janë aktivizuar elementët e sigurisë në Browsera, përsëri nuk jeni 100% i sigurt. Ndërmjet kohës kur shfaqen viruse të reja dhe mbrojtjes ndaj tyre me programet përkatëse, kalon një kohë e caktuar.

- ☑ Në përgjithësi ju dërgoni dhe hapni skedarë që nuk përmbajnë viruse. Ju mund të krijoni dhe dërgoni skedarë pdf ose RTF në vend të skedarëve të Microsoft-Office(*.doc* ose *.xls*). Skedarët PDF i krijoni p.sh. me programin freeware Ghostscript dhe i hapni për t'i parë me Adobe Reader.
- ☑ Gjatë dërgimit të skedarve të krijuar nga programet e Microsoft Office, duhet të merrni parasysh që programet e nevojshme për hapjen dhe leximin e tyre mund të mos jenë të instaluara.

Shënime

Siguria e fjelëkalimeve

Gjatë punës në Internet shpesh del i nevojshëm përdorimi i një fjalëkalimi. Shpesh fjalëkalimi përdoret kur p.sh. tërhiqni nga mailserver-i e-mailet e ardhura ne kutinë tuaj postare (mailbox) . Gjatë zgjedhjes së fjalëkalimit duhen ndjekur udhëzimet e mëposhtme, me qëllim që fjalëkalimi të mos zbulohet, apo hamendësohet lehtë nga persona të tjerë:

- ☑ Mos zgjidhni asnjëherë një fjalëkalim që përmban elementë të të dhënave tuaja personale si emri, mbiemri, ditëlindja, apo numri i telefonit.
- ☑ Mos përdorni fjalë të thjeshta, ose numra apo gërma të njëpasnjëshme.si ABCD, ... apo 1234 ...
- ☑ Fjalëkalimi duhet të përmbajë të paktën gjashtë gërma, mundësisht kombinim me numra, ose karaktere të veçanta.

15.4 Browser-i

Browsera të ndryshëm

Internet Explorer është një paketë komunikimi për Internet. Pas instalimit të plotë, paketa ndër të tjera, përmban modulin e programit **Internet Explorer** (Browser/WWW-Client), **Outlook Express** (E-Mail- dhe News-Client), **Windows Media Player** (për luajtjen e skedarëve Audio- dhe Video-) dhe **Net-Meeting** (komunikim në kohë reale).

Paketat e programeve të Browserave të mëposhtëm (që ofrohen pa pagesë) mund të shkarkohen nga faqet e Internetit të projekteve të ndryshme dhe më pas të instalohen.

Browser	
Internet Explorer	Internet Explorer (Browser-i) mundëson aksesin në të gjitha informacionet e vlefshme në Internet, ose në rrjetet e brendshme të firmave Intranet. Exploreri shërben p.sh. për paraqitjen e faqeve të Internetit me grafikë dhe animacione, për luajtjen e skedarëve audio dhe video si dhe për „lundrim" (navigim) në Internet.
Firefox	Falë lehtësisë së veprimit me regjistrat (Tabs) e Browser-it, karakteristikave të shumta të sigurisë dhe mundësisë së personalizimit gjatë instalimit të zgjerimit të funksionaliteteve (add-ons-ve), Firefox-i po bëhet gjithmonë e më i preferueshëm. Firefox, pas Internet Explorer-it është Browser-i më i përdorur. Ai është i vlefshëm edhe për sistemet operative Linx dhe Mac.*http://www.mozilla-europe.org/en/*
Opera	Një tjetër alternativë është Browser-i Opera: një Browser i lehtë dhe fleksibel për sistemin me klient e-mail-i i vlefshem për sistemet operative Windows, Linux, Mac ose OS/2.*http://www.opera.com/*
Mozilla Suite **SeaMonkey**	Mozilla Suite përmban një Browser, nje e-mail, newsgroup-client, dhe një editor HTML. Mozilla u zhvillua nga kodi publik i programit te Netscape dhe në fund të vitit 2005 u shfaq me versionin 1.7.12. të projekteve të veçanta Firefox (Browser) dhe Thunderbird (E-Mail). Pasuesi i Mozilla Suite doli me paketën e Internetit SeaMonkey http://www.mozilla.org/projects/seamonkey/
Netscape	Browser-i përmban programin e e-mail-it Netscape Mail, forume diskutimi dhe HTML-Editor Netscape Composer-in.*http://www.netscape.com*, Hyperlink Browser – Get Navigator

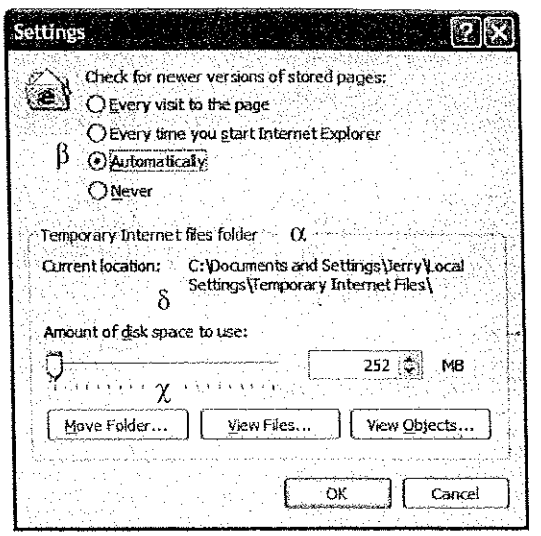
Në CD-të e revistave të kompjuterave shpesh gjenden versionet aktuale të Browserave pa pagesë. Në këtë mënyrë kurseni kohën që do të nevojitej për shkarkimin e tyre nga Interneti.

15.5 Përshtatja e konfigurimit të Internet Explorer-it

Fusha TEMPORARY INTERNET FILES

Dosja (folderi) *Temporary Internet Files* α përdoret nga Browser-i si memorje ndërmjetëse (Cache), me qëllim që faqet e vizituara më parë t'i memorizojë për t'i ngarkuar sipas nevojës direkt nga Cache-ja.

→ Hapni menunë TOOLS – INTERNET OPTIONS.
→ Klikoni mbi butonin " SETTINGS në fushën TEMPORARY INTERNET FILES.
→ Në zonën β të dritares dialoguese SETTINGS caktohet, duke klikuar dhe ngjedhur opsionin përkatës, se kur duhet të ngarkohet nga Interneti versioni i aktualizuar i një website të vizituar më parë, respektivisht kur një version i meparshëm duhet të ngarkohet nga cache –ja.



Konfigurimet për temporary Internet files

Standard është e aktivizuar fusha opsionale AUTOMATICALLY. Në rast se brenda një sesioni në Internet vizitohet sërish një website i vizituar më parë, ky website ngarkohet nga cache-ja. Versionin më të fundit mund ta ngarkoni nga Interneti duke klikuar mbi simbolin [?] Në një sesion të ri lidhje me Internetin do të ngarkohet website-i më aktual i vizituar herën e fundit.

→ Në fushën TEMPORARY INTERNET FILES FOLDERS te dritares dialoguese SETTINGS mund te konfigurohen c hapësira e lejuar e diskut ose vendi i memorizimit d të folderit *Temporary Internet Files*.
→ Klikoni mbi butonin VIEW FILES, me qëllim që të shikoni përmbajtjen e folderit *Temporary Inter-net Files*.
→ Klikoni mbi butonin VIEW OBJECTS, në rast se deshironi të shikoni përmbajtjen e folderit *Doën-loaded Program Files*, i cili përmban skedarët e shkarkuar nga Interneti.
→ Në rast se deshironi ta fshini përmbajtjen e *Temporary Internet Files*, klikoni mbi butonin DELETE FILES në dritaren dialoguese INTERNET OPTIONS.

Fusha HISTORY

Të gjitha adresat, qe zgjidhni për t'i vizituar gjatë punës në Internet, memorizohen në dosjen History.

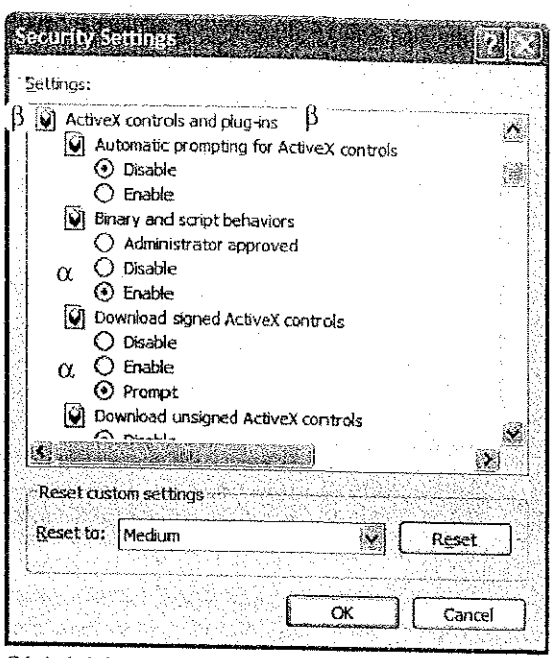
→ Caktoni tek HISTORY numrin e ditëve, brenda të cilave do të ruhen të memorizuara faqet e zgjedhura.
→ Në rast se deshironi ta boshatisni folderin, klikoni mbi butonin "Clear HISTORY".

URL-të e shkruara gabim ruhen në dosjen (folder-in) History.

Ç'aktivizimi i ActiveX-controls

ActiveX controls lejojnë integrimin e drejtpërdrejtë të përmbajtjeve të produkteve të Microsoft-it në Internet Explorer, respektivisht ekzekutimin e disa funksioneve të caktuara të Internetit (p. sh. Përditësimi automatik i Windows XP-së). Përveç kësaj, mund të kryeni çdo veprim mbi kompjuterin tuaj (p.sh. instalimi pa u vënë re i Dialer-it).

⇒ Aktivizoni regjistrin SECURITY në dritaren dialoguese INTERNET OPTIONS.
⇒ Zgjidhni ikonën INTERNET ( ).
⇒ Në zonën SECURITY LEVEL FOR THIS ZONE klikoni mbi butonin CUSTOM LEVEL...
⇒ Aktivizoni Sie fushen e opsioneve α.
⇒ Lëvizni rreshqitësin e dritares lart, dhe aktivizoni dy fusha opsionale në opsionin DISABLE. Këto fusha opsionale i përkasin zonës β ACTIVEX CONTROLS AND PLUG-INS.
⇒ Konfirmoni me OK.



Ç'aktivizimi i ActiveX

Websitet, të cilat përmbajnë elemente Acti-veX, nuk paraqiten siç duhet në qoftë se fushat opsionale përkatëse janë ç'aktivizuar.

Administrimi i Cookies

Çfarë janë Cookies?

Cookies janë skedarë, në të cilat Browser-i në diskun e ngurtë, memorizon të dhënat dhe konfigurimin e përdoruesit për llogari të webserverit që hoston website-t e vizituara. Kur i kthehemi sërish një website-i të vizituar, këto të dhëna nga Browser-i transferohen dhe vlerësohen në webserver. Këta skedarë do të ndihmojnë në sesionet e mëpasme, me qëllim që t'i "shërbehen" individualisht përdoruesit. Sigurisht, gjatë përdorimit, këtu memorizohen edhe të dhëna personale, të cilat mund t'u „vihen në dispozicion" edhe personave të panjohur.

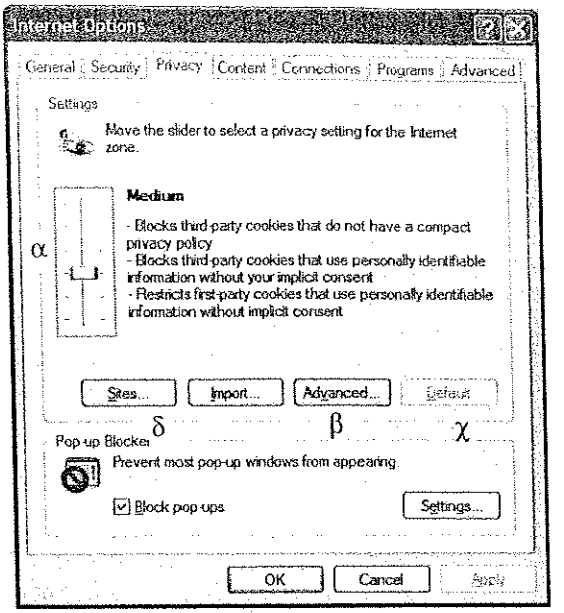
Cookies ruhen si skedarë Text në folderin e sistemit *C:\Dokuments and Settings\Username\Cookies*, dhe për këtë arsye nuk mund të transmetojnë viruse.

Ndryshimi i konfigurimit për Cookies me qëllim mbrojtjen e të dhënave

Në dritaren dialoguese INTERNET OPTIONS, në regjistrin PRIVACY, me ndihmën e një rregulluesi me rrëshqitës, mund të caktoni si duhen trajtuar cookies-et. Rrëshqitësi që lejon rregullimin e konfigurimit të zonave të Internetit në gjashtë nivele të ndryshme. Zona e Internetit përfshin të gjitha websitet, të cilat nuk gjenden lokalisht në kompjuter, ose në int-ra-net, si dhe nuk i përkasin një zone speciale.

Në rast se dëshironi të ndaloni memorizimin dhe leximin në kompjuter të të gjitha cookies zgjidhni konfigurimin BLOCK ALL COOKIES. Më tej ekzistojnë opsionet HIGH, MIDDLE HIGH, MIDDLE (konfigurimi standard), Low deri ACCEPT ALL COOKIES, në rast se cookies do të lejohet të memorizohen në kompjuter dhe të mund të lexohen sërish nga websitet që i kanë krijuar.

→ Hapni menunë TOOLS - IN-TER-NET- OPTIONS, dhe aktivizoni regjistrin PRIVACY.
→ Zgjidhni me anë të rreshqitësit a rregullues konfigurimin e deshiruar.
→ Klikoni mbi butonin Advanced β, për ta detajuar konfigurimin e trajtimit të cookies, p.sh. për të marrë të dhëna për Cookies.
→ Në qoftë se rreshqitësi rregullues α nuk tregon konfigurimin MIDDLE, mund të klikoni mbi butonin DEFAULT γ për të rikthyer vlerat e paravendosura.
→ Klikoni mbi butonin SITES δ, me qëllim që të përcaktoni trajtimin e cookies për website të veçanta.



Zgjedhja e konfigurimit për Cookie-s

Fshirja e Cookies

Të gjitha cookies të memorizuara në kompjuter mund të fshihen.

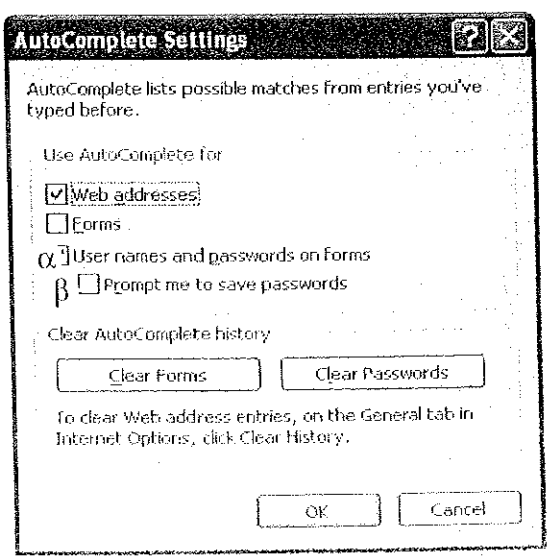
→ Hapni menunë TOOLS - IN-TER-NET- OPTIONS, dhe aktivizoni regjistrin GENERAL.
→ Klikoni në zonën TEMPORARY INTER-NET FILES mbi butonin DELETE COOKIES, dhe konfirmoni me OK PYETJEN E SIGURISE.

Përpara se të kryeni konfigurimet për trajtimin e cookies, duhet të fshini të gjitha cookies-et e memorizuara me parë, me qëllim që ndryshimet për trajtimin e cookies të mos ndikojnë tek cookies e memorizuara më parë.

Konfigurimi i opsionit AutoComplete

Ky funksion ju mundëson të memorizoni të dhënat tuaja personale dhe sipas nevojës t'i jepni më tej në website dhe në formularë. Gjatë plotësimit të formularëve funksioni AutoComplete identifikon ngjashmëritë me të dhënat tuaja dhe sugjeron vetëplotësimin, të cilin ju duhet ta miratoni, gjatë hedhjes së të dhënave nga ju.

