Köszöntünk a CCNA Bevezetés a hálózatok világába kurzuson! Ennek a tanfolyamnak a célja, hogy megismerkedjünk az alapvető hálózati fogalmakkal és technológiákkal. Ezek az online oktatási anyagok segítenek azoknak a készségeknek a kialakításában, amelyek egy kisvállalati LAN és WAN hálózat tervezéséhez és megvalósításához szükségesek. Az egyes fejezetekben található konkrét készségek a fejezet elején lesznek felsorolva.

A tananyag eléréséhez, az oktatóval történő kapcsolattartáshoz, az eredmények megtekintéséhez és az interaktív gyakorlati feladatok elvégzéséhez használható okostelefon, tablet vagy bármilyen más számítógép is. Némelyik anyag azonban összetettebb, és megköveteli számítógépen való megjelenítést, mint például a Packet Tracer feladatok, a tesztek és a vizsgák.

Amikor valaki a Hálózati Akadémia tagja lesz, akkor egyúttal csatlakozik egy globális közösséghez is, melyet a közös célok és technológiák kötnek össze. Világszerte 160 országban vesznek részt a programban különböző középiskolák, főiskolák, egyetemek és egyéb oktatási intézmények. A Cisco Hálózati Akadémia globális közösségének interaktív térképe a http://www.academynetspace.com címen érhető el.

További információk érhetők el a Cisco Hálózati Akadémia hivatalos Facebook© és LinkedIn© oldalain. A Facebook oldal az a hely, ahol a világ minden pontjáról az akadémiai diákok megismerkedhetnek és közös élményeket oszthatnak meg egymással. A Cisco Hálózati Akadémia LinkedIn oldalán álláshirdetésekkel találkozhatunk, valamint megtapasztalhatjuk, hogy mások hogyan kommunikálják hatékonyan a karrierépítéshez szükséges képességeiket.

A NetSpace tanulási környezet fontos részét képezi a teljes kurzusnak a Hálózati Akadémiai diákok és a oktatók számára egyaránt. Ezek az online oktatási anyagok tartalmazzák a kurzus szöveges részeit, a hozzájuk kapcsolódó interaktív médiatartalmakat, a szimulációs Packet Tracer feladatokat, a fizikai és távoli elérésű laborgyakorlatokat és számos különböző tesztfeladatot. Minden ilyen anyag fontos visszajelzést biztosít a tanfolyamban történő előrehaladásról.

A tananyag olyan technológiákról szól, amelyek megkönnyítik az emberek munkáját, hétköznapjait, szórakozását és tanulását az adat-, hang- és videókommunikáción keresztül. A hálózatok és az Internet különböző mértékben befolyásolják az embereket a világ különböző pontjain. A tananyag létrehozásában a világ legkülönbözőbb részein dolgozó oktatók vettek részt. Lényeges, hogy az akadémiai oktatók és hallgatók együttműködve alakítsák ki a helyi adottságoknak leginkább megfelelő tananyagot.

Az új képességek elsajátítása általában sok gyakorlást igényel. Ezt olyannyira fontosnak tartjuk az e-tanulás folyamatában is, hogy saját nevet is adtunk neki: e-gyakorlás. A tananyag több olyan beágyazott, interaktív, gyakorlat-orientált feladatot is tartalmaz, amely ösztönzi a hatékonyabb tanulást, növeli a tudás beágyazódását, és gazdagítja az egész tanulási élményt - megkönnyítve ezáltal a tananyag megértését is. Egy normál tanórán egy új anyag feldolgozása után annak megértése néhány interaktív feladat segítségével azonnal ellenőrizhető. Ha a diákok új utasításokat tanulnak, akkor azokat a Szintaktika Ellenőrzőben azon nyomban ki is lehet próbálni, még mielőtt alkalmazásra kerülnének egy-egy feladatban vagy a Packet Tracer-ben, a Hálózati Akadémia szimulációs alkalmazásában. Ezek után következhetnek azok a feladatok, amelyeket valós eszközökön hajthatunk végre az osztályteremben, vagy esetleg távolról elérve az interneten keresztül.

A Packet Tracer lehetőséget biztosít arra, hogy bármikor gyakorolhassunk saját magunk által létrehozott feladatok segítségével, vagy hogy többfelhasználós játékokban versenyezve összemérjük tudásunkat osztálytársainkkal. A Packet Tracer készségfelmérő és készségfejlesztő laborgyakorlatai által mindenki részletes visszajelzésben részesülhet az aktuális tudásáról, valamint kitűnő gyakorlási lehetőség az egyes fejezetvégi ellenőrző- és záróvizsgákhoz.

Az egyik legfontosabb oktatási cél a hallgatók tudásának gyarapítása. Fontos azonban leszögezni, hogy a tananyag és az oktató csupán elősegítheti ezt a folyamatot. Az egyénnek is mindig hozzá kell tennie saját erőfeszítését a tanulási folyamathoz. A következő oldalakon néhány javaslat kerül megvitatásra, hogy hogyan lehet a megszerzett készségeket munkaerőpiaci tudássá alakítani. Hálózati szakemberek gyakran tanulmányoznak olyan műszaki folyóiratokat, amelyekben protokollok vagy egy-egy speciális utasítás működését mutatják be. Egy műszaki folyóirat egyben referenciaként

is használható, amelyet egy IT munkakörben fel tudunk használni. Az írás az egyik módja annak, hogy erősítsük a tanulást - az olvasással, tanulmányozással és gyakorlással egyetemben.

Egy megvalósított technológiáról szóló esettanulmány tartalmazhatja a szükséges szoftveres parancsokat, a parancsok célját, a különböző szintaktikai változókat és azt a topológia diagramot, amelyek a technológia és a beállított utasítások sajátosságait mutatják be.

A Packet Tracer a legkülönbözőbb fizikai és logikai szimulációk megvalósítására alkalmas. Egyben egy vizualizációs eszköz is, amely segít megérteni egy hálózat belső működését.

A kurzus részét képezik olyan, a Packet Tracer-hez kidolgozott szimulációk, játékok, feladatok és kihívást jelentő gyakorlatok is, melyek nagyban fokozzák a tanulás élményét. Ezek az eszközök segítenek annak megértésében, hogy egy hálózatban hogyan is történik az adattovábbítás.

A Packet Tracer segítségével saját hálózati környezetünkben hajthatunk végre szimulációs kísérleteket. Reméljük, hogy idővel többen is kedvet kapnak - a beépített feladatok kipróbálásán túl - saját szerzői, felfedezői és kísérletező kedvük kiélésére is.

Amennyiben a Packet Tracer telepítve van, a kurzushoz kidolgozott Packet Tracer feladatok a Windows operációs rendszert futtató számítógépeken automatikusan elindulnak. Ez más operációs rendszereken Windows emuláció alatt is működik.

Oktatási játékok

A Packet Tracer többfelhasználós játéka lehetővé teszi, hogy egy diák vagy egy csapat összemérhesse tudását másokkal egy hálózat minél pontosabb és gyorsabb kiépítésében. Ez egy kiváló módja annak, hogy tovább lehessen gyakorolni azokat a készségeket, amelyeket egy diák a Packet Tracer és a valódi laborgyakorlatok során már elsajátított.

A Cisco Aspire egy egyfelhasználós, önálló stratégiai szimulációs játék. A játékosok egy virtuális városban tesztelhetik hálózati ismereteiket egy-egy projekt megvalósításával. A Hálózati Akadémiai változatának kifejezett célja, hogy segítsen felkészülni a CCENT minősítés megszerzésére. Egyben megmutatja, hogy mik lehetnek azok az üzleti és kommunikációs készségek, amelyeket az IT munkaadók keresnek az álláskeresőknél.

Teljesítmény-alapú értékelések

A Hálózati Akadémia teljesítményértékelése hasonlít azokhoz a Packet Tracer feladatokhoz, amelyeket a diákok már előzetesen is megismertek, viszont ez a megoldás rendelkezik egy online értékelési motorral, amely automatikusan kiértékeli az eredményeket és azonnali visszajelzést is szolgáltat. Ezekből a visszajelzésekből kiderül, hol vannak az erős és a gyenge pontjaink. A fejezetek végén kérdések, tesztek, valamint Packet Tracer-t alkalmazó vizsgák találhatók, amelyek további visszajelzést szolgáltatnak.

Ahogy a kurzus címe is mutatja, a hangsúly a hálózati alapismeretek elsajátításán van. Ebben a kurzusban a hálózati alapok megértéséhez szükséges gyakorlati és elméleti ismeretek tanulhatjuk meg. A következő témaköröket tartalmazza:

- az emberi és hálózati kommunikáció összevetése és hasonlóságok kimutatása,
- a két alapvető, a hálózatok tervezését és megvalósítását leíró modell megismerése: OSI és TCP/IP,
- a hálózatok "réteges" megközelítésének megértése,
- az OSI és a TCP/IP modell rétegek funkcióinak és szolgáltatásainak a vizsgálata,

- a különböző hálózati eszközök és a hálózati címzési rendszer megismerése,
- az adatok továbbításához használható különböző átviteli közegek megismerése.

A kurzus végére képesek leszünk egy egyszerű LAN hálózat kiépítésére, a forgalomirányítók (router-ek) és kapcsolók (switch-ek) alapvető beállítására és az IP-címzési rendszer kialakítására.

Napjainkban kritikus fordulópont előtt állunk a technológiai fejlődésben, ami által kommunikációs szokásaink és lehetőségeink ki fognak bővülni. Az internet elterjedése gyorsabban bekövetkezett, mint ahogy azt bárki képzelhette volna. Társadalmi, kereskedelmi, politikai és személyes kapcsolattartási szokásaink gyorsan változnak, hogy lépést tudjanak tartani a globális hálózat fejlődésével. A fejlődés következő szakaszában a feltalálók kifejezetten ezekre a fejlett hálózati képességekre alapozva fogják kifejleszteni új termékeiket és szolgáltatásaikat. Ahogy a fejlesztők a lehetőségek határait feszegetik, úgy játszanak egyre fontosabb szerepet ezen projektek sikerében az internetet alkotó összekapcsolt hálózatok.

Ez a fejezet bemutatja az adatátviteli hálózatok azon területét, amelyektől társadalmi és üzleti kapcsolataink egyre inkább függenek. A tananyag alapismereteket fog szolgáltatni a különböző szolgáltatásokról és technológiákról, valamint arról is, hogy a hálózati szakembereknek milyen felmerülő problémákkal kell szembenézniük egy modern hálózat tervezése, kialakítása és üzemeltetése során.

Üdvözlünk a Hálózati Akadémiai tananyagok legújabb elemében, a modellezési feladatban! Ezek a feladatok valamennyi fejezet elején és a végén megtalálhatók lesznek.

Némelyik feladatot egyedül is el lehet végezni (otthon vagy az osztályban), de némelyik csoportos vagy közösségi tanulási együttműködést igényel. A kurzus oktatója is segíteni fog becsatlakozni ezekbe az új típusú feladatokba.

Ezek a feladatok vizuális formában segítik majd jobban megérteni azokat az elvont fogalmakat, amelyeket a kurzus során tanulni fogunk. Legyünk kreatívak, és élvezzük ezeket a feladatokat!

Itt az első modellező feladat:

Rajzoljuk le az internetet!

Rajzoljuk le és lássuk el magyarázó szöveggel az internet térképét, ahogy azt jelenleg elképzeljük! Tartalmazza az otthonunk vagy iskolánk/egyetemünk elhelyezkedését és a hozzá tartozó kábelezést, berendezéseket, eszközöket stb. Néhány dolog, amit érdemes bejelölni:

- Eszközök / berendezések
- Média (kábelezés)
- Hivatkozási címek és nevek
- Forrás- és célállomások
- Internetszolgáltatók (ISP)

A feladat befejezése után nyomtassuk is ki a végeredményt, mert a fejezet végén szükségünk lesz még rá. Ha pedig ez egy elektronikus dokumentum, mentsük el az oktató által biztosított szerverre. Álljunk készen az osztályon belül megosztani és elmagyarázni a munkánkat!

Kezdésként néhány példát találhatunk a következő címen: http://www.kk.org/internet-mapping/.

Csoportos feladat - Magyarázat a "Rajzoljuk le az internetet" feladathoz

Az emberi létezés összes szükséglete között a kapcsolattartás igénye közvetlenül az életben maradás ösztöne után sorolható. A kommunikáció majdnem olyan fontos számunkra, mint a levegő, a víz, az élelmiszer és a menedék igénye.

Kommunikációnk formái folyamatosan változnak és fejlődnek. Egykor csak a szemtől-szembe történő kapcsolattartás volt lehetséges, mára a fontos technológiai áttörések jelentősen kiterjesztették a kommunikációnk határait. A barlangrajzoktól a nyomtatásig, majd onnan a rádióig és a televízióig, mindegyik új fejlesztés egyre növelte és fejlesztette a másokkal történő kapcsolatteremtést és a kommunikációt.

A megbízható adathálózatok létrejötte és egymással történő összekapcsolódása nagy hatással volt a kommunikációra, és ezek a hálózatok egyben a modern kommunikáció új felületévé is váltak.

A mai világban hálózatoknak köszönhetően sose látott mértékben állunk összeköttetésben egymással. Ötleteinket azonnal megoszthatjuk másokkal, hogy azok valósággá válhassanak. Hírek, események, felfedezések másodpercek alatt terjednek világszerte. Bárki közvetlen kapcsolatban állhat és játszhat egy barátjával, akitől amúgy óceánok és kontinensek választják el.

A hálózatok összekötik az embereket és elősegítik a határok nélküli kommunikációt. Mindenki csatlakozhat, megoszthat, hatással lehet a másikra.

Képzeljük el a világot internet nélkül! Nincs többé Google, YouTube, azonnali üzenetküldés, Facebook, Wikipedia, online játékok, Netflix, iTunes és a legfrissebb információkhoz történő könnyű hozzáférés. Nincsenek többé ár-összehasonlító honlapok, nélkülözni kell az online vásárlást, és már nem lehet telefonszámokat, vagy egy térképen különböző útvonalakat megkeresni néhány kattintás segítségével. Mennyivel lenne más az életünk mindezek nélkül? Pedig 15-20 éve még ebben a világban éltünk. Az évek során azonban az adatátviteli hálózatok lassan bővültek, és átalakították a mindennapjainkat, életünk minőségét.

Napjainkban az internet a következőkre ad lehetőséget:

- Fényképeket,otthoni videókat és élményeket oszthatunk meg barátainkkal vagy akár az egész világgal.
- Hozzáférhetünk bárhonnan az iskolai feladatokhoz.
- E-mail, azonnali üzenetküldés vagy internetes telefonhívások segítségével kommunikálhatunk barátokkal, családtagokkal vagy a társainkkal.
- Kedvünk szerint nézhetünk videókat, filmeket vagy televíziós sorozatokat.
- Online játékokat játszhatunk a barátokkal.
- Az online időjárás-jelentés alapján dönthetjük el, hogyan is öltözzünk fel.
- Webkamerák által ellenőrizhetjük a célunkhoz vezető út zsúfoltságát vagy az időjárási viszonyokat.
- Ellenőrizhetjük banki egyenlegünket és intézhetjük elektronikusan is számláink befizetését.

Újító szándékú emberek napról-napra az internet új használati módjait fejlesztik ki. Ahogy a fejlesztők a lehetőségek határait feszegetik, úgy bővülnek egyre jobban az internet képességei, egyben az

életünkre gyakorolt hatásai is. Tekintsük át, milyen változások történtek az elmúlt 25 évben, ahogyan ezt az ábra is mutatja! Most képzeljük el, milyen változások lesznek még az elkövetkező 25 évben! Ez a jövő elhozza a „Minden a hálón” (IoE - Internet of Everything) időszakát.

Az IoE olyan mértékben fogja összekapcsolni az embereket, a különböző folyamatokat, az információt és a berendezéseket, hogy a hálózatok még fontosabbá és értékesebbé fognak válni. Az információ olyan előnyökké alakul át, amelyek új képességeket, gazdagabb tapasztalatokat és példa nélküli gazdasági lehetőségeket biztosítanak az egyének, a vállalkozások, de akár egész országok számára is.

Gondoljuk végig, mi mindent leszünk még képesek megvalósítani a hálózat - mint egy átfogó platform - használata révén?

A hálózati technológiák különböző fejlesztései talán a világunk legjelentősebb változásainak az előfutárai. Olyan új világot fognak létrehozni, ahol a nemzeti határok, a földrajzi távolságok és a fizikai korlátok kevésbé lesznek relevánsak és a jelenleginél is kisebb akadályt fognak majd jelenteni.

Az internet már megváltoztatta a társadalmi, kereskedelmi, politikai és a személyes kapcsolattartásunk formáit. Az interneten történő közvetlen kommunikáció ösztönzi a globális közösségek kialakulását. A globális közösségek lehetővé tesznek olyanfajta közösségi együttműködést, amely független a helyszínektől vagy az időzónáktól. Az online közösségek létrejötte és az információ szabad áramlása világszerte magában hordozza a termelékenység növekedését.

A Cisco ezt a jelenséget a humán hálózatnak nevezi. A humán hálózat központjában az internet hatásai, valamint az emberek és az üzleti folyamatok hálózata áll.

Hogyan hat ránk a humán hálózat?

A hálózati világ és az internet mindent megváltoztat: amit csinálunk, ahogy tanulunk, ahogy kommunikálunk, ahogy dolgozunk, de még azt is, ahogy játszunk.

Tanulási módszereink változása

A kommunikáció, az együttműködés és az elkötelezettség alapvető építőkövei az oktatásnak. Az intézmények folyamatosan arra törekednek, hogy fejlesszék ezeket a folyamatokat, ezáltal maximalizálják a tudás átadását. A hagyományos tanulási módszerek a megszerezhető tudást elsősorban két forrás felhasználásával biztosítják, ezek a tankönyv és az oktató. Ebből a két forrásból származó tudás korlátozott, mind formájában, mind egy-egy előadás időbeli terjedelmében.

A hálózatok megváltoztatják tanulásunk folyamatát. Robusztus és megbízható hálózatok támogatják és gazdagítják a diákok tanulási élményeit. Számtalan formában biztosítanak oktatási anyagokat, ilyenek például az interaktív feladatok, a felmérések és a visszajelzések. Amint az 1. ábrán látható, a jelenben a hálózatok:

- támogatják a virtuális tantermek létrehozását,
- digitális videótárakat biztosítanak,
- lehetővé tesznek együttműködést biztosító tanulási portálokat,
- lehetővé teszik a mobil tanulást.

A magas színvonalú oktatási anyagokhoz történő hozzáférés többé már nem korlátozódik azokra a diákokra, akik épp közel tartózkodnak az anyag kibocsátásának helyszínéhez. Az online távoktatás megszüntette a földrajzi akadályokat és megnövelte a tanulók lehetőségeit. Az online (e-learning) tanfolyamok bárhonnan elérhetőek a hálózaton keresztül. Ezek a tanfolyamok a hallgatók számára bármikor és bárhonnan hozzáférhető adatokat (szöveg és linkek), hang-, és videó állományokat

tartalmazhatnak. Az online vitafórumok és üzenőfalak lehetővé teszik, hogy a diák együttműködhessen az oktatójával, más diáktársával az osztályban, mindezt akár világszerte is. A vegyes (blended) tanfolyamok vegyítik a hagyományos osztálytermi oktatást az online oktatási anyagok használatával, biztosítva ezáltal mindkét oktatási forma legjobb vonásait. A 2. ábrán egy videót láthatunk a kibővült tanterem fogalmáról.

A hallgatóknak biztosított előnyök mellett a hálózatok javították a kurzusok menedzselését és adminisztrációját is. Ezek közé online funkció közé tartozik a beiratkozás, a felmérők biztosítása és az előrehaladás nyomon követése.

A kommunikáció változása

Az internet globalizálódása új formájú kommunikációs lehetőségeket hívott életre. Ez tette lehetővé az egyén számára, hogy globális közönségek által is hozzáférhető tartalmakat hozzon létre.

Az új lehetőségek néhány formája:

- **Azonnali üzenetküldés (IM) / szöveges üzenetküldés** Az IM és a szöveges üzenetek egyszerre két vagy több ember között tesznek lehetővé valós idejű kommunikációt. Számos IM és üzenetküldő alkalmazás kibővül olyan további funkciókkal is, mint például a fájlátvitel. Az IM alkalmazások olyan kiegészítő szolgáltatásokat is kínálnak, mint amilyen a hang- és videókommunikáció.

- **Közösségi portálok** - A közösségi portálok olyan interaktív weboldalakból állnak, ahol az emberek és a közösségek létrehozhatnak és megoszthatnak saját készítésű tartalmakat a barátaikkal, családjukkal, társaikkal és a világgal.

- **Csoportmunka eszközök** - A csoportmunka eszközök alkalmazásával együtt dolgozhatunk másokkal megosztott dokumentumokon. A felhasználók a tartózkodási helyüktől vagy az időzónától függetlenül csatlakozhatnak a megosztott rendszerhez, beszélhetnek egymással, gyakran mindezt valós idejű, interaktív videóközvetítésen keresztül. Megoszthatnak egymással szövegeket és képeket, valamint dokumentumokat is szerkeszthetnek együtt. A folyamatosan elérhető csoportmunka eszközök segítségével a szervezetek könnyebben oszthatnak meg információkat és érhetik el céljaikat. Az adathálózatok széleskörű elterjedése azt eredményezi, hogy az emberek távoli helyekről is ugyanúgy férhetnek hozzá dolgokhoz, mintha egy nagy népsűrűségű központ szívében lennének.

- **Weblogok (blogok)** - A blogok könnyen frissíthető és szerkeszthető weboldalak. Ellentétben a kereskedelmi weboldalakkal - amelyeket kommunikációs szakértők hoznak létre - a blogokon keresztül bárki megoszthatja gondolatait egy globális közösséggel, anélkül hogy értenie kellene a honlaptervezés technikájához. Szinte minden eszünkbe jutó dologról létezik blog, és gyakran közösségek is kialakulnak egy-egy népszerűbb blog szerzője köré.

- **Wikik** - A Wikik csoportok által szerkeszthető és megtekinthető weboldalak. Míg a blog inkább egyéni, személyes napló jellegű, addig a wiki egy csoport közös alkotása. Mint ilyet, sokkal kiterjedtebb áttekintés és szerkesztés jellemzi. A blogokhoz hasonlóan a wikiket is fokozatosan hozzák létre, és bárki szerkesztheti azokat anélkül, hogy az egészet egy nagyobb kereskedelmi vállalkozás szponzorálná. A Wikipedia egy a közösségek által fejlesztett, átfogó információ forrássá - egy online enciklopédiává - vált. Magánszervezetek és magánszemélyek is építhetnek saját wikiket, hogy rögzíthessék egy adott témáról az összegyűjtött ismereteiket. Sok vállalkozás belső csoportmunka eszközként használja a wikiket. A wikikben a globális internet által az élet minden területéről érkező emberek vehetnek részt, és adhatják hozzá saját nézőpontjukat és tudásukat egy megosztott forráshoz.

- **Podcasting** - A podcasting egy hang alapú információhordozó, amely lehetővé teszi, hogy az emberek hangot rögzíthessenek és további felhasználásra átalakíthassák azt. A podcasting lehetővé teszi, hogy ezek a felvételek széles közönség számára váljanak elérhetővé. Ezeket a

hangfelvételeket felteszik egy weboldalra (blogra vagy wikire), ahonnan mások letölthetik és lejátszhatják saját számítógépükön, laptopjukon vagy más mobil eszközükön.

- **Peer-to-peer (P2P) fájlmegosztás** - A Peer-to-peer fájlcserélők lehetővé teszik, hogy ne egy központi szerverről töltsünk le, hanem közvetlenül osszunk meg egymással fájlokat. A felhasználó egy P2P szoftver telepítésével csatlakozhat a P2P hálózathoz. A szoftver lehetővé teszi továbbá a fájlok megtalálását és másokkal történő megosztását a P2P hálózaton. A média (mint zene- és videó-) fájlok széleskörű digitalizálása megnövelte az érdeklődést a P2P fájlcserélők iránt. A P2P fájlmegosztás nem mindenki által támogatott. Sokan aggódnak a szerzői jogok megsértése miatt.

Milyen más oldalakat vagy eszközöket használhatunk, hogy megosszuk gondolatainkat?

Munkamódszereink változása

Az üzleti világban az adatátviteli hálózatokat kezdetben a saját pénzügyi információk tárolására és az ezekhez való hozzáférésre, az ügyfél adatok elmentésére és a munkavállalói bérszámfejtő rendszerek elérésére használták. Ezeknek az üzleti hálózatoknak a fejlődése tette lehetővé olyan információs szolgáltatások elterjedését, mint az e-mail, videó, üzenetküldés és a telefonos kommunikáció.

Egyre növekszik a hálózatok elfogadottsága az eredményes és költséghatékony munkavállalói tanfolyamok területén is. Az online tanulási lehetőségek csökkentik az időigényes és költséges utazásokat, és biztosítják a biztonságos és hatékony munkavégzéshez szükséges megfelelő oktatást.

Számos esettanulmány mutat be olyan munkahelyi sikereket, amelyeket a hálózatok innovatív használata tett lehetővé. Néhány ilyen esettanulmány a Cisco honlapján is elérhető: http://www.cisco.com.

Szórakozási szokásaink változása

Az internet széleskörű használata lehetővé tette a szórakoztató ipar és az idegenforgalom számára, hogy élvezhetőbbé és megoszthatóbbá tegye a kikapcsolódás számos formáját, mindezt a földrajzi helyzetünktől függetlenül. Interaktív módon fedezhetünk fel olyan helyeket, amelyek meglátogatásáról korábban még csak álmodni se merhettünk volna, ahogy eddig az se volt lehetséges, hogy még az utazásunk előtt előzetes képet kapjunk a célállomásról. Az utazók most már online küldhetnek részleteket és fényképeket kalandjaikról, amit így mások is megtekinthetnek.

Ezen túlmenően internetet használunk a szórakozás hagyományos formái közben is. Művészek felvételeit hallgathatjuk meg, mozgóképeket nézhetünk, teljes könyveket olvashatunk el és különböző anyagokat tölthetünk le későbbi offline használatra. Élő sportesemények és koncertek is nyomon követhetők, de felvételről is visszanézhetjük ezeket.

A hálózatok olyan új szórakozási formák létrejöttét is lehetővé tették, mint az online játékok. Ma már a játékosok szívesen vesznek részt bármilyen online versenyen. Egy ilyen versenyen ugyanúgy megmérkőzhetünk a világ számos pontján tartózkodó barátainkkal és versenytársainkkal, mintha ugyanabban a szobában lennénk.

Még az offline tevékenységeket is jobban végre tudjuk hajtani a hálózati csoportmunka szolgáltatásokkal. Gyorsan megjelentek a hálózaton a közös érdeklődésen alapuló globális közösségek. Már nem csak a szomszédainkkal, vagy az egy városban, régióban élőkkel oszthatjuk meg az élményeinket. A sportrajongók már szabadon cserélhetnek véleményt vagy híreket kedvenc csapatukról. Gyűjtők szabadon megoszthatják egymással díjazott gyűjteményeiket és szakmai visszajelzést is kaphatnak róluk.

Online vásárlói és aukciós oldalakon bármilyen árut el tudunk adni vagy meg tudunk vásárolni.

Bármilyen típusú kikapcsolódást is részesítünk előnyben a humán hálózatban, a hálózatok által gazdagabb élményben részesülhetünk.

Hogyan játszunk az interneten?

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Csoportmunka eszközök használata.
- 2. rész: Dokumentumok megosztása a Google Drive-on.
- 3. rész: Konferenciák és a webes találkozók megismerése.
- 4. rész: Wiki oldalak létrehozása.

Laborgyakorlat - Hálózati csoportmunka eszközök megismerése

A legkülönbözőbb méretű hálózatok léteznek. A méretük az egyszerű, két számítógépes hálózattól egészen a több millió eszközt tartalmazó hálózatokig terjed.

Az egyszerű otthoni hálózatok lehetővé teszik az erőforrások megosztását néhány helyi számítógép között. Ilyen erőforrások a nyomtató, a dokumentumok, a képek vagy a zenék.

Az otthoni vagy a kisvállalati hálózatokat gyakran olyan felhasználók alkotják, akik otthonról vagy egy kis fiókirodából dolgoznak, és szükséges számukra a vállalati hálózathoz vagy egy központi erőforráshoz való csatlakozás. Emellett számos egyéni vállalkozó használ otthoni vagy kisebb irodai hálózatot termékei eladására és reklámozására, eszközök megrendelésére vagy az ügyfelekkel való kapcsolattartásra. A hálózatokon keresztüli kommunikáció általában jóval hatékonyabb és olcsóbb a tradicionális kommunikációs megoldásoknál, mint például a hagyományos levelezés vagy a nagy távolságú telefonhívások.

A vállalatok és a nagy szervezetek még szélesebb körben használják a hálózatokat, hogy biztosítsák dolgozóiknak a hatékonyabb munkavégzés lehetőségét, az adataik tárolását és a vállalati szervereken tárolt információkhoz való hozzáférést. A hálózatok olyan gyors kommunikációs lehetőségeket biztosítanak, mint például az e-mail, az azonnali üzenetküldés és a munkavállalók közötti együttműködés. Ezen belső előnyök mellett számos szervezet használja a saját hálózatát arra, hogy azon keresztül termékeket vagy szolgáltatásokat nyújtson ügyfeleiknek.

Az internet a legnagyobb létező hálózat. Valójában az internet jelentése a "hálózatok hálózata". Az internet az összekapcsolt magán- és nyilvános hálózatok összessége, ezeket a hálózatokat a fentiekben már ismertettük. A vállalatok, a kis irodai hálózatok, de még az otthoni hálózatok is általában egy megosztott internetkapcsolattal rendelkeznek.

Hihetetlen, hogy az internet milyen gyorsan vált a mindennapjaink szerves részévé.

Állomásnak (host) vagy végberendezésnek nevezünk minden hálózatra csatlakoztatott számítógépet, amelyek közvetlenül részt vesznek a hálózati kommunikációban. Az állomások üzeneteket küldhetnek és fogadhatnak a hálózaton. A modern hálózatokban a végberendezések működhetnek kliensként (más néven ügyfélként), szerverként (más néven kiszolgálóként), vagy mindkét módon. Hogy a számítógép milyen szerepet tölt be éppen, azt a feltelepített programjai határozzák meg.

A szerverek azok az állomások, amelyeknek a feltelepített programjai más hálózati állomások számára információt szolgáltatnak, mint például elektronikus levelezés vagy weboldalak formájában. Minden szolgáltatás különálló szerver szoftvert igényel. Például egy számítógépre webszerver program szükséges, hogy webszolgáltatást nyújtson a hálózat számára.

A kliensek azok az állomások, amelyeknek telepített programjai lehetővé teszik, hogy szerverektől információkat kérjenek és azokat megjelenítsék. A kliensprogramra egy példa az Internet Explorer webböngésző.

A szerverszoftverrel ellátott számítógép egyidejűleg egy vagy több kliens számára is nyújthat szolgáltatásokat.

Egy számítógép egyszerre több típusú szerver szoftvert is képes futtatni. Otthoni vagy kisvállalati környezetben szükség lehet rá, hogy egy számítógép egyszerre legyen fájlkiszolgáló, webkiszolgáló és levelező-kiszolgáló is egyben.

Egy számítógép többféle kliensprogramot is tud futtatni. Minden igényelt szolgáltatáshoz szükség van egy kliensprogramra. Több feltelepített kliensprogrammal egy állomás egyszerre több kiszolgálóhoz is tud kapcsolódni. Például, egy felhasználó megnézheti egyszerre az elektronikus leveleit és egy weboldalt is, miközben azonnali üzenetküldőn beszélget és internetes rádiót hallgat.

A kliens és a szerver programok általában külön számítógépeken futnak, de az is lehetséges hogy egy számítógép a két szerepet egyszerre töltse be. Kisvállalati és otthoni hálózatokban egy állomás gyakran egyszerre szerverként és kliensként is szolgál. Az ilyen hálózatot egyenrangú (peer-to-peer) hálózatnak nevezzük.

A legegyszerűbb egyenrangú hálózat két közvetlenül - vezetékkel, vagy vezeték nélkül - összekapcsolt számítógépet tartalmaz.

Nagyobb egyenrangú hálózat létrehozására egyszerre több PC-t is összekapcsolhatunk, de ilyenkor szükségünk van hálózati eszközökre is (például kapcsolóra).

A fő hátránya az egyenrangú hálózati környezetnek az, hogy ha az állomás kliensként és szerverként is működik egyszerre, akkor a teljesítménye lecsökkenhet.

Nagyobb vállalatoknál - a lehetséges nagyobb hálózati forgalom és a szolgáltatások megnövekedett száma miatt - gyakran szükséges a dedikált szerverek használata.

Az út - amelyet egy üzenet megtesz a küldőtől a címzettig - lehet olyan egyszerű is, mint a két számítógépet összekötő egyetlen kábel, vagy lehet olyan bonyolult is, mint a Földet szó szerint körbefonó hálózat. Ez a hálózati infrastruktúra biztosítja a mindennapjaink során használt hálózati kommunikációt. Ez teremti meg azt a stabil és megbízható csatornát, amelyen mindennapjaink kommunikációja folyhat.

A hálózati infrastruktúra három kategóriába sorolható:

- Eszközök
- Információhordozó közeg (vagy média)
- Szolgáltatások

Kattintsunk az egyes gombokra az ábrán, hogy a megfelelő hálózati összetevő kiemeléséhez!

Az eszközök és a média a hálózat fizikai alkotóelemei. A hardvert gyakran a hálózati infrastruktúra látható elemei közé soroljuk, ezek a laptop, a PC, a kapcsoló, a forgalomirányító, a vezeték nélküli hozzáférési pont vagy az összeköttetést biztosító kábelezés. Esetenként a hálózat bizonyos összetevőit nem is láthatjuk. Vezeték nélküli média esetén az üzeneteket láthatatlan rádiófrekvenciás vagy infravörös hullámok formájában továbbítjuk.

A hálózati eszközöket szolgáltatások és folyamatok biztosítására használjuk. Ezek a kommunikációs programok - az úgynevezett szoftverek - hálózatba kötött eszközökön futnak. Egy hálózati szolgáltatás válasz formájában biztosítja az igényelt információt. A szolgáltatások között sok olyan általános hálózati alkalmazás is szerepel, amelyeket az emberek nap mint nap használnak, mint például az e-mail vagy a tárhely biztosító szolgáltatások. Különböző folyamatok biztosítják azokat a tevékenységeket is, amelyek üzeneteinket irányítják és célba juttatják a hálózaton keresztül. Ezek a

folyamatok kevésbé nyilvánvalóak számunkra, ugyanakkor a hálózat működése szempontjából igencsak fontosak.

A leginkább ismert hálózati eszközöket végberendezéseknek vagy állomásoknak nevezzük. Ezek az eszközök biztosítják az interfészt a felhasználók és háttérben működő kommunikációs hálózat között.

Néhány példa a végberendezésekre:

- számítógépek (munkaállomások, laptopok, fájl- és webszerverek),
- hálózati nyomtatók,
- IP (vagy VoIP) telefonok,
- TelePresence végpontok,
- biztonsági kamerák,
- mobil kézi készülékek (mint például okostelefonok, tablet-ek, PDA-k, vezeték nélküli hitelkártya-olvasók és vonalkód szkennerek).

A végberendezés forrása vagy célállomása is lehet a hálózati kommunikációnak, amint ez az ábrán is látható. Annak érdekében, hogy meg tudjuk különböztetni az egyik készüléket a másiktól, minden állomást a hálózaton egy egyedi címmel kell azonosítanunk. Mikor az állomás kommunikációt kezdeményez, akkor a célállomás címével határozza meg, hogy hova kell az üzenetet továbbítani..

A közvetítő hálózati eszközök kapcsolják össze a végberendezéseket. Mint ahogy ez a mellékelt animáción is látható, a háttérben ezek az eszközök biztosítják a kapcsolatot és a szükséges folyamatokat, hogy lehetővé váljon az adatáramlás a hálózaton keresztül. Ezek a közvetítő eszközök kötik össze az egyes állomásokat a hálózattal, egyben más hálózatok felé is lehetővé téve az átjárást.

Példák a közvetítő hálózati eszközökre:

- hálózati hozzáférést biztosító berendezések (kapcsolók és a vezeték nélküli hozzáférési pontok),
- hálózat-összekapcsoló (internetworking) eszközök, mint például a forgalomirányítók,
- biztonsági eszközök (tűzfalak).

A hálózaton keresztül továbbított adatok kezelése is ezen közvetítő eszközök feladata. Ezek a berendezések a célállomás címe és az adott hálózat jellemzői alapján határozzák meg az üzenetek továbbítási útvonalát.

A közvetítő hálózati eszközökön futó folyamatok a következő funkciókat biztosítják:

- az adatjelek regenerálása és továbbítása,
- információ biztosítása a hálózaton belüli és a hálózatok közti különböző útvonalakról,
- más eszközök értesítése hibákról és a kommunikáció sikertelenségéről,
- kapcsolati hiba esetén alternatív útvonalak biztosítása,
- különböző üzenetek osztályozása és továbbítása a prioritási paramétereknek (Quality of Service, QoS) megfelelően,

- az adat továbbításának engedélyezése vagy megtagadása a biztonsági beállításoknak megfelelően.

A kommunikáció egy hálózaton a továbbító közegen (más néven médián) keresztül történik. Ez a közeg biztosítja azt a csatornát, amelyen keresztül az üzenet eljut a forrástól a célállomásig.

A modern hálózatok általában három különböző közeget használnak az eszközök összekapcsolására, illetve az adatok továbbítására. Amint az ábrán is látható, ezek a közegek a következők:

- fémvezetékek a kábelekben,
- üveg vagy műanyag szálak (optikai kábelek),
- vezeték nélküli átvitel.

A jel továbbításához szükséges kódolás minden átviteli közegen különböző. A fémvezetékeken az adatokat speciális mintáknak megfelelő elektromos impulzusokkal kódolják. Optikai átvitelnél az infravörös vagy a látható fény tartományában használt fény impulzusok adják a jeleket. A vezeték nélküli adatátvitelnél pedig az elektromágneses hullámok segítségével biztosítják a különböző biteket.

Az egyes adatátviteli közegek egyedi sajátosságokkal és előnyökkel rendelkeznek. Nem mindegyik hálózati közeg rendelkezik ugyanolyan tulajdonságokkal, illetve nem mindegyik alkalmas ugyanarra a célra. Az átviteli közeg megválasztásának szempontjai:

- a távolság, amelyen keresztül a közeg képes a jelet továbbítani,
- a környezet, ahol az átviteli közeget ki kell építeni,
- az adatok mennyisége, valamint az a sebesség, amellyel azokat továbbítani kell,
- a közeg anyag- és telepítési költsége.

Ha olyan összetett fogalmat kell bemutatnunk, mint egy nagyvállalati hálózat eszközei és a használt átviteli közegek, akkor érdemes képi megjelenítést használnunk. Egy ábra használata egyszerű módja annak, hogy megértsük egy nagy hálózat felépítését. Egy ilyen ábra különböző szimbólumokat használ a hálózatot felépítő eszközök és kapcsolatok megjelenítésére. Ezt a fajta hálózati "képet" topológiai ábrának nevezzük.

Mint minden más nyelv, a hálózatok nyelve is használ olyan közös szimbólumokat, amelyek az egyes végberendezéseket, hálózati eszközöket és az átviteli közegeket jelképezik. Szükséges elsajátítani a fizikai eszközök logikai ábrázolásának képességét, mert ez egy kritikus pont egy hálózat felépítésének és működésének ábrázolásakor. Ezen a tanfolyamon és a laborgyakorlatain elsajátíthatjuk a hálózati eszközök működését és az alapvető beállítási lehetőségeket.

A vizuális megjelenítés mellett sajátos szakmai nyelvet is használunk ezen eszközök és az átviteli közegek csatlakozásának leírásához. A következő fogalmakra fontos emlékeznünk:

- **Hálózati kártya (NIC, Network Interface Card)** - Ez az az eszköz, amely biztosítja a PC-k vagy más állomások számára a hálózathoz történő fizikai kapcsolódást. Gyakran hívják NIC-nek, vagy LAN adapternek. A PC és a hálózat közti átviteli közeg közvetlenül a NIC-be csatlakozik.
- **Fizikai port** - Egy hálózati eszközön a csatlakozást biztosító aljzat, ide csatlakozik az átviteli közegen keresztül egy állomás vagy egy másik hálózati eszköz.

- **Interfész** - Speciális port egy hálózati eszközön, amely más hálózatokhoz csatlakozik. Mivel a forgalomirányítók kötik össze a hálózatokat, ezért a forgalomirányító portjait nevezzük interfészeknek.

A topológiai ábrák használata kötelező mindazok számára, akik a hálózatokkal foglalkoznak. Ez biztosítja a hálózati összeköttetések vizuális térképét.

Kétféle topológiai ábra létezik:

- **Fizikai topológiai ábra** - Ez mutatja meg a közvetítő eszközök, a használt portok és a kábelezés fizikai elhelyezkedését.

- **Logikai topológiai ábra** - Ez azonosítja az eszközöket, a portokat és az IP-címzési rendszert.

A hálózati infrastruktúrák nagyban eltérnek egymástól a következőkben:

- a lefedett terület mérete,

- kapcsolódott felhasználók száma,

- az elérhető szolgáltatások száma és típusa.

Az ábra a két leggyakoribb hálózati infrastruktúrát szemlélteti:

- **Helyi számítógép-hálózat (LAN, Local Area Network)** - Egy hálózati infrastruktúra, amely kis földrajzi elhelyezkedésű területen biztosít összeköttetést a felhasználók és a végberendezések számára.

- **Nagytávolságú hálózat (WAN, Wide Area Network)** - Olyan hálózati infrastruktúra, amely széles földrajzi területen biztosít összeköttetést hálózatok között.

Egyéb hálózati típusok:

- **Nagyvárosi hálózat (MAN, Metropolitan Area Network)** - Olyan hálózati infrastruktúra, amely egy LAN-nál nagyobb, de egy WAN-nál kisebb fizikai területet fed le (pl. egy város területe). A MAN hálózatokat gyakran egyetlen szervezet működteti, például egy nagyvállalat.

- **Vezetéknélküli LAN (WLAN, Wireless LAN)** - Hasonló a LAN-hoz, de vezeték nélkül köti össze a felhasználókat és a végpontokat egy kis földrajzi területen.

- **Adattároló hálózat (SAN, Storage Area Network)** - Ezt a hálózati infrastruktúrát fájlszerverek támogatására tervezték, biztosítja az adatok tárolását, visszakereshetőségét és mentését. Modern szervereket, több lemezből álló adattárolókat (úgynevezett blokkokat) és Fibre Channel összeköttetéseket magában foglaló hálózat.

A helyi hálózatok (LAN) kis földrajzi területet lefedő hálózatok. A LAN-ok sajátosságai a következők:

- A LAN egy korlátozott nagyságú területen - mint például az otthonok, az iskolák, az irodaépületek vagy az egyetemi kampuszok - teszi lehetővé a végberendezések összekapcsolódását.

- A LAN-t rendszerint egyetlen szervezet vagy egy magánszemély felügyeli. Az adminisztratív feladatok közé tartozik többek között a hálózati szintű biztonsági és hozzáférési házirendek alkalmazása.

- A LAN-ok nagy sebességű sávszélességet biztosítanak a belső végberendezéseknek és hálózati közvetítő eszközöknek.

A nagytávolságú hálózatok (WAN, Wide Area Network) olyan hálózati infrastruktúrát jelentenek, amelyek nagy földrajzi területeket fednek le. A WAN hálózatokat általában szolgáltatói szervezetek, vagy internet szolgáltató cégek (ISP, Internet Service Provider) biztosítják.

A WAN hálózatok sajátosságai a következők:

- A WAN-ok biztosítják az összeköttetést a LAN-ok között olyan nagy földrajzi területeket átfogva, mint városok, államok, tartományok, országok vagy kontinensek.

- A WAN hálózatokat rendszerint több szolgáltató biztosítja.

- A WAN-ok jellemzően lassabb összeköttetést biztosítanak, mint a LAN-ok.
  - A LAN és WAN összeköttetések mellett a legtöbb felhasználónak más, külső hálózatokon található adatokra is szüksége van. Mindezt az interneten keresztül érhetik el.
  - Amint az ábrán is látható, az internet a különböző összekapcsolt hálózatok világméretű gyűjtőhelye, amelyek egymással együttműködnek, és közös szabványok alapján információt cserélnek egymással. Az internet felhasználói telefonvezetékeken, optikai kábeleken, vezeték nélküli átvitellel vagy műholdas kapcsolat segítségével cserélhetnek egymással adatokat.
  - Az internet a hálózatoknak olyan halmaza, amelyet nem birtokol egyetlen magánszemély vagy csoportosulás sem. A különböző hálózatok közti hatékony adatkommunikáció egységes és következetes szabványok alkalmazását igényli, egyben számos rendszerfelügyeleti szervezet együttműködését is feltételezi. Vannak olyan szervezetek, amelyek az internetes protokollok és folyamatok formai követelményeire és a szabványosítására felügyelnek. Ezen szervezetek közé tartoznak az Internet Engineering Task Force (IETF), az Internet Corporation for Assigned Names and Numbers (ICANN), az Internet Architecture Board (IAB) és még néhány más hasonló szervezet.
  - **Megjegyzés:** Az internet szót (kisbetűs "i"-vel) a többszörösen összekapcsolt hálózatokra használják. Amikor a globális hálózati rendszerre hivatkozunk, mint például a World Wide Web-re, akkor nagybetűs "I"-vel is írhatjuk az internetet.

Két másik kifejezés is van, amelyek hasonlatosak az internet kifejezéshez:

- intranet

- extranet

Az intranet kifejezést gyakran használjuk azokra a privát LAN és WAN hálózati összeköttetésekre, amelyek egy szervezethez tartoznak, és csak a szervezet tagjai, munkavállalói vagy meghatalmazott külső személyek használhatják. Az intranet alapvetően olyan internet, amely általában csak egy szervezeten belülről érhető el.

A szervezetek olyan weboldalakat tehetnek fel az intranetre, mint a belső események, egészségügyi és biztonsági előírások, dolgozói hírlevelek vagy céges telefonkönyvek. Például az iskoláknak lehet olyan intranetük, amely tartalmazza az osztályok órarendjét, az online tananyagokat és a vitafórumokat. Az intranet általában segíti a papírmunka mellőzését és a munkafolyamatok felgyorsítását. Az intranethez a dolgozók a szervezeten kívülről is hozzáférhetnek megfelelően biztonságos kapcsolat használatával.

Egy szervezet használhat extranet-et, hogy biztonságos és megbízható hozzáférést biztosítson a saját hálózata eléréséhez más szervezetek dolgozói számára is. Példák extranet-re a következők:

- Egy cég hozzáférést biztosít külső beszállítóik / vállalkozóik számára.

- Egy kórház foglalási rendszert biztosít az orvosok számára, akik így találkozókat egyeztethetnek a betegeikkel.

- Egy oktatásügyi helyi kirendeltség költségvetési és személyi adatokat szolgáltat a kerületi iskolákról.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Felmérés a konvergens hálózat értelmezéséről.

- 2. rész: Az ISP-k által kínált konvergált szolgáltatások megismerése.

- 3. rész: A helyi ISP-k által kínált konvergált szolgáltatások megismerése.

- 4. rész: A legjobb helyi ISP konvergált szolgáltatás a kiválasztása.

- 5. rész: Konvergens technológiákat alkalmazó helyi vállalatok vagy közintézmények megismerése.

Laborgyakorlat - Researching Converged Network Services

Számos módon lehet felhasználókat vagy szervezeteket az internetre kapcsolni.

Az otthoni felhasználók, a távmunkások (távoli dolgozók), és a kis irodák jellemzően egy ISP-hez csatlakoznak, hogy elérjék az internetet. Az elérhető csatlakozási lehetőségekben nagy különbségek találhatók ISP-k és földrajzi területek között. Népszerű csatlakozási lehetőség a szélessávú kábel, a szélessávú digitális előfizetői vonal (DSL), a vezeték nélküli WAN és a különböző mobil szolgáltatások.

Szervezetek jellemzően igénylik más vállalati honlapokhoz és az internethez történő hozzáférést. Gyors kapcsolat szükséges olyan üzleti szolgáltatások támogatására, mint az IP-telefonok, videokonferencia megoldások és az adatközponti tárolás.

Az üzleti osztályú összeköttetéseket általában szolgáltatók (SP, Service Providers) biztosítják. Népszerű üzleti osztályú szolgáltatás az üzleti DSL, a bérelt vonal és a Metro Ethernet.

Az ábrán általános csatlakozási lehetőségeket láthatunk, amelyeket a kis irodai vagy az otthoni felhasználók használnak, ezek a következők:

- **Kábel** - Általában kábeltelevíziós szolgáltatók kínálják, az internetes adatjelek szállítása ugyanazon a koaxiális kábelen történik, mint ami a kábeltévé jeleit továbbítja. Nagy sávszélességű és állandó internetkapcsolatot biztosít. Egy speciális kábelmodem választja el az internetes adatok jeleit a többi jeltől, és ez az eszköz biztosítja az Ethernet kapcsolatot a számítógép vagy a LAN felé.

- **DSL** - Nagy sávszélességű és állandó internetkapcsolatot biztosít. Szükséges hozzá egy speciális nagy sebességű modem, amely elválasztja a DSL jeleit a telefonos jelektől, és egy Ethernet kapcsolatot biztosít a számítógép vagy a LAN felé. A DSL a telefonvonalat használja, amelyet három különböző csatornára oszt szét. Az első csatorna szolgál a telefonhívásokra. Ez a csatorna teszi lehetővé, hogy az előfizető anélkül fogadjon telefonhívásokat, hogy bontania kellene az internet kapcsolatát. A második csatorna egy gyorsabb letöltési csatorna, ezen keresztül érkeznek az adatok az internet felől. A harmadik csatorna küldésre vagy feltöltésre használható. Ez a csatorna általában valamivel lassabb, mint a letöltési csatorna. A DSL minősége és a sebessége nagyban függ a telefonvonal minőségétől és a telefonos cég szolgáltató központjának távolságától. Minél messzebb van ettől a központtól az előfizető, annál lassabb lesz a kapcsolata.

- **Mobilhálózatok** - A mobil internet a mobiltelefonos összeköttetést használja csatlakozásra. Ahol a rádiójelek elérhetők, ott lehet mobil internet-hozzáférés is. A teljesítményt korlátozhatják a telefon, vagy a csatlakozást biztosító adótorony (bázisállomás) képességei. Azokon a helyeken előnyös a mobil internet használata, ahol egyébként nem lehet máshogy internet kapcsolatot biztosítani, vagy ahol a felhasználók folyton mozgásban vannak.

- **Műhold** - A műholdas szolgáltatás egy jó lehetőség azon otthonok vagy irodák számára, amelyek nem tudnak hozzáférni a DSL vagy a kábeles szolgáltatásokhoz. A parabola antennának tiszta rálátás szükséges a megfelelő műholdra, így ez a szolgáltatás nem mindig érhető el sűrű erdős, vagy más akadályokkal teli területen. A műholdas szolgáltatásnál alapvetően jó sávszélesség áll rendelkezésre, de a konkrét sebesség a választott szerződés függvénye. A berendezés- és telepítési költségek magasak lehetnek (érdemes ellenőrizni a szolgáltató kedvezményes ajánlatait), ezek mellett a havi díjak már mérsékeltebbek. A műholdas internet-hozzáférés ott előnyös igazán, ahol nincs más mód a csatlakozásra.

- **Modemes behívás** A modemes betárcsázás egy nem túl költséges, telefonvonal és modem használatával megvalósított internet elérési módszer. Az internetszolgáltatóhoz való kapcsolódáshoz a felhasználónak fel kell hívnia a szolgáltató elérési számát. A modemes behívás alacsony sávszélessége rendszerint nem elegendő a nagy adatátviteli műveletekhez, bár hasznos mobil hozzáférést biztosít utazás közben. A modemes behívás csak akkor jöhet számításba, ha nagyobb sebességű kapcsolat nem áll rendelkezésre.

Sok otthon és kisebb iroda egyre gyakrabban használ közvetlen optikai vonalat a csatlakozásra. Ez lehetővé teszi az internetszolgáltatók számára, hogy a nagyobb sávszélesség mellett egyszerre több szolgáltatást is biztosítsanak, úgymint internet, telefon és TV.

A lehetséges kapcsolódási opciók a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei.

Mik a te lehetőségeid az internetre csatlakozásra?

A vállalatok csatlakozási lehetőségei különböznek az otthoni felhasználók lehetőségeihez képest. A vállalatok nagyobb és dedikált sávszélességet, valamint menedzselt szolgáltatásokat igényelnek. A csatlakozási lehetőségek nagyban eltérőek attól függően, hogy hány szolgáltató működik a vállalat közelségében.

Az ábrán a szervezetek számára leggyakrabban elérhető csatlakozási lehetőségek láthatók, ezek:

- **Dedikált bérelt vonal** - Ez egy dedikált kapcsolat a szolgáltató és az ügyfél telephelyei között. A bérelt vonalak valóban saját használatú távközlési áramkörök, amelyek földrajzilag távol levő irodák saját hang- és/vagy adathálózatát biztosítják. A vonalakat általában bérlik viszonylag magas havi vagy éves díj ellenében. Észak-Amerikában gyakori bérelt vonali áramkörök a T1 (1,54 Mb/s) és a T3 (44,7 Mb/s), míg a világ más részein az E1 (2 Mb/s) és az E3 (34 Mb/s) kapcsolatok állnak a vállalatok rendelkezésére.

- **Metro Ethernet** - A Metro Ethernet általában közvetlen réz- vagy optikai kapcsolaton keresztül érhető el a szolgáltatótól, a biztosított sávszélesség pedig 10 Mb/s és 10 Gb/s között van. Sok esetben a réz alapú Ethernet (EOC, Ethernet over Copper) sokkal gazdaságosabb, mint az optikai Ethernet szolgáltatás, mert meglehetősen széles körben áll rendelkezésre, és sávszélessége elérheti akár a 40 Mb/s-ot is. A réz alapú Ethernet használata ugyanakkor függ a távolságtól. Az optikai Ethernet szolgáltatás biztosítja a leggyorsabb és ár-érték arányban a leggazdaságosabb kapcsolatot. Sajnos még sok olyan terület van, ahol ez a szolgáltatás nem érhető el.

- **DSL** - Az üzleti DSL több változatban létezik. A legnépszerűbb változat a szimmetrikus digitális előfizetői vonal (SDSL), amely hasonló az aszimmetrikus digitális előfizetői vonalhoz (ADSL), de ugyanazt a feltöltési és letöltési sebességet biztosítja. Az ADSL-t úgy tervezték, hogy különböző nagyságú legyen a letöltési és feltöltési sávszélesség. Például egy ügyfél internet-hozzáférése

letöltési irányban 1,5-9 Mb/s lehet, míg a feltöltési irány 16-640 Kb/s. Az ADSL átvitel 18000 láb (5488 méter) távolságig működik egy réz alapú csavart érpáron.

- **Műhold** - Műholdas szolgáltatást ott is lehet nyújtani, ahol a vezetékes megoldások nem állnak rendelkezésre. A parabola antennáknak szükséges a tiszta rálátás a műholdra. A berendezés- és telepítési költségek magasak lehetnek, de emellett a havi díjak már mérsékeltebbek. A kapcsolatok általában lassabbak és kevésbé megbízhatóak, mint a földi versenytársakéi, így ez a lehetőség kevésbé vonzó, mint a többi alternatíva.

A kapcsolódási lehetőségek a földrajzi elhelyezkedés és a szolgáltató elérhetőségének a függvényei.

A Packet Tracer egy szórakoztató, otthonról is elérhető, rugalmas szoftver, amely segíti a Cisco Certified Network Associate (CCNA) tanulmányokat. A Packet Tracer lehetővé teszi, hogy kísérletezzünk a különböző hálózati folyamatokkal, hálózati modelleket építsünk, és "mi lenne ha" kérdésekre kapjunk válaszokat. Ebben a feladatban egy viszonylag összetett hálózatot fogunk megismerni, amely egyben rá is világít a Packet Tracer néhány jellemzőjére. A feladat megoldása során megtanuljuk hogyan érhetők el a Súgó oldalai és a különböző segédletek. Azt is megtanuljuk, hogyan kell váltani a különböző módok és a munkaterületek között. Végül azt is meg fogjuk ismerni, hogy a Packet Tracer - mint modellező eszköz - hogyan képes megjeleníteni egy hálózatot.

Packet Tracer - Network Representation Instructions

Packet Tracer - Network Representation - PKA

A modern hálózatok folyamatosan fejlődnek, hogy megfeleljenek a felhasználói igényeknek. A korai adathálózatok csak karakter-alapú információ cseréjére voltak képesek a kapcsolódott számítógépek között. A hagyományos telefon, rádió és a televízió-hálózatok külön adatátviteli hálózatokként üzemeltek. A múltban minden ilyen szolgáltatás dedikált hálózatot igényelt, amelyek különböző kommunikációs csatornák és technológiák használatával vitték át az adott kommunikáció jeleit. Mindegyik szolgáltatásnak saját szabályai és szabványai voltak a kommunikáció sikeres lebonyolításához.

Vegyünk egy negyven évvel ezelőtt épült iskolát. Akkoriban a tantermek külön kábelezést használtak az adathálózathoz, a telefonhálózathoz és a videós hálózat által használt televíziókhoz. Ezek a különálló hálózatok eltérők voltak, vagyis nem tudtak egymással kommunikálni - ez látható az 1. ábrán.

A technológiai fejlesztések lehetővé tették, hogy ezeket a különálló hálózatokat egyetlen felületbe, a "konvergált hálózatba" integráljuk. A dedikált hálózatokkal ellentétben a konvergált hálózatok képesek sok különböző típusú eszköz között, de ugyanazt a kommunikációs csatornát használva egyszerre átvinni hang- és videojelet, valamint szöveg és képi jellegű adatokat is (lásd 2. ábra). A korábban különálló kommunikációs formák közös platformba olvadtak egybe. Ez a platform lehetővé tesz számos olyan alternatív és új kommunikációs módszert, amelyek által az emberek szinte azonnal közvetlen kapcsolatba kerülhetnek egymással.

Egy konvergált hálózatra még mindig különböző módokon és különböző eszközökkel lehet kapcsolódni (úgymint számítógépek, telefonok, televíziók és tabletek), de már minden egy közös hálózati infrastruktúrát használ. Ez a hálózati infrastruktúra már ugyanazokat a szabályokat, megállapodásokat és megvalósítási szabványokat használja.

A különböző kommunikációs hálózatok egyetlen közös platformra történő konvergenciája jelenti az első fázisát az intelligens információs hálózat kiépítésének. Jelenleg mi ebben a hálózati evolúciós fázisban vagyunk. A következő fázis az lesz, hogy nem csak a különböző típusú üzenetek kerülnek továbbításra egy egységes hálózatban, hanem maguk az alkalmazások - amelyek létrehozzák, továbbítják és biztosítják a kommunikációt - is összeolvadnak a hálózati eszközökkel.

Nem csak a hang és a videó kerül továbbításra ugyanazon a hálózaton, de maga a telefonos kapcsolást és a videó közvetítését biztosító eszköz válik a hálózati forgalom irányításért felelős

eszközzé is. Ez az egységes kommunikációs platform magas színvonalú és költséghatékony alkalmazások működését teszi majd lehetővé.

A tempó, amellyel az új és izgalmas konvergens hálózati alkalmazások fejlesztése történik, egyben azt is meg fogja határozni, hogy milyen gyorsan fog növekedni az internet. Jelenleg csak mintegy 10 milliárd eszköz - a létező 1,5 trillióból - csatlakozik az internetre, így még hatalmas potenciál van abban, hogy a maradékot is csatlakoztassuk az eszközök internetjére (IoE, Internet of Everything). Ez a terjeszkedés egy olyan széles közönséget hoz létre, amely számára így bármely üzenet, termék vagy szolgáltatás eljuttatható.

A robbanásszerű növekedést eredményező mögöttes mechanizmusok és folyamatok lehetővé tettek egy olyan hálózati infrastruktúrát, amely képes egyszerre megújulni és folyamatosan növekedni is. Ahogy a humán hálózatokban a mindennapos élet, a tanulás, a munka és a játék területein megtalálható különböző újszerű megoldásoknak, úgy a hálózati architektúrának is alkalmazkodnia kell a folyamatosan magasabb elvárásokat támasztó és biztonságosabb szolgáltatásokhoz.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: A hálózati összeköttetés ellenőrzése a Ping használatával.
- 2. rész: Egy távoli szerverhez vezető útvonal felderítése a Windows tracert utasításával.
- 3. rész: Egy távoli szerverhez vezető útvonal felderítése Web-es és Windows-os alkalmazásokkal.
- 4. rész: A traceroute eredmények összehasonlítása.

