KURS NË SHQIP · NGA BAZAT NË NIVEL TË AVANCUAR

Rrjetet kompjuterike

Rrjetet kompjuterike — nga bazat te arkitektura dhe diagnostikimi i avancuar.

Kurs tekstual në shqip me 40 module, 40 mësime, 80 materiale teori/laborator, 40 kuize modulesh dhe një provim final. Përfshin manualin e studentit, laborator Linux të ekzekutueshëm, konfigurime FRRouting, fletë pune, fjalor, projekte dhe rubrikë vlerësimi. Protokollet, komandat dhe emrat teknikë ruhen në formën origjinale.

Mbulohen LAN/WAN, IPv4/IPv6, Ethernet, VLAN, STP, routing, OSPF, IS-IS, BGP dhe RPKI, multicast, QoS, wireless, DNS/DHCP, TCP/QUIC/TLS, siguria dhe VPN, MPLS/SR, EVPN/VXLAN, cloud, Kubernetes, automatizimi dhe operimi.

Ngarkesë orientuese: 200–280 orë, në varësi të përvojës dhe pajisjeve. Leximi është vetëm një pjesë e punës; pjesa kryesore është praktikë, matje, lexim dokumentacioni dhe projekt. Kërkohen përdorimi i një kompjuteri, skedarëve dhe terminalit; rrjetet mësohen nga fillimi. Modulet e avancuara ndërtohen mbi bazat.

Për praktikën bazë mjafton një VM Linux e izoluar. FRRouting, switch-e virtuale me funksione L2 dhe pajisje/AP për radio kërkohen vetëm në laboratorët përkatës. Variantet analitike janë të shënuara dhe nuk zëvendësojnë verifikimin praktik. Shembujt e konfigurimit nuk janë konfigurime prodhimi.

Pragu i kuizeve: 75%; finali: 80%; projekti praktik: 80/100 me plotësimin e kontrolleve kritike. Nuk është certifikim i një prodhuesi. Mbulimi është i gjerë, por jo pretendim se përfshin çdo protokoll, implementim ose specializim ekzistues. Materialet importohen si draft; burimet bashkëngjiten manualisht.

Si ta ndjekësh kursin

Titulli i kursit është **Rrjetet kompjuterike**. Lexo modulet në rend nëse nis nga zero. Nëse ke përvojë, përdor kuizet për të identifikuar boshllëqet, por mos kapërce laboratorët e routing-ut, MTU-së dhe sigurisë vetëm sepse njeh termat.

Rruga mësimore dhe koha orientuese

- Modulet 1–10: themelet, infrastruktura, Ethernet, adresimi dhe routing. 35–45 orë.
- Modulet 11–16: transporti, shërbimet dhe analiza e paketave. 25–35 orë.
- Modulet 17–23: routing i avancuar, redundanca, multicast dhe QoS. 35–45 orë.
- Modulet 24–30: wireless, siguria, VPN dhe WAN/MPLS. 35–45 orë.
- Modulet 31–38: datacenter, cloud, hoste, containers, automatizim dhe specializime. 40–60 orë.
- Modulet 39–40: projektim, projekt final, riprovim dhe mbrojtje. 30–50 orë.

Gjithsej 200–280 orë orientuese; kohët e laboratorëve janë pika nisjeje. Përfshihen leximi, ndërtimi i mjedisit, dokumentacioni, ushtrimet, korrigjimet dhe projektet. Nuk është pretendim se një numër i caktuar orësh mjafton për çdo profesion ose certifikim.

Çfarë kërkohet

Duhet të përdorësh skedarë dhe terminal dhe të instalosh/përdorësh një VM sipas mjedisit që ke. Për fillimin mjafton një VM Linux me rreth 2 vCPU dhe 2–4 GB RAM; fabric-u dhe topologjitë me shumë pajisje mund të kërkojnë shumë më tepër. Këto janë pika praktike nisjeje, jo garanci për çdo imazh. Nuk duhen pajisje tregtare për të mësuar adresimin dhe routing bazë. Radio, PTP hardware dhe forwarding ASIC nuk verifikohen plotësisht nga një simulator.

Mjetet bazë Linux: Bash, iproute2, iputils-ping, tcpdump, curl dhe Python 3. Përkatësisht shtohen nftables, iperf3, dig/BIND utilities dhe FRRouting. Emrat e paketave ndryshojnë sipas distribucionit. Kontrollo versionet dhe ruaji në raport. Mos përdor Packet Tracer si provë të funksioneve që imazhi i tij nuk i implementon; FRRouting nuk simulon çdo funksion switch-i tregtar. Imazhet e prodhuesve duhen marrë me licencën përkatëse.

Organizimi i provave

Për çdo laborator ruaj: qëllimin, topologjinë, komandën, kohën, rezultatin e pritur, rezultatin real dhe shpjegimin. Mos kopjo output pa e interpretuar. Një screenshot mund të ndihmojë, por konfigurimet tekstuale dhe hapat e riprodhimit janë më të lehtë për review. Kur s'ke pajisjen, dorëzo variant analitik dhe shëno qartë **analizë, pa ekzekutim**. Plotëso praktikën përpara vlerësimit të aftësisë përkatëse.

Përdor vetëm pajisje dhe rrjete laboratorike të autorizuara. Shembujt me `ADRESA`, `EMRI` ose `RESOLVER` janë placeholder dhe duhen zëvendësuar. Adresat 2001:db8::/32, 192.0.2.0/24, 198.51.100.0/24 dhe 203.0.113.0/24 janë për dokumentim, jo për reklamim publik.

Vlerësimi

Çdo kuiz moduli ka 3 pyetje me një përgjigje të saktë. Pragu 75% kërkon 3/3; pyetjet janë kontroll i shkurtër, jo matje e plotë e zotërimit. Finali ka 24 pyetje, 60 minuta dhe prag 80%: duhen 20/24. Laboratorët kanë vlerësim sipas provave dhe projekti final prag 80/100 plus kontrollet kritike. Mos e barazo kalimin e kuizit me aftësi operimi në prodhim.

Laboratori i parë

Lexo `linux/README.sq.md`. Skripti krijon vetëm namespace të izoluara, nuk ndryshon routing-un ose forwarding-un e hostit kryesor dhe nuk lidh laboratorin me Internetin. Përdor VM ku ke privilegje administrimi. Eksperimentet që ndryshojnë MTU, rrugë ose firewall bëhen në namespace-in e përcaktuar. Ndale shërbimin testues përpara pastrimit.

Deri ku shkon kursi

Kursi ndërton bazë të gjerë dhe ushtrime të avancuara, por BGP global, RF, operimi ISP, datacenter, OT dhe storage janë specializime me praktikë shtesë. Shiko `burimet.sq.md` dhe `harta-e-mbulimit.sq.md` për dokumentacionin dhe kufijtë e moduleve. Referencat zyrtare shpesh janë në anglisht; teksti mësimor është në shqip.

1. Arkitektura e rrjeteve dhe udhëtimi i paketës

Modelet, planet dhe komunikimi skaj më skaj

Teori: Modelet, planet dhe komunikimi skaj më skaj

Objektivi: të ndjekësh një kërkesë nga aplikacioni deri te serveri dhe të dallosh përgjegjësinë e secilës shtresë.

Rrjeti lidh sisteme autonome që shkëmbejnë mesazhe sipas protokolleve. LAN përshkruan një shtrirje lokale; WAN lidh vendndodhje; Interneti është bashkësi rrjetesh me administrim të pavarur. Klient/server dhe peer-to-peer përshkruajnë role aplikacionesh, jo kabllot. Topologjia fizike tregon lidhjet; topologjia logjike tregon VLAN-et, subnet-et dhe rrugët. Një lidhje fizike mund të mbajë disa rrjete logjike.

Modeli OSI ka shtresat fizike, lidhje të dhënash, rrjet, transport, sesion, prezantim dhe aplikacion. Modeli TCP/IP grupon funksionet në lidhje, Internet, transport dhe aplikacion. Këto janë mjete arsyetimi; implementimi nuk ndahet gjithmonë pastër. TLS është shembull funksioni sigurie mbi transport, ndërsa QUIC bashkon transportin me mekanizma kriptografikë.

Kur hapet një faqe, klienti zgjidh emrin me DNS, zgjedh rrugën, gjen adresën MAC të hop-it të radhës dhe dërgon të dhënat. Enkapsulimi vendos të dhënat e aplikacionit brenda transportit, paketës IP dhe frame-it. Router-i heq frame-in hyrës dhe ndërton një frame tjetër për daljen. Adresat MAC zakonisht ndryshojnë në çdo segment; adresa IP e destinacionit mbetet e njëjtë përgjatë routing-ut të zakonshëm, por NAT dhe tunelet shtojnë përjashtime.

Plani i të dhënave përcjell paketa; plani i kontrollit ndërton gjendjen e përcjelljes; plani i menaxhimit administron pajisjen. Një sesion SSH që punon nuk provon se aplikacioni i përdoruesit punon. Rruga e kthimit mund të ndryshojë nga rruga e vajtjes. Për çdo përfundim kërko pikën e vrojtimit: host, switch, router apo aplikacion.

Shembull: PC 10.10.10.10/24 komunikon me 10.20.20.20. PC-ja dërgon frame drejt MAC-ut të gateway-t 10.10.10.1, jo drejt MAC-ut të serverit të largët. Switch-i përcjell sipas MAC/VLAN; router-i sipas IP/prefiksit.

Laborator: Modelet, planet dhe komunikimi skaj më skaj

Koha: 90 minuta. **Mjedisi:** një host Windows ose Linux, rrjet laboratorik dhe skeda e punës së kursit. Nuk kërkohet ndryshim konfigurimi.

- Vizato PC → switch → router → server. Shëno IP, MAC, subnet, VLAN dhe gateway për çdo ndërfaqe.
- Në Linux lexo `ip address`, `ip route` dhe `ip neigh`; në PowerShell përdor `Get-NetIPConfiguration`, `Get-NetRoute` dhe `Get-NetNeighbor`. Mos përziej sintaksat.

- Zgjidh një destinacion në subnet dhe një jashtë tij. Për secilin shkruaj vendimin që merr hosti para dërgimit.
- Në një kapje laboratorike identifiko Ethernet, IP, transportin dhe aplikacionin. Në Wi-Fi kapja mund të paraqitet e dekapsuluar si Ethernet; shëno çfarë sheh realisht.
- Defekti analitik: gateway i gabuar, por serveri lokal punon. Jep dy prova që ndajnë problemin e routing-ut nga problemi DNS.

Dorëzimi: diagram, tabelë e dy flukseve dhe një shpjegim i enkapsulimit me adresat konkrete. **Pranimi:** destinacioni jashtë subnet-it lidhet me MAC-un e hop-it të radhës; IP-ja dhe MAC-u nuk ngatërrohen; shpjegohet edhe kthimi. **Thellim:** cakto cilit plan i përket çdo tabelë dhe komandë. Pa host përdor adresat e shembullit dhe shëno dorëzimin si analizë.

2. Matematikë, kapacitet dhe performancë

Bitët, vonesa, humbja dhe buxheti i trafikut

Teori: Bitët, vonesa, humbja dhe buxheti i trafikut

Objektivi: të llogaritësh kapacitetin e nevojshëm dhe të dallosh bandwidth, throughput dhe goodput.

Një byte ka 8 bit. Shpejtësitë e lidhjeve zakonisht shprehen në bit/s me shumëfishime dhjetore; madhësitë e skedarëve mund të përdorin MB ose MiB. 100 MB të dhjetorë mbi 100 Mbit/s kërkojnë idealisht 8 sekonda, para overhead-it dhe kufizimeve të transportit. Throughput përfshin trafikun e matur në një pikë; goodput është pjesa e dobishme e aplikacionit.

Vonesa totale ka serializimin L/R, përhapjen d/v, përpunimin dhe pritjen në radhë. Një frame 1500 byte në 100 Mbit/s kërkon 120 mikrosekonda serializim, pa numëruar overhead shtesë. RTT është vajtje-kthimi; nuk është domosdoshmërisht dyfishi i një matjeje njëdrejtimëshe. Jitter është ndryshimi i vonesës dhe duhet shoqëruar me metodën e matjes.

Bandwidth-delay product tregon të dhënat që mund të jenë në fluturim. Me 1 Gbit/s dhe RTT 40 ms, BDP është 40 Mbit, pra rreth 5 MB. Një dritare efektive 1 MB e kufizon rrjedhën ideale afërsisht në 200 Mbit/s në atë RTT, para faktorëve të tjerë. Humbjet dhe kontrolli i congestion-it mund ta ulin më tej.

Kapaciteti nuk planifikohet vetëm me mesatare. Microburst-et mbushin buffer-at edhe kur mesatarja është e ulët. Percentilet p95/p99 zbulojnë bishtin e shpërndarjes; nuk llogariten duke mesatarizuar verbërisht percentilet e intervaleve. Oversubscription 4:1 do të thotë që kapaciteti i agreguar i burimeve është katër herë dalja, jo se çdo përdorues merr gjithmonë një të katërtën.

Shembull: 48 porta me 1 Gbit/s dhe dy uplink-e 10 Gbit/s japin raport nominal 48:20 = 2.4:1, nëse të dy uplink-et mund të përdoren. Një fluks i vetëm mbi LAG mund të mbetet në një anëtar.

Laborator: Bitët, vonesa, humbja dhe buxheti i trafikut

Koha: 120 minuta. **Mjedisi:** dy hoste laboratorikë me `iperf3`, ose analizë e të dhënave të ofruara.

- Llogarit kohën ideale për 2 GB në 100 Mbit/s, 1 Gbit/s dhe 10 Gbit/s. Shëno nëse përdor GB apo GiB.
- Në serverin laboratorik nis `iperf3 -s`; në klient përdor `iperf3 -c ADRESA_E_SERVERIT -t 20`. Zëvendëso adresën dhe kryej tri matje pa trafik tjetër të qëllimshëm.
- Përsërit me katër rrjedha, `-P 4`, dhe në drejtimin e kundërt me `-R`. Krahaso CPU-në, ndërfaqet dhe RTT para se të fajësosh kabllon.
- Për skenarin 500 Mbit/s dhe RTT 80 ms llogarit BDP. Pastaj vlerëso kufirin që sjell dritarja 2 MB.
- Defekti: throughput bie vetëm në intervale të shkurtra me shumë dërgues. Kërko prova për queue drops dhe microburst, jo vetëm mesatare pesëminutëshe.

Dorëzimi: tabelë matjesh, njësitë, llogaritjet dhe kufizimet e eksperimentit. **Pranimi:** dallohen rezultatet teorike nga ato të matura; 500 Mbit/s × 0.08 s del 40 Mbit; nuk pretendohet se ping mat bandwidth-in. **Thellim:** projekto një test që ndan kufirin e CPU-së nga kufiri i rrjetit.

3. Shtresa fizike dhe infrastruktura

Bakri, fibra, optika, energjia dhe instalimi

Teori: Bakri, fibra, optika, energjia dhe instalimi

Objektivi: të zgjedhësh mediumin dhe të diagnostikosh një lidhje fizike me matje.

Kabllot me çifte të përdredhura reduktojnë interferencën përmes transmetimit diferencial. Kategoria, gjatësia, përfundimi dhe mjedisi ndikojnë shpejtësinë e arritshme; një kanal bakri Ethernet i strukturuar zakonisht projektohet deri në 100 m për standardet përkatëse, por jo çdo shpejtësi mbështetet në çdo kategori për atë distancë. Patch panel, prizat dhe kabllot lidhëse hyjnë në buxhetin e kanalit.

Fibra multimode dhe single-mode ndryshojnë në përhapjen optike, distancat dhe transceiver-at. Përputh gjatësinë valore, tipin e fibrës, konektorin, shpejtësinë dhe karakteristikat e të dy skajeve. SFP, SFP+ dhe QSFP përshkruajnë familje modulesh/formatesh, jo një distancë universale. DAC dhe AOC shërbejnë shpesh për lidhje të shkurtra në rack ose datacenter.

Humbja optike llogaritet në dB; fuqia absolute shënohet në dBm. Nëse transmetuesi jep -3 dBm dhe rruga humb 5 dB, marrësi sheh afërsisht -8 dBm. Krahasoje me ndjeshmërinë dhe kufirin e mbingarkimit të marrësit dhe lër marzh. DOM jep telemetri të modulit; power meter dhe OTDR matin aspekte të ndryshme të rrugës optike. Një kabllo me dritë nuk është domosdoshmërisht lidhje pa gabime.

Autonegotiation, duplex dhe shpejtësia duhet të përputhen. CRC/FCS, symbol errors dhe link flaps janë prova, por jo diagnozë unike. PoE kërkon buxhet total të switch-it, klasë/fuqi në portë dhe llogaritje të humbjeve. LLDP mund të ndihmojë identifikimin dhe negocimin e fuqisë. Rack-u kërkon etiketa, ventilim, tokëzim të përshtatshëm dhe furnizim rezervë.

Shembull: një uplink me CRC në rritje dhe fuqi optike pranë pragut kontrollohet për ndotje, përkulje dhe përputhje modulesh përpara ndryshimeve në routing.

Laborator: Bakri, fibra, optika, energjia dhe instalimi

Koha: 120 minuta. **Mjedisi:** switch dhe dy lidhje laboratorike; alternativë analitike me inventar.

- Ndërto inventarin e katër lidhjeve: medium, gjatësi, konektor, transceiver, shpejtësi, portë dhe pajisje fundore.
- Regjistro counters para testit, gjenero trafik të kontrolluar dhe regjistro diferencën. Dallo numrin total të gabimeve nga shpejtësia e shtimit të tyre.
- Llogarit buxhetin për transmetues -2 dBm, fibra 3 dB, konektorë 1.5 dB dhe bashkime 0.5 dB. Krahaso fuqinë e marrë me ndjeshmërinë -12 dBm.
- Planifiko 12 AP me kërkesë 25 W secili dhe 20% rezervë. Kontrollo nëse buxheti 250 W mjafton.

- Defekti: zëvendëso vetëm një komponent laboratorik për herë; pas çdo prove rikthe gjendjen dhe shëno rezultatin. Mos shiko brenda fibrës optike.

Dorëzimi: skema e rack-ut, buxheti optik/PoE dhe raporti i counters. **Pranimi:** fuqia e pritshme është -7 dBm; marzhi ndaj ndjeshmërisë është 5 dB përpara rezervave të projektimit; kërkesa PoE me rezervë është 360 W. **Thellim:** shpjego pse pastrimi dhe certifikimi i kabllos japin prova të ndryshme.

4. Ethernet dhe switching

Frame-et, MAC learning dhe domenet e transmetimit

Teori: Frame-et, MAC learning dhe domenet e transmetimit

Objektivi: të parashikosh në cilat porta del një frame.

Ethernet përdor adresa MAC dhe një format frame-i me adresa burimi/destinacioni, tip ose gjatësi, payload dhe FCS. Preamble dhe inter-frame gap shpenzojnë kohë në tel, megjithëse zakonisht nuk shfaqen në kapjen e hostit. MTU 1500 për IP nuk është madhësia totale e trafikut fizik. CSMA/CD lidhet me Ethernet-in e vjetër half-duplex; lidhjet switched full-duplex nuk përdorin collision detection për operimin normal.

Switch-i mëson adresën MAC të burimit bashkë me VLAN-in dhe portën hyrëse. Nëse destinacioni unicast njihet, dërgon drejt portës përkatëse; nëse nuk njihet, flood brenda VLAN-it, duke përjashtuar portën hyrëse dhe portat që nuk përcjellin. Broadcast-i gjithashtu përhapet brenda atij domeni. Multicast-i mund të kufizohet nga snooping, sipas gjendjes dhe konfigurimit.

Tabela MAC plaket; ajo nuk është inventar i përhershëm. MAC flapping mund të tregojë loop, migrim virtual ose multihoming të konfiguruar gabim. Një switch L3 mund të kryejë si bridging ashtu edhe routing; emri i pajisjes nuk përcakton vetë funksionin. ARP e lidh IP-në me MAC-un; tabela MAC e switch-it e lidh MAC-un me portën. Janë dy tabela me qëllime të ndryshme.

Store-and-forward merr frame-in dhe mund të kontrollojë FCS para përcjelljes. Cut-through ul vonesën në kushte të përshtatshme, por mund të nisë dërgimin para zbulimit të gabimeve. Buffer-at, shpejtësitë e ndryshme dhe congestion-i ndikojnë sjelljen reale.

Shembull: A hyn në portën 1 me MAC AA; destinacioni BB është i panjohur. Switch-i mëson AA→1 dhe flood-on frame-in. Kur B përgjigjet nga porta 2, mëson BB→2; rrjedha pasuese A→B bëhet unicast drejt portës 2.

Laborator: Frame-et, MAC learning dhe domenet e transmetimit

Koha: 90 minuta. **Mjedisi:** një bridge Linux nga laboratori bazë ose switch virtual dhe tre hoste.

- Vendos A, B dhe C në të njëjtin VLAN. Lexo tabelën MAC para komunikimit. Në Linux bridge përdor `bridge fdb show`.
- Gjenero ping A→B dhe lexojeni përsëri. Shëno cilat MAC janë mësuar dinamikisht dhe cilat hyrje janë lokale/statike.
- Kap ARP dhe ICMP në C. Nëse kapja realizohet vetëm nga porta e C-së, shpjego pse unicast-i A→B mund të mos shihet pas mësimit.
- Analizo skenarin AA→portë 1, BB→portë 2 dhe VLAN 10 në porta 1–3. Parashiko daljen për destinacion BB, CC të panjohur dhe broadcast.

- Defekti: B zhvendoset në një portë tjetër. Vëzhgo rimësimin pas frame-it me burim B dhe krahasoje me pritjen e aging-ut.
- Regjistro veçmas hyrjet statike dhe dinamike që të mos interpretohet një adresë e vetë bridge-it si host i mësuar.

Dorëzimi: tri gjendje të tabelës dhe shpjegim i flood-it. **Pranimi:** mësimi lidhet me burimin; flood-i kufizohet në VLAN; port mirroring nuk supozohet i aktivizuar. **Thellim:** analizo ndikimin e një tabele MAC të mbushur pa gjeneruar trafik sulmues.