→ Hapni menunë TOOLS - INTER-NE-T -OP-TIO-NS, dhe aktivizoni regjistrin CONTENT.
→ Klikoni mbi butonin AUTOCOMPLETE.
→ Në zonën USE AUTOCOMPLETE FOR ç'aktivizoni fushat e kontrollit, tek të cilat opsioni AUTOCOMPLETE nuk duhet të jetë i aktivizuar.
→ Klikoni mbi butonin CLEAR FORMS, me qëllim që të gjithë formularët që keni plotësuar, t'i fshini nga dosja History.
→ Klikoni mbi butonin CLEAR PASSWORD, me qëllim që të fshihen fjalëkalimet në të gjitha skedarët që ndodhen në dosjen History.



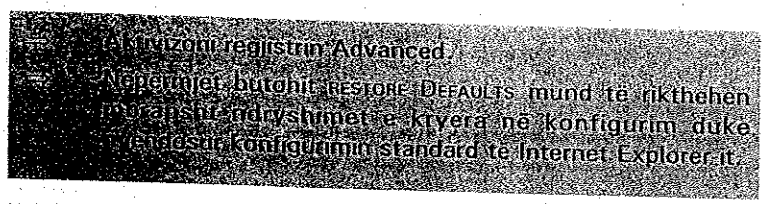
Përcaktimi i konfigurimit të AutoComplete

☑ Me qëllim që asnjë person i paautorizuar te mos ketë mundesi të lexojë fjalëkalimet tuaja, rekomandohet të ç'aktivizohet fusha e kontrollit α. Në këtë mënyrë pengoni që fjalëkalimet të memorizohen automatikisht në kompjuterin tuaj.

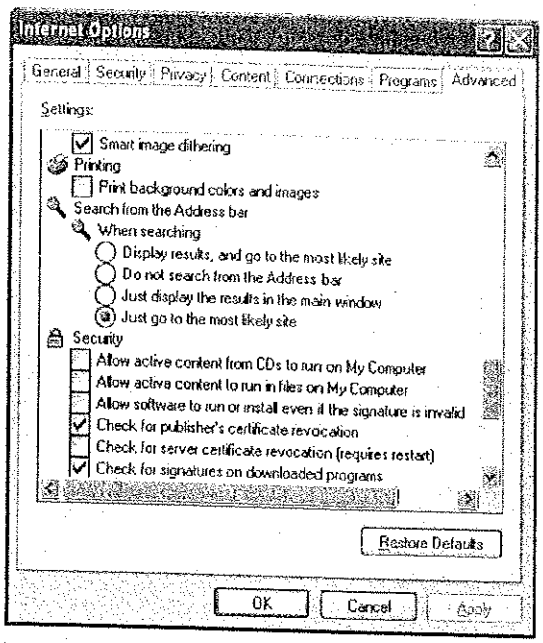
☑ Në rast se dëshironi të memorizoni fjalëkalime në formularë, sigurohuni që fusha e kontrollit β të jetë e aktivizuar

Advanced settings (konfigurim i avancuar)

Në Internet Explorer ekziston mundësia të kryhen konfigurime, të cilat kanë të bëjnë p.sh. me tregimin e websiteve, apo paraqitjen e dritareve të Internet Explorer-it. Opsionet e konfigurimit janë përmbledhur në regjistrin Advanced.



Konfigurimet e elementëve të veçantë mund t'i kryeni në listën e mëposhtme:



Konfigurim i avancuar i opsioneve të Internet-it

☑ **Browsing**

Këtu mund të caktoket p.sh, nëse duhet të informoheni ose nëse kur filloni të shkruani një URL, ajo te plotësohet automatikisht apo jo.

☑ **Printing**

Këtu caktohet nëse do të printohen apo jo sfondet me ngjyra, apo grafikët e paraqitura ne faqet e Internetit. Kur opsioni është i aktivizuar ulet ndjeshëm shpejtësia dhe lexueshmëria e printimit.

☑ **Accessibility**

Me këtë opsion mund të rregulloni p.sh. që të shfaqet tekst në vend të figurave në rast se fusha e kontrollit SHOW PICTURES në fushën MULTIMEDIA është e ç'aktivizuar.

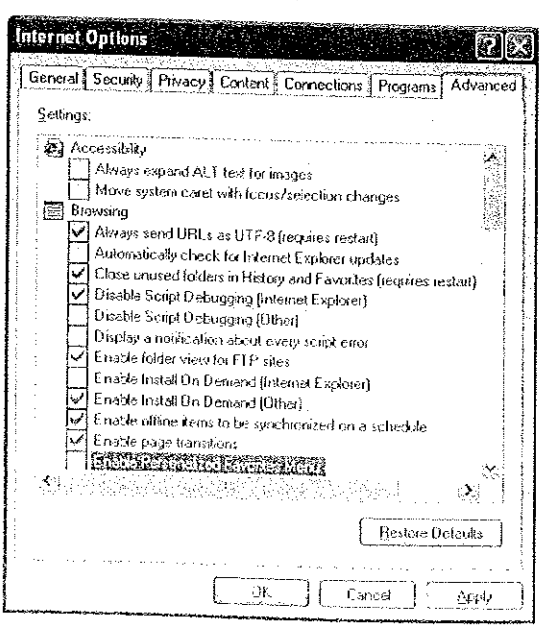
☑ **Konfigurimi për HTTP 1.1**

HTTP 1.1 është vrsioni i ri i versionit mjaft të përhapur të potokollit HTTP 1.0 (Protokoll për transferimin e të dhënave në WWW). Në rast se mund të përdorni versionin e ri (Version 1.1), konsultohuni me administratorin e sistemit.

☑ **Microsoft VM**

Ketu aktivizohet Java-Compiler-i i brendshëm i Internet Explo-rer-it, me qëllim që programet Java të mund të startohen direkt nga Browser-i, pavarësisht se cili sistem operativ përdoret.

Protokollimi Java vendos një protokoll për çdo program Java të ekzekutuar. Programistët e gjuhes Java mund të aktivizojnë konsolën Java si mjedis të veçantë për të kyer testet e tyre.



☑ **Multimedia**

Këtu caktohet se cilat funksione multimediale duhet të ekzekutojë Internet Explorer-i

☑ **Security**

Këtu caktohet konfigurimi i aspekteve të sigurisë, me qëllim që gjatë veprimeve kritike të shfaqen në ekran informacione parlajmëruese.

☑ Kërkoni në listën e adresave

☑ Këtu konfigurohen opsionet e kërkimit dhe paraqitjes.

Shënime

16 Siguria në LAN dhe WLAN

Në këtë kapitull do të lexoni:

- → Çfarë kuptohet me siguri të dhënash
- → Çfarë standardesh ekzistojnë në fushën e sigurimit të të dhënave
- → Çfarë është një Firewall (mur zjarri)
- → Ku mund të përdoret Firewall-i

Kushte paraprake:

- ✓ Njohuri mbi protokollet e rrjetit
- ✓ Njohuri mbi protokollin e Internet-it
- ✓ Njohuri mbi portat

16.1 Ç'kuptohet me siguri të dhënash?

Kërkesat bazë të sigurisë

Termi "siguri" në jetën e përditshme, ashtu si edhe në teknologjinë e informacionit, mund të ketë kuptime të ndryshme. Për ta përkufizuar më qartë, si dallohet një gjendje e sigurtë nga një e pasigurtë, egzistojnë disa kërkesa bazë (ose objektiva sigurie) të paraqitura më poshtë:

- ☑ Besueshmëria
- ☑ Integriteti (tërësia)
- ☑ Disponibiliteti

Informacione të shumëllojshme në lidhje me temën e sigurisë së të dhënave ofron në faqen e saj të internetit *www.bsi.de*, Zyra Federale për Sigurinë në fushën e Teknologjisë së Informacionit të RFGJ-së.

Besueshmëria

Me termin besueshmëri (angl. confidentiality) kuptohet, që informacionet do t'u arrijnë atyre të cilëve u lejohet t'i zotërojnë. Në lidhje me komunikimin në rrjet besueshmëria është e ngjashme me fshehtësinë e letrës. Në qoftë se dërgoni një e-mail tek një marrës i caktuar, ju prisni që vetëm ky i fundit ta lexojë përmbajtjen e tij.

Besueshmëria

Objektivi i besueshmërisë nuk kufizohet vetëm tek e-mail-et. Çdo informacion i memorizuar në një sistem kompjuterik shërben për një qëllim të caktuar dhe në shumicën e rasteve nuk është e nevojshme, apo e dëshirueshme që këto informacione të jenë të aksesueshme publikisht.

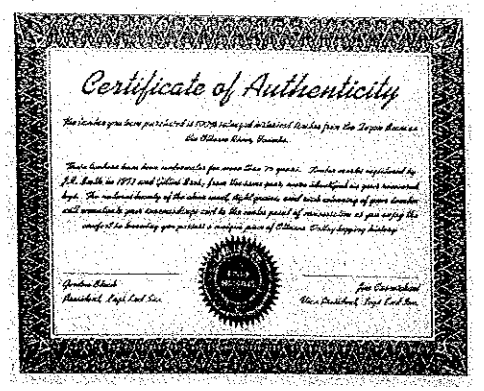
Në jetën e përditshme masat mbrojtëse në lidhje me besueshmërinë kanë të bëjnë p.sh. me një zarf në të cilin futet një mesazh i shkruar që nuk është për t'u publikuar, apo me një derë të mbyllur, e cila u lejon hyrjen vetëm personave që kanë çelsin e duhur.

Me qëllim që të garantohet besueshmëria duhen zbatuar masa të ndryshme: për shembull kodimi i të dhënave, ose mesazheve midis partnerëve në komunikim, apo një kontroll në hyrje, i cili i lejon vetëm personave të caktuar që të mund të shohim të dhënat e mbrojtura.

Integriteti (përfshirë autenticitetin)

Nëse do të punohet me të dhëna, duhet një sistem i sigurt që të mund të garantojë, që të dhënat të jenë të sakta (engl. integrity). Këtu vlen gjithashtu që të gjenden mundësi, nëpërmjet të cilave të pengohen gabimet gjatë transmetimit të të dhënave, ose të paktën të identifikohen dhe të mund të korrigjohen ato. Duhet mundësuar, që të dhënat, dokumentat dhe sistemet të mbrohen ndaj manipulimeve.

Kur bëhet e mundur të garantohet, apo të konfirmohet integriteti i të dhënave, si dhe të bashkangjitet një informacion mbi krijuesin, apo autorin e të dhënave, atëherë krijohet një i ashtuquajtur **Autenticitet** (engl. Authenti-city) i të dhënave respektive – me fjalë të tjera një nënshkrim dixhital.



Një certifikatë autenticiteti (në kohë reale)

Autenticiteti gjithashtu paraqet në një farë mënyre, një pamje të detajuar të integritetit si objektiv sigurie. Në diskutimin aktual politik në lidhje me nënshkrimet dixhitale pas një shqyrtimi më të saktë dallohet një nivel i mëtejshëm autentifikimi:

Një e-mail, i cili përmban një porosi, nuk përbën provë për gjykatën pa prova të tjera: Përmbajtja p.sh., mund të ketë qenë e manipuluar, ose dërguesi i e-mailit është falsifikuar dhe porositësi i supozuar nuk di asgjë për "porosinë" e tij.

Edhe në qoftë se do të merreshin si të mirëqëna, metodat për garantimin e integritetit të përmbajtjes (pa mundësi manipulimi) dhe autentifikimit (origjina e mail-it është vërtet nga dërguesi i përmendur), në aspektin juridik këto nuk mjaftojnë, si shprehje e vlefshme e vullnetit për mbylljen e një kontrate blerje. Do të ishte relativisht e lehtë, që të gjendej një argument, se përse ky e-mail nuk mund të ishte shprehje e vlefshme e vullnetit të dikujt.

Me vënien e nënshkrimit mbi një dokument ju provoni që jeni dakort me përmbajtjen e tekstit dhe pranoni pasojat që rrjedhin nga kjo. Meqë nënshkrimi vendoset direkt në të njëjtin dokument me tekstin (dhe është relativisht e vështirë të ndahet) kjo bën që në këtë mënyrë të garantohet lidhshmëria. Për shkak të natyrës së sistemeve të informacionit kjo mosndashmëri e përmbajtjes nga nënshkrimi nuk është kaq e thjeshtë për t'u realizuar.

Si një kërkesë paraprake, autenticiteti zgjerohet duke i dhënë kuptim një nënshkrimi dixhital, gjithashtu mund të përcaktohet lidhshmëria e detyrueshme (ose e pakundërshtueshme) e një nënshkrimi dixhital.

Në rast se në një sistem sigurohet komunikimi me lidhshmëri të detyrueshme, atëhere asnjë pjesëmarrës në komunikim nuk mund të pretendojë më vonë se komunikimi nuk ka ndodhur, apo se ka ndodhur, por me përmbajtje tjetër.

Disponibiliteti

Objektivi i tretë kryesor për sigurinë e të dhënave është disponibiliteti (engl. Availability). Një sistem i sigurtë duhet të mund të garantojë, që të dhënat, të cilat ai përpunon, të jenë të aksesueshme, dmth. që shërbimet që ofrohen të mund të shfrytëzohen vërtet.

Si rregull, disponibiliteti përfshin gjithashtu masat mbrojtëse logjike (p.sh. masa ndaj fshirjes gabimisht të të dhënave), po ashtu si masat e përshtatshme, të cilat parandalojnë pezullimin e punës si pasojë e defekteve të hard-apo softwareve. Këtu futen ndër të tjera krijimi rregullisht i kopjeve rezervë të të dhënave – backup (shih Kapitullin 13 dhe 14), të cilat mundësojnë rikthimin e shpejtë të të dhënave në gjendjen e mëparshme në rast defekti. Edhe ndikimet nga jashtë, si p.sh. ndërprerjet e energjisë elektrike, ose manipulime të qëllimshme nga sabotatorë me qëllim bllokimin e shërbimeve të sistemit për përdoruesit e autorizuar, janë probleme të cilat përfshihen në konceptin e disponibilitetit.

Veçanërisht për fushat e përdorimit, në të cilat disponibiliteti i shërbimit duhet të jetë i garantuar 24 orë, ekzistojnë zgjidhje të përshtatshme që mundësojnë disponibilitetin në nivele të tilla të larta, të cilat nëpërmjet pajisjeve speciale hardware dhe algoritmeve të përshtatshme në software, arrijnë maksimumin e mundshëm të besueshmërisë (reliability), pra të shmangies së rënies së sistemit.

Shembuj për këtë janë:

- ☑ Vendosja e serverave në ambjente të mbrojtjura nga zjarri dhe nga uji.
- ☑ Bllloqe ushqimi sekodare rezervë tek serverat
- ☑ Lidhje e dyfishtë (redundant) për komunikimin e të dhënave

nyrë të veçantë, gjatë përpunimit të të dhënave në ndërmarrje, si dhe gjatë sigurimit të sistemeve kompjuterike përcaktohet, nëpërmjet **aftësisë për revizionim**, një objektiv i mëtejshëm i sigurisë në fushën e TI-së. Në rast se ky objektiv përmbushet, atëherë të gjitha proceset dhe hapat e punës në një sistem protokollohen në mënyrë të tillë (e siguruar ndaj manipulimit), që në çdo kohë të mund të provohet, kush, kur dhe me cilat të dhëna ka punuar dhe në rast nevoje edhe se kush ka fshirë apo ndryshuar diçka.

16.2 Standardet në fushën e sigurisë së të dhënave

Siguria e të dhënave në fushën e TI-së - Kriteret

Kostoja për sigurinë e burimeve të TI-së (IT ressources) në një ndërmarrje mund të jetë disa herë shumë e lartë, pasi në mënyrë tradicionale duhet që të kryhet paraprakisht një analizë e objekteve ekzistuese që duhen mbrojtur (assets), pasuar nga një analizë e rreziqeve dhe kërcënimeve. Më pas zgjidhen masat e sigurisë, të cilat do të konsiderohen të nevojshme për mbrojtjen e aseteve përkatëse.

Me qëllim që të zvogëlohen koha dhe kostot e punës për sigurinë, dhe që të mund të krahasohen më mirë përpjekjet për rritjen e sigurisë, në praktikë përdoren shpesh katalogje me kritere, të cilat ndihmojnë në punën e tyre personat përgjegjës për sigurinë.

Kriteret e ndryshme kanë interpretime të ndryshme referuar zbatimit, metodave të përdorura dhe marrjes në konsideratë të problemeve. Me qëllim që të mund të vendosni, se cilat janë kriteret ideale për të përmbushur detyrat tuaja, më poshtë është dhënë një pamje e përgjithshme në lidhje me kriteret më të rëndësishme.