Laborgyakorlat - Mapping the Internet

A hálózatoknak számos alkalmazást és szolgáltatást kell támogatniuk, ugynakkor a fizikai infrastruktúrát alkotó különböző kábelekkel és eszközökkel is együtt kell működniük. A hálózati architektúra kifejezés ebben az összefüggésben azokra a technológiákra utal, amelyek támogatják azt az infrastruktúrát, valamint a különböző programozott szolgáltatásokat és szabályokat (más néven protokollokat), amelyek végül üzeneteket küldenek a hálózaton keresztül.

A hálózatok fejlődésével arra a négy alapvető hálózati jellemzőre is fény derült, amelyekkel a háttérben működő hálózati architektúrának foglalkoznia kell, hogy a hálózat meg tudjon felelni a felhasználói elvárásoknak:

- hibatűrés (1. ábra)
- skálázhatóság (2. ábra)
- a szolgáltatás minősége (QoS, Quality of Service - 3. ábra)
- biztonság (4. ábra)
  - **Hibatűrés**
  - Az elvárás az, hogy az internet mindig rendelkezésre álljon annak a több millió felhasználónak a számára, akik használnák a hálózatot. Ehhez az szükséges, hogy a hálózati architektúra hibatűrő módon legyen felépítve. Az a hibatűrő hálózat, amely képes korlátozni egy hálózati kiesés hatását, vagyis hogy minél kevesebb eszköz legyen érintve a hibában. Ezek a hálózatok úgy vannak felépítve, hogy egy hiba bekövetkezésekor lehetővé tegyék a gyors helyreállást. Az ilyen hálózatok azon alapulnak, hogy az üzenet forrása és a célja közötti több útvonal is létezik. Ha egy útvonal megszakad, az üzeneteket azonnal egy másik kapcsolaton továbbítják. Redundanciának hívják, ha egy célállomáshoz egyszerre több út is vezet.
  - **Vonalkapcsolt és kapcsolatorientált hálózatok**

- Ahhoz, hogy megértsük a redundancia szükségességét, vissza kell tekintenünk a korai telefonos rendszerek működésére. Ha valaki egy hagyományos telefonhívást kezdeményezett, akkor a hívásnak előbb fel kellett épülnie. Ez a folyamat állapította meg a szükséges kapcsolási helyszíneket a hívó fél (forrás) és a fogadó fél eszköze (célállomás) között. Egy átmeneti útvonal, pontosabban egy vonal épült ki a telefonhívás idejére. Ha bármelyik eszköz vagy kapcsolat megszakadt, az egész hívás sikertelenné vált. Újrakapcsolódás esetén pedig egy teljesen új hívást kellett kezdeményezni, új vonalak használatával. Ezt a kapcsolódási formát vonalkapcsolásnak nevezzük, részletei a mellékelt ábrán láthatók.
- Több vonalkapcsolt hálózat előnyben részesítette a már kiépült vonalakat, mindezt akár a felépítendő új kapcsolatok rovására is. Amint két eszköz között egy vonal felépült, folyamatos használatba került, függetlenül attól, hogy volt-e kommunikáció az eszközök között, vagy sem. Ez mindaddig tartott, míg az egyik fél le nem bontotta a vonalat. Mivel csak véges sok kapcsolatot lehetett felépíteni, ezért megeshetett, hogy egy új hívás felépítésére már nem maradt elég erőforrás. A különböző alternatív útvonalak kiépítési költsége a megannyi hívás számára, valamint hálózati hiba esetén a kiesett kommunikációs elemek újraépítése túl költséges volt ahhoz, hogy optimális legyen ez a kapcsolódási mód az internetre való csatlakoztatáshoz.
- **Csomagkapcsolt hálózatok**
- A hibatűrő hálózat kutatása során az internet kezdeti tervezői kifejlesztették a csomagkapcsolt hálózatot. Ennek az átvitelnek az volt a különlegessége, hogy az üzeneteket kisebb blokkokra lehetett bontani, amelyek mindegyike tartalmazta a szükséges címzési információkat, vagyis a küldő és a fogadó állomás címét. Ezen beágyazott információk segítségével a blokkokat - más néven csomagokat - képesek voltak akár különböző útvonalakon is elküldeni a célállomás felé, majd elérve azt vissza lehetett állítani a csomagokból az eredeti üzenetet. Ezt láthatjuk a mellékelt ábrán.
- A hálózati eszközök az egyes csomagok tartalmával általában nincsenek tisztában. A továbbítás szempontjából csak a célállomás címe fontos. Ezeket a címeket gyakran IP-címeknek nevezik, amelyeket decimális számokkal, egymástól pontokkal elválasztva jelölnek, mint például 10.10.10.10 címet. Mindegyik csomag egymástól függetlenül kerül elküldésre egyik helyről a másikra. Minden egyes továbbító eszköznél forgalomirányítási döntés születik, hogy a célállomás felé melyik útvonalat kell majd használni. Ez olyan, mintha egy hosszú levelet írnánk egy barátnak, csak mindezt tíz képeslap használatával. Mindegyik képeslap tartalmazza a célállomás címét. A postai rendszer a képeslapok továbbításánál a célállomás címét használja a továbbítási útvonal meghatározásához. Az üzeneteknek végül mind el kell jutniuk a képeslapokon található célállomáshoz.
- Ha egy korábban használt útvonal már nem érhető el, akkor a következő legjobb útvonal dinamikusan kerül kiválasztásra a forgalomirányítás révén. Mivel az üzeneteket nem egyben, hanem darabokban küldik el, ezért ezt a néhány csomagot amelyik esetleg elveszik, egy másik útvonalon újra el lehet küldeni célállomásnak. Sok esetben a célállomás nem is érzékeli, hogy valamilyen hiba, vagy átirányítás történt volna. Használva az előző képeslapos példát, ha az egyik képeslap elveszik az út során, akkor csak azt az egyetlen képeslapot kell újra küldeni.
- Előre kiépített és fenntartott vonalra nincs szükség a csomagkapcsolt hálózatban. Minden egyes üzenetdarabot akár különböző útvonalakon is el lehet küldeni. Továbbá egyidejűleg akár különböző küldőktől származó csomagokat is lehet továbbítani a hálózaton. A hálózat felhasználói beavatkozás nélkül, dinamikusan kezeli a redundáns útvonalakat, ezáltal az internet hibatűrő kommunikációt tesz lehetővé. Ahogy a képeslapos példánkban is, az általunk küldött leveleknek osztozniuk kell a postai továbbítási rendszerben más képeslapokkal, levelekkel és csomagokkal. Például az egyik képeslapunknak együtt kell utaznia egy repülőgépen más csomagokkal és levelekkel, miközben mindegyik küldemény a saját végső rendeltetési helye felé tart.
- Habár a csomagkapcsolt és nem kapcsolatorientált hálózatok az elsődleges alkotóelemei a jelenlegi internetnek, a kapcsolatorientált rendszereknek is - mint a vonalkapcsolt telefonos rendszer - vannak előnyeik. Ilyen például az, hogy a rendelkezésre álló kapcsolási helyeken csak véges számú és dedikált vonal található, ezért ez az átvitel képes az üzenetek minőségét és egységességét is garantálni. Egy másik előnye a vonalkapcsolt hálózatoknak, hogy a szolgáltató a nyújtott szolgáltatása teljes időtartamát képes rögzíteni és kiszámlázni ügyfelei számára. Az aktív vonalhasználati díjak kiszámlázhatósága az ügyfelek felé egy alapvető célkitűzés a szolgáltatói piacon.

- **Skálázhatóság**
- Minden héten több ezer új felhasználó és szolgáltató kapcsolódik az internethez. Annak érdekében hogy az internet támogathassa ezt a gyors növekedést, méretezhetőnek - más néven skálázhatónak - kell lennie. A skálázható hálózatokat gyorsan lehet bővíteni az új felhasználók és alkalmazások támogatására, mindezt anélkül, hogy az befolyásolná a már meglévő felhasználók számára nyújtott szolgáltatások teljesítményét. Az ábra az internet szerkezetét mutatja.
- Az internet ilyen mértékű bővíthetősége a különböző hálózati protokollok és működtető technológiák felépítésének köszönhető. Az internet hierarchikus rétegekből álló címzési-, elnevezési- és kapcsolódási szolgáltatások együtteséből épül fel. Ennek eredményeként a hálózati forgalom helyi vagy regionális jellegű szolgáltatásához nem szükséges igénybe venni a központi elosztó szinteket. Anélkül lehet közös szolgáltatásokat egyszerre több régióban is igénybe venni, hogy ezek a központi gerinchálózatot terhelnék.
- A skálázhatóság arra is utal, hogy a hálózat képes új termékeket és alkalmazásokat is működtetni. Bár nem létezik olyan szervezet, amelyik szabályozná az internetet, mégis az azt alkotó sok különálló hálózat elfogadott szabványokat és protokollokat használ. A szabványok követése teszi lehetővé a hardver- és szoftvergyártó cégek számára, hogy csak valóban a szükséges termékfejlesztésre koncentráljanak a teljesítmény és kapacitás növelésének tekintetében. Ehhez előzetesen szükséges tudni azt, hogy a termékük biztosan integrálható lesz más termékekkel, vagy hogy a megoldásuk biztosan fokozza a meglévő hálózat tudását.
- A internet jelenlegi architektúrája annak ellenére, hogy igen jól méretezhető, nem mindig tud lépést tartani a felhasználói igényekkel. Új protokollok és címzési rendszerek állnak jelenleg is fejlesztés alatt, hogy ezek majd meg tudjanak felelni az internetes alkalmazások és szolgáltatások egyre bővülő körének.

Szolgáltatás minősége

A szolgáltatás minősége (QoS) ugyancsak egyre erősödő követelmény a jelenlegi hálózatokban. Egyre újabb hálózati alkalmazások állnak a felhasználók rendelkezésére, mint például az élő hang- és videóközvetítési szolgáltatások (lásd 1. ábra). Ezen új szolgáltatások egyben magasabb minőségi elvárásokat is támasztanak a szolgáltatások biztosítására. Próbáltál már úgy megnézni egy videót, hogy az állandóan akadozott vagy leállt?

A hálózatoknak kiszámítható, mérhető és szükség esetén garantált szolgáltatásokat kell biztosítaniuk. A csomagkapcsolt hálózati architektúra nem garantálja, hogy egy összefüggő üzenetet alkotó csomagok közül mindegyik időben, a helyes sorrendben megérkezik, vagy egyáltalán mindegyik megérkezik-e az adott célállomáshoz.

Szükséges, hogy a hálózatok tudják kezelni az esetleges torlódásokat a forgalomban. A hálózati sávszélesség az a mérőszám, amely jellemzi egy hálózat adatátviteli képességének a mennyiségét. Másképp fogalmazva: mennyi információt lehet továbbítani egy meghatározott idő alatt? A hálózati sávszélesség az egy másodperc alatt átvihető bitek számát adja meg, vagyis a mértékegysége a bit per másodperc (bps). Ha egyszerre több kommunikáció használja a hálózatot, akkor előfordulhat, hogy az összesített igény meghaladja a rendelkezésre álló hálózati sávszélességet, vagyis torlódás alakul ki. A hálózatnak egyszerűen több bitet kell ilyenkor továbbítania, mint amit a kommunikációs csatorna sávszélessége lehetővé tenne.

A legtöbb esetben, amikor a csomagok mennyisége nagyobb, mint amit a hálózat képes lenne kezelni, az eszközök a memóriába beolvasott csomagokat késleltetik, illetve sorba állítják azokat addig, míg újra elégséges források nem válnak elérhetővé a továbbításra (lásd 2. ábra). Ezek a sorban álló csomagok késedelmet okoznak, mert nem lehet addig új csomagot továbbítani, amíg a korábbi csomagok nem kerültek feldolgozásra. Ha a sorban álló csomagok száma folyamatosan növekszik, a memória egy idő után megtelik és az újonnan érkező csomagok eldobásra kerülnek.

A szükséges QoS értékek elérésében, vagyis a sikeres végponttól végpontig történő kommunikáció érdekében a késedelmeknek és a csomagvesztés mértékének a kezelése kulcsfontosságúvá válik. Ennek egyik módja az osztályokba sorolás (classification). Az adatok QoS osztályainak létrehozásához a kommunikáció jellegének és az adott alkalmazáshoz rendelt relatív fontosságnak kombinációját használhatjuk fel, ahogy ez a 3. ábrán is látható. Ezek után az egy osztályba sorolt

adatokat ugyanolyan szabályokat követve kell feldolgozni. Az időérzékeny kommunikáció (ilyen lehet a hangátvitel) például más osztályba kerül besorolásra, mint az a kommunikáció, amelyik jobban viseli a késleltetést (például fájlátvitel).

A prioritások felállításakor a következőkre érdemes figyelni:

- **Időérzékeny kommunikáció** - A kiemelt szolgáltatások prioritásának növelése (például hang vagy videó továbbítása esetén).
- **Nem időérzékeny kommunikáció** - Csökkentsük a prioritásokat olyan esetekben, mint a weboldalak böngészése vagy az e-mail kommunikáció.
- **Rendkívül fontos a szervezet részére** - Növeljük a prioritásokat a termelés szabályozásához, illetve az üzleti tranzakciókhoz szükséges forgalmak esetén.
- **Nemkívánatos kommunikáció** - Csökkentsük a prioritását a különböző kéretlen alkalmazásoknak, mint például a peer-to-peer fájlcserélő vagy valósidejű szórakoztató alkalmazások adatai.

Biztonság

Az internet egy szigorúan ellenőrzött oktatási és kormányzati szervezetek közti hálózatból egy széles körben elérhető üzleti és személyes kommunikációt is lehetővé tevő platformmá változott. Ennek eredményeképpen a hálózattal szemben támasztott biztonsági követelmények is megváltoztak. A hálózati infrastruktúra, a különböző szolgáltatások és a hálózatra csatlakoztatott eszközökön átmenő adatforgalom létfontosságúakká váltak a személyes és az üzleti világban. Ezek biztonságának veszélyeztetése komoly következményekkel járhat, mint például:

- Hálózati kiesések, amelyek megakadályozzák a kommunikációt és a tranzakciók végrehajtását, ezáltal üzleti kár keletkezik.
- Szellemi tulajdon (kutatási ötletek, szabadalmak, vagy tervezetek) eltulajdonítása, hogy majd a versenytársak visszaéljenek ezekkel a javakkal.
- Személyes vagy privát információk nyilvánosságra hozatala a felhasználó beleegyezése nélkül.
- A személyes, illetve az üzleti jellegű pénzügyi forgalmak megtévesztése vagy megkárosítása.
- A fontos adatok elvesztése, amelynek pótlása jelentős munkaerő igénybevételt jelentene, vagy akár pótolhatatlanná is válhat ez a veszteség.

Két típusú hálózati biztonsági probléma létezik, amelyekkel foglalkozni kell: a hálózati infrastruktúra biztonsága és az információbiztonság.

A hálózati infrastruktúra biztosítása magában foglalja a kapcsolatokért felelős eszközök fizikai biztonságának a megteremtését, valamint ezen eszközök felügyeleti szoftvereihez történő illetéktelen hozzáférés megakadályozását is.

Az információbiztonság azt jelenti, hogy szükséges védeni az adatokat tartalmazó csomagok továbbítását, valamint a különböző hálózati eszközökön történő tárolásukat is. A biztonsági intézkedéseknek magukban kell foglalniuk a következő biztonsági veszélyek megakadályozását:

- az információk illetéktelenül történő nyilvánosságra hozatalát,
- az információ eltulajdonítását (1. ábra),

- az illetéktelenül történő adatmódosítást,

- a szolgáltatás-megtagadási (Denial of Service, DoS) támadást.

Annak érdekében, hogy a hálózati biztonság terén kitűzött célokat elérjük, három elsődleges követelményt kell biztosítanunk (lásd 2. ábra):

- **Adatok bizalmas kezelése (confidentiality)** - Az adatok bizalmas kezelése azt jelenti, hogy csak a kívánt és felhatalmazott címzettek - egyének, folyamatok vagy eszközök - képesek elérni és olvasni az adatokat. Ez úgy érhető el, hogy egy erős felhasználói hitelesítést kell használni, vagyis nehezen kitalálható jelszavakat kell beállítani és gyakran kell azokat változtatni. Az adatok titkosítása is része azok bizalmas kezelésének, használatával valóban csak a címzett lesz képes elolvasni az adatokat.

- **A kommunikáció integritásnak megtartása** - Az adat integritásáról akkor beszélünk, ha biztosítani tudjuk, hogy az adatokat senki sem tudja módosítani a küldő és a célállomás közti átvitel során. Az adatok integritása veszélybe kerülhet, ha az információ - szándékosan vagy véletlenül - valahol megsérül. Az adatok integritása a küldő fél hitelesítésén és azokon a folyamatokon alapul, amelyekkel meg lehet bizonyosodni arról, hogy a kapott csomagokat nem változtatták meg az átvitel során.

- **Elérhetőség biztosítása** - Az elérhetőség azt jelenti, hogy biztosítjuk a jogosult felhasználók számára a naprakész és megbízható adathozzáférést. Hálózati tűzfal eszközök, valamint az asztali és szerveroldali víruskereső szoftverek biztosíthatják a rendszer megbízhatóságát az ilyen jellegű támadások felderítésével, kezelésével és kivédésével. Teljesen redundáns hálózati infrastruktúra kiépítésével csökkenthetjük ezeknek a veszélyeknek a hatásait.

Ha megnézzük, hogy az internet hogyan változtatott meg oly sok mindent napi elfoglaltságaink közül, nehéz elhinni, hogy mindez csak 20 éve kezdődött el. Az internet teljes mértékben átformálta kommunikációs szokásainkat, egyéni és szervezeti szinten is. Például mielőtt az internet annyira széles körben elérhető lett volna, a különböző szervezetek és kisvállalkozások nagymértékben támaszkodtak a nyomtatott marketingre, hogy a fogyasztókat megismertessék termékeikkel. Nehéz volt megállapítani a vállalkozások számára, hogy melyik háztartások voltak a potenciális vásárlók, így tömegesen kellett kinyomtatniuk marketing anyagaikat. Ez a fajta marketing drága és változó hatékonyságú volt. Hasonlítsuk össze ezt azzal, hogy hogyan érhetők el a fogyasztók a jelenben. A legtöbb vállalkozás rendelkezik valamilyen internetes jelenléttel, ahol a fogyasztók megismerhetik a termékeket, olvashatnak vásárlói véleményeket, és akár közvetlenül a weboldalon meg is rendelhetik a termékeket. A közösségi oldalak pedig együttműködnek a vállalkozásokkal a különböző termékek és szolgáltatások hirdetésében. A bloggerek ugyancsak partnerek a különböző termékekre és szolgáltatásokra történő figyelemfelhívásban, azok értékelésében. A legtöbb ilyen termékelhelyezés kifejezetten a potenciális fogyasztók számára történik, ahelyett hogy a tömegeket célozna meg. Az 1. ábrán néhány jóslat látható az internet közeljövőjéről.

Mivel folyamatosan új technológiák és felhasználói készülékek lépnek a piacra, ezért a vállalkozásoknak és a fogyasztóknak is állandóan alkalmazkodniuk kell a mindig változó környezethez. A hálózat szerepének megváltozása teszi lehetővé az emberek, az eszközök és az információ összekapcsolását. Számos olyan új hálózati trend bontakozik ki, amely hatással lesz a szervezetekre és a fogyasztókra. Néhány a legismertebb trendek közül:

- minden eszközhöz, minden tartalomhoz és mindenhogy csatlakozhatunk,

- online csoportmunka,

- videó,

- felhő alapú számítástechnika (Cloud computing),

Ezek a trendek összefüggésben állnak egymással, és a következő években tovább erősítik majd egymást, vagy hoznak létre új trendeket. A következő néhány téma ezeket az új tendenciákat részletesebben is tárgyalja.

De ne felejtsük el, hogy új trendek minden nap megálmodásra és megvalósításra kerülnek a mai világban. Mit gondolsz, az internet mennyit fog változni a következő 10 évben? És 20 év múlva? A 2. ábrán egy videó látható a Cisco elképzelt jövőbeni fejlesztéseiről.

Bring Your Own Device (Hozd a saját eszközödet)

A "minden eszközhöz, minden tartalomhoz és mindenhogy csatlakozhatunk" koncepció egy fontos globális trend, amely jelentős változásokat követel meg abban, ahogy az eszközeinket használjuk. Ez a trend az úgynevezett "Hozd a saját eszközödet" (Bring Your Own Device, BYOD).

A BYOD lehetővé teszi a felhasználók számára, hogy akár a saját privát eszközeik használatával érjenek el információkat, vagy kommunikáljanak másokkal egy szervezet hálózatán belül. A fogyasztói eszközök számának növekedésével és az ehhez kapcsolódó költségek csökkenésével várható, hogy a munkavállalók és a diákok személyesen is rendelkezni fognak a legmodernebb számítástechnikai és hálózati eszközökkel. Ezen személyes eszközök közé tartoznak a laptopok, netbookok, tabletek, okostelefonok, és az ebook-olvasók. Ezeket az eszközöket vagy egy cég illetve iskola, vagy maga az egyén fogja megvásárolni, de akár közösen is megvehetik.

A BYOD minden olyan eszközt jelent, amelynek bárki lehet a tulajdonosa és bárhol lehet használni azokat. Például a múltban, amikor egy diák kapcsolódni szeretett volna az iskolai hálózathoz vagy az internetre, akkor azt csak az iskola számítógépével tudta megtenni. Ezek az eszközök jellemzően korlátozottak voltak valamilyen módon, és csak egy tantermi vagy könyvtári munkaeszközként tekintettek rájuk. Az iskolai hálózathoz történő kibővült - mobil vagy távoli - hozzáférés óriási rugalmasságot tett lehetővé a diákok számára, és egyben több tanulási lehetőséget is biztosított számukra.

A BYOD egy sok mindenre befolyással lévő trend, amely a jelenben vagy a jövőben miden informatikai szervezetet érint.

Online csoportmunka

A magánszemélyek nem csak azért szeretnének a hálózathoz csatlakozni, hogy hozzáférhessenek adatokhoz, hanem azért is, hogy képesek legyenek egymással együttműködni. Az együttműködés meghatározása szerint: "az a folyamat, amikor mással vagy másokkal egy közös projekten dolgozunk."

Az együttműködés (más néven csoportmunka) a vállalkozások számára kritikus és stratégiai fontosságú. Hogy a szervezetek versenyképesek maradjanak, három fő együttműködési kérdést kell megválaszolniuk:

- Hogyan érhető el, hogy mindenki jelen legyen?
- Csökkenő költségvetés és kisegítő személyzet mellett hogyan lehet kialakítani az erőforrások egyenlő elosztását egyszerre akár több helyszínen is?
- Hogyan lehet fenntartani a közvetlen és személyes kapcsolatot a kollégák, ügyfelek és partnerek egyre növekvő hálózatával, amelyek egyre inkább igénylik a napi 24 órás elérhetőséget?

Az oktatásban szintén fontos az együttműködés. A diákoknak együtt kell működniük, hogy segítsék egymást a tanulásban, hogy kifejlesszenek közösségi képességeket a munkavégzéshez, és hogy közreműködjenek egymással a csapatos projektek során.

Az online csoportmunka eszközök használata egy lehetséges módja annak, hogy mindezekre a kérdésekre a jelenlegi környezetben kielégítő választ találjunk. Hagyományos munkahelyeken vagy akár BYOD környezetben is, a hang- és videokonferencia szolgáltatások használhatók együttműködésre.

Az online együttműködés képességével változnak az üzleti folyamatok is. Az új és fejlődő csoportmunka eszközök lehetővé teszik az egyén számára, hogy gyorsan és egyszerűen, függetlenül a fizikai elhelyezkedéstől képes legyen együtt dolgozni valaki mással. A szervezetek egyre jobban rugalmassá fognak válni. Az egyéneket nem korlátozza többé a fizikai elhelyezkedésük. A szakértői tudás könnyebben elérhetővé válik, mint valaha. Az együttműködés kibővülése lehetővé teszi a szervezetek számára, hogy javuljon az információszerzés, az innováció és a termelékenység. Az ábra az online együttműködésből származó néhány előnyt sorol fel.

A csoportmunka eszközök által a munkavállalók, diákok, tanárok, ügyfelek és a partnerek képessé válnak az azonnali kapcsolatfelvételre, együttműködésre, üzleti tevékenység folytatására, valamint céljaik elérésére - bármilyen kommunikációs csatornát is részesítsenek előnyben.

Videó kommunikáció

A videó használata egy másik hálózati trend, amely kritikus a kommunikáció és az együttműködés területén. Videót használunk kommunikációra, együttműködésre és szórakozásra is. A videohívások egyre népszerűbbek, mert elősegítik a kommunikációt a humán hálózatokban. Egy internetkapcsolat segítségével bárhonnan lehet videohívást kezdeményezni és fogadni is, akár otthonról vagy akár a munkahelyről is.

A videohívások és videokonferencia használata különösen hasznos az értékesítési és az üzleti folyamatokban. A videó egy hasznos eszköz, legyen szó helyi vagy globális szintű üzleti folyamatról. Manapság az üzleti vállalkozások videót használnak, hogy átalakítsák üzleti tevékenységüket. A videó versenyelőnyt biztosít a vállalkozásoknak, csökkenti a költségeket, és a kevesebb utazás révén csökkenti a környezetre gyakorolt hatást is. Az 1. ábra a videó kommunikáció trendjét mutatja be.

Mind a fogyasztók, mind a vállalkozások meghatározóak ezekben a változásokban. A videó kulcsfontosságú tényezővé vált a hatékony együttműködés tekintetében, mert a vállalatok gyakran terjeszkednek ország- vagy kulturális határokon keresztül. A videó felhasználók megnövelik azt az igényt, hogy bármilyen eszközről bármikor képesek legyünk csatlakozni.

A vállalkozások úgyszintén felismerték a videó szerepét a humán hálózatban. A különböző médiák térnyerése és azok új felhasználói teremtik meg az igényt, hogy a hangot és a videót együttesen lehessen használni a kommunikáció különböző formáiban. Az audiokonferencia a legtöbb esetben ki fog egészülni a videokonferenciával. A csoportmunka eszközök célja, hogy a videókapcsolat révén közelebb hozza egymáshoz a földrajzilag szétszórt munkavállalókat.

Számos előny, többek között stratégiai előnyök is származnak a videó használatából. Minden szervezet egyedi. A videó felhasználásának mértéke és annak jellege szervezetenként és üzleti funkciónként változó. A marketing például a globalizációra és gyorsan változó fogyasztói ízlésre fókuszál, míg az informatikai igazgató (Chief Information Officer, CIO) számára az utazási költségek csökkentése és a költséghatékonyság a fő szempont. A 2. ábrán láthatunk néhány olyan tényezőt, amelyek elősegítik egy szervezet videóhasználati stratégiájának kialakítását és megvalósítását.

A 3. ábrán egy videót láthatunk, amely betekintést nyújt abba, hogy a TelePresence videó megoldás hogyan válhat a hétköznapi élet és vállalkozások részévé.

Egy másik trend a digitális videótár (video-on-demand) és az élő videóközvetítések (streaming video). A hálózaton keresztüli videoszolgáltatások lehetővé teszik, hogy bárhonnan és bármikor nézhessünk meg mozifilmeket vagy televíziós műsorokat.

Felhő alapú szolgáltatások

A felhő alapú szolgáltatások (cloud computing) használatával a hálózaton keresztül szolgáltatásként vehetünk igénybe számítógépes hardver- és szoftvererőforrásokat. Egy vállalat szolgáltatási díj ellenében használhatja a felhőben lévő hardver- és a szoftvererőforrásokat.

A helyi számítógépeknek már nem kell a saját erőforrásaikat használniuk, amikor valamilyen hálózati alkalmazást futtatnak. Ezeket a feladatokat a felhő, vagyis hálózatba kötött számítógépek sokasága fogja ellátni. Ezáltal a felhasználói oldali hardver-és szoftver követelmények csökkenek. A felhasználó számítógépének valahogy el kell érnie a felhőt - például egy webböngésző segítségével -, minden más tevékenységet pedig már a felhő végez.

A felhő alapú szolgáltatások terjedése egy másik globális trend, amely megváltoztatja az adatainkhoz való hozzáférési és tárolási szokásainkat. A valós idejű, internetes felhő alapú szolgáltatások lehetnek előfizetésen alapulók vagy alkalmanként fizetendők. A felhő alapú szolgáltatások lehetővé teszik, hogy személyes fájlokat vagy éppen egész merevlemezünk biztonsági másolatát tároljuk interneten lévő távoli szervereken. Alkalmazások, mint például a szövegszerkesztő és képszerkesztő is elérhetők a felhőn keresztül.

A felhő megnöveli a vállalkozások informatikai lehetőségeit anélkül, hogy új infrastruktúrába kellene beruházni, új embereket kellene kiképezni, vagy éppen új szoftverlicenceket vásárolni. Ezek a szolgáltatások igény szerint elérhetők és a biztonság vagy a funkció veszélyeztetése nélkül gazdaságosan juttathatók el bármely eszközre a világon.

A "felhő alapú szolgáltatások" kifejezés valójában a web-alapú szolgáltatásokra utal. Az online banki szolgáltatások, az online kiskereskedelmi boltok és az online zeneletöltés mind példák a felhő alapú szolgáltatásokra. Ezek a szolgáltatások legtöbbször egy webböngészőn keresztül érhetők el. A felhasználóknak nem kell semmilyen más szoftvert telepíteniük a saját eszközükre. Ez számos különböző típusú eszköz felhőhöz csatlakozását teszi lehetővé.

A felhő alapú szolgáltatások a következő előnyöket nyújthatják:

- **Szervezeti rugalmasság** - A felhasználók egy webböngésző segítségével bármikor és bárhonnan hozzáférhetnek az információkhoz.

- **Agilitás és gyors megvalósítás** - A gyors megvalósítás mellett az informatikai részleg olyan eszközök kifejlesztésére is összpontosíthat, amelyek által az adatbázisokból, a fájlokból vagy a felhasználói tevékenységekből kinyerhető adatok és tudás könnyebben értékelhetőbbé, elemezhetőbbé és megoszthatóbbá válik.

- **Kisebb infrastruktúra költségek** - A technológia átkerül a felhasználói helyszínről a felhőbe, ezáltal csökken a helyi hardverhez és szoftverhez társítható költségigény.

- **Az IT-erőforrások átcsoportosítása** - A hardver és szoftver jellegű költségmegtakarítást máshol fel lehet használni.

- **Új üzleti modellek létrehozása** - Az alkalmazások és erőforrások könnyebben elérhetővé válnak, így a vállalatok gyorsabban tudnak reagálni az ügyfelek igényeire. Ez segíthet új innovatív stratégiák felállításában, vagy új potenciális piacokra való belépésben.

Jelenleg négy fő típusát különítjük el a felhőknek, ahogy ez a 2. ábrán is látható. Több részletért kattintsunk az egyes felhőkre!

A felhő alapú szolgáltatások terjedése az adatközpontok miatt vált lehetségessé. Az adatközpont egy olyan létesítmény, amely fogadja a számítógépes rendszereket és a következő kapcsolódó elemeket:

- Redundáns adatkommunikációs kapcsolatok

- Nagy sebességű virtuális szerverek (néha ezt szerverfarmoknak, vagy szerver-klaszthereknek hívják)
- Redundáns tárolórendszerek (általában SAN technológiát használnak)
- Redundáns vagy tartalék tápegységek
- Környezeti hatások elleni védelem (pl. klíma, tűzoltó rendszer)
- Biztonsági berendezések

Egy adatközpont lehet egy szoba méretű, de elfoglalhat egy vagy több emeletet is, vagy akár egy egész épületet. A modern adatközpontok teszik lehetővé, hogy a számítási felhő és a virtualizáció akár nagy méretű és tömeges adatátvitelt is hatékonyan tudjon kezelni. A virtualizáció valamilyen erőforrás virtuális változatának a létrehozását jelenti, ami lehet egy hardver platform, operációs rendszer (OS), tárolóeszköz, vagy akár hálózati erőforrás is. Míg a fizikai számítógép egy valóságos és jól körülhatárolható eszköz, addig egy virtuális gép egy fizikai gépen tárolt néhány fájlból és futó programból áll. A többfeladatúsággal (multitasking) ellentétben, itt nem egy operációs rendszeren futó több alkalmazásról van szó, hanem a virtualizáció által egy CPU akár egyszerre több operációs rendszert is képes futtatni párhuzamosan. Ez drasztikusan csökkenti az adminisztratív feladatokat és a különböző költségráfordításokat is.

Az adatközpontokat általában nagyon drága felépíteni és fenntartani. Emiatt csak a nagy szervezetek tehetik meg, hogy saját adatközpontot építsenek és nyújtsanak általuk szolgáltatásokat a felhasználóik számára. Például egy nagy kórház rendelkezhet egy saját adatközponttal, amelyen az elektronikus betegnyilvántartási rendszere fut. A kisebb szervezetek, amelyek nem engedhetik meg maguknak a saját adatközpontot, egy nagyobb adatközponttól vesznek bérbe szerver és tárolási szolgáltatásokat.

A mellékelt képen egy videó látható a számítási felhő és az adatközponti szolgáltatások növekvő használatáról.

A hálózati trendek nemcsak a munkahelyi vagy iskolai kommunikációnkat befolyásolják, hanem kifejtik hatásukat szinte az összes otthoni tevékenységünkre is.

A legújabb ilyen otthoni tendencia az "intelligens otthoni technológia". Az intelligens otthon technológiája egy olyan technológia, amely beépül a nap mint nap használt készülékeinkbe, lehetővé téve, hogy azok más eszközökkel kapcsolódjanak össze, ezáltal "intelligensebbé" vagy automatizáltabbá téve azokat. Képzeljük el, hogy lehetővé válik az, hogy csak előkészítjük az ételt egy sütőre tett tálba és elhagyjuk otthonunkat egy teljes napra. Képzeljük el, hogy ez a sütő képes "tudomást venni" a belehelyezett ételről, és össze van kapcsolva a naptárunkkal is, így képes megállapítani a sütés kezdetét és időtartamát, hogy érkezésünkkor az ételt frissen elkészülve fogyaszthassuk el. Még a sütési időt és a hőfokot is hozzá tudja igazítani naptárunk váratlan változásaihoz. További lehetőség, hogy egy okostelefon vagy egy tablet segítségével közvetlen módon kapcsolódjunk a tűzhelyhez és elvégezzük rajta a kívánt beállításokat. Ha az étel fogyasztásra kész, a tűzhely egy figyelmeztető üzenetet küldhet egy meghatározott készülékünkre, hogy az étel elkészült és még meleg.

Ez a kis történet még folytatható. Valójában az intelligens otthoni technológia jelenleg az otthonunk valamennyi helységére kifejlesztés alatt áll. Az intelligens otthoni technológiák egyre inkább valósággá válnak, amint a hálózatok és a nagy sebességű internet technológiák egyre inkább elterjednek az otthonokban is. Napról-napra új otthoni hálózati technológiákat fejlesztenek ki, hogy kiszolgálják az egyre növekvő igényeket.

Az elektromos hálózatot használó adathálózat (powerline network) egy új trend az otthoni hálózatok számára, amely a már meglévő elektromos kábelezést használja az eszközök összeköttetésére, ahogy ezt az ábra is mutatja. A "nincs új vezeték" koncepció azt jelenti, hogy az eszközöket bárhol a hálózatra lehet csatlakoztatni, ahol van egy elektromos falicsatlakozó. Ez csökkenti a kábelek

telepítési költségét, és nem növeli meg a felhasználó elektromos számláját sem. Az adatkommunikáció és az áramellátás ugyanazt a vezetéket használja, csak a powerline hálózat az adatokat más frekvencián küldi, hasonlóan, mint ahogy azt a DSL-hálózatok teszik.

Egy szabványos HomePlug powerline adaptert használva eszközeinket egy elektromos falicsatlakozón keresztül csatlakoztathatjuk a LAN hálózatra. A powerline hálózat különösen akkor hasznos, ha a vezeték nélküli hozzáférési pontok nem használhatóak, vagy nem tudjuk megoldani a kábelezést a házban. A powerline hálózatot nem arra tervezték, hogy egy dedikált adathálózati kábelezést helyettesítsen. Ugyanakkor ez egy alternatíva, amennyiben a hagyományos kábelezés, vagy a vezeték nélküli kommunikáció nem járható megoldás.

Az internetre csatlakozás létfontosságú az intelligens otthoni technológia esetén. A DSL és a kábeles internetelérés általánosan alkalmazott technológiák az otthonok és kis vállalatok csatlakoztatására. Ugyanakkor számos helyen a vezeték nélküli hozzáférés is egy lehetőség.

Vezeték nélküli internetszolgáltató

A vezeték nélküli internetszolgáltató (Wireless Internet Service Provider, WISP) egy olyan szolgáltató, amely az otthoni WLAN hálózatokhoz hasonló technológiát alkalmazva csatlakoztatja az előfizetőket egy kijelölt hozzáférési ponthoz vagy hot spot-hoz. A WISP-ek gyakrabban találhatók olyan vidéki helyeken, ahol a DSL vagy kábeles szolgáltatások nem állnak rendelkezésre.

Habár külön adótornyot is lehet az antenna számára telepíteni, mégis gyakori, hogy az antenna egy már meglévő magas szerkezetre csatlakozik, mint például egy víztorony vagy egy rádiótorony. A WISP adóállomásának hatókörében az előfizetők házának a tetejére egy kis parabola vagy egy másik típusú antennát kell telepíteni. Az előfizető hozzáférését biztosító eszköz a házon belüli vezetékes hálózatra csatlakozik. Az otthoni felhasználó szemszögéből ennek a megoldásnak a telepítése nem sokban különbözik a DSL vagy kábeles szolgáltatásétól. A legfőbb különbség, hogy az előfizető és az ISP közötti kapcsolat a fizikai kábel helyett vezeték nélküli átvitellel van megoldva.

A vezeték nélküli szélessávú szolgáltatás

Az otthoni és kisvállalkozások számára egy másik vezeték nélküli megoldás a vezeték nélküli szélessávú hozzáférés. Ez ugyanazt a mobil technológiát használja az internet elérésre, mint egy okostelefon vagy egy tablet. A házon kívül egy antenna kerül telepítésre, amely a házon belüli eszközöknek vezeték nélküli vagy akár vezetékes csatlakozást is biztosíthat. Számos helyen az otthoni vezeték nélküli szélessávú elérés egyenesen a DSL vagy a kábeles szolgáltatásokkal versenyez.

A hálózati biztonság szerves része a számítógépes hálózatoknak, függetlenül attól, hogy csak egy otthoni környezetben lévő hálózatról és egyetlen internet kapcsolatról, vagy egy nagyvállalati, több ezer felhasználós hálózatról van szó. A megvalósított hálózati biztonsági rendszernek figyelembe kell venni az adott környezetet, valamint a hálózati eszközöket és számos egyéb követelményt is. Képesnek kell lennie megvédenie az adatokat, miközben továbbra is biztosítania kell az elvárt szolgáltatási minőséget.

A hálózat biztonságossá tétele és a fenyegetések kivédése speciális protokollok, technológiák, eszközök és technikák használatával érhető el. Napjainkban számos külső hálózati biztonsági fenyegetés terjed az interneten keresztül. A leggyakoribb külső hálózati fenyegetések a következők:

- **Vírusok, férgek és trójai lovak** - rosszindulatú szoftverek vagy bármilyen kód elemek, amelyek egy felhasználói eszközön futnak.

- **Kémprogram- és reklámprogram (spyware és adware)** - egy olyan telepített szoftver a felhasználó eszközén, amely titokban információkat gyűjt a felhasználóról.

- **Nulladik napi támadások, más néven nulladik órás támadások** - a sebezhetőség felfedezésének első napján történő támadások.

- **Hacker támadások** - egy hozzáértő személy által elindított támadás egy eszköz, vagy hálózati erőforrás ellen.

- **Szolgáltatásmegtagadási támadások (Denial of Service, DoS)**- a támadások célja, hogy lelassítsanak, vagy elérhetetlenné tegyenek hálózati eszközön futó alkalmazásokat és folyamatokat.

- **Adatlehallgatás és a lopás** - egy támadás, amelynek célja, hogy egy szervezet hálózatáról személyes információkhoz férjenek hozzá.

- **Személyazonosság-lopás** - egy támadás, amely a személyes adatainkhoz használt felhasználói belépési azonosítók ellopására irányul.

Ugyanilyen fontos, hogy figyelembe vegyük a belső fenyegetéseket is. Számos tanulmány kimutatta, hogy az adatokkal történő visszaélések leggyakrabban a hálózat belső felhasználói miatt történnek. Ez az elvesztett vagy ellopott eszközöknek, az alkalmazottak véletlen visszaélésének, vagy üzleti környezetben akár még a rosszindulatú alkalmazottaknak is tulajdonítható. Az elterjedő BYOD stratégiák miatt a vállalati adatok sokkal sérülékenyebbé válnak. Ezért egy biztonsági házirend kialakításakor egyformán kell figyelembe venni a külső és belső biztonsági fenyegetéseket is.

Egyetlen megoldás nem képes megvédeni a hálózatot a különböző fenyegetésektől. A biztonságot emiatt több rétegben, több biztonsági megoldást is alkalmazva kell megvalósítani. Ha az egyik biztonsági összetevő nem azonosítja a támadást, vagy nem tudja megvédeni attól a hálózatot, akkor még mindig ott van egy másik összetevő is.

Az otthoni hálózatbiztonsági rendszerek általában meglehetősen egyszerűek. Gyakran a csatlakozó számítógépen és az internetes összeköttetést biztosító eszközön történik meg a védekezés, valamint az ISP is biztosíthat szerződéses védelmi szolgáltatásokat.

Ezzel szemben nagyvállalati környezetben a hálózati biztonság megvalósítása több elemből tevődik össze, amelyek folyamatosan figyelik és szűrik a forgalmat. Ideális esetben minden összetevő együttműködik, ami minimálisra csökkenti a karbantartási feladatokat és növeli a biztonságot.

Egy otthoni vagy kisvállalati hálózatban minimum a következő biztonsági elemeknek kell jelen lenniük:

- **Vírus-és kémprogramvédelem** - a felhasználói eszközök rosszindulatú szoftverekkel szembeni védelme érdekében.

- **Tűzfal szűrés** - hogy blokkolja a jogosulatlan hozzáférést a hálózathoz. Ez lehet egy munkaállomás alapú tűzfalrendszer, amely megakadályozza a jogosulatlan hozzáférést a munkaállomáshoz, vagy ugyanígy az otthoni forgalomirányító is képes lehet megakadályozni alapvető szűrési beállításokkal a külvilág irányából a belső hálózathoz történő jogosulatlan hozzáférést.

A fent említettek mellett, nagyobb hálózatoknak és a vállalati hálózatoknak gyakran más biztonsági követelményeik vannak:

- **Dedikált tűzfalrendszerek** - hogy a fejlettebb tűzfal képességek miatt az eszköz képes legyen akár jelentős mértékű forgalom mellett is részletesebb szűréseket végezni.

- **Hozzáférés-szabályozó listák (ACL)**- szűrési feltételek a hozzáférésről és a forgalom továbbításáról.

- **Behatolás-megelőző rendszerek (IPS)** - azonosítani olyan gyorsan terjedő fenyegetéseket, mint például a nulladik napi vagy nulladik órás támadások.

- **Virtuális magánhálózatok (Virtual private networks, VPN)** - biztonságos hozzáférés kialakítása a távoli dolgozók részére.

A hálózati biztonsági követelményeknek figyelembe kell venniük a hálózati környezetet, valamint a különféle alkalmazásokat és informatikai követelményeket. Mind az otthoni, mind pedig az üzleti környezeteknek képeseknek kell lenni megvédenie az adatokat, miközben továbbra is biztosítani kell minden technológia számára az elvárt szolgáltatási minőséget. Emellett a megvalósított biztonsági megoldásnak illeszkednie kell a folyamatosan növekvő és változó hálózati trendekhez.

A hálózati szolgáltatások rendszerezéséhez a hálózatbiztonsági fenyegetésekről és a védekezésről szóló tanulmányoknak a hálózat kapcsolási és forgalomirányítási infrastruktúrájának tiszta megértésével kell kezdődni.

A hálózat szerepe az idők során átalakult. Kizárólag adatátviteli hálózatból egy olyan multimédiás, konvergált hálózati környezetté változott, amely lehetővé teszi a kapcsolatot az emberek, az eszközök és a különböző információk között. Hogy a hálózatok hatékonyan működhessenek és növekedhessenek egy ilyen típusú környezetben, ahhoz az egész hálózatot egy szabványos hálózati architektúra alapján kell kiépíteni.

A hálózati architektúra azokra az eszközökre, kapcsolatokra és termékekre utal, amelyek integrációja lehetővé teszi a szükséges technológiák és alkalmazások támogatását. Egy jól megtervezett hálózati architektúra segít biztosítani a különböző eszközök kapcsolódását hálózatok különböző kombinációján keresztül is. A csatlakoztathatóság biztosítása a hálózati biztonság és menedzsment integrációjával a költséghatékonyságot is növeli, amely legvégül az üzleti folyamatokat is javítja. Minden hálózati architektúra alapja, sőt, valójában az egész internet alapja a forgalomirányítók (router) és kapcsolók (switch) hálózata. A forgalomirányítók és kapcsolók szállítják az adat-, hang- és videokommunikációt, biztosítják a vezeték nélküli hozzáférést és gondoskodnak a biztonságról is.

Ha olyan hálózatokat akarunk építeni, amelyek megfelelnek a mai kor igényeinek, valamint a jövőbeli igényeknek is, akkor ez a hálózatokat felépítő kapcsolási és útválasztási infrastruktúra pontos megértésével kezdődik. Miután az alapot biztosító irányítási és kapcsolási infrastruktúra kiépült, az egyének, kisvállalkozások és szervezetek idővel elkezdhetik saját hálózatuk fejlesztését, mindezt további integrált funkciók és szolgáltatások hozzáadásával.

Ahogy egyre több ilyen integrált és folyamatosan bővülő hálózat kezd kialakulni, úgy válik egyre inkább szükségessé azon személyek képzése, akik ezeket a hálózatokat kialakítják és üzemeltetik. Ennek a képzésnek a forgalomirányítás és a kapcsolás alapjaival kell kezdődnie. A Cisco Certified Network Associate (CCNA) minősítés megszerzése az első lépés a hálózati karrier felé vezető úton.

A CCNA minősítés igazolja, hogy valaki képes közepes méretű LAN és WAN hálózatokat telepíteni, konfigurálni, üzemeltetni és a hibakeresést elvégezni. A CCNA tananyag kitér az alapvető biztonsági fenyegetések elleni védelemre, a vezeték nélküli hálózati fogalmak megismerésére, valamint a teljesítmény-alapú készségek fejlesztésére is. A CCNA tananyag tartalmazza a legfontosabb protokollok megismerését, mint az IP, az Open Shortest Path First (OSPF), a Serial Line Interface Protocol, a Frame Relay, a VLAN, az Ethernet, a hozzáférés-szabályozó listák (ACL-ek) és még számos másét is.

Ez a kurzus segít a hálózati koncepciók megértésében, az alapvető forgalomirányítási és kapcsolási konfigurációk megismerésében, valamint a CCNA minősítésre való felkészülésben.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Állásajánlatok keresése.
- 2. rész: A keresés tapasztalatainak megbeszélése.

Laborgyakorlat - Researching IT and Networking Job Opportunities

Rajzoljuk le újra az internetet!

Ebben a feladatban a fejezet elején elkezdett modellezési feladatunk eredményeit egészíthetjük ki azzal a tudással, amit a fejezet során megszereztünk. A feladat elvégzéséhez felhasználhatók a korábban teljesített Packet Tracer és egyéb feladatok.

Rajzoljuk le az internet térképét úgy, ahogy azt most a fejezet végén látjuk! Használjuk a fejezetben bemutatott ikonokat az átviteli közeg, a végberendezések és továbbító eszközök megjelenítésére!

Ebben a módosított rajzban érdemes feltüntetni a következőket is:

- WAN-ok,
- LAN-ok,
- felhő alapú szolgáltatások (Cloud computing),
- internetszolgáltatók (több szintben).

Mentsük el a rajzot nyomtatott formátumban is! Ha pedig ez egy elektronikus dokumentum, mentsük el az oktató által meghatározott helyre! Álljunk készen az osztályon belül megosztani és elmagyarázni a munkánkat!

Csoportos feladat - Utasítások a Rajzoljuk le újra az Internetet! feladathoz

A hálózatok és az internet megváltoztatta azt, ahogy tanulunk, ahogy kommunikálunk, ahogy dolgozunk, de még azt is, ahogy játszunk.

A legkülönbözőbb méretű hálózatok léteznek. A méretük az egyszerű, két számítógépes hálózattól egészen a több millió eszközt tartalmazó hálózatokig terjed.

Az internet a legnagyobb létező hálózat. Valójában az internet jelentése a "hálózatok hálózata". Az internet biztosítja azokat a szolgáltatásokat, amelyek lehetővé teszik szánunkra, hogy kapcsolatba lépjünk és kommunikáljunk a családtagjainkkal, a barátainkkal, a munkahelyünkkel vagy az érdeklődési körünkbe tartozókkal.

A hálózati infrastruktúra biztosítja a mindennapjaink során használt hálózati kommunikációt. Ez teremti meg azt a stabil és megbízható csatornát, amelyen mindennapjaink kommunikációja folyhat. Ez olyan összetevőkből áll, mint a végberendezések, a közvetítő eszközök és az átviteli közeg.

A hálózatoknak megbízhatónak kell lenniük. Ez azt jelenti, hogy a hálózatnak hibatűrőnek és skálázhatónak kell lenni, biztosítania kell a szolgáltatások minőségét, valamint az információ és az erőforrások védelmét. A hálózati biztonság szerves része a számítógépes hálózatoknak, függetlenül attól, hogy csak egy otthoni környezetben lévő hálózatról és egyetlen internetkapcsolatról, vagy egy nagyvállalati, több ezer felhasználós hálózatról van szó. Egyetlen megoldás nem képes megvédeni a hálózatot a különböző fenyegetésektől. A biztonságot emiatt több rétegben, több biztonsági megoldást is alkalmazva kell megvalósítani.

A hálózati infrastruktúrák nagyban eltérnek egymástól a nagyság, a felhasználók száma, a támogatott szolgáltatások típusa és mennyisége tekintetében. A hálózati infrastruktúrának az új felhasználási igényeknek megfelelően kell nőnie és alkalmazkodnia azokhoz. A forgalomirányítás és kapcsolás az a közös platform, amely minden hálózati infrastruktúra alapja.

Ez a fejezet a hálózatokra, mint elsődleges kommunikációs platformra összpontosított. A következő fejezet bemutatja a Cisco Internet Operating System (IOS) operációs rendszert, amely lehetővé teszi a forgalomirányítást és kapcsolást a Cisco hálózati környezetben.

Az otthoni hálózatok végberendezések széles skáláját kötik össze, ide értve a PC-ket, laptopokat, tableteket, okostelefonokat, okostévéket, és a hálózati játékkonzolakat, mint például az Xbox 360 vagy a PlayStation 3.

Ezen végberendezések rendszerint egy otthoni forgalomirányítóhoz kapcsolódnak, mely valójában négy egybeépített eszközt takar:

- **Forgalomirányító -** Adatcsomagokat továbbít az internet felé és fogad onnan.
- **Kapcsoló -** Összeköti a vezetékes hálózat végberendezéseit.
- **Vezeték nélküli hozzáférési pont -**Rádióhullámú adó-vevő, mely a végberendezéseket vezeték nélkül köti össze.
- **Tűzfal -** Biztosítja a kimenő és korlátozza a bejövő forgalmat.

A több eszközt tartalmazó és jelentősen nagyobb forgalommal rendelkező vállalati hálózatok esetén ezeket a funkciókat különálló berendezések dedikált szolgáltatásai látják el. A végberendezések, mint például a PC-k és a laptopok, vezetéken csatlakoznak a hálózati kapcsolókhoz. A helyi hálózaton kívülre küldött csomagok továbbítása érdekében a kapcsolókat forgalomirányítókhoz csatlakoztatják. A hálózati infrastruktúra további eszközei a vezeték nélküli hozzáférési pontok és a dedikált biztonsági berendezések, például a tűzfalak.

A berendezések nagyon különböznek fizikai felépítésükben, felhasználási módjukban és képességeikben. Azonosok viszont abban, hogy az operációs rendszer az, ami működésre bírja az őket alkotó hardvert.

Gyakorlatilag minden internetre csatlakoztatott végberendezést és hálózati eszközt operációs rendszer működtet. A végfelhasználói berendezések közé tartoznak az okostelefonok, tabletek, PC-k és laptopok. A hálózati, más néven közvetítő eszközök az adattovábbítást szolgálják. Ide tartoznak a kapcsolók, a forgalomirányítók, a vezeték nélküli elérési pontok és a tűzfalak. A hálózati eszközökön futó operációs rendszert hálózati operációs rendszernek nevezik.

A Cisco hálózati eszközökön használt operációs rendszerek összefoglaló neve Cisco IOS (Internetwork Operating System). Cisco IOS fut a legtöbb Cisco eszközön tekintet nélkül annak típusára vagy méretére.

Ebben a fejezetben egy két kapcsolóból és két PC-ből összeállított alap topológia segítségével ismerkedhetünk meg a Cisco IOS működésével.

Ez is csak egy operációs rendszer

Ebben a feladatban képzeljük magunkat egy autógyár mérnökének. A vállalat egy új modell fejlesztésén dolgozik, melynek néhány kiválasztott funkcióját a vezető hangjával kívánja vezérelni.

Tervezzük meg a hangvezérlő rendszer parancsait és határozzuk meg működésüket! Az autó hangvezérléssel irányítani kívánt funkciói:

- lámpák
- ablaktörlők
- rádió
- mobiltelefon

- klímaberendezés
- gyújtás

Csoportos feladat - It Is Just an Operating System Instructions

Mind a végberendezések, mind pedig a hálózati eszközök operációs rendszer segítségével hajtják végre feladataikat.

A számítógép bekapcsolása után történik az operációs rendszer betöltése, általában valamely lemezmeghajtóról a RAM-ba. Az operációs rendszer kódjának a számítógépes hardverrel közvetlenül kommunikáló része a rendszermag. Az operációs rendszert az alkalmazásokkal és a felhasználóval összekapcsoló része a parancsértelmező. A felhasználó a parancssoron (Command Line Interface, CLI) vagy a grafikus kezelőfelületen (Graphical User Interface, GUI) keresztül kommunikálhat a parancsértelmezővel.

A parancssor használata során a felhasználó karakteres környezetben kiadott utasításokkal közvetlenül a rendszerrel kommunikál. A rendszer végrehajtja a parancsot, amelynek végeredményéről általában szöveges üzenetet ad. A grafikus kezelőfelület lehetővé teszi a felhasználó számára, hogy egy grafikus, multimédiás és szöveges elemeket egyaránt használó környezetben kommunikáljon a rendszerrel. A műveletek elvégzése a képernyő grafikus elemeivel lehetséges. A grafikus kezelőfelület felhasználóbarátabb a parancssornál, és a rendszer használata is kevesebb tudást igényel. Ebből kifolyólag meglehetősen sokan használják a grafikus kezelőfelületet. A legtöbb operációs rendszer rendelkezik mind parancssorral, mind grafikus felülettel.

Bővebb információért kattintsunk az ábrán a hardver, kernel (rendszermag) és a shell (parancsértelmező) részekre!

A végberendezések leggyakoribb operációs rendszerei grafikus felhasználói felülettel rendelkeznek, ilyenek például az MS Windows, a MAC OS X, a Linux, az Apple iOS, az Android stb.

Az otthoni forgalomirányítók operációs rendszerét rendszerint firmware-nek nevezik. Ezen eszközök konfigurálása leggyakrabban böngésző programból elérhető, egyszerű grafikus felületen végezhető. A rajtuk lévő firmware frissíthető, ha a gyártó új funkciókat vagy biztonsági megoldásokat fejleszt ki.

A hálózati infrastruktúra eszközei hálózati operációs rendszert használnak. A Cisco eszközök hálózati operációs rendszerének neve IOS (Internetwork Operating System), mely egyben ezen hálózati szoftverek gyűjtőneveként is szolgál. Cisco IOS fut a legtöbb Cisco eszközön tekintet nélkül annak típusára vagy méretére. A leggyakoribb hozzáférési mód ezen eszközökhöz a parancssori üzemmód.

A fejezetben egy két kapcsolóból és két PC-ből álló kisvállalati hálózaton keresztül kerül bemutatásra a Cisco IOS parancssoros felülete.

A hálózati operációs rendszerek sok dologban hasonlítanak a PC-s operációs rendszerekhez, melyek olyan funkciók hátterét biztosítják a felhasználó számára, mint:

- egér használata,
- monitoron való megjelenítés,
- szöveges parancsok bevitele,
- választási lehetőség dialógus ablakban.

Kapcsolók és forgalomirányítók esetében a funkciók hátterének biztosítása nagyon hasonló. A hálózati szakember számára mindkét eszközön az IOS jelenti a csatlakozási felületet. A szakember parancsok segítségével tudja konfigurálni vagy programozni az eszköz különféle hálózati funkcióit. Az

IOS hálózati eszközön való működésének részletei különbözőek, függően a berendezés jellemzőitől és használatának céljától.

A Cisco IOS egy fogalom, mely a különböző hálózati eszközökön futó többféle operációs rendszert takarja. Például a következőket:

- IOS a kapcsolók, forgalomirányítók és egyéb Cisco hálózati eszközök számára
- Számozott IOS változat egy adott Cisco hálózati eszközhöz
- IOS gyűjtemények, melyek különböző szolgáltatási csomagokat tartalmaznak

Míg egy PC Windows 8-at, egy MacBook OS X-et futtat, addig egy Cisco hálózati eszköz a Cisco IOS egy bizonyos változatát használja. Ezen IOS verzió függ a használt eszköz típusától és a szükséges funkcióktól. Bár az összes eszköz alap IOS-szel és szolgáltatáskészlettel kerül forgalomba, lehetőség van a képességek bővítésének céljából az IOS verzió vagy a szolgáltatáskészlet cseréjére.

Ez a kurzus elsősorban a Cisco IOS Release 15.x használatára összpontosít. Az 1. árán a Cisco Catalyst 2960 kapcsoló, a 2. ábrám pedig a Cisco 2911 ISR (Integrated Services Router) IOS verzióinak listája látható.

Az IOS egy több megabájt méretű, flash memórián tárolt állomány. Az ábrán egy CF (Compact Flash) kártya látható. A flash memória egy nem felejtő tárolóegység. Ez azt jelenti, hogy az áramellátás megszűnése esetén nem veszíti el tartalmát, de az szükség esetén lecserélhető vagy felülírható. Ez lehetővé teszi az IOS frissítését vagy új szolgáltatásokkal való bővítését a hardver cseréje nélkül. Ezenkívül a flash kártya alkalmas egyidejűleg több IOS verzió tárolására is.

A Cisco eszközök bekapcsolásakor az IOS a flash memóriából a RAM-ba (Random Access Memory) töltődik, és ott fut a berendezés működése során. A RAM további funkciója a hálózati műveletekhez szükséges adatok tárolása. Az IOS RAM-ban való futtatása növeli az eszköz teljesítményét, ugyanakkor a RAM felejtő memória lévén elveszíti a tárolt adatokat áramkimaradás esetén, ide értve az akarattal vagy véletlenül történő ki-be kapcsolást (power cycle).

Az IOS változattól függően igen eltérő lehet a szükséges flash memória és RAM mennyisége. Ezért a hálózat tervezése és karbantartása esetén nagyon fontos az eszközök flash és RAM követelményeinek meghatározása, beleértve a maximálisan konfigurálható méretet is. Előfordulhat ugyanis, hogy a telepítendő új IOS verzió több flash-t és RAM-ot igényel, mint amennyi az eszközbe beépíthető.

A Cisco forgalomirányítókon és kapcsolókon futó IOS biztosítja a szakember számára a hálózat működtetéséhez szükséges funkciókat, melyek közül a legfontosabbak a következők:

- Hálózatbiztonság
- IP-címzés virtuális és fizikai interfészeken
- Interfész specifikus konfigurációs lehetőség az adott közeghez való kapcsolódás optimalizálására
- Forgalomirányítás
- A szolgáltatás minőségének biztosítása (Quality of Service, QOS)
- Hálózatfelügyelet támogatása

A hálózati szakember által megvalósításra kerülő minden feladathoz és szolgáltatáshoz konfigurációs parancsok egy csoportja tartozik.

A Cisco IOS szolgáltatásaihoz való hozzáférés rendszerint parancssori üzemmódon (CLI) keresztül biztosított.

