UNIVERSITETI “ISA BOLETINI” MITROVICË

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

Mentori:
Asist. Agon Bajgora, PhD(c)

Kandidati:
Eltrin Kadriu

Mitrovicë, Korrik 2026

UNIVERSITETI “ISA BOLETINI” MITROVICË

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

PROJEKTIMI DHE IMPLEMENTIMI I NJË RRJETI TË SIGURT SHUMË-DEPARTAMENTAL TË NDËRMARRJES ME REDUNDANCË

Mentori:
Asist. Agon Bajgora, PhD(c)

Kandidati:
Eltrin Kadriu

Mitrovicë, Korrik 2026

UNIVERSITY “ISA BOLETINI” MITROVICË

FACULTY OF MECHANICAL AND COMPUTER ENGINEERING DEPARTMENT: ENGINEERING INFORMATICS

DIPLOMA THESIS

DESIGN AND IMPLEMENTATION OF A SECURE MULTI-DEPARTMENTAL ENTERPRISE NETWORK WITH REDUNDANCY

Mentor:

Asist. Agon Bajgora, PhD(c)

Candidate:

Eltrin Kadriu

Mitrovicë, July 2026

DEKLARATA E ORIGJINALITETIT

Ky punim diplome i nivelit bachelor është punë origjinale e imja, e hartuar duke respektuar autorësinë e çdo burimi të informacionit dhe rregullat për një punim të mirëfilltë shkencor. Punimi nuk është dorëzuar, në tërësi ose pjesërisht, për fitimin e ndonjë grade në këtë apo në ndonjë universitet tjetër.

Sipas njohurive të mia, punimi nuk përmban material të botuar ose të shkruar nga ndonjë person tjetër, përveç rasteve të cituara dhe të deklaruara në tekst.

Gjithashtu, deklaroj se gjatë hartimit të punimit kam respektuar rregullat etike të punës shkencore dhe akademike të UIBM-së.

FALËNDERIME

Me frymëzimin që vjen nga fjala e parë e shpallur në Kur'an, "Lexo" (Iqra), e cila përçon rëndësinë e diturisë dhe kërkimit të saj, dua të shpreh mirënjohjen time të thellë ndaj të gjithë atyre që kanë qenë pjesë e këtij udhëtimi drejt dijes.

Së pari, të gjitha falënderimet dhe lavdimet i takojnë Zotit të Plotfuqishëm, i cili më ka dhënë fuqi, durim dhe dritë për të kaluar çdo pengesë dhe për të arritur këtë moment. Pa bekimin dhe udhëzimin e Tij, asgjë nuk do të ishte e mundur.

Gjithashtu, falënderoj përzemërsisht mentorin tim, Asist. Agon Bajgora, PhD(c), për mbështetjen e palodhshme dhe këshillat e çmuara që më kanë ndihmuar të realizoj këtë punim diplome. Përkushtimi dhe ekspertiza e tij kanë qenë udhërrëfyes i domosdoshëm në këtë proces.

Një mirënjohje e pakufishme i drejtohet familjes sime, shtyllës sime të jetës, që gjithmonë më kanë ofruar dashuri, mbështetje dhe kurajo në çdo hap të rrugëtimit tim. Fjalët nuk mjaftojnë për të shprehur sa shumë ka vlejtur mbështetja e tyre.

Së fundmi, falënderoj miqtë dhe kolegët e mi që përmes inkurajimeve të tyre dhe ndihmës së sinqertë, më kanë ndihmuar të përballoj sfidat e këtij udhëtimi.

ABSTRAKT

Rrjetet e ndërmarrjeve janë thelbësore për të siguruar komunikim të sigurt, ndarje efikase të burimeve dhe akses të besueshëm në shërbimet organizative në shumë departamente. Ky studim paraqet projektimin dhe zbatimin e një rrjeti të sigurt shumë-departamental për një ndërmarrje, me theks në siguri, redundancë dhe disponueshmëri të lartë. Arkitektura e propozuar ndan departamentet duke përdorur Rrjete Virtuale Lokale (VLAN), duke mundësuar menaxhim efikas të trafikut dhe siguri të përmirësuar të rrjetit. Politikat e firewall-it dhe mekanizmat e kontrollit të aksesit zbatohen për të mbrojtur burimet e brendshme nga aksesi i paautorizuar.

Për të arritur funksionim të vazhdueshëm, redundanca përfshihet përmes shtigjeve të shumta të rrjetit dhe mekanizmave të redundancës së gateway-t. Rrjeti përdor Open Shortest Path First (OSPF) për rrugëtim dinamik, Hot Standby Router Protocol (HSRP) për redundancën e gateway-t dhe Spanning Tree Protocol (STP) për të eliminuar sythet e Shtresës 2 dhe për të optimizuar shtigjet e ndërrimit. Rrjeti i plotë zbatohet dhe testohet brenda një mjedisi simulimi duke përdorur pajisje rrjeti të nivelit të ndërmarrjes, duke përfshirë routerë, switch-e, serverë dhe kompjuterë klientë.

Konfigurimet dhe skenarët e testimit u përdorën për të verifikuar lidhshmërinë, konvergjencën pas dështimeve dhe rikuperimin gjatë ndërprerjeve të simuluara të lidhjeve dhe pajisjeve. Rezultatet, të dokumentuara me daljet origjinale të Cisco Packet Tracer-it, konfirmuan funksionimin e segmentimit me VLAN, zbatimin e politikave ACL, kalimin e gateway-t virtual përmes HSRP, rikonvergjencën e OSPF-së dhe kalimin e rrugës së parazgjedhur te routeri rezervë. Dizajni i propozuar tregon se integrimi i segmentimit të rrjetit, protokolleve të rrugëzimit, teknologjive të redundancës dhe mekanizmave të sigurisë me shtresa mund të prodhojë një rrjet ndërmarrjeje elastik dhe të shkallëzueshëm. Ai ofron një kornizë praktike për organizatat që kërkojnë të përmirësojnë vazhdimësinë operacionale, të rrisin sigurinë kibernetike dhe të mbështesin zgjerimin e ardhshëm të rrjetit, duke ruajtur nivele të larta besueshmërie dhe performance.

Fjalë kyçe: rrjet ndërmarrjeje, siguri rrjeti, VLAN, OSPF, redundancë.

ABSTRACT

Enterprise networks are essential for ensuring secure communication, efficient resource allocation, and reliable access to organizational services across multiple departments. This study presents the design and implementation of a secure multi-departmental enterprise network that emphasizes security, redundancy, and high availability. The proposed architecture separates departments using Virtual Local Area Networks (VLANs), enabling efficient traffic management and improved network security. Firewall policies and access control mechanisms are implemented to protect internal resources from unauthorized access. To achieve continuous operation, redundancy is incorporated through multiple network paths and gateway redundancy mechanisms. The network uses Open Shortest Path First (OSPF) for dynamic routing, Hot Standby Router Protocol (HSRP) for default-gateway redundancy, and Spanning Tree Protocol (STP) to eliminate Layer 2 loops and optimize switching paths. The complete network is implemented and tested within a simulation environment using enterprise network equipment, including routers, switches, servers, and client computers.

The configurations and test scenarios were used to verify connectivity, convergence after failures, and recovery during simulated link and device outages. The results, documented with original Cisco Packet Tracer outputs, confirmed VLAN segmentation, ACL enforcement, HSRP gateway failover, OSPF reconvergence, and the transition of the default route to the backup edge router. The proposed design demonstrates that integrating network segmentation, routing protocols, redundancy technologies, and layered security mechanisms can produce a resilient and scalable enterprise network.

Keywords: Enterprise network, network security, VLAN, OSPF, redundancy.

Tabela e përmbajtjes

LISTA E FIGURAVE

LISTA E TABELAVE

LISTA E SHKURTESAVE

ACL	Lista e Kontrollit të Aksesit	Access Control List
DHCP	Protokolli i Konfigurimit Dinamik të Hosteve	Dynamic Host Configuration Protocol
DNS	Sistemi i Emrave të Domain-eve	Domain Name System
FTP	Protokolli i Transferimit të Skedarëve	File Transfer Protocol
GUI	Ndërfaqe Grafike e Përdoruesit	Graphical User Interface
HSRP	Protokolli i Routerit Rezervë Aktiv	Hot Standby Router Protocol
HTTP	Protokolli i Transferimit të Hipertekstit	Hypertext Transfer Protocol
HTTPS	Protokolli i Sigurt i Transferimit të Hipertekstit	Hypertext Transfer Protocol Secure
ICMP	Protokolli i Mesazheve të Kontrollit të Internetit	Internet Control Message Protocol
IP	Protokolli i Internetit	Internet Protocol
IPv4	Versioni 4 i Protokollit të Internetit	Internet Protocol Version 4
IPv6	Versioni 6 i Protokollit të Internetit	Internet Protocol Version 6
ISP	Ofruesi i Shërbimeve të Internetit	Internet Service Provider
LAN	Rrjet Lokal	Local Area Network
MAC	Adresa e Kontrollit të Aksesit në Media	Media Access Control Address
NAT	Përkthimi i Adresave të Rrjetit	Network Address Translation
OSPF	Protokolli i Rrugëzimit me Shtegun më të Shkurtër	Open Shortest Path First
PC	Kompjuter Personal	Personal Computer
QoS	Cilësia e Shërbimit	Quality of Service
SSH	Shell i Sigurt	Secure Shell
STP	Protokolli i Pemës Shtrirëse	Spanning Tree Protocol
TCP	Protokolli i Kontrollit të Transmetimit	Transmission Control Protocol
UDP	Protokolli i Datagramit të Përdoruesit	User Datagram Protocol
VLAN	Rrjet Lokal Virtual	Virtual Local Area Network
VoIP	Zëri përmes Protokollit të Internetit	Voice over Internet Protocol
WAN	Rrjet me Shtrirje të Gjerë	Wide Area Network

1. Hyrje – Çfarë është një rrjet ndërmarrjeje dhe pse është i rëndësishëm

Një rrjet ndërmarrjeje është infrastruktura logjike dhe fizike që mundëson komunikimin, shkëmbimin e të dhënave, aksesin në shërbime dhe koordinimin e proceseve organizative brenda një institucioni. Ai nuk përbëhet vetëm nga kabllo, routera, switche ose servera, por nga një sistem i integruar rregullash, protokollesh, politikash sigurie, mekanizmash administrimi dhe objektivash biznesi. Rrjeti i ndërmarrjes shërben si shtylla teknologjike mbi të cilën funksionojnë aplikacionet financiare, sistemet e burimeve njerëzore, komunikimi me klientët, platformat e prodhimit, sistemet e ruajtjes së dokumenteve dhe shërbimet cloud. Për këtë arsye, rëndësia e tij është strategjike, një ndërprerje në rrjet nuk është thjesht problem teknik, por ndërprerje e operacioneve, humbje produktiviteti, rritje e kostos dhe potencialisht cenim i besimit institucional. Rekhter et al. (1996) e trajtojnë ndërmarrjen si një njësi që administron në mënyrë autonome planin e saj të adresimit dhe komunikimin TCP/IP, gjë që tregon se rrjeti është i lidhur drejtpërdrejt me identitetin operacional të organizatës. Në mjediset moderne, rrjeti i ndërmarrjes ka kaluar nga modeli i thjeshtë i lidhjes së kompjuterëve në një sistem kompleks ku bashkëjetojnë përdorues të brendshëm, pajisje mobile, servera lokalë, shërbime cloud, aplikacione të jashtme, sisteme monitorimi dhe pajisje IoT. Kjo e bën arkitekturën më të ndërlikuar, sepse kufiri tradicional midis "brenda" dhe "jashtë" rrjetit nuk është më i mjaftueshëm për të përkufizuar sigurinë. Rose et al. (2020) theksojnë se arkitekturat zero trust zhvendosin fokusin nga perimetri statik te përdoruesi, pajisja, aplikacioni dhe burimi konkret që kërkohet të aksesohet. Në këtë kuptim, rrjeti i ndërmarrjes duhet të projektohet jo vetëm që të lidhë departamentet, por edhe të kontrollojë, verifikojë, monitorojë dhe kufizojë aksesin në mënyrë dinamike. Kjo qasje e bën rrjetin një mekanizëm të menaxhimit të riskut, jo vetëm një mjet transporti për paketat e të dhënave.

Rëndësia e një rrjeti ndërmarrjeje lidhet edhe me ndarjen funksionale të organizatës në departamente. Departamentet zakonisht kanë nevoja të ndryshme, pasi financa kërkon konfidencialitet të lartë, burimet njerëzore trajtojnë të dhëna personale, administrata ka nevojë për akses të gjerë në dokumente, departamenti teknik kërkon shërbime të menaxhimit dhe monitorimit, ndërsa mysafirët ose përdoruesit e jashtëm duhet të izolohen nga burimet kritike. Këto ndryshime e bëjnë të domosdoshme segmentimin e rrjetit në zona logjike, zakonisht përmes VLAN-eve, subnet-eve dhe politikave të kontrollit të aksesit. IEEE (2022) e vendos

802.1Q si standard qendror për bridged networks dhe virtual LAN, duke treguar se ndarja logjike në shtresën e dytë është një koncept i institucionalizuar në rrjetet moderne. Në praktikë, kjo do të thotë se rrjeti duhet të pasqyrojë strukturën organizative dhe njëkohësisht të kufizojë lëvizjen horizontale të trafikut të panevojshëm ose të rrezikshëm. Një aspekt tjetër i rëndësisë së rrjetit ndërmarrës është vazhdimësia e shërbimit. Organizatat nuk presin që rrjeti thjesht të funksionojë në kushte normale; ato presin që ai të vazhdojë të funksionojë edhe kur një link, pajisje, rrugë ose shërbim dështon. Në këtë pikë, koncepti i redundancës bëhet pjesë e projektimit bazë. Redundanca nuk është luks, por masë e domosdoshme për të ulur probabilitetin që një pikë e vetme dështimi të ndalojë gjithë sistemin. Protokollet si HSRP dhe OSPF lidhen me këtë nevojë: i pari krijon vazhdimësi të gateway-t të parazgjedhur, ndërsa i dyti mundëson llogaritjen dinamike të rrugëve alternative brenda një sistemi autonom (Li et al., 1998; Moy, 1998). Këto protokolle nuk kanë vlerë vetëm teknike; ato mbështesin objektivin e ndërmarrjes për qëndrueshmëri dhe shërbim të pandërprerë.

Siguria është një tjetër arsye pse rrjeti i ndërmarrjes duhet të projektohet me kujdes. Trafiku që lëviz në rrjet mund të përmbajë të dhëna financiare, dokumente kontraktuale, kredenciale, informacione personale dhe të dhëna operative. Nëse ky trafik nuk kontrollohet, monitorohet dhe kufizohet, rrjeti mund të shndërrohet nga mjet produktiviteti në sipërfaqe sulmi. Scarfone dhe Hoffman (2009) argumentojnë se firewall-et kontrollojnë rrjedhën e trafikut midis rrjeteve ose hosteve me nivele të ndryshme sigurie, duke i bërë ato elementë të domosdoshëm të politikës së sigurisë. Por firewall-i nuk është i mjaftueshëm në vetvete. Ai duhet të bashkëveprojë me VLAN, ACL, autentikim, menaxhim të log-eve, monitorim të ngjarjeve dhe politika të qarta për përdoruesit. Rrjeti i ndërmarrjes ka edhe vlerë organizative sepse standardizon mënyrën si punonjësit, aplikacionet dhe pajisjet marrin pjesë në proceset e punës. Pa një rrjet të strukturuar, departamentet krijojnë zgjidhje të përkohshme, përdorin lidhje të paautorizuara, ruajnë të dhëna në vende të ndryshme dhe rrisin mundësinë e gabimeve. Një arkitekturë e mirë rrjeti krijon disiplinë teknike: përcakton ku ndodhen serverët, kush i administron pajisjet, si regjistrohet trafiku, cilat shërbime janë kritike dhe si duhet të rikuperohen ato. Kjo e bën rrjetin pjesë të qeverisjes së teknologjisë së informacionit. Nga kjo perspektivë, rrjeti nuk është vetëm objekt i administratorëve, por instrument i menaxhimit institucional, sepse përmes tij zbatohen politika të konfidencialitetit, integritetit, disponueshmërisë dhe përgjegjshmërisë.

