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

MATERIAL MESIMOR

Në mbështetje të mësuesve të profilit mësimor

RRJETE TË DHËNASH

Niveli IV i KSHK

NR. 9

Ky material mësimor i referohet:

- **Lëndës profesionale: "Rrjete kompjuterike", kl.12 (L-26-205-11).**

E përgatitën:

Besmir Kanushi
Ornela Çerpja
Elida Mesi

Tiranë, 2020

Tema 1. Modelet e rrjeteve (*OSI, DoD, TCP*), shtresat dhe ndërtimi i paketave.

Një rrjet është një sistem që lejon komunikimin mes dy apo më shumë kompjuterëve, printerëve, skanerëve etj, shpërndarjen e të dhënave mes tyre apo kryerjen e shërbimeve të tjera. Në botën e rrjeteve kompjuterike duhet të përcaktohen mirë rregullat e komunikimit, pasi nëse kompjuterët nuk e kuptojnë njëri-tjetrin, nuk mund të kemi akses interneti, shpërndarje skedarësh apo printim.

Përparësi e përdorimit të tyre është se ata mundësojnë kalimin dhe shkëmbimin e shpejtë të informacionit. Përpara rrjeteve, njerëzit përdornin disketat e përpara tyre letërkëmbimin. Një tjetër përparësi është se ata lejojnë ndarjen (*sharing*) e burimeve. Kjo ul së tepërmi koston e shkëmbimit, pasi të njëjtat burime përdoren nga shumë njerëz. P.sh. nëse kemi 10 kompjuterë të lidhur në rrjet, mjafton të lidhet vetëm një printer dhe të gjithë mund të printojnë, ndërkohë që mungesa e rrjetit do të kërkonte blerjen dhe instalimin e 10 printerëve.
Në qendër të idesë së rrjetit është ekzistenca e një dërguesi dhe e një marrësi. Dërguesi, ose burimi, është një kompjuter që përcjell informacion në një kompjuter tjetër. Marrësi njihet ndryshe edhe me emërtimin "destinacioni". Rrjeti mund të përmbajë dhe pajisje të tjera. Çdo makinë (kompjuter, printer, skaner etj.) që është në gjendje të komunikojë në rrjet njihet me emrin *pajisje* ose *nyjë*.
Për të mundësuar komunikimin, duhet që nyjat të jenë të lidhura nëpërmjet kabllove ose mikrovalëve.

Llojet e rrjeteve kompjuterike dhe ndarja e tyre

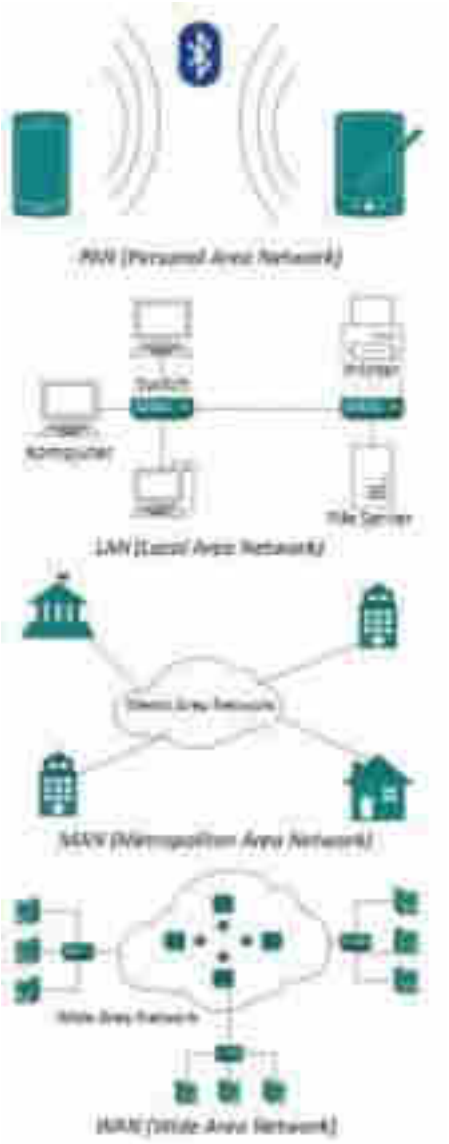
Përgjithësisht, llojet e rrjeteve ndahen nga shpërndarja e tyre gjeografike. Një rrjet mund të jetë i vogël aqsa distanca e telefonit tuaj dhe e kufjeve me *bluetooth*, por mund të jetë aq i madh sa gjithë globi, që është *Interneti*.

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 brënda 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.

Shtresat në rrjet

Sot është e rëndësishme që zhvilluesit e programeve të jenë të aftë të ndërtojnë programe që komunikojnë lehtësisht me programe të tjerë në rrjet, veçanërisht në internet. Për shembull, një program duhet të krijojë lidhje me një databazë në distancë, të bëjë një *query* në databazë, të marrë rezultatet e *query*-të dhe të mbyllë komunikimin.

Komunikimet e thjeshta përmes internetit përfshijnë kalimin e një mesazhi poshtë në shtresa në burimin e mesazhit dhe mbrapa përmes shtresave të ngjashme në destinacionin e mesazhit. Në një komunikim më kompleks, mesazhet dërgohen nëpërmjet disa entiteteve të ndërmjetme të komunikimit të quajtur router.

Në çdo router, kalon një mesazh nëpër disa shtresa dhe pastaj kthehet në rrugën drejt një router-i tjetër ose në destinacion.

Çdo shtresë i shërben një qëllimi të ndryshëm dhe përdor një protokoll të ndryshëm për komunikim. Një protokoll përcakton formatin dhe rendin e mesazheve të shkëmbyera midis dy ose më shumë njësive të komunikimit, si dhe veprimet e ndërmarra në transmetimin dhe/ose marrjen e një mesazhi ose ngjarjeve të tjera.

Subjektet komunikuese shpesh janë klient, ose proces që kanë nevojë për një shërbim, dhe një server, ose proces që ofron shërbimin. Protokollet në përgjithësi përfshijnë një skemë kodimi për kodimin dhe dekodimin e të dhënave.

Modelet e rrjeteve (*OSI, DoD, TCP*). Modeli OSI - Historik i shkurt

Modeli ISO/OSI u zhvillua në vitin 1984 nga Organizata Ndërkombëtare e Standardeve - ISO (*International Standards Organisation*), në vijim të përvojës së krijuar nga ARPAN-et, për të krijuar një model teorik, i cili do të shërbente si standard per të plotësuar kërkesat për paraqitjen e komunikimit në rrjet. Meqë modeli nuk i përket ndonjë familje të caktuar protokollesh, ai quhet ndryshe si *Open-System-Interaction-Model* (OSI). Në tabelën e mëposhtme do të gjeni të vendosura karshi njëra tjetrës shtresat që i korrespondojnë shembullit të mësipërm me ato të nomenklaturës së modelit OSI:

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

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

- ☑ Çdo shtresë siguron një grup shërbimesh (*services*) për shtresën e mësipërme me anë të një ndërfaqeje të përcaktuar mirë, e ashtuquajtura ***Service Access Point*** **(SAP)**. Këto shërbime sigurojnë akses tek strukturat e të dhënave.
  Sa më e lartë shtresa, aq më komplekse janë detyrat që ajo përmbush. Funksionaliteti i çdo shtrese bazohet mbi standardet e shtresës së mëposhtme.
- ☑ Gjatë trafikut të të dhënave, secila nga shtresat individuale të nyjeve (nodes) të rrjetit të përfshira në komunikim, reagon sikur të komunikonte me shtresën korresponduese (peer layer) të node-it partner (komunikim horizontal përmes një lidhje logjike). Në fakt, të gjitha të dhënat kalojnë përmes të gjitha shtresave (komunikim vertikal ose ndërshtresor).
- ☑ Ndërveprimi ndodh gjithmonë midis shtresave fqinje, pra me fjalë të tjera shtresa të vecanta nuk mund të kapërcehen.

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

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

Vështrim i përgjithshëm në lidhje me detyrat
Tabela e mëposhtme jep një përmbledhje të shkurtër të paraqitjes së detyrave të një modeli të pastër OSI:

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

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

Grupet e shtresave	**Nr.**	**Shtresat sipas modelit OSI**	**Shembuj**		
			Protokollet e aplikacioneve	**Shërbimet specifike të sistemit**	**Protokollet e rrjetit**
Shtresat e aplikacioneve	7	Application	Transmetitmi i file-eve, Post, WWW		
	6	Presentation	FTP, SMTP, HTTP		
	5	Session		SMB, WinSocket	
Shtresat e rrjetit	4	Transport			TCP, UDP, SPX
	3	Network			IP, IPX, ARP
	2	Data Link			MAC
	1	Physical			ETH0, Token Ring

Nga njëra anë janë shtresat 1 deri në 4, të cilat merren me detyrat specifike për rrjetin që kanë të bëjnë me komunikimin. Nga ana tjetër janë shtresat 5 deri në 7, në të cilat sigurohen shërbime

specifike për sistemin operativ, përpunohen të dhëna dhe sigurohet mbështetja për aplikacionet.

Nënshtresat e shtresës së dytë të modelit OSI (Data Link Layer)
Praktika ka treguar, se është e nevojshme një nëndarje e mëtejshme teorike e shtresës Data Link Layer, meqë ajo merr përsipër të kryejë dy funksione shumë të ndryshme nga njëra tjetra. Dy nëndarjet e saj janë: Logical Link Control (LLC) dhe Media Access Control (MAC).

Modeli DoD
Ka luajtur rol vendimtar në shumë zhvillime që i përkasin fushës së rrjeteve. Ai është një model proprietar i zhvilluar nga Ministria e Mrojtjes e Sh.B.A – Department of Defence = DoD), i cili vëmendje më të madhe i kushton komunikimit në Internet, dhe më pak komunikimit mes shtresave dhe aplikacioneve.

Modeli TCP
Si familja më e përhapur e protokolleve, modeli TCP provon një thjeshtim të logjikës së ndërtimit me shtresa, me qëllim që t'i përshtatet më mirë praktikës së komunikimit. Komponentët qendrorë janë vendosur në shresën 3 dhe 4 të modelit OSI. Ajo që ndodh me shtresat më poshtë (*Network Interface Layer*) dhe më lart (*Application Layer*) luan një rol të dorës së dytë.

Tema 2. Bashkësia e protokolleve TCP/IP. Protokollet dhe detyrat e tyre. Ndërveprimi midis protokolleve dhe shërbimeve

Modeli TCP/IP *(Transmission Control Protocol / Internet Protocol)*
Të gjithë protokollet e internetit, ndryshe grupi i rregullave quhet TCP/IP. TCP/ IP specifikon mënyrën e shkëmbimit të të dhënave në internet duke ofruar komunikime që identifikojnë se si duhet të thyhet në paketa, të adresohen, të transmetohen, të dërgohen dhe të arrijnë në destinacion. TCP / IP është i dizenjuar për t'i bërë rrjetet të besueshme, me aftësinë për t'u rikuperuar automatikisht nga dështimi i çdo pajisjeje në rrjet.

Dy protokollet kryesore në suportën e protokollit të internetit i shërbejnë funksioneve specifike. TCP përcakton se si aplikacionet mund të krijojnë kanale të komunikimit në një rrjet. Ai gjithashtu menaxhon se si një mesazh është ndarë në paketa të vogla përpara se ato të transmetohen më pas në internet dhe të rikonfirmohen në rendin e duhur në adresën e destinacionit. IP përcakton adresën dhe rrugën që çdo pako të arrijë destinacionin e duhur. Çdo portë dalëse në rrjet kontrollon këtë adresë IP për të përcaktuar se ku duhet ta përcjellë mesazhin.

Funksionimi i modelit TCP/IP
TCP / IP përdor modelin e komunikimit klient /server në të cilin një përdoruesi i jepet një shërbim (si dërgimi i një faqeje) nga një kompjuter tjetër (një server) në rrjet. Në protokollet TCP / IP, çdo kërkesë e klientit konsiderohet e re sepse nuk lidhet me kërkesat e mëparshme. Kjo liron rrugën e rrjetit në mënyrë që ato të mund të përdoren vazhdimisht. Sidoqoftë, shtresa e transportat është e ndjeshme. Transmeton një mesazh të vetëm dhe lidhja e tij mbetet në vend derisa të gjitha paketat në një mesazh të jenë pranuar dhe të rikonfirmohen në destinacion.

Shtresat e modelit TCP / IP

Funksionaliteti TCP/IP është i ndarë në katër shtresa, secila prej të cilave përfshin protokollet specifike.

Shtresa e aplikacionit siguron aplikacione me shkëmbim të standardizuar të të dhënave. Protokollet e saj përfshijnë Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) dhe Simple Network Management Protocol (SNMP).

Shtresa e transportat është përgjegjëse për mbajtjen e komunikimit në rrjet. TCP trajton komunikimin midis hosteve dhe siguron besueshmërinë. Protokollet e transportat përfshijnë TCP dhe User Datagram Protocol (UDP), i cili nganjëherë përdoret në vend të TCP për qëllime të veçanta.

Shtresa e rrjetit, e quajtur edhe shtresa e internetit, merret me paketa dhe lidh rrjetet e pavarura për të transportuar paketat në të gjithë kufijtë e rrjetit. Protokollet e shtresës së rrjetit janë IP dhe Internet Control Message Protocol (ICMP), i cili përdoret për raportamin e gabimeve.

Shtresa fizike përbëhet nga protokollet që veprojnë vetëm në një lidhje - komponenti i rrjetit që ndërlidh nyjet ose hostet në rrjet. Protokollet në këtë shtresë përfshijnë Ethernet për rrjetet e zonës lokale (LAN) dhe Address Resolution Protocol (ARP).

Përparësitë e modelit TCP / IP

TCP / IP është model në përputhje me standartet që përdoren gjerësisht, si rezultat, nuk kontrollohet nga një kompani e vetme. Prandaj, grupi i protokollit të internetit mund të modifikohet lehtësisht. Është në përputhje me të gjitha sistemet operative, kështu që mund të komunikojë me çdo sistem tjetër. Paketa e protokollit të internetit është gjithashtu në përputhje me të gjitha llojet e pajisjeve kompjuterike dhe rrjeteve.

TCP / IP është shumë e shkallëzuar dhe, si një protokoll rutimi, mund të përcaktojë rrugën më efikase në rrjet.

Bashkësia e protokolleve TCP/IP dhe detyrat

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

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

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

Protokolli i Internetit (IP) – Shtresa 3 – Network Layer

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

ARP/RARP – Shresa 2 – Data Link Layer

Address Resolution Protocol (ARP) shërben për gjetjen e adresës së hardware-it të një hosti të njohur IP, ndërsa me Reverse ARP (RARP) adresës së hardware-it i caktohet adresa përkatëse e IP-së. Për këtë qëllim, sistemi dërgon një MAC broadcast në shtresën Data Link Layer dhe një kërkesë në shtresën e rrjetit (Network Layer). Kërkesa ARP (ARP Request) është një dërgim drejt e në adresën e IP-së së hostit destinacion, adresa MAC e të cilit duhet të zgjidhet (resolution). Në këtë rast sistemi, me adresën e IP-së në fjalë, kërkon te informojë sistemin të cilit i është bërë kërkesa për adresën MAC të tij.

ICMP – Shresa 3 – Network Layer

Internet Control Message Protocol (ICMP) shërben për përcaktimin e gabimeve, të cilat ndeshen gjatë transmetimit të paketave të IP-së. Në këtë rast në destinacion dërgohet një i ashtuquajtur Echo Request. Aplikimi më i njohur, që kthehet dhe përdor ICMP-në, është komanda PING.

Protokollet e sotme të komunikimit; detyrat dhe shërbimet

Protokollet
Protokollet shërbejnë për të garantuar transportin e të dhënave. Ato paraqesin në vetvete „gjuhët“, me të cilat sisteme të ndryshme komunikojnë me njëri tjetrin. Sigurisht, në çdo proces komunikimi marrin pjesë disa protokolle. Sipas detyrave që kryejnë protokollet mund të klasifikohen si më

poshtë;

- ☑ Protokolle për transmetimin fizik të të dhënave.
- ☑ Protokolle për gjetjen e rrugës së paketave dhe për transportin e tyre.
- ☑ Protokolle për transport të dhënash.

Shërbimet

Shërbimet u vënë në dispozicion protokolleve një mjedis në të cilin mund të kryhen detyra si konfigurimi i informacioneve të rrjetit, ose përgatitja e të dhënave për t'u dërguar në sisteme në distancë. Të gjesh vijën ndarëse midis shërbimeve dhe protokolleve nuk është gjithmonë aq e lehtë. Kështu, shërbimi i Internetit bazohet në një protokoll të vetin (HTTP), ndërsa shërbimi i rezolucionit të emrit DNS (Domain Name System) përdor protokollin DNS. Shërbimet e përhapura në kohën e sotme përfshijnë një numër mjaft të madh detyrash të ndryshme. Shumë nga këto detyra garantohen nga më shumë se një protokoll, por mbulohen nëpërmjet disa shërbimeve të ndryshme. Kjo pjesërisht çon në një performancë të ndryshme të rrjeteve, sistemeve e shfrytëzimit, përdoruesve dhe aplikacioneve.

Shërbimet në rrjete ndahen në tre grupe të mëdha:

- ☑ Shërbime për punën në rrjet
- ☑ Shërbime për sistemet e shfrytëzimit
- ☑ Shërbime për përdoruesit dhe aplikacionet

Service Access Points

Çdo komunikim në rrjet ka nevojë për përdorimin e disa protokolleve, me qëllim që të sigurojë transportën pa gabime të të dhënave në rrjet. Në mënyrë që të dhënat të kalojnë nga një shtresë në shërbimin përkatës të shtresës tjetër ato duhet të adresohen tek portat e caktuara për këtë qëllim. Këto quhen ndryshe edhe si Service Access Points (SAP).

Portat dhe shërbimet

Portat janë fusha adrese, të cilat përdoren tek protokollet e rrjetit, me qëllim që paketave me të dhëna t'u caktohen shërbimet përkatëse. Portat e përdorshme numërohen si më poshtë:

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

Disa nga portat për shërbime të njohura paraqiten më poshtë:

FTP (File Transfer Protocol) 21, **SMTP** (Simple Mail Transfer Protocol) 25, **Telnet** 23,
POP (Post Office Protocol) 110, **IMAP** (Interactive Mail Access protocol) 143,
SSH (Secure Shell) 22, **HTTP** (Hyper Text Transfer Protocol) 80, **HTTPS**443,

DNS (Domain Name System) 53, **SNMP** (Simple Network Management Protocol) 161.

Tema 3. Adresat MAC dhe adresat e IP-së.

Adresat Mac dhe IP

Nëse ju duhet të dërgoni një letër, keni nevojë për adresën e shtëpisë të marrësit. Adresa është një tregues për postierin se ku duhet të shkojë letra, kështu që adresa duhet të jetë unike. Nuk duhet të ketë dy shtëpi me adresa saktësisht të njëjta, përndryshe do të kishte ngatërrim të adresave. Interneti punon në të njëjtën mënyrë si shërbimi postar. Në vend të dërgimit të letrave, pajisjet dërgojnë "paketa të dhënash" dhe adresat IP dhe adresat MAC përcaktojnë se ku shkojnë këto paketa të dhënash.

Çfarë është adresa IP?

Një adresë IP (*Internet Protocol*) është një grup unik numrash që identifikon një pajisje të lidhur me internetin. Për të kuptuar se nga vjen kjo adresë, ne duhet të kuptojmë si funksionon interneti.
Në terma të thjeshtë, interneti është vetëm një mori rrjetash të veçuara që janë të lidhura së bashku. Çdo rrjet quhet një *Internet Service Provider* (ISP) dhe nëse blini një shërbim nga një ISP, mund të lidheni me atë rrjet të ISP-së dhe të gjitha rrjetet e tjera të lidhura me ISP-në tuaj.
Çdo ISP ka një grup adresash IP që ata menaxhojnë dhe kur blini shërbimin, ju caktohet një adresë IP. Kur të dhënat nga interneti duhet të vijnë te ju, rrjeti i ISP-së sheh se destinacioni është adresa juaj unike e IP, më pas ju dërgon këto të dhëna.

Ka dy lloje adresash IP:
• ***IPv4***, i cili formohet nga katër grupe numrash të ndara me pikë, ku secili numër varion nga 0 deri në 255. Për shembull: 192.168.10.2.
• ***IPv6***, i cili formohet nga tetë grupe me vargje me katër karaktere secili të ndara me dy pika, ku secili varg përmban numër dhe shkronja. Për shembull: 2001:1265:0:0:ae4:0:5b:6b0. Edhe pse janë 4.3 bilion adresa IP në total, ato janë pothuajse të zëna dhe drejt mbarimit. Kjo është arsyeja pse po shkohet drejt IPv6, ku ka mbi 320 trilion adresa të mundshme në total.

Çfarë është adresa MAC?

Një adresë MAC (*Media Access Control*) identifikon një "ndërfaqe rrjeti" unike në një pajisje. Ndërsa adresat IP janë caktuar nga ISP-të dhe mund të ri-përcaktohen pasi pajisjet lidhen dhe shkëputen, adresat MAC janë të lidhura me një përshtatës fizik dhe janë caktuar nga prodhuesit.
Adresa MAC është një varg me 12 karaktere ku secili karakter mund të jetë një numër nga 0 në 9 ose shkronjë ndërmjet A dhe F. Për t'u lexuar më lehtë vargu ndahet në pjesë. Ka tre forma më të përdorshme, e para është më e preferuara dhe më e zakonshme:

1. 68:7F:74:12:34:60
2. 3A-34-52-C4-69-B8
3. E80.888.CB3.FB4

Gjashtë karakteret e para (të quajtura prefiks) përfaqësojnë prodhuesin, ndërsa gjashtë karakteret e fundit përfaqësojnë numrin identifikues unik për pajisje të veçanta. Adresa MAC nuk përmban informacion rreth rrjetit që lidhen pajisjet.

Adresa IP dhe MAC punojnë së bashku

Kur dërgohet një pako, vetëm adresa e shtëpisë nuk është e mjaftueshme. Duhet adresa e shtëpisë dhe emri juaj, sepse për ndryshe do të merrni pakon dhe nuk do të dini nëse është për ju, prindërit e tu apo për ndonjë pjesëtar tjetër të familjes.

Adresa IP përcakton ku jeni, ndërsa adresa MAC përcakton kush jeni. Modemi/ruteri juaj ka një adresë IP unike të vendosur nga ISP. Pajisjet e lidhura me ruterin/modemin kanë një adresë MAC unike. Adresa IP merr të dhënat në ruterin/modemin tuaj dhe routeri/modemi i dërgon ato në pajisjen e duhur.

Adresa IP përdoret për të transportuar të dhëna nga një rrjet në një rrjet tjetër duke përdorur protokollin TCP/IP. Adresa MAC përdoret për të dërguar të dhënat në pajisjen e duhur në një rrjet.

Tema 4. Protokolli i Internetit (*IP*), pjesët përbërëse dhe detyrat e tij. Caktimi i adresave të IP-së.

Funksioni dhe pjesët përbërëse të adresave të IP-së

Kërkesë kryesore për shkëmbimin e të dhënave në rrjet është që çdo kompjuter (host) dhe informacionet e caktuara të dërguara për të mund të identifikohen qartë. Ky identifikim mundësohet me ndihmën e një adrese. Në rast se rrjeti duhet të shtrihet globalisht, atëhere kërkohet një procedurë shtesë, e cila mundëson lokalizimin e një hosti brënda gjithë rrjetit.
Në suitën e protokolleve TCP/IP, Protocoli i Internetit (IP) është përgjegjës për adresimin e hosteve dhe për shkëmbimin e paketave me të dhëna mes tyre. Të gjithë hostet marrin në këtë mënyrë një adresë IP-je (angl. IP-Address), e cila përbëhet nga një rradhë 32 shifrash binare me 0 dhe 1-sha, p.sh.: 11000000101010000000000111111110.
Për përdoruesin, paraqitja në sistemin decimal e adresave të IP-së është më e lehtë për t'u kuptuar edhe për t'u mbajtur mend, sesa paraqitja në sistemin binar. Për këtë arsye, adresat e IP-së ndahen në katër blloqe të quajtura ndryshe oktete ku secila i korrespondon 1 Byte (respektivisht 8 Bit). Secili nga këto blloqe përfaqëson 2^8=256 kombinime të mundshme të 8 shifrave binare, që i korrespondojnë një vlere decimale nga 0...255. Të katër oktetet shkruhen njëra pas tjetrës dhe ndahen me pika:

11000000 10101000 00000001 11111110 = 192.168.1.254

Këtu vlejnë rregullat e zakonshme të konvertimit të numrave binarë në decimalë. P.sh.

⇒ Vini re se për cdo shifër binare të një okteti ka nje vlere korresponduese decimale.

Shifrat binare	1	0	1	0	1	0	0	0
Vlera decimale (dhjetore)	128	64	32	16	8	4	2	1
	(2^7)	(2^6)	(2^5)	(2^4)	(2^3)	(2^2)	(2^1)	(2^0)

⇒ Bëni shumën e të gjitha vlerave decimale, shifra binare e të cilave është 1. Rezultati është vlera decimale përkatëse e oktetit.

128 + 32 + 8 = 168

Pjesët përbërëse të një adrese IP-je

Adresat e IP-së ndahen në disa pjesë, si edhe numrat e telefonit, në prefiks dhe numrin lokal, Secila nga këto pjesë përmbush një detyrë të caktuar. Në këtë mënyrë është e mundur, që një host të lokalizohet njëlloj si lokalisht, ashtu edhe në një rrjet global IP-je (Internet).

Çdo adresë IP-je përmban respektivisht dy pjesë përbërëse:

- ☑ Adresa e rrjetit, e cila jep segmentin përkatës të rrjetit, në të cilin ndodhet një host
- ☑ Adresa e hostit, e cila dallon hostet e vecanta në një segment

Adresa e rrjetit mund të ndahet nga ana e saj në një adresë identifikuese të rrjetit në Internet dhe në një adresë identifikuese subneti vetëm brënda një segmenti rrjeti.

Sipas përcaktimit të bërë, adresa e IP-së fillon me adresën e rrjetit dhe mbaron me adresën e hostit. Në njërën nga shifrat ndodh kthimi i adresës së rrjetit në adresa hostesh.
Në përcaktimin klasik të IP-së këto shifra fiksohen me ndihmën e një klase adresash. Në fushën e adresave të hosteve duhen marrë parasysh edhe dy raste të vecanta:

- ☑ Një adresë hosti, e cila përbëhet nga shifra binare 0, p.sh. 192.168.1.**0**, është vetë adresa e rrjetit dhe nuk lejohet të përdoret si adresë e një host të caktuar.
- ☑ Në rast se të gjitha shifrat binare të një adrese hosti përbëhen nga 1-sha, psh. 192.168.1.**255**, këtu mund të flitet për një broadcast address të rrjetit respektiv. Nëpërmjet kësaj adrese u adresohemi bashkërisht të gjitha hosteve të një rrjeti. Ajo nuk lejohet të përdoret për hoste të tjera të veçanta.

Klasat e adresave

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

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

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

Caktimi i adresave të IP-së

Caktimi i adresave statike

Gjatë konfigurimit standard, kur nuk ka server DHCP, Windows-i përdor proçesin e konfigurimit automatik të adresës së IP-së dhe parametrave të tjera për TCP/IP-në (APIPA – 169.254.X.X).
TCP/IP-ja mund të konfigurohet edhe manualisht. Pjesa më e madhe e elementëve të konfigurimit gjendet tek dritarja Local Area Connection - Properties. Më pas, zgjidhet Internet Protocol (TCP/IP) dhe butoni Properties. Për TCP/IP-në kërkohet minimumi dhënia e një adrese IP-je dhe një Subnetmaske β .
Komunikimi me subnete të tjera ose në Internet kërkon akoma dhënien e një adrese për *Default gateway* χ dhe të paktën një adresë për serverin DNS δ.
DNS-ja nevojitet edhe për integrimin e një kompjuteri në një Windows Domain.

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

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

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

DHCP është zgjerim i *Bootstrap-Protokols* (BootP) dhe bazohet në modelin Client-Server. Serveri DHCP disponon një diapazon (pool) adresash IP-je, të cilat mund t'ua japë klientëve. Çdo klient

DHCP, kërkon gjatë startimit, dhe në vazhdim, në intervale të caktuara, një server DHCP në rrjet. Kur e gjen dhe arrin të komunikojë me të merr prej tij për një periudhe kohe të caktuar, një adresë IP-je dhe të gjitha të dhënat e tjera të nevojshme për konfigurim. Ky proces njihet si Lease.

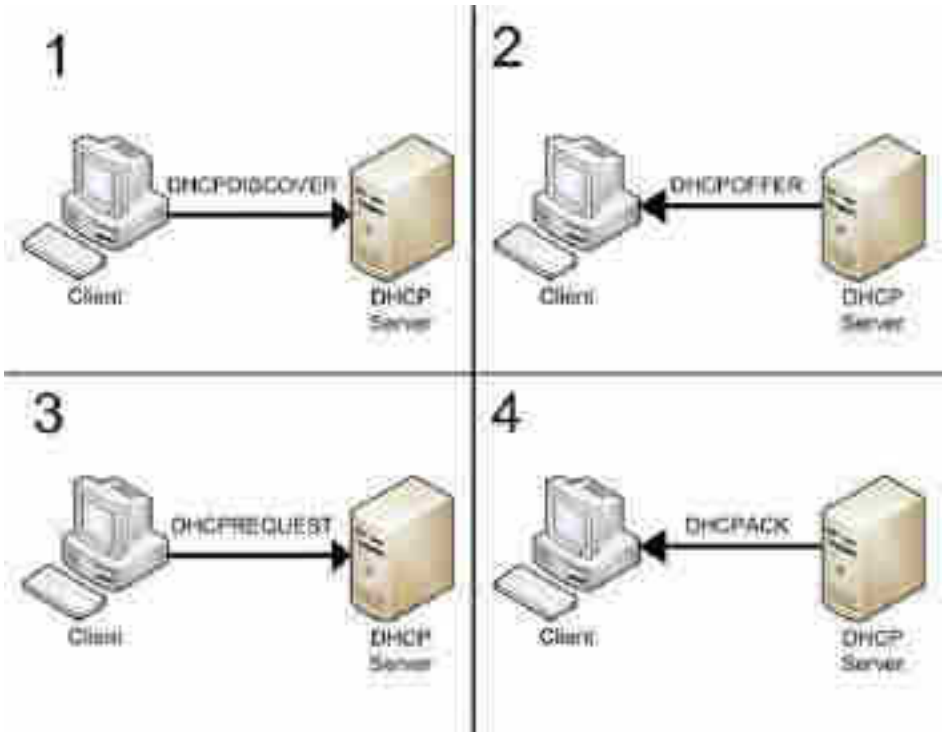
Caktimi i adresave të IP-së me DHCP

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

- ☑ Caktimi automatik, gjatë të cilit Serveri DHCP i cakton klientit një adresë IP-je brënda një diapazoni të përcaktuar. Adresa është e lidhur me adresën MAC të klientit për një kohë të pacaktuar. Pas fshirjes së DHCP-Caches në Server, mund të fillojë sërish caktimi i adresave të reja të IP-së.
- ☑ Gjatë caktimit dinamik të IP-ve, adresat e dhëna memorizohen në një skedar konfigurimi. Klienti, gjatë një periudhe kohe të përcaktuar (Lease-Time), duhet ta konfirmojë adresën, përndryshe adresa mbetet e lirë dhe mund t'i caktohet një kompjuteri tjetër që identifikohet në rrjet.