Információkat ad a CCO működéséről és az elérhető Cisco termékekről és szolgáltatásokról. A parancssori környezet többféleképpen is elérhető, a leggyakoribb módok:

- Konzol
- Telnet vagy SSH
- Aux port

Konzol

A konzol port egy sávon kívüli elérést biztosító menedzsment port a Cisco eszközökhöz. A sávon kívüli azt jelenti, hogy ez egy dedikált felügyeleti csatorna kizárólag az eszköz karbantartására. A konzol port használatának előnye, hogy az eszköz akkor is elérhető, ha semmilyen hálózati szolgáltatás nincs még telepítve, mint például a kezdeti konfiguráció idején. Ilyenkor a terminál emulációs programot futtató számítógép egy speciális kábellel van összekötve az eszköz konzol portjával, és ezen keresztül kerülnek kiadásra a forgalomirányító vagy kapcsoló beállítására szolgáló parancsok.

Szintén a konzol port használható, ha a hálózati szolgáltatások meghibásodnak és az eszköz távoli elérése nem lehetséges. Mindkét esetben egy konzolon keresztüli közvetlen számítógépes kapcsolat segítségével az eszköz állapota meghatározható. Alapértelmezés szerint a konzol megjelenít minden indítási, nyomkövetési (debug) és hibaüzenetet. Az eszközhöz való kapcsolódás után a hálózati szakember bármilyen szükséges utasítást kiadhat rajta keresztül.

Sok IOS-t futtató eszköz konzol hozzáférése alapértelmezés szerint nem követel meg biztonságos belépést, ezért jelszavas védelmet kell konfigurálni az illetéktelen hozzáférés megakadályozása érdekében. Jelszó elfelejtése esetén létezik egy speciális eljárás az eszköz jelszó nélküli elérésére. Az illetéktelen fizikai hozzáférés megakadályozása érdekében a berendezést zárható szobában vagy rack környezetben kell elhelyezni.

Telnet

A Telnet a parancssor távoli elérési módja hálózaton keresztül, virtuális interfész segítségével. Ellentétben a konzol kapcsolattal, a Telnet hozzáférés igényli a hálózati szolgáltatások működését. Az eszköznek rendelkeznie kell legalább egy aktív interfésszel, amely például IPv4-címmel rendelkezik. A Cisco IOS beépített Telnet szervere engedélyezi a Telnet klienssel rendelkező felhasználóknak a parancssorhoz való hozzáférést, illetve kiegészítésként egy Telnet klienst is tartalmaz. Ez lehetővé teszi a hálózati rendszergazda számára, hogy Telnet használatával egy Cisco eszköz parancssorából egy másik eszközbe bejelentkezzen.

SSH

Az SSH (Secure SHell) protokoll a Telnet-hez hasonló távoli bejelentkezést tesz lehetővé, csak sokkal biztonságosabb hálózati szolgáltatások segítségével. Az SSH erősebb jelszó hitelesítést alkalmaz és az adatok továbbítását titkosítva végzi, ezáltal védve a nyilvánosságtól a felhasználó azonosítóját, jelszavát és a felügyeleti folyamat elemeit. Lehetőség szerint Telnet helyett használjunk SSH-t.

A legtöbb Cisco IOS verzió tartalmaz SSH-szervert. Egyes eszközökön az SSH szolgáltatás már alapértelmezésként fut, míg másokon külön engedélyezni kell. A Cisco IOS csomagok tartalmaznak egy SSH-klienst is, ami lehetővé teszi SSH-kapcsolat létesítését más eszközökkel.

AUX

Egy régebbi módszer a parancssor távoli elérésére a betárcsázós telefonkapcsolat, ahol egy modem van összekötve a forgalomirányító AUX (auxiliary, segéd) portjával, lásd kiemelve az ábrán. Hasonlóan a konzolhoz, az AUX mód is sávon kívüli kapcsolat, így nem igényli semmilyen hálózati szolgáltatás konfigurálását az eszközön. A hálózati kapcsolat megszakadása esetén lehetőséget biztosít a rendszergazda számára, hogy telefonvonalon keresztül érje el a kapcsolót vagy forgalomirányítót.

Az AUX port a konzol porthoz hasonlóan helyben is használható egy közvetlen összeköttetésen keresztül a számítógép terminál emulációs programjával. Hibaelhárításhoz inkább a konzol port használata javasolt, mivel az alapértelmezésben minden indítási, debug és hibaüzenetet megjelenít.

Megjegyzés:A Cisco Catalyst kapcsolók nem rendelkeznek AUX porttal.

Sok kitűnő terminál emulátciós program létezik a hálózati eszközök konzol porton keresztüli soros eléréséhez és a távoli Telnet/SSH kapcsolódáshoz. Néhány közülük:

- PuTTY (1. ábra)
- Tera Term (2. ábra)
- SecureCRT (3. ábra)
- HyperTerminal
- OS X Terminal

Ezek a programok lehetővé teszik az ablakok méretezését, a betűkészlet változtatását és a színek beállítást, ezáltal is növelve a hatékonyságot.

Egy eszközhöz való kapcsolódás után a hálózati szakember már képes annak konfigurálására. A beállítás számos IOS-mód használatával végezhető el. A Cisco IOS parancssori módjai azonosak forgalomirányítók és kapcsolók esetében.

Hierarchikus sorrendjük az egyszerűbbtől a speciálisabb módok felé a következő:

- Felhasználói mód (User EXEC)
- Privilegizált mód (Privileged EXEC)
- Globális konfigurációs mód
- További specifikus konfigurációs módok, például interfész konfigurációs mód

Minden módhoz különböző készenléti jel (prompt) tartozik, valamint egy utasításkészlet, mely a módra jellemző feladatok elvégzését teszi lehetővé. A globális konfigurációs mód például a teljes eszközre hatással lévő beállítási lehetőségeket tartalmaz, többek között itt adható meg az eszköz neve is. Más mód szükséges azonban egy kapcsoló portjának biztonsági beállításaihoz. Ebben az esetben a hálózati szakembernek az adott port interfész konfigurációs módjába kell belépni. Az itt végrehajtásra kerülő összes parancs csak erre a portra érvényes.

A hierarchikus struktúra védelmet is biztosít, hiszen a különféle módokhoz más-más felhasználói azonosítás állítható be, így vezérelhetők a kezelőszemélyzethez rendelt jogosultsági szintek.

Az ábrán az IOS-módok készenléti jelei és jellemző sajátosságai láthatók.

A két elsődleges működési mód a felhasználói EXEC és a privilegizált EXEC mód. A Cisco IOS biztonsági sajátossága, hogy az EXEC folyamatot két hozzáférési szintre bontja. Ahogy az ábrán is látható, a privilegizált EXEC mód több jogosultságot biztosít a felhasználó számára az eszközön végezhető műveletek tekintetében.

Felhasználói EXEC mód

A felhasználói EXEC mód korlátozott lehetőségei alapvető műveletek elvégzését teszik lehetővé. A hierarchikus struktúra legalsó szintjén helyezkedik el, az eszköz parancssorába való belépéskor először ez a mód jelenik meg.

A felhasználói EXEC mód csak az alapvető felügyeleti parancsokat teszi hozzáférhetővé. Sokszor „betekintő” módnak nevezik, mivel nem teszi lehetővé az eszköz konfigurációs parancsainak futtatását.

Alapértelmezés szerint a felhasználói EXEC mód eléréséhez nincs szükség hitelesítésre, de a kezdeti konfiguráció során ajánlott ennek beállítása.

A felhasználói EXEC mód készenléti jele > szimbólummal végződik.

```
Switch>
```

Privilegizált EXEC mód

A konfigurációs és vezérlő parancsok futtatásához a hálózati rendszergazdának privilegizált EXEC módban vagy a hierarchia egy további üzemmódjában kell lenni. Ez azt jelenti, hogy a felhasználónak először a felhasználói EXEC módba, majd onnan tovább a privilegizált EXEC módba kell belépni.

A privilegizált EXEC mód készenléti jelének végén # szimbólum található:

```
Switch#
```

Alapértelmezés szerint a privilegizált EXEC mód eléréséhez nincs szükség hitelesítésre, de ajánlott ennek beállítása.

A globális konfigurációs mód és a többi specifikus konfigurációs mód csak privilegizált EXEC módból érhető el. A fejezet későbbi részében megismerkedünk egy eszköz alapkonfigurációjával és néhány konfigurációs móddal.

A globális és interfész konfigurációs mód csak a privilegizált EXEC módból érhető el.

Globális konfigurációs mód

Az elsődleges konfigurációs módot globális konfigurációs módnak nevezik, az itt végrehajtott beállítások az eszköz működését egészében befolyásolják. A specifikus konfigurációs módok csak a globális konfigurációs módból érhetők el.

Privilegizált EXEC módból globális konfigurációs módba az alábbi CLI-parancs használatával lehet átlépni:

```
Switch# configure terminal
```

Az utasítás végrehajtása után a prompt megváltozik, mutatva ezzel a kapcsoló globális konfigurációs módját.

```
Switch(config)#
```

Specifikus konfigurációs módok

A globális konfigurációs módból a felhasználó továbbléphet különféle al-konfigurációs módokba, melyek az eszköz egy-egy részfunkciójának beállítására szolgálnak. Néhány ezek közül:

- **Interfész mód** - a hálózati interfészek konfigurálása (Fa0/0, S0/0/0)
- **Vonal mód** - fizikai vagy virtuális összeköttetések konfigurálása (konzol, AUX, VTY)

Az 1. ábra a különböző módokhoz tartozó készenléti jeleket mutatja. A specifikus konfigurációs módból való kilépéshez és a globális konfigurációs módba való visszatéréshez írjuk be az **`exit`**parancsot. A globális konfigurációs mód elhagyásához és a privilegizált EXEC módba való visszatéréshez gépeljük be az**`end`** parancsot, vagy használjuk a következő billentyűkombinációt: **Ctrl-Z**.

Készenléti jelek (prompt)

Parancssor használata esetén a készenléti jel egyedi az adott módra nézve. Alapértelmezésben a prompt az eszköz nevével kezdődik és a módra jellemző rövidítéssel folytatódik. Például, egy kapcsoló globális konfigurációs módjának készenléti jele:

```
Switch(config)#
```

Amikor az üzemmód megváltozik, a prompt is tükrözi az aktuális környezetet (Lásd 2. ábra).

Váltás a felhasználói és a privilegizált EXEC módok között

Az **`enable`** és a **`disable`** utasítások szolgálnak a felhasználói EXEC és a privilegizált EXEC módok közötti váltásra.

A privilegizált EXEC módba való belépéshez használjuk az **`enable`**parancsot. A privilegizált EXEC módot néha enable módnak is nevezik.

Az **`enable`** parancs szintaxisa a következő:

```
Switch> enable
```

A parancsnak nincs paramétere vagy kulcsszava. Az Enter billentyű leütése után a prompt a következő lesz:

```
Switch#
```

A készenléti jel végén levő # jelzi, hogy a kapcsoló privilegizált EXEC módban van.

Ha jelszavas védelem került beállításra a privilegizált EXEC mód számára, az IOS kéri annak megadását.

Például:

```
Switch> enable

Password:

Switch#
```

A **disable** utasítás szolgál a felhasználói EXEC módba való visszatérésre.

Például:

```
Switch# disable

Switch>
```

Mint az ábrán is látható, a privilegizált EXEC módba való belépés és a felhasználói EXEC módba való visszatérés parancsai a Cisco kapcsolók és forgalomirányítók esetében azonosak.

Mozgás a globális konfigurációs mód és alüzemmódjai között

A globális konfigurációs módból való kilépéshez és a privilegizált EXEC módba való visszatéréshez írjuk be az **exit**parancsot.

Vegyük figyelembe, hogy az **exit** parancs kiadása privilegizált EXEC módban a konzol munkamenet befejezését eredményezi, ezért az **exit** parancs kiadását követően a konzol kapcsolat kezdeményezése során látott képernyőt kapjuk vissza. Innen az Enter billentyű lenyomásával kerülünk felhasználói EXEC módba.

A parancsmódok hierarchiájában bármely alüzemmódból egy szintet visszalépni az **exit** paranccsal tudunk. Az 1. ábra bemutatja a felhasználói, privilegizált, globális és interfész konfigurációs módokba való belépést, majd a visszalépést a globális konfigurációs, végül a privilegizált EXEC módba az **exit**parancs segítségével.

Bármely alüzemmódból a privilegizált EXEC módba való visszatéréshez gépeljük be az **end** parancsot vagy használjuk a következő billentyűkombinációt: **Ctrl+Z**. A 2. ábrán az látható, hogyan lehet a VLAN konfigurációs módból egy lépésben visszajutni a privilegizált EXEC módba az **end** parancs segítségével.

Bármely alüzemmódból egy másik alüzemmódba való átlépéshez gépeljük be a globális konfigurációs módban használt parancsot. A 3. ábra a vonali konfigurációs módból, `Switch(config-line)#`, az interfész konfigurációs módba, `Switch(config-if)#` való közvetlen átlépést (exit nélkül) mutatja be.

Ebben a videóban bemutatásra kerülnek a Cisco IOS-t futtató forgalomirányítók és kapcsolók különféle parancssori módjai. **Az IOS-parancsok alapvető felépítése**

A Cisco IOS sok parancsot tartalmaz, melyek mindegyike egyedi alakkal vagy szintaxissal bír és csak meghatározott üzemmódban futtatható. A parancsok alapvető formája a következő: parancsszó, majd a megfelelő kulcsszavak és paraméterek. Néhány parancsnak több kulcsszava és paramétere is van, melyek kiegészítő funkciókat látnak el. A parancsok eljárásokat hajtanak végre, a kulcsszavak pedig meghatározzák, hogy hol és hogyan kell megvalósítani ezeket.

Az 1. árán látható, hogy a parancs a készenléti jel után begépelt egy vagy több szóból áll, melyek nem nagybetű-kisbetű érzékenyek. A parancs után egy vagy több kulcsszó és paraméter áll. A parancs érvényesítése, annak teljes bevitele után, az Enter billentyű lenyomásával történik.

A kulcsszavakon keresztül jutnak el meghatározott paraméterek a parancsértelmezőhöz. Például nézzük meg a **show** parancsot, ami formációkat jelenít meg az eszközről. Ennek a parancsnak számos kulcsszava van, melyek használatával különféle eredmények jeleníthetők meg. Például:

```
Switch# show running-config
```

A **show** parancsot a **running-config**paraméter követi. Ez határozza meg, hogy kimenetként az aktív konfiguráció jelenjen meg.

IOS-parancs konvenciók

A parancsok egy vagy több paraméterrel rendelkezhetnek. Ellentétben a kulcsszóval, a paraméter nem egy előre meghatározott szó, hanem a felhasználó által definiált érték vagy változó. A parancsok kulcsszavait és paramétereit a szintaxis határozza meg, mely mintát és formátumot ad a parancsok beviteléhez.

Például a **description** parancs szintaxisa a következő:

```
Switch(config-if)# description string
```

Ahogy a 2. ábra is mutatja, vastagított betű jelöli a begépelendő parancsokat és kulcsszavakat, míg dőlten szedve jelennek meg az értéket váró paraméterek. A **description** parancs esetében a paraméter egy szöveglánc, ami legfeljebb 80 tetszőleges karaktert tartalmazhat.

Tehát, ha megjegyzést fűzünk egy interfészhez a **description** paranccsal, gépeljük be a következőt:

```
Switch(config-if)# description MainHQ Office Switch
```

Ebben az esetben a **description** a parancs és a **MainHQ Office Switch** a paraméter.

A következő példák a tananyagban szereplő IOS-parancsok használatát mutatják be.

A **ping** parancs:

Szintaxis:

```
Switch> ping IP-cím
```

Például:

```
Switch> ping 10.10.10.5
```

Ebben az esetben a **ping** a parancs és a **10.10.10.5** a felhasználó által definiált paraméter.

Hasonlóan, a **traceroute** parancs szintaxisa a következő:

Szintaxis:

```
Switch> traceroute IP-cím
```

Például:

```
Switch> traceroute 192.168.254.254
```

Ebben az esetben a **traceroute** a parancs és a **192.168.254.254** a felhasználó által definiált paraméter.

A Cisco IOS Command Reference egy online dokumentum gyűjtemény, melyben a Cisco eszközök IOS-parancsainak részletes leírása található. A Command Reference alapvető információforrás a konkrét IOS-parancsokhoz, hasonlóan a szótárakhoz vagy lexikonokhoz.

A Command Reference a hálózati mérnökök lényeges információforrása, ahol ellenőrizhetik egy adott IOS-parancs összes jellemzőjét. Néhány ilyen fontosabb jellemző:

- **Szintaxis** - a legrészletesebb fellelhető parancsleírás
- **Alapértelmezés** - az eszköz gyári konfigurációjában lévő parancs alapbeállítása
- **Mód** - konfigurációs üzemmód, ahol a parancs használható
- **Előzmény** - a parancs megvalósításának leírása az IOS előző verzióiban
- **Útmutató** - részletes segédlet a parancs használatához
- **Példák** - hasznos példák a parancs leggyakoribb alkalmazásaira

A Command Reference eléréséhez és a parancsok kereséséhez kövessük az alábbi lépéseket:

1. Keressük fel: www.cisco.com.

2. Kattintsunk: **Support**.

3. Kattintsunk: **Networking Software** (IOS & NX-OS).

4. Kattintsunk: **15.2M&T** (például).

5. Kattintsunk: **Reference Guides**.

6. Kattintsunk: **CommandReferences**.

7. Kattintsunk a kívánt kategóriára, amelybe a keresett parancs tartozik.

8. A bal oldali listában kattintsunk a parancs kezdőbetűjének megfelelő hivatkozásra.

9. Kattintsunk a parancsra.

Például a **`description`** parancs a *Cisco IOS Interface and Hardware Component Command Reference* alatt a *D through E* linken keresztül érhető el.

Megjegyzés: Egy kiválasztott technológiához tartozó teljes Command Reference letölthető PDF formátumban a 7. pontban megadott webhelyről.

Az IOS többféle segítséget is biztosít:

- Környezetérzékeny súgó
- Parancs szintaxis ellenőrzés
- Gyorsbillentyűk és billentyűkombinációk

Környezetérzékeny súgó

A környezetérzékeny súgó megmutatja az adott üzemmódban elérhető parancsokat és azok paramétereit. A súgó eléréséhez gépeljünk be egy kérdőjelet (**`?`**) bármely prompt mögé. Azonnali választ kapunk, nem szükséges az Enter billentyű lenyomása.

A rendelkezésre álló parancsok listáját akkor használjuk, ha nem vagyunk biztosak a parancs nevében vagy meg akarunk győződni arról, hogy az adott parancs az adott üzemmódban használható-e.

Például a felhasználói EXEC mód parancsainak kilistázásához gépeljük be a kérdőjelet (**?**) a `Switch>` prompt után.

A környezetérzékeny súgó használatának másik módja egy adott karakterrel vagy karakterekkel kezdődő parancsok és kulcsszavak kilistázása. A begépelt karaktersor után közvetlenül (szóköz nélkül) bevitt kérdőjel hatására az IOS kilistázza az adott betűkkel kezdődő parancsokat vagy kulcsszavakat.

Például ha begépeljük, hogy **`sh?`** , akkor megkapjuk az **`sh`** -val kezdődő parancsokat.

A környezetérzékeny súgó további felhasználási területe a parancsok beállítási lehetőségeinek, kulcsszavainak és paramétereinek lekérdezése. A parancs beírása után üssük le a szóközt, majd a **?**szimbólumot, így megállapíthatjuk, hogy mivel folytatódhat a beírás.

Ahogy az ábrán is látható, a **`clock set 19:50:00`** parancs bevitele után a **?**beírásával meghatározhatjuk a parancshoz tartozó további opciókat és kulcsszavakat.

Parancs szintaxis ellenőrzés

Egy parancs Enter billentyűvel történő érvényesítése után a parancsértelmező balról jobbra haladva értelmezi az utasítást, hogy meghatározza a végrehajtandó műveletet. Az IOS rendszerint csak a negatív eredményről küld visszajelzést (lásd 1. ábra). Ha a parancsértelmező felismeri az utasítást, a kért művelet végrehajtódik és a CLI visszatér az aktuális prompthoz. Ha a parancsértelmező nem ismeri fel az utasítást, visszajelzést küld a hiba okáról.

A 2. ábrán három különféle hibaüzenet látható:

- Ambiguous command (nem egyértelmű parancs)
- Incomplete command (hiányos parancs)
- Incorrect command (hibás parancsbevitel)

A **`clock set`** parancs ideális IOS-utasítás a különféle szintaxis-ellenőrző üzenetekkel való kísérletezésre (lásd 1. ábra). A 2. ábra a három hibatípus leírását tartalmazza.

Gyorsbillentyűk és billentyűkombinációk

Az IOS CLI tartalmaz konfigurálást, ellenőrzést és hibaelhárítást megkönnyítő gyorsbillentyűket és billentyűkombinációkat.

Az ábrán a legfontosabb gyorsbillentyűk láthatók, melyek közül az alábbiakat érdemes megjegyezni:

- **Lefelé nyíl** - Visszagörgeti a korábbi parancsokat
- **Felfelé nyíl** - Előregörgeti a korábbi parancsokat
- **Tab** - Kiegészíti a részlegesen begépelt parancsokat
- **Ctrl+A** - Ugrás a parancssor elejére

- **Ctrl+E** - Ugrás a parancssor végére
- **Ctrl+R** - Újra megjelenít egy sort
- **Ctrl+Z** - Kilép a konfigurációs módból és visszatér felhasználói EXEC módba
- **Ctrl+C** - Kilép a konfigurációs módból vagy elveti az aktuális parancsot
- **Ctrl+Shift+6** - Megszakít egy IOS-folyamatot, mint például egy ping vagy traceroute futását

Néhány ezek közül részletesebben:

Tab

A Tab billentyű a rövidített parancsok és paraméterek kiegészítésére szolgál, de csak abban az esetben működik, ha a rövidítés elég betűt tartalmaz az azonos kezdetű parancsoktól való megkülönböztetéshez. A parancs elejének begépelése után nyomjuk le a **Tab**billentyűt és a CLI kiegészíti a parancsot vagy kulcsszót a hiányzó résszel.

Ez egy hasznos funkció a tanulás során, mert pontosan megmutatja a használni kívánt parancs vagy kulcsszó teljes alakját.

Ctrl+R

Újra megjeleníti az aktuálisan begépelt sort. Például használhatjuk a **Ctrl+R**kombinációt, ha az IOS éppen akkor küld üzenetet, mikor parancsot gépelünk be. Ekkor a **Ctrl+R** frissíti a már beírt sort és elkerülhető annak újragépelése.

Az alábbi példában egy parancs begépelése közben egy hibás interfészre vonatkozó üzenet érkezett.

```
Switch# show mac-

16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10,
changed state to down
```

A begépelt sor újbóli megjelenítéséhez üssük le a **Ctrl+R** billentyűkombinációt:

```
Switch# show mac
```

Ctrl+Z

Kilép bármely konfigurációs üzemmódból és visszatér privilegizált EXEC módba. Mivel az IOS-módok hierarchikus felépítésűek, több szinttel lejjebb találhatjuk magunkat. Az üzemmódokból egyesével való kilépés helyett, használjuk a **Ctrl+Z** kombinációt a privilegizált EXEC módhoz történő közvetlen visszatéréshez.

Felfelé és lefelé nyilak

Mivel a Cisco IOS tárolja a begépelt utasításokat és karaktereket, a billentyűk segítségével visszahívhatók a korábban begépelt parancsok. Ez hasznos, mivel nincs szükség az utasítások újragépelésére.

Billentyűkombinációk is rendelkezésre állnak a tárolt parancsok görgetéséhez. Használjuk a **felfelé nyíl** billentyűt (**Ctrl+P**) a korábban begépelt parancsok megjelenítéséhez. A billentyű minden további lenyomásakor egy még korábbi parancs jelenik meg. Használjuk a **lefelé nyíl** billentyűt (**Ctrl+N**) a tárolt parancsok előregörgetéséhez.

Ctrl+Shift+6

Ez egy menekülési parancs (escape sequence), mely minden futó folyamatot megszakít. Ha egy IOS-eljárást elindítunk, mint például egy ping vagy egy traceroute, akkor a parancs mindaddig fut, míg be nem fejeződik vagy meg nem szakítjuk. A folyamat során a CLI elérhetetlen, ezért megszakításához és a parancsértelmezőhöz való visszatéréshez nyomjuk le a**Ctrl+Shift+6**billentyűkombinációt.

Ctrl+C

Megszakítja a parancsbevitelt és visszatér az adott konfigurációs módba. Hasznos, ha törölni szeretnénk egy begépelt parancsot.

Rövidített parancsok és kulcsszavak

A parancsok és kulcsszavak addig a minimális karakterszámig rövidíthetők, amíg egyértelműségük biztosított. Például a **configure** parancs lerövidíthető **conf** -ra, mivel a **configure** az egyetlen olyan parancs, aminek a kezdete **conf**. A **con**rövidítés nem működik, mivel több parancs is a **con**betűkkel kezdődik.

A kulcsszavak is rövidíthetők.

Például a **show interfaces** a következőképpen rövidíthető:

```
Switch# show interfaces
```

```
Switch# show int
```

Rövidíthetjük egyszerre a parancsot és a kulcsszót is, például:

```
Switch# sh int
```

A hálózati működés ellenőrzése és javítása érdekében szükség van az eszközök működésének vizsgálatára. Ennek legfontosabb utasítása a **show** parancs.

A parancsnak sokféle változata létezik. Az IOS egyre mélyebb megismerése során megtanuljuk használni és értelmezni mindazt az információt, amit a **show**parancsok nyújtanak számunkra. Használjuk a **show ?** parancsot egy adott környezetben vagy módban elérhető opciók kilistázásához.

Egy tipikus **show** parancs információkat szolgáltat a konfigurációról, a működésről és a Cisco kapcsoló vagy forgalomirányító részeinek állapotáról. Az ábrán néhány gyakori show parancs látható.

Ebben a kurzusban az alapvető **show**parancsokkal foglalkozunk.

Nagyon gyakran használt **show** parancs a **show interfaces**. Ez a parancs információkat jelenít meg az eszköz összes interfészéről. Egy konkrét interfész adatainak megtekintéséhez gépeljük be a **show interfaces** parancsot, majd folytassuk az interfész típusával és a slot/port számmal. Például:

```
Switch# show interfaces fastethernet 0/1
```

További **show** parancsok, amelyeket a hálózati szakemberek gyakran használnak :

show startup-config - Az NVRAM-ba lementett konfigurációt jeleníti meg.

show running-config - Az aktuálisan futó konfigurációs fájl tartalmát jeleníti meg.

A More prompt

Amikor egy parancs kimenete hosszabb, mint amennyi a képernyőre kifér, akkor a képernyő alján a **--More--** prompt jelenik meg. Ha a **--More--** prompt megjelenésekor lenyomjuk a **Space**billentyűt, akkor a kimenet következő része válik láthatóvá. Csak a következő sor megjelenítéséhez üssük le az **Enter**billentyűt. Bármely más billentyű megnyomására a kimenet megszakad és visszatérünk a parancssorhoz.

A kapcsolókon és forgalomirányítókon használt egyik leggyakoribb parancs:

```
Switch# show version
```

A parancs információkat jelenít meg az aktuálisan betöltött IOS verzióról, az eszközről és a hardver összetevőkről. Ha egy forgalomirányítóra vagy kapcsolóra távolról jelentkeztünk be, a **show version** parancs kitűnően használható a csatlakoztatott eszközről való gyors információszerzéshez. A parancs a következőkről ad tájékoztatást:

- **Szoftver verzió** - Az IOS verizója (a flash memóriában tárolt)
- **Bootstrap verzió** - A rendszerbetöltő program verziója (a ROM-ban tárolt)
- **Rendszer felkapcsolási idő** - Az utolsó újraindítás óta eltelt idő
- **Rendszer újraindulási információ** - Az újraindulás módja (pl.: áramkimaradás, összeomlás)
- **A rendszer képfájl neve** - A flash memóriában tárolt IOS-fájl neve
- **Az eszköz és a processzor típusa** - Modell szám és processzor típus
- **Memória típus és foglalás (fő/osztott)** - A fő és az I/O puffer memória mérete
- **Szoftver tulajdonságok** - A támogatott protokollok és jellemzők
- **Hardver interfészek** - Az eszköz rendelkezésre álló interfészei
- **Konfigurációs regiszter** - Indítási előírások, konzolsebesség és kapcsolati paraméterek összessége

Az 1. ábrán a Cisco 1941 ISR forgalomirányító, a 2. ábrán pedig a Cisco 2960 Catalyst kapcsoló show version kimenete látható.

Ebben a feladatban gyakorlati ismereteket szerzünk a Cisco IOS használatáról, beleértve a különféle hozzáférési módokat, konfigurációs üzemmódokat és a gyakran előforduló parancsokat. Megismerkedünk a környezetérzékeny súgóval is, melyben segítségünkre lesz a **clock** parancs.

Packet Tracer - Navigating the IOS Instructions

Packet Tracer - Navigating the IOS - PKA

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

- 1. rész: Belépés egy Cisco kapcsolóba soros konzol porton keresztül.
- 2. rész: Az eszköz alapvető paramétereinek konfigurálása és megjelenítése.
- 3. rész (választható): A Cisco forgalomirányító elérése mini-USB konzol kábel segítségével.

Laborgyakorlat - Establishing a Console Session with Tera Term

Ahogy már korábban szó volt róla, a Cisco kapcsolók és forgalomirányítók sok hasonlóságot mutatnak. Operációs rendszerük parancsainak felépítése megegyezik és sok azonos utasítást tartalmaznak. Mindkét eszköztípus azonos kezdeti konfigurációt igényel, mielőtt a hálózathoz csatlakoztatnánk őket.

A Cisco kapcsoló az egyik legegyszerűbb eszköz, amivel hálózat alakítható ki, mivel alapvető működéséhez nem kell konfigurálni. A kapcsoló tehát mindenféle beállítás nélkül beilleszthető a hálózatba és továbbítja az adatokat a csatlakoztatott eszközök között.

A kis hálózatok építése során is alapvető jelentőségű berendezés a kapcsoló. Ha két PC-t csatlakoztatunk egy kapcsolóhoz, azonnal képesek kommunikálni egymással.

Következésképpen, a fejezet további részében egy olyan kisméretű hálózattal foglalkozunk, melyben két PC és egy alapkonfigurációval ellátott kapcsoló található. Alapkonfiguráción értjük az állomásnév, a korlátozott hozzáférés és a bejelentkezési üzenet beállítását, valamint a konfiguráció mentését.

Hálózati berendezés konfigurálása során az egyik legelső lépés az eszköznév vagy állomásnév beállítása. Az állomásnév megjelenik a parancssori promptban, használható eszközökhöz való csatlakozás bejelentkezési folyamatában és része a hálózati diagramoknak.

Minden aktív hálózati eszköznek van állomásneve. Ha ez mégsem kerül konfigurálásra, úgy a Cisco kapcsoló gyári alapértelmezett neve: "Switch".

Képzeljük el, hogy egy hálózat számos kapcsolójának neve az alapértelmezett "Switch" (amint az ábra is mutatja). Ez jelentős zűrzavart okozhat a rendszer konfigurálása és karbantartása során. Egy távoli eszközhöz történő SSH-csatlakozás esetén fontos megbizonyosodni arról, hogy valóban a kívánt berendezéshez kapcsolódtunk. Ha az összes állomásnevet alapértelmezésben hagyjuk, igen nehéz lesz a csatlakoztatott eszköz azonosítása.

Okosan megválasztott nevek esetén könnyű a hálózati eszközökre emlékezni, beszélni róluk, dokumentálni és azonosítani őket. A berendezések következetes és használható elnevezéséhez vállalati, de legalábbis helyi szintű névadási szabályzat létrehozása szükséges. Ajánlott a névadási és címzési sémát egyidejűleg létrehozni a szervezeti folytonosság érdekében.

A névadásra vonatkozó szabályok alapján egy név:

- betűvel kezdődik
- nem tartalmaz szóközt
- betűvel vagy számmal végződik
- betűt, számot, kötőjelet vagy aláhúzásjelet tartalmaz
- legfeljebb 63 karakter hosszú

Állomásnevek esetén a Cisco IOS megkülönbözteti a kis- és nagybetűket. Mindez lehetővé teszi a nevek megszokott használatát, ellentétben sok internetes névadási szokással, ahol a kis- és nagybetűk egyenértékűek.

Az állomásnevek lehetőséget biztosítanak a hálózati rendszergazda számára az eszközök hálózaton vagy interneten keresztüli azonosítására.

Példák nevek alkalmazására

Nézzünk egy példát három hálózatba kötött kapcsolóval, melyek különböző emeleteken vannak elhelyezve.

Az elnevezési szabály kialakításához vegyük tekintetbe az eszközök telepítési helyét és működésük célját.

Például az ábrán a három kapcsoló neve rendre Sw-Floor-1, Sw-Floor-2, és Sw-Floor-3.

Ezután a hálózati dokumentációban rögzítjük ezeket a neveket és kiválasztásuk okát, biztosítva ezzel névadási rendszerünk folytonosságát további hozzáadott eszközök esetében is.

Az elnevezési rendszer kialakítása után következő feladat a nevek hozzárendelése az eszközökhöz parancssorból.

IOS állomásnév beállítása

Privilegizált EXEC módból globális konfigurációs módba való átlépéshez gépeljük be a **configure terminal**parancsot:

```
Switch# configure terminal
```

Ezután a prompt megváltozik:

```
Switch(config)#
```

Ezt követően állítsuk be az állomásnevet:

```
Switch(config)# hostname Sw-Floor-1
```

Ezután az új prompt:

```
Sw-Floor-1 (config)#
```

Vegyük észre, hogy a prompt most már tartalmazza az állomásnevet. A globális konfigurációs módból való kilépéshez használjuk az **exit** parancsot.

Mindenképpen frissítsük a dokumentációt, valahányszor egy eszközt telepítünk vagy módosítunk. A berendezések azonosítása a dokumentációban elhelyezkedésük, működésük célja és címzésük alapján történik.

Megjegyzés: Egy utasítás visszavonásához írjuk a parancs elé a **no**kulcsszót.

Például egy eszköz nevének eltávolítása:

```
Sw-Floor-1 (config)# no hostname
```

```
Switch(config)#
```

Vegyük észre, hogy a **`no hostname`**parancs hatására a kapcsoló neve az alapértelmezett "Switch" re változott.

Az ábrán lévő parancsszimulátorban gyakoroljuk az állomásnév beállítást.

A fizikai biztonság megvalósítása érekében ajánlott a hálózati eszközöket zárható szobába és állványba elhelyezni; mégis a jelszó jelenti az elsődleges védelmet a jogosulatlan hozzáférés ellen. Minden eszközt, beleértve az otthoni forgalomirányítókat is, helyileg konfigurált jelszóval kell ellátni. A későbbiekben bemutatjuk, hogyan lehet megnövelni a védelmet felhasználónév és jelszó pár beállításával. Ebben a fejezetben alapvető biztonsági beállításokat végzünk jelszavak használatával.

Korábban már említettük, hogy az IOS hierarchikus üzemmódjai támogatják az eszközök biztonságát. Ennek részeként az IOS különféle jelszavakat használ a különféle hozzáférési jogok biztosításához.

A következő jelszavak kerülnek bemutatásra:

- **Enable jelszó** - Korlátozza a priviegizált EXEC módhoz való hozzáférést
- **Enable secret jelszó** - Titkosított jelszóval védi a privilegizált EXEC módot
- **Konzol jelszó** - Korlátozza a konzol kapcsolaton történő hozzáférést
- **VTY-jelszó** - Korlátozza a Telnet-en történő hozzáférést

Ajánlott ezekhez a hozzáférési szintekhez más-más jelszót alkalmazni. Bár a több különböző bejelentkezési jelszó kényelmetlenséget okoz, ez mégis egy szükséges elővigyázatosság ahhoz, hogy megvédjük a hálózati infrastruktúrát az illetéktelen hozzáféréstől.

Másrészt, használjunk nehezen kitalálható, erős jelszavakat. A gyenge és könnyen megfejthető jelszavak biztonsági problémát jelentenek az üzleti világ szempontjából is.

Jelszó választásakor ügyeljünk a következőkre:

- Használjunk 8 karakternél hosszabb jelszavakat.
- Használjunk kis- és nagybetűket, számokat, speciális karaktereket és/vagy számsorozatokat.
- Ne használjunk azonos jelszót minden eszközön.
- Kerüljük a gyakori szavak, mint például a "password" vagy az "administrator" használatát, mivel ezek könnyen kitalálhatók.

Megjegyzés:A kurzus laborgyakorlataiban legtöbbször egyszerű jelszavakat használunk, mint például **cisco** vagy **class**. Ezek a jelszavak gyengék és könnyen megfejthetők, ezért éles környezetben kerüljük a használatukat! Csak tantermi környezetben vagy példa konfiguráció esetén alkalmazzuk őket!

A privilegizált EXEC hozzáférés biztonságossá tételéhez használjuk az **`enable-secret`** *`jelszó`* parancsot. Ennek korábbi, kevésbé biztonságos változata az **`enable password`** *`jelszó`*parancs. Bár mindkét parancs alkalmas a privilegizált EXEC mód hitelesített elérésére, használjuk inkább az **`enable-secret`** parancsot. Az **`enable-secret`**parancs nagyobb biztonságot nyújt, mivel titkosítja a jelszót.

Példa a jelszó beállítására:

```
Switch(config)# enable secret class
```

Az ábrán látható, hogy az **enable**parancs első alkalmazásakor nincs szükség jelszóra. Ezután az **enable secret class** parancs hatására a privilegizált EXEC hozzáférés védelme megtörténik. Figyeljük meg, hogy biztonsági okból a beírás során a jelszó nem jelenik meg.

A hálózati eszközök konzol portját is védeni kell, minimálisan egy erős felhasználói jelszóval. Ez megakadályozza, hogy egy kábellel fizikailag csatlakozó jogosulatlan személy hozzáférjen az eszközhöz.

A konzol vonal jelszavának beállításához globális konfigurációs módban használjuk a következő parancsokat:

```
Switch(config)# line console 0

Switch(config-line)# password cisco

Switch(config-line)# login
```

A globális konfigurációs módban kiadott**line console 0** parancs használatával jutunk a konzol vonal konfigurációs módjába. A nulla (0) jelöli az első (legtöbb esetben az egyetlen) konzol interfészt.

A második parancs, a **password cisco**állítja be a konzol vonal jelszavát.

A **login** parancs állítja be a kapcsolón, hogy bejelentkezéskor hitelesítést kérjen. Ha a jelszó és a login is beállításra került, a konzolon bejelentkező felhasználótól jelszót kér a rendszer, mielőtt hozzáférhetne a parancssorhoz.

VTY-jelszó

A vty vonalak a Cisco eszközök Telnet-en keresztül történő elérésére szolgálnak. Alapértelmezetten a legtöbb kapcsoló 16 vty vonalat kezel, 0-tól 15-ig számozva őket. A Cisco forgalomirányítók vty-vonalainak száma függ a forgalomirányító típusától és az IOS verziójától. Leggyakrabban öt vty vonalat szoktak konfigurálni, ezek sorszáma alapértelmezésben 0-tól 4-ig terjed, ám további vonalak is beállíthatók. Minden rendelkezésre álló vty-vonalra jelszót kell konfigurálni, melyek megegyezhetnek az összes kapcsolat esetében. Gyakran szükséges azonban, hogy egyedi jelszó legyen beállítva egy adott vonalon, biztosítva ezzel egy tartalék hozzáférési lehetőséget a többi kapcsolat foglaltsága esetén.

Használjuk a következő parancsokat a vty-vonalak jelszavának beállításához:

```
Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line)# login
```

Alapértelmezésben az IOS tartalmazza a**login** parancsot a VTY-vonalakon. Ez megakadályozza a hitelesítés nélküli Telnet bejelentkezéseket. Ha véletlenül kiadjuk a**no login** parancsot, ami megszünteti a hitelesítési kötelezettséget, akkor jogosulatlan személyek is csatlakozni tudnak az eszközhöz a hálózaton keresztül Telnet használatával. Ez komoly biztonsági kockázatnak számít.

Az ábra a felhasználói EXEC mód védelmét mutatja be konzol és vty vonalak esetében.

A hálózati eszközök konzol portját is védeni kell, minimálisan egy erős felhasználói jelszóval. Ez megakadályozza, hogy egy kábellel fizikailag csatlakozó jogosulatlan személy hozzáférjen az eszközhöz.

A konzol vonal jelszavának beállításához globális konfigurációs módban használjuk a következő parancsokat:

```
Switch(config)# line console 0

Switch(config-line)# password cisco

Switch(config-line)# login
```

A globális konfigurációs módban kiadott **`line console 0`** parancs használatával jutunk a konzol vonal konfigurációs módjába. A nulla (0) jelöli az első (legtöbb esetben az egyetlen) konzol interfészt.

A második parancs, a **`password cisco`** állítja be a konzol vonal jelszavát.

A **`login`** parancs állítja be a kapcsolón, hogy bejelentkezéskor hitelesítést kérjen. Ha a jelszó és a login is beállításra került, a konzolon bejelentkező felhasználótól jelszót kér a rendszer, mielőtt hozzáférhetne a parancssorhoz.

VTY-jelszó

A vty vonalak a Cisco eszközök Telnet-en keresztül történő elérésére szolgálnak. Alapértelmezetten a legtöbb kapcsoló 16 vty vonalat kezel, 0-tól 15-ig számozva őket. A Cisco forgalomirányítók vty-vonalainak száma függ a forgalomirányító típusától és az IOS verziójától. Leggyakrabban öt vty vonalat szoktak konfigurálni, ezek sorszáma alapértelmezésben 0-tól 4-ig terjed, ám további vonalak is beállíthatók. Minden rendelkezésre álló vty-vonalra jelszót kell konfigurálni, melyek megegyezhetnek az összes kapcsolat esetében. Gyakran szükséges azonban, hogy egyedi jelszó legyen beállítva egy adott vonalon, biztosítva ezzel egy tartalék hozzáférési lehetőséget a többi kapcsolat foglaltsága esetén.

Használjuk a következő parancsokat a vty-vonalak jelszavának beállításához:

```
Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line)# login
```

Alapértelmezésben az IOS tartalmazza a **`login`** parancsot a VTY-vonalakon. Ez megakadályozza a hitelesítés nélküli Telnet bejelentkezéseket. Ha véletlenül kiadjuk a **`no login`** parancsot, ami megszünteti a hitelesítési kötelezettséget, akkor jogosulatlan személyek is csatlakozni tudnak az eszközhöz a hálózaton keresztül Telnet használatával. Ez komoly biztonsági kockázatnak számít.

Az ábra a felhasználói EXEC mód védelmét mutatja be konzol és vty vonalak esetében.

Bár a jelszavak megkövetelése egy jó módszer a jogosulatlan személyek kizárására a hálózatból, mégis lényeges annak kinyilvánítása, hogy az eszközbe csak jogosultak léphetnek be. Ennek érdekében készítsünk banner üzenetet.

A bannerek fontos szerepet játszhatnak egy hivatalos eljárásban, ahol valakit egy eszköz feltörésével vádolnak. Néhány jogszabály nem engedi a felelősségre vonást, de még a felhasználók figyelemmel kísérését sem, ha hiányoznak a figyelmeztető üzenetek.

A banner üzenet tartalma és megfogalmazása függ a helyi törvényektől és a vállalati szabályoktól. Íme néhány példa az üzentekben lévő tartalomra:

- "Az eszközt kizárólag jogosult személyek használhatják."
- "A tevékenység ellenőrizhető."
- "A jogosulatlan használat büntetést von maga után."

Mivel az üzenetek minden belépni szándékozó számára megjelennek, megfogalmazásuknak nagyon pontosnak kell lenni. Bármely "üdvözöljük" vagy "meghívjuk" tartalmú szövegezés nem helyénvaló. Ha a jogosulatlan belépő tönkreteszi a hálózatot, nehéz lesz felelősségre vonni, ha még meghívást is kapott.

A feliratok létrehozása egyszerű, de ügyelni kell helyes használatukra. A banner soha ne tartalmazzon üdvözlő szöveget. Arra kell figyelmeztetnie, hogy az eszközbe csak jogosult személyek léphetnek be. Ezen felül tartalmazhat még ütemezett rendszerleállásra vagy egyéb, a hálózati felhasználókra vonatkozó információkat.

Az IOS többféle banner típust tartalmaz, az egyik leggyakoribb "a nap üzenete" (Messagge Of The Day, MOTD). Gyakran hivatalos üzenetek közvetítésére használják, mivel minden csatlakoztatott berendezésen megjelenik.

Beállításához használjuk a **`banner motd`**parancsot a globális konfigurációs módban.

A **`banner motd`** parancsban határolójelet kell használni az üzenet kijelöléséhez. A **`banner motd`** parancs után egy szóköz, majd a határolójel következik. Ezután egy vagy több sorba az üzenet szövegét kell beírni, végül egy második határolójel zárja az utasítást. A határolójel tetszőleges karakter lehet, mely nem szerepel az üzenet szövegében. Emiatt az egyik leggyakrabban használt jel a #.

A MOTD szintaxisa globális konfigurációs módban a következő:

```
Switch(config)# banner motd #üzenet #
```

A parancs végrehajtása után az üzenet minden bejelentkezési próbálkozásnál megjelenik, mindaddig, amíg az eszközről el nem távolítják.

Az ábrán egy banner konfigurálás látható # határolójel használatával. Figyeljük meg, hogyan jelenik meg az üzenet a kapcsolóhoz való hozzáféréskor.

Az aktív konfiguráció a Cisco IOS aktuális beállításait tükrözi, tartalmazza a hálózati működéshez szükséges parancsokat, amint az 1. ábrán is látható. Az aktív konfiguráció módosítása azonnali hatással van a Cisco eszköz működésére.

Az aktív konfiguráció a berendezés operatív memóriájában (Random Access Memory, RAM) található, ami azt jelenti, hogy csak a berendezés bekapcsolt állapotában aktív. Következésképpen, áramszünet vagy az eszköz újraindulása esetén a nem mentett konfigurációs módosítások elvesznek.

Az aktív konfigurációs fájlban történt változtatások után tekintsük át a következő lehetőségeket:

- Az eszköz eredeti konfigurációjának visszaállítása.
- Az összes konfiguráció eltávolítása az eszközről.
- A módosított konfiguráció mentése az új indító konfigurációba.

Az indító konfiguráció az eszköz bekapcsolásakor vagy újraindulásakor használt beállításokat tartalmazza. Az indító konfigurációt tartalmazó állomány az NVRAM-ban található. A hálózati eszköz beállítása és az aktív konfiguráció módosítása esetén, nagyon fontos a változtatások mentése az indító konfigurációs állományba. Ez a művelet megakadályozza a beállítások elvesztését áramkimaradás vagy szándékos újraindítás során.

A változtatások mentése előtt használjuk a megfelelő **show** parancsokat az eszköz működésének ellenőrzéséhez. Amint az ábrán is látható, a **show running-config** parancs az aktív konfigurációs állományt jeleníti meg. A módosítások helyességének ellenőrzése után használjuk a **copy running-config startup-config** parancsot a privilegizált EXEC módban. Az aktív konfiguráció indító konfigurációs állományba mentéséhez alkalmazott parancs:

```
Switch# copy running-config startup-config
```

Végrehajtás után az aktív konfiguráció frissíti az indító konfigurációt.

Ha az aktív konfiguráció módosítása nem vezet a kívánt eredményre, szükség lehet az eszköz korábbi beállításainak visszaállítására. Feltéve, hogy az indító konfiguráció nem került felülírásra, kicserélhetjük az aktív konfigurációt az indító konfigurációval. Ennek legegyszerűbb módja az eszköz újraindítása, melyhez használjuk a **reload**parancsot a privilegizált EXEC módban.

Az újraindulás megkezdésekor az IOS érzékeli, hogy az aktív konfiguráció nem került elmentésre az indító konfigurációs állományba, és egy kérdéssel jelzi ezt. A változtatások mentésének elvetéséhez írjuk be: **n** vagy **no**.

Egy következő üzenet az újraindítás megerősítését kéri. Ennek megtételéhez üssük le az Enter-t, bármely más billentyű lenyomása megszakítja a folyamatot.

Például:

```
Switch# reload

System configuration has been modified Save? [yes/no]: n

Proceed with reload? [confirm]

*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload
Reason:

Reload Command.

System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 2004 by cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 processor with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled
```

Ha a nem kívánt beállítások mentésre kerültek az indító konfigurációba, szükséges lehet az összes konfiguráció törlése. Ehhez az indító konfiguráció törlése és az eszköz újraindítása kell.

Az indító konfiguráció eltávolításához használjuk az **erase startup-config**parancsot.

Az indító állomány törléséhez privilegizált EXEC módban gépeljük be az **erase NVRAM:startup-config** vagy **erase startup-config** parancsot:

```
Switch# erase startup-config
```

Az utasítás kiadása után a kapcsoló megerősítést kér:

```
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
```

Az alapértelmezés szerinti válasz az elfogadás. Az indító konfigurációs állomány törléséhez nyomjunk Enter-t, bármely más billentyű leütése megszakítja a folyamatot.

Figyelmeztetés: Elővigyázatosan használjuk az **erase** parancsot! Az utasítás téves használata alkalmas az eszközön lévő összes fájl törlésére, beleértve magát az IOS-t és egyéb fontos állományokat is.

Kapcsolók esetében még ki kell adnunk a **delete vlan.dat** parancsot is az **erase startup-config** utasításon kívül, az eszköz gyári alapértelmezett beállításainak visszaállításához:

```
Switch# delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]

[OK]

Erase of nvram: complete

Switch#
```

Az indító konfiguráció (és kapcsolók esetében a vlan.dat fájl) NVRAM-ból való törlése után indítsuk újra az eszközt az aktív konfigurációs fájl RAM-ból való eltávolítása érdekében. Indítás után az eszköz a gyári alapértelmezett beállításokat fogja betölteni.

A 2. ábrán lévő parancsszimulátorban gyakorolhatjuk az aktív konfiguráció mentését a RAM-ból az NVRAM-ba.

Biztonsági másolat készítése szöveg rögzítésével

Az aktív konfiguráció indító konfigurációba mentésén kívül mód van a beállítások szöveges állományba történő archiválására is. Az alábbi lépések lehetőséget adnak a konfigurációs fájlból egy munkaállomány létrehozására, mely szabadon szerkeszthető és később felhasználható.

Az 1. ábrán az aktív konfiguráció szöveges állományba történő mentése látható Tera Term használatával.

A lépések a következők:

- A File menüben kattintsunk ide: **Log**.
- Válasszunk elérési utat. A Tera Term megkezdi a szöveg rögzítését.
- A rögzítés elindítása után adjuk ki a **`show running-config`** vagy **`show startup-config`** parancsot privilegizált EXEC módban. A terminál ablakban megjelenő szövegek mentésre kerülnek a kiválasztott állományba.
- Ha végeztünk a rögzítéssel, válasszuk a **Close** gombot a Tera Term Log ablakában.
- Ellenőrzés céljából nyissuk meg a mentett állományt.

Hasonlóan a 2. ábrán az aktív konfiguráció szöveges állományba történő mentése látható HyperTerminal használatával.

A szöveges konfiguráció visszatöltése

A mentett szövegfájl visszamásolható az eszközre. Mivel a terminálra történő beillesztés során az IOS minden szöveget parancsként futtat le, ezért az állományt bemásolás előtt valószínűleg át kell szerkeszteni. Ajánlott a titkosított jelszavak egyszerű szöveggé alakítása és a titkosítás szintjét jelző 5-ös és 7-es számok eltávolítása. A parancsként nem értelmezhető "--More--" szöveg és az IOS egyéb üzeneteinek törlése is szükséges. Ennek részleteit a laborgyakorlat ismerteti.

Ezen felül az eszköz parancssorában globális konfigurációs módba kell lépni a szövegfájlból beillesztett parancsok fogadása érdekében.

Tera Term esetén a lépések:

- A parancsként nem értelmezhető szövegek eltávolítása, majd mentés.
- A **File** menüben kattintsunk ide: **Send**file.
- Keressük meg az eszközre másolandó állományt és kattintsunk: **Open**.
- A Tera Term beilleszti a fájlt az eszközre.

A szövegek parancsként futnak le és bekerülnek az aktív konfigurációba. Ez egy kényelmes módja az eszközök kézzel történő konfigurálásának.

A feladatban a kapcsoló alapvető konfigurálását fogjuk elvégezni. Biztonságos elérést állítunk be a parancssorhoz és a konzol porthoz titkosított és egyszerű szöveges jelszavak segítségével. Ezenkívül megtanuljuk, hogyan kell üzenetet küldeni a kapcsolóba bejelentkező felhasználóknak és figyelmeztetni a jogosulatlan belépőket a tiltott hozzáférésről.

Packet Tracer - Configuring Initial Switch Settings Instructions

Packet Tracer - Configuring Initial Switch Settings - PKA

Az IP-címzés, legyen az IPv4 vagy IPv6, elsődleges jelentőségű az interneten lévő eszközök számára egymás azonosításához és a végponttól végpontig terjedő kommunikáció biztosításához. Tény tehát,

hogy bármely hálózatról is van szó, az IP-címek nélkülözhetetlenek a berendezések számára a forrástól a célig és vissza irányuló kommunikációhoz.

Minden hálózati végberendezésnek rendelkeznie kell IP-címmel. Ilyen eszközök például:

- Számítógépek (munkaállomások, laptopok, fájl- és webszerverek)
- Hálózati nyomtatók
- VoIP-telefonok
- Biztonsági kamerák
- Okostelefonok
- Hordozható eszközök (például a vezeték nélküli vonalkód olvasó)

Az IPv4-címek írásmódját pontozott decimális jelölésnek nevezik, és négy darab 0-255 közötti számmal ábrázolják. Az IPv4-címek a hálózati eszközökhöz rendelt egyedi számok. Működésüket tekintve logikai címek, így a berendezések elhelyezkedéséről is szolgáltatnak információt.

Minden IP-címhez tartozik egy alhálózati maszk. Az alhálózati maszk egy speciális IP-cím, amely meghatározza, hogy az eszköz a nagy hálózat melyik részhálózatához tartozik.

IP-cím rendelhető a készülékek fizikai portjaihoz és virtuális interfészeihez is. A virtuális interfész azt jelenti, hogy nincs fizikai hardver elem hozzárendelve az eszközben.

A hálózati kommunikáció fontos részét alkotják a végberendezések és a hálózati eszközök interfészei, valamint az őket összekötő kábelek.

Minden fizikai interfészhez tartozik egy leírás vagy szabvány, amely egyúttal meghatározza a hozzá csatlakoztatható kábel típusát is. Ilyen hálózati átviteli közeg a csavart érpáras rézkábel, az optikai szál, a koaxiális kábel vagy a vezeték nélküli közeg. A különféle adathordozó típusoknak különféle sajátosságai és előnyei vannak, ezért rendeltetési területük is más és más. Néhány jellegzetesség, amelyben az egyes átviteli közegek különbözhetnek:

- Hatótávolság, azaz a jel által a közegben sikeresen megtett út.
- Az adathordozó telepítési környezete.
- Az átvitelre kerülő adatok mennyisége és az átvitel sebessége.
- Bekerülési és telepítési költségek.

Az internet összeköttetései nem csak egy konkrét átviteli közeget, hanem egy meghatározott átviteli technológiát is igényelnek. Napjainkban az Ethernet a leggyakoribb helyi hálózati (Local Area Network, LAN) kapcsolódási mód. Ethernet portok vannak azokon a végberendezéseken, kapcsolókon és egyéb hálózati eszközökön, melyek kábellel csatlakoznak a fizikai hálózathoz. Az Ethernet porthoz vezetékkel bekötött eszközök kábelein RJ-45 csatlakozók találhatók.

A Cisco IOS kapcsolók nem csak fizikai portokkal rendelkeznek, hanem egy vagy több virtuális interfésszel (Switch Virtual Interface, SVI) is. Ezek az interfészek nem kötődnek az eszköz fizikai hardver elemeihez, az IOS hozza létre őket. A virtuális interfész (SVI) lehetőséget biztosít a kapcsoló távoli elérésére IPv4-hálózaton keresztül. A kapcsolók alapértelmezett gyári konfigurációjában egyetlen SVI található, melynek neve VLAN1 interfész.

A kapcsoló távoli eléréséhez IP-cím és alhálózati maszk konfigurálása szükséges a virtuális interfészen (SVI):

- **IP-cím** - Az alhálózati maszkkal együtt egyedileg azonosít egy végberendezést a hálózaton.
- **Alhálózati maszk** - Meghatározza, hogy egy nagyobb hálózat melyik részében található az IP-cím.

Most először az IPv4-gyel foglalkozunk, később megismerkedünk az IPv6-tal is.

Rövidesen megtanuljuk az IP-címzés részleteit is, de most a legfontosabb a kapcsoló távoli elérésének gyors konfigurálása. Az ábrán az S1 kapcsoló IP-címének (192.168.10.2) beállítása és engedélyezése látható:

- **`interface vlan 1`** - A parancs globális konfigurációs módból interfész konfigurációs módba vált.
- **`ip address 192.168.10.2 255.255.255.0`** - Beállítja a kapcsoló IP-címét és alhálózati maszkját (ez csupán egy a lehetséges sok cím-maszk kombináció közül).
- **`no shutdown`** - Engedélyezi az interfész aktív állapotba kerülését.

A beállítás után a kapcsoló rendelkezik minden olyan IP beállítással, amely a hálózati kommunikációhoz szükséges.

Megjegyzés: A kapcsoló legalább egy fizikai portjának és a VTY-vonalaknak konfigurálva kell lenniük a sikeres távoli felügyeleti kapcsolat létesítéséhez.

Az ábrán lévő parancsszimulátorban gyakorolhatjuk az SVI konfigurálását.

Egy végberendezés hálózati működésének biztosításához pontos IP-cím információk beállítása szükséges. Hasonlóan az SVI-hez, a végberendezés beállításához is IP-címet és alhálózati maszkot kell megadni.

Ezek a beállítások szükségesek a végberendezés megfelelő hálózati csatlakozásához. Az IP-cím és maszk információn kívül konfigurálható még az alapértelmezett átjáró és a DNS-szerver is (lásd ábra).

Az alapértelmezett átjáró a forgalomirányító azon interfészének címe, melyen keresztül a forgalom képes a helyi hálózat elhagyására. A címet rendszerint a hálózati rendszergazda határozza meg a távoli hálózatok elérése céljából.

A DNS (Domain Name System) szerver IP-címe azonosítja azt a rendszert, ami a web címeket IP-címekké alakítja, mint például: www.cisco.com - 2.21.96.170. Az interneten található összes eszköznek van IP-címe, melyen keresztül elérhető. Mivel az emberek számára sokkal könnyebb a nevek megjegyzése, mint a számoké, ezért a weblapoknak nevük is van. A DNS-szerver a különféle eszköznév - IP-cím összerendeléseket felügyeli és tartja karban.

Egy állomás IP-cím információi megadhatók kézzel, vagy DHCP (Dynamic Host Configuration Protocol) használatával, mely automatikusan biztosítja azokat.

A DHCP-technológia majdnem minden hálózatban megtalálható. Népszerűségét könnyen megérthetjük, ha végiggondoljuk, hogy nélküle mennyi többletmunkát kellene végezni.

A DHCP automatikus IP-cím hozzárendelést biztosít minden hálózati végberendezés számára, melyen a DHCP engedélyezve van. Gondoljuk végig, hogy mennyi időt emésztene fel, ha minden hálózatra való csatlakozás alkalmával manuálisan kellene megadni az IP-címet, a maszkot, az

alapértelmezett átjárót és a DNS-szervert. Szorozzuk meg ezt az összes felhasználó és az általuk használt hálózati eszközök számával, így láthatjuk a probléma méretét.

A DHCP a legjobb példa arra, amikor egy technológia elsődleges célja az általa végzett műveletek minél egyszerűbb megvalósítása. DHCP használatával a végfelhasználók bárhol csatlakozhatnak az adott hálózathoz Ethernet kábellel vagy vezeték nélkül, és azonnal hozzájuthatnak a kommunikációhoz szükséges IPv4-cím információkhoz.

Amint az 1. ábrán látható, a DHCP konfigurálása egy Windows PC-n az "Obtain an IP address automatically" (IP-cím automatikus kérése) és a "Obtain DNS server address automatically" (DNS-szerver címének automatikus kérése) opciók kiválasztásával történik. Hatására a PC címbeállításokhoz jut a DHCP-szerveren konfigurált IP-cím tartományból és a hozzá kapcsolódó egyéb IP információkból.

A Windows PC IP-cím beállításai megjeleníthetők a parancssorba írt **`ipconfig`** utasítás segítségével. A kimenetben megjelenik az IP-cím, az alhálózati maszk és az alapátjáró, melyet a PC a DHCP-szervertől kapott.

A 2. ábrán lévő parancsszimulátorban gyakorolhatjuk a Windows PC IP-cím beállításának megjelenítését.