5. VLAN, trunk dhe segmentimi L2

802.1Q, gateway dhe ndarja e domeneve

Teori: 802.1Q, gateway dhe ndarja e domeneve

Objektivi: të ndërtosh ndarje L2 dhe të dallosh kur kërkohet routing.

Një VLAN krijon domen logjik broadcast-i mbi infrastrukturë të përbashkët. Porta access zakonisht lidh pajisje që dërgojnë frame pa tag; trunk-u transporton disa VLAN-e me tag 802.1Q. Tag-u përmban identifikuesin VLAN dhe fusha prioriteti. ID-të e përdorshme dhe sjelljet e rezervuara varen nga standardi dhe pajisja; intervali i zakonshëm i VLAN-eve të konfigurueshme është 1–4094.

PVID klasifikon trafikun hyrës pa tag; koncepti native VLAN përcakton sjelljen e trafikut pa tag në një trunk sipas platformës. Mos supozo se të gjithë prodhuesit dërgojnë ose pranojnë native VLAN në të njëjtën mënyrë. Lista allowed VLAN dhe përputhja në të dy skajet janë vendimtare. Trunk-u nuk bën routing ndërmjet VLAN-eve.

Komunikimi ndërmjet VLAN-eve kërkon ndërfaqe L3: nënndërfaqe të një router-i ose SVI në switch L3. Një VLAN dhe një subnet shpesh korrespondojnë në projektim, por janë koncepte të ndryshme. Mund të vendosësh disa subnet-e në të njëjtin VLAN, megjithëse kjo ndërlikon operimin dhe nuk krijon izolim L2.

Voice VLAN, VLAN menaxhimi dhe VLAN për mysafirë ndihmojnë organizimin. Izolimi i sigurisë kërkon edhe policy L3/L4, kontroll të portave dhe plane menaxhimi. QinQ vendos një tag shërbimi mbi tag-un e klientit për transport operatori; kërkon kontroll të MTU-së dhe kufijve të domenit.

Shembull: përdoruesit VLAN 10 kanë 10.10.10.0/24; serverët VLAN 20 kanë 10.20.20.0/24. Lejo DNS dhe aplikacionin e nevojshëm mes tyre, jo çdo trafik. Një trunk me vetëm VLAN 10 do ta ndërpresë VLAN 20 edhe nëse gateway-t janë të saktë.

Laborator: 802.1Q, gateway dhe ndarja e domeneve

Koha: 120 minuta. **Mjedisi:** dy switch-e virtuale me 802.1Q dhe router L3; në mungesë pajisjesh përdor analizë konfigurimesh.

- Krijo planin VLAN 10 përdorues, 20 serverë dhe 99 menaxhim. Shëno subnet-in dhe gateway-n për secilin.
- Konfiguro porta access për dy hoste në VLAN 10 në switch-e të ndryshme. Konfiguro trunk-un me VLAN-et e lejuara të përcaktuara shprehimisht.
- Verifiko fillimisht komunikimin brenda VLAN 10. Shto gateway-t L3, pastaj provo trafikun e lejuar drejt VLAN 20.

- Hiq VLAN 20 nga lista allowed vetëm në një skaj laboratorik. Ruaj provën e dështimit dhe identifiko pse ping mes gateway-ve nuk e provon të gjithë shërbimin.
- Rikthe konfigurimin. Kontrollo trafikun pa tag, native/PVID dhe porta të papërdorura me dokumentacionin e pajisjes.

Dorëzimi: tabelë portash, konfigurime dhe matricë testesh pozitive/negative. **Pranimi:** VLAN 10 kalon trunk-un; VLAN 20 rikthehet pas korrigjimit; rrugëtimi dhe policy shpjegohen veçmas. **Thellim:** llogarit overhead-in dhe planifiko QinQ për dy klientë që përdorin të njëjtat ID VLAN.

6. STP, LACP dhe disponueshmëria L2

Loop-et, pemët dhe lidhjet e agreguara

Teori: Loop-et, pemët dhe lidhjet e agreguara

Objektivi: të projektosh redundancë pa krijuar loop dhe të shpjegosh kufijtë e një LAG-u.

Frame-i Ethernet nuk ka TTL si IP-ja. Një loop L2 mund të ripërhapë broadcast dhe unknown unicast, të shkaktojë MAC flapping dhe të konsumojë kapacitetin. STP ndërton topologji pa cikël duke bllokuar rrugë rezervë. Root bridge zgjidhet me bridge ID më të ulët, ku prioriteti dhe identifikuesit përkatës ndikojnë zgjedhjen. Root port ofron rrugën më të mirë drejt root-it; designated port përcjell për segmentin; portat alternative mbeten rezervë sipas variantit.

RSTP përshpejton tranzicionet me role dhe mekanizma të ndryshëm nga STP klasik. MSTP map-on VLAN-e në instanca. Përputhja e emrit, revision dhe mapping është e rëndësishme për kufijtë e rajonit MST. Edge/PortFast përdoret për porta fundore, jo verbërisht për uplink-e. BPDU guard mbron supozimin se aty nuk lidhet switch; root guard dhe loop guard adresojnë raste të tjera.

LACP negocion një bundle lidhjesh të përputhshme. Hash-i shpërndan flukse në anëtarë; një fluks zakonisht qëndron në një anëtar për të shmangur riorganizimin. Dy lidhje 10 Gbit/s nuk garantojnë 20 Gbit/s për një sesion. Minimum links dhe gjendja e anëtarëve ndikojnë disponueshmërinë. Agregimi statik me mospërputhje është veçanërisht problematik.

MLAG dhe stacking mundësojnë lidhje drejt dy pajisjeve, por sjellin kontroll shtesë: peer-link, keepalive, dual-active dhe sjellje në ndarje. Nuk janë sinonime të LACP ose protokoll universal. Routing në access ose fabric mund të zvogëlojë domenet L2 të dështimit.

Shembull: cakto root-in pranë gateway-t kryesor dhe root-in rezervë shprehimisht; mos ia lër zgjedhjen rastësisë së MAC-ut.

Laborator: Loop-et, pemët dhe lidhjet e agreguara

Koha: 150 minuta. **Mjedisi:** tre switch-e virtuale me RSTP dhe LACP; topologjia është e izoluar.

- Vizato trekëndëshin S1–S2–S3–S1 dhe cakto root S1 me prioritet të përshtatshëm. Para lidhjes së tretë verifiko se STP është aktiv.
- Regjistro root ID, rolet dhe gjendjet e portave. Parashiko portën alternative nga kostot; pastaj krahasoje me gjendjen reale.
- Shkëput një uplink në emulator dhe mat paketat e humbura gjatë konvergjencës; mos e përshkruaj vetëm si “i shpejtë”.

- Në një segment të veçantë ndërto LAG me dy anëtarë dhe LACP. Gjenero një, pastaj disa flukse; krahaso counters për anëtar.
- Defekti: një anëtar ka VLAN/MTU të ndryshëm. Regjistro nëse platforma e pezullon apo krijon trafik të pjesshëm dhe korrigjoje.

Dorëzimi: topologji, gjendje para/pas, konfigurimi i LAG-ut dhe koha e rikuperimit. **Pranimi:** nuk ka loop; redundanca testohet; throughput i një fluksi nuk barazohet me shumën e anëtarëve. **Thellim:** paraqit tabelë të dështimeve MLAG për peer-link dhe keepalive pa i simuluar në rrjet real.

7. IPv4 dhe planifikimi i adresave

Binari, CIDR, VLSM dhe agregimi

Teori: Binari, CIDR, VLSM dhe agregimi

Objektivi: të llogaritësh subnet-e dhe të ndërtosh plan adresimi pa mbivendosje.

IPv4 ka 32 bit. Prefiksi /n përcakton bitët e rrjetit; bitët e mbetur përcaktojnë hapësirën e adresave. Për /26 mbeten 6 bit, pra 64 adresa. Në subnet-in klasik me broadcast ka 62 hoste të zakonshme, por formula 2^h−2 nuk përdoret verbërisht: /31 për lidhje point-to-point dhe /32 për një adresë të vetme kanë përdorime të posaçme.

Adresa e rrjetit del nga AND bit më bit mes adresës dhe maskës. 192.168.50.77/26 bie në bllokun 64–127: rrjeti .64, broadcast .127, hostet .65–.126. Një host e përcakton nëse destinacioni është lokal përmes prefiksit dhe tabelës së routing-ut; ngjashmëria vizuale e adresave nuk mjafton.

CIDR lejon prefikse me gjatësi të ndryshme; VLSM ndan bllokun sipas nevojës. Ndaj fillimisht segmentet më të mëdha, rezervo rritje dhe dokumento kufijtë. Për 100, 50 dhe 20 hoste brenda 10.40.0.0/24 mund të përdorësh /25, /26 dhe /27, duke lënë hapësirë rezervë. Agregimi kërkon vazhdimësi dhe rreshtim binar; dy /24 fqinjë nuk bëhen gjithmonë /23.

Adresat private janë 10.0.0.0/8, 172.16.0.0/12 dhe 192.168.0.0/16. Loopback, link-local, multicast dhe blloqet e dokumentimit kanë kuptime të veçanta. Private nuk do të thotë automatikisht e sigurt. Adresat e mbivendosura mes partnerësh, VPN-sh dhe cloud-it krijojnë probleme routing-u edhe nëse të dy palët përdorin adresim privat.

Shembull: 10.0.2.0/24 dhe 10.0.3.0/24 përmblidhen në 10.0.2.0/23; 10.0.3.0/24 dhe 10.0.4.0/24 jo në një /23 të vetëm që i përfshin vetëm ato.

Laborator: Binari, CIDR, VLSM dhe agregimi

Koha: 150 minuta. **Mjedisi:** letër dhe Python 3; nuk nevojiten privilegje.

- Pa kalkulator gjej rrjetin, broadcast-in dhe intervalin për 172.20.37.99/20, 10.8.5.201/27 dhe 192.168.50.77/26.
- Kontrollo përgjigjet në Python me `import ipaddress` dhe `ipaddress.ip_interface('192.168.50.77/26').network`. Mos e përdor rezultatin pa shpjeguar bitët.
- Ndaj 10.40.0.0/24 për 100, 50 dhe 20 hoste me gateway brenda kapacitetit. Shëno rezervën dhe kontrollo që subnet-et nuk mbivendosen.
- Ndërto plan për tri degë që mund të përmblidhen në prefikse të qarta. Shëno adresat loopback dhe transit veçmas nga përdoruesit.

- Defekti: një host në /25 është konfiguruar /24. Shpjego pse mund të provojë ARP drejt adresave që në projekt janë përtej router-it.

Dorëzimi: zgjidhje me binar, tabelë VLSM dhe validim me `ipaddress`. **Pranimi:** /20 i shembullit fillon në 172.20.32.0 dhe mbaron në 172.20.47.255; përjashtimet /31 dhe /32 përmenden saktë. **Thellim:** argumento pse një aggregate mund të tërheqë trafik për subnet-e që nuk ekzistojnë dhe si ndihmon një discard route e kontrolluar.

8. IPv6 dhe tranzicioni

Prefikset, SLAAC, DHCPv6 dhe dual stack

Teori: Prefikset, SLAAC, DHCPv6 dhe dual stack

Objektivi: të projektosh adresim IPv6 dhe të kuptosh varësitë e një hosti dual stack.

IPv6 përdor 128 bit me shkrim heksadecimal. Zerot udhëheqëse të një grupi hiqen dhe një varg grupesh zero mund të shkurtohet me :: vetëm një herë. 2001:db8 është bllok dokumentimi; nuk është prefiks prodhimi. Global unicast shërben për routing global, link-local për komunikim në një lidhje dhe ULA për skenarë lokalë me planifikim. IPv6 nuk ka broadcast; përdor multicast dhe anycast kur është e nevojshme.

Një LAN që përdor SLAAC zakonisht ka /64. Prefikse /127 përdoren në lidhje router-router dhe /128 në loopback. Router Advertisement shpall prefikse dhe informacione të gateway-t. DHCPv6 mund të japë adresa dhe parametra, por mekanizmi standard i default router-it mbetet RA. DNS mund të njoftohet përmes RA ose DHCPv6 sipas klientit dhe konfigurimit.

SLAAC nuk kërkon domosdoshmërisht EUI-64: adresat e qëndrueshme private dhe temporary addresses shmangin ekspozimin e drejtpërdrejtë të MAC-ut. Duplicate Address Detection kontrollon përdorimin e adresës në lidhje. Neighbor Discovery përdor ICMPv6, prandaj bllokimi i gjithë ICMPv6 prish funksione themelore. Router-at IPv6 nuk fragmentojnë paketat tranzit; Path MTU Discovery kërkon trajtim të saktë të Packet Too Big.

Dual stack do të thotë operim i dy planeve IP me policy dhe monitorim për të dy. NAT64/DNS64 lejon disa klientë IPv6-only të arrijnë shërbime IPv4; nuk është zgjidhje universale për protokollet me adresa të futura në payload. 464XLAT shton përkthim në skajin e klientit për skenarë të caktuar. Tunelimi dhe përkthimi kanë overhead dhe kufizime të ndryshme.

Shembull: një /48 përmban 65 536 subnet-e /64. Nëse ndahet sipas degëve, rezervo blloqe të rreshtuara që përmblidhen lehtë dhe ruaj IPAM për të dy familjet.

Laborator: Prefikset, SLAAC, DHCPv6 dhe dual stack

Koha: 150 minuta. **Mjedisi:** dy namespace nga laboratori Linux dhe një router virtual për RA nëse disponohet.

- Zgjero dhe shkurto tri adresa IPv6. Ndaj 2001:db8:1200::/48 në blloqe /56 për degë dhe /64 për VLAN-e.
- Në Linux lexo `ip -6 address`, `ip -6 route` dhe `ip -6 neigh`. Për link-local shëno ndërfaqen ose zone ID kur kërkohet.
- Konfiguro adresat statike të dhëna në laboratorin e izoluar dhe provo IPv6 veçmas nga IPv4. Një ping IPv4 nuk është provë e IPv6.
- Në një kapje RA identifiko router lifetime, prefix information dhe flamujt përkatës. Dallo prefiksin on-link nga adresa e default router-it.

- Defekti analitik: DHCPv6 jep adresë, por mungon RA/default route. Parashiko komunikimin lokal dhe atë jashtë subnet-it.

Dorëzimi: plan /48→/56→/64 dhe prova të ndara IPv4/IPv6. **Pranimi:** /48 ka 256 blloqe /56; secili /56 ka 256 subnet-e /64; gateway nuk nxirret gabimisht nga DHCPv6. **Thellim:** projekto test për DNS64, një destinacion me vetëm rekord A dhe një aplikacion që përdor literal IPv4.

9. ARP, NDP dhe zbulimi i fqinjëve

Gjendjet e cache-it dhe dështimet lokale

Teori: Gjendjet e cache-it dhe dështimet lokale

Objektivi: të ndash mungesën e fqinjit nga mungesa e rrugës.

ARP zgjidh një adresë IPv4 të hop-it të radhës në adresë të lidhjes lokale, zakonisht MAC Ethernet. Kërkesa ARP shpërndahet në broadcast; përgjigjja zakonisht vjen unicast. Router-i nuk e përcjell broadcast-in ARP në subnet tjetër. Për një server të largët kërkohet MAC-u i gateway-t, jo MAC-u i serverit. ARP cache ka jetëgjatësi dhe gjendje që varen nga implementimi.

Gratuitous ARP dhe ARP announcements përdoren për njoftim ndryshimesh dhe kontrolle konfliktesh. Proxy ARP përgjigjet në emër të një adrese tjetër në skenarë të kontrolluar, por mund të fshehë maska dhe projektim të gabuar. ARP vetë nuk autentikon pronarin e adresës; dynamic ARP inspection dhe lidhja me DHCP snooping mund të reduktojnë manipulimin brenda një domeni.

IPv6 përdor Neighbor Solicitation dhe Neighbor Advertisement si pjesë e NDP. Solicited-node multicast kufizon kërkimin në grupin përkatës. Neighbor Unreachability Detection kalon në gjendje si REACHABLE, STALE, DELAY dhe PROBE sipas implementimit. STALE nuk do të thotë domosdoshmërisht se lidhja ka dështuar; do të thotë se arritshmëria duhet rivlerësuar kur përdoret hyrja.

NDP përfshin edhe RA/RS dhe mekanizma të tjerë. RA guard dhe politika e portave ndihmojnë mbrojtjen e segmentit, por duhet të zbatohen me mbështetjen reale të platformës. Në fabric EVPN, ARP/ND suppression mund të përgjigjet nga gjendja e kontrollit dhe të ulë flooding-un; gjendja e vjetruar krijon një klasë tjetër problemesh.

Shembull diagnostikimi: default route ekziston, por hyrja e gateway-t është INCOMPLETE. Heto VLAN, link, adresën e gateway-t dhe filtrimin lokal para se të ndryshosh BGP. Një tabelë MAC e saktë nuk provon se gateway ka IP-në e pritur.

Laborator: Gjendjet e cache-it dhe dështimet lokale

Koha: 90 minuta. **Mjedisi:** namespace a dhe b në laboratorin Linux të kursit, me subnet të përbashkët.

- Regjistro `ip -n cn-a neigh show` para trafikut. Dërgo ping nga a te b dhe regjistro gjendjen pas tij.
- Kap ARP me `ip netns exec cn-a tcpdump -ni eth0 -c 10 arp` në një terminal dhe gjenero trafik nga një tjetër. Ndalo kapjen nëse limiti nuk arrihet.
- Për IPv6 përdor filtrin e kapjes `icmp6` dhe identifiko NS/NA. Dallo DAD nga kërkimi i një fqinji për trafik normal.

- Shkëput ndërfaqen e b vetëm brenda laboratorit, provo përsëri dhe shëno kohën/gjendjet. Riktheje për të mos ndikuar laboratorët pasues.
- Analizo një rast me gateway të vendosur në VLAN tjetër dhe një rast me IP të dyfishuar. Jep provën që i ndan.

Dorëzimi: kapje e shkurtër, adresat e kërkesës dhe tabela e gjendjeve. **Pranimi:** kërkohet hop-i i duhur; STALE nuk etiketohet automatikisht si defekt; përfundimi lidhet me një paketë konkrete. **Thellim:** shpjego çfarë ndryshon kur aktivizohet proxy ARP ose ARP suppression.

10. Routing dhe tabelat e përcjelljes

Longest prefix match, RIB/FIB dhe rrugët statike

Teori: Longest prefix match, RIB/FIB dhe rrugët statike

Objektivi: të parashikosh daljen e paketës nga tabela e routing-ut dhe të identifikosh kthimin.

RIB përmban informacionin e routing-ut të kontrollit; FIB është gjendja e përdorur për përcjellje. Jo çdo rrugë e mësuar instalohet në FIB. Një kandidat duhet të ketë next hop të zgjidhshëm, të fitojë përzgjedhjen për prefiksin e vet dhe të përputhet me kufizimet e platformës. Rruga connected vjen nga një ndërfaqe e adresuar; rruga statike konfigurohet; protokollet dinamike shkëmbejnë arritshmëri.

Përcjellja përdor prefiksin më specifik që përputhet. Nëse ekzistojnë /16 dhe /24, destinacioni brenda /24 ndjek /24, pavarësisht se /16 ka metrikë më të ulët. Preferenca administrative ndihmon zgjedhjen mes burimeve për të njëjtin prefiks në platforma që e përdorin; vlerat nuk janë universale. Metrikat e protokolleve të ndryshme nuk krahasohen si e njëjta njësi.

Default route është /0 dhe përdoret kur mungon rrugë më specifike. Next-hop recursion zgjidh një next hop përmes një rruge tjetër. ECMP lejon disa dalje me kosto të barabartë dhe zakonisht shpërndan sipas hash-it të fluksit. Policy-based routing mund ta ndryshojë vendimin sipas burimit ose kushteve të tjera; Linux policy routing përdor rregulla dhe tabela të shumta.

VRF krijon tabela të ndara routing-u. Kjo mundëson mbivendosje adresash dhe izolim logjik, por kalimi mes VRF-ve kërkon route leaking dhe policy të menduar. Null/discard route hedh trafikun për prefiksin përkatës dhe mund të mbështesë agregimin; një discard tepër specifik mund të krijojë blackhole.

Shembull: 10.0.0.0/8→R1, 10.20.0.0/16→R2 dhe 10.20.30.0/24→R3. Destinacioni 10.20.30.9 del te R3. Përgjigjja kërkon rrugë të vlefshme drejt burimit; suksesi nuk garantohet nga tabela vetëm e njërit skaj.

Laborator: Longest prefix match, RIB/FIB dhe rrugët statike

Koha: 120 minuta. **Mjedisi:** laboratori `lab-netns.sh` i kursit, me a–r–b.

- Nis laboratorin dhe lexo `ip -n cn-r route`. Identifiko rrugët connected dhe krahasoji me default route të hosteve.
- Përdor `ip -n cn-a route get 10.20.20.20` dhe `ip -n cn-r route get 10.20.20.20`. Shpjego dallimin e vendimit në secilën pikë.
- Kryej ping a→b dhe kap një frame në secilën anë të router-it. Shëno TTL dhe adresat L2.
- Defekti: fshi default route vetëm te b me `ip -n cn-b route del default`. Provo përsëri; verifiko se kërkesa mbërrin, por përgjigjja nuk ka rrugën e nevojshme. Riktheje me `ip -n cn-b route add default via 10.20.20.1`.

- Në letër zgjidh gjashtë destinacione kundrejt tabelës me /0, /8, /16 dhe /24. Përfshi një adresë jashtë çdo rrjeti specifik.

Dorëzimi: tabelë vendimesh, prova e vajtjes dhe kthimit dhe korrigjimi. **Pranimi:** longest prefix match zbatohet përpara krahasimit të metrikave për prefikse të ndryshme; defekti riprodhohet dhe rikthehet. **Thellim:** paraqit dy VRF me të njëjtin subnet dhe një kërkesë të kontrolluar route leaking.

11. ICMP, MTU dhe rrugët e padukshme

PMTUD, fragmentimi dhe kufijtë e ping-ut

Teori: PMTUD, fragmentimi dhe kufijtë e ping-ut

Objektivi: të diagnostikosh rastin kur lidhja punon për paketa të vogla, por jo për transferime reale.