Caktimi i adresave të IP-së nëpërmjet DHCP-së

Dhënia e sukseshme e një adrese IP-je, për një klient DHCP të pa konfiguruar, kryhet gjatë katër hapave:



Klienti DHCP, gjatë inicializimit të TCP/IP-së, dërgon një broadcast në subnet-in lokal, me anë të të cilit kërkon dhëniën e konfigurimit të IP-së. Ky mesazh i dërguar quhet DHCPDISCOVER (1). Serveri DHCP, që është aktiv në rrjet, reagon ndaj kësaj kërkese me një DHCPOFFER (2), e cila përmban një adresë IP-je dhe një subnetmask për klientin. Klienti e zgjedh ofertën në formë Lease-i dhe e bën të njohur sërish në rrjetin lokal nëpërmjet një DHCPREQUEST (3). Në këtë mënyrë, të gjithë serverat DHCP e dinë tashmë cila ofertë u mor në përdorim dhe nga cidi klient. Serveri DHCP, oferta e të cilit u zgjodh nga klienti, konfirmon përfundimisht zgjedhjen me dërgimin e një DHCPACK (4) (*acknowledge*), e cila përmban të gjitha informacionet e mëtejshme që duhen për konfigurimin e TCP/IP-së së klientit.

Tema 5. Protokollet *Ipv4* dhe *Ipv6*, ndertimi dhe dallimet mes tyre.

Ka dy lloje adresash IP:
• ***IPv4***, i cili formohet nga katër grupe numrash të ndara me pikë, ku secili numër varion nga 0 deri në 255. Për shembull: 192.168.10.2.
• ***IPv6***, i cili formohet nga tetë grupe me vargje me katër karaktere secili të ndara me dy pika, ku secili varg përmban numër dhe shkronja. Për shembull: 2001:1265:0:0:ae4:0:5b:6b0.

Edhe pse janë 4.3 bilion adresa IP në total, ato janë pothuajse të zëna dhe drejt mbarimit. Kjo është arsyeja pse po shkohet drejt IPv6, ku ka mbi 320 trilion adresa të mundshme në total.

IP adresa është një adresë logjike e protokollit IP, që vepron në shtresën e Rrjeteve të modelit OSI, dhe në versionin e 4 të saj (IPv4) paraqet një vlerë sekuenciale numerike 32- bitëshe apo 4-bajtëshe të shprehur me numra binarë 1 dhe 0.

Adresa IP e shprehur në vlerë binare dhe decimale

IP Adresa:
Vlera Binare: **11000000 10101000 00001010 00011001**
Vlera Decimale: **192.168.10.25**

Terminologji bazë të IP adresimit:

1. **Bit** – Paraqet një numër dhe mund te marr vlerat 1 ose 0
2. **Byte** – është njësi që përfshin 8 bite.
3. **Okteti** – është vlerë 8-bitëshe dhe përdoret në skemat adresuese ku çdo IP adresë përbëhet nga 4 oktete, sepse 8 x 4 = 32, është gjatësia e versionit 4 të adresave IP.
4. **Adresa e rrjetit** – përcakton rrjetin që përdoret.
5. **Adresa Broadcast** – adresa që dërgon informacione periodike në hostet që permban rrjeti.

Struktura IP

Çdo oktet mund të marrë vlerat nga 0 deri në 255, sepse kemi 8 bite në dispozicion, d.m.th. 2^8 = 256.

Formati 32 bitësh i IP adresës (IPv4)

Klasat e IP adresave

Për të përcaktuar dhe për të përkufizuar rrjetet kompjuterike në ato të vogla, të mesme dhe të mëdha, IP adresat ndahen në 5 klasa.

Shpërndarja e adresave IPv4 sipas klasave:

- Klasa A
- Klasa B
- Klasa C
- Klasa D dhe E

Klasa A e IP

Okteti i parë definon rrjetin ndërsa 3 bajtët (oktetët) e tjerë përdoren për të adresuar hostet në rrjet. Në figurë është paraqitur struktura IP e adresave të klasës A.

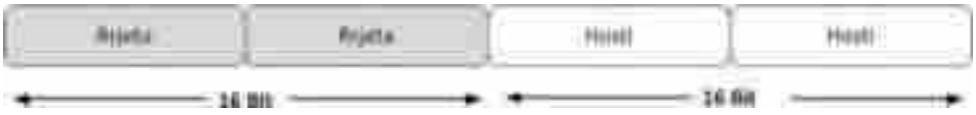
Formati i adresave të Klasës A

Hapësira e adresave që mund të përdorë klasa A është nga 0.0.0.0 deri në 127.0.0.0
Numri maksimal i hosteve në një rrjet të klasës A është: $2^{24} - 2 = 16{,}777{,}214$ hoste

Klasa B e IP

Dy oktet e parë janë të dedikuar për adresën e rrjetit, ndërsa dy oktetët e mbetur përdoren për adresim të hosteve në rrjet.

Formati i adresave të Klasës B



Hapësira e adresave që mund të përdorë klasa B është: nga 128.0.0.0 deri në 191.0.0.0
Numri maksimal i hosteve në një rrjet të klasës B është: $2^{16} - 2 = 65{,}534$ hoste.

Klasa C e IP

Tre oktetet e parë janë të dedikuar për adresën e rrjetit, ndërsa okteti i mbetur përdoret për adresim të hosteve në rrjet.

Formati i adresave të Klasës C

Hapësira e adresave që mund të përdorë klasa C është: nga 192.0.0.0 deri në 223.0.0.0
Numri maksimal i hosteve në një rrjet të klasës C është: $2^{8} - 2 = 254$ hoste.

Klasa D e IP

Në bazë të standartit IPv4 tre bitët e parë në oktetin e parë te adresa e klasës D çdo herë duhet të kenë vlerën 1 ndërsa biti i katërt duhet të ketë vlerën 0.

Formati i adresave të Klasës D

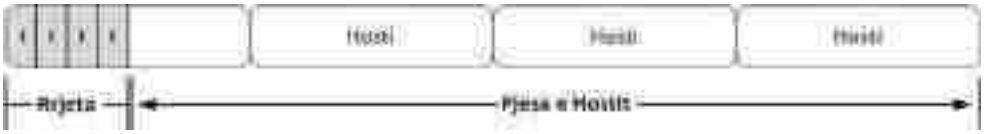
IP adresat, të cilave okteti i parë i fillon me vargun nga 224 dhe përfundon me 239 janë IP adresat e klasës D, multicast.

Tabela. Protokollet e rrugëtimit që përdorin multicast IP adresat e klasës D

Protokolli i rrugëtimit	Adresa multicast
Routing Information Protocol verzioni 2 (RIPv2)	224.0.0.9
Enhanced Interior Gateway Protocol (EIGRP)	224.0.0.10
Open Shortest Path First (OSPF)	224.0.0.5 224.0.0.6

Klasa E e IP

Në bazë të standardit IPv4 katër bitët e parë në oktetin e parë te adresa e klasës E, çdo herë duhet të kanë vlerën 1.



Formati i adresave të Klasës E

IP adresat okteti i parë i të cilave fillon me vargun nga 240 dhe përfundon me 255 janë IP adresat e klasës E.

Internet Protokolli versioni 6 – IPv6

Historiku i zhvillimit të protokollit IPv6 filloi në fillim të viteve 90, kur u kuptua se hapësira e adresimit që është në dispozicion të protokollit IPv4 shumë shpejt do të shpenzohet. Sipas disa analizave, protokolli IPv4 do të mbetej pa IP adresa diku rreth vitit 2010. Këto rezultate e sfiduan komunitetin e Internetit që të vije me një zgjidhje. Para tyre ishin dy mundësi:

Ndryshime minimale: protokolli të mos ndryshohet fare, por vetëm të rritet hapësira e adresimit. Kjo strategji ishte me e lehtë si nga aspekti i zhvillimit të protokollit po ashtu edhe nga aspekti i implementimit të tij në praktikë.

Ndryshime maksimale: Të zhvillojnë versionin e ri të protokollit. Një qasje e tillë do të mundësonte inkorporimin e veçorive dhe shtesave të avancuara në protokollin IP.

Pasi kjo çështja nuk ishte urgjente, është marrë vendimi që të zhvillohet një protokoll i ri nga fillimi. Fillimisht ky protokoll është quajtur IP i gjeneratës së ardhshme IPng (*IP next generation*) ndërsa si emër definitiv është vendosur IP versioni 6 (IPv6).

Arkitekturë adresimi e protokollit IPv6

Më herët kemi thënë se protokolli IPv4 përdor hapësirë adresimi 32-bitëshe që gjithsej na ofron 4,3 miliardë adresa unike. Në shikim të parë ky numër duket shumë i madh, mirëpo për arsye të rritjes eksponenciale të Internetit ky numër nuk mjafton më. Protokolli IPv6 përdorë hapësirë adresimi prej 128-bitëshe që gjithsej na ofron 2^{128} që është e barabartë me 3.4 x 10^{38} adresa unike.

IPv6 adresat shkruhen duke përdorur tetë blloqe me nga katër shifra heksadecimale. Çdo bllok, i ndarë nga kolonat, paraqet një numër me 16 bit. Adresa e plotë IPv6 është:

2001:0CE8:5AD9:0000:0000:0000:00F7:2C2A

Kjo adresë mund të shkurtohet duke eliminuar zerot vazhduese brënda bllokut. Atëherë në vazhdim kjo adresë do të marrë formën:

2001:CE8:5AD9:0:0:0:F7:2C2A

Ne mund ta shkurtojmë këtë adresë me tej duke i zëvendësuar zerot në IP adresë me dy pika të dyfishta (**::**). Kjo mund të bëhet vetëm një herë në një adresë IPv6. Adresa e mësipërme do te marrë formën:

2001:CE8:5AD9::F7:2C2A

Pasi IPv6 adresa përbëhet nga 8 blloqe, shumë lehtë mund të përcaktojmë se sa blloqe janë zëvendësuar me kolona të dyfishta (**::**). Në shembullin tonë 3 blloqe me zero janë zëvendësuar me kolonë të dyfishtë.

Ekzistojnë tre lloje të IPv6 adresave:

- Adresat *Unicast*
- Adresat *Multicast*
- Adresat *Anycast*

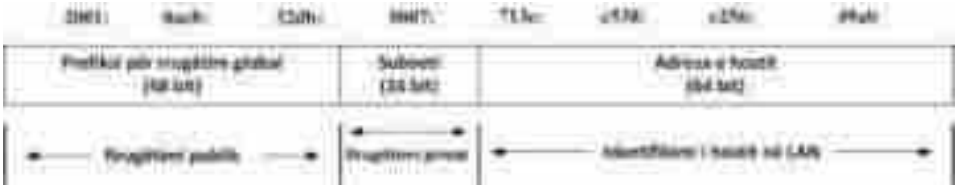
Adresat *Unicast* – përdoren për të identifikuar një ndërfaqe të vetme. Adresa Unicast ndahet në dy pjesë: 64 bitët e parë identifikojnë pjesën e rrjetit, ndërsa 64 bitë të dytë identifikojnë pjesën e hostit. Kjo adresë është më tepër e përdorur gjatë komunikimit në rrjetet IPv6 në Internet. Ekzistojnë dy lloje të adresave unicast:

Adresat globale unicast – janë adresat ekuivalente me adresat publike të protokollit IPv4 dhe rrugëtohen globalisht në rrjetet IPv6 të internetit. Prefiksi aktual i adresave unicast globale është 2000::/3, nga kjo rrjedh se blloku i parë merrë vlerat të shprehura me numrat heksadecimalë nga 2000 e deri në 3FFF. Shembull i një adrese globale unicast është:

2001:0ac8:32db:7:713e:c538:e256:49ab

Struktura e adresës globale unicast e paraqitur në figurë:

- 48 bite të parë të adresës IPv6 paraqesin prefiksin për rrugëtimin global i cili e identifikon sajtin e organizatës përkatëse. Tre bitë të parë janë 001 dhe tregojnë se adresa është unicast. Vlera prej 16 bitëve paraqet fushën e rezervuar për subneta të brendshme të organizatës. Numri i përgjithshëm i subnetave që mund të krijohen brënda organizatës është 216 apo 65536 subneta.
- 64 bitë të fundit të adresës IPv6 identifikojnë ndërfaqen unike të hostit brënda subnetës. Kjo pjesë e adresës IPv6 është ekuivalente me pjesën e hostit të adresës IPv4.



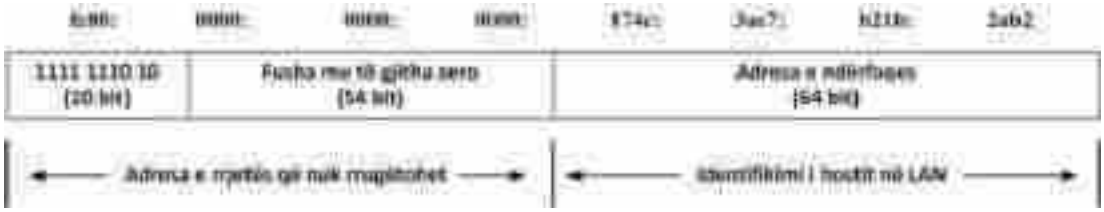
Struktura e IPv6 adresës globale unicast

Adresa unicast e lidhjes-lokale (*Link-local unicast address*) – janë të ngjashme me IP adresat automatike private APIPA (*Automatic Private IP Addresses*) të protokollit IPv4 rangu i të cilëve është 169.254.0.0/16. Këto adresa janë automatike që do të thotë se vetëkonfigurohen, nuk rrugëtohen, që do të thotë se përdoren vetëm për komunikim në subnetat lokale. Adresat *unicast* të lidhjes-lokale gjithmonë fillojnë me vlerën heksadecimale "**fe80**". Shembull i një adrese të tillë është:

Fe80::174e:3ae7:b21b:2ab2

Strukturën e adresës unicast të lidhjes-lokale të paraqitur në figurë e shpjegojmë në vazhdim:

- Gjysma e parë e adresës shkruhet në formën " fe80:: " ndërsa në formën e zgjeruar do të shkruhet si " fe80:0000:0000:0000 ".
- Gjysma e dytë e adresës paraqet adresën e ndërfaqes.



Struktura e IPv6 adresës unicast të lidhjes-lokale

Adresat *Multicast* – identifikojnë një grup të ndërfaqeve që zakonisht i përkasin hosteve të ndryshëm. Paketa e të dhënave, që si destinacion ka adresën *multicast*, dërgohet te të gjitha ndërfaqet që identifikohen me këtë lloj adrese. Adresat *multicast* identifikohen nga prefiksi "**ff00::/8**", që do të thotë se cdo adresë *multicast* fillon me " **ff** " gjë që i bën ato shumë lehtë për t'u dalluar.

Struktura e adresës *multicast* është paraqitur në figurë

- 8 bite të parë çdo herë kanë vlerën 1111 1111 për të treguar se kemi të bëjmë me adresa *multicast*.
- Fusha *Flags* me gjatësi 4 bitë tregon rolin e adresës së caktuar *multicast*. Tre bitët e parë të fushës *flags* çdo herë janë zero, ndërsa biti i 4 merr vlerat 1 dhe 0. Nëse ky bitë e ka vlerën 0 tregon se adresa *multicast* është permanente, nëse merr vlerën 1 atëherë tregon se adresa *multicast* është jo-permanente apo në tranzicion.
- Fusha *scope* mundëson krijimin e adresave *multicast* që mund të jenë të dukshme në Internet, ose të kufizuara që mund të jenë të dukshme brënda një organizate të caktuar.
- Pjesa e fundit e adresës *multicast* ka gjatësi prej 112 bit, identifikon *multicast* grupe të shumëfishta dhe është vlerë unike brënda *scope*.

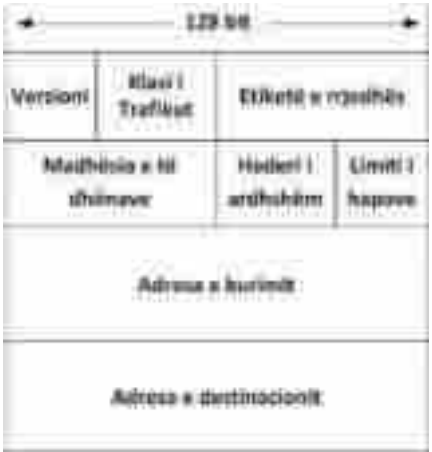
Struktura e IPv6 adresës multicast

Adresa *Anycast* – definon një grup të kompjuterëve ku të gjithë kompjuterët e ndajnë një adresë të përbashkët. Paketa që si destinacion ka një adresë *anycast* dërgohet te një anëtar i grupit, zakonisht anëtarit më të afërt. Adresimi *anycast* përdoret zakonisht në rastet kur kemi disa server që mund të përgjigjen në një kërkesë. Kërkesa do t'i dërgohet serverit që është më i arritshëm. Nga ky proçes komunikimi gjenerohet vetëm një kopje e kërkesës, kjo kopje do të arrijë vetëm te një server. Dallimi në mes të adresave *multicast* dhe *anycast* qëndron në atë se të gjithë hostët që janë pjesë e grupit *multicast* pranojnë kopje të paketës, ndërsa për grupin *anycast*, paketa arrin vetëm te hosti më i afërt. Protokolli IPv6 nuk e ka të definuar një bllok të caktuar për adresat *anycast*, mirëpo adresat caktohen nga blloku i adresave *unicast*.

Është me rëndësi të theksojmë se protokolli IPv6 nuk ka të definuar adresën *broadcast*, sikurse ndodh me protokollin IPv4. Në rastet e caktuara IPv6 e konsideron *broadcast* rastin e posaçëm të procesit *multicast*.

Hederi i paketës IPv6

Hederi i paketës IPv6 përbëhet nga 40 oktete, në dallim nga hederi i paketës IPv4 që ka vetëm 20 oktete siç është paraqitur në figurë. Për dallim nga hederi i IPv4, hederi i paketës IPv6 ka më pak



fusha gjë që e bën më te lehtë për t'u procesuar nga pajisjet e rrjeteve.

Hederi i protokollit IPv6

Hederi i protokollit IPv6 përmban këto fusha:

Versioni – është fushë 4-bitëshe, njësoj me IPv4. E cila përmban vlerën 6 që përfaqëson protokollin IPv6.

Klasa e Trafikut (*Traffic Class*) – është fushë 8-bitëshe e ngjashme me fushën e llojit të shërbimit (ToS) në IPv4. E cila etiketon paketën me klasën e trafikut që përdoret në shërbimet e diferencuara (DiffServ). Këto funksionalitet janë të njëjta si për IPv6 ashtu edhe për IPv4.

Etiketë e rrjedhës (*Flow Label*) – është fushë 20-bitëshe që e bën etiketimin e rrjedhës së trafikut. Mund të përdoret për teknikat komutuese shumë-shtresore (ang. *multilayer switching*) dhe për përshpejtim të komutimit të paketave.

Madhësia e të dhënave (*Payload Length*) – i ngjashëm me fushën e madhësisë së përgjithshme në IPv4. E përshkruan madhësinë e të dhënave, në bajt, që i enkapsulon paketa.

Hederi i ardhshëm (*Next Header*) – tregon se cili heder e pason hederin e paketës IPv6. Kjo fushë është e ngjashme me fushën e Protokollit në IPv4.

Limiti i hapave (*Hop Limite*) – Paraqet numrin e hapave që mund t'i kalojë një paketë.

Adresa e burimit (*Source Address*) – Kjo fushë përbëhet nga 16 oktete apo 128 bite. E identifikon burimin e paketës.

Adresa e destinacionit (*Destination Address*) – kjo fushë përbëhet nga 16 oktete apo 128 bite dhe identifikon destinacionin e paktës.

Veçorit e protokollit IPv6

Protokolli IPv6 ofron shumë përmirësime dhe veçori funksionale në krahasim me protokollin IPv4. Disa prej tyre janë:

Hapësirë adresimi më e madhe – IPv6 e rrit numrin e biteve për adresim katër herë, nga 32 bitë në 128 bitë. Prandaj, IPv6 i ofron përdoruesve adresa të shumta globale të cilat mund të përdoren për të adresuar pajisjet e ndryshme duke përfshirë këtu telefonat e mençur, tablet, kompjuter etj.

Hederi më i thjeshtë - *Hederi* i paketës IPv6 ka më pak fusha gjë që e bën më të lehtë për t'u procesuar si dhe mundëson rrugëtim më efikas.

Mobilitet dhe siguri – është plotësisht kompatible me standardet mobile të protokollit IP dhe me komponentin e sigurisë IPsec.

Mundësi tranzicioni – ofron mundësin për përfshirje të veçorive të protokollit IPv4 në atë te IPv6. Kete mund ta realizojmë në këtë mënyrë:

- Në një ndërfaqe të hostit konfigurojmë një grup të dyfishtë të përbërë nga IPv4 dhe IPv6.

- Gjithashtu mund të përdorim teknikën IPv6 mbi IPv4 ndryshe quhet tuneli 6 mbi 4, e cila përdor tunelin IPv4 për të bartur trafikun e IPv6.

IPv6 (Protokolli i Internetit – versioni 6)

Nëpërmjet protokollit IPv6 synohet të shmanget mungesa e adresave IPv4 në Internet. Adresat IPv6, në ndryshim nga adresat IPv4, përbëhen jo më nga 32 Bit, por nga 128 Bit. Adresa IPv6 paraqitet si tetë grupe katër shifrore hegzadecimale. Secili grup paraqet 16 bite (dy oktete). Grupet ndahen nga njeri tjetri me (:).

Shembull i një adrese IPv6 është adresa: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Disa avantazhe janë rritja e sigurisë, QoS etj.

Tema 6. Subnetet *IP* dhe subnetmaskat. *Variable length subnet masks* (*VLSM*)

Subnetmaska

Gjatë vlerësimit të adresave të IP-së, nëpërmjet klasave të adresave, mjafton dhënia e një adrese IP-je, që të identifikohet adresa e rrjetit dhe e hostit. Subnetmaska (Subnet Mask) paraqet një alternativë për përdorimin e klasave të adresave. Përparësia kryesore është mundësia që gjatësia e adresës së rrjetit të shtrihet jo vetëm në nivelin e okteteve të plota, siç ndodh me adresat e klasave A deri C. Me ndihmën e dhënies së një subnetmaske të caktuar, së bashku me caktimin e një adrese IP-je, egziston mundësia që adresa e rrjetit të mbarojë në çdo shifër të adresës së IP-së që ne preferojmë.
Subnetmaska përpunohet nga hosti si çdo adresë IP-je dhe e dhënë 32 bit-she e gjatë. Ajo nuk përbëhet nga një rradhë e çfarëdoshme numrash binarë, por fillon me një binar 1 dhe përmban maksimumi një ndryshim në binarin 0, p.sh
:

11111111 .00000000.00000000.00000000 ose 255.0.0.0

Si rregull, shifrat binare të subnetmaskës, vlera e të cilave është 1 tregojnë adresën e rrjetit. Të gjitha shifrat binare të subnetmaskës që e kanë vlerën 0, i përkasin adresës së hostit:

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

Krahas mënyrës decimale të të shkruarit, ekziston edhe një mënyrë e thjeshtuar e paraqitjes së subnetmaskës, e cila tregon numrin e shifrave që mbuloijnë adresën e rrjetit, pas një adrese IP-je. P.sh adresa e IP-së, 192.168.1.100 me subnetmaskë 255.255.255.0 (me 24 shifra në pjesën e rrjetit) mund të paraqitet edhe si 192.168.1.100/24.

Funksioni i subnetmaskës

Subnetmaska cakton se cilës pjesë të rrjetit i përket adresa e IP-së. Prandaj, është e detyrueshme që së bashku me adresën e IP-së, të jepet edhe subnetmaska. Me anë të subnetmaskës përcatkohet saktë përkatësia në rrjet e një adrese IP-je. Hosti, nëpërmjet subnetmaskës së partnerit të tij në komunikim, përcakton si duhet të transmetohen të dhënat tek ky i fundit. Për këtë përdoret një operator logjik EDHE (angl. AND) që mbledh adresën e IP-së me subnetmaskën e vet. Kështu, çdo Bit i adresës së IP-së mblidhet me Bit-in përkatës të subnetmaskës. Në bazë të rregullave të mbledhjes së shifrave binare, duke përdorur operatorin logjik AND, marrim adresën e rrjetit, p.sh.:

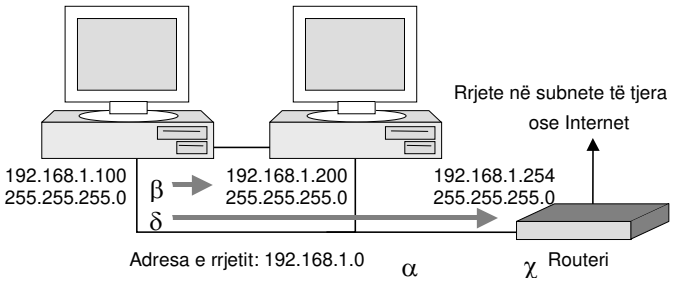
Adresa e IP	192.168.1.100 =	11000000	10101000	00000001	01100100	
Subnetmask	255.255.255.0 =	11111111	11111111	11111111	00000000	
Mbledhja	192.168.1.0 =	11000000	10101000	00000001	00000000	Adresa e rrjetit

Si përfundim, ky proçes përsëritet me subnetmaskën e vet për adresën e IP-së të partnerit me të cilin komunikon (adresa e destinacionit), p.sh:

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

Në këtë rast adresa e pjesës së rrjetit të hostit dhe të partnerit në komunikim janë të njëjta α. Duke qenë se marrësi dhe dërguesi gjenden në të njëjtën pjesë të rrjetit mundësohet dërgimi direkt i të dhënave nga njëri tek tjetri.

Në rast se hosti dhe partneri në komunikim gjenden në subnete të ndryshme, pra subnetmaska në pjesën e rrjetit është e ndryshme, atëhere komunikimi i tyre bëhet i mundur vetëm nëpërmjet një routeri χ (*standard gateway*). Të dhënat dërgohen në router δ, i cili më pas merr përsipër dërgimin më tej të tyre.



Komunikimi brënda dhe jashtë një segmenti rrjeti IP

Konvertimi i IP adresave nga numrat Decimalë në Binarë dhe anasjelltas

Për ta kuptuar IP adresimin në rrjetet kompjuterike është e nevojshme të mësojmë konvertimin e tyre nga formati binar në atë decimal dhe anasjelltas.

Gjatë proçesit të konvertimit të IP adresave duhet të kemi parasysh dy rregulla:

- Gjatë konvertimit të IP adresës nga formati decimal në atë binar, çdo numër decimal konvertohet në numër binar 8-bitësh

- Gjatë konvertimit të IP adresës nga formati binar në atë decimal, atëherë çdo sekuencë binare 8-bitëshe konvertohet në një numër decimal

Siç e kemi theksuar më herët, numrat në sistemin binar kanë bazën 2, pesha (vlera) e tyre varet nga pozita në numër duke e llogaritur nga e djathta në të majtë. Numrat binarë përdorin vetëm dy shifra dhe ato janë 0 dhe 1 që ndryshe quhen bit. Pesha e bitit në numër binarë llogaritet si 2 në fuqi n-1, ku n është pozita e bitit në numër, prandaj pesha $= 2^{n-1}$. Pesha individuale e 8 bitëve të një bajti janë paraqitur në këtë tabelë:

Tabela. Pesha binare e numrave 8 bitësh

Pesha	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Pozicioni bitit	biti 7	biti 6	biti 5	biti 4	biti 3	biti 2	biti 1	biti 0
Vlera e kolonës	128	64	32	16	8	4	2	1

Në tabelë mund të shohim se duke shkuar nga e djathta në të majtë vlera e bitit dyfishohet. Duke përdorur tabelën e peshave të numrave binarë me lehtësi mund të konvertojmë numrat binar në decimal dhe anasjelltas.

Shembull: Të konvertohet IP adresa e klasës B 139.177.22.5 nga forma decimale në atë binare dhe anasjelltas duke përdorur tabelën e peshave binare.

Zgjidhja: Për ta konvertuar IP adresën nga forma decimale në atë binare do përdorim tabelën e peshave binare dhe duke u bazuar në dy rregullat, do të konvertojmë çdo oktet të IP adresës:

Konvertimi i IP adresës nga vlera decimale në atë binare

Pesha	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**
Vlera e kolonës	128	64	32	16	8	4	2	1
139	1	0	0	0	1	0	1	1
177	1	0	1	1	0	0	0	1
22	0	0	0	1	0	1	1	0
5	0	0	0	0	0	1	0	1

IP adresa e shprehur në formë binare do të jetë

139.177.22.5 = 10001011 10110001 00010110 00000101

Anasjelltas, duke përdorur të njëjtën tabelë mund të konvertojmë IP adresën nga forma binare në atë decimale.

Operacioni DHE i Bulit dhe subnetimi

Për të zbuluar se në cilën subnet IP adresa e caktuar bënë pjesë, ruterët përdorin operacionin DHE

të Bulit, ndërmjet IP adresës dhe subnet maskës.

Operacioni DHE i Bulit në mes të IP adresës dhe Subnet maskës

	Decimal	Binar
Adresa	139.177.22.5	10001011 10110001 00010110 00000101
Subnet Maska	255.255.240.0	11111111 11111111 11110000 00000000
Operacioni DHE	139.177.16.0	10001011 10110001 00010000 00000000

Në rreshtin e parë të tabelës IP adresën 139.177.22.5 e kemi paraqitur në formë decimale dhe binare. Në rreshtin e dytë e kemi paraqitur subnet maskën 255.255.240.0. Ndërsa, në rreshtin e fundit është paraqitur rezultati pas ekzekutimit të operacionit DHE të Bulit në mes të IP adresës dhe subnet maskës. Nga ky proçes vijmë në përfundim se subneti në të cilin bënë pjesë IP adresa 139.177.22.5 është 139.177.16.0.
Për të thjeshtuar shkrimin e IP adresës dhe subnet maskës, në shumicën e rasteve subnet maska paraqitet si prefix (prapashtesë) e IP adresës. Pasi subnet maska përbëhet nga 1-shet binar të njëpasnjëshëm të pasuar nga zerot atëherë prefiksi i subnet maskës do të jetë numri i të gjitha 1-sheve në varg dhe do të shprehet me " / ". Prandaj IP adresa 139.177.16.0 me subnet maskë 255.255.240.0 duke e përdorur prefiksin do ta shkruajmë si 139.177.16.0 /20.
Përdorimi i prefiksit na lehtëson punën rreth leximit të subnet maskës, por gjithashtu edhe informacionet të cilat i paraqet ruteri janë më të shkurtra.

Shembull praktik i subnetimit

Organizatës tonë i është caktuar IP adresa e rrjetit e klasës C me vlerë 193.1.1.0/24. Për t'i plotësuar kërkesat e organizatës kjo adresë e rrjetit duhet të ndahet në gjashtë subneta, ku subneta më e madhe duhet të ketë 25 hoste.

Definimi i subnetave

Fillimisht do të përcaktojmë numrin e nevojshëm të biteve për të krijuar gjashtë subnetet e kërkuar në detyrë. Pasi që adresat e rrjeteve mund të subnetohen vetëm përgjatë kufijve të tyre binarë, atëherë subnetët do të krijohen në blloqet e numrave në fuqi dy si p.sh blloku i parë 2 subnete nga 21, blloku i dytë 4 subneta nga 22, blloku i tretë 8 subnete nga 23, blloku i katërt 16 subneta nga 24 etj. Nga ky shembull vërejmë se është e pamundur të definojmë një bllok të IP adresave që do të përmbajë saktësisht gjashtë subneta. Prandaj, për të plotësuar kushtin e detyrës duhet të definojmë një bllok që përmban 8 subneta (23) prej të cilave dy subneta janë të tepërta dhe mund të mbahen rezervë për rritje të rrjetit në të ardhmen. Në detyrën tonë subnet maska e adresës së rrjetit përmban 24 bite apo /24, prandaj do të na nevojiten 3 bite shtesë apo subnet maska me 27 bite /27 siç e kemi paraqitur në tabelë.