Po ashtu, rrjeti i ndërmarrjes duhet parë si platformë zhvillimi afatgjatë. Nëse infrastruktura fillestare projektohet pa standarde, çdo shërbim i ri shtohet me vështirësi dhe rrit

borxhin teknik të organizatës. Nëse projektohet me parime të qarta, rrjeti mund të mbështesë virtualizim, shërbime cloud, punë në distancë, telefoninë IP, sisteme sigurie dhe automatizim. Kjo tregon se rrjeti nuk është investim i mbyllur, por bazë mbi të cilën ndërtohen shërbimet e ardhshme digjitale. Pikërisht për këtë arsye, analiza e rrjetit duhet të nisë nga nevojat e institucionit dhe jo nga pajisjet që janë në dispozicion. Rrjeti ndërmarrës duhet të analizohet si kombinim i tre dimensioneve: funksionalitetit, sigurisë dhe qëndrueshmërisë. Funksionaliteti garanton që departamentet komunikojnë me njëra-tjetrën dhe me shërbimet që u nevojiten. Siguria garanton se komunikimi ndodh vetëm kur është i autorizuar dhe i arsyetuar. Qëndrueshmëria garanton se shërbimet vazhdojnë edhe në prani të dështimeve të pjesshme. Nëse njëri prej këtyre aspekteve mungon, rrjeti bëhet i paplotë. Një rrjet shumë funksional, por i pasigurt, krijon risk të lartë; një rrjet shumë i sigurt, por i ngurtë, pengon punën; një rrjet pa redundancë mund të ndalet nga një defekt i vetëm. Prandaj, tema e projektimit dhe implementimit të një rrjeti të sigurt shumë-departamental me redundancë është e rëndësishme sepse bashkon nevojat reale të organizatës me parimet teknike të inxhinierisë së rrjeteve.

2. Qëllimi

Qëllimi kryesor është ndërtimi i një modeli rrjeti që i shërben një organizate me disa departamente, duke garantuar komunikim të kontrolluar, siguri të brendshme, vazhdimësi shërbimi dhe mundësi zgjerimi. Ky qëllim nuk duhet kuptuar vetëm si krijim i një topologjie në një simulator, por si formulim i një zgjidhjeje të argumentuar, ku çdo vendim teknik lidhet me një kërkesë funksionale ose sigurie. Një rrjet i tillë duhet të lejojë që departamenti i financës të përdorë serverët financiarë, departamenti i burimeve njerëzore të menaxhojë të dhënat personale, administrata të aksesojë shërbime të përbashkëta, ndërsa përdoruesit mysafirë të kenë vetëm akses të kufizuar në internet. Kjo kërkon ndarje logjike, kontroll trafiku, politika të qarta dhe mekanizma që reduktojnë ndërprerjet.

Qëllimi ndahet në disa objektiva të ndërvarura. Objektivi i parë është segmentimi i rrjetit sipas funksioneve organizative. Segmentimi ul kompleksitetin administrativ dhe kufizon përhapjen e problemeve. Nëse një kompjuter i infektuar ndodhet në VLAN-in e mysafirëve, ai nuk duhet të ketë mundësi të skanojë serverët e financës ose pajisjet e menaxhimit. Kjo logjikë përputhet me parimin e minimizimit të aksesit, i cili është i afërt me qasjet moderne zero trust, ku asnjë përdorues ose pajisje nuk supozohet e besueshme vetëm sepse ndodhet brenda rrjetit (Rose et al., 2020). Pra, qëllimi nuk është thjesht ndarja për rend estetik, por ndërtimi i kufijve të kontrolluar midis zonave të ndryshme të besimit.

Objektivi i dytë është siguria e komunikimit ndërmjet departamenteve. Në një ndërmarrje, jo të gjitha departamentet duhet të komunikojnë lirshëm me njëra-tjetrën. Politikat e aksesit duhet të bazohen në nevojën për punë, jo në lehtësinë teknike. Për shembull, departamenti i marketingut mund të ketë nevojë të përdorë serverin e dokumenteve, por nuk ka arsye të aksesojë bazën e të dhënave të pagave. Në këtë pikë, firewall-et, listat e kontrollit të aksesit dhe filtrimi ndër-VLAN bëhen instrumente të domosdoshme. Scarfone dhe Hoffman (2009) e trajtojnë firewall-in si mekanizëm që kontrollon rrjedhën e trafikut ndërmjet zonave me qëndrime të ndryshme sigurie. Kjo do të thotë se firewall-i nuk është vetëm pajisje në skaj të internetit, por edhe komponent i kontrollit të brendshëm midis segmenteve me risk të ndryshëm.

Objektivi i tretë është redundanca dhe disponueshmëria. Një rrjet i sigurt por që bie shpesh nuk i përmbush nevojat e ndërmarrjes. Prandaj projekti duhet të përfshijë mekanizma që sigurojnë funksionim edhe në rast dështimi të një pajisjeje, një lidhjeje ose një rruge. Në shtresën e gateway-t, HSRP mundëson që disa routera të paraqiten për hostet si një router

virtual, duke ulur ndikimin e dështimit të routerit aktiv (Li et al., 1998). Në shtresën e routing-ut, OSPF ndihmon në zgjedhjen dinamike të rrugëve bazuar në një bazë të përbashkët të topologjisë (Moy, 1998). Në shtresën e switching-ut, STP ose variantet e tij parandalojnë loop-et dhe mundësojnë rikuperim të kontrolluar kur ka lidhje redundante.

Objektivi i katërt është menaxhueshmëria. Një rrjet i madh pa dokumentim, emërtim, plan adresimi dhe logjikë të qartë konfigurimi bëhet i vështirë për t'u mirëmbajtur. Për këtë arsye, qëllimi i projektit duhet të përfshijë hartimin e një plani të adresimit IP, përcaktimin e VLAN ID-ve, emërtimin e pajisjeve, ndarjen e roleve të serverëve, përcaktimin e interfejseve trunk dhe access, si dhe dokumentimin e rregullave të firewall-it. Rekhter et al. (1996) theksojnë rëndësinë e adresimit privat për rrjetet e brendshme, duke ofruar hapësira që mund të përdoren pa koordinim publik. Por përdorimi i adresave private nuk mjafton; ato duhet të organizohen në mënyrë të lexueshme, të shkallëzueshme dhe të lidhur me strukturën e departamenteve.

Objektivi i pestë është testueshmëria e zgjidhjes. Një rrjet i projektuar teorikisht duhet të verifikohet në një mjedis simulimi përpara se të konsiderohet i vlefshëm. Cisco Packet Tracer dhe GNS3 përdoren gjerësisht për të ndërtuar, testuar dhe analizuar topologji rrjeti në mjedise virtuale (Cisco Networking Academy, n.d.; GNS3, n.d.). Në kontekstin e këtij punimi, simulimi nuk është thjesht demonstrim vizual, por metodë për të provuar nëse VLAN-et janë izoluar, nëse routing-u funksionon, nëse HSRP bën failover, nëse STP shmang loop-et dhe nëse rregullat e sigurisë lejojnë vetëm trafikun e autorizuar.

Një objektiv plotësues është që rrjeti të jetë i zgjerueshëm. Zgjerueshmëria nënkupton që shtimi i një departamenti të ri, një serveri të ri ose një lidhjeje të re nuk duhet të kërkojë rindërtim të plotë të arkitekturës. Kjo arrihet përmes skemës së rregullt të adresimit, rezervimit të hapësirave IP, dokumentimit të VLAN-eve dhe përdorimit të protokolleve dinamike që pranojnë ndryshime të kontrolluara. Nëse rrjeti projektohet vetëm për nevojat minimale të momentit, ai mund të funksionojë në demonstrim, por bëhet pengesë kur organizata rritet. Prandaj qëllimi i projektit nuk është vetëm të ndërtojë një topologji që punon sot, por të paraqesë një model që mund të evoluojë pa humbur sigurinë dhe qartësinë.

Qëllimi i projektit përfshin edhe ndërtimin e një modeli të kuptueshëm për vendimmarrje. Një menaxher nuk ka nevojë të dijë çdo komandë konfigurimi, por duhet të kuptojë pse investohet në firewall, pse departamentet ndahen dhe pse blihen pajisje të dyfishta.

3. Struktura e rrjetit – Si ndahen departamentet dhe si lidhen mes tyre

Struktura e rrjetit është mënyra se si organizohen segmentet, pajisjet, lidhjet dhe shërbimet brenda ndërmarrjes. Në një rrjet shumë-departamental, struktura nuk mund të jetë e rastësishme, sepse ajo duhet të pasqyrojë logjikën e organizatës dhe të mbështesë sigurinë, performancën dhe administrimin. Një model i zakonshëm është ndarja në shtresa: access layer, ku lidhen përdoruesit fundorë; distribution layer, ku bëhet agregimi, filtrimi dhe routing-u ndërmjet VLAN-eve dhe core layer, ku sigurohet transport i shpejtë dhe i qëndrueshëm ndërmjet segmenteve kryesore. Edhe kur topologjia është e vogël dhe simulohet në Packet Tracer, ky model është i dobishëm sepse krijon qartësi funksionale. Shtresa access merret me lidhjen e hosteve, shtresa distribution me politikat dhe kufijtë, ndërsa core me shpejtësinë dhe redundancën. Ndarja e departamenteve zakonisht realizohet përmes VLAN-eve dhe subnet-eve të veçanta. Për shembull, mund të krijohet VLAN 10 për Administratën, VLAN 20 për Financën, VLAN 30 për Burimet Njerëzore, VLAN 40 për IT, VLAN 50 për Serverët, VLAN 60 për Menaxhimin dhe VLAN 70 për Mysafirët. Kjo ndarje krijon izolim logjik edhe kur pajisjet përdorin të njëjtën infrastrukturë fizike switching. IEEE (2022) e trajton standardin 802.1Q si bazë për rrjetet e bridge-uara dhe VLAN-et, duke mundësuar identifikimin e trafikut sipas përkatësisë logjike. Në këtë mënyrë, rrjeti i ndërmarrjes nuk ka nevojë për kabllim të veçantë fizik për çdo departament; ai mund të përdorë të njëjtën infrastrukturë, por me ndarje të kontrolluar në nivel frame-sh.

Lidhja ndërmjet departamenteve duhet të realizohet në mënyrë të kontrolluar përmes routing-ut ndër-VLAN. Nëse VLAN-et mbeten plotësisht të izoluara, departamentet nuk mund të përdorin shërbime të përbashkëta, si serveri i dokumenteve, DNS, DHCP ose aplikacionet e brendshme. Nëse, nga ana tjetër, routing-u ndër-VLAN lejon gjithçka, atëherë segmentimi humb vlerën e tij të sigurisë. Prandaj, struktura optimale kërkon që çdo VLAN të ketë subnet-in e vet, gateway-n e vet virtual ose fizik dhe politika të qarta për trafikun e lejuar. Për shembull, VLAN-i i Financës mund të lejohet të komunikojë vetëm me serverin financiar dhe printera të caktuar, ndërsa VLAN-i i Mysafirëve duhet të lejohet vetëm drejt internetit, pa akses në rrjetin e brendshëm. Kjo filozofi e lidh strukturën me kontrollin e riskut. Planifikimi i adresimit IP është pjesë e pandashme e strukturës. Hapësirat private të RFC 1918, si 10.0.0.0/8, 172.16.0.0/12 dhe 192.168.0.0/16, përdoren gjerësisht për rrjetet e brendshme sepse nuk janë të rutueshme drejtpërdrejt në internet (Rekhter et al., 1996). Një organizatë mund të përdorë, për shembull, 10.10.0.0/16 dhe të ndajë subnet-e /24 për departamente të ndryshme: 10.10.10.0/24 për administratën, 10.10.20.0/24 për financën, 10.10.30.0/24 për burimet

njerëzore dhe kështu me radhë. Një plan i tillë e bën rrjetin të lexueshëm dhe ndihmon në zbatimin e politikave të firewall-it. Kur një administrator sheh trafik nga 10.10.20.0/24, ai e kupton menjëherë se burimi lidhet me departamentin e financës.

Struktura e rrjetit duhet të përfshijë edhe zonën e serverëve. Serverët nuk duhet të vendosen pa dallim në të njëjtin segment me përdoruesit e zakonshëm, sepse ata përfaqësojnë burime kritike. Një VLAN serverësh lejon aplikimin e politikave të veçanta: vetëm porta dhe protokolle të nevojshme hapen nga departamentet drejt serverëve, ndërsa aksesi administrativ kufizohet te VLAN-i i IT-së ose menaxhimit. Kjo përputhet me parimin e minimizimit të privilegjeve dhe me logjikën e zero trust, ku aksesi jepet në mënyrë të kontrolluar sipas identitetit, pajisjes dhe nevojës konkrete (Rose et al., 2020). Përveç kësaj, serverët mund të vendosen pas firewall-it të brendshëm ose në një segment të ndërmjetëm, sidomos kur ofrojnë shërbime që duhet të aksesohen edhe nga jashtë. Në aspektin fizik, struktura duhet të shmangë varësinë nga një pajisje e vetme. Switchet access duhet të kenë lidhje redundante drejt distribution switch-eve; routerat ose firewall-et kryesorë duhet të punojnë në çift; lidhjet trunk duhet të dokumentohen; dhe protokollet e shtresës së dytë duhet të parandalojnë loop-et. STP është i rëndësishëm pikërisht sepse redundanca fizike në Ethernet mund të krijojë loop-e nëse nuk menaxhohet. IEEE 802.1Q-2022 përfshin mekanizma të bridge-uara dhe lidhet me menaxhimin e rrjeteve që duhet të ruajnë funksionimin edhe gjatë rikonfigurimit ose dështimit të komponentëve (IEEE, 2022). Kjo tregon se struktura e rrjetit nuk është vetëm hartë lidhjesh, por edhe mekanizëm kontrolli për sjelljen e trafikut në kushte normale dhe anormale.