Manuali bazë i mbrojtjes në fushën e TI-së	ISO 17799
Taskforce Secure Internet	ITSEC/Common Criteria
ISO TR 13335	ISO 9000
FIPS 140	

Edhe ndërmarrjet e vogla, për arsye ligjore edhe të garantimit të funksionalitetit të tyre, duhet të marrin masa të sigurisë teknike. Megjithëse kriteret e listuara më lart janë krijuar për ndërmarrjet e mëdha, ato japin këshilla me vlerë edhe për firmat e vogla përsa i përket garantimit të sigurisë së të dhënave.

Manuali bazë i mbrojtjes në fushën e TI-së

Manuali bazë i mbrojtjes në fushën e TI-së ka si qëllim, që nëpërmjet masave teknike, organizative, infrastrukturore dhe atyre që kanë të bëjnë me personelin, të krijojnë një nivel sigurie standard, i cili të mund të zhvillohej më tej edhe për fusha me pretendime më të larta sigurie.

Manuali bazë i mbrojtjes i vënë në dispozicion nga BSI (Bundesamt für Sicherheit in der Informationstechnik - Zyra Federale për Sigurinë në Fushën e Teknologjisë së Informacionit-RFGJ) në pjesën kryesore përbëhet nga tri kapituj:

Përbërësit	☑ Përshkruhen komponentë të organizimit dhe të infrastrukturës së përpunimit elektronik të të dhënave (PED) ☑ Referenca ndaj gjendjes së rreziqeve të mundshme dhe kundërmasat e rekomanduara
Katalogu i rreziqeve	Përmbahen përshkrime të hollësishme të të gjitha rreziqeve që kërcënojnë sigurinë
Katalogu i masave	Përmbahen përshkrime të hollësishme të të gjitha masave të marra për sigurinë

I plotë ky manual paraqitet në formën elektronike të tij në CD, apo në faqen e Internetit të BSI-së. Tematikat në manualin e masave mbrojtëse janë në formë hyperlink-esh, kështu që tek ato mund të kalohet direkt duke klikuar mbi hyperlinkun përkatës.

Ky ndërtim ju mundëson të kaloni happashapi, përmes komponentëve të TI-së të firmës tuaj, të cilën dëshironi ta bëni më të sigurt, pa qenë nevoja të humbni kohë e të kërkoni kërkoni për të gjitha informacionet përkatëse.

Manuali i mbrojtjes bazë në fushën e TI-së gjendet në website-n *www.bsi.de* dhe që atje mund të shkarkohet, ose të porositet pa pagesë në versionin në CD-ROM, apo me pagesë në formë manuali.

Taskforca për një Internet të sigurtë

Taskforcës i është dhënë detyrë të vlerësojë informacionet në lidhje me llojin dhe shkallën e kërcënimit të sigurisë në fushën e TI-së. Ajo përgatit manuale me kundërmasat e nevojshme. Rekomandimet e dhëna nuk janë të detyrueshme, por ato këshillojnë, se më cilat mjete mund të minimizohen apo shmangen rreziqet dhe dobësitë e sistemit.

ISO TR 13335

ISO TR 13335 përbëhet nga pesë raporte teknike. Këto japin këshilla në lidhje me menaxhimin e sigurisë së TI-së, pa detyruar një zgjidhje të caktuar. Raportet përfshijnë tematikën në fushat e mëposhtme:

Pjesa 1: Koncepte dhe modele të sigurisë në TI	☑ Termat bazë të sigurisë në TI ☑ Kërcënimet, rreziqet, pikat e dobta ☑ Planifikimi i rreziqeve, analiza e risqeve, sensibilizimi
Pjesa 2: Menaxhimi dhe planifikimi i sigurisë së TI-së	☑ Strukturimi i proceseve të sigurisë TI ☑ Integrimi në proceset ekzistuese të ndërmarrjes ☑ Organizatat e sigurisë-TI
Pjesa 3: Teknikat për menaxhimin e sigurisë së TI-së	☑ Përmirësimi i proceseve të sigurisë ☑ Metodat dhe teknikat për proceset e sigurisë
Pjesa 4: Zgjedhja e masave të sigurisë	☑ Masat e sigurisë ndaj kërcënimeve
Pjesa 5: Udhëzues për menaxhimin e sigurisë në rrjet	☑ Siguria në komunikim ☑ Llojet e rrjeteve dhe organizimet ☑ Vazhdimësia e biznesit (Business Continuity)

FIPS 140-1/2

Publikimi amerikan i NIST (National Institute of Standards and Technology) "Federal In-for-mation Proces-sing Standard 140" përblidhet në Versionin 1 dhe në atë që doli më pas, Versionin 2. dhe merret me kontrollin dhe vlerësimin e vlefshmërisë së moduleve kriptografike (sistem kodifikimi).

ISO 17799

Qëllimi i ISO 17799 është t'i japë përdoruesit një katalog kriteresh me zgjidhje të praktikave më të mira (best practices solutions) për sigurinë e informacionit. Këtu duhen marrë parasysh fushat e mëposhtme:

- ☑ Politika e sigurisë dhe siguria fizike
- ☑ Organizimi dhe personeli
- ☑ Menaxhimi i komunikacionit
- ☑ Kontrolli i aksesit
- ☑ Menaxhimi i bizneseve operative

ITSEC/Common Criteria

ITSEC Common Criteria (CC) paraqet një proces kontrolli, me të cilin të mund të kontrollohen aspektet relevante të sigurisë të hard- dhe software -eve, në mënyrë që të arrihen rezultate të kuptueshme dhe krahasueshme.

ISO 9000

Normat e ISO-9000 përcaktojnë një proces kontrolli për një sistem të menaxhimit të cilësisë. Karakteristikat e sistemit të menaxhimit të cilësisë duhen dokumentuar dhe duhet të jenë të kuptueshme si brenda dhe jashtë firmës. Në këtë kuadër duhet kontrolluar, nëse pajisja me TI dhe organizimi i përshtaten qëllimit të ndërmarrjes. ISO 9000, e cila merret me menaxhimin e cilësisë në të gjithë ndërmarrjet, nuk i trajton hollësisht temat e sigurisë së TI-së. Meqë një sistem i mirë i menaxhimit të cilësisë ofron parakushte të mira për një nivel të lartë sigurie, kjo ndërvarësi është përshtatur nga ISO 9000.

Grupet e synuara

Kriteret e paraqitura kanë objektiva të ndryshme dhe janë përshtatur më parë për përdorimin në grupe të synuara të përcaktuara. Sidoqë kritere të veçanta mund të jenë të dobishme edhe si mjete ndihmëse për fusha të tjera përdorimi, prioritet është përdorimi i disa prej tyre në fushat e mëposhtme:

		TI-mbrojtja baze	Task-force	ISO TR 13335	FIPS 140	ISO 17799	ITSEC/ CC	ISO 9000
Kategoria e ndërmarrjes	Prodhues hardwaresh				X			X
	Prodhues softwaresh		X		X		X	X
	Operator serveri	X	X			X		X
	Ofrues interneti (provider)		X					X
	Content-provider	X	X			X		X
	Ndërmarrje (si klient)	X		X		X		X
Roli i personelit	Drejtues i TI-së	X	X	X		X		
	Administrator	X	X					
	Përfaqësues i TI-së për sigurinë/mbrojtjen e të dhënave	X	X	X	X	X	X	
	Management			X		X		X
	Menaxher projekti	X	X	X	X	X	X	X

X = grupi i synuar/kryesor

16.3 Kontrollet e aksesit përmes NT-LM dhe Kerberos

Identifikimi në rrjet

Me qëllim që përdoruesi të mund të identifikohet qartë në sistemin operativ, zakonisht kërkohen informacionet për identifikim në formën e kombinimit emër përdoruesi/fjalëkalim. Në rast se identifikimi i një përdoruesi nuk duhet të kryhet vetëm lokalisht, por në një server ose „domain controller" në rrjetin e firmës, atëhere parimisht këto të dhëna duhen dërguar nëpërmjet rrjetit.

Meqë dërgimi i pa koduar nëpërmjet rrjetit i emrave të përdoruesve dhe para së gjithash fjalëkalimeve respektive nuk ka kuptim, ekzistojnë protokolle të ndryshme, të cilat marrin përsipër problemet e autentifikimit gjatë identifikimit të përdoruesit në rrjet.

NT - LAN-Manager

Tek sistemet operative të Microsoft-it për një kohë të gjatë është në përdorim protokolli LAN-Manager. Ky i fundit, në një version të aktualizuar, gjendet ende tek Windows 2000, ose Windows XP. LAN-Manager-i, në sistemet operative të Microsoft-it është zbatuar në versionet e mëposhtme:

LAN-Manager (LM)	Me këtë protokoll kompjuterat me Windows-2000, ose -XP mund të aksesojnë të dhënat e përbashkësuara (shared) të kompjuterave me Windows for Workgroups, Wndows 95 dhe Windows 98.
NTLM Versioni 1	Versioni 1 i NTLM-së përdoret tek kompjuterat me Windows-NT-4.0 deri në Service Pack 3.
NTLM Versioni 2	Versioni 2 i NTML-së përdoret tek kompjuterat me Windows NT 4.0 deri në Service Pack 4 .

Në NTLM punohet me të dhënat e koduara të fjalëkalimeve të përdoruesve, të cilat memorizohen edhe lokalisht. Këto vlera Hash përcaktohen me një procedurë relativisht të dobët, e cila bazohet në algoritmin e vjetëruar DES.

Problematik është fakti, që deri tek NTLM v1 në fjalëkalimet me gjatësi maksimumi 14 karaktere nuk bëhet dallimi midis gërmave të vogla dhe të mëdha, si dhe fjalëkalimi lokalizohet dhe memorizohet i ndarë në dy blloqe me nga 7 karaktere secila. Këto kufizime e lehtësojnë mjaft përdorimin nga hackerat të sulmit të quajtur Brute-Force-Attack mbi informacionin e koduar.

Në rast se ju duhet që në rrjetin tuaj të përdorni NTLM-në, duhet të jeni të ndërgjegjshëm, se ajo nuk është patjetër metoda më e sigurt, që të mbani „jashtë" rrjetit një hacker të angazhuar dhe motivuar. Sigurohuni që në një rast të tillë, të përdorni të paktën NTLM v2, meqë NTML v2 i konsideron karakteret e fjalëkalimit si të dhëna Unicode (përfshi gërmat e vogla dhe të mëdha) dhe si bazë përdor algoritmin RC4.

Në një mjedis, i cili mbështet përdorimin e NTLM-së vetëm për shkak kompatibiliteti me versionet e mëparshme (backward compatibility), duhet menduar ndalimi i përdorimit të mëtejshëm të saj. Në rast se në një mjedis të sigurisë së lartë lihet aktiv NTLM-ja, një hacker, i cili nuk mund t'i thyejë procedurat e avancuara të sigurisë, si Kerberos, apo Certificate, mundet ama që me relativisht pak përpjekje, nëpërmjet një devijimi të detyrojë autentifikimin nëpërmjet një procedure të caktuar të cilën mund ta thyejë me lehtësi (Fallback-Attack) dhe në këtë mënyrë të thyejë sigurinë e një kompjuteri të vjetër që përdor vetëm NTML (NTLM-only).

Kerberos

Kerberosi është një protokoll, i cili u zhvillua për të mundësuar autentifikimin e përdoruesve në rrjetet e „pasigurta". I pasigurt d.m.th, që parimisht asnjë kompjuteri nuk i besohet dhe që rrugët e transmetimit të të dhënave nuk janë të sigurta. Me daljen e Windows 2000, kerberosi u bë protokoll autentifikimi edhe për rrjetet e Windows-it. Microsoft-i përdor në Windows 2000/XP versionin 5 të Kerberosit.

Përparësitë e Kerberos-it ndaj NTLM-së

Autentifikimi i ndërsjellë	Klienti dhe serveri mund të kërkojnë një autentifikim reciprok. Në këtë mënyrë si serveri, ashtu edhe klienti kalojnë testin e sigurisë që vërteton që partneri në komunikim është vërtet ai për të cilin pretendon. Serveri i vetëm në rrjet, të cilit duhet t'i besohet gjithmonë, është serveri Kerberos.
Etiketsiteti	Nëpërmjet NTLM-së një server duhet të lidhet me kontrolluesin e domainit (domain controler), me qëllim që të kontrollojë autenticitetin e klientëve. Në rastin e autentifikimit me Kerberos serveri mund ta zbulojë direkt identitetin e klientit, mjafton të kontrollojë etiketën/biletën (ticket) e tij.
Transferimi i autentifikimit	NTLM nuk ofron asnjë mundësi, që autentifikimi i klientëve nga një server të kalojë në një tjetër. Kerberosi ofron një proxy, ose ndryshe një mekanizëm forward, që e mundëson këtë.
Tranzitiviteti	Domainet nuk kanë nevojë të përcaktojnë tek Kerberosi ndonjë status kompleks besimi. Ekziston një raport besimi i dyanshëm. Raportet midis domaineve janë raporte tranzitive. Kjo do të thotë që në qoftë se domainet A dhe B kanë një raport besueshmërie dhe domaini B i beson domainit C, atëhere domainet B dhe C kanë raport besueshmërie mes tyre.
Ndëroperabiliteti	Ndryshe nga NTLM, Kerberos është një protokoll standard, i cili gjendet në shumicën e platformave kompjuterike. Nëpërmjet tij një kompjuter me UNIX p.sh. mund të intergohet pa problem në një domain me Windows 2000/XP.

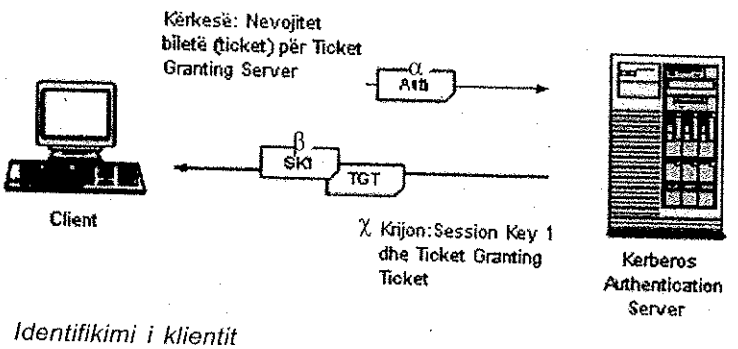
Biletat Kerberos (Kerberos-Tickets)

Parimisht kerberos bazohet mbi një sistem „biletash" (ticket system). Përveç kësaj, të gjithë pjesëmarrësit në kerberos duhet t'i bazojnë serverit kerberos.

Kerberosi parimisht shfrytëzon simetrinë kriptografike për mbrojtjen e informacioneve, por funksionet e tij mund të zgjerohen me simetrinë kriptografike dhe autorizimin nëpërmjet çelsave publikë (public keys).

Një proces tipik logimi, si dhe aksesi i një klienti mbi resurset e një serveri, ndjek zakonisht katër hapat e mëposhtëm:

Së pari, klienti duhet të identifikohet tek një server autentifikimi (Authentication Server). Në këtë rast klienti dërgon një kërkesë për lëshimin nga serveri të një TGT-je (Ticket Granting Ticket) – biletë për garanantimin e aksesit tek serveri α. Fjalëkalimi i koduar, i dërguar nga klienti, shqyrtohet nga serveri në bazën e të dhënave që ky i fundit ka për këtë qëllim dhe vlerësohet nëse kërkesa justifikohet.

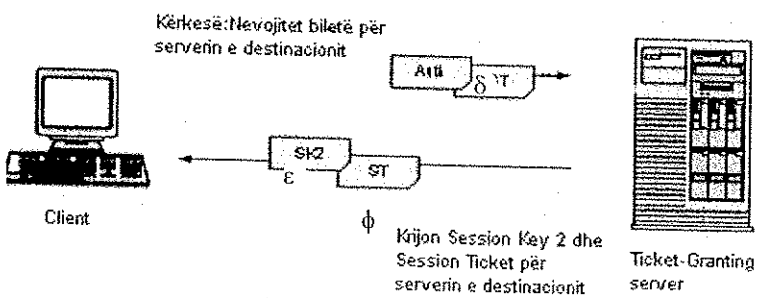


Identifikimi i klientit

Serveri gjeneron një Çelës Sesioni 1 (Session Key 1 (SK1)), i cili parashikohet për komunikimin midis klientit dhe Serverit Lëshues të Biletave (Ticket Granting Server), e kodon me çelsin e fshehtë të klientit dhe ia dërgon mbrapsht atij β. Më pas, Çelës Sesioni 1 (Session Key 1) dhe informacione të tjera (p. sh. një vulë kohore-timestamp) kodohen me çelsin e fshehtë të Serverit Lëshues të Biletave (Ticket Granting Server) dhe dërgohen tek klienti si paketë me të dhëna. Kjo paketë me të dhëna është Bileta për Garantimin e Aksesit (Ticket Granting Ticket) (TGT) χ.