Tabela - Definimi i subnet maskës

		Bit për subneta	Bit për hostet
193.1.1.0 /24	11000001.00000001.00000001.	**000**	00000

255.255.255.224	11111111.11111111.11111111.	**111**	00000

Nga tabela shohim se subnet maska me prefiks /27 bitësh e krijuar në këtë rast, si mbetje do të ketë 5 bite që do të definojnë adresat e hosteve për çdo subnet. Prandaj, çdo subnet me prefiks /27 bite përfaqëson blloqet e vazhdueshme të 2^5 = 32 IP adresa të hosteve. Tetë subnetët e krijuara sipas detyrës sonë do të numërohen duke filluar nga 0 e deri në 7.

Këto subneta janë paraqitur në tabelë.

Tabela - Definimi i subnetave

Subneta #0	11000001.0000001.00000001.	**000**	00000	193.1.1.**0** /27
Subneta #1	11000001.0000001.00000001.	**001**	00000	193.1.1.**32** /27
Subneta #2	11000001.0000001.00000001.	**010**	00000	193.1.1.**64** /27
Subneta #3	11000001.0000001.00000001.	**011**	00000	193.1.1.**96** /27
Subneta #4	11000001.0000001.00000001.	**100**	00000	193.1.1.**128** /27
Subneta #5	11000001.0000001.00000001.	**101**	00000	193.1.1.**160** /27
Subneta #6	11000001.0000001.00000001.	**110**	00000	193.1.1.**192** /27
Subneta #7	11000001.0000001.00000001.	**111**	00000	193.1.1.**224** /27

Për të verifikuar saktësinë e llogaritjes së subnetave duhet të sigurohemi se të gjitha subnetat janë shumëfishat e adresës së subnetës #1. Në rastin tonë, të gjitha subnetat janë shumëfishat e vlerës 32, pra vlerat e subnetave do të jenë 0, 32, 64, 96, 128 e kështu me radhë.

Definimi i adresave të hosteve në subnete

Në bazë të RFC 950 si dhe të praktikave të adresimit në internet, fusha e hostit e IP adresës nuk mund të përmbajë të gjitha bitet me vlerë "**0**" e as të gjitha bitet me vlerë "**1**". Pjesa e adresës së hostit që përmban të gjitha "**0**" paraqet adresën e rrjetit për atë subnetë, ndërsa pjesa e adresës së hostit që përmban të gjitha "1" paraqet adresën broadcast për atë subnet.

Në shembullin tonë, 5 bite nga fusha e adresës së hostit mund të përdoren për adresim në çdo subnet. Prandaj çdo subnet përfaqëson një bllok të 30 adresave për host (25-2 = 30, këtu zbriten dy IP adresa që përfshijnë në vetvete të gjitha "0" dhe "1").

Në shembullin tonë, adresat valide për Subnetën #3 i kemi paraqitur në tabelë

Tabela - Brezi i adresave valide për Subnetën #3

Subneta #3	11000001.0000001.00000001.	011	**00000**	193.1.1.96 /27
Host #1	11000001.0000001.00000001	011	**00001**	193.1.1.97 /27

	.			
Host #2	11000001.0000001.00000001	011	**00010**	193.1.1.98 /27
	.			
Host #3	11000001.0000001.00000001	011	**00011**	193.1.1.99 /27
	.			
--	--			--
--	--			--
Subneta #27	11000001.0000001.00000001	011	**11011**	193.1.1.123 /27
	.			
Subneta #28	11000001.0000001.00000001	011	**11100**	193.1.1.124 /27
	.			
Subneta #29	11000001.0000001.00000001	011	**11101**	192.1.1.125 /27
	.			
Subneta #30	11000001.0000001.00000001	011	**11110**	192.1.1.126 /27
	.			

Definimi i adresës broadcast për subnet

Adresa broadcast për Subnetin #3 është adresa e cila përmban të gjitha "1" në pjesën e hostit. E shprehur me numra kjo adresë do të jetë:

11000001.0000001.00000001.	011	**11111**	192.1.1.127 /27

Nga ky shembull vëm re se adresa broadcast e Subnetës #3 është për një me e vogël se adresa e rrjetit për Subnetën #4 që është 193.1.1.128. Prandaj, adresa broadcast për Subnetën #**n**, ku "**n**" paraqet numrin rendor të subnetës, është për një më e vogël se adresa bazë e Subnetës #(**n+1**).

Adresa broadcast e subnetës #6 është adresa e cila përmban të gjitha "**1**" në pjesën e hostit. E shprehur me numra kjo adresë do të jetë:

11000001.0000001.00000001.	110	**11111**	192.1.1.223 /27

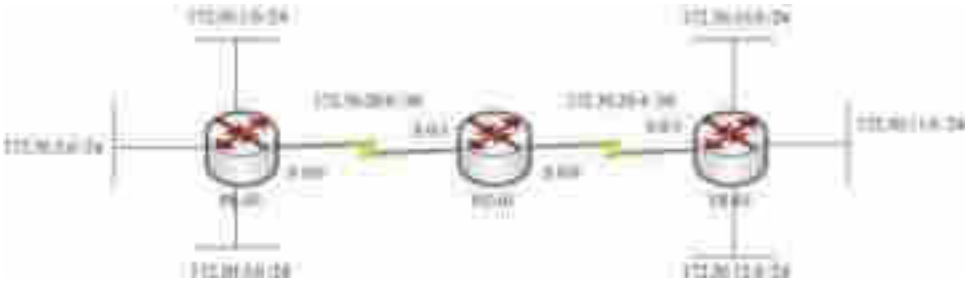
Adresa broadcast e subnetës #6 është saktësisht për një më e vogël se adresa bazë për Subnetën #7 që është (193.1.1.224).

Subnet Maska me gjatësi variable – VLSM

Subnet Maska me Gjatësi Variable – VLSM (*Variable Length Subnet Mask*) është koncept i definuar në RFC 1812 dhe i mundëson administratorëve të rrjeteve të subnetojnë klasat A, B, C të IP adresave duke përdorur subnet maska me gjatësi të ndryshme. Kjo realizohet duke e subnetuar

subnetin. Aplikimi i VLSM-së do të na kursejë me mijëra IP adresa, që me subnetim tradicional do të shkonin dëm.

Për arsye se subnet maska e përcakton madhësinë dhe numrin e hosteve në rrjet, VLSM i ofron mundësi inxhinierëve që të ndërtojnë rrjete me numër të kërkuar të adresave. Në figurë kemi paraqitur një shembull të zbatimit të VLSM-së në rrjetin e klasës B 172.30.0.0.



Zbatimi i VLSM në rrjetin 172.30.0.0 me subnet maskën /30 dhe /24

Në figurë është paraqitur një rast tipik ku për linqet direkte seriale kemi përdorur subnet maskën me prefiks /30, që na jep vetëm 2 adresa për subnet. Ndërsa për rrjetet LAN kemi përdorur subnet maskën me prefiks /24.

Tema 7. *Network Address Translation* (*NAT*)

IP adresat publike dhe private

Stabiliteti dhe funksionimi normal i Internetit në mënyrë direkte varet nga caktimi i adresave IP unike në nivel global. Për këtë arsye është paraqitur nevoja që të definohen disa procedura që do të menaxhonin dhe garantonin shpërndarjen e IP adresave unike në Internet. Fillimisht, organizata e njohur si "*Internet Network Information Center*" (InterNIC) ka qenë përgjegjëse për menaxhimin e këtyre procedurave. Pas mbylljes së kësaj organizate, detyrat e saj i ka trashëguar organizata "*Internet Assigned Number Authority" (IANA)*. IANA edhe në ditët e sotme me kujdes menaxhon shpërndarjen e IP adresave dhe garanton që ato të jenë unike në Internet. Kjo detyrë është shumë e rëndësishme pasi IP adresat e duplifikuara në internet do të shkaktonin funksionim jostabel të Internetit dhe njëkohësisht do ta kompromentonin aftësinë e Internetit të transportojë paketat e të dhënave deri te destinacionet e tyre.

IP adresat publike duhet të janë unike që do të thotë se dy hoste që janë të kyçur në Internet nuk mund të kenë IP adresat e njëjta, sepse IP adresat publike janë të standardizuara dhe janë globale. Mirëpo me rritjen e shpejtë të shërbimeve në Internetit është rritur edhe kërkesa për IP adresat publike e që në një të ardhme shumë të afërt IPv4 adresat do të shpenzohen. Si zgjidhje e këtij problemi është përpiluar protokolli i ri IPv6 i cili me shpenzimin e adresave do ta zëvendësoj adresimin IPv4.

IP adresat private janë një zgjidhje e problemit të shpenzimit të shpejtë të IP adresave publike. IETF në RFC 1918 ka ndarë tri blloqe të IP adresave për përdorim në rrjete private të brendshme. Këto

tri blloqe të adresave përbehen nga një adresë e klasës A, një varg adresash të klasës B dhe një varg adresash të klasës C siç mund të shihet në tabelë:

Vargjet e IP adresave të brendshme të definuara nga RFC 1918

Klasa	Vargu i adresave të brendshme
A	10.0.0.0 deri 10.255.255.255
B	172.16.0.0 deri 172.31.255.255
C	192.168.0.0 deri 192.168.255.255

Adresat që i përkasin këtyre vargjeve nuk do të rrugëtohen nga ruterët e Internetit. Në momentin që e pranojnë paketën me IP adresë nga vargjet e IP adresave private ruteri i shkatërron ato paketa. Mirëpo, për ta kyçur një rrjet privat në Internet është e nevojshme që të bëhet përkthimi i IP adresave private në ato publike. Ky proçes përkthimi quhet përkthimi i adresave të rrjetit (*Network Address Translation*) NAT.

Adresat Private – NAT

Janë të përcaktuara tre grupe adresash IPv4 për përdorim në rrjetet e brendëshme. Këto rrjete nuk janë të lidhura publikisht ose direkt me internetin, por përdorin mekanizmat **NAT** dhe paisje ndërmjetesuese **Proxy** për të komunikuar në internet.

Principi bazë i NAT *(**N**etwork **A**ddress **T**ranslation)* është që shumë kompjutera mund të fshihen pas një adrese të vetme IP të regjistruar. *NAT është një proçes që përkthen adresat IP të kompjuterave të një rrjeti lokal, në një adresë IP të vetme.*

NAT është proçes i përkthimit të një IP adrese të brendshme (private) me një adresë publike. Tre forma të NAT ose tre mënyra operimi të NAT janë:

- *NAT Statik* Korrespondencë 1 me 1, adresa IP Private – IP Publike. Përdoret kryesisht në organizata të vogla.
- *NAT Dinamik* Përdoret më tepër në koorporatat e mëdha. Në dallim nga NAT statik, përdor një grup adresash IP Publike në dispozicion (pool) për të maskuar IP Private. Adresat IP Publike nuk mbeten të njëjtë (statike) për secilën IP Private. Përkthimet nuk ekzistojnë në tabelën NAT derisa ruteri merr trafik që kërkon përkthim. Përkthimet dinamike hiqen nga tabela pas një periudhe inaktive.
- *NAT i tejngarkuar/overload (PAT)* Metoda më e përdorshme e NAT. Njohur si NATP ose NAT me PAT (*Porta Address Translation*). Futet koncepti i portës (shtresa e transportat) si identifikuës i lidhjes – avantazhi i metodës. Mundëson përdorimin e të njëjtës IP Publike për PC të ndryshëm duke përdorur portën si identifikues të trafikut të secilës.

Të përdorësh NAT do të thotë që mjafton vetëm një adresë IP në ndërfaqen e jashtme të sistemit që vepron si gateway ndërmjet një rrjeti privat të brendshëm dhe një rrjeti të madh publik siç është Interneti. ***Kjo adresë shpesh përdoret nga ruteri i cili lidh kompjuterat me internetin, ku NAT është bërë një funksion i domosdoshëm.***

Një sistem që përdor NAT, kanalizon kërkesat që i jepen atij drejt një rrjeti të jashtëm. Psh: një klient kërkon një faqe web dhe kërkesa shkon përmes serverit NAT, në internet.

Paisjes marrëse apo sistemit në distancë, i duket sikur kërkesa i vjen nga një adresë e vetme, ajo e serverit NAT, dhe jo nga paisja apo sistemi individual që bëri kërkesën.

Sistemi që po kryen funksionin e NAT, mban gjurmë se cili sistem e bëri kërkesën, dhe siguron që kur të dhënat të kthehen të shkojnë në destinacionin e duhur.

Kur paisjet në internet përpiqen që të lidhen me kompjuterat e një LAN, ato mund të shohin vetëm adresën e ruterit. Kjo gjë shton dhe nivelin e sigurisë, duke qenë se një ruter mund të konfigurohet si një *firewall,* duke lejuar vetëm sisteme të autorizuara të komunikojnë me paisjet e rrjetit të brendshëm.

Pasi paisja nga rrjeti i jashtëm është lejuar të komunikojë me një kompjuter të rrjetit lokal, adresa IP përkthehet nga adresa e ruterit në adresën unike të kompjuterit.

Adresa gjendet në tabelën e NAT, në të cilën janë të përcaktuara adresat e kompjuterave të rrjetit të brendshëm dhe adresa globale që shihet nga kompjuterat jashtë rrjetit.

ICS *(**I**nternet **C**onnection **S**haring)* nuk është gjë tjetër veçse një implementim i NAT në platformën e windows-it, i cili lejon disa kompjutera të lidhen me internetin duke përdorur të njëjtën lidhje dhe adresë IP.

Tema 8. Protokollet *TCP* dhe *UDP*, ndërtimi dhe funksionimi i tyre.

Protokollet TCP dhe UDP punojnë në shtresën 4 – *Transport Protocol* të modelit OSI.
Megjithëse si TCP, ashtu edhe UDP kanë për detyrë të garantojnë transportën e datagrameve, brënda familjes së protokolleve TCP/IP, të dyja protokollet punojnë në një mënyrë shumë të ndryshme.

TCP

Transport Control Protocol dallohet ndaj UDP-së nga një rradhë karakteristikash komplekse, të

cilat nga njëra anë sigurojnë transportën e datagrameve, por nga ana tjetër ndikojnë dukshëm në rritjen e ngarkesës së protokollit (angl. protocol-overhead).
Për TCP-në, vecanërisht të rëndësishme janë karakteristikat e mëposhtme:

- ☑ Orientimi nga lidhja (connection oriented)
- ☑ Besueshmëria
- ☑ Fleksibiliteti në shfrytëzimin e gjerësisë së bandës

Aplikacionet që përdorin TCP-në janë:

- ❖ Web browsers
- ❖ E-mail
- ❖ Transferimi i file-ve

UDP

User Datagram Protocol, nga ana tjeter, eshte zhvilluar duke patur parasysh para se gjithash karakteristikat e meposhtme:

- ☑ Shpejtësia
- ☑ Ngarkesa më e vogël
- ☑ Heqja e kontrolleve të tepruara të transportat

Aplikacionet që përdorin UDP përfshijnë:

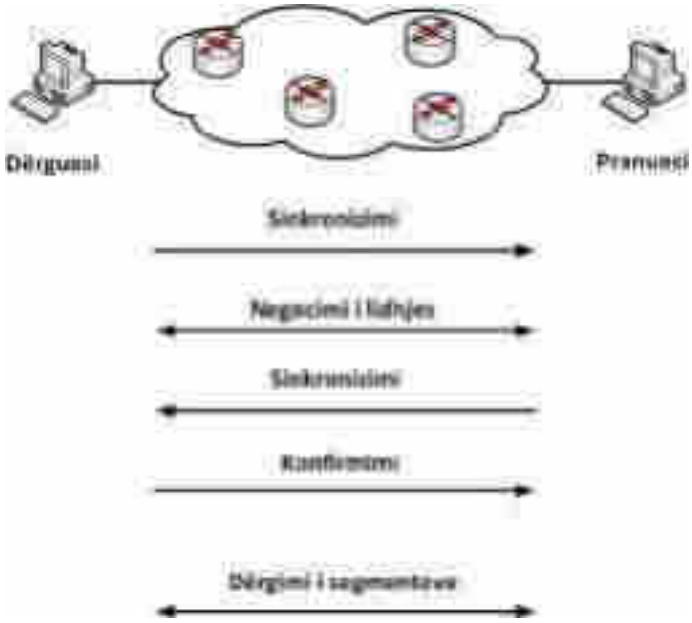
- ❖ Domain Name System (DNS)
- ❖ Video Streaming
- ❖ Voice over IP (VoIP)

Në shtresën e Transportat veprojnë dy protokolle, njëri është i besueshëm dhe i sigurt. Ky protokoll është TCP (*Transmission Control Protocol*). Protokolli i dytë është i thjeshtë, i shpejtë dhe nuk garanton dorëzimin e informacioneve ne destinacion. Ky protokoll është UDP (*User Datagram Protocol*).

TCP – është protokoll i shtresës së Transportat i cili në mënyrë të besueshme mundëson transmetimin e segmenteve me dupleks të plotë (*full-duplex*). Protokolli TCP i ndan të dhënat në segmente, në destinacion i ribashkon ato. Ndërsa në rastet kur ndonjë segment humbet gjatë transmetimit, i ridërgon ato që mungojnë.

Gjatë transmetimit të segmenteve në rrjet, shtresa e transportat çdo herë tenton të garantojë se të dhënat e transmetuara nuk do të humbasin. Humbja e të dhënave ndodh kur ato arrijnë më shpejt se sa hosti pranues është në gjendje t'i procesojë. Për të shmangur humbjen e të dhënave mekanizmi i kontrollit të qarkullimit i të dy hosteve cakton ritmin e transmetimit duke siguruar që hosti transmetues të mos e tejkalojë aftësinë pranuese, apo ta mbingarkojë memorien e hostit pranues.

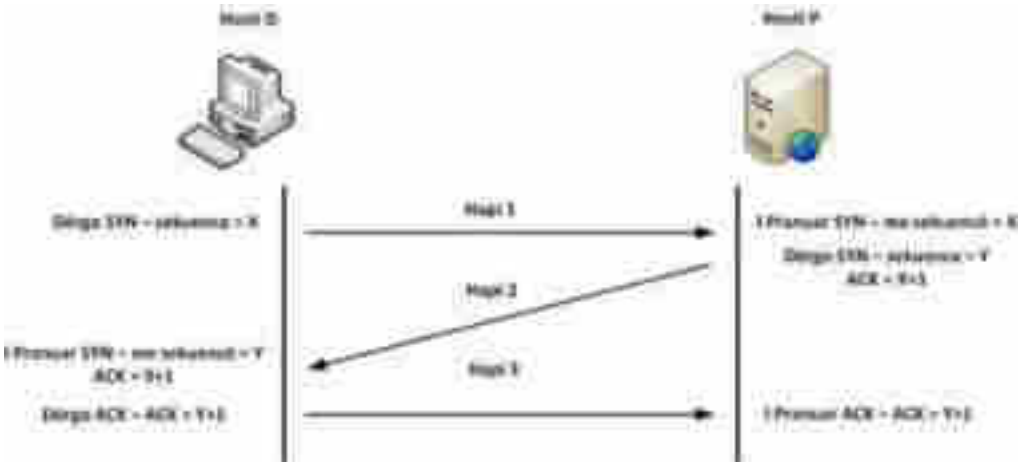
Për të filluar transmetimin e të dhënave, aplikacionet e kompjuterit iniciues dhe kompjuterit në destinacion e informojnë sistemin operativ se do të vendosin lidhjen e komunikimit. Modulet softuerike në të dy sistemet operative i shkëmbejnë mesazhet për të verifikuar se a është i autorizuar fillimi i transferimit si dhe a janë të gatshme të dy palët për komunikim.



Vendosja e lidhjes në mes të dy hosteve

Në figurë kemi paraqitur një shembull konkret të inicimit të lidhjes në mes të dy hosteve gjatë komunikimit direkt. Në hapin e parë hosti iniciues bën kërkesë për lidhje dhe sinkronizim. Në hapin e dytë hosti pranues konfirmon pranimin e kërkesës për sinkronizim si dhe sinkronizon parametrat në drejtimin e kundërt. Në hapin e tretë dërgohet segmenti i konfirmimit, i cili e informon iniciuesin se të dy palët janë pajtuar që lidhja është vendosur. Pasi është vendosur lidhja, fillon dërgimi i segmenteve. Pasi ka përfunduar transmetimi i segmenteve, hosti inicues i dërgon një sinjal hostit pranues, për përfundimin e transmetimit.

Vendosja e lidhjes trekahëshe (*three-way handshake*) në TCP realizohet duke sinkronizuar numrat sekuencialë të hostit dërgues dhe atij pranues sic tregohet në figurë



Vendosja e lidhjes trekahëshe

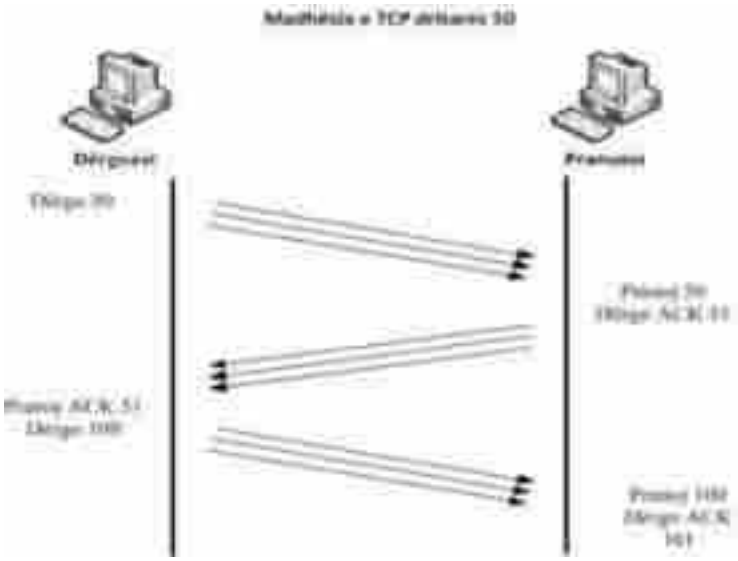
Vendosja e lidhjes trekahëshe bëhet në këtë mënyrë:

- Hapi i parë: Hosti dërgues, D, e inicon lidhjen duke ia dërguar segmentin sinkronizues SYN hostit pranues, P, me sekuencë inicuese INS = X.

- Hapi i dytë: Hosti P e pranon segmentin, e regjistron numrin sekuencial X dhe i përgjigjet me konfirmim ACK = X+1 dhe e inicon sekuencën INS=Y.

- Hapi i tretë: Hosti D e pranon segmentin e dërguar nga hosti P dhe i përgjigjet me segmentin konfirmues ACK = Y+1 për ta finalizuar procesin. Ky shkëmbim i segmenteve pra quhet procesi i vendosjes së lidhjes trekahëshe.

TCP si protokoll i besueshëm dhe i orientuar në ndërlidhje, lejon që disa segmente të transmetohen para se të marrë konfirmimin se janë pranuar nga destinacioni. Mekanizmi i cili i mundëson TCP-së që të transmetojë segmentet e të dhënave para se të marrë konfirmimin se ato kanë arritur në destinacion quhet mekanizmi i dritareve (*Window*). Madhësia e dritares transmetuese negociohet në mënyrë dinamike nga dy hostet komunikues për çdo sesion TCP. Varësisht nga kushtet transmetuese në rrjet madhësia e dritareve mund të rritet apo zvogëlohet. P.sh. me madhësinë e dritares 50, hosti mund të dërgojë 50 bajtë në drejtim të destinacionit para se të pranoj konfirmimin siç është paraqitur në figurë.



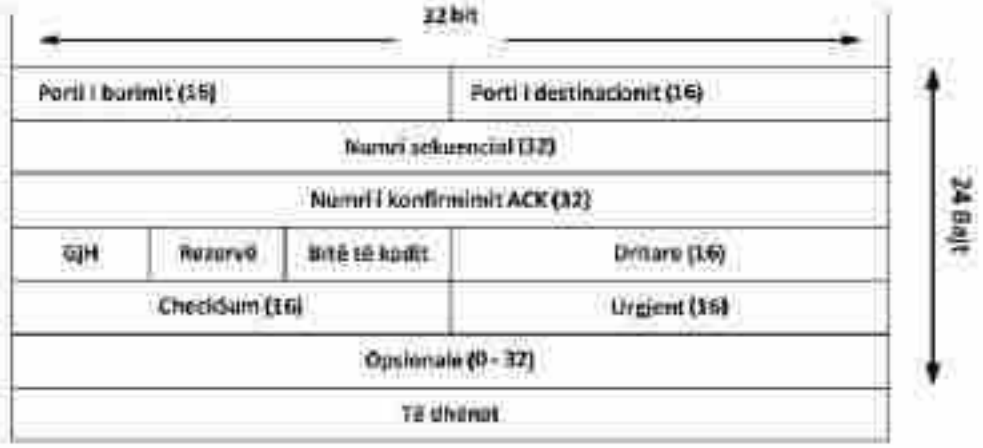
TCP mekanizmi i dritares

Nëse destinacioni i pranon të gjithë 50 bajtë, atëherë ia dërgon konfirmim (*Acknowledgment* ACK) hostit dërgues duke kërkuar që të transmetojë 50 bajtë shtesë. Nëse destinacioni nuk i ka pranuar 50 bajtët e transmetuar atëherë nuk dërgon konfirmimin.

Disa nga protokolle të shtresës së Aplikacionit që përdorin shërbimet e protokollit TCP janë:

- HTTP
- FTP
- SMTP
- DNS

Segmenti i protokollit TCP përbëhet nga dy pjesë, nga pjesa e hederit dhe nga pjesa e të dhënave. Në figurë janë paraqitur fushat e hederit të protokollit TCP që i shtohen çdo segmenti gjatë procesit të enkapsulimit.



Formati i segmentit TCP

Në vazhdim do të përshkruajmë fushat e segmentit TCP siç janë paraqitur në figurë:

- **Porta e burimit –** Numri i portes që dërgon të dhënat
- **Porta e destinacionit –** Numri i portes që pranon të dhënat
- **Numri sekuencial –** Numri i cili siguron se të dhënat kanë arritur sipas radhitjes
- **Numri i konfirmimit –** paraqet vlerën e oktetit të ardhshëm të TCP-së
- **Gjatësia e hederit –** Vlera e gjatësisë së hederit në segment
- **Rezervë** – Fusha e rezervuar e mbushur me zero
- **Bite të kodit –** Përgjegjës për funksione kontrolli, për vendosjen dhe terminimin e sesionit
- **Dritare –** Madhësia e dritares transmetuese
- **Checksum –** Vlera e kalkuluar për fushën e hederit dhe të dhënave
- **Urgjent –** Tregon fundin e të dhënave urgjente
- **Opsionale –** Fushë opsionale që definon madhësinë e TCP segmentit
- **Të dhënat –** Të dhënat nga protokollet e shtresave të larta

UDP – është protokoll i thjeshtë dhe i cili paraprakisht nuk vendos lidhje me destinacionin, por bën shkëmbimin e të dhënave pa garantuar se ato do të arrijnë në destinacion. Për të ritransmetuar të dhënat që nuk kanë arritur në destinacion protokolli UDP mbështetet në protokollet e shtresave më të larta.

Disa nga protokollet e shtresës së Aplikacionit që përdorin shërbimet e protokollit UDP janë: TFTP, SNMP, DHCP, DNS

Segmenti i protokollit UDP përbëhet nga dy pjesë, nga pjesa e hederit të segmentit dhe nga pjesa e të dhënave. Në figurë janë paraqitur fushat e hederit të protokollit UDP që i shtohen çdo segmenti gjatë procesit të enkapsulimit:

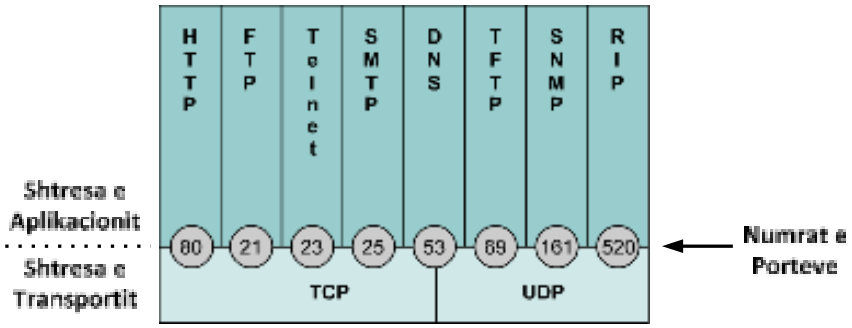
Formati i segmentit UDP

Në vazhdim janë përshkruar fushat e segmentit UDP:

- **Porta e burimit –** Numri i portes që dërgon të dhënat
- **Porta e destinacionit –** Numri i portes që pranon të dhënat

- **Gjatësia e hederit –** Vlera e gjatësisë së hederit në segment
- **Checksum –** Vlera e kalkuluar për fushën e hederit dhe të dhënave
- **Të dhënat –** Të dhënat nga protokollet e shtresave të larta

Të dy protokollet e shtresës së Transportat, protokolli TCP dhe UDP, për të shkëmbyer informacionet me protokollet e shtresës së Aplikacionit përdorin numrat e portave. Portat i shërbejnë këtyre protokolleve për të përcjellë komunikimet e shumëfishta që ndodhin në rrjet në të njëjtën kohë në mes të dy hosteve, pa shkaktuar konflikte midis komunikimeve të ndryshme.



Numrat e portave

Gjatë programimit të aplikacioneve, zhvilluesit softuerikë përdorin porta të definuara nga organizata IANA (*Internet Assigned Numbers Authority*). Numrat e portave janë të ndara në këto grupe:

- Portat e definuara marrin vlerat nga 0 – 1023
- Portat e regjistruara marrin vlerën nga 1024 – 49151
- Portat dinamike apo private 49152 – 65535

Hosti që inicion komunikimin përdor portat e caktuara për të zgjedhur aplikacionin përkatës. Gjatë inicimit të komunikimit porta e burimit të trafikut definohet në mënyrë dinamike dhe zakonisht merr vlerën numerike më të madhe se 1023, ndërsa si destinacion do të ketë porten e aplikacionit përkatës me të cilin dëshiron te vendos komunikimin si p.sh porta 80 apo 443 përfaqëson web shërbimin.

Tema 9. Protokollet *IPX/SPX*, ndërtimi dhe fusha e përdorimit të tyre

Fusha e përdorimit të IPX/SPX

Ashtu sikurse Microsoft doli me familjen e vet të protokolleve NetBEUI, e cila u mendua të përdorej në rrjetet e vogla dhe të mesme, edhe firma Novëll krijoi një familje protokollesh të vetën, e cila përshtatej me fushat speciale të përdorimit të sistemit opërativ NetWare.
Që në fillimet e viteve 80, Novell-i, si pasues i XNS (*Xerox Network System*) filloi të zhvillonte të ashtuquajturin NetWare-Suit si NOS (*Network Operating Sistem*). Si fushë përdorimi duhet të ishin lidhjet e rrjetëve të mëdha të routeushme LAN, pasi për mjedise të tilla rekomandohëj vecanërisht përdorimi i strukturës me përformancë të lartë të bazës së të dhënavë të Novell-it.

