Agjencia Kombëtare e Arsimit, Formimit Profesional dhe Kualifikimeve
Sektori i Skeletkurrikulave dhe Standardeve të Trajnimit të Mësuesve në AFP

MATERIAL MESIMOR

Në mbështetje të mësuesve të prolifit mësimor

"RIPARIME TË PAJISJEVE ELEKTRONIKE"

Niveli IV i KSHK

NR. 13

Ky material mësimor i referohet:

- **Lëndës profesionale: "Rrjetet e komunikimit", kl.12 (L-12-526-20)**
- **Temave mësimore:**

1. **Tipologjitë e rrjeteve të komunikimit**
2. **Pajisjet e rrjetit**
3. **Konektorët**
4. **Mjediset e transmetimit në rrjetet e komunikimit**
5. **Rrjeti me fibra optike**
6. **Rrjeti Ethernet LAN**
7. **Standardet e ndërfaqeve dhe pajisjet**
8. **Rrjetet e komunikimeve industriale**
9. **Sistemet periferike HMI, GUI**
10. **Të dhënat, magazinimi, kartat e komunikimit, Back-up, Restore**
11. **Siguria e rrjeteve të komunikimit**

E përgatitën:

Jonida Haxhi
Besa Marku
Besmir Kanushi

Tiranë, 2020

Tema 1. Tipologjitë e rrjeteve të komunikimit

Në shek 20 modeli i një kompjuteri të vetëm që i shërbente të gjithë nevojave kompjuterike të organizatës është zëvendësuar me një të vetëm në të cilin një numër i madh por të ndërlidhur kompjutrash që e bëjnë këtë punë.
Këto sisteme quhen rrjete kompjuterike = koleksion i kompjutrave autonom të ndërlidhur me një teknologji të vetme.
Dy kompjutra thuhet se janë të ndërlidhur kur ata janë në gjendje të shkëmbejnë informacion. As interneti dhe as www. nuk jane rrjet kompjutrash. Interneti eshte rrjet rrjetash ndersa ëëë eshte nje sistem shperndares, i cili eshte nje koleksion i kompjutrave indipendent qe i shfaqen perdoruesit si nje sistem i vetem koherent, ka nje model te vetin i cili implementohen nga nje shtrese softëeri ne maje te sistemit operativ e quajtur middleëare. Ngjashmeria qendron ne ate qe si rrjeti kompjuterik ashtu edhe sistemi shperndares sherbejne per te levizur files ndryshimi qendron ne ate qe kush e provokon sistemi apo perdoruesi. Ekzistojnë këto tipe rrjetesh kompjuterike sipas shtrirjes gjeografike:

LAN-Local Area Network
Një LAN dallohet nga dy karakteristika bazë: Shtrirja e tij gjeografike është e kufizuar, dhe kjo shtrirje nuk e kalon kufirin e sipërfaqes ku është vendosur firma. I gjithë hardëare-i gjendet plotësisht në zonën e juridiksionit dhe nën mbikqyrjen e një përdoruesi, respektivisht një firme. Në rrjetet lokale transferimi i të dhënave kryhet në shumicën e rasteve përmes kabllit. Karta e rrjetit administron transferimin e të dhënave nga kompjuteri në kabëll dhe anasjelltas. Çdo kartë rrjeti ka një numer (adresë), i cili është unik dhe i pandryshueshëm në të gjithe botën dhe quhet adresa MAC(**media access control**). Adresa MAC (angl. MAC-Address) shërben për identifikimin e qartë të stacionit të punës brenda rrjetit.

WLAN-Wireless Local Area Network
Wireless Local Area Network (rrjeti lokal pa kabell) është nje 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 i cili përdoret mjaft kohët e fundit për transferimin e të dhënave (në një zonë rrethuese afro 10 metra), është Bluetooth-i.

MAN - Metropolitan Area Network
Shtrirja e MAN-it kufizohet në hapësirën e një qyteti ose një qendre industriale dhe përfshin largësi 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. Ne formën e tij klasike ai shërbente për lidhjen e pajisjeve kompjuterike në distanca të largeta. Të dhënat, në shumicën e rasteve, transferohen në linjat publike, për shfrytëzimin e të cilave ka tarifa të caktuara. Firmat mund ta shfrytëzojnë WAN-in si lidhje ndërmjet 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 largesitë ndermjet kompjuterave që komunikojnë mund t'i kalojnë mijëra kilometrat.. Të dhënat kalojne 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.

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

Topologjitë fizike
Topologjia fizike e një rrjeti lidhet me rrugët e trafikut. Këtu do të përshkruhet, me fjalë të tjera, ndërtimi fizik i një rrjeti, pra në cilën strukturë janë lidhur me njëri tjetrin komponentet individuale 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 pa kabëll. Topologjia fizike është e krahasueshme me një hartë, në të cilën janë shënuar rrugët e trafikut. Format bazë më të rëndësishme të topologjive fizike janë bus, star(yll), ring (Unazë)

Topologjia logjike e një rrjeti përshkruan rregullat bazë të trafikur të cilat vlejnë në rrugët e trafikut. Këtu bëhet fjalë ndër të tjera edhe se kush ka të drejtë të aksesojë mediumin e transmetimit.
Në praktikë ekziston një varësi e ngushtë midis dy termave, kështu që në një rast normal një topologji fizike e caktuar sjell me vete një topologji logjike të caktuar. Topologjitë fizike dhe logjike nuk duhet të jenë identike me njëra-tjetrën.
Gjithësesi 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 përdoretapo sa elastik është rrjeti në rast se del nevoja e zgjerimit me përdorues të tjerë. Përvec kësaj, me zgjedhjen e topologjisë lidhen ngushtë dhe varen aspekte si siguria dhe defektet, shpejtësia e komunikimit, gjerësia e bandës në dispozicion,pa ngelizuar kostot përkatëse që lidhen me aplikimin e topologjisë së zgjedhur.

Topologjia Bus
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 (sga-red media). Topologjia bus citohet edhe si rrjet pajisjesh në një linjë/rradhë.
Topologjia bus është pasive gjë që do të thotë se kompjuterat e lidhur në këtë rrjet nuk e rishpërndajnë sinjalin më tek. Ato kapin sinjalet që vijnë përmes kabllit, ose dërgojnë sinjale në kabëll, sinjale të cilat përhapen në të dyja drejtimet. Këtu flitet për një rrjet difuziv. Në rrugën përgjat kabllit sinjalet humbin dhe/ose dobësohen, kështy që gjatësia e busit është e kufizuar. Nëpërmjet përdorimit të përforcuesve të sinjalit (repeater-at) mundësohet që gjatësia e lejuar të shtrihet më tej.
Përparësitë e topogjisë bus janë:

1. Kosto relativisht të ulta, meqë nevojitet pak kabëll për të bërë lidhjen
2. Mosfunksionimi i një kompjuteri nuk shkakton probleme në rrjet.

Disavantazhet e topologjisë bus janë:

1. Të gjithë të dhënat transferohen nëpërmjet një kablli të vetëm
2. 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.
3. Një interferencë, në një vend të caktuar të bus-it, në mediumin e transmetimit (kabëll me defekt, lidhje e lirë tek bashkuesit, bashkuesit, kompjuteri është konfiguruar gabim) bllokon të gjithë rrjetin dhe con në një proces të mundimshëm për gjetjen e defektit

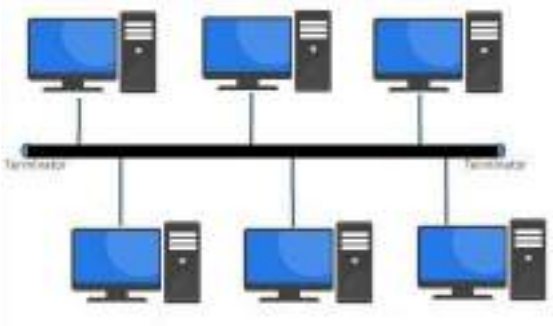


Figura 1.1. Topologjia bus

Topologjia Ring

Në topologjinë ring kabllot e përdorura formojnë një formë të mbyllur unaze. Nuk ka fillim apo fund kablli. Të gjitha stacionet e punës lidhen në "unazë", si elemente të cilat përpunojnë dhe përforcojnë sinjalet që kalojnë në kabëll dhe i dërgojnë ato më tej. Këtu qëndron dhe disavantazhi më i madh, pasi defekti i një kompjuteri, apo i një pjesë kablli 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 ka një pararendës dhe një pasardhës. Trafiku i të dhënave kryhet vetëm në një drejtim. Kjo topologji fizike ndeshet rrallë në rrjetet e sotme locale, meqë kostot e shtrirjes së kabllit janë relativisht të larta.

Fugura 1.2. Topologjia ring

Topologjia Star

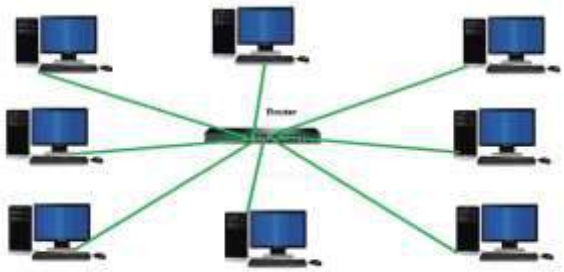
Në topologjinë star secili kompjuter lidhet me shpërndarësin qëndror mëpërmjet një kablli. Ekziston pra, një lidhje kokë më kokë (poin to point) midis shpërndarësit qëndor dhe pajisjes të lidhur veças në të. Shpërndarësi qëndor përgjithësisht përcaktohet si hub. Përcaktime të tjera për të si përqëndrues kabllosh, apo shpërndarës në formë ylli, thjesht qartësojnë se detyra bazë e kësaj pajisje është vënia në dispozicion e një pajisjeje qendrore me shumë mundësi lidhjeje për pajisjet e tjera.

Përparësitë e topologjisë star:

1. Mosfunksionimi i një stacioni pune ose i një kablli nuk ka asnjë ndikimi në pjesën tjetër të rrjetit.
2. Shpërndarësit aktiv funksionojnë njëkohësisht edhe si përforcues sinjali.
3. Gjatë një mënyre funksionimi të caktuar të shpërndarësit, dy stacione pune mund të shfrytëzojnë për komunikim 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.
4. Stacione të tjera pune dhe/ose shpërndarës të tjerë mund të lidhen pa problem më pas.

Disavantazhet e topologjisë star

1. Kërkon përdorimin e një sasie të madhe kablli
2. Mosfunksionimi i shpërndarësit nxjerr jashtë loje të gjithë rrjetin, pra nuk ka më trafik të dhënash



Fugura 1.3. Topologjia star

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. si në rastin kur rrjete (apo pjesë rrjetesh) egzistuese bashkohen së bashku në ndërtimin e backbon-it

Backbone
Me backbone kuptohet lidhja fizike e shumë rrjeteve me njëri-tjetrin. Bëhet fjalë për një rrjet më 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 një kabëll bus.
Po japim një shembull të thjeshtë për ta qartësuar si ide. Në një ndërtesë trekatëshe, cdo kat është lidhur duke përdorur topologjinë star. Të treja katet ose më saktë hub-et, lidhen me njëri-tjetrin përmes një kablli bus. Nëse 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 përmesnjë 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 tre katëshe me zyra, secili kat është lidhur në rrjet me kabëll duke përdorur topologjinë star. Të treja katet, dmth hub-et lidhen me njëri-tjetrin përmes një kablli me një hub qëndror.
Në rast të mosfunksionimit të hub-it qëndror, komunikimi brenda çdo kati është ende i mundur. Për arsye sigurie hub-i qëndror mund të jetë rendundant (i dubluar), gjë që do të thotë se një hub i dytë qëndron në stand by modus dhe futet menjëherë në punë në rast mosfunksionimi të të parit. Në rast se kablli që kalon nga hub-i qëndror tek njëri nga hub-et e kateve ka defekt, atëherë ky kat nuk do të jetë në gjendje të komunikojë me katet e tjera.

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

Rrjeti Mesh
Në një rrjet mesh ekzistojnë shumë nyja nëpërmjet nyjave individuale të rrjetit. 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 në rrjetet WAN. Më tej mund të dallojmë nëse linjat rezerve që do të përdoren janë aktive (load sharing, me ndarje të ngarkesës), apo pasive (standby).

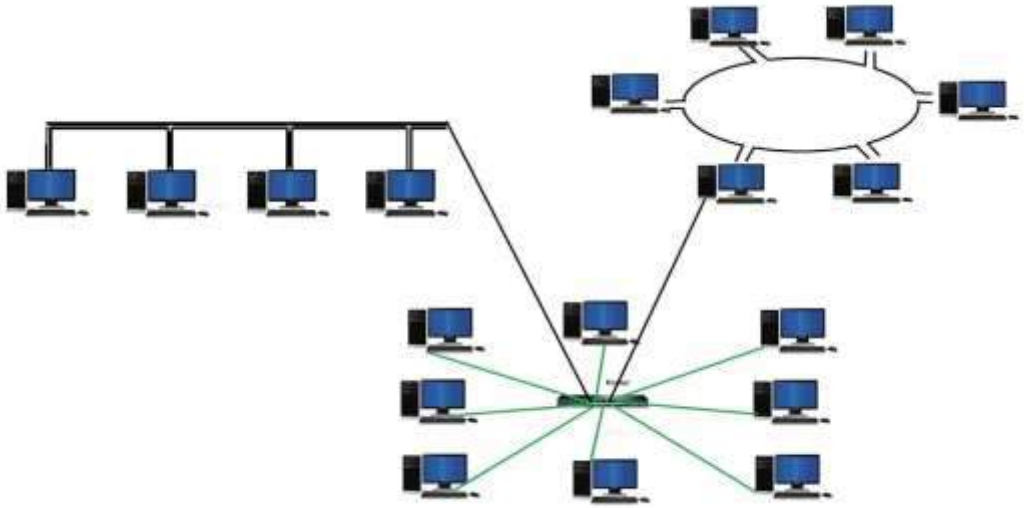


Figura 1.4. Një formë mikse

Tema 2. Pajisjet e rrjetit

Përbërësit aktivë të rrjetit shërbejnë për të lidhur rrjetet kompjuterike me njeri tjetrin ose për të kapërcyer kufizimet e gjatësisë së mediave lidhëse. Pjesërisht, ato kontribojnë në lidhjen e rrjeteve që përdorin media transmetimi, protokolle, apo shpejtësi transmetimi të ndryshme. Nëpërmjet përdorimit të përbërësve aktiv të rrjetit, mund të rritet fluksi i transmetimit të të dhënave në rrjet.

Hub-i
Një Hub shpesh përshkruhet si përqëndrues kabllosh ose si shpërndarës yll, pasi ai përdoret si qendra e një rrjeti. Hub-et janë në gjendje të lidhin me njeri tjetrin topologji të ndryshme rrjeti. 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. Hub-et, parimisht, janë të ndërtuara në mënyrë të ngjashme me topologjinë bus, në të cilën e gjithë gjërësia e bandës ndahet midis pjesmarrësve të lidhur në rrjet. Në një rrjet 10 Mbits me 10 pjesmarrës, cdo pjesmarrësi i takon një gjerësi bande teorike prej 1 Mbit, dhe nëse bëhen 20 pjesmarrës 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 të cilës ndodh shkëmbimi i të dhënave në rrjet rritet. Rastet në të cilat mund të përdoret një hub janë:
1.Në rastin kur duhen lidhur 4-8 stacione pune për një periudhë të shkurtër (psh provizorisht gjatë rinovimit të zyrës)
2.Në rast kur duhet lidhur grupi i punës i cili punon në një segment me tipologji bus(lidhje bnc) me grupin e punës që punon me tipologjinë yll (star)
3.Në rast se ngrihet një rrjet për qëllime demonstrimi.

Sot hub-et janë zëvendësuar gjerësisht nga Switch-et.

Figura 2.1 Hub

Repeater-i (rigjeneruesi i sinjalit)
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.

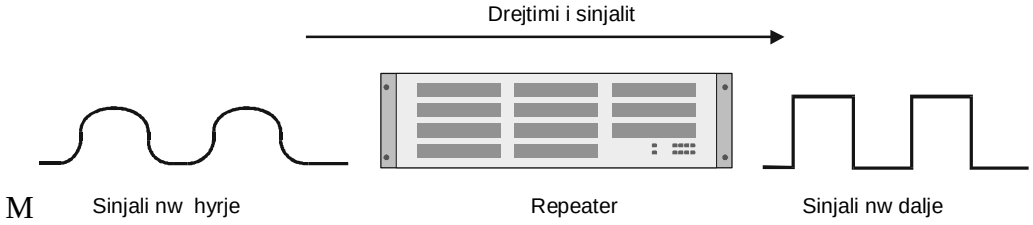


Figura 2.2 Rigjenerimi i sinjalit përmes një repeater-I

Figura 2.3 Repeater

Veçoritë rigjeneruese të repeaters-ave kanë përparësi, pasi sinjalet difektoze nuk i përçojnë tek segmenti tjetër.

Switch-i
Switchet punojnë në shtresën 2 (Data Link Layer) të modelit OSI. Switchi memorizon MAC adresat 48 Bit të gjata të kompjuterave të lidhura në të dhe të portave përkatëse në SAT (angl. 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 përcon 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).

Kriteret që duhen patur parasysh gjatë blerjes
Në qoftë se do të blini një Switch, duhen marrë parasysh faktorët e mëposhtëm:

1. Numri i portave

2. I menaxhueshëm ose jo
3. Standalone Switch
4. Half-duplex- dhe/ose Full-duplex
5. 10/100 Mbit ose 10/100/1000 Mbit
6. Layer-2- ose Layer-3-Switch
7. Mundëson VLAN (LAN-e virtuale)
8. Kryen agregim portash

Figura 2.4 Switch-e

Bridge-t (Urat)

Me ndihmën e brixheve (urave) krijohet mundësia e zgjerimit më tej të 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 brixhi rrjeti ndahet në dy subnete.

Meqë paketat me të dhëna të brixhit, të cilat i takojnë rrjetit të vet, nuk transferohen më tej, atëhere ngarkesa lokale e rrjetit zvoglohet ndjeshëm. Brixhi lexon paraprakisht kokën (header-in) e paketës dhe më pas krahason informacionet e adresës së burimit dhe destinacionit në një tabelë adresash. Në rast se adresa përkatëse gjendet në tabelë, atëhere paketa dërgohet më tej tek kjo adresë. Në të kundërt 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 dergimi i broadcast-eve kufizohet. Për krijimin dhe mbarëvajtjen e këtyre tabelave të adresave egzistojnë dy mundësi bazë:

1. Tabela adresash statike
2. Tabela adresash dinamike

Sipas fushës së përdorimit urat (bridges) ndahen në:

1. Ura lokale (local bridge)
2. Ura në largësi (remote bridge)
3. 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 gjëndje të lidhin rrjete të llojeve të ndryshme.

Figura 2.5. Bridge

Router-i

Routerat janë përbërës aktivë 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, 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 (Fiber Distributed Data Interface).
Dallojme llojet e mëposhtme të routerave:

1. Router me një protokoll
2. Router multiprotokoll
3. Router hibrid

Figura 2.6 Router

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

1. High Performance Router
2. Gigabit-Router
3. Enterprise-Router
4. Access-Router
5. 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 routerat SoHo realizohen më së shumti lidhjet në Internet apo ndërmjet degëve. Access-routerat shërbejnë si një administrim qendror, nëpërmjet të cilit degët lidhen me njëra tjetrën. Këto lloj routerash janë modularë dhe mund të pajisen sipas nevojës me modulet përkatëse (ISDN, S2M, ATM, etj.).

Gateway

Me Gateway kuptohet një sistem, me anë të të cilit rrjete të ndryshme lidhen me njëri tjetrin, ose u bashkohen rrjeteve të tjera nëpërmjet konvertimit të protokollit. Për arsye, 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.

Konvertuesit e Mediave

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 optikë. 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 te 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.

Konvertuesit e mediave transformojnë sinjalet elektrike të një medie në sinjalet 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 se konvertimi është i mundur vetëm midis dy mediave p.sh. TP në FOC dhe se konvertuesit e mediave nuk mbështesin autosensing.

Figura 2.7. Pamje e një konvertuesi mediash

Kartat e rrjetit

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 dallojmë elementët lidhës të mëposhtëm:

1. Dalje 15-inch Sub-D për lidhjen AUI
2. Portë RJ-45 për lidhjen në një rrjet 10BaseT- 100BaseT, ose 1000BasrT
3. Dalje BNC për rrjet 10Base2
4. Dalje ST- ose SC për rrjetet me fibra optike (10BaseFL, 100BaseFX, ose 1000BaseFX)

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:

1. 1000BASE-TX Half / Full duplex
2. 100BASE-TX Half / Full duplex
3. 10BASE-T Half / Full duplex

Çdo pajisje në një rrjet identifikohet nga një adresë unike, e quajtur shpesh si hardëare address, MAC address, physical address, device address, adapter address, ose node address.Çdo kartë rrjeti (NIC card) ka një adresë 48-bit Adresat MAC shkruhen duke perdorur numra hexadecimale (me bazë 16).

Dallohen dy formate adresash: MAC 00.00.0c.12.34.56 ose 00-00-0c-12-34-56.

Figura 2.8. Kartë rrjeti

Tema 3: Konektorët

Kur i referoheni kabllove, konektori është lidhësi fundit të kabllos në një port. Për shembull, fundi i një kablloje ka një konektor USB që e lejon atë të lidhet me një portë USB. Të gjitha kabllot kanë konektorët e tyre të cilat përdoren në varësi të kërkesave. Konektorët shkaktojnë një shuarje të fuqisë së sinjalit gjatë transmetimit. Ka një tërësi pajisjesh që përdoren për kabllimin dhe për vendos e konektorëve korrekt në fund të kabllove.

RJ45 është konektori më i zakonshëm. Ai është konektor me 8 pine dhe përdoret për të lidhur kompjuterat dhe pajisjet e rrjetit në një rrjet LAN. Ai përdoret për ciftet e përdredhura.

Bashkuesi UTP përdoret për të zgjatur rrjetin. Ky bashkues lidh dy konktor RJ45

Figura 3.1. Bashkues UTP

RJ48 është një konektor i ngjashëm me RJ45 por ai përdoret për kabllot STP

RJ11 është konektori që përdoret për të lidhur pajisjen e telefonit. Konektori RJ11 përdoret gjithashtu për të lidhur kompjuterat me anë të kartës NIC me modemin.

BNC është konektor që përdoret për kabllot koaksial. Ai përdoret për të transmetuar video dhe audio analoge dhe dixhitale. Ka shumë lloje të konektorëve BNC, si BNC T që shërbejnë për lidhjen e tre kabllove koaksial me njëri tjetrin, bashkuesit BNC që përdoret për të lidhur dy kabllo koaksial dhe BNC terminator (fundor) që vendoset në fundin e kabllos
Konektori i tipit F përdoret për kabllot koaksial. Ata përdoren nga ofruesit e kabllove që të lidhen me modemin kabllor. Këto konektor përdoren gjithashtu edhe për internetin satelitor.
Konketori USB përdoret për kompjuterat dhe laptopët. Këta konektor kanë një fushë të gjerë përdorimi psh një usb adapter mund ti jap kompjuterit akses në Wireless.
Me një USB ethernet adapter (përshtatës) mund të lidhet kompjuteri me një kabllo twistet pair me RJ45 për të patur akses në internet nëpërmjet një porte usb.
Ka disa lloje konektorësh për fibrën optike. Ata ndryshojnë nga madhësia dhe mënyra e kabllimit.
Konektori SC (Standard connector) është konektori i parë i përdorur. Ai është konektor push pull (femër mashkull) si konektorët e audios dhe videos
Konektori MTRJ është një lidhës kabllor për fibra optike që është shumë i popullarizuar për pajisjet me faktor të formës së vogël për shkak të madhësisë së tij të vogël. Vendosja e dy fibrave dhe bashkimi së bashku me kunjat e vendosjes në prizë, MT-RJ vjen nga lidhësi MT, i cili mund të përmbajë deri në 12 fibra.