Me TGT-në klienti aplikon tek Ticket Granting Server (TGS). Ky shërbim mund të ofrohet në të njëjtin makinë që që përdoret si server autentifikimi (Authen-tication Ser-ver), por mund të ofrohet si shërbim edhe nga një makinë tjetër e rrjetit.

Pasi klienti, me ndihmën e çelësit të tij të fshehtë, ka nxjerrë Çelës Sesionin 1 (Session Key 1) nga mesazhi i marrë nga Severi i Autentifikimit (Authentication Server), klienti e përdor atë për të koduar të dhënat e tij dhe kërkesën për TGS-në. Ai bashkëngjit në këtë rast edhe TGT-në δ.

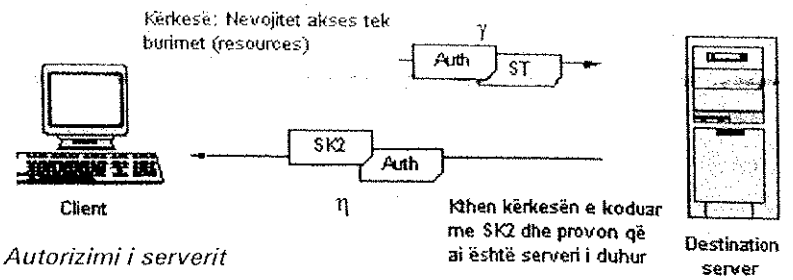


Kërkimi i Session Ticket-Kërkimi i një bilete sesioni

Kërkesa drejtuar TGS-së i kërkon serverit, t'i paraqesë klientit një Biletë Sesioni (Session Ticket) për serverin e destinacionit (Destination Server). TGS-ja mund ta dekodojë TGT-në, sepse ajo vetë është koduar nga Serveri i Autentifikimit (Authentication Server) me çelësin e fshehtë të TGS-së. Këtu, ndër të tjera përmbahet dhe Çelës Sesioni 1 (Session Key 1), i cili i nevojitet TGS-së, me qëllim që të mund të kryejë dekodimin e autentifikimit të klientit. Në rast se TGS ka mundur të bëjë siç duhet dekodimin e TGT-së dhe të autentifikimit, të cilat i ka marrë nga klienti, atëhere është përcaktuar si më poshtë:

- ☑ Klienti ka kryer paraprakisht identifikimin e duhur në serverin e autentifikimit, prandaj edhe ka marrë TGT-në përkatëse.
- ☑ Klienti është në të vërtetë ai klient, meqenëse ai zotëron Çelës Sesionin 1 (Session Key 1), i cili ishte përfshirë në TGT dhe ishte paketuar nga serveri i autentifikimit (Authentication Server).

TGS-ja gjeneron një Çelës Sesioni (Session Ticket) për serverin destinacion, nëpërmjet krijimit të një Çelës Sesioni 2 (Session Key 2). Ky i fundit kodohet me Çelës Sesionin 1 (Session Key 1) dhe dërgohet tek klienti e. Përveç kësaj, krijohet një Biletë Sesioni (Session Ticket), me të cilin, Çelës Sesioni 2 (Session Key 2) së bashku me informacionet shtesë kodohen me çelësin e fshehtë të serverit destinacion dhe dërgohen tek klienti ϕ.

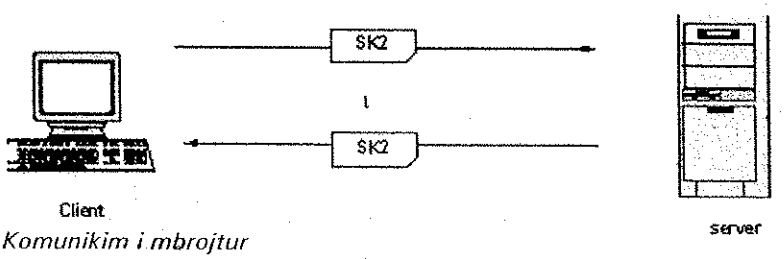


Autorizimi i serverit

Klienti mund ta dekodojë informacionin e marrë nga TGS-ja dhe në këtë mënyrë merr Çelës Sesionin 2 (Session Key 2). Klienti kodifikon kërkesën për serverin e destinacionit duke përdorur për këtë qëllim Session Key 2. Kërkesën në serverin e destinacionit g ai e dërgon së bashku me Biletë Sesionin (Session Ticket).

Serveri destinacion mund ta dekodojë Biletë Sesionin (Session Ticket), pasi ky i fundit ka qenë i mbrojtur me çelësin e tij të fshehtë. Çelës Sesionin 2 (Session Key 2) që serveri ka marrë mund ta përdorë, me qëllim që të dekodojë kërkesën e klientit. Në këtë mënyrë serveri destinacion e kupton, që klienti me të cilin po komunikon është ai i duhuri dhe që është identifikuar sipas procedurës së kërkuar.

Si përgjigje, serveri destinacion dërgon mbrapsht mesazhin e marrë, të koduar me Session Key 2 η. Mesazhi sigurisht përmban një vulë kohore (time stamp) të aktualizuar. Klienti, i cili e merr këtë përgjigje e kupton, që serveri destinacion ka qenë në gjendje ta dekodojë kërkesën e tij dhe si rrjedhim duhet të jetë serveri i duhur.



Komunikim i mbrojtur

Për lidhjen dhe komunikimin e mëtejshëm, si klienti, ashtu edhe serveri i destinacionit, mund të kenë besim se po komunikojnë me partnerin e vërtetë. Për kodim, që të dy, përdorin Session Key 2 ι.

Vlefshmëria e TGT

Përparësia e Kerberos-it qëndron jo vetëm në faktin se fjalëkalimet kalojnë të koduara në rrjet, por edhe sepse autentifikimi origjinal duhet të ndodhë vetëm një herë. Klienti identifikohet paraprakisht një herë tek serveri që bën autentifikimin dhe me TGT-në e marrë mund të kërkojë shumë session tickets për shërbime të tjera tek TGS-ja.

Me qëllim që të pengohen sulmet përsëritës (Replay-Attacks), tek të cilat agresori luan me bileta shërbimi të kopjuara, në bileta (tickets) janë të memorizuara edhe informacione në lidhje me kohën e lëshimit të tyre, kohëzgjatjen e vlefshmërisë, si dhe emrat dhe adresat e IP-ve të partnerëve në komunikim.

Në domainet e Windows 2000/XP kohëzgjatja standarde e vlefshmërisë së TGT-së është 10 orë. Kjo mjafton, që autentifikimi të bëhet vetëm një herë në ditë. Pas skadimit, klienti duhet të kryejë një identifikim të ri.

Në një rrjet të mbrojtur me Kerberos është jashtëzakonisht e rëndësishme, që të gjithë kompjuterat ta kenë orën e sinkronizuar. Në qoftë se ora e një kompjuteri ndryshon me një vlerë tolerance të pranueshme (Microsoft default: 5 Minuta) nga ora e një kompjuteri tjetër, kompjuteri, i cili merr një ticket të tillë, nuk bën dot dallimin, nëse bëhet fjalë për një biletë të vlefshme apo për një biletë shërbimi të kopjuar. Biletat me vulë kohore (timestamp) të pavlefshme nuk pranohen, dhe kompjuteri që ka orën gabim nuk mund të marrë pjesë në komunikimin e mbrojtur me Kerberos.

16.4 Siguria në WLAN

Aksesi në WLAN

Me qëllim që të mund të arrihet të aksesohet një WLAN, është i nevojshëm të kryhet një njoftim paraprak i komponenteve pjesmarrës në komunikim: Dërguesi dhe marrësi duhet të njohin njëri-tjetrin, përpara se të dërgojnë të dhënat.

Në këtë rast mund të kryhet një kontroll aksesi shtesë, i cili gjithsesi nuk përbën ndonjë parakusht. Megjithatë, sipas mundësive, ky kontroll aksesi shtesë është mirë të bëhet, në mënyrë ta mbrohet rrjeti nga aksesi i personave të paautorizuar. Standardet, të cilat gjejnë përdorim këtu para së gjithash janë:

☑ Autentifikim me sistem të hapur -Open System Authentication (802.11)
☑ Autentifikim me çelës kodimi të përbashkët -Shared Key Authentication (802.11)
☑ 802.1X-Autentifikim me nënprocedura

Open System Authentication

Open System Authentication bazohet në parimin e njohjes së ndërsjelltë të komponentëve pjesëmarrës në komunikim dhe nuk përmban ndonjë formë kontrolli të aksesit. Bëhet fjalë vetëm për një rradhë informacionesh, nëpërmjet të cilave pajisjet i bëjnë të njohura njëra-tjetrës frekuencat e përdorura, shpejtësitë dhe aksesibilitetin e tyre në përgjithësi, duke bërë të pamundur që një pajisje të jetë në gjendje t'ia refuzojë të drejtën për akses pajisjes tjetër. Open System Authentication është procedura standarde e pajisjeve WLAN sipas specifikimeve të 802.11.

Shared Key Authentication (Autentifikimi me çelës kodimi të përbashkët)

Shared Key Authentication përdoret sipas 802.11, si proces me siguri aksesi të integruar. Ai bazohet në një çelës të përbashkët, i cili shkëmbehet nga pjesëmarrësit në komunikim para aksesit të WLAN-it. Kjo mund të ndodhë me anë të një diskete për shembull. Çelësi në fjalë nuk lejohet të dërgohet përmes radiovalëve, pasi ato mund të interceptohen (kapen) nga një sulmues potencial. Të gjitha pajisjet brenda rrjetit, të cilat dëshirojnë të komunikojnë me njëra-tjetrën, duhet të disponojnë të njëjtin çelës. Përveç kësaj, atyre iu nevojitet një implementim i algoritmit Wired-Equivalent-Privacy (WEP-Algorithm), i cili përdor si mekanizëm kodimi atë të Shared Key Authentication.

Një autentifikim Shared Key punon si më poshtë:

Dërguesi	Marrësi
Dërgon një mesazh njohje, i cili është përfshirë në formën e një vlere në paketë, si dhe është koduar me një çelës.	
	Dërgon një konfirmim marrje me një 128-Bit-challenge-block, i cili gjenerohet gjatë përdorimit të WEP-it.
Kopjon challenge-block-un në një paketë të re dhe e kodon atë me WEP gjatë përdorimit të shared key.	
	Ç'kodon challenge-block-un e marrë me shared key-n e vet dhe e krahason atë me mesazhin origjinal. Në rast se të dyja janë identike, autentifikimi mbyllet me sukses.

Autentifikimi 802.1X

Authentifikimi i hosteve nëpërmjet 802.1X nuk është përcaktuar për një media transmetuese të caktuar, por paraqet një procedurë standarde për kontrollin e aksesit në rrjete. Ky autentifikim është një procedurë standarde me emrin RADIUS (Remote Authentication Dial-In User Service), që përdoret para së gjithash tek serverat dial-in, e cila ka funksionuar me sukses në implementime të ndryshme. Në fushën e WLAN-it mund të përdoren protokolle të ndryshme autentifikimi me RADIUS. Më i përhapuri është një nënversion i Extensible Authentication Protocols (EAP), i cili përdoret veçanërisht në shtresën e transportit (referuar modelit OSI).

EAP-TLS

Extensible Authentication Protocol - Transport Level Security (EAP-TLS) është një procedurë e përhapur për autentifikimin e ndërsjelltë dhe të sigurt gjatë aksesimit të rrjetit, e cila bazohet në Private Key Infrastructure (PKI) dhe presupozon përdorimin e certifikatave dixhitale.

PEAP-MS-CHAP v2

Një procedurë e mëtejshme është protokolli i vet (proprietar) Microsoft-it - PEAP-MS-CHAP v2 (Protected EAP-Microsoft Challenge-Handshake Authentication Protocol), i cili bazohet në transmetimin e elementeve të autentifikimit CHAP-v2 të koduar dobët brenda një kanali të koduar fort. Kjo procedurë përdoret në mjediset me Wndows-Server-2003 dhe me Windows XP, në të cilat nuk është implementuar PKI-ja.

Kodimi (WEP dhe WPA)

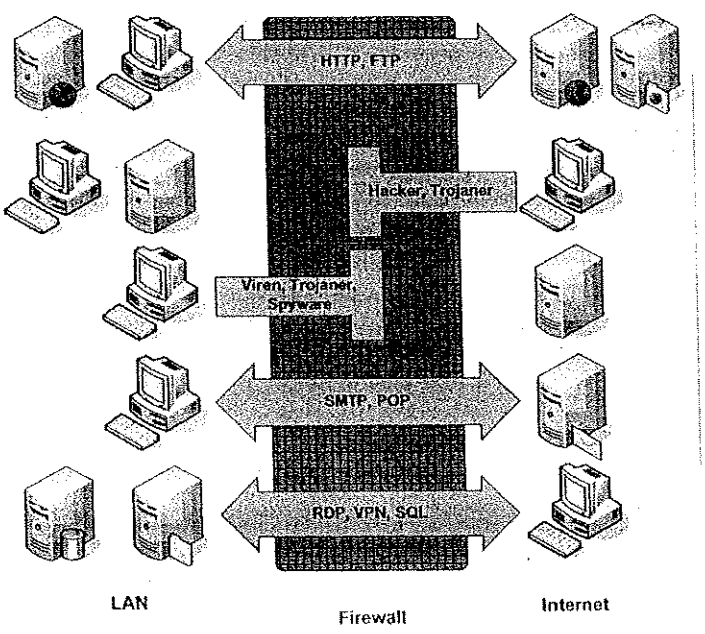
Me qëllim që të sigurohet trafiku i të dhënave në WLAN, duhet patjetër që komunikimi të kodohet. Procedura standarde për kodim është, sipas standartit 802.11, një kodim RC4 me Wired Equivalent Privacy (WEP), i cili ndërtohet mbi Shared Key Authentication. Në rast se kodimi përdoret në kombinim me EAP-TLS ose PEAP-MS-CHAP v2, atëhere futen në përdorim çelsat kodues respektivë, të cilët i përdorin këto protokolle. Në rast se kërkohet mbrojtje të veçantë, mund të përdoren mekanizma që veprojnë mbi shtresën e rrjetit (Network Layer), si IPSec, të cilat i krijojnë një siguri shtesë gjithë trafikut të IP-së.

Me qëllim rritjen e sigurisë, nëpërmjet Wi-Fi u publikua një pjesë e IEEE 802.11i si procedurë e re WPA (WiFi Protected Access). Ndryshe nga procedura WEP (çelës 32-Bitsh), me ndihmën e TKIPs (Temporal Key Integrity Protocol) krijohet një çelës kodimi dinamik 48 Bit i gjatë ose tek WPA2 nëpërmjet AES (Advanced Encryption Standard) 256 Bit i gjatë.

16.5 Firewall-i

Detyrat e një Firewall-i

Firewall-i në parim s'është gjë tjetër veçse një filtër inteligjent. Firewall-et shërbejnë për filtrimin e aksesit në rrjet të përdoruesve, adresave, ose aplikimeve, me qëllim që të pengohen transmetimet armiqësore në rrjet. Nga njëra anë firewall-i duhet të mundësojë trafikun e patrazuar nga LAN-i për tek rrjetet e tjera, nga ana tjetër ai duhet të lejojë paketat të hyjnë në LAN, nëse paraprakisht ato janë kërkuar nëpërmjet LAN-it nga klientët brenda tij.



Firewall-et përdoren me qëllim sigurimin e kalimit të të dhënave midis rrjeteve private "të sigurta" dhe rrjeteve publike "të pasigurta". Fusha kryesore e përdorimit për Firewall-et është lidhja e LAN-eve me Internetin. Por Firewall-et mund të përdoren edhe midis pjesëve të rrjetit që i përkasin një LAN-i, me qëllim që të përmbushen kërkesa të veçanta në lidhje me sigurinë.
Krahas mbrojtjes nga sulmet firewall-et mund të shfrytëzohen për kufizimin e aksesit të përdoruesve tek adresat dhe shërbimet e jashtme „të lejuara". Kështu kufizohet deri diku aksesi në adresa interneti të caktuara.