ICMP raporton gabime dhe jep mekanizma diagnostikimi. Echo request/reply provon vetëm se një përgjigje e atij tipi u kthye nga pika e synuar. Mungesa e përgjigjes mund të vijë nga filtrimi ose kufizimi i përgjigjeve. Traceroute përdor skadimin e TTL/hop limit; disa variante dërgojnë UDP, ICMP ose TCP. Router-i që nuk përgjigjet në një hop mund të vazhdojë të përcjellë trafikun normalisht.

MTU është kufiri i njësisë së transmetuar në një lidhje të caktuar; Path MTU është minimumi përgjatë rrugës. Me IPv4, një router mund të fragmentojë kur lejohet; DF e pengon dhe kërkon njoftim për MTU të pamjaftueshme. Në IPv6 fragmentimin e bën vetëm burimi. PMTUD klasik mbështetet në njoftime ICMP; PLPMTUD provon madhësi nga shtresa e paketizimit dhe ndihmon kur njoftimet mungojnë.

Një ping IPv4 me payload 1472 byte plus 20 byte IP dhe 8 byte ICMP jep 1500 byte pa opsione. Kjo nuk është formula për IPv6 ose çdo encapsulation. VPN, VXLAN dhe MPLS shtojnë overhead; planifiko underlay MTU ose ul MTU-në e brendshme. MSS clamping mund të ndihmojë TCP, por nuk zgjidh të gjitha protokollet.

Checksum offload dhe segmentation offload mund të tregojnë paketa të mëdha ose checksum të paplotë në kapje te hosti. Verifiko pikën e kapjes para diagnozës. Fragmentimi rrit punën dhe mundësitë e humbjes; fragmentet që humbin ndikojnë të gjithë datagramin.

Shembull: SSH ndërtohet, por kopjimi i skedarëve ngec pas disa byte-ve. Në vend të ndryshimit të DNS-it, krahaso MTU, encapsulation, retransmissions dhe Packet Too Big në të dy drejtimet.

Laborator: PMTUD, fragmentimi dhe kufijtë e ping-ut

Koha: 120 minuta. **Mjedisi:** laboratori Linux a–r–b; `ping` nga iputils.

- Mat ping bazë dhe lexo MTU me `ip -n cn-r link show`. Pastaj ul MTU vetëm të daljes së router-it drejt b në 1400: `ip -n cn-r link set rb mtu 1400`.
- Nga a provo `ip netns exec cn-a ping -c 3 -M do -s 1372 10.20.20.20`, pastaj payload 1472. Kap ICMP në a dhe gjej njoftimin për madhësinë e papërshtatshme.
- Llogarit kufirin për IPv4 pa opsione dhe krahasoje me matjen. Përsërit për IPv6 duke përdorur madhësitë e header-ave përkatës.
- Analizo një traceroute me yje në hop-in 3, por destinacion që përgjigjet. Shpjego pse kjo nuk provon humbje tranziti në hop-in 3.
- Rikthe `rb` në 1500 përpara laboratorit tjetër.

Dorëzimi: tabela madhësi/rezultat, paketa e gabimit dhe llogaritja. **Pranimi:** dallohen payload, IP packet dhe frame; MTU rikthehet; nuk propozohet lejimi verbër i çdo trafiku si zgjidhje. **Thellim:** projekto test për blackhole PMTUD me ICMP të filtruar vetëm në namespace dhe shpjego dallimin nga MSS.

12. TCP, UDP dhe QUIC

Besueshmëria, dritaret dhe kontrolli i congestion-it

Teori: Besueshmëria, dritaret dhe kontrolli i congestion-it

Objektivi: të lexosh sjelljen e një transporti nga sequence, ACK, dritarja dhe koha.

UDP dërgon datagrame me porta dhe checksum sipas rregullave të familjes IP. Nuk ofron vetë renditje, retransmetim ose kontroll congestion-i; aplikacioni mund t'i implementojë. Kjo nuk e bën çdo aplikacion UDP më të shpejtë. TCP ofron rrjedhë byte-sh të renditur; nuk ruan kufijtë e mesazheve të aplikacionit. Tre segmente të aplikacionit nuk garantojnë tri lexime identike në marrës.

Handshake TCP përdor SYN, SYN-ACK dhe ACK. Sequence numbers identifikojnë byte-t; ACK tregon byte-n e ardhshëm të pritur. SACK përshkruan intervale të marra jashtë rendit. Retransmission mund të vijë nga timeout ose mekanizma zbulimi humbjeje; analiza e kapjes duhet të marrë parasysh paketa të humbura nga vetë kapja.

Receive window mbron buffer-in e marrësit; congestion window menaxhon ngarkesën ndaj rrugës. Fluturimi kufizohet nga minimumi i tyre dhe faktorë të tjerë. Zero window tregon presion nga marrësi, jo domosdoshmërisht humbje në rrjet. Slow start, congestion avoidance dhe algoritme si CUBIC/BBR kanë sjellje të ndryshme. ECN sinjalizon congestion pa kërkuar gjithmonë drop.

QUIC ndërtohet mbi UDP, ofron streams të besueshme, siguri me TLS dhe mekanizma të vet transporti. Humbja në një stream nuk krijon të njëjtin bllokim të rendit të byte-ve për të gjithë streams si në një lidhje TCP të vetme, megjithëse congestion-i dhe humbja ende ndikojnë lidhjen. Connection IDs ndihmojnë skenarë migrimi; nuk anashkalojnë policy-n e rrjetit.

Shembull: RTT i lartë dhe receive window i vogël kufizojnë throughput edhe pa humbje. Një reset TCP pas SYN-ACK tregon situatë tjetër nga një SYN që retransmetohet pa përgjigje.

Laborator: Besueshmëria, dritaret dhe kontrolli i congestion-it

Koha: 150 minuta. **Mjedisi:** dy hoste të izoluar, një shërbim HTTP lokal dhe Wireshark/tcpdump.

- Nis serverin lokal sipas udhëzuesit Linux dhe kap trafikun TCP në portën 8080. Kryej një kërkesë me `curl`.
- Identifiko handshake, sequence relative, ACK, FIN ose RST. Shëno se SYN dhe FIN konsumojnë nga një numër sequence.
- Me `ss -tin` në namespace të klientit vëzhgo RTT dhe gjendjen kur lidhja zgjat. Krahaso me BDP të modulit 2.

- Analizo dy regjistra: marrësi reklamon window 0; në tjetrin ka duplicate ACK dhe retransmissions. Jep hipoteza të ndryshme dhe prova që mungojnë.
- Krahaso një kapje UDP me TCP dhe shpjego pse vetëm porta UDP/443 nuk provon që trafiku është QUIC pa interpretimin e protokollit.

Dorëzimi: diagram kohor i një lidhjeje, një tabelë flags dhe analizë e dy defekteve. **Pranimi:** receive window dhe congestion window dallohen; UDP nuk quhet “gjithmonë pa besueshmëri aplikacioni”. **Thellim:** argumentoji efektet e humbjes në HTTP/2 dhe HTTP/3 pa pretenduar eliminim të çdo bllokimi.

13. DNS dhe infrastruktura e emrave

Delegimi, cache, DNSSEC dhe diagnostikimi

Teori: Delegimi, cache, DNSSEC dhe diagnostikimi

Objektivi: të ndjekësh zgjidhjen e një emri dhe të dallosh dështimin DNS nga dështimi i aplikacionit.

DNS organizon emra në hierarki. Resolver-i rekursiv kërkon përgjigjen për klientin dhe ruan cache; serveri autoritativ mban të dhënat e zonës. Root dhe TLD japin delegime, jo domosdoshmërisht adresën përfundimtare. Rekordet A/AAAA japin adresa; CNAME alias; MX postën; NS delegimin; SOA parametrat e zonës; PTR drejtimin e kundërt; TXT të dhëna me përdorime të përcaktuara nga aplikacionet.

TTL kufizon kohën e cache-it sipas rregullave përkatëse. Ulja e TTL-së menjëherë para migrimit nuk fshin kopjet që janë ruajtur me TTL të vjetër. NXDOMAIN tregon se emri nuk ekziston; NODATA mund të tregojë emër ekzistues pa tipin e kërkuar. SERVFAIL tregon se zgjidhja dështoi, për shembull nga delegimi, komunikimi ose validimi. Split DNS jep pamje të ndryshme sipas vendit të klientit dhe kërkon kontroll të konsistencës.

DNS përdor UDP dhe TCP; TCP nuk duhet bllokuar si “i panevojshëm”. EDNS lejon mesazhe më të mëdha dhe zgjerime, por madhësitë e rrugës mbeten të rëndësishme. DoT/DoH kriptojnë transportin drejt resolver-it; DNSSEC verifikon origjinën dhe integritetin e të dhënave të nënshkruara. DNSSEC nuk kripton pyetjen dhe nuk provon se faqja e gjetur është e padëmshme.

Zinxhiri i besimit DNSSEC varet nga delegimi DS, DNSKEY dhe nënshkrimet. Ora e pasaktë mund të prishë validimin. Anycast shpërndan një adresë shërbimi në disa vende përmes routing-ut; nuk garanton afërsi gjeografike absolute.

Shembull: adresa e faqes ndryshon, por vetëm një resolver kthen adresën e vjetër. Kontrollo TTL dhe burimin autoritativ para ndryshimit të routing-ut.

Laborator: Delegimi, cache, DNSSEC dhe diagnostikimi

Koha: 120 minuta. **Mjedisi:** `dig` dhe një zonë laboratorike; përdor emra nën `.test` për shembuj lokalë.

- Krahaso `dig EMRI A`, `dig EMRI AAAA` dhe `dig @RESOLVER EMRI A`, duke zëvendësuar vlerat me zonën e laboratorit. Regjistro status, flags, server dhe TTL.
- Kërko drejtpërdrejt nga autoritativi lokal dhe krahaso me resolver-in. Provo emër që nuk ekziston dhe tip rekordi që mungon për një emër ekzistues.
- Ndrysho një rekord me TTL të planifikuar. Regjistro përgjigjen përpara dhe pas ndryshimit, pa pastruar fillimisht cache-in: mat sjelljen që sheh përdoruesi.
- Defekti analitik: resolver validues jep SERVFAIL, ndërsa pyetja pa validim kthen të dhëna. Kontrollo zinxhirin DNSSEC dhe orën, jo vetëm ping-un.

- Testo aplikacionin edhe me adresë të njohur dhe emrin e duhur TLS, për shembull `curl --resolve EMRI:443:IP https://EMRI/` në laborator.

Dorëzimi: katër përgjigje të interpretuara dhe plan migrimi. **Pranimi:** emër/adresë/TLS ndahen; DNSSEC nuk paraqitet si kriptim; TTL i vjetër merret parasysh. **Thellim:** projekto DNS për dy site me split horizon dhe rikuperim.

14. DHCP, IPAM dhe koha

Shpërndarja e konfigurimit dhe varësitë bazë

Teori: Shpërndarja e konfigurimit dhe varësitë bazë

Objektivi: të projektosh dhënien e adresave dhe të ruash burim të saktë të së vërtetës.

DHCPv4 përdor zakonisht Discover, Offer, Request dhe Acknowledgement për marrëveshjen fillestare. Klienti mund të përdorë rrjedha të tjera kur rinovon ose kujton një lease. Serveri jep adresë, maskë dhe opsione si router-i dhe DNS. Lease ka afat; T1/T2 rregullojnë rinovimin dhe rebinding sipas parametrave. DHCP nuk është thjesht “një server që përgjigjet në broadcast”.

DHCP relay lejon server në subnet tjetër. Informacioni i relay-t i tregon serverit scope-in e duhur; filtrimi dhe routing-u duhet të lejojnë të dy drejtimet. Rezervimi lidh një identitet klienti me adresë, por mënyra e identifikimit mund të përdorë client identifier përveç MAC. Përjashto adresat statike dhe gateway-t nga pool-i për të shmangur konflikte.

DHCP snooping përcakton porta të besuara për përgjigjet dhe mund të ndërtojë bazën e binding-ve. DAI dhe IP source guard shpesh varen nga ajo bazë. Një uplink i klasifikuar gabim mund të ndërpresë klientët pa asnjë problem te serveri. DHCPv6 dhe RA kanë role të ndryshme, siç u trajtua në IPv6.

IPAM regjistron prefikse, VLAN, VRF, lease/reservation dhe pronarë. Inventari dhe DNS duhet të përputhen me konfigurimin real; një spreadsheet i paverifikuar nuk është burim i besueshëm vetëm sepse ekziston. NTP sinkronizon orën për log-e dhe autentikim. Stratum nuk është matje e drejtpërdrejtë e cilësisë; monitoro offset, jitter dhe burimet. PTP përdoret kur kërkohet sinkronizim më i saktë me mbështetje të përshtatshme hardware.

Shembull: klienti merr IP, por DNS i gabuar prish aplikacionet. Prova e suksesit të DHCP duhet të përfshijë opsionet, jo vetëm adresën.

Laborator: Shpërndarja e konfigurimit dhe varësitë bazë

Koha: 120 minuta. **Mjedisi:** klient dhe DHCP server vetëm në rrjetin e brendshëm të një emulatori; mos e lidhe serverin me LAN-in e jashtëm.

- Krijo scope me 50 adresa, interval të përjashtuar për infrastrukturën dhe lease të dokumentuar. Shëno opsionet gateway dhe DNS.
- Kap një cikël marrjeje dhe një rinovim. Lidh transaction ID me klientin dhe shpjego mesazhet që ndryshojnë.
- Nëse ke dy subnet-e, shto relay dhe verifiko se klientët marrin adresa nga scope-i përkatës. Përndryshe bëj analizë të giaddr dhe rrugës së përgjigjes.

- Defekti: scope i mbushur ose relay që tregon subnet të gabuar. Parashiko çfarë shfaq klienti dhe çfarë duhet parë në log-un e serverit.
- Plotëso IPAM për pesë pajisje dhe kontrollo orën e tyre. Në Linux lexo `timedatectl`; kontrollo burimet me mjetin NTP të instaluar, pa supozuar se çdo sistem ka chrony.

Dorëzimi: scope, kapje, IPAM dhe raport kohe. **Pranimi:** nuk ka mbivendosje pool/statike; opsionet verifikohen; relay nuk trajtohet si broadcast i zakonshëm mes router-ave. **Thellim:** planifiko redundancë DHCP dhe rikthim pa dyfishim lease-esh.

15. Aplikacionet, TLS dhe shpërndarja e shërbimeve

HTTP, reverse proxy, CDN dhe load balancing

Teori: HTTP, reverse proxy, CDN dhe load balancing

Objektivi: të ndash problemin e rrjetit nga problemi i sesionit dhe i aplikacionit.

HTTP përcakton kërkesa, përgjigje, metoda dhe status codes. HTTP/1.1 përdor lidhje TCP; HTTP/2 shumëfishon streams brenda TCP; HTTP/3 përdor QUIC. Versioni i transportit nuk e zëvendëson semantikën e aplikacionit. 404 do të thotë se një shërbim HTTP u përgjigj; 502/504 shpesh kërkojnë analizë të proxy-t dhe upstream-it, jo vetëm të klientit.

TLS autentikon skajin sipas certifikatës dhe krijon çelësa për konfidencialitet/integritet. Zinxhiri i certifikatës, emri/SAN, koha dhe trust store duhet të jenë të vlefshme. SNI ndihmon serverin të zgjedhë identitetin; ALPN negocion protokollin e aplikacionit. Certifikata e besuar nuk provon se backend-i është i shëndetshëm. TLS 1.3 ndryshon handshake dhe heq mekanizma të vjetër; 0-RTT kërkon analizë të replay-it sipas aplikacionit.

Load balancer L4 shpërndan lidhje sipas adresave/portave; L7 interpreton aplikacionin dhe mund të përfundojë TLS. Health check duhet të provojë varësitë që kanë rëndësi, pa mbingarkuar shërbimin. Session persistence mund të jetë e nevojshme, por fsheh çekuilibra. Source NAT dhe ruajtja e IP-së së klientit ndryshojnë log-et dhe policy-n.

Reverse proxy ndërmjetëson kërkesat e serverit; CDN afron përmbajtjen dhe mban cache. Cache key, headers, invalidimi dhe TTL janë pjesë e korrektësisë, jo vetëm performancë. SMTP, IMAP, SSH, SMB, NFS dhe protokolle të tjera kanë negociata dhe varësi të ndryshme; porta e hapur nuk provon funksionimin e plotë.

Shembull: `curl` lidhet me IP-në, por TLS dështon me emrin. Heto SAN, SNI dhe zinxhirin; mos fik verifikimin si zgjidhje.

Laborator: HTTP, reverse proxy, CDN dhe load balancing

Koha: 150 minuta. **Mjedisi:** shërbim HTTP lokal dhe, për pjesën TLS, server laboratorik me certifikatë të kontrolluar.

- Përdor `curl -v http://10.20.20.20:8080/` në laborator dhe identifiko lidhjen, kërkesën dhe statusin.
- Në shërbimin TLS provo `openssl s_client -connect ADRESA:443 -servername EMRI -verify_return_error`. Zëvendëso vlerat; lexo zinxhirin dhe rezultatin e verifikimit. Përdor CA laboratorike të instaluar me qëllim për certifikatat lokale.
- Ndërto matricë: DNS i gabuar, portë e mbyllur, certifikatë e skaduar, backend i ndalur dhe përmbajtje e vjetër në cache. Për secilin cakto provën dalluese.

- Nëse ke reverse proxy, ndalo vetëm backend-in dhe krahaso health check me përgjigjen reale. Regjistro kodin e statusit dhe kohën.
- Përcakto headers që ruajnë IP-në e klientit dhe kufijtë e besimit; një header i dërguar nga klienti nuk është vetë provë identiteti.

Dorëzimi: transkript i shkurtër, matricë defektesh dhe konfigurim i shërbimit. **Pranimi:** transporti, TLS dhe HTTP analizohen veçmas; verifikimi i certifikatës ruhet. **Thellim:** argumento HTTP/2 kundrejt HTTP/3 për rrugë me humbje dhe firewall që kufizon UDP.

16. Analiza e paketave

Wireshark, tcpdump dhe prova e riprodhueshme

Teori: Wireshark, tcpdump dhe prova e riprodhueshme

Objektivi: të ndërtosh diagnozë që mbështetet në paketat dhe pikën e kapjes.

Një kapje është pamje e një pjese të rrjetit për një interval kohe. Në një switch, hosti zakonisht sheh trafikun e vet, broadcast dhe multicast të caktuar. Për trafik tjetër përdoren SPAN/mirror ose TAP me kufizime të njohura. Një port mirror mund të humbasë paketa kur trafiku i burimit tejkalon portën e monitorimit. Kapja nga të dy skajet dhe ora e sinkronizuar ndihmojnë të dallohet humbja reale nga mungesa në instrument.

Capture filter zbatohet gjatë marrjes dhe përdor sintaksë BPF, për shembull `tcp port 443`. Display filter zbatohet pas kapjes në Wireshark, për shembull `tcp.port == 443`. Ato nuk janë sintaksë e këmbyeshme. Snap length kufizon byte-t e ruajtura; ring buffer kufizon diskun; drop counters tregojnë kufizime të kapjes. Përdor interval të kufizuar dhe të dhëna testimi.

Ndiq një flow me adresat, portat dhe protokollin. Për TCP analizo handshake, RTT, retransmissions, out-of-order, window dhe mbylljen. Për DNS ndiq ID, emrin dhe përgjigjen; për ICMP shiko edhe header-in e paketës origjinale të cituar. Enkriptimi fsheh payload-in, por koha, madhësitë dhe metadata ende japin prova. Mos nxirr përfundime për përmbajtjen e kriptuar vetëm nga porta.

Offload në host mund të japë checksum “të gabuar” para përfundimit në hardware ose paketa më të mëdha se frame-et në tel. PCAP nuk provon vetë që pajisja e largët e mori paketën; prova e ACK ose kapja e largët ndihmon. Redakto ose anonimizoi të dhënat para ndarjes.

Shembull: tre SYN pa SYN-ACK kërkojnë krahasim me kapjen e serverit dhe firewall counters; nuk identifikojnë automatikisht fajtorin.

Laborator: Wireshark, tcpdump dhe prova e riprodhueshme

Koha: 150 minuta. **Mjedisi:** laboratori Linux; `tcpdump`, Wireshark dhe kërkesa testimi.

- Kap maksimumi 200 paketa te dalja e router-it me `ip netns exec cn-r tcpdump -ni rb -c 200 -w /tmp/cn-lab.pcap`. Ndalo manualisht nëse testi mbaron më herët.
- Gjenero ping dhe HTTP. Hape skedarin në Wireshark; përdor `icmp`, `tcp.port == 8080` dhe filtrin për një IP të vetme.
- Krijo tabelë kohore për një kërkesë: nisja e lidhjes, përgjigjja e parë, madhësia, përfundimi. Shëno zonën kohore dhe pikën e kapjes.
- Krahasoni BPF `host 10.20.20.20 and tcp port 8080` me display filter përkatës. Shpjego çfarë humbet nëse capture filter është tepër i ngushtë.

- Defekti: kapja e klientit ka retransmission, kapja e serverit jo. Formulo dy shpjegime dhe çfarë prove shtesë kërkohet.

Dorëzimi: PCAP laboratorik pa kredenciale reale dhe raport me pesë numra paketash. **Pranimi:** çdo pretendim lidhet me paketë ose counter; kufizimet e kapjes deklarohen. **Thellim:** harto plan kapjeje për trafik asimetrik dhe pajisje me hardware offload.

17. OSPF i avancuar

Fqinjësitë, LSDB, zonat dhe redistribuimi

Teori: Fqinjësitë, LSDB, zonat dhe redistribuimi

Objektivi: të dallosh dështimin e fqinjësisë, të shkëmbimit të databazës dhe të instalimit të rrugëve.