Ha egy hálózati eszköz, például nyomtató, statikusan kap IP-címet, majd egy DHCP-szerver kerül a rendszerbe, akkor duplikált IP-cím ütközés történhet az eszköz és egy olyan PC között, mely automatikusan jut IP-címhez a DHCP-szervertől. Ütközés akkor is történhet, ha egy DHCP-szervert érintő hiba miatt a hálózatban statikusan kell IP-címeket adni, és a leállás után a DHCP-szerver újra elérhető lesz.

Az IP-címzési hibák kivédése érdekében a statikus IP-címmel konfigurált eszközöket tegyük DHCP-klienssé, vagy zárjuk ki a statikus címeket a DHCP hatóköréből.

Utóbbi megoldás feltételezi, hogy rendszergazdai jogokkal rendelkezünk a DHCP-szerveren és ismerjük a DHCP konfigurálását.

Olyan hálózatban is találkozhatunk IP-cím ütközéssel, ahol a végberendezések kizárólag statikus címeket használnak. Ilyenkor állapítsuk meg, hogy mely IP-címek szabadak az adott alhálózatban és ennek megfelelően konfiguráljunk. Ez az eset is jól mutatja, mennyire fontos a hálózati rendszergazda számára a részletes hálózati dokumentáció karbantartása, beleértve a végberendezések számára kiosztott IP-címeket is.

Megjegyzés: A kis és közepes hálózatokban rendszerint statikus IP-címet kapnak a szerverek és a nyomtatók, míg a felhasználói eszközök számára a DHCP-szerver nyújt címinformációt.

Ebben a feladatban először a kapcsoló alapvető beállítását hajtjuk végre, majd a kapcsolat megvalósítása következik a kapcsoló és a PC IP-címének konfigurálásával. A címzés beállítása után különféle **`show`** parancsok segítségével ellenőrizzük a konfigurációt, és a **`ping`**utasítással teszteljük az eszközök közötti kapcsolatot.

Packet Tracer - Implementing Basic Connectivity Instructions

Packet Tracer - Implementing Basic Connectivity – PKA

A visszacsatolás (loopback) tesztelése

Az ábrán az ellenőrzési folyamat első lépése látható. A **`ping`** parancs használatával ellenőrizhető az állomás saját IP konfigurációja. A teszt végrehajtásához használjuk a **`ping`**parancsot egy speciális címmel, melyet visszacsatolási (loopback, 127.0.0.1) címnek neveznek. A loopback cím a TCP/IP protokoll készlet egy lefoglalt címe, mely a csomagokat visszairányítja az állomáshoz.

Az állomás parancssorába begépelésre kerülő ping parancs szintaxisa:

```
C:\> ping 127.0.0.1
```

Az utasítás válasza egy ehhez hasonló üzenet:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Az eredmény azt mutatja, hogy a kiküldött négy 32 bájtos csomag a 127.0.0.1 című állomásról kevesebb, mint 1 ms alatt visszaérkezett. A sikeres ping válasz jelzi, hogy a hálózati kártya, a meghajtóprogram és a TCP/IP protokoll készlet rendben működik.

A 2. ábrán lévő parancsszimulátorban gyakorolhatjuk a loopback cím tesztelését.

Hasonlóan az álommásokon használt ellenőrző parancsokhoz és segédprogramokhoz, a hálózat közvetítő eszközein is parancsokat használunk az interfészek tesztelésére. Az IOS rendelkezik a kapcsolók és forgalomirányítók interfészeinek ellenőrzésére szolgáló utasításokkal.

A kapcsoló interfészeinek ellenőrzése

Az S1 és S2 interfészeinek vizsgálatához használjuk a **`show ip interface brief`** parancsot a kapcsolón, az ábrán látható módon. Az S1 kapcsoló VLAN 1 interfészéhez rendelt IP-cím a 192.168.10.2. Az S2 kapcsoló VLAN 1 interfészéhez rendelt IP-cím a 192.168.10.3. Az S1 és S2 fizikai FE0/1 és FE0/2 interfészei működőképesek.

Az ábrán lévő parancsszimulátorban gyakorolhatjuk az interfészek tesztelését.

Hasonlóan az álommásokon használt ellenőrző parancsokhoz és segédprogramokhoz, a hálózat közvetítő eszközein is parancsokat használunk az interfészek tesztelésére. Az IOS rendelkezik a kapcsolók és forgalomirányítók interfészeinek ellenőrzésére szolgáló utasításokkal.

A kapcsoló interfészeinek ellenőrzése

Az S1 és S2 interfészeinek vizsgálatához használjuk a **`show ip interface brief`** parancsot a kapcsolón, az ábrán látható módon. Az S1 kapcsoló VLAN 1 interfészéhez rendelt IP-cím a 192.168.10.2. Az S2 kapcsoló VLAN 1 interfészéhez rendelt IP-cím a 192.168.10.3. Az S1 és S2 fizikai FE0/1 és FE0/2 interfészei működőképesek.

Az ábrán lévő parancsszimulátorban gyakorolhatjuk az interfészek tesztelését.

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

- 1. rész: A hálózati topológia összeállítása (csak Ethernet).
- 2. rész: A PC-k konfigurálása.
- 3. rész: A kapcsoló alapbeállításainak konfigurálása és ellenőrzése.

Laborgyakorlat - Building a Simple Network

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

- 1. rész: Hálózati eszköz alapvető konfigurálása.
- 2. rész: Beállítások ellenőrzése és hálózati kapcsolatok tesztelése.

Laborgyakorlat - Configuring a Switch Management Address

Taníts meg!

A tanulók párokban fognak dolgozni. A feladat elvégzéséhez Packet Tracer szükséges.

Tegyük fel, hogy egy új munkatárs érdeklődik nálunk a Cisco IOS parancssora után. A kolléga eddig még sohasem dolgozott Cisco eszközökkel.

Mutassuk be neki az alapvető parancsokat és a CLI felépítést úgy, hogy megértse, a CLI egyszerű és hatékony parancsnyelv, melyet könnyű elsajátítani és eligazodni benne.

Használjuk a Packet Tracer-t és a fejezetben lévő egyik feladatot, mint hálózati modellt (például: 2.3.3.5 Laborgyakorlat - Configuring a Switch Management Address).

Összpontosítsunk a következőkre:

- Bár a parancsok technikai jellegűek, mégis hasonlítanak egyszerű angol kifejezésekre.
- Hogyan rendezhetők a parancsok csoportokba vagy módokba? Honnan tudja a rendszergazda, hogy éppen milyen üzemmódot használ?
- Milyen konkrét parancsokkal konfigurálhatók egy Cisco eszköz alapbeállításai? Hogyan tudjuk a parancsot egyszerű szavakkal elmagyarázni? Keressünk hasonlóságot a valós életből, amikor csak tudunk!

Hívjuk fel a figyelmet, hogy az azonos módba tartozó parancsokat érdemes csoportba fogva használni, elkerülve ezzel az üzemmódok közötti gyakori váltást.

Csoportos feladat - Tutor Me! Instructions

A hálózatmenedzser megkért - mint frissen felvett technikust -, hogy mutassuk be képességeinket egy kis hálózat konfigurálásán keresztül. Feladatunk két Cisco IOS kapcsoló alapbeállításainak konfigurálása és IP-cím hozzárendelése egy állomáshoz a végponttól végpontig terjedő összeköttetés biztosítása érdekében. A két kapcsoló és a két PC bekapcsolt és összekötött állapotban vannak.

Packet Tracer - Skills Integration Challenge Instructions

Packet Tracer - Skills Integration Challenge - PKA

A Cisco IOS egy összefoglaló elnevezés, mely különféle eszközökön futó számos operációs rendszert takar. A szakember parancsok segítségével tudja konfigurálni vagy programozni az eszköz különféle hálózati funkcióit. A Cisco forgalomirányítókon és kapcsolókon futó IOS biztosítja a szakember számára a hálózat működtetéséhez szükséges funkciókat.

A Cisco IOS szolgáltatásai általában a parancssorból (CLI) érhetők el, melyhez a belépés a konzol porton, AUX porton, Telnet-en vagy SSH-n keresztül biztosított. A parancssorhoz való kapcsolódás után a hálózati szakember hozzákezdhet a Cisco eszköz konfigurálásához. A Cisco IOS szerkezetileg egy modális operációs rendszer, ami a hálózati szakember számára biztosítja a különféle üzemmódok közötti átjárást. Minden üzemmód különféle IOS-parancsokat tartalmaz.

A Cisco IOS Command Reference egy olyan online dokumentum gyűjtemény, mely tartalmazza a Cisco eszközön, például Cisco IOS kapcsolókon és forgalomirányítókon használható parancsok részletes leírását.

A Cisco IOS kapcsolók és forgalomirányítók hasonló operációs rendszert futtatnak, melyek parancsszerkezete és parancskészlete is azonos. Mindkét eszköztípus azonos kezdeti konfigurációt igényel, mielőtt a hálózathoz csatlakoztatnánk őket.

Ebben a fejezetben a Cisco IOS került bemutatásra, részletesen felsorolva a különféle üzemmódokat és elemezve a használható parancsok szerkezetét. Ezenkívül ismertetésre kerültek a Cisco IOS kapcsoló alapbeállításai, beleértve az állomásnév és a hozzáférések konfigurálását, a bejelentkezési üzenet létrehozását és a konfiguráció mentését.

A következő fejezetben megvizsgáljuk, hogyan továbbítódnak az adatcsomagok a hálózati infrastruktúrában, és megismerkedünk ennek szabályaival.

Egyre inkább a hálózatok kapcsolnak össze bennünket. Bárhol is járunk, online módon kommunikálhatunk egymással. Az osztálytermi beszélgetések azonnali üzenetküldéses csevegéssé válnak, és online viták zajlanak az iskolában. Napról-napra új hálózati technológiákat fejlesztenek ki, hogy a hálózat előnyeit kihasználhassuk.

Ahelyett, hogy egyedi és különálló rendszereket dolgoznának ki minden új szolgáltatás továbbításához, a hálózati iparág egésze elfogadott egy fejlesztési keretrendszert, amely lehetővé teszi a tervezők számára, hogy megértsék a jelenlegi hálózati platformokat és fenntartsák azokat. Ugyanakkor ennek a keretrendszernek a segítségével megkönnyíthető az új technológiák fejlesztése a jövőbeni kommunikációs igények és a technológiai fejlesztések számára.

Ennek a fejlesztési keretrendszernek a középpontjában azoknak az általánosan elfogadott modelleknek a használata áll, amelyek leírják a hálózati funkciókat és szabályokat.

Ebben a fejezetben megismerjük ezeket a modelleket, a szabványokat, amelyek a hálózatokat működtetik, valamint hogy hogyan történik a kommunikáció a hálózaton keresztül.

Beszélgessünk róla...

Épp most vásároltunk egy új autót személyes használatra. Nagyjából egy hét használat után úgy találjuk, hogy nem működik megfelelően.

Miután megtanácskoztuk a problémát több ismerőssel, úgy döntünk, hogy elvisszük egy autószerelő műhelybe, amelyet nagyon ajánlanak. Ez az egyetlen javítóműhely a közvetlen közelben.

Amikor megérkezünk a műhelybe, azt halljuk, hogy a szerelők egy másik nyelven beszélnek. Nehezen tudjuk elmagyarázni az autó teljesítménybeli problémáit, de a javítást tényleg el kellene végezni. Nem vagyunk biztosak benne, hogy hazavezethetjük, hogy további lehetőségeket keressünk.

Meg kell találni annak a módját, hogy együttműködjünk a szakemberekkel az autó megfelelő javítása érdekében.

Hogyan fogunk kommunikálni a szerelőkkel? Tervezzünk egy kommunikációs modellt annak érdekében, hogy biztosak lehessünk benne: az autót megfelelően kijavították.

Csoportos feladat - Let's just talk about this... Instructions

Egy hálózat lehet annyira bonyolult, mint amikor eszközök az interneten keresztül kapcsolódnak egymáshoz, vagy olyan egyszerű, mint amikor két számítógép van direktben összekötve egy kábellel, és bármi más is e két véglet között. A hálózatok mérete, formája és funkciója különböző. Mindamellett önmagában a fizikai kapcsolat kiépítése a végberendezések között még nem elegendő ahhoz, hogy biztosítsa a kommunikációt. A kommunikációhoz az is kell, hogy az eszközök tudják, "hogyan" kell kommunikálni.

Az emberek különböző kommunikációs módszerekkel osztják meg egymással gondoltaikat. Ugyanakkor a választott módszertől függetlenül minden kommunikációs módszernek három közös eleme van. Ezek közül az első az üzenet forrása vagy küldője. Az üzenetek forrásai emberek vagy elektronikus eszközök, amelyeknek üzenetet kell küldeniük más személyeknek vagy eszközöknek. A kommunikáció második alkotóeleme az üzenet célja vagy fogadója. A cél fogadja és értelmezi az üzenetet. A harmadik elemet, az úgynevezett csatornát az a közeg (média) alkotja, amely azt az utat biztosítja, amelyen az üzenetek haladnak a forrástól a célig.

A kommunikáció egy üzenettel vagy információval kezdődik, amelyet a forrástól kell eljuttatni a célig. Az üzenet küldését, legyen az szemtől szembe vagy hálózaton keresztüli kommunikáció, szabályok irányítják, amiket protokolloknak hívunk. Ezek a protokollok a használt kommunikációs módtól függnek. A hétköznapi személyes kommunikációnkban azok a szabályok, amelyeket egy adott médiumon használunk (mint például egy telefonhíváskor), nem feltétlenül egyeznek meg azokkal a protokollokkal, amelyeket más közegen használunk (például levélküldéskor).

Vegyük például azt, amikor két ember szemtől szembe kommunikál, amint az 1. ábrán látható. A kommunikáció előtt meg kell egyezniük, hogy hogyan fognak kommunikálni. Ha a kommunikáció beszéddel történik, akkor először meg kell állapodni a nyelvben. Ezután ha van egy megosztandó üzenet, akkor képesnek kell lenniük arra, hogy érthetően megformázzák. Például, ha valaki az angol nyelvet használja, de rossz a mondat szerkezete, az üzenet könnyen félreérthető lesz. Mindezek a feladatok jellemzik azokat a protokollokat, amelyeket a kommunikáció megvalósításához használni kell. Ugyanez igaz a számítógépes kommunikációra is, amint a 2. ábrán látható.

Gondoljunk bele, milyen sok különböző szabály és protokoll szabályozza az egyes kommunikációs módszereket, amik a mai világban léteznek.

A szabályok létrehozása

A kommunikáció megkezdése előtt a feleknek meg kell állapodniuk a beszélgetés szabályaiban. Például protokollok szükségesek a hatékony kommunikációhoz (lásd 1. ábra). A használt protokollok specifikusan jellemzők a kommunikációs módszerre, beleértve a forrás, a cél és a csatorna jellemzőit. Ezeket a szabályokat vagy protokollokat kell követni annak érdekében, hogy az üzenetet sikeresen eljuttassuk és a címzett megértse. Számos protokoll van, amelyek a sikeres emberi kommunikáció szabályozzák. Amennyiben van egy egyeztetett módszer a kommunikációra (szemtől szemben, telefonon, levélben, fotón), akkor a használt protokolloknak meg kell felelnie az alábbi követelményeknek:

- Azonosított küldő és fogadó
- Közös nyelv és nyelvtan
- A kézbesítés sebessége és időzítése

- Megerősítési vagy nyugtázási követelmények

A hálózati kommunikáció során használt protokollok számos alapvető tulajdonságukban hasonlítanak azokra, amelyek a sikeres emberi beszélgetéseket szabályozzák (lásd 2. ábra). Amellett, hogy azonosítják a forrást és a célt, a számítógépes és hálózati protokollok meghatározzák annak részleteit, hogyan kell egy üzenetet továbbítani a hálózaton keresztül, hogy megfeleljen a fenti követelményeknek. Miközben számos protokollnak kell együttműködnie, a számítógépes protokollok általában a következőkből állnak:

- üzenet kódolása
- üzenet formázása és beágyazása
- üzenet mérete
- üzenet időzítése
- üzenet szállítási feltételei

Mindegyikről részletesebben lesz szó a következőkben.

Üzenet kódolása

Az üzenetküldés egyik első lépése az üzenet kódolása. A kódolás az a folyamat, melynek során átalakítjuk az információt egy másik, az átvitelhez megfelelő formába. A dekódolás az információ értelmezésekor megfordítja ezt a folyamatot.

Képzeljünk el egy embert, aki nyaralást tervez egy barátjával és felhívja, hogy megbeszéljék a részleteket arról, hogy hova menjenek (lásd 1. ábra). Az üzenet küldőjének az üzenetet először szavakba kell önteni, vagyis kódolnia kell a a gondolatait és észrevételeit a helyszínről. A beszélt nyelv nyelvtani szerkezetét és ragozását használva telefonba mondja a szavakat, amik az üzenetet közvetítik. A telefonvonal másik végén a partner hallgatja a leírást, fogadja és dekódolja a hangokat, hogy elképzelje a küldő által leírt naplementét.

Kódolást a számítógépes kommunikációban is alkalmazzuk, ahogy a 2. ábrán látható. Két állomás közötti kódolásnak az átviteli közegnek megfelelő formátumúnak kell lennie. A hálózaton küldött üzenetet a küldő állomás először bitekké konvertálja. Minden bitet hangmintákká, fény- vagy elektromos impulzusokká kódolunk, attól függően, hogy milyen hálózati közegen fogjuk a biteket továbbítani. A célállomás fogadja és az üzenet értelmezéséhez dekódolja a jeleket.

Üzenet formázása és a beágyazása

Amikor egy üzenetet küldünk a forrástól a célig, sajátos formátumot vagy struktúrát kell használni. Az üzenet formátuma az üzenet típusától és az átvitelhez használt csatornától függ.

Az emberi írásbeli kommunikáció egyik leggyakoribb formája az írott levél. A magánlevelek egyezményes formája évszázadok óta nem változott. A magánlevelek a legtöbb kultúrában a következő elemeket tartalmazzák:

- a címzett azonosítója
- megszólítás vagy üdvözlés
- üzenet tartalma
- zárómondat, az üzenet lezárása

- a küldő azonosítója

Amellett, hogy a megfelelő formátumra alakítjuk, a legtöbb személyes levelet be kell rakni egy borítékba, vagyis be kell ágyazni a szállításhoz, amint az 1. ábrán látható. A borítékon szerepel a küldő és a fogadó címe, mindegyik a megfelelő helyen. Ha a célcím vagy a formátum helytelen, a levelet nem szállítják el. Beágyazásnak hívjuk azt a folyamatot, amikor egy üzenetformátumot (levél) egy másik üzenetformátumba (boríték) helyezünk. Amikor a fogadó a folyamatot megfordítja, kicsomagolás történik, a levelet kivesszük a borítékból.

A levél írója megegyezés szerinti formátumot használ annak érdekében, hogy a levelet elszállítsák, és a fogadó megértse az üzenetet. Hasonlóképpen, a továbbításhoz és a feldolgozáshoz a számítógép-hálózaton küldött üzenet is egy meghatározott formázási szabályt követ. Ahogy a levelet borítékba ágyaztuk a szállításhoz, ehhez hasonlóan a számítógépes üzeneteket is beágyazzuk. A hálózaton való továbbítás előtt minden számítógépes üzenetet egy keretnek nevezett meghatározott formátumba ágyazunk be. Egy keret úgy működik, mint egy boríték, ez tartalmazza a megszólított célállomás, valamint a forrásállomás címét (lásd 2. ábra).

A keret formátumát és a tartalmát a küldött üzenet típusa és a közlésre használt csatorna határozza meg. A nem megfelelően formázott üzenetek továbbítása általában nem lehetséges, de az is előfordulhat, hogy megérkezés után a célállomás nem tudja feldolgozni azokat.

Üzenet mérete

A kommunikáció egy másik szabálya a méret. Amikor az emberek egymással kommunikálnak, a küldendő üzenetet általában kisebb részekre, rendszerint mondatokra tördelik. Ezek a mondatok méretükben akkorára vannak korlátozva, amit a fogadó személy még egyszerre fel tud dolgozni (lásd 1. ábra). Az emberek kommunikációja sok kisebb mondatból áll, ezzel biztosítva, hogy az üzenet minden részét a címzett fogadja és megértse. Képzeljük el, hogy milyen lenne ezt a tananyagot úgy olvasni, hogy az egész egyetlen hosszú mondatból állna. Nem lenne könnyű elolvasni és megérteni.

Hasonlóképpen, amikor egy állomás egy hosszú üzenetet küld egy másiknak a hálózaton keresztül, szükséges az üzenet kisebb darabokra tördelése, ahogy a 2. ábrán látható. A hálózaton továbbított darabok (kereteket) méretét meghatározó szabályok nagyon szigorúak, és a használt csatornától függően eltérőek is lehetnek. A túlságosan hosszú vagy rövid keretek nem kerülnek továbbításra.

A keretek méretkorlátozásai megkívánják, hogy a forrásállomás a hosszú üzeneteket olyan darabokra tördelje, amik megfelelnek a minimális és maximális méret követelményeknek. Ez az úgynevezett szegmentálás. Minden szegmenst a címadatokkal együtt egy külön keretbe ágyazunk, és elküldjük a hálózaton keresztül. A fogadó állomás a fogadáshoz és az értelmezéshez az üzeneteket kicsomagolja és újból összerakja.

Üzenet időzítése

Egy másik tényező, amely az üzenet megfelelő fogadását és megérthetőségét befolyásolja, az időzítés. Az időzítést az emberek annak meghatározására használják, hogy mikor, milyen gyorsan vagy lassan beszéljenek és mennyit várjanak a válaszra. Ezek megegyezésen alapuló szabályok.

Hozzáférési mód

A hozzáférési mód meghatározza, hogy mikor küldhet valaki üzenetet. Ezek az időzítési szabályok a környezethez igazodnak. Például egy ember bármikor elkezdhet beszélni ha szeretne valamit mondani. Ebben a környezetben a beszéd előtt várni kell addig, amíg mindenki más befejezi a beszédet. Ha két ember egyszerre beszél, akkor az információk "összeütköznek", és ilyen esetben szükségessé válik,hogy mindkét fél visszalépjen és újrakezdje a beszédet (lásd 1. ábra). Hasonlóképpen, a számítógépek számára is definiálni kell a hozzáférési módot. A hálózaton lévő állomásoknak is szükségük van egy hozzáférési módra, hogy tudják, mikor kezdhetik az üzenet küldését, és hogyan viselkedjenek ha hiba történik.

Adatfolyam-vezérlés

Az időzítés azt is befolyásolja, hogy mennyi információt lehet küldeni és mekkora sebességgel lehet azt továbbítani. Ha valaki túl gyorsan beszél, akkor a másik személynek azt nehéz meghallgatni és megérteni (lásd 2. ábra). Ilyen esetben a fogadó személynek meg kell kérnie a küldőt, hogy lassítson. A hálózati kommunikáció során is előfordulhat, hogy a küldő állomás gyorsabban továbbítja az üzenetet, mint ahogyan azt a célállomás fogadni és feldolgozni tudná. A forrás- és célállomások adatfolyam-vezérlést használnak a sikeres kommunikációhoz megfelelő időzítés egyeztetésére.

Válaszidő túllépés

Ha valaki feltesz egy kérdést és nem kap rá választ egy elfogadható időn belül, azt feltételezi, hogy a válasz nem is fog megérkezni, és ennek megfelelően reagál (lásd 3. ábra). Lehet, hogy megismétli a kérdést, de az is lehet, hogy folytatja a párbeszédet. A hálózati állomásoknak is vannak szabályai, amelyek meghatározzák, hogy mennyit kell várni a válaszra, és mit kell csinálni, ha válaszidő túllépés történik.

Üzenet szállítási feltételei

Szükség lehet rá, hogy egy üzenetet különböző módokon továbbítsunk, ahogy az 1. ábrán látható. Vannak olyan helyzetek, mikor csupán egyetlen emberrel szeretnénk valamilyen információt megosztani. Máskor előfordulhat, hogy emberek egy csoportjával, vagy akár egy adott területen lévő összes emberrel szeretnénk egyszerre közölni valamit. A két ember közötti párbeszéd példa az egy-az-egyhez típusú kommunikációra. Amikor fogadók egy csoportjának kell ugyanazt az üzenetet fogadnia, akkor egy-a-többhöz vagy egy-a-mindenkihez üzenetminta érvényesül.

Néha az üzenet küldőjének meg kell győződnie arról, hogy az üzenetet sikeresen kézbesítették a címzettnek. Ebben az esetben szükséges, hogy a fogadó egy nyugtát küldjön vissza a küldőnek. Ha a nyugtázás nem szükséges, a szállítási feltételt nem nyugtázottnak nevezzük.

A hálózaton az állomások hasonló üzenetmintákat használnak a kommunikációhoz, amint a 2. ábrán látható.

Az egy-az-egyhez szállítási opciót egyedi címzésnek (unicast) nevezik, ami azt jelenti, hogy csak egyetlen célja van az üzenetnek.

Amikor egy állomásnak egy-a-többhöz szállítási feltétellel kell üzenetet küldeni, azt csoportos (multicast) címzésnek nevezzük. A csoportos címzés ugyanazt az üzenetet párhuzamosan a célállomások egy csoportjának továbbítja.

Ha a hálózaton az összes állomásnak egyszerre kell megkapnia az üzenetet, akkor üzenetszórást (broadcast) használunk. A szórás egy-a-mindenkihez típusú szállítási feltétel. A fenti sémák mellett egyes esetekben a fogadónak nem kell megerősítést küldenie (nyugtázatlan üzenetküldés), míg máskor a küldő elvárhatja, hogy visszajelzést kapjon a sikeres kézbesítésről (nyugtázott üzenetküldés).

Csakúgy, mint az emberi kommunikációban, a különböző hálózati és számítógépes protokolloknak képesnek kell lennie arra, hogy a sikeres hálózati kommunikáció érdekében kölcsönhatásba lépjenek és együttműködjenek egymással. Az egymáshoz kapcsolódó protokollok csoportját, amelyek egy kommunikációs funkció végrehajtásához szükségesek, protokollkészletnek nevezzük. A protokollkészlet megvalósítása az állomásokon és a hálózati eszközökön történhet szoftveresen, hardveresen vagy mindkét féle módon.

Az egyik legjobb mód annak szemléltetésére, hogy a protokollok a készleten belül hogyan lépnek kölcsönhatásba, ha az együttműködést egy veremként szemléljük. A protokollverem megmutatja, hogy az egyes protokollok a készleten belül hogyan hajtódnak végre. A protokollokat rétegek formájában szemléljük, ahol minden egyes magasabb szintű szolgáltatás az alsóbb rétegekben definiált protokollok szolgáltatásaitól függ. A verem alsóbb rétegei az adatok hálózaton belüli mozgatását és a

felsőbb rétegek számára történő szolgáltatások nyújtását végzik, amelyek középpontjában az üzenet tartalmának elküldése áll.A verem alsóbb rétegei az adatok hálózaton belüli mozgatását végzik és a felsőbb rétegek számára nyújtanak szolgáltatásokat, amelyek középpontjában az üzenet tartalmának elküldése áll. Amint az ábra mutatja, a rétegeket használhatjuk a szemtől szembeni kommunikációs példában lévő tevékenységek leírására is. Az alsó rétegben (fizikai réteg) van két ember, mindegyik hangot ad ki, amellyel el lehet mondani a szavakat. A második rétegben (szabály réteg) van egy megállapodás arról, hogy egy közös nyelvet beszéljenek. A legfelső rétegben (tartalmi réteg) vannak a ténylegesen kimondott szavak. Ez a közlés tartalma.

Ha tanúi lennénk a beszélgetésnek, akkor valójában nem látnánk ezeket a rétegeket. A rétegek használata egy olyan modell, amely módot ad egy komplex feladat kezelhető részekre tördelésére és működésének leírására.

Az emberek viszonylatában bizonyos kommunikációs szabályok csak formálisak, másokat pedig egyszerűen a szokás és a gyakorlat határoz meg. Az eszközök sikeres kommunikációjához a hálózati protokollkészletnek pontosan kell a követelményeket és kölcsönhatásokat előírnia. Az eszközök közti üzenettovábbítás közös formátumát és szabályrendszerét a hálózati protokollok határozzák meg. Néhány gyakori hálózati protokoll az IP, HTTP és a DHCP.

Az ábra hálózati protokollokat szemléltet, amelyek leírják a következők folyamatokat írják le:

- Hogyan van az üzenet megformázva vagy strukturálva? (lásd 1. ábra)
- Az a folyamat, amellyel a hálózati eszközök információkat cserélnek útvonalakról más hálózatokkal. (lásd 2. ábra)
- Hogyan és mikor kerülnek átadásra a hiba- és rendszerüzenetek a készülékek között? (lásd 3. ábra)
- Az adatátviteli munkamenetek beállítása és lezárása. (lásd 4. ábra)

Például az IP határozza meg, hogy egy adatcsomagot hogyan továbbítunk a hálózaton belül vagy egy távoli hálózathoz. Az információt az IPv4 protokoll egy olyan meghatározott formában továbbítja, hogy azt a vevő megfelelően értelmezni tudja. Ez nem sokban különbözik attól a protokolltól, amit egy levél elküldésekor a boríték megcímzéséhez használunk. Az információnak be kell tartania egy bizonyos formátumot, különben a levelet nem tudja a posta elszállítani.

Egy példa a protokollkészlet használatára a hálózati kommunikációban a webszerver és a webes kliens közötti kölcsönhatás. Ez a kölcsönhatás számos protokollt és szabványt használ a közöttük lévő információcsere folyamatában. A különböző protokollok együttműködnek annak biztosítására, hogy a üzeneteket mindkét fél megkapja és megértse. Ilyen protokollok például:

- **Alkalmazási protokoll** - A hiperszöveg átviteli protokoll (Hypertext Transfer Protocol, HTTP) a webszerver és a bögésző kölcsönhatásának módját szabályozza. A HTTP meghatározza a kliens és a szerver közötti kérések és válaszok formáját és tartalmát. Az alkalmazás részeként a HTTP-t mind a kliens, mind pedig a webszerver szoftver egyaránt használja. A HTTP más protokollokra bízza, hogy az üzenetek szállítása hogyan történjen a kliens és a szerver között.
- **Szállítási protokoll** - Az átvitelvezérlési protokoll (Transmission Control Protocol, TCP) az szállítási protokoll, amely a webszerverek és a webes kliensek közötti egyedi párbeszédeket kezeli. A TCP a HTTP üzeneteket kisebb darabokra, úgynevezett szegmensekre osztja. Ezeket a szegmenseket küldik át a webszerver és a célállomáson futó kliensfolyamatok között. A TCP felelős a szerver és a kliens között váltott üzenetek méretének és sebességének szabályozásáért is.

- **Internet Protokoll** - Az IP felelős a kialakított szegmensek TCP-től való átvételéért, azok csomagokba ágyazásáért, megfelelő címekkel történő ellátásukért, valamint a legjobb útvonalon a célállomáshoz továbbításukért.

- **Hálózatelérési protokollok** - A hálózatelérési protokollok két elsődleges feladatot látnak el: az adatkapcsolat kezelését és az adatok hálózati közegen történő fizikai átvitelét. Az adatkapcsolati protokollok a csomagokat átveszik az IP-től és előkészítik azokat a közegen való továbbításhoz. A fizikai közeg szabványai és protokolljai azt szabályozzák, hogy milyen módon kerüljenek továbbításra a jelek a közegen és hogyan értelmezzék őket a fogadó állomások. Az Ethernet például egy hálózatelérési protokoll.
  - Mint azt korábban már említettük, a protokoll készlet egy sor protokoll, amelyek együttműködnek annak érdekében, hogy átfogó hálózati kommunikációs szolgáltatásokat biztosítsanak. A protokollkészletet megadhatja egy szabványügyi szervezet vagy akár kifejlesztheti egy gyártó is.
  - Az IP, HTTP és a DHCP protokollok mind részei az internet protokollkészletének, amit TCP/IP-nek (Transmission Control Protocol/Internet Protocol) hívnak. A TCP/IP protokollkészlet egy nyílt szabvány, ami annyit jelenti, hogy a protokollok a nyilvánosság számára szabadon hozzáférhetőek, és bármely gyártó alkalmazhatja ezeket a protokollokat hardverében vagy a szoftverében.
  - A szabványosított protokoll egy olyan folyamat vagy protokoll, amelyet a hálózati ipar elfogadott és amelyet már egy szabványügyi szervezet is ratifikált, vagyis jóváhagyott. A szabványok használata a protokollok kidolgozása és végrehajtása során biztosítja, hogy a különböző gyártók termékei sikeresen együtt tudjanak működni. Ha egy protokollt nem szigorúan vesz figyelembe egy adott gyártó, a berendezései vagy szoftverei nem lesznek képesek sikeresen kommunikálni más gyártók termékeivel.
  - Az adatkommunikációban például ha egy beszélgetés egyik végpontján egy egyirányú kommunikációt vezérlő protokollt használunk, a másik végén pedig kétirányú kommunikációt leíró protokollt feltételezünk, minden valószínűség szerint nem tudunk adatot cserélni.
  - Egyes protokollok gyártóspecifikusak. A gyártóspecifikus ebben az összefüggésben azt jelenti, hogy egy vállalat vagy gyártó cég határozza meg a protokoll funkcióit és működését. Bizonyos protokollokat a tulajdonos engedélyével más szervezetek is használhatnak. Mások csak olyan berendezéseken alkalmazhatók, amelyeket a tulajdonos készített. Gyártóspecifikus protokollok az AppleTalk és a Novell Netware.
  - Több cég akár együtt is létrehozhat egy saját protokollt. Nem ritka, hogy a gyártó (vagy a gyártók csoportja) kidolgoz egy saját protokollt, hogy megfeleljen a fogyasztók igényeinek, majd segítséget nyújt abban, hogy ez a zárt protokoll nyílt szabvánnyá váljon. Az Ethernet protokollt például eredetileg Bob Metcalfe fejlesztette ki a XEROX Palo Alto Research Center-nél (PARC) az 1970-es években. 1979-ben Bob Metcalfe megalapította saját cégét 3COM néven, ezután együtt dolgozott a Digital Equipment Corporation (DEC), az Intel és a Xerox cégekkel azért, hogy támogassák a "DIX" szabványú Ethernet-et. 1985-ben az Institute of Electrical and Electronics Engineers (mérnököket egyesítő nemzetközi szervezet, IEEE) közzétette az IEEE 802.3 szabványt, amely szinte azonos az Ethernet-tel. Ma a 802.3 egy általános helyi hálózati (LAN) szabvány. Egy másik nem is olyan régi példa, amikor a Cisco megnyitotta az EIGRP útválasztási protokollt információs RFC-ként, hogy az ügyfelek igényeinek megfeleljen, akik vegyes hálózatokban is használni szeretnék.
  - Az IP protokollkészlet egy protokollcsomag, ami az információk interneten keresztüli továbbításához és vételéhez kell. Az általánosan ismert elnevezése TCP/IP, mert az első két hálózati protokoll, amit definiáltak ehhez a szabványhoz, a TCP és az IP volt. A nyílt szabványokon alapuló TCP/IP váltotta le más gyártók saját protokollkészleteit, mint amilyen például az Apple AppleTalk és a Novell Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).
  - Az első csomagkapcsolt hálózat és a mai internet elődje az Advanced Research Projects Agency Network (Speciális Kutatási Programok Hivatalának hálózata, ARPANET) volt, amely 1969-ben kelt életre négy helyszínen egymáshoz csatlakozó mainframe számítógépekből. Az ARPANET-et az Egyesült Államok Védelmi Minisztériuma finanszírozta, hogy egyetemek és kutató laboratóriumok használhassák. Bolt, Beranek and Newman (BBN) voltak azok a vállalkozók, akik sokat tettek az ARPANET kezdeti fejlődéséért, beleértve az első forgalomirányító létrehozását Interface Message Processor (üzenetfeldolgozó interfész, IMP) néven.

- 1973-ban Robert Kahn és Vinton Cerf elkezdett dolgozni a TCP-n a következő generációs ARPANET kifejlesztéséért. A TCP-t az ARPANET-ben működő akkori Network Control Program (hálózatvezérlési program, NCP) helyettesítésére tervezték. 1978-ban a TCP-t két protokollra osztották fel: TCP-re és IP-re. Később a TCP/IP protokollkészlet egyéb protokollokkal is bővült, mint a Telnet-et, az FTP-t, a DNS-t és még sok más.
- Kattintsunk az ábra idővonalára, hogy további részleteket láthassunk más hálózati protokollok és az alkalmazások fejlesztéséről.
- Mára a protokollkészlet több tucat protokollt tartalmaz, ahogy az 1. ábrán látható. Kattintsunk az egyes protokollokra a leírásukhoz. Ezek rétegekbe vannak szervezve a TCP/IP modell alapján. A TCP/IP protokollok az internet rétegtől az alkalmazási rétegig szerepelnek, amikor a TCP/IP modellre hivatkozunk. Az adatkapcsolati- vagy hálózatelérési rétegben lévő alsóbb rétegbeli protokollok az IP-csomag fizikai közegen történő továbbításáért felelősek. Ezeket az alsóbb rétegbeli protokollokat szabványügyi szervezetek fejlesztették ki, mint például az IEEE.
- A TCP/IP protokollkészlet mind a küldő, mind a fogadó állomáson egy TCP/IP-veremként van valósítva, végponttól végpontig történő továbbítást biztosítva az alkalmazásoknak a hálózaton keresztül. A 802.3 vagy Ethernet-protokollokat az IP-csomagoknak a LAN által használt fizikai közegen történő továbbítására használjuk.
- A 2. és 3. ábrák egy példán keresztül bemutatják be azt a teljes kommunikációs folyamatot, ahogyan egy webszerver adatokat továbbít a kliensnek.
- Kattintsunk a Lejátszás gombra a animált bemutatók megtekintéséhez:
- **1**. A webszerver Hypertext Markup Language (hiperszöveg leíró nyelv, HTML) oldala az az adat, amit el kell küldeni.
- **2**. A HTTP alkalmazási protokoll fejléce hozzáadódik a HTML adatok elejéhez. A fejléc különböző információkat tartalmaz, beleértve a szerver által használt a HTTP-verziót és egy állapotkódot, amely azt jelzi, hogy információkkal rendelkezik a webes kliens számára.
- **3.** Az alkalmazási rétegbeli HTTP protokoll a HTML-formátumú weboldal adatait a szállítási réteghez továbbítja. A szállítási rétegbeli TCP protokollt használjuk az egyes párbeszédek kezelésére a webszerver és webes kliens között.
- **4**. Ezután az IP-információk adódnak hozzá a TCP-információk elejéhez. Az IP hozzárendeli a megfelelő forrás és cél IP-címeket. Ez az információ az úgynevezett IP-csomag.
- **5**. Az Ethernet protokoll további információkat ad az IP-csomag mindkét végéhez, amit ezután adatkapcsolati keretnek nevezünk. Ez a keret továbbítódik el a legközelebbi forgalomirányítóhoz a webes kliens felé vezető útvonalon. A forgalomirányító eltávolítja az Ethernet információkat, elemzi az IP-csomagot, meghatározza a legjobb útvonalat a csomag számára, beilleszti a csomagot egy új keretbe és elküldi azt a következő szomszédos forgalomirányítóhoz a cél felé. A csomag továbbítása előtt minden forgalomirányító eltávolítja a régi adatkapcsolati információkat és hozzáteszi az újakat.
- **6**. Az adatokat átviteli közegekből és közvetítő eszközökből álló összekapcsolt hálózatokon keresztül továbbítjuk.
- **7**. A kliens megkapja az adatokat tartalmazó adatkapcsolati kereteket, majd feldolgozza az egyes protokollok fejléceit és hozzáadással ellentétes sorrendben eltávolítja azokat. Feldolgozza és eltávolítja az Ethernet információkat, őket az IP protokoll információi követit, majd a TCP információk, végül pedig a HTTP információk.
- **8**. A weboldal információi ezután a kliens böngésző programjához továbbítódnak.

A nyílt szabványok ösztönzik a versenyt és az innovációt. Azt is garantálják, hogy egyetlen cég terméke ne sajátíthassa ki a piacot, vagy szerezhessen tisztességtelen előnyt a versenyben. Jó példa erre, amikor egy otthoni vezeték nélküli forgalomirányítót vásárolunk. Számos különböző gyártó termékei közül választhatunk, amelyek mindegyike tartalmazza az olyan szabványos protokollokat, mint az IPv4, DHCP, 802.3 (Ethernet) és a 802.11 (vezeték nélküli LAN). Ezek a nyílt szabványok teszik lehetővé egy Apple OS X operációs rendszert futtató kliens számára, hogy letölthessen egy weboldalt egy Linux operációs rendszert futtató webszerverről. Azért lehetséges ez, mert a két operációs rendszer nyílt szabványú protokollokat használ, mint például a TCP/IP készlet.

A szabványügyi szervezetek fontosak a internet nyitottságának fenntartásában, szabadon hozzáférhető előírásokat és protokollokat készítenek, amelyeket minden gyártó alkalmazhat. Egy szabványügyi szervezet magától is kidolgozhat egy szabályrendszert, vagy bizonyos esetekben kiválaszthat egy zárt protokollt is, ami majd az alapját képezheti a szabványnak. Ha egy

gyártóspecifikus protokollt használ, ez általában annak a gyártónak a bevonásával történik, aki a protokollt megalkotta.

A szabványügyi szervezetek általában gyártófüggetlen, non-profit szervezetekként jönnek létre, hogy fejlesszék és támogassák a nyílt szabványok koncepcióját.

Szabványügyi szervezetek a következők:

- Az Internet Társaság (Internet Society, ISOC)
- Az Internet Architektúra Tanács (Internet Architecture Board, IAB)
- Az Internet Mérnöki Munkacsoport (Internet Engineering Task Force, IETF)
- A mérnököket egyesítő nemzetközi szervezet (Institute of Electrical and Electronics Engineers, IEEE)
- Nemzetközi Szabványügyi Hivatal (International Organization for Standardization, ISO)

Mindegyik szervezetről részletesebben lesz szó a következő pár oldalon.

Az ábrán kattintsunk a logókra a szabványok információinak megtekintéséhez.

Az Internet Society (ISOC) felelős a nyílt fejlesztés, az internet fejlődésének és használatának előmozdításáért az egész világon. Az ISOC elősegíti az internet műszaki infrastruktúrájához tartozó nyílt szabványok és protokollok fejlesztését, beleértve az Internet Architecture Board (IAB) felügyeletét.

Az Internet Architecture Board (IAB) felelős az internet szabványok általános felügyeletéért és fejlesztéséért. Az IAB biztosítja az interneten használt protokollok és eljárások architektúrájának felügyeletét. Az IAB 13 tagból áll, köztük van az Internet Engineering Task Force (IETF) elnöke is. Az IAB tagjai önálló személyek, és nem képviselői semmilyen társaságnak, hivatalnak vagy egyéb szervezetnek.

Az IETF feladata, hogy kidolgozza, frissítse és fenntartsa az internet és a TCP/IP technológiákat. Az egyik legfontosabb feladata az IETF-nek az, hogy RFC (Request for Comments, vitára bocsátott anyag) dokumentumokat állítson elő, amelyek az interneten alkalmazott protokollokat, folyamatokat és technológiákat írnak le. Az IETF munkacsoportokból áll, ami az elsődleges mechanizmus az IETF előírások és irányelvek kifejlesztésében. A munkacsoportok rövid távon léteznek, és miután a csoport céljai teljesülnek, megszűnnek. Az Internet Engineering Steering Group (Internet Mérnöki Kormányzócsoport, IESG) felelős az IETF, valamint az internetes szabványok kidolgozási folyamatának műszaki irányításáért.

Az Internet Research Task Force (Internet Kutatási Munkacsoport, IRTF) az internethez és a TCP/IP protokollokhoz, az alkalmazásokhoz, a felépítéshez és a technológiákhoz kötődő hosszú távú kutatásokra összpontosít. Míg az IETF a szabványalkotás rövidebb távú kérdéseivel foglalkozik, az IRTF olyan kutatócsoportokból áll, amelyek a hosszú távú fejlesztések irányába tesznek erőfeszítéseket. Néhány a jelenlegi kutatócsoportok közül: Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), Peer-to-Peer Research Group (P2PRG) és a Router Research Group (RRG).

Az Institute of Electrical and Electronics Engineers (villamosmérnökök nemzetközi szervezete, IEEE) egy szakmai szervezet azok számára az elektrotechnika és az elektronika területén, akik elkötelezettek a technológiai innováció és a szabványok létrehozása iránt. A 2012-es állapot szerint az IEEE 38 társaságból áll, közzé tesz 130 folyóiratot, és több mint 1300 konferenciát szponzorál minden évben világszerte. Az IEEE-nek több mint 1300 szabványa és projektje áll jelenleg fejlesztés alatt.

Az IEEE több mint 400 000 taggal rendelkezik, több mint 160 országban. A tagok közül több mint 107 000 tanuló. Az IEEE az oktatási és szakmai előmenetelt segítő lehetőségeket nyújt, amelyek elősegítik a készségek és ismeretek megszerzését az elektronikai iparban.

Az IEEE az egyik vezető szabványalkotó szervezet a világon. Számos iparági szabványt fejleszt és tart karban, többek között az áramellátás és az energetika, az egészségügy, a távközlés, valamint az informatikai hálózatok területén. Az IEEE 802 szabványok családja foglalkozik a helyi és nagyvárosi hálózatokkal, beleértve a vezetékes és vezeték nélküli hálózatokat is. Amint az ábrán látható, mindegyik IEEE szabvány tartalmaz egy a szabványok létrehozásáért és finomításáért felelős munkacsoportot.

Az IEEE 802.3 és IEEE 802.11 szabványok jelentős IEEE szabványok a számítógépes hálózatok területén. Az IEEE 802.3 szabvány határozza meg a vezetékes Ethernet közeghozzáférés-vezérlését (Media Access Control, MAC). Ez a technológia általában a LAN-okra jellemző, de a nagy kiterjedésű hálózatokban (WAN) is alkalmazzák. A 802.11 szabvány a vezeték nélküli helyi hálózatok (WLAN) megvalósítására vonatkozó szabványkészletet definiál. Ez a szabvány határozza meg az OSI (Open Systems Interconnection) fizikai- és adatkapcsolat közeghozzáférés-vezérlést a vezeték nélküli kommunikáció vonatkozásában.

Az ISO a Nemzetközi Szabványügyi Szervezet, a világ legnagyobb nemzetközi szabványok kifejlesztésére szakosodott szervezete. Az ISO nem csak egy mozaikszó a szervezet nevéből, hanem inkább egy kifejezés, amely a görög "isos", azaz egyenlő szón alapul. A Nemzetközi Szabványügyi Szervezet azért döntött az ISO kifejezés mellett, hogy az országok közti egyenlőségét jelképezze.

A hálózatok területén az ISO leginkább a OSI (Open Systems Interconnection, nyílt rendszerek összekapcsolása) referencia modelljéről ismert. Az ISO 1984-ben adta ki az OSI referencia modellt, hogy kidolgozzon egy többrétegű keretrendszert a hálózati protokollokhoz. A projekt eredeti célja nem csak egy referencia modell létrehozása volt, hanem hogy alapot biztosítson egy az interneten alkalmazott protokollkészlet számára. Ez volt az úgynevezett OSI protokollkészlet. Robert Kahn, Vinton Cerf és mások által kifejlesztett TCP/IP protokollkészlet növekvő népszerűsége miatt azonban nem az OSI protokollkészletet választották az interneten használt protokollkészletnek. Helyette a TCP/IP protokollkészletet lett kijelölve. Az OSI protokollkészletet távközlési berendezéseken alkalmazták és a régebbi távközlési hálózatokon még a mai napig megtalálható.

Biztosan ismerünk olyan termékeket, amelyek ISO szabványokat használnak. Az ISO fájlkiterjesztést számos CD képfájlon használják, jelezve, hogy a fájlrendszer az ISO 9660 szabványt használja. Az ISO a forgalomirányító protokollok szabványainak létrehozásáért is felelős.

A hálózati szabványok más szabványosító szervezeteket is érintenek. Néhány a leggyakoribbak közül:

- **EIA -** Az EIA (Electronics Industry Alliance), korábbi nevén Electronics Industries Association egy nemzetközi szabványügyi és kereskedelmi szervezet az elektronikai szervezetek számára. Az EIA leginkább az elektromos kábelezésre és csatlakozókra vonatkozó szabványairól ismert, valamint a hálózati eszközök beszereléséhez használt 19 hüvelykes rack-ekről.

- **TIA -** A TIA (Telecommunications Industry Association) számos terület kommunikációs szabványainak fejlesztéséért felelős, mint a rádióberendezések, a mobil átjátszótornyok, a VoIP (Voice over IP) eszközök, a műholdas kommunikáció, és még ezeken kívül is. Sok szabványukat az EIA-val együttműködve alkották.

- **ITU-T -** Az ITU-T (International Telecommunications Union Telecommunications Standardization Sector) az egyik legnagyobb és legrégebbi kommunikációs szabványügyi szervezet. Az ITU-T olyan területek számára ír elő szabványokat, mint a videó tömörítés, az IPTV (Internet Protocol Television) és a szélessávú kommunikáció, mint például a digitális előfizetői vonal (DSL). Például, ha egy másik országba telefonálunk, akkor az ITU országkódokat használjuk a kapcsolat felépítéséhez.

- **ICANN -** Az ICANN (Internet Corporation for Assigned Names and Numbers) egy USA-beli nonprofit szervezet, amely az IP-címek kiosztását, a DNS által használt domain nevek, valamint a TCP és UDP által használ protokollazonosítók, vagy más néven portszámok kezelését koordinálja. Az ICANN alkotja meg a szabályokat, és teljes körű felelősséggel rendelkezik ezekért a feladatokért.

- **IANA -** Az IANA (Internet Assigned Numbers Authority, IANA) az ICANN egy osztálya, amely az IP-címek kiosztásáért és figyelemmel kíséréséért, a tartománynevek kezeléséért és a protokollazonosítókért felelős.

A hálózati szabványokat kialakító szervezetek megismerése segít annak megértésében, hogy ezek a normák egy nyitott és gyártósemleges internetet alkotnak, valamint lehetővé teszik, hogy megismerjük az újonnan kidolgozott szabványokat.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Hálózati szabványügyi szervezetek felkutatása.

- 2. rész: Internetes és számítógép-hálózati tapasztalatok mérlegelése.

Laborgyakorlat - Researching Networking Standards

Egy réteges modellt, mint amilyen a TCP/IP modell, gyakran használnak a különböző protokollok együttműködésének szemléltetésére. A rétegmodell az egyes rétegekben található protokollok működését és az alatta, illetve a fölötte levő rétegekkel történő kölcsönhatását ábrázolja.

Vannak előnyei, ha rétegmodellt használunk a hálózati protokollok és műveletek leírására. Egy réteges modell használata:

- Segít a protokolltervezésben, mert egy adott rétegben működő protokoll esetén egyértelműen meghatározott, hogy mit kell tennie, és hogyan kapcsolódik az alatta és felette lévő rétegekhez.

- Elősegíti a versenyt, mivel a különböző gyártóktól származó termékek képesek együttműködni.

- Véd attól, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta és felette levő rétegekre.

- Közös nyelvet biztosít a hálózat működésének és képességeinek leírásához.

A hálózati modelleknek két alapvető típusa van:

- **Protokoll modell** - Ez a modell szorosan illeszkedik egy bizonyos protokollkészlet szerkezetéhez. Egy protokollkészlet hierarchikusan egymáshoz kapcsolódó protokolljai általában az emberi hálózat és az adathálózat közötti interfész valamennyi funkcióját képviselik. A TCP/IP modell egy protokollmodell, mivel a TCP/IP protokollkészletben lévő protokollok valamennyi rétegének funkcióit leírja.

- **Referencia modell** - Ez a modell az egységességet biztosítja hálózati protokollok és szolgáltatások valamennyi típusán belül azzal, hogy leírja, mit kell tenni egy bizonyos rétegben, de nem írja elő, hogy hogyan kell azt megvalósítani. A referencia modellnek nem az a célja, hogy végrehajtási előírás legyen, vagy hogy kellő részletességgel, pontosan meghatározza a hálózati architektúra szolgáltatásait. A referencia modell elsődleges célja, hogy segítse az érintett funkciók és folyamatok pontosabb megértését.

Az OSI modell a legismertebb hálózati referencia modell. Ezt alkalmazzák az adathálózatok tervezésnél, az üzemeltetési előírásokhoz és a hibaelhárításhoz.

Amint az ábrán látható, a TCP/IP és az OSI modellek az elsődleges modellek a hálózati működés tárgyalása során. A hálózati protokollok, szolgáltatások vagy eszközök tervezői létrehozhatják saját modelljeiket a termékeik szemléltetésére. Végül azonban szükséges, hogy az iparág szereplőivel való kommunikáció érdekében a termékük vagy szolgáltatásuk vagy az OSI, vagy TCP/IP, esetleg mindkét modellnek megfeleljen.

Eredetileg az ISO által tervezett OSI modell olyan keretrendszernek készült, amelyre egy nyílt rendszerű protokollkészletet lehet építeni. Az elképzelés az volt, hogy ezeket a protokollokat egy olyan nemzetközi hálózat kifejlesztésére lehetne használni, amely nem függne gyártóspecifikus rendszerektől.

Végül az a sebesség, amellyel a TCP/IP-alapú internetet elfogadták, valamint az ütem ahogyan az növekedett azt eredményezték, hogy az OSI protokollkészlet fejlesztése és elfogadtatása elmaradt. Bár néhány, az OSI előírásokhoz fejlesztett protokollt ma is széles körben használnak, a hétrétegű OSI modell minden új hálózattípus esetében jelentős mértékben járult hozzá az egyéb protokollok és a termékek fejlesztéséhez.

Az OSI modell részletes listát ad valamennyi réteg funkcióiról és szolgáltatásairól. Leírja továbbá a rétegek kölcsönhatását a közvetlenül alattuk és felettük lévő rétegekkel. Bár a tanfolyam tartalma az OSI referencia modell köré épül, a tárgyalás hangsúlya a TCP/IP protokoll modell által meghatározott protokollokon van. A részletekért kattintsunk az egyes rétegek nevére.

Megjegyzés: Bár a TCP/IP modellben főleg név szerint említik a rétegeket, az OSI modell hét rétegét gyakrabban említik a sorszámukkal. Például a fizikai réteget 1. rétegnek nevezik az OSI modellben.

A TCP/IP protokoll modellt a hálózatközi kommunikációhoz hozták létre a 1970-es években, néha internet modellnek is nevezik. Amint az ábrán látható, a funkciók négy kategóriáját határozza meg, amelyeknek a sikeres kommunikációhoz teljesülni kell. A TCP/IP protokollkészlet követi ennek a modellnek a szerkezetét. Ezért az internet modellt általában TCP/IP modellnek hívjuk.

A legtöbb protokoll modell gyártóspecifikus protokollkészletet ír le. Mivel azonban a TCP/IP modell egy nyílt szabvány, egyik vállalat sem felügyeli a modell meghatározását. A szabvány és a TCP/IP protokollok definícióját egy nyilvános fórum tárgyalja, és nyilvánosan elérhető RFC-kben vannak meghatározva. Az RFC-k tartalmazzák mind az adatkommunikációs protokollok formális meghatározását, mind az erőforrásokat, amelyek leírják a protokollok használatát.

Az RFC-k technikai és szervezési dokumentumokat is tartalmaznak az internetről, beleértve a műszaki előírásokat és az IETF rendeleteit.

A TCP/IP protokollkészletet protokolljai is leírhatók az OSI referencia modellből kiindulva. Az OSI modellben a TCP/IP modell hálózatelérési rétege és az alkalmazási rétege további részekre van felosztva, hogy leírják a rétegekben előforduló különálló funkciókat.

A hálózatelérési rétegben a TCP/IP protokollkészlet nem határozza meg, hogy mely protokollokat kell használni egy fizikai közegen való továbbításakor, hanem csak azok átadását írja le az internet rétegből a fizikai hálózati protokollok felé. Az OSI 1. és 2. rétegek tárgyalják a közeghez-hozzáféréshez szükséges eljárásokat és a hálózaton keresztül történő adattovábbítás fizikai eszközeit.

Amint az ábrán látható, a fontos párhuzam a két hálózati modell között a 3. és 4. OSI rétegben található. Az OSI 3. réteget, a hálózati réteget szinte univerzálisan használják a valamennyi adathálózatban meglévő címzési folyamatok, valamint összekapcsolt hálózatokban előforduló irányítási folyamatok leírására. Az IP a TCP/IP protokollkészletnek az a tagja, amely magában foglalja az OSI 3. rétegében leírt funkcionalitást.

A 4. réteg, az OSI modell szállítási rétege írja le azokat általános szolgáltatásokat és funkciókat, amelyek az adatok sorrendhelyes és megbízható szállítását biztosítják a forrás és a cél között. Ezen

funkciók közé tartozik a nyugtázás, a hibajavítás és a sorszámozás. Ebben a rétegben a TCP/IP protokollok közül a TCP és az UDP biztosítja a szükséges funkciókat.

A TCP/IP alkalmazási réteg számos protokollt tartalmaz, amelyek a különböző végfelhasználói alkalmazások számára nyújtanak szolgáltatásokat. Az OSI modell 5., 6. és 7. rétegeit referenciaként használják a szoftverfejlesztők és gyártók olyan termékek előállításához, amelyeknek hálózati hozzáférésre van szükségük, mint például a webböngészők.

Ennek a szimulációs feladatnak a célja, hogy alapot nyújtson a TCP/IP protokollkészlet és az OSI modell kapcsolatának megértéséhez. A szimulációs mód lehetővé teszi, hogy megnézzük az adatok tartalmát minden rétegben, amint a hálózat továbbítja azokat.

Ahogy az adatok áthaladnak a hálózaton, kisebb darabokra bontják szét őket és megjelölik, hogy a darabokat újra egyesíteni lehessen, amikor megérkeznek a rendeltetési helyre. Minden darabhoz egy meghatározott protokoll adategység (Protocol Data Unit, PDU) nevet rendelünk és a TCP/IP és OSI modellek egy konkrét rétegéhez kötjük. A Packet Tracer szimulációs módja lehetővé teszi, hogy megtekintsük az egyes rétegeket és a kapcsolódó PDU-kat. A következő lépések végigvezetik a felhasználót azon a folyamaton, ahogy lekérünk egy weboldalt egy webszerverről a kliens PC-n elérhető webböngésző alkalmazás segítségével.

Annak ellenére, hogy sok megjelenített információról később lesz szó részletesebben, ez egy lehetőség arra, hogy megvizsgáljuk a Packet Tracer funkcionalitását és lássuk a beágyazási folyamatot.

Packet Tracer - Investigating the TCP/IP and OSI Models in Action Instructions

Packet Tracer - Investigating the TCP/IP and OSI Models in Action - PKA

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Az RFC Editor használata.
- 2. rész: RFC-k publikálása.

Laborgyakorlat - Researching RFCs

Elméletileg egy általános kommunikáció - mint például a zene, a videó, vagy egy e-mail üzenet - továbbítása a küldő és fogadó között egyetlen nagyméretű, megszakítatlan bitfolyam formájában is történhetne. Ha az üzeneteket valóban ilyen módon továbbítanák, akkor ez azt jelentené, hogy ez idő alatt más eszköz nem lenne képes üzeneteket küldeni vagy fogadni ugyanazon a hálózaton. Ez a nagy adatfolyamok továbbításakor jelentős késleltetéseket okozna. Továbbá, ha ebben a közvetlen összekapcsolt hálózati infrastruktúrában megszakadna a kapcsolat, akkor a teljes üzenet elveszne, vagyis az egészet újra kellene küldeni.

Jobb megoldás, ha az adatokat kisebb, könnyebben kezelhető részekre osztjuk, és így küldjük el a hálózaton keresztül. Az adatfolyam kisebb darabokra történő felosztását szegmentálásnak nevezzük. Az üzenetek szegmentálásának két fő előnye:

- Ha kisebb egységeket küldünk a forrástól a célig, akkor egyszerre számos különböző párbeszéd adatai is összefűzhetők és szállíthatók a hálózaton. A különálló párbeszédek darabjait összefűző eljárást multiplexelésnek hívjuk. Kattintsunk az 1. ábrán lévő gombokra, majd a Lejátszás gombra a szegmentációt és a multiplexelést bemutató animáció megtekintéséhez.
- A szegmentáció által növelhetjük a hálózati kommunikáció megbízhatóságát. A különálló üzeneteknek nem szükséges a hálózat ugyanazon útvonalán eljutniuk a forrástól a rendeltetési helyükig. Ha egy adott útvonal zsúfolttá válik, vagy meghibásodik, akkor az üzenet egyes

darabjait még mindig átirányíthatjuk egy alternatív útvonalra. Ha az üzenet egy része elveszik a cél felé haladva, akkor elegendő csak a hiányzó darabot újraküldeni.