Firewall-et mund të implementohen si zgjidhje hardware-i, apo software-i. Firewall-et e ngritura me software përdoren shpesh si pjesë përbërëse e sistemeve të tjera. Kështu, një router, ose një proxy-server bëjnë njëkohësisht filtrimin e paketave duke kufizuar në këtë mënyrë fluksin e të dhënave.

Ndryshimi: Hacker dhe Cracker
Më poshtë do të përdoren gjithmonë e më tepër termat Hacker dhe Cracker.

Hacker-i është dikush, që sulmon një rrjet kompjuterash, për të identifikuar dobësitë potenciale të tij dhe të influencojë në eliminimin e tyre. Nga hacker-at përgjithësisht nuk ka rrezik për rrjetet, pasi ata nuk kanë si qëllim dëmtimin e sistemeve. Sigurisht edhe një hacker mund të shkaktojë pa dashje (gabimisht) dëme, ose të monopolizojë në një masë të madhe resurset e rrjetit.

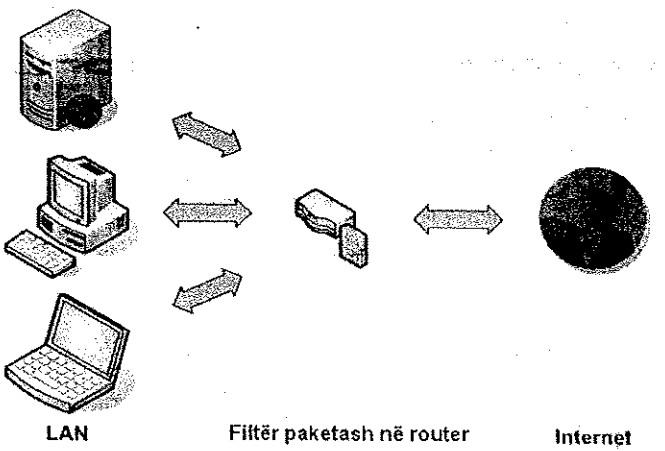
Cracker-at në dallim nga hacker-at i sulmojnë rrjetet, me qëllim që t'ua dëmtojnë, t'ua vjedhin, apo t'ua ndyshojnë të dhënat, të lidhen me burimet e rrjetit dhe të sabotojnë punën në rrjet. Firewall-et kanë për detyrë të mbrojnë rrjetin nga cracker-at, gjë që do të thotë, që në rastin ideal edhe hacker-at të mos e çajnë dot mbrojtjen e sistemit, duke qenë se të dy palët (hacker-at dhe cracker-at) shfrytëzojnë të njëjtat dobësi dhe të çara të sistemit për të hyrë në të.

Llojet e Firewall-it

Firewall-et mund të kryejnë filtrimin e fluksit të të dhënave në komunikim sipas aspekteve të ndryshme. Parimisht dallohen tri lloje të ndryshme Firewall-esh:

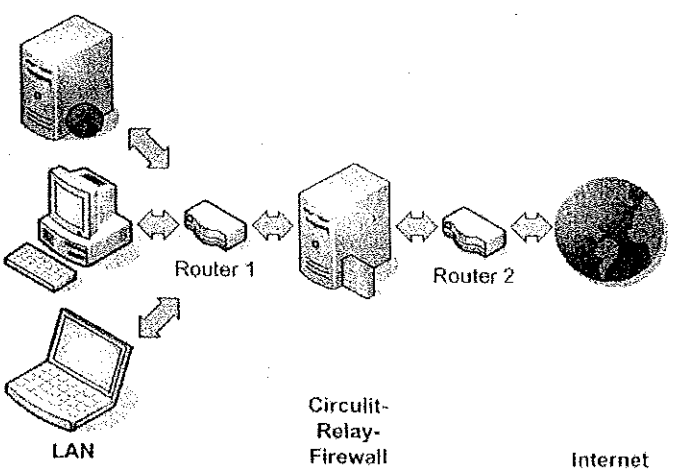
- ☑ Filtrues paketash (Packet Filter)
- ☑ Firewall në qark (Circuit-Relay-Firewalls)
- ☑ Portale aplikacionesh (Application-Gateways)

Packet filter (filtri i paketave)



Filtrat e paketave analizojnë adresat e dërguesit dhe marrësit të paketave, me qëllim që t'i transmetojnë më tej, apo t'i refuzojnë ato. Si rregull shqyrtohen adresat në shtresën 3 dhe portat në shtresën 4. Në këtë mënyrë mund të kufizohet transporti i të dhënave midis subnet-eve nëpërmjet analizmit të IP-Header-it. Kërkesat e shërbimeve mund të interpretohen nëpërmjet vlerësimit të numrave të portave dhe më pas kontrollohen në një tabelë, nëse të dhënat duhet të transportohen më tej, apo jo. Si rregull vlerësimi i trafikut të të dhënave kryhet nga tabelat e firewall-it, të cilat e rregullojnë transportin nëpërmjet kritereve përkatëse të skualifikimit të paketave. Filrat e paketave i gjejmë shpesh të zbatuara tek router-at, proxy-t, ose serverat tek RAS, meqë tek këto pajisje kryhet një interpretim i header-it pra nuk kryhet ndonjë përpunim që kërkon angazhim dhe kosto shtesë. Filtrat e paketave janë transparente ndaj mënyrës së transportit të paketave. Filtrat e paketave janë transparente ndaj linjës së transmetimit të të dhënave. Kjo do të thotë, që ato nuk konsiderohen si komponente të pavarura nga pajisjet e tjera të rrjetit, por si pajisje që lejojnë, ose nuk lejojnë, në pamje të parë në mënyrë rastësore, kalimin e paketave me të dhëna nëpërmjet tyre.

Circuit-Relay-Firewalls



Circuit-Relay-Firewalls (ndryshe: firewall-et e lidhjes në qark) e kanë parimin e punës të ngjashëm me parimin e punës të filtrave të paketave. Ato sigurisht nuk analizojnë të gjithë trafikun e të dhënave që kalon rastësisht nëpërmjet tyre, por përdoren si komponentë që kanë si qëllim të kryejnë lidhjen dhe autorizimin.

Një Circuit-Relay-Firewall është një Host (kompjuter), i cili vendoset midis dy routerave. Nëse një sistem kërkon të dërgojë të dhëna nëpërmjet segmentit Circuit-Relay, ai duhet paraprakisht të autorizohet nga firewall-i. Ky i fundit kontrollon, nëse sistemi në fjalë mund të provojë, që i ka të drejtat e nevojshme për transportin respektiv të të dhënave. Pas kësaj Firewall-i jep „lejen" për transportin më tej të të dhënave.

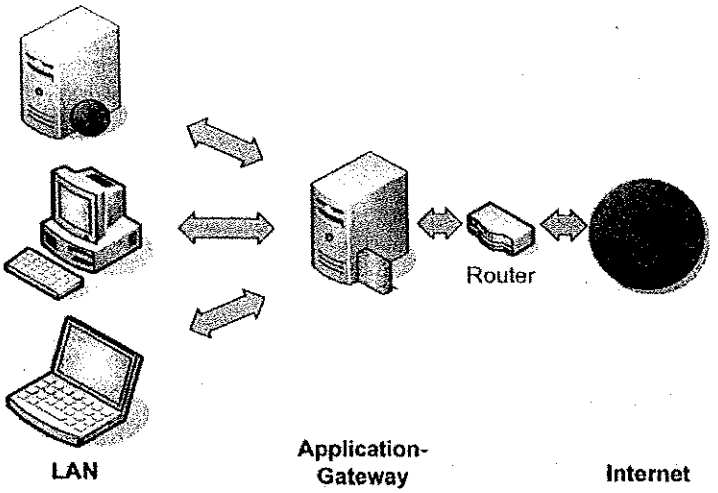
Firewall-i dyfishon fluksin e të dhënave për tek segmenti tjetër i rrjetit. Një kontroll i përsëritur ndodh, nëse duhet të fillojë një fluks i ri komunikimi. Rrjeti në distancë (remote) nuk duket nëpërmjet Circuit-Relay-Firewall.

Meqë Circuit-Relay-Firewalls nuk përpunojnë vetëm paketa, por punojnë në shtresën e Transportit dhe Aplikacioneve (Transport and Application Layer), ato janë relativisht të ngadalta. Në këtë mënyrë, nevojitet një implementim nga ana e klientit, që duhet të identifikohet tek firewall-i, në mënyrë që të fillohet transporti i të dhënave.

Application-Gateway

Application-Gateways punojnë në shtresat e larta të modelit OSI. Ato shërbejnë gati si server aplikacionesh, që ve në dispozicion të klientëve aplikacionet e nevojshme në rrjet. Në këtë mënyrë Application-Gateways nuk kërkojnë asnjë modifikim të softwareve të klientit. Klienti akseson njëlloj një terminal server.

Application-Gateways, përpara se të fillojnë me transportin e të dhënave, kontrollojnë çdo lidhje së pari në lidhje me besueshmërinë. Nga këndvështrimi i klientit objektivi i komunikimit është Application-Gateway. Kjo e fundit më pas merr përsipër shërbimet e tjera në rrjet. Application-Gateways punojnë sipas parimit të proxy-t.



Sigurisht mekanizmat komplekse të kontrollit të Application-Gateways nuk mund të krahasohen me ato të proxy-t klasik. Nëpërmjet shkëputjes së plotë të rrjeteve të lidhura me njëra-tjetrën, Application-Gateways paraqesin formën më të sigurtë të firewall-it.

Sigurisht, sasia e llogaritjeve që ato duhet të kryejnë rritet ndjeshëm duke zvogëluar në mënyrë të dukshme fluksin e të dhënave në rrjet. Nga ana tjetër, kemi një shkallëzim të shkëlqyer përsa i përket aspekteve përkatëse të sigurisë në lidhje me aksesin në rrjet dhe nga rrjeti.

Aksesi në një website-i në Internet

Në rast se p.sh. një kompjuter klient dëshiron të thërrasë një faqe që ndodhet e hostuar në një web-server të caktuar, lidhja bëhet paraprakisht me firewall-in. Ky i fundit kontrollon, nëse duhet autorizuar, apo jo lidhja dhe nëse po krijon nga ana tjetër lidhjen me serverin e dëshiruar. Faqja HTML transferohet dhe përmbajtja e saj analizohet. Nëse firewall-i duhet të filtrojë bannerat e reklamave, atëhere nga faqja e marrë HTML hiqen të gjitha instruksionet që bëjnë të mundur shfaqjen e popup-eve, apo të banner-ave. Faqja e modifikuar në mënyrë të tillë i dërgohet klientit. Klienti nga ana e tij e vlerëson faqen e marrë HTML dhe si përfundim kërkon paraqitjen e pamjeve të dëshiruara prej tij. Firewall-i ngarkon me kujdes pamjet përkatëse nga web-server-i dhe ia kalon ato më tej klientit. Si rezultat, klienti shikon një faqe interneti pa reklama. Me këtë rast kursehet edhe banda e komunikimit, meqë banner-at nuk duhen shkarkuar paraprakisht.

Mundësi fleksibël përdorimi

Sipas mënyrës së ndërtimit dhe organizimit të bashkësisë së rregullave të filtrimit, webseite-t, shërbimet FTP, apo ndonjë protokoll Interneti dhe aplikacion tjetër, filtrohen dhe përpunohen paraprakisht, përpara se të lejohet përdorimi i tyre për klientët brenda rrjetit. Proxy-it ofrojnë mundësitë më të mëdha për filtrimin e trafikut të të dhënave, por janë të kushtueshme, pasi funksionet e proxy-it duhen zhvilluar në mënyrë speciale për çdo aplikacion.

Shënime

Firewall-e të certifikuara

Firewall-et personale, apo Desktop-Firewalls janë programe, të cilat punojnë lokalisht tek kompjuterat, të cilët duhet të mbrojnë. Firewalli në këtë rast nuk filtron trafikun midis rrjeteve, por kontrollon trafikun e të dhënave midis kompjuterit që mbrohet dhe rrjetit me të cilin ai është lidhur, respektivisht Internetit.

Firewall-i tek kompjuterat lokalë lejon filtrimin e aplikacioneve të caktuara. Pas instalimit në mënyrë standarde, bllokohet fillimisht i gjithë trafiku i të dhënave. Në rast se një aplikacion tenton të aksesojë Internetin, atëhere bashkë me kërkesën dërgohet një pyetje, me anë të të cilës përdoruesi i aplikacionit përkatës lejon kalimin e firewall -it.

Efikasiteti i firewall-eve personale është i diskutueshëm. Shpeshtësia dhe paqartësia e pyetjeve mund të çojnë në lodhjen e përdoruesit deri në atë pikë, sa ta ulë firewallin duke lejuar që në këtë mënyrë të bëhet pre e viruseve, trojanëve dhe spywareve, që mund ta aksesojnë kompjuterin e tij nëpërmjet Internetit.

Firewall-et në praktikë

Në praktikë Firewallet implementohen si zgjidhje hardware. Sipas kerkesave të sigurisë që ka firma mund të përdoren edhe disa firewalle në formë kaskade, me qëllim që të sigurohet rrjeti nga lloje sulmesh të shumëfishta.

Zgjidhjet bazuar në software mund të jenë të përshtatshme në raste të veçanta, me qëllim sigurimin e një rrjeti, ose një kompjuteri të veçantë ndaj sulmeve. Gjithsesi, konfigurimi i këtyre softwareve kërkon njohuri të thella profesionale. Prandaj për një përdorim profesional të tyre, duhet të këshilloheni paraprakisht.

Tek disa sisteme të reja operative, si Windows XP, është implementuar një firewall i thjeshtë i parakonfiguruar. Kjo zgjidhje, e cila kuptohet është më e mirë se sa rasti pa firewall fare, por në të shkuarën në shumë raste është provuar si e pamjaftueshme.

Me përhapjen gjithnjë në rritje të lidhjeve DSL tek personat privatë, firewallet e të ashtuquajturave routera DSL po marrin një kuptim dhe rol gjithmonë e më domethënës. Sigurisht, që këtu duhet pasur kujdes, që konfigurimi i një zgjidhjeje firewalli në formë kaskade kërkon njohuri profesionale shumë speciale, me qëllim që firewall-et të mos e pengojnë njëri-tjetrin. Normalisht kjo i tejkalon aftësitë e diletantëve.

Konfigurimi i Firewall-it

Tek konfigurimi i një firewalli në përgjithësi vlen thënia: "Çfarë nuk lejohet qartë, ndalohet." Cracker-at nuk njohin kod etik, apo moral, që t'i ndalojnë të keqpërdorin një të çarë „të padëmshme" që mund të gjejnë në sistemin e sigurisë. NUK EKZISTOJNË TË ÇARA TË PADËMSHME NË SISTEMIN E SIGURISË!

Për këtë arsye, duhet që një firewall të jetë i konfiguruar në atë mënyrë, që të lejojë vetëm trafikun në dalje që gjenerohet nga aplikacione të caktuara për në destinacione të përcaktuara dhe të pengojë në përgjithësi trafikun në hyrje, në qoftë se ky i fundit nuk vjen si përgjigje e një kërkese direkte nga rrjeti.

Software-ve nuk iu kontrollohet vetëm emri, por edhe autenticiteti siç është p.sh rasti i përdorimit për këtë qëllim i një MD5-Hash. Në të kundërt, trojanë të ndryshëm në rrjet do të tentojnë të maskohen si software ekzistues duke iniciuar kërkesa prej rrjetit.

Edhe software-ve që bëjnë kërkesa për hyrje në rrjet duhet patjetër t'u kontrollohet autenticiteti. Për këtë arsye, nuk lejohet që në një mjedis me një koncept të pjekur sigurie të hiqet dorë nga përdorimi i kodimit nëpërmjet çelsave publik (public keys) dhe certifikatave. Vetëm atëhere kur të gjitha fushat e konceptit të sigurisë janë marrë gjerësisht parasysh, mund të garantohet një siguri relative ndaj sulmeve. Sigurisht, siguri absolute nuk ka. Mos hezitoni asnjëherë të thërrisni profesionistë të specializuar për një vlerësim të gjendjes së sigurisë së sistemit tuaj, në rast se përdorni aplikacione, apo të dhëna që janë kritike për kompaninë. Mos harroni gjithashtu, që mund të bëheni përgjegjës p.sh për dëmet nga viruset, të cilat mund të përhapen pa u vënë re në rrjetin tuaj.