Shërbimet që duhet të ofroheshin ishin para së gjithash sigurimi aksesit në rrjet mbi skedarët, aplikimet në largësi (*remote applications*), si dhe akses mbi printerat e rrjetit dhe autentifikimi i përdoruesve në rrjet.
Novell-i pretendonte të ofronte një produkt dinamik dhe me përformancë të lartë, sic qe rasti me IP – në dhe DNS – në. Kostot administrative për administrimin e bazës së të dhënave për DNS – në i bëjnë këto sisteme, në rastet me gjerësi bande të kufizuara dhë në rrjetet lokale dinamike, shumë të papërshtatshme. Përmes teknikave të reja si NetBIOS dhe WINS, në bashkëpunim me DHCP, TCP/IP u bë një produkt konkurues në fushën e LAN – it.

Grupi i protokolleve NetWare

Tabela klasifikon protokollet e familjes NetWare sipas modelit ISO/OSI:

<table>
<tr><td>Shtresat në modelin OSI</td><td colspan="4">Netware – Protocols</td></tr>
<tr><td>Application Layer</td><td colspan="2">Applications</td><td rowspan="3">NCP</td><td rowspan="3">More</td></tr>
<tr><td>Presenation Layer</td><td rowspan="2">NetBIOS</td><td rowspan="2">NetWare Shell</td></tr>
<tr><td>Session Layer</td></tr>
<tr><td>Transport Layer</td><td>SPX</td><td colspan="3"></td></tr>
<tr><td>Network Layer</td><td colspan="4">IPX</td></tr>
<tr><td>Data Link Layer</td><td rowspan="2">Ethernet 802.2</td><td rowspan="2">Ethernet 802.3</td><td rowspan="2">Token Ring</td><td rowspan="2">etj.</td></tr>
<tr><td>Physical Layer</td></tr>
</table>

Shtresa e aplikacioneve

Në shtresën e aplikacioneve nga Netware mbështeten një sërë aplikacionesh të zakonshme rrjeti. Këto nga njëra anë mbështeten nga një version i përshtatur i NetBIOS over IPX/SPX – Emulation, dhe nga ana tjetër mbështeten nga NetWare – Shell.

Server Routines

Thirrjen e Server Routines në familjen e protokolleve NetWare e merr përsipër NPC, *Netware Control Protocol*. Ky protokoll është i krahasueshëm me *Server Message Blocks* të Microsoft-it. Për kërkesa të vecanta në rrjet mund të angazhohen edhe protokolle të tjëra. Kështu psh.: mbështeten formate skedarësh në shtresën e prezantimeve. Këtu duhen përmendur vetëm protokollet speciale të Netware.

Shtresa e transportat

Në shtresën e transporteve Netware përdoret *Sequenced Packet Exchange* (SPX). Ky është i krahasueshëm me protokollin TCP, që garanton transport të besueshëm dhe të orientuar nga lidhja e të dhënave. Në rast se kjo nuk nevojitët, ndryshe nga familja e protokolleve TCP/IP, e cila përdor një protokoll të llojit UDP. Netware përdor protokollin IPX për marrjen përsipër të së njëjtës detyrë.

Shtresa e rrjetit

Përbërsi qëndror i familjes së protokolleve Netware është protokolli *Internet – Exchange* (IPX). Në mënyrë të ngjashme si tek protokolli internetit IP, këtu mbikqyret transmetimi i paketave ndërmjet rrjetave. Transporta i paketave ndodh pa kontroll të transmetimit dhe lidhjes. Ndryshe nga IP, i ashtuquajturi protocol-over-head është më i vogël, gjë që përmirëson shfrytëzimin e gjerësisë së bandës në dispozicion. Ky përmirësim shihet vecanërisht qartë, në rast se në shtresën 4 nuk nevojitet transport i orientuar nga lidhja. Më pas IPX mund të marrë përsipër funksionet e UDP – së dhe të përdoret për transportën e paketave dhe transmetimin e të dhënave.

Shtresa pranë hardware-it

Netware mbështet një sërë protokollesh që punojnë në shtresën e dytë – *Data Link Layer*. Krahas proceseve të sotme si *Ethernet*, me versionet e tij të ndryshme, mbështeten edhe *Token Ring, FDDI* etj. Një domethënie të vecantë merr lloji i kapsulimit. Kështu për cdo kartë rrjeti duhet konfiguruar në mënyrë që të përcaktohet se cilës adresë rrjeti të kësaj karte i duhet caktuar, cili lloji frame-i. Klientët të cilët punojnë në një rrjet psh.: me *Netware 3.1* dhe Netware 4.x, si dhe që duhet të komunikojnë me të dy llojet e frame-ve, duhet të integrohen si me numrin e parë të rrjetit tek Ethernet II (802.2, versioni më i ri i llojit të frame-it) ashtu edhe me një numër të dytë tek 802.3. Kjo bën që në kuadrin e versionit 802.3, në vend të informacionit për tipin, të paraqitet një informacion për gjatësinë dhe nga ana tjetër kuadri nuk mund të ndryshohët.

Ndërtimi i adresës

Ndërtimi i adresës IPX në krahasim më adresat e IP-së është i thjeshtë. Një adrësë IPX ka dy pjësë përbërsë:

- Numri i rrjetit deri në 32 Bit në vlera hexadecimale
- Adresa e kompjuterit {knot address} = adresën MAC të kartës së rrjetit

Parimisht numri i rrjetit mund të marrë cdo vlerë nga 1 deri FF:FF:FF:FE. Ne këtë mënyrë disponohen më shumë rrjete se në të gjithë familjen TCP/IP. Për më tepër nëpërmjet dhënies së kufirit ndarës të adresës midis pjesës që tregon rrjetin dhe asaj që tregon hostet, nuk del më e nevojshme dhënia e subnetmaskës. Një adresë MAC është gjithmonë 48 Bit e gjatë. Edhe këtu garantohet uniciteti në mbarë botën, për sa kohë prodhuesit e kartave të rrjetit do të vazhdojnë të ndalen në specifikimin e dhënies së adresave MAC.

Një shembull për adresën IPX do të ishte:

1B:00:A0:24:5A:CE:3F

Ku 1B është numri i rrjetit (po të shprehej në formë decimale do të ishte 27), 00:A0:24 është kodi i prodhuesit (3Com), dhe 5A:CE:3F numri serial i kartës së rrjetit.

IPX/SPX – *Internetwork Packet Exchange/Sequenced Packet Exchange*. Është një protokoll rrjeti i përdorur në rrjetet *Novell (Netware)*. Është një protokoll rout-imi i cili përdoret si në rrjetet e vogla dhe në ato të mëdha. Punon në shtresën e network-ut.

Tema 10. Përbërësit aktivë të rrjetit (*hub*-et, *repeater*-at, *switch*-et)

Komponentët e rrjetit dhe funksionet e tyre

Nëse dëshirojmë të dimë se si është shtrirë një rrjet, do të vërejmë që mbrapa kompjuterave tanë është një kabëll i lidhur. Ky kabëll shkon nga kompjuteri ynë nëpërmjet kartës së rrjetit te një pajisje diku në dhomë *(switch)*. Nëse shkojmë deri te kjo pajisje, vërejmë që të gjithë kabllot që vijnë nga kompjuterat tanë përfundojnë në këtë pajisje *(switch)*, ku vetë kjo pajisje lidhet me një pajisje tjetër *(router)*.
Komponentët e parë të rëndësishëm të rrjetit janë pajisjet fundore (në rastin tonë, kompjuterat e nxënësve), që mund të jenë: kompjuter, printer, *smartfon*, *tablet* etj. Këto pajisje lidhen në rrjet me atë që quhet *karta e rrjetit.* Nga karta e rrjetit në kompjuterin tonë shtrihet një kabëll (media e transmetimit) deri te një *switch*. *Switch*-i lidhet me një pajisje, që quhet *router*.
Komponentët kryesorë të rrjetit janë:

- pajisjet fundore,
- *switch*-i,
- *router*-i,
- media e transmetimit,
- *Wireless Access Point,*
- *NIC (Network Interface Card).*
- etj

Pajisjet fundore

Në botë ka disa kompani që merren me prodhimin e pajisjeve të rrjetit, ku si lider mund të përmendim kompaninë CISCO, e cila ofron një gamë të gjerë të pajisjeve që kërkohen nga rrjetet më të avancuara sot. Ndër kompanitë e tjera që mund të përmendim, janë: *HP, Netgear, Alcatel* etj. Pajisjet fundore përfshijnë çdo pajisje që klientët përdorin për t'u bërë pjesë e rrjetit. Komunikimi në rrjet nga klientët kryhet me anë të këtyre pajisjeve, që mund të jenë: kompjuter, *smartfon*, *tablet*, IP, kamera, printer etj.

Përbërësit aktivë të rrjetit, nyjet 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. Referuar modelit

ISO/OSI, përbërësve aktivë u caktohen shtresat përkatëse në të cilat ato punojnë:

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

Hub-i

Simboli i hub-it

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. Hub-i punon në shtresën 1, referuar modelit OSI (Physical Layer). 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.

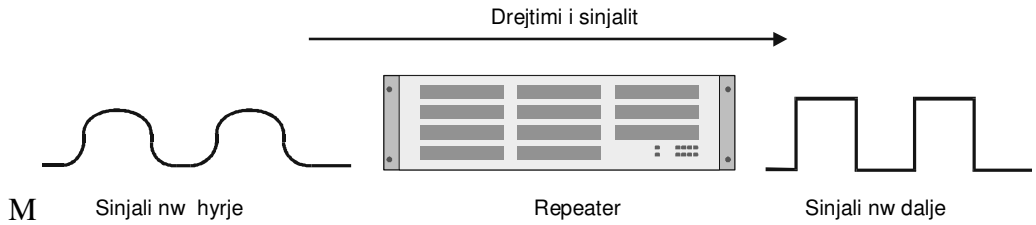
Përplasjet e vazhdueshme të paketave me të dhëna janë të pashmangshme. Si pasojë, koha e pritjes gjatë të cilës ndodh shkëmbimi i të dhënave në rrjet rritet. Sot hub-et janë zëvendësuar gjerësisht nga switch-et. Treguesit më të rëndësishëm janë: numri i portave, shpejtësia e komunikimit dhe mundësitë e zgjerimit të përbërësve (extention slots).

Ekzistojnë tri lloje të hubeve:

1. **Hubi pasiv** – i cili nuk përdor rrymën elektrike, por bën ndarjen e sinjalit për shumë shfrytëzues, duke mos e trajtuar sinjalin që kalon nëpër të.
2. **Hubi aktiv** – përdor rrymën elektrike për të rigjeneruar dhe forcuar sinjalin i cili kalon nëpër portat e tij.
3. **Hubi inteligjent –** gjithashtu përdor rrymën elektrike dhe posedon porten dhe konzolën nëpërmjet të cilit mund të programohet për të menaxhuar trafikun në rrjet.

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.



Rigjenerimi i sinjalit përmes një repeater-i

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*).

Simboli i switch-it

Switch

Switch grupon të gjitha pajisjet fundore, duke bërë të mundur komunikimin e tyre me anë të *MAC* adresave. *Switch* është lidhja e parë e pajisjes së klientit me rrjetin, për këtë arsye *switch*-et kanë përdorim të gjerë në rrjetet e sotme. Kemi disa lloje *switch*-esh të cilat dallojnë si nga funksioni, ashtu dhe nga kostoja.

Switch normal

(layer 2)

Switch-i normal është nga më të përdorshmit në ditët e sotme për arsye të kostos së ulët dhe është më i favorshëm për: kompani të vogla, zyra, shtëpi etj. Komunikimi ndodh me anë të *MAC* adresave.

Switch (layer 3)

Në shumicën e rasteve përdoret në pjesën kryesore të rrjetit dhe ka përdorim të gjerë në kompani të mesme ose të mëdha. Për arsye se kostoja e tyre është më e lartë se *switch*-et *layer 2*, nga vetitë që e dallojnë këtë *switch* është aftësia e komunikimit me anë të adresave *IP*.

Switch POE (Power Over Ethernet)

Me futjen e teknologjive *VOIP, IP camera* dhe shumë llojeve të tjera në kompanitë e sotme, lindi problemi se ku do ta merrnin këto pajisje energjinë elektrike, duke mos cenuar fleksibilitetin e secilës pajisje. Me zhvillimin e teknologjisë *POE (Power Over Ethernet),* një pajisje rrjeti e merr energjinë elektrike nga një *Switch POE* me anë të kabllit të rrjetit, pa pasur nevojë për prize ose diçka tjetër. Kjo lloj alternative e shton koston për çdo *switch,* për këtë arsye përdoret nga kompani të mesme dhe të mëdha.

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.

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

- ☑ Numri i portave
- ☑ I menaxhueshëm ose jo
- ☑ Standalone Switch
- ☑ Half-duplex- dhe/ose Full-duplex
- ☑ 10/100 Mbit ose 10/100/1000 Mbit
- ☑ Layer-2- ose Layer-3-Switch
- ☑ Mundëson VLAN (LAN-e virtuale)
- ☑ Kryen agregim portash

Tema 11. Përbërësit aktivë të rrjetit (*bridge*-t, *router*-at, *gateway*-t)

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.

- ☑ Tabela adresash statike
- ☑ Tabela adresash dinamike

Sipas fushës së përdorimit urat (bridges) ndahen në:

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

Ndërsa urat lokale lidhin me njëri tjetrin vetëm rrjete të të njëjtit tip, urat në largësi mund të çiftojnë dy rrjete nëpërmjet një lidhje WAN-i. Në ndryshim nga dy të parat, urat shumëportëshe janë në gjëndje të lidhin rrjete të llojeve të ndryshme.

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 transportat (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:

Simboli i router-it

- ☑ Router me një protokoll
- ☑ Router multiprotokoll
- ☑ Router hibrid

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

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

Ndërsa High Performance Router, Gigabit-Router dhe Enterprise-Router përdoren vetëm në rrjetet e mëdha, që kërkojnë performancë të lartë, *Access-Router* dhe *SoHo-Router* (SmallOffice, HomeOffice) janë konceptuar të përdoren në rrjete të madhësive mesatare. Me 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.).

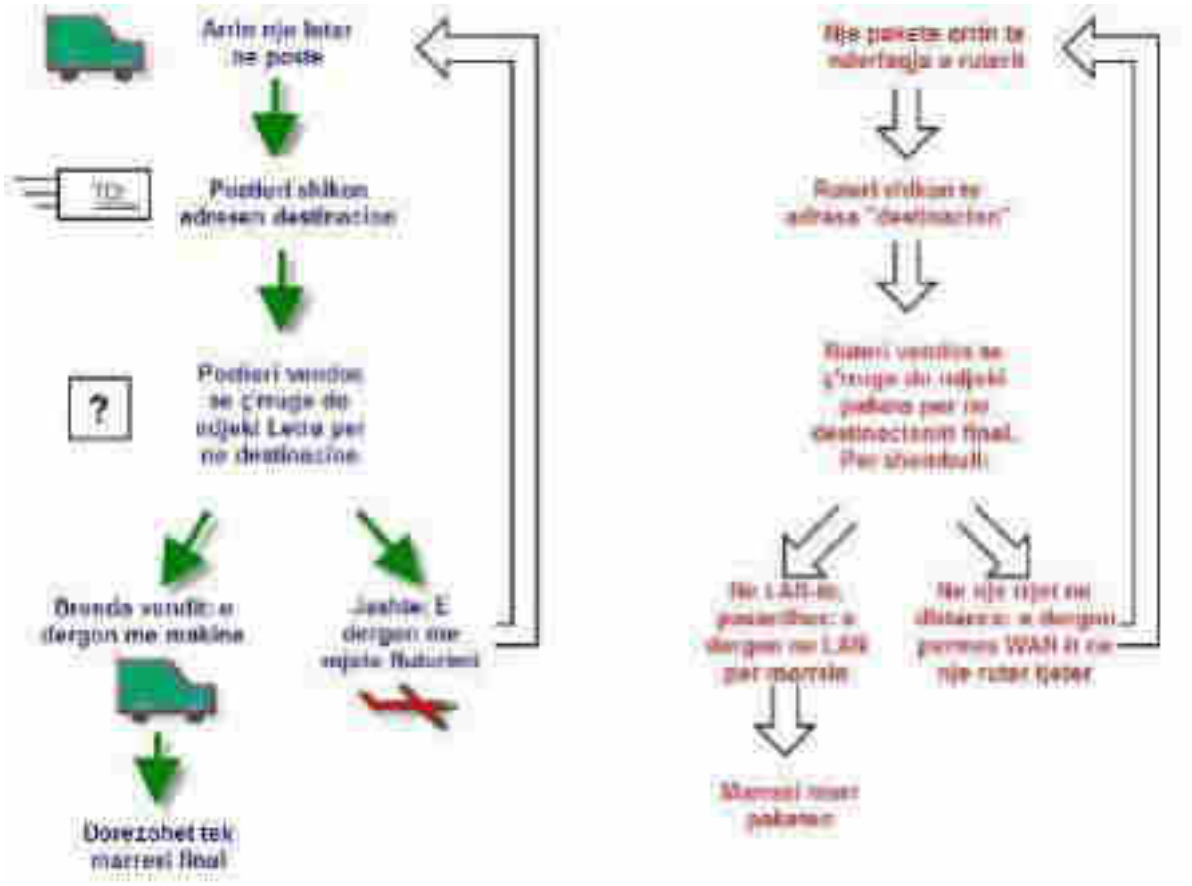
Router

Router-i është një pajisje rrjeti që bën lëvizjen e të dhënave (paketave) nga një rrjet në tjetrin. *Router*-at janë pajisje pa të cilat ne kurrë nuk do të mund të aksesonim *internetin*. Kur në kompjuterin tonë duam të aksesojmë internetin, është *router*-i ai që bën të mundur kalimin e informacionit nga rrjeti ynë personal në rrjetin e madh global, që quhet *internet*. Ndryshe nga *switch*-et, *router*-at janë vetëm *layer 3* dhe, ndryshe nga *switch*-et, që vendndodhjen në rrjet e kanë pranë pajisjeve fundore, *router*-at në shumicën e rasteve ndodhen në pjesët e kufirit të rrjetit tonë dhe shërbejnë si përfaqësues të rrjetit tone në kontakt me rrjetet e jashtme.

Routimi

Kjo pjese ekzaminon se si punon një router...

Ruterat punojnë në shtresat e networkut të modelit OSI. Funksionet kryesore të një ruteri janë, e para të gjeje rrugën më të mirë që çdo pakete I duhet të ndjekë për të shkuar në destinacionin e saj dhe e dyta të dërgojë paketat në rrugën e tyre. Kështu qe, puna e një ruteri i ngjan me shume një punonjëse të një poste. Ajo shikon në zonën e adresës së letrës (adresa e shtreses së Networkut në paketë), dikton se cilën rrugë do ndjekë letra (paketa), dhe pastaj dërgohet. Krahasimi midis postës dhe ruterit është ilustruar në figurë.



Një ruter vepron si një punonjes i një zyre postare

Ky diskutim mbi ruterin është lidhur me rolin tradicional të ruterit në rrjet, në shtresën e Networkut të modelit OSI. Ruterat tani sa vjen dhe po marrin funksione të tjera shtesë, për shembull, në fushën e QoS dhe sigurisë.

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.

Tema 12 Përbërësit aktivë të rrjetit (kartat e rrjetit, konvertuesit e mediave)

Përbërësit aktivë të rrjetit shërbejnë për të lidhur rrjetet kompjuterike me njëri 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.

Kartat e rrjetit

NIC (Network Inteface Card) është një hardware i cili bën të mundur lidhjen e një kompjuteri në rrjet. Karta e rrjetit është nje qark i vendosur në motherboard i cili siguron një lidhje të dedikuar të një kompjuteri në rrjet. Quhet ndryshe kontrollues i ndërfaqes së rrjetit, përshtatës rrjeti ose përshtatës LAN.

NIC lejon komunikimin nëpërmjet kabujve, si dhe komunikimin wireless.

NIC lejon komunikimin ndërmjet kompjuterave në një LAN, si dhe komunikimin në një rrjet më të gjerë nëpërmjet IP (Internet Protocoll).

Network Inteface Card është dy llojësh:

1. **Internal Network Card** – Karta e brendshme e rrjetit vendoset në slotin e posaçëm në motherboard, dhe lidhet në rrjet nëpërmjet kabllit Ethernet.

Intenal Network Card

2. **External Network Card** – Kartat e jashtme të rrjetit përdoren në ato pajisje që nuk kanë nje kartë rrjeti te brendshme. Kartat e jashtme janë dy llojëshe, USB dhe Wireless. Karta Wireless vendosen në motherboard dhe aksesohen në rrjet nëpërmjet sinjalit wireless.

External Network Card Wireless *External Network Card USB*

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 fibër optike. Një konvertues mediash ka dy ndërfaqe që varen nga standarti i kabllit, që do të përdoret në rrjetet lokale.

Tema 13 Protokollet e aplikacioneve dhe shërbimeve të rrjetit (HTTP, FTP, SNMP, SMTP, IMAP, POP, etj.).

Protokollet vendosin rregulla për shkëmbimin e të dhënave. Mund të përdoren shumë protokollet gjatë një komunikimi të vetëm.

HTTP (Hypertext Transfer Protocol) specifikon një protokoll kërkesë/përgjigje.

Kur një client, zakonisht një web browser, i dërgon një kërkesë një serveri, protokolli HTTP përcakton tipin e mesazhit që përdor client për t'ja kërkuar web page-t dhe gjithashtu tipin e mesazhit që përdor serveri që të përgjigjet.

Tre tipet e zakonshme të mesazheve janë:

1. GET: client kërkon të dhëna. Një web browser dërgon mesazhin GET për të kërkuar faqe nga një web server.
2. POST dhe PUT: përdoren për të dërguar mesazhe që ngarkojnë (upload) të dhëna në web server.

FTP (File Transfer Protocol) - u zhvillua për të lejuar transferimin e file-ve midis një client dhe një server-i. Një FTP client është një aplikacion që ekzekutohet në një kompjuter që përdoret për të ngarkuar dhe shkarkuar skedarë (to push and pull files) nga një server që ekzekuton FTP daemon (FTPd).

Client krijon lidhjen e parë me serverin në TCP në portën 21. Kjo lidhje përdoret për të kontrolluar trafikun, dhe konsiston në komanda të client dhe përgjigje të serverit.

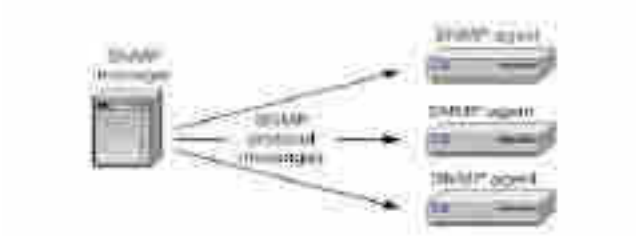
Client krijon lidhjen e dytë me serverin në TCP port 20. Kjo lidhje është për transferimin e file-ve dhe krijohet sa herë ka për të dërguar file.

Transferimi i file-ve bëhet në të dy drejtimet. Client mund të download (pull) një file nga serveri ose të upload (push) një file në server.

SNMP **(Simple Network Management Protocol) është protokoll i shtresës së aplikacionit i cili merret me menaxhimin e pajisjeve të rrjetit. Ky protokoll mbledh informacionin e vlefshëm të rrjetit nga switch-et, router-at, server-at, printerat dhe pajisjet e tjera të lidhura në rrjet.**

Një rrjet i menaxhuar nga SNMP përbëhet nga dy komponentë:

1. **SNMP Manager ose ndryshe Sistemi i menaxhimit të rrjetit (NMS), është një software I cili instalohet në kompjuterin e administratorit të rrjetit, për të monitoruar rrjetin.**
2. **SNMP Agent është nje software i cili ekzekutohet në pajisjen që duam të monitorojmë (p.sh router, switch, server etj.)**



SMTP (Simple Mail Transfer Protocol) ,POP(Post Office Protocol) dhe IMAP (Internet Message Access Protocol) përfshihen në shërbimet email.
Për të dërguar mesazhe email si nga një client ose një server përdoren formati i mesazheve dhe command strings të përcaktuara nga protokolli SMTP.
SMTP – protokoll dalës

- Server⇨ Client
- Server⇨ Server

POP – protokoll hyrës

- Client⇨ Server

IMAP (Internet Message Access Protocol) protokolli IMAP përdoret nga aplikacioni i e-Postës për të tërhequr e-Postat nga serveri duke i lënë kopjet e e-Postave edhe në server.

Tema 14 Protokollet e komunikimit. Protokollet në LAN, WAN dhe në kufinjtë mes tyre. Shërbimet e rezolucionit të emrit.

Protokollet e komunikimit
Fakti që ky material është i shkruar në gjuhën shqipe tregon që i dedikohet lexuesit shqipfolës. Atëherë, nga kjo kuptojmë që për tu realizuar komunikimi në mes të dy individëve paraprakisht kërkohet që të përmbushet kriteri i njohjes së gjuhës së komunikimit nga të dy palët. Po kështu, edhe në botën e rrjeteve kompjuterike sa herë që dy kompjuter kërkohet të komunikojnë në mes tyre, ata paraprakisht duhet të dakordohen për protokollin e komunikimit. Mu për këtë arsye, sistemet operative të sotme përkrahin më shumë se një protokoll për të komunikuar e të cilat quhen pako të protokolleve. Disa nga pakot e protokolleve më të njohura në historinë e rrjeteve kompjuterike janë: IPX/SPX i Novell, X.25 i ITU, AppleTalk i Apple dhe TCP/IP. Meqë më e përdorura nga këta pako që u përmendën është pako e protokollit të TCP/IP, atëherë në vijim do të përmendim disa nga protokollet më të njohura që e përbëjnë pakon e protokollit TCP/IP.

- **protokolli i internetit (IP)** – është protokoll pa-lidhje-të-orientuara që ka për detyrë të bartë paketat nga kompjuteri në burim deri te kompjuteri në destinacion
- **protokolli i kontrollit të transmetimit (TCP)** – është protokoll i orientuar-në-lidhje që ofron transport të besueshëm, të rregullt dhe të kontrolluar për gabime në transmetim
- **protokolli i datagramit të përdoruesit (UDP) –** është protokoll pa-lidhje-të-orientuara që bën të kundërtën e punës së protokollit TCP duke mos ofruar transport të besueshëm, rregullt dhe të kontrolluar për gabime në transmetim
- **protokolli i kontrollit të mesazhit në Internet (ICMP) –** është protokoll që përdoret nga pajisjet aktive të rrjetit për të dërguar mesazhe gabimi ashtu që të përcaktoj disponueshmërinë e shërbimit apo të pajisjes në destinacion

- **protokolli i transferimit të hipertekstit (HTTP)** – është protokoll që përdoret nga shfletuesi dhe që funksionon në principin kërkesë-përgjigje e hipertekstit të përbërë nga HTML dhe elementet shoqëruese në arkitekturën klient-server
- **protokolli i zyrës postare (POP)** – është protokoll që përdoret nga aplikacioni i e-Postës për të tërhequr e-Postat nga server
- **protokolli i transferimit të skedarëve (FTP)** – është protokoll i ndërtuar mbi arkitekturën klient-server dhe përdor lidhjet e veçanta të kontrollit dhe të dhënave në mes të klientit dhe serverit
- **protokolli i qasjes së mesazhit në Internet (IMAP)** – si edhe protokolli POP, protokolli IMAP përdoret nga aplikacioni i e-Postës për të tërhequr e-Postat nga serveri duke i lënë kopjet e e-Postave edhe në server

Tema 15 Teknikat e transmetimit pa kabëll. WAN dhe WLAN. Instalimi dhe testimi i tyre.

Tek rrjetet pa kabël bëhet fjalë për rrjete, në të cilat në vend të mediave tradiocionale, prej bakri apo fibrash optike, transmetimi i sinjaleve bëhet nëpermjet valëve të radios.

Avantazhet e përdorimit të WLAN:

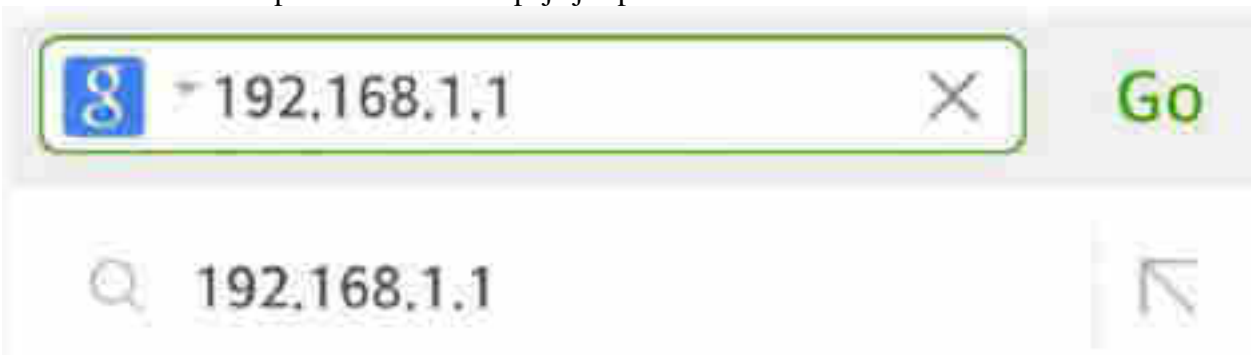
- Brënda rrezes së mbulimit me sinjal, aksesi në rrje mund të bëhet kudo, i pakushtëzuar nga gjatësia e kabllit apo vendodhja e prizes së rrjetit.
- Për rrjetëzim nuk duhen parashikuar ndryshime në elementët e ndrërtimit.
- Teknologji fleksibël për zgjerim të metejshëm.

Këto përparësi kanë çuar ne një rritje të shpejtë të preferencave për zgjidhjet që ofron WLAN-i. Kjo vlen sidomos për përdorimin e WLAN-it për lidhjen e kompjutera-ve portabël në rrjetet ekzistuese, ose për akses në internet.

Krahas përparësive, përdorimi I WAN-ve sjell me vete edhe një sërë problemesh, të cilat nuk hasen në procesin e transmetimit në rrjetet me kabëll:

- Interferencë e lartë.
- Siguri e ulët.
- Shpejtësi më e ulët transmetimi.

Krijimi i një rrjeti wireless realizohet duke kaluar në disa hapa:
Hapi 1: Bëhet lidhja e routerit wireless me kompjuterin (porta LAN). Bëhet lidhja e routerit wireless me modemin e ofruesit të shërbimit të internetit (porta WAN).
Hapi 2: Ndizet kompjuteri, modemi dhe routeri wireless.
Hapi 3: Ne një browser që ndodhet në komjuter (Internet explorer, Mozilla. Google Chrome), shkruani IP adressen për menaxhimin e pajisjes p.sh 192.168.1.1.



Hapi 4: Vendos username-in dhe fjalëkalimin e administratorit.

Hapi 5: Aplikoni sigurinë tek "wireless scurity" (WPA, WPA2, AES)

Hapi 6: Ndryshoni emrin e wireless-it (SSID).
Hapi 7: Mbaroni instalimin - Finish
Testimi i rrjetit WLAN realizohet duke u lidhur në rrjetin e krijuar, në SSID e vendosu me password-in përkatës.

Tema 16 Transmetimi i të dhënave me radiovalë, Bluetooth dhe lazer.