Figura 3.2 Konektor MT

Konektori ST janë konektorët më të përdorur për fibra optike në aplikimet e rrjeteve. Ato janë cilindrike me bashkim bllokues rrotullues me diametër 2.5 mm. Lidhësit ST përdoren si aplikacione në distancë të shkurtër ashtu edhe në sisteme me shtrirje të madhe gjeografike. Konektori ST ka një montim në bërthamë dhe një unazë cilindrike të gjatë për të mbajtur fibrën. Ata futen dhe hiqen lehtësisht për shkak të dizajnit të tyre. Lidhësit ST vijnë në dy versione: ST dhe ST-IIHumbja tipike e shkaktuar nga konektorët ST është 0.25 dB.

Figura 3.3. Konektori ST

LC (Lucent Connector). LC është një konektor i vogël i fibrës optike.
Konektori LC përdor një unazë 1,25 mm, gjysmën e madhësisë së ST, i cili është një konektor standard me unazë qeramike. LC-ja ka performancë të mirë dhe përdoret për fibrat singlemode.

Figura 3.4 Konektori LC

Bashkuesit e fibrës përdoren për të lidhur dy konektor të njëjtë fibre. Konektorët e fibrës optike janë përmirësuar nga variant PC në UPC dhe më pas APS duke zvogëluar humbjen e sinjalit për shkak të reflektimit të dritës pas në kontaktin e dy fibrave.

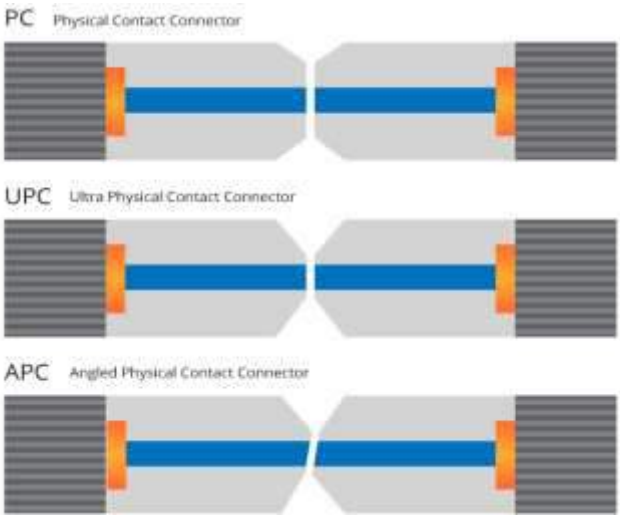


Figura 3.3 Bashkues fibrash

Tema 4. Mjediset e transmetimit në rrjetet e komunikimit

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 psh 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, radhiten më poshte sipas rëndësisë:

Rezistenca e përcjellësit	Rezistenca e përcjellësit përcaktohet nga cilësia e bakrit të përdorur (përcjellshmëria 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 rëndësishëm 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 e 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 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.
Vonesa 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 transmetuesit në kabllot prej bakri).
Deformimi i sinjalit	Sinjalet elektrike, në varësi të kapacitetit elektrik të vetë kabllit, deformohen në krahun fundor të sinjalit kuadratik. Deformime të tilla mund të balacohen me ndihmën e përforcuesve (repeaters).

Klasifikimi i kabllove prej bakri
Në thelb, media e transmetimit prej përcjellësish metalikë, klasifikohen në tre grupe sipas formës së ndërtimit.

1. Kabëll koaksial
2. Kabëll simetrik
3. Kabëll asimetrik

Tek kabllot e grupit të fundit, fijet përbërëse janë të thurura në të gjithë gjatësinë e kabllit. Fusha e përdormit 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 trasmetimet 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.

Ndërtimi i kabllove prej bakri
Karakteristikat më të rëndësishme të përcjellësve elektrik, që përdoren për transmetimin e të dhënave, janë karakteristika mekanike dhe elektrike si:

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

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 Bus. Fluksi maksimal i transmetimit arrin në 10 MBit/s.

1. Përcjellësi i brendshëm (bakri) mbështillet me një shtresë izoluese (dielektrike).
2. Mbështjella prej rrjete metalike apo prej aluminofolie mbron të dhënat që transmetohen nëpërmjet absorbimit të 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 "shtrembërohen,, gjatë transmetimit.
3. Mbështjellja e jashtme e mbron kabllin nga influencat e drejtpërdrejta mbi të si papastërtitë, nxehtësia dhe magnetizimi.

Përcjellësi i brendshëm

Përcjellësi i brendshëm i një kablli koaksial transmeton sinjale elektrike, 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 vetëm, atëhere ai në shumicën e rasteve është prej bakri. Përcjellësi I brendshëm rrethohet nga një shtresë e trashë jopërcjellëse, 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 brendshëmnga interferencat elektrike dhe interferencat e kabllove fqinj. Përcjellësi I brendshëm dhe rrjeta metalike duhet 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 jamë më pak të ndjeshmë se kabllot me çifte të përdredhura, përsa I përket humbjeve dhe interferencave të tjera.

Kryesisht dallojmë dy lloje kabllosh koaksiale:

1. Thinnet (të hollë)
2. Thicknet (të trashë)

Kablli Thinnet

Ky lloj kablli koaksial është mjaft i përkulshëm dhe i përshtatshëm 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 patur humbje të konsiderueshme të sinjalit. Kablli Thinnet i përket grupit të kabllove RG-58. Ai paraqet një rezistencë prej 50 Ohm.

Kablli Thicknet

Kabllot Thicknet janë janë të ngurtë dhe kanë një diametër prej rreth 1,27 centimetra (0,5 Inch). Bazuar në diametrin e trashë, nëpërmjet këtij lloj kablli mund të të transmetohen të dhëna nëlargësi më të mëdha se nëpërmjet kabllit Thinnet. Largësia maksimale është rreth 500 Metra. Për shkak të vështirësive të përpunimit, përdorimi i kabllove thicknet ka qenë i kushtëzuar.

Figura 4.1 Kablli koaksial thicknet dhe thinnet

Kablli Twisted-Pair (me çifte të përdredhura)
Një formë e vecantë e kabllit të bakrit simetrik është kablli twisted-pair. Në teknikën e lidhjes yll 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, sidomos në variantin e skremuar (shielded – STP). Kabllin twisted-pair e gjejmë gjerësisht në dy forma :

1. Si kabëll Twisted-Pair të pambrojtur (unshielded) = UTP
2. Si kabëll Twisted-Pair të mbrojtur (shielded) = STP

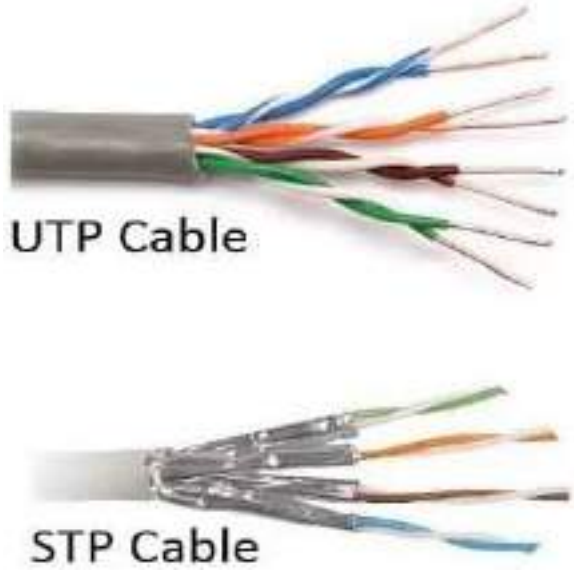


Figura 4.2. Çiftet e përdredhura UTP dhe STP

Kategoritë e kabllove sipas ISO/IEC

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

Në varësi nga qëllimi i përdorimit, fijet e kabllit lidhen në kokën e kabllit në mënyrë të drejtë ose të kryqëzuar (straight through ose crossover). Kablli RJ45 përdor vetëm dy 2- çifte

fijesh: Portokalli (pin-et 1 & 2) dhe Jeshile (pin-et 3 & 6). Pin-et 4, 5 (Blu) dhe 7, 8 (Kafe) nuk përdoren.

Ne figurën e mëposhtme, krahas kodit të ngjyrave të kabllove dhe lidhjes së tyre sipas standardit EIA/TIA T568B, jepet edhe pajisjet se ku përdoren.

Figura 4.3 Diagrama e EIA/TIA T568B

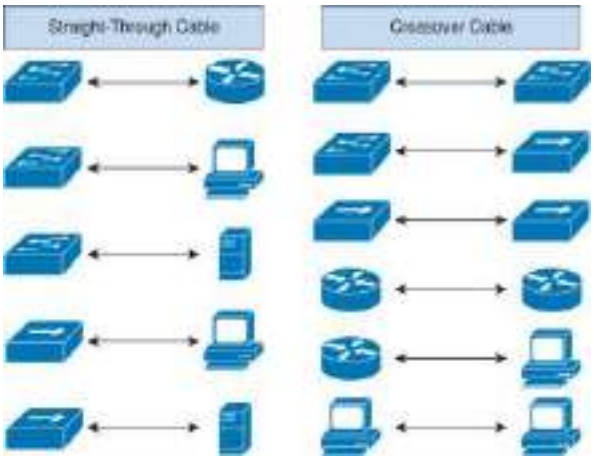


Figura 4.4 Përdorimi i straight through dhe crossover në rrjetet e komunikimit

Kabllot me fibra optike

Kabllot me fibra optike bënë revolucion në botë në komunikimin rrjetor që nga momenti kur janë patentuar, para thuajse katër dekadave. Edhe pse të gjithë e dimë se kabllot optike janë dukshëm më të mirë se ato tradicionale, prej bakri, a keni pyetur veten ndonjëherë se pse?
Nëse i krahasojmë kabllot optike me ato të bakrit, menjëherë do ta shohim se ato janë më të lehta dhe më fleksibile. Por, përparësia e tyre kryesore është në atë që kanë kapacitet të bartin shumë më shumë të dhëna me shpejtësi të mëdha.

Fibrat optike janë bërë nga qelqi dhe transferojnë informacione në formë të dritës, ndërsa bakri zbaton energji elektrike. Sinjali përmes kabllove prej bakri gjithashtu udhëton shpejtë, por ajo që e bën optikën shumë më të mirë se bakri është vëllimi thuajse i pakufizuar. Fibrat optike mund të transferojnë vëllime më të mëdha, pasi drita është sinjal me frekuencë më të lartë për dallim prej bakrit tek i cili sinjali elektrik transferohet në frekuenca relativisht të ulëta.

Një karakteristikë tjetër që i jep përparësi optikës është fakti se përmes fibrave optike mund të dërgohet sinjal në mbi 200 kilometra pa u humbur cilësia, ndërsa sinjalet e bartura përmes kabllove prej bakri vuajnë prej degradimit serioz të cilësisë së distancave prej vetëm disa kilometra. Midis tjerash, kjo i referohet faktit që optika është shumë më pak e ekspozuar ndaj

pengesave elektromagnetike sesa kabllot prej bakri. Nëse kabllot prej bakri nuk janë të instaluara siç duhet, ato prodhojnë rryma elektromagnetike të cilat mund të shkaktojnë degradime serioze në sinjalin e rrjetit.

Përmirësimet në teknologjinë për prodhimin e fibrave optike dhe kabllove optike në të ardhme do të mundësojë sinjalet të udhëtojnë në distanca akoma më të mëdha para se të duhej të rigjeneroheshin. Nga ana tjetër, përmirësimet e teknologjisë për transferimin e sinjaleve optike do të mundësojnë shpejtësi më të mëdha të transferimit përmes infrastrukturës ekzistuese të kabllove optike. Dy faktorët do të kontribuojnë për mundësimin e shpejtësive në terabajt, për çka ekzistojnë kërkesa reale.

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 (buffer) për mbrojtjen nga dëmtimet mekanike drejtimi i një impulsi drite bëhet në bërthamë dhe veshje. Midis cladding dhe buffer gjendet një shtresë llaku me trashësi deri 5 μm. Ajo shërben për të mbrojtur fibrën nga depërtimi i lagështirës.

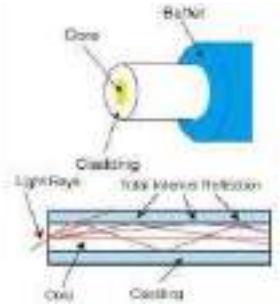


Figura 4.3 Ndërtimi i fibrës optike dhe përçimi i dritës

Produkti gjerësi bande - distancë
Produkti gjerësi bande – distancë (gjerësia e bandës në MHz, distanca në km) është parametri bazë për përcaktimin e transmetueshmërisë në gjerësinë e dhënë të bandës dhe distancës së mbuluar. Produkti gjerësi bande – distancë mund të jepet si për mjediset prej metali të transmetimit, ashtu edhe për ato optike**.** Një produkt me gjerësi bande MHz x km punon:

1. në gjatësi 500 m me një gjerësi bande prej 1,6 GHz
2. në një gjatësi 1 km me një gjerësi bande prej 800 MHz
3. në një gjatësi 1.5 km - 2 km me një gjerësi bande prej 400 MHz

Tema 5: Rrjeti me fibra optike

Ndërtimi i fibrës optike
Kablli me fibra optike përdor një fije qelqi ose plastike për të transmetuar sinjale e të dhënave duke përdorur dritën; të dhënat barten në impulset e dritës. Ndryshe nga teknikat e transmetimit të përdorura në kabujt e bakrit, transmetimi në fijet optike nuk është i natyrës elektrike. Kablloja me bërthamë plastike është më e lehtë për t'u instaluar sesa bërthama tradicionale e qelqit, por plastika nuk mund të transmetojë të dhënat në distanca të largëta si qelqi.
Si burim drite në linjat me fibër optike shërbejnë diodat (LED) ose lazerët. Në linjat e reja LAN të dizajnuara për të funksionuar në distanca më të gjata, të tilla si me 1000Base-LX,

zakonisht përdoren lazer. Një kabëll me fibra optike (treguar në Figurën 5.1) përbëhet nga një xhaketë (mbështjellëse), material mbrojtës dhe pjesa e kabllos me fibra optike. Fibra optike përbëhet nga një bërthamë (8.3, 50, ose 62.5 mikronë në diametër, në varësi të llojit) që është më e vogël se një fije floku, e cila është e rrethuar nga një veshje. Veshja (me diametër tipik 125 mikrometra) është e rrethuar nga një shtresë, material zbutës dhe, së fundmi, një xhaketë. Veshja siguron një indeks të ulët të thyerjes për të shkaktuar reflektim brenda bërthamës, në mënyrë që valët e dritës të transmetohen në bërthamën e fibrës.

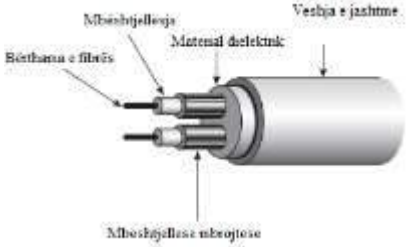


Figura 5.1. Ndërtimi i kabëllit të fibrës optike

Llojet e fibrës optike

Ekzistojnë tre kategori të fibrave optike, të cilat dallohen nga vetitë e tyre modale dhe fizike:

1. Step Index (multimode);
2. Graded Index (multimode);
3. Single Mode (i quajtur edhe monomode).

Fibra Step index karakterizohet nga një ndryshim i menjëhershëm i indeksit të përthyerjes dhe Graded Index karakterizohet nga një ndryshim i vazhdueshëm dhe gradual i indeksit të përthyerjes (d.m.th., nga n_1 në n_2). Figura 5.2 tregon ndërtimin e fibrave dhe profilin e indeksit të përthyerjes për fibra stepindex (Figura 5.2a) dhe fibra graded index (Figura 5.2b). Transmetimi i dritës si tek fibra SI (në vazhdim do të quhet e tillë për *Step Index*) ashtu edhe tek GI (në vazhdim do të quhet e tillë për *Graded Index*) karakterizohen si multimode sepse përhapen më shumë se një mënyrë. Fibra me indeks të graduar ka një prodhim më të madh të distancës me gjerësinë e bandës krahasuar me atë të fibrave SI. Me fjalë të tjera, ai mund të transportojë me shpejtë sesa fibra SI. Është gjithashtu më i shtrenjtë.

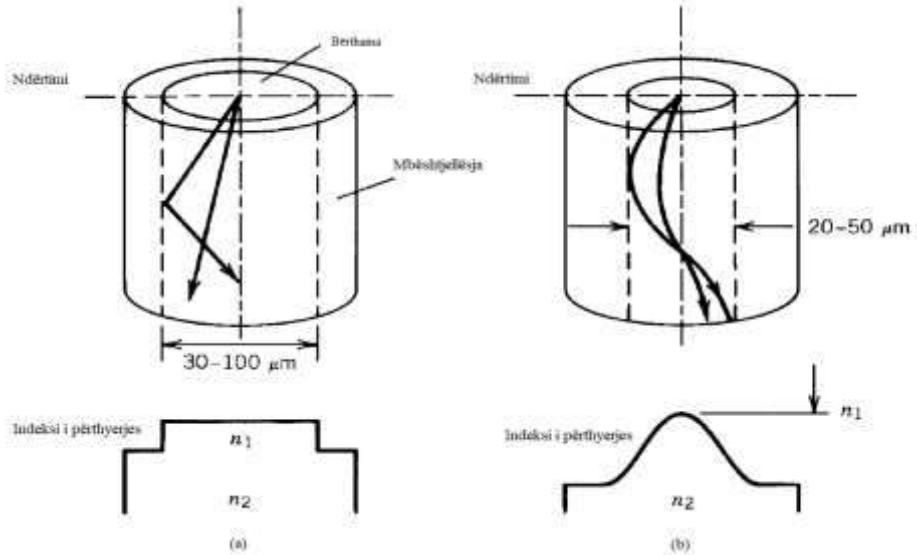


Figura 5.2. Ndërtimi dhe përthyerja në fibrën SI (a) dhe GI (b)

Avantazhet e përdorimit të fibrës optike

Fibrat optike si mjedis transmetues kanë një gjerësi bande relativisht të pakufizuar. Ka veti të shkëlqyera të shkuarjes, deri në 0.25 dB/km. Gjithashtu, ndarja e përsëritësit është në rendin 10–100 herë më të madh se ajo e kabllit koaksial për gjerësi të njëjtë brezi. Përparësitë e tjera

janë:
• Imuniteti i lartë elektromagnetik;
• Eliminimi i nevojës për tokëzim;
• Siguria;
• Madhësia e vogël dhe pesha e lehtë;
• Mundësi e zgjerimit të rrjetit
Fibrat optike sot përdorin tre breza gjatësi vale: (1) rreth 800 nm (nanometra), (2) 1300 nm dhe (3) 1600 nm ose infra të kuqe gati të dukshme. Kapaciteti i lartë i transmetimit të informacionit në një fibër optike lidhet gjithashtu me teknikat e posaçme të multipleksimit. Teknika e përdorur për teknologjinë e fibrës optike është tenika e multipleksimit me ndarje në gjatësi vale WDM (Wavelength Devision Multiplexing).

Burimet e dritës
Një burim drite, ka funksionin themelor në një sistem komunikimi me fibra optike për të shndërruar në mënyrë efikase energjinë elektrike në energji optike (dritë) në një mënyrë që të lejojë burimin e dritës të transmetohet në mënyrë efektive nëpër fibër optike. Sinjali i dritës i gjeneruar kështu duhet të gjurmojë me saktësi sinjalin elektrik hyrës në mënyrë që zhurmat dhe shtrembërimet të minimizohen. Dy burimet më të përdorura të dritës për sistemet e komunikimit me fibra optike janë dioda emetuese e dritës (LED) dhe lazeri gjysmëpërçues, ndonjëherë i quajtur diodë lazer (LD). LED dhe LD janë të fabrikuara nga të njëjtat përbërje gjysmëpërçuese dhe kanë struktura të ngjashme. Ato ndryshojnë në mënyrën e lëshimit të dritës dhe në karakteristikat e tyre të performancës.
Një LED është një bashkim p–n që lëshon dritë përmes emetimit spontan, një fenomen i referuar si elektrolumineshencë. LD lëshojnë dritë përmes emetimit të stimuluar. LED-të janë më pak efikase se LD-të, por janë dukshëm më ekonomike. Ata gjithashtu kanë një jetë më të gjatë operacionale. Drita e emetuar e një LED është jokoherent me një gjerësi relativisht të gjerë të vijës spektrale (nga 30 nm në 60 nm) dhe një përhapje këndore relativisht të madhe, rreth 1008. Nga ana tjetër, një lazer gjysmëpërçues lëshon një gjerësi relativisht të ngushtë të vijës (nga < 2 nm deri 4 nm). Figura 5.3a tregon vijën spektrale për një LED dhe Figura 5.3b tregon vijën spektrale për një LD.

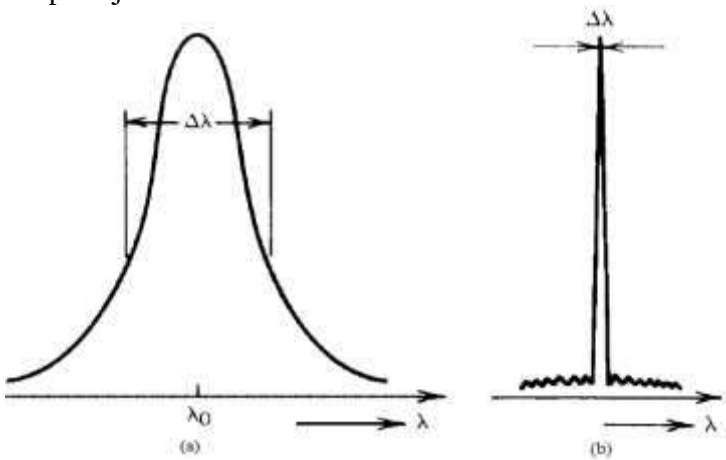


Figura 5.3 Gjerësia spektrale e një diode LED (a) dhe e një LD (b)a

Detektorët e dritës
Detektorët (marrësit) më të përdorur për sistemet e komunikimit me fibra optike janë fotodiodat, PIN ose APD. Terminologjia PIN rrjedh nga konstruksioni gjysmëpërçues i pajisjes ku përdoret një material i brendshëm (I) midis kryqëzimit p–n të diodës. Një lloj tjetër detektori është fotodioda e ortekut (APD), e cila është një pajisje përforcuese që shfaq përforcime të rendit 15 dB deri në 20 dB. Dioda PIN nuk është një pajisje përforcimi. Nga dy llojet e fotodiodave të diskutuara këtu, detektori PIN është më ekonomik dhe kërkon qark më

pak kompleks sesa homologu i tij APD. Dioda PIN ka ndjeshmërinë maksimale nga 800 nm në 900 nm. Koha e përgjithshme e përgjigjes për diodën PIN është e mirë. Koha e përgjigjes së APD është shumë më e mirë se ajo e diodës PIN, por APD shfaq paqëndrueshmëri të caktuara të temperaturës, ku përgjigja mund të ndryshojë ndjeshëm me temperaturën. Tensioni i polarizimit për APD-të janë shumë më të larta sesa për diodat PIN, dhe disa APD-të kërkojnë tensione deri në 200 V.