Një strukturë e pjekur duhet të përfshijë edhe zonën e menaxhimit dhe zonën e mysafirëve si segmente të dallueshme. VLAN-i i menaxhimit përdoret për administrimin e pajisjeve të rrjetit, prandaj duhet të jetë i aksesueshëm vetëm nga stafi i autorizuar i IT-së. Nëse administrimi i switch-eve dhe routerave lejohet nga çdo departament, kompromet imi i një kompjuteri të zakonshëm mund të shndërrohet në kompromet im të infrastrukturës. Nga ana tjetër, rrjeti i mysafirëve duhet të jetë i izoluar nga burimet e brendshme dhe të ketë vetëm dalje të kontrolluar drejt internetit. Këto dy segmente tregojnë se struktura e rrjetit nuk ndjek vetëm organigramën e ndërmarrjes, por edhe nivelet e besimit. Sa më i ulët niveli i besimit, aq më i kufizuar duhet të jetë komunikimi. Struktura duhet të marrë parasysh edhe trafikun e shërbimeve të përbashkëta. DNS, DHCP, autentikimi, serverët e dokumenteve dhe sistemet e backup-it përdoren nga disa departamente, prandaj nuk mund të izolohen në mënyrë absolute. Zgjidhja nuk është hapja e plotë e rrjetit, por krijimi i rrugëve të kontrolluara drejt këtyre shërbimeve. Kjo kërkon që çdo shërbim i përbashkët të ketë vend të

qartë në arkitekturë dhe rregulla të veçanta aksesi. Në këtë mënyrë, struktura mbështet bashkëpunimin pa sakrifikuar ndarjen dhe sigurinë. Një strukturë e mirë rrjeti duhet të jetë e dokumentuar, e shkallëzueshme dhe e auditueshme. Dokumentimi përfshin topologjinë logjike, topologjinë fizike, tabelën e VLAN-eve, planin e adresimit, rolet e pajisjeve, trunk-et, gateway-t, politikat ndër-VLAN dhe pikat e redundancës. Shkallëzueshmëria nënkupton që mund të shtohen departamente të reja pa prishur logjikën ekzistuese. Auditueshmëria nënkupton që një palë e tretë mund të kuptojë pse një trafik lejohet ose bllokohet. Në këtë kuptim, struktura e rrjetit është themeli mbi të cilin ndërtohen siguria, protokollet, testimi dhe rezultatet.

4. Siguria – Përdorimi i firewall, VLAN dhe rregulla për akses të sigurt

Siguria në një rrjet ndërmarrjeje duhet kuptuar si sistem kontrollesh të shtresuara dhe jo si një pajisje e vetme. Një firewall në hyrje të rrjetit është i rëndësishëm, por nuk mjafton nëse brenda rrjetit të gjitha departamentet komunikojnë pa kufizim. Po ashtu, VLAN-et krijojnë ndarje logjike, por nuk garantojnë siguri nëse routing-u ndërmjet tyre lejohet pa rregulla. Për këtë arsye, siguria duhet të projektohet sipas parimit defense in depth, ku secila shtresë ul mundësinë që një dobësi e vetme të kompromentojë të gjithë sistemin. Scarfone dhe Hoffman (2009) e përshkruajnë firewall-in si mjet që kontrollon rrjedhën e trafikut midis rrjeteve ose hosteve me postura të ndryshme sigurie. Në kontekst ndërmarrjeje, kjo përfshin filtrimin midis internetit dhe rrjetit të brendshëm, por edhe filtrimin midis departamenteve. VLAN-et janë baza e segmentimit logjik. Ato ndajnë broadcast domain-et dhe ulin ekspozimin e pajisjeve ndaj trafikut të panevojshëm. Në aspekt sigurie, VLAN-et reduktojnë mundësinë që një përdorues i një departamenti të ketë dukshmëri direkte mbi pajisjet e një departamenti tjetër. Megjithatë, është e rëndësishme të theksohet se VLAN-i nuk është firewall. Ai ndan trafikun në shtresën e dytë, por sapo aktivizohet routing-u ndër-VLAN, kontrolli i vërtetë varet nga ACL-të, firewall-i ose politikat e aksesit. IEEE (2022) standardizon mekanizmat e VLAN tagging për rrjetet e bridge-uara, por siguria praktike kërkon konfigurim të kujdesshëm: portat e përdoruesve duhet të jenë access ports, trunk-et duhet të lejohen vetëm aty ku nevojiten, VLAN-i default nuk duhet të përdoret për hoste, dhe VLAN-i i menaxhimit duhet të jetë i ndarë.

Firewall-i luan rol kyç në kontrollin e trafikut. Në një arkitekturë shumë-departamentale, firewall-i mund të vendoset në perimetër për të filtruar trafikun drejt internetit dhe në brendësi për të kontrolluar komunikimin mes VLAN-eve kritike. Politikat e firewall-it duhet të bazohen në parimin ‘deny by default’ dhe ‘allow by exception’. Kjo do të thotë se trafiku nuk lejohet përveç rasteve kur ekziston arsye e dokumentuar. Për shembull, departamenti i Burimeve Njerëzore mund të lejohet të përdorë serverin e bazës së të dhënave në një port specifik, por jo të hapë lidhje administrative SSH drejt serverëve. Kjo qasje redukton sipërfaqen e sulmit dhe bën më të lehtë auditimin. Scarfone dhe Hoffman (2009) theksojnë se firewall-et duhet të planifikohen, testohen, vendosen dhe menaxhohen sipas politikave të qarta, jo të konfigurohen në mënyrë spontane.

Rregullat e aksesit duhet të ndërtohen mbi identifikimin e roleve. Në rrjetin e një ndërmarrjeje, përdoruesit nuk janë të barabartë nga pikëpamja e privilegjeve. Administratorët e IT-së kanë nevojë për akses në pajisjet e rrjetit, por ky akses duhet të vijë vetëm nga një segment menaxhimi, me autentikim të fortë dhe logim. Përdoruesit e zakonshëm kanë nevojë për aplikacione biznesi, email, dokumente dhe internet, por jo për akses në konfigurimet e pajisjeve. Mysafirët duhet të kufizohen rreptësisht. Kjo filozofi është në përputhje me zero trust, ku besimi nuk jepet nga vendndodhja në rrjet, por verifikohet për çdo kërkesë dhe burim (Rose et al., 2020). Në praktikë, kjo mund të përkthehet në ACL, 802.1X, lista lejuese aplikacionesh, VPN me autentikim shumëfaktorësh dhe monitorim të vazhdueshëm. Një çështje e rëndësishme është mbrojtja e planeve të menaxhimit dhe kontrollit. Shpesh rrjetet kompromethen jo vetëm nga trafiku i përdoruesve, por nga keqmenaxhimi i pajisjeve. Routerat, switchet, firewall-et dhe serverët duhet të kenë akses administrativ të kufizuar, kredenciale të forta, protokolle të sigurta si SSH në vend të Telnet, sinkronizim kohe përmes NTP, logging të centralizuar dhe backup të konfigurimeve. Menaxhimi duhet të kalojë përmes VLAN-it të dedikuar dhe jo nga çdo segment përdoruesish. Kjo e bën më të vështirë që një sulmues i vendosur në një kompjuter të zakonshëm të arrijë pajisjet kritike të infrastrukturës. Siguria e rrjetit nuk është vetëm mbrojtje e të dhënave, por edhe mbrojtje e vetë mekanizmave që kontrollojnë trafikun (Cisco, 2024b).

Siguria duhet të përfshijë edhe monitorimin dhe reagimin. Firewall-et dhe pajisjet e rrjetit duhet të gjenerojnë log-e që analizohen për anomali skanime portash, tentime të dështuara autentikimi, trafik të pazakontë midis VLAN-eve, rritje të papritur të bandwidth-it ose përdorim të protokolleve të ndaluara. Pa monitorim, rregullat e sigurisë mbeten statike dhe organizata nuk kupton nëse ato po funksionojnë. Në një mjedis akademik ose simulimi, kjo mund të paraqitet përmes testimit të ping, traceroute, aksesit të lejuar ose të bllokuar, dhe skenarëve ku një host nga VLAN-i i mysafirëve tenton të arrijë serverë të brendshëm. Në një mjedis real, monitorimi do të zgjerohej me SIEM, IDS/IPS dhe analiza të sjelljes. Politikat e sigurisë duhet të jenë të dokumentuara në gjuhë të kuptueshme përpara se të kthehen në rregulla teknike. Një problem i zakonshëm në rrjete është që konfigurimi bëhet burimi i vetëm i së vërtetës, ndërsa askush nuk e di pse një rregull ekziston. Kjo krijon rrezik gjatë mirëmbajtjes, sepse administratorët kanë frikë të heqin rregulla të vjetra ose shtojnë përjashtime të reja pa analizë. Një politikë e mirë përcakton burimin, destinacionin, shërbimin, arsyen, pronarin dhe kohën e rishikimit. Kjo qasje e kthen sigurinë nga reagim teknik në proces administrativ. Për

një rrjet shumë-departamental, dokumentimi i politikave është po aq i rëndësishëm sa konfigurimi, sepse provon se aksesi është dhënë për nevojë pune dhe jo për lehtësi.

Siguria duhet të përfshijë edhe aspektin njerëzor. Shumë incidente nuk ndodhin sepse mungon teknologjia, por sepse përdoruesit nuk kuptojnë kufijtë e aksesit, administratorët përdorin kredenciale të përbashkëta ose ndryshimet nuk miratohen formalisht. Një rrjet i projektuar mirë duhet të shoqërohet me politika përdorimi, ndarje përgjegjësish dhe procedura ndryshimi. Nëse një rregull firewall-i shtohet pa miratim, ai mund të dobësojë gjithë arkitekturën. Prandaj siguria teknike dhe qeverisja organizative janë të pandara. Firewall-i, VLAN-et dhe rregullat e aksesit duhet të funksionojnë si një sistem i vetëm. VLAN-i ndan, firewall-i kontrollon, ACL-ja specifikon, autentikimi verifikon, ndërsa monitorimi vërteton se politika po zbatohet. Pa këtë ndërveprim, rrjeti mund të jetë i organizuar, por jo i sigurt ose i sigurt në letër, por i dobët në zbatim. Siguria e një rrjeti shumë-departamental kërkon që çdo rrugë komunikimi të ketë arsye, çdo privilegj të ketë kufi dhe çdo shkelje të jetë e dukshme.

5. Redundanca – Si sigurohet që rrjeti të vazhdojë punën edhe në rast dështimi

Redundanca është aftësia e rrjetit për të ruajtur funksionimin kur një komponent dështon. Në një ndërmarrje, dështimi mund të ndodhë në disa nivele: kabllo e dëmtuar, switch i fikur, router i bllokuar, firewall joaktiv, energji e ndërprerë, gabim konfigurimi ose rrugë e humbur drejt një serveri. Një rrjet pa redundancë është i ekspozuar ndaj single point of failure, pra një pikë e vetme që mund të ndalojë gjithë shërbimin. Në aspekt teorik, redundanca nuk e eliminon dështimin; ajo e bën dështimin të përballueshëm. Qëllimi është që përdoruesit të vazhdojnë punën me ndërprerje minimale ose pa ndërprerje të dukshme, ndërsa infrastruktura kalon automatikisht në rrugë alternative. Redundanca duhet të projektohet në shtresa. Në shtresën fizike, kjo do të thotë lidhje të dyfishta midis switch-eve access dhe distribution, furnizim alternativ energjie për pajisjet kritike dhe ndarje fizike të rrugëve kur është e mundur. Në shtresën e dytë, redundanca kërkon kujdes sepse lidhjet e shumta në Ethernet mund të krijojnë loop-e, të cilat shkaktojnë broadcast storms dhe rrëzim të rrjetit. Për këtë arsye përdoret STP ose variante të tij, të cilat zgjedhin një topologji aktive pa loop dhe mbajnë lidhje rezervë që aktivizohen kur rruga kryesore dështon. Standardi IEEE 802.1Q lidhet me rrjetet e bridge-uara dhe me menaxhimin e rikonfigurimit pas dështimeve të komponentëve, duke treguar se redundanca dhe kontrolli i loop-eve janë pjesë e dizajnit formal të LAN-it (IEEE, 2022). Në shtresën e tretë, redundanca lidhet me routing-un dinamik. OSPF është një protokoll link-state që ndërton një bazë të përbashkët të topologjisë dhe llogarit rrugët më të shkurtra drejt destinacioneve (Moy, 1998). Në një rrjet ndërmarrjeje, OSPF mund të përdoret midis routerave ose switch-eve Layer 3 për të siguruar që nëse një link dështon, trafiku të kalojë në një rrugë tjetër të vlefshme. Vlera e OSPF nuk qëndron vetëm te funksionimi automatik; është edhe kontrolli i qartë i zonave, kostove, summarization-it dhe konvergjencës. Nëse një rrjet ka disa departamente dhe disa rrugë drejt serverëve ose internetit, routing-u statik bëhet i vështirë për mirëmbajtje. OSPF ofron fleksibilitet dhe reagim më të shpejtë ndaj ndryshimeve.

Redundanca e gateway-t është një element kritik për hostet. Edhe nëse rrjeti ka disa routera, kompjuterët zakonisht përdorin një default gateway. Nëse ai gateway dështon, hostet mund të humbasin komunikimin jashtë subnet-it edhe kur ekziston router tjetër funksional. HSRP e zgjidh këtë problem duke krijuar një router virtual që përfaqësohet nga një IP virtuale. Routeri aktiv përgjigjet për trafikun, ndërsa routeri standby merr rolin nëse aktiv dështon (Li et al., 1998). Kjo është shumë e rëndësishme për departamentet, sepse përdoruesit nuk kanë nevojë të ndryshojnë konfigurimin IP kur ndodh dështimi. Nga këndvështrimi i

tyre, gateway mbetet i njëjtë, ndërsa infrastruktura prapa tij ndryshon rolin automatikisht. Redundanca duhet të balancohet me kompleksitetin. Sa më shumë rrugë alternative dhe protokolle failover të shtohen, aq më shumë rritet nevoja për dokumentim, testim dhe monitorim. Një konfigurim HSRP pa tracking mund të mbajë aktiv routerin që ka humbur lidhjen drejt internetit, duke krijuar dështim të pjesshëm. Një konfigurim OSPF me kosto të gabuara mund të zgjedhë rrugë jo optimale. Një STP root bridge i vendosur rastësisht mund të çojë trafikun në rrugë të padëshiruara. Prandaj redundanca nuk është vetëm "shtim pajisjesh", por projektim i roleve, prioriteteve dhe kushteve të kalimit. Çdo mekanizëm failover duhet të ketë skenar testimi: çfarë ndodh kur bie link-u kryesor, kur fiket routeri aktiv, kur humbet një trunk ose kur një switch access del jashtë pune. Në aspektin e sigurisë, redundanca duhet të mos krijojë shtigje të pakontrolluara. Ndonjëherë organizatat ndërtojnë rrugë rezervë që anashkalojnë firewall-in ose politikat e kontrollit, duke krijuar dobësi. Një rrugë alternative duhet të ruajë të njëjtat rregulla sigurie si rruga kryesore. Nëse trafiku i financës kalon përmes firewall-it në kushte normale, ai nuk duhet të kalojë pa filtrim gjatë failover-it. Kjo kërkon sinkronizim politikash, konfigurime të njëjta sigurie dhe testim të skenarëve të dështimit. Scarfone dhe Hoffman (2009) theksojnë nevojën që firewall-et të testohen dhe menaxhohen sipas politikave, gjë që bëhet edhe më e rëndësishme kur firewall-et janë në çift ose kur rrjeti ka rrugë alternative. Një dimension tjetër i redundancës është rikthimi pas dështimit. Failover-i është vetëm gjysma e problemit; gjysma tjetër është failback-u. Kur pajisja kryesore kthehet në punë, rrjeti duhet të vendosë nëse trafiku do të kthehet automatikisht te ajo apo do të qëndrojë te pajisja rezervë deri në ndërhyrje të administratorit. Kthimi automatik mund të jetë i dobishëm, por në disa raste krijon ndërprerje të dytë ose luhatje nëse problemi nuk është zgjidhur plotësisht. Për këtë arsye, projektimi i redundancës duhet të përfshijë politika operative: kur pranohet kalimi automatik, kur kërkohet verifikim manual dhe si dokumentohen incidentet. Kjo e bën redundancën pjesë të menaxhimit të vazhdimësisë, jo vetëm funksion të protokolleve.