Firewall-e të certifikuara

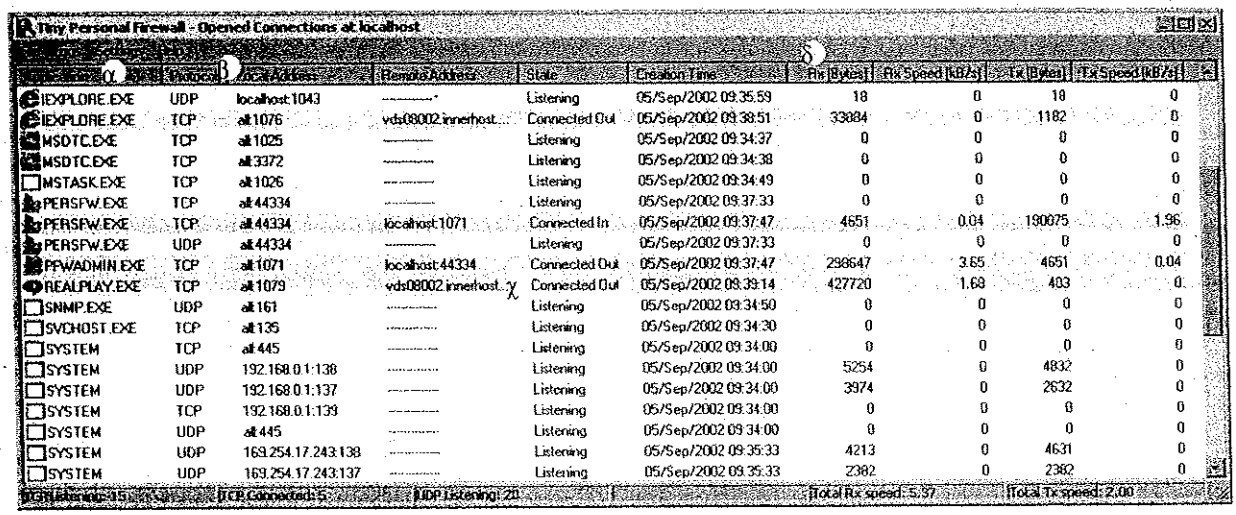
Për firewall-et ofrohen certifikata sigurie. Çertifikimi më domethënës është ai i laboratoreve ICSA (ICSA-Labs), një kompani bijë, e pavarur, e TruSecure Corporation. ICSA Labs teston firewall-et, programet antivirus, si dhe komponentë të tjerë të sigurisë së rrjetit në lidhje me „porozitetin" e tyre dhe pas testimeve rigoroze lëshon një certifikatë, e cila mund të konsiderohet sot si standard industrie.

Freeware dhe Shareware

Ndërkaq në treg mund të gjenden disa produkte freeware, apo shareware, të cilat ofrojnë një siguri të mjaftueshme për kompjuterat e veçantë, ose rrjetet e vogla private. Si shembull mund të përmendim firewall-in personal të ofruar nga Kerio *(www.kerio.com)*, i cili është pasardhësi i TinyPersonal Firewall. Kërkoni në internet për ofertat akutuale në këtë fushë. Kini parasysh, që edhe firewalli-më i mirë nuk mund t'u mbrojë, nëse nuk është konfiguruar dhe administruar siç duhet. Familjarizohuni rregullisht me zhvillimet e reja në Internet.

Mbikqyrja e trafikut të të dhënave

Një funksion i rëndësishëm i firewalleve është mbikëqyrja në kohë reale e trafikut që kalon në to. Mbikqyrja online lejon studimin e sjelljes së firewallit në lidhje me trafikun e të dhënave, si dhe bën të mundur identifikimin dhe eliminimin e pikave të dobta. Kjo sigurisht presupozon përvojë të gjatë në këtë drejtim. Meqë kjo në praktikën e punës është e vështirë për t'u bërë, administratorët kryejnë trajnime speciale, ose ia besojnë këtë punë firmave të specializuara.



Mbikqyrja e trafikut të të dhënave tek një firewall me anë të software-ve

Në figurën e mësipërme tregohen aplikacionet që punojnë (α), në cilat porta kalon trafiku (β), cilat lidhje kanë krijuar (χ) po ashtu edhe informacione në lidhje më sasinë dhe shpejtësinë e përpunimit të informacionit (δ)

Protokollimi

Një firewall i mirë duhet të mundësojë edhe një protokollim të diferencuar, me qëllim që të dedektojë tentativat potenciale për sulme. Kini parasysh, që edhe protokollimi më i mirë nuk mund të ndikojë në mbrojtje, nëse protokollet vetë nuk vlerësohen rregullisht.

Përvoja ka treguar, që është më mirë të shqyrtohet rregullisht protokollimi për disa ngjarje (events) relevante, sesa të protokollohet çdo paketë ICMP që hyn dhe pas pak javësh, nga pamundësia e shqyrtimit të sasisë së madhe të ngjarjeve të protokolluara të fshihen të gjithë skedarët e protokollimit.

16.6 Sisteme Dedektimi të Hyrjeve të Paautorizuara (Intrusion-Detection-Systems)

Firewall-i i vetëm nuk mjafton

Ndërkaq, firewall-et instalohen në rrjetet e kompanive si masa mbrojtëse kundër hyrjeve të paautorizuara në rrjet dhe u përkasin pajisjeve standarde të një rrjeti të administruar në mënyrë profesionale. Megjithatë, edhe me një firewall të konfiguruar mirë, ekziston njëfarë mundësie që masat mbrojtëse ekzistuese të anashkalohen.

Një Intrusion-Detection-System (IDS) është, siç edhe termi anglisht le të kuptohet, një sistem për detektimin e një hyrje të paautorizuar në rrjet. Ndërsa masat e tjera kanë si qëllim pengimin e hyrjeve të pautorizuara në rrjetin e mbrojtur, një IDS instalohet në një sistem, me qëllim që të paktën të mund të dedektojë një hyrje të paautorizuar në rrjet pasi ajo ka arritur të ndodhë.

Kjo mund të krahasohet me bravën e derës së shtëpisë. E mbyllur,ajo pengon hyrjet e paautorizuara në shtëpi. Por nëse keni harruar një dritare hapur në pjesën e mbrapme të shtëpisë, apo nëse keqbërësi do ta hapte bravën, në çdo rast shtëpia do të grabitej. Pas grabitjes, keqbërësi do ta mbyllte sërish derën, apo dritaren nga hyri. Kur të ktheheni në mbrëmje në shtëpi, do ta kuptoni se dikush ka hyrë në shtëpi, vetëm kur të vini re mungesën e objekteve me vlerë.

Pajisje „alarmi" për rrjetet

Në një rast të tillë do të ishte praktike të insalohej një pajisje alarmi. Kjo pajisje do të aktivizohej p.sh. nëse do të hapej brava e portës së shtëpisë. Në këtë rast nuk pengohet hapja e bravës së portës, por të paktën do të kuptohet që porta, apo që një dritare ishte hapur.

Se si do të reagonte në një rast të tillë pajisja e alarmit, kjo mund të përcaktohet nga ju. Dëshironi ta trembni hajdutin me një alarm që bie fort, apo dëshironi që alarmi të jetë i heshtur dhe të bjerë në stacionin më të afërt të policisë, me qëllim që në rastin ideal hajduti të kapej me „presh në dorë" dhe të arrestohej?

Shumë sulme mbeten të pazbuluara

Përsa i përket rrjeteve kompjuterike paraqitet një situatë e zymtë: Sipas një studimi të DISA (Defense Information Systems Agency) 88 % e tentativave për hyrje të pautorizuara në kompjuterat e autoriteteve të SH.B.A.-së kanë rezultuar të suksesshme dhe 96% kanë kaluar pa u vënë re nga „viktimat" e tyre.

Me qëllim që mos të lihet që gjendja të përkeqësohet më tej, apo me qëllim që të merren kundërmasa të përshtatshme ndaj vazhdimit të cënimit të sigurisë së sistemit, atëherë është i nevojshëm dhe urgjent aplikimi i një sistemi paralajmërimi përveç masave mbrojtëse ekzistuese. Në rast se një IDS arrin të identifikojë sulmet e vazhdueshme të një hackeri, atëhere informacionet e regjistruara përdoren për të siguruar provat për gjetjen e agresorit.

Mënyra e punës e një IDS-je

Identifikimi i anomalive

Një tentativë për thyerjn e sigurisë së një rrjeti kompjuterik, apo një shkelje tjetër e masave të sigurisë tregon që proceset elektronike kanë devijuar nga gjendja normale. Një IDS, e cila punon edhe pas konstatimit të një anomalie, niset nga fakti që nga ana statike, klienti dhe komponentët e një rrjeti, sillen në mënyrë konstante. Kjo sjellje statike përkufizohet si një shembull i mënyrës së sjelljes.

Në rast se më pas gjatë punës modeli i sjelljeve të segmentit të mbikqyrur të rrjetit devijon nga normalja, kjo do të thotë që kemi të bëjmë me një thyerje të sistemit të sigurisë në rrjet.

Për një IDS, e cila punon për identifikimin e anomalive, është para së gjithash e nevojshme, të grumbullojë nëpërmjet matjeve të dhëna të mjaftueshme në rrjet gjatë një periudhe të caktuar kohe. Këtu përfshihen dhe konsiderohen një numër i madh parametrash të rrjetit dhe të punës së kompjuterave. Prej këtyre të dhënave të grumbulluara identifikohet një model të dhënash për punën në kushte normale me vlera tolerance të parashikuara.

Më pas sistemi IDS tarohet të punojë më „mprehtë". Ai mbikqyr gjatë punës të dhënat e matura dhe i krahason ato, nëse janë brenda vlerave të dhëna të tolerancës. Në qoftë se këto vlera kapërcehen, atëhere IDS merr kundërmasa, apo thjesht jep alarmin.

Përparësia e kësaj metode është që modeli i sulmit nuk është i nevojshëm të përcaktohet qartë. Thyerjet e sigurisë, të panjohura më parë identifikohen si të tilla, në rastet kur ka devijime nga parametrat normale të punës. IDS-të për identifikim anomalish në fillim janë krijuar sipas modeleve të sjelljes dhe nuk kanë nëvojë për mirëmbajtje.

Sigurisht, në këtë mënyrë nuk do të identifikohen ato sulme, modeli i sjelljeve të të cilave nuk devijon nga modeli statistikor i vlerësimit. Përveç kësaj, mund të aktivizohen alarme, në rast se një përdorues ndryshon sjelljet e tij në mënyrë të ligjshme.

Analiza e nënshkrimit

Software-i që kryen analizën e nënshkrimit punon në mënyrë të ngjashme me një antivirus që skanon për viruse. Ai ka një bazë të dhënash me skenaret tipike të sulmeve. Për çdo sulm të kapur dhe regjistruar në bazën e të dhënave ekziston një model tipik sulmi që ka nënshkrimin e vet (signature). Në bazë të nënshkrimeve të regjistruara në bazën e vet të të dhënave IDS-ja mbikqyr fluksin e trafikut të të dhënave dhe informon në rast se ka thyerje të sigurisë.

Analiza e nënshkrimit kursen regjistrimin e të dhënave të matura në kushte normale dhe vlerësimin e tyre nëpërmjet analizave të sofistikuara statistikore, duke u përqendruar thjesht në përditësimin e bazës së të dhënave të nënshkrimeve (signatures database). Në mënyrë të ngjashme si tek antiviruset, një IDS e bazuar tek nënshkrimet e sulmeve mund të identifikojë ato sulme, për të cilat në bazën e të dhënave të nënshkrimeve ekziston një model nënshkrimi. Sulmet e reja të pazakonta dhe që nuk janë në bazën e të dhënave nuk identifikohen nga IDS-ja.

Ndryshe nga analiza e anomalive, rasti për një alarm fals (fals positiv) tek IDS-të që analizojnë nënshkrimin është dukshëm më i vogël. Ndërsa gjatë një analize anomalie devijimi nga sjelljet e përditshme në rrjetin kompjuterik çon në aktivizimin e alarmit, IDS-signature e aktivizon alarmin vetëm në rastet, kur një model i gjetur në rrjet përputhet me modelin e nënshkrimit të një sulmi të njohur.

IDS për hoste, apo rrjete

Në rast se duhen mbrojtur hoste (kompjutera) të veçantë, atëhere aplikohet një e ashtuquajtur IDS për host. Kjo e fundit mbikqyr direkt kompjuterin që duhet mbrojtur. Për mbikqyrjen e të gjithë segmentit të rrjetit, kohët e fundit janë përdorur IDS-të për rrjet. IDS-të për rrjet duhet të kenë performancë të lartë, pasi ato duhet të jenë në gjendje të analizojnë dhe vlerësojnë në kohë reale, të gjithë fluksin e të dhënave që kalon nëpërmjet lidhjeve të rrjetit. Teknikat moderne të LAN-it, të cilat punojnë në diapazonet 100-Mbit/s- apo 1-Gbit/s, paraqesin sfida të veçanta për hard dhe softwaret, të cilat do të kryejnë analizimin dhe vlerësimin e të dhënave në kohë reale.

Vendosja e IDS-së

Përsa i përket vendosjes së një IDS-je ekzistojnë mundësi të ndryshme, të cilat varen nga qëllimi për të cilin do të përdoret IDS-ja:

☑ Para firewall-it dhe rrjetit që do të mbrohet
☑ Mbrapa firewall-it në rrjetin e mbrojtur

Nëse e vendosni IDS-në para firewall-it, atëhere IDS-ja i shqyrton të gjitha sulmet nga jashtë. Nuk ka rëndësi nëse sulmi pati sukses apo jo, e rëndësishme është që IDS-ja të jetë aktive dhe ta ketë dedektuar sulmin.

Nëse IDS-ja vendoset në rrjetin e mbrojtur, atëhere regjistrohen vetëm sulmet e sukseshme nga jashtë, të cilat kanë qenë në gjendje të kalojnë firewallin. Për më tepër, IDS-ja është në gjendje të zbulojë edhe thyerjet e sigurisë nga punonjësit brenda kompanisë. Në këtë mënyrë identifikohen gabimet, pakujdesitë apo manipulimet e qëllimshme, të cilat janë të pritshme nga persona që kanë akses mbi LAN-in e mbrojtur.

17 Planifikimi dhe dokumentimi

Në këtë kapitull do të lexoni:
- → si të planifikoni një kabllim të strukturuar
- → si të krijoni parakushtet për një kabllim të strukturuar
- → si ta vini në jetë kabllimin e strukturuar

Kushte paraprake:
- ✓ Njohuri mbi përbërësit pasivë të rrjetit
- ✓ Njohuri mbi instruksionet/udhëzuesit e instalimit
- ✓ Njohuri mbi standardin ISO/IEC për kabllim të strukturuar

17.1 Planifikimi i objektivave

Kabllimi i strukturuar

Kabllimi i strukturuar presupozon një plan instalimi për një kabllim të njëjtë për shërbime të ndryshme (të dhëna, video, telefon), si dhe hedh bazat për një infrastrukturë rrjeti të orientuar nga e ardhmja, pra që t'i paraprijë ndryshimeve që mund të kryhen në të ardhmen. Parë nga një perspektivë tridimensionale, dallojmë zonat e mëposhtme:

- ☑ **Zona e parë** përshkruan kabllimin midis ndërtesave të vendosura brenda një hapësire të caktuar (site). Këtu bëhet fjalë për distanca deri në 1500 m. Si kabëll përdoren fibrat optike.
- ☑ **Zona e dytë** përshkruan lidhjen midis kateve të ndërtesës, si dhe përfshin kabllin lidhës dhe shpërndarësin respektiv të katit (switch-in). Si kabëll përdoren fibrat optike sipas standardit deri në një gjatësi maksimale prej 500 m.
- ☑ **Zona e tretë** përfshin elementët e kabllimit horizontal të katit (kabli nga shpërndarësi (switch-i) i katit deri tek priza fundore e rrjetit). Si kabëll përdoret Twsted-Pair (deri në 100 m), ose më rrallë fibrat optike.

Zgjidhjet e kabllimeve të strukturuara përcaktohen në Standardin Evropian (EN 50173-1 të vitit 2003) për sistemet e kabllimit të sistemeve të informacionit, neutrale ndaj aplikimeve të ndryshme.