Ndarësit dhe bashkuesit

Kablli i fibrave optike është zakonisht i disponueshëm në seksione 1 km; është gjithashtu i disponueshëm në seksione më të gjata, në disa lloje deri në 10 km ose më shumë. Në çdo rast duhet të ekzistojë një mënyrë e lidhjes së fibrës me burimin dhe me detektorin, si dhe lidhja fundeve të kabllos së bashku, qoftë në 1 km ose më shumë gjatësi, siç kërkohet. Ekzistojnë dy metoda të lidhjeve. Objektivi në secilin rast është të transferojë sa më shumë dritë të jetë e mundur përmes bashkimit. Një bashkim i mirë mund të ketë një humbje deri në 0.09 dB. Një bashkim i fibrave optike kërkon një shtrirje shumë të saktë dhe një përfundim të shkëlqyeshëm përfundimtar të fibrave. Ekzistojnë tre shkaqe të humbjeve në bashkim:

1. Zhvendosja anësore e akseve të fibrave;
2. Ndarja e fundit të fibrave;
3. Mbivendosja këndore.

Ekzistojnë dy lloje bashkimesh, bashkimi mekanik dhe bashkimi me ngjitje. Me një bashkim mekanik përdoret një substancë përputhëse optike për të zvogëluar humbjet e bashkimit. Substanca që përputh duhet të ketë një indeks të thyerjes afër indeksit të bërthamës së fibrës. Përdoret gjithashtu një çimento me veti të ngjashme, që i shërben qëllimit të dyfishtë të përputhjes së indeksit të thyerjes dhe lidhjes së fibrave. Bashkimi me ngjitje, i quajtur gjithashtu bashkim i nxehtë, është vendi ku fijet ngjiten së bashku. Fibrat që do të bashkohen afrohen së bashku dhe nxehen me një hark elektrik derisa të ndodhin zbutja dhe shkrirja. Bashkimet kërkojnë pajisje speciale bashkuese dhe teknikë të trajnuar.

Kështu mund të shihet që bashkimet zakonisht janë të vështira për t'u realizuar në mjedisin e punës siç është një pus kabllor. Bashkimet është mirë të bëhen në terren. Sidoqoftë, bashkimet fusin shuarje dhe mund të jenë të kushtueshme. Çiftëzimi i përsëritur i një konektori mund të jetë gjithashtu një problem, veçanërisht nëse papastërtitë ose depozitat e pluhurit hyjnë në zonën ku bëhet çiftëzimi i fibrave. Sidoqoftë, duhet theksuar që pajisjet bashkuese po bëhen më ekonomike, më të pagabueshme dhe më miqësore për përdoruesit. Trajnimi i teknikut gjithashtu po bëhet më pak barrierë. Konektorët përdoren gati në mënyrë universale në burim dhe në detektor për të lidhur fijen kryesore me këto njësi. Kjo e bën më të lehtë ndërrimin e detektorit dhe burimit kur ato dështojnë ose kanë degraduar funksionimin.

Tema 6: Rrjeti Ethernet LAN

Konfigurimi i rrjeteve të komunikimit

Konfigurimi i rrjetit është procesi i vendosjes së kontrolleve, rrjedhës dhe funksionimit të një rrjeti për të mbështetur komunikimin e rrjetit të një organizate dhe/ose administratorit të rrjetit. Ky term i gjerë përfshin procese të konfigurimit dhe proceseve të setup-it në pjesën hardware të rrjetit, software dhe pajisjeve e komponentëve të tjerë mbështetës.

Konfigurimi i rrjetit njihet gjithashtu si setup i rrjetit.

Konfigurimi i rrjetit lejon që një administrator i sistemit të konfigurojë një rrjet me ato parametra që i duhen për të përmbushur objektivat e komunikimit. Procesi përfshin detyrat e mëposhtme:

- Konfigurimi i routerit: Specifikon adresat e sakta IP dhe cilësimet e rrugëzimit, etj.

- Konfigurimi i hostit: Vendos lidhjen e rrjetit në një kompjuter/laptop duke regjistruar cilësimet e parazgjedhura të rrjetit, të tilla si adresimi IP, proxy, emri i rrjetit dhe ID/fjalëkalimi, për të mundësuar lidhjen dhe komunikimin e rrjetit.
- Konfigurimi i softuerit: Janë programe të dedikuara, të bazuara në rrjet që mundësojnë shërbime të mundshme në të, siç është p.sh. kontrolli i kredencialeve, monitorimi i trafikut të rrjetit, etj.

Për më tepër, konfigurimi i rrjetit përfshin edhe ndarjen e Internetit/rrjetit, instalimin e software-it/ aplikacionit dhe instalimin/konfigurimin e firewall-it.

Ndërtimi dhe funksionimi i një rrjeti LAN

Ethernet është teknologjia që përdoret zakonisht në rrjetet lokale me tela (LAN). Një LAN është një rrjet kompjuterash dhe pajisjesh të tjera elektronike që mbulojnë një zonë të vogël si dhoma, zyra ose ndërtesa, në ndryshim nga rrjeti WAN, i cili shtrihet në një zonë të madhe gjeografike. Ethernet është një protokoll rrjeti që kontrollon se si transmetohen të dhënat përmes një LAN dhe referohet si protokolli IEEE 802.3. Protokolli ka evoluar dhe është përmirësuar me kalimin e kohës për të transferuar të dhëna me shpejtësi më shumë se një gigabit për sekondë.

Për të konfiguruar një rrjet LAN Ethernet, nevojiten të konsiderohen çështjet e mëposhtme:

- Kompjuterët dhe pajisjet për tu lidhur: Ethernet lidh çdo kompjuter ose pajisje tjetër elektronike në rrjetin e saj për sa kohë që pajisja ka një adaptor Ethernet ose një kartë rrjeti.
- Kartat e ndërfaqes së rrjetit në pajisjet: Një kartë e ndërfaqes së rrjetit është e integruar në motherboard ose instalohet veçmas në pajisje. Ekzistojnë edhe versione USB të kartave Ethernet.
- Një router, hub, switch ose gateway për të lidhur pajisjet: Një shpërndarës është një pajisje që vepron si një pikë lidhëse midis pajisjeve në një rrjet. Përbëhet nga disa porta RJ-45 në të cilat lidhni kabllot.
- Kabllot: Kabllot UTP (Unshielded Twisted Pair) përdoren zakonisht në LAN-et Ethernet. Ky kabëll është i ngjashëm me llojin e përdorur për pajisjet telefonike fikse por më i trashë, me tetë çifte telash të përdredhur me ngjyra të ndryshme brenda. Fundi është i lidhur me një lidhës RJ-45, i cili është një version më i madh i foleve RJ-11 që futet në një telefon fiks.
- Program kompjuterik për të menaxhuar rrjetin: Sistemet operative moderne si versionet e fundit të Windows, Linux dhe macOS mundësojnë menaxhimin LAN-eve Ethernet.

Komanda DOS

Komandat DOS janë komandat e disponueshme në MS-DOS që përdoren për të bashkëvepruar me sistemin operativ dhe software të tjerë duke përdorur vetëm komanda.

Komandat DOS janë mënyra kryesore në të cilat përdoret një sistemin operimi. Windows dhe OS të tjerë modernë përdorin një sistem të bazuar në grafikë dhe ku ndërveprimi është përmes prekjes ose mouse-it.

Ndërveprimi me sistemin e operimit përmes komandave është e mundur duke shkuar në *Search-cmd*, siç tregohet në figurën e mëposhtme:

Figura 6.1 Gjetja e *comandline*

Në terminalin që shfaqet më pas është mundësia për të ekzekutuar një numër shumë të madh komandash për ndërveprimin me kompjuterin. Po tregojmë më poshtë sesi mund të gjendet adresa MAC e një kompjuteri duke përdorur vetëm comandline-in.

Figura 6.2 Gjetja e adresës MAC përmes *comandline*

Adresa unike MAC

MAC qëndron për emërtimin anglisht "*Media Access Control Address*". Një adresë MAC është një numër identifikimi që identifikon në mënyrë unike secilën pajisje në një rrjet. Adresa MAC prodhohet në çdo kartë rrjeti, siç është karta Ethernet ose karta Wi-Fi, dhe për këtë arsye nuk mund të ndryshohet.

Për shkak se ekzistojnë miliona pajisje në rrjet dhe secila pajisje duhet të ketë një adresë unike MAC, numri i adresave të tilla është shumë i madh. Për këtë arsye, adresat MAC përbëhen nga gjashtë numra heksadecimal dyshifror, të ndara me dy pika. Për shembull, një kartë Ethernet mund të ketë një adresë MAC prej 00: 0d: 83: b1: c0: 8e. Për fat të mirë, nuk keni nevojë ta mbani mend këtë adresë, pasi ajo njihet automatikisht nga shumica e rrjeteve.

Llojet e adresave IP

Adresa IP qëndron për adresën e Protokollit të Internetit (Internet Protocol); është një numër identifikues që lidhet me një kompjuter specifik ose rrjet kompjuterik. Kur lidhen në internet, adresa IP lejon kompjuterët të dërgojnë dhe të marrin informacione.

Shumica e adresave IP janë thjesht numerike, por ndërsa përdorimi i internetit rritet, adresës i janë shtuar edhe disa shkronja.

Ekzistojnë katër lloje të ndryshme të adresave IP: publike, private, statike dhe dinamike. Ndërsa adresat publike dhe private janë tregues i vendndodhjes së rrjetit - private që përdoret brenda një rrjeti ndërsa publike përdoret jashtë një rrjeti - statika dhe dinamika tregojnë qëndrueshmërinë.

Një adresë IP statike i vendoset një pajisjeje fundore manualisht. Një adresë statike gjithashtu nuk ndryshon, ndërsa një adresë dinamike IP caktohet nga një server (DHCP) dhe mund të ndryshojë. Adresat dinamike IP janë lloji më i zakonshëm i adresave të protokollit të internetit. Adresat dinamike IP janë aktive vetëm për një kohë të caktuar, pas së cilës skadojnë. Kompjuteri ose do të kërkojë automatikisht një adresë të re, sa herë lidhet në një rrjet.

Një adresë IP mund të krahasohet me një Numër të Sigurimeve Shoqërore (SSN) pasi secila prej tyre është plotësisht unike për kompjuterin ose përdoruesin të cilit i është caktuar. Krijimi i këtyre numrave lejon që router-at të identifikojnë se ku po dërgojnë informacion në internet. Ata gjithashtu sigurohen që pajisjet e sakta po marrin atë që po dërgohet.

Tema 7: Standardet e ndërfaqeve dhe pajisjet

Njohuri të përgjithshme mbi ndërfaqet e rrjetit

Kartat e Ndërfaqes së Rrjetit (NIC – Network Interface Card) janë qarqe të integruara në

bordet e qarqeve të printuara që ofrojnë qasje fizike nga pajisja fundore në një rrjet LAN. NIC është përgjegjës për fragmentimin e të dhënave për transmetim dhe formatimin e paketave të të dhënave me *hearder-in* dhe *trailer-in* e nevojshëm. Sipas standartit IEEE, një NIC përmban një adresë logjike unike, të koduar, të cilën e përfshin në kokën e secilës paketë të të dhënave që transmeton. NIC zakonisht ka gjithashtu një memorje dhe një mikroprocesor. Sipas Modelit të Referencës OSI, NIC funksionojnë në dy shtresat e poshtme, në shtresën Fizike dhe atë të Datalink-ut. NIC mund të vijë në forma të ndryshme, si një kartë e integruar që vendoset në slotet e zgjerimit në kompjuter, si një pajisje e veçantë, që instalohet së jashtmi, etj. Gjithashtu një NIC mund t'i mundësojë pajisjes fundore të lidhet në LAN vetëm përmes kabëllit Ethernet, ndërsa të tjera shtohen/instalohen në kompjuter për t'i mundësuar atij edhe lidhjen wireless (WNIC – Wireless NIC). Më poshtë, tregohen imazhet e të dyjave.

Figura 6.1. NIC dhe WNIC

Instalimi i një kate rrjeti në kompjuter

Që një kompjuter të lidhet me rrjetin, duhet të ketë një ndërfaqe rrjeti. Sidoqoftë, përsëri mund të hasni një kompjuter të rastit më të vjetër që nuk ka një ndërfaqe rrjeti të integruar. Instalimi i një karte ndërfaqeje rrjeti është një detyrë e thjeshtë, vetëm nëse etapat ndiqen siç duhet.

Hapi 1: Bëni gati materialet

Mblidhni kartën e rrjetit, CD/USB me drivera-t dhe CD-në e instalimit të Windows për çdo rast.

Hapi 2: Mbyllni Windows-in, fikni kompjuterin dhe hiqeni nga priza.

Asnjëherë mos punoni në brendësinë e kompjuterit tuaj kur është i ndezur ose është i lidhur në energji elektrike.

Hapi 3: Hapni kasën e kompjuterit

Zakonisht duhen hequr një numër vidash përpara se të shfaqet qarku i motherboard. Vidat duhen sistemuar diku me qëllim që të mos humbasin apo enden.

Hapi 4: Gjeni slotin e papërdorur brenda kompjuterit

Slotet e zgjerimit rreshtohen njëra pas tjetrës në pjesës së pasme të kompjuterit, ndaj nuk mund të ngatërrohen. Çdo kompjuter më pak se 5 vjet i vjetër, ka të paktën 2 ose 3 të këtilla të njohura si slotet PCI.

Hapi 5: Hiqni mbrojtësin metalik të slotit nga pjesa e pasme e kasës së kompjuterit.

Nëse ka vida fiksuese që e mbajnë slotin, hiqini dhe ruajini në një vend të sigurt pasi do të duhen më vonë.

Hapi 6: Vendosni kartën e ndërfaqes së rrjetit në slot

Rreshtoni konektorët në pjesën e poshtme të kartës me koenktorët në slot dhe më pas shtypni kartën për poshtë. Ndonjëherë do t'ju duhet të shtypni me forcë që karta të hyjë në slot.

Hapi 7: Siguroni kartën e ndërfaqes së rrjetit

Vida e hequr në etapën 5, duhet të vendoset në vend për të fiksuar slotin.

Hapi 8: Mbyllet kasa e kompjuterit

Tregoni kujdes kabujt brenda kompjuterit. Nuk duhet të mbyllet kasa me forcë pasi kështu rrezikohet të dëmtohet ndonjë kabëll. Kasa sigurohet me vidat e hequra në etapën 3.

Hapi 9: Vendosni kompjuterin në prizë dhe ndizeni

Nëse karta është *Plug and Play* (vendoset në kompjuter dhe funksionon menjëherë), nuk ka

nevoj për ndonjë konfigurim pasi ndizet Windows. Nëse karta nuk është e tillë, atëherë pasi Windows ka startuar, duhet të instalohen driverat që zakonisht gjenden në CD-në që shoqëron paketimin e kartës.

Komponentët e NIC
Komponentët e kartës së ndërfaqes së rrjetit janë:
Shpejtësia – Vlerësimi i shpejtësisë në të gjitha NIC jepet në terma Mbps që tregon performancën e përgjithshme të kartës kur implementohet në një rrjet kompjuterik me një gjerësi të caktuar brezi. Nëse gjerësia e brezit është më e ulët se NIC ose kompjutera të shumtë janë të lidhur me të njëjtin kontrollues, kjo do të ngadalësojë shpejtësinë e përcaktuar. NIC për linjat Ethernet ofrohen në opsionet 10 Mbps, 100 Mbps, 1000 Mbps dhe 1 Gbps.
Driver - Ky është program i nevojshëm që mundëson kalimin e të dhënave ndërmjet sistemit operativ të kompjuterit (OS) dhe NIC. Kur një NIC është i instaluar në një kompjuter, instalohet gjithashtu edhe software-i përkatës i driver-it. Ai duhet të jetë vazhdimisht i përditësuar dhe i padëmtuar për të siguruar një performancë optimale nga NIC.
Adresa MAC - Adresat unike, të pandryshueshme MAC, të njohura gjithashtu si adresat fizike të rrjetit, u caktohen kartave të rrjetit për të marr dhe dërguar paketa Ethernet.
LED i lidhjes - Shumica e NIC-ve kanë një tregues LED të integruar në konektor për të njoftuar përdoruesin se kur rrjeti është i lidhur dhe të dhënat transmetohen.
Router - Një router ndonjëherë është i nevojshëm për të lejuar komunikimin midis një kompjuteri dhe pajisjeve të tjera. Në këtë rast, NIC lidhet me routerin i cili nga ana tjetër është i lidhur në internet.

Tema 8: Rrjete e komunikimeve industriale

Rëndësia e rrjetit të komunikimit
Ka lloje të ndryshme rrjetesh, por ne do të përqendrohemi te rrjetet e komunikimit, të cilat zënë pjesën më të rëndësishme në fushën TIK. Rrjetet nuk janë absolutisht të kufizuara nga lidhjet fizike. Nëse shikojmë telefonat tanë personalë, vëmë re se ata nuk kanë asnjë kabëll që lidhet me ta dhe përsëri ne mund të bëjmë telefonata, të aksesojmë internetin, të çojmë mesazhe (sms) etj. Në këtë rast, lidhja në rrjet bëhet pa kabëll, ose siç e quajmë ndryshe, *wireless*. Rrjetet kanë ndihmuar të gjithë botën të afrohet virtualisht, duke bërë të mundur atë që para disa kohësh shihej si e pamundur nga gjithë njerëzimi. Sot, ne kemi komunikim dhe shkëmbejmë informacion të menjëhershëm me këdo, edhe pse mund të ndodhet në anën tjetër të botës.
Duke thyer çdo kufizim fizik, rrjetet luajnë një rol kryesor në jetën tonë dhe kanë një sërë avantazhesh në çdo aspekt, si ato: financiare, kohore, informative, produktive, fleksibël etj.

Rrjetet kompjuterike
Një rrjet kompjuterik përbëhet nga e pakta dy kompjutera, të cilët, në shumicën e rasteve, lidhen me kabëll që quhet *UTP (Unshielded Twisted Pair*). Ka disa lloje kabllosh, si: *STP (Shielded Twisted Pair), Fiber, Coaxial.* Në shumicën e rasteve, ne përdorim më shumë se dy kompjutera në rrjetet tona dhe për këtë arsye përdorim një pajisje që quhet *switch,* e cila bën lidhjen e këtyre pajisjeve në rrjet, që mund të jenë: kompjutera, printera, telefona *VOIP*, smartfon, smart TV etj.

Si lidhen pajisjet tona me *switch-in* në mënyrë që të jenë pjesë e rrjetit?
Kemi dy mënyra lidhjeje:

- pajisje që lidhen fizikisht;

• pajisje që bëhen pjesë e rrjetit tonë pa lidhje fizike.

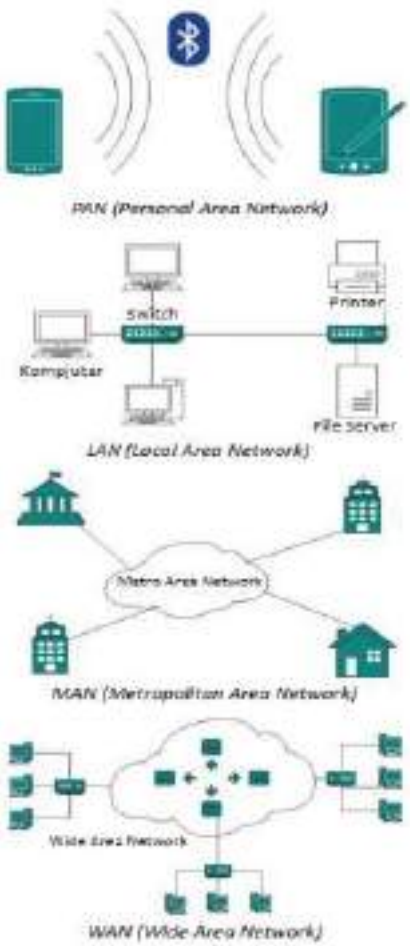
Pajisjet që lidhen fizikisht, përdorin atë që ne e quajmë kartë e rrjetit ose *NIC (Network Interface Card),* e cila është e instaluar në çdo pajisje rrjeti, si p.sh.: kompjutera, printera, telefona *VOIP*, smart TV etj.
Pajisjet *wireless* ose pa kabllo përdorin atë që quhet *Wireless Network Card ose Wireless Adapter,* i cili vjen i instaluar në këto pajisje, si: *smartfon, tablet, laptop* etj.

Llojet e rrjeteve kompjuterike dhe ndarja e tyre

Përgjithësisht, llojet e rrjeteve ndahen nga shpërndarja e tyre gjeografike. Një rrjet mund të jetë i vogël aq sa distanca e telefonit tuaj dhe e kufjeve me *bluetooth,* por mund të jetë aq i madh sa gjithë globi, që është *Interneti*.
Llojet e rrjeteve janë*:* *PAN (Personal Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Are Network), INTERNETWORK.*

• ***PAN (Personal Area Network)***
PAN është një rrjet shumë i vogël dhe personal, që mund të përfshijë pajisje me *bluetooth* ose *infrared,* dhe ka një rreze prej 10 metrash. Nëse shikoni një person që flet në telefon me kufjet e tij të lidhura me *bluetooth*, ai është një *PAN*. Në *PAN* përfshihen: tastiera, mausi *(mouse), wireless,* kufje me *bluetooth*, *printer wireless* etj.

• ***LAN (Local Area Network)***
LAN është një nga rrjetet më të përhapura, duke përfshirë: organizata, shkolla, zyra, shtëpi etj. *LAN* është një rrjet i shpërndarë brenda një godine dhe që në shumicën e rasteve administrohet lokalisht. Ai mund të jetë i lidhur fizikisht me kabëll ose *wireless* (pa kabëll). Nëse shkoni te laboratori i informatikës së shkollës suaj, ju do të jeni të pranishëm në një rrjet *LAN,* që përfshin të gjithë kompjuterat dhe pajisjet e tjera në laborator.



• ***MAN (Metropolitan Area Network)***
MAN bën lidhjen e disa *LAN*-eve që shtrihen në kufijtë e një qyteti ose zone të caktuar. Mendoni rrjetin e një kompanie e cila ka disa degë të saj të shtrira në qytetin e Tiranës. Ky lloj rrjeti është një *MAN*.

• ***WAN (Wide Area Network)***
WAN është një rrjet i cili ka shtrirje në disa qytete dhe deri në kufijtë e një shteti. Mendoni, për shembull, një kompani që ofron internet, e cila shtrihet në çdo cep të Shqipërisë, ky rrjet është një *WAN*.