A hálózati adattovábbítás során használt szegmentáció és a multiplexelés hátránya, hogy növeli a folyamat összetettségét. Képzeljük el, ha egy 100 oldalas levelet oldalanként külön borítékban kellene elküldeni. A 100 boríték címzése, címkézése, küldése, fogadása és megnyitása időigényes feladat lenne mind a feladó, mind a címzett számára.

A hálózati kommunikáció minden egyes üzenetszegmensének egy hasonló folyamaton kell keresztül mennie ahhoz, hogy biztosítva legyen a megfelelő célállomáshoz történő eljutása és az eredeti üzenet tartalmának a visszaállítása. Ez látható a 2. ábrán.

Különböző típusú eszközök vesznek részt abban, hogy az üzenetdarabok megbízhatóan érkezzenek meg a rendeltetési helyükre.

Ahogy az alkalmazás adatai haladnak lefelé a protokollveremben, a különböző protokollok minden szinten további adatokkal egészítik ki. Ezt általánosan beágyazási folyamatnak hívjuk.

Az egyes rétegekhez tartozó adathalmazt protokoll adategységnek nevezzük (Protocol Data Unit, PDU). Az adatbeágyazás során minden újabb réteg becsomagolja a felsőbb rétegből származó PDU-t az alkalmazott protokollnak megfelelő módon. A folyamat minden egyes szakaszában a PDU egy másik nevet kap, jelezve ezáltal az új funkcióját is. Bár nincs általános érvényű elnevezés a PDU-kra, ezen a kurzuson a PDU-kat a TCP/IP protokollcsalád szerint nevezzük meg, amint ez az ábrán is látható:

- **Adat** - Általános kifejezés az alkalmazási rétegben használt PDU-ra.
- **Szegmens** - Szállítási rétegbeli PDU.
- **Csomag** - Internet rétegbeli PDU.
- **Keret** - Hálózatelérési rétegbeli PDU.
- **Bitek** - Az átviteli közegen történő fizikai adattovábbításhoz használt PDU.
  - Az adatok beágyazása az a folyamat, ahol az adatot a továbbítása előtt további protokollfejléccel látják el. A legtöbb adatkommunikációs folyamatban az eredeti adatot több különböző protokoll szerint ágyazzák vagy csomagolják be a tényleges továbbítás előtt.
  - Amikor üzeneteket küldünk a hálózaton keresztül, akkor az adott munkaállomáson működő protokollkészlet fentről lefelé irányban működik. A következő webszerveres példában a TCP/IP modellt használjuk egy HTML alapú weboldal klienshez történő elküldésének szemléltetésére.
  - A folyamatot az alkalmazási rétegbeli HTTP protokoll kezdi a HTML formátumú adatok továbbításával a szállítási réteg felé. Ott az alkalmazás adatai TCP szegmensekre lesznek széttördelve. Mindegyik TCP szegmens kap egy címkét, az úgynevezett fejlécet, amely többek között beazonosítja azt az alkalazást, amelynek az üzenetet a célállomáson majd fel kell dolgozni. A fejléc az eredeti információ visszaállítását segítő információkat is tartalmaz.
  - A szállítási réteg beágyazza a weboldal HTML-adatrészeit egy szegmensbe, és elküldi azt az internet réteg számára, ahol az IP protokoll működik. Itt a teljes TCP szegmens beágyazásra kerül egy IP csomagba, amely egy újabb címke, az IP-fejléc hozzáadását jelenti. Az IP-fejléc tartalmazza a forrás- és célállomás IP-címét, valamint a csomag feldolgozását szabályozó folyamatok meghatározását.
  - Ezután az IP csomagot a hálózatelérési réteg kapja meg, ahol egy keretfejléc és egy utótag közé ágyazzák be a csomagot. Minden keret fejléce tartalmazza a forrás és a cél fizikai címét. Az eszközöket a fizikai cím egyedileg azonosítja a helyi hálózaton. Az utótag hibaellenőrzési információkat tartalmaz. Végül a szerver hálózati kártyája (NIC) az átviteli közegen történő továbbításhoz a biteket megfelelően kódolja. Kattintsunk a Lejátszás gombra az ábrán a beágyazási folyamat bemutatásához.

A kicsomagolás folyamata a fogadó oldalon zajlik. A kicsomagolási folyamat során a fogadó oldal eltávolít egy vagy több protokoll fejlécet. Az adat folyamatosan kicsomagolásra kerül, ahogy halad felfelé a protokollkészleten a végfelhasználói alkalmazás irányába. Kattintsunk a Lejátszás gombra az ábrán a kicsomagolási folyamat megtekintéséhez. Az OSI modell leírja a hálózati adattovábbítás során használt kódolás, formázás, szegmentálás és adatbeágyazás folyamatait is. A hálózati és az adatkapcsolati réteg feladata az adatok eljuttatása a forrás eszköztől vagy feladótól a célállomásig, más néven a vevőig. Mindkét réteg protokolljai használnak forrás és célcímeket, de a címek feladata különböző.

Hálózati cím

A hálózati vagy 3. rétegbeli logikai cím tartalmazza azokat az információkat, amelyek szükségesek az IP-csomag elszállításához a forrástól a célállomásig. A harmadik rétegbeli IP-cím két részből áll, a hálózati előtagból és az állomás részből. A hálózati előtagot az útválasztók használják a csomag továbbításához a megfelelő hálózat felé. Az állomás részt az útvonal utolsó forgalomirányítója használja a csomag eljuttatásához a címzett eszköz számára.

Egy IP csomag két IP-címet tartalmaz:

- **Forrás IP-cím** - A küldő készülék IP-címe.
- **Cél IP-cím** - A fogadó készülék IP-címe. A cél IP-címet használják a forgalomirányítók, hogy a csomagot a célhoz irányítsák.

Adatkapcsolati cím

Az adatkapcsolati vagy 2. rétegbeli fizikai címe más szerepet tölt be. Az adatkapcsolati cím célja, hogy a keretet ugyanazon hálózaton lévő két hálózati interfész között továbbítsa. Mielőtt egy IP csomagot elküldenénk vezetékes vagy vezeték nélküli hálózaton keresztül, azt egy adatkapcsolati keretbe kell ágyazni, hogy a saját hálózata által használt fizikai közegen továbbítható legyen. Az Ethernet LAN és vezeték nélküli LAN két példa arra, hogy az eltérő hálózatok különböző fizikai közeget és adatkapcsolati protokollokat használnak.

Az IP csomag adatkapcsolati keretbe kerül beágyazásra, hogy továbbítható legyen a cél hálózat felé. Ekkor történik meg az adatkapcsolati forrás és a cél címek hozzáadása, ahogy ezt az ábra is mutatja:

- **Forrás adatkapcsolati cím** - A csomagot küldő eszköz fizikai címe. Kezdetben ez az IP csomagot küldő állomás hálókártyájának a címe.
- **Cél adatkapcsolati cím** - Ez a következő forgalomirányító vagy a cél készülék hálózati kártyájának a fizikai címe.

Ahhoz hogy a sikeres hálózati kommunikáció működését megértsük, fontos megérteni a hálózati réteg címeinek és az adatkapcsolati réteg címeinek a szerepét is, amikor a két kommunikáló készülék azonos hálózatban található. A következő példában a PC1 kliens számítógép kommunikál az azonos IP hálózatban levő fájl- és FTP-szerverrel.

Hálózati címek

A hálózati rétegbeli címek, az IP-címek jelentik a küldő és a fogadó állomások hálózati- és állomáscímeit. Ebben az esetben a címek hálózati része megegyezik, és csak az állomás részben különböznek.

- **Forrás IP-cím** - A küldő készülék IP-címe, ez a kliens számítógép (PC1) címe: 192.168.1.110.
- **Cél IP-cím** - A fogadó eszköz IP-címe (FTP szerver): 192.168.1.9.

Adatkapcsolati címek

Amikor az IP csomagot küldő és fogadó állomások azonos hálózaton vannak, akkor az adatkapcsolati keret közvetlenül a fogadó eszköznek kerül elküldésre. Egy Ethernet hálózaton az adatkapcsolati címet Ethernet MAC-címnek hívják. A MAC-címek 48 bites címek, amelyek az Ethernet NIC áramköreibe ténylegesen is be vannak "égetve". A MAC-címet ezért gyakran nevezik fizikai címnek vagy beégetett címnek (Burned-in Address, BIA) is.

- **Forrás MAC-cím** - Ez az IP csomagot küldő eszköz (PC1) adatkapcsolati címe, vagy az Ethernet MAC-címe. A PC1 Ethernet NIC MAC-címe AA-AA-AA-AA-AA-AA.

- **Cél MAC-cím** - Ha a fogadó készülék ugyanazon a hálózaton van mint a küldő készülék, akkor ez maga a fogadó eszköz adatkapcsolati címe. Ebben a példában a cél FTP szerver MAC-címe: CC-CC-CC-CC-CC-CC.

A forrás és a cél címek hozzáadódnak az Ethernet kerethez. A keretet a beágyazott IP csomaggal most már PC1 továbbítani tudja közvetlenül az FTP szerver számára.

Most már érthető, hogy az adatok azonos LAN hálózaton belüli küldéséhez a küldő félnek ismernie kell a fogadó oldal fizikai és logikai címét is. Ha ezek a címek ismertek, akkor létrehozhatja a keretet, és elküldheti a hálózati közegen. A forrás állomás több módon képes megtanulni a cél IP-címét. Például megtanulhatja az IP-címet a Domain Name System (DNS) használatával, vagy lehet hogy tudja is a címet, mert a felhasználó kézzel beírta, mint mondjuk az FTP szerver címét a megfelelő alkalmazásban. De honnan tudja meg az állomás a másik eszköz Ethernet MAC-címét?

A legtöbb hálózati alkalmazás a logikai IP-címekre támaszkodik a célállomások helyének meghatározásakor. Az adatkapcsolati MAC-cím ahhoz kell, hogy az Ethernet keretbe ágyazott IP csomagot el lehessen juttatni a hálózaton keresztül a célig.

A küldő eszköz a címmeghatározó protokollt (Address Resolution Protocol, ARP) használja, hogy kiderítse az azonos hálózaton lévő eszközök MAC-címeit. A küldő fél ARP kérés (ARP Request) üzenetet küld a teljes LAN számára. Az ARP kérés szórt üzenet. Az ARP kérés a cél eszköz IP-címét tartalmazza. A LAN minden eszköze megvizsgálja az ARP kérést, hogy a saját IP-címe van-e benne. Csak az készülék fog válaszolni a kérésre, amelyik IP-címe az ARP kérésben szerepel. Az ARP válasz tartalmazni fogja a kérdéses IP-címhez tartozó MAC-címet.

Egy állomás távoli hálózatba történő üzenetküldésének a módja különbözik attól, mint ahogyan az állomás saját helyi hálózatán belül küld üzeneteket. Amikor egy állomásnak a saját hálózatában található állomásnak kell üzenetet küldenie, akkor az üzenetet közvetlenül fogja továbbítani. Az állomás az ARP protokollt használja a célállomás MAC-címének kiderítésére. A csomag fejlécében elhelyezi a cél IP-címét, egy keretbe ágyazza a csomagot, amely a cél MAC-címét tartalmazza, majd továbbítja azt.

Amikor az állomásnak egy távoli hálózatba kell üzenetet küldenie, használnia kell a forgalomirányítót, vagy más néven az alapértelmezett átjárót. Az alapértelmezett átjáró a forgalomirányító azon interfészének az IP-címe, amely a küldővel azonos hálózaton van.

Fontos, hogy az alapértelmezett átjáró címe minden helyi hálózatban levő gépen konfigurálva legyen. Ha a TCP/IP-beállításokban nincs alapértelmezett átjáró meghatározva, vagy rossz alapértelmezett átjáró van megadva, akkor üzeneteket nem lehet a távoli hálózatok célállomásai felé továbbítani.

Az ábrán az állomás az azonos hálózatban levő R1-et használja az alapértelmezett átjárónak, vagyis a 192.168.1.1 címet kell megadni a TCP/IP beállításokban. Ha egy PDU célállomása egy másik IP-hálózaton található, az állomás a PDU-t az alapértelmezett átjárónak fogja elküldeni továbbításra.

De mi a szerepe a hálózati és az adatkapcsolati rétegbeli címeknek, ha a készülék egy távoli hálózatban levő eszközzel kommunikál? Ebben a példában a PC1 kliens számítógép egy másik IP-hálózatban található Web Server nevű géppel kommunikál.

Hálózati címek

Az IP-címek a küldő és a fogadó eszközök hálózati és állomáscímeit jelölik. Amennyiben a csomag feladója és vevője két különböző hálózaton található, akkor a forrás és cél IP-címek is különböző hálózati tartományokból kerülnek ki. Ez a célállomás IP-címének hálózati részéből derül ki.

- **Forrás IP-cím** - A küldő készülék IP-címe, ez a kliens számítógép (PC1) címe: 192.168.1.110.
- **Cél IP-cím** - A fogadó Web Server készülék IP-címe: 172.16.1.99.

Adatkapcsolati címek

Amikor az IP csomag küldője és a vevője nem ugyanabban a hálózatban található, akkor az adatkapcsolati rétegbeli Ethernet keretet nem lehet közvetlenül a célállomásnak küldeni, mert az a küldő hálózatán közvetlenül nem elérhető. Az Ethernet keretet egy másik készüléknek, a forgalomirányítónak vagy más néven alapértelmezett átjárónak kell elküldeni. A példánkban az R1 az alapértelmezett átjáró. R1 rendelkezik egy olyan interfésszel és IP-címmel, ami azonos hálózatban található PC1-el. Ez teszi lehetővé PC1 számára, hogy közvetlenül érhesse el a forgalomirányítót.

- **Forrás MAC-cím** - A küldő PC1 eszköz Ethernet MAC-címe. A PC1 Ethernet NIC MAC-címe AA-AA-AA-AA-AA-AA.

Cél MAC-cím - Ha a fogadó és küldő eszközök különböző hálózaton vannak, akkor ez a cím az alapértelmezett átjáró vagy forgalomirányító Ethernet MAC-címe. A példában a cél MAC-címe az R1 forgalomirányító PC1 hálózatára csatlakozó Ethernet interfészének a MAC-címe, vagyis 11-11-11-11-11-11.

Az Ethernet keret a beágyazott IP-csomaggal már elküldhető az R1-nek. Az R1 ezek után a csomagot a célállomás, a Web Server felé továbbítja. Ez azt jelenti, hogy az R1 a csomagot vagy egy másik forgalomirányítónak, vagy közvetlenül a Web Server állomásnak továbbítja, amennyiben az az R1 egy közvetlenül csatlakozó hálózatán van.

Hogyan határozza meg a küldő állomás a forgalomirányító MAC-címét?

Minden állomás ismeri a forgalomirányító IP-címét, ami a TCP/IP beállításokban található alapértelmezett átjáró. Az alapértelmezett átjáró címe a forgalomirányító azon interfészének a címe, amelyik a forrásállomással azonos helyi hálózatra csatlakozik. A helyi hálózat minden állomása az alapértelmezett átjáró címét használja arra, hogy a forgalomirányítónak üzenetet küldjön. Mivel az állomás tudja az alapértelmezett átjáró IP-címét, ezért használhatja az ARP protokollt az alapértelmezett átjáró MAC-címének meghatározására. Ezután az alapértelmezett átjáró MAC-címe már felhasználható a keretben célcímként.

Ennek a szimulációs feladatnak az a célja, hogy segítse megérteni egy komplex hálózaton belül az adattovábbítás menetét és az adatcsomagok kialakítását. A kommunikáció három különböző helyszínen kerül megvizsgálásra, szimulálva a tipikus üzleti és otthoni hálózatokat.

Packet Tracer - Explore a Network Instructions

Packet Tracer - Explore a Network - PKA

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: A Wireshark letöltése és telepítése.
- 2. rész: Helyi ICMP adatforgalom elfogása és elemzése Wireshark alkalmazásával.

- 3. rész: Távoli ICMP adatforgalom elfogása és elemzése Wireshark alkalmazásával.

Laborgyakorlat - Using Wireshark to View Network Traffic

Garantált hogy működik!

Éppen most fejeztük be a hálózati protokollokról és szabványokról szóló 3. fejezetet.

Feltéve, hogy a fejezet elején lévő modellezési feladatot sikeresen elvégeztük, hogyan hasonlítanánk össze a kommunikációs hálózatok tervezési lépéseit a kommunikációban használt hálózati modellekkel?

- Egy kommunikációs nyelv létrehozása.
- Az üzenet kisebb egységekre osztása, egy időben csak egy kis darab szállítása, a problémák megértésének megkönnyítése.
- Annak ellenőrzése, hogy az adatok teljes mértékben és helyesen kerültek továbbításra.
- A minőségi adatkommunikációt és továbbítást biztosító időzítések.

Csoportos feladat - Guaranteed to work! Instructions

Az adathálózatok végberendezésekből, közvetítő eszközökből és az azokat összekötő átviteli közegekből állnak. A kommunikációhoz ezeknek az eszközöknek tudniuk kell, hogy hogyan is kommunikáljanak.

Ezeknek az eszközöknek meg kell felelniük a kommunikációs szabályoknak és protokolloknak. A TCP/IP példa egy protokollkészletre. A legtöbb protokollt szabványügyi szervezetek hozták létre, mint például az IETF vagy az IEEE. Az IEEE (Institute of Electrical and Electronics Engineers) egy szakmai szervezet azok számára, akik az elektrotechnika és az elektronika területén tevékenykednek. Az ISO, a Nemzetközi Szabványügyi Szervezet a világ legnagyobb nemzetközi szabványok kifejlesztésére szakosodott szervezete.

A legszélesebb körben használt hálózati modellek az OSI és a TCP/IP. Az adatkommunikációs protokollok társítása ezeknek a modelleknek a különböző rétegeihez hasznos annak meghatározásában, hogy a LAN és WAN hálózatokon történő adatátvitel meghatározott pontjain mely eszközöket és szolgáltatásokat alkalmazzák.

Az OSI modell rétegein (a protokollveremben) lefelé haladó adatokat kisebb darabokra tördelik, majd címekkel és egyéb információkkal ellátva beágyazzák azokat. A folyamatot visszafordítva az adatok a darabokból kicsomagolásra kerülnek és a felsőbb protokoll szintekhez továbbítják azokat. Az OSI modell leírja a hálózati adattovábbítás során használt kódolási, formázási, szegmentálási és az adatbeágyazási folyamatokat.

A TCP/IP protokollkészlet egy olyan nyílt és szabványos protokoll együttes, amelyet a hálózati ipar szereplői és a szabványügyi szervezetek elfogadtak és jóváhagytak. Az internet protokollkészlet egy olyan protokollcsomag, amely az interneten keresztüli információ továbbításhoz és fogadáshoz szükséges.

A protokoll-adategységek (PDU) elnevezései a TCP/IP protokollkészletben: adat, szegmens, csomag, keret, valamint a bitek.

A modellek alkalmazása lehetővé teszi az egyének, a vállalatok és a szakmai szövetségek számára a jelenlegi hálózatok elemzését, valamint a jövő hálózatainak megtervezését.

A hálózati kommunikáció támogatása érdekében az OSI modell rétegekre tagolja szét az adatátviteli hálózat feladatait. Mindegyik réteg az alatta és a felette álló rétegekkel együttműködve végzi az adatok továbbítását. Az OSI modell két rétege olyan szorosan kapcsolódik egymáshoz, hogy a TCP/IP modellben gyakorlatilag egy rétegnek tekintjük őket. Ez a két réteg az adatkapcsolati és a fizikai réteg.

A küldő eszköz adatkapcsolati rétegének feladata, hogy előkészítse az adatokat a hálózati átvitelre, és szabályozza az átviteli közeg elérését. A fizikai réteg viszont az adatok átviteli közegre történő továbbadását végzi azáltal, hogy a bináris adatokat a közegnek megfelelő jelekké alakítja.

A vételi oldalon a fizikai réteg az átviteli közeg jeleit fogadja. Miután visszaalakítja a jeleket adatokká, továbbadja azokat az adatkapcsolati rétegnek elfogadásra és feldolgozásra.

Ez a fejezet kezdetben a fizikai réteg általános feladataival, valamint az adatok fizikai közegen történő átvitelének szabványaival és protokolljaival foglalkozik. Ezen kívül, az adatkapcsolati réteg funkcióit és a hozzá kapcsolódó protokollokat is bemutatja.

Az átviteli közeg felügyelete

Képzeljük el, hogy a kollégánkkal együtt egy hálózati témájú konferencián veszünk részt. Az eseményen számos előadás és bemutató zajlik egyidejűleg, és az átfedések miatt csak korlátozott számú előadáson tudnánk együtt részt venni.

Ezért elhatározzuk, hogy külön válunk, és mindegyikünk különböző előadásokat hallgat meg, majd a rendezvény után megosztjuk egymással a megszerzett prezentációkat és új ismereteket.

Próbáljuk megválaszolni az alábbi kérdéseket:

- Hogyan szerveznénk meg egy olyan konferenciát, ahol több előadás is zajlik egyidejűleg? Egy vagy több előadóterembe sorolnánk be az előadásokat? Melyiket milyen okból választanánk?

- Tegyük fel, hogy a konferenciaterem megfelelő audiovizuális eszközökkel rendelkezik a nagyméretű vetítés és a megfelelő hangosítás biztosítása érdekében. Ha valaki részt szeretne venni valamely előadáson, befolyásolhatja-e őt az ülések elrendezése, vagy csak a konferenciaterem kialakítása számít?

- Előnyösnek vagy hátrányosnak érezzük-e azt, ha az előadó beszéde áthallatszik az egyik teremből a másikba?

- Ha a hallgatóság részéről valakiben kérdés merülne fel az előadás alatt, egyszerűen csak kiáltsa be azt, vagy szükség van a kérdések feltevésével kapcsolatos szabályok bevezetésére, mint például azok összeírása és átadása az egyik szervezőnek? Mi történne, ha nem lennének ilyen szabályozások?

- Ha egy érdekesebb téma kapcsán olyan vita alakul ki, ahol több résztvevőnek is kérdése vagy hozzáfűznivalója van a témához, előfordulhat-e az, hogy az előadó kifut az előírt időből anélkül, hogy minden érintett témát átbeszéltek volna? Miért alakulhat ez így?

- Képzeljük el, hogy az előadás olyan szerkezetű, hogy a résztvevőknek több lehetőségük is van kötetlen vitát folytatni az előadókkal és akár egymással is. Ha ugyanabban a teremben két személy meg akarja szólítani egymást, akkor megtehetik-e ezt nyíltan? Mit kellene tenni, ha az előadó egy olyan személyt akar bevonni az előadásába, aki jelenleg nincs a teremben?

- Mit értünk el azzal, hogy az előadások különálló előadótermekben lettek megtartva, ha a rendezvény után a résztvevőknek lehetőségük van arra, hogy megosszák egymással az információkat?

Csoportos feladat - Mondd el, mit hallottál a konferencián!

Akár egy helyi nyomtatóhoz, akár egy távoli országban található weboldalhoz szeretnénk kapcsolódni, mielőtt bármilyen hálózati kommunikációt folytatnánk, elsőként a fizikai kapcsolatot kell kialakítani a helyi hálózaton. A kapcsolat lehet vezetékes vagy vezeték nélküli, attól függően, hogy kábelt vagy rádióhullámokat használunk az átvitelhez.

A fizikai kapcsolat típusa teljes mértékben a hálózat kialakításától függ. Például, számos vállalati irodában az alkalmazottak asztali és hordozható számítógépei egyaránt kábellel csatlakoznak egy kapcsolóhoz. Ez a fajta kiépítés vezetékes hálózatot jelent, ilyenkor az adatok kábelen keresztül továbbítódnak.

A vezetékes összeköttetés mellett számos vállalat kínál vezeték nélküli kapcsolatot laptopok, táblagépek és okostelefonok számára. Vezeték nélküli eszközök esetében az adatok továbbítását rádióhullámok végzik. A vezeték nélküli kapcsolatok használata a benne rejlő előnyök felfedezésének köszönhetően egyéni és vállalati környezetben is egyre elterjedtebb. Vezeték nélküli szolgáltatások biztosításához a hálózatnak tartalmaznia kell egy vezeték nélküli hozzáférési pontot (Wireless Access Point, WAP), amihez az eszközök csatlakozni tudnak.

A kapcsolók és a hozzáférési pontok általában két különböző eszközként jelennek meg a hálózat megvalósításában. Vannak viszont olyan eszközök is, amelyek vezetékes és vezeték nélküli csatlakozási lehetőséget egyaránt biztosítanak. Számos helyen, például a háztartásokban integrált szolgáltatású forgalomirányítót (ISR) használnak. Egy ilyen eszköz képe látható az 1. ábrán. Az ISR eszközökben található egy több portból álló kapcsolómodul, amely a helyi hálózathoz történő vezetékes kapcsolódási lehetőséget biztosítja néhány eszköz számára. Ez látható a 2. ábrán. Emellett az ISR eszközök általában WAP funkcióval is el vannak látva, amely az eszközök vezeték nélküli kapcsolódását teszi lehetővé.

A hálózati kártyák (NIC) eszközöket csatlakoztatnak a hálózathoz. Az Ethernet kártyák vezetékes, míg a WLAN kártyák vezeték nélküli kapcsolatok létrehozására használhatók. A végfelhasználói eszközökben a két típus legalább egyike megtalálható. Ha egy hálózati nyomtató például csak Ethernet csatlakozóval rendelkezik, akkor a hálózathoz csak kábel használatával tud kapcsolódni. Más eszközök, például a táblagépek és az okostelefonok, csak WLAN adapterrel rendelkeznek, így csak vezeték nélküli kapcsolatot képesek létesíteni.

Hálózati kapcsolódás esetén nem minden fizikai kapcsolat egyenértékű a teljesítmény tekintetében.

Egy vezeték nélküli eszköz például teljesítményromlást tapasztalhat a hozzáférési ponttól való távolsága függvényében. Minél távolabb kerül tőle, annál gyengébbnek érzékeli a vezeték nélküli jelet. Ez akár kisebb sávszélességet vagy a kapcsolat megszakadását is eredményezheti. Az ábrán egy vezeték nélküli jelerősítő látható, amely a ház azon részein található eszközök vezeték nélküli jeleinek felerősítésére használható, amelyek távol esnek a hozzáférési ponttól. Alternatív megoldásként használható vezetékes kapcsolat is, amelynek nem romlik a teljesítménye, viszont rendkívül korlátozott a mozgástere, és általában kötött elhelyezést igényel.

A vezeték nélküli eszközöknek osztozniuk kell a rádióhullámok hozzáférésén. Ez alacsonyabb hálózati teljesítményt is eredményezhet, amint egyidejűleg több eszköz is hozzáfér a hálózathoz. A vezetékes készüléknek nem kell megosztoznia a hálózati hozzáférésen más eszközökkel. Mindegyik eszköz külön kommunikációs csatornát használ a saját Ethernet kábelén keresztül. Ez olyan alkalmazások esetében fontos, mint az online játékok, az online videoközvetítés vagy egy videokonferencia, amelyek a többi alkalmazáshoz képest nagyobb sávszélességet igényelnek.

A következő néhány témakörben részletesebben lesz szó a fizikai rétegbeli kapcsolatokról, valamint azok adatátvitelre gyakorolt hatásáról.

Az OSI modell fizikai rétege biztosítja a adatkapcsolati réteg kereteit alkotó bitek továbbítását a hálózati közegen. Ez a réteg egy teljes keretet fogad az adatkapcsolati rétegtől, és olyan jelek sorozatává alakítja, amelyek továbbíthatók az átviteli közegen. A keretet alkotó bitek származhatnak végberendezéstől vagy közvetítő eszköztől egyaránt.

Az adatok forrásállomástól célállomásig tartó útjának folyamata a következő:

- A felhasználói adatokat a szállítási réteg részekre bontja (szegmentálja), az egyes részeket a hálózati réteg csomagokba helyezi, az adatkapcsolati réteg pedig keretekbe zárja.
- A fizikai réteg kódolja a kereteket és létrehozza azokat az elektromos, optikai vagy rádióhullám jeleket, amelyek a keret bitjeinek felelnek meg.
- Ezután a jelek egyesével elküldésre kerülnek az átviteli közegen.
- A célállomás fizikai rétege fogadja ezeket a jeleket a közegen, bitekké alakítja őket, majd a biteket keretként továbbítja az adatkapcsolati rétegnek.

A hálózati átviteli közegek három alapvető típusa létezik. A fizikai réteg a következő típusú átviteli közegekre állítja elő a bitek megfelelőjét:

- **Rézkábel:** A jelek elektromos impulzusoknak felelnek meg.
- **Optikai kábel:** A jelek fényimpulzusoknak felelnek meg.
- **Vezeték nélküli:** A jelek a mikrohullámú átvitel mintáinak felelnek meg.

Az ábrán réz alapú, optikai és vezeték nélküli átvitel jeleire láthatunk példákat.

A fizikai réteg együttműködési képességének biztosításához olyan szabványügyi szervezetekre van szükség, amelyek az egyes funkciókat minden szempontból felügyelik.

Az OSI modell felső rétegeiben található protokollok szoftveres megvalósítását szoftvertervező mérnökök és számítógépes szakemberek felügyelik. A TCP/IP modell szolgáltatásait és protokolljait például az IETF (Internet Engineering Task Force) nevű szervezet RFC dokumentumok formájában definiálja, ez látható az 1. ábrán.

A fizikai réteg elektromos áramkörökből, átviteli közegekből és mérnökök által kifejlesztett csatlakozókból áll. Emiatt szükséges, hogy a hardverelemek működését irányító szabványokat a megfelelő villamosmérnöki és hírközlési szervezetek hozzák létre.

Számos különböző nemzetközi és nemzeti szervezet, kormányzati szerv és magánvállalat vesz részt a fizikai réteg szabványainak létrehozásában és továbbfejlesztésében. A hardverelemekre, az átviteli közegre, a kódolásra és jelátalakításra vonatkozó szabványokat például a következő szervezetek szabályozzák:

- Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO)
- Távközlési Ipari Szövetség (Telecommunications Industry Association, TIA) és az Elektronikai Iparágak Szövetsége (Electronic Industries Association, EIA)
- Nemzetközi Távközlési Szövetség (International Telecommunication Union, ITU)
- Amerikai Nemzeti Szabványügyi Intézet (American National Standards Institute, ANSI)
- Mérnököket egyesítő nemzetközi szervezet (Institute of Electrical and Electronics Engineers, IEEE)

- Nemzeti távközlési hatóságok, mint például az Egyesült Államokban található Szövetségi Kommunikációs Bizottság (Federal Communication Commission, FCC) és az Európai Távközlési Szabványügyi Intézet (European Telecommunications Standards Institute, ETSI)

A fentieken kívül gyakran helyi kábelezési szabványokért felelős szervezetekkel is találkozhatunk, ilyenek például a kanadai CSA (Canadian Standards Association), az európai CENELEC (European Committee for Electrotechnical Standardization), valamint a japán JSA/JSI (Japanese Standards Association).

A 2. ábrán a főbb szervezetek és azok néhány jellemző szabványának felsorolása látható.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Hálózati eszközök azonosítása
- 2. rész: Hálózati átviteli közegek azonosítása

Laborgyakorlat - Hálózati eszközök és átviteli közegek azonosítása

A fizikai réteg szabványai három fő területtel foglalkoznak:

Fizikai összetevők

Fizikai összetevők alatt olyan elektronikus hardvereszközöket, átviteli közegeket és csatlakozókat értünk, amelyek a biteket reprezentáló jelek továbbítását végzik. A hardverösszetevők, mint például a hálózati kártyák (NIC), a csatlakozófelületek és csatlakozók, a kábelezési anyagok és tervek leírásait a fizikai réteghez kapcsolódó szabványok tartalmazzák. Ilyen szabványosított fizikai összetevőket találhatunk például a Cisco 1941 típusú forgalomirányítóban is.

Kódolás

A kódolás vagy vonali kódolás bitek sorozatának előre meghatározott 'kóddá' történő átalakítási módszerét jelenti. A kódok bitek olyan csoportját jelentik, amelyek elősegítik egy meghatározott minta felismerését a küldő és a fogadó fél által egyaránt. Hálózatok esetében a kódolás során a feszültséget vagy az áramerősséget használjuk az alacsony (0) és a magas bitek (1) reprezentálására.

Az adatok kódolása mellett, a fizikai réteg kódolási eljárásai vezérlési célokra is használhatók, például a keret kezdetének és végének jelölésére.

A leggyakoribb kódolási módszerek az alábbiak:

- **Manchester-kódolás:** A 0 a magas-alacsony, az 1 pedig az alacsony-magas feszültségátmenetet jelenti. Ezt a kódolási típust az Ethernet régebbi változataiban, az RFID azonosításnál és a rövid hatótávú kommunikációban használták.
- **Nullára vissza nem térő (Non-Return to Zero, NRZ):** Egy általánosan használt eljárás, amely az adatok kódolására két állapotot különböztet meg: a nullát és az egyet. A semleges vagy nyugalmi állapotot nem értelmezi. A 0 jelölésére meghatároz egy feszültségszintet a közegen, az 1-et pedig egy ettől különböző feszültségszint jelzi.

Megjegyzés: A gyorsabb adatátviteli sebesség bonyolultabb kódolási eljárásokat igényel. Ilyen például a 4B/5B, amelynek ismertetésével viszont jelen tananyag nem foglalkozik.

Jelzés

A fizikai réteg feladata a közegen továbbított, 1-eseket és 0-kat ábrázoló elektromos, optikai vagy vezeték nélküli jelek létrehozása. A bitek ily módon történő megjelenítésére szolgáló módszert nevezzük jelzési módszernek. Az 1 és a 0 megjelenítésére használható jelek típusát a fizikai réteg szabványaiban kell meghatározni. Ezt a megfeleltetést akár olyan egyszerű dolog is jelentheti, mint az elektromos vagy optikai jelek szintjének megváltozása. A hosszú impulzus például jelentheti az 1-et, a rövid pedig a 0-t.

A Morse-kódot is hasonlóképpen használják a kommunikáció során. Ez egy olyan jelzési módszer, ahol a be- és kikapcsolt hang-, fény- vagy csettintésjelek sorozatát használják szöveges tartalom telefonvonalon keresztüli vagy tengeri hajók közötti továbbítására.

A jelek továbbítása kétféle módon történhet:

- **Aszinkron módon**: Az adatjelek továbbítása órajel hozzárendelése nélkül történik. Az adatokat alkotó karakterek vagy karakterblokkok közötti időtartam tetszőleges lehet, vagyis az időzítési különbség nem szabványosított. Ezért a keretek elejét és végét jelzőbitekkel kell jelölni.

- **Szinkron módon**: Az adatok elküldése egy órajellel együtt történik, amely egyenlő időközönként, más néven bitidőnként fordul elő.

A jelek továbbításának számos módja létezik. Az adatok küldésének legelterjedtebb módja a modulációs technikák használata. A moduláció olyan folyamat, amelynek során az egyik hullám (jel) módosítja a másikat (vivő). A közegen történő adattovábbításhoz az alábbi modulációs technikákat használják széles körben:

- **Frekvenciamoduláció (FM)**: Olyan átviteli módszer, amelyben a vivő frekvencia és a jel egymással összhangban váltakozik.

- **Amplitúdómoduláció (AM)**: Olyan átviteli módszer, amelyben a vivő amplitúdója és a jel egymással összhangban váltakozik.

- **Impulzuskód-moduláció (PCM)**: Olyan technika, amelyben egy analóg jelet (pl.: hangot) a jel amplitúdójának mintavételezésével úgy alakítanak digitális jellé, hogy a különböző amplitúdóértékeket bináris számoknak feleltetik meg. A mintavételezés gyakorisága legalább kétszerese kell legyen a jel legnagyobb frekvenciájának!

A biteket ténylegesen ábrázoló jelek természete függ a használt jelzési módszertől. Egyes módszerek a jel valamely tulajdonságát a 0, egy másik tulajdonságát pedig az 1 ábrázolására használhatják.

A 2. ábra az AM és FM technikák jelek továbbításában történő használatát szemlélteti.

Az egyes átviteli közegek különböző sebességgel biztosítják a bitek továbbítását. Az adatátvitelt általában a sávszélességgel és az átbocsátóképességgel kapcsolatban emlegetik.

A sávszélesség a közeg adatátviteli kapacitását jelenti. A digitális sávszélességet adott idő alatt egyik helyről a másikra átvitt adatmennyiséggel jellemezhetjük. Nagyságát általában kilobit per másodpercben (kb/s) vagy megabit per másodpercben (Mb/s) mérjük.

Egy hálózatban a sávszélesség tényleges értékét az alábbi tényezők kombinációja határozza meg:

- Az átviteli közeg jellemzői.

- A jelátvitelre és jelfelismerésre használt módszerek.

Az átviteli közeg tulajdonságai, az alkalmazott technológiák és a fizikai törvényszerűségek mind szerepet játszanak a rendelkezésre álló sávszélesség meghatározásában.

A táblázat a sávszélesség általánosan használt mértékegységeit tartalmazza.

Az átbocsátóképesség a közegen adott idő alatt átvitt bitek mennyiségét jelenti.

Számos tényezőt figyelembe véve az átbocsátóképesség nem egyezik meg az adott fizikai közegre megadott sávszélesség értékével. A befolyásoló tényezők többek között az alábbiak:

- A forgalom nagysága.
- A forgalom típusa.
- A hálózati eszközök által létrehozott, a forrás és a cél között felmerülő késleltetés.

A késleltetés azt az időtartamot jelenti, amely az adatok egyik pontból a másikba történő eljutásához szükséges.

Egy több szegmensből álló hálózatban az átbocsátóképesség nem lehet nagyobb, mint a forrástól a célig tartó útvonal leglassabb kapcsolatának sebessége. Ez akkor is igaz, ha az összes vagy majdnem az összes szegmens nagy sávszélességű. Elég mindössze egyetlen kis átbocsátóképességű szegmens, amely szűk keresztmetszetet képezhet az egész hálózaton.

Számos online sebességmérő teszt létezik, amelyekkel meghatározható az internetkapcsolat átbocsátóképessége. Az ábra egy sebességmérő teszt mintaeredményét mutatja.

Megjegyzés: Létezik egy harmadik módszer az adattovábbítás mérésére; ez az úgynevezett hasznos átbocsátóképesség (goodput). A goodput értéke az adott idő alatt átvitt használható adatok mennyiségét jelenti. A goodput értékét megkaphatjuk, ha az átbocsátóképességből kivonjuk a kapcsolat felépítésére, nyugtázásra és beágyazásra fordított forgalomtöbbletet.

A fizikai réteg állítja elő a bitcsoportok feszültség, rádiófrekvenciás vagy fényimpulzus formájú megfelelőjét. Különböző szabványügyi szervezetek működtek közre az eltérő átviteli közegek fizikai, elektromos és mechanikai követelményeinek létrehozásában. Ezek a szabványok garantálják, hogy az egyes kábelek és csatlakozók az elvárásoknak megfelelően működjenek, az adatkapcsolati réteg eltérő megvalósításainak esetében is.

A réz alapú átvitelre vonatkozó szabványok például az alábbiakat írják elő:

- A használt rézkábel típusa.
- A kommunikáció sávszélessége.
- A használt csatlakozók típusa.
- A kábel csatlakozóinak lábkiosztása és színkódja.
- A kábel maximális hossza.

Az ábrán a 1941 típusú forgalomirányítón megtalálható interfészek és portok láthatók.

A hálózatokban azért használunk rézkábelt, mert olcsó, könnyen telepíthető és kicsi az ellenállása az elektromos árammal szemben. Hátránya viszont, hogy korlátozott a kábelhossz, és érzékeny az interferenciára.

A rézkábelben az adatok elektromos impulzusok formájában továbbítódnak. A vevőkészülék hálózati interfészének érzékelője fogadja azokat a jeleket, amelyekből sikeresen vissza tudja állítani az elküldött jelet. Azonban minél nagyobb távolságra továbbítódik a jel, annál inkább érvényesül a

csillapításnak nevezett jelenség. Emiatt minden réz alapú kábelnél be kell tartani a szabványokban meghatározott szigorú hosszúsági korlátozásokat.

Az elektromos impulzusok időzítési és feszültségértékei két forrásból származó interferenciára érzékenyek:

- **Elektromágneses interferencia (EMI) vagy rádiófrekvenciás interferencia (RFI) -** Az EMI és az RFI jelek torzíthatják és tönkretehetik a rézkábelben továbbított adatjeleket. A jellemző zavarforrások közé sorolhatók a rádióhullámok és az elektromágneses eszközök, például a fluoreszkáló lámpák vagy az elektromos motorok.

- **Áthallás** - Áthallás alatt azt értjük, ha egy vezetéken haladó jel elektromos vagy mágneses mezője által keltett zavar átterjed a szomszédos vezetéken található jelre. Telefonvonalakon az áthallás következménye lehet, hogy halljuk egy szomszédos vonalon zajló másik beszélgetés részleteit. Tehát, amikor egy vezetéken elektromos áram folyik keresztül, a huzal körül kis méretű, körkörös mágneses mező alakul ki, amely a szomszédos vezetékre is kifejti hatását.

Az ábrán látható animáció lejátszásával megtekinthetjük, hogyan befolyásolja az interferencia az adatátvitelt.

Az EMI és az RFI negatív hatásainak ellensúlyozására néhány rézkábel típusban fémes árnyékolást alkalmaznak és előírják a kapcsolat megfelelő földelését.

Az áthallás negatív hatásainak csökkentése érdekében bizonyos rézkábel fajtákban az ellentétes áramköri érpárokat összesodorják, ezzel tudnak hatékonyan fellépni ellene.

A rézkábel elektromos zajokra való érzékenysége az alábbi tényezőkkel korlátozható:

- Az adott hálózati környezetben leginkább alkalmazható kábel típusának vagy kategóriájának kiválasztása.

- Kábelezési terv készítése az ismert és az előre látható interferencia források elkerülésére.

- A kábelek megfelelő kezelésére és lezárására vonatkozó kábelezési technikák használata.

A hálózatokban használt réz alapú átviteli közegeknek három fő típusa létezik:

- **Árnyékolatlan csavart érpár (Unshielded Twisted-Pair, UTP)**

- **Árnyékolt csavart érpár (Shielded Twisted-Pair, STP)**

- **Koaxiális**

Ezeket a kábeleket LAN hálózati csomópontok és eszközök, például kapcsolók, forgalomirányítók, valamint vezeték nélküli hozzáférési pontok összekötésére használjuk. A különböző kapcsolattípusok és a velük járó eszközök esetében fizikai rétegbeli szabványok határozzák meg a kábelezési követelményeket.

A különféle szabványok eltérő csatlakozók használatát írják elő. Ezekben határozzák meg minden csatlakozótípus esetében a fizikai paramétereket és a megfelelő elektromos tulajdonságokat. A hálózati közegek moduláris aljzatokat és csatlakozókat használnak az egyszerű csatlakoztatás és szétkapcsolás érdekében. Egyetlen csatlakozótípus többféle kapcsolat esetén is használható. Például, az RJ-45 típusú csatlakozót széles körben alkalmazzák LAN és WAN hálózati közegekben is.

Az árnyékolatlan csavart érpáras kábel (UTP) a leggyakrabban használt hálózati átviteli közegtípus. Az UTP kábelek RJ-45-ös csatlakozókban végződnek, hálózati állomások és hálózati eszközök (pl.: kapcsolók,forgalomirányítók) közötti összeköttetés létrehozására használják.

A helyi hálózatokban használt UTP kábel négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amely rugalmas műanyag köpenybe van befoglalva a fizikai károsodástól való védelem miatt. A vezetékek csavarása a más vezetékekről származó jelinterferencia elleni védelemre szolgál.

Ahogy az ábrán is látható, a színkódok az egyes vezetékpárok és a párokban található vezetékek azonosítására szolgálnak, valamint segítenek a kábelek végződéseinek létrehozásában.

Az árnyékolt csavart érpáras kábel (STP) jobb zaj elleni védelmet biztosít, mint az UTP kábel. Viszont az UTP-hez hasonlítva az STP kábel lényegesen drágább, és nehezebb is telepíteni. Az UTP-hez hasonlóan RJ-45-ös csatlakozót használ.

Az STP kábel az EMI és az RFI ellen használt árnyékolási technikákat kombinálja az áthallás elleni védelmet szolgáló vezetékcsavarással. A teljes értékű árnyékolás eléréséhez az STP kábelek speciálisan árnyékolt STP csatlakozókban végződnek. Ha a kábel nem megfelelően van leföldelve, az árnyékolás antennaként viselkedve összegyűjtheti a nemkívánatos jeleket.

Számos különböző STP kábeltípus áll rendelkezésre, amelyek mindegyike eltérő tulajdonságokkal bír. A két legelterjedtebb típus viszont a következő:

- Az STP kábel a teljes vezetékköteget árnyékolja egy fóliával, ezzel gyakorlatilag az összes interferenciát kiküszöböli (elterjedtebb).

- Az STP kábel a teljes vezetékköteg árnyékolása mellett az egyes vezetékpárokat is fóliával borítja, így akadályozva meg az interferenciát.

Ahogy látható, az STP kábel négy érpárt használ. Ezek mindegyike fóliaárnyékolással van borítva, amelyek aztán még egy fémhálóval vagy fóliával is be vannak burkolva.

Sok éven át az STP volt a vezérjeles hálózatok telepítésére előírt kábelezési megoldás. Azonban a vezérjeles hálózatok iránti kereslet csökkenésével az STP kábel iránti igény is megcsappant. Az új 10GB-es Ethernet szabvány viszont az STP kábel használatára vonatkozó rendelkezést is tartalmaz, amely az árnyékolt csavart érpáras kábelek iránti érdeklődés megújulását eredményezheti.

A koaxiális kábel vagy röviden koax elnevezés a vezeték szerkezetéből származik, azaz két vezető (conductor) egy közös tengelyen (axis) osztozik. Ahogy az ábrán is látható, a koaxiális kábel az alábbi részekből áll:

- Egy rézvezető, amely az elektronikus jelek továbbítását végzi.

- A rézvezetőt körülvevő rugalmas műanyag szigetelőréteg.

- A szigetelőanyagot beborító rézfonat vagy fémfólia, amely az áramkör második vezetékeként és a belső vezető árnyékolójaként működik. Ez a második réteg (más néven árnyékolás) a külső elektromágneses interferencia hatását is csökkenti.

- A kisebb fizikai sérülések elleni védelem érdekében az egész kábel egy borítással van bevonva.

Megjegyzés: A koaxiális kábelhez különböző típusú csatlakozók használhatók.

A koaxiális kábelt hagyományosan a kábeltelevíziós technológiáknál használták egyirányú adattovábbításra. A korai Ethernet változatokban is széles körben elterjedt volt.

Habár a mai Ethernet hálózatokban az UTP kábel lényegében felváltotta a koax kábelt, a koax kábelnek több felhasználási területe is létezik:

- **Vezeték nélküli berendezések:** A koaxiális kábel antennákat kapcsol össze vezeték nélküli eszközökkel. A kábel hordozza a rádiófrekvenciás (RF) energiát az antennák és a rádiós berendezés között.

- **Kábeles internet-megvalósítások**: A kábelszolgáltatók a jelenlegi egyirányú rendszereiket kétirányúra alakítják át, hogy képesek legyenek internetkapcsolatot nyújtani az ügyfeleiknek. Az internetszolgáltatások biztosítása érdekében a koaxiális kábelt és az erősítő eszközöket bizonyos részeken le kell cserélni optikai kábelre. Habár az előfizető helyi kapcsolatánál és az ügyfél telephelyén még mindig a koaxiális kábel a jellemző. Az optikai és koaxiális közegek kombinált használatát fényvezető-koax hibrid (HFC) rendszernek hívjuk.
  - Mindhárom típusú réz alapú közeg érzékeny a tűz és az elektromosság okozta veszélyekre.
  - A tűzveszély a kábelek szigetelését és borítását alkotó anyagokból ered, mivel ezek gyúlékonyak lehetnek, és felmelegedve vagy elégve mérges gázok felszabadulását okozhatják. A kábelezésre és a hardvereszközök telepítésére vonatkozó biztonsági előírásokat az építési hatóságok vagy szervezetek szabályozhatják.
  - Az áramütést is veszélyforrásnak tekinthetjük, mivel a rézvezeték kiszámíthatatlan módon képes vezetni az elektromosságot. Így a személyzet és a berendezések is egy sor áramütés okozta veszélynek vannak kitéve. Egy hibás hálózati eszköz például átvezetheti az áramot más eszközök vázaiba. Továbbá a hálózati kábelezés nem kívánatos feszültségszinteket is eredményezhet, ha olyan eszközöket csatlakoztatunk, amelyek eltérő földpotenciálú áramforráshoz kapcsolódnak. Ilyen helyzetek akkor fordulhatnak elő, ha különböző épületben vagy másik szinten található hálózatokat kötünk össze rézkábellel, és ezekben eltérő elektromos berendezéseket használunk. Végezetül a rézkábelek a villámcsapásból származó feszültségtöbbletet is elvezethetik a hálózati eszközök felé.
  - A nemkívánatos feszültség és áram következményeként kár keletkezhet a hálózati eszközökben és a csatlakoztatott számítógépekben, illetve a személyzet sérülését is okozhatja. Fontos, hogy a rézkábelek telepítése megfelelően történjen, a rájuk vonatkozó előírások és szerelési szabályok betartásával, annak érdekében, hogy a potenciális veszélyhelyzetek elkerülhetőek legyenek.
  - Az ábrán a helyes kábelezési gyakorlat képei láthatók, ennek köszönhetően elkerülhetők az esetleges tűz és áramütés okozta balesetek.

Hálózati átviteli közegként használva az árnyékolatlan csavart érpár (UTP) négy pár, színkóddal jelölt, egymással összecsavart vezetékből áll, amelyek rugalmas műanyag köpenybe vannak befoglalva. A hálózati UTP kábel négy pár 22-es vagy 24-es értékű mérőszámmal (a vezeték átmérőjéből számítják) rendelkező vezetékből áll. A kábel külső átmérője körülbelül 0,43 cm (0,17 inch), a kis méret a telepítés során jelenthet előnyöket.

Az UTP kábel nem használ árnyékolást az EMI és az RFI hatásainak kivédésére. A kábeltervezők ehelyett felismerték, hogy mivel tudják ellensúlyozni az áthallás negatív hatásait:

- **Kioltás**: A tervezők a vezetékpárokat egy áramkörként hozzák létre. Ha az áramkörben ezt a két vezetéket közel helyezzük el egymáshoz, a két vezeték által keltett mágneses mező pontosan ellentétes irányú lesz. Emiatt a két mágneses mező kioltja egymást, valamint a külső forrásból származó EMI és RFI jeleket is.

- **A vezetékpárok csavarásszámainak változtatása**: A kioltási effektus hatásának fokozása érdekében eltérő számú csavarást alkalmaznak az egyes vezetékpárokban. UTP kábel használatakor szigorú előírásokat kell követni a méterenkénti csavarások számát illetően. Figyeljük meg az ábrán, hogy a narancs/narancs-fehér vezetékpár kevésbé csavart mint a kék/kék-fehér pár! Mindegyik színezett vezetékpár eltérő számú csavarást tartalmaz.

Az UTP kábel kizárólag a vezetékek csavarásából eredő kioltási hatásra támaszkodik a jelromlás csökkentésének érdekében, valamint hatékonyan biztosítja a vezetékpárok önárnyékolását a közegen belül.

Az UTP kábel a TIA/EIA által közösen összeállított szabványokban foglaltaknak felel meg. Pontosabban a TIA/EIA-568A szabvány az, amely meghatározza a LAN hálózatok kábelezési előírásait, és a leggyakrabban előforduló LAN kábelezési szabványnak számít. Néhány, a szabványban definiált elem a következő:

- Kábeltípus
- Kábelhossz
- Csatlakozó
- Kábelvégződés
- Kábeltesztelési módszerek

A rézkábel elektromos jellemzőit a mérnököket egyesítő nemzetközi szervezet, az IEEE határozza meg. Az IEEE az UTP kábeleket a teljesítményük alapján minősíti. Kategóriákba sorolja őket aszerint, hogy mekkora adatátviteli sebességre képesek. Az 5-ös kategóriájú (Cat5) kábelt például a 100BASE-TX FastEthernet típusú megvalósításoknál használják. A további kategóriák közé tartozik a továbbfejlesztett 5-ös kategóriájú (Cat5e), 6-os kategóriájú (Cat6) és a 6a kategóriájú (Cat6a) kábel is.

A magasabb kategóriájú kábel nagyobb adatátviteli sebességeket támogat. Az új, gigabites sebességű Ethernet technológiák bevezetésével a Cat5e kevésbé elfogadott kábeltípussá vált, helyette a Cat6 típus használata javasolt új kábelezések kiépítésekor.

Az ábra a különböző kategóriájú UTP kábeleket emeli ki.

Megjegyzés: Néhány gyártó a Cat6a kategória követelményeit túlteljesítő kábeleit Cat7 jelzővel látja el.

Az UTP kábel végződéseit általában az ISO 8877 szabványú RJ-45 csatlakozóval zárjuk le. Ezt a csatlakozót használják számos fizikai réteg specifikációjában, amelyek egyike az Ethernet. A TIA/EIA 568 szabvány az Ethernet kábelben található vezetékek színkódjait és az aljzatok bekötését (lábkiosztást) írja le.

Az 1. ábrán lévő videón egy UTP kábel RJ-45 csatlakozóval történő lezárását lehet megtekinteni.

A 2. ábrán látható, hogy az RJ-45 csatlakozó a kábel végére szorított (krimpelt) dugaszt jelenti. A csatlakozóaljzat a konnektor típusú összetevőt jelenti, amelyet hálózati eszközbe, falba, kabinszerű munkahelyi fülkékbe vagy patch panelbe szerelnek bele.

A rézkábelek csatlakozóinak szerelésekor fennáll a jelveszteség és az áramkörben fellépő zaj kialakulásának esélye. Minden egyes helytelenül szerelt csatlakozó potenciális forrása lehet a fizikai jelek teljesítménycsökkenésének. Fontos, hogy a rézkábeleket lezáró csatlakozók jó minőségűek legyenek, annak érdekében, hogy a a jelenlegi és jövőbeni hálózati technológiák esetében is optimális teljesítményt tudjanak nyújtani.

A 3. ábrán egy helyesen és egy helytelenül lezárt UTP kábelre láthatunk példát.

Az eltérő helyzetek különböző szabványú UTP kábelbekötések használatát követelik meg. Ez azt jelenti, hogy az egyes vezetékeket a kábelben különböző sorrendben kell csatlakoztatni az RJ-45 csatlakozó különböző érintkezőihez.

A kábelezési szabványoknak megfelelően a fő kábeltípusok az alábbiak:

- **Egyeneskötésű Ethernet kábel**: A leggyakrabban használt hálózati kábeltípus. Általában állomás és kapcsoló, valamint kapcsoló és forgalomirányító közötti összeköttetéseknél használjuk.

- **Keresztkötésű Ethernet kábel**: Egy nem túl gyakran használt kábeltípus, hasonló eszközök összekötésére. Összeköthetünk vele például kapcsolót kapcsolóval, állomást állomással vagy forgalomirányítót forgalomirányítóval.

- **Rollover kábel**: A Cisco saját tervezésű kábele, amelyet a forgalomirányítók vagy kapcsolók konzolportjához történő csatlakozásra használhatunk.

A kereszt- vagy egyeneskötésű kábelek helytelen használata nem károsítja az eszközt, ilyen esetben viszont nem jön létre az eszközök közötti kapcsolat és adatkommunikációra sem kerül sor. Laborhasználat során ez gyakori hibának számít, ezért ha a kapcsolat nem elérhető, a hibaelhárítás első lépéseként az eszközök összeköttetéseinek helyességét kell ellenőrizni.

Az ábra az UTP kábeltípusokat, a kapcsolódó szabványokat és a kábelek jellemző alkalmazási területeit mutatja. Ezen felül azonosítja a TIA 568A és TIA 568B szabványok szerinti vezetékpárokat.

Kábelkészítés után egy UTP kábeltesztelővel a következő paramétereket ajánlott ellenőrizni:

- Vezetéktérkép

- Kábelhossz

- A csillapítás következtében fellépő jelveszteség

- Áthallás

Javasolt az UTP kábel készítésére vonatkozó összes követelmény teljesülését alaposan ellenőrizni!

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: Ethernet kábelezési szabványok és érintkezőkiosztások tanulmányozása.

- 2. rész: Keresztkötésű Ethernet kábel készítése.

- 3. rész: Keresztkötésű Ethernet kábel tesztelése.

Laborgyakorlat - Keresztkötésű Ethernet kábel készítése

A hálózatok gerincét alkotó eszközök összekapcsolására leginkább optikai kábelt használnak. Bármely más hálózati közeghez képest hosszabb távolságú és nagyobb sávszélességű adatátvitelt tesz lehetővé.

Az optikai szál egy rugalmas, de rendkívül vékony, átlátszó anyagú nagyon tiszta üveg (szilícium-dioxid), amely nem sokkal vastagabb az emberi hajszálnál. A bitek fényimpulzusként jelennek meg a szálon. A száloptikai kábel hullámvezetőként vagy 'fénycsőként' viselkedik amikor minimális veszteséggel továbbítja a fényt két végpont között.

A működés szemléltetésére képzeljünk el egy ezer méter hosszúságú üres papírhengert, amelynek a belseje tükörrel van bevonva, benne egy kis lézerpointert használnak Morze-kódok fénysebességgel történő továbbítására. A száloptikai kábel lényegében így működik, kivéve, hogy kisebb az átmérője és kifinomultabb fénykibocsátó és -fogadó technológiákat használ.

A réz vezetékekkel ellentétben az optikai kábel kisebb csillapítással képes a jeltovábbításra, valamint teljesen érzéketlen az EMI és az RFI okozta zavarokra.

Az optikai kábelnek jelenleg az alábbi négy ipari felhasználási területe létezik:

- **Nagyvállalati hálózatok**: Gerinchálózat kábelezése és a hálózat infrastruktúráját alkotó eszközök összekötése.

- **FTTH és felhasználói hálózatok**: Az üvegszál az otthonig (Fiber-to-the-home, FTTH) típusú hálózat folyamatos szélessávú kapcsolatot biztosít az otthoni és kisvállalati felhasználók számára. Nagy sebességű internet-hozzáférést nyújt elérhető áron, valamint támogatja a számítógépes távmunkát, a távfelügyeleti orvosi ellátást, azaz a telemedicinát, valamint a digitális videótárat (Video on Demand).

- **Nagytávolságú hálózatok**: Országok és városok összekötésére a szolgáltatók nagytávolságú, szárazföldi optikai hálózatokat használnak. A hálózatok mérete jellemzően a néhány tucattól a néhány ezer kilométerig terjed, és akár 10 Gb/s sebességen is működhetnek.

- **Tenger alatti hálózatok**: A nagy sebességet és kapacitást biztosító, óceáni távolságokat is áthidaló megvalósításokhoz olyan speciális optikai káblelt használnak, amely képes ellenállni a tengerek alatt lévő mostoha körülményeknek is.

A tananyag a vállalati hálózatokban használt optikai kábelekre fekteti a hangsúlyt.

Annak ellenére, hogy az optikai kábel nagyon vékony, kétféle üvegből és egy külső védőrétegből áll. Ezek az alábbiak:

- **Mag**: Tiszta üvegből áll, és az optikai szál ezen része továbbítja a fényimpulzusokat.

- **Héj**: Ez az üvegrész veszi körül a magot, és úgy működik mint egy tükör. A fényimpulzusok addig terjednek a magban, amíg a héj vissza nem tükrözi őket. Így a fényimpulzusok a mag belsejében maradnak. Ezt a jelenséget teljes visszaverődés néven ismerjük.

- **Köpeny**: Általában egy műanyag burkolatot jelent, amely a mag és a héj védelmére szolgál. Emellett megerősítést biztosító anyagokat és védőbevonatot is tartalmazhat, amelyek célja az üveg karcolásoktól és nedvességtől való védelme.

Habár a mag és a héj az erős hajlításokra érzékeny, a tulajdonságaikat molekuláris szinten úgy alkották meg, hogy azok nagyon erősek legyenek. Az optikai kábel szigorú ellenőrzéseken esik át a gyártási folyamat során, hogy elviselje a legalább 100.000 font per négyzethüvelyk (~690MPa) nagyságú nyomást is. A kábelnek olyan tartósnak kell lennie, hogy a ellenálljon a telepítéskor fellépő hatásoknak, valamint világ bármely táján előforduló szélsőséges környezeti hatásoknak is.

A közegen továbbított adatoknak megfelelő fényimpulzusokat a következő módokon állíthatjuk elő:

- Lézerfénnyel

- Fénykibocsátó diódával (LED-del)

A beérkező fényimpulzusokat elektronikus félvezető eszközök, úgynevezett fotodiódák érzékelik, és alakítják át őket feszültségszintekké, amelyekből előállíthatóak az elküldött adatkeretek.