OSPF është protokoll link-state brenda një domeni administrativ. Router-at shkëmbejnë informacion LSA dhe ndërtojnë LSDB; SPF llogarit rrugët sipas kostos. Kostoja e bazuar në bandwidth referencë kërkon përputhje të projektimit; default-et mund të mos dallojnë lidhjet moderne të shpejta. Router ID duhet të jetë unik dhe i qëndrueshëm.

Fqinjësia varet nga area, timers, parametrat e autentikimit dhe lloji i rrjetit. Gjendjet përfshijnë Down, Init, 2-Way, ExStart, Exchange, Loading dhe Full. Në rrjet broadcast, dy DROther mund të mbeten normalisht 2-Way; jo çdo fqinj duhet të jetë Full me çdo tjetër. DR/BDR zvogëlon numrin e adjacencies. Mospërputhja MTU shpesh shfaqet gjatë shkëmbimit të databazës.

Area 0 është backbone i topologjisë OSPF me shumë zona; ABR lidh zonat dhe ASBR sjell rrugë të jashtme. LSA 1/2 përshkruajnë topologjinë brenda zonës; 3/4 shërbejnë për informacion ndërmjet zonave; 5 për rrugë të jashtme; NSSA përdor 7 që mund të përkthehet në 5 në kufi. Stub, totally stubby dhe NSSA kanë dallime standardi dhe implementimi që kontrollohen te platforma.

Agregimi bëhet në kufij të përshtatshëm, jo kudo sipas dëshirës. Redistribuimi mes protokolleve kërkon filtra dhe tags për të shmangur feedback. E1 përfshin edhe koston e brendshme drejt ASBR, ndërsa E2 e trajton ndryshe komponentin e jashtëm. OSPFv3 lidhet me IPv6 dhe mund të mbështesë address families sipas zgjerimeve/implementimit.

Shembull: fqinjësia Full nuk garanton rrugën e dëshiruar në FIB. Ndiq reklamimin në LSA, përzgjedhjen në RIB dhe instalimin në FIB veçmas.

Laborator: Fqinjësitë, LSDB, zonat dhe redistribuimi

Koha: 180 minuta. **Mjedisi:** tre router-a FRRouting të lidhur sipas `frr/README.sq.md`; përdor konfigurimet e kursit.

- Aktivizo zebra dhe ospfd në secilin router të laboratorit. Apliko konfigurimin me ndërfaqet e përshtatura; mos e kopjo në hostin e punës.
- Lexo `show ip ospf neighbor`, `show ip ospf database` dhe `show ip route ospf`. Gjej loopback-et e tri pajisjeve dhe provo komunikimin.
- Ndrysho koston e një lidhjeje dhe parashiko rrugën para testit. Regjistro SPF/rrugën para dhe pas ndryshimit.

- Defekti: vendos area të ndryshme në një lidhje dhe provo cilat fqinjësi mungojnë. Rikthe parametrin. Analizo veçmas rastin me MTU të ndryshme dhe gjendje ExStart.
- Në fazën e dytë bëj R3 ABR me një subnet në area 10. Shëno çfarë ndryshon në LSDB të R1.

Dorëzimi: konfigurimet, tre komanda verifikimi dhe raporti i dështimit. **Pranimi:** loopback-et arrihen; area dhe network type shpjegohen; 2-Way normal nuk trajtohet gabim si incident. **Thellim:** projekto redistribuim me një prefix-list dhe tag kundër feedback, duke justifikuar çdo prefiks.

18. IS-IS dhe protokollet e tjera IGP

Level-et, metrikat dhe migrimi i routing-ut

Teori: Level-et, metrikat dhe migrimi i routing-ut

Objektivi: të krahasosh mekanizmat IGP dhe të zgjedhësh protokollin sipas kërkesës.

IS-IS është link-state dhe formon adjacencies drejtpërdrejt mbi lidhjen, jo mbi TCP/IP. NET përmban area address, system ID dhe selector; system ID duhet unik. Level 1 shërben routing brenda zonës dhe Level 2 lidh zonat sipas arkitekturës së IS-IS. Router-at L1/L2 marrin pjesë në të dy nivelet. Një domen i thjeshtë operatori mund të përdorë L2-only me projektim të dokumentuar.

LSP shpërndan topologjinë; TLV-të mundësojnë zgjerime për IPv4, IPv6 dhe funksione të tjera. Wide metrics japin hapësirë më të përshtatshme se metrikat e vjetra. Në media broadcast zgjidhet DIS me sjellje që nuk duhet barazuar mekanikisht me DR/BDR të OSPF. MTU dhe kapaciteti për LSP/PDU mbeten të rëndësishëm edhe kur IP-ja e ndërfaqes duket e saktë.

RIP është distance-vector me hop count dhe kufi të vogël praktik; përdoret për mësim dhe sisteme të caktuara të trashëguara. Split horizon, route poisoning dhe timers synojnë të kontrollojnë loop-et dhe konvergjencën, por nuk e bëjnë të barabartë me IGP modern për shkallë të madhe. EIGRP përdor DUAL dhe koncepte successor/feasible successor; mbështetja ndryshon sipas prodhuesit dhe licencës.

Zgjedhja mes OSPF dhe IS-IS përfshin përvojën e ekipit, ekosistemin, telemetrinë, shkallën dhe planin e migrimit. Nuk ka protokoll “më të mirë” për çdo situatë. Redistribuimi dypalësh i pakontrolluar krijon rrugë të ricikluara; filtrat, tags dhe pika të kufizuara shkëmbimi janë pjesë e projektimit.

Shembull: gjatë migrimit OSPF→IS-IS mos aktivizo redistribuim të plotë në çdo router. Zgjidh kufij, cakto prefikset e lejuara dhe monitoro RIB/FIB për rrugët e ricikluara.

Laborator: Level-et, metrikat dhe migrimi i routing-ut

Koha: 150 minuta. **Mjedisi:** tre instanca FRRouting me isisd; në mungesë të imazhit bëj analizë të tabelave.

- Cakto tri NET me system ID unike dhe një domen L2-only. Aktivizo IS-IS për IPv4/IPv6 në lidhjet përkatëse sipas dokumentacionit të versionit.
- Lexo fqinjësitë, databazën dhe rrugët me komandat `show isis neighbor`, `show isis database` dhe tabelat IP.
- Defekti: ndrysho level-in e lejuar në një skaj ose përsërit system ID në konfigurimin analitik. Përshkruaj pse IP ping në lidhje nuk është provë që protokolli punon.
- Ndërto matricë OSPF, IS-IS, RIP, EIGRP: gjendja e shkëmbyer, metrika, shkalla, kufizimet e ekosistemit dhe diagnostikimi.

- Projekto migrim me një pikë redistribuimi, filtrim të tre prefikseve dhe plan rikthimi. Shëno kriteret për kalimin final.

Dorëzimi: NET-të, tabela e krahasimit dhe plani i migrimit. **Pranimi:** L1/L2 nuk ngatërrohen me shtresat OSI; system ID është unik; redistribuimi ka kontroll të drejtimit. **Thellim:** analizo përfitimet dhe kostot e një IGP të vetëm IPv4/IPv6 kundrejt instancave të ndara.

19. BGP dhe routing ndërmjet domeneve

eBGP, iBGP, next hop dhe route reflectors

Teori: eBGP, iBGP, next hop dhe route reflectors

Objektivi: të ndërtohet sesion BGP dhe të ndiqet prefiksi nga marrja te reklamimi dhe instalimi.

BGP shkëmben arritshmëri mes sistemeve autonome dhe mbështet policy. Sesioni përdor TCP 179; gjendja Established tregon që sesioni u ngrit, jo që prefikset e duhura pranohen. OPEN, KEEPALIVE, UPDATE dhe NOTIFICATION kanë role të ndryshme. AS_PATH ndihmon zbulimin e loop-eve dhe zbatimin e politikës; BGP nuk zgjedh thjesht rrugën fizikisht më të shkurtër.

eBGP lidh zakonisht AS të ndryshme; iBGP shpërndan informacion brenda AS. Rrugët e mësuara nga iBGP nuk reklamohen te një tjetër fqinj iBGP në modelin bazë, ndaj përdoret full mesh ose route reflection/confederation. Route reflector ul numrin e sesioneve, por kërkon analizë të redundancës, cluster ID dhe path visibility.

NEXT_HOP duhet të jetë i arritshëm për rrugën që të përdoret. `next-hop-self` në kufirin e përshtatshëm është praktikë e zakonshme brenda një topologjie të projektuar, jo ilaç universal. Reklamimi me `network` në FRRouting kërkon rrugën përkatëse në RIB sipas sjelljes së konfigurimit. Address families ndajnë IPv4 unicast, IPv6 unicast, VPN dhe EVPN; sesioni bazë mund të jetë lart ndërsa një familje nuk shkëmben rrugë.

Përzgjedhja merr parasysh atribute dhe rregulla që ndryshojnë sipas implementimit: politika lokale, LOCAL_PREF, AS_PATH, ORIGIN, MED dhe faktorë të tjerë. Mos përdor një rend universal pa dokumentuar platformën. Adj-RIB-In, Loc-RIB dhe Adj-RIB-Out janë pika konceptuale që ndihmojnë ndarjen e marrjes, zgjedhjes dhe reklamimit.

Shembull: dy fqinjë Established, por zero rrugë. Kontrollo address family, prefix-list, policy eBGP dhe origjinimin; mos ndrysho transportin që tashmë punon.

Laborator: eBGP, iBGP, next hop dhe route reflectors

Koha: 180 minuta. **Mjedisi:** R1 dhe R2 FRRouting, AS privatë 65001/65002, sipas burimeve `frr/`.

- Apliko shembullin eBGP me prefix-list hyrëse/dalëse dhe vetëm loopback-et e përcaktuara. Kontrollo lidhjen IP para BGP.
- Lexo `show bgp ipv4 unicast summary`, rrugën për prefiksin dhe tabelën e routing-ut. Verifiko origjinimin dhe next hop.
- Defekti: hiq rrugën që mbështet një `network` ose ndalo prefiksin me filtër. Regjistro sesionin Established me prefiks të munguar dhe gjej saktësisht fazën ku humbet.
- Shto një fqinj iBGP në topologjinë e zgjeruar. Shpjego pse kërkohet arritshmëri loopback dhe si përdoret next-hop-self.

- Llogarit numrin e sesioneve full mesh për 8 router-a dhe projekto dy route reflectors me klientë.

Dorëzimi: konfigurime, rrugë e marrë/zgjedhur/reklamuar dhe raport i defektit. **Pranimi:** filtrat janë të kufizuar; 8 router-a full mesh kërkojnë 28 sesione; Established nuk përdoret si provë e shërbimit. **Thellim:** analizo çfarë humbet nga path visibility kur route reflector shpërndan vetëm një rrugë më të mirë.

20. Politikat BGP dhe siguria e routing-ut

LOCAL_PREF, communities, RPKI dhe mbrojtja e prefikseve

Teori: LOCAL_PREF, communities, RPKI dhe mbrojtja e prefikseve

Objektivi: të kontrollosh hyrjen/daljen e trafikut dhe të reduktosh route leaks dhe hijacks.

Politika e importit cakton çfarë pranon dhe si e vlerëson; politika e eksportit cakton çfarë i tregon fqinjit. LOCAL_PREF zakonisht përdoret brenda AS për preferencën e daljes. AS_PATH prepending dhe communities të ofruesit mund të ndikojnë hyrjen nga jashtë, por vendimi përfundimtar i takon rrjetit të largët. MED ka kontekst krahasimi dhe nuk është metrikë globale ndërmjet çdo rruge.

Prefix-list filtron prefikse dhe gjatësi; route-map mund të kombinojë përputhje dhe ndryshime atributesh. Kupto implicit deny dhe rendin e rregullave. Një filtër që lejon 10.0.0.0/8 me çdo gjatësi deri /32 lejon shumë më tepër se vetëm agregatin /8. Communities standarde dhe large communities kodojnë sinjale të politikës; marrëveshja e kuptimit duhet të dokumentohet.

RPKI Route Origin Validation krahason prefiksin, origin AS dhe maxLength me ROA-të. Rezultati mund të jetë Valid, Invalid ose NotFound. NotFound nuk do të thotë Invalid. ROV nuk vërteton të gjithë AS_PATH dhe nuk eliminon çdo route leak. IRR filtering, max-prefix, kontrolli i bogon-eve, politika e eksportit dhe marrëveshjet me partnerët plotësojnë mbrojtjen.

Rrjedhjet ndodhin kur një klient/peer e reklamon rrugën në marrëdhënie ku nuk duhet. BGP Roles/OTC sipas mbështetjes së implementimit mund të ndihmojnë; projekti ende ka nevojë për filtra. Graceful shutdown dhe maintenance communities lehtësojnë mirëmbajtjen, por duhen testuar. Monitoro ndryshimet e origin-it dhe prefikset më specifike.

Shembull: ROA për 203.0.113.0/24, AS65001, maxLength /24 nuk autorizon një /25 edhe nëse ka të njëjtin origin. Shembulli përdor adresë dokumentimi, jo prefiks për reklamim publik.

Laborator: LOCAL_PREF, communities, RPKI dhe mbrojtja e prefikseve

Koha: 180 minuta. **Mjedisi:** topologji BGP e izoluar dhe analizë ROA; nuk reklamohet asgjë në Internet.

- Krijo dy dalje dhe cakto LOCAL_PREF 200 në të preferuarën, 100 në rezervë. Vërteto zgjedhjen në router-at e AS dhe jo vetëm te fqinjët kufitarë.
- Për eksport lejo vetëm prefikset e zotëruara të laboratorit. Provo një prefiks të marrë nga peer-i dhe vërteto që nuk i del një peer-i tjetër.
- Defekti: një rregull prefix-list lejon gabimisht më shumë prefikse përmes `le`. Shkruaj tri adresa që demonstrojnë dallimin para/pas korrigjimit.
- Klasifiko katër raste RPKI duke ndryshuar origin dhe maxLength. Përfshi një prefiks pa ROA.

- Planifiko dështimin e cache-it RPKI: politika ndaj gjendjes së vjetruar duhet të dokumentohet, të monitorohet dhe të mos ngatërrohet me origjinë realisht Invalid.

Dorëzimi: tabelë import/eksport, prova të filtrave dhe klasifikim ROV. **Pranimi:** prefikset tranzit nuk rrjedhin; NotFound trajtohet saktë; politika e jashtme nuk pretendohet plotësisht e kontrollueshme. **Thellim:** projekto communities për tre nivele preferencash dhe mirëmbajtje pa ndryshuar manualisht çdo peer.

21. Redundanca dhe konvergjenca

VRRP, BFD, ECMP dhe domenet e dështimit

Teori: VRRP, BFD, ECMP dhe domenet e dështimit

Objektivi: të matësh rikuperimin dhe të dallosh redundancën logjike nga pavarësia fizike.

Redundanca kërkon që funksioni të mbijetojë pas dështimit të një komponenti të caktuar. Dy lidhje në të njëjtin kanal fizik ose te e njëjta kartë nuk japin të njëjtën pavarësi si dy rrugë të ndara. Një diagram duhet të tregojë furnizimin, rack-un, operatorin, fiber path dhe kontrollin, jo vetëm dy vija.

VRRP paraqet një gateway virtual për hostet me router kryesor dhe rezervë sipas zgjedhjes së protokollit. Prioriteti, preemption dhe tracking i uplink-ut ndikojnë sjelljen. Nëse ndërfaqja LAN mbetet lart por dalja dështon, vetëm gjendja e LAN-it nuk mjafton për të zgjedhur gateway-n e shëndetshëm. HSRP dhe mekanizma të tjerë kanë qëllim të ngjashëm me dallime implementimi.

BFD zbulon mungesën e komunikimit më shpejt se timers të disa protokolleve të routing-ut. Koha e zbulimit lidhet me intervalet e negociuara dhe multiplier, jo vetëm me një vlerë të shkruar. Timers tepër agresivë mund të shkaktojnë flaps nga ngarkesa e CPU-së. Graceful restart ruan përkohësisht gjendje gjatë rifillimit të kontrollit; mund të zgjasë blackhole nëse plani i të dhënave nuk vazhdon realisht.

Konvergjenca përfshin zbulimin, përhapjen e informacionit, llogaritjen dhe programimin e FIB. Microloops mund të ndodhin gjatë ndryshimeve asinkrone. ECMP dhe fast reroute ndihmojnë në disa skenarë, por kërkojnë topologji dhe kapacitet rezervë. Rrjedhat stateful mund të humbin edhe kur IP-ja gjen rrugë alternative, nëse firewall/VPN nuk ndan gjendjen.

Shembull: 1 s zbulim + 0.3 s llogaritje/programim mund të japë më shumë se 1.3 s ndërprerje në aplikacion për shkak të retransmission timers dhe gjendjes së sesionit.

Laborator: VRRP, BFD, ECMP dhe domenet e dështimit

Koha: 150 minuta. **Mjedisi:** dy gateway virtuale, një host dhe dy dalje; mund të bëhet analizë kohore në mungesë VRRP.

- Cakto gateway virtual dhe IP reale të dy router-ave. Dokumento prioritetin, tracking dhe sjelljen pas rikthimit të pajisjes kryesore.
- Nis matje ping dhe një sesion aplikacioni që zgjat. Dështo LAN-in, pastaj në test të veçantë vetëm uplink-un. Mos i ngatërro dy skenarët.
- Regjistro momentin e defektit, zbulimit, ndryshimit të gateway-t dhe përgjigjes së parë të rikthyer. Shëno saktësinë e orëve.

- Në topologjinë FRRouting vlerëso BFD për lidhjet e nevojshme; krahaso efektin në konvergjencë me ngarkesën dhe false positives.
- Defekti analitik: dy operatorë përdorin të njëjtën fibër hyrëse. Rishiko diagramin sipas failure domain dhe jo sipas numrit të kontratave.

Dorëzimi: katër skenarë dështimi, timeline dhe plan kapaciteti pas humbjes së një lidhjeje. **Pranimi:** testohet edhe aplikacioni; kthimi në gjendjen normale është i kontrolluar; nuk deklarohet zero downtime vetëm nga VRRP. **Thellim:** analizo një sesion TCP pas ndryshimit të daljes me NAT dhe një firewall stateful.

22. Multicast dhe shpërndarja një-me-shumë

IGMP, MLD, PIM dhe RPF

Teori: IGMP, MLD, PIM dhe RPF

Objektivi: të gjurmosh anëtarësinë dhe pemën multicast pa e trajtuar si broadcast.

Unicast lidh një burim me një destinacion; multicast dërgon drejt një grupi me marrës të interesuar. IPv4 përdor hapësirën multicast 224.0.0.0/4 me nënintervale dhe kufizime; IPv6 përdor ff00::/8 me scope të koduar. Jo çdo grup duhet të routohet mes site-ve. Anycast është model tjetër: e njëjta adresë për disa instanca, me zgjedhje përmes routing-ut.

IGMP për IPv4 dhe MLD për IPv6 sinjalizojnë anëtarësinë nga hostet. Snooping në switch përdor këtë informacion për të kufizuar trafikun në portat me marrës; querier ruan rifreskimin e gjendjes. Nëse mungon querier ose timers nuk përputhen, sjellja mund të ndryshojë pas disa minutash edhe kur testi fillestar punon.

PIM ndërton pemët ndërmjet router-ave duke u mbështetur në informacionin unicast për kontrollin RPF. Reverse Path Forwarding verifikon nëse paketa vjen nga ndërfaqja e pritshme drejt burimit. ASM mund të përdorë RP dhe pemë të përbashkët; SSM identifikon burimin dhe grupin, (S,G), dhe shmang nevojën e RP për atë model. IGMPv3/MLDv2 ofrojnë mekanizma të lidhur me filtrimin e burimit.

Tabela multicast dhe tabela unicast kanë role të ndryshme. OIL tregon daljet e pemës. TTL/hop limit, ACL, anëtarësia, RPF dhe MTU mund të pengojnë trafikun në pika të ndryshme. Multicast UDP nuk jep vetë retransmetim; aplikacionet e videos ose financave kërkojnë mekanizma të tjerë nëse kërkohet rikuperim.

Shembull: burimi dëgjohet në VLAN lokal, por jo në site tjetër. Kontrollo routing multicast dhe RPF; ping drejt adresës unicast të marrësit nuk e provon pemën multicast.

Laborator: IGMP, MLD, PIM dhe RPF

Koha: 150 minuta. **Mjedisi:** dy router-a me multicast routing dhe tri hoste laboratorike; alternativë analizë (S,G).

- Cakto burim S dhe grup lokal të përshtatshëm për laborator. Dokumento nëse përdoret ASM apo SSM dhe ku është RP nëse nevojitet.
- Bashko dy marrës dhe lër të tretin jashtë grupit. Regjistro anëtarësinë IGMP/MLD dhe portat e snooping.
- Verifiko incoming interface, OIL dhe rrugën unicast drejt S. Pastaj krahaso me kapjen reale në lidhjen hyrëse.
- Defekti: ndrysho rrugën unicast drejt burimit pa ndryshuar rrugën e paketave të ardhura. Shpjego një dështim RPF dhe korrigjimin e projektimit.

- Testo largimin e një marrësi dhe ruajtjen e trafikut për marrësin tjetër. Shëno timers dhe vonesën e largimit.

Dorëzimi: pema, gjendja (S,G) dhe prova për anëtarësinë. **Pranimi:** multicast nuk përhapet pa kontroll në çdo portë; RPF lidhet me burimin; querier dhe RP dallohen. **Thellim:** projekto shpërndarje video në dy site me redundancë RP ose SSM, duke justifikuar zgjedhjen dhe kufijtë e dështimit.

23. QoS dhe menaxhimi i radhëve

DSCP, shaping, policing dhe congestion

Teori: DSCP, shaping, policing dhe congestion

Objektivi: të ndash trafikun sipas kërkesës dhe të provosh sjelljen kur lidhja mbushet.

QoS menaxhon konkurrimin për burime; nuk krijon bandwidth. Klasifikimi identifikon trafikun, marking vendos sinjalin si DSCP në IP ose PCP në Ethernet, dhe queueing përcakton sjelljen kur paketat presin. Trust boundary cakton ku besohen shënimet. Trafiku i përdoruesit nuk duhet të fitojë prioritet kritik vetëm sepse ka vendosur DSCP vetë.