• ***Internetwork***
Internetwork është një rrjet i përbërë nga disa lloje rrjetesh të tjera. Është rrjeti më i madh që ekziston në botë. Interneti lidh të gjitha rrjetet *WAN* kudo që janë dhe ofron lidhje për rrjetet *LAN* dhe shtëpitë tona.

SISTEMI SCADA/EMS

Sistemi SCADA mund të përdoret si një bllok i rëndësishëm ndërtimi për automatizimin e rrjetit shpërndarës. Sistemi SCADA ishte miratuar dhe u bë funksional në mes të vitit 1988.

Sistemi SCADA

Ç'është sistemi SCADA dhe si ai mund të përmirësojë jetën tonë ?

Termi i referohet një shkalle të gjerë, sistemit të matjes së shpërndarjes (dhe kontrollimi). Sistemet SCADA përdoren për të monitoruar dhe kontrolluar proçeset kimike ose të transportimit, në bashki tek sistemet e shpërndarjes së ujit, kontrollimin e prodhimit të energjisë elektrike dhe shpërndarjen e saj, tubacionet e gazit dhe të naftës, dhe proçese të tjera shpërndarëse. Në parim ky sistem përfshin:

- Pajisjen e mbledhjes së të dhënave
- Pajisjen telemetrike për transmetimin e të dhënave
- Pajisjen e monitorimit të të dhënave
- Ndërfaqja njeri-makineri (HMI)
- Rrjetet, baza e të dhënave të komunikimit, programet kompjuterike, etj.

Në botën e sotme, pothuajse kudo mund të vëzhgojmë sistemet SCADA, qoftë një fabrikë për trajtimin e ujërave të zeza, supermarkete, industri apo edhe në shtëpitë tona.
Sistemet SCADA variojnë nga konfigurimet e thjeshta e gjer tek ato më të ndërlikuarat. Shumica e aplikimeve të sistemit SCADA përdorin softuerin e ndërfaqjes njeri-makineri (HMI) e cila lejon që përdoruesit të ndërveprojë me makineritë për të kontrolluar pajisjet. HMI është e lidhur me motorrët, valvulat dhe shumë pajisje të tjera.
Softueri SCADA merr informacion nga PLC (kontroller logjik i programueshëm) ose nga RTU (njësi komanduese në skaje), të cilat nga ana tjetër marrin informacionin e tyre nga sensorët ose nga vlerat e vendosura manualisht. SCADA në një sistem energjitik përdoret për të mbledhur, analizuar dhe monitoruar të dhënat në mënyrë efektive, e cila redukton humbjet dhe përmirëson efikasitetin e të gjithë sistemit duke kursyer kohë dhe para.

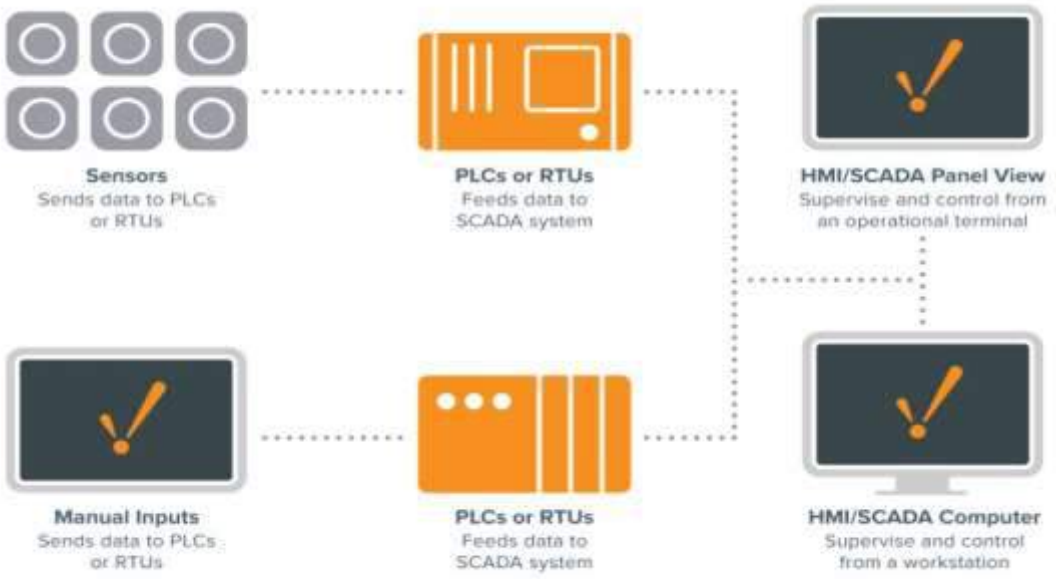


Fig. 1 Diagrama bazë e SCADA

Për të kuptuar origjinën e SCADA, duhet që të kuptojmë problemet që organizatat industriale po përpiqen që të zgjidhin. Para se koncepti i SCADA të prezantohej në mesin e

shekullit 20-të, shumë industri prodhuese, impiante industriale dhe vendndodhje të largëta mbështeteshin tek personeli për të kontrolluar manualisht dhe monitorimi i pajisjeve nëpërmjet pulsantëve dhe thirrjeve analoge.

Teksa industritë prodhuese dhe vendndodhjet e largëta filluan të zgjerohen, duhej një zgjidhje për të kontrolluar pajisjet në distance të largëta. Organizatat industriale filluan të përdornin releté dhe kohëmatësit për të siguruar njëfarë niveli mbikqyrjeje pa qënë nevoja për të dërguar njerëzit në vende të largëta.

Teksa releté dhe kohëmatësit zgjidhnin shumë probleme duke siguruar funksionim të kufizuar të automatizimit. Releté dhe kohëmatësit ishin të vështirë për tu rikonfiguruar, gjetja e gabimeve dhe panelet e kontrollit morën hapësira gjithnjë e më shumë. Një sistem kontrolli plotësisht i automatizuar dhe efikas për monitorim u bë i nevojshëm.

Në fillim të viteve 50-të, u zhvilluan për herë të parë kompjuterat dhe u përdorën për qëllim të një kontrolli industrial. Kontrolli mbikëqyrës filloi të jetë më i kërkuari gjatë atyre viteve. Në vitet 1960, telemetria u krijua për monitorim, e cila lejonte që komunikimet e automatizuara të transmetonin matjet dhe të dhëna të tjera nga vendndodhjet e largëta tek pajisja monitoruese. Termi "SCADA" u krijua në fillim të viteve 1970, dhe lindja e mikroproçesorëve dhe PLC-ve gjatë asaj dekade rriti aftësinë e ndërmarrjeve për të monitoruar dhe kontrolluar proçeset e automatizuara më shumë se kurrë më pare.

Evolucioni i SCADA

Udhëtimi i parë i SCADA nisi me kompjuterët kryesorë. Rrjetet siç i njohim ne sot nuk ishin të disponueshme dhe secili sistem SCADA qëndronte më vehte. Këto sisteme sisteme ishin ato të cilat tani do të quheshin sisteme monolitike SCADA. Në vitet '80 dhe '90, SCADA vazhdoi të evoluojë falë sistemeve më të vogla kompjuterike., teknologjisë LAN (Local Area Networking) dhe softuerit HMI të bazuar në kompjuter.

Fig.2 Evolucioni i SCADA

Sistemet SCADA shumë shpejt ishin në gjendje të lidheshin me sisteme të tjera të ngjashme. Shumë prej protokolleve LAN të përdorura në këto sisteme ishin të regjistruara, gjë e cila i dha përdoruesit kontrollin se si të optimizonin transferimin e të dhënave. Fatkeqësisht, këto sisteme nuk ishin në gjendje të komunikonin me sistemet tek përdoruesit e tjerë. Këto sisteme u quajtën sisteme SCADA.

Në vitet ’90 dhe fillimin e vitit 2000, duke u bazuar në modelin e sistemit të shpërndarë, SCADA miratoi një ndryshim shtesë duke zgjedhur një arkitekturë të sistemit të hapur dhe protokollet e komunikimit që nuk ishin specifikë për përdoruesit. Kjo përsëritje e SCADA-s, e quajtuar një sistem SCADA e rrjetëzuar, përfitoi nga teknologjia komunikimit siç është Ethernet. Ky sistem SCADA i rrjetëzuar lejoi sistemet nga përdorues të tjerë të komunikonin me njëri-tjetrin, duke lehtësuar kufizimet e vendosura nga sistemet më të vjetra SCADA, dhe lejuan organizatat që të lidhnin më shumë se një pajisje me rrjetin.

Teksa sistemet SCADA kanë pësuar ndryshime thelbësore evolucioni, shumë organizata industriale vaazhduan betejën me qasjen e të dhënave industriale nga niveli ndërmarrjes. Nga fundi i viteve 1990 e gjer në fillim të viteve 2000, një bum teknologjik ndodhi dhe teknologjitë e IT përshpejtuan në zhvillim.

Databaza e gjuhës së strukturuar të pyetjeve (SQL) u bë standarti i databazës së IT por nuk u miratuan nga zhvilluesit e SCADA. Kjo rezultoi në një përçarje midis fushave të kontrollit dhe IT, dhe teknologjia SCADA u vjetërsua me kalimin e kohës.

Sistemet tradicionale SCADA ende përdorin teknologjinë e tyre bazë për trajtimin e të dhënave. Dhe si pasojë sjell që transferimi i të dhënave është e çrregullt dhe tepër e kushtueshme.
Sistemet moderne SCADA kanë si qëllim zgjidhjen e këtij problem duke shfrytëzuar më të mirën e kontrollit dhe teknologjinë e informacionit.

Fig. 3 Sistemet Moderne SCADA

Sistemi EMS
Një sistem i menaxhimit të energjisë (EMS) është një mjet i ndihmuar nga kompjuteri i përdorur nga operatorët e sistemit të energjisë për të monitoruar, kontrolluar dhe realizuar menaxhimin optimal të energjisë. Qëllimi i një EMS është që të përcaktojë gjenerimin e energjisë ose kërkesën e energjisë që minimizon një objektiv të caktuar siç është kostoja e gjenerimit, humbja e energjisë, ose efekti mjedisor.

Pse ka rëndësi ?
Menaxhimi i energjisë është kontrollimi dhe reduktimi i konsumit të energjisë së një ndërtese, e cila mundëson:

- **Ulje kostoje** – energjia përfaqëson 25% të të gjithë kostos të funksionimit të një ndërtese zyrash.
- Redukton emetimet e karbonit në mënyrë që të përmbushni qëllimet e brendshme të qëndrueshmërisë dhe kërkesat rregullatore.

- **Ulja e rrezikut** – sa më shumë energji të konsumoni, aq më i madh rreziku që çmimi i energjisë të rritet ose kufizimi i furnizimit i cili mund të ndikojë seriozisht në përfitimin tuaj.

Me sistemet e menaxhimit të energjisë, ju mund ta zvogëloni këtë rrezik duke reduktuar kërkesën tuaj për energji dhe duke e kontrolluar atë në mënyrë që të bëhet sa më i parashikueshëm.

Fig. 4 Sistemi Menaxhimit të Energjisë (EMS)

Teknologjia e kompjuterave është referuar edhe si SCADA/EMS ose EMS/SCADA. Në këto aspekte, terminologjia EMS më pas përjashton funksionet e monitorimit dhe kontrollit, por më specifikisht i referohet grupit kolektiv të aplikacioneve të rrjetit të energjisë dhe aplikacioneve të kontrollit dhe planifikimit të gjenerimit. Prodhuesit e EMS gjithashtu zakonisht furnizojnë një imitues përkatës të trajnimit të dispeçerit (DTS). Kjo teknologji e lidhur bën përdorimin e përbërësve të SCADA dhe EMS si një mjet trajnimi për operatorët e qendrës së kontrollit.

Efikasiteti energjisë

Në një kontekst paksa të ndryshëm, EMS gjithashtu mund t'i referohet një sistemi të dizajnuar për të arritur efikasitetin e energjisë përmes optimizmit të procesit duke raportuar për përdorimin e energjisë. Sistemet më të reja të menaxhimit të energjisë me bazë cloud ofrojnë:

- mundësinë për ti kontrolluar nga distanca HVAC dhee pajisjet e tjera që konsumojnë energji;
- mbledhin të dhëna të hollësishme dhe në kohë reale për secilën pjesë të pajisjeve;
- gjeneron udhëzime inteligjente, specifike, në kohë reale për të gjetur dhe kapur mundësitë më imponuese të kursimit.

Sistemi i menaxhimit të energjisë në shtëpi

Menaxhimi i energjisë në shtëpi (HEM) mundëson që konsumatorët vendas të marrin pjesë në aktivitetet e pjesës kërkuese. Por, ajo ballafaqohet me disa probleme që vijnë nga paqartësitë e burimeve të rinovueshme të energjisë dhe sjellja e konsumatorëve. Ndërsa, konsumatorët vendas synojnë nivelin më të lartë të rehatisë që duhet të merret parasysh duke minimizuar fenomenin e "lodhjes së përgjigjes".

Kontroll i automatizuar në ndërtesa

Termi “Sistemi i Menaxhimit të Energjisë” gjithashtu mund t'i referohet një sistemi kompjuterik i cili është krijuar posaçërisht për kontrollin dhe monitorimin e automatizuar të atyre objekteve elektromekanike në një ndërtesë që japin konsum të konsiderueshëm të energjisë si:

- instalimet e ngrohjes,
- ventilimit
- ndriçimit.

Fig 5. BEMS (Sistemi i menaxhimit të energjisë në ndërtesa)

Shtrirja mund të përfshijë:

1. një ndërtesë të vetme
2. një grup ndërtesash (siç janë universitetet , ndërtesat e zyrave, rrjetet e dyqaneve me pakicë ose fabrikat).

Shumica e këtyre sistemeve të menaxhimit të energjisë gjithashtu ofrojnë lehtësira për leximin e matësve të energjisë elektrike, gazit dhe ujit.

Këto të dhëna të marra do të na shërbejnë për të kryer rutina vetë-diagnostikuese dhe optimizuese në baza të shpeshta për të prodhuar analizën e prirjeve dhe parashikimet vjetore të konsumit. Sistemet e menaxhimit të energjisë shpesh përdoren nga njësitë individuale tregtare për të:

1. monitoruar
2. matur
3. kontrolluar ngarkesat e tyre elektrike të ndërtesave.

Sistemet e menaxhimit të energjisë mund të përdoren për të kontrolluar pajisjet qendrore si njësitë HVAC dhe sistemet e ndriçimit nëpër vende të shumta, të tilla si shitjet me pakicë, vende ushqimore dhe restorante. Sistemet e menaxhimit të energjisë (EMS) gjithashtu mund të ofrojnë funksione matëse, nën-matëse dhe monitoruese që lejojnë menaxherët e strukturave dhe ndërtesave të mbledhin të dhëna që i mundeson atyre të marrin vendime më të informuara në lidhje me aktivitetet e energjisë në vendet e tyre.

Historiku

Deri në fillim të vitit 1990 ishte e zakonshme të gjeje sisteme EMS bazuar në harduer të veçantë dhe në sisteme operative. Më parë furnizuesit EMS si Harris Controls (tani GE), Hitachi, Cebyc, Control Data Corporation, Siemens dhe Toshiba prodhuan harduerin e tyre.

Furnizuesit EMS që nuk e prodhonin vetë harduer-in shpesh mbështeteshin në produktet e zhvilluara nga Digital Equipment, Gould Electronics dhe MODCOMP. VAX 11/780 nga Pajisjet Dixhitale ishte një zgjedhje e popullarizuar në mesin e disa furnizuesve EMS.

Sistemet EMS tani mbështeten në një qasje të bazuar në model. Modelet tradicionale të planifikimit dhe modelet EMS gjithmonë ruheshin në mënyrë të pavarur dhe rrallë në sinkronizim me njëri-tjetrin. Përdorimi i softuerit EMS lejon planifikuesit dhe operatorët të ndajnë një model të përbashkët duke zvogëluar mos pajtimin midis të dyve dhe mirëmbajtjes së modelit në dy pjesë. Të kesh një ndërfaqe të zakonshme të përdoruesit gjithashtu lejon kalimin më të lehtë të informacionit nga planifikimi në përdorim.

Ndërsa sistemet u bënë jo ekonomike, furnitorët EMS filluan të ofrojnë zgjidhje bazuar në platformat standarte të një hardueri industrie si ato të Pajisjeve Dixhitale (më vonë Compaq i njohur në ditët e sotme me emrin HP), IBM dhe Sun. Sistemi i zakonshëm operativ atëherë ishte DEC, OpenVMS ose Unix. Deri në vitin 2004, furnitorë të ndryshëm EMS përfshirë Alstom, ABB dhe OSI kishin filluar të ofronin zgjidhje të bazuara në Windows.

Deri në vitin 2006, klientët kishin një zgjedhje të sistemeve bazuar në UNIX, Linux ose Ëindoës. Disa furnizues përfshirë ETAP, NARI, PSI-CNI dhe Siemens vazhdojnë të ofrojnë zgjidhje me bazë UNIX. Tani është e zakonshme që furnizuesit të integrojnë zgjidhje të bazuara në UNIX ose në platformën Sun Solaris ose në IBM. Sistemet më të reja EMS zënë një pjesë të hapësirës së kërkuar më parë. Për shembull, një raft me 20 servera zë të njëjtën hapësirë me atë të zënë më parë nga një server i vetëm MicroVAX.

Fig 6. Evolimi i softuerit të EMS

Nënstacionet e Tensionit të lartë (TL)

Nënstacioni është një pjesë e një sistemi të gjenerimit, transmetimit dhe shpërndarjes elektrike. Nënstacionet shndërrojnë tensionin nga i lartë në të ulët dhe anasjelltas, ose kryejnë ndonjë nga funksionet e tjera të rëndësishme. Midis stacionit gjenerues dhe konsumatorit, energjia elektrike mund të rrjedhë nëpër disa nënstacione në nivele të ndryshme të tensionit. Një nënstacion mund të përfshijë transformatorët për të ndryshuar nivelet e tensionit ndërmjet tensioneve të larta të transmetimit dhe tensioneve më të ulët të shpërndarjes, ose në ndërlidhjen e dy voltazheve të ndryshme të transmetimit.

Zbatime të ndryshme të nënstacioneve çojnë në nënstacione të TL me dhe pa transformatorë

të energjisë. Ndër funksionet që ndodhin gjatë këtij veprimi janë:

1. Rritja nga një gjenerator tensioni në një sistem të tensionit të lartë (TM / TL)
    a. Termocentralet (në qendrat e ngarkesës).
    b. Termocentralet me energji të rinovueshme .

2. Transformimi i niveleve të tensionit brenda sistemit të tensionit të lartë (TL / TL).
3. Zbritja në nivelin e tensionit të mesëm të një sistemi shpërndarës (TL / TM).
4. Ndërlidhja në të njëjtin nivel të tensionit.

Nënstacionet e tensionit të lartë përmbajnë jo vetëm pajisjet e tensionit të lartë, të cilat janë të rëndësishme për funksionalitetin në sistemin e furnizimit me energji elektrike. Ato janë planifikuar dhe ndërtuar që të përmbajnë:

- ndërprerës të tensionit të lartë
- ndërprerës të tensionit të mesëm
- përbërës kryesorë siç janë pajisjet dhe transformatorët e tensionit të lartë
- pajisjet ndihmëse

Instalimet e furnizuara në të gjithë botën variojnë nga nënstacionet themelore me një shirit të vetëm për nënstacionet e interkonjeksionit me kabina të shumta, ose një aranzhim ndërprerës dhe gjysmë për voltazhet e vlerësuar deri në 800 kV, rryma me vlera deri në 8,000A. Rryma me qark të shkurtër deri në 100 kA.

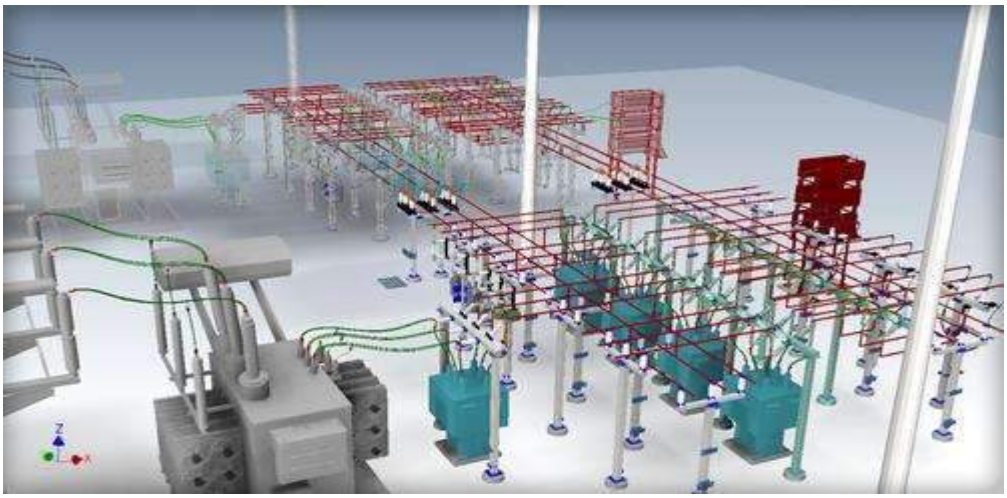


Fig 7. Pamje e një nënstacioni të tensionit të lartë

Nënstacionet e tensionit të lartë janë pika në sistemin energjitik ku energjia elektrike mund të grumbullohet nga burimet gjeneruese, dërgohet dhe shndërrohet, dhe shpërndahet në pikat e ngarkesës. Ato janë të ndërlidhur me njëri-tjetrin, në mënyrë që sistemi i energjisë të bëhet një rrjet i ndërprerë.

Kjo rrit besueshmërinë e sistemit të furnizimit me energji duke siguruar shtigje alternative për rrjedhën e energjisë për t'u kujdesur për çdo emergjencë, në mënyrë që shpërndarja e energjisë në ngarkesa të mbahet dhe gjeneratorët të mos përballen me ndonjë ndërprerje.

Nënstacioni i tensionit të lartë është komponent kritik në sistemin e energjisë, dhe besueshmëria e sistemit të energjisë varet nga nënstacioni. Prandaj, konfigurimi i qarkut të nënstacionit të tensionit të lartë duhet të zgjidhet me kujdes.

Zbarrat janë pjesa e nënstacionit, ku e gjithë fuqia është përqendruar nga degëzimi në hyrje, dhe shpërndahet në degëzimin dalës. Kjo do të thotë se besueshmëria e çdo nënstacioni të tensionit të lartë varet nga besueshmëria e zbarrave të pranishme në sistemin e energjisë.

Një ndërprerje e çdo zbarre mund të ketë efekte dramatike në sistem. Si rezultat, fluksi i energjisë zhvendoset në linjat e shëndetshme që mbijetojnë që tani po mbajnë më shumë fuqi sesa që janë në gjendje. Kjo çon në rrëzimin e këtyre linjave dhe ky efekt vazhdon derisa të ketë një ndërprerje ose situatë të ngjashme.
Rëndësia e besueshmërisë së zbarrave duhet të mbahet në mend kur të hidhni një vështrim në sistemet e ndryshme të zbarrave që janë të përhapura.