Megjegyzés: Az optikai kábelekben alkalmazott lézerfény az emberi szem számára veszélyes lehet. Ügyelni kell arra, hogy ne nézzünk bele a működő optikai kábel végébe!

Az optikai kábelek nagyjából két csoportba sorolhatók:

- **Egymódusú kábel (Single-mode fiber, SMF)**: Nagyon vékony magból áll, valamint drága lézeres technológiát használ a fénysugár elküldésére. Főleg az egymástól nagy távolságra, akár több száz kilométerre lévő helyek összekötésére használják, például hosszútávú telefonos és kábeltelevíziós felhasználás során.

- **Többmódusú kábel (Multimode Fiber, MMF)**: Nagyobb a mag átmérője, és LED forrást használ a fényimpulzusok kibocsátására. A LED-ből származó fény különböző szögekben léphet be a szál belsejébe. Helyi hálózatokban népszerű, mivel alacsony költségű LED-ekkel üzemel. Akár 10 Gb/s adatátviteli sebességet is elérhetünk vele, a maximális 550 méteres kábelhosszon.

Az 1. és a 2. ábra az egy- és többmódusú kábelek jellemzőit tartalmazza. A kiemelt különbségek egyike a szóródás mértékét jelenti. A szóródás arra utal, hogy a fényimpulzus mennyire terjed szét egy bizonyos idő eltelte után. Minél nagyobb a szóródás mértéke, annál inkább csökken a jelerősség.

Az optikai csatlakozók az optikai szálak végződéseit zárják le. Ezeknek számos típusa elérhető. A fő különbség közöttük a méretből és a mechanikai kapcsolódás módjából adódik. A szervezetek általában azt az egyféle csatlakozótípust szabványosítják, amelyet gyakran használnak a berendezéseikben, illetve kábeltípusokként egy-egy szabványt hoznak létre (egyet az egymódusú, egyet a többmódusú kábelnek). Az összes generációt figyelembe véve, napjainkban körülbelül 70 csatlakozótípus van használatban.

Az első ábrán a három leggyakrabban használt optikai csatlakozótípus látható, ezek az alábbiak:

- **ST csatlakozó (Straight-Tip)**: Régi bajonettzáras csatlakozó, amelynek használata a többmódusú szálak esetében elterjedt.

- **SC csatlakozó (Subscriber Connector)**: Négyzetes vagy szabványos csatlakozónak is nevezik. Széles körben elterjedt LAN és WAN hálózati csatlakozótípus, amely megnyom-kihúz (push-pull) típusú mechanizmust használ a biztos csatlakozás érdekében. Egy- és többmódusú kábelek esetében egyaránt használják ezt a típust.

- **LC csatlakozó (Lucent Connector)**: A kicsi vagy helyi csatlakozó néven is említett típus gyors népszerűségre tett szert a kis mérete miatt. Leginkább egymódusú kábeleknél használják, de támogatja a többmódusú szálakat is.

Megjegyzés: Más típusú optikai csatlakozók is léteznek, például az FC (Ferrule Connector) és az SMA (Sub Miniature A) csatlakozók, azonban ezeket nem igazán használják a LAN és WAN hálózatokban. A Biconic és a D4 csatlakozók pedig már elavult típusnak számítanak. Ezen csatlakozók ismertetése nem tartozik a fejezet feladatai közé.

Mivel a fény csak egy irányban továbbítódik a szál belsejében, ezért a full duplex átvitel megvalósításához két optikai szál szükséges. Az optikai lengőkábelek (patch kábelek) emiatt két optikai szálat foglalnak magukban, a végződésüket pedig szabványos optikai csatlakozópárral valósítják meg. Az 1. ábrán látható duplex csatlakozó néven ismert típusok mindegyike alkalmas az adó és vevő szálak bekötésére egyaránt.

Az optikai patch kábelt a hálózatok gerincét alkotó eszközök összekötésére használják. A 2. ábrán ilyen kábelre láthatunk példákat:

- SC-SC többmódusú patch kábel

- LC-LC egymódusú patch kábel

- ST-LC többmódusú patch kábel

- SC-ST egymódusú patch kábel

A kábeleket műanyag lezáró kupakkal kell védeni, amikor nem használjuk őket.

Vegyük észre, hogy az egy- és többmódusú kábelek között a kábel színe tesz különbséget! Ennek oka, hogy a TIA-568 szabvány a sárga színt javasolja az egymódusú, a narancs (vagy vízkék) színt pedig a többmódusú kábelek külső borításaként.

Az optikai szálak lezárása és összeillesztése speciális képzettséget és gyakorlatot igénylő feladat. A kábel helytelen lezárása az átviteli távolság lerövidülését vagy az átvitel teljes sikertelenségét eredményezheti.

A három leggyakoribb hiba a következő:

- **Nem megfelelő illesztés**: Az optikai kábelek nem pontosan igazodnak egymáshoz az összeillesztéskor.
- **Záró hézag**: A kábel nem teljesen érintkezik az illesztésnél vagy a lezárásnál.
- **A végek megmunkálása**: A kábelvégek nincsenek megfelelően megtisztítva, illetve a lezárásnál szennyeződés található.

Egy gyors és egyszerű vizsgálat a helyszínen is elvégezhető, ha erős fényű zseblámpával a kábel egyik végén bevilágítunk, és eközben figyeljük a kábel másik végét. Ha ott fény látható, akkor a szál képes a fény továbbítására. Habár ez a módszer nem alkalmas a kábel teljesítményének vizsgálatára, mégis egy gyors és olcsó lehetőséget biztosít a törött szálak felderítésére.

Optikai kábelek vizsgálatára az ábrán is látható optikai tesztelő eszköz használata javasolt. Az optikai időtartománybeli reflektométer (Optical Time Domain Reflectometer, OTDR) bármely kábelszakasz ellenőrzésére használható. A készülék egy teszt-fényjelet bocsát a kábel belsejébe, és az idő függvényében méri annak visszaverődését. Ebből számítja ki azt a körülbelüli távolságot, amellyel meghatározható, hogy a kábel melyik részén található a hiba.

Az optikai kábel használatának számos előnye van a rézkábelekhez képest.

Tekintve, hogy az optikai kábelben használt szálak nem elektromos vezetők, ezáltal a közeg nem érzékeny a elektromágneses interferenciára, továbbá a földelés kérdésével sem kell foglalkozni, mivel az elektromos áramot sem vezeti. Mivel az optikai kábel vékony és a jelvesztesége is viszonylag alacsony, ezért a rézkábelhez képest lényegesen nagyobb távolságokon is használható jelerősítés nélkül. Az optikai kábel fizikai leírására vonatkozó szabványok némelyike akár több kilométeres távolság áthidalását is engedélyezi.

Az optikai kábelek kivitelezésével kapcsolatos kérdések az alábbiak:

- Ugyanakkora távolság áthidalásakor (általában) drágább, mint a rézkábeles megvalósítás (viszont nagyobb teljesítményű).
- Speciális készségek és eszközök szükségesek a kábelek lezárásához és összeillesztéséhez.
- Alaposabb kezelést igényel, mint a rézkábel.

Napjainkban az optikai kábelt vállalati környezetben elsősorban gerinchálózati kábelezésnél használják különböző létesítmények nagyforgalmú pont-pont összeköttetéseinek megvalósításakor, illetve egyetemeken az egyes épületek összekötésére. Az optikai kábel remekül alkalmazható ezen célokra, mivel nem vezeti az elektromosságot és kicsi a jelvesztesége.

Az ábrán a főbb különbségek vannak kiemelve.

A vezeték nélküli közeg rádió- vagy mikrohullámok használatával továbbítja az elektromágneses jeleket, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg.

A vezeték nélküli átvitel hálózati közege a réz és optikai közeggel ellentétben nincs vezetékekhez kötve. Az összes közegtípus közül a vezeték nélküli biztosítja a legnagyobb mobilitást. Ezen felül a vezeték nélküli átvitelt használó eszközök száma is folyamatosan növekszik. Ezen okok miatt válhatott az otthoni hálózatok elterjedt közegtípusává. A hálózati sávszélesség növekedésének köszönhetően rövid idő alatt a vállalati hálózatokban is egyre nagyobb teret fog hódítani magának.

Az ábrán a vezeték nélküli átvitelhez kapcsolódó különféle szimbólumok láthatók.

Vannak azonban a vezeték nélküli átvitelnek is problémás területei, többek között:

- **Lefedettségi terület**: A vezeték nélküli adatátviteli technológiák kiválóan működnek nyitott környezetben. Ugyanakkor az épületekben használt egyes építési anyagok és a helyi földrajzi viszonyok korlátozzák a tényleges lefedettséget.

- **Interferencia**: A vezeték nélküli átvitel érzékeny az interferenciára, és olyan hétköznapi eszközök is zavarhatják az átvitelt, mint például a vezeték nélküli telefonok, bizonyos fénycsőtípusok, mikrohullámú sütők és más vezeték nélküli eszközök.

- **Biztonság**: A lefedettségi területen belül nem kell fizikailag a közeghez kapcsolódni annak használatához. Emiatt az erre nem jogosult eszközök és felhasználók is hozzáférhetnek a hálózathoz. Következésképpen a hálózatbiztonság a vezeték nélküli hálózatok felügyeletének egyik fő összetevője.

Habár a vezeték nélküli technológia egyre népszerűbb a kis távolságú összeköttetések esetében, még mindig a réz- és optikai kábel számít a legnépszerűbb fizikai közegnek a hálózati alkalmazásokban.

A vezeték nélküli átvitelre vonatkozó IEEE és ipari távközlési szabványok mind az adatkapcsolati, mind pedig a fizikai rétegre kiterjednek.

A következő adatátviteli szabványok mindegyike a vezeték nélküli átvitelre vonatkozik:

- **IEEE 802.11**: A vezeték nélküli LAN (WLAN) technológia, közismertebb nevén Wi-Fi, egy versengés alapú vagy nem determinisztikus rendszer, amely az ütközést elkerülő, vivőérzékeléses, többszörös hozzáférésű (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) rendszert használja a közeghozzáférés vezérlésére.

- **IEEE 802.15**: A vezeték nélküli személyes hálózatok (Wireless Personal Area Network, WPAN) szabványa, közismert nevén a Bluetooth, amely egy eszközpárosítási folyamatot használ az 1 és 100 méter közötti kommunikáció lebonyolítására.

- **IEEE 802.16**: Közismert nevén a WiMAX (Worldwide Interoperability for Microwave Access), amely pont-multipont topológiát használ a szélessávú vezeték nélküli hozzáférés biztosításához.

Az ábra az egyes vezeték nélküli technológiák közti különbségeket tartalmazza.

Megjegyzés: Más vezeték nélküli technológiák, például a mobil és a műholdas kommunikáció szintén nyújthat adathálózati kapcsolatot. Ezek a technológiák azonban nem képezik részét a fejezetnek.

A fenti példák mindegyikének fizikai rétegre vonatkozó specifikációja a következő területeket foglalja magában:

- Az adatok rádiójelekké történő átalakítása.

- Átviteli frekvencia és teljesítmény

- A jel vételére és dekódolására vonatkozó követelmények.

- Antennák tervezése és kivitelezése.

Megjegyzés: A Wi-Fi védjegy tulajdonosa a Wi-Fi Szövetség. A Wi-Fi megnevezés azokra a tanúsított WLAN eszközökre vonatkozik, amelyek a 802.11 szabványok alapján működnek.

A vezeték nélküli hálózat közös adatátviteli közege lehetővé teszi az eszközök számára, hogy vezeték nélkül csatlakozzanak egymáshoz egy LAN-on keresztül. Egy vezeték nélküli LAN általában a következő eszközök használatát követeli meg:

- **Vezeték nélküli hozzáférési pont (Access Point, AP)**: Fogadja a felhasználók vezeték nélküli jeleit, és általában rézkábellel csatlakozik a meglévő vezetékes hálózathoz, például az Ethernethez. Ahogy az ábrán is látható, az otthoni és kisvállalati környezetben használt vezeték nélküli forgalomirányító egy eszközben tartalmazza a forgalomirányító, a kapcsoló és a hozzáférési pont funkcióit.

- **Vezeték nélküli hálózati kártya**: Vezeték nélküli kommunikációs képességeket biztosít a hálózati állomások számára.

A technológia fejlődésével számos Ethernet alapú WLAN szabvány alakult ki. Körültekintően kell eljárni a vezeték nélküli eszközök vásárlásakor a kompatibilitás és az együttműködési képesség biztosítása érdekében.

A vezeték nélküli kommunikáció előnyei nyilvánvalóak, különösen ha a költséges kábelezés megtakarításáról és a hordozhatóságból adódó kényelemről beszélünk. Azonban a hálózati rendszergazdának úgy kell megalkotnia és alkalmaznia a szigorú biztonsági szabályokat, hogy a vezeték nélküli LAN védve legyen az illetéktelen hozzáférésektől és támadásoktól.

Az évek során különböző 802.11 szabványok fejlődtek ki. Ezek az alábbiak:

- **IEEE 802.11a**: Az 5 GHz-es frekvenciasávban működik, és maximális adatátviteli sebessége 54 Mb/s. A magasabb üzemelési frekvenciák miatt kisebb a lefedettségi területe, és kevésbé hatékony az épületfalakon keresztül történő továbbításban. A szabvány alapján működő eszközök nem képesek együttműködni az alábbiakban részletezett 802.11b és 802.11g eszközökkel.

- **IEEE 802.11b**: A 2,4 GHz-es frekvenciasávban működik, és maximális adatátviteli sebessége 11 Mb/s. A szabvány alapján működő eszközök a 802.11a-hoz hasonlítva nagyobb hatótávolsággal rendelkeznek, és a jeleik hatékonyabban tudnak áthatolni az épületfalakon.

- **IEEE 802.11g**: A 2,4 GHz-es frekvenciasávban működik, és maximális adatátviteli sebessége 54 Mb/s. A szabvány alapján működő eszközök emiatt a 802.11b-vel megegyező frekvencián és lefedettségi területtel működnek, ugyanakkor a 802.11a által biztosított sávszélességgel.

- **IEEE 802.11n**: A 2,4 GHz-es és az 5GHz-es frekvenciasávokon üzemel. A tipikus adatátviteli sebesség 100 Mb/s és 600 Mb/s között mozog, a maximális hatótávolság pedig 70 méter. Visszafelé kompatibilis a 802.11a/b/g eszközökkel.

- **IEEE 802.11ac**: Egyidejűleg képes a 2,4 GHz-es és az 5 GHz-es frekvenciatartományban történő működésre, maximális adatátviteli sebessége 450 Mb/s-tól 1,3 Gb/s-ig (1300 Mb/s) terjed. Visszafelé kompatibilis a 802.11a/b/g/n eszközökkel.

- **IEEE 802.11ad**: "WiGig" néven is ismert. A 2,4 GHz-es, az 5 GHz-es, valamint a 60 GHz-es frekvenciasávokat használva képes a háromsávos működésre, az elméleti adatátviteli sebessége pedig akár a 7 Gb/s-ot is elérheti.

Az ábrán a főbb különbségek vannak kiemelve.

A Packet Tracer-rel történő munkavégzés (laboratóriumi vagy vállalati környezetben) során tudnunk kell, hogyan válasszuk ki a megfelelő kábeltípust és hogyan csatlakoztassuk megfelelően az eszközöket. A feladat megoldásakor Packet Tracer-ben kell bizonyos eszközök konfigurációját megvizsgálni, a beállításoknak megfelelő kábeltípust kiválasztani, majd az eszközök csatlakoztatását elvégezni. A feladat a hálózat fizikai nézetével is foglalkozik.

Packet Tracer - Kapcsolódás a vezetékes és vezeték nélküli LAN-hoz - Feladatlap

Packet Tracer - Connecting a Wired and Wireless LAN - PKA

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: A számítógép hálózati kártyáinak azonosítása és a velük történő munkavégzés.
- 2. rész: A tálcán lévő Hálózatok ikon azonosítása és használata.

Laborgyakorlat - Vezetékes és vezeték nélküli hálózati kártya információinak megtekintése

A TCP/IP modell hálózatelérési rétege az alábbi OSI rétegekkel egyenértékű:

- Adatkapcsolati (2. réteg)
- Fizikai (1. réteg)

Ahogy az ábrán is látható, az adatkapcsolati réteg felelős a keretek csomópontok közötti továbbításáért a fizikai közegen. Lehetővé teszi a felsőbb rétegek számára az átviteli közeg elérését, valamint vezérli az adatok közegre helyezésének és fogadásának módját.

Megjegyzés: Az egy közös átviteli közeghez csatlakozó hálózati eszközök második rétegbeli jelölésére a csomópont megnevezést használjuk.

Az adatkapcsolati réteg konkrétan a következő két alapszolgáltatást nyújtja:

- Fogadja a 3. rétegbeli csomagokat, majd egy keretnek nevezett adategységbe helyezi őket.
- Vezérli a közeghez való hozzáférést, és hibakeresést végez.

Az adatkapcsolati réteg hatékonyan végzi az adatok különböző közegek közötti átalakítását, amely a magasabb rétegekből induló kommunikációs folyamatok során lép fel. Fogadja egy felsőbb rétegbeli protokoll (például IPv4 vagy IPv6) csomagjait, illetve csomagokat továbbít a protokoll számára. Arról, hogy a kommunikáció milyen átviteli közegen zajlik, a felső rétegbeli protokollnak nincs tudomása.

Megjegyzés: Ebben a fejezetben a média és a médium kifejezés nem az animációs, televíziós, hang- és videoanyagokhoz hasonló digitális és multimédiás tartalmakra utal. Jelen esetben az adatjelek továbbítását végző átviteli közeget, például a réz- és optikai kábelt értjük alatta.

Az adatkapcsolati réteg két alrétegre tagolódik:

- **Logikai kapcsolatvezérlés (Logical Link Control, LLC)**: Ez a felső alréteg határozza meg azokat a szoftveres folyamatokat, amelyek a hálózati réteg protokolljainak nyújtanak

szolgáltatásokat. Információkat helyez el a keretben annak a hálózati rétegbeli protokollnak az azonosítására, amelyik a keretet használni fogja. Ez az információ lehetővé teszi, hogy több 3. rétegbeli protokoll is ugyanazt a hálózati interfészt és közeget használja.

- **Közeghozzáférés-vezérlés (Media Access Control, MAC)**Ez az alsó alréteg határozza meg a hardver által végzett közeghozzáférési folyamatokat. Biztosítja az adatkapcsolati szintű címzést, valamint az átviteli közeg jelzési rendszerének és a használatban lévő adatkapcsolati protokollnak megfelelő adatcsomag keretezését.

Az adatkapcsolati réteg alrétegekre történő bontása lehetővé teszi, hogy a felső rétegben létrehozott valamely típusú keret az alsó réteg bármely közegtípusához hozzáférjen. Ez a helyzet számos LAN technológiánál fennáll, többek között az Ethernetnél is.

Az ábra az adatkapcsolati réteg LLC és MAC alrétegekre történő felosztását szemlélteti. Az LLC kommunikál a hálózati réteggel, míg a MAC alréteg a különböző hálózatelérési technikákat tartalmazza. A keretek réz- vagy optikai kábelen történő továbbítására a MAC alréteg például az Ethernet technológiát használja. A vezeték nélkül történő kerettovábbításra pedig vezeték nélküli (pl.: Wi-Fi, Bluetooth) technológiákat használ.

A csomag keretbe ágyazását, valamint a beágyazott csomag közegre bocsátását és a közegről történő kiolvasását 2. rétegbeli protokollok határozzák meg. Azt a technikát, amelynek használatával a keret a közegre kerül, vagy kiolvassák onnan, közeghozzáférés-vezérlésnek nevezzük.

A csomagok a forrástól célig tartó útjuk során általában több különböző hálózaton haladnak keresztül. Ezen hálózatok eltérő átviteli közegtípusokat tartalmazhatnak, például rézvezetéket (elektromágneses jelek), optikai kábelt (fényjelek) és vezeték nélküli közeget (rádió- és mikrohullámok, valamint műholdas kapcsolatok) foglalnak magukban.

A csomagok nem férhetnek közvetlenül hozzá az átviteli közeghez. Az OSI modell adatkapcsolati rétegének feladata, hogy előkészítse a hálózati réteg csomagjait az átvitelre, és vezérelje a fizikai közeghez való hozzáférést. Az adatkapcsolati réteg protokolljai által leírt közeghozzáférés-vezérlési módszerek határozzák meg azt, hogy melyik hálózati eszköz férhet hozzá a közeghez és továbbíthat adatot a különböző hálózati környezetekben.

Az adatkapcsolati réteg nélkül a hálózati réteg protokolljainak (például az IP-nek) kellene gondoskodnia az összes olyan közegtípushoz történő csatlakozásról, amely a szállítási útvonalon előfordulhat. Továbbá, minden egyes új hálózati technológia vagy közeg megjelenésekor az IP-t is tovább kellene fejleszteni. Ez a folyamat akadályozná a protokollok és a hálózati közegek fejlődését is. Ez az egyik legfontosabb oka a hálózatok rétegszerű megközelítésének.

Az ábrán lévő animáció egy Párizsban található PC és egy Japánban lévő laptop csatlakozására mutat példát. Habár a két gép kizárólag IP-t használva kommunikál egymással, valószínűleg számos adatkapcsolati rétegben működő protokoll dolgozik, miközben az IP-csomagok a különböző LAN és WAN hálózatokban haladnak a cél felé. A forgalomirányítókon történő áthaladás során másik adatkapcsolati rétegbeli protokoll használatára lehet szükség, ha az adattovábbítás eltérő közegen folytatódik.

Egy egyszerű kommunikációs folyamat során is szükség lehet a különböző közeghozzáférési módszerekre. A csomagok a helyi állomástól a távoli állomás felé tartó útjuk során számos, különböző tulajdonságokkal rendelkező hálózati környezettel találkozhatnak. Az Ethernet hálózat például az átviteli közeg alkalmi használatáért versengő állomásokból áll. A soros összeköttetés pedig két eszköz között jelent közvetlen kapcsolatot, ahol az adatbitek áramlása egymás után, rendezett módon történik.

A forgalomirányító interfészei a megfelelő keretbe ágyazzák be a csomagokat, és egy alkalmas közeghozzáférési módszert használnak a kapcsolatok kezelésére. A hálózati rétegbeli csomagok továbbítása során számos átmenet léphet fel az adatkapcsolati rétegben és az átviteli közegen. Az útvonal minden egyes ugrásánál a forgalomirányító az alábbi műveleteket végzi el:

- Fogadja a keretet a közegtől.
- Kibontja a keretet.
- A csomagot egy új keretbe ágyazza be.
- Továbbítja az új keretet a hálózati szegmens közegének megfelelő formában.

Az ábrán látható forgalomirányító Ethernet interfésze egy LAN-hoz, a soros interfésze pedig egy WAN hálózathoz csatlakozik. A forgalomirányító a keretek feldolgozásakor az adatkapcsolati réteg szolgáltatásaira támaszkodik, amikor fogadja a keretet az egyik közegtől, kibontja a keretből a 3. rétegbeli adategységet, újra keretbe ágyazza a csomagot, majd az új keretet a kimeneti vonal közegére helyezi.

Az adatkapcsolati réteg egy fejléccel és utótaggal ellátott keretbe ágyazza be a csomagot, ezzel készíti elő azt a közegen való továbbításra. A keretleírás az adatkapcsolati protokollok kulcsfontosságú elemei közé tartozik.

Az adatkapcsolati réteg protokolljainak vezérlési információra van szükségük a protokollok működésének engedélyezéséhez. A vezérlési információ általában a következő kérdésekre ad meg a választ:

- Mely csomópontok kommunikálnak egymással?
- Mikor kezdődik és mikor fejeződik be az egyes csomópontok közti kommunikáció?
- A csomópontok kommunikációja során milyen hibák fordultak elő?
- Mely csomópontok fognak legközelebb kommunikálni egymással?

A fejezetben tárgyalt többi PDU-val ellentétben az adatkapcsolati rétegbeli keret a következőket tartalmazza:

- **Fejléc**: A keret elején található, és a vezérlési információkat tartalmazza, például a címzési adatokat.
- **Adatrész**: Az IP és a szállítási réteg fejlécét, valamint az alkalmazási réteg adatait tartalmazza.
- **Utótag**: A keret végén található, és a hibadetektáláshoz szükséges vezérlési információkat tartalmazza.

A keret elemeit az ábrán láthatjuk, részletesebben később foglalkozik velük a tananyag.

A közegen továbbított adatokat bitek, vagyis 1-esek és 0-k sorozatává alakítják az átvitel során. Mi alapján dönti el az állomás egy hosszú bitfolyam fogadásakor, hogy hol kezdődik és hol végződik a keret, és melyik bitek jelentik a címet?

A keretezéssel olyan csoportokra bontjuk a bitfolyamot, amelyeknek fejlécében és utótagjában megtalálható vezérlőinformációk különböző adatmezők értékeiként jelennek meg. Ez a formátum egy olyan szerkezetet ad a jelsorozatnak, amely alapján a fogadó állomás képes a jeleket visszaalakítani adatcsomagokká.

Ahogy az ábrán is látható, a keret általános mezőtípusai az alábbiak:

- **A keret kezdetét és végét jelző bitek**: A MAC alréteg használja a keret kezdetének és végének jelölésére.

- **Címzés**: A MAC alréteg használja a forrás- és célállomások azonosítására.
- **Típus**: Az LLC alréteg használja a 3. rétegbeli protokoll azonosítására.
- **Vezérlés**: Speciális adatfolyam-vezérlési szolgáltatásokat azonosít.
- **Adatrész**: A keret hasznos részét tartalmazza (azaz a csomag fejlécét, a szegmens fejlécét és az adatokat).
- **Hibafelismerés**: Az adatrész után található utótagot alkotja, hibák észlelésére használjuk.

Nem minden protokoll tartalmazza ezen mezők mindegyikét. Az adatkapcsolati protokollok szabványai határozzák meg a tényleges keretformátumot.

Megjegyzés: Az egyes keretformátumokra a fejezet végén láthatunk majd példákat.

A TCP/IP modell felsőbb rétegeiben található protokollokkal ellentétben, az adatkapcsolati réteg protokolljait általában nem RFC dokumentumokban definiálják. Habár az IETF felelős a TCP/IP felsőbb rétegeiben működő protokollok és szolgálatatások karbantartásáért, a hálózatelérési réteg működését és feladatait már nem ez a szervezet szabályozza.

Az adatkapcsolati réteg szolgáltatásait és előírásait olyan szabványokban fogalmazták meg, amelyek eltérő, de a protokollok által támogatott technológiákon és közegeken alapulnak. A szabványok némelyike 1. és 2. rétegbeli szolgáltatásokat is magában foglal.

Az adatkapcsolati rétegben működő protokollok és szolgáltatások előírásait a következő szervezetek határozzák meg:

- A nyílt szabványokat és protokollokat létrehozó mérnöki szervezetek.
- Kommunikációs cégek, akik saját (szabadalommal védett) protokollokat dolgoznak ki és használnak annak érdekében, hogy kihasználják az új technológiákban és a piacban rejlő lehetőségeket.

Az adatkapcsolati rétegre vonatkozó nyílt szabványokat és protokollokat létrehozó mérnöki szervezetek az alábbiak:

- Mérnököket egyesítő nemzetközi szervezet (Institute of Electrical and Electronics Engineers, IEEE)
- Nemzetközi Távközlési Szövetség (International Telecommunication Union, ITU)
- Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO)
- Amerikai Nemzeti Szabványügyi Intézet (American National Standards Institute, ANSI)

Az ábrán látható táblázat különböző szabványosító szervezeteket és a fontosabb adatkapcsolati protokolljaikat tartalmazza.

Az adatkeretek közegre helyezésének szabályozása a közeghozzáférés-vezérlési alréteg feladata.

A közeghozzáférés-vezérlés egyenértékű azon forgalmi szabályokkal, amelyek a gépjárművek úttestre hajtását szabályozzák. A közeghozzáférés szabályozásának hiánya egyenértékű lenne azzal a helyzettel, amikor a járművek minden más forgalmat figyelmen kívül hagyva az útra hajthatnának. Azonban nem minden út és felhajtási lehetőség egyforma. A forgalom az utak csatlakozásánál

egyszerű besorolással, a stoptáblánál való várakozással vagy a jelzőlámpák jeleinek figyelembe vételével kerülhet az utakra. A vezetőnek minden felhajtótípusnál különböző szabályokat kell követnie.

Ugyanígy, a keretek közegre helyezésének is számos módja létezik. Az adatkapcsolati réteg protokolljainak feladata a különböző közegek hozzáférési szabályainak meghatározása. Néhány módszer szigorúan ellenőrzött folyamatokat használ annak érdekében, hogy biztosítsa a keretek biztonságos közegre helyezését. Az ilyen módszerek működését kifinomult protokollok szabályozzák, melyekhez azonban olyan mechanizmusokat szükségesek, amelyek többletterhelést eredményeznek a hálózaton.

Az adatkapcsolati protokollok eltérő változatai között különböző módszerek léteznek a közeghozzáférés szabályozására. Ezek a módszerek határozzák meg, hogy az állomások megosztozzanak-e a közegen, és ha igen, akkor milyen módon.

A megfelelő közeghozzáférési módszer kiválasztása az alábbiaktól függ:

- **Topológia**: Milyennek látja az adatkapcsolati réteg az állomások közötti kapcsolatot.

- **A közeg megosztása**: Az állomások miként osztoznak a közegen. A közegmegosztás lehet pont-pont típusú, mint a WAN kapcsolatoknál, de lehet megosztott is, mint a LAN hálózatok esetében.

A hálózat topológiája a hálózati eszközök elrendezését és a köztük lévő összeköttetéseket jelenti. A LAN és WAN topológiák kétféle módon ábrázolhatók:

- **Fizikai topológia**: A fizikai összeköttetésekre utal, meghatározza a végberendezések és a köztes eszközök (pl.: forgalomirányítók, kapcsolók és vezeték nélküli hozzáférési pontok) kapcsolódási módját. A fizikai topológia általában pont-pont vagy csillag típusú. Lásd az 1. ábrát!

- **Logikai topológia**: Arra utal, hogy a hálózat miként szállítja a kereteket egyik állomástól a másikig. Ez az elrendezés az állomások közötti virtuális kapcsolatokból áll. A hozzájuk tartozó logikai jelutakat az adatkapcsolati réteg protokolljai határozzák meg. A pont-pont kapcsolatokon alapuló logikai topológia viszonylag egyszerű, a megosztott közeg esetében viszont beszélhetünk determinisztikus és nem determinisztikus módszerekről is. Lásd a 2. ábrát!

Az adatkapcsolati réteg a hálózat logikai topológiáját "figyeli" a közeghozzáférés vezérlése közben. A logikai topológia az, amely befolyással van a keretezés típusára és a közeghozzáférés módjára.

A WAN hálózatok jellemzően az alábbi fizikai topológiák használatával kapcsolódnak egymáshoz:

- **Pont-pont**: Ez a legegyszerűbb topológiafajta, mindössze egyetlen, két végpont közötti állandó kapcsolatból áll. Emiatt nagyon népszerű WAN topológiának számít.

- **Csillagpont**: A csillag topológia WAN változata, amelyben egy központ pont-pont kapcsolatok használatával köti össze a telephelyeket.

- **Hálós**: Ez a topológiatípus nagyfokú rendelkezésre állást biztosít, viszont megköveteli, hogy minden végrendszer mindegyik másikkal össze legyen kapcsolva. Emiatt a fenntartási és kivitelezési költségek magasak lehetnek. Minden egyes kapcsolat egy pont-pont összeköttetést jelent valamely másik csomóponttal. A topológia egy másik változata a részleges hálós típus, amelyben nincs minden végberendezés összekapcsolva egymással.

Az ábrán a három gyakori WAN topológia rajza látható.

Ahogy az ábrán is látható, a fizikai pont-pont összeköttetések közvetlenül két végpontot kapcsolnak össze egymással.

Ebben az elrendezésben a végpontoknak nem kell más állomásokkal megosztozniuk a közegen. Ezen felül az állomásoknak nem kell eldönteniük, hogy a beérkező keretet nekik vagy egy másik csomópontnak szánták. Emiatt a logikai adatkapcsolati protokollok nagyon egyszerű felépítésűek is lehetnek, hiszen a keretek csak a két állomás egyikének lehetnek címezve vagy csak tőlük származhatnak. A kereteket a pont-pont kapcsolat egyik végén az állomás ráhelyezi a közegre, a túlsó végén lévő másik állomás pedig leveszi azokat.

Pont-pont topológiák esetében az adatkapcsolati protokoll sokkal kifinomultabb közeghozzáférési módszereket is tudna biztosítani, viszont ezek felesleges többletterhelést jelentenének a protokoll számára.

A végberendezések pont-pont hálózaton keresztüli kommunikációja során a kapcsolat közvetítő eszközökön keresztül jöhet létre. Ezek használata viszont nincs befolyással a logikai topológiára.

Ahogy az első ábrán is látható, a forrás- és a célállomás közvetve, nagy földrajzi távolságok áthidalásával kapcsolódik egymáshoz. Bizonyos esetekben az állomások közötti logikai kapcsolat úgynevezett virtuális áramkört alkot. A virtuális áramkör a hálózaton belül kiépített logikai kapcsolatot jelent, amely két hálózati eszköz között jön létre. A virtuális áramkör két végén található állomások egymás között továbbítják a kereteket. Ez akkor is így történik, ha a keretek közben más eszközön is áthaladnak. A virtuális áramkör a logikai kommunikáció fontos építőeleme, amelyet számos 2. rétegbeli technológia is használ.

Az adatkapcsolati protokollok által használt közeghozzáférési módszert a logikai pont-pont topológia határozza meg, nem pedig a fizikai. Ez azt jelenti, hogy az állomások közötti logikai pont-pont összeköttetésen nem feltétlenül a két állomás közötti közvetlen fizikai kapcsolatot értjük.

A 2. ábrán a két forgalomirányító közötti kapcsolat fizikai eszközei is láthatók.

Az 1. ábrán egy pont-pont topológia látható. A pont-pont hálózatokban az adatok az alábbi két módon áramolhatnak:

- **Félduplex kommunikáció**: Mindkét eszköz képes adatküldésre és -fogadásra a közegen, de nem egyidejűleg. Az Ethernet megfelelő kiválasztási szabályokat biztosít azokra az esetekre, amikor egynél több állomás is megpróbál egyszerre adni. A 2. ábrán a félduplex kommunikáció látható.

- **Duplex kommunikáció**: Mindkét eszköz képes az egyidejű továbbításra és fogadásra is a közegen. Az adatkapcsolati réteg feltételezi, hogy a közeg bármikor elérhető mindkét állomás számára. Emiatt nincs szükség közegkiválasztásra az adatkapcsolati rétegben. A 3. ábrán a duplex kommunikáció látható.

A fizikai topológia azt határozza meg, hogy a végrendszerek milyen módon kapcsolódnak egymáshoz. Megosztott hálózati közegen az alábbi fizikai topológiákat használjuk:

- **Csillag**: A végberendezések egy központi közvetítő eszközhöz csatlakoznak. A korai csillag topológiáknál a végberendezések hub használatával kapcsolódtak egymáshoz. A mai csillag topológiákban viszont már kapcsolókat használnak. A csillag topológia a leggyakrabban használt fizikai LAN topológia. Ennek elsődleges oka, hogy könnyű telepíteni, skálázható (egyszerűen lehet végberendezéseket hozzáadni és eltávolítani), valamint a hibák elhárítása is egyszerű.

- **Kiterjesztett csillag vagy hibrid**: Több topológia kombinációjából áll, ilyen például a csillag topológiák egymáshoz kapcsolása busz topológia használatával.

- **Busz**: Az állomások egymás után vannak láncolva és valamilyen formában a lánc mindkét végén le vannak zárva. A végberendezések összekapcsolásához nincs szükség (a kapcsolóhoz hasonló) hálózati eszközökre. A busz topológiát az Ethernet korábbi változataiban használták, annak olcsósága és könnyű telepíthetősége miatt.

- **Gyűrű**: Az állomások a megfelelő szomszédaikkal összeköttetésben állva alkotnak egy gyűrűt. A busz topológiával ellentétben a gyűrűt nem kell lezárni. A gyűrű topológiát az FDDI hálózatok korábbi változataiban használták. Az FDDI hálózatokban egy második gyűrűt is alkalmaznak a hibatűrés és a teljesítmény javítása érdekében.

Az ábra azt mutatja, hogy a végberendezések miként kapcsolódhatnak egymáshoz LAN hálózatok esetében.

A hálózat logikai topológiája szorosan kapcsolódik a hálózati hozzáférések vezérlésénél alkalmazott módszerhez. Ezek a módszerek úgy végzik a hozzáférés vezérlését, hogy a hálózat elérése minden állomás számára biztosított legyen. Amennyiben több egység is osztozik ugyanazon a közegen, akkor a hálózati hozzáférés szabályozására valamilyen mechanizmust kell alkalmazni. Az egyes hozzáférési módszereket a közeg elérésének szabályozására alkalmazzák a hálózatokban.

Számos hálózati topológia használ több csomóponttal rendelkező, megosztott átviteli közeget. Ezekben előfordulhat, hogy egyidejűleg több eszköz is megpróbál adatot küldeni és fogadni a hálózati közegen. Előírások szabályozzák, hogy ezek az eszközök milyen módon osztozzanak meg a közegen.

Két alapvető közeghozzáférési módszer létezik osztott átviteli közeg esetében:

- **Versengéses hozzáférés**: Az állomások versengenek a közeg használatáért, ütközés esetén viszont meghatározott rend szerint viselkednek. Az első ábra a versengés alapú hozzáférést mutatja.

- **Szabályozott hozzáférés**: Az állomások meghatározott időszeletet kapnak a közeg használatára. A 2. ábra a szabályozott hozzáférést mutatja.

Az adatkapcsolati protokoll határozza meg a közeghozzáférés-vezérlés módját. Ez biztosítja a megfelelő egyensúlyt a keretvezérlés, a keretvédelem és a hálózati túlterheltség között.

Nem determinisztikus versengéses módszer használatakor a hálózati eszköz bármikor hozzáférhet a közeghez, amikor küldeni szeretne. Az ilyen módszerek a teljes káosz elkerülése érdekében a vivőérzékeléses többszörös hozzáférés (Carrier Sense Multiple Access, CSMA) nevű technikát használják annak megállapítására, hogy a közegen van-e jeltovábbítás.

Egy másik csomóponttól származó vivőjel érzékelése esetén megállapítható, hogy a közegen éppen adatátvitel zajlik. Ha a készülék ilyenkor próbál meg adni, a közeg foglaltságát fogja tapasztalni. Ekkor várakozni kényszerül, majd egy rövid idő múlva újra próbálkozhat. Ha nem észleli a vivőjelet, akkor továbbíthatja az adatokat. Az Ethernet és a vezeték nélküli hálózatok versengéses közeg-hozzáférési módszert használnak.

Előfordulhat, hogy a CSMA folyamat sikertelen lesz, és két eszköz egyidejű adatküldése ütközést eredményez. Amennyiben ez megtörténik, akkor mindkét készülék által küldött adat megsérül és újra kell őket küldeni.

A versengéses módszerek nem jelentenek többletterhelést a szabályozott hozzáféréshez képest. Ugyanis nem szükséges nyomon követni azt, hogy éppen melyik állomás használja a közeget. A versengéses rendszerek viszont nem jól skálázhatóak a közeg nagymértékű igénybevétele mellett. Az igénybevétel és a csomópontok számának növekedésével csökken annak a valószínűsége, hogy sikeresen (azaz ütközés nélkül) hozzá lehessen férni a közeghez. Ezen felül az ütközésekből származó hibák kijavítására szolgáló helyreállítási mechanizmusok is tovább rontják a teljesítményt.

A CSMA-t általában a közegért történő versengés megoldási módszerével együtt alkalmazzák. A két leggyakrabban használt módszer a következő:

- **Vivőérzékeléses többszörös hozzáférés ütközésfigyeléssel (Carrier Sense Multiple Access with Collision Detection, CSMA/CD)**: A végberendezés a közeg figyelésével ellenőrzi, hogy van-e rajta adatjel. Ha nem érzékel jelet, az a közeg szabad használatát jelzi. Ilyenkor a készülék továbbíthatja az adatokat. Az adatjelek észlelése azt jelzi, hogy egy másik készülék is forgalmaz ugyanabban az időben. Ilyenkor minden eszköz leállítja a küldést, majd később újra próbálkozhat. Az Ethernet korai megvalósításai használják ezt a módszert.

- **Vivőérzékeléses többszörös hozzáférés ütközés-elkerüléssel (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA)**: A végberendezés a közeg vizsgálatával ellenőrzi, hogy van-e adatjel a közegen. Ha a közeg szabad, a készülék egy értesítést küld a közegen keresztül arról a szándékáról, hogy használni szeretné azt. Amint megkapja az engedélyt a továbbításra, elküldi az adatokat. Ezt a módszert használják a 802.11 szabványt használó vezeték nélküli technológiák.

Az ábra az alábbiakat tartalmazza:

- A versengés alapú hozzáférési módszerek működése.

- A versengéses hozzáférési módszerek jellemzői.

- Példák versengéses hozzáférési módokra.
  - A logikai többes hozzáférésű topológia több állomás számára is lehetővé teszi a kommunikációt egy közös, megosztott közeg használatával. A közegre egyidejűleg csak egy csomóponttól származó adatokat lehet ráhelyezni. Minden csomópont látja a közegen lévő összes keretet, de csak az dolgozza fel a tartalmát, amelynek címezték.
  - Több csomópont megosztott közeghozzáférése esetén adatkapcsolati szintű közeghozzáférés-vezérlés szükséges az adattovábbítás szabályozásához, és ezáltal a különböző jelek közti ütközések csökkentéséhez.
  - Az animáció lejátszásával megtekinthetjük, hogyan férnek hozzá a csomópontok a közeghez többes hozzáférésű topológiák esetében.

Szabályozott hozzáférési mód használatakor a hálózati eszközök felváltva, egymás után férnek hozzá a közeghez. Ha valamelyik végberendezés nem kívánja használni a közeget, a lehetőség továbbadódik a következő eszköznek. A folyamatot vezérjel használatával lehet megkönnyíteni. A végberendezés a megszerzett vezérjel birtokában keretet helyezhet el a közegen. Más eszköz csak azután teheti ezt meg, miután a keret megérkezik a célhoz, amely feldolgozza azt, majd felszabadítja a vezérjelet.

Megjegyzés: A módszer ütemezett vagy determinisztikus hozzáférés néven is ismert.

Annak ellenére, hogy a szabályozott hozzáférés jól tervezhető és kiszámítható teljesítménnyel rendelkezik, a determinisztikus módszereket kevésbé hatékonynak is ítélhetjük, mivel az eszközöknek várniuk kell, mielőtt használni tudják a közeget.

Szabályozott hozzáférésre példaként említhetjük a következőket:

- Vezérjeles gyűrű (Token Ring, IEEE 802.5)

- FDDI, amely az IEEE 802.4 vezérjeles busz protokollon alapul

Megjegyzés: Mindkét közeghozzáférési módszer elavultnak tekinthető.

Az ábra a következőket tartalmazza:

- Szabályozott hozzáférési módok működése.

- Szabályozott hozzáférési módok jellemzői.

- Példák szabályozott hozzáférési módokra.
  - A logikai gyűrű topológiában a csomópontok minden körben kapnak egy keretet. Ha a keret nem nekik szól, akkor tovább adják azt a következő csomópontnak. Így egy szabályozható közeghozzáférési technika használata válik lehetővé a gyűrűben, amelyet vezérjel-továbbításnak hívunk.
  - A logikai gyűrű topológia csomópontjai eltávolítják a keretet a gyűrűről, megvizsgálják a címet, majd továbbküldik, ha nem nekik szól. A gyűrűben minden csomópont (a forrás- és a célcsomópontok között) megvizsgálja a keretet.
  - Számos olyan közeghozzáférési technika létezik, amely az elvárt ellenőrzési szinttől függően használható a logikai gyűrűben. Például, a közeg egyidejűleg csak egy keret továbbítását végzi. Ha épp nincs adattovábbítás, akkor egy jelet (más néven vezérjelet) helyeznek a közegre, és az állomásnak csak akkor van lehetősége adatkeretet továbbítani, ha nála van a vezérjel.
  - Ne feledjük, hogy az adatkapcsolati réteg 'látja' a logikai gyűrű topológiát! A kábelezés tényleges fizikai topológiája ettől eltérő típusú is lehet.
  - Az animáció lejátszásával megtekinthetjük, hogy a csomópontok milyen módon érik el a közeget logikai gyűrű topológia esetében.

Annak ellenére, hogy számos különböző adatkapcsolati protokoll létezik az adatkapcsolati keretek leírására, mindegyik kerettípus három fő részből áll:

- Fejléc

- Adatrész

- Utótag

Az adatkapcsolati réteg protokolljai a 3. rétegbeli protokoll adategységet (PDU) ágyazzák be a keret adatmező részébe. A keret felépítése, valamint a fejlécben és az utótagban található mezők viszont protokollonként eltérőek lehetnek.

Az adatkapcsolati réteg protokolljai írják le azokat a funkciókat, amelyek ahhoz kellenek, hogy a csomagokat különböző közegeken továbbítani lehessen. A protokoll ezen funkciói a keretbeágyazás részét képezik. Miután a keret megérkezett a célállomásra, és az adatkapcsolati protokoll eltávolította azt a közegről, a keretezési információk kiolvasása, majd eldobása történik meg.

Olyan keretszerkezet nem létezik, amely mindenféle átviteli közegre kielégítené az összes adattovábbítási igényt. A keretben lévő vezérlési információk mennyisége a környezettől függően változik, amiatt, hogy megfeleljen a közeg és a logikai topológia közeghozzáférési követelményeinek.

Ahogy az 1. ábra is mutatja, érzékeny környezetben több ellenőrzésre van szükség. A 2. ábrán viszont az látható, hogy védett környezetben kevésbé van szükség szabályozásra.

A keret fejléce tartalmazza azokat a vezérlési információkat, amelyeket az adatkapcsolati protokollok meghatároznak, valamint megfelelnek a használt logikai topológiának és közegnek.

A keret vezérlőinformációi minden egyes protokolltípusnál egyediek. Ezeket alkalmazzák a 2. rétegbeli protokollok annak érdekében, hogy biztosítsák a kommunikációs környezet által megkövetelt funkciókat.

Az ábrán az Ethernet keret fejlécének mezői láthatók:

- **Keretkezdet mező**: A keret kezdetét jelzi.

- **Forrás- és célcím mezők**: A közegen található forrás- és célállomásokat jelzi.

- **Típus mező**: A keretben szereplő felsőbb rétegbeli szolgáltatást jelzi.

A különböző adatkapcsolati protokollok ezektől eltérő mezőket is használhatnak. Más 2. rétegbeli protokollok keretének fejléc mezői például az alábbiak lehetnek:

- **Prioritás/szolgáltatásminőség mező**: Bizonyos típusú kommunikációs szolgáltatásokat jelez.
- **Logikai kapcsolatvezérlés mező**: Csomópontok közötti logikai kapcsolat létrehozására szolgál.
- **Fizikai kapcsolatvezérlés mező**: Fizikai kapcsolat létrehozására szolgál.
- **Adatfolyam-vezérlés mező**: A közegen zajló forgalom elindítására és megállítására szolgál.
- **Torlódásvezérlés mező**: A közegen jelentkező torlódást jelzi.

Mivel az adatkapcsolati protokollok céljai és feladatai konkrét topológiához és közeghez kapcsolódnak, ezért minden protokollt meg kell vizsgálni annak érdekében, hogy részletesen megismerjük a keretszerkezetét. Ahogy a protokollokat megtárgyaljuk a fejezetben, úgy azok keretszerkezetéről is egyre több információt kapunk.

Az adatkapcsolati réteg biztosítja azt a címzést, amelyet a megosztott közegen történő kerettovábbításnál használunk. Az eszközök címét ebben a rétegben fizikai címnek hívjuk. Az adatkapcsolati réteg címzését a keret fejlécében találhatjuk, ez határozza meg a keret céljának csomópontját a helyi hálózaton. A keret fejléce tartalmazhatja a forráscímet is.

A 3. rétegben található, hierarchikus felépítésű logikai címmel ellentétben, a fizikai cím nem jelzi azt, hogy a készülék melyik hálózaton található. A fizikai címe inkább az eszközre jellemző egyedi cím. Attól, hogy a készülék egy másik hálózatba vagy alhálózatba kerül át, még ugyanazzal a 2. rétegbeli címmel működik tovább.

Az eszköz-specifikus és nem hierarchikus cím viszont nem használható egy eszköz nagyméretű hálózatokban vagy az interneten történő azonosítására. Ez olyan lenne, mintha mindössze utcanév és házszám alapján próbálnánk egy házat megtalálni a nagyvilágban. A fizikai cím ugyanakkor felhasználható egy eszköz korlátozott területen belüli azonosítására. Emiatt az adatkapcsolati rétegbeli címeket csak helyi továbbításra használhatjuk. Az ebben a rétegben található címek nem jelentenek semmit a helyi hálózaton túl. Vessük össze ezt a 3. réteggel, ahol a csomag fejlécében szereplő címek a forrásállomástól a célállomásig utaznak, függetlenül az út során megtett hálózati ugrások számától!

Ha az adatokat egy másik hálózati szegmensbe kell továbbítani, egy közvetítő eszközre (pl.: forgalomirányítóra) van szükség. A forgalomirányító a keretet a fizikai cím alapján fogadja, majd kibontja azt annak érdekében, hogy megvizsgálja a hierarchikus címet, vagyis az IP-címet. Az IP-cím alapján a forgalomirányító képes megállapítani a célkészülék hálózati helyét és a hozzá vezető legjobb útvonalat. Amint megtudja, hogy hova továbbítsa a csomagot, egy új keretet állít össze neki, majd elküldi ezt a keretet a végső cél felé vezető következő szegmensre.

Az ábra a 2. rétegbeli címzés követelményeit mutatja többes hozzáférésű, valamint pont-pont topológiák esetében.

Az adatkapcsolati protokoll minden keret végéhez egy utótagot ad hozzá. Az utótag annak meghatározására szolgál, hogy a keret hiba nélkül érkezett-e meg. Ezt a folyamatot hibakeresésnek hívják, és úgy valósítják meg, hogy az utótagba a keretet alkotó bitek logikai vagy matematikai összegzését helyezik el. A hibadetektálás azért az adatkapcsolati rétegben történik, mert a közegen továbbított jelek interferencia, torzítás vagy veszteség következtében jelentős mértékben megváltoztathatják az általuk ábrázolt bitek értékét.

A továbbítást végző csomópontok készítik el a keret tartalmának logikai összegzését. Ez ciklikus redundancia-ellenőrzés (CRC) érték néven is ismert. A kiszámított értéket a keret keretellenőrző összeg (Frame Check Sequence, FCS) mezőjébe helyezik, hogy a keret tartalmát képviselje.

További információért kattintsunk az ábra FCS és Stop Frame mezőire!

Miután a keret megérkezett a célcsomóponthoz, a fogadó eszköz kiszámítja a kerethez tartozó logikai összegzést, vagyis a CRC-t. Ezután a két CRC értéket összehasonlítja. Ha a két érték megegyezik, a beérkezett keretet kézbesítettnek tekintjük. Ha az FCS mező CRC értéke eltér a fogadó fél által számított értéktől, akkor a keret eldobásra kerül.

Emiatt a FCS mezőt a keret átvitele és a fogadása során keletkező hibák felderítésére használják. Az FCS mező hibakeresési módszerének használatával a közegen keletkező legtöbb hiba felderíthető.

Egy kicsi esély mindig van arra is, hogy egy helyes CRC értékkel rendelkező keret valójában hibás. A CRC számításakor a bitekben keletkező hibák kiolthatják egymást. Ilyenkor felsőbb rétegbeli protokollokra van szükség az adatvesztés felismeréséhez és javításához.

Egy TCP/IP hálózatban minden 2. rétegbeli protokoll a 3. rétegben található IP-vel működik együtt. A ténylegesen használt 2. rétegbeli protokoll viszont a hálózat logikai topológiájától és a fizikai réteg megvalósításától függ. Mivel a különböző hálózati topológiákban számos fizikai közegtípus van használatban, ennek megfelelően az elérhető 2. rétegbeli protokollok száma is meglehetősen nagy.

Bizonyos 2. rétegbeli logikai topológiákon minden protokoll közeghozzáférés-vezérlést végez. Ez azt jelenti, hogy számos különböző hálózati eszköz viselkedhet adatkapcsolati rétegben működő csomópontként, miközben ezeket a protokollokat használja. Ezek közé tartoznak a számítógépek hálózati adapterei vagy hálózati kártyái (NIC), csakúgy mint a forgalomirányítók és a 2. rétegbeli kapcsolók interfészei.

Az, hogy egy bizonyos hálózati topológiánál melyik 2. rétegbeli protokollt használjuk, azon múlik, hogy a topológia megvalósításához milyen technológiára van szükség. A technológiát viszont az állomások számától és a földrajzi kiterjedéstől függő hálózatméret, valamint a hálózaton nyújtandó szolgáltatások határozzák meg.

A helyi hálózatokban jellemzően nagyszámú állomás kiszolgálására alkalmas, nagy sávszélességű technológiát használunk. Ezt a technológiát a hálózat viszonylag kis földrajzi területe (egy vagy több épületből álló egyetem), valamint a felhasználók sűrű elhelyezkedése teszi költséghatékonnyá.

Ugyanakkor a nagy sávszélességű technológiák általában nem költséghatékonyak WAN hálózatok esetében, mivel azok nagy földrajzi területeket fednek le (például városok vagy nagyvárosok). A nagytávolságú fizikai kapcsolatok magas költsége és az ekkora távolságokra használt jeltovábbító technológiák miatt jellemzően alacsonyabb sávszélességet kapunk.

A sávszélességben jelentkező különbség általában eltérő protokollok használatát eredményezi LAN és WAN hálózatok esetében.

Az adatkapcsolati réteg elterjedt protokolljai a következők:

- Ethernet
- Pont-pont protokoll (PPP)
- 802.11 szabványú vezeték nélküli

A CCNA tananyagban szerepel még a magas szintű adatkapcsolat-vezérlés (High-Level Data Link Control, HDLC) és a Frame Relay protokoll is.

A lejátszás gombra kattintva 2. rétegbeli protokollokra láthatunk példákat.

Ethernet

Az Ethernet a LAN hálózatok vezető technológiája. Hálózati technológiák egész családja, amelyeket az IEEE 802.2 és 802.3 szabványok határoznak meg.

Az Ethernet szabványok meghatározzák a második rétegbeli protokollokat és az első rétegbeli technológiákat is. Az Ethernet a legelterjedtebb LAN technológia, amely a 10 Mb/s, 100 Mb/s, 1 Gb/s (1000 Mb/s), vagy a 10 Gb/s (10000 Mb/s) sávszélességeket támogatja.

Az alapvető keretformátum és az IEEE által kidolgozott, az OSI modell első és második rétegének megfelelő alrétegek minden Ethernet-változatnál azonosak. Az adatok érzékelésének és közegre helyezésének módszerei viszont az egyes változatoknál eltérőek lehetnek.

Az Ethernet, mint közeghozzáférési módszer nyugtázás nélküli, összeköttetésmentes szolgáltatást biztosít egy megosztott hálózati közegen, a CSMA/CD használatával. A megosztott közeg miatt szükséges, hogy az Ethernet keret fejléce tartalmazzon egy adatkapcsolati címet a forrás és a cél azonosítására. Ezt a címet, a legtöbb LAN protokoll elnevezéséhez hasonlóan, a csomópont MAC-címének nevezzük. Az Ethernet MAC-cím 48 bites, és általában hexadecimális formában ábrázolják.

Az ábra az Ethernet keret számos mezőjét mutatja. Az adatkapcsolati réteg szintjén a keretszerkezet gyakorlatilag az Ethernet összes különböző sávszélességű változatánál azonos. A fizikai réteg szintjén viszont az egyes Ethernet változatok eltérő módon helyezik rá a biteket a közegre. Az Ethernetet a következő fejezetben részletesebben is tárgyaljuk.

Pont-pont protokoll (Point-to-Point Protocol)

Egy másik adatkapcsolati protokoll a pont-pont protokoll. A PPP két csomópont közötti kerettovábbításra használt protokoll. Ellentétben több más adatkapcsolati protokollal, amelyeket mérnöki szervezetek definiálnak, a PPP szabványt RFC dokumentumokban határozzák meg. A PPP-t WAN hálózati protokollként hozták létre, és továbbra is soros WAN összeköttetéseknél használják. Számos különböző fizikai közegen használható, többek között csavart érpáras, optikai és műholdas átvitelnél, valamint virtuális kapcsolatoknál.

A PPP réteges architektúrát alkalmaz. Amiatt, hogy a különböző közegtípusokat kezelni tudja, a két csomópont között egy logikai kapcsolatot, úgynevezett munkamenetet hoz létre. Ez a PPP munkamenet végzi a fizikai közeg elrejtését a felsőbb PPP protokoll elől. Ezen felül biztosítja annak a lehetőségét is, hogy a PPP számos protokoll beágyazását végezze a pont-pont kapcsolaton keresztül. A beágyazott protokollok mindegyikének külön PPP munkamenet épül ki a vonalon.

A PPP azt is lehetővé teszi, hogy két csomópont egyeztesse a kapcsolat részleteit a PPP munkameneten keresztül. Ez magába foglalja a hitelesítés, tömörítés és a több fizikai kapcsolat (multilink) használatának elemeit.

Az ábrán a PPP keret alapvető mezői találhatók.

802.11 szabványú vezeték nélküli

Az IEEE 802.11 szabvány ugyanazt a 802.2 logikai kapcsolatvezérlést (LLC) és 48 bites címzési rendszert használja, mint számos más 802-es szabványú helyi hálózat. Ugyanakkor a MAC alréteg és a fizikai réteg használatában számos eltérés van. A vezeték nélküli környezet speciális szempontok figyelembevételét követeli meg. Mivel nincs kézzelfogható fizikai kapcsolat, az adatátvitelt külső tényezők is megzavarhatják, továbbá a közeghozzáférés szabályozása is nehézségekbe ütközik. Azért, hogy ezeknek a kihívásoknak megfeleljenek, a vezeték nélküli szabványok további ellenőrzéseket alkalmaznak.

A 802.11 szabvány széleskörűen használt, elterjedt neve a Wi-Fi. Ez egy versengés alapú rendszer, amely a CSMA/CA használatával biztosítja a közeghozzáférés-vezérlés folyamatát. A CSMA/CA egy véletlen hosszúságú visszatartási eljárást határoz meg azon csomópontok számára, amelyek továbbításra várakoznak. A közegért való versengés kialakulása akkor a legvalószínűbb, mikor a közeg újra elérhetővé válik. Mivel a csomópontoknak véletlen hosszúságú ideig kell várakozniuk, jelentősen csökken az ütközés veszélye.

A 802.11 szabványú hálózatokban is használhatunk nyugtázást annak megerősítésére, hogy a keret sikeresen megérkezett. Ha az eredeti adatkeret vagy a nyugta elveszése következtében a küldő állomás nem kap nyugtakeretet, a keret újraküldésre kerül. Ezzel a közvetlen nyugtázás típussal leküzdhetők az interferenciából és egyéb, rádiós kapcsolatból eredő problémák.

A 802.11 szabvány által támogatott további szolgáltatások közé tartozik a hitelesítés, a társítás (kapcsolódás vezeték nélküli eszközhöz), valamint az adatvédelem (titkosítás).

Ahogy az ábrán is látható, a 802.11 szabványú keret az alábbi mezőket tartalmazza:

- **Protokollverzió mező**: A használatban lévő 802.11 szabványú keret verziója.
- **Típus és altípus mezők**: A kerethez tartozó három funkció (vezérlés, adatok és felügyelet), valamint az alfunkciók közül azonosít egyet.
- **Elosztó rendszer (To Distribution System, To DS) felé mező**: Értéke az elosztó rendszerek (vezeték nélküli hálózati eszközök) felé továbbított keretek esetében 1.
- **Elosztó rendszer (From Distribution System, From DS) felől mező**: Értéke az elosztó rendszer felől érkező adatkeretek esetében 1.
- **További töredék (More Fragments) mező**: Értéke 1, ha a keret tördelve lett és további részletei a következő keretekben érkeznek.
- **Újraküldés (Retry) mező**: Értéke 1, ha a keret egy korábbi keret újraküldött változata.
- **Energiagazdálkodás mező**: Az 1-re állított érték azt jelzi, hogy egy csomópont energiatakarékos üzemmódban működik.
- **További adatok (More Data) mező**: Az 1-re állított érték jelzi az energiatakarékos üzemmódú csomópont számára, hogy további adatkeretek vannak pufferelve a számára.
- **WEP mező**: Értéke 1, ha a keret biztonsági okokból WEP titkosítással kódolt információt tartalmaz.
- **Egyéb mező**: Értéke 1-re van állítva azoknál az adatkereteknél, amelyek egy bizonyos szolgáltatásminőség funkciót használnak (így nincs szükség az ismételt sorba rendezésükre).
- **Időtartam/ID mező**: A keret típusától függően a keretátvitelhez szükséges időt adja meg mikroszekundumban, vagy annak az állomásnak az azonosítóját (AID), amely a keretet továbbította.
- **Célcím (Destination Address, DA) mező**: A célcsomópont MAC-címe.
- **Forráscím (Source Address, SA) mező**: A forráscsomópont MAC-címe.
- **Vevő címe (Receiver Address, RA) mező**: Annak a vezeték nélküli eszköznek a MAC-címe, amely közvetlen címzettje a keretnek.