Policer mat normën dhe zakonisht hedh ose rishënon trafikun jashtë profilit. Shaper vonon daljen me buffer për të përshtatur normën; kjo mund të shtojë latency. Token bucket përdor normë dhe burst; njësitë bit/byte duhet të kontrollohen te platforma. Një policer shumë i ngushtë shkakton humbje edhe në trafik me mesatare nën kapacitet nëse burst-et tejkalojnë profilin.

Strict priority i shërben klasës prioritare shpejt, por pa kufij mund të lërë klasa të tjera pa shërbim. Weighted scheduling ndan kapacitetin sipas politikës. AQM si RED ose fq_codel/CAKE në mjedise të përshtatshme synon menaxhimin e radhëve dhe vonesës; algoritmet nuk janë sinonime dhe varen nga vendi i bottleneck-ut. ECN mund të sinjalizojë congestion pa drop për flukse që e mbështesin.

Projektimi për zë/video kërkon latency, jitter dhe humbje të kontrolluar. Shëno drejtimin: QoS në dalje të një lidhjeje nuk kontrollon automatikisht radhën e operatorit para se trafiku të mbërrijë. Tunneling mund të kopjojë ose ndryshojë DSCP mes header-it të brendshëm dhe të jashtëm; verifiko sjelljen.

Shembull: shaping në 95 Mbit/s para një shërbimi 100 Mbit/s mund ta sjellë bottleneck-un në pajisjen që kontrollon, por vlera duhet përshtatur me overhead-in dhe mënyrën e faturimit/matjes.

Laborator: DSCP, shaping, policing dhe congestion

Koha: 150 minuta. **Mjedisi:** dy burime trafiku dhe një router laboratorik; opsional `tc` në namespace.

- Ndërto tri klasa: zë i simuluar, aplikacion biznesi dhe transferim i madh. Cakto objektiva dhe kufij në vend të një liste vetëm me DSCP.
- Mato latency në qetësi dhe gjatë transferimit që mbush lidhjen. Përdor matje të njëjta dhe regjistro p95, humbje dhe throughput.
- Apliko shaping/queueing vetëm te ndërfaqja laboratorike. Nëse përdor `tc`, ruaj komandat dhe gjendjen `tc -s qdisc show` për rikthim.
- Krahaso policer me shaper për të njëjtën normë; analizo drop dhe vonesën, jo vetëm shpejtësinë mesatare.

- Defekti analitik: klienti shënon çdo paketë EF. Vendos trust boundary dhe riklasifiko trafikun pa hequr prioritetin nga zëri real.

Dorëzimi: policy, matje para/pas dhe counters për klasë. **Pranimi:** përfitimi verifikohet në congestion; trafiku tjetër nuk vuan starvation; të gjitha ndryshimet laboratorike rikthehen. **Thellim:** llogarit overhead-in e një stream-i zëri me packetization 20 ms dhe shpjego ndikimin e shumë rrjedhave të vogla.

24. Wireless dhe fizika e radios

Spektri, airtime, kanalet dhe projektimi RF

Teori: Spektri, airtime, kanalet dhe projektimi RF

Objektivi: të projektosh kapacitet wireless me matje RF dhe kërkesa klientësh.

Wi-Fi përdor medium të përbashkët radio me konkurrim për airtime. Shpejtësia PHY nuk është throughput i aplikacionit. Menaxhimi, pritja, acknowledgements, retries dhe klientët me shpejtësi të ulët konsumojnë kohë. CSMA/CA nuk është i njëjti mekanizëm si CSMA/CD i Ethernet-it të vjetër. Hidden node dhe interferenca mund të ekzistojnë edhe kur niveli i sinjalit duket i mirë.

RSSI jep një vlerësim të fuqisë së marrë; SNR krahason sinjalin me zhurmën. Antenat, muret, orientimi dhe njerëzit ndryshojnë mbulimin. dBm është fuqi absolute; dB diferencë. Një rritje 3 dB afërsisht dyfishon fuqinë, jo automatikisht distancën. Fuqia e lartë e AP-së nuk korrigjon klientin që nuk mund të transmetojë në kthim.

Gjerësia e kanalit rrit kapacitetin potencial, por konsumon spektër dhe mund të ulë mundësitë e ripërdorimit. Planet 2.4/5/6 GHz varen nga rajoni, rregullat, DFS dhe pajisjet. Mos zbato një listë kanalesh të një vendi në një tjetër. OFDM/OFDMA, MIMO, beamforming dhe mekanizma nga 802.11n/ac/ax/be përmirësojnë efikasitetin në kushte të caktuara; mbështetja e klientit është vendimtare.

Site survey përfshin parashikim, matje në terren dhe validim pas instalimit. Dendësia dhe aplikacioni ndikojnë më shumë se numri i metrave katrorë. Roaming është vendim me pjesëmarrje të klientit; një AP i shtuar pa projektim mund të rrisë ndërhyrjen co-channel.

Shembull: një sallë me 100 klientë kërkon analizë airtime dhe njëkohshmërie. Katër AP në të njëjtin kanal nuk japin automatikisht katërfish bandwidth-in.

Laborator: Spektri, airtime, kanalet dhe projektimi RF

Koha: 180 minuta. **Mjedisi:** një ose më shumë AP të autorizuar dhe dy klientë; pa radio bëhet projektim analitik.

- Vizato një kat me pengesa, klientë dhe kërkesa aplikacionesh. Shëno vendet ku duhen matje, jo vetëm qendra gjeometrike.
- Regjistro RSSI/SNR kur mjeti i jep, kanal, gjerësi, bandë dhe PHY rate në pesë pika. Testo throughput ndaj serverit lokal me kabllo për të mos matur edhe Internetin.
- Krahaso një klient afër dhe një larg me trafik njëkohësisht. Regjistro retries dhe airtime nëse AP i ekspozon.
- Ndrysho vetëm një parametër laboratorik, si gjerësia e kanalit; përsërit matjen dhe ruaj profilin fillestar.

- Defekti: sinjal i fortë, throughput i dobët dhe retries të larta. Dallo interferencën, congestion-in dhe kufirin e uplink-ut.

Dorëzimi: hartë matjesh, plan kanalesh sipas vendit të instalimit dhe përfundim i mbështetur në të dhëna. **Pranimi:** PHY nuk quhet goodput; fuqia e klientit merret parasysh; kanalet verifikohen me rregullat lokale aktuale. **Thellim:** projekto kapacitet për zë me klientë në roaming dhe ndarje bandash.

25. Siguria wireless dhe mobiliteti

WPA, 802.1X, roaming dhe rrjetet e mysafirëve

Teori: WPA, 802.1X, roaming dhe rrjetet e mysafirëve

Objektivi: të ndërtosh akses wireless me identitet, segmentim dhe rikthim të kontrolluar.

WPA2/WPA3 përfshijnë mekanizma autentikimi dhe mbrojtjeje të lidhjes. Personal përdor model të ndryshëm nga Enterprise me 802.1X/EAP dhe server AAA. SAE në WPA3-Personal ndryshon marrëveshjen nga PSK klasik; modalitetet transition ruajnë përputhshmëri por duhet të shqyrtohen sipas pajisjeve dhe politikës. WEP dhe mekanizmat e vjetër nuk janë bazë për projekt të ri.

Në Enterprise klienti/supplicant, AP/authenticator dhe serveri i autentikimit kanë role të dallueshme. EAP-TLS përdor certifikata dhe kërkon PKI, shpërndarje identitetesh, verifikim të serverit dhe proces revokimi/rinovimi. Lejimi i klientit të besojë çdo server certifikate mund të ekspozojë identitetin. Protected Management Frames mbrojnë kategori të caktuara frame-esh menaxhimi, jo çdo lloj sulmi radio.

SSID nuk është vetë VLAN ose kufi sigurie. AP/controller mund të map-ojë role dhe VLAN dinamike nga AAA. Rrjeti i mysafirëve kërkon izolim klientësh, policy ndaj LAN-it dhe dalje të kontrolluar. Captive portal kontrollon një rrjedhë hyrjeje; nuk zëvendëson kriptimin ose identitetin e pajisjes. Numri i madh i SSID-ve shton overhead menaxhimi.

802.11k ndihmon me informacion fqinjësh, 802.11v me menaxhim tranzicioni dhe 802.11r me fast transition sipas mbështetjes. Roaming-u duhet provuar me klientët realë, VLAN/subnet, aplikacionin dhe AAA. Dështimi pas lëvizjes mund të jetë RF, ri-autentikim, ndryshim IP ose policy e papërputhur.

Shembull: laptopi lidhet, por telefoni jo. Krahaso EAP, CA trust, PMF dhe mbështetjen e klientit; mos ul të gjithë rrjetin në një modalitet të pasigurt pa diagnozë.

Laborator: WPA, 802.1X, roaming dhe rrjetet e mysafirëve

Koha: 180 minuta. **Mjedisi:** dy AP dhe server AAA laboratorik; alternativë analizë e log-eve dhe politikave.

- Projekto dy SSID: staf me Enterprise dhe mysafir me izolim. Përcakto PKI dhe mënyrën e shpërndarjes së profilit të klientit.
- Autentiko një klient, regjistro EAP/AAA dhe verifiko VLAN/rolin e marrë. Provo një klient me CA të gabuar; lidhja duhet të refuzohet sipas profilit.
- Nise një sesion zëri ose një stream lokal dhe lëviz mes dy AP-ve. Mat ndërprerjen dhe lidhe me event-et e roaming.
- Testo mysafir→Internet laboratorik, mysafir→staf dhe mysafir→mysafir. Mbaj prova për ndalimin dhe lejimin.

- Defekti: autentikimi pranohet por klienti nuk merr IP. Ndiq VLAN, trunk, DHCP dhe policy pas AAA.

Dorëzimi: profile, matricë aksesesh dhe timeline roaming. **Pranimi:** certifikata e serverit verifikohet; izolimi provohet; EAP success nuk barazohet me shërbim të plotë. **Thellim:** projekto rinovimin e certifikatave dhe aksesin e pajisjeve pa supplicant pa krijuar rrugë të pakontrolluar drejt stafit.

26. Firewall, NAT dhe segmentimi

Gjendja e lidhjeve, ACL dhe mbrojtja e zonave

Teori: Gjendja e lidhjeve, ACL dhe mbrojtja e zonave

Objektivi: të përkthesh një kërkesë biznesi në policy të testueshme dhe me privilegj minimal.

ACL stateless vlerëson paketat sipas fushave dhe rendit të rregullave. Firewall stateful mban gjendje lidhjesh dhe lejon trafikun e kthimit sipas politikës. Rendi, drejtimi, implicit action dhe vendi i zbatimit janë pjesë e kuptimit të rregullit. Një rregull që funksionon në hyrje mund të mos ketë të njëjtat adresa pas NAT në një fazë tjetër të pipeline-it.

SNAT ndryshon burimin; DNAT destinacionin; PAT ndan një adresë me porta të ndryshme. NAT nuk është mekanizëm i plotë sigurie: kufizimi i hyrjeve vjen nga politika dhe gjendja, jo nga garancia kriptografike e përkthimit. Hairpin NAT, port exhaustion dhe aplikacionet që fusin adresa në payload kërkojnë analizë të veçantë. IPv6 mund të filtrohet pa NAT.

Zona përdorues, serverë, menaxhim, mysafirë dhe DMZ duhet të kenë rrjedha të dokumentuara. Default deny me leje konkrete është i menaxhueshëm kur ekziston inventar i varësive. DNS, NTP, PKI dhe shërbimet e identitetit shpesh harrohen. Log-o ngjarjet e dobishme pa krijuar volum që fsheh incidentet. Ndryshimet kanë pronar, arsye dhe afat rishikimi.

Asimetria e routing-ut mund të prishë firewall stateful kur drejtimet kalojnë në pajisje që nuk ndajnë gjendjen. Anti-spoofing/uRPF redukton burime të falsifikuara, por strict mode mund të ndikojë rrugë legjitime asimetrike. IDS zbulon dhe IPS mund të bllokojë; false positives dhe kapaciteti duhet të maten. DDoS volumetrik që mbush uplink-un kërkon bashkëpunim upstream, jo vetëm rregull lokal.

Shembull: lejo klientët drejt serverit vetëm TCP/443, DNS drejt resolver-it dhe menaxhim vetëm nga jump host. Testo edhe refuzimin e portave të tjera.

Laborator: Gjendja e lidhjeve, ACL dhe mbrojtja e zonave

Koha: 180 minuta. **Mjedisi:** router Linux në namespace ose firewall virtual; ruaj konfigurimin para provës.

- Shkruaj matricën burim, destinacion, protokoll, portë, drejtim dhe arsye. Përfshi varësitë e aplikacionit.
- Në namespace të router-it apliko policy vetëm për laboratorin. Përdor shembullin `firewall.nft` nga burimet dhe lexo rendin e chain-eve përpara aplikimit.
- Testo HTTP në 8080 si trafik i lejuar dhe një portë tjetër si e ndaluar. Verifiko counters dhe kthimin e lidhjes.
- Defekti: një rregull i gjerë përpara rregullit specifik e bën këtë të fundit të padobishëm. Jep provën nga counters dhe korrigjo rendin.

- Në letër ndiq adresat para/pas SNAT dhe DNAT dhe shëno çfarë sheh klienti, firewall dhe serveri.

Dorëzimi: policy, rezultatet pozitive/negative dhe diagram NAT. **Pranimi:** testi nuk prek firewall-in e hostit kryesor; rregullat kanë scope të qartë; NAT dhe siguria dallohen. **Thellim:** projekto HA stateful me dy dalje dhe shpjego çfarë ndodh me sesionet ekzistuese gjatë failover.

27. Identiteti, NAC dhe menaxhimi i sigurt

AAA, 802.1X, plane menaxhimi dhe hardening

Teori: AAA, 802.1X, plane menaxhimi dhe hardening

Objektivi: të kontrollosh kush hyn në rrjet dhe kush mund të ndryshojë pajisjet.

AAA ndan authentication, authorization dhe accounting: identitetin, lejet dhe gjurmën e veprimeve. RADIUS përdoret gjerësisht për akses rrjeti; TACACS+ përdoret shpesh për administrim pajisjesh me kontroll komandash sipas platformës. Transporti, mbrojtja dhe integrimi ndryshojnë; mos trajto një shared secret si zëvendësim automatik të një kanali të sigurt. RBAC lidh detyrat me role të kufizuara.

802.1X përdor supplicant, authenticator dhe server autentikimi. NAC mund të përdorë identitetin, llojin e pajisjes dhe posture për VLAN/role dinamike. MAB mbështetet te MAC dhe është më i dobët ndaj imitimit; përdoret me segmente dhe leje të kufizuara. Fail-open dhe fail-closed kanë pasoja biznesi të ndryshme kur AAA mungon dhe duhet të projektohen, jo të zbulohen gjatë incidentit.

Menaxhimi ka nevojë për rrjet/VRF të dedikuar, OOB kur është e mundur, jump host, SSH me identitete të kontrolluara dhe MFA në pikat përkatëse. SNMPv3 me autentikim/privatësi është zgjedhje më e përshtatshme se community strings të pambrojtura. Control-plane policing mbron burimet e router-it nga trafik i tepërt pa ndryshuar domosdoshmërisht politikën e trafikut tranzit.

Hardening përfshin çaktivizimin e shërbimeve të panevojshme, kontrollin e discovery protokolleve sipas portës, përditësimet, backup-in e konfigurimit dhe verifikimin e rikthimit. Çelësat dhe secrets mbahen jashtë repos dhe log-eve. Një llogari emergjence kërkon ruajtje, auditim dhe testim të kontrolluar; nuk duhet të bëhet hyrja e përditshme.

Shembull: një operator mund të shohë gjendjen e portave, por jo të ndryshojë BGP. Autentikimi i suksesshëm nuk nënkupton autorizim për çdo komandë.

Laborator: AAA, 802.1X, plane menaxhimi dhe hardening

Koha: 150 minuta. **Mjedisi:** pajisje virtuale me AAA dhe konsolë rezervë ose analizë profilesh.

- Krijo tri role: vëzhgues, operator dhe administrator. Cakto komanda/shërbime të lejuara dhe të ndaluara për secilin.
- Konfiguro AAA laboratorik duke ruajtur konsolën dhe një rrugë rikthimi të provuar. Testo fillimisht hyrjen, pastaj autorizimin, pastaj accounting.
- Simulo mungesën e serverit AAA vetëm në laborator. Verifiko nëse sjellja reale përputhet me planin fail-open/fail-closed dhe llogarinë emergjente.
- Për një printer pa 802.1X cakto segment të kufizuar dhe prova që nuk arrin menaxhimin e router-it.

- Defekti: identiteti pranohet, por roli është i gabuar. Ndiq atributet e përgjigjes AAA dhe mapping në pajisje.

Dorëzimi: matrica e roleve, rezultatet e hyrjes dhe provat e autorizimit. **Pranimi:** ruhet akses rikthimi; secrets nuk dorëzohen; testohen edhe komandat e ndaluara. **Thellim:** projekto ndarje detyrash për ndryshime të routing-ut dhe rishikim periodik të lejeve të menaxhimit.

28. VPN dhe kriptimi i lidhjeve

IPsec, WireGuard dhe akses në distancë

Teori: IPsec, WireGuard dhe akses në distancë

Objektivi: të zgjedhësh tunelin sipas modelit të besimit dhe ta diagnostikosh sipas fazave.

Një tunel mbart një paketë brenda një tjetre; jo çdo tunel kripton. GRE dhe VXLAN vetëm nuk japin konfidencialitet. VPN shton mekanizma sigurie sipas teknologjisë dhe konfigurimit. Site-to-site lidh rrjete; remote access lidh përdorues ose pajisje me policy dhe identitete të veçanta.

IPsec përdor Security Associations, selektorë dhe ESP për mbrojtje të trafikut. IKEv2 negocion dhe autentikon marrëveshjet. Tunnel mode mbart paketën e plotë të brendshme; transport mode mbron pjesën e përshtatshme pa të njëjtën paketizim të jashtëm. NAT-T ndihmon kalimin e disa skenarëve NAT. “IKE up” nuk provon se child SA, selektorët dhe routing-u për trafikun real janë të saktë.

WireGuard përdor çelësa publikë për peers dhe AllowedIPs për lidhjen e prefikseve me peer-in dhe kontrollin e adresave të brendshme. Kërkon menaxhim identitetesh, shpërndarje/rrotullim çelësash dhe routing të qartë; nuk ka vetë të gjitha funksionet e një sistemi të plotë identiteti përdoruesish. Keepalive mund të ndihmojë gjendjen NAT kur është i nevojshëm.

Split tunnel dërgon vetëm destinacione të caktuara në VPN; full tunnel përfshin zakonisht daljen e përgjithshme. DNS split, prefikset e mbivendosura, IPv6 dhe policy e endpoint-it ndikojnë rezultatin. Overhead-i ul MTU-në efektive. Rekey, certifikata të skaduara, ora dhe algoritmet e papërputhshme krijojnë dështime periodike ose gjatë ngritjes.

Shembull: numëruesit e encrypt rriten, por decrypt jo. Kontrollo skajin e largët, kthimin, NAT dhe selektorët. Mos përfundo se “tuneli punon” vetëm nga ikona e gjelbër.

Laborator: IPsec, WireGuard dhe akses në distancë

Koha: 180 minuta. **Mjedisi:** dy gateway virtuale të izoluara, me implementim IPsec ose WireGuard të dokumentuar.

- Përgatit planin e jashtëm, subnet-et e brendshme, identitetet dhe rrjedhat e lejuara. Gjenero çelësa testimi; mos i vendos në raport.
- Ngri tunelin dhe verifiko handshake/SA, pastaj routing, policy dhe transferimin real. Kap në të jashtmen për të vërtetuar se payload-i i brendshëm nuk shihet si trafik i hapur.
- Testo dy madhësi paketash dhe një transferim që zgjat. Regjistro MTU dhe counters në të dy skajet.
- Defekti: një prefiks mungon te selektorët ose AllowedIPs. Krahaso një subnet që punon me një që nuk punon dhe lokalizo fazën.

- Projekto rikthimin pas rekey dhe rinovimin e identitetit pa ndërprerje të panevojshme.

Dorëzimi: diagram, konfigurim i redaktuar pa secrets dhe prova në dy drejtimet. **Pranimi:** testi përfshin shërbim real; kufizimet e routing-ut dhe kriptimit ndahen; çelësat mbahen privatë. **Thellim:** zgjidh mbivendosjen 192.168.1.0/24 mes dy site-ve përmes riadresimit ose përkthimit të dokumentuar.

29. WAN, SD-WAN dhe skajet e ndërmarrjes

Underlay, overlay, politika dhe përzgjedhja e rrugës

Teori: Underlay, overlay, politika dhe përzgjedhja e rrugës

Objektivi: të ndërtosh lidhje mes site-ve me objektiva të matshëm dhe sjellje të qartë në dështim.

WAN mund të përdorë shërbime Ethernet operatori, MPLS VPN, Internet, lidhje radio ose celular. CIR, SLA, demarkacioni, MTU dhe modeli i përgjegjësisë duhen kuptuar nga kontrata dhe matjet. Një shërbim L2 nuk menaxhon routing-un e klientit si një shërbim L3. PPP/PPPoE mbeten të pranishme në akses dhe mund të ulin MTU-në efektive.

Underlay jep transportin bazë IP; overlay krijon lidhjet logjike dhe policy mbi të. SD-WAN zakonisht ndan kontrollin, orkestrimin dhe përcjelljen, duke matur rrugët dhe duke zbatuar politika aplikacionesh. Nuk eliminon nevojën për routing, DNS, kapacitet dhe diagnostikim të lidhjes bazë. Dy tunele mbi një uplink fizik mbeten një failure domain për atë uplink.

Application-aware routing përdor metrika si humbje, latency dhe jitter. Hysteresis dhe hold-down shmangin kalime të shpeshta. Matjet aktive nuk përfaqësojnë domosdoshmërisht të gjithë trafikun në çdo klasë QoS. Local breakout ul kthimin në qendër, por kërkon kontroll sigurie dhe shërbime identiteti/DNS që funksionojnë në degë.