Tema 9: Sistemet periferike HMI, GUI

Përkufizimi i një sistemi HMI
Një sistem HMI (*En. Human-Machine Interface, Al. Ndërfaqja njëri-përdorues*) është një ndërfaqe përdoruesi ose panel kontrolli që lidh një person me një makineri, sistem ose pajisje. Ndërsa termi teknikisht mund të zbatohet për çdo ekran që e lejon një përdorues të ndërveprojë me një pajisje, HMI përdoret më së shpeshti në kontekstin e një procesi industrial. GUI (*Graphic User Interface*) shpesh shfrytëzohet brenda HMI për aftësitë e vizualizimit.
Në mjediset industriale, HMI mund të përdoren për të:

- Shfaqur të dhënat vizualisht
- Të ndjekur kohën e prodhimit, tendencat dhe etiketat
- Të mbikëqyrur Treguesin e Performancës
- Monitoruar hyrjet dhe daljet e makinerisë

Ngjashëm me mënyrën se si do të ndërvepronit me sistemin tuaj të kondicionimit për të kontrolluar dhe kontrolluar temperaturën në shtëpinë tuaj, një operator i fabrikës mund të përdorë një HMI për të kontrolluar dhe komanduar temperaturën e një rezervuari industrial të ujit, ose për të parë nëse një pompë e caktuar në objekt po funksionon apo jo.
HMI vijnë në një larmi formash, nga ekranet e integruara në makina, te monitorët e kompjuterëve apo tabletët, por pavarësisht nga formati i tyre ose cilin term përdorni për t'iu referuar, qëllimi është të sigurojnë njohuri për performancën mekanike dhe ecurinë.

Përdorimet më të zakonshme të HMI
HMI komunikojnë me Kontrolluesit e Programueshëm Logjikë (PLC) dhe sensorët e hyrjes/daljes për të marrë dhe shfaqur informacione që për përdoruesit janë të rëndësishme.

Ekranet HMI mund të përdoren për një funksion të vetëm, si monitorimi dhe gjurmimi, ose për kryerjen e operacioneve më të sofistikuara, si fikja e makinave ose rritja e shpejtësisë së prodhimit, në varësi të mënyrës se si implementohen.
HMI-të përdoren për të optimizuar një proces industrial duke dixhitalizuar dhe centralizuar të dhënat për një shikues. Duke përdorur HMI, operatorët mund të shohin informacione të rëndësishme të shfaqura në grafikë, diagrame ose tabela dixhitale, të shikojnë dhe menaxhojnë alarme dhe të lidhen me sistemet SCADA apo MES.
Më parë, operatorëve u duhej të lëviznin nga një makineri në tjetrën vazhdimisht për të kontrolluar ecurinë mekanik të proceseve prodhuese dhe për ta regjistruar atë në një letër ose tabelë të bardhë. Duke lejuar PLC-të të komunikojnë informacionin në kohë reale drejtpërdrejt në një ekran HMI, teknologjia HMI eliminon nevojën për këtë praktikë të vjetëruar dhe në këtë mënyrë zvogëlon shumë probleme të kushtueshme të shkaktuara nga mungesa e informacionit ose gabimit njerëzor.
Në dekadën e kaluar, ndryshimi i nevojave operacionale të biznesit ka nxitur zhvillime interesante në teknologjinë HMI. Tani, është duke u bërë më e zakonshme të shohim forma të evoluara të HMI të tilla si HMI me performancë të lartë, ekranet me prekje dhe pajisjet mobile, së bashku me modelet më tradicionale. Këto ndërfaqe të modernizuara po krijojnë më shumë mundësi për ndërveprim dhe analizë të pajisjeve.

HMI me performancë të lartë
Operatorët dhe përdoruesit gjithnjë e më shumë po shkojnë drejt HMI me performancë të lartë, një metodë e dizajnit HMI që ndihmon në sigurimin e ndërveprimit të shpejtë dhe efektiv. Vetëm duke tërhequr vëmendjen ndaj treguesve më të nevojshëm ose kritikë në ndërfaqen, kjo teknikë e projektimit ndihmon shikuesin të shohë dhe t'i përgjigjet problemeve në mënyrë më efikase, si dhe të marrë vendime më të informuara. Elemente të tjerë të dizajnit, si ngjyra, madhësia dhe vendosja, përdoren për të optimizuar përvojën e përdoruesit.
Disa HMI të performancës së lartë janë:

Ekranet me prekje dhe pajisjet mobile: Ekranet me prekje dhe HMI celular janë dy shembuj të përparimeve teknologjike që janë shfaqur me ardhjen e telefonave inteligjentë. Në vend të butonave dhe çelsave, HMI-të e modernizuara lejojnë operatorët të prekin ekranin fizik për të hyrë në proceset kontrolluese. Mobile HMI ofron një larmi avantazhesh për operatorët, duke përfshirë qasjen e menjëhershme në informacionin HMI dhe monitorimin në distancë.

Monitorimi në distancë: Monitorimi në distancë nga celularët lejon fleksibilitet dhe qasje më të madhe për operatorët dhe menaxhuesit e sistemeve. Me këtë veçori, një inxhinier i sistemit të kontrollit jashtë vendit mund, për shembull, të vendosë temperaturën e një depoje në një pajisje portative, duke eleminuar nevojën për mbikëqyrjen pas orëve të punës.

Edge-of-Network dhe HMI: HMI-të e rrjetit janë gjithashtu shumë të kërkuara sepse lejojnë operatorët të kenë akses në të dhëna dhe vizualizim prej pajisjeve në terren. Për më tepër, është duke u bërë më e zakonshme dërgimi i të dhënave nga HMI-të lokale në cloud, ku mund të arrihen dhe të analizohen në distancë, duke mbajtur aftësitë e kontrollit në nivel lokal.

Përkufizimi i një GUI
Një GUI (Graphic User Interface) është një sistem kontrolli që lejon një përdorues të kryejë komanda në një kompjuter ose pajisje elektronike përmes përdorimit të ikonave dhe imazheve të tjera të krijuara dixhitalisht. Një shembull i zakonshëm është një smartphone ose tabletë me prekje. Pajisjet mobile me ekran me prekje të këtilla, shfaqin pamje në ekran, me

të cilat përdoruesi mund të bashkëveprojë për të kontrolluar pajisjen. Nëse një përdorues dëshiron të hyjë në internet përmes një tablete, mund të prekë ikonën për web browser-in e pajisjes. Për shkak se ndërfaqja është krijuar dixhitalisht në ekran, ajo konsiderohet një GUI.
Ndërfaqja grafike e përdoruesit, e zhvilluar në fund të viteve 1970 nga laboratori kërkimor Xerox Palo Alto dhe i vendosur komercialisht në Macintosh të Apple dhe sistemet operative Windows të Microsoft-it, u krijua si një përgjigje ndaj problemit të përdorimit joefikas në ndërfaqet e hershme, të bazuara në tekst, me rresht komandash për përdoruesin mesatar.
GUI do të bëhen standardi i dizajnit me në qendër përdoruesin në programimin e aplikacioneve softuerike, duke u siguruar përdoruesve aftësinë për të komanduar në mënyrë intuitive kompjuterët dhe pajisjet e tjera elektronike përmes manipulimit të drejtpërdrejtë të ikonave grafike si butona, shirita lëvizës, dritare, skeda, menu, kursorë, dhe mouse. Shumë ndërfaqe moderne grafike të përdoruesit paraqesin ekran me prekje dhe aftësi ndërveprimi me komandë zanore.

Parimi i punës së GUI
Parimet e projektimit të GUI përputhen me modelin e softuerit *pamje-kontrollues*, i cili veçon mënyrën sesi informacioni përpunohet së brendshmi nga mënyra sesi informacioni i paraqitet përdoruesit, duke rezultuar në një platformë ku përdoruesve u tregohen se cilat funksione janë të disponueshme në vend që t'u kërkohet shkrimi i komandave. Përdoruesit ndërveprojnë me informacionin duke komanduar opsione vizuale, të cilat janë krijuar për t'u përgjigjur në përputhje me llojin e të dhënave që ata mbajnë dhe mbështesin veprimet e nevojshme për të përfunduar detyrën e përdoruesit.
Pamja e një sistemi operimi ose softueri aplikacioni mund të ridizenjohet sipas dëshirës për shkak të vetë natyrës së ndërfaqeve grafike të përdoruesit që janë të pavarura nga funksionet e aplikacionit. Aplikacionet zakonisht implementojnë elementet e tyre unike grafik përveç atyre të pranishëm në sistemin ekzistues të operimit. Një ndërfaqe tipike grafike e përdorimit gjithashtu përfshin formate standarde për grafikë dhe tekst.
Testimi grafik i ndërfaqes së përdoruesit i referohet procesit sistematik të gjenerimit të rasteve të provës me qëllim vlerësimin e funksionalitetit të sistemit dhe elementeve të tij të dizajnit. Mjetet grafike të testimit të ndërfaqes së përdoruesit, të cilat janë manuale ose të automatizuara dhe që zbatohen zakonisht nga operatorë të palëve të treta, janë në dispozicion nën një shumëllojshmëri licencash dhe mbështeten nga një shumëllojshmëri platformash. Shembuj të njohur përfshijnë: Tricentis Tosca, Squish GUI Tester, Unified Functional Testing (UFT), Maveryx, Appium dhe eggPlant Functional.

Shembuj të përdorimit të GUI
Sketchpad, që besohet të jetë programi i parë grafik i dizajnit i projektuar për t;u përdorur në kompjuter, i zhvilluar në 1962 nga Ivan Sutherland, përbëhej nga një stilolaps me dritë i cili u mundësoi përdoruesve të krijonin dhe manipulonin objekte në vizatime inxhinierike në kohë reale me grafikë të koordinuar.
Sistemet moderne të operimit dhe ndërfaqet grafike të përdoruesit janë të inkoorporuara në pothuajse çdo aplikacion ndërveprues, të tilla si ATM, arkat e vetë-shërbimit, check-in dhe check-out të biletave, vidoe-lojërat, smartphone-t, etj. Disa shembuj gjerësisht të njohur të ndërfaqeve grafike moderne, përfshijnë Microsoft Windows, macOS, Ubuntu Unity dhe GNOME Shell për ambiente desktop dhe Android, iOS të Apple, BlackBerry OS, Windows 10 Mobile, Palm OS-WebOS dhe Firefox OS për smartphone.

Avantazhe të GUI
Avantazhi i një ndërfaqe grafike është mundësia për t'u përdorur gjerësisht prej njerëzve. Vetë veçoritë e një ndërfaqe grafike i përafrohen përqasejeve dhe termave të njohur gjerësisht, siç është drag&drop (zvarritja dhe rënia) për transferimin e skedarëve apo

përdorimi i ikonave të njohura, të tilla si një koshi i mbeturinave për skedarët e fshirë, duke mundësuar kështu një mjedis në të cilin veprimet në kompjuter janë intuitive dhe kontrollohen lehtësisht pa ndonjë patur nevojë për njohuri paraprake kompjuterike. Ikonat e aplikacioneve të GUI janë vetëpërshkruese

Ndryshimi ndërmjet HMI dhe GUI
Dallimi kryesor midis HMI dhe GUI qëndron në mënyrën e tyre të funksionimit. GUI karakterizohen nga përdorimi i pamjeve të krijuara dixhitalisht që shërbejnë si ndërfaqe, ndërsa HMI përfshijnë të gjitha llojet e ndërfaqeve - duke supozuar se ato përdoren për të kontrolluar një makinë ose pjesë të pajisjeve.
Disa HMI përmbajnë ose përbëhen nga një GUI. Të tjerët, megjithatë, nuk mbështeten në pamje të krijuara dixhitalisht për ndërfaqen. HMI e një makine mund të përfshijë asgjë më shumë sesa rrotëzat e kontrollit dhe butonat. Edhe pa ekran, një operator mund të kontrollojë makinerinë e lidhur përmes komandimit të butonave HMI. HMI-të përdoren kryesisht në sektorët e prodhimi, ndërsa GUI-të përdoren si në sektorët tregtar ashtu edhe në sektorët jo-tregtarë.

Figura 9.1 HMI dhe GUI

Me pak fjalë, një HMI është një sistem kontrolli që lejon një operator njerëzor të kontrollojë një makinë ose pjesë të pajisjeve. Në krahasim, një GUI është një ndërfaqe e krijuar dixhitalisht që përdoret për të kontrolluar një pajisje elektronike.

Tema 10: Të dhënat, magazinimi, kartat e komunikimit, Back-up, Restore.

Fatmirësisht, çdo kompjuter na ofron në ditët e sotme disa mjete të cilat e lehtësojnë shumë punën tonë me të dhënat digjitale. Këto mjete janë të integruara në sistemin e operimit të kompjuterit tonë dhe na ofrojnë mundësinë që të punojmë me të dhënat duke i: modifikuar, ruajtur, nxjerrë ato si *output* në pajisje të ndryshme (USB, CD, DVD) etj. Për përdoruesin normal, këto programe që na ofron kompjuteri janë të mjaftueshme, por, në rastet profesionale, do të duhej të mbështeteshim në programe të treta, që janë të përshtatura për profesionistët dhe mund t'i instalojmë. Përpara se t'i shohim vetë mjetet që përdoren për të menaxhuar të dhënat digjitale, në fillim duhet të kuptojmë nëse kompjuteri është në gjendje t'i përpunojë këto të dhëna dhe të bëjë ruajtjen e tyre.

Llojet e të dhënave digjitale
Më poshtë do të merremi me llojet më të përdorshme të të dhënave kryesore digjitale, që kryesisht janë:

1. *tekst;*
2. *imazhe;*
3. *video;*

4. *audio.*

1.Tekst

Nga të gjitha llojet e të dhënave, këta tipa të dhënash janë ato që kanë kërkesat më të pakta kompjuterike, duke filluar me hapësirën e vogël që zënë në hard disk e deri duke mos angazhuar shumë procesorin.

Formatet e tekstit

• Dokumente tekst

Ky lloj formati mund të përpunohet shumë lehë me çfarëdo programi. Një nga mjetet që kompjuteri na ofron për këtë format është programi *Notepad.* Dokumentet e këtij formati mbarojnë me *.txt.*

• Dokumente Word-i (Microsoft Word)

Ky lloj formati përpunohet duke përdorur programin *Microsoft Word*. Dokumentet e këtij formati mbarojnë me *.docx*.

• Dokumente PDF

Ky lloj formati dokumentesh ka përdorim të gjerë në ditët e sotme. Kompjuteri nuk na ofron program për leximin e këtij formati, por mund të shkarkojmë dhe të instalojmë programin *Acrobat Reader*, që është falas dhe na plotëson shumicën e nevojave që kemi për të kryer mbi *PDF*. Zakonisht, skedarët ruhen në këtë format për të mos i përpunuar më tutje. Dokumente të këtij formati mbarojnë me .pdf.

2. Imazhe

Këta tipa të dhënash kanë kërkesa më të larta se ato më sipër. Programet profesionale që përdoren për përpunimn e këtyrë të dhënave kërkojnë fuqi kompjuterike të lartë dhe pajisje bashkëkohore.

Formatet e imazheve

• JPG

Dallimi kryesor në formatet e imazheve është cilësia e imazhit dhe madhësia e tij. *JPG* ka qenë dhe është formati më i përdorur në internet dhe kudo. Duhet treguar kujdes të mos e përdorim në imazhe ku detajet janë të rëndësishme, si në: imazhet e artit, tipografi, imazhe me viza të qarta etj. Imazhet e këtij formati mbarojnë me .jpg ose .jpeg.

• PNG

PNG është një format shumë i mirë kur duam të përdorim imazhe me pjesë transparente. Duke qenë transparente, këto pjesë marrin ngjyrën e sfondit ku ndodhen, duke na dhënë fleksibilitet në përdorim dhe mundësinë të arrijmë gjëra që me formatet e tjera do të ishte e pamundur. Ky format mund të kompresohet, por madhësia e imazhit do të jetë më e madhe se në formatet e tjera. Imazhet e këtij formati mbarojnë me .png.

• GIF

Edhe formati *GIF* përdor kompresim për të ulur madhësinë e imazhit dhe, për këtë arsye, ka gjetur përdorim në pjesën e internetit. *GIF* i përket së kaluarës dhe nuk përdoret në fushën e fotografisë moderne. Një nga specifikimet që e dallojnë formatin *GIF*, është mundësia e animacionit ose, më qartë, e një fotografie që lëviz. Imazhet e këtij formati mbarojnë me .gif.

• ***BPG***
Ky është një format i ri dhe qëllimi kryesor është të zëvendësojë formatin *JPG*. Specifika kryesore e këtij formati është që, për të njëjtën cilësi, ofron madhësi më të vogël se formati *JPG*. Imazhet e këtij formati mbarojnë me .bpg.

3. Video
Të dhënat digjitale të tipit video janë ato që kanë kërkesat më të larta kompjuterike, këto lloje të dhënash kërkojnë procesor dhe *RAM* të fuqishëm, po ashtu sugjerohet kartë grafike e dedikuar. Përsa i përket hard diskut, këto të dhëna zënë pjesën më të madhe, me rritjen e cilësisë në HD (*High Definiton*), një video njëminutëshe e regjistruar nga një *iPhone* shkon rreth 1GB në madhësi.

Formatet e videove

• ***AVI***
AVI është një format videoje i prezantuar nga *Microsoft* dhe në shumicën e rasteve është ideal në pajisje *Windows*. Formati *AVI* nuk i mbështet pajisjet *Apple* dhe, nëse duam të shohim një video në ato pajisje, do të duhet të përdorim format tjetër. Për sa i përket madhësisë së skedarit *AVI*, ai është i pakompresuar dhe zë shumë hapësirë në hard disk (1 orë video *AVI* zë rreth 33 GB hapësirë). Videot e këtij formati mbarojnë me .avi.

• ***MPEG***
Ndryshe nga *AVI*, *MPEG* mbështet çdo lloj pajisje, qoftë *Apple*, *Android*, *Microsoft* etj., dhe përdor kompresim duke e ulur në mënyrë drastike madhësinë e skedarit dhe në mënyrë të papërfillshme cilësinë e videos. Nëse në rastin më sipër do të kishim formatin *MPEG*, videoja njëorëshe do të ishte vetëm 650 MB. Madhësia më e vogël na rrit performancën kur duam të modifikojmë videon. Videot e këtij formati mbarojnë me .mpg.

• ***MP4***
MP4 është aktualisht formati më i përdorur në botë, duke pasur si përdorim primar internetin. Për këtë arsye gjen përdorim pothuajse në çdo pajisje që përdoret nga konsumatorët sot. *MP4* përdor kompresim, kështu që madhësia që përdor në hard disk është deri diku e vogël. Videot e këtij formati mbarojnë me .mp4.

• ***FLV***
FLV është konkurrenti më i afërt i formatit *MP4*. Të dyja këto formate e kanë përdorimin kryesor në internet dhe përdoren nga kompani të mëdha, si: *Youtube*, *Hulu* dhe shumë të tjera. *FLV* ka kufizime për sa i përket përdorimit në pajisjet mobile; *Apple* nuk e suporton si format në pajisjet e saj.

Për të luajtur formatet video të mësipërme, kompjuteri na ofron programin Windows Media Player, por një alternativë tjetër që na jep mundësinë për të luajtur pothuajse çdolloj formati video që ekziston është VLC Player.

4. Audio

Audio përmban formate të ndryshme, ku secili prej tyre ka avantazhet e tij. Formatet *audio* ndahen në *lossless* (jo i kompresuar) dhe *lossy* (i kompresuar). Dallimi kryesor ndërmjet tyre është që formati *lossless* ruan cilësinë origjinale të regjistrimit, duke na ofruar cilësi tepër të lartë dhe madhësia e skedarit, gjithashtu, është e lartë; *lossy* bën kompresimin e audios, duke ulur madhësinë e skedarit, por duke ulur edhe cilësinë.

• ***WAV***

Formati *WAV* bën pjesë në tipin e pakompresuar (*lossless*). Ky format përdoret shumë në studio muzikore, për arsye të cilësisë së lartë që ruan. Sigurisht që me cilësinë kemi rritje madhësie.

• ***MP3***

MP3 është formati më i përdorshëm në botë për arsye se përdor kompresim (*lossy*), që e bën të favorshëm për internet dhe të suportueshëm nga shumica e pajisjeve. *MP3* është kthyer në sinonim për muzikën, falë përdorimit të gjerë të tij.

• ***AAC***

AAC është si *MP3*, por pak më efikas, në kuptimin që mund të kemi skedarë që zënë më pak hapësirë duke ruajtur cilësinë. *AAC* u bë e famshme nga *Apple Itunes* dhe po fiton popullaritet dita-ditës.

Pajisjet e magazinimit

Përpara se kompjuteri ynë të përpunojë të dhënat tona, duhet një mënyrë për t'i future këto të dhëna në kompjuter dhe pastaj të marrim rezultatin e dalë nga këto të dhëna. Ky rezultat mund të na shfaqet në monitor, në letër (print), në format audio, në format video etj.

Sigurisht, që nga pajisjet më multifunksionale dhe më të rëndësishme në botën e sotme TIK, janë pajisjet e magazinimit, që përfshijnë nga një *USB (Flash Drive)* të vogël, deri te pajisjet e përdorura për të ruajtur sasi të mëdha të dhënash. Kur ne hedhim disa këngë që kemi në kompjuter në një USB, kryejmë një funksion *output*, duke përdorur *USB*-në. Po ashtu, nëse këtë USB ia japim një mikut tonë, për t'i hedhur këto këngë në kompjuterin e tij, ai kryen një funksion *input*, pra nga *USB*-ja jonë te kompjuteri i tij.

Pajisjet e magazinimit janë dy formash: të brendshme dhe të jashtme.

Të brendshme janë ato pajisje që ndodhen brenda kompjuterit tonë dhe shërbejnë për të ruajtur të dhënat tona, ndërsa të jashmet, që në shumicën e rasteve lidhen me anë të *USB*-së, i kemi portabël dhe mund t'i lidhim shumë kollaj nga një kompjuter në një tjetër.

Modulet RAM

RAM-i është memoria afatshkurtër e kompjuterit, e cila përdoret sa herë që kompjuteri ynë do të ruajë të dhëna përkohësisht dhe t'i tërheqë kur ka nevojë. Quhet afatshkurtër për arsye se, nëse e mbyllim kompjuterin, të dhënat që ndodhen në memorien RAM zhduken.

Hard disku

Hard disku është memoria afatgjatë e kompjuterit, që do të thotë se, nëse e fikim

kompjuterin, përsëri i kemi të ruajtura të dhënat tona. Kjo është arsyeja që *hard disku* është vendi ku ne ruajmë programet, dokumentet, fotografitë dhe çdo gjë tjetër në kompjuterin tonë.

Pajisjet ruajtëse optike, magnetike dhe flash. Karakteristikat e tyre

Disku i ngurtë

Një *hard drive disk* (HDD) është një pajisje ruajtëse që përmban disqe magnetike të cilat rrotullohen me shpejtësi të lartë për të lexuar dhe shkruar informacionet. *Hard disku* na mundëson ruajtjen e të dhënave edhe kur kompjuteri është i fikur, pra është një memorje sekondare që ruan të dhënat në mënyrë të përhershme. Një *hard disk* ndodhet brenda një *hard drive* i cili lexon dhe shkruan të dhënat. *Hard drive* gjithashtu transmeton të dhënat ndërmjet CPU-së dhe disk-ut.

Pajisja më e madhe ruajtëse *hardware*-ike e kompjuterit konsiderohet vetë *hard disk*-u i cili ndodhet brenda kasës së kompjuterit.