- **Töredék száma (Fragment Number) mező**: Az egyes kerettöredékeket azonosítja.
- **Sorszám mező**: A kerethez rendelt sorszámot jelenti, az újraküldött kereteket az ismétlődő sorszámok alapján lehet azonosítani.
- **Adó címe (Transmitter Address, TA) mező**: Annak a vezeték nélküli eszköznek a MAC-címe, amelyik a keretet küldte.
- **Keret adatmező**: A továbbított információt tartalmazza, adatkeretek esetében jellemzően egy IP-csomagot.
- **FCS mező**: A keret 32 bites CRC ellenőrző összegét tartalmazza.

Kapcsolódj be!

Megjegyzés: A feladat leginkább 2-3 fős diákcsoportok számára javasolt.

Kisvállalkozásunk új telephelyre költözik. Egy teljesen új épületről van szó, és a mi feladatunk egy fizikai terv létrehozása, amely alapján elkezdődhet a hálózat telepítése.

A feladat végrehajtásához egy tervrajz is rendelkezésre áll (az oktató biztosít egy másolatot róla), ahol – az 1-el jelölt terület a recepciót – az RR jelű pedig a mellékhelyiséget jelöli.

A helyiségekben legfeljebb a Cat6 típusú UTP kábel előírásait (100 méter) kell betartani, így nem kell az épület kábelezési nehézségeivel foglalkozni. A tervrajzon lévő helyiségek mindegyikében legalább egy hálózati csatlakozási lehetőséget biztosítani kell a felhasználók és a közvetítő eszközök számára.

A csoportársakkal együtt a következőket kell jelölni a rajzon:

- A központi kábelrendező helyét, a biztonsági szempontok figyelembevételével.
- A használni kívánt közvetítő eszközök számát és azok elhelyezését.
- A használni kívánt kábelezési típust (UTP, STP, vezeték nélküli, optikai, stb.), valamint a csatlakozók elhelyezkedését.
- A használni kívánt végberendezések típusát (vezetékes, vezeték nélküli, laptop, asztali számítógép, táblagép, stb.).

A tervezés során nem kell túlzásokba esni. Csak a fejezetben tanul ismereteket használjuk, hogy meg tudjuk indokolni a döntéseinket az osztálynak!

Csoportos feladat - Kapcsolódj be! Utasítások

A TCP/IP hálózat elérési rétege az OSI modell adatkapcsolati (2. réteg) és fizikai (1. réteg) rétegeinek megfeleltetése.

Az OSI modell fizikai rétege biztosítja a adatkapcsolati réteg kereteit alkotó bitek továbbítását a hálózati közegen. Fizikai összetevők alatt olyan elektronikus hardvereszközöket, átviteli közegeket és csatlakozókat értünk, amelyek a biteket reprezentáló jelek továbbítását végzik. A hardverösszetevők, mint például a hálózati kártyák (NIC), a csatlakozófelületek és csatlakozók, a kábelezési anyagok és tervek leírásait a fizikai réteghez kapcsolódó szabványok tartalmazzák. A fizikai réteg szabványai három fő területtel foglalkoznak: fizikai összetevők, keretkódolási technikák és jelzési módszerek.

A hálózati kommunikáció fontos részét képezi a megfelelő átviteli közeg használata. Akár a vezetékes, akár a vezeték nélküli kapcsolatot nézzük, két eszköz közötti kommunikáció nem jöhet létre megfelelő fizikai összeköttetés nélkül.

A vezetékes kommunikációt a réz és optikai átviteli közegek alkotják.

- Hálózatok esetében három fő típusa létezik a rézkábelnek: árnyékolatlan csavart érpár (UTP), árnyékolt csavart érpár (STP) és a koaxiális kábel. A leggyakoribb réz alapú hálózati közegnek az UTP kábelt tekintjük.

- A hálózatok gerincét alkotó eszközök összekapcsolására leginkább az optikai kábelt használjuk. Bármely más hálózati közeghez képest hosszabb távolságú és nagyobb sávszélességű adatátvitelt tesz lehetővé. A rézvezetékekkel ellentétben az optikai kábel kisebb csillapítással képes a jeltovábbításra, valamint teljesen érzéketlen az EMI és RFI okozta zavarokra.

A vezeték nélküli közegek rádió- vagy mikrohullámok használatával továbbítják az elektromágneses jeleket, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg.

A vezeték nélküli átvitelre képes eszközök száma egyre növekszik. Emiatt válhatott a vezeték nélküli átvitel az otthoni hálózatok közegtípusává, továbbá vállalati hálózatok esetében is egyre nő a népszerűsége.

Az adatkapcsolati réteg felelős a keretek csomópontok közötti továbbításáért a fizikai közegen. Lehetővé teszi a felsőbb rétegek számára az átviteli közeg elérését, valamint vezérli az adatok közegre helyezésének és fogadásának módját.

Az adatkapcsolati protokollok eltérő változatai között különböző módszerek léteznek a közeghozzáférés szabályozására. Ezek a módszerek határozzák meg, hogy az állomások megosztozzanak-e a közegen, és ha igen, akkor milyen módon. A megfelelő közeghozzáférési módszer kiválasztása a topológiától és a közeg megosztásától függ. A LAN és WAN topológiák fizikai vagy logikai topológiák lehetnek. A logikai topológia az, amely befolyással van a keretezés típusára és a közeghozzáférés módjára. A WAN hálózatok összekapcsolása pont-pont, csillagponti vagy hálós topológiák használatával történik. Osztott közegű helyi hálózatok esetén a végberendezések csillag, busz, gyűrű vagy kiterjesztett csillag (hibrid) topológiák használatával kapcsolódhatnak egymáshoz.

Az adatkapcsolati réteg protokolljai a 3. rétegbeli protokoll adategységet (PDU) ágyazzák be a keret adatmező részébe. A keret felépítése, valamint a fejlécben és az utótagban található mezők viszont protokollonként eltérőek lehetnek.

Az OSI modell fizikai rétege biztosítja egy adatkapcsolati rétegbeli keret bitjeinek hálózati közegen történő továbbításának eszközeit.

Jelenleg az Ethernet az uralkodó LAN technológia a világon. Az Ethernet az OSI modell két rétegében működik: az adatkapcsolati és a fizikai rétegben. Az Ethernet protokoll szabványai a hálózati kommunikációt sok szempontból definiálják, beleértve a keret formátumát, a keret méretét, az időzítést és a kódolást. Amikor egy Ethernet hálózaton üzeneteket küldünk az állomások között, akkor azok a szabványokban meghatározott keretformátumúvá alakítják az üzeneteket. A kereteket protokoll adategységeknek (Protocol Data Unit, PDU) is nevezik.

Mivel az Ethernet-et ezen alsóbb rétegek szabványai tartalmazzák, legjobban talán az OSI modellre hivatkozva lehet megérteni. Az OSI modell elkülöníti az adatkapcsolati réteg címzési, keretezési és közeg-hozzáférési funkcióit a közeg fizikai rétegbeli szabványaitól. Az Ethernet szabványok mind a második rétegbeli protokollokat, mind pedig az első rétegbeli technológiákat meghatározzák. Bár az Ethernet szabvány különböző közegeket, sávszélességeket és eltérő 1. és 2. rétegbeli variációkat támogat, az alapvető keretformátum és a címzési rendszer az Ethernet mindegyik változatánál ugyanaz.

Ez a fejezet megvizsgálja az Ethernet működését és jellemzőit, ahogyan egy osztott közegű, versengésen alapuló adatkommunikációs technológiából napjaink nagy sebességű, full-duplex technológiájává fejlődött.

Csatlakozz az ismerősi körömhöz!

A legtöbb hálózati kommunikációnk üzenetküldés (szöveges vagy azonnali), videó kapcsolat, közösségi média hozzászólások stb. formájában történik.

Ehhez a feladathoz válasszunk ki egyet az általunk leggyakrabban használt kommunikációs hálózatokból:

- Szöveges (vagy azonnali) üzenetküldés
- Audió / videó konferencia
- E-mailezés
- Játék

Miután kiválasztottunk egy hálózati kommunikációs típust, jegyezzük fel a válaszokat az alábbi kérdésekre:

- Van-e olyan eljárás, amit követnünk kell a magunk és mások regisztrálásához azért, hogy kommunikációs csoportot alkossunk?
- Hogyan kezdeményezzük a kapcsolatot azzal személlyel (vagy személyekkel), akivel kommunikálni szeretnénk?
- Hogyan korlátozzuk a párbeszédeket, hogy csak azok kapják meg az üzeneteket, akikkel kommunikálni szeretnénk?

Készüljünk fel, hogy megvitassuk a rögzített válaszokat az osztállyal.

Csoportos feladat - Utasítások a Csatlakozz az ismerősi körömhöz! feladathoz

Az Ethernet manapság a legelterjedtebb LAN technológia.

Az Ethernet az OSI modell adatkapcsolati és fizikai rétegeiben működik. Az IEEE 802.2 és 802.3 szabványok a hálózati technológiáknak egy egész családját definiálják Az Ethernet a következő sávszélességeket támogatja:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10000 Mb/s (10 Gb/s)
- 40000 Mb/s (40 Gb/s)
- 100000 Mb/s (100 Gb/s)

Amint az 1. ábrán látható, az Ethernet szabványok meghatározzák mind a 2. rétegbeli protokollokat, mind pedig az 1. rétegbeli technológiákat. Mint minden 802 IEEE-szabvány, az Ethernet működése is az adatkapcsolati rétegben lévő két különálló alrétegre, az LLC- (Logical Link Control) és a MAC- (Media Access Control) alrétegekre támaszkodik.

LLC-alréteg

Az Ethernet LLC-alréteg kezeli a felsőbb és az alsó rétegek közötti kommunikációt. Ez jellemzően a hálózati szoftver és a készülék hardvere között zajlik. Az LLC-alréteg veszi a hálózati protokoll adatait - ami jellemzően egy IPv4 csomag - és olyan vezérlő információkkal látja el, amelyek segítik a csomagnak a célállomáshoz történő eljuttatását. Az LLC-t az alkalmazás felsőbb rétegeivel történő kommunikációra, valamint a csomag átalakítására használjuk, hogy az alsóbb rétegek továbbítani tudják.

Az LLC szoftveresen van megoldva, és így a megvalósítása független a hardvertől. Egy számítógépen a hálózati kártya (NIC) meghajtóprogramja tekinthető az LLC-nek. A hálózati kártya meghajtóprogramja egy olyan program, amely közvetlen kölcsönhatásban van a kártya hardverével, hogy az adatokat továbbadja a MAC-alréteg és a fizikai közeg között.

MAC-alréteg

A MAC-alréteg az adatkapcsolati réteg alsó alrétege. A MAC-alréteget hardveresen valósítják meg, tipikusan a számítógép hálózati kártyájában. A részleteket az IEEE 802.3 szabványok határozzák meg. A 2. ábra az általános IEEE Ethernet szabványokat sorolja fel.

Amint az ábrán látható, az Ethernet MAC-alrétegnek két fő feladata van:

- Adatbeágyazás
- Közeghozzáférés-vezérlés

Adatbeágyazás

Az adatbeágyazási folyamat magában foglalja a keret összeállítását a továbbítás előtt, és a szétbontását a kézhezvétel után. A keret felépítésekor a MAC-réteg egy fejlécet és egy utótagot ad a hálózati réteg PDU-jához.

Az adatbeágyazás három fő funkciót biztosít:

- **Keret határolás**: A keretezési folyamat fontos határolókat biztosít, amiket a keretet alkotó bitek csoportjának azonosítására használnak. Ez a folyamat biztosítja a szinkronizációt az adó és a vevő csomópontok között.
- **Címzés**: A beágyazási folyamat az adatkapcsolati réteg címzését is biztosítja. Minden Ethernet keret fejléce tartalmazza a fizikai címet (MAC-cím), amely lehetővé teszi a keret kézbesítését a rendeltetési helyére.
- **Hibafelismerés**: Mindegyik Ethernet keret tartalmaz egy utótagot a keret tartalmára vonatkozóan, ami egy ciklikus redundancia ellenőrzés (CRC). Egy keret vétele után a fogadó csomópont is készít egy CRC-t, hogy összehasonlítsa azt a keretben lévővel. Ha a két CRC-számítás eredménye megegyezik, a keret nagy valószínűséggel hiba nélkül érkezett.

A keretek használata segíti a közegre helyezett bitek átvitelét és a fogadó csomóponton a bitek csoportosítását is.

Közeghozzáférés-vezérlés

A MAC-alréteg másik feladata a közeghozzáférés-vezérlés. Ez felelős a keretek közegre való elhelyezéséért és azok eltávolításáért. Ahogy a neve is mutatja, ez szabályozza a közeghez való hozzáférést. Ez az alréteg közvetlenül a fizikai réteggel kommunikál.

Az Ethernet mögöttes logikai topológiája egy többszörös hozzáférésű sín (vagy busz), ezért az azonos hálózati szegmensen lévő csomópontok (eszközök) osztoznak a közegen. Az Ethernet a hálózatkezelés egy versengés alapú módszere. Emlékezzünk rá, hogy a versengés alapú, vagy nem-determinisztikus módszer azt jelenti, hogy bármelyik eszköz megpróbálhat adatot továbbítani a megosztott közegen, amennyiben van elküldendő adata. Hasonlóan ahhoz, mint amikor két ember próbál meg egyszerre beszélni, ha több eszköz próbál ugyanazon közegen és egy időben adatokat továbbítani, az adatok ütköznek, ami sérült vagy használhatatlan adatokat eredményez. Emiatt az Ethernet biztosít egy módszert a csomópontok közeghozzáférésének vezérlésére, ez a módszer a Vivőérzékeléses Többszörös Hozzáférés (Carrier Sense Multiple Access, CSMA) technológia.Ezért az Ethernet egy vivőérzékeléses többszörös hozzáférésnek (Carrier Sense Multiple Access, CSMA) nevezett technológiát alkalmazó módszert biztosít a csomópontok közeghozzáférés-vezérlésének kezelésére.

A CSMA-folyamatot először annak érzékelésére használjuk, hogy a közegen történik-e jeltovábbítását. Ha egy másik csomóponttól származó vivőjelet érzékelünk a közegen, az azt jelenti, hogy egy másik készülék adásban van. Ha a készülék - amelyik továbbítani próbál - azt látja, hogy a közeg foglalt, akkor vár és kis idő múlva újra próbálkozik. Ha nem észlel vivőjelet, akkor továbbítja az adatokat. Előfordulhat hogy a CSMA-folyamat meghiúsul, mert két eszköz ugyanabban az időben továbbít.. Ez az úgynevezett adatütközés, vagy röviden ütközés. Amennyiben ez történik, akkor mindkét készülék elküldött adatai megsérülnek és újra el kell őket küldeni.

A versengés alapú közeghozzáférési módszerek nem igényelnek olyan mechanizmusokat, amelyek nyomon követik, hogy ki fog legközelebb hozzáférni a közeghez, ezért nincs is bennük az ellenőrzött módszerekre jellemző többletterhelés. Ugyanakkor a versengés alapú rendszerek nagy mértékű közeghasználat esetén nem jól skálázhatók. Ahogy a közeghasználat és a csomópontok száma növekszik, egyre csökken annak a valószínűsége, hogy ütközés nélküli, vagyis sikeres legyen a közeghez való hozzáférés. Ezen felül az ütközési hibákat kijavító helyreállítási mechanizmusok tovább rontják a teljesítményt.

Amint az ábrán látható, a CSMA-t általában a közegért való versengés megoldására szolgáló módszerrel együtt valósítják meg. A két leggyakrabban használt módszer a következő:

CSMA/CD (ütközésérzékelés)

Az ütközésérzékelés (CSMA/Collision Detection, CSMA/CD) esetén a készülék figyeli, hogy van-e adatjel a közegen. Amennyiben az adatjel hiányzik, jelezve hogy a közeg szabad, a készülék továbbítja az adatokat. Ha ezek után adatjeleket érzékelünk - ami azt jelzi, hogy egy másik készülék is ugyanabban az időben forgalmazott -, minden más eszköz leállítja a küldést és később újra próbálkozik. Az Ethernet hagyományos változatait ennek a módszernek a használatára fejlesztették ki.

A kapcsolt technológiák széleskörű elterjedése a modern hálózatokban nagymértékben megváltoztatta a CSMA/CD használatával kapcsolatos igények. A LAN-eszközök között szinte az összes vezetékes kapcsolat manapság full-duplex, vagyis a készülék egyszerre képes küldeni és fogadni is. Ez azt jelenti, hogy míg az Ethernet hálózatokat a CSMA/CD-technológiára tervezték, a mai közvetítő eszközöknél ütközések nem fordulnak elő, és a CSMA/CD által használt folyamatok valójában feleslegesekké váltak.

A vezeték nélküli LAN-környezetben lévő kapcsolatoknál azonban még figyelembe kell venni az ütközéseket. A vezeték nélküli LAN-eszközök a CSMA/Collision Avoidance (ütközés elkerülés, CSMA/CA) közeg-hozzáférési módot alkalmazzák.

CSMA/Collision Avoidance (ütközés elkerülés)

A CSMA/CA estében a készülék megvizsgálja a közeget, hogy érzékelhető-e adatjel. Ha a közeg szabad, akkor a készülék küld egy értesítést a média használati szándékáról. A készülék ezután elküldi az adatokat. Ezt a módszert használják a 802.11 vezeték nélküli hálózati technológiák.

Mint korábban említettük, az Ethernet logikai topológiája egy többes hozzáférésű sín. Minden hálózati eszköz ugyanahhoz megosztott közeghez csatlakozik és minden csomópont megkapja a közegen továbbított összes keretet. A kérdés csupán az, hogy ha minden eszköz megkap minden keretet, akkor hogyan tudják az egyes eszközöknek beazonosítani, hogy ők-e a valódi címzettek, és mindezt anélkül, hogy fel kellene dolgozniuk és ki kellene bontaniuk a kereteket az IP-cím megszerzése érdekében? A kérdés még inkább problematikus nagyméretű és nagy forgalmú hálózatok esetében, ahol rengeteg keretet továbbítanak.

Az összes keretek feldolgozásából adódó túlzott mértékű többletterhelés megakadályozása érdekében egy MAC-címnek nevezett egyedi azonosítót hoztak létre, hogy a tényleges forrás- és célcsomópontokat azonosítani lehessen egy Ethernet hálózaton belül. Függetlenül attól, hogy melyik Ethernet verziót használjuk, az OSI modell alsóbb szintjén a MAC-címzés azonosítja az eszközt. Mint bizonyára emlékszünk rá, a MAC-címzés a második rétegbeli PDU-hoz adódik hozzá. Az Ethernet MAC-cím egy 48 bites bináris érték, amit 12 hexadecimális számjeggyel írunk le (egy hexadecimális számjegy 4 bitet jelöl).

A MAC-címek szerkezete

A MAC-címek az egész világon egyediek kell hogy legyenek. Az Ethernet eszközök MAC-címeinek globálisan is egyedi értékei az IEEE-szervezet gyártókra vonatkozó szabályozásának az eredménye. Az IEEE által létrehozott szabályok bármely Ethernet eszköz gyártójától elvárják, hogy regisztrálja magát az IEEE-nél. Az IEEE a gyártóhoz egy 3 bájtos (24 bites) kódot rendel hozzá, az úgynevezett egyedi szervezetazonosítót (OUI).

Az IEEE elvárja a gyártótól, hogy kövessenek két egyszerű szabályt, ahogy azt az ábra mutatja:

- A hálózati kártyának vagy más Ethernet eszköznek adott MAC-cím első 3 bájtjának tartalmaznia kell a gyártóhoz rendelt OUI-t.

Az ugyanolyan OUI-val rendelkező MAC-címeknek egy egyedi értéket (vendor kód vagy sorozatszám) kell tartalmazniuk az utolsó 3 bájtban.

A MAC-címet gyakran nevezik beégetett címnek (Burned-In Addresss, BIA), mert régen ezt a címet beleégették a hálózati kártya ROM-jába (Read-Only Memory). Ez azt jelenti, hogy a cím véglegesen bele van kódolva a ROM chipbe - nem lehet szoftveresen megváltoztatni.

Megjegyzés: A modern operációs rendszerek és a hálózati kártyák esetén szoftveresen is meg lehet változtatni a MAC-címet. Ezt például akkor használják, ha megpróbálnak behatolni olyan hálózatba, amely BIA alapján szűri a hozzáférést - következésképpen, a forgalom MAC-címen alapuló szűrése vagy ellenőrzése ma már nem olyan biztonságos.

A MAC-címet hozzárendelhetjük munkaállomásokhoz, szerverekhez, nyomtatókhoz, kapcsolókhoz és forgalomirányítókhoz - minden olyan eszközhöz, amelyről adat származik, és/vagy adatokat fogadhat a hálózaton. Minden Ethernet LAN-ra csatlakozott eszköz interfészének van egy MAC-címe. A különböző hardver- és szoftver-gyártók a MAC-címet különböző hexadecimális formátumban adhatják meg. A címformátumok az alábbiakhoz hasonlók lehetnek:

- 00-05-9A-3C-78-00
- 00:05:9A:3C:78:00
- 0005.9A3C.7800

A számítógép elindulásánál a NIC első teendője, hogy bemásolja a MAC-címet a ROM-ból a RAM-ba. Amikor egy eszköz üzenetet továbbít egy Ethernet hálózatra, fejléc információt csatol a csomaghoz. A fejléc információi tartalmazzák a forrás és a cél MAC-címeket. A forrás készülék elküldi az adatokat a hálózaton keresztül.

A hálózaton minden NIC megvizsgálja az adatokat a MAC-alrétegben, hogy a keretbeli cél MAC-cím megegyezik-e a készülék RAM-ban tárolt fizikai MAC-címével. Ha nincs egyezés, akkor a készülék eldobja a keretet. Amikor a keret eléri azt a helyet, ahol a cél MAC-cím megegyezik a NIC címével, a hálózati kártya átadja a keretet a felsőbb OSI-rétegeknek, ahol elkezdődik a kibontási folyamat.

1973 - az Ethernet megalkotása - óta szabványok egész sora született a technológia egyre gyorsabb és rugalmasabb változatainak kifejlesztésére. Az Ethernet képes volt fejlődni az idők folyamán, ez a legfőbb oka annak, hogy ilyen népszerűvé vált. Az Ethernet korai változatai viszonylag lassúak, 10 Mb/s sebességűek voltak. A legújabb Ethernet verziók már 10 Gb/s vagy gyorsabb sebességgel működnek. Az 1. ábra a különböző Ethernet változatokban bekövetkezett változásait szemlélteti.

Az adatkapcsolati réteg szintjén a keretszerkezet gyakorlatilag az Ethernet összes változatánál azonos. Az Ethernet keretszerkezet fejléceket és utótagokat ad a 3. rétegbeli PDU elé és mögé, hogy beágyazza az elküldendő üzenetet.

Mind az Ethernet fejléc, mind az utótag több szakaszban tárol információkat, amelyet az Ethernet protokoll használ. A keret minden szakaszát mezőnek nevezzük. Amint a 2. ábrán látható, két típusú Ethernet keretezés létezik:

- Az IEEE 802.3 Ethernet szabvány, amely az új technológiák támogatására már többször változott.

- A DIX Ethernet szabvány, amelyet manapság Ethernet II-ként emlegetnek.

A keretezési szabványok közti különbség minimális. A legjelentősebb különbség a két szabvány között, hogy a 802.3-ban hozzáadtak egy keretkezdő mezőt (Start Frame Delimiter, SFD) és a típus mező hossz mezőre változott.

Az Ethernet II a TCP/IP-hálózatokon használt Ethernet keretformátuma.

Mind az Ethernet II, mind az IEEE 802.3 szabványok úgy határozzák meg a keret méretét, hogy minimum 64 bájt, illetve maximum 1518 bájt lehet. Ez magában foglalja az összes bájtot a cél MAC-cím mezőtől kezdve a keretellenőrző (Frame Check Sequence, FCS) mezőig. Az előtag és keretkezdő mezőket nem vesszük figyelembe, amikor megadjuk a keret méretét.

Minden keretet, ami kevesebb, mint 64 bájt hosszúságú, ütközési töredéknek vagy runt-nak nevezünk és ezeket automatikusan eldobja a fogadó állomás.

Az 1998-ban megjelent IEEE 802.3ac szabvány 1522 bájtra terjesztette ki a megengedett legnagyobb keret méretét. A keret méretét azért növelték meg, hogy támogassa az úgynevezett virtuális helyi hálózat (VLAN) technológiát. A VLAN-ok egy kapcsolt hálózatban jönnek létre, és egy későbbi kurzus folyamán kerülnek bemutatásra. Továbbá a legtöbb szolgáltatásminőséggel (QoS) foglalkozó technológia kihasználja a felhasználói prioritás mezőt, hogy különböző szolgáltatási szinteket tudjon biztosítani, például prioritásos szolgáltatást a hangforgalom számára. Az ábrán a 802.1Q VLAN címkében lévő mezők láthatók.

Ha egy átvitt keret mérete kisebb, mint a minimális vagy nagyobb, mint a maximális érték, a fogadó készülék eldobja a keretet. Az eldobott keretek valószínűleg ütközések és más nem kívánt jelek eredményei, ezért érvénytelennek tekintendők.

Az adatkapcsolati réteg szintjén a keret szerkezete majdnem azonos. A fizikai rétegben az Ethernet különböző változatai eltérő módszereket használnak az adatok érzékelésére és közegre való helyezésére.

Az elsődleges mezők az Ethernet kereten belül a következők:

- **Előtag és keretkezdő mezők**: Az előtag (7 bájt) és a keretkezdő (Start Frame Delimiter, SFD, más néven Start of Frame, 1 bájt) mezőket szinkronizálásra használják a küldő és fogadó készülékek között. A keretnek ezt az első nyolc bájtját használják, hogy a fogadó csomópontnak felhívják a figyelmét. Lényegében az első néhány bájt azt mondja a vevőnek, hogy álljon készen az új keret fogadására.

- **Cél MAC-cím mező**: Ez a 6 bájtos mező azonosítja a címzettet. Ha visszaemlékszünk, ezt a címet használja a második réteg, hogy segítse az eszközöket annak meghatározásában, hogy egy keret nekik szól-e. A keretben lévő címet összehasonlítják a készülék MAC-címével. Ha egyezés van, a készülék elfogadja a keretet.

- **Forrás MAC-cím mező**: Ez a 6 bájtos mező a keretet küldő hálózati kártyát vagy interfészt azonosítja.

- **Hossz mező**: Minden 1997-nél régebbi IEEE 802.3 szabványban a hossz mező határozza meg a keret adatmezejének pontos hosszát. Ezt később az FCS részeként használják, hogy biztosak legyünk abban, az üzenet megfelelően megérkezett. Egyéb esetekben a mező célja annak jelzése, hogy melyik magasabb szintű protokoll lett a keretbe beágyazva. Ha a két-oktettes érték nagyobb vagy egyenlő, mint 1536 (decimálisan) vagy 0x0600 hexadecimálisan, akkor az adatmező tartalmát aszerint dekódoljuk, amit az EtherType protokoll jelez. Ha az érték kisebb vagy egyenlő, mint az 1500 (decimálisan) vagy 0x05DC hexadecimális érték, akkor a hossz mezőt használják arra, hogy jelezze az IEEE 802.3 keretformátum használatát. Így különböztethetők meg az Ethernet II és a 802.3 keretek.

- **Adat mező**: Ez a mező (46-1500 bájt) tartalmazza a magasabb rétegbeli beágyazott adatokat, amely egy általános 3. rétegbeli PDU, vagy még gyakrabban egy IPv4 csomag. Minden keretnek legalább 64 bájt hosszúnak kell lennie. Ha egy kis csomagot ágyazunk be, akkor további biteket, úgynevezett kitöltést (pad) használnak, hogy megnöveljék a keret méretét a minimális méretre.

- **Keretellenőrző mező**: A keretellenőrző (Frame Check Sequence, FCS) mezőt (4 bájt) a hibák észlelésére használják a keretben. Ez a ciklikus redundancia-ellenőrzést (CRC) használja. A küldő készülék beleteszi a CRC-számítás eredményét a keret FCS-mezejébe. A fogadó készülék megkapja a keretet, és szintén generál egy CRC-t a hibakereséséhez. Ha a számítások megegyeznek, nem történt hiba. Ha a számítások nem egyeznek, az azt jelzi, hogy az adat megváltozott, ezért a keretet el kell dobni. Az adatban bekövetkezett változás annak a következménye lehet, hogy a biteket képviselő elektromos jelekben zavar keletkezett.
    - A MAC-cím használata az egyik legfontosabb szempontja az Ethernet LAN technológiának. A MAC-címek hexadecimális számozást használnak.
    - A hexadecimális egy olyan szó, amit mind főnévként, mind melléknévként is használnak. (Megjegyzés: ez az eredeti angol "hexadecimal" kifejezésre igaz, ám a magyar nyelvben jellemzően melléknévként használt.) Amikor önmagában (mint főnév) használjuk, a tizenhatos (hexadecimális) számrendszert jelenti. A hexadecimális rendszer egy kényelmes módját biztosítja a bináris értékek leírásának. Ahogy a decimális egy tízes alapú, a bináris pedig egy kettes alapú számrendszer, úgy a hexadecimális egy tizenhatos alapú rendszer.
    - A tizenhatos alapú számrendszer 0 és 9 közötti számokat használ, valamint betűket az A és az F között. Az 1. ábra a 0000-1111 közötti bináris értékek decimális és hexadecimális megfeleltethetőségét ábrázolja. Könnyebb egy értéket egyetlen hexadecimális számjeggyel kifejezni, mint négy darab bináris jeggyel.
    - Tekintettel arra, hogy 8 bit egy közös bináris csoportot (bájtot) alkot, a bináris 00000000-11111111 közti értékeket ki lehet fejezni a hexadecimális 00-tól FF-ig terjedő tartománnyal. A bevezető nullákat mindig megjelenítjük a teljes 8 bites kiírásnál. Például a 0000 1010 bináris értéket hexadecimális 0A-ként írjuk le.

- **Megjegyzés**: Fontos, hogy megkülönböztessük a hexadecimális értékeket a decimális értéktől a 0-9 karakterek tekintetében, amint azt az 1. ábra mutatja.
- **Hexadecimális értékek leírása**
- A hexadecimális értékeket általában szövegesen írjuk le, ahol a konkrét értéket egy 0x előzi meg (pl. 0x73), vagy használhatunk egy 16-os alsó index-et is a jelölésre. Ritkábban egy H is követheti a számot, például 73H. Mivel azonban az index szövegét nem ismeri fel a parancssor vagy egy programozási környezet, a műszaki leírásban a hexadecimális értéket a "0x" (nulla X) vezeti be. Ezért a fenti példák így jelennek meg: 0x0A és 0x73.
- A hexadecimális jegyeket használják az Ethernet MAC-címek és az IPv6-címek leírására is.
- **Hexadecimális számok átváltása**
- A decimális és hexadecimális számok közti átváltás nem bonyolult művelet, de 16-tal gyorsan osztani vagy szorozni nem mindig könnyű. Ha ilyen átalakítások szükségesek, általában könnyebb a decimális vagy hexadecimális értéket binárissá átalakítani, majd azután a binárist értéket alakítani át decimális vagy hexadecimális értékké.
- Megfelelő gyakorlattal fel lehet ismerni a decimális és hexadecimális értékeknek megfeleltethető bináris bitmintákat. A 2. ábra ezeket a mintákat mutatja a kiválasztott 8 bites értékekhez.
- Windows munkaállomáson az **`ipconfig /all`** paranccsal lehet megállapítani egy Ethernet adapter MAC-címét. Az 1. ábrán figyeljük meg a kimenetben a Physical Address (MAC) értéket, a számítógépen ez 00-18-DE-C7-F3-F8. Ha van hozzáférésünk, akkor érdemes ezt kipróbálni a saját számítógépen.
- A készüléktől és az operációs rendszertől függően a MAC-címek különböző ábrázolásait figyelhetjük meg, mint ez a 2. ábrán látható. A Cisco forgalomirányítók és kapcsolók a következő formátumot használják: XXXX.XXXX.XXXX, ahol X egy hexadecimális karakter.
- Az Etherneten belül különböző MAC-címeket használunk a második rétegbeli egyedi címzésű, szórásos és csoportos kommunikációra.
- Az egyedi címzésű (unicast) MAC-címet használunk, amikor egy keretet az adó eszközről egyetlen cél eszköznek küldünk.
- Az ábrán látható példában a 192.168.1.5 (forrás) IP-című állomás lekér egy weboldalt a 192.168.1.200 IP-című szervertől. Ahhoz, hogy egyedi címzésű csomagot küldhessünk és fogadhassunk, a cél IP-címnek szerepelnie kell az IP-csomag fejlécében. A megfelelő cél MAC-címnek szintén benne kell lennie az Ethernet keret fejlécében. Az IP-cím és a MAC-cím együttesen kézbesíti az adatokat egy adott célállomáshoz.
- A szórásos csomagban cél címként egy olyan IP-cím van, ami csupa 1-est tartalmaz az állomás részében. Ez a számozás a címben azt jelenti, hogy a helyi hálózat összes gépe (a szórási tartomány) fogadja és feldolgozza a csomagot. Számos hálózati protokoll, mint például a DHCP és az ARP (Address Resolution Protocol) szórásos üzenetküldést használ. Azt, hogy az ARP hogyan képezi le a 2. rétegbeli címeket 3. rétegbelire, ennek a fejezetnek egy későbbi részében tárgyaljuk.
- Amint az ábrán látható, egy szórásos IP-címnek szüksége van a megfelelő szórásos MAC-címre is az Ethernet keretben. Az Ethernet hálózatokon a szórásos MAC-cím 48 darab egyesből áll, ez hexadecimálisan megjelenítve FF-FF-FF-FF-FF-FF.
- A csoportos címek lehetővé teszik a forráseszköz számára, hogy eszközök egy csoportjának küldjön csomagot. Azoknak az eszközöknek, amik többes címzésű csoporthoz tartoznak, csoportos IP-címe van. Az IPv4 multicast címek tartománya 224.0.0.0 - 239.255.255.255. Mivel a multicast cím a címek egy csoportját jelenti (néha állomás-csoportnak is hívják), csak csomagok cél címeként használható. A forrásnak mindig egyedi címe van.
- A csoportos címzésre példaként említhetjük a távoli játékokat, ahol sok távoli játékos kapcsolódik össze, de mégis ugyanazt a játékot játsszák. Egy másik alkalmazása ezeknek a címeknek egy távoktatási videokonferencia lehet, ahol sok diák csatlakozik be ugyanabba az osztályba.
- Mint a unicast és broadcast címek, a multicast IP-cím is igényel egy megfelelő csoportos MAC-címet, hogy el tudja juttatni a kereteket a helyi hálózaton. A csoportos MAC-cím egy speciális érték, ami hexadecimális 01-00-5E-vel kezdődik. A csoportos MAC-cím fennmaradó része úgy jön létre, hogy a csoportos IP-cím alsó 23 bitjét átalakítjuk 6 hexadecimális karakterré.
- Az animáció példájában látható hexadecimális csoportcím a 01-00-5E-00-00-C8.

Ebben a laborgyakorlatban a következő feladatokat hajtjuk végre:

- 1. rész: A topológia kiépítése és az eszközök kezdeti beállítása.
- 2. rész: Az eszközök konfigurálása és a kapcsolat ellenőrzése.
- 3. rész: Az Ethernet MAC-címek megjelenítése, leírása és elemzése.

Laborgyakorlat - Viewing Network Device MAC Addresses

Két fő címet rendelünk egy állomáshoz:

- fizikai címet (MAC-címet)
- logikai címet (IP-címet)

A MAC- és IP-cím közösen azonosítják be a készüléket a hálózaton. A folyamat, amelynek során a MAC-cím és az IP-cím segítségével megtalálunk egy számítógépet, hasonló ahhoz, mint amikor egy egyén nevét és címét használjuk levélküldés céljából.

Egy személy neve általában nem változik. Másrészről a személy címe lakóhelyéhez kötődik és változhat is.

Egy adott személy nevéhez hasonlóan az állomás MAC-címe sem változik, fizikailag rendelik hozzá a gép hálózati kártyájához és fizikai címként ismeretes. A fizikai cím nem változik, függetlenül attól, hogy a gép hova kerül.

Az IP-cím hasonló egy személy címéhez. Ez a cím azon alapul, hogy az állomás ténylegesen hol található. Ezt a címet felhasználva lehetséges az, hogy egy keret meghatározza azt a helyet, ahova a keretet el kell küldeni. Az IP-cím vagy hálózati cím úgynevezett logikai cím, mert logikailag rendeljük hozzá az állomáshoz. Minden állomáshoz aszerint rendeli hozzá a hálózati rendszergazda, hogy az állomás melyik helyi hálózatra csatlakozik. Az ábra annak a hierarchikus jellegét mutatja be, ahogyan egy egyént keresünk meg egy "logikai" címre alapozva. Kattintsunk az egyes csoportosításokra, hogy lássuk, a cím hogyan tevődik össze.

Mind a fizikai MAC-, mind pedig a logikai IP-cím szükséges a számítógép számára ahhoz, hogy egy hierarchikus hálózaton kommunikálni tudjon, mint ahogy egy személyről is szükséges tudni a nevét és a címét, hogy levelet tudjunk küldeni neki.

A forrás eszköz a csomagot egy IP-cím alapján küldi el. Az egyik leggyakoribb módja annak, hogy a forrás eszköz meghatározza a cél eszköz IP-címét a DNS-szolgáltaatás (Domain Name Service), amelyben az IP-címhez egy tartománynevet társítunk. Például a www.cisco.com egyenértékű 209.165.200.225 címmel. Ez az IP-cím juttatja el a csomagot arra a hálózati helyre, ahol a cél eszköz van. A forgalomirányítók ezt az IP-címet fogják használni, hogy meghatározzák a cél eléréséhez a legjobb útvonalat. Röviden jellemezve, az IP-címzés határozza meg az IP-csomagok végpontok közötti viselkedését.

Mindamellett egy IP-csomag az útvonal mentén minden kapcsolatszakaszon külön-külön beágyazódik az arra a szakaszra jellemző keretbe, mint például amilyen az Ethernet is. Egy Ethernet hálózaton a végberendezések a kapott kereteket nem az IP-cím, hanem a MAC-cím alapján fogadják és dolgozzák fel.

Az Ethernet hálózatok a MAC-címeket használják a forrás és a cél állomások azonosítására. Amikor egy Ethernet hálózaton lévő állomás kommunikál, akkor olyan kereteket küld ki, amelyekben a saját MAC-címe a forráscím, és a kívánt címzett MAC-címe a célcím. Minden eszköz, amely a keretet megkapja kiolvassa belőle a cél MAC-címét. Az állomás kizárólag abban az esetben fogja a teljes üzenetet feldolgozni, amennyiben a cél MAC-cím megegyezik az állomás hálózati kártyáján beállított MAC-címmel.

Az 1. ábra azt mutatja, hogy egy IP-cím információkat tartalmazó adatcsomag hogyan ágyazódik be a MAC-címet is tartalmazó adatkapcsolati rétegbeli keretbe.

A 2. ábra azt szemlélteti, hogy a kereteket hogyan ágyazódnak be a tényleges kapcsolat technológiájára alapozva.

Hogyan társítjuk azonban a célhoz vezető valamennyi kapcsolaton egy adatfolyam csomagjaiban lévő IP-címeket a MAC-címekhez? Ezt a folyamatot az úgynevezett címfeloldási vagy címmeghatározó protokoll (Address Resolution Protocol, ARP) végzi.

Emlékezzünk vissza, hogy egy IP-hálózaton minden egyes csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Mindkét cím használata szükséges annak érdekében, hogy egy állomás adatokat küldhessen. Az állomásnak a saját MAC- és IP-címét kell használnia a forrás mezőkben, valamint meg kell adnia a célállomás MAC- és IP-címét is. Míg a cél IP-címet egy magasabb OSI-réteg fogja biztosítani, a küldő csomópontnak szüksége van egy módszerre ahhoz, hogy egy adott Ethernet kapcsolaton megtalálja a cél MAC-címét. Ez az ARP feladata.

Az ARP az Ethernet bizonyos szórásos és egyedi címzésű üzeneteire támaszkodik, az úgynevezett ARP-kérésekre és az ARP-válaszokra.

Az ARP-protokoll két alapvető funkciót biztosít:

- IPv4-címek összerendelése MAC-címekkel.

- Az összerendelési táblázat kialakítása.
  - **IPv4-címek összerendelése MAC-címekkel**
  - Ahhoz, hogy egy keretet a LAN átviteli közegére helyezhessünk, annak minimum egy cél MAC-címmel kell rendelkeznie. Amikor egy csomagot egy adatkapcsolati keretbe ágyazva elküldünk, az állomás a memóriájában lévő táblázatra támaszkodik, hogy megtalálja a cél IPv4-címhez tartozó adatkapcsolati rétegbeli címet. Ez a táblázat az úgynevezett ARP-táblázat vagy ARP-gyorsítótár (cache). Az ARP-táblázatot a készülék RAM-ja tárolja.
  - Az ARP-tábla minden bejegyzése vagy sora egy IP-címet köt össze egy MAC-címmel. A két érték közti kapcsolatot összerendelésnek vagy leképezésnek hívjuk - ez egyszerűen azt jelenti, hogy megkeresve az IP-címet a táblában megtalálhatjuk a megfelelő MAC-címet is. Az ARP-tábla csak ideiglenesen tárolja (cache-eli) a helyi LAN-eszközökhöz tartozó összerendeléseket.
  - A folyamat indításához a továbbító állomás megpróbálja megtalálni a cél IPv4-címhez társított MAC-címet. Ha ez az összerendelés megtalálható a táblázatban, akkor az állomás azt a MAC-címet fogja használni cél MAC-címként a keretben. A keretet ezután rákódolják a hálózati közegre.
  - **Az ARP-táblázat karbantartása**
  - Az ARP-táblázatot dinamikusan kezelik az eszközök. Két módja van, hogy egy készülék összegyűjthesse a MAC-címeket. Az egyik módszer az, hogy figyelemmel kíséri a helyi hálózati szegmensen előforduló forgalmat. Ahogy az állomás kereteket kap a közegen, a keret forrás IP- és MAC-címeit rögzíti az ARP-táblázatában. Miközben a keretek továbbításra kerülnek, addig a készülék folyamatosan fel is tölti az ARP-tábláját a megfelelő címpárokkal.
  - A készülék címpárokhoz jutásának egy másik módja, ha ARP-kéréseket küld ki, ahogy ezt az ábra is mutatja. Az ARP-kérés egy 2. rétegbeli szórás az Ethernet LAN minden eszközének . Az ARP-kérés tartalmazza a célállomás IP-címét és a szórásos MAC-címet, ami FFFF.FFFF.FFFF. Mivel ez egy szórás, minden állomás az Ethernet LAN-on megkapja és megnézi a tartalmát. Az az állomás fog válaszolni, amelynek az IP-címe megegyezik a kérésben lévő IP-címmel. A válasz egy egyedi címzésű keret lesz, amely magában foglalja a kérdéses IP-címhez tartozó MAC-címet is. Ezt a választ a küldő fél egy új tételként hozzá tudja majd adni ARP-táblájához.
  - Az ARP-táblázatban lévő bejegyzést hasonló időbélyeggel látják el, mint ahogy a kapcsolók kezelik a MAC-címtáblájuk bejegyzéseit. Ha a készülék nem kap keretet egy adott eszköztől az időbélyeg lejárta előtt, az eszközhöz tatozó bejegyzés kikerül az ARP-táblázatból.

- Emellett statikus bejegyzéseket is lehet írni az ARP-táblába, de ez elég ritkán történik meg. A statikus ARP-bejegyzések nem járnak le az idő múlásával, és így kézzel kell őket eltávolítani.
- **A keret létrehozása**
- Mit tehet egy csomópont, ha egy keretet kell létrehoznia, és az ARP-cache nem tartalmaz bejegyzést a cél MAC-címhez tartozó IP-címről? Létrehoz egy ARP-kérést!
- Amikor az ARP-nek meg kell állapítania egy IPv4-címhez tartozó MAC-címet, azt először az ARP-táblázatban keresi. Ha a bejegyzés nem található, az IPv4 csomag beágyazása nem sikerül és a 2. rétegbeli folyamatok értesítik az ARP-t, hogy szükség van egy új összerendelésre. Az ARP folyamat ekkor kiküld egy ARP-kérést, hogy felderítse a helyi hálózaton a cél eszköz MAC-címét. Amennyiben egy eszköz a kérésben kapott cél IP-címmel rendelkezik, akkor egy ARP-választ küld vissza. Így létrejön az összerendelés az ARP-táblázatban. Az erre az IPv4-címre szóló csomagokat immár be lehet ágyazni a keretekbe.
- Ha egyetlen eszköz sem válaszol az ARP-kérésre, a csomagot eldobják, mivel a keret nem hozható létre. Ezt a beágyazási hibát jelenteni kell az eszköz felsőbb rétegei felé. Ha az eszköz egy közvetítő eszköz, például egy forgalomirányító, a felső rétegek dönthetnek úgy, hogy a forrás állomásnak egy hibát jelző ICMPv4-csomaggal válaszolnak.
- Az 1-5 ábrák egy a helyi fizikai hálózaton lévő állomás MAC-címének megszerzésére alkalmazott folyamatot szemléltetik.
- Minden keretet egy a helyi hálózati szegmensen lévő állomás felé kell továbbítani. Amennyiben a cél IPv4-állomás a helyi hálózaton van, a keret ennek a készüléknek a MAC-címét fogja használni mint cél MAC-címet.
- Ha a cél IPv4-állomás nem a helyi hálózaton található, abban az esetben a forrás csomópontnak a keretet ahhoz a forgalomirányító interfészhez kell továbbítani, amelyet ezen cél eléréséhez átjáróként vagy más néven a következő ugrásként (next hop) használunk. A forrás csomópont az átjáró MAC-címét fogja használni a célállomás címeként minden olyan keret esetében, amely olyan IPv4-csomagot tartalmaz, amelyet másik hálózaton lévő állomásnak címeznek.
- Az átjárónak, azaz a forgalomirányító interfészének a címét az állomások az IPv4-konfigurációjukban tárolják. Amikor az állomás létrehoz egy csomagot egy célállomásnak, összehasonlítja a cél IP-címet és a saját IP-címét annak meghatározására, hogy a két IP-cím ugyanazon a 3. rétegbeli hálózaton található-e. Ha a fogadó gép nem ugyanazon a hálózaton van, a forrás az ARP folyamatot az átjáró MAC-címének meghatározására használja.
- Abban az esetben, ha az átjáró bejegyzés nem szerepel a táblázatban, a normál ARP folyamat kiküld egy ARP-kérést, hogy megszerezze a forgalomirányító interfész IP-címéhez társított MAC-címet.
- Az 1-5 ábrák az átjáró MAC-címének megszerzésére alkalmazott folyamatot szemléltetik.
- Egy ARP-cache időzítő távolítja el minden eszközön azokat az ARP-bejegyzéseket, amelyeket egy meghatározott idő óta nem használtak. Az időzítő függ a készüléktől és annak operációs rendszerétől. Egyes Windows operációs rendszerek például 2 percig tárolják az ARP-cache bejegyzéseket. Ha ez idő alatt a bejegyzést ismételten használják, a hozzá tartozó ARP-időzítő 10 percre meghosszabbodik.
- Parancsokat is használhatunk, hogy az ARP-táblából manuálisan távolítsunk el bizonyos bejegyzéseket, vagy akár az összeset. Egy bejegyzés eltávolítása után, az ARP-kérés küldés és ARP-válasz fogadás folyamatának ismét meg kell történnie, hogy az összerendelés az ARP-táblázatba újból bekerülhessen.
- Minden készülék egyedi, az operációs rendszertől függő paranccsal rendelkezik az ARP-cache tartalmának törlésére. Ezek a parancsok semmilyen módon nem eredményezik az ARP végrehajtását. Egyszerűen csak eltávolítják a bejegyzéseket az ARP-táblából. Az ARP-szolgáltatást az IPv4-protokollba integrálják és maga a készülék hajtja végre. Működése észrevehetetlen mind a felső rétegbeli alkalmazások, mind a felhasználók számára.
- Amint az ábrán látható, bizonyos esetekben szükséges egy ARP-bejegyzés eltávolítása a táblából.
- Egy Cisco forgalomirányítón a **`show ip arp`**parancsot használjuk az ARP-táblázat megjelenítéséhez, amint az 1. ábrán látható.
- Egy Windows 7 PC-n az **arp -a** parancsot használjuk az ARP-táblázat megjelenítéséhez, amint a 2. ábrán látható.
- Az ábra az ARP-hez kapcsolodó két lehetséges problémát szemléltet.
- **A közeg túlterhelése**

- Szórásos keret lévén egy ARP-kérést a helyi hálózaton minden eszköz megkap és feldolgoz. Egy általános üzleti hálózaton ezek a szórások valószínűleg minimális hatással vannak a hálózati teljesítményre. Ugyanakkor ha nagy számú készüléket kapcsolnak be egyszerre és az összes hálózati szolgáltatás elérése ugyanabban az időben kezdődik, a teljesítmény egy kis időre csökkenhet. Ha például a laborban minden diák egyszerre jelentkezik be a tantermi számítógépekre és próbálja meg elérni az internetet, előfordulhatnak késések. Azonban miután a készülékek kiküldték az első ARP-szórásokat és megtanulták a szükséges MAC-címeket, a későbbi tanulási folyamatok hatása már csak minimális terhelést fog jelenteni.
- **Biztonság**
- Bizonyos esetekben az ARP használata potenciális biztonsági kockázatot jelenthet. Az ARP-spoofing (hamisítás) vagy az ARP-mérgezés egy-egy olyan technika, amely által a támadó hamis MAC-cím összerendeléseket juttat a hálózatra hamis ARP-kérések segítségével. Ha a támadó meghamisítja egy eszköz MAC-címét, akkor azután a kereteket már nem a megfelelő helyre fogják küldeni.
- Az ARP-hamisítás megakadályozásának egyik módja a manuálisan beállított statikus ARP-bejegyzések. Bizonyos hálózati eszközökön hitelesített MAC-címeket lehet beállítani, hogy a hálózati hozzáférést csak ezekre a listán szereplő eszközökre korlátozzuk.
- Az ARP-vel kapcsolatos szórási és biztonsági kérdések enyhíthetők a modern kapcsolókkal. A Cisco kapcsolók számos általános, de kifejezetten ARP jellegű biztonsági technológiát is alkalmaznak, hogy enyhítsék az Ethernet szórásokkal kapcsolatos problémákat.
- A kapcsolók szegmentálást biztosítanak a LAN-on, felosztva a LAN-t önálló ütközési tartományokra. A kapcsolón minden port egy külön ütközési tartományt jelent, és biztosítja a közeg teljes sávszélességét a portra csatlakozó állomás vagy állomások számára. Bár a kapcsolók alapértelmezés szerint nem akadályozzák a szórások továbbítását, de elkülönítik az egyedi címzésű Ethernet kommunikációt, hogy azt csak a forrás és a cél eszközök "hallhassák". Tehát lehet akár nagyszámú ARP-kérés is, az ARP-válaszok mindegyike már csak két eszköz között fog létrejönni.
- Tekintettel az Ethernet hálózatokon gyakori különféle szórásos támadások enyhítésére, a hálózati mérnökök különböző biztonsági beállításokkal védekezhetnek ezek ellen. Ilyenek lehetnek például a speciális hozzáférési listák és a portbiztonság alkalmazása.
- Emlékezzünk vissza, hogy egy Ethernet hálózat logikai topológiája egy többes hozzáférésű sín, amelyen az eszközök osztoznak a közeghez történő hozzáférésen. Ez a logikai topológia határozza meg, hogy a hálózaton lévő állomások hogyan látják és dolgozzák fel a küldött és fogadott kereteket. Ugyanakkor a legtöbb mai Ethernet hálózat csillag vagy kiterjesztett csillag fizikai topológiát használ. Ez azt jelenti, hogy a legtöbb Ethernet hálózaton a végberendezések jellemzően pont-pont alapon csatlakoznak egy 2. rétegbeli LAN-kapcsolóhoz.
- Egy 2. rétegbeli (Layer 2) LAN-kapcsoló a kapcsolási és szűrési műveleteit kizárólag az OSI adatkapcsolati rétegbeli MAC-címek alapján végzi. A kapcsoló teljesen átlátszó - más néven transzparens - a hálózati protokollok és a felhasználói alkalmazások számára. Egy Layer 2 kapcsoló egy MAC-címtáblát épít fel, amelyet a továbbítási döntéseihez használ. A Layer 2 kapcsolók a forgalomirányítókra támaszkodnak az egymástól független IP-alhálózatok közötti adattovábbításhoz.
- A kapcsolók a MAC-címeket használják ahhoz, hogy mindig a megfelelő porton kerüljenek továbbításra a keretek a célállomás felé. A kapcsoló szerkezete az integrált áramkörökből, valamint a hozzá társuló gépi programból áll, amelyek lehetővé teszik, hogy az adatútvonalakat a kapcsolón keresztül szabályozni lehessen. Ahhoz, hogy egy kapcsoló megtudja, hogy melyik portot használja egy egyedi címzésű keret továbbításához, először meg kell tanulnia, mely állomások vannak az egyes portokon.
- Egy kapcsoló a MAC-címtáblája segítségével határozza meg, hogyan kell kezelnie a beérkező adatkereteket. A kapcsoló úgy építi fel a MAC-címtábláját, hogy rögzíti a portjaihoz kapcsolódó állomások MAC-címeit. Miután a kapcsoló egyszer már egy adott porton lévő állomás MAC-címét rögzítette a címtáblájában, egy későbbi átvitel során már tudni fogja, hogy az adott állomásnak szánt forgalmat a hozzá társított porton keresztül kell továbbítania.
- Amikor a kapcsoló egy bejövő adatkeretet kap, és a cél MAC-címe nem szerepel a táblázatban, a kapcsoló a keretet az összes portján keresztül kiküldi, kivéve azt a portot, amelyen a keret beérkezett. Amikor a címzett csomópont visszaválaszol, a kapcsoló rögzíti a keret forráscímét a MAC-címtáblájába. A több összekötött kapcsolót tartalmazó hálózatokban a MAC-címtáblák több MAC-címet is rögzíthetnek a kapcsolókhoz csatlakozó portokhoz, ami

azt tükrözi, hogy azon a porton keresztül több állomás is elérhető. A két kapcsolót összekötő portokhoz általában több MAC-címet rögzítenek a címtáblában.

- Hogy lássuk, hogyan is működik ez, tekintsük meg az egyes lépéseket az 1-6. ábrákon!
- A következők írják le a folyamatot:
- **1. lépés:** A kapcsoló kap egy szórásos keretet a PC1-től az 1-es porton.
- **2. lépés:** A kapcsoló beírja a címtáblába a forrás MAC-címet és a portot, amelyen keresztül megkapta a keretet.
- **3. lépés:** Mivel a cél cím szórásos, a kapcsoló elárasztja a kerettel az összes portot, kivéve azt, amelyen megkapta a keretet.
- **4. lépés:** A cél eszköz egy egyedi címzésű kerettel válaszol, melynek címzettje a PC1.
- **5. lépés:** A kapcsoló beírja a címtáblájába a PC2 forrás MAC-címét és annak a portnak a számát, amelyen át megkapta a keretet. A keret célcíme és a hozzá kapcsolódó port már megtalálhatók a MAC-címtáblában.
- **6. lépés:** A kapcsoló most már elárasztás nélkül képes továbbítani a kereteket a forrás és a cél között, mert már megvannak a kapcsolóportokat beazonosító címtála bejegyzések.
- **Megjegyzés**: A MAC-címtáblát gyakran nevezik tartalom szerint címezhető memória (Content Addressable Memory, CAM) táblázatnak is. Bár a CAM-tábla kifejezés meglehetősen gyakori, ebben a kurzusban MAC-címtáblaként hivatkozunk rá.

Bár a kapcsolók transzparensek a hálózati protokollok és a felhasználói alkalmazások számára, különböző olyan módokban képesek működni, amiknek pozitív és negatív hatásai is vannak, amikor Ethernet kereteket továbbítanak a hálózaton. A kapcsoló minden egyes portjának az egyik alapvető beállítása a duplexitás. A kapcsoló egy portját úgy kell beállítani, hogy az megfeleljen a közegtípus duplexitási beállításainak. Az Ethernet hálózatokon történő kommunikációra kétféle duplexitási beállítást használunk: fél-duplex és teljes duplex.

Fél-duplex

A fél-duplex kommunikáció egyirányú adatfolyamokon alapszik, ahol az adatok küldését és fogadását nem ugyanabban az időben végzik. Ez hasonló ahhoz, ahogyan a walkie-talkie vagy kétirányú rádiók működnek, ahol egy időben csak egy ember beszélhet. Ha valaki beszélne, miközben már valaki más is beszél, akkor ütközés következik be. Ennek eredményeként a fél-duplex kommunikáció a CSMA/CD módszert hívja segítségül a lehetséges ütközések csökkentésére és felismerésére. A fél-duplex kommunikáció teljesítménybeli problémákkal küzd az állandó várakozás miatt, mivel az adatok egy időben csak egy irányban áramolhatnak. A fél-duplex kapcsolatokat tipikusan a régebbi hardvereken találjuk meg, mint például a hub-okon. A hub-okhoz csatlakozó állomások egymással osztozva férnek hozzá a közeghez, ezért hogy képesek legyenek felismerni az ütközéseket, fél-duplex módban kell működniük. Az állomásoknak akkor is fél-duplex módban kell működniük, ha a hálózati kártyájuk nem támogatja a teljes duplex működési módot. Ebben az esetben a kapcsoló portja is alapértelmezés szerint fél-duplex módban van. Ezen korlátozások miatt a legtöbb modern hardveren a teljes duplex kommunikáció váltotta fel a fél-duplexet.

Teljes duplex

A teljes duplex (full-duplex) kommunikációnál az adatáramlás kétirányú, így az adatok ugyanabban az időben küldhetők és fogadhatók is. A kétirányúság azáltal javítja a teljesítményt, hogy az átvitelek között csökkenti a várakozási időt. A legtöbb ma forgalomban lévő Ethernet, FastEthernet és Gigabit Ethernet hálózati csatoló (NIC) teljes duplex képességgel rendelkezik. Full-duplex módban az ütközést érzékelő áramkör le van tiltva. A két csatlakozó végpont keretei nem tudnak ütközni, mert az állomások két külön áramkört használnak a hálózati kábelen. Minden full-duplex kapcsolat csak egy portot használ. A full-duplex kapcsolatok olyan kapcsolót igényelnek, amely támogatja a full-duplex módot, vagy olyan közvetlen kapcsolatot két állomás között, ahol mindkét fél támogatja a full-duplex módot. Azokat az állomásokat, amelyek közvetlenül kapcsolódnak egy dedikált kapcsolóportra és a hálózati kártyájuk is támogatja a teljes duplex módot, olyan portra kell csatlakoztatni, ami full-duplex módra van beállítva.

Az ábrán a modern hálózati berendezéseken rendelkezésre álló két duplexitási beállítás látható.

Egy Cisco Catalyst kapcsoló három duplex beállítást támogat:

- A full opció beállítja a full-duplex módot.
- A half opció beállítja a fél-duplex üzemmódot.
- Az auto opció beállítja a duplex mód automatikus egyeztetését. Ha engedélyezett az automatikus egyeztetés, a két port kommunikációja dönti el a legjobb üzemmódot.

A FastEthernet és 10/100/1000 portokon az auto az alapértelmezett. A 100BASE-FX portokon a full az alapértelmezés. A 10/100/1000 portok működhetnek fél- vagy teljes duplex módban is, ha 10 vagy 100 Mb/s-ra vannak állítva, de amikor 1000 Mb/s-ra, akkor csak teljes duplex módban működhetnek.