Përpos rrjetave me tela (kabllo), ekzistojnë teknologji të ndryshme të cilat mundësojnë transmetimin e informacioneve ndërmjet paisjeve të rrjetit pa kabllo (tela). Këto teknologji njihen si teknologji ajrore (wireless). Teknologjitë ajror përdorin valët elektromagnetike për bartjen e informacioneve në mes të paisjeve. Këto valë elektromagnetike janë të ngjashme me valët që bartin radio sinjalet nëpër ajr. Spektri elektromagnetik përfshinë brezet valor për transmetim të radio sinjaleve, TV sinjaleve, rrezet X dhe rrezet gamma , pastaj dritën e dukshme (që e shofim), etj. Secila prej tyre që përmendëm përdor brezin e veqantë (specifik) të valëve elektromagnetike.

Karakteristikat e valëve elektromagnetike për bartje të sinjaleve mund të përmblidhen:

- Disa tipe të valëve elektromagnetike nuk janë të përshtatshme për bartje të sinjaleve.
- Disa pjesë tjera të spektrit të këtyre valëve administrohen nga qeveritë dhe u ipen organizatave në ndryshme për aplikime specifike.
- Pjesë të caktuara të këtij spektri janë ndarë për përdorim publik pa pasur nevojë për ndonjë leje ose licencë. Pjesa më e madhe e këtyre valëve "publike", përfshijnë valet Infra të kuqe dhe një pjesë të valëve radio frekuencore.

Radio valët - mund të depertojnë nëpër mure dhe pengesa tjera, duke mundësuar shtrirje më të madhe se sa rrezet IR. Breze të caktuara të valëve RF janë lënë për përdorim nga paisje të pa licensuara, sikur: LAN-at ajror (wireless LAN), telefonat ajror (Cordless phones). Brezet që përdoren për këto qëllime janë në frekuencat: 900 MHz, 2.4 GHz, dhe 5 GHz.

Rrezet Infra të kuqe (IR – Infra red) - Rrezet infra te kuqe (IR) kanë relativisht energji të vogël dhe nuk mund ti depertojnë muret ose pengesat tjera. Ato zakonisht përdoren për lidhje dhe bartje të të dhënave ndërmjet paisjeve kompjuterike manuale (PDA –Personal Digital Assistant) dhe kompjuterëve (PC). Zakonisht valët IR mundësojnë lidhjen një më një (one - to – one). Rrezet IR, gjithashtu përdoren për lidhje të njësive të ndryshme të PC-së me te, sikur Mausi ajror, tastiera etj. Pra përgjithësisht rrezet IR përdoren për distanca të vogla komunikimi dhe kur paisjet "shihen" ndër veti. (Është e mundur që të rritet distanca, dhe rrezet IR edhe të reflektohen nga objekete – për këtë nevojiten frekueca më të larta të valëve elektromagnetike).

Bluetooth-i Është teknologji që shfrytëzon brezin në 2.4 GHz. Ai është i kufizuar në shpejtësi të vogla, në shtrirje (distanca) të shkurtëra, por që ka përparësinë e komunikimit me më shumë paisje në të njejtën kohë. Ky komunikim një-me-shumë e ka bërë teknologjinë Bluetooth metodë më të preferuar se sa ajo e lidhjes me rreze IR p.sh. për lidhje të mousit, tastierës dhe printerit në të njejtën kohë! Teknolgjitë tjera të cilat shfrytëzojnë përdorimin e brezeve në frekuencat: 2.4GHz dhe 5GHz, janë rrjetat lokale ajror (wireless LAN) sipas standardeve të ndryshme 802.11 të IËE –së. Për dallim nga teknologjia Bluetooth, teknologjitë e rrjetave LAN, transmetojnë sinjale të fuqisë më të madhe dhe arrijnë distanca më të mëdha të komunikimit.

Lazer - Komunikimi me lazer siguron një zgjidhje me kosto efektive për problemin e komunikimit të besueshëm dhe me shpejtësi të lartë me rreze të shkurtër (1.2 km) që mund të lindë gjatë lidhjes së sistemeve telekomunikuese të ndërtesave të ndryshme.

Komunikimi me lazer, lejon lidhjet pikë-pikë për pikë me shkallët e transferimit të informacionit deri në 155 Mbit / s. Në rrjetet kompjuterike dhe telefonike, komunikimi me lazer siguron shkëmbimin e informacionit në modalitetin e plotë të dyfishit. Për aplikacionet që nuk kërkojnë një shkallë të lartë transmetimi (për shembull, për transmetimin e sinjaleve video dhe sinjaleve të kontrollit në sistemet e televizionit teknologjik dhe të sigurisë), është në dispozicion një zgjidhje e veçantë me kosto efektive me komunikim gjysmë dupleks.

Tema 17 Siguria në LAN, WAN dhe WLAN. Standartet në fushën e sigurisë së të dhënave.
Siguria në rrjetet kompjuterike ka të bëjë me moslejimin e aksesimit të të dhënave nga persona të pautorizuar.
Disa nga mënyrat për të rritur nivelin e sigurisë ne rrjetet kompjuterike janë:

1. Përdorimi i një router që ka të aktivizuar nje Firewal.
2. Përdorimi i enkriptimit WPA2 ne WLAN.
3. Sigurimi fizik i pajisjeve të rrjetit.
4. Çaktivizimi I portave të papërdorura të router-it.
5. Filtrimi i Mac Adresave.

Teknologjia Spread Spectrum, e përdorur ne WLAN, garanton shkallë të lartë sigurie. Përveq kësaj shumë pajisje Wireless kanë të integruar opsionin për enkriptim.

Standartet në fushën e sigurisë të të dhënave

Me qëllim që të zvogëlohen koha dhe kostot e punës për sigurinë, si dhe që të mund të krahasohen më mire përpjekjet për rritjen e sigurisë, në praktikë përdoren shpesh katalogje me kritere, të vilat mbështesin në punën e tyre personat përgjegjës për sigurinë.
Më poshtë jepen disa standarte në fushën e sigurisë:

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

Tema 18 Funksionet administrative të routera-ve dhe switch-eve.
Router dhe switch-at janë pajisje të rrjetit kompjuterik, që bëjnë të mundur lidhjen e 2 ose më shumë kompjuterave me njëri-tjetrin, pajisje të tjera në rrjet ose rrjetat me njëri tjetrin.

Router:

- Router-i operon në shtresën Network në modelin OSI.
- Router përdoret për te lidhur LAN dhe WAN.
- Router tranferon të dhënat në formën e paketave.
- Router bën leximin e adresave IP te pajisjeve në rrjet.
- Router perdor tabelen e ruterit per transferimin e të dhënave.
- Përdor IP address.

Switch:

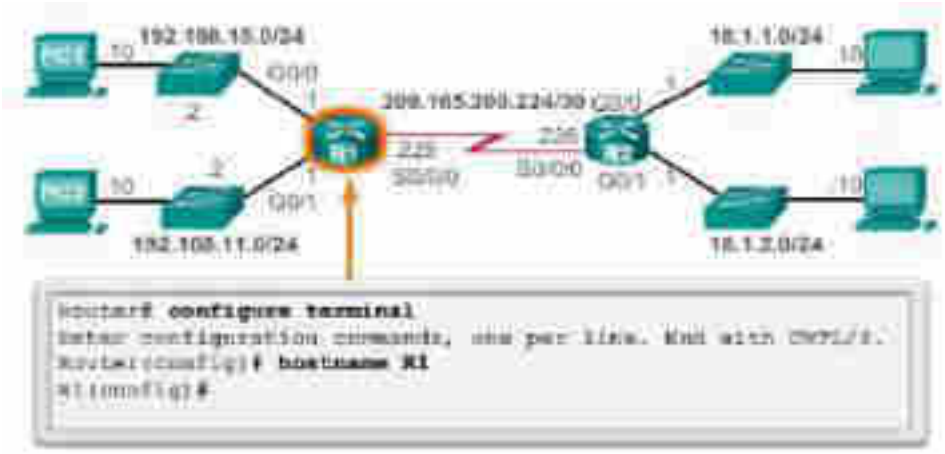
- Switch-I operon në shtresën DataLink në modelin OSI.
- Switch është një bridge me shume porta. 24-48 ports.
- Switch është një pajisje e rrjetës kompjuterike që përdoret për të lidhur shumë pajisje së bashku në një rrjet kompjuterik.
- Përdor Mac Address.

Tema 19 Ndërfaqja e përdoruesit dhe ndërfaqja e komandave të një router-i CISCO.
Ndërfaqja e përdoruesit ne një Router Cisco, ka disa nivele konfigurimi. Çdo nivel konfigurimi ka një grup të caktuar komandash.
Gjatë konfigurimit të një router-i Cisco do të hasim nivelet e mëposhtme të konfigurimit:
User EXEC mode - Login për të hyrë në server.
Komanda: *Router>?*

Shembull: *Router> enable*

Privileged EXEC mode – vendosen parametra në një set komandash të cilat ndalojnë aksesin e personave të paautorizuar. Gjithashti Privileged EXEC mode, përfshin komanda të një niveli të lartë të testimit, të tilla si korrigjimi i gabimeve.
Global configuration mode – Për të bërë konfigurimin në nivel global, duhet që ne rradhë te parë të aksesojmë Privileged EXEC mode. Në këtë nivel bejmë të mundur vendosjen e një emri dhe password-i për Router-in.
Komanda: *nnnnconfigure {terminal|_memory|_network}*
<CR>
Shembull: *Router# configure*
Router (config) # hostname

Emërtimi i pajisjes



Interface configuration – Bëhet konfigurimi në nivel ndërfaqje, duke përcaktuar llojin dhe numrin e ndërfaqes.
Komanda: interface *Lloji i ndërfaqes Numri i ndërfaqes*
Shembull: *interface serial 0*
Subinterface Configuration Mode – Bëhet konfigurimi i disa ndërfaqe-ve virtual ne një ndërfaqe fizike.
Line Configuration Mode – konfiguron një linjë ndihmëse, terminal virtual ose linjë tty.
Komanda: *line [aux | console | tty | vty] line-number [ending-line-number]*
Shembull: *line tty 7*
Router Configuration Mode - konfigurojnë një protokoll routimi dhe gjithmonë përdorin komandat router.
Komanda: *Router (config)# router (protokoll)*
Shembull: *Router (config)# router RIP*

Tema 20 Procesi i routimit. Routimi statik, dinamik dhe default.

Procesi i routimit është procesi i gjetjes së rrugës që duhet të bëje paketa nga Hosti burim deri ne Hostin destinacion.

Një router mund të mësojë rreth rrjeteve të largëta në një nga dy mënyrat:

1. Manualisht: Rrjetet në distancë futen manualisht në tabelën e rutimit duke përdorur routimin static.

2. Dinamikisht: Rrjetet në distance mësohen automatikisht duke përdorur një protokoll dinamik të drejtimit.

Routimi statik – një administrator rrjeti duhet të konfigurojë në mënyrë manuale një rrugë statike për të arritur një rrjet specifik. Rrugët statike nuk ndryshohen automatikisht, por duhet të ndryshohen nga administratori sa here që ndryshohet topologjia e rrjetit.

Routimi statik ofron disa avantazhe mbi drejtimin dinamik, duke përfshirë:

- Routimet statike nuk reklamohen në rrjet, duke rezultuar në siguri më të lartë.
- Routimet statike përdorin më pak bandwidth sesa protokollet dinamike të drejtimit, nuk përdoren cikle të CPU për të llogaritur dhe komunikuar.

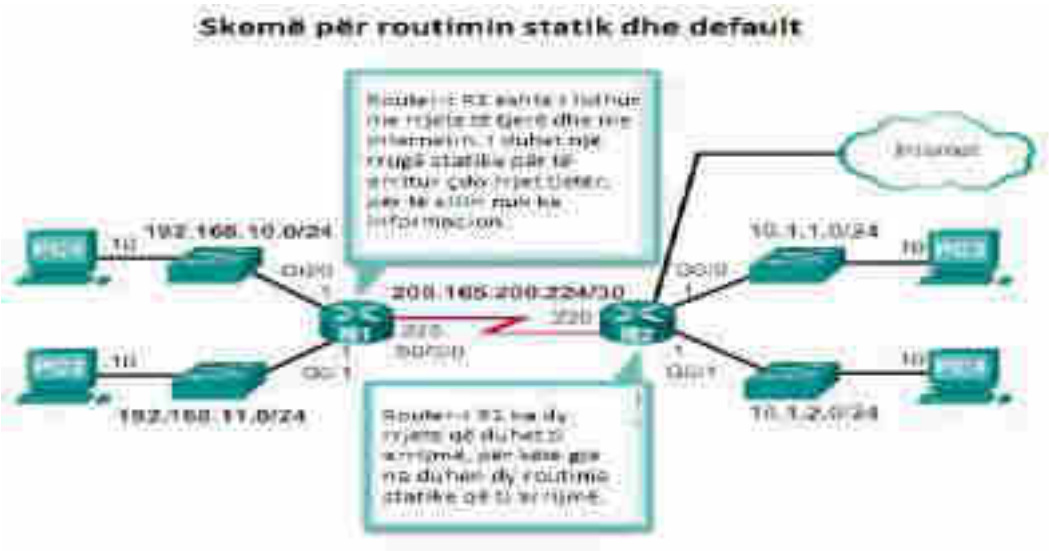
Aplikimet statike të routimit

Routimet statike përdoren:

- Për tu lidhur me një rrjet të caktuar.
- Për të ulur numrin e rrugëve të reklamuara duke përmbledhur disa rrjete të afërta si një rrugë statike.
- Për të krijuar një rrugë rezewrvë në rast se lidhja kryesore e rrugës dështon.

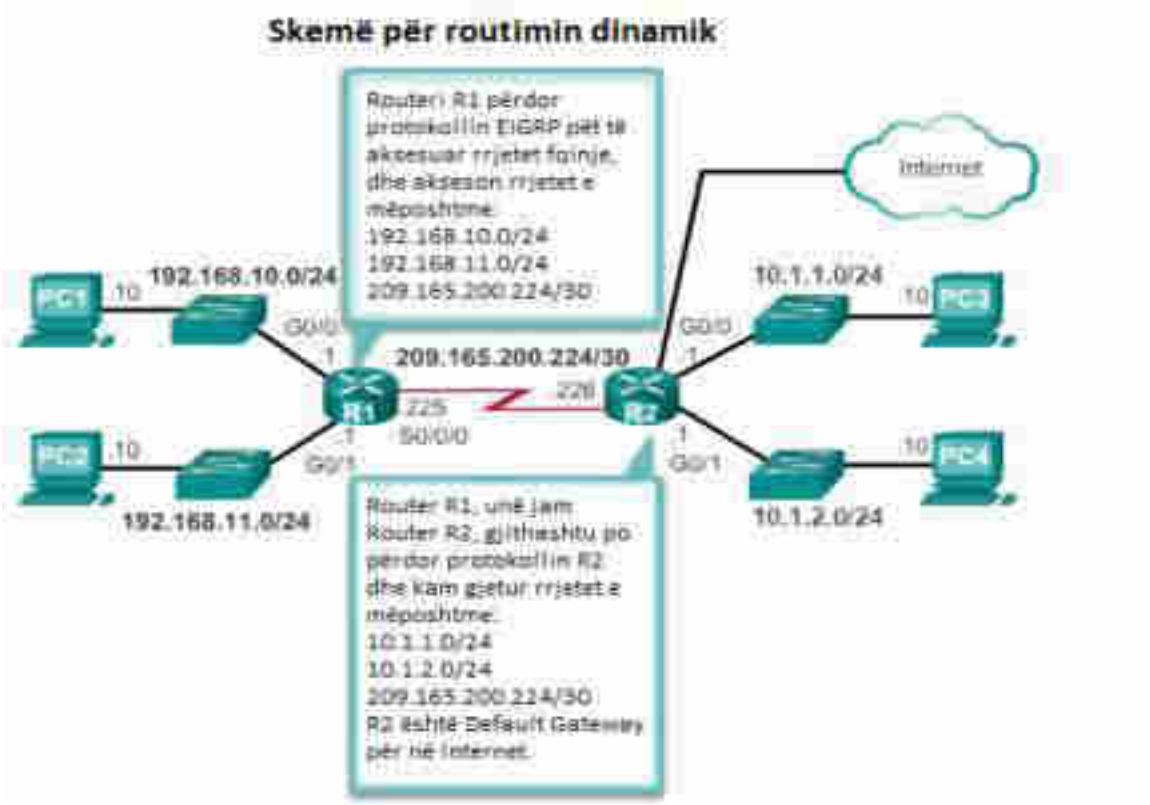
Routimi statik default

- Një routim statik default është një rutim që përputhet me të gjitha paketat.
- Një routim default identifikon adresën IP të gateway në të cilën router dërgon të gjitha paketat IP se nuk ka një rrugë të mësuar ose statike.
- Një routim statike default është thjesht një rrugë statike me 0.0.0.0/0 si adresa e destinacionit IPv4.

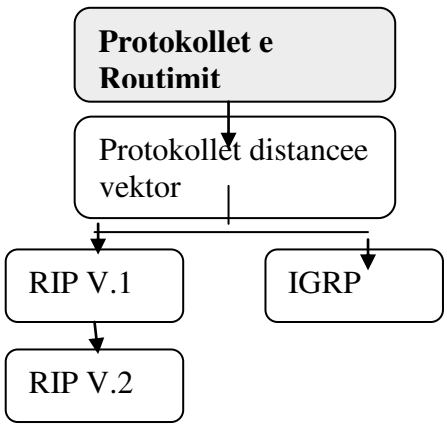


Routimi dinamik

- Ndryshon në mënyrë automatike ndryshimet që ndodhin në topologjinë e rrjetit.
- Routerat e mësojnë rrugën për te destinacioni nëpërmjet update-ve të rregullta nga router-at e tjerë.



Tema 21: Bazat e protokolleve të routimit. Routing Information Protocol (RIP) dhe Interior Gateway Routing Protocol (IGRP).



RIP është protokolli më i përdorur në rrjete të vogla, që do të thotë deri ne 20 rrejte të lidhura. RIP është një distance vector Routing Protocol dhe përdor Hop Count si njësi matëse. Routing updates bëhen çdo 30 sekonda dhe aplikohen në topologjinë e rrjetit në rast ndryshimesh. Kur një router merr një router update, që përmban ndryshime në informacionet e deritanishme, atëhere routing table sillet në gjendje të re. Protokolli RIP bën të mundur gjetjen e rrugës mët e shkurtër nga burimi deri në destinacion. Ky protokoll i përket shtresës së Aplikacionit dhe përdor UDP Port 520.

RIP parandalon “loops” të vazhdueshëm të dergimit të paketave nëpër rrjet, përmes kufizimit të numrit te hopeve, max 15. Në rast se routëri përmban një routing update me numër mbi 15 dhe destinacioni ndërkohë nuk është arritur akoma, atëherë ky i fundit konsiderohet si i paarritshëm.
RIP është në dy versione:
RIP v1 –Classful Routing Protocol
RIP v2 – Classless Routing Protocol

Krahasimi mes RIP v.1 dhe RIP v.2

RIP v.1	**RIP v.2**
Mbështet vetëm “Classful” Routing Protocol	Mbështetet vetën “Classless” Routing Protocol
Routing-Update nuk përmban informacion nënrrjeti.	Routing-Update nuk përmban Subnet Mask Information me Update.
Nuk mbështet Prefix-Routing, të gjithë njësitë në rrjet duhet të përdorin të njëjten Subnet Mask.	Mbështet Prefix-Routing, nënrrjete të ndryshme Brënda të njëjtit rrjet mund të përdorin Subnet Mask të ndryshme.
Update nuk përmban autentifikim.	Update mund të përmbajë autentifikim.
Updates dërgohen në Broadcast 255.255.255.255.	Updates dërgohen me Multicast Address 224.0.0.9 Class D, efikasitet më të mire.

Algoritmi i përditësimit të RIP

1. Shto nga 1 hop në numërimin e hop për çdo destinacion të ri të lajmëruar
2. Përsërit hapat vijues për çdo destinacion të lajmëruar 30
   If (Destinacioni nuk është në tabelën e rrugëtimit)
   Shto informacionin e lajmëruar në tabelë
   Else
   If (Fusha e hapit të ardhshëm është e njejtë)
   Zëvendëso shënimin në tabelë me një të lajmëruar
   Else
   If (numri i hapave të reklamuar është më i vogël se ai në tabelë)
3. Zëvendëso shënimin në tabelën e rrugëtimit return

Interior Gateway Routing Protocol (IGRP) është distancë vector, i cili është krijuar ne mes të viteve 1980 nga CISCO.
IGRP është një IGP e ndërtuar nga CISCO, i cili përdor distancë vector për rrugëzimin si në rastin e protokollit RIP. IGRP vendos në IP protokollin nr 9.
Me anë të Update transportohet metrika dhe numri i rrjetit. Metrika përdor rregullisht Bandwith-in, vonesat në rrjet, besueshmërinë dhe ngarkesën për të zgjedhur rrugën. Parametra të tjerë shtesë janë madhësia e Maximal Transfer Unit MTU. Vonesat dhe Bandwith-i nuk maten por mund të përdoren si parametra të interface-it.
IGRP-ja nuk transporton Subnet Mask-ën si “classful” Routing Protocol në Update-t në rrjet. Një router dërgon çdo 30 sek një Routing Update. Kur Brënda tre cikleve të Update-ve nuk merret informacion i ri, kjo rrugë nuk është e vlefshme, domethënë përshkruhet si rrugë që nuk mund të përdoret. Pas shtatë cikleve të Update-ve kjo rrugë fshihet fare nga tabela e routerit.

Tema 22. Konfigurimi i nje adrese IP dhe verifikimi i tij. Komandat baze.

Hapat	Komadat ose veprimet	Qellimi
Hapi 1	enable Per shembull: Router> enable	aktivizon “privileged EXEC mode”

Hapi 2	kofigurimi i terminalit Per shembull: Router# configure terminal	hyrje ne modalitetin global configuration
Hapi 3	nderfaqesi shkruajm numrin Per shembull: Router (config) # interface fastethernet 0/0	specifikon nje nderfaqe dhe hyn ne nderfaqen e konfigurimit
Hapi 4	no shutdown Per shembull: Router (config-if) # no shutdown	aktivizon nderfaqen
Hapi 5	adresa IP ip-address mask Per shembull: Router (config-if) # ip address 172.16.16.1 255.255.240.0	konfigurimi i adreses IP
Hapi 6	fund Per shembull: Router(config-if) # end	dalje nga modaliteti i konfigurimit dhe kthimi tek "privileged EXEC mode"

```
! interface FastEthernet0/0
no shutdown
ip address 172.16.16.1 255.255.240.0
!
interface FastEthernet 0/1
no shutdown
ip address 172.16.32.1  255.255.240.0
!
interface FastEthernet 0/2
no shutdown
ip address 172.16.48.1 255.255.240.0
!
```

Komandat e meposhtme mundesojne testimin e adreses IP

- Ping – teston lidhjen
- Traceroute/tracert – jep informacion mbi paisjet qe ndodhen ne rrjet si dhe jep informacion mbi shtetin ose vendin ku ndodhet rrjeti
- Ipconfig/ifconfig – (Windows/Linux) kur duam te dim adresen IP te hostit ku po punojme
- Nslookup – lokalizimi i adreses IP te lidhur me nje emer domain-i dhe verifikimi i merit te domain-it.
- show ip interface – shfaq parametrat e IP per nderfaqen
- show ip route connected – shfaq IP e rrjetit dhe paisjen e rrjetit ku eshte e lidhur

Tema 23. Sekuencat e boot-imit te router-it. Sigurimi dhe rikthimi ne pune i CISCO IOS.

Nëse dëshironi që pajisjet të jenë në gjendje të dërgojnë dhe marrin të dhëna jashtë rrjetit tuaj, do t'ju duhet të konfiguroni router-at.

Router-at Cisco dhe switch-et Cisco kanë shumë ngjashmëri. Ata suportojne një sistem operativ modal të ngjashëm, struktura të ngjashme komanduese dhe shumë komanda të njëjta. Përveç kësaj, të dy pajisjet kanë hapa të ngjashëm fillestarë të konfigurimit. Për shembull, detyrat e

mëposhtme të konfigurimit duhet të kryhen gjithmonë. Emërtoni pajisjen për ta dalluar nga routerët e tjerë dhe konfiguroni fjalëkalimet, siç tregohet në shembull.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