Përveç qëllimit për të ruajtur dhe lexuar të dhënat, përmban edhe sistemin operativ dhe aplikacionet. Disku i ngurtë zakonisht është i konfiguruar si njësia e parë në renditjen për startim të kompjuterit. Shpejtësia e një disku të ngurtë matet me numrin e rrotullimeve për minutë (Revolution per Minute) – RPM. Koha e kërkimit është koha e nevojshme nga momenti kur procesorit i paraqitet kërkesa për një skedar deri në momentin kur fillon të shfaqet bajti i parë i këtij skedari. Kjo kohë e kërkimit është 10 deri 20 milisekonda. HDD është i përbërë nga disqe të mbuluara nga një shtresë materiali magnetik.

Pajisja e Hard Disk-ut

Njësitë matëse të *hard diskut*

Çdo gjë që mund të ruhet në një *hard disk* matet duke u bazuar në madhësinë e saj. E dimë që një tekst zë shumë pak kapacitet, fotografitë pak më shumë se teksti dhe videot duan hapësirë më të madhe. *Hard disku* nuk e di dallimin ndërmjet elementeve, ai e di vetëm madhësinë e tyre, të cilat maten me megabajt (MB), gigabajt (GB) dhe terabytes (TB).

Kë duhet të zgjedhim?

Nëse duam të transferojmë skedarë midis kompjuterave ose nëse kemi nevojë për një disk për të ruajtur vetëm disa nga të dhënat tuaja, do të jetë i mjaftueshëm një kapacitet relativisht i vogël (p.sh. 500 GB).

Përparësitë e Hard Disk-ut

Hard Disk-u është përgjegjës për ruajtjen e informacionit. Çdo gjë që mbajmë në kompjuter ruhet në një *hard disk*. Jo vetëm dokumente, foto, muzikë dhe video, por edhe programet tuaja, preferencat tuaja, madje edhe sistemi operativ ruhet në hard disk.

Disavantazhet

Nëse *hard disku* dëmtohet, mund të humbasim të gjitha të dhënat që kemi ruajtur në të. Kjo

është arsyeja pse shumë përdorues kanë një sistem rezervë. Në këtë mënyrë, ata janë të pajisur me një disk të dytë në të cilën ata kopjojnë të gjitha dosjet e tyre të rëndësishme.

Llojet e Hard disqeve

Hard disqet ndahen në 2 kategori:

• *Disqet e jashtme* lidhen me kompjuterat ose sistemet kompjuterike nga jashtë me ndihmë të kabllove të ndryshëm.

• *Disqet e brendshme HDD* (hard disk drive) janë instaluar brenda njësisë qendrore dhe kanë lidhje specifike si për fuqinë ashtu edhe për transmetimin e informacionit. Një disk I brendshëm ofron ruajtje të integruar të të dhënave dhe shpejtësi maksimale. Një disk I jashtëm garanton fleksibilitet më të madh dhe ruajtje të përhershme kur kemi nevojë për të.

Lidhja e hard disk-ut me kompjuterin

Ekzistojnë katër metoda kryesore për lidhjen e *hard diskut*:

1. USB. Ky është lloji më i zakonshëm i lidhjes dhe nuk kërkon ndonjë konfigurim. Mjafton ta vendosim në portë dhe kompjuteri e njeh *drive*-in dhe mund të lexojmë dhe ruajmë skedarët pothuajse në çast.

2. Firewire. Plug-and-play: shërben si USB, por është shumë më i shpejtë, gjë që shpjegon përhapjen e saj masive për transferimin e skedarëve video.

3. SATA. Kjo është lidhja standarde për disqet e brendshme. Ofron shpejtësinë më të mirë të transferimit të skedarëve, pavarësisht formatit.

4. eSATA. Lidhja më pak e zakonshme dhe shumë e fuqishme, e përdorur shpesh në PC. Një lidhje **eSATA** vepron në një shpejtësi afërsisht të barabartë me atë të një drive të brendshëm.

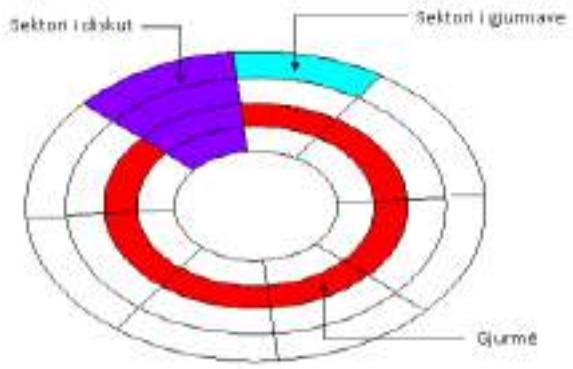
Shpejtësia e hard drive

Pllaka magnetike është pjesa më kryesore dhe kjo pjesë rrotullohet me shpejtësi prej 3200 deri 10000 rrot/min. Sa më shpejt të rrotullohet pllaka aq më shpejt e gjen *hard disku* skedarin që po kërkojmë ose e shkruan. Një disk me shpejtësi prej 7,200 rpm është më i shpejtë sesa një disk me shpejtësi 5,400 rpm. Për të rritur sasinë e ruajtjeve të të dhënave, *hard disku* ka pllaka të shumëfishta (multiple platters). Koka lexuese/shkruese është e rëndësishme për shpejtësinë dhe performancën e *hard diskut*.

Koka lexuese/shkruese e hard diskut

Të dhënat ruhen në sipërfaqe të pllakës të ndara në sektorë dhe gjurmë. Gjurmat janë në

formë të rrathëve, ndërsa sektorët janë ndarje në formë të segmenteve, si më poshtë:



Pjesët përbërëse të diskut të ngurtë

DVD-ROM, CD-ROM, krahasimet

DVD (Digital Versatile Disc) është një disk i aftë për ruajtjen e sasive të mëdha të të dhënave me madhësinë e një kompakt disku standard. Disqet DVD u shitën së pari në vitin 1997. Ato u përdoren gjerësisht për ruajtjen dhe parë filmat dhe të dhëna të tjera. Për të luajtur DVD-në në një kompjuter duhet të kemi një DVD drive dhe një softuer që luan DVD-në.

CD (Compact Disc) gjithashtu përdoret për ruajtjen e programeve, të dhënave të ndryshme, muzikës, videos etj. Fizikisht, një DVD dhe CD duken të njëjta. Të dy disqet kanë të njëjtën madhësi dhe zakonisht kanë një anë me një etiketë dhe anën tjetër që lexon lazeri, përveçse nëse është një *DVD* me dy anë. Megjithatë, teknologjia nga e cila përbëhet një DVD lejon që disku me të njëjtën madhësi të mbajë më shumë të dhëna sesa një CD. CD-të kanë përafërsisht kapacitet prej 600 – 800 MB, ndërsa DVD-të kanë kapacitet prej disa GB.

Pajisja luajtëse e CD/DVD ROM dhe CD

Përdorueshmëria e tyre

DVD, CD-të janë ende shumë të njohura e të përdorura gjerësisht. Për shkak të teknologjive më të reja si disqet *Blu-ray* dhe shërbimet e transmetimit si *Netflix* dhe shërbimet e tjera Cloud computing, shitjet dhe përdorimi i DVD-ve, CD-ve, ka rënë ndjeshëm.

USB Flash Driver

Një USB Flash Drive është një pajisje ruajtëse e të dhënave që përfshin kujtesën flash në një ndërfaqe të integruar USB. Zakonisht është i lëvizshëm, i rishkrueshëm dhe shumë më i vogël se një disk optik. USB-ja flash drive i parë doli në treg në vitin 2000 me një kapacitet ruajtjeje prej 8 MB. Tashmë ata kanë kapacitete që variojnë nga 8 GB deri në 1 TB, në varësi të prodhuesit dhe nivelet e kapaciteteve të ardhshme priten të arrijnë në 2 TB.

Përparësitë e USB flash driver

• USB flash driver-at janë të vogla dhe të lehta dhe përdorin

pak energji. Pajisjet janë mjaft të forta për të përballuar goditjet mekanike, gërvishtjet dhe pluhurin, dhe në përgjithësi janë të papërshkueshme nga uji.
• USB flash driver-at mund të mbajnë të dhënat për periudha të gjata edhe kur pajisja është e shkëputur nga kompjuteri ose kur kompjuteri është i fikur. Kjo e bën USB-në të përshtatshme për transferimin lehtësisht të të dhënave nga një kompjuter në një tjetër. Ata përdoren dhe për backup (ruajtje të kopjes së të dhënave).
• Ndryshe nga shumica e disqeve të lëvizshme, një USB flash drive nuk kërkon bateri ose furnizim të jashtëm të energjisë dhe nuk është i varur nga platforma.

Mangësitë e USB flash driver
• USB-të duke qenë se kalojnë të dhëna nga një kompjuter në një tjetër kanë shanse ekspozimi ndaj marrin viruseve.
• Rrjedhja e të dhënave është një problem sepse pajisjet janë të lëvizshme dhe të vështira për t'u ndjekur. Nëse një sistem është i infektuar, atëherë edhe USB-ja infektohet dhe të dhënat që ka mund të humbasin.

Ruajtja e informacioneve në kompjuter dhe protokollet *backup*
Shpesh, gjatë punës në kompjuter, na ka ndodhur që informacione të ndryshme të kenë humbur, pasi kompjuteri është prishur në çast. Çfarë duhet të bëjmë për t'i ruajtur këto informacione?

Rëndësia e ruajtjes së informacionit në kompjuter
Sot, kompjuterat luajnë një rol të rëndësishëm në jetën tonë të përditshme, na lehtësojnë: marrjen e informacioneve, përpunimin dhe shkëmbimin e informacioneve të ndryshme, për të cilat do të na duhej shumë kohë pa këto pajisje kompjuterike. Zhvillimet e teknologjisë kanë bërë të mundur që çdo informacion të rëndësishëm ta kalojmë te pajisje, si: *smartfon (smartphone), tablet*, kompjuter etj.
Kompjuterat nuk janë të përsosur dhe ky fakt na përball me një problem tepër të rëndësishëm, i cili është siguria e këtij informacioni që mbajnë këto pajisje. Kush na e siguron ruajtjen dhe moscenimin e këtij informacioni kaq të rëndësishëm për ne?
Imagjinoni një kompjuter në bankë që mban të gjitha të dhënat financiare të klientëve dhe, papritur, ky kompjuter të prishej. Të dhënat e klientëve do të humbisnin. Kjo do ishte një katastrofë për bankën dhe klientët e saj. Po ashtu mendoni që në kompjuterin tuaj keni fotografi të të gjitha udhëtimeve që keni bërë gjatë jetës suaj dhe çdo gjë do të humbte për arsye se kompjuteri juaj do të prishej në çast. Në vitin 2014, kompania e njohur "Sony" ra pre e një sulmi kibernetik, ku piratët fshinë një masë të madhe të dhënash nga serverat e kësaj kompanie. Dëmi llogaritej në miliona dollarë, por ky dëm i shkaktuar u kufizua shumë nga fakti që kompani serioze, si "Sony", kryejnë praktikat më të mira për sa i përket ruajtjes së të dhënave (*backup*) dhe menaxhimit të tyre.
Në vitin 2011, 8.3 milionë qytetarëve britanikë iu kompromentuan të dhënat e tyre personale për arsye se një laptop i Shërbimit të Shëndetit Kombëtar ra pre e një vjedhjeje. Të dhënat në kompjuter na humbasin për shkaqe të ndryshme, siç mund të jenë: dëmtimi fizik i pajisjes elektronike; vjedhja e saj; fshirja gabimisht e të dhënave; futja e një virusi në sistem etj.

Mbrojta e të dhënave nëpërmjet backup-it
Mbrojtjen më të mirë për ruajtjen e informacionit dhe rikuperimin e tij e mundëson *backup*-i. *Backup do të thotë ruajtja e një kopjeje të informacionit, e cila mund të përdoret në rast të humbjes së informacionit origjinal.*

Llojet e *backup*-eve

1. Local backup - ruajtja e të dhënave bëhet lokalisht në *hard diskun* e kompjuterit ose në një pajisje të jashtme, si: *hard disk, USB drive, CD, DVD* etj.

2. Internet backup - ruajtja e të dhënave bëhet në një server diku në internet *(cloud)*.
Ajo që ne duhet të zgjedhim varet nga disa faktorë, ndër të cilët po përmendim: siguria, koha dhe çmimi. Të dyja mënyrat e sipërpërmendura kanë avantazhet dhe disavantazhet e tyre.

Local backup

Avantazhet: shpejtësi e lartë e ruajtjes së informacionit dhe çmim i ulët.
Disavantazhet: siguri e ulët e ruajtjes së informacionit, pasi pajisjet kompjuterike mund të vidhen ose prishen fizikisht. Nëse jemi të detyruar të bëjmë *backup local*, atëherë është mirë që pajisjen në të cilën kemi bërë *backup* mos ta mbajmë në të njëjtin vend ku janë të dhënat tona origjinale. Kjo për faktin se, e njëjta arsye që bën humbjen e të dhënave origjinale, mund të bëjë dhe humbjen e *backup*-it. Për shembull, nëse USB-në në të cilën kemi bërë *backup*-in *(ruajtjen)* e të dhënave, e mbajmë në të njëjtën çantë me laptopin tonë, një humbje e laptopit na sjell edhe humbjen e *backup*-it.

Internet backup (cloud)

Avantazhet: siguri e lartë për arsye se, çfarëdo që të ndodhë në ambientin tonë lokal, të dhënat gjenden diku në internet dhe mund të aksesohen nga çdo pajisje e jona.
Disavantazhet: ky lloj *backup*-i, shpesh, është më i kushtueshëm dhe më i ngadaltë, për arsye se përdor internetin si mënyrë transmetimi dhe varet nga cilësia e tij.

Mënyrat e ruajtjes së të dhënave

Mësuam pse *backup*-i dhe ruajtja e herëpashershme e të dhënave është kaq kritike në botën e teknologjisë. Si ruhen të dhënat? *Backup*-i i të dhënave mund të kryhet me anë të komandave *Copy* dhe *Paste*. Kjo është mënyra më e thjeshtë, por është e kufizuar, sepse na e vështirëson shumë mënyrën e rikthimit të të dhënave në rast humbjeje.
Ka mënyra më efikase për ruajtjen e të dhënave, që përfshijnë shërbime të integruara në sistemin tonë të operimit, po ashtu dhe programe që mund të instalohen në kompjuterin tonë.

Një nga aplikacionet e integruara është W*indows Backup*, i cili ndodhet në çdo sistem operimi *Windows;* ose *Time Machine* në *Mac*. Nga programet që mund të instalohen po përmendim: *Acronis True Image, EaseUS Todo Backup, Norton Ghost* etj.

Për sa i përket *Internet backup* kemi disa kompani që e ofrojnë si shërbim, ku ndër më kryesoret përmendim: *Google Drive, Microsoft SkyDrive, Apple iCloud, DropBox*.

Praktike

- Klikoni nga kompjuteri juaj në menunë *Start – Control Panel - Backup and Restore.*
- Në opsionin *Set up backup* ruani të dhënat në një folder të kompjuterit tuaj, në një particion tjetër ose në *USB.*
- Fshini folderin nga kompjuteri dhe bëni rikthimin e këtij folderi me shërbimin *Backup and Restore,* që ndodhet në *Control Panel*.

Tema 11: Siguria e rrjeteve të komunikimit

Aspekte të sigurisë në LAN dhe standardet përkatëse

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 përafruar më qartë, si dallohet një gjendje e sigurtë nga një e pasigurtë, ka disa kërkesa bazë (ose objektiva sigurie) që jepen më poshtë:

4. Besueshmëria
5. Integriteti (Tërësia)
6. Vlefshmëria

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 mesazhit. Në qoftë se dërgoni një e-mail tek një marrës i caktuar, ju prisni që vetëm ky i fundit ta lexojë përmbajtjen e tij.
Me qëllim që të garantohet besueshmëria duhen zbatuar masa të ndryshme: për shembull kodimi i të dhënave, ose i 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 korrekte (angl. Integrity). Këtu vlen gjithashtu që të gjenden mundësi, nëpërmjet të calave të pengohen gabimet gjatë transmetimit të të dhënave, ose të paktën të identifikohen dhe të mund të korrigjohen ato. Të dhënat, dokumentat dhe sitemet duhet të mbrohen ndaj manipulimeve.

Kur bëhet e mundur të garantohet apo të konfirmohet integriteti i të dhënave, si dhe të çiftohet informacioni në lidhje me krijuesin apo autorin e të dhënave me marrësin e tyre, krijohet një i ashtuquajtur autenticitet (angl. authenticity) i të dhënave respektive – me fjalë të tjera një nënshkrim dixhital. Autenticiteti paraqet gjithashtu, në një farë mënyre, një pamje të detajuar të integritetit si objektiv sigurie.

Certifikatë autenticiteti

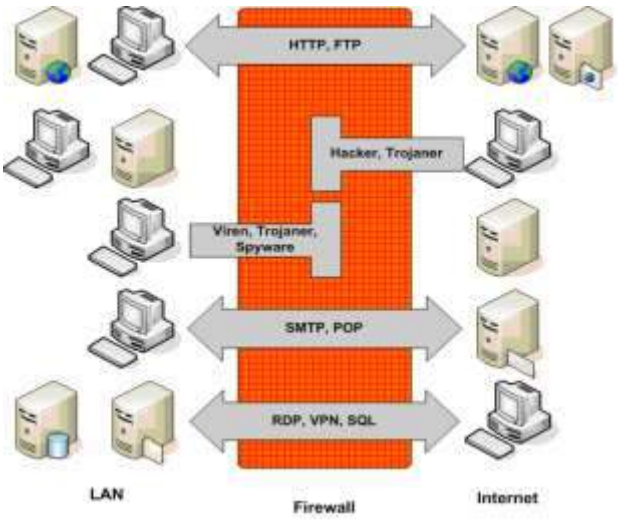
Vlefshmëria

Objektivi i tretë kryesor për sigurinë e të dhënave është vlefshmëria (angl. Availability). Një sistem i sigurtë duhet të mund të garantojë, që të dhënat, të cilat ai përpunon, të jenë të aksesueshme, që shërbimet që ofrohen vërtet të mund të shfrytëzohen.

Vlefshmëria përfshin si rregull, masat mbrojtëse logjike si p.sh. masa ndaj fshirjes gabimisht të të dhënave, si dhe masat, 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, 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 me të cilat duhet të merrej koncepti i vlefshmërisë. Atëhere kur vlefshmëria e shërbimit duhet të jetë e garantuar 24 orë, ekzistojnë zgjidhje të përshtatshme që mundësojnë vlefshmërinë në nivele të tilla të larta, të cilat, nëpërmjet pajisjesh special, algoritmesh të përshtatshme në software, si dhe nëpërmjet hardware-sh speciale provojnë të arrijnë maksimumin e mundshëm të besueshmërisë (angl. reliability), pra të shmangies së rënies së sistemit. P.sh.

- Instruksione për mbrojtjen nga zjarri dhe nga uji te dhomës së serverave
- Blloqe dyfish ushqimi tek serverat
- Lidhje e dyfishtë (redundant) për komunikimin e të dhënave
- Lidhje e dy ose më shumë hard disqeve ne RAID tek serverat

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 aplikacioneve, me qëllim që të pengohen sulmet armiqësore nga rrjeti. Ato sigurojnë kalimin e 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. Firewall-et mund të përdoren edhe midis pjesve të rrjetit që i përkasin një LAN-i. Krahas mbrojtjes nga sulmet firewall-et mund të shfrytëzohen për kufizimin e aksesit të përdoruesve tek adresat dhe shërbimet „e lejuara" jashrë LAN-it. Kështu kufizohet deri diku aksesi në adresa interneti të caktuara. Firewall-et mund të implementohen si zgjidhje hardware apo software.

IDS – Intrusion Detection System (IDS)
IDS është një pajisje apo aplikacion që monitoron rrjetin kompjuterik ose sistemin për aktivitete të dyshimta, keqdashëse, shkelje të politikave të kompanisë duke gjeneruar një raport për administratorët e sistemit. Ai mund të krahasohet me një system alarmi të instaluar në shtëpi/dyqan, i cili bie kur hyjnë hajdutët.

Standardet në fushën e sigurisë së të dhënave
Me qëllim që të zvogëlohen koha dhe kostot e punës për sigurinë, si dhe që të mund të krahasohen më mirë përpjekjet për rritjen e sigurisë, në praktikë përdoren shpesh katalogje me kritere, të cilat mbështesin në punën e tyre personat përgjegjës për sigurinë.
Më poshtë jepen disa nga standarded në fushën e sigurisë:

Taskforce Secure Internet	ISO/IEC 27001:2013
FIPS 140-2	ITSEC/Common Criteria

Rregullat e njohjes së rrjetit
Ç'janë rrjetat kompjuterike? Pse mendoni se njohja e rrjetit është e rëndësishme?
Një rrjet paraqet një grup pajisjesh të lidhura me njëra-tjetrën që mund të komunikojnë ndërmjet tyre. Nëse janë të lidhur të paktën dy kompjutera, të cilët shkëmbejnë informacione ndërmjet tyre, themi se kemi të bëjmë me një rrjet kompjuterik.

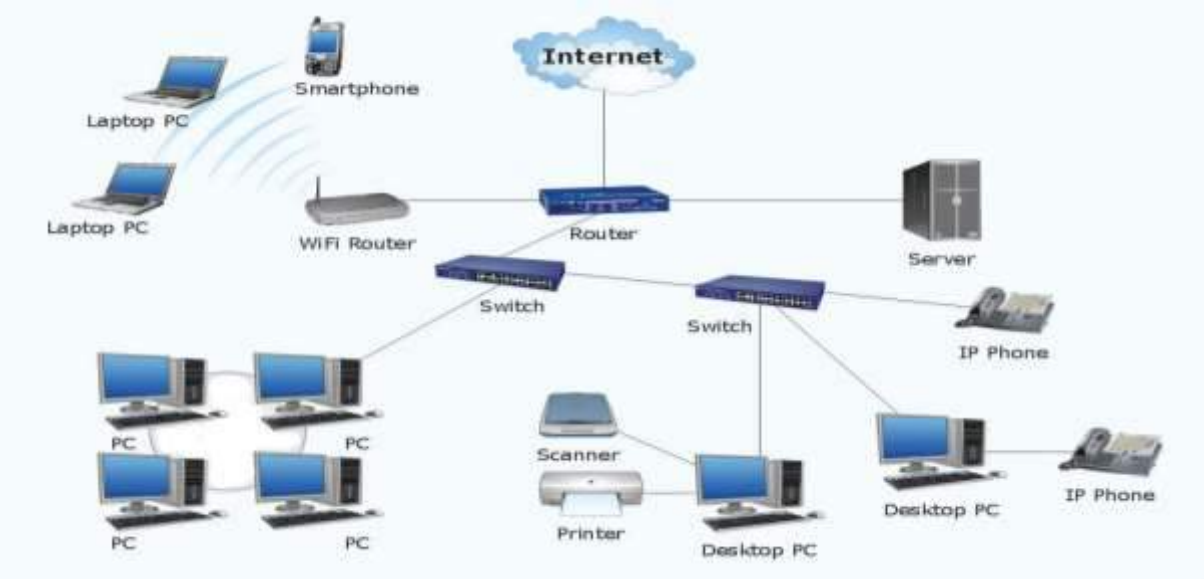
Rrjetet e komunikimit zënë pjesën më të rëndësishme në fushën e *TIK*-ut. Ato janë të kufizuara nga lidhjet fizike. Vëmë re që në aparatët celular nuk kemi asnjë kabëll që lidhet me ta dhe përsëri mund të komunikojmë apo dërgojmë mesazhe, si dhe të aksesojmë internetin. Në këtë rast, lidhja nuk bëhet me kabëll, por me teknologji si *wireless*. Rrjetat kanë ndihmuar që e gjithë bota të afrohet virtualisht. Informacioni në ditët e sotme mund të shpërndahet menjëherë dhe me këdo.