Punimet strukturore në ndërtesë

Detyra më e rëndësishme në metodikën e kryerjes së punimeve strukturore është inspektimi i hapësirave, në të cilat do të kryhen punimet. Jepini vetes kohë të mjaftueshme dhe kontrolloni nga brenda mjedisin, ku do të kryhen punimet strukturore. Kushtojini rëndësi pyetjeve të mëposhtme:

- ☑ A janë të gjitha faqet e mureve të lira apo ka p. sh. dollapë të fiksuar brenda në mur?
- ☑ A mund të kryhen pa probleme çarjet e kërkuara të mureve?
- ☑ Si do të duket vijueshmëria e kalimit të kanelinave (mbajtëseve të kabllove) në hapësirat ku ato mendohet që do të kalojnë?
- ☑ A duhet të kalojë kabli kryesor përmes dhomave të punës (zyrave)?
- ☑ Ku dhe si duhet të kalojë kabli kyesor?
- ☑ A janë pajisur pjesë të ndërtesës me fikse zjarri?
- ☑ A mund të ruhen parametrat e lejuara të kabllit gjatë përthyerjeve, veçanërisht për kabllin LWC?
- ☑ A ka nevojë për punime shtesë (p.sh. në rrjetin elektrik)?
- ☑ A ka ndonjë plan të qartë për mbrojtjen nga goditjet e tensionit?
- ☑ A mund të ketë probleme me mbrojtjen potenciale?
- ☑ A ka kërkesa të veçanta ndaj formës dhe ngjyrës së kanelinave?
- ☑ A duhen kryer çarje shtesë në shkallë?
- ☑ A ruhet gjatësia maksimale prej 100 m e kabllit nga porta e switch-it në portën lidhëse të prizës së rrjetit/ pajisjes?
- ☑ A nevojiten punime shtesë (suvatime, lyerje etj.)?

Qartësojeni paraprakisht periudhën kohore, gjatë të cilës do të kryen punime të zhurmshme, si p.sh. kryerja e shpimeve të vrimave dhe çarja e mureve. Gjatë punimeve duhet të mendoni, që kolegët e tjerë në këto kushte duhet të kryejnë detyra që kanë një afat të përcaktuar. Në një rast të tillë duhet të gjeni mënyrën t'u siguroni kolegëve hapësirë të lirë pune, ose zhvendosje të përkohshme.

Punimet përgatitore

Qëllimi i shtrimit të mundimshëm të kabllove është pajisja e vendeve të punës me mundësinë për lidhje TI-je. Në këtë rast nuk ka rëndësi për cilin shërbim është parashikuar lidhja. Elementët më të rëndësishëm teknikë për kabllimin rregullohen nga përcaktimet e standardeve EN dhe ISO/IEC.

Në rast se na jepet detyra e planifikimit, apo ngritjes nga e para të infrastrukturës së komunikimit të kompanisë, atëhere duhet të veprojmë me një strategji të menduar thellë. Vendimet e nxituara, apo aksionet për t'i mbauar punët brenda natës nuk këshillohen. Në shumicën e rasteve, veprime të tilla pasojnë gjithmonë me kosto më të larta dhe përfundojnë në një kaos rjetesh të pjesshme me pajisje të ndryshme, si dhe me pak, ose aspak mundësi zgjerimi në të ardhmen.

Hapi i parë për kryerjen e një kabllimi është të mendohet, se si do të paraqitej zgjidhja ideale. Në këtë rast është e nevojshme të grumbullohet dhe të vlerësohet i gjithë dokumentacioni i nevojshëm:

- ☑ Siguroni gen-planin e hapësirave ku do kryhen punimet, ose të gjithë ndërtesës.
- ☑ Në qoftë se disa ndërtesa do të lidhen me njëra-tjetrën, kontrolloni kushtet dhe gjendjen në të cilën ndodhen (mundësisht direkt në vend).
- ☑ Përcaktoni, si do të jenë vendet, ku do të bëhen lidhjet dhe cilat shërbime do të nevojiten.
- ☑ Skicojeni zgjidhjen tuaj në formën e një bllokskeme (duke filluar nga pozicioni i shpërndarësit/switch-it).
- ☑ Përcaktoni numrin e vendlidhjeve (p.sh. daljeve të prizave ku do të bëhen lidhjet me pajisjet).
- ☑ Mbani parasysh, ose planifikoni mirë mundësinë e zgjerimit në të ardhmen.

Në çdo rast zgjidhjen e dëshiruar duhet ta hidhni në letër, sidoqoftë ajo, në formë vizatimi teknik, skice, apo në formë të shkruar. Duke menduar se keni përcaktuar zgjidhjen ideale mund të zgjidhni më pas mjetet dhe metodat, me të cilat të arrihet kjo zgjidhje.

Kabllimi me kabllo bakri, ose me fibra optikë

Një vendim shumë i rëndësishëm është zgjedhja midis përdorimit të kabllove të bakrit, apo atyre me fibra optike. Pasi merret ky vendim, duhet të përcaktohen kërkesat specifike në lidhje me cilësinë dhe karakteristikat teknike të tyre.

Për backbone-in që lidhet me serverin, apo për lidhjet e kateve dhe ndërtesave duhen përdorur në çdo rast fibrat optike. Si alternativë, për distanca të shkurtra mes kateve, apo për lidhjen e rack-eve me njëri-tjetrin mund të përdoren edhe kabllot prej bakri. Sidoqoftë, mendoni që me këtë zgjidhje, në rast ndryshimi të teknologjisë, apo të kërkesës për transmetimin e një një fluksi më të madh të dhënash (bottleneck) mund të hasni vështirësi të mëdha përshtatjeje. Tek ky variant duhet që të shtrini kabllo me fibra optike për të garantuar zgjerimin e mëvonshëm. Në këtë rast kostot e përgjithshme rriten, por ekziston gjithmonë mundësia, që pa punime të mëdha shtesë në strukturë, të mund të arrihet një fluks më i madh të dhënash të transmetueshme. Përveç kësaj, reduktohen kostot e investimit gjatë instalimit të parë, si dhe kosto shtesë do të ketë vetëm në rastin, kur backbone-i nuk përmbush më nevojat e kërkuara.

Në instruksionet që jepen për gjatësitë maksimale të kabllove dhe kuotën më të lartë të lejuar të gabimit përcaktohet gjithashtu edhe fluksi maksimal i të dhënave që do të kalojnë në kabëll. Në këtë rast, është njëlloj nëse përdoret kabëll bakri, apo fibra optike. Kabllot me fibra optike duhen përdorur gjithmonë, kur duhen kapërcyer distanca të mëdha, ose në rastet kur kërkohet të transmetohen në mënyrë të sigurtë të dhënat në një mjedis të ndjeshëm ndaj interferencave. Në zonat industriale me makineri që prodhojnë fusha elektrike të fuqishme, apo në zona, të cilat duhet të jenë të sigurta ndaj përgjimit, duhen përdorur kabllot me fibra optike.

Argument, i cili flet qartë në favor të përdorimit të kabllove me fibra optike, është kërkesa për gjerësi bande në vendin e punës. Aplikacionet e dizenjuara në ditët tona, brenda një kohe të shkurtër janë bërë shoqërues të pandarë në vendin e punës. Fotografitë me rezolucion të lartë, aplikacionet multimediale, videot live në chat dhe Internet, si dhe videokonferencat kërkojnë rritje drastike të gjerësisë së bandës.

Meqë kablimi i strukturuar bazuar në kabllot Twisted-Pair përdoret më shpesh, komponentët korrespondues të tij janë mjaft të përhapur dhe relativisht të lirë. Teknika e transmetimit me kabllo bakri është më pak e kushtueshme se ajo me kabllo me fibra optike dhe instalimet mund të kryhen nga firmat e specializuara për këtë qëllim.

Fiber-to-the-Desk

Përparësitë e dukshme të kablimit me fibra optike, kushtet e instalimit dhe teknikat e transmetimit janë të qarta tashmë. Shtrirja e këtyre kabllove deri në vendin e punës varet pak nga kostot. Punët për shtrimin dhe lidhjet janë pak më të shtrenjta se tek kabllot e bakrit. Kostot kryesore bien mbi komponentet aktive si p.sh. tek switchet, apo kartat e rrjetit.

Ndërtesat muzeale

Këto ndërtesa paraqesin shpesh kërkesa të veçanta për pajiset teknike dhe mënyrën si do të instalohen ato. Këtu lind nevoja e këshillimit me një arkitekt, i cili ka pasur përvojë me objekte të tilla. Megjithatë, edhe këtu vlejnë të njëjtat standarde për kablimin, si tek ndërtesat tradicionale.

Hapësira mes ndërtesave

Për lidhjen e ndërtesave me njëra-tjetrën duhet që në çdo rast të zgjidhet fibra optike si kabëll lidhës. Meqë në këtë rast kabli do të kryejë funksionin e backbonit në rrjet, nuk luan ndonjë rol të madh numri i kabllove dhe dendësia e fibrave në kabëll. Sidoqoftë, në qoftë se është e mundur, duhet shtruar edhe një kabëll i dytë me fibra optike (për të siguruar redundancën) edhe sikur ky të mos vihet në punë. Në rastin e një dëmtimi të kabllit të parë, p.sh. gjatë gërmimeve, ekziston gjithmonë mundësia e kalimit në kabllin e dytë dhe vazhdimit normal të punës. Shtrimi i kabllit redundant, sipas mundësive, nuk duhet bërë paralel me kabllin kryesor.

Në parim, gjatë gjithë etapave të planifikimit dhe parapërgatitjes nuk duhet ta humbni lidhjen me praktikën. Përse duhet atëhere një planifikim i mirë kur zbatimi i tij në praktikë ecën me probleme. Një kombinim i katër faktorëve të rëndësishëm, si kostot, koha, cilësia dhe mbrojtja e investimit, do të çojë me siguri në rezultatin e dëshiruar.

17.2 Kërkesat ndaj infrastrukturës

Kërkesa të përgjithshme ndaj infrastrukturës

Për kablimin në zonën e tretë duhet që në plan të vendosen kushte të përcaktuara ndaj infrastrukturës së komunikimit. Gjatë zgjedhjes së prizave dhe patcheve duhet të bazoheni në një prodhues të caktuar. Duhet pasur kujdes që vendi, ku do të porositen këto komponentë, të garantojë furnizim për një kohë të gjatë të tyre dhe kohë të shkurtët lëvrimi. Nuk keni ndonjë avantazh, nëse përdorni një produkt që është me kosto të ulët, por që ofrohet vetëm nga një furnizues (shitës ekskluziv).

Prizat e rrjetit und patchpanel-i

Për prizat e rrjetit dhe patchpanelin për çdo rast vlen, që në gjendjen e instaluar duhen ruajtur karakteristikat e kërkuara sipas EN 50 173 dhe ISO/IEC DIS 11 801.

Përdorimi i sistemeve modulare ka përparësi, pasi lejon që njësinë e informacionit teknik ta përdorësh variabël në vendin e punës. Një ripajisje e mëvonshme mund të kryhet thjesht përmes ndërrimit të elementëve përkatës. Sisteme të tilla kanë si disavantazh kostot e larta.

Kablli i shtruar

Kablli i të dhënave për zonën e tretë duhet të suportojë të gjitha shërbimet e deritashme të përdorura në rrjet. Sipas mundësive përdorni kabëll me karakteristika të larta, edhe në rastet kur shërbimet e nevojshme kërkojnë gjerësi të vogël bande. Kabli i shtruar duhet që për një standard të mëvonshëm, të suportojë gjerësinë maksimale të bandës. Përshtasni me njëra-tjetrën të gjitha kabllot (kabllot lidhëse, patch kabllot dhe kabllot e shtruara) të përdorura në zonën e tretë.

Kontrolloni paraprakisht që distancat e transmetimit të kabllit të shtruar përfshi dhe kabllin lidhës, nuk i kalojnë 100 metrat. Në administratë për të zvogëluar shpërbërjen në rast zjarri, përdoret kabëll pa përbërës halogjeni. Në çdo rast para përdorimit të një kabli kërkoni dokumentacionin me karakteristikat përkatëse të prodhuesit dhe kontrolloni karaktersitikat e kërkuara.

Kjo vlen edhe për kabllot me fibra optike. Këtu para së gjithash duhet pasur kujdes që gjatë shtrimit të kabllit në kthina të ruhen parametrat këndore të përkuljes, si dhe gjendja e tij në tërësi. Kontrolloni që këto kërkesa të mbahen parasysh gjatë shtrimit. Përdorimi i kabllove jashtë ndërtesës varet nga rrugëzimi i përcaktuar i kabllit. Brenda ndërtesës mund të përdoret i ashtuquajturi kabëll universal (përshkrimi A/I). Në rast se kabli kalon përmes hapësirave të bodrumeve, apo magazinave, atëhere duhet të zgjidhet kabëll që përdoret në mjediset jashtë ndërtesës me mbrojtje ndaj lagështirës dhe brejtësve.

Racks

Para përdorimit të rackeve kontrolloni cilat kërkesa janë absolutisht të nevojshme për t'u përmbushur dhe cilat karakteristika mund të neglizhohen. Gjatë përcaktimit të kërkesave që duhet të plotësojë rack-u, mendoni edhe aspektin e sigurisë së të dhënave.

Për racket vlejnë kërkesat që iu përgjigjen pyetjeve të mëposhtme:

- ☑ A është i nevojshëm një kuadër i pjerrët (kuadër i rrotullueshëm)?
- ☑ Si vijnë kabllot në rack (nga lart, poshtë, apo anash)?
- ☑ A duhet të jetë dera e përparme prej xhami (ESG, apo mjafton një derë me llamarinë çeliku)?
- ☑ A mund të hiqen muret anësore?
- ☑ A është e nevojshme një derë e pasme, apo mjafton muri mbështetës?
- ☑ A janë të mbyllshme dera e përparme dhe e pasme?
- ☑ A është e nevojshme që të sigurohen muret anësore ndaj hapjeve të padëshiruara?
- ☑ A nevojitet ndriçim me çelës brenda rack-ut, apo mjafton ndriçimi i dhomës ku është vendosur?
- ☑ A ekziston në rack një numër i mjaftueshëm daljesh për priza korrenti?
- ☑ A kërkohet ventilim shtesë?
- ☑ A duhet vendosur e integruar në rack një UPS për rastet kur mund të ndërpritet energjia elektrike?

Kontrolloni bazuar mbi këto dhe pika të tjera, të cilat i kosideroni të nevojshme, cilat parakushte duhet të plotësojë një rack që të përdoret në kompaninë tuaj. Shqyrtoni gjithashtu mundësinë, nëse ka kuptim, për vendosjen e rack-eve të tjerë, p.sh një për komponentet pasive dhe një për komponentet aktive.

Skiconi në të gjitha rastet si do të jetë i ndërtuar racku juaj duke konsideruar kontrollin për pajisjen dhe rezervat në lidhje me to. Në këtë rast është e rëndësishme dhënia e komponentëve në njësi lartësie (HE). Në qoftë se keni vendosur për komponentë aktivë, ose pasivë, mund t'i përshkruani në skicën tuaj bazuar mbi të dhënat e prodhuesit.

17.3 Shpërndarësit dhe pajisja e vendeve të punës

Vendndodhjet dhe përshkrimi i shpërndarësve

Zona e shpërndarësve paraqet qendrën e kabllimit të strukturuar të ndërtesës. Në të gjenden pajisjet teknike për një rrjet. Atje gjejnë vend si përbërësit aktivë, ashtu edhe ata pasivë të rrjetit. Rack-et, sipas përdorimit ndahen në:

- ☑ Shpërndarës lokalë (SV)
- ☑ Shpërndarës ndërtese (SN)
- ☑ Shpërndarës kati (SK)

Shpërndarësit lokalë

Shpërndarësi lokal, ose i quajtur ndryshe Campus Distributor (CD), është qendra e një firme, respektivisht e ndërtesës, ku është vendosur firma. Shpërndarësi lokal është shpesh dhe në të njëjtën kohë, qendra shpërndarëse e një ndërmarrjeje.

Shpërndarësit e ndërtesës

Shpërndarësi i ndërtesës, ose siç quhet ndryshe Building Distributor (BD) ekzistojnë një herë për ndërtesë. Rekomandohet një kabllim në formë ylli për lidhjen me shpërndarësit e kateve. Për të siguruar një lloj redundance, është e mundur të ndërtohet një strukturë në formë ringu.

Shpërndarësit e katit

Shpërndarësit e katit (quhen ndryshe si Floor Distributors (FD) paraqesin pjesën qendrore të rrjetit brenda një kati. Ata sigurojnë lidhjet brenda katit, apo në pjesë të veçanta të tij. Në varësi të madhësisë së ndërtesës, shpërndarësi i katit mund të jetë edhe shpërndarës ndërtese.