SASE dhe ZTNA përfshijnë modele sigurie dhe akses sipas identitetit/kontekstit; nuk janë emra të një protokolli të vetëm. Vendosja cloud e një pike sigurie sjell varësi nga vendndodhja, shërbimi, rezidenca e të dhënave dhe rrugët e kthimit. Skenarët duhet të provohen për site, aplikacion dhe dështim të veçantë.

Shembull: prefero lidhjen A për zë kur humbja dhe jitter janë brenda objektivit; kalo në B vetëm pas konfirmimit të qëndrueshëm dhe kthehu sipas politikës së dokumentuar.

Laborator: Underlay, overlay, politika dhe përzgjedhja e rrugës

Koha: 180 minuta. **Mjedisi:** dy site virtuale me dy lidhje të emuluara; në mungesë SD-WAN përdor analizë politikash.

- Dokumento dy lidhje me kapacitet, RTT, humbje, MTU dhe kosto. Përcakto objektiva për zë, ERP dhe backup.
- Shkruaj policy për zgjedhjen e rrugës dhe kthimin, me hysteresis. Dallo aplikacionet që mund të kalojnë lidhje nga ato që humbin sesionin.
- Në emulator shto vonesë ose humbje vetëm në një lidhje testimi; mat përzgjedhjen dhe përvojën e aplikacionit.

- Defekti: overlay është down, por underlay ping punon. Kontrollo transportin e tunelit, identitetin, NAT, kontrollin dhe MTU-në sipas fazave.
- Analizo dështimin e kontrollorit dhe humbjen e të dy uplink-eve: cilat politika dhe shërbime lokale vazhdojnë?

Dorëzimi: policy, timeline dhe matrica e përgjegjësisë klient/operator. **Pranimi:** vendimet janë të matshme; tunelet nuk numërohen si pavarësi fizike; kthimi testohet. **Thellim:** krahaso central breakout me local breakout për siguri, latency dhe kosto operimi.

30. MPLS dhe Segment Routing

Label switching, L3VPN dhe inxhinieria e trafikut

Teori: Label switching, L3VPN dhe inxhinieria e trafikut

Objektivi: të ndash arritshmërinë e operatorit nga rrugët e klientit dhe të ndjekësh label stack.

MPLS përcjell me labels me kuptim lokal sipas kontekstit të shpërndarjes. Operacionet kryesore janë push, swap dhe pop. Një label nuk është adresë globale e hostit. LSP është rruga e label switching; LFIB ruan gjendjen përkatëse. IGP jep arritshmëri të underlay-t, ndërsa LDP, RSVP-TE ose mekanizma Segment Routing krijojnë gjendjen e labels sipas arkitekturës.

Në një L3VPN, CE lidhet me PE; P transporton pa pasur nevojë për të gjitha rrugët e klientëve. VRF ndan tabelat e klientit. Route Distinguisher bën rrugët VPN unikale në kontroll; Route Target kontrollon import/eksport sipas politikës. RD dhe RT nuk janë të këmbyeshme. MP-BGP shpërndan rrugët VPN me metadata përkatëse.

Në një rrugë tipike përdoren label transporti për të arritur PE-në dhe label VPN për kontekstin e klientit. Numri dhe sjellja ndryshojnë me dizajnin, PHP dhe shërbimin. MTU duhet të llogarisë çdo label dhe encapsulation shtesë. MPLS VPN jep ndarje logjike, jo automatikisht kriptim.

Segment Routing shpreh një rrugë ose udhëzim me segments. SR-MPLS përdor labels; SRv6 përdor IPv6 dhe funksione të koduara sipas arkitekturës. Node-SID, adjacency-SID, SRGB, TI-LFA dhe traffic engineering kanë parakushte topologjie dhe mbështetje hardware. SRv6 nuk është thjesht “MPLS me adresë më të gjatë”; ndikimi në header, policy dhe kapacitet duhet matur.

Shembull: dy klientë përdorin 10.0.0.0/24 në VRF të ndryshme. RD-të i bëjnë rrugët të dallueshme në MP-BGP; RT-të përcaktojnë kush i importon. Kriptimi shtohet veçmas nëse kërkohet.

Laborator: Label switching, L3VPN dhe inxhinieria e trafikut

Koha: 180 minuta. **Mjedisi:** emulator me dy PE, një P dhe dy CE; kërkohet imazh që mbështet funksionet e zgjedhura.

- Vizato dy VPN me adresa të mbivendosura. Cakto VRF, RD dhe RT dhe shkruaj saktësisht cilat rrugë importohen.
- Verifiko fillimisht IGP dhe transportin mes loopback-eve të PE-ve. Pastaj kontrollo labels dhe MP-BGP VPN routes.
- Gjurmo një paketë klienti në hyrje të PE, në P dhe në dalje. Nëse kapja nuk tregon hardware forwarding, përdor tabelat dhe deklaro kufirin.
- Defekti: RT i importit është i gabuar. Dallo rrugën ekzistuese në BGP VPN nga mungesa e saj në VRF.

- Llogarit MTU për dy labels mbi paketë 1500 byte dhe krahaso me rastin SR që kërkon stack më të gjatë.
- Shëno nëse numërimi përfshin vetëm paketën MPLS apo edhe header-in Ethernet të lidhjes fizike.

Dorëzimi: diagram labels, tabela import/eksport dhe analiza e MTU-së. **Pranimi:** RD/RT dallohen; dy labels shtojnë 8 byte; izolimi nuk quhet kriptim. **Thellim:** projekto një shërbim shared-services me route leaking të kufizuar dhe pa krijuar komunikim të pakontrolluar mes klientëve.

31. Datacenter dhe EVPN/VXLAN

Leaf-spine, VTEP, VNI dhe kontrolli i fabric-ut

Teori: Leaf-spine, VTEP, VNI dhe kontrolli i fabric-ut

Objektivi: të ndajësh underlay-in IP nga overlay-i i tenant-it dhe të diagnostikosh një endpoint të paarritshëm.

Leaf-spine ofron rrugë me numër të parashikueshëm hop-esh dhe ECMP mes leaf-eve. Serverët lidhen te leaf; spine transporton mes tyre. Planifiko oversubscription, failure domain, shpejtësi dhe kapacitet pas dështimit të një spine-i. East-west përshkruan trafik mes shërbimeve brenda mjedisit; north-south hyrje/dalje nga ai mjedis.

VXLAN mbart frame Ethernet mbi UDP/IP. VTEP kryen encapsulation/decapsulation; VNI identifikon segmentin overlay. Underlay duhet të arrijë loopback-et e VTEP-ve dhe të përballojë MTU-në shtesë. Për IPv4 të jashtëm pa opsione dhe Ethernet pa tag, overhead-i tipik ndaj frame-it të brendshëm është 50 byte, duke numëruar Ethernet-in e jashtëm; përcakto gjithmonë çfarë niveli mat.

EVPN përdor MP-BGP për të shpërndarë arritshmëri të MAC/IP dhe shërbime të tjera. Route type 2 për MAC/IP, type 3 për informacionin e BUM dhe type 5 për prefikse IP shërbejnë qëllime të ndryshme. Type 1/4 lidhen me multihoming sipas modelit. Route targets kontrollojnë importin e tenant-it; type 5 nuk zëvendëson çdo route type tjetër.

Distributed anycast gateway mundëson gateway të qëndrueshëm afër hostit. Symmetric IRB përdor kontekste L2/L3 VNI sipas arkitekturës. ARP/ND suppression redukton flooding, por varet nga gjendja e saktë. MAC mobility duhet të trajtojë migrimet reale pa fshehur loop-et. EVPN multihoming kërkon ESI, zgjedhje DF dhe split-horizon të sakta.

Shembull: endpoint-i lokal punon, ai i largët jo. Kontrollo VTEP reachability, VNI/VRF, import RT, route type 2/5 dhe pastaj FDB/ARP. Një sesion BGP Established nuk e provon gjithë fabric-un.

Laborator: Leaf-spine, VTEP, VNI dhe kontrolli i fabric-ut

Koha: 240 minuta. **Mjedisi:** dy leaf dhe një spine me Linux VXLAN/FRRouting ose imazh fabric të mbështetur. Ky laborator nuk mbulohet nga skripti bazë a–r–b.

- Cakto loopback-et e VTEP, subnet-et transit, L2VNI 10100 dhe një VRF tenant-i. Ndiq udhëzimin zyrtar EVPN për versionin e zgjedhur.
- Provo underlay me IP dhe MTU përpara aktivizimit të overlay-t. Regjistro tabelën e routing-ut të loopback-eve.
- Aktivizo EVPN address family dhe kontrollo route type 2/3; për routing mes subnet-eve shto L3VNI/IRB sipas modelit të dokumentuar.

- Defekti: ndrysho RT import vetëm në një leaf. Vëzhgo rrugën në BGP global dhe mungesën në tenant; riktheje.
- Gjurmo një frame lokal dhe një të encapsuluar, duke shënuar outer/inner MAC dhe IP.

Dorëzimi: tabelë VNI/VRF/RT, verifikim underlay/overlay dhe prova e defektit. **Pranimi:** MTU llogaritet; konfigurimi është i lidhur me një platformë/version; endpoint-i testohet në dy drejtimet. **Thellim:** analizo lëvizjen e një MAC dhe dështimin e një lidhjeje multihoming pa supozuar se MLAG dhe EVPN ESI janë e njëjta teknologji.

32. Rrjetet cloud dhe hibride

VPC/VNet, peering, transit dhe shërbimet private

Teori: VPC/VNet, peering, transit dhe shërbimet private

Objektivi: të projektosh adresim dhe policy cloud pa supozuar semantikën e LAN-it fizik.

VPC/VNet përfaqëson një kufi logjik rrjeti sipas ofruesit. Subnet, route table, gateway, firewall/security group dhe shërbimet private janë objekte me semantikë specifike. Broadcast, multicast dhe kontrolli i L2 nuk ofrohen si në një switch fizik në çdo platformë. Adresat e rezervuara për subnet dhe kapaciteti i shërbimeve duhen verifikuar në dokumentacionin e ofruesit.

Një subnet “publik” ose “privat” përcaktohet nga routing-u, adresimi dhe politika, jo vetëm nga emri. NAT gateway mundëson disa dalje me përkthim; private endpoint lidh shërbime në një model tjetër. Security groups shpesh janë stateful dhe ACL subnet shpesh kanë model tjetër, por sjellja nuk përgjithësohet pa emërtuar platformën.

Peering lidh dy rrjete sipas kufizimeve të ofruesit; transitiviteti nuk duhet supozuar. Transit hub/gateway centralizon lidhjet me kosto, throughput dhe failure domain shtesë. VPN dhe lidhjet e dedikuara hibride përdorin routing, shpesh BGP. Prefikset e mbivendosura, route limits dhe MTU mund të bllokojnë integrimin edhe kur tuneli ngrihet.

Cloud DNS dhe conditional forwarding duhet të lidhin emrat privatë me rrugët e arritshme. Load balancer, CDN, NAT dhe egress kanë kosto sipas modelit përkatës; transferimi mes zonave mund të ndryshojë buxhetin. Flow logs janë metadata dhe mund të kenë vonesë, sampling ose kufizime; nuk janë zëvendësim i plotë i PCAP.

Shembull: aplikacioni arrin IP publike por jo private endpoint. Kontrollo DNS-in që kthen adresën, route table, policy dhe miratimin e endpoint-it. Rruga më e shkurtër në diagram nuk është domosdoshmërisht rruga reale e faturuar.

Laborator: VPC/VNet, peering, transit dhe shërbimet private

Koha: 180 minuta. **Mjedisi:** projektim lokal; zbatimi cloud është opsional në sandbox të kontrolluar dhe nuk kërkohet blerje.

- Zgjidh një ofrues dhe dokumento semantikën e route table, firewall dhe adresave të rezervuara nga burimi zyrtar para zbatimit.
- Projekto dy zona, subnet-e aplikacioni dhe të dhënash, dalje të kontrolluar dhe lidhje me zyrën. Përdor CIDR që nuk mbivendosen.
- Plotëso matricën aplikacion→databazë, admin→menaxhim dhe Internet→frontend. Shëno ku zbatohet çdo kontroll.

- Defekti analitik: A peer-on me B dhe B me C; A nuk arrin C. Jep plan që nuk supozon transitivitet të peering-ut.
- Vlerëso trafikun mujor, dalje/transferim ndërzona dhe koston me parametrat e dokumentuar të sandbox-it; mos përdor çmime të vjetra nga kujtesa.

Dorëzimi: diagram, route tables, DNS plan dhe përllogaritje me datë/burim. **Pranimi:** nuk krijohen burime me pagesë si kusht i kursit; semantika lidhet me një ofrues; testi përfshin trafikun e ndaluar. **Thellim:** projekto failover hibrid me dy lidhje dhe prefikse më specifike pa blackhole.

33. Rrjetëzimi në Linux dhe Windows

Host routing, sockets, DNS dhe virtual switching

Teori: Host routing, sockets, DNS dhe virtual switching

Objektivi: të diagnostikosh endpoint-in përpara ndryshimit të infrastrukturës.

Hosti ka tabela routing-u, cache fqinjësh, sockets, firewall dhe resolver. Një aplikacion mund të dëgjojë vetëm në loopback dhe të mos pranojë lidhje nga rrjeti edhe kur porta duket e hapur lokalisht. Binding në 0.0.0.0 mbulon ndërfaqet IPv4 sipas sistemit; sjellja dual stack me :: duhet verifikuar. Network namespace ndan gjendjen e rrjetit në Linux; VRF dhe namespace nuk janë sinonime për çdo burim.

Në Linux, `ip address`, `ip route`, `ip rule`, `ip neigh`, `ss` dhe `resolvectl` kur disponohet mbulojnë pjesë të ndryshme. `ip route get` tregon vendimin për një destinacion në kontekstin e komandës. Konfigurimi runtime me `ip` mund të humbasë pas rinisjes; NetworkManager, systemd-networkd ose mjeti i distribucionit ruan konfigurimin sipas mjedisit.

Në Windows, PowerShell ofron `Get-NetIPConfiguration`, `Get-NetRoute`, `Get-NetNeighbor`, `Get-NetTCPConnection`, `Resolve-DnsName` dhe `Test-NetConnection`. Profili Domain/Private/Public ndikon rregullat e firewall-it. Hyper-V vSwitch, teaming dhe adapter-at virtualë shtojnë shtresa që duhet të vendosen në diagram. Një VPN klient mund të ndryshojë route metrics dhe DNS vetëm për disa emra.

Container, VM dhe host fizik mund të kenë disa MTU dhe firewall-e. Kontrollo ku dëgjon shërbimi, ku zbatohet NAT dhe cilën IP përdor klienti. Një test lokal në loopback anashkalon shumë komponentë të rrugës reale.

Shembull: serveri punon me `curl localhost:8080`, por jo nga hosti tjetër. Kontrollo bind address, firewall, routing dhe kapjen në server sipas radhës; testi lokal nuk provon hyrjen nga rrjeti.

Laborator: Host routing, sockets, DNS dhe virtual switching

Koha: 120 minuta. **Mjedisi:** një Linux dhe, nëse disponohet, Windows; nuk kërkohet ndryshim i rrjetit të hostit fizik.

- Mblidh IP, rrugët, fqinjët, DNS dhe sockets aktive. Në raport redakto adresat/identitetet reale që nuk i përkasin laboratorit.
- Nise HTTP vetëm në loopback të namespace b, provo lokalisht dhe nga a, pastaj lidhe me adresën e laboratorit. Krahaso rezultatet.
- Në Windows teston veçmas `Resolve-DnsName EMRI` dhe `Test-NetConnection ADRESA -Port 8080`, duke zëvendësuar vlerat; shëno cilën pjesë provon secila.
- Defekti: dy default route me metrika të ndryshme ose VPN me rrugë më specifike. Parashiko daljen për tre destinacione.

- Dallo konfigurimin runtime nga ai persistent dhe shkruaj si verifikohet pas një rinisjeje të VM-së laboratorike.

Dorëzimi: inventar hosti dhe tabela lokal/larg. **Pranimi:** bind address është identifikuar; sintaksat Windows/Linux nuk ngatërrohen; ndryshimet bëhen në VM/namespace. **Thellim:** analizo policy routing me dy burime IP dhe dy dalje dhe ndikimin e source address selection.

34. Containers dhe Kubernetes

CNI, Services, NetworkPolicy dhe rrjeti i cluster-it

Teori: CNI, Services, NetworkPolicy dhe rrjeti i cluster-it

Objektivi: të ndjekësh një kërkesë nga klienti deri te pod-i dhe të dallosh rrjetin nga discovery.

Container-at në Linux shpesh përdorin network namespaces, veth dhe bridge ose dataplane alternativ. Docker bridge zakonisht shton NAT për dalje sipas konfigurimit; host networking ndan rrjetin e hostit. Port publishing map-on një portë të hostit drejt shërbimit; nuk provon që aplikacioni brenda container-it po dëgjon në adresën e duhur.

Kubernetes ia delegon lidhjen e Pod-it një implementimi CNI. Pod CIDR, Service CIDR dhe rrjeti i node-ve duhet të jenë të planifikuara pa mbivendosje. CNI mund të përdorë overlay, routing të drejtpërdrejtë ose mekanizma të tjerë. ClusterIP është adresë virtuale shërbimi me dataplane që varet nga implementimi; nuk është domosdoshmërisht IP e vendosur në ndërfaqen e një hosti.

Service zgjedh endpoints sipas selectors dhe gjendjes. CoreDNS zgjidh emrat e cluster-it, por DNS i saktë nuk garanton endpoint të shëndetshëm. NetworkPolicy ka nevojë për CNI që e zbaton; krijimi i objektit nuk garanton enforcement. Politikat e lejuara kombinohen sipas modelit Kubernetes; rendi i YAML-ve nuk është rend ACL klasik. DNS dhe trafiku drejt kontrollit duhen trajtuar sipas nevojës.

Ingress/Gateway API dhe LoadBalancer ofrojnë hyrje në nivele të ndryshme me controller përkatës. Service mesh mund të shtojë mTLS, policy dhe observability, por shton proxy dhe plane kontrolli. eBPF mund të implementojë funksione dataplane; nuk eliminon kuptimin e rrugës, policy dhe MTU-së.

Shembull: Service nuk përgjigjet sepse selector nuk përputhet me labels e pod-eve. Ndryshimi i routing-ut të node-ve nuk e krijon endpoint-in që mungon.

Laborator: CNI, Services, NetworkPolicy dhe rrjeti i cluster-it

Koha: 180 minuta. **Mjedisi:** cluster lokal testimi me CNI të dokumentuar; nuk kërkohet cluster publik.

- Regjistro Pod CIDR, Service CIDR, CNI dhe mënyrën e forwarding. Krijo një aplikacion testimi dhe një Service me selector të qartë.
- Kontrollo `kubectl get pods -o wide`, `kubectl get svc` dhe `kubectl get endpointslices`. Ndiq një kërkesë drejt Pod IP dhe një drejt Service.
- Provo DNS nga një pod diagnostikimi. Shëno namespace-in dhe emrin e plotë të Service-it.
- Apliko `network-policy.yaml` të kursit vetëm pasi të përshtatësh labels/namespace dhe DNS e cluster-it. Verifiko enforcement me një klient të lejuar dhe një të ndaluar.
- Defekti: ndrysho selector në Service dhe krahaso DNS-in që ende zgjidhet me mungesën e endpoints.

Dorëzimi: diagram Pod→Service→endpoint, YAML dhe rezultatet. **Pranimi:** CNI identifikohet; një objekt NetworkPolicy pa test nuk quhet kontroll i verifikuar; konfigurimi është vetëm për namespace laboratorik. **Thellim:** ndjek një paketë ndërmjet node-ve me overlay dhe llogarit MTU efektive.

35. Automatizimi dhe rrjeti si kod

API, NETCONF, YANG, Ansible dhe validimi

Teori: API, NETCONF, YANG, Ansible dhe validimi

Objektivi: të ndërtosh ndryshim të përsëritshëm me kontroll para dhe pas, pa ekspozuar secrets.

Automatizimi fillon me inventar dhe model të saktë të gjendjes së dëshiruar. Një script që dërgon komanda më shpejt mund të përhapë gabime më shpejt. Source of truth mban identitetin e pajisjeve, adresat, rolet dhe lidhjet; templating e kthen në konfigurim. Validimi duhet të kontrollojë tipe, vlera, prefikse, marrëdhënie dhe kufizime platforme.

SSH CLI scraping është i dobishëm por varet nga tekst/formati. NETCONF ofron operacione të strukturuara me datastore dhe aftësi që negociohen; candidate dhe confirmed commit nuk mbështeten njësoj në çdo pajisje. RESTCONF jep akses HTTP ndaj të dhënave të modeluara sipas mbështetjes. YANG përshkruan strukturën dhe kufizimet; OpenConfig ofron modele të përbashkëta për disa funksione. gNMI përdoret për operacione dhe streaming telemetry sipas implementimit.

Idempotence do të thotë që përsëritja drejt së njëjtës gjendje nuk krijon ndryshime të panevojshme. Ansible, Python dhe mjete të tjera mund ta realizojnë kur modulet dhe modelet janë të sakta; emri i mjetit nuk e garanton. Diff, dry run dhe backup japin review, por testi në topologji dhe verifikimi operacional janë thelbësorë.

Një pipeline duhet të ketë validim lokal, lint/schema, kontroll policy, preview, pilot, zbatim të kufizuar, post-check dhe rollback. Secrets ruhen në vault ose mekanizëm identiteti të përshtatshëm, jo në JSON publik. Kufizo concurrency për të mos ndryshuar të gjitha rrugët rezervë njëherësh.

Shembull: një template BGP nuk duhet të eksportojë çdo rrugë sepse inventari nuk përmban prefix-list. Fusha e munguar duhet të ndalë gjenerimin, jo të krijojë leje të përgjithshme.

Laborator: API, NETCONF, YANG, Ansible dhe validimi

Koha: 180 minuta. **Mjedisi:** Python 3 dhe skedari `inventory-example.json`; nuk kërkohen kredenciale pajisjesh.