Rëndësia e njohjes së rregullave të rrjetit
Njohja e rregullave të rrjetit na ofron një rrjet më të sigurt, gjë që çon në përmbushjen e kërkesave të çdo individi apo grupe individësh.

Disa nga rregullat për të pasur një rrjet të mire
• **Siguria e informacionit**: Në pjesën më të madhe përdorim lidhjen me kabëll për një rrjet. Nëpërmjet kabllit dërgohen të dhënat nga njëra pajisje në tjetrën. Rrjeti lokal i ngritur, për shembull LAN, përdoret për shkëmbimin e informacioneve në një kompani. Për shembull, njoftimet për punonjësit dërgohen nëpërmjet *email*-it. Edhe nëse në një moment të caktuar marrësi nuk është duke punuar në kompjuterin e tij, informacioni nuk humbet. Kjo sepse të dhënat memorizohen dhe marrësi i merr ato në momentin që ndez kompjuterin dhe identifikohet në të.
• **Përdorimi i përbashkët i të dhënave**: Të dhënat që përdoren nga disa persona, memorizohen në një vend të caktuar në rrjet. Të gjithë punonjësit nga kompjuteri i tyre mund të aksesojnë këto të dhëna nëpërmjet rrjetit.

• ***Backup*-i qendërzuar/ruajtja e të dhënave**: Përmes ruajtjes së të dhënave në një kompjuter, në rrjet lind nevoja e *backup*-it në mënyrë qendrore të të dhënave të rëndësishme. Ky lloj *backup*-i i sjell një lehtësim të madh administratorit të rrjetit krahasuar me *backup*-in e secilit kompjuter.
• **Përdorimi i përbashkët i mjeteve të punës**: Pajisjet e kushtueshme, si printerat me ngjyra, mund të përdoren nga të gjithë përdoruesit e rrjetit. Kjo zvogëlon kostot për investime.
• **Përdorimi i përbashkët i Software-ve**: Në rrjet ekzistojnë shumë programe aplikative. Këto programe instalohen në serverin e rrjetit dhe mund të kërkohen nga disa klientë. Pas kërkimit, programi ngarkohet në memorien operative të kompjuterave që janë në rolin e klientit. Kështu kursehet dhe vend në memorien e *hard diskut* të klientit. Puna e sektorit të IT është më efektive, pasi bëhet e mundur që programet e përditësuara të mos instalohen veçmas në çdo kompjuter. Gjithashtu përdorimi i përbashkët i *software*ve thjeshton administrimin, si dhe mundëson zgjidhje më ekonomike për *software* të kushtueshëm, të cilët mund të vihen në dispozicion njëkohësisht për të gjitha sistemet.
• **Administrimi i qendërzuar:** Lejon përcaktimin e përbashkët të elementeve të sigurisë.

Ndërtimi i një rrjeti të strukturuar
Në kompani të mëdha është shumë i nevojshëm strukturimi i rrjetit. Në shumicën e rasteve struktura e rrjetit pasqyron edhe strukturën e kompanisë. Në një rrjet të strukturuar është e mundur që punonjësit të grupohen sipas departamenteve ku bëjnë pjesë.



Rrjeti i një kompanie

Në mënyrë që të ndërtojmë një rrjet të strukturuar, nevojitet mundësimi i administrimit qendror dhe klasifikimi i punonjësve, sasisë së të dhënave dhe mjeteve të punës.

• **Administratori i rrjetit**: Në çdo rrjet ka të paktën një administrator, i cili kujdeset për serverin, i cili e administron atë dhe pajisjet e tjera të punës, si dhe mbështet përdoruesit në problemet që dalin gjatë punës.

• **Llogaritë e përdoruesve dhe identifikimi i tyre**: Një punonjës duhet të identifikohet në rrjet në mënyrë që të mund të përdorë burimet. Prandaj, çdo përdoruesi të rrjetit të kompanisë i hapet një llogari në rrjet. Kjo llogari përmban emrin e përdoruesit bashkë me fjalëkalimin përkatës. Për çështje sigurie, fjalëkalimin është e mira ta dijë vetëm punonjësi në fjalë. Kjo pengon në njëfarë mënyre që një individ i panjohur të hyjë në rrjet dhe të aksesojë të dhënat konfidenciale të një kompanie.

Grupet e përdoruesve: Kjo konsiston në grupimin e punonjësve që kryejnë detyra të njëjta apo të ngjashme, si dhe ata që i përkasin një departamenti (*users group*). Në këtë ë mënyrë dhe administratori, në bazë të grupimit, mund të caktojë se cilat pajisje dhe të dhëna lejohen të përdorin punonjës të caktuar gjatë orarit të punës.

Zbatimi i mënyrave të sigurimit të rrjetit
Nëse komunikimi në rrjet nuk do të kishte mënyra për ta siguruar atë, çfarë do të ndodhte me të dhënat tona personale që mbajmë në kompjutera apo në pajisjet tona celularë?

Rëndësia e sigurisë në rrjet
"Siguria e rrjetit" i referohet mbrojtjes së përdorimit të rrjetit dhe të dhënave që kalojnë në të. Siguria maksimale e rrjetit arrin të menaxhojë trafikun në rrjet, si dhe ndalon sulmet që tentojnë të hyjnë apo të përhapen në rrjetin tonë.

Llojet e sigurisë në rrjet

Kontrolli i aksesimit të rrjetit
Jo çdo përdorues duhet të ketë të drejtë për të aksesuar një rrjet. Për të lënë jashtë rrjetit sulmues të mundshëm, duhet të njihet çdo përdorues dhe çdo pajisje që lidhet në rrjet. Më pas do të mund të zbatohen politikat e sigurisë. Mund të bllokoni pajisjet fundore ose mund t'iu jepni atyre të drejta të limituara. Ky proces njihet si *network access control* (NAC) / kontrolli i aksesimit të rrjetit.

Instalimi i programeve antivirus
Instalimi i programeve antivirus mbron kompjuterat ose telefonat celularë nga infektimi i *malware*-ve.

Këshilla mbi përdorimin e programit antivirus.
• Gjeni antiviruse nga burime të njohura dhe të besuara. Shpeshherë, keqbërësit shpërndajnë si programe antivirusi programe *malware* duke mashtruar përdoruesit e kompjuterit.
• Bëni përditësim të antivirusit, duke e skanuar periodikisht kompjuterin tuaj.
• Mos instaloni njëkohësisht disa programe antivirus, pasi bien në konflikt me njëri-tjetrin.
• Skanoni çdo USB sa herë që e vini atë në përdorim.
• Mos e çinstaloni programin antivirus duke menduar se iu ngadalëson kompjuterin dhe shikoni me vëmendje njoftimet në formë alarmi që shfaq ai gjatë punës suaj në kompjuter.

"Malware", shkurtimi i "*malicious software* – i referohet çdo lloj programi të dëmshëm", ku përfshihen *viruset*, *krimbat* (*worm*), *Trojan* dhe *spyware*. Ndonjëherë *malware*-t rrinë të fshehur, ato mund të infektojnë një rrjet dhe mund të rrinë në gjendje qetësie për disa ditë ose edhe javë. Një program i mire kundër *malware*-ve, jo vetëm që mund të skanojë për *malware* në hyrje të portave, por gjithashtu mund të kontrollojë vazhdimisht skedarët për të gjetur anomali, për të larguar *malware* dhe për të rregulluar dëmet e shkaktuara prej tyre.

Siguria e aplikacioneve
Çdo program që përdorni ka nevojë për mbrojtje. Për fat të keq, çdo aplikacion mund të përmbajë mangësi apo dobësi, që sulmuesit mund t'i përdorin për të hyrë në rrjetin tuaj. Siguria e aplikacioneve përfshin pjesët *hardware, software. P*rocese të caktuara përdoren për të mbyllur hapësirat që mund të jenë të depërtueshme në një rrjet.

Analiza e sjelljes

Për të zbuluar sjellje jo normale në një rrjet, duhet të njihni se si është një sjellje normale. Mjetet e analizimit të sjelljes automatikisht dallojnë veprimtari që devijojnë nga normalja dhe që mund të shkaktojnë problem në rrjet.

Parandalimi i humbjes së të dhënave

Organizata ose kompani të ndryshme duhen të sigurohen që stafi i tyre të mos dërgojë informacione të rëndësishme jashtë rrjetit të kompanisë. Parandalimi i humbjes së të dhënave mund të ndalojë përdoruesit të ngarkojnë dhe të transferojnë të dhënat në rrjete të jashtme, madje edhe të printojnë informacione të rëndësishme në një mënyrë jo të sigurt.

Siguria e email-eve

Portat e *email*-eve janë numri *një* i kërcënimeve për shkelje të sigurisë. Sulmuesit përdorin informacione personale dhe rrjetet sociale për të ndërtuar mënyra të sofistikuara të sulmeve *phishing*, për të mashtruar përdoruesit dhe për t'i dërguar ata nëpërmjet faqjes së *web*-it drejt *malware*-ve. Një aplikacion për sigurinë e *email*-eve bllokon sulmet që vijnë dhe kontrollon mesazhet e dërguara në rrjete të jashtme për të parandaluar humbjen e të dhënave të rëndësishme.

Firewall

Firewall-et vendosin barriera ndërmjet rrjetit të brendshëm të besueshëm dhe rrjetit të jashtëm jo të besueshëm, siç është interneti. Ato përdorin një grup rregullash të përcaktuara për të lejuar apo bllokuar trafikun.

Sistemet e parandalimit të ndërhyrjeve

Një sistem parandalimi i ndërhyrjeve (*IPS – intrusion prevention system*) është një pajisje ose aplikacion *software*-ik që monitoron një rrjet ose sistem për veprimtari të dëmshme ose shkelje të politikave. Ky sistem skanon trafikun e rrjetit për të bllokuar në mënyrë aktive sulmet që mund të ndodhin.

Siguria e telefonave cellular

Kriminelët kibernetikë po rritin sulmet ndaj aplikacioneve dhe telefonave celular. Duhet kontrolluar se cila pajisje mund të hyjë në rrjet, si dhe nevojitet konfigurimi i lidhjeve të tyre për të mbajtur trafikun e rrjetit privat.

Segmentimi i rrjetit

Programe për përcaktimin e segmentimit vendosin trafikun e rrjetit në grupime të ndryshme dhe zbatojnë politikat e sigurisë. Grupimet bazohen në identifikimin e pajisjeve fundore, jo

vetëm të adresave IP. Mund të caktohen të drejtat e hyrjes në rrjet në bazë të rolit që një përdorues duhet të ketë, vendndodhjes së tij dhe shumë të tjera, në mënyrë që niveli i të drejtave të aksesit t'u jepet përdoruesve të duhur.

Rrjeti virtual privat
Një *virtual private network* (VPN) kodon lidhjen nga një pajisje fundore në një rrjet, shpesh në internet. Në mënyrë tipike, një VPN e aksesueshme në distancë përdor elemente sigurie për të vërtetuar komunikimin ndërmjet pajisjes dhe rrjetit.

Siguria e web-it
Siguria në *web* kontrollon përdorimin e *web*-eve, bllokon sulmet dhe ndalon hyrjet në *website* të dëmshme. "Siguria e rrjetit" gjithashtu i referohet hapave që duhen ndjekur për të mbrojtur *website*-in.

Siguria në wireless
Rrjetet *wireless* nuk janë aq të sigurta sa ato të lidhura me kabëll. Pa masa të rrepta të sigurisë, instalimi i një rrjeti LAN *wireless* mund të jetë njësoj si vendosja gjithandej e portave *Ethernet*. Për të parandaluar dëmtime nga *hacker*-at, nevojiten programe specifike të ndërtuara për mbrojtjen e rrjeteve *wireless*.

Siguria kibernetike
Tashmë interneti është bërë pjesë e pandarë e jetës sonë. Por sa të sigurt ndihemi në botën virtuale?
Mbrojtja e paisjeve *digjitale* të rrjetit kompjuterik ka qenë e lehtë. Për këtë mjaftonte të aktivizohej *firewall* në kompjuter, si dhe të instalohej programi *antivirus*. Por tani çdo gjë ka ndryshuar, pasi mund të prekesh nga viruset thjesht duke vizituar një *website* të manipuluar. Grupet e organizuara të krimit kibernetik përpiqen të hyjnë në llogaritë tuaja, të vjedhin identitetin ose të marrin në kontroll rrjetin kompjuterik për të dërguar mesazhe *spam* (i njëjti mesazh u dërgohet shumë personave në internet) dhe sulmuar pajisjet kompjuterike. Të rrezikuar nga sulmi kibernetik janë: kompjuteri, laptopi, serveri, celulari (smartphone), pajisjet smart, dekoderat etj.

Sulmet
Një sulm mbi një sistem kompjuterik përcaktohet si "një mundësi potenciale e rrezikshme që mund të ketë një efekt të padëshirueshëm mbi asetet dhe burimet që janë lidhur me sistemin kompjuterik".

Sulmet nga jashtë
Në këtë rast ndërhyrësi nuk është i autorizuar të përdorë as kompjuterin, as të dhënat apo programet e ndryshme. Si shembull për të ilustruar këtë rast mund të marrim një punonjës të një organizate që do të aksesojë intranetin privat të një kompanie rivale në mënyrë që të përvetësojë informacione nga baza e të dhënave.

Sulme të brendshme
Në këtë rast, ndërhyrësi është i autorizuar të përdorë kompjuterin, por nuk është i autorizuar të përdorë të dhënat apo programet e ndryshme. Si shembull për të ilustruar këtë rast mund të marrim një punonjës të një organizate që ka akses te intraneti i kompanisë me anë të lidhjes në distancë ose nga terminali i zyrës.

Kërcënimet në rrjet
Faqet në rrjet janë një tjetër mjet që keqbërësit zgjedhin për të shpërndarë programet e tyre në sa më shumë viktima. Teksa vizitoni faqet, personi që ka hapur atë faqe me anën e gjuhëve të ndryshme të skriptimit mund të shkruajë në kompjuterin tuaj, me anë të kërkuesit, informacion që dëmton, ose vjedh informacion nga kompjuteri juaj. Siç mund ta dini, në kompjuterin tuaj kini të ruajtur informacion hyrjeje për shumë faqe prestigjoze ku ju mund të vizitoni apo kryeni transaksione financiare. Në këtë mënyrë, personat e dashakeqës mund t'u vjedhin që nga fjalëkalimi i adresës suaj të *email*-it në internet e deri te numri juaj i kartës së kreditit që përdorni për të blerë artikuj në internet. Këshilla jonë për ju: *Asnjëherë mos vizitoni një faqe që jua servir dikush tjetër me reklamë, email etj. Dhe gjithmonë, përpara se të klikoni shikoni adresën se ku të çon ajo lidhje.* Gjithashtu, për t'u mbrojtur nga kjo mund të konfiguroni kërkuesin tuaj në një nivel të lartë sigurie, dhe sa herë që ju klikoni në një faqe të tillë, kërkuesi do t'ju shfaqë një mesazh që me pak fjalë do t'iu thotë: "Nuk ju rekomandojmë ta vizitoni këtë faqe"

Email-i është mjeti më i rrezikshëm për t'u infektuar. Të gjithë ata që përdorin internetin, përdorin *email*-in për të komunikuar me shokë, miq e bashkëpunëtorë. Kjo bën që mundësitë për t'u infektuar me anën e *email*-it të jenë shumë herë më të mëdha.

Disa mënyra të mbrojtjes të kompjuterit nga sulmet
Le të përmendim disa nga mënyrat më efikase që mbrojnë kompjuterin tuaj nga sulme të ndryshme.

1 Instalimi i programeve antivirus dhe përditësimi / update i tyre
Skanimi i *malware*-ve nuk arrin t'i kapë të gjitha viruset. Por një program *antimalware* I licensuar, mund t'iu mbrojë nga pjesa më e madhe e kërcënimeve *online*. Fatmirësisht ka shumë aplikacione për sigurinë e pajisjeve telefonike. Shumica e tyre janë falas. Disa më kryesore për sigurinë e aplikacioneve *iPhone* janë prodhuar nga *Trend Micro, McAfee* dhe *Lookout Mobile*. Përveç *ESET Mobile Security*, për programet *android* ka aplikacione *anti-malware* shumë të rekomanduara nga *Avast* dhe *Avira*.

2 Përditësimi i sistemit të operimit
Sulmuesit preferojnë të zvarriten nëpërmjet hapësirave të sistemit të operimit të kompjuterit tuaj, e cila është arsyeja pse gjithmonë duhet të punojmë me versionin më të fundit të sistemit të operimit. Mënyra më e lehtë për të mbajtur *Windows*-in të përditësuar është shkarkimi automatik dhe instalimi i përditësimeve të tij sapo ato shfaqen. Kjo do të shkaktojë rindezje të sistemit, i cili mund të humbasë tërësisht çdo punë të paruajtur, megjithatë sistemi ju njofton përpara se të rindizet.

3 Përforcimi i WiFi-së
Gjithmonë në pajisjet e ruterit WiFi, gjëja e parë që duhet ndryshuar është emir *default* (emri i parazgjedhur), fjalëkalimi, si dhe aktivizimi i WPA ose WPA2. Gjithashtu nevojitet që të kemi programin e brendshëm të ruterit të përditësuar. *Website*-t e prodhuesve të ruterave kanë informacion si të përditësohet *firmware*.

4 Largimi i aplikacioneve të papërditësuara
Kur programi përfundon afatin e përcaktuar nga prodhuesi dhe prodhuesit e kanë të ndaluar ofrimin e mbështetjes ndaj tij, është koha që ai të zëvendësohet me program më të ri.

5 Kujdesi me fjalëkalimet

Ka mjaft histori rreth llogarive të personave që janë vjedhur sepse ata përdornin fjalën "password" si një fjalëkalim, kur duhet të zgjidhet një fjalëkalim më I komplikuar dhe më I gjatë. Mund përdorni një fjalëkalim të koduar i cili përmban shifra, numra, simbole dhe të jetë më shumë se 6 karaktere, si për shembull "fjAl3kal1m".

Aktivizimi i opsioneve shtesë për autentifikim
Edhe fjalëkalimet më komplekse mund të thyhen me disa përpjekje të mjaftueshme. Mënyra për të dëmtuar pajisjet në rrjet janë të disponueshme falas ose dhe me kosto të ulët.

Autentifikimi me kodin PIN

Shtimi i një elementi dytësor – si kodi PIN i dërguar me SMS, që duhet të vendoset pas fjalëkalimit – ndihmon në eliminimin e mundësive të hyrjes së një të huaji në llogarinë tuaj. Nëse dikush tenton të aksesojë llogarinë nga një pajisje e panjohur, vjen një njoftim, duke dhënë mundësinë e ndryshimit të fjalëkalimit përpara se llogaria të vidhet.

2 Largimi i pajisjeve hardware-ike
*Harddrive*rat e vjetër, USB, telefonat dhe disqet e *backup*-eve mund të jenë plot e përplot me të dhëna personale si dhe fjalëkalime dhe informacione të rëndësishme të tjera. Gjithmonë duhet të sigurohemi për pastrimin e tyre përpara se të rishiten ose shkatërrojini ato fizikisht para se të riciklohen.

3 Siguria në rrjetet sociale
Nuk duhet të ndani çdo aspekt të jetës suaj me të tjerët. Shmangni ekspozimin e të dhënave personale që mund të jenë gjithashtu përgjigjja e pyetjeve të sigurisë për rikthimin e fjalëkalimit (mbiemrin e vajzërisë së mamasë tuaj, shoqja/shoku ngushtë, shkolla jote e mesme etj.). Ky lloj informacioni ndihmoi *hacker*-at të hynin në llogarinë e *iCloud*-it të Jennifer Lawrence, Rihanës dhe të personave të tjerë të famshëm.

4 Të tregojmë kujdes
Zakonisht jeni në rregull kur nuk bëni asnjë "gjë të gabuar". Kuptimi i "gjë e gabuar" i referohet hapjes së një materiali të papritur të bashkangjitur në postën elektronike, hapjes së *website*-ve të dyshimta.

Rreziqet në rrjet
Përdorimi i teknologjisë ka përfitime të mëdha, por gjithashtu ka rreziqe për të cilat duhet të jemi të kujdeshshëm. Për shkak se internet është lehtësisht i arritshëm nga të gjithë, mund të jetë një vend me rrezik. Është e rëndësishme të identifikohen ato për t'i reduktuar apo menaxhuar në mënyrë që të kemi sa më pak dëme. Rreziku në rrjet përfshin dështime hardware-ike dhe softwareike, gabime njerëzore, spam, viruse apo sulme të jashtme, si dhe katastrofa natyrore si zjarri, tërmeti apo përmbytje. Rreziqet e përgjithshme për sistemet dhe të dhënat IT përfshijnë:
• Dështime hardware-ike dhe software-ike – të tilla si humbja e energjisë elektrike apo korruptimi i të dhënave.

• Malware – software të dëmshëm që ndërpresin veprimet kompjuterike.
• Viruset – kode kompjuterike që mund të kopjojnë vetëveten dhe të përhapen nga njëri kompjuter në tjetër, shpesh ndërpresin veprimet kopjuterike.
• Spam dhe phishing – email-e të pa dëshiruara për të mashtruar njerëz në zbulimin e të dhënave personale apo në blerje të mallrave për mashtrim.
• Gabime njerëzore – procesimi i të dhënave të gabuara, hedhja e të dhënave pa kujdes, apo hapja pa dashje e një materiali i infektuar të bashkangjitur në email.

Kërcënimet kriminale specifike ose të synuara për sistemet dhe të dhënat IT përfshijnë:
• Hacker-a – persona që në mënyrë ilegale thyejnë sistemin kompjuterik.
• Mashtrim – përdorimi i kompjuterave për të ndryshuar të dhëna për përfitime të paligjshme.
• Thyerja e fjalëkalimeve – shpesh është një objektiv për hacker-at për të marrë aksesin.
• Refuzim shërbimi – sulme online për të parandaluar aksesin e përdoruesve të autorizuar në website.
• Shkeljet e sigurisë – përfshin grabitje fizike, si dhe ndërhyrje online.
• Pandershmëria e pjesëtarëve të rrjetit – vjedhja e të dhënave ose informacioneve të rëndësishme.

Fatkeqësitë natyrore dhe sistemet IT
Fatkeqësitë natyrore si zjarri, ciklonet dhe përmbytjet paraqesin gjithashtu rreziqe për sistemet, të dhënat dhe infrastrukturën e IT. Dëmtimi i ndërtesave dhe pajisjeve kompjuterike mund të rezultojë në humbje ose korruptim të të dhënave / transaksioneve të konsumatorëve.