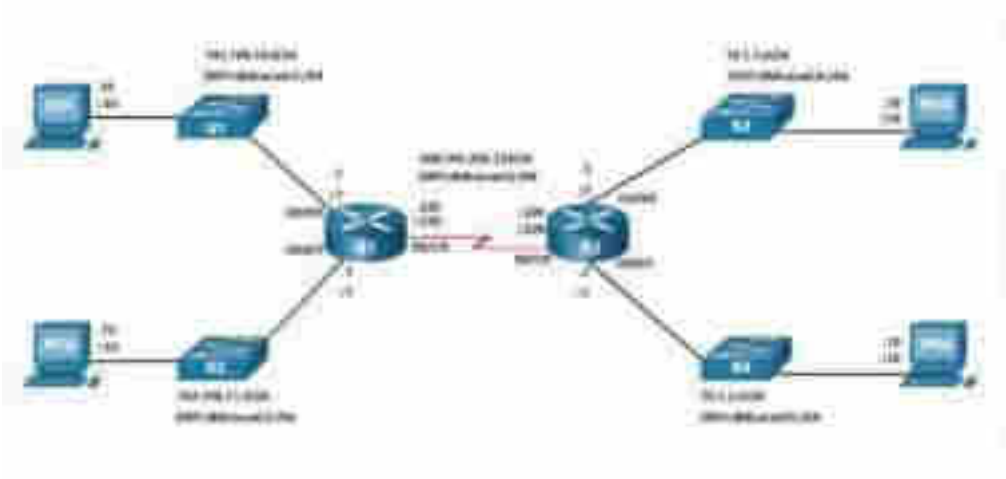
Konfiguroni një banner për të siguruar njoftimin e ligjshëm të hyrjes së paautorizuar, siç tregohet në shembull.

```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Ruaj ndryshimet në router siç e tregon figura.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

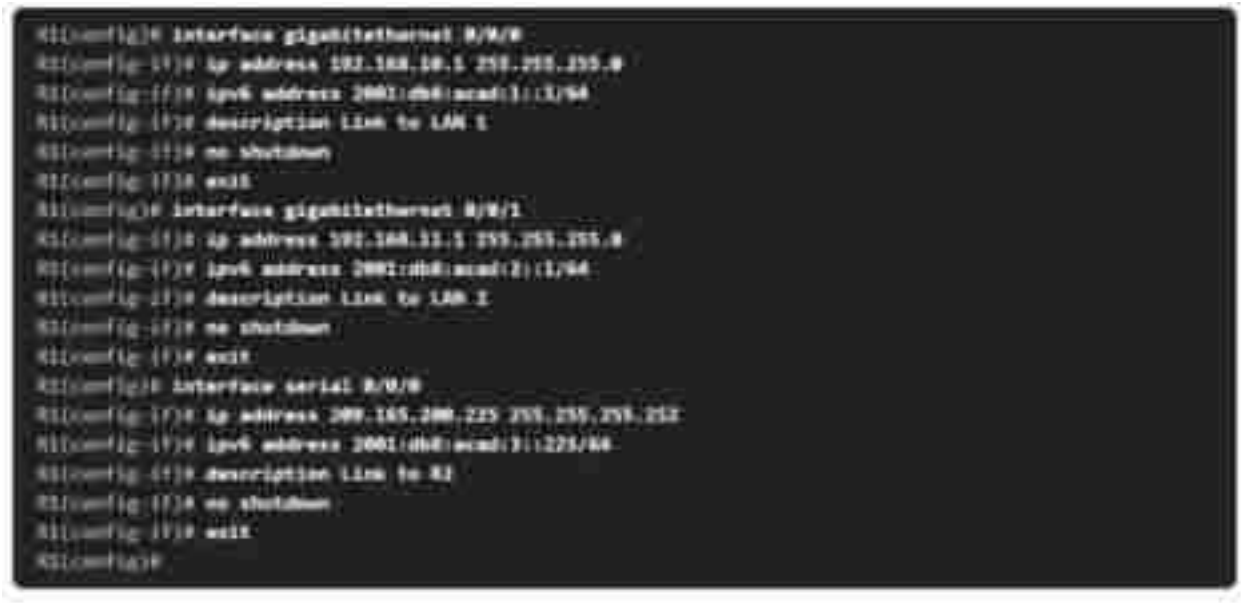
Një tipar dallues midis switch-eve dhe router-ave është lloji i ndërfaqeve të mbështetura nga secila. Për shembull, switch-et e shtresës së 2-të mbështesin LAN; prandaj, ata kanë shumë porta FastEthernet ose Gigabit Ethernet. Topologjia dual stack në figurë përdoret për të demonstruar konfigurimin e ndërfaqeve të router-it IPv4 dhe IPv6.



Router-at mbështesin LAN dhe WAN dhe mund të ndërlidhin lloje të ndryshme të rrjeteve; prandaj, ata mbështesin shumë lloje të ndërfaqeve. Për shembull, G2 ISR ka një ose dy ndërfaqe Gigabit Ethernet të integruara dhe slote me shpejtësi të lartë WAN Interface Card (HWIC) për të akomoduar lloje të tjera të ndërfaqeve të rrjetit, duke përfshirë ndërfaqet serike, DSL dhe kabllot. Për të qenë në dispozicion, një ndërfaqe duhet të jetë:

- **Konfiguruar me të paktën një adresë IP** - Përdorni komandën e **ip address** *ip-address subnet-mask* dhe **ipv6 address** *ipv6-address/prefix*.
- **Të aktivizohet** – By default, ndërfaqet LAN dhe WAN nuk janë të aktivizuara (shutdown). Për të mundësuar një ndërfaqe, ajo duhet të aktivizohet duke përdorur komandën **no shutdown**. (Kjo është e ngjashme me furnizimin me energji të ndërfaqes.) Ndërfaqja duhet gjithashtu të jetë e lidhur me një pajisje tjetër (një hub, një switch ose një router tjetër) që shtresa fizike të jetë aktive.
- **Përshkrimi** - Sipas dëshirës, ndërfaqja mund të konfigurohet gjithashtu me një përshkrim të shkurtër deri në 240 karaktere. Është praktikë e mirë të konfiguroni një përshkrim në secilën ndërfaqe. Në rrjetet e prodhimit, përfitimet e përshkrimeve të ndërfaqeve kuptohen shpejt pasi ato janë të dobishme në zgjidhjen e problemeve dhe në identifikimin e një lidhjeje të palës së tretë dhe informacionit të kontaktit.

Shembulli i mëposhtëm tregon konfigurimin për ndërfaqet në
R1



Ndërfaqja **loopback** është një ndërfaqe logjike që është e brendshme për router-in. Nuk është caktuar në një port fizik dhe nuk mund të lidhet kurrë me ndonjë pajisje tjetër. Konsiderohet si një ndërfaqe softuerike që vendoset automatikisht në një gjendje "up", për sa kohë që funksionon router-i. Ndërfaqja loopback është e dobishme në testimin dhe menaxhimin e një pajisjeje Cisco IOS sepse siguron që të paktën një ndërfaqe të jetë gjithmonë në dispozicion. Për shembull, mund të përdoret për qëllime testimi, të tilla si testimi i proceseve të router-it të brendshëm, duke imituar rrjete pas routerit. Përdoren gjithashtu zakonisht në mjediset laboratorike për të krijuar ndërfaqe shtesë. Për shembull, mund të krijoni ndërfaqe në një router për të simuluar më shumë rrjete për praktikën e konfigurimit dhe qëllimet e testimit. Në këtë kurrikulë, ne shpesh përdorim një ndërfaqe loopback për të simuluar një lidhje në internet.

Aktivizimi dhe caktimi i një adrese loopback është i thjeshtë:

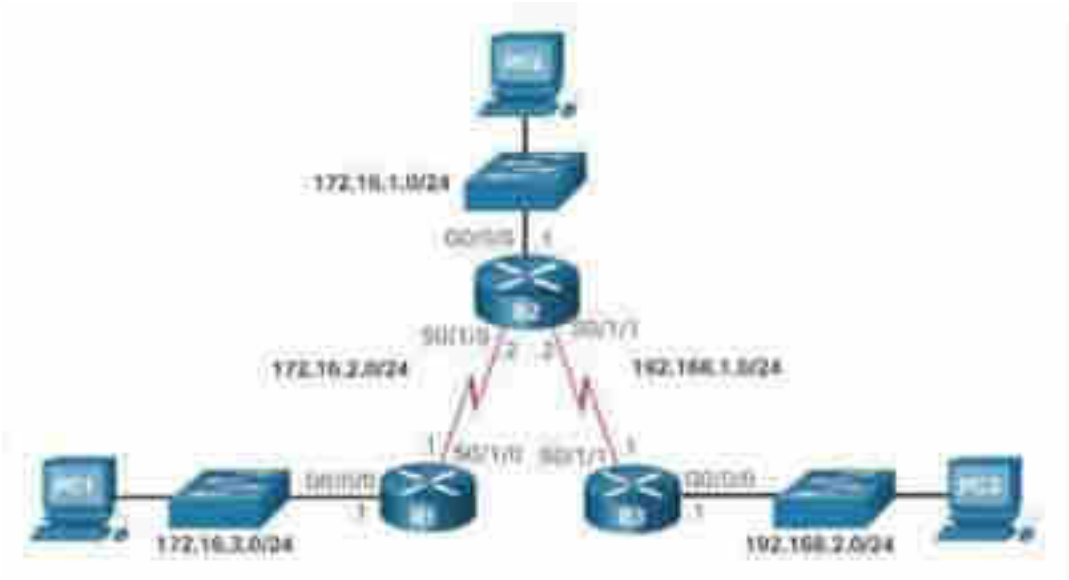
Ndërfaqet e shumëfishta loopback (Multiply loopback) mund të aktivizohen në një router. Adresa IPv4 për secilën ndërfaqe loopback duhet të jetë unike dhe e papërdorur nga çdo ndërfaqe tjetër, siç tregohet në shembullin e konfigurimit të ndërfaqes loopback 0 në R1.

Tema 24. Sigurimi dhe rikthimi ne pune i konfigurimit te router-it CISCO.

Gjetja e një rruge të humbur (ose të konfiguruar gabim) është një proces relativisht i drejtpërdrejtë nëse mjetet e duhura përdoren në një mënyrë metodike.

Për shembull, përdoruesi në PC1 raporton se nuk mund të ketë qasje në burimet në R3 LAN. Kjo mund të konfirmohet duke ping-uar ndërfaqen LAN të R3 duke përdorur ndërfaqen LAN të R1 si burim. Përsëri, ne do të përdorim topologjinë në figurë për të demonstruar se si të zgjidhim problemin e këtij problemi të lidhjes.

Figura përshkruan PC2 të lidhur me një switch në rrjetin 172.16.1.0/24. Më pas switch-i lidhet me router-in (R2) në ndërfaqen Gigabit G0/0/0 me një adresë Gateway prej 0,1. R2 ka dy lidhje serike S0 / 1/0 dhe S0 / 1/1 të lidhura me routerin (R1) për S0 / 1/0 dhe routerin (R3) në lidhjen S0 / 1/1. Adresa e rrjetit nga R1 në R2 është 172.16.2.0/14 dhe për R2 në R3 është 192.181.1.0/24. Adresat e lidhjes Serike për R2 janë .2 ndërsa R1 dhe R3 janë .1. R1 është i lidhur përmes ndërfaqes Gigabit G0 / 0/0 me një switch në një rrjet me adresën 172.16.3.0/24 me PC1 të lidhur në switch. R3 ka një lidhje Gigabit me një switch në rrjetin 192.168.2.0/24 me PC3 të lidhur në switch.



Ping LAN në distancë

Administratori i rrjetit mund të provojë lidhjen midis dy LAN-ve nga R1 në vend të PC1. Kjo mund të bëhet duke marrë ping-un nga ndërfaqja G0 / 0/0 në R1 në ndërfaqen G /0/0 në R3, siç tregohet në shembull. Rezultatet e ping-ut tregojnë se nuk ka asnjë lidhje ndërmjet këtyre LAN-ve.

Ping Router Next-Hop

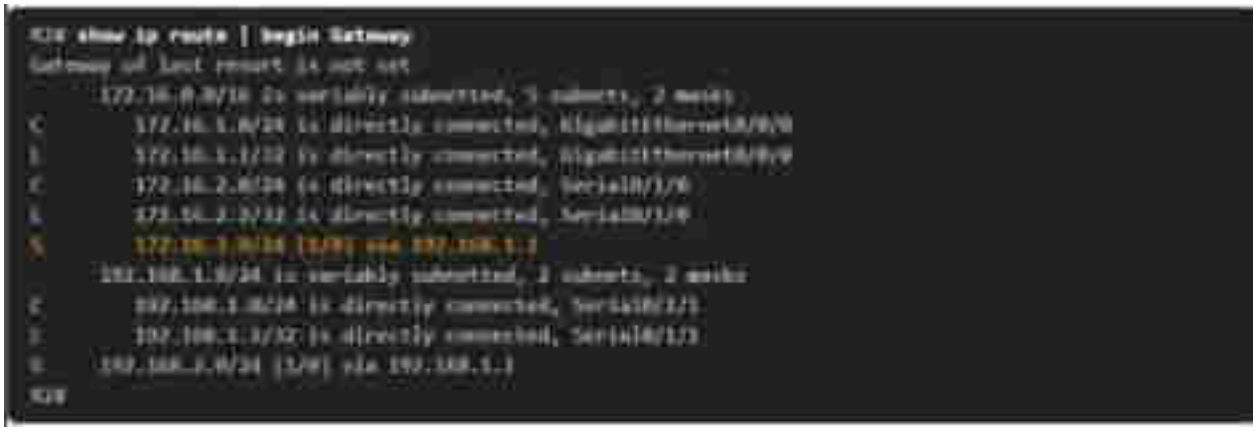
Tjetra, një ping në ndërfaqen S0/1/0 në R2 është i suksesshëm. Kjo ping buron nga ndërfaqja S0/1/0 e R1. Prandaj, çështja nuk është humbja e lidhjes midis R1 dhe R2.

Ping R3 LAN nga S0/1/0

Një ping nga R1 në ndërfaqen R3 192.168.2.1 është gjithashtu i suksesshëm. Kjo ping buron nga ndërfaqja S0/1/0 në R1. R3 ka një rrugë kthimi në rrjet midis R1 dhe R2, 172.16.2.0/24. Kjo konfirmon që R1 mund të arrijë LAN-in e largët në R3. Sidoqoftë, paketat me burim nga LAN në R1 nuk munden. Kjo tregon që ose R2 ose R3 mund të kenë një rrugë të pasaktë ose që mungon në LAN në R1.

Verifikoni Tabelën R2 të Routing

Hapi tjetër është të hetojmë tabelat e rutimit të R2 dhe R3. Tabela e rutimit për R2 është treguar në shembull. Vini re se rrjeti 172.16.3.0/24 është konfiguruar gabimisht. Rruga statike në rrjetin 172.16.3.0/24 është konfiguruar duke përdorur adresën tjetër të hopit 192.168.1.1. Prandaj, paketat e destinuara për rrjetin 172.16.3.0/24 dërgohen përsëri në R3 në vend të R1.

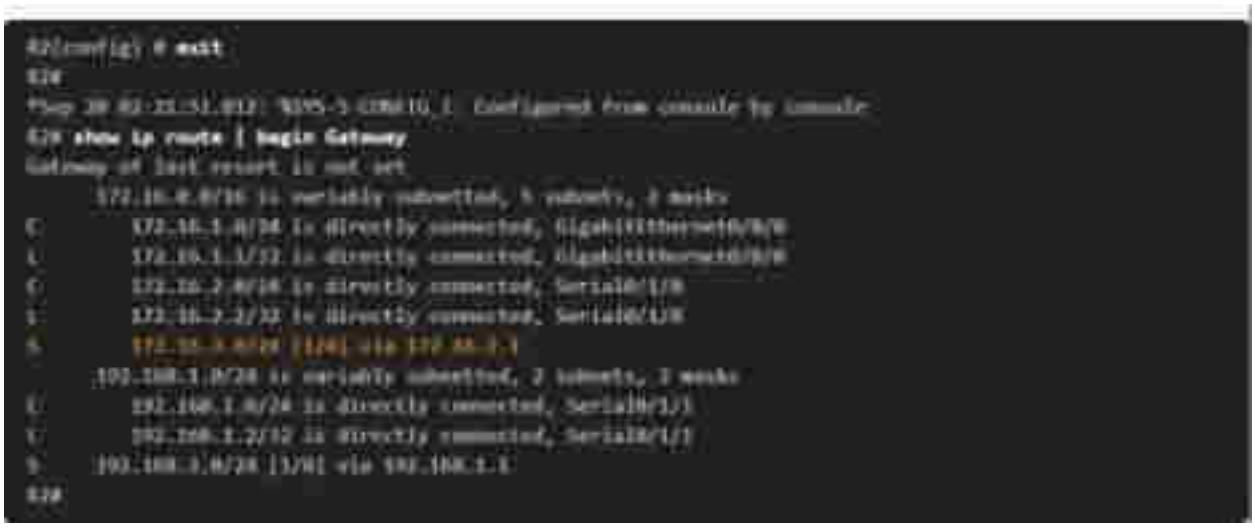


Korrigjimi i konfigurimin R2 Static Route

Në vazhdim, konfigurimi i ekzekutuar, në të vërtetë, zbulon deklaratën e pasaktë të **ip route**. Rruga e pasaktë hiqet dhe rruga e saktë futet më pas.

Verifikoni nëse është instaluar rruga e re statike

Tabela e rutimit në R2 kontrollohet edhe një herë për të konfirmuar hyrjen e router-it në LAN në R1, 172.16.3.0, është e saktë dhe tregon drejt R1.



Ping përsëri në LAN të largët

Më tej, përdoret një ping nga R1 me burim nga G0/0/0 për të verifikuar që R1 tani mund të arrijë në ndërfaqen LAN të R3. Si hap i fundit në konfirmim, përdoruesi në PC1 duhet gjithashtu të provojë lidhjen me LAN 192.168.2.0/24.

Tema 25. Grumbullimi i informacioneve ne lidhje me paisjet fqinje nepermjet telnet dhe CDP

Ju nuk mund të keni gjithmonë qasje të drejtpërdrejtë në switch-in tuaj kur duhet ta konfiguroni. Ju duhet të jeni në gjendje të përdorni atë nga distanca dhe është e domosdoshme që qasja juaj të jetë e sigurt. Kjo temë diskuton se si të konfiguroni Secure Shell (SSH) për qasje në distancë.

Telnet përdor portën TCP 23. Është një protokoll më i vjetër që përdor transmetimin e pasigurt të tekstit të thjeshtë si të vërtetimit të hyrjes (emri i përdoruesit dhe fjalëkalimi) ashtu edhe të të dhënave të transmetuara ndërmjet pajisjeve komunikuese. Një kërcënues threat mund të monitorojë paketat duke përdorur Wireshark.

CDP: Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) është një protokoll i Cisco që përdoret për të mbledhur informacione në lidhje me pajisjet Cisco të lidhura drejtpërdrejt. CDP është një Protokoll i Shtresës 2 që është i pavarur nga protokolli i medias dhe rrjetit, që do të thotë se dy pajisje fqinje mund të mësojnë për njëra-tjetrën edhe nëse nuk flasin të njëjtin protokoll rrjeti. CDP aktivizohet si parazgjedhje në shumicën e Ndërfaqeve në Pajisjet Cisco dhe dërgon mesazhe njoftimi të CDP në adresën e destinacionit multicast 01-00-0c-cc-cc-cc çdo 60 sekonda.

Informacioni i marrë nga një pajisje Cisco ruhet dhe mund të shikohet me komandën **show cdp [detaje].**

Figura më poshtë tregon prodhimin e komandës show cdp neighbors.

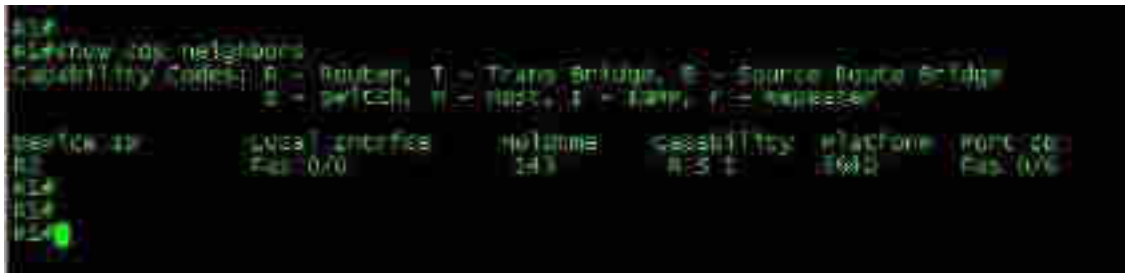
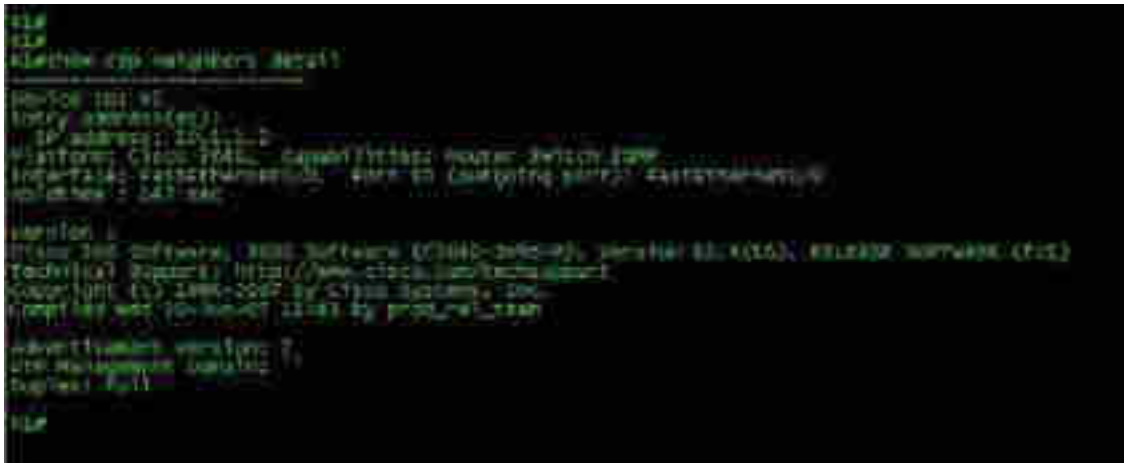


Figura më poshtë tregon output-in e komandës **show cdp neighbors** që përfshin informacione shtesë siç janë softueri IOS dhe adresa e shtresës së rrjetit.



Tema 26. Perdorimi i komandave Ping dhe Traceroute per testimin e lidhjes

Shumë skenarë ju kërkojnë të provoni gjërat lokalisht në kompjuterin tuaj duke përdorur command line. Për shembull, nëse po përpiqeni të provoni lidhjen midis kompjuterit tuaj dhe një host të largët, një mjet i bazuar në internet nuk mund ta sigurojë këtë informacion. Teston vetëm lidhjen nga serveri i tij në hostin e largët. Hapat e saktë për të përdorur mjetet **ping** dhe **traceroute** nga command line varen nga sistemi operativ i kompjuterit tuaj. Ndiqni procedurat e duhura më poshtë për sistemin tuaj operativ.
Testi themelor i ping-ut është një nga gjërat më të lehta që mund të bëni për të verifikuar lidhjen midis kompjuterit tuaj dhe një host të largët. Ky test është i lehtë për tu ekzekutuar nga CLI.
Për të përdorur programin ping në Microsoft Windows, ndiqni këto hapa:

1. Hapni një dritare të komandës DOS. Për ta bërë këtë, klikoni Start, klikoni Run, shtypni cmd, dhe pastaj shtypni Enter.
2. Në komandën e shpejtë, shtypni komandën e mëposhtme. Zëvendësoni example.com me domenin që dëshironi të testoni:

```
3.    ping example.com
```

4. Interpreton output-in nga ping:
    a. Nëse hosti në distancë është aktiv dhe i konfiguruar për t'iu përgjigjur kërkesave

të ping, shfaqen përgjigjet. Për shembull, rezultati i mëposhtëm tregon përgjigjet ping nga një server A2 Hosting:

b. C:\Documents and Settings\user>ping a2s78.a2hosting.com
c. Pinging a2s78.a2hosting.com [216.119.143.98] with 32 bytes of data:
d. Reply from 216.119.143.98: bytes=32 time=46ms TTL=54
e. Reply from 216.119.143.98: bytes=32 time=45ms TTL=54
f. Reply from 216.119.143.98: bytes=32 time=47ms TTL=54
g. Ping statistics for 216.119.143.98:
h. Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
i. Approximate round trip times in milli-seconds:
j. Minimum = 45ms, Maximum = 47ms, Average = 46ms
k. Përndryshe, nëse hosti i largët është i fikur, ose nuk është konfiguruar për t'iu përgjigjur kërkesave të ping-ut, ju nuk shihni ndonjë përgjigje.

Firewall-et mund të konfigurohen për bllokimin e pingimit të paketave. Nëse një host i largët nuk i përgjigjet kërkesës për pingim, ka mundësi që të jetë i aktivizuar dhe duke funksionuar normalisht, por po injoron kërkesën për pingim.

1. Për të përdorur programin ping në Mac OS X dhe Linux, ndiqni këto hapa:
2. Hapni një dritare terminale. Procedura për ta bërë këtë varet nga sistemi juaj operativ dhe mjedisi i desktopit:

- Në Mac OS X, klikoni **Applications**, klikoni **Utilities**, dhe pastaj klikoni **Terminal**.
- Në Linux, hapni një dritare terminale.

3. Në komandën e shpejtë, shtypni komandën e mëposhtme. Zëvendësoni example.com me domenin që dëshironi të testoni:

```
4. ping example.com
```

5. Shtypni Ctrl + C për të ndaluar ping-un pasi të keni ekzekutuar disa prova dhe më pas interpretoni prodhimin:

- Nëse hosti në distancë është aktiv dhe i konfiguruar për t'iu përgjigjur kërkesave të ping, shfaqen përgjigjet. Për shembull, rezultati i mëposhtëm tregon përgjigjet ping nga një server A2 Hosting:
- user@localhost:~$ ping a2s78.a2hosting.com
- PING a2s78.a2hosting.com (216.119.143.98) 56(84) bytes of data.
- 64 bytes from a2s78.a2hosting.com (216.119.143.98): icmp_req=1 ttl=54 time=44.4 ms
- 64 bytes from a2s78.a2hosting.com (216.119.143.98): icmp_req=2 ttl=54 time=43.8 ms
- 64 bytes from a2s78.a2hosting.com (216.119.143.98): icmp_req=3 ttl=54 time=44.7 ms
- Nga ana tjetër, nëse host-i i largët është i fikur, ose nuk është konfiguruar për t'iu përgjigjur kërkesave të ping-ut, nuk shihni ndonjë përgjigje.
- Programi **traceroute** ofron informacion shumë më të detajuar në lidhje me një lidhje me një host të largët sesa ping. Traceroute (ose tracert në sistemet Microsoft Windows) tregon informacionin për secilin "hop" që një paketë merr nga kompjuteri juaj në hostin e largët. Shpesh është një mënyrë e mirë për të përcaktuar çështjet e mundshme të lidhjes ISP ose ngushtimet e rrjetit.
- Në sistemet e bazuara në Windows, përdorni programin **tracert** për të testuar rrugën drejt një serveri. Për ta bërë këtë, ndiqni këto hapa:
- Hapni një dritare të komandës DOS. Për ta bërë këtë, klikoni **Start**, klikoni **Run**, shtypni **cmd**, dhe pastaj shtypni **Enter**.
- Në komandën e shpejtë, shtypni komandën e mëposhtme. Zëvendësoni example.com me domenin që dëshironi të testoni.

- Interpreton output-in nga tracerti.
- Tracert shfaq çdo hop, të treguar me një numër në kolonën e majtë. Ai gjithashtu shfaq domenin dhe adresën IP në secilin hop, si dhe kohën e kaluar. Për shembull, rezultati i mëposhtëm tregon rrugën për në një server A2 Hosting.
- C:\>tracert a2s78.a2hosting.com
- Tracing route to a2s78.a2hosting.com [216.119.143.98]
- over a maximum of 30 hops.
- 1 ms <1 ms <1 ms Linksys [192.168.0.1]
- [Lines omitted for brevity]
- 45 ms 38 ms 38 ms pos-1-6-0-0-pe01.350 ecermak.il.ibone.comcast.net [68.86.87.130]
- 67 ms 150 ms 76 ms cr-1.sfld-mi.123.net [66.208.233.62]
- 44 ms 63 ms 46 ms gateway1.a2hosting.com [216.234.104.254]
- 72 ms 57 ms 63 ms a2s78.a2hosting.com [216.119.143.98]
- Trace complete.

Ju mund të shqyrtoni kohën midis secilit hop për të kërkuar vende ku "varet" lidhja. Në disa raste, edhe koncerti mund të skadojë, gjë që tregohet me yll (*).
Për të përdorur programin traceroute në Mac OS X dhe Linux, ndiqni këto hapa:

1. Hapni një dritare terminale. Procedura për ta bërë këtë varet nga sistemi juaj operativ dhe mjedisi i desktopit:
- Në Mac OS X, klikoni Applications, klikoni Utilities, dhe pastaj klikoni Terminal.
- Në Linux, hapni një dritare terminale.
2. Në komandën e shpejtë, shtypni komandën e mëposhtme. Zëvendësoni example.com me domenin që dëshironi të testoni:

```
3. traceroute example.com
```

4. Interpreton output-in nga tracerti:

a. Traceroute shfaq çdo hop, të treguar nga një numër në kolonën e majtë. Ai gjithashtu shfaq domenin dhe adresën IP në secilin hop, si dhe kohën e kaluar. Për shembull, rezultati i mëposhtëm tregon rrugën për në një server A2 Hosting:
b. user@localhost:~$ traceroute a2s78.a2hosting.com
c. Linksys (192.168.0.1) 0.315 ms 0.452 ms 0.472 ms
d. [Lines omitted for brevity]
e. pos-1-6-0-0-pe01.350ecermak.il.ibone.comcast.net (68.86.87.130) 39.010 ms 38.054 ms 38.092 ms
f. cr-1.sfld-mi.123.net (66.208.233.62) 45.056 ms 44.335 ms 44.974 ms
g. gateway1.a2hosting.com (216.234.104.254) 45.274 ms 46.650 ms 46.089 ms
h. a2s78.a2hosting.com (216.119.143.98) 44.654 ms 46.028 ms 43.852 ms

Ju mund të shqyrtoni kohën midis secilit hop për të kërkuar vende ku "varet" lidhja. Në disa raste, traceroute gjithashtu mund të skadojë, gjë që tregohet me një yll (*).

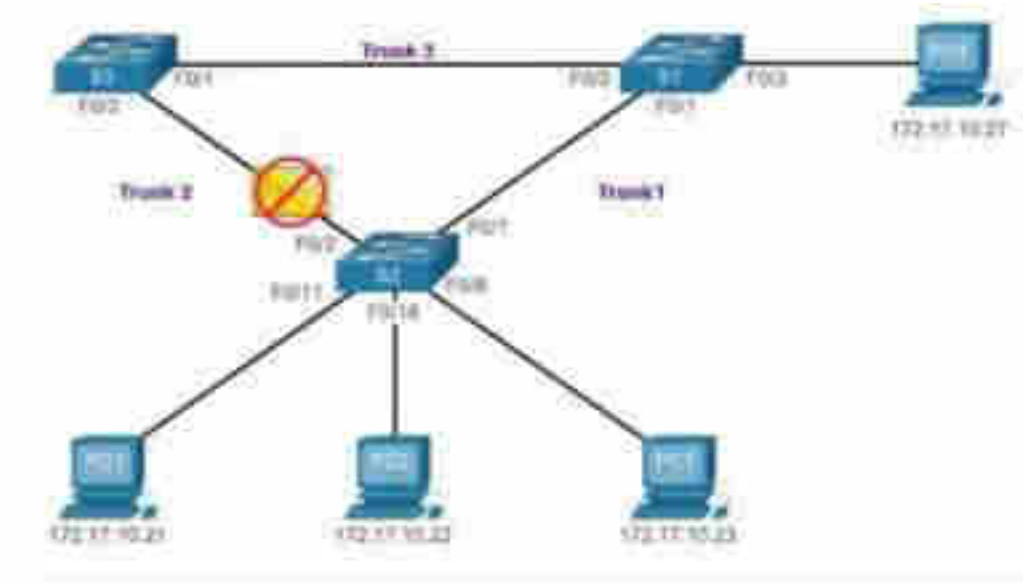
Tema 27. Layer 2 switching. Tre funksionet e switching ne shtresen e dyte (Layer 2). Spaning Tree Protocol (SPT).

Në këtë temë trajtohen shkaqet e cikleve në një rrjet Shtresa 2 dhe shpjegon shkurtimisht se si funksionon protokolli spanning tree. Teprica është një pjesë e rëndësishme e dizajnit hierarkik për eliminimin e pikave të vetme të dështimit dhe parandalimin e ndërprerjes së shërbimeve të rrjetit për përdoruesit. Rrjetet e tepërta kërkojnë shtimin e rrugëve fizike, por teprica logjike duhet të jetë gjithashtu pjesë e dizajnit. Pasja e rrugëve alternative fizike që të dhënat të

përshkojnë rrjetin bën të mundur që përdoruesit të kenë qasje në burimet e rrjetit, pavarësisht nga ndërprerja e rrugës. Sidoqoftë, rrugët e tepërta në një rrjet të Ethernet swithed mund të shkaktojnë cikle fizike dhe logjike të Shtresës 2.

LAN-et Ethernet kërkojnë një topologji pa cikël me një shteg të vetëm ndërmjet dy pajisjeve. Një cikël në një LAN Ethernet mund të shkaktojë përhapjen e vazhdueshme të frame-ve Ethernet derisa një lidhje të prishet dhe të prishë ciklin.

Spanning Tree Protocol (STP) është një protokoll rrjeti për parandalimin e ciklit (loop) që lejon tepricë ndërsa krijon një topologji të shtresës 2 pa cikël. IEEE 802.1D është standardi origjinal IEEE MAC Bridging për STP.



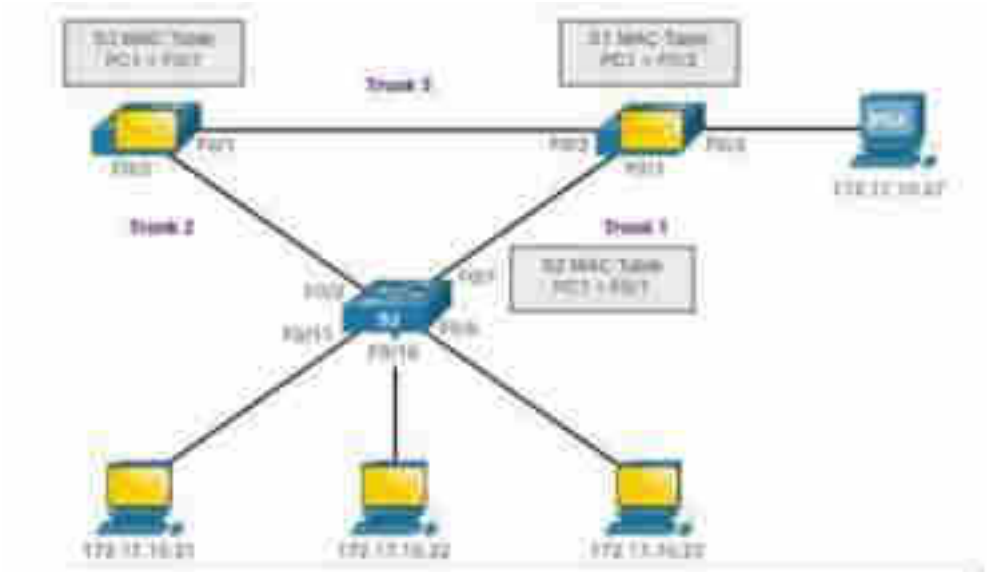
Teprica e rrugës (Path redundancy) siguron shërbime të shumëfishta të rrjetit duke eliminuar mundësinë e një pike të vetme të dështimit. Kur ekzistojnë pathe të shumëfishta midis dy pajisjeve në një rrjet Ethernet dhe nuk ka zbatim të STP në switch, ndodh një cikël (loop) në shtresën 2. Një cikël i shtresës 2 mund të rezultojë në paqëndrueshmëri në adresat MAC, mbushje të lidhjeve dhe përdorim të lartë të CPU-së në switch dhe pajisjet fundore, duke rezultuar në rrjeti si i papërdorshëm.

Ndryshe nga protokollet e shtresës 3, IPv4 dhe IPv6, shtresa 2 Ethernet nuk përfshin një mekanizëm për të njohur dhe eleminuar frame looping pafund. Të dy IPv4 dhe IPv6 përfshijnë një mekanizëm që kufizon numrin e herëve që një pajisje e rrjetit të shtresës 3 mund të ritransmetojë një paketë. Një router do të zvogëlojë TTL (Time to Live) në çdo paketë IPv4, dhe fushën Hop Limit në çdo paketë IPv6. Kur këto fusha zbriten në 0, një router do të heqë paketën. Switche-t Ethernet dhe Ethernet nuk kanë asnjë mekanizëm të krahasueshëm për të kufizuar numrin e herëve që një switch ritransmeton një frame të shtresës 2. STP u zhvillua posaçërisht si një mekanizëm parandalues i ciklit për Shtresën 2 Ethernet.

Pa aktivizuar STP, ciklet e shtresës së 2 mund të formohen, duke bërë që frame-t broadcast, multicast dhe unknown unicast të shfaqen pa fund. Kjo mund të rrëzojë një rrjet brënda një kohe shumë të shkurtër, ndonjëherë në vetëm disa sekonda. Për shembull, frame-t e transmetimit, siç është një Kërkesë ARP, përcillen nga të gjitha portat e switch-ut, përveç portës origjinale të hyrjes. Kjo siguron që të gjitha pajisjet në një domen të transmetuar të jenë në gjendje të marrin frame-in. Nëse ka më shumë se një rrugë që frame-i të përcillet jashtë, mund të rezultojë një

cikël i pafund. Kur ndodh një cikël, tabela e adresave MAC në një switch do të ndryshojë vazhdimisht me përditësimet nga frame-t e transmetimit, gjë që rezulton në paqëndrueshmëri të bazës së të dhënave MAC. Kjo mund të shkaktojë përdorim të lartë të CPU-së, gjë që e bën kalimin të mos jetë në gjendje të përcjellë frame-t.

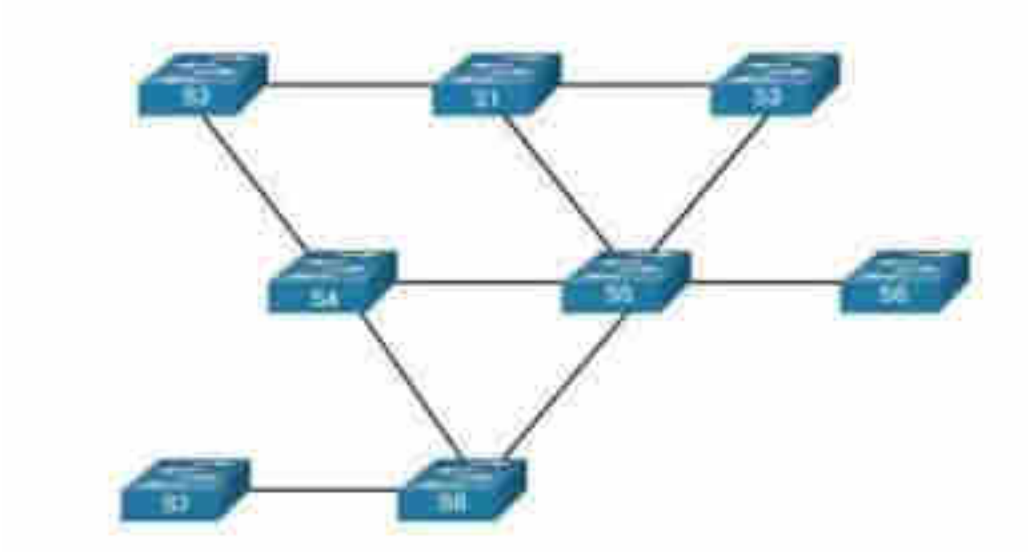
Broadcast frames nuk janë lloji i vetëm i frame-ve që preken nga ciklet. Unknown unicast frames të dërguara në një rrjet të cikluar mund të rezultojnë në frame e kopjuara që mbërrijnë në pajisjen e destinacionit. Një Unknown unicast frames është kur switch-i nuk ka adresën MAC të destinacionit në tabelën e saj të adresave MAC dhe duhet ta përcjellë frame-in nga të gjitha portat, përveç portës së hyrjes.



STP bazohet në një algoritëm të shpikur nga Radia Perlman ndërsa punonte për Digital Equipment Corporation, dhe botuar në gazetën e vitit 1985. Algoritmi spanning tree algorithm (STA) krijon një topologji pa cikël (loop) duke zgjedhur një urë rrënjë të vetme ku të gjithë switch-et e tjerë përcaktojnë një rrugë të vetme me kosto më të ulët.

Skenarit i Topologjisë STA

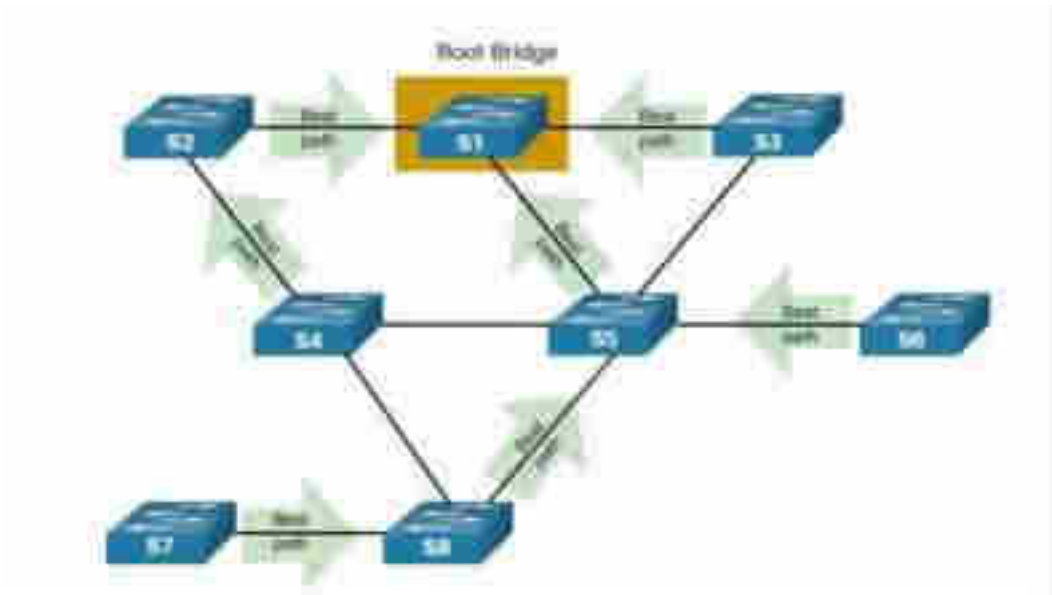
Ky skenar STA përdor një LAN Ethernet me lidhje të tepërta ndërmjet shumë switch-eve.



Zgjidhja e Root Bridge

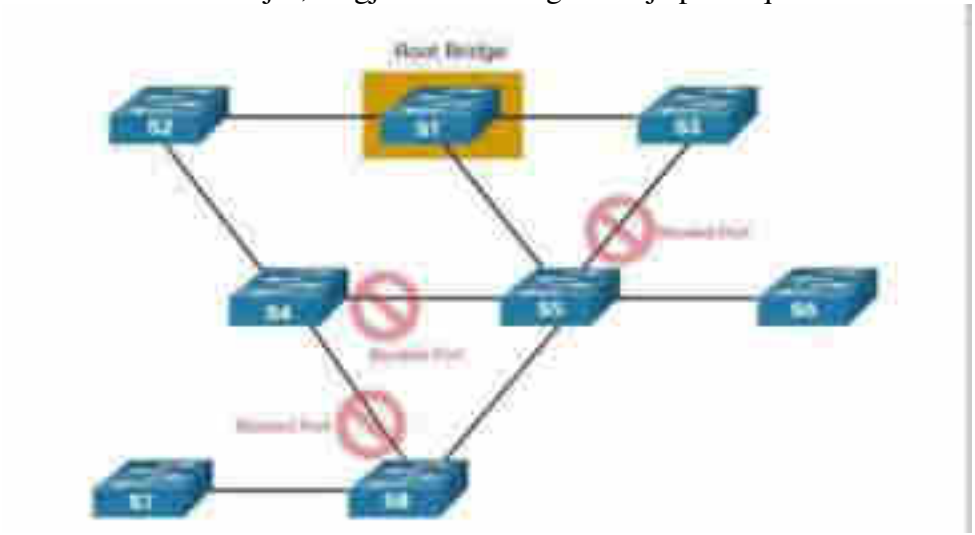
Algoritmi Spanning tree fillon duke zgjedhur një urë të vetme rrënjë. Figura tregon se S1 është zgjedhur si ura rrënjë. Në këtë topologji, të gjitha lidhjet janë me kosto të barabartë (i njëjti bandwidth). Çdo switch do të përcaktojë një rrugë të vetme, me kosto më të vogël nga vetja në urën rrënjë.

Shënim: STA dhe STP u referohet switch-eve si ura. Kjo sepse në ditët e para të përdorimi të Ethernet, switch-et referoheshin si ura (bridge).



Bllokimi i shtigjeve (paths) të tepërta
STP siguron që ekziston vetëm një rrugë logjike midis të gjitha destinacioneve në rrjet duke bllokuar qëllimisht shtigjet e tepërta që mund të shkaktojnë një cikël, siç tregohet në figurë. Kur një port bllokohet, të dhënat e përdoruesit nuk lejohen të hyjnë ose dalin nga ajo port. Bllokimi i shtigjeve të tepërta është thelbësor për parandalimin e cikleve në rrjet.

Topologji pa cikël (loop)
Një port i bllokuar ka efektin që e bën atë lidhje një lidhje jo-përcjellëse midis dy switch-eve, siç tregohet në figurë. Vini re se kjo krijon një topologji ku secili switch ka vetëm një rrugë të vetme në urën e rrënjës, e ngjashme me degët në një pemë që lidhen me rrënjën e pemës.



Deri më tani, ne kemi diskutuar STP në një mjedis ku ka vetëm një VLAN. Sidoqoftë, STP mund të konfigurohet për të funksionuar në një mjedis me shumë VLAN.

Në versionet Per-VLAN Spanning Tree (PVST) të STP, ekziston një urë rrënjë e zgjedhur për secilin shembull të pemës që shtrihet. Kjo bën të mundur që të ketë ura të ndryshme rrënjësore për grupe të ndryshme të VLAN. STP operon një shembull të veçantë të STP për secilin VLAN individual. Nëse të gjitha portat në të gjithë çelsat janë anëtarë të VLAN 1, atëherë ekziston vetëm një shembull peme që shtrihet. Deri më tani, ne kemi diskutuar STP në një mjedis ku ka vetëm një VLAN. Sidoqoftë, STP mund të konfigurohet për të funksionuar në një mjedis me shumë VLAN.

Tema 28. Menyrat e switching ne LAN (Real-Time, Cut-Through dhe Store and Forword)

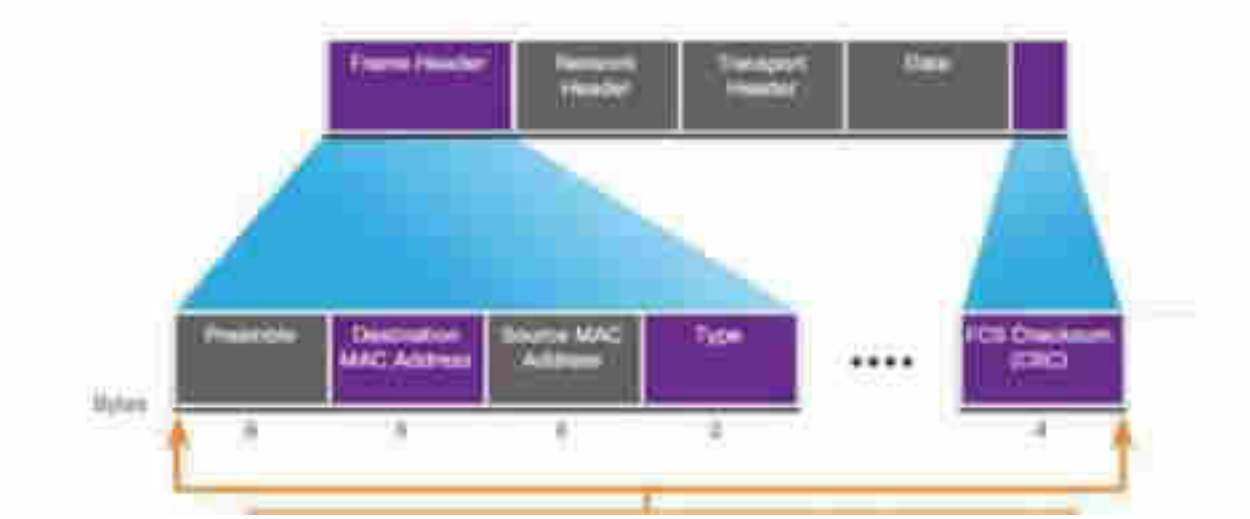
Switch-et i marrin shumë shpejt vendimet për përcjelljen (forwording) në shtresën e 2. Kjo është për shkak të softuerit të aplikacioneve-specifike-të qarqeve-të integruara (ASIC). ASIC zvogëlojnë kohën e trajtimit të frame-it brënda pajisjes dhe lejojnë që pajisja të menaxhojë një numër më të madh fraim-esh pa rënie performance.

Switch-et e shtresës 2 përdorin një nga dy metodat për të ndërruar frame-t:

- **Store-and-forward switching** - Kjo metodë merr një vendim transferimi në një frame pasi të ketë marrë frame-n e plotë dhe ta kontrollojë atë për gabime duke përdorur një mekanizëm matematikor të kontrollit të gabimeve të njohur si një cyclic redundancy check (CRC). Store-and-forward switching është mënyra kryesore e ndërrimit të LAN të Cisco.
- **Cut-through switching** - Kjo metodë fillon procesin e përcjelljes pasi të jetë përcaktuar adresa MAC e destinacionit të një frame hyrëse dhe porta dalëse.

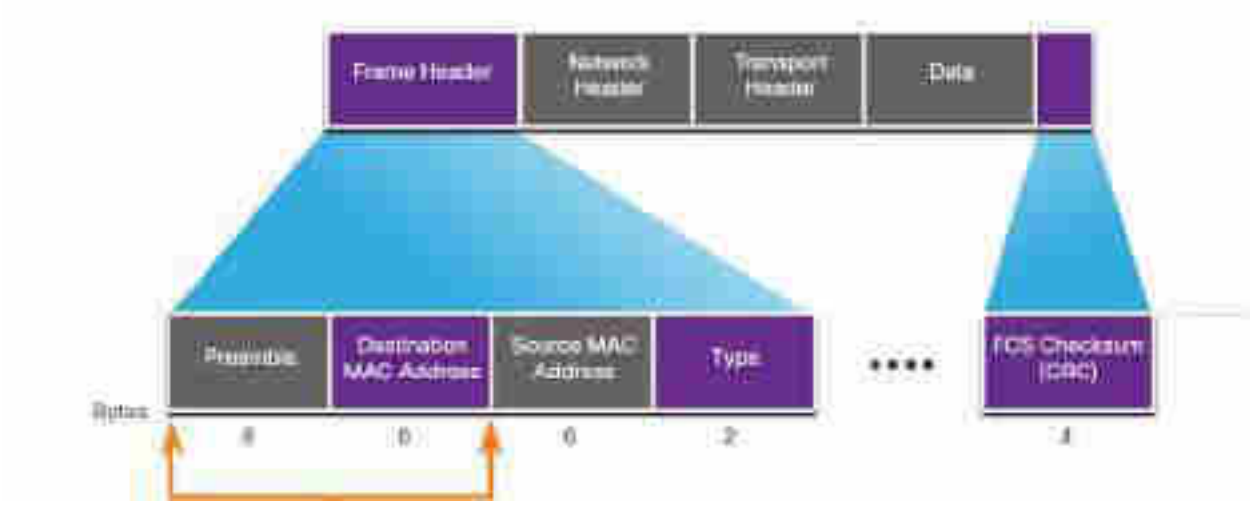
Store-and-forward switching, siç dallohet nga cut-through switching, ka këto dy karakteristika kryesore:

- **Error checking** - Pasi të marrë frame-n të plote në portën e hyrjes, switch-i krahason vlerën e FCS në fushën e fundit të datagramit kundrejt llogaritjeve të veta të FCS. FCS është një proces i kontrollit të gabimeve që ndihmon për të siguruar që frame-t të jetë pa gabime fizike dhe të Data Link-ut. Nëse frame është pa gabime, switch-i përcjell atë. Përndryshe bie lidhja.
- **Automatic buffering** - Procesi port buffering në hyrje i përdorur nga store-and-forward switches siguron fleksibilitetin për të mbështetur çdo përzierje të shpejtësive Ethernet. Për shembull, trajtimi i një frame-i hyrëse që udhëton në një port Ethernet 100 Mbps që duhet të dërgohet nga një ndërfaqe 1 Gbps do të kërkonte përdorimin e metodës store-and-forward. Me çdo mospërputhje të shpejtësive ndërmjet portave hyrëse dhe dalëse, switch-i ruan të gjithë frame-in në një buffer, llogarit kontrollin FCS, e përcjell atë në buffer portën dalëse dhe më pas e dërgon atë.



Metoda store-and-forward switching prish frame-t që nuk kalojnë kontrollin e FCS. Prandaj, nuk përcjell frame të pavlefshme.

Në të kundërt, metoda e kalimit përmes ndërprerjes mund të përcjellë frame të pavlefshme sepse nuk kryhet asnjë kontroll FCS. Sidoqoftë, cut-through switching ka aftësinë për të kryer ndërrimin e shpejtë të frame-it. Kjo do të thotë që switch-i mund të marrë një vendim ridërgimi sapo të verifikojë adresën MAC të frame në tabelën e saj të adresave MAC, siç tregohet në figurë.



Switch-i nuk duhet të presë që pjesa tjetër e frame-it të hyjë në portën e hyrjes përpara se të marrë vendimin e saj të përcjelljes.
Metoda cut-through switching mund të përcjellë frame-t me gabime. Nëse ka një normë të lartë gabimi (frame të pavlefshme) në rrjet, cut-through switching mund të ketë një ndikim negativ në bandwidth, duke bllokuar kështu atë me frame-t të dëmtuara dhe të pavlefshme.

Tema 29. Konfigurimi i switch-eve CISCO

Para se të konfiguroni një switch, duhet ta ndizni dhe ta lejoni të kalojë në sekuencën e nisjes me pesë hapa. Kjo temë përfshin bazat e konfigurimit të një switch-i dhe përfshin një laborator në fund.
Pasi të aktivizohet një switch Cisco, ai kalon në sekuencën vijuese të nisjes (ngarkimit) me pesë hapa:
Hapi 1: Së pari, switch-i ngarkon një program të POST të ruajtur në ROM. POST kontrollon nënsistemin e CPU. Teston CPU, DRAM dhe pjesën e pajisjes flash që përbën sistemin e skedarëve flash.
Hapi 2: Tjetra, switch-i ngarkon softuerin e boot loader. Boot loaderështë një program i vogël i ruajtur në ROM që ekzekutohet menjëherë pasi POST të ketë përfunduar me sukses.
Hapi 3: Boot loader kryen fillimin e nivelit të ulët të CPU-së. Inicializon regjistrat e CPU-së, të cilët kontrollojnë se ku është shënuar kujtesa fizike, sasia e kujtesës dhe shpejtësia e saj.
Hapi 4: Boot loader inicializon sistemin e skedarëve flash në bordin e sistemit.
Hapi 5: Më në fund, **boot loader** lokalizon dhe ngarkon në kujtesë një imazh të paracaktuar të sistemit operativ IOS dhe jep kontrollin e kalimit në IOS.

Switch-et përpiqet të startojë automatikisht duke përdorur informacionin e variablit në mjedisin e BOOT. Nëse kjo variabël nuk është vendosur, switch-i përpiqet të ngarkojë dhe ekzekutojë skedarin e parë të ekzekutueshëm që mund të gjejë. Në switch-et e serive Catalyst 2960, skedari (image file) zakonisht përmbahet në një direktori që ka të njëjtin emër si skedari (duke përjashtuar shtesën e skedarit .bin). Sistemi operativ IOS pastaj inicializon ndërfaqet duke përdorur komandat Cisco IOS që gjenden në skedarin e konfigurimit fillestar (startup-config file). Skedari i konfigurimit fillestar quhet config.text dhe ndodhet në flash.

Në shembull, variabla e mjedisit BOOT vendoset duke përdorur komandën boot system të global configuration mode. Vini re që IOS ndodhet në një dosje të veçantë dhe rruga e dosjes është specifikuar. Përdorni komandën show boot se në çfarë është vendosur skedari aktual i nisjes së IOS.

```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

Tabela përcakton secilën pjesë të komandës së sistemit boot.

Komanda	Përkufizimi
boot system	Komanda kryesore
flash:	Pajisja e ruajtjes
c2960-lanbasek9-mz.150-2.SE/	Rruga për në sistemin e skedarëve
c2960-lanbasek9-mz.150-2.SE.bin	Emri i skedarit IOS

Switch-et Cisco Catalyst kanë disa drita treguese LED të statusit. Mund të përdorni LED-të e switch-it për të monitoruar shpejt aktivitetin dhe performancën e tij. Switch-et e modeleve dhe grupeve të veçorive të ndryshme do të kenë LED të ndryshëm dhe vendosja e tyre në panelin e përparmë të tij mund të ndryshojë gjithashtu.
Butoni Mode (7 në figurë) përdoret për të ndryshuar statusin e portës, dupleksin e portat, shpejtësinë e portës dhe nëse mbështetet, statusi Power over Ethernet (PoE) i LED-ve të portës (8 në figurë).

1 SYST
2 RPS
3 STAT

4 DUPLX
5 SPEED
6 PoE

LED i sistemit

Tregon nëse sistemi po merr energji dhe po funksionon si duhet. Nëse LED është i fikur, kjo do të thotë se sistemi nuk është ndezur. Nëse LED është jeshil, sistemi po funksionon normalisht. Nëse LED është qelibar, sistemi po merr energji por nuk po funksionon si duhet.

LED i Sistemit të Energjisë së tepërt (RPS)

Tregon statusin RPS. Nëse LED është i fikur, RPS është i fikur, ose nuk është i lidhur siç duhet. Nëse LED është jeshil, RPS është i lidhur dhe i gatshëm për të siguruar energji rezervë. Nëse LED po pulson jeshile, RPS është e lidhur por është e padisponueshme sepse po siguron energji në një pajisje tjetër. Nëse LED është qelibar, RPS është në modalitetin e gatishmërisë ose në një gjendje defekti. Nëse LED po pulson qelibar, furnizimi i brendshëm i rrymës në switch ka dështuar dhe RPS po siguron energji.

LED i statusit të portat

Tregon se mënyra e statusit të portat është zgjedhur kur LED është e gjelbër. Kjo është mënyra e paracaktuar. Kur të zgjidhen, LED-të e portat do të shfaqin ngjyra me kuptime të ndryshme. Nëse LED është i fikur, nuk ka asnjë lidhje, ose porta është mbyllur administrativisht. Nëse LED është e gjelbër, një lidhje është e pranishme. Nëse LED po ndizet e gjelbër, ka aktivitet dhe porta po dërgon ose merr të dhëna. Nëse LED alternon jeshile-qelibar, ka një defekt në lidhje. Nëse LED është qelibar, porta është e bllokuar për të siguruar që një cikël nuk ekziston në domenin e transferimit dhe nuk po përcjell të dhëna (zakonisht, portat do të qëndrojnë në këtë gjendje për 30 sekondat e para pasi të aktivizohen). Nëse LED po pulson qelibar, porta bllokohet për të parandaluar një cikël të mundshëm në domenin e përcjelljes.

LED Duplex Port

Tregon se mënyra duplex e portat zgjidhet kur LED është e gjelbër. Kur zgjidhen, LED-të e portat që janë të fikura janë në modalitetin gjysmë të dyfishtë. Nëse LED i portës është i gjelbër, porta është në modalitetin full-duplex.

LED me shpejtësi porta

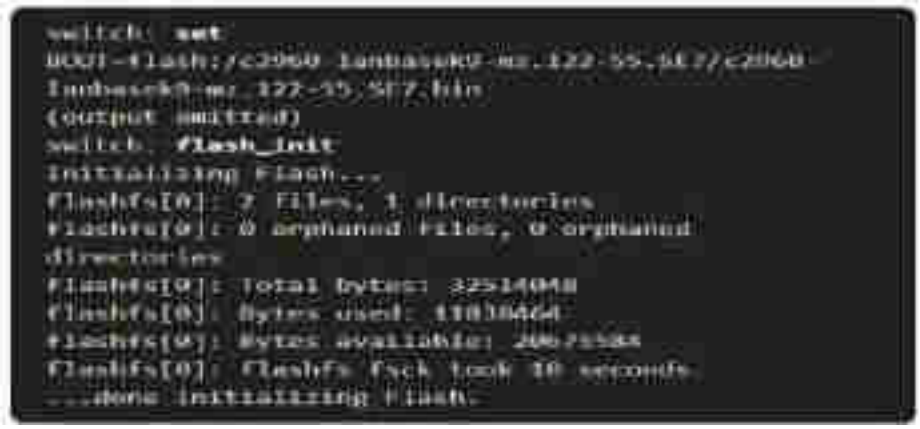
Tregon se është zgjedhur mënyra e shpejtësisë së portës. Kur të zgjidhen, LED-të e portat do të shfaqin ngjyra me kuptime të ndryshme. Nëse LED është i fikur, porta po funksionon me 10 Mbps. Nëse LED është i gjelbër, porta po funksionon me 100 Mbps. Nëse LED po pulson jeshile, porta po funksionon me 1000 Mbps.

PoE LED

Nëse PoE mbështetet, një LED i modës PoE do të jetë i pranishëm. Nëse LED është i fikur, kjo tregon se modaliteti PoE nuk është zgjedhur dhe se asnjë prej portave nuk i është mohuar energjia ose nuk është vendosur në një gjendje defekti. Nëse LED po pulson qelibar, modaliteti

PoE nuk zgjidhet, por të paktën një prej portave i është refuzuar energjia ose ka një defekt PoE. Nëse LED është jeshil, kjo tregon se është zgjedhur modaliteti PoE dhe LED-të e portat do të shfaqin ngjyra me kuptime të ndryshme. Nëse LED i portës është i fikur, PoE është i fikur. Nëse LED i portës është jeshil, PoE është i ndezur. Nëse LED i portës është i alternuar me jeshile-qelibar, PoE refuzohet sepse sigurimi i energjisë në pajisjen e furnizuar do të tejkalojë kapacitetin e energjisë së switch-it. Nëse LED po pulson qelibar, PoE është fikur për shkak të një defekti. Nëse LED është qelibar, PoE për portën është çaktivizuar.

Boot Loader siguron hyrjen në switch nëse sistemi operativ nuk mund të përdoret për shkak të skedarëve të sistemit të humbur ose të dëmtuar. Boot loader ka një command line që siguron qasje në skedarët e ruajtur në memorjen flash.
Në boot loader mund të arrihet përmes një lidhje konsolë duke ndjekur këto hapa:
Hapi 1. Lidhni një PC me kabllo konsole në portën e konsolës së switch-it. Konfiguroni softuerin e emulimit të terminalit për t'u lidhur me switch-in.
Hapi 2. Shkëputni kabllon e rrymës nga switch-i.
Hapi 3. Rilidhni kordonin e rrymës me switch-in dhe, brënda 15 sekondave, shtypni dhe mbani të shtypur butonin Mode ndërsa LED i Sistemit është ende i ndezur jeshil.
Hapi 4. Vazhdoni të shtypni butonin Mode derisa LED i Sistemi të kthehet për pak kohë në qelibar dhe më pas në të gjelbër të fortë; pastaj lëshoni butonin Mode.
Hapi 5. Boot loader i switch-it: prompt shfaqet në softuerin e emulimit të terminalit në PC.
Type the help or ? në promptin e boot loader për të parë një listë të komandave të disponueshme.
By default, switch-i përpiqet të startojë automatikisht duke përdorur informacionin në variablin e mjedisit BOOT. Për të parë shtegun e ndryshores së mjedisit BOOT shtypni shtypni komandën **set**. Pastaj, filloni sistemin e skedarëve flash duke përdorur komandën **flash_init** për të parë skedarët aktualë në flash, siç tregohet në output.



Pasi të keni mbaruar inicializimin, mund të ekzekutoni komandën dir: për të parë direktoritë dhe skedarët në flash, siç tregohet në output.

Ekzekutoni komandën **BOOT=flash** për të ndryshuar rrugën e të variablit të mjedisit BOOT që switch-i përdor për të ngarkuar IOS të ri në flash. Për të verifikuar rrugën e re të variablit të

mjedisit BOOT, përdorni përsëri komandën set. Më në fund, për të ngarkuar IOS-in e ri shtypni komandën **boot** pa asnjë argument, siç tregohet në output.

Komandat e boot loader mbështesin fillimin e flash-it, formatimin e flash-it, instalimin e një IOS-i të ri, ndryshimin e variablit së mjedisit BOOT dhe rikuperimin e fjalëkalimeve të humbura ose të harruara.
Për të përgatitur një switch për qasje në menaxhim të largët, ai duhet të ketë një SVI të konfiguruar me një adresë IPv4 dhe subnet mask ose një adresë IPv6 dhe një prefiks për IPv6. SVI është një ndërfaqe virtuale, jo një port fizik i switch-it. Mbani në mend se për të menaxhuar kalimin nga një rrjet i largët, switch-i duhet të konfigurohet me një portë të paracaktuar. Kjo është shumë e ngjashme me konfigurimin e informacionit të adresës IP në pajisjet host. Switch-i është I konfiguruar që menaxhimi i tij të kontrollohet përmes VLAN 1. Të gjitha portat i janë caktuar VLAN 1 si parazgjedhje. Për qëllime të sigurisë, konsiderohet si një praktikë më e mirë për të përdorur një VLAN tjetër nga VLAN 1 për menaxhimin e VLAN, siç është VLAN 99 në shembull.

Hapi 1
Konfiguroni ndërfaqen e menaxhimit
Nga mënyra e konfigurimit të ndërfaqes VLAN, një adresë IPv4 dhe një subnet mask zbatohet në menaxhimin SVI të switch-it. Konkretisht, SVI VLAN 99 do të caktohet adresa 172.17.99.11/24 IPv4 dhe adresa 2001: db8: acad: 99 :: 1/64 IPv6 siç tregohet.
Shënim: SVI për VLAN 99 nuk do të shfaqet si "up / up" derisa të krijohet VLAN 99 dhe të ketë një pajisje të lidhur me një port switch-i të lidhur me VLAN 99.
Shënim: Switch-i mund të ketë nevojë të konfigurohet për IPv6. Për shembull, përpara se të konfiguroni adresimin IPv6 në një Cisco Catalyst 2960 që ekzekuton IOS version 15.0, do t'ju duhet të futni komandën globale të konfigurimit s **sdm prefer dual-ipv4-and-ipv6 default** dhe më pas të ristartoni switch-in.

Task	Komanda në IOS
Futja ne global configuration mode.	S1# configure terminal
Futja ne interface configuration mode për SVI.	S1(config)# interface vlan 99
Konfigurimi i adresës IPv4 të ndërfaqes së menaxhimit.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Konfigurimi i adresës IPv6 të ndërfaqes së menaxhimit.	S1(config-if)# ipv6 address 2001:db8:acad:99::11/64
Aktivizoni ndërfaqen e menaxhimit.	S1(config-if)# no shutdown
Rikthimi ne privileged EXEC mode.	S1(config-if)# end
Ruajtja e running config tek startup config.	S1# copy running-config startup-config

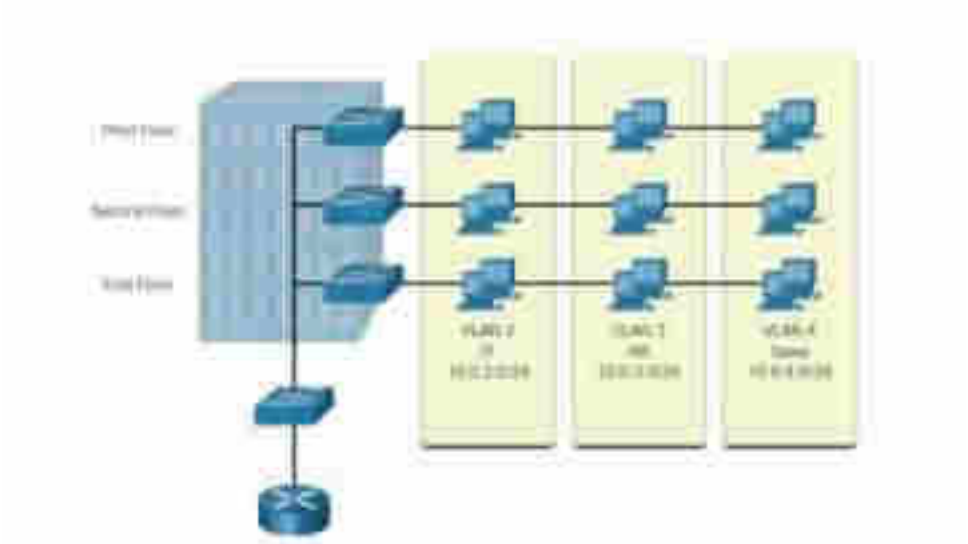
Hapi 2
Konfigurimi i Default Gateway
Switch-i duhet të konfigurohet me një portë të paracaktuar nëse do të menaxhohet në distancë nga rrjetet që nuk janë të lidhura drejtpërdrejt.
Shënim: Për shkak se, ai do të marrë informacionin e tij të paracaktuar të portës nga një mesazh i router advertisement (RA), switch-i nuk kërkon një portë të paracaktuar IPv6.