- Ekzekuto `validate_inventory.py` mbi inventarin e kursit. Lexo kodin dhe kontrollo CIDR, IP të përsëritura dhe fushat e kërkuara.
- Shto një subnet që mbivendoset dhe verifiko refuzimin; pastaj korrigjoje. Shto një gateway jashtë subnet-it për një refuzim tjetër të dallueshëm.
- Gjenero planin e adresimit dhe krahaso diff-in. Ky mjet është validator lokal, jo sistem i plotë konfigurimi pajisjesh.

- Projekto playbook ose rrjedhë API që merr backup, kontrollon fqinjësitë, ndryshon vetëm një router dhe krahason rrugët kritike pas ndryshimit.
- Defekti: ndryshimi përfundon me timeout. Përshkruaj si kontrollohet gjendja reale para riprovimit për të shmangur dyfishim veprimesh.

Dorëzimi: inventari i vlefshëm, dy prova refuzimi dhe pipeline i dokumentuar. **Pranimi:** secrets mungojnë; gabimi ndal ekzekutimin; post-check mat rrjetin dhe jo vetëm statusin e komandës. **Thellim:** projekto confirmed commit dhe rollback kur një ndryshim prek vetë rrugën e menaxhimit.

36. Monitorimi dhe diagnostikimi operacional

Telemetria, logs, flow dhe metoda e hipotezave

Teori: Telemetria, logs, flow dhe metoda e hipotezave

Objektivi: të lokalizosh defektin me prova dhe të shmangësh ndryshime të rastësishme.

Metrics japin seri kohore; logs japin ngjarje; flow records përmbledhin komunikime; packet capture tregon paketat. SNMP polling dhe streaming telemetry kanë interval, kosto dhe semantikë të ndryshme. Syslog kërkon orë të sinkronizuar, identitet pajisjeje dhe ruajtje. NetFlow/IPFIX dhe sFlow ndryshojnë në modelin e eksportit dhe sampling; bytes e raportuar nuk përfaqësojnë domosdoshmërisht çdo paketë të telit.

Counter është vlerë kumulative; rate llogaritet nga diferenca në kohë. Rinisja, wrap dhe reset duhet të dallohen nga trafik negativ. Utilization matet kundrejt kapacitetit të saktë të ndërfaqes; port-channel dhe anëtarët nuk duhet të dyfishohen në total. CPU e ulët nuk provon se ASIC nuk po hedh paketa. Queue drops, errors, discards dhe control-plane drops janë kategori të ndryshme.

SLI përshkruan matjen; SLO objektivin; SLA marrëveshjen. Alarmet lidhen me ndikimin dhe pragje të dobishme, me deduplikim dhe pronar. Një alarm për çdo event krijon lodhje. Synthetic tests provojnë një rrjedhë të njohur, ndërsa matjet e përdoruesve zbulojnë variacionin real.

Diagnostikimi fillon me shtrirjen: kush, ku, kur, cilat aplikacione dhe çfarë ndryshoi. Ndaj plane dhe shtresa, formulo hipotezë të falsifikueshme, merr baseline, ndrysho një faktor dhe verifiko rikthimin. Dokumento edhe hipotezat e refuzuara. Postmortem shpjegon mekanizmin dhe veprimet parandaluese, jo vetëm personin që preku konfigurimin.

Shembull: ping mes router-ave punon, por aplikacioni jo vetëm për një VLAN. Ngushto te subnet/VLAN, DNS, policy dhe rruga e aplikacionit; mos rinis backbone-in pa prova.

Laborator: Telemetria, logs, flow dhe metoda e hipotezave

Koha: 180 minuta. **Mjedisi:** laboratorët e mëparshëm dhe fleta e incidentit nga burimet.

- Përgatit dashboard me disponueshmëri aplikacioni, latency, humbje, interface errors/drops, fqinjësi routing dhe gjendje DNS/NTP.
- Mblidh baseline dhjetëminutësh ose të dhëna analitike me interval të shënuar. Llogarit rate nga dy counters dhe trajto rastin e rinisjes.
- Zgjidh tre defekte: gateway i munguar, policy që bllokon portën dhe DNS i gabuar. Për secilin shkruaj hipotezën para testit.
- Lidh log-et dhe kapjet me kohën dhe identifikuesit e pajisjeve. Dallo provën e munguar nga prova që e refuzon hipotezën.

- Krijo një alarm me ndikim dhe një runbook me kontroll fillestar, eskalim dhe kriter mbylljeje.

Dorëzimi: tre raporte incidenti dhe një dashboard i skicuar ose i zbatuar. **Pranimi:** çdo korrigjim ka provë para/pas; shkaku rrënjësor dallohet nga simptoma; alarmi ka pronar dhe veprim. **Thellim:** dizajno monitorim për microburst pa u mbështetur vetëm në polling pesëminutësh.

37. Storage, industri dhe rrjete me kërkesa të veçanta

SAN, RDMA, OT dhe rrjetet deterministe

Teori: SAN, RDMA, OT dhe rrjetet deterministe

Objektivi: të kuptosh kur supozimet e rrjetit të zyrës nuk mjaftojnë.

Storage përdor protokolle si NFS, SMB, iSCSI, Fibre Channel dhe NVMe over Fabrics. iSCSI mbart komanda storage mbi TCP/IP; Fibre Channel ka arkitekturë dhe adresim të vetin; NVMe/TCP dhe NVMe/RDMA kanë kërkesa të ndryshme. MTU jumbo nuk aktivizohet vetëm në një host: gjithë rruga dhe endpoint-et duhet të përputhen. Multipath është mekanizëm i hostit/shërbimit dhe nuk barazohet me LACP.

RDMA ul pjesëmarrjen e CPU-së në transferime të caktuara. RoCE v2 përdor UDP/IP; projektimi shpesh kërkon menaxhim congestion-i dhe, sipas sistemit, PFC/ECN me konfigurim të kujdesshëm. “Lossless Ethernet” nuk do të thotë se çdo dështim zhduket. PFC mund të shkaktojë head-of-line blocking dhe përhapje presioni; monitoro pause dhe congestion në të gjithë fabric-un.

OT/ICS lidh procese fizike, sensorë dhe kontrollorë me prioritete disponueshmërie dhe sigurie funksionale. Modbus/TCP, EtherNet/IP, PROFINET dhe OPC UA kanë role dhe profile të ndryshme; emrat nuk nënkuptojnë automatikisht autentikim/kriptim. Segmentimi me zona dhe conduits, jump host dhe inventari pasiv shpesh janë më të përshtatshëm se zbulimi aktiv pa koordinim.

Time-Sensitive Networking kombinon mekanizma Ethernet për kohë, scheduling dhe kontroll trafiku sipas profileve dhe mbështetjes. PTP me timestamp hardware, boundary/transparent clocks dhe menaxhim domain-i kërkon projektim të saktë. Audio/video profesionale dhe sistemet financiare mund të kenë kërkesa kohe që NTP i zakonshëm nuk i plotëson.

Shembull: një storage cluster me latency të paqëndrueshme kërkon korrelacion mes IO, queues, pause, MTU dhe hostit. Shtimi i bandwidth-it pa lokalizuar pritjen mund të mos ndryshojë asgjë.

Laborator: SAN, RDMA, OT dhe rrjetet deterministe

Koha: 180 minuta. **Mjedisi:** projektim dhe analiza të dhënash; ndryshimet në pajisje industriale reale nuk janë pjesë e laboratorit.

- Zgjidh storage IP ose një celulë OT. Dokumento trafikun, latency, humbjen e tolerueshme, rikuperimin dhe kërkesën e kohës.
- Për storage vizato dy rrugë multipath dhe identifiko komponentët e përbashkët. Për OT vizato zonat, conduits dhe aksesin e mirëmbajtjes.
- Analizo tabelë me RTT, retransmissions, queue drops, pause frames dhe latency aplikacioni. Jep dy hipoteza dhe provën për secilën.

- Defekti: jumbo MTU në hoste, por jo në një switch transit. Projekto test madhësie dhe plan rikthimi pa prekur prodhimin.
- Për një sistem PTP cakto burimet e kohës, failure domain dhe alarmet për offset/ndryshim grandmaster.

Dorëzimi: projekt specializimi dhe matricë kërkesash/provash. **Pranimi:** LACP dhe multipath dallohen; nuk bëhet skanim në OT real; PFC nuk propozohet si zgjidhje universale. **Thellim:** argumento kur NVMe/TCP është zgjedhje më e menaxhueshme se RDMA dhe cilat matje do ta ndryshonin vendimin.

38. Rrjetet e operatorëve dhe aksesit

Optika, PON, celulari, CGNAT dhe satelitët

Teori: Optika, PON, celulari, CGNAT dhe satelitët

Objektivi: të identifikosh varësitë dhe kufijtë jashtë LAN-it të ndërmarrjes.

Rrjeti i operatorit ka shtresa akses, agregim, core dhe interconnection. Shërbimet optike përdorin fibra, amplifikim dhe teknologji si DWDM/OTN sipas distancës dhe kapacitetit. Buxheti optik dhe mbrojtja e rrugëve kërkojnë njohje të traseve reale; dy wavelengths mbi të njëjtën fibër nuk janë dy rrugë fizike të pavarura.

PON ndan medium optik mes OLT dhe ONU/ONT me mekanizma të planifikimit. Split ratio, buxheti optik dhe ngarkesa e përdoruesve ndikojnë shërbimin. Rrjetet kabllore DOCSIS dhe aksesi DSL kanë mekanizma e kufizime të tjera. Një portë Ethernet 1 Gbit/s në ONT nuk garanton 1 Gbit/s të dedikuar deri në Internet.

Rrjetet celulare 4G/5G ndajnë radio access dhe core. SIM/eSIM identifikon abonimin; adresimi IP, APN/DNN, policy dhe tunelet varen nga shërbimi. GTP përdoret në plane transporti sipas arkitekturës. Roaming celular, handover radio dhe Wi-Fi roaming janë procese të ndryshme. Private 5G kërkon kompetenca radio dhe licencimi përtej një LAN-i.

CGNAT ndan IPv4 publike mes abonentëve dhe kufizon disa hyrje/sesione; adresa WAN e router-it mund të mos jetë publike. IPv6, port mapping dhe shërbimet private ndryshojnë mundësitë. Satelitët GEO kanë RTT të lartë nga distanca; LEO ul komponentin e përhapjes por sjell variacion, handovers dhe varësi nga pamja e qiellit. Mesh wireless dhe lidhjet point-to-point kërkojnë line-of-sight dhe buxhet RF.

Shembull: një VPN punon me fibër por jo me backup celular. Kontrollo NAT, MTU, portat/protokollet, adresimin dhe timers; mos supozo se çdo akses IP ka të njëjtën sjellje.

Laborator: Optika, PON, celulari, CGNAT dhe satelitët

Koha: 150 minuta. **Mjedisi:** analizë shërbimesh dhe, opsionalisht, lidhje laboratorike me dy lloje aksesi.

- Ndërto tabelë fibër/PON, celular, radio dhe satelit: kapacitet, RTT, jitter, adresim, NAT, MTU, disponueshmëri dhe kosto sipas parametrave të dhënë.
- Krahasoni adresën WAN të pajisjes me adresën e dukshme në dalje në një shërbim të autorizuar. Dallo NAT lokal nga CGNAT; mungesa e njëjtësisë nuk identifikon vetë çdo hop.
- Për një degë me backup celular projekto VPN që ngrihet nga brenda, monitorim, kufi trafiku dhe DNS të qëndrueshëm.
- Defekti: ndërrimi i uplink-ut ndryshon IP publike dhe prish sesionin. Dallo rikthimin e reachability nga ruajtja e sesioneve.
- Analizo dy oferta operatorësh dhe kërko dokumentim të demarkacionit dhe diversitetit fizik.

Dorëzimi: zgjedhje e arsyetuar dhe plan testimi të backup-it. **Pranimi:** port speed nuk ngatërrohet me CIR; diversiteti provohet; adresat shembull nuk përdoren për reklamim publik. **Thellim:** projekto komunikim për një site të largët me latency të ndryshueshme, store-and-forward dhe aplikacione që duhet të punojnë offline.

39. Projektimi dhe cikli i jetës së rrjetit

Kërkesat, dokumentimi, ndryshimet dhe rikuperimi

Teori: Kërkesat, dokumentimi, ndryshimet dhe rikuperimi

Objektivi: të dorëzosh një rrjet që mund të operohet, të testohet dhe të rikthehet.

Projektimi fillon me aplikacionet, përdoruesit, vendndodhjet, rritjen dhe objektivat e shërbimit. HLD përshkruan arkitekturën dhe kompromiset; LLD adresat, portat, protokollet, policy dhe konfigurimet konkrete. Bill of materials duhet të përfshijë licenca, module, kabllo, energji, suport dhe kapacitet rezervë. Blerja e pajisjeve para përcaktimit të kërkesave e kthen projektin në përshtatje të kufizimeve të rastit.

Domenet e dështimit, agregimi, hierarkia e adresimit, kufijtë L2/L3 dhe OOB janë vendime që ndikojnë operimin. Kapaciteti pas dështimit $N-1$ duhet të mbajë trafikun kritik. RTO përshkruan kohën e synuar të rikuperimit; RPO humbjen e pranueshme të të dhënave/gjendjes sipas shërbimit. Backup i konfigurimit pa prova rikthimi nuk përmbush vetë objektivin.

Çdo ndryshim kërkon gjendje fillestare, diff, ndikim, kontrolle, kohëzgjatje, pronar dhe rollback me kriter të qartë. Migrimi mund të bëhet me pilot, grupe të kufizuara dhe periudhë vëzhgimi. Mos ndrysho dy rrugët rezervë njëkohësisht vetëm sepse automatizimi mundet. Mbaj rrugë menaxhimi që nuk varet plotësisht nga komponenti që ndryshohet.

Dokumentet as-built duhet të pasqyrojnë gjendjen reale: diagram fizik/logjik, IPAM, matrica e flukseve, konfigurime të redaktuara, monitorim dhe runbooks. Testet e pranimit përfshijnë funksionim normal, siguri, dështim, rikthim dhe ngarkesë. Ekipi duhet ta kuptojë rrjetin pa pasur nevojë për autorin e parë.

Shembull: para migrimit të gateway-t, ul varësitë e papritura, verifiko ARP/ND, DHCP options dhe firewall. Kriteri i suksesit është aplikacioni i përdoruesit, jo vetëm interface up.

Laborator: Kërkesat, dokumentimi, ndryshimet dhe rikuperimi

Koha: 180 minuta. **Mjedisi:** dokumentacioni dhe topologjitë e kursit.

- Shkruaj kërkesa për një organizatë me 120 përdorues, dy site dhe një shërbim publik. Ndaj kërkesat e detyrueshme nga preferencat.
- Krijo HLD me dy alternativa dhe shpjego kompromiset për kosto, kompleksitet, disponueshmëri dhe rritje.
- Për alternativën e zgjedhur krijo LLD me adresim, VLAN/VRF, routing, DNS/DHCP, siguri dhe OOB.
- Defekti i procesit: rollback kërkon akses që humbet nga vetë ndryshimi. Riprojekto planin dhe testo rrugën e rikthimit.

- Hartoni procedurë backup/restore dhe një ushtrim rikuperimi me matje kohe. Dokumento çfarë nuk ruhet nga backup-i i konfigurimit.
- Cakto një person tjetër që ndjek vetëm dokumentin dhe shënon çdo hap që kërkon sqarim nga autori.

Dorëzimi: HLD, LLD, plan ndryshimi dhe prova rikthimi. **Pranimi:** dokumentet përputhen; RTO është i matshëm; N−1 ka kapacitet të arsyetuar; rollback është i ekzekutueshëm. **Thellim:** planifiko ndërrimin e adresimit për bashkim kompanish me subnet-e të mbivendosura dhe periudhë bashkëjetese.

40. Projekti përfundimtar dhe mbrojtja teknike

Ndërto, prish, diagnostiko dhe mbro projektin

Teori: Ndërto, prish, diagnostiko dhe mbro projektin

Objektivi: të integrosh routing, shërbime, siguri dhe operim në një sistem me prova të verifikueshme.

Organizata e projektit ka seli me 120 përdorues, degë me 40, VLAN për staf, zë, mysafirë dhe menaxhim, një DMZ me aplikacion dhe një mjedis cloud të projektuar. Kërkohen IPv4/IPv6, routing i brendshëm, dy dalje të simuluara, DNS/DHCP, kontroll fluksesh, VPN dhe monitorim. Datacenter EVPN dhe BGP multi-provider janë zgjerime të avancuara që mund të emulohen veçmas kur burimet nuk mjaftojnë në një topologji të vetme.

Ndarja e detyrave fillon me kërkesat dhe planin e provave, jo me komandat. Çdo funksion duhet të ketë burim konfigurimi, test pozitiv, test negativ kur ka policy dhe provë pas dështimit. Për funksionet e projektuara por jo të ekzekutuara përdor etiketën “projektim”; kjo nuk jep të njëjtën kredi praktike si zbatimi. Objektivi është arsyetim teknik, jo grumbullim screenshots.

Kriteret përfshijnë adresim pa mbivendosje, segmentim që punon, routing të parashikueshëm, arritshmëri shërbimi në dy familje IP, menaxhim të kufizuar dhe rikthim pas një dështimi. Testo kufijtë: klient i paautorizuar, DNS i gabuar, prefiks i munguar, MTU e vogël dhe një uplink i ndalur. Për çdo incident ruaj simptomën, hipotezën, provën, ndryshimin dhe konfirmimin.

Prezantimi final duhet të mbrojë kompromiset: pse ky IGP, ku përfundon L2, si shmanget route leak, çfarë ndodh kur AAA ose DNS mungon, dhe si do të rritet organizata. Një zgjidhje më e thjeshtë me prova të plota vlen më shumë se fabric kompleks pa verifikim. Provimi teorik nuk zëvendëson projektin praktik.

Përgatitja: përdor `projektet.sq.md`, fletën e provave dhe rubrikën e mësuesit. Ruaj vetëm kredenciale testimi jashtë paketës së dorëzuar.

Laborator: Ndërto, prish, diagnostiko dhe mbro projektin

Koha: 1200 minuta, të shpërndara në disa seanca. **Mjedisi:** emulator/VM; pajisjet fizike janë opsionale për pjesën e radios.

- Dorëzo fillimisht HLD/LLD dhe matricën e testeve. Ndërto një segment bazë dhe provo shërbimin përpara shtimit të redundancës.
- Shto segmentim, routing, dual stack dhe shërbimet. Pastaj aktivizo sigurinë, VPN dhe monitorimin me teste pas çdo faze.
- Ekzekuto të paktën 16 teste të përcaktuara te projekti, përfshirë trafik të ndaluar dhe kthim pas dështimit. Bashkëngjit komandën, kohën dhe rezultatin e pritur/real.

- Diagnostiko katër defekte të zgjedhura nga mësuesi pa ditur paraprakisht shkakun. Ndrysho vetëm atë që mbështetet nga prova.
- Kryej backup, ndryshim të kontrolluar dhe rollback. Riprovo rrjedhat kritike pas rikthimit dhe përditëso as-built.

Dorëzimi: diagramet, konfigurimet e redaktuara, inventari, provat, raportet e incidenteve dhe prezantim 20-minutësh. **Pranimi:** të paktën 80/100; të gjitha kontrollet kritike të izolimit, filtrimit të prefikseve, menaxhimit dhe rikthimit duhet të kalojnë. **Thellim:** shto EVPN ose peering BGP me dy dalje dhe demonstro pse politika nuk rrjedh rrugë të palëve të treta. Pjesët vetëm analitike identifikohen qartë.

Projektet dhe burimet e studentit

Projekte dhe ushtrime integruese

Projekti 1 — Një LAN i dokumentuar

Pas modulit 10, ndërto dy subnet-e IPv4 dhe IPv6 me router mes tyre. Përdor laboratorin a–r–b dhe shto hostin c për bridging. Dorëzo diagramin, adresimin, tabelat e fqinjëve dhe katër prova: lokal, i largët, rrugë kthimi e munguar dhe rikthim. Pranimi kërkon shpjegim të MAC-ut të hop-it të radhës dhe longest prefix match. Koha orientuese 4–6 orë.

Projekti 2 — Një incident aplikacioni

Pas modulit 16, një HTTP testues duhet të arrihet me adresë dhe emër laboratorik. Mësuesi zgjedh një defekt nga DNS, bind address, portë e bllokuar dhe MTU. Dorëzo timeline, të paktën dy hipoteza të refuzuara dhe provën e shkakut. Nuk lejohet që “rinisa gjithçka dhe punoi” të jetë raporti përfundimtar. Koha 4–8 orë.

Projekti 3 — Routing me policy

Pas modulit 23, zbato OSPF trekëndësh dhe eBGP në topologji të veçantë ose të integruar me kufij të qartë. Kërkohen loopback-e të arritshme, preferencë rruge, filtër eksporti dhe dështim i një lidhjeje. Provo që një prefiks i palejuar nuk reklamohet. Nëse ke dy dalje, përdor LOCAL_PREF për daljen, jo ndryshime arbitrare adresimi. Koha 8–12 orë.

Projekti final — Organizata me dy site

Selia: 120 staf, 30 telefona, 25 mysafirë të njëkohshëm, 12 pajisje menaxhimi, 10 serverë. Dega: 40 staf, 10 telefona, 15 mysafirë, 6 pajisje menaxhimi. Këta numra përfaqësojnë kërkesën fillestare; rezervo të paktën 30% rritje për subnet-et e stafit. Gateway dhe infrastrukturën numëroji brenda kapacitetit sipas modelit. DMZ ka dy serverë aplikacioni. Organizata përdor një shërbim të jashtëm të simuluar dhe ka dy dalje logjike të shënuara me failure domain fizik.

Përdor hapësirën 10.60.0.0/16 për subnet-et e përdoruesve/site-ve dhe 10.255.0.0/24 për loopback-e; 2001:db8:6000::/48 për IPv6 laboratorike. Zgjidh VLAN-et, VRF-të dhe blloqet sipas arsyetimit tënd. Mos e përdor /48 e dokumentimit në prodhim. AS privatë lejohen vetëm në topologjinë e izoluar.