Redundanca duhet të vlerësohet edhe në raport me koston. Dyfishimi i çdo pajisjeje dhe çdo lidhjeje mund të krijojë rrjet shumë të qëndrueshëm, por edhe të shtrenjtë dhe kompleks. Prandaj projektimi kërkon prioritet: cilat shërbime janë kritike, cilat departamente nuk mund të ndërpriten, cilat lidhje duhet të kenë rezervë dhe cilat mund të rikuperohen manualisht. Ky vlerësim e lidh redundancën me analizën e riskut. Një rrjet akademik i mirë nuk pretendon redundancë absolute, por propozon redundancë të arsyetuar, aty ku ndërprerja ka ndikim më të madh. Kjo qasje e bën redundancën të mbrojtshme edhe nga pikëpamja financiare dhe menaxheriale. Ajo ndihmon që investimi teknik të arsyetohet me ndikimin real në

vazhdimësinë e punës. Redundanca duhet të matet me tregues të qartë: koha e rikuperimit, humbja e paketave gjatë kalimit, ndikimi te përdoruesit, stabiliteti pas rikuperimit dhe aftësia për t'u kthyer në gjendje normale. Në një simulim, këta tregues mund të vlerësohen duke fikur një router, duke ndërprerë një link, duke parë tabelat OSPF, statusin HSRP dhe gjendjen STP. Në një rrjet real, do të përdoreshin sisteme monitorimi, SLA dhe alarme. Analiza teorike tregon se redundanca e suksesshme nuk është ajo që ekziston në diagram, por ajo që funksionon kur provohet. Prandaj, një rrjet i sigurt ndërmarrjeje duhet të projektohet me supozimin se dështimet do të ndodhin dhe se rrjeti duhet të reagojë në mënyrë të parashikueshme.

6. Pajisjet – Routera, switche, servera dhe mënyra e konfigurimit të tyre

Pajisjet e rrjetit janë komponentët përmes të cilëve konceptet teorike kthehen në funksion praktik. Routerat, switchet, firewall-et dhe serverët kanë role të ndryshme, por të ndërvarura. Routeri lidh rrjete të ndryshme dhe merr vendime në shtresën e tretë; switch-i lidh pajisjet brenda LAN-it dhe menaxhon trafikun në shtresën e dytë; firewall-i kontrollon trafikun sipas politikave të sigurisë; serverët ofrojnë shërbime si DHCP, DNS, file sharing, web, autentikim ose aplikacione biznesi. Në një rrjet ndërmarrjeje, konfigurimi i këtyre pajisjeve nuk duhet të bëhet si veprim i izoluar, por si zbatim i një arkitekture të dokumentuar. Çdo pajisje duhet të ketë rol, emër, adresë menaxhimi, lidhje të përcaktuara dhe politika të qarta. Switchet access janë pika e parë ku përdoruesit lidhen me rrjetin. Konfigurimi i tyre duhet të ndajë portat sipas VLAN-eve të departamenteve dhe të shmangë përdorimin e trunk-eve të panevojshme. Një port ku lidhet një kompjuter finance duhet të jetë access port në VLAN-in përkatës, jo trunk port. Kjo ul rrezikun e VLAN hopping dhe gabimeve të konfigurimit. Për portat e papërdorura, praktika e mirë kërkon çaktivizim ose vendosje në VLAN të izoluar. Switchet duhet të kenë gjithashtu mekanizma mbrojtës si port security, BPDU Guard dhe kufizime për MAC address-at kur është e përshtatshme. Edhe pse këto mekanizma nuk zëvendësojnë firewall-in, ato forcojnë shtresën access dhe e bëjnë më të vështirë abuzimin lokal. Switchet distribution ose Layer 3 kryejnë rol më të avancuar. Ato mund të realizojnë routing ndër-VLAN, të zbatojnë ACL, të marrin pjesë në OSPF dhe të lidhen me firewall-in ose core-in. Në këtë nivel, konfigurimi duhet të jetë i kujdesshëm sepse gabimet prekin shumë departamente njëkohësisht. Për çdo VLAN duhet të ketë një interface virtual ose gateway të përcaktuar. Nëse përdoret HSRP, dy pajisje distribution mund të ndajnë një gateway virtual për secilin VLAN. Kjo krijon vazhdimësi për hostet edhe kur një pajisje distribution dështon. Li et al. (1998) e përshkruajnë HSRP si mekanizëm që u lejon hosteve të duken sikur përdorin një router të vetëm, duke ruajtur lidhjen kur routeri i parë dështon.

Routerat janë të rëndësishëm për lidhjen ndërmjet segmenteve më të mëdha, degëve ose internetit. Në një projekt ndërmarrjeje, routerat mund të përdorin OSPF për të shpërndarë rrugët e brendshme dhe default route drejt internetit. Moy (1998) e përkufizon OSPF si protokoll link-state për një sistem autonom, ku routerat ruajnë një bazë të përbashkët topologjie dhe llogarisin rrugët përmes algoritmit të pemës më të shkurtër. Nga këndvështrimi i konfigurimit, kjo do të

thotë se routerat duhet të kenë interface të adresuara qartë, zona OSPF të përcaktuara, kostot të kontrolluara dhe rregulla për shpërndarjen e default route. Routing-u dinamik duhet të kombinohet me filtrimin, në mënyrë që rrugët e panevojshme ose të pasigurta të mos përhapen pa kontroll. Firewall-i është pajisja ku politika e sigurisë bëhet rregull teknik. Konfigurimi i tij duhet të fillojë nga zonat: internet, DMZ, serverë të brendshëm, departamente, menaxhim dhe mysafirë. Pastaj përcaktohet trafiku i lejuar midis zonave. Në vend që të krijohen rregulla shumë të përgjithshme, si "lejo të gjithë trafikun nga LAN në serverë", duhet të krijohen rregulla specifike sipas protokollit, portës dhe burimit. Scarfone dhe Hoffman (2009) theksojnë rëndësinë e politikave të firewall-it dhe testimit të tyre. Në praktikë, kjo nënkupton se çdo rregull duhet të ketë arsye biznesi, pronar, datë rishikimi dhe logim të përshtatshëm. Firewall-i duhet të mos bëhet vend ku grumbullohen përjashtime të pakuptueshme.

Serverët duhet të vendosen në segmente të mbrojtura dhe të konfigurohen me parimin e rolit minimal. Një server DHCP duhet të ofrojë adresa sipas VLAN-eve, por nuk duhet të ketë akses administrativ të hapur nga çdo departament. Një server DNS i brendshëm duhet të përgjigjet për zonat e organizatës, por të mbrohet nga transferimet e paautorizuara. Serverët e aplikacioneve duhet të komunikojnë vetëm me bazat e të dhënave që u nevojiten. Këto rregulla janë pjesë e sigurisë së rrjetit sepse serverët janë objektiva me vlerë të lartë. Segmentimi i tyre në VLAN të veçantë dhe kontrolli i trafikut drejt tyre e zvogëlon rrezikun e kompromet imit të përgjithshëm. Një element që shpesh neglizhohet është konfigurimi i shërbimeve mbështetëse. DHCP duhet të jetë i organizuar sipas scope-eve të qarta për çdo VLAN, DNS duhet të jetë i besueshëm dhe i monitoruar, ndërsa NTP duhet të sigurojë kohë të sinkronizuar për log-et. Pa kohë të saktë, analiza e incidenteve bëhet e vështirë sepse ngjarjet nuk mund të renditen saktë. Pa DNS të qëndrueshëm, aplikacionet mund të dështojnë edhe kur rrjeti fizik funksionon. Pa DHCP të strukturuar, përdoruesit mund të marrin adresa të gabuara ose të mos marrin fare adresë. Kështu, pajisjet e rrjetit dhe serverët e shërbimeve bazë duhet të trajtohen si pjesë e së njëjtës arkitekturë operative.

Pajisjet duhet të zgjidhen edhe në bazë të kapacitetit dhe rolit. Një switch access nuk ka të njëjtat kërkesa si një core switch; një router perimetri nuk ka të njëjtën ngarkesë si një router laboratorik; një firewall duhet të përballojë jo vetëm bandwidth-in, por edhe numrin e sesioneve dhe inspektimin e trafikut. Nëse pajisjet zgjidhen vetëm sipas çmimit, rrjeti mund të funksionojë në fillim, por të dështojë kur rritet numri i përdoruesve ose aplikacioneve. Prandaj konfigurimi duhet të paraprihet nga vlerësimi i kapacitetit, funksioneve të nevojshme dhe mundësive të zgjerimit. Kjo e lidh zgjedhjen e pajisjeve me planifikimin

afatgjatë të ndërmarrjes dhe jo vetëm me laboratorin e momentit. Përzgjedhja e drejtë ul nevojën për zëvendësime të shpeshta dhe rrit stabilitetin operacional të të gjithë sistemit informatik. Konfigurimi i pajisjeve duhet të shoqërohet me standardizim. Emërtimi i pajisjeve, përdorimi i banner-ëve ligjorë, sinkronizimi i orës, backup i konfigurimeve, autentikimi i centralizuar, logimi dhe dokumentimi janë pjesë e administrimit profesional. Nëse një organizatë ka dhjetë switche me emra të paqartë dhe konfigurime të ndryshme, mirëmbajtja bëhet e pasigurt. Një rrjet i mirë është ai që mund të kuptohet edhe nga një administrator tjetër pas disa muajsh. Kjo kërkon që konfigurimi të mos jetë vetëm funksional, por i lexueshëm dhe i riprodhueshëm.

7. Protokollet – Përdorimi i OSPF, HSRP, STP për komunikim të qëndrueshëm

Protokollet janë rregullat që bëjnë të mundur funksionimin e koordinuar të pajisjeve të rrjetit. Në një rrjet ndërmarrjeje me disa departamente dhe redundancë, protokollet kryesore që lidhen me qëndrueshmërinë janë OSPF, HSRP dhe STP. Secili vepron në një shtresë ose funksion të ndryshëm: OSPF merret me routing-un dinamik në shtresën e tretë, HSRP me redundancën e gateway-t të parazgjedhur për hostet, ndërsa STP me parandalimin e loop-eve në shtresën e dytë. Së bashku, këto protokolle krijojnë një rrjet që jo vetëm dërgon trafik, por edhe reagon ndaj ndryshimeve të topologjisë. Pa to, redundanca fizike do të ishte e vështirë për t'u kontrolluar dhe dështimet do të kërkonin ndërhyrje manuale. OSPF është protokoll link-state dhe përdoret brenda një sistemi autonom. Moy (1998) shpjegon se çdo router OSPF mban një bazë të dhënash që përshkruan topologjinë e sistemit autonom dhe nga kjo bazë llogarit tabelën e routing-ut. Avantazhi i kësaj qasjeje është se routerat nuk varen vetëm nga informacioni i fqinjëve të drejtpërdrejtë, por ndërtojnë një pamje të strukturuar të rrjetit. Në një ndërmarrje, OSPF mund të përdoret për të lidhur core-in, distribution-in, server farm-in dhe daljet drejt internetit. Ai lejon rikonvergjencë kur një link dështon, duke zgjedhur rrugë alternative sipas kostove. Për rrjete më të mëdha, OSPF mund të ndahet në zona, ku area 0 shërben si backbone dhe zona të tjera lidhen me të për të ulur kompleksitetin e tabelave dhe përhapjen e update-eve.

Në përdorimin akademik të OSPF, rëndësi kanë disa koncepte: neighbor adjacency, link-state advertisement, cost, area design dhe convergence. Neighbor adjacency krijohet midis routerave që ndajnë link dhe parametra të përputhshëm. LSAs shpërndajnë informacionin e topologjisë. Cost përdoret për të zgjedhur rrugën më të mirë, zakonisht bazuar në bandwidth. Area design ndihmon në shkallëzim. Convergence mat sa shpejt rrjeti stabilizohet pas ndryshimit. Nëse rrjeti projektohet pa menduar këto elemente, OSPF mund të funksionojë, por jo domosdoshmërisht në mënyrë optimale. Për shembull, nëse kostot lihen default, trafiku mund të kalojë në rrugë jo të dëshiruara. Nëse zonat krijohen pa logjikë, administrimi bëhet më i vështirë. HSRP trajton një problem tjetër: çfarë ndodh me hostet kur default gateway i tyre dështon. Ndryshe nga routerat, hostet e zakonshëm nuk llogarisin rrugë alternative. Ata dërgojnë trafikun jashtë subnet-it te një IP gateway. HSRP krijon një IP virtuale dhe një grup routerash ku njëri është aktiv dhe tjetri standby. Nëse routeri aktiv nuk përgjigjet, standby merr rolin dhe vazhdon të përdorë IP-në virtuale për hostet (Li et al., 1998). Kjo e bën kalimin transparent për përdoruesit. Në një rrjet shumë-departamental, HSRP mund të konfigurohet për

çdo VLAN, duke siguruar gateway redundant për financën, burimet njerëzore, administratën dhe segmentet e tjera. Megjithatë, HSRP duhet të përdoret me kujdes. Vetëm prania e dy routerave nuk garanton disponueshmëri reale. Nëse routeri aktiv është ende ndezur, por ka humbur lidhjen drejt core-it ose internetit, hostet mund të vazhdojnë ta përdorin atë dhe të humbasin komunikimin. Për këtë arsye përdoret interface tracking ose objekt tracking, ku prioriteti i routerit aktiv ulet nëse humbet një link kritik. Gjithashtu, preemption duhet të konfigurohet në mënyrë të arsyeshme që routeri me prioritet më të lartë të rimarrë rolin kur rikthehet, por pa krijuar lëkundje të shpeshta. Kjo tregon se protokollet e redundancës nuk janë vetëm komanda; ato kërkojnë analizë të skenarëve të dështimit.

STP është i domosdoshëm në rrjetet Ethernet me lidhje redundante. Pa STP, një frame broadcast mund të qarkullojë pa fund në një topologji me loop, duke e mbingarkuar rrjetin. STP zgjedh një root bridge dhe bllokon disa porta për të krijuar një topologji logjike pa loop. Kur një lidhje aktive dështon, portat e bllokuara mund të kalojnë në gjendje forwarding dhe të rikthejnë lidhshmërinë. IEEE 802.1Q dhe familja 802.1 lidhen me funksionimin e bridge-eve dhe VLAN-eve në LAN, duke e vendosur kontrollin e topologjisë si pjesë të rëndësishme të standardizimit (IEEE, 2022). Në praktikë, administratorët duhet të zgjedhin qëllimisht root bridge-in, zakonisht në distribution layer, dhe të mos e lënë zgjedhjen rastësore. Në një projekt akademik, protokollet duhet të analizohen edhe nga perspektiva e kohës së konvergjencës dhe ndikimit te përdoruesi. OSPF mund të rikonvergojë pas ndryshimit të topologjisë, por gjatë asaj kohe mund të humbasin paketa. HSRP mund të bëjë kalimin nga aktiv në standby, por intervalet hello dhe hold ndikojnë sa shpejt ndodh ndryshimi. STP, në varësi të variantit, mund të kërkojë më shumë ose më pak kohë për të kaluar portat në gjendje forwarding. Prandaj zgjedhja e parametrave nuk duhet bërë mekanikisht. Ajo duhet të reflektojë tolerancën e organizatës ndaj ndërprerjes, kompleksitetin e rrjetit dhe stabilitetin e pajisjeve. Një rrjet shumë agresiv në konvergjencë mund të bëhet i ndjeshëm ndaj luhatjeve, ndërsa një rrjet shumë konservator mund të rikuperohet ngadalë (Cisco, 2024a).