Kërkesat për vendndodhjen e shpërndarësit

Për të bërë zgjedhjen e duhur të vendndodhjes së shpërndarësve duhet të shqyrtohet me saktësi, nëse dhoma e zgjedhur është e përshtatshme për këtë qëllim. Një dhomë e vogël si ajo ku mbahen mjetet e pastrimit, ashtu si dhe një dhomë e madhe me shumë „trafik" hyrje daljesh, nuk janë të përshtatshme. Vendodhja për shpërndarësit duhet të zgjidhet gjithmonë një vend, në të cilin kanë të drejtë hyrjeje vetëm persona të caktuar.
Ky është parakusht i detyrueshën bazuar mbi sigurinë e kërkuar të të dhënave. Krejtësisht të papërshtatshme janë p.sh. dhomat me lagështirë të bodrumeve. Gjatë zgjedhjes së vendodhjes së duhur duhet kërkuar gjithmonë pozicioni sa më në qendër dhe më i leverdisshëm në ndërtesë, me qëllim që rrugët e kalimit të kabllove të mbahen sa më të shkurtra. Edhe pajisjet e dhomës duhet të jenë në përputhje të arsyeshme me funksionin kryesor të saj. Mendoni që në një dhomë të tillë do të mund të kryhen edhe detyra administrative. Në varësi nga rrethanat vendi, ku vendoset shpërndarësi, shërben njëkohësisht si vendndodhje për file-serverin.

Një mjedis ideal ku vendoset shpërndarësi duhet të përmbushë kërkesat e mëposhtme:

- ☑ Të gjitha dyert të mbyllen mirë
- ☑ Temperatura e mjedisit të jetë midis 12° dhe 30°
- ☑ Të ketë lidhje telefonike për suport teknik
- ☑ Ndriçim të mjaftueshëm
- ☑ Furnizim të mjaftueshëm dhe të sigurt me rrymë elektrike (në rastin më të mirë me qarkun e vet)
- ☑ Dalje të mjaftueshme për prizat
- ☑ Vendosje qendrore në kat / ndërtesë
- ☑ I aksesueshëm sipas mundësive nga të tre anët (edhe nga dy anë mjafton)

Prizat lidhëse në vendin e punës

Në vendin e punës duhen përdorur priza të veshura (shielded) me mbrojtje ndaj interferencave me ndërfaqe RJ45. Përdorni priza me dy dalje, edhe nëse medohet paraprakisht se një dalje është e mjaftueshme. Gjatë zgjerimit të mëvonshëm të rrjetit mund të lindë nevoja e përdorimit të daljes së dytë të prizës, gjë që mund të bëhet pa qenë e nevojshme të çmontohet paraprakisht. Ndryshimi i çmimit midis prizave lidhëse me 1 dhe me 2 dalje nuk është domethënës. Prizat duhen instaluar në mënyrë të tillë, që të plotësojnë karakteristikat e kërkuara sipas standardeve.

Vendndodhja e prizave lidhëse duhet zgjedhur në mënyrë të tillë, që të jetë sa më pranë vendit të punës. Në këtë mënyrë shmangni rastet e pengimit nga rrëmuja e panevojshme e kabllove në ambjentet e zyrave. Për çdo vend pune duhet të planifikoni gjithmonë minimumi tri mundësi lidhjeje: një për telefonin, një për të dhënat dhe një tjetër si rezervë, ose për një lidhje tjetër të dhënash (për të lidhur p.sh. një printer rrjeti). Edhe nëse lidhjet telefonike kalojnë për momentin nëpërmjet një rruge tjetër nga ato të të dhënave, në rast të një infrastrukture të re komunikimi, duhet

marrë në konsideratë transferimi i tyre i mëvonshëm dhe përfshirja në shtrirjen dhe lidhjet e rrjetit të të dhënave.

Merrni në konsideratë, që në vendin e punës të ketë mjaftueshëm dalje për lidhjet me rrymën elektrike, apo zgjatues për këtë qëllim. Në rast se nuk është kështu, atëhere duhen marrë masa për sigurimin e tyre. Gjithashtu, duhet siguruar që prizat e furnizimit me rrymë të jenë sa me afër të jetë e mundur me vendin e punës.

Mbrojtja nga goditjet e tensionit të lartë

Një nga shkaqet që ndeshet shumë shpesh (mbi çerekun e rasteve) për rënien e një rrjeti, janë dëmtimet si pasojë e goditjeve të tensionit, që vjen mbi normat e lejuara. Këto goditje shkaktojnë jo vetëm dëme me kosto të larta që lidhen me riparimin dhe blerjen e pajisjeve zëvendësuese, por edhe – sipas rëndësisë dhe rrethanave– një rënie drastike të mundësisë së shfrytëzimit të infrastrukturës. Problemet më të rëndësishme gjatë goditjeve të tensionit të lartë krijohen përmes:

- ☑ Goditjeve direkte dhe indirekte nga rrufeja
- ☑ Proceseve të kyçjes dhe ç'kycjes së rrymës në rrjetin elektrik
- ☑ Shkarkesave për shkak të elektricitetit statik
- ☑ Probleme me linjat e tensionit
- ☑ Probleme me tensionin e lartë në rrjetin elektrik shkaktuar nga furnizuesi me energji i firmës

Gjatë planifikimit të infrastrukturës së komunikimit duhen zbatuar edhe masat ndaj goditjeve të tensionit. Këto masa mund të shtrihen që nga zgjedhja e rrugëkalimeve të kabllove, larg nga burimet e mundshme të interferencave, deri në lidhjen e komponentëve specialë të mbrojtjes nga interferencat.

Standardet sipas DIN VDE

Për planifikimin dhe ngritjen e struktutave të mbrojtjes nga rrufetë duhen pasur parasysh përcaktimet e VDE-sipas DIN VDE 0185 pjesa 1 dhe pjesa 2. Krahas gjendjes teknike aktuale rekomandohet zbatimi i standardeve evropiane ENV në këtë fushë (ENV 61024-1). Përmbajtja e këtij standardi ka të bëjë me mbrojtjen kundër zjarrit (vetëtimë shoqëruar me flakë), mbrojtjen ndaj dëmtimeve mekanike (vetëtimë e pashoqëruar me flakë), ashtu si edhe mbrojtjen e instalimeve elektrike brenda ndërtesave.

Në standardin DIN VDE 0185, pjesa 103, përshkruhen veçanërisht masat për mbrojtjen ndaj rrufeve të ndërtesave me shumë pajisje elektronike brenda.

Një mbrojtje e plotë nga goditjet e rrufesë jepet sipas standardit DIN VDE 0185, që përshkruan një mbrojtje të jashtme dhe të brendshme. Të dyja plotësojnë njëra-tjetrën për të siguruar një mbrojtje të plotë dhe nuk duhen parë asnjëherë si të ndara nga njëra-tjetra. Të gjitha pjesët e standardit, që devijojnë rrymën e rrufesë, i përkasin zonës së jashtme të mbrojtjes. Mbrojtja e jashtme siguron që në rast goditjeje, rrufeja të shkarkohet pa rrezik në tokë.

17.4 Dokumentimi

Bazat e dokumentimit

Krijimin e dokumentacionit për infrastrukturën e komunikimit duhet ta filloni që gjatë kryerjes së punimeve. Dokumentacioni është veçanërisht i rëndësishëm, në qoftë se do të duhen të planifikohen zgjerime në të ardhmen të rrjetit, ose në rastin, kur fillon punë një koleg i ri. Në një vështrim të përgjithshëm, infrastruktura e komunikimit mund t'u jepte p.sh një informacion të shpejtë në lidhje me gjendjen e prizave të lira, apo të zëna në rrjet. Kryesisht i gjithë dokumentacioni i rrjetit mbahet në një dosje të vetme. Ndajeni dosjen në nëndosje me rubrikat përkatëse, si p.sh. nëndosja e komponentëve aktiv.

Në një dokumentacion të përgjithshëm në çdo rast bëjnë pjesë:

- ☑ Skicat/vizatimet e ndërtimit të rrjetit
- ☑ Planet përmbledhëse
- ☑ Mbulimet me panele lidhëse dhe daljet e prizave për lidhje
- ☑ Protokollet e matjes së linjave prej bakri dhe fibrash optike
- ☑ Indeksi i prodhuesve në rast zgjerimi të mëtejshëm
- ☑ Komponentët aktivë të rrjetit

Skicat e ndërtimit të rrjetit

Skicat e ndërtimit të rrjetit duhet të përmbajnë të gjithë komponentët aktivë dhe pasivë të instaluar me të dhëna mbi njësitë e lartësive të pajisjeve. Nëpërmjet tyre jeni në gjendje të merrni menjëherë informacion për rezervat ekzistuese në rrjet. Skicat e ndërtimit të rrjetit shërbejnë si një bazë e mirë diskutimi edhe për mundësitë e zgjerimit të rrjetit në të ardhmen. Skicat për shpërndarësit/racks duhet të përmbajnë informacionin e mëposhtëm:

- ☑ Të dhëna mbi vendndodhjen e shpërndarësve (lloji, kati, dhoma, shfrytëzimi)
- ☑ Të dhëna mbi madhësinë nëpërmjet njësive të lartësisë (Rack Units)
- ☑ Përshkrimi i shpërndarësve/racks
- ☑ Ndarja e paneleve që bëjnë lidhjet me kabllo bakri, fibra optike dhe komponentëve aktiv
- ☑ Këshilla për ndriçimin dhe ventilimin e rack-eve
- ☑ Numri i daljeve të prizave të rrjetit
- ☑ Numri i portave – kabëll për panel

Planet përmbledhëse

Këto shërbejnë për të patur një pasqyrë të plotë në lidhje me infrastrukturën e rrjetit. Planet përmbledhëse paraqiten në formën e bllok-skemave, ose japin rrugët e kabllimit. Ato nuk japin asnjë informacion në lidhje me rezervat ekzistuese. Shpesh ka kuptim, që planet përmbledhëse për komponentet aktiv të krijohen dhe të mbahen të ndara nga ato të komponenteve pasiv të rrjetit. Bllok-skema të tilla mund të përdoren gjithashtu, për të paraqitur një rrjet në fazën e planifikimit.

Mbulimi me panele lidhëse

Plani i mbulimit me panele lidhëse përmbaë numrat në vazhdim të paneleve (kabllove prej bakri, fibra optike), po ashtu dhe klasifikimin sipas numrit të dhomës dhe katit të kabllove të veçanta. Plani i mbulimit me panele ndihmon veçanërisht gjatë punës, ose në rast kërkimi të defektit. Lidhja me defekt merret në shqyrtim dhe mund të identifikohet shpejt, në cilin kat dhe në cilën dhomë gjendet priza lidhëse respektive.

Protokollet e matjes

Sipas shtrirjes dhe numrit të lidhjeve në rrjet, mund të ndodhë që të kemi deri në 100, ose më shumë protokolle matjesh për portat. Në një rast të tillë këshillohet, që protokollet e matjeve t'i memorizoni në një mbartës të dhënash (p.sh. CD-ROM), i cili më pas skedohet në dosjen e auditit.
Të gjitha lidhjet e rrjetit duhen testuar. Edhe në një rrjet me topologji yll, sidomos në ato me shumë lidhje, kërkimi i defektit harxhon kohë dhe energji. Elementët e mëposhtëm janë ato që zakonisht kontrollohen:

- ☑ Regjistrimi i rradhës së matjeve
- ☑ Gjatësia e kabllit
- ☑ Humbja/dobësimi i sinjalit
- ☑ Rezervimi i PIN-it
- ☑ Rezistenca-DC

Gjatë problemeve që lindin me gjatësitë mbi 90 m të kabllove, regjistrimi korrespondues i protokollit të matjes duhet bërë me ngjyrë. Edhe në rastet, kur është bërë një planifikim i mirë dhe vlerësim i mirë i gjatësive të kabllove, mund të ndodhë gjithmonë një herë që të bëhen ndryshime gjatë punës. Shumica e shërbimeve mundet të punojnë pa probleme, edhe në rastin e kabllove me gjatësi 100 m, në rast se është bërë një shtrim dhe lidhje e mirë e kabllit. Kujdesuni që caktimet e emrave të protokolleve të matjeve, sipas numrave të dhomave ku janë kryer, të jenë të qarta për t'u kuptuar dhe të përçojnë informacion.

Indeksi i prodhuesve

Indeksi i prodhuesve përmban të gjitha të dhënat përkatëse për produktet, si dhe për prodhuesit dhe lëvruesit e këtyre produkteve. Gjatë zgjerimit të mëvonshëm, ose ndyshimeve të infrastrukturës së rrjetit regjistrimet e tij ndihmojnë jashtëzakonisht, pasi aty merret menjëherë informacioni i nevojshëm për porositë që duhen kryer. Regjistriml i indeksit të prodhuesve bëhët në mënyrë tabelare dhe plotësohet në vazhdimësi. Në qoftë se përdorni një prodhues, apo produkt të ri në rrjet, atëhere duhet patjetër të hidhni të dhënat e tij në regjistrin përkatës të indeksit të prodhuesve.

Në indeksin e prodhuesve duhen listuar të dhënat e mëposhtme:

- ☑ Emri dhe adresa e prodhuesit/lëvruesit
- ☑ Numri origjinal i prodhimit dhe përshkrimi i artikujve të komponentëve
- ☑ Të dhënat e prodhuesit dhe të dhënat dokumentare për kabllin e përdorur (prej bakri, fibrash optike, etj.)
- ☑ Të dhëna mbi ngjyrat e njësive lidhëse (p.sh. RAL9010 për të bardhën)

Dokumentimi i komponentëve aktivë të rrjetit

Dokumentacionet e përfshira në kompnentët aktivë përshkruajnë thjesht mënyrën e funksionimit të pajisjeve dhe përmbajnë karakteristikat teknike të komponenteve përkatës. Tek këto dokumeta nuk gjenden informacione për këto pajisje në lidhje me të dhëna specifike të klientëve. Këto dokumentacione, sidoqoftë, duhen kërkuar për shërbime mirëmbajtjeje të mëvonshme, si dhe defekte, apo identifikim të problemeve.

Dokumentacioni specifik për komponentët aktivë të rrjetit duhet të mbahet në mënyrë të ngjashme si një regjistër i indeksit të prodhuesve. Listoni në mënyrë tabelare të gjitha pajisjet, dhe në njërën nga kolonat e tabelës regjistroni vendndodhjen e pajisjes. Konsiderojeni dokumentacionin specifik të komponentëve aktivë të rrjetit si një lloj liste inventari, të cilin ju si përgjegjës për rrjetin duhet ta krijoni dhe të kujdeseni për të. Duhet të mbani parasysh të përfshini në listë të dhënat e mëposhtme:

- ☑ Vendodhjen e pajisjeve, të dhëna mbi ndërtesën, katin dhe numrin e dhomës
- ☑ Adresat e IP-së së komponentëve (në rast se disponohen) (edhe tek përshtatësit SNMP)
- ☑ Numrat e serisë së prodhimit të pajisjes
- ☑ Përshkrimin e saktë të prodhuesit të pajisjes (i rëndësishëm në rast se do të kërkohet ndër të tjera blerja e pjesëve të këmbimit)
- ☑ Llojin dhe mënyrën e funksionimit të pajisjes (p. sh. switch me 24-Porta me dy vende modulare për shtesa)
- ☑ Adresa MAC e pajisjes (në rast se disponohet)
- ☑ Numrat e njëpasnjëshëm tek etiketa brenda pajisjes (Switch 24P_EG_R251)

Shumë komponentë aktivë ofrojnë mundësinë, nëpërmjet protokollit IP, të administrohen me anë të Telnet-it. Tek këto komponentë aktiv mund të hidhen nëpërmjet menusë përkatëse të dhënat e mëposhtme:

- ☑ System-Name (emri i pajisjes)
- ☑ Vendndodhja
- ☑ Personi i kontaktit (Emri i administratorit)
- ☑ Përshkrimi i pajisjes

Këto informacione janë shumë të nevojshme dhe ndihmëse në rastin kur kërkohet një defekt, meqë nëpërmjet tyre del qartë, nëse bëhet fjalë për pajisjen e kërkuar që ndodhet në një segment rrjeti / switch të caktuar.

1

5

8

A

B

C

D

E

F

G

H

I

K

L

S

T

U

V

W

X

Y

Z