Kërkesat bazë të zbatimit

- IPv4 dhe IPv6 për të paktën dy segmente të rutueshme; çdo funksion tjetër që mbetet vetëm projektim identifikohet.

- VLAN staf, zë, mysafir, menaxhim dhe serverë/DMZ. Nëse përdor vetëm namespaces, deklaro që kjo provon segmentimin L3 dhe jo gjithë funksionet e një switch-i fizik.
- OSPF në brendësi dhe policy eBGP në një segment të izoluar me filtrim prefiksesh. Mund të jenë topologji të ndara me lidhje të dokumentuar të kërkesave.
- DNS dhe konfigurim adresash me DHCP në një segment të izoluar, ose shëno si projektim derisa të ekzekutohet laboratori i serverit.
- Shërbim HTTP testimi, kontroll portash dhe menaxhim vetëm nga segmenti i autorizuar.
- VPN site-to-site e ekzekutuar në dy gateway virtuale. Konfigurimet dorëzohen pa çelësa privatë.
- Monitorim i disponueshmërisë dhe së paku një alarm me runbook.
- Backup dhe rikthim të provuar me retestim të rrjedhave kritike.

Matrica minimale e pranimit

ID	Prova	Rezultati i pritur
T01	Staf→gateway IPv4	Kalon në secilin subnet të zbatuar
T02	Staf→shërbim në subnet tjetër	Kalon vetëm në portat e lejuara
T03	Staf→server IPv6	Kalon me rrugë kthimi të dokumentuar
T04	Mysafir→menaxhim	Refuzohet dhe provohet nga policy/counter
T05	Mysafir→shërbim i jashtëm i simuluar	Kalon sipas policy
T06	Host pa rol admin→SSH menaxhimi	Refuzohet
T07	DNS me A dhe AAAA	Kthen adresat që i përkasin shërbimit
T08	Marrje/rinovim DHCP	Adresa dhe opsionet përputhen me scope
T09	OSPF normal dhe humbje lidhjeje	Rrugët rikthehen brenda objektivit të projektit
T10	BGP prefiks i lejuar	Merret dhe instalohet sipas policy
T11	BGP prefiks i palejuar	Nuk eksportohet drejt peer-it
T12	VPN transferim në dy drejtimet	Kalon dhe rrit counters përkatës
T13	Paketë mbi Path MTU	Jepet mekanizmi i pritur i përshtatjes/gabimit
T14	Dështim i shërbimit	Alarmi ngrihet dhe lokalizohet nga runbook
T15	Backup/restore	Konfigurimi dhe shërbimet kritike provohen përsëri
T16	Rikthim pas defektit të futur nga mësuesi	Prova e shkakut dhe korrigjimit ruhet

Për secilin test ruaj burim/destinacion, komandë, kohë, pritshmëri, rezultat, skedar prove dhe interpretim. “Nuk u testua” nuk regjistrohet si “kaloi”. Objektivat kohore caktohen para provave dhe mbrohen teknikisht. Matjet brenda emulatorit nuk garantohen për hardware prodhimi.

Zgjerime të avancuara

Zgjidh të paktën një për specializim: EVPN me dy leaf dhe një spine; dy dalje BGP me communities dhe provë mosrrjedhjeje; cluster lokal Kubernetes me NetworkPolicy të verifikuar; Wi-Fi Enterprise me certifikata dhe matje roaming; multicast me kontroll RPF; rrjet storage me matje congestion-i. Secili kërkon diagram, konfigurim, dy teste pozitive, dy negative dhe një dështim të matur. Koha shtesë 8–16 orë sipas mjetit.

Paketa e dorëzimit

Përfshi README me versionet, HLD/LLD, konfigurimet e redaktuara, IPAM, matricën e flukseve, provat T01–T16, incidentet dhe planin e rikthimit. Lidh çdo pretendim me skedarin e provës. Përgatis prezantim 20 minuta dhe përgjigju për kompromiset. Mos dorëzo fjalëkalime, tokens ose të dhëna reale përdoruesish.

Fletë pune të studentit

Regjistri i laboratorit — kopjo për çdo modul

Moduli: ___ Data/ora/zona: ___ Versionet: ___ Praktikë apo analizë: ___

Qëllimi: ___ Pajisjet/namespace: ___ Konfigurimi fillestar: ___

Hapi	Komanda ose veprimi	Pritshmëria	Rezultati real	Skedari i provës
1				
2				
3				

Çfarë provohet: ___ Çfarë nuk provohet: ___ Rikthimi: ___ Retestimi: ___

Ushtrime llogaritjeje

1. Gjej rrjetin, broadcast dhe intervalin e hosteve për 10.8.5.201/27, 172.20.37.99/20 dhe 192.168.50.77/26. Trego AND-in binar të të paktën njërit.

2. Ndaj 10.40.0.0/24 për 100, 50 dhe 20 hoste. Numëro gateway-n brenda kërkesës dhe shëno rezervën.

3. Ndaj 2001:db8:1200::/48 në /56 për degët A dhe B dhe jep dy /64 për secilën.

4. Llogarit kohën ideale për 2 GB dhjetorë në 100 Mbit/s, 1 Gbit/s dhe 10 Gbit/s.

5. Llogarit BDP për 500 Mbit/s dhe RTT 80 ms; sa throughput ideal lejon dritarja 2 MB dhjetorë?

6. Paketë IPv4 pa opsione me ICMP payload 1472 kalon MTU 1500. Sa payload lejohet në MTU 1400? Bëj llogaritje të ndarë për IPv6 pa extensions.

7. Një transmetues -2 dBm kalon 5 dB humbje drejt marrësit me ndjeshmëri -12 dBm. Llogarit fuqinë dhe marzhin pa rezervë shtesë.

8. Counter bytes është 1 000 000, pastaj pas 10 s është 3 500 000. Gjej bit/s. Si ndryshon llogaritja kur pajisja riniset?

9. Një host ka /0→R1, 10.0.0.0/8→R2, 10.20.0.0/16→R3 dhe 10.20.30.0/24→R4. Zgjidh daljen për 8.8.8.8, 10.9.1.1, 10.20.40.1 dhe 10.20.30.9.

10. Llogarit sesionet iBGP full mesh për 4, 8 dhe 20 router-a dhe argumento kur kërkohet route reflection.

Regjistri i incidentit

Ndikimi dhe shtrirja: ___ Kur filloi dhe çfarë ndryshoi: ___

Hipoteza H1 dhe prova që do ta refuzonte: ___

Hipoteza H2 dhe prova që do ta refuzonte: ___

Pika e kapjes, ora dhe kufizimet: ___

Shkaku i mbështetur nga prova: ___ Korrigjimi minimal: ___

Rollback dhe rezultat: ___ Retestimi i aplikacionit: ___

Parandalimi, pronari dhe afati: ___

Matrica e flukseve

Burimi/roli	Destinacioni	Protokolli/porta	Drejtimi	Lejo/refuzo	Arsyeja	Prova

Vetëkontroll para dorëzimit

- Mund ta shpjegoj çdo fushë dhe nuk kam dorëzuar vetëm output.
- Diagrami përputhet me konfigurimin dhe provat.
- Kam testuar kthimin, jo vetëm vajtjen.
- Kam rikthyer MTU, route dhe firewall të ndryshuar në laborator.
- Kam shënuar qartë çfarë është analizë dhe çfarë është ekzekutim.
- Nuk ka secrets ose të dhëna reale në skedarët e ndarë.

Fjalor teknik shqip

Termat ruhen edhe në formën e tyre të zakonshme që të mund të lexosh CLI dhe dokumentacionin.

Termi	Kuptimi në këtë kurs
ACK	Konfirmim; në TCP tregon byte-n e ardhshëm të pritur
ACL	Listë rregullash filtrimi me rend dhe drejtim
Address family	Familje adresimi/shërbimi e negociuar, p.sh. IPv4 unicast ose EVPN

Anycast	E njëjta adresë në disa instanca, me zgjedhje sipas routing-ut
ARP	Zgjidhje IPv4→adresë lokale lidhjeje
AS/ASN	Domen routing-u dhe identifikuesi i sistemit autonom
ASIC	Qark i specializuar për funksione si forwarding
BDP	Produkti bandwidth × RTT, vëllim potencial në fluturim
BFD	Mekanizëm zbulimi të dështimit të komunikimit
BGP	Protokoll routing-u me policy mes dhe brenda AS-ve
Blackhole	Trafik i hedhur ose pa rrugë të vlefshme drejt shërbimit
BPDU	Mesazh i kontrollit spanning tree
Broadcast	Trafik për të gjithë domenin përkatës lokal
BUM	Broadcast, unknown unicast dhe multicast
CIDR	Prefikse pa kufizim në klasat historike A/B/C
CNI	Ndërfaqe dhe implementime për lidhjen e containers me rrjetin
Congestion	Kërkesë që tejkalon burimin e disponueshëm në një pikë
CoPP	Politikë për mbrojtjen e planit të kontrollit
CRC/FCS	Kontroll gabimi i frame-it; nuk është autentikim
DAD	Kontroll IPv6 për adresë të dyfishuar
dB/dBm	Raport logaritmik/fuqi absolute kundrejt 1 mW
Default route	Rrugë /0 për destinacione pa përputhje më specifike
DHCP	Shpërndarje parametrash konfigurimi me lease sipas versionit
DNS	Sistem hierarkik emrash dhe rekordesh
DNSSEC	Verifikim i të dhënave DNS të nënshkruara
DSCP	Fushë IP për klasifikim trajtimi QoS
EAP	Kornizë metodash autentikimi, përdorur me 802.1X
ECMP	Përcjellje me disa rrugë me kosto të barabartë
ECN	Sinjalizim eksplicit congestion-i
Encapsulation	Mbështjellje e të dhënave me headers të një protokolli tjetër
EVPN	Familje shërbimesh VPN Ethernet/IP me kontroll MP-BGP
Failure domain	Bashkësi komponentësh që mund të dështojnë nga i njëjti shkak
FIB	Tabelë/gjendje për vendimet e forwarding-ut
Flow	Rrjedhë komunikimi e identifikuar sipas kontekstit dhe fushave
Flooding	Dërgim në disa porta brenda domenit të lejuar
Gateway	Hop/router për të dalë nga lidhja/subnet-i sipas routing-ut
Goodput	Norma e të dhënave të dobishme të aplikacionit

HLD/LLD	Projekt arkitekturor/projekt i hollësishëm zbatimi
ICMP	Mesazhe kontrolli, gabimi dhe diagnostikimi për IP
Idempotence	Përsëritje drejt së njëjtës gjendje pa ndryshime të panevojshme
IGP	Protokoll routing-u brenda domenit administrativ
IGMP/MLD	Sinjalizim anëtarësie multicast IPv4/IPv6
IPAM	Menaxhim dhe dokumentim i adresave/prefikseve
IRB	Integrim bridging/routing sipas arkitekturës
Jitter	Variacion i vonesës, me përkufizim sipas matjes
LACP/LAG	Negocim agregimi/grup lidhjesh Ethernet
Latency	Kohë nga një pikë/ngjarje te një tjetër e përcaktuar
Lease	Marrëveshje me afat për përdorimin e konfigurimit DHCP
LOCAL_PREF	Atribut preference brenda AS për policy BGP
Longest prefix match	Zgjedhje e prefiksit të përputhshëm më specifik
LSDB/LSA	Databazë link-state/njoftim i saj në OSPF
MAC	Adresë lidhjeje e përdorur në Ethernet dhe kontekste të tjera
Microburst	Kulm i shkurtër trafiku që mund të mbushë buffer
MPLS	Forwarding me labels sipas kontekstit të shpërndarjes
MSS	Kufiri i payload-it TCP i negociuar sipas mekanizmit
MTU/PMTU	Kufiri i paketës në lidhje/minimumi në rrugë
NAC	Kontroll i aksesit të pajisjeve/përdoruesve në rrjet
NAT/PAT	Përkthim adresash/përkthim edhe sipas portave
NDP	Zbulim fqinjësh dhe funksione të tjera kontrolli në IPv6
NETCONF/YANG	Protokoll menaxhimi i strukturuar/gjuhë modelimi të dhënash
Next hop	Hapi i radhës në vendimin e routing-ut
NTP/PTP	Protokolle sinkronizimi kohe me modele dhe saktësi të ndryshme
OOB	Menaxhim jashtë rrugës normale të të dhënave
OSPF/IS-IS	Protokolle IGP link-state me hierarki përkatëse
Overlay/underlay	Rrjet logjik sipër/transport bazë poshtë tij
PCAP	Format kapjeje paketash dhe familje skedarësh për analizë
PFC	Kontroll rrjedhe sipas prioritetit në Ethernet
PIM/RPF	Protokoll ndërtimi pemësh multicast/kontroll i rrugës drejt burimit
PKI	Infrastrukturë çelësash publikë, certifikatash dhe besimi
Policing/shaping	Kontroll profili me hedhje/rishënim ose pritje në radhë
Prefix	Pjesa udhëzuese e adresës dhe gjatësia e saj

QoS	Trajtim trafiku sipas klasave dhe burimeve
QUIC	Transport me siguri dhe streams mbi UDP
RA/RS	Njoftim/kërkim router-i në IPv6
RD/RT	Dallues unik rrugësh VPN/kontroll import-eksporti
RIB	Informacion routing-u në planin e kontrollit
ROA/ROV	Autorizim origjine prefiksi/verifikim origjine
Rollback	Rikthim i kontrolluar pas ndryshimit
RPKI	Infrastrukturë çelësash publikë për burime numrash Interneti
RSSI/SNR	Fuqi e marrë/raport sinjal-zhurmë sipas instrumentit
RTT	Koha vajtje-kthim e matur sipas provës
RTO/RPO	Objektiv kohe rikuperimi/objektiv humbjeje të dhënash
SACK	Raportim TCP i intervaleve të marra jashtë rendit
SLAAC	Autokonfigurim IPv6 pa server adresash stateful
SLI/SLO/SLA	Matje/objektiv/marrëveshje e nivelit të shërbimit
Socket	Pikë komunikimi e sistemit dhe aplikacionit
SPAN/TAP	Mekanizma kopjimi ose vrojtimi trafiku për kapje
SR-MPLS/SRv6	Segment Routing mbi MPLS ose IPv6
SSID	Identifikues rrjeti wireless, jo garanci sigurie
STP/RSTP/MSTP	Familje mekanizmash për topologji L2 pa loop
TCP/UDP	Transport rrjedhe byte-sh/datagramesh me funksione të ndryshme
Telemetry	Të dhëna operative të mbledhura nga sistemi
Throughput	Normë transferimi sipas pikës dhe metodës së matjes
TLS	Mbrojtje komunikimi me autentikim dhe çelësa kriptografikë
Trunk/access	Role portash për shumë VLAN-e ose lidhje fundore sipas platformës
TTL/hop limit	Kufizim hop-esh IP; DNS TTL ka kuptim tjetër, cache
VLAN/VNI	Identifikues segmenti Ethernet/segmenti VXLAN
VRF	Kontekst i ndarë routing-u
VRRP	Protokoll redundance për gateway virtual
VTEP	Pikë encapsulation/decapsulation VXLAN
VXLAN	Encapsulation Ethernet mbi UDP/IP
Zero trust	Model besimi dhe kontrolli me verifikim sipas kontekstit, jo një protokoll i vetëm

Harta e mbulimit dhe specializimi

Zbatim praktik i gatshëm do të thotë që kursi jep skedarë dhe hapa për mjedisin përkatës, jo që është provuar në çdo sistem. **Laborator i drejtuar** kërkon mjetin/pajisjen dhe konfigurim sipas versionit. **Projektim** zhvillon analizën dhe nuk certifikon aftësi operimi hardware.

Modulet	Fusha	Niveli dhe forma
1–2	OSI/TCP-IP, encapsulation, plane, performancë	Themele me llogaritje dhe matje
3	Kabllo, optikë, transceivers, PoE	Projektim dhe laborator me pajisje
4–6	Ethernet, VLAN, QinQ, STP, LACP, MLAG	Bazë deri i avancuar; bridge gati, switch për pjesën tjetër
7–10	IPv4/IPv6, VLSM, SLAAC, NDP, VRF, routing	Ushtrime dhe laborator Linux i gatshëm
11–12	ICMP, PMTUD, MSS, TCP, UDP, QUIC	Laborator dhe analizë transporti
13–15	DNS/DNSSEC, DHCP/IPAM/NTP, HTTP/TLS/proxy	Laborator i drejtuar dhe diagnostikim
16	Wireshark, tcpdump, SPAN, offloads	Analizë me laboratorin bazë
17–20	OSPF, IS-IS, RIP/EIGRP, BGP/RPKI	FRR OSPF/eBGP gati; IS-IS model zgjerimi; policy e avancuar
21–23	VRRP/BFD, multicast, QoS	Laborator i drejtuar dhe prova dështimi
24–25	RF, Wi-Fi, Enterprise, roaming	Kërkon AP/klientë; variant projektimi
26–28	Firewall/NAT, AAA/NAC, VPN	nftables gati; AAA/VPN laborator i drejtuar
29–30	WAN, SD-WAN, MPLS, Segment Routing	Laborator me imazh të përshtatshëm ose projektim
31	EVPN/VXLAN, IRB, multihoming	Laborator fabric me referencë zyrtare
32	Cloud dhe hybrid	Projektim pa blerje; zbatim opsional
33–34	Linux/Windows, containers/Kubernetes	Linux gati; Windows/cluster sipas mjedisit
35–36	Automatizim, telemetri, incidente	Validator lokal dhe prova operacionale
37–38	Storage, RDMA, OT, PTP, operator, radio/celular	Hyrje teknike dhe projekt specializimi
39–40	HLD/LLD, migrim, recovery, projekt	Integrim i avancuar dhe mbrojtje

Thellimi pas kursit

Për drejtimin **enterprise** zgjero campus switching, dizajn RF, NAC/PKI, akses dhe menaxhim. Për **datacenter** zgjero EVPN multihoming, DCI, storage/RDMA dhe matje në ASIC. Për **ISP** zgjero BGP policy në shkallë, RPKI/IRR, MPLS/SR, peering dhe operim optik. Për **cloud/platform** zgjero CNI/eBPF, hybrid DNS, multi-cluster dhe observability. Për **OT** kërko praktikë me protokollet/profilin industrial dhe ekipin e sigurisë funksionale.

Tema si dizajni elektronik i radios, matematika e kodeve korrigjuese, implementimi i kernel-it TCP, çdo komandë prodhuesi, certifikimi i kabllimit, siguria funksionale OT dhe çdo profil 3GPP nuk trajtohen si specializime të plota këtu. Ato kërkojnë kurse dhe pajisje të veçanta. Ky kufi e bën të qartë çfarë provojnë materialet, jo më pak të nevojshme bazat e përbashkëta.

Burime zyrtare për lexim dhe verifikim

Lista u përgatit më 16 nëntor 2026. RFC-të janë bazë protokollesh; kontrollo statusin, errata dhe RFC-të që i përditësojnë. Dokumentacioni `latest` ndryshon: për laborator përdor versionin që ke instaluar. Teksti i kursit është shpjegim origjinal në shqip; burimet nuk janë riprodhuar si kapituj të përkthyer.

Protokollet

- Modulet 7–11: IPv6, RFC 8200 — https://www.rfc-editor.org/info/rfc8200/
- Modulet 2 dhe 12: TCP, RFC 9293 — https://www.rfc-editor.org/info/rfc9293/
- Modulet 12 dhe 15: QUIC, RFC 9000 — https://www.rfc-editor.org/info/rfc9000/
- Moduli 15: HTTP Semantics, RFC 9110 — https://www.rfc-editor.org/info/rfc9110/
- Moduli 15: TLS 1.3, RFC 8446 — https://www.rfc-editor.org/info/rfc8446/
- Moduli 17: OSPFv2, RFC 2328 — https://www.rfc-editor.org/info/rfc2328/
- Modulet 19–20: BGP-4, RFC 4271 — https://www.rfc-editor.org/info/rfc4271/
- Moduli 20: BGP Prefix Origin Validation, RFC 6811 — https://www.rfc-editor.org/info/rfc6811/
- Moduli 30: BGP/MPLS IP VPN, RFC 4364 — https://www.rfc-editor.org/info/rfc4364/
- Moduli 31: VXLAN, RFC 7348 — https://www.rfc-editor.org/info/rfc7348/
- Moduli 31: EVPN, RFC 7432 — https://www.rfc-editor.org/info/rfc7432/

Mjetet dhe konfigurimet

- Modulet 11, 33: Linux IP sysctl — https://docs.kernel.org/networking/ip-sysctl.html
- Modulet 12 dhe 16: Wireshark User’s Guide — https://www.wireshark.org/docs/wsug_html_chunked/
- Moduli 17: FRRouting OSPF — https://docs.frrouting.org/en/latest/ospfd.html
- Moduli 18: FRRouting IS-IS — https://docs.frrouting.org/en/latest/isisd.html
- Modulet 19–20: FRRouting BGP — https://docs.frrouting.org/en/latest/bgp.html
- Moduli 31: FRRouting EVPN, topologji dhe konfigurim i plotë reference — https://docs.frrouting.org/en/latest/evpn.html
- Moduli 28: WireGuard Quick Start — https://www.wireguard.com/quickstart/
- Moduli 34: Kubernetes Network Policies — https://kubernetes.io/docs/concepts/services-networking/network-policies/

Si punohet me referencën

Për çdo laborator të avancuar shëno versionin, faqen/seksionin dhe komandën që po verifikon. Lexo parakushtet, sjelljen default dhe kufizimet para kopjimit të konfigurimit. Një shembull EVPN për një tip IRB nuk kombinohet pa analizë me shembull tjetër që përdor model të ndryshëm. Një komandë që pranohet në CLI ende ka nevojë për provë funksionale.

Për wireless, optikë, cloud dhe switching tregtar shto datasheet/dokumentacionin e pajisjes konkrete. Kanale radio, fuqi të lejuara, çmime cloud, licenca dhe specifika hardware kontrollohen në momentin e zbatimit; ky kurs nuk jep një tabelë universale që mbetet e vlefshme kudo. Për standarde IEEE dhe profile industriale përdor dokumentin/profilin e zbatueshëm dhe ekipin përgjegjës të instalimit.