Protokollet duhet të mbrohen edhe nga konfigurimet e pasigurta. OSPF mund të përdorë autentikim midis fqinjëve për të ulur rrezikun e injektimit të rrugëve të rreme. HSRP duhet të kufizohet në segmentet ku nevojitet dhe të mos ekspozohet pa kontroll. STP duhet të mbrohet me mekanizma si BPDU Guard në porta access për të shmangur që një pajisje e paautorizuar të ndikojë topologjinë. Këto masa tregojnë se protokollet e disponueshmërisë kanë edhe dimension sigurie. Një protokoll që rrit qëndrueshmërinë, nëse konfigurohet dobët, mund të kthehet në burim rreziku. Prandaj protokollet duhet të trajtohen njëkohësisht si mekanizma

komunikimi, qëndrueshmërie dhe kontrolli. Analiza e tyre duhet të përfshijë edhe ndikimin në siguri dhe mirëmbajtje. Ndërveprimi i OSPF, HSRP dhe STP kërkon koherencë arkitekturore. STP kontrollon rrugët aktive në shtresën e dytë; HSRP përcakton gateway-n aktiv për hostet; OSPF përcakton rrugët në shtresën e tretë. Nëse këto protokolle nuk harmonizohen, mund të krijohen rrugë asimetrike, vonesa ose përdorim jo optimal i lidhjeve. Për shembull, root bridge-i i STP dhe routeri aktiv i HSRP duhet të jenë të koordinuar për VLAN-et kryesore, në mënyrë që trafiku të mos kalojë pa nevojë nëpër lidhje të tërthorta. Po ashtu, OSPF duhet të reflektojë rrugët reale që janë të preferuara në dizajn. Qëndrueshmëria nuk vjen nga protokollet individuale, por nga konfigurimi i tyre si pjesë e një sistemi.

8. Zbatimi praktik – Ndërtimi dhe testimi i rrjetit në simulim

Zbatimi praktik i një rrjeti shumë-departamental me siguri dhe redundancë zakonisht fillon me modelimin në një mjedis simulimi. Simulimi lejon testimin e topologjisë përpara investimit në pajisje fizike dhe ul rrezikun e gabimeve në prodhim. Cisco Packet Tracer është një mjet i përdorur gjerësisht për mësim dhe praktikë në rrjete, IoT dhe siguri kibernetike, duke ofruar një laborator virtual për konfigurime bazë dhe të ndërmjetme (Cisco Networking Academy, n.d.). GNS3, nga ana tjetër, përdoret shpesh për topologji më të avancuara dhe testim me imazhe reale ose virtuale të pajisjeve (GNS3, n.d.). Zgjedhja midis tyre varet nga objektivat: Packet Tracer është më i thjeshtë për demonstrim akademik, ndërsa GNS3 ofron fleksibilitet më të madh për skenarë profesionalë. Në një zbatim praktik, hapi i parë është ndërtimi i topologjisë logjike. Kjo përfshin vendosjen e switch-eve access për çdo grup përdoruesish, switch-eve distribution për routing ndër-VLAN, routerave për dalje drejt rrjeteve të tjera, firewall-it për kontroll të trafikut dhe serverëve për shërbime të brendshme. Topologjia duhet të reflektojë ndarjen departamentale: administratë, financë, burime njerëzore, IT, serverë, menaxhim dhe mysafirë. Çdo departament merr VLAN dhe subnet të veçantë. Kjo fazë nuk duhet parë si vizatim i thjeshtë, por si përkthim i kërkesave të biznesit në komponentë rrjeti. Nëse organizata kërkon izolim të fortë të financës, atëherë VLAN-i i financës duhet të lidhet me politika të posaçme në firewall dhe jo vetëm me një emërtim në switch.

Hapi i dytë është konfigurimi i adresimit dhe VLAN-eve. Në simulim mund të përdoret një hapësirë private RFC 1918, për shembull 10.10.0.0/16, me subnet-e të ndara për çdo departament (Rekhter et al., 1996). VLAN-et krijohen në switche, portat e përdoruesve vendosen në mode access, ndërsa lidhjet midis switch-eve dhe pajisjeve distribution vendosen në mode trunk. Në këtë fazë duhet të testohet që hostet brenda të njëjtit VLAN komunikojnë me njëri-tjetrin, ndërsa hostet e VLAN-eve të ndryshme nuk komunikojnë pa routing. Ky test verifikon izolimin fillestar të shtresës së dytë. Pastaj konfigurohen interface-et virtuale ose subinterface-et për routing ndër-VLAN (Cisco, 2023b, 2023c).

Hapi i tretë është zbatimi i politikave të sigurisë. Nëse përdoret firewall në simulim, ai duhet të vendoset midis rrjetit të brendshëm dhe internetit, si dhe mundësisht midis segmenteve kritike. Nëse simulatori nuk mbështet plotësisht funksione firewall-i, ACL-të në routera ose switch-e Layer 3 mund të përdoren për të modeluar rregullat. Qasja duhet të jetë deny by default dhe allow by exception. Për shembull, VLAN-i i mysafirëve lejohet të dalë

drejt internetit, por bllokohet drejt serverëve të brendshëm; VLAN-i i IT-së lejohet të menaxhojë pajisjet; VLAN-i i financës lejohet të përdorë serverin financiar në porta të caktuara. Kjo e lidh simulimin me parimet që Scarfone dhe Hoffman (2009) përshkruajnë për firewall-et dhe politikat e tyre.

Hapi i katërt është konfigurimi i protokolleve të redundancës. Për HSRP, dy routera ose dy switch-e Layer 3 konfigurohen për të ndarë një IP virtuale për çdo VLAN. Testimi bëhet duke fikur pajisjen aktive ose duke ndërprerë link-un e saj dhe duke vëzhguar nëse standby merr rolin. Për OSPF, routerat konfigurohen me zonat dhe rrjetet përkatëse, pastaj kontrollohen fqinjësitë dhe tabelat e routing-ut. Testimi bëhet duke ndërprerë një link dhe duke parë nëse trafiku kalon në rrugë alternative. Për STP, testimi bëhet duke krijuar lidhje redundante midis switch-eve dhe duke verifikuar se një port bllokohet për të shmangur loop-in. Këto teste e bëjnë redundancën të verifikueshme, jo vetëm të supozuar.

Hapi i pestë është dokumentimi i rezultateve të testimit. Një punim akademik nuk mjaftohet me pohimin “rrjeti funksionon”; ai duhet të tregojë si është vërtetuar funksionimi. Testet mund të përfshijnë ping brenda VLAN-it, ping ndërmjet VLAN-eve të lejuara, tentime të bllokuara nga VLAN-i i mysafirëve, traceroute për të parë rrugën e trafikut, statusin e HSRP para dhe pas dështimit, tabelat OSPF para dhe pas ndërprerjes së link-ut, si dhe gjendjen STP. Nëse përdoret Packet Tracer, mjetet e simulation mode ndihmojnë për të parë lëvizjen e paketave. Nëse përdoret GNS3, mund të përdoren mjete shtesë monitorimi dhe analiza paketash.

Një zbatim i plotë duhet të përfshijë edhe skenarë negativë, sepse rrjeti nuk vlerësohet vetëm në kushte ideale. Skenarët negativë mund të përfshijnë vendosjen e një hosti në VLAN të gabuar, tentimin e aksesit administrativ nga një departament i zakonshëm, dështimin e serverit DHCP, humbjen e një trunk-u ose krijimin e një rruge të padëshiruar. Këto teste ndihmojnë në zbulimin e varësive që nuk duken në diagram. Nëse rrjeti funksionon vetëm kur gjithçka është e saktë, por nuk ka kontroll ndaj gabimeve të zakonshme, atëherë dizajni është i brishtë. Prandaj simulimi duhet të përdoret jo vetëm për të provuar suksesin, por edhe për të kërkuar dobësi. Në nivel metodologjik, zbatimi praktik duhet të ruajë gjurmë të qarta të ndryshimeve. Çdo konfigurim i rëndësishëm duhet të shoqërohet me përshkrim: çfarë u ndryshua, pse u ndryshua dhe si u testua. Kjo është e rëndësishme sepse simulimi shpesh bëhet në mënyrë eksperimentale dhe pa dokumentim humbet lidhja midis vendimit teknik dhe rezultatit. Një projekt i mirë akademik paraqet jo vetëm topologjinë përfundimtare, por edhe arsyetimin që çoi te ajo. Kjo e bën punimin më të besueshëm dhe më të lehtë për t’u riprodhuar. Dokumentimi është pjesë e zbatimit, jo shtesë formale pas përfundimit të

konfigurimit. Ai shërben si provë se zgjidhja është ndërtuar në mënyrë metodike, me hapa të verifikueshëm dhe me lidhje të qartë midis objektivit, konfigurimit dhe rezultatit të testuar në çdo skenar. Kjo rrit cilësinë shkencore të punimit dhe shmang paqartësitë në vlerësim. Zbatimi praktik duhet të ruajë lidhjen me analizën teorike. Simulimi nuk është qëllim në vetvete, por mënyrë për të provuar hipotezën se segmentimi, kontrolli i aksesit dhe redundanca krijojnë rrjet më të sigurt dhe më të qëndrueshëm. Nëse një test tregon se VLAN-i i mysafirëve mund të aksesojë serverët e brendshëm, atëherë dizajni duhet të rishikohet. Nëse failover-i HSRP funksionon, por trafiku mbetet pa dalje për shkak të humbjes së link-ut uplink, duhet të shtohet tracking. Nëse OSPF zgjedh rrugë të gabuar, duhet rishikuar cost-i. Pra, zbatimi praktik është proces iterativ ku teoria, konfigurimi dhe testimi korrigjojnë njëra-tjetrën.

9. Implementimi dhe kodimi i konfigurimeve

Kjo pjesë shton komponentin praktik të projektit. Implementimi është ndërtuar si konfigurim real për pajisje Cisco IOS dhe mund të përdoret në Cisco Packet Tracer, GNS3 ose në pajisje fizike Cisco me përshtatje minimale të emrave të interfejseve. Qëllimi i implementimit është të tregojë se analiza teorike mund të kthehet në konfigurim funksional: departamentet ndahen me VLAN, gateway-t bëhen redundant me HSRP, rrugët llogariten me OSPF, loop-et kontrollohen me Rapid PVST/STP, ndërsa trafiku kufizohet me ACL dhe politika sigurie.

Topologjia praktike përbëhet nga dy switch-e multilayer në shtresën distribution/core (DSW1 dhe DSW2), dy routera perimetralë (EDGE-R1 dhe EDGE-R2), dy switch-e access për përdoruesit dhe serverët, si dhe një segment serverësh. DSW1 dhe DSW2 mbajnë VLAN-et dhe SVI-të për gateway-t e departamenteve. HSRP përdor adresën virtuale .1 për çdo VLAN, ndërsa DSW1 mban prioritet kryesor për shumicën e VLAN-eve dhe DSW2 mban prioritet kryesor për VLAN-in e mysafirëve. EDGE-R1 dhe EDGE-R2 ofrojnë NAT, default route dhe shpërndarje të rrugës default përmes OSPF.

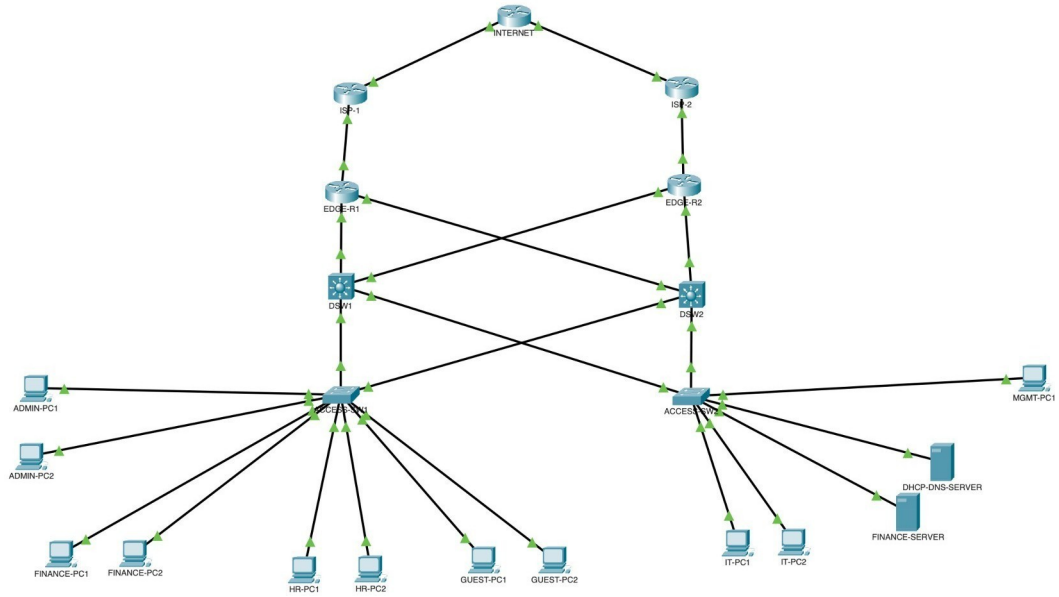

Figura 1. Topologjia logjike e rrjetit të implementuar në simulim
Burimi: Autori, nga simulimi në Cisco Packet Tracer.

Plani IP dhe VLAN

Tabela 1. Plani IP dhe VLAN i rrjetit të implementuar
Burimi: Autori.

VLAN	Emri	Subnet	Gateway virtual
10	ADMIN	10.10.10.0/24	10.10.10.1
20	FINANCE	10.10.20.0/24	10.10.20.1
30	HR	10.10.30.0/24	10.10.30.1
40	IT	10.10.40.0/24	10.10.40.1

50	SERVERS	10.10.50.0/24	10.10.50.1
60	MGMT	10.10.60.0/24	10.10.60.1
70	GUEST	10.10.70.0/24	10.10.70.1

Adresat kryesore të pajisjeve

Tabela 2. Adresat kryesore të pajisjeve dhe serverëve
Burimi: Autori.

Pajisja	Roli	Adresa kryesore
DSW1	Core/Distribution primar	10.10.254.1/30 dhe 10.10.254.5/30; router-id 1.1.1.1
DSW2	Core/Distribution sekondar	10.10.254.9/30 dhe 10.10.254.13/30; router-id 2.2.2.2
EDGE-R1	Router perimetral primar	10.10.254.2/30, 10.10.254.10/30 dhe 203.0.113.2/30; router-id 11.11.11.11
EDGE-R2	Router perimetral sekondar	10.10.254.6/30, 10.10.254.14/30 dhe 203.0.113.6/30; router-id 22.22.22.22
DHCP/DNS	Server i brendshëm	10.10.50.10
Finance APP	Server financiar	10.10.50.30

9.1. Konfigurimi i DSW1

Ky konfigurim krijon VLAN-et, aktivizon routing-un, vendos HSRP për gateway-t virtuale, konfiguron Rapid PVST, OSPF, ACL për mysafirët dhe financën, si dhe kufizon aksesin administrativ vetëm nga VLAN-i i menaxhimit (Cisco, 2023a, 2023b, 2023c, 2024a, 2024b).