Task	Komanda në IOS
Hyrja global configuration mode.	S1# configure terminal
Konfigurimi i default gateway switch-in.	S1(config)# ip default-gateway 172.17.99.1
Rikthimi ne privileged EXEC mode.	S1(config)# end
Ruajtja e running config tek startup config.	S1# copy running-config startup-config

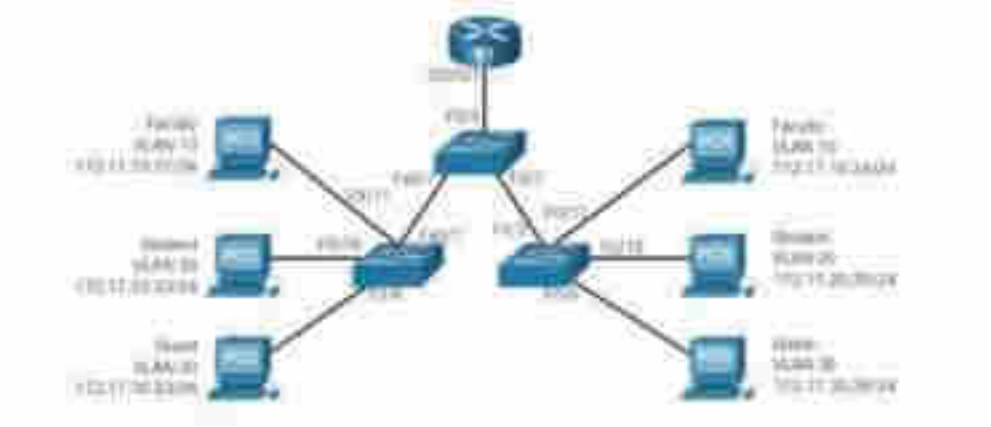
Hapi 3
Verifikimi i konfigurimeve
Komandat show ip interface brief dhe show ipv6 interface brief janë të dobishme për përcaktimin e statusit të ndërfaqeve fizike dhe virtuale. Output-i i treguar konfirmon që ndërfaqja VLAN 99 është konfiguruar me një adresë IPv4 dhe IPv6.
Shënim: Një adresë IP e aplikuar në SVI është vetëm për qasjen e menaxhimit të largët në switch; kjo nuk lejon kalimin në itinerarin e paketave të shtresës së 3-të.

Tema 30. LAN-et virtuale (VLAN-et). Protokolli VTP (Virtual Trunking Protocol)
Sigurisht që organizimi i rrjetit tuaj në rrjete më të vogla nuk është aq i thjeshtë sa ndarja e vidave dhe vënia e tyre në kavanoza. Por kjo do ta bëjë rrjetin tuaj më të lehtë për t'u menaxhuar. LAN-et Virtual (VLAN) sigurojnë segmentimin dhe fleksibilitetin organizativ në një rrjet switched. Një grup pajisjesh brënda një VLAN komunikojnë sikur secila pajisje të ishte e bashkangjitur në të njëjtën kabllo. VLAN-et bazohen në lidhje logjike, në vend të lidhjeve fizike.
Siç tregohet në figurë, VLAN në një rrjet switched u mundësojnë përdoruesve në departamente të ndryshme (d.m.th. IT, HR, dhe Sales) të lidhen me të njëjtin rrjet pavarësisht nga switch-i fizik që po përdoret ose vendndodhja në një LAN të kampusit.
Figura tregon një ndërtesë 3-katëshe me një switch në secilin kat. Switch-et janë të lidhur me një switch tjetër i cili është i lidhur me një router. Çdo kat ka shumë hostë të lidhur me të. Ekzistojnë tre VLAN që shtrihen në të tre katet dhe përmbajnë shumë presë në secilin kat.

VLAN-et janë: VLAN 2, IT, 10.0.2.0/24; VLAN 3, HR, 10.0.3.0/24; VLAN 4, Sales, 10.0.4.0/24.



VLAN lejojnë një administrator të segmentojë rrjetet bazuar në faktorë të tillë si funksioni, ekipi ose aplikacioni, pa marrë parasysh vendndodhjen fizike të përdoruesve ose pajisjeve. Çdo VLAN konsiderohet si një rrjet i veçantë logjik. Pajisjet brënda një VLAN veprojnë sikur të jenë në rrjetin e tyre të pavarur, edhe nëse ndajnë një infrastrukturë të përbashkët me VLAN-të e tjera. Çdo port switch-i mund të jetë i një VLAN.
Paketat unicast, broadcast dhe multicast përcillen dhe përmbyten (flooded) vetëm për t'i dhënë fund pajisjeve brënda VLAN ku burojnë paketat. Paketat e destinuara për pajisjet që nuk i përkasin VLAN duhet të përcillen përmes një pajisje që mbështet rutimin.
Nën-rrjeta të shumta IP mund të ekzistojnë në një rrjet switched, pa përdorimin e shumë VLAN-eve. Sidoqoftë, pajisjet do të jenë në të njëjtin fushë të transmetimit të Shtresës 2. Kjo do të thotë që çdo transmetim i Shtresës 2, siç është një kërkesë ARP, do të merret nga të gjitha pajisjet në rrjetin e ndërruar, madje edhe nga ato që nuk synojnë të marrin transmetimin.
Një VLAN krijon një domen logjik të transmetimit që mund të përfshijë segmente të shumta LAN fizike. VLAN përmirësojnë performancën e rrjetit duke ndarë domenet e mëdha të transmetimit në ato më të vogla. Nëse një pajisje në një VLAN dërgon një frame Ethernet të transmetuar, të gjitha pajisjet në VLAN marrin frame-in, por pajisjet në VLAN të tjera jo.
Duke përdorur VLAN, administratorët e rrjetit mund të zbatojnë politikat e aksesimit dhe të sigurisë sipas grupimeve specifike të përdoruesve. Secila portë e switch-it mund t'i caktohet vetëm një VLAN (përveç një porte të lidhur me një telefon IP ose me një switch tjetër).
Çdo VLAN në një rrjet switched i korrespondon një rrjeti IP. Prandaj, dizajni VLAN duhet të marrë në konsideratë zbatimin e një skeme hierarkike të adresimit të rrjetit. Adresimi hierarkik i rrjetit do të thotë që numrat e rrjetit IP të zbatohen në segmentet e rrjetit ose VLAN në një mënyrë që merr në konsideratë rrjetin në tërësi. Blloqet e adresave të rrjetit ngjitur rezervohen dhe konfigurohen në pajisjet në një zonë specifike të rrjetit, siç tregohet në figurë.



VLAN përdoren për arsye të ndryshme në rrjetet moderne. Disa lloje VLAN përcaktohen nga klasat e trafikut. Llojet e tjera të VLAN përcaktohen nga funksioni specifik që ato shërbejnë.

Default VLAN

Default VLAN në një switch Cisco është VLAN 1. Prandaj, të gjitha portat e switch-it janë në VLAN 1 përveç nëse konfigurohet qartë që të jetë në një VLAN tjetër. By default, i gjithë trafiku i kontrollit të Shtresës 2 është i lidhur me VLAN 1.

Faktet e rëndësishme për të mbajtur mend rreth VLAN 1 përfshijnë sa vijon:

- Të gjitha portat janë caktuar në VLAN 1 si parazgjedhje.
- VLAN origjinal është VLAN 1 si parazgjedhje.
- Menaxhimi VLAN është VLAN 1 si parazgjedhje.
- VLAN 1 nuk mund të riemërtohet ose fshihet.

Për shembull, në output-in e show vlan brief, të gjitha portat janë caktuar aktualisht në VLAN të paracaktuar 1. Asnjë VLAN vendas nuk është caktuar në mënyrë të qartë dhe asnjë VLAN tjetër nuk është aktiv; prandaj, rrjeti është dizenjuar me VLAN vendas njësoj si menaxhimi VLAN. Ky konsiderohet si një rrezik i
sigurisë.

Data VLAN

Të dhënat VLAN janë VLAN-e të konfiguruara për të ndarë trafikun e krijuar nga përdoruesit. Ata cilësohen si VLAN të përdoruesve sepse ndajnë rrjetin në grupe përdoruesish ose pajisjesh. Një rrjet modern do të kishte shumë VLAN të të dhënave në varësi të kërkesave organizative.

Nativ VLAN

Trafiku i përdoruesit nga një VLAN duhet të etiketohet me ID-në e tij VLAN kur dërgohet në një switch tjetër. Portat e trunk-ut përdoren midis switch-eve për të mbështetur transmetimin e trafikut të etiketuar. Veçanërisht, një port trunk-u 802.1Q shton një tag prej 4-bajtësh në header-in e Ethernet frame për të identifikuar VLAN-it, së cilës i përket frame-i.
Një switch gjithashtu mund të duhet të dërgojë trafik të pa-taguar nëpër një lidhje trunk-u. Trafiku i pa-taguar gjenerohet nga një switch dhe mund të vijë gjithashtu nga pajisje Legacy. Porta 802.1Q vendos trafik të pa-taaguar në nativ VLAN.
Është një praktikë më e mirë për të konfiguruar këtë VLAN si një VLAN të papërdorur, i dallueshëm nga VLAN 1 dhe VLAN të tjerë. Në fakt, nuk është e pazakontë të dedikohet një VLAN fiks për të shërbyer rolin e native VLAN për të gjitha portat e trunk-ut në domen-in e ndërruar.

VLAN I menaxhimit

VLAN i menaxhimit është një e dhënë VLAN e konfiguruar posaçërisht për trafikun e menaxhimit të rrjetit duke përfshirë SSH, Telnet, HTTPS, HTTP dhe SNMP. By deafult, VLAN 1 është konfiguruar si VLAN menaxhimi në një switch të shtresës 2.

VLAN me zë

Nevojitet një VLAN i veçantë për të mbështetur Voice over IP (VoIP). Trafiku VoIP kërkon sa vijon:

• Bandwidth I garantuar për të siguruar cilësinë e zërit

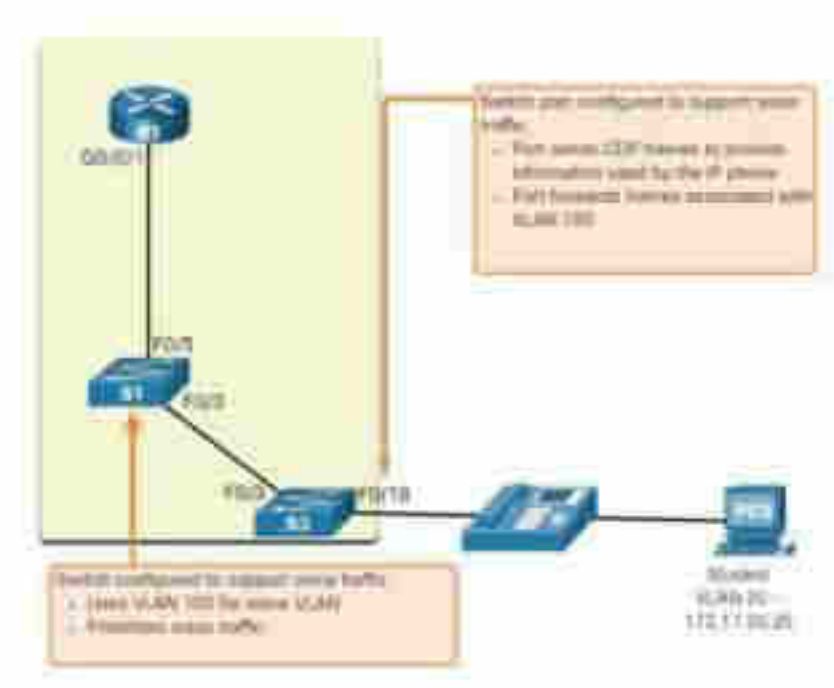
• Përparësia e transmetimit mbi llojet e tjera të trafikut të rrjetit

• Aftësi për t'u rout-uar nëpër zona të mbingarkuara në rrjet

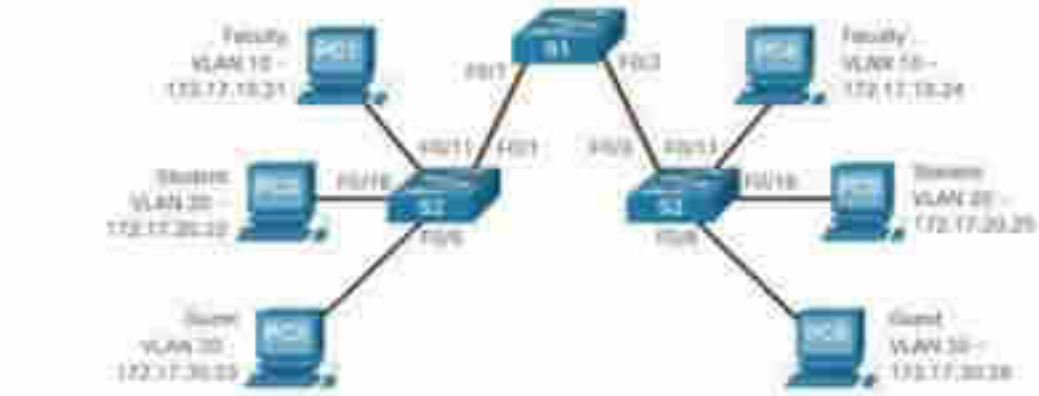
• Vonesë prej më pak se 150 ms në të gjithë rrjetin

Për të përmbushur këto kërkesa, i gjithë rrjeti duhet të projektohet për të mbështetur VoIP.

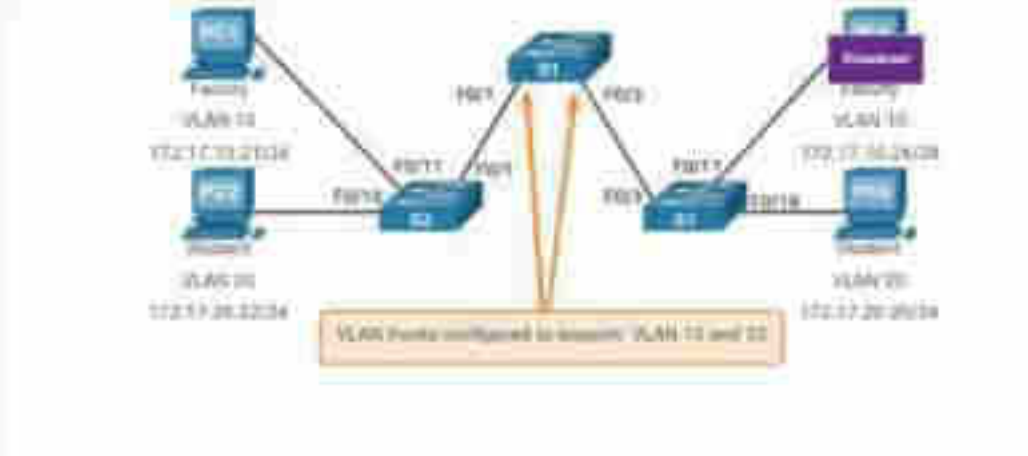
Në figurë, VLAN 150 është krijuar për të kryer trafik zëri. Kompjuteri student PC5 është i bashkangjitur në telefonin IP Cisco, dhe telefoni është i bashkangjitur tek switch S3. PC5 është në VLAN 20, e cila përdoret për të dhënat e studentëve.



Në VLAN nuk do të ishin shumë të dobishme VLAN trunk. Trunk-et VLAN lejojnë që i gjithë trafiku VLAN të përhapet midis switch-eve. Kjo mundëson që pajisjet e lidhura me switch-e të ndryshëm por në të njëjtën VLAN të komunikojnë pa kaluar një router.
Një trunk është një lidhje point-to-point midis dy pajisjeve të rrjetit që mbart më shumë se një VLAN. Një trunk VLAN shtrihet VLAN në të gjithë një rrjet të tërë. Cisco mbështet IEEE 802.1Q për koordinimin e trunk-eve në ndërfaqet e Fast Ethernet, Gigabit Ethernet dhe Gigabit10.
Ajo nuk i përket një VLAN specifik. Në vend të kësaj, ai është një kanal për shumë VLAN midis switch-eve dhe router-ave. Përdoret gjithashtu midis një pajisjeje rrjeti dhe serverit ose një pajisjeje tjetër që ka një NIC të përshtatshëm me aftësi 802.1Q. By defualt, në një switch Cisco Catalyst, të gjitha VLAN-et mbështeten në një port të trunk-ut.
Në figurë, lidhjet e theksuara midis switch-eve S1 dhe S2 dhe S1 dhe S3 janë konfiguruar për të transmetuar trafik që vjen nga VLANs 10, 20, 30 dhe 99 (d.m.th., VLAN vendas) në të gjithë rrjetin. Ky rrjet nuk mund të funksionojë pa VLAN Trunk.



VLAN shoqërohen dhe konfigurohen në portat individuale të switch-eve. Pajisjet e lidhura në ato porta nuk kanë asnjë koncept të VLAN. Sidoqoftë, këto pajisje janë konfiguruar me adresë IP dhe janë anëtare të një rrjeti specifik IP. Kjo është ajo ku lidhja midis VLAN dhe rrjetit IP është e dukshme. Një VLAN është ekuivalent me një rrjet IP (ose nënrrjet). VLAN konfigurohen në switch, ndërsa adresimi IP është konfiguruar në pajisje.



Pajisjet e fakultetit janë caktuar në VLAN 10 dhe pajisjet e studentëve janë caktuar në VLAN 20. Kur një frame broadcast dërgohet nga kompjuteri i fakultetit, PC1, për te S2, switch-i e ridërgon atë frame vetëm në ato porta switch-i të konfiguruara për të suportuar VLAN 10. Portat që përbëjnë lidhjen midis switch-eve S2 dhe S1 (portat F0/1) dhe S1e S3 (portat F0/3) janë trunk dhe janë konfiguruar për të mbështetur të gjitha VLAN-et në rrjet.
Kur S1 merr frame-in broadcast në portën F0/1, S1 përcjell atë frame nga porta e vetme tjetër e konfiguruar për të mbështetur VLAN 10, që është porta F0/3. Kur S3 merr frame-in broadcast në portën F0/3, ajo përcjell atë frame transmetimi nga porta e vetme tjetër e konfiguruar për të mbështetur VLAN 10, e cila është porta F0/11. Frame-i broadcast arrin te kompjuteri tjetër i vetëm në rrjet i konfiguruar në VLAN 10, i cili është kompjuteri PC4.
Kur VLAN-et implementohen në një switch, transmetimi i trafikut unicast, multicast dhe broadcast nga një host në një VLAN të veçantë kufizohet në pajisjet që janë në atë VLAN.

Tani që keni konfiguruar dhe verifikuar VLAN, është koha të konfiguroni dhe verifikoni trunk-et VLAN. Një trunk VLAN është një lidhje e shtresës së 2-të midis dy switch-eve që mbart trafik për të gjithë VLAN (përveç nëse lista e lejuar VLAN kufizohet manualisht ose dinamikisht).

Për të mundësuar lidhjet e trunk-ut, konfiguroni portat e ndërlidhura me grupin e komandave të konfigurimit të ndërfaqes të treguar në
tabelë.

Task	IOS Command
Enter global configuration mode.	`Switch# configure terminal`
Enter interface configuration mode.	`Switch(config)# interface interface-id`
Set the port to permanent trunking mode.	`Switch(config-if)# switchport mode trunk`
Sets the native VLAN to something other than VLAN 1.	`Switch(config-if)# switchport trunk native vlan vlan-id`
Specify the list of VLANs to be allowed on the trunk link.	`Switch(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`Switch(config-if)# end`

Tema 31. Konfigurimi i VLAN-eve dhe routimi mes tyre

Switch-et e ndryshëm të Cisco Catalyst mbështesin numra të ndryshëm të VLANs. Numri i VLAN-ve të mbështetur është mjaft i madh për të përmbushur nevojat e shumicës së organizatave. Për shembull, switch-et e serive Catalyst 2960 dhe 3650 mbështesin mbi 4,000 VLAN. VLAN-et me range normal në këto switche numërohen nga 1 deri në 1,005.

Karakteristikat e VLAN-eve me range normal:

- Ato përdoren në të gjitha rrjetet e bizneseve dhe ndërmarrjeve të vogla dhe të mesme.
- Ata identifikohen nga një ID VLAN midis 1 dhe 1005.
- ID-të 1002 deri 1005 janë të rezervuara për teknologjitë e lashta të rrjetit (d.m.th., Token Ring dhe Fiber Distributed Data Interface).
- ID-të 1 dhe 1002 deri 1005 krijohen automatikisht dhe nuk mund të hiqen.
- Konfigurimet ruhen në memorjen flash të switch-it në një skedar të dhënash VLAN të quajtur vlan.dat.
- Kur konfigurohet, VLAN trunking protocol (VTP), ndihmon në sinkronizimin e bazës së të dhënave VLAN midis switch-eve.

Karakteristikat e VLAN-eve me range të zgjatur:

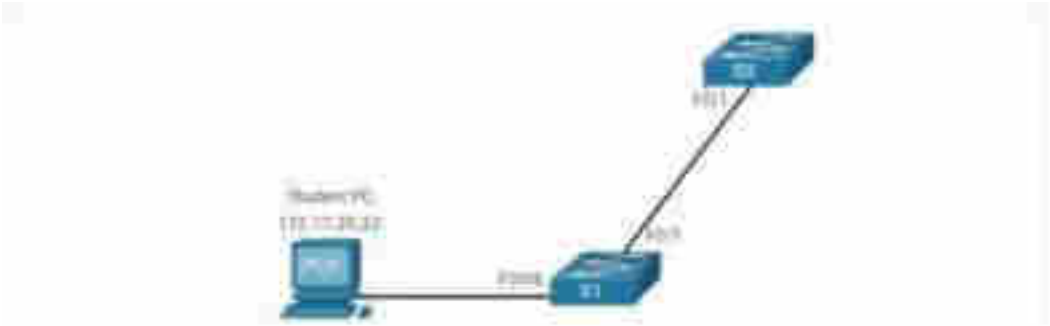
- Ato përdoren nga ofruesit e shërbimeve për të shërbyer klientë të shumtë dhe nga ndërmarrjet globale mjaft të mëdha që kanë nevojë për ID të VLAN me gamë të gjerë.
- Ata identifikohen nga një ID VLAN midis 1006 dhe 4094.
- Konfigurimet ruhen, by default, në konfigurimin e ekzekutimit.
- Ata suportojnë më pak karakteristika VLAN sesa VLAN me range normal.

Kur konfiguroni VLAN me range normal, detajet e konfigurimit ruhen në memorjen flash të switch-it në një skedar të quajtur vlan.dat. Memoria flash është e vazhdueshme dhe nuk kërkon komandën Copy running-config startup-config. Sidoqoftë, për shkak se detajet e tjera shpesh konfigurohen në një switch Cisco në të njëjtën kohë kur krijohen VLAN, është praktikë e mirë të ruani ndryshimet e konfigurimit që funksionojnë në konfigurimin e fillimit (startup config).

Tabela tregon sintaksën e komandës Cisco IOS që përdoret për të shtuar një VLAN në një switch dhe për t'i dhënë asaj një emër. Emërtimi i secilit VLAN konsiderohet si një praktikë më e mirë në konfigurimin e switch-it.

Task	IOS Command
Enter global configuration mode.	Switch# configure terminal
Create a VLAN and assign an ID number.	Switch(config)# vlan vlan-id
Specify a unique name to identify the VLAN.	Switch(config-vlan)# name vlan-name
Return to the privileged EXEC mode.	Switch(config-vlan)# end

Në topologji, kompjuteri student (PC2) nuk është shoqëruar ende me një VLAN, por ka një adresë IP prej 172.17.20.22, e cila i përket VLAN 20.

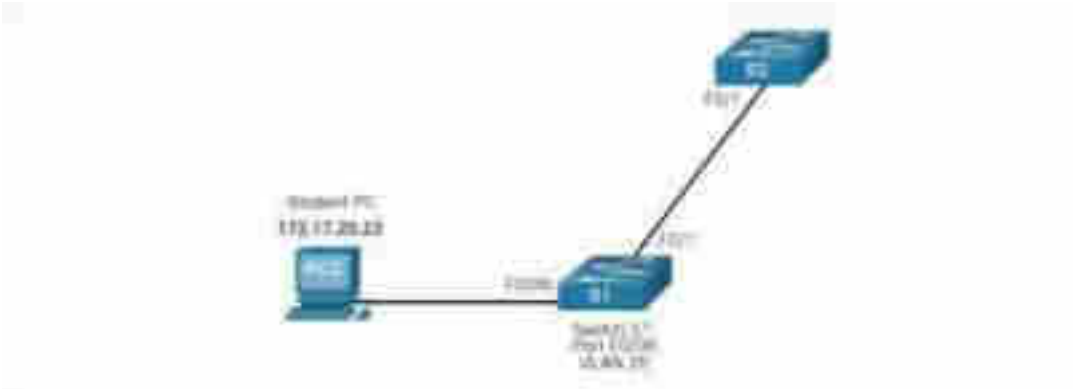


```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Pas krijimit të një VLAN, hapi tjetër është caktimi i portave në VLAN.

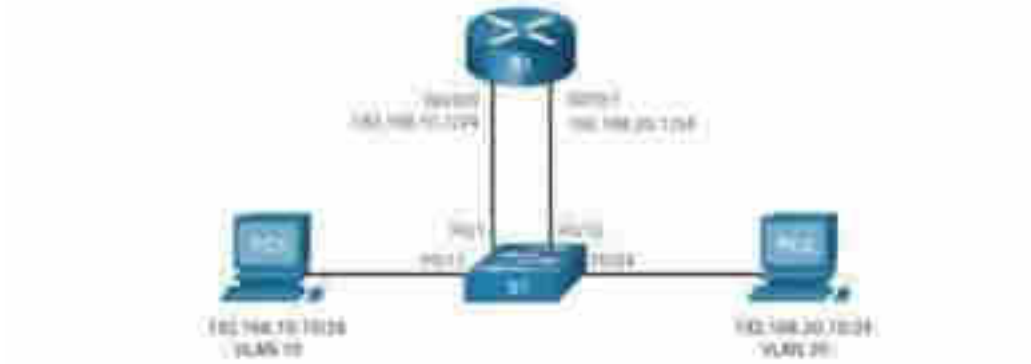
Task	IOS Command
Enter global configuration mode.	Switch# configure terminal
Enter interface configuration mode.	Switch(config)# interface interface-id
Set the port to access mode.	Switch(config-if)# switchport mode access
Assign the port to a VLAN.	Switch(config-if)# switchport access vlan vlan-id
Return to the privileged EXEC mode.	Switch(config-if)# end

Tabela tregon sintaksën për përcaktimin e një porte që të jetë një portë hyrjeje dhe caktimin e tij në një VLAN. Komanda e aksesit në mënyrën switchport është opsionale, por rekomandohet fuqimisht si një praktikë më e mirë e sigurisë. Me këtë komandë, ndërfaqja ndryshon në mënyrën hyrjes e kontrolluar. Modaliteti i hyrjes tregon që porta i përket një VLAN të vetëm dhe nuk do të negociojë për t'u bërë një lidhje trungu.



Në figurë, porta F0 / 6 në switch-in S1 është konfiguruar si një port hyrjeje dhe i është caktuar VLAN 20. Çdo pajisje e lidhur me atë portë do të shoqërohet me VLAN 20. Prandaj, në shembullin tonë, PC2 është në VLAN 20.

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```



VLAN janë konfiguruar në portën e switch-it dhe jo në pajisjen fundore. PC2 është konfiguruar me një adresë IPv4 dhe subnet mask që shoqërohet me VLAN, e cila është konfiguruar në portën e switch-it. Në këtë shembull, është VLAN 20. Kur VLAN 20 konfigurohet në swith-e të tjerë, administratori i rrjetit duhet të konfigurojë kompjuterat e tjerë studentë që të jenë në të njëjtën nënrrjet me PC2 (172.17.20.0/24).

Komanda **no vlan vlan-id** e konfigurimit global përdoret për të hequr një VLAN nga skedari i switch-it vlan.dat.

Kujdes: Para se të fshini një VLAN, caktoni të gjitha portat anëtare në një VLAN tjetër së pari. Çdo port që nuk zhvendoset në një VLAN aktiv nuk është në gjendje të komunikojë me hostet e tjerë pasi të jetë fshirë VLAN dhe derisa të caktohen në një VLAN aktiv.

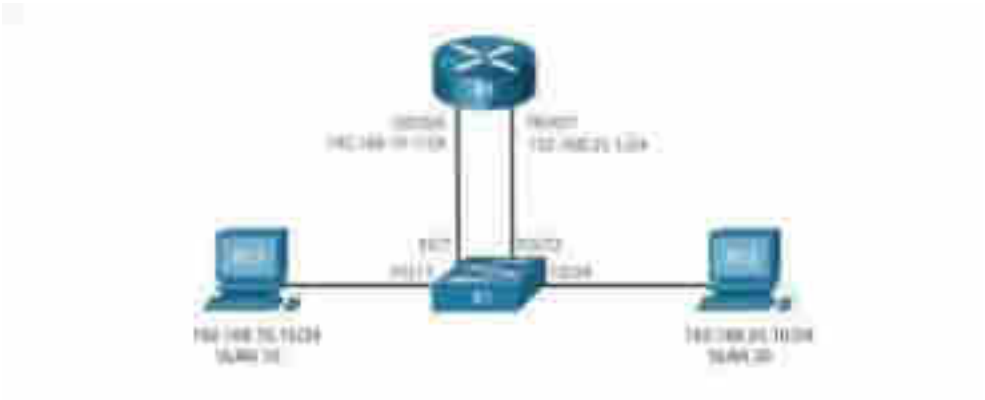
I gjithë skedari vlan.dat mund të fshihet duke përdorur delete flash:vlan.dat privileged EXEC mode. Versioni i shkurtuar i komandës (delete vlan.dat) mund të përdoret nëse skedari vlan.dat nuk është zhvendosur nga vendndodhja e tij e paracaktuar. Pas lëshimit të kësaj komande dhe ringarkimit të switch-it, asnjë VLAN i konfiguruar më parë nuk është më i pranishëm. Kjo në mënyrë efektive vendos kalimin në gjendjen e tij të paracaktuar të fabrikës në lidhje me konfigurimet VLAN.

Ekzistojnë tre mundësi rutimi ndër-VLAN:

• Legacy Inter-VLAN routing - Kjo është një zgjidhje Legacy. Nuk shkallëzohet mirë.
• Router-on-a-Stick - Kjo është një zgjidhje e pranueshme për një rrjet të vogël dhe të mesëm.
• Layer 3 switch using switched virtual interfaces (SVIs) - Kjo është zgjidhja më e shkallëzuar për organizatat e mesme në të mëdha.

Zgjidhja e parë e rutimit ndër-VLAN mbështetet në përdorimin e një router me ndërfaqe të shumta Ethernet. Çdo ndërfaqe e routerit ishte e lidhur me një portë switch-i në VLAN të ndryshme. Ndërfaqet e routerit shërbyen si porta të paracaktuara për hostet lokalë në nën-rrjetin VLAN.

Për shembull, referuar topologjisë ku R1 ka dy ndërfaqe të lidhura për të kaluar S1.



MAC Address table for S1

Port	MAC Address	VLAN
F0/1	R1 G0/0/0 MAC	10
F0/11	PC1 MAC	10
F0/12	R1 G0/0/1 MAC	20
F0/24	PC2 MAC	20