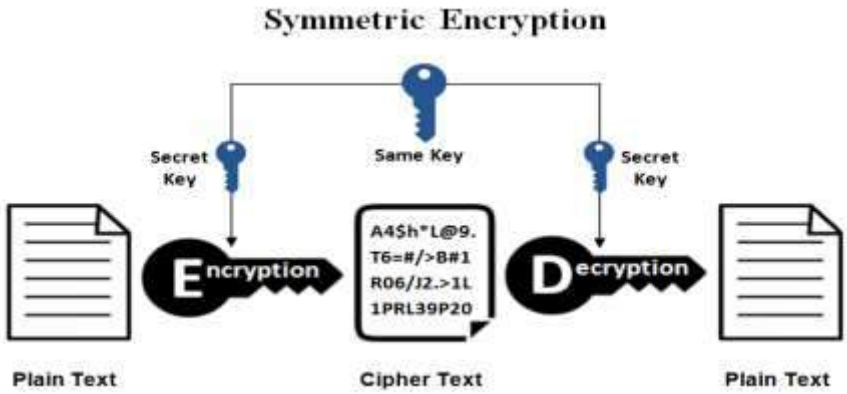
Mbrojtja e të dhënave në trasmetim
Ndërsa strategjitë e mira të sigurisë mund të jenë efektive në mbrojtje të rrjetit duke lënë jashtë saj sulmuesit e ndryshëm, si mendoni për të dhënat që transmetohen ndërmjet pajisjeve mobile, shfetuesëve të internetit dhe databazave? Enkriptimi ndryshon tekstin duke e bërë atë të palexueshme nga të tjerët përveç atyre që kanë çelësin për të dëshifruar.

Ndërsa siguria IT kërkon të mbrojë asetet fizike, kompjuterat e rrjetit, databazën, serverat etj., enkriptimi mbron të dhënat që këto asete apo që trasmetohen ndërmjet tyre. Enkriptimi i bazuar në kriptografi, përdor kompjuterat dhe algoritmet për të kthyer tekstin e thjeshtë në formë të palexueshme, përzierje kodesh. Për të dekriptuar kodin në tekst duhet çelësi i enkriptimit, një seri bitesh që dekodon tekstin. Çelësi është diçka që ju ose marrësi i synuar ka posedimin e tij.
Kompjuterët janë në gjendje të thyejnë kodimin duke supozuar një çelës enkriptimi, por për algoritme shumë të sofistikuara kjo mund të marrë një kohë shumë të gjatë.
Nëse dërgoni një email të koduar, vetëm personi me çelësin e enkriptimit mund ta lexojë atë.
Nëse po përdorni një lidhje të koduar në internet për të bërë blerje në internet, informacionet dhe numri i kartës së kreditit janë të fshehura nga përdoruesit e paautorizuar, vëzhgimet e paligjshme ose hajdutët e identitetit.
Por enkriptimi mund të përdoret gjithashtu për keq. Sulmet *Ransoware* po bëhen më të përhapura dhe sulmet e DOS (denial of service – refuzim shërbimi) që përdorin software-t e enkriptimit për të bllokuar përdoruesit nga kompjuterët e tyre derisa të paguajnë një tarifë.

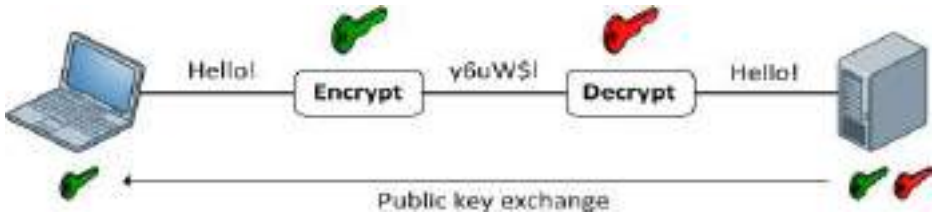
Të dhënat që ne enkriptojmë janë:
• Në transit, që do të thotë se po lëviz përmes email-it, aplikacioneve ose përmes shfletuesve dhe lidhjeve të tjera të webit.
• Në pushim, kur të dhënat ruhen në bazat e të dhënave, cloud, hard disqet e kompjuterit ose pajisjet telefonike.

Si funksionon enkriptimi
Të dhënat e pa enkriptuara, shpesh ju referohemi si tekste të thjeshta. Ato enkriptohen duke përdorur një algoritëm dhe një çelës enkriptimi. Ky proces gjeneron kode të cilat mund të shikohen në formën e tyre fillestare nëse dekriptohen me çelësin e duhur. Dekriptimi është i kundërti i enkriptimit, duke ndjekur hapa të njëjtë por duke përmbysur kodin në të cilin është aplikuar çelësi. Në ditët e sotme algoritme enkriptimesh më të përdorura janë: simetrike dhe asimetrike.

Enkriptimi simetrik, shpesh i referohemi si "çelës sekret", përdor një çelës të vetëm. Sistemi që bën enkriptimin duhet të ndajë çelësin e enkriptimit me çdo njësi që synon të jetë në gjendje të dekriptojë të dhënat e koduara.



Enkriptimi asimetrik, i njohur si kriptografi me çelës publik, përdor dy çelësa të ndryshëm po të lidhura matematikisht, një publik dhe një privat. Çelësi publik mund të ndahet me të gjithë, ndërsa çelësi privat duhet të mbahet sekret.



Përparësitë e enkriptimit
Qëllimi primar i enkriptimit është të mbrojë konfidencialitetin e të dhënave digjitale të ruajtura në sistemet kompjuterike ose ato që transmetohen nëpërmjet internetit apo ndonjë rrjeti tjetër kompjuterik. Një numër i organizatave dhe organeve të standardeve rekomandojnë ose kërkojnë që të dhënat e ndjeshme të kodohen në mënyrë që të parandalojnë palët e treta të paautorizuara ose faktorë kërcënimi të kenë qasje në të dhëna.

Hashing
Hashing është gjenerimi i një vlere ose vlerave nga një varg teksti duke përdorur një funksion matematikor. Hashing është një mënyrë për të mundësuar sigurinë gjatë procesit të transmetimit të mesazhin kur ai është i destinuar vetëm për një marrës të veçantë. Formula gjeneron hash-in, i cili ndihmon për të mbrojtur sigurinë kundër ndërhyrjeve të mundshme.
Hashing është gjithashtu një metodë për renditjen e vlerave kryesore në një tabelë të databazës në mënyrë efikase. Kur një përdorues dërgon një mesazh të sigurt, një hash i mesazhit të synuar gjenerohet dhe kodohet, më pas dërgohet së bashku me mesazhin. Kur të marrë mesazhin, marrësi dekripton hashin si dhe mesazhin. Pastaj, marrësi krijon një hash

tjetër nga mesazhi. Nëse të dy hashet janë identik kur krahasohen, atëherë ka ndodhur një transmetim i sigurt. Ky proces hashing siguron që mesazhi të mos ndryshohet nga një përdorues i paautorizuar.
Hashing përdoret për të indeksuar dhe për të gjetur të dhëna në një databazë sepse është më e lehtë për të gjetur diçka duke përdorur çelësin hash të shkurtër sesa të kërkosh vlerën fillestare.

Funksioni hash
Algoritmi i hashing quhet funksioni hash - ndoshta termi rrjedh nga ideja se vlera e hash rezultuese mund të mendohet si një version "i përzier" i vlerës së përfaqësuar. Përveç rikthimit të shpejtë të të dhënave, hashing përdoret gjithashtu për të koduar dhe dekriptuar nënshkrimet digjitale (përdoren për të vërtetuar dërguesit dhe marrësit e mesazhit). Shenjat digjitale transformohet me funksionin e hash dhe pastaj të dy vlerat hash dhe shenjat dërgohen në transmetime të ndara për te marrësi. Duke përdorur funksionin e njëjtë të hash-it si dërguesi, marrësi nxjerr një mesazh dhe e krahason atë me mesazhin që e ka marrë. Ata duhet të jenë të njëjtë.
Funksioni hash përdoret për të indeksuar vlerën fillestare ose çelësin dhe pastaj përdoret më vonë çdo herë që duhet të merren të dhënat e lidhura me vlerën ose çelësin. Hashing është gjithmonë një operacion me një drejtim.
Një funksion i mirë hash gjithashtu nuk duhet të prodhojë të njëjtën vlerë hash nga dy inpute të ndryshme. Nëse kjo ndodh, kjo njihet si një përplasje. Një funksion hash që ofron një rrezik jashtëzakonisht të ulët të përplasjes mund të konsiderohet i pranueshëm.

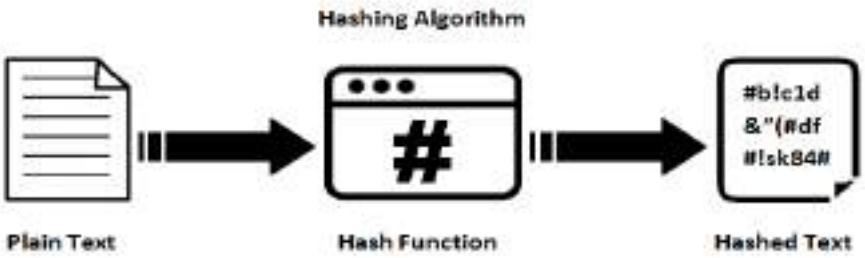
Këtu janë disa funksione relativisht të thjeshta hash që janë përdorur:

• **Metoda e ndarje-mbetje**: Përllogaritet madhësia e numrit të artikujve në tabelë. Ky numër përdoret më pas si pjesëtues në çdo vlerë fillestare ose çelës për nxjerrjen e një koeficienti dhe mbetjes. Mbetja është vlera hash. (Meqë kjo metodë mund të prodhojë një sërë përplasjesh, çdo mekanizëm kërkimi duhet të jetë në gjendje të njohë një përplasje/konflikt dhe të ofrojë një mekanizëm të kërkimit alternativ.)

• **Metoda e palosjes**: Kjo metodë ndan vlerën fillestare (shifrat në këtë rast) në disa pjesë, shton pjesët së bashku dhe pastaj përdor katër shifrat e fundit (ose ndonjë numër tjetër arbitrar të shifrave që do të funksionojnë) si vlerë hash ose çelës.

• **Metoda e transformimit Radix**: Kur vlera ose çelësi është me shifra, baza e numrave (ose radix) mund të ndryshohet duke rezultuar në një rend tjetër shifrash. (Për shembull, një çelës me numër dhjetor mund të shndërrohet në një çelës me numër heksadecimal.)

• **Metoda e riorganizimit të shifrës**: Kjo është thjesht marrja pjesë në vlerën fillestare ose çelësin, siç janë shifrat në pozicionet 3 deri 6, duke kthyer rendin e tyre dhe pastaj duke përdorur atë rend të shifrave si vlerë hash ose çelës.
Ka disa funksione të njohura hash të përdorura në kriptografi. Këto përfshijnë funksionet e thyerjes së mesazhit të tilla si MD2, MD4, dhe MD5, të përdorura për hash-timin e shenjave në një vlerë më të shkurtër të quajtur *message-digest* dhe Algoritmi i Sigurt Hash (Secure Hash Algorithm - SHA), një algoritëm standard, që bën një mesazh të gjatë (60-bit) dhe është e ngjashme me MD4. Një funksion hash që punon mirë për ruajtjen dhe rikthimin e bazës së të dhënave, megjithatë, mund të mos funksionojë si për qëllime kriptografike ose gabime.



Siguria operacionale

Si e mendoni sigurinë në rrjet apo internet? A mund të arrihet siguria maksimale?

Siguria operacionale (opserational security – OPSEC), e njohur edhe si siguri proceduriale, është një proces i menaxhimit të rrezikut që inkurajon menaxherët të shikojnë operacionet nga këndvështrimii një kundërshtari në mënyrë që të mbrohen informacionet e rëndësishme nga rënia në duar të gabuara.

Megjithëse përdorej fillimisht nga ushtria, OPSEC po bëhet popullore edhe në sektorin privat. OPSEC përfshin sjelljet dhe zakonet e monitorimit në faqet e mediave sociale, si dhe parandalimi i punonjësve nga shkëmbimi i kredencialeve të identifikimit përmes postës elektronike ose mesazheve.

Proceset e sigurisë operacionale mund të kategorizohen në këto pesë hapa:

1. Identifikimi të dhënave të ndjeshme, duke përfshirë pronësinë intelektuale, pasqyrat financiare, informacionin e klientit dhe informacionin e punonjësve. Këto janë të dhëna që zakonisht duhet të përqendrohemi t'i mbrojmë.

2. Identifikimi i kërcënimeve të mundshme. Për secilën kategori të informacionit që konsiderohet e ndjeshme, duhet identifikuar se çfarë lloj kërcënimesh janë të pranishëm. Ndërsa duhet treguar kujdes ndaj palëve të treta që përpiqen të vjedhin informacione nga sistemi, duhet gjithashtu kujdes për kërcënime të brendshëm, siç janë punonjësit e pakujdesshëm dhe ata me synime dashakeqëse.

3. Analizimi i hapësirave të sigurisë dhe dobësitë e tjera. Vlerësimi i masave për mbrojtjen aktuale dhe përcaktimi se çfarë dobësish ekzistojnë dhe që mund të shfrytëzohen për të pasur akses në të dhënat e rëndësishme të sistemit.

4. Vlerësimi i nivelit të rrezikut që lidhet me secilën dobësi. Renditen dobësitë e sistemit duke përdorur faktorë të tillë si gjasat që të ndodhë një sulm, shtrirja e dëmit që pësohet dhe sasia e punës dhe kohës që do të duhet për ta rikthyer në gjendje të mëparshme. Sa më shumë mundësi për të ndodhur dhe dëme të ketë një sulm, aq më shumë duhet patur në prioritet zvogëlimi I rrezikut.

5. Kundërmasat. Hapi i fundit i sigurisë operacionale është krijimi dhe zbatimi i një plani për eliminimin e kërcënimeve dhe zbutjen e rreziqeve. Kjo mund të përfshijë përditësimin e hardware-it tuaj, krijimin e politikave të reja në lidhje me të dhënat e ndjeshme, ose trajnimin e përdoruesve për praktikat e dobishme të sigurisë dhe politikat e sistemit. Kundërmasat duhet të jenë të drejtpërdrejta dhe të thjeshta. Përdoruesit duhet të jenë në gjendje të zbatojnë masat e kërkuara nga ana e tyre me ose pa trajnime shtesë.

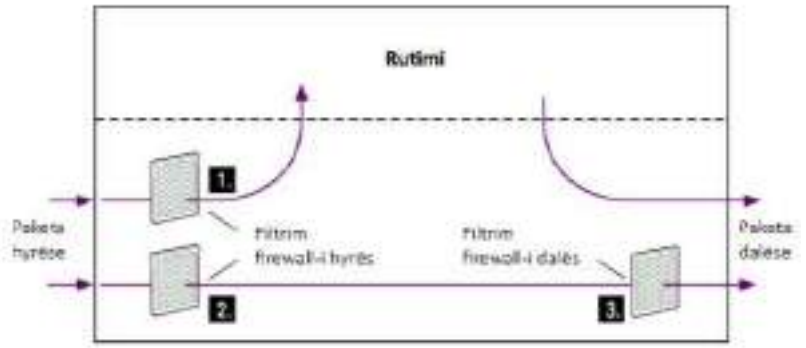
Të kuptojmë se si firewall-i kontrollon filtrimin e paketave

Një switch përdor firewall-in që të lejohet kontrolli i rrjedhës së paketave të të dhënave dhe paketave lokale. Paketat e të dhënave kalojnë në switch pasi ato përcillen nga një burim në një destinacion. Paketat lokale janë të destinuara ose të dërguara nga një Routing Engine (ata nuk kalojnë në një switch). Paketat lokale zakonisht përmbajnë të dhënat e protokollit të drejtimit, të dhënat për shërbimet IP siç janë Telnet ose SSH, ose të dhënat për protokollet

administrative siç është Internet Control Message Protocol (ICMP).

Filtrimet e firewall-it ndikojnë kalimin e paketave që futen ose dalin nga një switch si më poshtë:
• Filtrat hyrëse të firewall-it ndikojnë në kalimin e paketave të të dhënave që pranohen në ndërfaqet e switch-it. Kur një switch merr një paketë të dhënash, Packet Forwarding Engine në sistemin që përmban ndërfaqen e hyrjes përcakton se ku ta përcjellë paketën duke parë në tabelën e rutimit të shtresës 2 ose shtresës 3 për rrugën më të mirë në destinacion. Paketat e të dhënave përcillen në një ndërfaqe dalëse. Paketat e destinuara në nivel lokal përcillen në routing engine.
• Filtrat dalëse të firewall-it ndikojnë në paketat e të dhënave që kalojnë në një switch por nuk ndikojnë në paketat e dërguara nga routing engine. Këto filtra aplikohen nga Packet Forwarding Engine në sistemin që përmban ndërfaqen e daljes.

Figura ilustron aplikimin e filtrave të firewall-it hyrëse dhe dalëse për të kontrolluar kalimin e paketave nëpërmjet një switch:
1. Filtrimi firewall hyrës zbatohet në paketat e destinuara në nivel lokal të cilat pranohen në ndërfaqet e switch-it dhe janë të destinuara për routing engine.
2. Filtrimi firewall hyrës zbatohet në paketat e të dhënave që pranohen në ndërfaqet e switch-it dhe do të kalojnë përmjet tij.
3. Filtrimi firewall dalës i përdorur për paketat e të dhënave që kalojnë përmes switch-it.



Aplikimi i filtrave të Firewal-it për kalimin e paketave të kontrolluara

Mbrojtja e kompjuterit nëpërmjet Firewall
Një *Firewall* (rrjeti apo *hardware*-ësh), që në anglisht do të thotë "mur djegës", krijon një lidhje të kontrolluar ndërmjet dy rrjeteve. Këto mund të jenë për shembull një rrjet privat (LAN) dhe një internet (WAN). Por e mundshme është edhe një lidhje e segmenteve të ndryshme rrjetesh apo e të njëjtit rrjet. *Firewall* mbikëqyr qarkullimin e të dhënave që kalojnë nëpërmjet tij dhe vendos sipas rregullave të përcaktuara qartë nëse një paketë të dhënash duhet të kalojë apo jo. Në këtë mënyrë, *Firewall* përpiqet të mbrojë rrjetin privat apo segmentin e tij nga ndërhyrjet e paautorizuara. E parë nga këndvështrimi i shkeljes së rregullave, funksioni i *Firewall* nuk qëndron në faktin që të njohë dhe të shmangë ndërhyrje të palejueshme. Në të vërtetë, funksioni i tij qëndron në atë që të lejojë marëdhënie të caktuara komunikimi, të bazuara në adresat e dërguesit, marrësit dhe shërbimeve të përdorura prej tyre. Për të kapur ndërhyrjet, përdoren të ashtuquajturat module IDS (*Intrusion Detection System*), të cilat i mbivendosen një *Firewall*-i. Megjithatë, ato nuk bëjnë pjesë në modulin e tij.

Si të konfiguroni Windows Firewall në një kompjuter
Windows Firewall ndihmon për të mbrojtur kompjuterin duke bllokuar trafikun. Trafiku i

dhënë është çdo përpjekje për të komunikuar me kompjuterin tuaj në një lidhje të rrjetit që nuk është kërkuar në mënyrë specifike nga programet që janë në funksionim në kompjuterin tuaj. Prandaj, programe si *Microsoft Internet Explorer* ose *Outlook Express* vazhdojnë të funksionojnë me sukses me aktivizimin e *Windows Firewall.*

Në këtë projekt do të shpjegohet si të konfiguroni *Windows Firewall* në një kompjuter të vetëm nëse konfigurimet e rekomanduara të parazgjedhura nuk përmbushin kërkesat tuaja. Do të fokusohemi në konfigurimin e *Windows Firewall General Setting*s. *Windows Firewall General Settings* ju lejon të konfiguroni këto opsione:

• **On (recommended).** Ky është opsioni i parazgjedhur (me zgjerimin *Don't allow* të papërzgjedhur).

Don't allow exceptions. Kur ky opsion zgjidhet, *Firewall*-i është vendosur në *On With No Exceptions mode*, e cila bllokon të gjitha kërkesat e dhëna për t'u lidhur me kompjuterin tuaj. Përdorni *Don't allow exceptions* kur ju duhet mbrojtje maksimale për kompjuterin tuaj.

• **Off (not recommended)**. Fikja e *Windows Firewall* mund ta bëjë kompjuterin tuaj më të rrezikuar nga dëmtimet e viruseve, krimbave (*worms*) ose ndërhyrjeve. Për të modifikuar parametrat e paparazgjedhura të *Windows Firewall*, ndiqni këto hapa:
• hapni **Windows Security Center**;
• hapni **Windows Firewall**;
• konfiguroni **Windows Firewall On with No Exceptions mode**;
• çaktivizoni **Windows Firewall**;
• verifikoni që janë zbatuar konfigurimet në **Windows Firewall General settings**. *Për të kryer këtë veprimtari duhet* të jeni të loguar si një pjesëtar i grupit të administratorëve lokalë.

***Hapni* Windows Security Center**

1. Klikoni **Start** dhe më pas **Control Panel**.
2. Në *Control Panel* klikoni **Security Center**.

Paneli i kontrollit / Control Panel

Qendra e sigurisë së Windows-it / Windows Security Center

3. Hapni **Windows Firewall**
Në **Windows Security Center**, poshtë **Manage security settings for**, klikoni **Windows Firewall**. Konfiguroni *Windows Firewall* On pa mënyrën e përjashtimit (exceptions) Në dritaren dialoguese të **Windows Firewall**, zgjidhni **Don't allow exceptions** dhe më pas klikoni **OK**.

Windows Firewall & Windows Firewall On with No Exceptions mode

Çaktivizimi i Windows Firewall
Kujdes: Çaktivizimi i *Windows Firewall* do të ekspozojë kompjuterin tuaj në internet, nëse nuk ekziston asnjë *Firewall* tjetër. Opsioni që do të trajtohet në këtë pjesë duhet të bëhet vetëm nga përdoruesit administratorë të kompjuterit ose nëse kompjuteri juaj është i mbrojturnga një *Firewall* tjetër.

Për të çaktivizuar *Windows Firewall* veprojmë në këtë mënyrë:
1. Në **Windows Security Center** poshtë **Manage security settings for**, klikoni **Windows Firewall**.

2. Në dritaren dialoguese të **Windows Firewall,** klikoni **Off (not recommended).**
3. Klikoni **OK,** më pas mbylleni **Security Center**, pastaj mbyllni dhe **Control Panel**.

Verifikoni që janë zbatuar konfigurimet e *Windows Firewall General settings*. Kur verifikoni mjedisin *Windows Firewall*, disa tabela dhe opsione në dritaren dialoguese të Windows Firewall mund të jenë të padisponueshme në varësi të konfigurimeve tuaja.

Për të verifikuar *Windows Firewall General settings* duhet të kryejmë këto veprime:
1. Klikoni **Start** dhe më pas klikoni në **Control Panel**.
2. Poshtë **Pick a category** klikoni **Security Center**.
3. Poshtë **Manage security settings for** klikoni **Windows Firewall**.
4. Klikoni tabelën **General** dhe verifikoni se konfigurimi juaj është aplikuar në Windows Firewall dhe më pas klikoni **OK.**