Tabela 3. Komponentët e implementuar, arsyetimi dhe mënyra e testimit
Burimi: Autori.

Komponenti	Implementimi	Arsyeja	Testimi
VLAN	Ndarje sipas departamenteve	Izolim logjik dhe administrim më i qartë sipas IEEE 802.1Q	show vlan brief; ping brenda/ndërmjet VLAN-eve
OSPF	Area 0 në lidhjet DSW/EDGE	Rrugëtim dinamik dhe rikalkulim pas dështimit sipas RFC 2328	show ip ospf neighbor; show ip route ospf
HSRP	Gateway virtual .1 për çdo VLAN	Vazhdimësi e gateway-t sipas RFC 2281	show standby brief; fikje e linkut aktiv
STP/Rapid PVST	Root primar/sekondar	Parandalim i loop-eve në lidhje redundante	show spanning-tree root
ACL	Kufizim për Guest/Finance/MGMT	Kontroll aksesesh dhe privilegj minimal	show access-lists; teste ping/SSH të lejuara dhe të bllokuara

```
! DSW1 - Distribution/Core switch primary
enable
configure terminal
hostname DSW1
no ip domain-lookup
ip routing
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET
ip domain-name enterprise.local
crypto key generate rsa modulus 2048
```

```
ip ssh version 2

vlan 10
 name ADMIN
vlan 20
 name FINANCE
vlan 30
 name HR
vlan 40
 name IT
vlan 50
 name SERVERS
vlan 60
 name MGMT
vlan 70
 name GUEST

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,50,60 root primary
spanning-tree vlan 70 root secondary

interface GigabitEthernet1/0/1
 description Routed link to EDGE-R1
 no switchport
 ip address 10.10.254.1 255.255.255.252
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet1/0/2
 description Routed link to EDGE-R2
 no switchport
 ip address 10.10.254.5 255.255.255.252
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet1/0/23
 description Trunk to ACCESS-SW1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 spanning-tree guard root
 no shutdown
interface GigabitEthernet1/0/24
 description Trunk to ACCESS-SW2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 spanning-tree guard root
 no shutdown

interface Vlan10
 description Gateway ADMIN
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 10.10.50.10
 standby 10 ip 10.10.10.1
 standby 10 priority 110
 standby 10 preempt
 standby 10 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface  Vlan20
 description Gateway
 FINANCE
 ip address 10.10.20.2 255.255.255.0
 ip helper-address 10.10.50.10
 ip access-group VLAN20-IN in
 standby 20 ip 10.10.20.1
 standby 20 priority 110
 standby 20 preempt
 standby 20 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface Vlan30
 description Gateway HR
 ip address 10.10.30.2 255.255.255.0
 ip helper-address 10.10.50.10
 standby 30 ip 10.10.30.1
 standby 30 priority 110
 standby 30 preempt
 standby 30 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface Vlan40
 description Gateway IT
 ip address 10.10.40.2 255.255.255.0
 ip helper-address 10.10.50.10
 standby 40 ip 10.10.40.1
 standby 40 priority 110
 standby 40 preempt
 standby 40 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface  Vlan50
 description Gateway
 SERVERS
 ip address 10.10.50.2 255.255.255.0
 standby 50 ip 10.10.50.1
```

```
 standby 50 priority 110
 standby 50 preempt
 standby 50 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface Vlan60
 description Gateway MANAGEMENT
 ip address 10.10.60.2 255.255.255.0
 standby 60 ip 10.10.60.1
 standby 60 priority 110
 standby 60 preempt
 standby 60 track GigabitEthernet1/0/1 decrement 30
 no shutdown
interface Vlan70
 description Gateway GUEST
 ip address 10.10.70.2 255.255.255.0
 ip helper-address 10.10.50.10
 ip access-group GUEST-IN in
 standby 70 ip 10.10.70.1
 standby 70 priority 90
 standby 70 preempt
 no shutdown

ip access-list extended GUEST-IN
 remark Guests may use DHCP/DNS and Internet, but not internal networks
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.10.50.10 eq domain
 permit tcp any host 10.10.50.10 eq domain
 deny ip any 10.10.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20-IN
 remark Finance: DHCP/DNS, Finance APP and web access only
 permit udp any eq bootpc any eq bootps
 permit udp 10.10.20.0 0.0.0.255 host 10.10.50.10 eq domain
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.10 eq domain
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.30 eq 443
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.30 eq 1433
 permit icmp 10.10.20.0 0.0.0.255 host 10.10.50.30 echo
 deny ip 10.10.20.0 0.0.0.255 10.10.0.0 0.0.255.255 log
 permit tcp 10.10.20.0 0.0.0.255 any eq 80
 permit tcp 10.10.20.0 0.0.0.255 any eq 443
 deny ip 10.10.20.0 0.0.0.255 any log
ip access-list standard MGMT-ONLY
 permit 10.10.60.0 0.0.0.255
 deny any

router ospf 10
 router-id 1.1.1.1
 passive-interface default
 no passive-interface GigabitEthernet1/0/1
 no passive-interface GigabitEthernet1/0/2
 network 10.10.0.0 0.0.255.255 area 0

line vty 0 15
 login local
 transport input ssh
 access-class MGMT-ONLY in
end
write memory
```

9.2. Konfigurimi i DSW2

DSW2 shërben si pajisje rezervë për shumicën e VLAN-eve dhe si root primar për VLAN-in e mysafirëve. Kjo shpërndan ngarkesën logjike dhe tregon se redundanca nuk duhet të jetë vetëm kopje pasive, por pjesë e dizajnit.

```
! DSW2 - Distribution/Core switch secondary
enable
configure terminal
hostname DSW2
no ip domain-lookup
ip routing
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET
ip domain-name enterprise.local
crypto key generate rsa modulus 2048
ip ssh version 2
```

```
vlan 10
 name ADMIN
vlan 20
 name FINANCE
vlan 30
 name HR
vlan 40
 name IT
vlan 50
 name SERVERS
vlan 60
 name MGMT
vlan 70
 name GUEST

spanning-tree mode rapid-pvst
spanning-tree vlan 10,20,30,40,50,60 root secondary
spanning-tree vlan 70 root primary

interface GigabitEthernet1/0/1
 description Routed link to EDGE-R1
 no switchport
 ip address 10.10.254.9 255.255.255.252
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet1/0/2
 description Routed link to EDGE-R2
 no switchport
 ip address 10.10.254.13 255.255.255.252
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet1/0/23
 description Trunk to ACCESS-SW1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 spanning-tree guard root
 no shutdown
interface GigabitEthernet1/0/24
 description Trunk to ACCESS-SW2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 spanning-tree guard root
 no shutdown

interface Vlan10
 ip address 10.10.10.3 255.255.255.0
 ip helper-address 10.10.50.10
 standby 10 ip 10.10.10.1
 standby 10 priority 100
 standby 10 preempt
 no shutdown
interface Vlan20
 ip address 10.10.20.3 255.255.255.0
 ip helper-address 10.10.50.10
 ip access-group VLAN20-IN in
 standby 20 ip 10.10.20.1
 standby 20 priority 100
 standby 20 preempt
 no shutdown
interface Vlan30
 ip address 10.10.30.3 255.255.255.0
 ip helper-address 10.10.50.10
 standby 30 ip 10.10.30.1
 standby 30 priority 100
 standby 30 preempt
 no shutdown
interface Vlan40
 ip address 10.10.40.3 255.255.255.0
 ip helper-address 10.10.50.10
 standby 40 ip 10.10.40.1
 standby 40 priority 100
 standby 40 preempt
 no shutdown
interface Vlan50
 ip address 10.10.50.3 255.255.255.0
 standby 50 ip 10.10.50.1
 standby 50 priority 100
 standby 50 preempt
 no shutdown
interface Vlan60
 ip address 10.10.60.3 255.255.255.0
 standby 60 ip 10.10.60.1
 standby 60 priority 100
 standby 60 preempt
 no shutdown
interface Vlan70
 ip address 10.10.70.3 255.255.255.0
```

```
 ip helper-address 10.10.50.10
 ip access-group GUEST-IN in
 standby 70 ip 10.10.70.1
 standby 70 priority 110
 standby 70 preempt
 no shutdown

ip access-list extended GUEST-IN
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.10.50.10 eq domain
 permit tcp any host 10.10.50.10 eq domain
 deny ip any 10.10.0.0 0.0.255.255
 permit ip any any
ip access-list extended VLAN20-IN
 remark Finance: DHCP/DNS, Finance APP and web access only
 permit udp any eq bootpc any eq bootps
 permit udp 10.10.20.0 0.0.0.255 host 10.10.50.10 eq domain
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.10 eq domain
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.30 eq 443
 permit tcp 10.10.20.0 0.0.0.255 host 10.10.50.30 eq 1433
 permit icmp 10.10.20.0 0.0.0.255 host 10.10.50.30 echo
 deny ip 10.10.20.0 0.0.0.255 10.10.0.0 0.0.255.255 log
 permit tcp 10.10.20.0 0.0.0.255 any eq 80
 permit tcp 10.10.20.0 0.0.0.255 any eq 443
 deny ip 10.10.20.0 0.0.0.255 any log
ip access-list standard MGMT-ONLY
 permit 10.10.60.0 0.0.0.255
 deny any

router ospf 10
 router-id 2.2.2.2
 passive-interface default
 no passive-interface GigabitEthernet1/0/1
 no passive-interface GigabitEthernet1/0/2
 network 10.10.0.0 0.0.255.255 area 0

line vty 0 15
 login local
 transport input ssh
 access-class MGMT-ONLY in
end
write memory
```

9.3. Konfigurimi i routerave perimetralë

Routerat EDGE-R1 dhe EDGE-R2 ofrojnë dalje drejt internetit, NAT overload për adresat private dhe default route të shpërndarë me OSPF. EDGE-R1 ka metrikë më të ulët, ndërsa EDGE-R2 përdoret si rrugë rezervë.

```
! EDGE-R1 - Primary edge router with NAT and default route
enable
configure terminal
hostname EDGE-R1
no ip domain-lookup
ip routing
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET

interface GigabitEthernet0/0
 description To DSW1
 ip address 10.10.254.2 255.255.255.252
 ip nat inside
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet0/1
 description To DSW2
 ip address 10.10.254.10 255.255.255.252
 ip nat inside
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet0/2
 description To ISP-1
```

```
 ip address 203.0.113.2 255.255.255.252
 ip nat outside
 ip access-group OUTSIDE-IN in
 no shutdown

ip access-list standard NAT-INSIDE
 permit 10.10.0.0 0.0.255.255
ip nat inside source list NAT-INSIDE interface GigabitEthernet0/2 overload
ip route 0.0.0.0 0.0.0.0 203.0.113.1

ip access-list extended OUTSIDE-IN
 remark No unsolicited inbound traffic in this basic scenario
 deny ip any 10.10.0.0 0.0.255.255 log
 permit ip any any

router ospf 10
 router-id 11.11.11.11
 default-information originate
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 network 10.10.254.0 0.0.0.15 area 0
end
write memory
```

```
! EDGE-R2 - Secondary edge router with NAT and backup default route
enable
configure terminal
hostname EDGE-R2
no ip domain-lookup
ip routing
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET

interface GigabitEthernet0/0
 description To DSW1
 ip address 10.10.254.6 255.255.255.252
 ip nat inside
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet0/1
 description To DSW2
 ip address 10.10.254.14 255.255.255.252
 ip nat inside
 ip ospf 10 area 0
 no shutdown
interface GigabitEthernet0/2
 description To ISP-2
 ip address 203.0.113.6 255.255.255.252
 ip nat outside
 ip access-group OUTSIDE-IN in
 no shutdown

ip access-list standard NAT-INSIDE
 permit 10.10.0.0 0.0.255.255
ip nat inside source list NAT-INSIDE interface GigabitEthernet0/2 overload
ip route 0.0.0.0 0.0.0.0 203.0.113.5

ip access-list extended OUTSIDE-IN
 deny ip any 10.10.0.0 0.0.255.255 log
 permit ip any any

router ospf 10
 router-id 22.22.22.22
 default-information originate metric 20
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 network 10.10.254.0 0.0.0.15 area 0
end
write memory
```

9.4. Konfigurimi i switch-eve access

Switch-et access vendosin portat e përdoruesve në VLAN-et përkatëse, aktivizojnë port-security, portfast dhe bpduguard. Kjo e bën pjesën e access layer më të kontrolluar dhe ul mundësinë e gabimeve ose sulmeve bazike në shtresën e dytë.

```
! ACCESS-SW1 - Access switch for users
enable
configure terminal
hostname ACCESS-SW1
no ip domain-lookup
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET

vlan 10
 name ADMIN
vlan 20
 name FINANCE
vlan 30
 name HR
vlan 40
 name IT
vlan 50
 name SERVERS
vlan 60
 name MGMT
vlan 70
 name GUEST

spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree bpduguard default

interface GigabitEthernet0/1
 description Uplink trunk to DSW1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 no shutdown
interface GigabitEthernet0/2
 description Uplink trunk to DSW2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 no shutdown

interface range FastEthernet0/1-6
 description ADMIN users
 switchport mode access
 switchport access vlan 10
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 spanning-tree portfast
 no shutdown
interface range FastEthernet0/7-12
 description FINANCE users
 switchport mode access
 switchport access vlan 20
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 spanning-tree portfast
 no shutdown
interface range FastEthernet0/13-18
 description HR users
```

```
 switchport mode access
 switchport access vlan 30
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 spanning-tree portfast
 no shutdown
interface range FastEthernet0/19-22
 description GUEST users
 switchport mode access
 switchport access vlan 70
 spanning-tree portfast
 no shutdown

interface Vlan60
 description Switch management
 ip address 10.10.60.11 255.255.255.0
 no shutdown
ip default-gateway 10.10.60.1
line vty 0 15
 login local
 transport input ssh
end
write memory
```

```
! ACCESS-SW2 - Access switch for IT and servers
enable
configure terminal
hostname ACCESS-SW2
no ip domain-lookup
service password-encryption
enable secret
STRONG_ENABLE_SECRET
username netadmin privilege 15 secret STRONG_ADMIN_SECRET

vlan 10
 name ADMIN
vlan 20
 name FINANCE
vlan 30
 name HR
vlan 40
 name IT
vlan 50
 name SERVERS
vlan 60
 name MGMT
vlan 70
 name GUEST

spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree bpduguard default

interface GigabitEthernet0/1
 description Uplink trunk to DSW1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 no shutdown
interface GigabitEthernet0/2
 description Uplink trunk to DSW2
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40,50,60,70
 no shutdown

interface range FastEthernet0/1-8
 description IT users
 switchport mode access
 switchport access vlan 40
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 spanning-tree portfast
```

```
 no shutdown
interface range FastEthernet0/9-16
 description SERVER ports
 switchport mode access
 switchport access vlan 50
 spanning-tree portfast
 no shutdown
interface range FastEthernet0/17-20
 description MANAGEMENT stations
 switchport mode access
 switchport access vlan 60
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 spanning-tree portfast
 no shutdown

interface Vlan60
 description Switch management
 ip address 10.10.60.12 255.255.255.0
 no shutdown
ip default-gateway 10.10.60.1
line vty 0 15
 login local
 transport input ssh
end
write memory
```

9.5. DHCP dhe shërbimet bazë

Nëse përdoret server grafik në Packet Tracer, DHCP mund të konfigurohet në serverin 10.10.50.10 dhe SVI-të përdorin ip helper-address. Nëse kërkohet konfigurim me kod IOS, mund të përdoret konfigurimi i mëposhtëm në DSW1 për qëllime simulimi (Cisco, 2023a).

```
! Optional DHCP configuration if DHCP is implemented on DSW1 in Packet Tracer.
! In production, use redundant DHCP servers. Exclude gateway and reserved server
addresses.
configure terminal
ip dhcp excluded-address 10.10.10.1 10.10.10.30
ip dhcp excluded-address 10.10.20.1 10.10.20.30
ip dhcp excluded-address 10.10.30.1 10.10.30.30
ip dhcp excluded-address 10.10.40.1 10.10.40.30
ip dhcp excluded-address 10.10.70.1 10.10.70.30

ip dhcp pool VLAN10_ADMIN
 network 10.10.10.0
 255.255.255.0
 default-router 10.10.10.1
 dns-server 10.10.50.10
 domain-name enterprise.local
ip dhcp pool VLAN20_FINANCE
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.1
 dns-server 10.10.50.10
 domain-name enterprise.local
ip dhcp pool VLAN30_HR
 network 10.10.30.0 255.255.255.0
 default-router 10.10.30.1
 dns-server 10.10.50.10
 domain-name enterprise.local
ip dhcp pool VLAN40_IT
 network 10.10.40.0 255.255.255.0
 default-router 10.10.40.1
 dns-server 10.10.50.10
 domain-name enterprise.local
ip dhcp pool VLAN70_GUEST
 network 10.10.70.0
 255.255.255.0
 default-router 10.10.70.1
```

```
dns-server 10.10.50.10
```

```
 domain-name enterprise.local
end
write memory
```

9.6. Procedura e testimit

Testimi duhet të provojë jo vetëm që rrjeti punon, por edhe që politikat e sigurisë dhe redundanca funksionojnë. Komandat e mëposhtme verifikojnë VLAN-et, trunk-et, root bridge, HSRP, OSPF, ACL, NAT dhe skenarët e dështimit.

```
! Verification commands
show vlan brief
show interfaces trunk
show spanning-tree root
show standby brief
show ip ospf neighbor
show ip route ospf
show ip route 0.0.0.0
show access-lists VLAN20-IN
show access-lists GUEST-IN
show ip interface brief
show ip nat translations
ping 10.10.50.10
ping 10.10.50.30
traceroute 8.8.8.8

! Failure and security tests
! 1. Record HSRP state on DSW1/DSW2, then shut down DSW1 Gi1/0/1 and verify role change.
! 2. Record OSPF neighbors/routes, interrupt the EDGE-R1 link and verify reconvergence.
! 3. From Finance, verify DNS and access to 10.10.50.30; verify that HR/internal subnets are denied.
! 4. From Guest, verify DHCP/DNS and Internet access; verify that internal networks are denied.
! 5. Shut down EDGE-R1 outside interface and verify that the default path changes to EDGE-R2.
```

Skedari i Packet Tracer-it, konfigurimet e pajisjeve dhe komandat e verifikimit duhet të ruhen së bashku me punimin, në mënyrë që testet të mund të riprodhohen gjatë verifikimit ose mbrojtjes së diplomës.

10. Rezultatet – Si funksionon rrjeti dhe si reagon ndaj dështimeve

Rezultatet u vlerësuan sipas katër objektivave kryesore: segmentimit të departamenteve, zbatimit të politikave të aksesit, funksionimit të rrugëzimit dinamik dhe reagimit ndaj dështimeve. Daljet origjinale nga Cisco Packet Tracer, të paraqitura në Figurat 2–5, konfirmojnë se ACL-të lejojnë dhe bllokojnë trafikun sipas politikave të përcaktuara, HSRP realizon kalimin nga DSW1 te DSW2, OSPF rikonvergon pas ndërprerjes së link-ut dhe rruga e parazgjedhur kalon nga EDGE-R1 te EDGE-R2. Nënkapitulli 10.1 paraqet evidencën e testeve, ndërsa nënkapitulli 10.2 analizon rezultatet e vërejtura.

10.1. Evidenca e testimit në Packet Tracer

```
DSW1#show standby brief
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri  P State    Active          Standby         Virtual IP
V110         10   110  P Active   local           10.10.10.3      10.10.10.1
V120         20   110  P Active   local           10.10.20.3      10.10.20.1
V130         30   110  P Active   local           10.10.30.3      10.10.30.1
V140         40   110  P Active   local           10.10.40.3      10.10.40.1
V150         50   110  P Active   local           10.10.50.3      10.10.50.1
V160         60   110  P Active   local           10.10.60.3      10.10.60.1
V170         70   110  P Active   local           10.10.70.3      10.10.70.1
DSW1#
```

a) Gjendja para dështimit – DSW1 (Active)

```
DSW2#show standby brief
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri  P State    Active          Standby         Virtual IP
V110         10   100  P Standby  10.10.10.2      local           10.10.10.1
V120         20   100  P Standby  10.10.20.2      local           10.10.20.1
V130         30   100  P Standby  10.10.30.2      local           10.10.30.1
V140         40   100  P Standby  10.10.40.2      local           10.10.40.1
V150         50   100  P Standby  10.10.50.2      local           10.10.50.1
V160         60   100  P Standby  10.10.60.2      local           10.10.60.1
V170         70   100  P Standby  10.10.70.2      local           10.10.70.1
DSW2#
```

b) Gjendja para dështimit – DSW2 (Standby)

```
DSW2#show standby brief
                     P indicates configured to preempt.
                     |
Interface    Grp  Pri  P State    Active          Standby         Virtual IP
V110         10   100  P Active   local           unknown         10.10.10.1
V120         20   100  P Active   local           unknown         10.10.20.1
V130         30   100  P Active   local           unknown         10.10.30.1
V140         40   100  P Active   local           unknown         10.10.40.1
V150         50   100  P Active   local           unknown         10.10.50.1
V160         60   100  P Active   local           unknown         10.10.60.1
V170         70   100  P Active   local           unknown         10.10.70.1
DSW2#
```

c) Gjendja pas dështimit – DSW2 bëhet Active (DSW1 jashtë funksionit)

Figura 2. Gjendja e HSRP para dhe pas dështimit të uplink-ut aktiv
Burimi: Autori, nga simulimi në Cisco Packet Tracer.

```
DSW2#show ip ospf neighbor

Neighbor ID       Pri   State           Dead Time   Address         Interface
1.1.1.1             1   FULL/BDR        00:00:30    10.10.10.2      Vlan10
1.1.1.1             1   FULL/BDR        00:00:30    10.10.20.2      Vlan20
1.1.1.1             1   FULL/BDR        00:00:30    10.10.30.2      Vlan30
1.1.1.1             1   FULL/BDR        00:00:30    10.10.40.2      Vlan40
1.1.1.1             1   FULL/BDR        00:00:30    10.10.50.2      Vlan50
1.1.1.1             1   FULL/BDR        00:00:30    10.10.60.2      Vlan60
1.1.1.1             1   FULL/BDR        00:00:30    10.10.70.2      Vlan70
11.11.11.11         1   FULL/DR         00:00:36    10.10.254.10    GigabitEthernet1/0/1
22.22.22.22         1   FULL/DR         00:00:35    10.10.254.14    GigabitEthernet1/0/2
DSW2#show ip route ospf
     10.0.0.0/8 is variably subnetted, 20 subnets, 3 masks
O       10.10.254.0 [110/2] via 10.10.254.10, 00:00:24, GigabitEthernet1/0/1
                    [110/2] via 10.10.10.2, 00:00:24, Vlan10
                    [110/2] via 10.10.20.2, 00:00:24, Vlan20
                    [110/2] via 10.10.30.2, 00:00:24, Vlan30
                    [110/2] via 10.10.40.2, 00:00:24, Vlan40
                    [110/2] via 10.10.50.2, 00:00:24, Vlan50
                    [110/2] via 10.10.60.2, 00:00:24, Vlan60
                    [110/2] via 10.10.70.2, 00:00:24, Vlan70
O       10.10.254.4 [110/2] via 10.10.254.14, 00:00:34, GigabitEthernet1/0/2
                    [110/2] via 10.10.10.2, 00:00:34, Vlan10
                    [110/2] via 10.10.20.2, 00:00:34, Vlan20
                    [110/2] via 10.10.30.2, 00:00:34, Vlan30
                    [110/2] via 10.10.40.2, 00:00:34, Vlan40
                    [110/2] via 10.10.50.2, 00:00:34, Vlan50
                    [110/2] via 10.10.60.2, 00:00:34, Vlan60
                    [110/2] via 10.10.70.2, 00:00:34, Vlan70
O*E2 0.0.0.0/0 [110/1] via 10.10.254.14, 00:17:48, GigabitEthernet1/0/2

DSW2#
```

a) Fqinjësitë dhe rrugët OSPF para ndërprerjes së link-ut

```
EDGE-R1(config)#int g0/1
EDGE-R1(config-if)#shut
EDGE-R1(config-if)#shutdown

EDGE-R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

04:22:49: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on GigabitEthernet0/1 from FULL to
DOWN, Neighbor Down: Interface down or detached
```

b) Ndërprerja e link-ut në EDGE-R1 (GigabitEthernet0/1)

```
DSW2#show ip ospf neighbor

Neighbor ID       Pri   State           Dead Time   Address         Interface
1.1.1.1             1   FULL/BDR        00:00:36    10.10.10.2      Vlan10
1.1.1.1             1   FULL/BDR        00:00:36    10.10.20.2      Vlan20
1.1.1.1             1   FULL/BDR        00:00:36    10.10.30.2      Vlan30
1.1.1.1             1   FULL/BDR        00:00:36    10.10.40.2      Vlan40
1.1.1.1             1   FULL/BDR        00:00:36    10.10.50.2      Vlan50
1.1.1.1             1   FULL/BDR        00:00:36    10.10.60.2      Vlan60
1.1.1.1             1   FULL/BDR        00:00:36    10.10.70.2      Vlan70
22.22.22.22         1   FULL/DR         00:00:32    10.10.254.14    GigabitEthernet1/0/2
DSW2#show ip route ospf
     10.0.0.0/8 is variably subnetted, 18 subnets, 3 masks
O       10.10.254.0 [110/2] via 10.10.10.2, 00:01:08, Vlan10
                    [110/2] via 10.10.20.2, 00:01:08, Vlan20
                    [110/2] via 10.10.30.2, 00:01:08, Vlan30
                    [110/2] via 10.10.40.2, 00:01:08, Vlan40
                    [110/2] via 10.10.50.2, 00:01:08, Vlan50
                    [110/2] via 10.10.60.2, 00:01:08, Vlan60
                    [110/2] via 10.10.70.2, 00:01:08, Vlan70
O       10.10.254.4 [110/2] via 10.10.254.14, 00:02:15, GigabitEthernet1/0/2
                    [110/2] via 10.10.10.2, 00:02:15, Vlan10
                    [110/2] via 10.10.20.2, 00:02:15, Vlan20
                    [110/2] via 10.10.30.2, 00:02:15, Vlan30
                    [110/2] via 10.10.40.2, 00:02:15, Vlan40
                    [110/2] via 10.10.50.2, 00:02:15, Vlan50
                    [110/2] via 10.10.60.2, 00:02:15, Vlan60
                    [110/2] via 10.10.70.2, 00:02:15, Vlan70
O*E2 0.0.0.0/0 [110/1] via 10.10.254.14, 00:19:29, GigabitEthernet1/0/2

DSW2#
```

c) Fqinjësitë dhe rrugët OSPF pas ndërprerjes së link-ut

Figura 3. Fqinjësitë dhe rrugët OSPF para dhe pas ndërprerjes së link-ut
Burimi: Autori, nga simulimi në Cisco Packet Tracer.

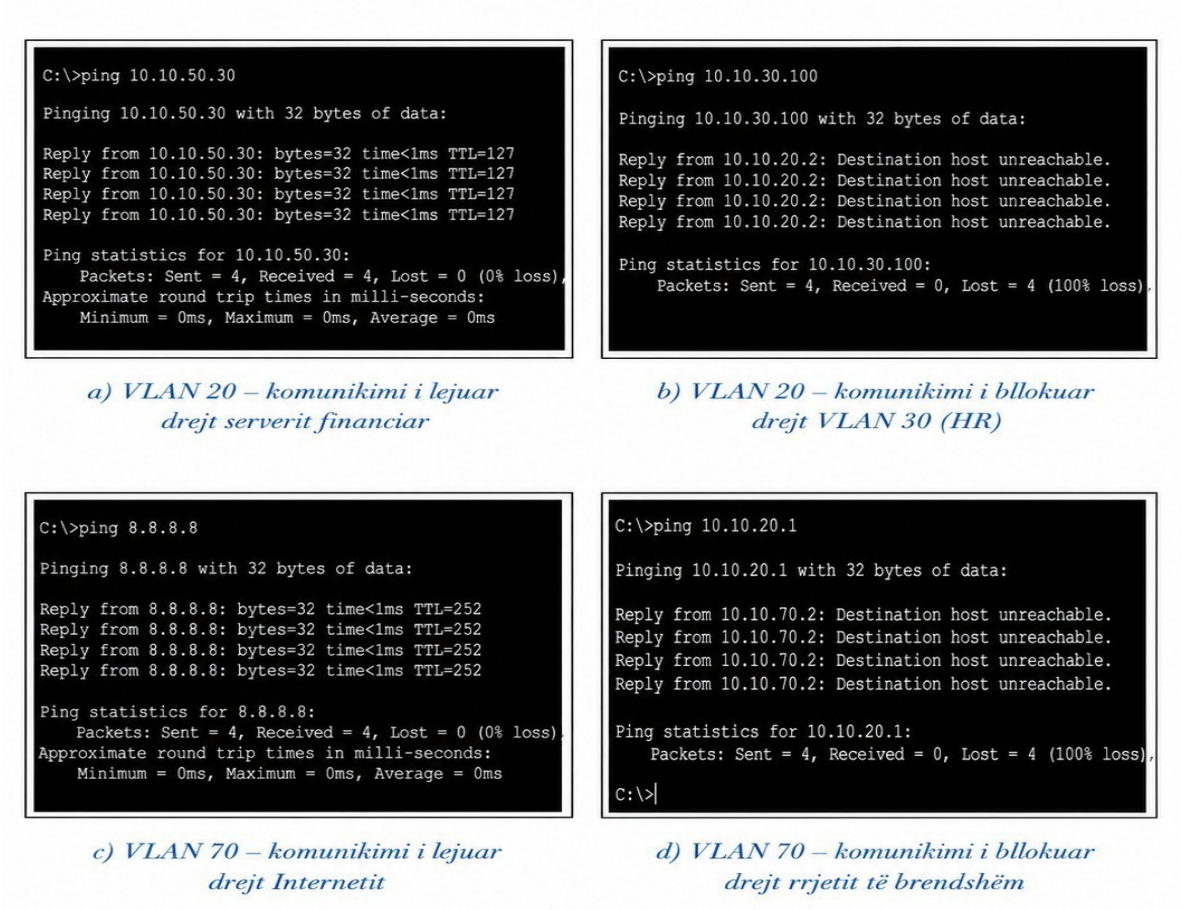

Figura 4. Testet ACL të lejuara dhe të bllokuara për VLAN 20 dhe VLAN 70
Burimi: Autori, nga simulimi në Cisco Packet Tracer.

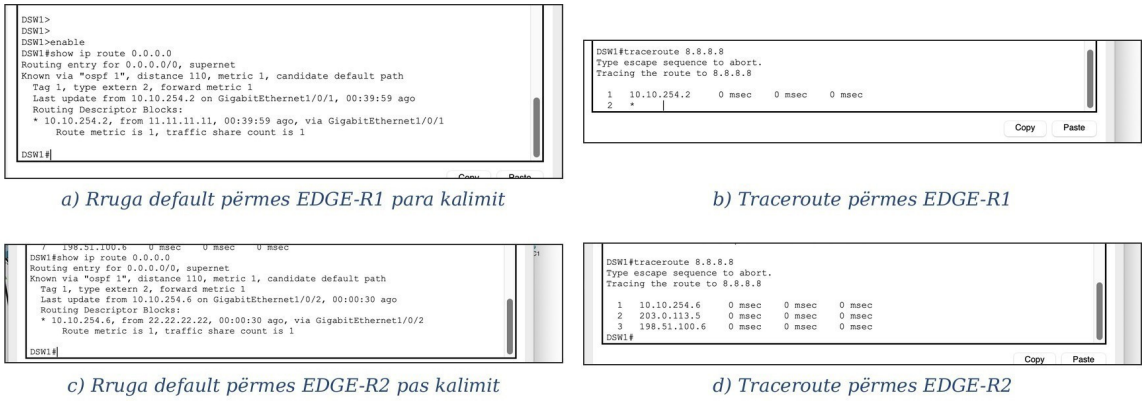

Figura 5. Kalimi i rrugës default nga EDGE-R1 te EDGE-R2
Burimi: Autori, nga simulimi në Cisco Packet Tracer.

Tabela 4. Skenarët dhe kriteret e verifikimit të sigurisë dhe redundancës
Burimi: Autori.

Nr.	Skenari	Rezultati i pritur	Evidenca që duhet të regjistrohet	Statusi
1	DHCP në VLAN 20	IP 10.10.20.x dhe gateway 10.10.20.1	ipconfig dhe/ose DHCP binding	Kaluar
2	Finance drejt 10.10.50.30	Lejohen ICMP diagnostik, HTTPS dhe SQL	Ping/shërbim + hit counters në permit	Kaluar

3	Finance drejt VLAN 30/rrjeteve të tjera të brendshme	Bllokohet nga VLAN20-IN	Ping i dështuar + deny counter	Kaluar
4	Guest drejt rrjetit të brendshëm	Lejohen vetëm DHCP/DNS; trafiku tjetër i brendshëm bllokohet	Ping i dështuar + deny counter	Kaluar
5	Dështim i DSW1/uplink-ut aktiv	Gateway virtual kalon te DSW2	show standby brief para/pas + ping i vazhdueshëm	Kaluar
6	Dështim i EDGE-R1/link-ut OSPF	Rruga default dhe trafiku kalojnë te EDGE-R2	show ip ospf/route para/pas + traceroute	Kaluar

Rezultatet e paraqitura në Tabelën 4 konfirmojnë se skenarët e testimit u realizuan me sukses. Klienti në VLAN 20 mori konfigurim të vlefshëm nga DHCP; komunikimi me serverin financiar 10.10.50.30 u lejua, ndërsa komunikimi me VLAN 30 u bllokua. VLAN 70 arriti internetin, por nuk pati akses në rrjetet e brendshme. Pas dështimit të DSW1, DSW2 mori rolin Active në HSRP, ndërsa pas ndërprerjes së EDGE-R1, rruga e parazgjedhur dhe trafiku kaluan përmes EDGE-R2. Megjithatë, simulimi mbetet provë konceptuale dhe nuk pasqyron plotësisht ngarkesën, vonesën dhe defektet fizike të një infrastrukture reale.

10.2. Kriteret e analizës së rezultateve

Rezultatet e OSPF-së tregojnë se para ndërprerjes ishin aktive fqinjësitë me EDGE-R1 dhe EDGE-R2. Pas ndërprerjes së link-ut të EDGE-R1, fqinjësia përkatëse u hoq, ndërsa rrugët mbetën të disponueshme përmes EDGE-R2. Kalimi i rrugës së parazgjedhur nga next-hop-i 10.10.254.2 te 10.10.254.6 u konfirmua gjithashtu përmes komandës traceroute. Adresa 10.10.254.6 i përket EDGE-R2, me router-id 22.22.22.22.

Rezultatet e HSRP-së tregojnë se adresa virtuale e gateway-t mbeti e pandryshuar për hostet dhe se roli Active kaloi nga DSW1 te DSW2 pas dështimit. Daljet e komandës show standby brief para dhe pas dështimit e konfirmojnë këtë kalim.

Testet e ACL-ve tregojnë se VLAN 20 komunikoi me sukses me serverin financiar 10.10.50.30, ndërsa komunikimi drejt VLAN 30 u bllokua. VLAN 70 pati akses në internet, por jo në segmentet e brendshme. Këto rezultate konfirmojnë se politikat e aksesit u zbatuan sipas konfigurimit të përcaktuar.

11. Përfundim – Çfarë u arrit dhe si mund të zgjerohet më tej projekti

Në aspekt teorik, rrjeti ndërmarrës u trajtua si sistem i integruar dhe jo thjesht si bashkësi pajisjesh. Kjo qasje është e rëndësishme sepse një ndërmarrje moderne nuk kërkon vetëm lidhje, por lidhje të kontrolluar, të dokumentuar dhe të aftë për të përballuar dështime. Përmes VLAN-eve, subnet-eve, firewall-it, ACL-ve, OSPF, HSRP dhe STP, projekti tregon se arkitektura e rrjetit mund të ndërtohet mbi parime të qarta: segmentim, minimizim aksesi, kontroll trafiku, routing dinamik dhe failover i parashikueshëm.

Në aspekt sigurie, projekti arrin të argumentojë se segmentimi departamental është themel për mbrojtjen e rrjetit të brendshëm. VLAN-et ndajnë trafikun logjikisht, por siguria reale krijohet kur kjo ndarje shoqërohet me politika firewall-i dhe rregulla të qarta aksesi. Kjo është në përputhje me rekomandimet e Scarfone dhe Hoffman (2009), të cilët e shohin firewall-in si mekanizëm të kontrollit të trafikut midis zonave me postura të ndryshme sigurie. Po ashtu, projekti lidhet me qasjen zero trust të Rose et al. (2020), sipas së cilës aksesi nuk duhet të jepet automatikisht vetëm sepse pajisja ndodhet në rrjetin e brendshëm. Për rrjedhojë, projekti nuk mbështetet te supozimi "brenda është e sigurt", por te verifikimi dhe kufizimi i vazhdueshëm.

Në aspekt qëndrueshmërie, projekti arrin të shpjegojë se redundanca duhet të jetë e pranishme në disa shtresa. STP mbron rrjetin Ethernet nga loop-et kur ekzistojnë lidhje redundante; HSRP siguron vazhdimësi të gateway-t për hostet; OSPF mundëson rrugë alternative dhe rikonvergjencë në routing. Secili protokoll zgjidh një problem të veçantë, por vlera e tyre shfaqet kur projektohen në harmoni. Moy (1998) për OSPF dhe Li et al. (1998) për HSRP ofrojnë bazën konceptuale për dy mekanizma qendrorë të disponueshmërisë në rrjetet IP. Në këtë kuptim, projekti arrin të tregojë se një rrjet i qëndrueshëm nuk është ai që nuk dështon kurrë, por ai që ka rrugë të kontrolluara për të reaguar kur dështimi ndodh.

Zbatimi në simulim është një arritje metodologjike, sepse lidh teorinë me verifikimin. Packet Tracer ose GNS3 lejojnë ndërtimin e topologjisë, konfigurimin e VLAN-eve, routing-ut, firewall-it dhe protokolleve të redundancës, si dhe testimin e skenarëve të ndryshëm (Cisco Networking Academy, n.d.; GNS3, n.d.). Përmes simulimit mund të provohet nëse departamentet komunikojnë sipas politikave, nëse trafiku i ndaluar bllokohet, nëse gateway virtual kalon nga routeri aktiv te ai standby dhe nëse routing-u dinamik rikuperohet pas ndërprerjes së një link-u. Kjo e bën projektin të verifikueshëm dhe e largon nga niveli i thjeshtë

teorik. Megjithatë, simulimi ka kufizime: nuk pasqyron gjithmonë performancën reale, ngarkesën e trafikut, sjelljen e pajisjeve fizike ose kompleksitetin e incidenteve operative.

Projekti mund të zgjerohet në disa drejtime. Zgjerimi i parë është integrimi i autentikimit të përdoruesve dhe pajisjeve përmes 802.1X, RADIUS ose sistemeve të identitetit. Kjo do ta bënte kontrollin e aksesit më të lidhur me identitetin, jo vetëm me portën ose VLAN-in. Zgjerimi i dytë është implementimi i monitorimit të centralizuar me syslog, SNMP, NetFlow ose platforma SIEM, në mënyrë që politika e sigurisë të mos jetë vetëm parandaluese, por edhe vëzhguese dhe reaguese. Zgjerimi i tretë është përdorimi i IDS/IPS për të identifikuar trafik të dyshimtë brenda dhe jashtë rrjetit. Zgjerimi i katërt është krijimi i një DMZ-je për shërbimet që duhet të aksesohen nga jashtë, duke i ndarë ato nga serverët e brendshëm kritikë.

Një drejtim tjetër zgjerimi është përfshirja e cloud-it dhe punës në distancë. Ndërmarrjet moderne shpesh nuk operojnë vetëm me serverë lokalë; ato përdorin shërbime cloud, VPN, SaaS dhe përdorues që punojnë jashtë zyrës. Kjo do të kërkonte politika më të avancuara të identitetit, tunelime të sigurta, segmentim të bazuar në aplikacione dhe integrim me qasje zero trust. Rose et al. (2020) e vendosin zero trust si qasje që mund të udhëheqë projektimin e infrastrukturave ndërmarrëse, ndaj zgjerimi i projektit drejt këtij modeli do ta bënte atë më të përshtatshëm për realitetin bashkëkohor. Në vend që rrjeti të mbështetet vetëm në VLAN dhe firewall, ai mund të kombinojë identitetin, pajisjen, kontekstin dhe politikat dinamike.

Një zgjerim i mëtejshëm mund të lidhet me automatizimin dhe menaxhimin e konfigurimeve. Në rrjetet reale, konfigurimi manual i shumë pajisjeve krijon mundësi gabimesh dhe mospërputhjesh. Përdorimi i template-ve, backup-eve automatike, kontrollit të versioneve dhe mjeteve të orkestrimit do ta bënte rrjetin më të qëndrueshëm dhe më të lehtë për auditim. Ky zgjerim nuk ndryshon parimet themelore të projektit, por e forcon zbatimin praktik të tyre. Nëse VLAN-et, rregullat e firewall-it dhe parametrat e routing-ut dokumentohen dhe aplikohen në mënyrë të standardizuar, organizata ul varësinë nga kujtesa e administratorëve individualë dhe rrit kontrollin institucional mbi infrastrukturën.

Projekti mund të zgjerohet edhe me analiza sasiore, si matja e kohës së failover-it, krahasimi i vonesës para dhe pas dështimit, vlerësimi i përdorimit të bandwidth-it dhe testimi i ngarkesës mbi serverët. Këto matje do ta bënin punimin më empirik dhe do të plotësonin analizën teorike. Për shembull, në vend që të thuhet vetëm se HSRP funksionon, mund të matet sa paketa humben gjatë kalimit. Në vend që të thuhet se OSPF gjen rrugë alternative, mund të

matet koha e konvergjencës. Kjo qasje do ta kthente projektin në bazë për studime më të avancuara.

Kështu projekti nuk mbetet vetëm model demonstrues, por mund të zhvillohet në analizë të plotë të performancës dhe sigurisë. Kjo do t'i jepte punimit karakter më të gjerë kërkimor dhe do ta lidhte më fort me nevojat praktike të ndërmarrjeve reale dhe me standardet profesionale. Zgjerimi i tillë do të rriste vlerën aplikative.

Në përfundim, ky punim tregon se dizajni i një rrjeti të sigurt shumë-departamental me redundancë kërkon mendim sistemik. Nuk mjafton të vendosen disa pajisje dhe të aktivizohen disa protokolle. Duhet të kuptohet se pse departamentet ndahen, pse aksesi kufizohet, pse protokollet e redundancës konfigurohen, si testohen dështimet dhe si dokumentohen rezultatet. Rrjeti i mirë është ai që funksionon, mbron dhe rikuperohet. Ai mbështet organizatën në punën e përditshme, ul riskun dhe krijon bazë për zgjerim të ardhshëm.

REFERENCAT

Cisco. (2023a). *Configuring DHCP.* Cisco Systems. Accessed July 19, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-12/configuration_guide/ip/b_1712_ip_9300_cg/configuring_dhcp.html

Cisco. (2023b). *Configuring VLAN trunks.* Cisco Systems. Accessed July 19, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-13/configuration_guide/vlan/b_1713_vlan_9300_cg/configuring_vlan_trunks.html

Cisco. (2023c). *Configuring VLANs.* Cisco Systems. Accessed July 19, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-13/configuration_guide/vlan/b_1713_vlan_9300_cg/configuring_vlans.html

Cisco. (2024a). *Configuring Spanning Tree Protocol.* Cisco Systems. Accessed July 19, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-15/configuration_guide/lyr2/b_1715_lyr2_9300_cg/configuring_spanning_tree_protocol.html

Cisco. (2024b). *IPv4 ACLs.* Cisco Systems. Accessed July 19, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-15/configuration_guide/sec/b_1715_sec_9300_cg/configuring_ipv4_acls.html

Cisco Networking Academy. (n.d.). *Cisco Packet Tracer.* Cisco Systems. Accessed July 19, 2026, from https://www.netacad.com/cisco-packet-tracer

GNS3. (n.d.). *GNS3 documentation.* GNS3 Technologies Inc. Accessed July 19, 2026, from https://docs.gns3.com/

IEEE. (2022). *IEEE Std 802.1Q-2022: IEEE standard for local and metropolitan area networks—Bridges and bridged networks.* IEEE Standards Association. Accessed July 19, 2026, from https://standards.ieee.org/ieee/802.1Q/10323/

Li, T., Cole, B., Morton, P., & Li, D. (1998). *Cisco Hot Standby Router Protocol (HSRP) (RFC 2281).* RFC Editor. Accessed July 19, 2026, from https://www.rfc-editor.org/info/rfc2281

Moy, J. (1998). *OSPF Version 2 (RFC 2328).* RFC Editor. Accessed July 19, 2026, from https://www.rfc-editor.org/info/rfc2328

Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). *Address allocation for private internets (RFC 1918).* RFC Editor. Accessed July 19, 2026, from https://www.rfc-editor.org/info/rfc1918

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology. Accessed July 19, 2026, from https://doi.org/10.6028/NIST.SP.800-207

Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41 Revision 1).* National Institute of Standards and Technology. Accessed July 19, 2026, from https://csrc.nist.gov/pubs/sp/800/41/r1/final