Amellett, hogy a megfelelő duplex beállítással rendelkezünk, az is szükséges, hogy minden porthoz a megfelelő típusú kábelt használjuk. Bizonyos eszközök összekapcsolásához (például kapcsoló-kapcsoló, kapcsoló-forgalomirányító, kapcsoló-állomás és forgalomirányító-állomás között) adott típusú kábel használata szükséges (kereszt- vagy egyeneskötésű). Ugyanakkor a legtöbb Cisco kapcsoló ma már támogatja az`mdix auto` interfész konfigurációs CLI-parancsot az automatikus közegfüggő interfész (Media Dependent Interface crossover, auto-MDIX) funkció engedélyezéséhez.

Amikor az Auto-MDIX funkciót bekapcsoljuk, a kapcsoló érzékeli a réz alapú Ethernet csatlakozáshoz szükséges kábeltípust és megfelelően bekonfigurálja az interfészeket. Ezért függetlenül a kapcsolat másik végén lévő készülék típusától, keresztkötésű és egyeneskötésű kábelt is használhatunk a kapcsoló 10/100/100 réz alapú portjaihoz.

Az automatikus MDIX-funkció alapértelmezés szerint engedélyezett a Cisco IOS 12.2(18)SE vagy újabb verziót futtató kapcsolókon. A Cisco IOS 12.1(14)EA1 és 12.2(18)SE kiadások között az automatikus MDIX-funkció alapértelmezés szerint tiltott.

A múltban a kapcsolók az alábbi továbbítási módszerek valamelyikét használták az adatok hálózati portok közötti kapcsolásához:

- tárol-és-továbbít kapcsolás
- közvetlen kapcsolás

Az 1. ábra a két módszer közötti különbségeket emeli ki.

A tárol-és-továbbít módszernél a kapcsoló, miután megkapja a keretet, pufferekben tárolja az adatokat addig, amíg a teljes keret meg nem érkezik. A tárolás során a kapcsoló elemzi a keret információit a rendeltetési hely megállapításához. Ebben a folyamatban a kapcsoló egy hibaellenőrzést is végrehajt az Ethernet keret CRC (Cyclic Redundancy Check) utótagját felhasználva.

A CRC egy matematikai képletet használ a keretben lévő bitek száma (1-esek) alapján annak meghatározására, hogy a fogadott keretben van-e hiba. Miután a keret sértetlensége megerősítést nyert, továbbítja azt a megfelelő portra a rendeltetési hely felé. Ha a kapcsoló hibát észlel a keretben, akkor eldobja azt. A hibás keretek eldobása csökkenti a sértetlen keretek számára rendelkezésre álló sávszélességet. A konvergált hálózatokban tárol-és-továbbít kapcsolásra van szükség a szolgáltatásminőség (Quality of Service, QoS) biztosítására, ahol a forgalom prioritásának meghatározásához szükséges a keretek osztályozása. Az IP-alapú hangátvitel (Voice over IP, VoIP) számára például elsőbbséget kell biztosítani a web-böngészési forgalommal szemben.

Játsszuk le az animációt a 2. ábrán a tárol-és-továbbít folyamat bemutatásához. A tárol-és-továbbít az egyetlen továbbítási módszer a jelenlegi Cisco Catalyst kapcsolómodelleken.

A közvetlen kapcsolás esetén amint megérkezik az adat, a kapcsoló máris cselekszik, még ha az átvitel nem is teljes. A kapcsoló csak annyit tárol el a keretből, hogy ki tudja olvasni a cél MAC-címet

annak meghatározásához, hogy melyik porton kell továbbítania az adatokat. A cél MAC-címe a keret első 6 bájtjában található, az előtagot követően. A kapcsoló megnézi a cél MAC-címet a kapcsolási táblájában, meghatározza a kimenő interfészt és továbbítja a keretet a rendeltetési helyére a kijelölt porton keresztül. A kapcsoló nem végez semmilyen hibaellenőrzést a kereten. Mivel a kapcsolónak nem kell megvárnia a keret teljes pufferelését, és mivel nem végez hibaellenőrzést, a közvetlen kapcsolás gyorsabb, mint a tárol-és-továbbít kapcsolás. Mivel azonban a kapcsoló nem végez hibaellenőrzést, a hibás kereteket is továbbítja a hálózaton keresztül. A hibás keretek a továbbításuk során sávszélességet használnak el. A cél NIC végül eldobja ezeket.

Játsszuk le az animációt a közvetlen kapcsolási folyamat bemutatásához!

A közvetlen kapcsolásnak két változata van:

- **Gyorskapcsolás**: A gyorskapcsolás esetén a legkisebb a késleltetés. A gyorskapcsolás a célcím kiolvasása után azonnal továbbítja a csomagot. Mivel a gyorskapcsolás a teljes csomag beérkezése előtt elkezdődik, lehet, hogy a csomagokat hibásan továbbítjuk. Ez ritkán történik meg, és a fogadó hálózati kártya a beérkező hibás kereteket egyébként is figyelmen kívül hagyja. Gyorstovábbító módban a késleltetést az első beérkezett bittől az első elküldött bitig számítjuk. A gyorskapcsolás a tipikus módszer közvetlen kapcsolás esetén.

- **Töredékmentes kapcsolás**: A töredékmentes kapcsoláskor a kapcsoló még a keret továbbítása előtt eltárolja az első 64 bájtot. A töredékmentes kapcsolás tulajdonképpen egy kompromisszum a tárol-és-továbbít kapcsolás, valamint a gyorskapcsolás között. Az ok, amiért a töredékmentes kapcsolás a keret első 64 bájtját tárolja el, hogy a legtöbb hálózati hiba és ütközés az első 64 bájt továbbítása alatt történik. A töredékmentes kapcsolás megpróbálja kibővíteni a gyorskapcsolást egy kisebb hibaellenőrzés elvégzésével a keret első 64 bájtján annak érdekében, hogy megbizonyosodjon, nem történt-e ütközés a keret továbbítása előtt. A töredékmentes kapcsolás tehát kompromisszum a nagy késleltetésű, de magas integritást nyújtó tárol-és-továbbít módszer, valamint az alacsony késleltetésű és csökkentett integritású gyorskapcsolás között.

Az ábra a közvetlen kapcsolásra mutat példát.

Bizonyos kapcsolók portonkénti közvetlen kapcsolásra vannak beállítva mindaddig, amíg a hibák száma el nem ér egy a felhasználó által definiált hibaküszöb szintet, ami után automatikusan átvált tárol-és-továbbít módra. Amikor a hibaarány a küszöbérték alá csökken, a port automatikusan visszavált közvetlen kapcsolásra.

Mint említettük, egy kapcsoló megvizsgálja a kereteket vagy esetleg csak néhányat közülük, mielőtt azokat továbbítaná a célállomáshoz. Egy Ethernet kapcsoló különböző pufferelési technikákat alkalmazhat a keretek továbbítás előtti tárolására. A pufferelést abban az esetben is lehet alkalmazni, ha a célport egy esetleges torlódás miatt foglalt, és ilyenkor a kapcsoló a keretet eltárolja egészen addig, amíg azt továbbítani nem lehet.

Amint az ábrán látható, két módszer létezik memória pufferelésre: a port-alapú és az osztott.

Port-alapú memória pufferelés

A port-alapú memória pufferelésnél a kereteket várósorokban tároljuk, amelyek az adott bejövő és kimenő portokhoz kapcsolódnak. Egy keret csak akkor kerül át a kimeneti portra, ha a sorban előtte álló keretek már mind sikeresen továbbítódtak. Előfordulhat, hogy egyetlen keret késlelteti a memóriában lévő összes többi keret átvitelét egy foglalt kimeneti port miatt. Ez a késleltetés akkor is fellép, ha a többi keretet szabad portokra lehetne továbbítani.

Osztott memória pufferelés

Az osztott memória pufferelés minden keretet egy közös memória pufferbe helyez el, amelyen az összes port osztozik. Egy port számára szükséges memóriamennyiség kiosztása dinamikusan

történik. A keretek a pufferben a célportokhoz dinamikusan kapcsolódnak. Ez teszi lehetővé, hogy anélkül lehessen fogadni a csomagokat az egyik porton majd továbbítani egy másikon, hogy egy másik sorba kellene áthelyezni őket.Ez teszi lehetővé azt, hogy a csomagokat anélkül lehessen az egyik porton fogadni majd egy másikon továbbítani, hogy egy másik sorba át kellene helyezni őket.

A kapcsoló egy nyilvántartást vezet a keret-port kapcsolatokról, amely megmutatja, hogy egy csomagot hol kell továbbítani. A keret sikeres továbbítása után törlődik ez a megfeleltetés. A pufferben tárolható keretek számát csak a teljes memóriapuffer mérete korlátozza, és az nem korlátozza le egyetlen portpuffer mérete. Így nagyobb keretek is továbbíthatók, és kevesebb keretet kell eldobni. Ez különösen fontos aszimmetrikus kapcsolás esetén. Az aszimmetrikus kapcsolás különböző portokon különböző adatátviteli sebességet biztosít. Ez lehetővé teszi nagyobb sávszélesség biztosítását bizonyos portoknak, mint például a szerverhez csatlakozó port.

Amikor kiválasztunk egy kapcsolót, fontos, hogy megértsük a kapcsoló legfontosabb jellemzőit és lehetőségeit. Ez azt jelenti, hogy olyan funkciókról kell dönteni, mint például hogy szükség van-e a Power over Ethernet-re (PoE), és hogy mi a kívánt továbbítási sebesség.

Amint az 1. ábrán látható, a PoE lehetővé teszi, hogy egy kapcsoló a meglévő Ethernet-kábelezésen keresztül biztosítson tápfeszültséget eszközöknek, mint például az IP-telefonok és egyes vezeték nélküli hozzáférési pontok. Ez nagyobb rugalmasságot tesz lehetővé a telepítéskor.

A továbbítási sebesség határozza meg egy kapcsoló feldolgozási képességeit, rangsorolva, hogy mennyi adatot képes feldolgozni másodpercenként. A kapcsolók termékcsaládját a továbbítási ráták alapján sorolják be. A belépő szintű kapcsolók alacsonyabb továbbítási rátákkal rendelkeznek, mint a vállalati szintű kapcsolók. Egyéb szempontok közé tartozik, hogy az eszközök egymáshoz köthetők-e (stackable), hogy mekkora egy kapcsoló magassága (ezt számszerűen rack-egységben, vagy unit-ban fejezik ki), valamint hogy mekkora a kapcsoló portsűrűsége (mennyi a kapcsolón a rendelkezésre álló portok száma). Egy eszköz portsűrűsége attól függően változhat, hogy az eszköz rögzített konfigurációjú vagy moduláris készülék.

Ezeket a tulajdonságokat néha a kapcsoló formai tényezőinek (form factor) nevezik.

Rögzített konfigurációjú kapcsolók

A rögzített konfigurációjú kapcsolók - ahogy a nevük is utal rá - fix kiépítettséggel rendelkeznek. Ez azt jelenti, hogy nem lehet funkciókat és beállításokat hozzáadni a kapcsolóhoz azon túl, mint amivel eredetileg rendelkezett. A konkrét megvásárolt modell meghatározza a rendelkezésre álló funkciókat és lehetőségeket. Ha például vásárolunk egy 24 portos fix kiépítettségű gigabites kapcsolót, akkor szükség esetén azt nem lehet további portokkal bővíteni. Vannak jellemző kiépítettségű modellek (például 24 vagy 48 portos kapcsoló), amelyek aszerint változnak, hogy hány és milyen típusú portjaik van.

Moduláris kapcsolók

A moduláris kapcsolók kiépítettségükben nagyobb rugalmasságot biztosítanak. A moduláris kapcsolók általában különböző méretű házzal érkeznek, amely lehetővé teszi különböző számú moduláris vonali kártya telepítését. A vonali kártyák tartalmazzák tulajdonképpen a portokat. A vonali kártya úgy illeszkedik a kapcsoló házába, mint ahogy a bővítőkártyák illeszkednek a PC-be. Minél nagyobb a ház, annál több modult támogat. Mint az a 2. ábrán látható, számos különböző méretű készülékház közül lehet választani. Ha vásároltunk egy moduláris kapcsolót egy 24 portos vonali kártyával, akkor ahhoz könnyen hozzá lehet adni még egy további 24 portos vonali kártyát, így az összes port száma már 48 lesz.

A 2. ábra példákat mutat a fix, moduláris és egymáshoz köthető konfigurációjú kapcsolókra.

A Cisco kapcsolók termékcsaládjait világszerte széles körben alkalmazzák, nagy részben azért, mert rugalmasságot biztosítanak a bővítési lehetőségek tekintetében. A Cisco IOS más operációs

rendszerekhez viszonyítva nemcsak a leggazdagabb funkciókkal rendelkezik, de testre szabottan alkalmazható minden Cisco hálózati eszközre, különösképpen a kapcsolókra.

A rendelkezésre álló lehetőségek illusztrálására, amelyek a szó szoros értelmében túl terjedelmesek ahhoz, hogy itt felsoroljuk, most csak a Catalyst 3560 kapcsolókra összpontosítunk. A Catalyst 3560 kapcsolók SFP-portokkal (Switch Form-Factor Pluggable) rendelkeznek, amelyek több SFP adóvevő modult támogatnak. Itt egy lista azon SFP-modulokról, amelyeket egy vagy több típusú 3560 kapcsoló támogat:

FastEthernet SFP-modul –

- 100BASE-FX (multimódusú optikai, MMF) 2 kilométer távolságra
- 100BASE-LX10 (egymódusú optikai, SMF) 2 kilométer távolságra
- 100BASE-BX10 (SMF) 10 km-re
- 100BASE-EX (SMF) 40 km-re
- 100BASE-ZX (SMF) 80 km-re

Gigabit Ethernet SFP-modulok –

- 1000BASE-SX 50/62.5 um (MMF), maximum 550/220 m
- 1000BASE-LX/LH (SMF / MMF) 10 km-ig
- 1000BASE-ZX (SMF) 70 km-ig
- 1000BASE-BX10-D és 1000BASE-BX10-U (SMF) 10 km-ig
- 1000BASE-T (réz vezetékes adóvevő)

10 Gigabit Ethernet SFP-modulok –

- 10G-SR (MMF) 400 m-ig
- 10G-SR-X (MMF), maximum 400 m-ig (támogatja a szélsőséges hőmérsékleti viszonyokat)
- 10G-LRM (MMF) 220 m-ig
- FET-10G (MMF), 100 m-ig (a Nexus belső szerkezeti uplink-ekhez)
- 10G-LR (SMF) 10 km-ig
- 10G-LR-X (SMF) 10 km-ig (támogatja a szélsőséges hőmérsékleti viszonyokat)
- 10G-ER (SMF) 40 km-ig
- 10G-ZR (SMF) 80 km-ig
- Twinax (réz vezetékes adóvevő), 10 m-ig
- Aktív optika 10 m-ig (rack-en belüli és azok közti csatlakozáshoz)

A 40 Gigabit Ethernet és a 100 Gigabit Ethernet modulokat a csúcsszintű Cisco eszközök támogatják, mint például a Catalyst 6500, a CRS és az ASR 9000 forgalomirányítók, valamint a Nexus 7000-es sorozatú kapcsolók.

A kapcsolók különböző formai tényezőinek meghatározása mellett arra is szükség lehet, hogy válasszunk egy Layer 2 (második rétegbeli) és egy Layer 3 (harmadik rétegbeli vagy többrétegű) kapcsoló között.

Emlékezzünk vissza, hogy egy Layer 2 LAN-kapcsolón a továbbítás és szűrés alapja kizárólag az OSI adatkapcsolati rétegbeli (Layer 2) MAC-cím, és független IP-alhálózatok közötti adattovábbításhoz forgalomirányító használatára szorul (lásd 1. ábra).

Amint a 2. ábrán látható, egy Layer 3 kapcsoló, mint például a Catalyst 3560, hasonlóan működik, mint egy Layer 2 kapcsoló (például a Catalyst 2960), de ahelyett, hogy kizárólag a 2. rétegbeli MAC-cím információkat használná a továbbítási döntésekhez, a Layer 3 kapcsoló az IP-címet is használja.Amint a 2. ábrán látható, egy Layer 3 kapcsoló (például a Catalyst 3560) is hasonlóan működik, mint egy Layer 2 kapcsoló (például a Catalyst 2960), de a 2. rétegbeli MAC-cím információk kizárólagos használata helyett a továbbítási döntésekhez egy Layer 3 kapcsoló az IP-címet is használja. Ahelyett, hogy csak azt tanulná meg, mely MAC-címek társulnak az egyes portjaihoz, egy Layer 3 kapcsoló azt is megtanulja, mely IP-címek társulnak az interfészeihez. Ez lehetővé teszi a Layer 3 kapcsoló számára, hogy a forgalmat a hálózaton keresztül az IP-cím alapján is irányítsa.

A Layer 3 kapcsolók forgalomirányítási funkciókat is képesek teljesíteni, így nincs szükség külön forgalomirányítóra a LAN-on. Mivel a többrétegű kapcsolók speciális kapcsolási hardverrel rendelkeznek, általában olyan sebességgel képesek irányítani az adatokat, mint amilyen gyorsan kapcsolni tudják azokat.

A Cisco Layer 3 kapcsolói a Cisco Express Forwarding (CEF) kapcsolást használják. Ez a továbbítási módszer meglehetősen bonyolult, de szerencsére, mint minden jó technológia, nagy része a "színfalak mögött" játszódik le. Általában nagyon kevés CEF konfigurálás szükséges egy Cisco eszközön.

Alapvetően, a CEF elválasztja egymástól a megszokott szoros kölcsönös függőséget a Layer 2 és Layer 3 döntéshozatalban. Amitől az IP-csomagok továbbítása lassú egy hálózati eszközön, az az, hogy állandóan oda-vissza kell hivatkozni a 2. és 3. rétegbeli szerkezetek között. Így amennyiben ezeket az adatszerkezeteket függetleníteni lehet, a továbbítás felgyorsulhat.

A CEF működésének két fő összetevője:

- Továbbítási információs adatbázis (Forwarding Information Base, FIB)
- Szomszédsági táblák

A FIB fogalmilag hasonló az irányítótáblához. A forgalomirányító az irányítótáblát használja, hogy meghatározza a legjobb útvonalat egy célhálózat felé a cél IP-cím hálózati része alapján. A CEF-nél a korábban cache-ben tárolt útvonal adatokat több adatstruktúrában tároljuk a CEF-kapcsoláshoz. Az adatstruktúrák optimalizált keresést nyújtanak a hatékony csomagtovábbításhoz. Egy hálózati készülék a FIB keresési táblát használja, hogy a célra vonatkozó döntéseket hozzon anélkül, hogy hozzáférne az irányítótábla caché-hez.

A FIB frissül, ha változás történik a hálózatban, és a változás után tartalmazni fogja az összes adott időpontban ismert útvonalat.

A szomszédsági táblázatok 2. rétegbeli következő ugrás címeket tartanak karban minden egyes FIB-bejegyzéshez.

Az elérhetőségi adatok (a FIB-táblázatban) és a továbbítási információk (a szomszédsági táblázatban) elválasztása számos előnnyel jár:

- A szomszédsági tábla külön is kialakítható a FIB-táblától, amely lehetővé teszi mindkettő felépítését anélkül, hogy a csomagok folyamat-kapcsolva lennének.

- A MAC-fejléc átírását arra használják, hogy továbbítsuk a cache bejegyzésekben nem tárolt csomagot, így a változások egy MAC-fejléc újraíró szövegben nem igénylik a cache bejegyzések érvénytelenítését.

A CEF a Layer 3 kapcsolást végző Cisco eszközök többségén alapértelmezés szerint engedélyezve van.

A Cisco hálózati eszközök több különböző típusú Layer 3 interfészt támogatnak. A Layer 3 interfész az IP-címek alapján végzi az IP-csomagok továbbítását a végső rendeltetési hely felé.

A Layer 3 interfészek fő típusai:

- **Switch Virtual Interface (SVI)** - Logikai interfész egy kapcsolón, amit virtuális helyi hálózathoz (VLAN) társítunk.

- **Irányított (routed) port** - Fizikai port egy Layer 3 kapcsolón, ami forgalomirányító portként konfigurálható.

- **Layer 3 EtherChannel** - Logikai interfész egy Cisco eszközön, amit kötegelt irányított porthoz társítunk.

Amint azt korábban bemutattuk, az alapértelmezett VLAN-ban (VLAN1) az SVI-t engedélyezni kell ahhoz, hogy IP-alapú kapcsolat lehessen egy állomás és a kapcsoló között, amely lehetővé teszi a kapcsoló távoli adminisztrálását. Az SVI-ket ahhoz is be kell állítani, hogy forgalomirányítás lehessen a VLAN-ok között. Ahogyan említettük, az SVI-k logikai interfészek az egyes VLAN-okoz beállítva; a forgalomirányításhoz két vagy több VLAN között minden VLAN-nak külön engedélyezett SVI-kre van szüksége.

A routed portok lehetővé teszik a (Layer 3) kapcsolóknak, hogy forgalomirányítóként viselkedjenek. Minden port egy ilyen kapcsolón úgy konfigurálható, mint egy független IP-hálózaton lévő interfész.

A Layer 3 EtherChannel-eket arra használják, hogy összefogjanak Layer 3 Ethernet kapcsolatokat a Cisco eszközökön annak érdekében, hogy növeljék a sávszélességet, jellemzően a főkapcsolati (uplink) kapcsolatokon.

Megjegyzés: Az SVI-k és L3 EtherChannel-ek mellett más logikai interfészek is vannak a Cisco eszközökön, például visszacsatoló (loopback) interfészek és alagút (tunnel) interfészek.

Egy kapcsolóportot be lehet úgy állítani, hogy Layer 3 irányított port legyen, és úgy viselkedjen, mint egy hagyományos forgalomirányító interfész. Pontosabban, egy irányított portra jellemző:

- nem társítjuk egyetlen adott VLAN-hoz sem,

- be lehet állítani rajta egy Layer 3 irányító protokollt,

- kizárólag Layer 3 interfész, és nem támogatja a Layer 2 protokollokat.

Az interfészt Layer 3 módba lehet állítani a`no switchport` interfész konfigurációs paranccsal. Ezután IP-címet adhatunk a porthoz. Ennyi az egész!

A következő fejezetben többet fogunk megtudni a forgalomirányításról.

A hálózati rendszergazda felváltja a jelenlegi forgalomirányítót és kapcsolót egy új Layer 3 kapcsolóval. Hálózati szakemberként a mi feladatunk, hogy beállítsuk és üzembe helyezzük a kapcsolót. Munkaidő után fogunk dolgozni, hogy minimális fennakadást okozzunk az üzletmenetben.

Packet Tracer - Configure Layer 3 Switches Instructions

Packet Tracer - Configure Layer 3 Switches - PKA

Keresd MAC az információt!

Megjegyzés: Ezt a feladatot külön-külön, kis csoportokban vagy a teljes iskolai tanulói környezetben is végre lehet hajtani.

Nézzük meg az alábbi linken található videót:

http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet

A tárgyalt témakörök között nem csak az szerepel, hogy honnan indultunk az Ethernet fejlesztésében, hanem hogy hová juthatunk el a technológiával (egy futurisztikus megközelítésben).

A videó megtekintése, és tartalmának az 5. fejezettel történő összehasonlítása után menjünk ki a webre és keressünk információt az Ethernetről! Használjunk konstruktivista megközelítést:

- Hogyan nézett ki az Ethernet, amikor először kifejlesztették?
- Hogyan maradt ugyanaz az Ethernet az elmúlt 25 év során, és milyen változások történnek annak érdekében, hogy hasznos/alkalmazható legyen a mai adatátviteli módszerekhez?

Gyűjtsünk össze három képet régi, jelenlegi és jövőbeli Ethernet fizikai átviteli közegekről és eszközökről (a hangsúly a kapcsolókon legyen) - osszuk meg ezeket a képeket az osztállyal, és vitassuk meg:

- Hogyan változott az Ethernet fizikai közege és a közvetítő eszközök?
- Hogy maradtak ugyanazok az Ethernet fizikai közegei és közvetítő eszközei?
- Hogyan változik az Ethernet a jövőben?

Csoportos feladat - utasítások a Keresd MAC az információt! feladathoz

Az Ethernet ma a legelterjedtebb LAN technológia. Az Ethernet hálózati technológiák egész családját alkotja, amelyeket az IEEE 802.2 és 802.3 szabványok határoznak meg. Az Ethernet szabványok meghatározzák a második rétegbeli protokollokat és az első rétegbeli technológiákat is. A második rétegbeli protokollok, mint minden 802 IEEE-szabvány, az adatkapcsolati rétegben két különálló alrétegre támaszkodnak, a Logical Link Control (LLC-) és a MAC-alrétegekre.

Az adatkapcsolati réteg szintjén a keretszerkezet gyakorlatilag az Ethernet összes változatánál azonos. Az Ethernet keretszerkezet fejléceket és utótagokat ad a 3. rétegbeli PDU köré, hogy beágyazza az elküldendő üzenetet.

Két Ethernet keretezési típus létezik: az IEEE 802.3 Ethernet szabvány és a DIX Ethernet szabvány, amelyet manapság Ethernet II néven ismerünk. A legjelentősebb különbség a két szabvány között, hogy a a 802.3 szabványban hozzáadtak egy keretkezdő mezőt (Start Frame Delimiter, SFD) és a "típus" mező "hossz" mezőre változott. Az Ethernet II a TCP/IP-hálózatokon használt Ethernet

keretformátuma. Mint az IEEE 802.2/3 szabványok megvalósítása, az Ethernet keret MAC-címzést és hibajavítást biztosít.

Az Ethernet által biztosított 2. rétegbeli címzés támogatja az egyedi, csoportos és szórásos (unicast, multicast és broadcast) kommunikációt. Az Ethernet címfeloldási protokollja (ARP) meghatározza a célállomások MAC-címét és leképezi azokat az ismert hálózati rétegbeli címekre.

Egy IP-hálózaton minden csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Az állomásnak a saját MAC- és IP-címét kell használnia a forrás mezőkben, valamint meg kell adnia a célállomás MAC- és IP-címét is. Míg a cél IP-címét egy magasabb OSI-réteg fogja biztosítani, a cél MAC-címét a küldő csomópontnak kell megtalálni egy adott Ethernet kapcsolaton. Ez az ARP feladata.

Az ARP bizonyos típusú Ethernet szórásos és egyedi címzésű üzenetekre támaszkodik, az úgynevezett ARP-kérésekre és az ARP-válaszokra. Az ARP-protokoll megkeresi az IPv4-címekhez tartozó MAC-címeket és létrehoz egy táblázatot az összerendelésekről.

A legtöbb Ethernet hálózaton a végberendezések általában, pont-pont alapon, egy Layer 2 LAN-kapcsolóhoz csatlakoznak. A 2. rétegbeli (Layer 2) LAN-kapcsoló a kapcsolási és szűrési műveleteit kizárólag az OSI adatkapcsolati rétegbeli MAC-címek alapján végzi. A Layer 2 kapcsoló is felépít egy MAC-címtáblát, amelyet a továbbítási döntéseihez használ. A Layer 2 kapcsolók a forgalomirányítókra támaszkodnak az egymástól független IP-alhálózatok közötti adattovábbításhoz.

A Layer 3 kapcsolók forgalomirányítási funkciókat is képesek teljesíteni, így nincs szükség külön forgalomirányítóra a LAN-on. Mivel a többrétegű kapcsolók speciális kapcsolási hardverrel rendelkeznek, általában olyan sebességgel képesek irányítani az adatokat, mint amilyen gyorsan kapcsolni tudják azokat.

A különböző végberendezéseken lévő hálózati alkalmazások és szolgáltatások képesek egymással kommunikálni. De miként tud ez az adatkommunikáció hatékonyan végbemenni?

Az OSI-modell hálózati rétegének protokolljai határozzák meg a címzést és azokat a folyamatokat, amelyek lehetővé teszik a szállítási réteg adatainak becsomagolását és továbbítását. A hálózati rétegben történő beágyazás segítségével az adatok minimális többletterheléssel jutnak el egy hálózaton belüli vagy egy másik hálózaton található célhoz.

A fejezet a hálózati réteg szerepét tárgyalja. Megvizsgálja, hogyan történik a hálózatok felbontása állomások csoportjaira az adatfolyam kezelése érdekében. Foglalkozik a hálózatok közötti kommunikáció kezelésével is, melyet röviden forgalomirányításnak nevezünk.

Járt utat járatlanért ..., vagy mégsem?

Elhatároztuk, hogy az elkövetkező hétvégén meglátogatjuk az otthon betegen fekvő osztálytársunkat. Ismerjük az utca nevét, ahol lakik, de még soha nem jártunk abban a városban. Úgy döntünk, hogy nem nézzük meg térképen a címet, hanem a városban lakóktól kérünk segítséget az eligazodáshoz. A város lakói nagyon segítőkészek, de igen különösen viselkednek. Ahelyett, hogy elmondanák a teljes útvonalat a célig, mindenki a következőt mondja: "Menj ezen az úton végig, és ha kereszteződéshez érsz, kérdezz meg ismét valakit".

Kicsit meglepődve ugyan, de követjük az utasításokat és kereszteződéstől kereszteződésig haladva elérjük a barátunk házát.

Válaszoljunk az alábbi kérdésekre:

- Jelentősen más lett volna-e a helyzet, ha a teljes utat vagy annak nagy részét egyszerre elmagyarázzák, és nem csak a következő kereszteződésig küldenek?

- Mennyivel lett volna könnyebb, ha a konkrét házszámot is ismerjük? Mi történt volna, ha egy megkérdezett járókelő nem ismeri a keresett utcát, vagy esetleg rossz irányba küld?

- Tételezzük fel, hogy hazafelé ismét a járókelők segítségével utazunk. Biztos, hogy ugyanazon az útvonalon megyünk, mint amin odafelé? Válaszunkat indokoljuk meg!

- Szükséges a megkérdezetteknek mindig elmondanunk, hogy honnan jöttünk?

Csoportos feladat - The road less traveled...or is it?

A hálózati réteg, vagy más néven az OSI 3. rétege olyan szolgáltatásokat biztosít, amelyek lehetővé teszik a végberendezések közötti kommunikációt a hálózaton. A végponttól-végpontig történő szállításhoz a hálózati réteg négy alapvető folyamatot használ:

- **Végberendezések címzése** Mint ahogy egy telefon egyedi telefonszámmal rendelkezik, úgy egy végberendezés is csak egyedi IP-címmel azonosítható a hálózaton. Egy adott IP-címmel rendelkező végberendezést állomásnak nevezünk.

- **Beágyazás -** A hálózati réteg a szállítási rétegtől fogad egy protokoll adategységet (PDU - protocol data unit). A beágyazás során a hálózati réteg ezt a PDU-t IP-fejléc információkkal egészíti ki, mint például a forrás- és a célállomás IP-címe. A fejléc információkkal kiegészített PDU-t nevezzük csomagnak.

- **Forgalomirányítás -** A hálózati réteg szolgáltatásainak segítségével a csomagok egy másik hálózaton lévő célállomáshoz irányíthatók. A csomag másik hálózatba történő továbbításához forgalomirányítóra van szükség. A forgalomirányító feladata a célállomás felé vezető út kiválasztása és a csomagok cél felé továbbítása. Ezt a folyamatot nevezzük forgalomirányításnak. A csomag számos közvetítő eszközön haladhat keresztül, mielőtt elérkezik a célállomáshoz. A célállomáshoz vezető útvonal egyes szakaszait ugrásnak nevezzük.

- **Kicsomagolás -** Amikor a csomag megérkezik a célállomás hálózati rétegéhez, az állomás ellenőrzi a csomag IP-fejlécét. Ha a fejlécben lévő cél IP-cím megegyezik a saját IP-címével, akkor eltávolítja a csomagról az IP-fejlécet. Az alacsonyabb rétegek fejlécének eltávolítását nevezzük kicsomagolásnak. A hálózati rétegben történő kicsomagolást követően a keletkezett 4. rétegbeli PDU a szállítási réteg megfelelő szolgáltatásához kerül.

Míg a szállítási réteg (OSI 4. réteg) az állomásokon futó folyamatok közötti adattovábbítást kezeli, addig a hálózati réteg a csomagok felépítését és feldolgozását definiálja, ami az adatok állomásról állomásra történő továbbításához szükséges. A csomagokban szállított adatoktól független működésnek köszönhetően, a hálózati réteg képes az állomások közötti különböző típusú kommunikáció továbbítására.

Az ábrán látható animáció két állomás közötti adatátvitelt mutat be.

Számos hálózati rétegbeli protokoll létezik, de leginkább az alábbi, ábrán is látható kettőt használják a gyakorlatban:

- IPv4 (Internet Protocol Version 4)

- IPv6 (Internet Protocol Version 6)

További, ritkábban használt hálózati rétegbeli protokollok:

- IPX (Novell Internetwork Packet Exchange)

- AppleTalk

- CLNS/DECNet (Connectionless Network Service)

Ezekről a régebbi protokollokról csak érintőlegesen lesz szó.

Az IP- a TCP/IP-protokollkészlet hálózati rétegbeli szolgáltatása.

Az IP-t kis többletterhelésű protokollnak tervezték. Ennek megfelelően csak azokat a funkciókat tartalmazza, amelyek feltétlenül szükségesek ahhoz, hogy egy csomag összekapcsolt hálózatokon keresztül a forrástól a célig eljusson. A protokollnak nem feladata a csomagok nyomon követése és felügyelete. Ezeket a funkciókat szükség esetén más rétegbeli protokollok biztosítják.

Az IP legfőbb jellemzői:

- **Összeköttetés-mentes -** Az adatküldést megelőzően nem épül fel kapcsolat a küldő és a fogadó állomás között.

- **Legjobb szándékú (nem megbízható) -** A csomagok kézbesítése nem garantált.

- **Közegfüggetlen -** Működése független az adattovábbításhoz használt átviteli közegtől.
  - A hálózati réteg feladata a csomagok állomások közötti továbbítása a hálózatra nézve a lehető legkisebb többletterheléssel. A hálózati réteg nem foglalkozik, vagy tudatában sincs a csomagban zajló kommunikáció típusával. Az IP összeköttetés-mentes, ami azt jelenti, hogy az adatküldést megelőzően a végpontok között nem épül ki kapcsolat. Az összeköttetés-mentes kommunikáció hasonló ahhoz, mint amikor egy levelet küldünk anélkül, hogy arról a címzettet előre értesítenénk.
  - Ahogy az ábrán is látható, a posta a borítékon lévő információkat használja a levél kézbesítéséhez. A borítékon lévő cím nem tartalmaz információt a címzett létezéséről, mint ahogy arról sem, hogy a levél megérkezik-e, vagy hogy a címzett el tudja-e olvasni azt. Valójában a posta nem ismeri a kézbesítendő levél vagy csomag tartalmát, így a felmerülő hibák javítására sem képes.
  - Az összeköttetés-mentes kommunikáció is hasonló elven működik.
  - Mivel az IP összeköttetés-mentes, így a csomagtovábbítás előtt nincs szükség a végpontok közötti kapcsolat kiépítéséhez fontos vezérlési információk cseréjére sem. Szintén nincs szükség a PDU-fejlécében olyan további információkra, amelyek a felépített kapcsolat kezelését segítenék. Mindezek nagy mértékben csökkentik az IP által okozott többletterhelését. Mivel nem épül fel kapcsolat a végpontok között, így a küldőnek nincs információja a megcímzett eszköz létezéséről vagy működéséről, illetve arról sem, hogy a csomagja megérkezik-e vagy hogy a címzett fel tudja-e azt dolgozni. A 2. ábrán egy összeköttetés-mentes kommunikáció látható.
  - Az IP-t gyakran nevezik nem megbízható vagy legjobb szándékú kézbesítést (best-effort delivery) biztosító protokollnak. Ez nem azt jelenti, hogy az IP időnként megfelelően működik, máskor pedig nem, vagy hogy az IP gyenge adatkommunikációs protokoll. A nem megbízható mindössze annyit jelent, hogy az IP nem képes felügyelni és helyreállítani a nem kézbesített vagy hibás csomagokat. Ez amiatt van, hogy az IP-csomag a feladási helyen kívül semmilyen információt nem tartalmaz, ami alapján a küldőt értesíteni lehetne a sikeres kézbesítésről. Az IP fejléce nem tartalmaz szinkronizációs adatokat a csomagok kézbesítési sorrendjének nyomon követéséhez, nem nyugtázza a csomagok megérkezését, és nem tartalmaz hibajavítási adatot sem, amellyel ellenőrizhető a csomagok hibamentes kézbesítése. Előfordulhat, hogy a csomagok hibásan, rossz sorrendben vagy egyáltalán nem érkeznek meg a célállomáshoz. Az IP-fejlécben található információk alapján, egyik hiba esetében sincs mód a csomag újraküldésére.
  - Rossz sorrendben érkező vagy elveszett csomagok esetén a magasabb rétegbeli szolgáltatások, mint például a TCP feladata a probléma kezelése. Mindezek eredményeképpen az IP nagyon hatékonyan képes működni. Ha az IP-fejléc a megbízhatósághoz szükséges többlet információkat is tartalmazná, akkor az összeköttetést vagy megbízhatóságot nem igénylő kommunikációk esetében sávszélesség felhasználási és késleltetési problémák merülnének fel. A TCP/IP-protokollkészletben a szállítási rétegbeli protokoll lehet TCP vagy UDP attól függően, hogy az adott kommunikáció esetében mennyire

fontos a megbízhatóság. Annak köszönhetően, hogy az IP a megbízhatósági feladatokat a szállítási rétegre bízza, egy rugalmas és különböző típusú kommunikációk esetén is használható protokoll.

- Az ábrán egy IP-kommunikáció látható. Az összeköttetés-alapú protokollok esetében, mint például a TCP, a kapcsolat létrehozásához szükség van a vezérlő információk cseréjére, és a felépült kapcsolat kezelése is további mezőket igényel a PDU-fejlécben.
- A hálózati réteg nem foglalkozik a csomagok továbbításához használt átviteli közeg jellemzőivel sem. Az IP teljesen függetlenül működik az átviteli közegtől, ahol a protokollkészlet alacsonyabb rétegeiben zajló adatátvitel történik. Ahogy az ábrán is látható, az IP-csomagok továbbíthatók elektromos úton kábelen keresztül, optikai jelként üvegszálat használva, vagy vezeték nélküli környezetben rádió jelként.
- Az IP-csomagok fogadása és felkészítése az átviteli közegen történő továbbításra az OSI adatkapcsolati rétegének feladata. Mindez azt jelenti, hogy az IP-csomagok továbbítása nincs korlátozva egyetlen átviteli közegre sem.
- A hálózati réteg azonban figyelembe veszi az átviteli közeg egy fő jellemzőjét, a közegen átvihető maximális PDU méretét. Ezt nevezzük maximális átviteli egységnek (Maximum Transmission Unit, MTU). A csomagok maximális méretének meghatározása az adatkapcsolati és a hálózati réteg közötti kommunikáció során történik. Az adatkapcsolati réteg megadja a hálózati réteg számára az MTU értékét, a hálózati réteg pedig meghatározza a maximális csomagméretet.
- Bizonyos esetekben egy közvetítő eszköznek, általában egy forgalomirányítónak át kell méreteznie a csomagokat ahhoz, hogy egy kisebb MTU-értékkel rendelkező közegen továbbítani tudja őket. Ezt a folyamatot nevezik tördelésnek vagy feldarabolásnak (fragmentation).
- Az IP egy fejléc hozzáadásával csomagolja be a szállítási réteg szegmenseit. Ez a fejléc teszi lehetővé a csomagok célállomáshoz továbbítását, és mindaddig szükség van rá, amíg a csomag a forrás hálózati rétegét elhagyva megérkezik a célállomás hálózati rétegéhez.
- Az 1. ábrán a szállítási rétegbeli, a 2. ábrán pedig a hálózati rétegbeli PDU létrehozásának folyamata látható.
- Az adatok rétegről rétegre történő becsomagolásának folyamata teszi lehetővé, hogy az egyes rétegek szolgáltatásai más rétegektől függetlenül fejlődjenek és bővüljenek. Mindez azt jelenti, hogy a szállítási réteg szegmensei becsomagolhatók IPv4, IPv6 vagy akár egy új, a jövőben kifejlesztett protokoll segítségével is.
- A forgalomirányítók képesek a különböző hálózati rétegbeli protokollok egyidejű működtetésére, összekötve a hálózat különböző típusú állomásait. A közvetítő eszközök a forgalomirányítás során csak a csomag fejlécének tartalmát veszik figyelembe. A csomag adat része - a szállítási rétegbeli PDU - a hálózati rétegbeli feldolgozás során minden esetben változatlan marad.

Az IPv4-et 1983-ban fejlesztették ki az Internet elődjének tekinthető ARPANET (Advenced Tesarch Projects Agency Network) hálózat működéséhez. Az internet elsősorban az IPv4 protokollra épül, ami a legszélesebb körben használt hálózati rétegbeli protokoll.

Az IPv4 csomag két részből áll:

- **IP-fejléc -** A csomag jellemzőit határozza meg.

- **Adattartalom -** A 4. rétegbeli szegmens információkat és a tényleges adatokat tartalmazza.

Ahogy az ábrán is látható, az IPv4-csomag fejléce olyan mezőkből áll, melyek a csomagról tartalmaznak fontos információkat. Ezek a mezők bináris számok, melyeket a 3. réteg dolgoz fel. Az egyes mezők bináris értékei az IP-csomag különböző tulajdonságait határozzák meg.

A legfontosabb IPv4-fejléc mezők:

- **Verzió -** Az IP-csomag verzióját határozza meg 4 biten. IPv4 esetén ez az érték mindig 0100.

- **Differenciált szolgáltatások (Differentiated Services, DS) -** A korábban ToS-nak (Type of Service, szolgáltatás típus) nevezett DS mező egy 8 bites érték, ami a csomagok prioritását adja meg. Az első 6 bit a DCSP (Differentiated Services Code Point, differenciált szolgáltatások kódpont) érték, amit a szolgáltatási minőség (Quality of Service, QOS) biztosításához használnak. Az utolsó 2 bit pedig az ECN (explicit congestion notification, explicit torlódásjelzés) érték, ami hálózati torlódás esetén a csomagvesztések elkerülésére szolgál.

- **Élettartam (Time-To-Live, TTL) -** A csomag élettartamát korlátozó 8 bites bináris szám. Értéke másodpercben van megadva, de rendszerint ugrásszámmal hivatkoznak rá. A csomag küldője beállít egy kezdeti TTL-értéket, amit a csomagot feldolgozó minden forgalomirányító vagy 3. rétegbeli továbbító eszköz eggyel csökkent. Ha a TTL értéke eléri a nullát, a forgalomirányító eldobja a csomagot és egy ICMP Time Exceeded üzenetet küld a forrás állomásnak.
  A **traceroute** parancs ezt a mezőt használja a forrás- és a célállomás közötti forgalomirányítók azonosításához.

- **Protokoll -** 8 bites érték, ami meghatározza a csomagban szállított adattartalom típusát. Ennek segítségével továbbítja a hálózati réteg az adatot a megfelelő felsőbb rétegbeli protokoll számára. A leggyakoribb értékei: 0x01 (ICMP), 0x06 (TCP), 0x11 (UDP).

- **Forrás IP-cím -** A csomag forrásállomásának címét megadó 32 bites bináris szám.

- **Cél IP-cím -** A csomag célállomásának címét megadó 32 bites bináris szám.

A két leggyakrabban hivatkozott mező a forrás és cél IP-cím. Ezek határozzák meg, hogy a csomag honnan indult és hová tart. Általában ezek a címek nem változnak a forrástól a célállomásig vezető út során.

Az eddig nem említett mezők a csomag azonosításához és érvényesítéséhez, vagy a szétdarabolt csomag újbóli összeállításához szükségesek.

Az azonosításra és érvényesítésre használt mezők:

- **Internet fejléc hossz (Internet Header Length, IHL) -** Egy 4 bites érték, ami megadja a csomag fejlécében található 32 bites szavak számát. Az IHL értéke változhat az Options (opciók) és a Padding (kitöltés) mezők miatt. A mező legkisebb értéke 5 (5x32=160bit=20 bájt), legnagyobb értéke pedig 15 (15x32=480bit=60 bájt) lehet.

- **Teljes hossz (Total Lenght) -** Az időnként Packet Lenght-nek (csomaghossz) is nevezett 16 bites mező a teljes csomag (fejléc és adat) bájtokban mért hosszát adja meg. A minimális csomagméret 20 bájt (20 bájt fejléc + 0 bájt adat), a maximális pedig 65535 bájt.

- **Fejléc ellenőrző összeg (Header Checksum) -** 16 bites mező az IP-csomag sértetlenségének ellenőrzésére. Egy csomag megérkezésekor a fejléc ellenőrző összegét újraszámolják és összehasonlítják a mező értékével. Ha a kér érték nem egyezik, akkor a csomag eldobásra kerül.

Amikor egy forgalomirányító a csomagokat egy kisebb MTU-értékkel rendelkező átviteli közegre továbbítja, akkor a csomagokat kisebb egységekre kell feldarabolnia. Ezt a folyamatot nevezzük feldarabolásnak (fragmentation). A feldarabolt adategységek nyomon követéséhez az IPv4-csomag a következő mezőket használja:

- **Azonosítás (Identification) -** 16 bites szám, ami egyértelműen azonosítja az IP-csomag egy darabját.

- **Jelzők (Flags) -** A csomag feldarabolásának módját meghatározó 3 bit. A Fragment Offset (csomagdarab eltolás) és az Identification mezőkkel együtt elősegíti a csomagdarabokból az eredeti csomag visszaállítását.

- **Csomagdarab eltolás (Fragment Offset) -** 13 bites érték, ami a csomag darabokból történő összeállításánál megadja a csomagok sorrendjét.

Megjegyzés: Az Opciók és a Kitöltés mezők használata igen ritka, így a tananyag ezeket nem tárgyalja.

A Wireshark minden hálózati szakember számára igen hasznos hálózatmegfigyelő eszköz, valamint jól alkalmazható adatelemzésre és hibakeresésre a CCNA kurzusok laborgyakorlataiban. Segítségével példákat láthatunk az IP-fejléc mezőinek értékeire.

A három ábrán Wiresharkkal elfogott IP-csomagok láthatók.

- Az 1. ábra az elkapott csomagfolyamból a 2.csomag tartalmát mutatja. A csomagban a forráscím 192.168.1.109, a célcím pedig 192.168.1.1. A középső ablakban találhatók az IPv4-fejléc információk, mint például a fejléc hossza, a csomag teljes hossza és a beállított jelzők.

- A 2. ábrán a 8. csomag tartalma látható, ami egy HTTP csomag. Figyeljük meg a TCP rész utáni információt.

- Végezetül a 3. ábrán a 16. csomag figyelhető meg. Ez a csomag egy ping kérés, amit a 192.168.1.109 IP-című állomás küldött a 192.168.1.1 állomásnak. Figyeljük meg, hogy mivel egy ICMP (Internet Control Message Protocol) csomagról van szó, így nincs TCP vagy UDP információ.

Az elmúlt évek során az IPv4 protokollt a megjelenő újabb és újabb kihívásoknak köszönhetően számtalanszor frissítették. Mindezek ellenére az IPv4-nek maradt három alapvető problémája:

- **Elfogytak az IPv4-címek -** Az IPv4 korlátozott számú egyedi nyilvános címmel rendelkezik. Bár megközelítőleg 4 billió IPv4-cím létezik, az IP-alapú eszközök számának növekedése, a permanens kapcsolatok és a fejletlen országok várható igényei nagyban megnövelték a szükséges címek számát.

- **Megnövekedett irányítótábla méret az interneten -** Az irányítótáblát a forgalomirányítók a legjobb útvonal kiválasztásához használják. Az internetre csatlakozó szerverek számának növekedésével növekszik a hálózati útvonalak száma is. Ezen IPv4-útvonalak kezelése rengeteg memóriát és processzorteljesítményt igényel az internet forgalomirányítóin.

- **Végponttól végpontig tartó kapcsolatok hiánya -** A hálózati címfordítás (Network Address Translation, NAT) az IPv4-hálózatokban gyakorta alkalmazott technológia. A NAT lehetővé teszi, hogy több eszköz egyetlen nyilvános IP-címet használjon. Mivel a nyilvános IP-címek a megosztottak, a belső állomások IP-címei rejtve maradnak. Ez problémát okozhat a végponti kapcsolatokat igénylő technológiák esetén .

Az 1990-es évek elején az IETF (Internet Engineering Task Force) egyre nagyobb aggodalommal figyelte az IPv4 kapcsán felmerülő problémákat, és elkezdte keresni a megoldást. Ez vezetett aztán az IPv6 kifejlesztéséhez. Az IPv6 megoldja az IPv4 problémáit, és egy olyan robusztus megoldás biztosít, amely tulajdonságainak köszönhetően alkalmasabb a jelenlegi és a várható hálózati igények kielégítésére.

Az IPv6 kibővített tulajdonságai:

- **Megnövekedett címtér -** Az IPv6-címek, a 32 bites IPv4-címekkel ellentétben, 128 bites hierarchikus felépítésűek, melynek köszönhetően nagyságrendekkel több IP-címet biztosítanak.

- **Továbbfejlesztett csomagkezelés -** Az IPv6-fejléc kevesebb mezőt tartalmaz. Ez növeli a csomagkezelés hatékonyságát a forgalomirányítókon és lehetővé teszi a skálázhatóságot biztosító kiterjesztések és opciók használatát.

- **Nincs szükség címfordításra -** A nagy számú nyilvános IPv6-címnek köszönhetően nincs szükség címfordításra (NAT). A legnagyobb vállalatok telephelyeitől a kis háztartásokig mindenhova kioszthtató IPv6-os hálózati cím. Ez megoldja a NAT használatával keletkezett problémákat azoknál az alkalmazásoknál, amelyek végponti kapcsolatokat igényelnek.

- **Integrált biztonság -** Az IPv6 támogatja a hitelesítést és a titkosítást. IPv4 esetén ezekhez további kiegészítések szükségesek.

A 32 bites IPv4-címtér megközelítőleg 4.294.967.296 egyedi címet tartalmaz. Mivel az IPv4 a címeket osztályokba sorolja, valamint címeket tart fent a csoportos címzésre, a tesztelésre és egyéb felhasználás érdekében, így a teljes címtérből csak 3,7 milliárd a ténylegesen kioszthtató.

Ahogy az ábrán is látható, az IPv6 340.282.366.920.938.463.463.374.607.431.768.211.456 vagyis kb. 340 szextillió címet biztosít, ami megközelítőleg annyi, mint a Föld összes homokszeme.

Az IPv6 kapcsán az egyik legfőbb tervezési változás az IPv4-hez képest az egyszerűsített fejléc.

Az IPv4-fejléc 20 oktett (maximum 60 byte az Opciók mezővel együtt), ami az Opciók és a Kitöltés mezőket leszámítva 12 alapvető mezőből áll.

Az IPv6-fejléc ezzel szemben 40 oktett (a forrás- és célcím mérete miatt ilyen nagy), ami 3 IPv4 alap és 5 további mezőt, azaz összesen 8 mezőt tartalmaz.

Az 1. ábrán lévő IPv4-fejléc felépítéséből látható, hogy az IPv6-hoz képest néhány IPv4 mező változatlan maradt, vannak amiket nem használnak és némelyikük neve és elhelyezkedése megváltozott.

Ezen felül új, korábban nem használt mezők is kerültek az IPv6-fejlécbe. Az IPv6 egyszerűsített fejléce a 2. ábrán látható.

Az IPv6 egyszerűbb fejléce számos előnnyel jár:

- Hatékonyabb forgalomirányítás és skálázhatóbb átviteli sebesség.

- Nincs ellenőrzőösszeg vizsgálat.

- Egyszerűbb és lényegesen hatékonyabb kiterjesztett fejléc kezelés (az IPv4 Opciók mezőjéhez viszonyítva).

- A folyamatonkénti feldolgozáshoz használt Flow Label (folyamcímke) mezőnek köszönhetően a különböző forgalmak azonosításához nincs szükség a szállított csomag megnyitására.

Az IPv6-csomag fejléc mezői:

- **Verzió -** Ez a 4 bit adja meg az IP-csomag verzióját, ami IPv6 esetén 0110.

- **Forgalom osztály (Traffic Class) -** Ez a 8 bit megegyezik az IPv4-fejléc differenciált szolgáltatások (Differentiated Services, DS) mezőjével. Szintén egy 6 bites DSCP (Differentiated Services Code Point) érték osztályozza a csomagokat és egy 2 bites ECN (Explicit Congedtion Notification) mező szolgál torlódásvezérlésre.

- **Folyamcimke (Flow Label) -** A 20 bites mező lehetővé teszi a valós idejű alkalmazások speciális kezelését. Segítségével értesíthetők a forgalomirányítók és a kapcsolók, hogy egy csomagfolyam esetén ugyanazt az útvonalat használják, így a csomagokat nem kell összerendezni.

- **Adatmező hossza (Payload Length) -** Ez a 16 bites mező megegyezik az IPv4-fejléc Total Length (Teljes hossz) mezőjével. A teljes csomag (töredék) méretét adja meg a fejrésszel és az opcionális kiegészítésekkel együtt.

- **Következő fejléc (Next Header) -** A 8 bites mező megegyezik az IPv4 Protokoll mezőjével. Ez adja meg a csomagban lévő adattartalom típusát, lehetővé téve ezzel a hálózati réteg számára, hogy az adatokat a megfelelő felsőbb rétegbeli protokollnak továbbítsa. A mezőt akkor is használják, ha az IPv6-csomagban opcionális kiterjesztések vannak.

- **Ugrás korlát (Hop Limit) -** Ez a 8 bit felel meg az IPv4 csomag TTL-mezőjének. Értéke mindig eggyel csökken, amikor egy forgalomirányító továbbítja a csomagot. Amikor a számláló eléri a 0 értéket, a csomagot az adott forgalomirányító eldobja és egy ICMPv6 üzenettel értesíti a küldő állomást arról, hogy a csomag nem érkezett meg a célhoz.

- **Forrás IP-cím (Source Address) -** Ez a 128 bites mező adja meg a küldő állomás IPv6 címét.

- **Cél IP-cím (Destination Address) -** Ez a 128 bites mező adja meg a fogadó állomás IPv6-címét.

Az IPv6-csomag kiterjesztett fejléct (Extension Header, EH) is tartalmazhat, ami további hálózati rétegbeli információkat biztosít. Ez a kiterjesztett fejléc opcionális és az IPv6-fejléc és az adat között helyezkedhet el. Használják például csomagok feldarabolása vagy biztonság és mobilitás támogatás esetén is.

Az ábrán lévő Wireshark kimenet alapján egyértelműen látható, hogy az IPv6-fejléc kevesebb mezőből áll, mint az IPv4. Ennek köszönhető, hogy az IPv6-fejlécet a forgalomirányító könnyebben és gyorsabban tudja feldolgozni.

Az IPv6-címek lényegesen különböznek az IPv4-címektől. Mivel az IPv6-címek 128 bitesek, így az egyszerűbb megjelenítés miatt hexadecimális formában használjuk őket. A címekben a 16 bites hexadecimális blokkokat kettőspontok választják el.

Az 1. ábrán egy Wireshark-kal elfogott csomagfolyam 46.csomagjának tartalma látható. A csomag egy IPv6-állomás és egy IPv6-szerver közötti TCP-kapcsolat 3 utas kézfogásának első üzenete. Figyeljük meg a kiterjesztett IPv6-fejléc értékeit. Vegyük észre, hogy bár ez egy TCP-csomag, mégsem tartalmaz semmi további információt a TCP részről.

A 2. ábrán ugyanennek a csomagfolyamnak a 49. csomagja látható. A csomag egy szervernek küldött HTTP (HyperText Transfer Protocol) GET-csomag. Vegyük észre, hogy bár ez egy HTTP-csomag, mégsem tartalmaz információkat a TCP résznél.

Végezetül a 3. ábrán látható 1. sorszámú csomag egy ICMPv6 Neighbor Solicitation (szomszédság egyeztető) üzenet. Vegyük észre, hogy a csomag nem tartalmaz TCP vagy UDP információt.

A hálózati réteg másik feladata a csomagok állomások közötti irányítása. Egy állomás által küldött csomag címzettje lehet:

- **Saját maga** - Ilyenkor egy speciális IP-címet, a 127.0.0.1-et használja, amit visszahurkolási (loopback) interfésznek nevezünk. Ez a loopback cím automatikusan hozzárendelődik minden állomáshoz, amint a TCP/IP futni kezd. Az, hogy egy állomás a hálózat segítségével saját magának is tud üzenetet küldeni tesztelési célból fontos. A 127.0.0.0/8 hálózat bármely IP-címe a helyi állomásra utal.

- **Helyi állomás** - A küldő állomással egy hálózatban lévő másik állomás. A két állomás hálózati címe azonos.

- **Távoli állomás** - Távoli hálózat egy állomása. A két állomás hálózati címe különböző.

Az, hogy egy csomagot helyi vagy távoli állomásnak címeztek, a forrásállomás IP-cím és hálózati maszk kombinációjának a célállomás IP-címével történő összevetése dönti el.

Otthoni vagy vállalati hálózatokban számos vezetékes és vezeték nélküli eszköz kapcsolódik össze közvetítő hálózati eszköz, mint például LAN-kapcsoló és/vagy vezeték nélküli hozzáférési pont (Wireless Access Point, WAP) segítségével. Ez a közvetítő eszköz biztosítja a kapcsolatot a helyi hálózat állomásai között. A helyi állomások további eszközök használata nélkül képesek egymást elérni és információt megosztani. Amikor egy állomás ugyanazon a hálózaton lévő állomásnak küld üzenetet, a csomag egyszerűen az állomás interfészéről a közvetítő eszközön keresztül a célállomáshoz kerül továbbításra.

Természetesen a legtöbb esetben szeretnénk, hogy eszközeink helyi hálózaton kívüli állomásokhoz, vállalatokhoz és az internethez is csatlakozni tudjanak. A helyi hálózaton kívüli berendezéseket távoli állomásoknak nevezzük. Amikor egy állomás egy távoli célállomásnak küld üzenetet, akkor forgalomirányítóra és irányításra van szükség. A forgalomirányítási folyamat feladata a legjobb útvonal megtalálása a célállomáshoz. A helyi hálózati szegmenshez csatlakozó forgalomirányítót nevezzük **alapértelmezett átjárónak**.

Az alapértelmezett átjáró irányítja a forgalmat a helyi hálózatról a távoli hálózatok eszközeihez. Otthoni vagy kisvállalati környezetben gyakori, hogy az alapértelmezett átjárót az internethez való csatlakozáshoz használják.

Amikor egy állomás csomagot küld egy másik IP-hálózaton lévő eszköznek, akkor azt egy közvetítő eszközön keresztül az alapértelmezett átjárónak kell küldenie. Ez azért van így, mert a helyi állomás nem tárol irányítási információkat a helyi hálózaton kívül lévő, távoli célállomásokról, az alapértelmezett átjáró viszont rendelkezik a szükséges információkkal. Az alapértelmezett átjáró, ami leggyakrabban egy forgalomirányító, egy iránytótáblát tart fenn. Az irányítótábla egy RAM-ban tárolt adatfájl, amiben a közvetlenül csatlakozó és az eszköz által megtanult távoli hálózatok adatai szerepelnek. A forgalomirányító a táblában lévő információkat használja fel a célhoz vezető legjobb útvonal megtalálásához.

Hogyan tudja eldönteni az állomás, hogy a csomagokat az alapértelmezett átjáróhoz kell-e továbbítania? Az állomásnak saját, helyi irányítótáblát kell fenntartania ahhoz, hogy a hálózati rétegbeli csomagokat a megfelelő célhálózatba tudja küldeni. Ez a helyi tábla jellemzően az alábbiakat tartalmazza:

- **Közvetlen kapcsolat** - Út a visszahurkolási interfészhez (127.0.0.1).

- **Helyi hálózati útvonal** - Az állomáshoz csatlakozó hálózat automatikusan bekerülnek az állomás irányítótáblájába.

- **Helyi alapértelmezett útvonal** - Az alapértelmezett útvonal segítségével érhető el minden távoli hálózat. Az alapértelmezett útvonal akkor jön létre, amikor egy alapértelmezett átjáró beállításra kerül az állomáson. Az alapértelmezett átjáró címe a helyi hálózathoz csatlakozó forgalomirányító hálózati interfészének IP-címe. Ez a cím beállítható manuálisan vagy megtanulható dinamikusan.

Fontos megjegyezni, hogy az alapértelmezett útvonal, és így az alapértelmezett átjáró is csak abban az esetben szükséges, ha egy állomásnak távoli hálózatba kell csomagot küldeni. Nincs rá szükség és így beállítani sem kell, ha csak a helyi hálózat állomásainak történik üzenetküldés.

Vegyünk példaként egy hálózati nyomtatót/szkennert. Ha a hálózati nyomtató IP-címmel és alhálózati maszkkal rendelkezik, akkor a helyi állomások képesek rajta dokumentumokat nyomtatni, és a nyomtató is továbbítani tudja a beszkennelt dokumentumokat bármelyik helyi állomásnak. Amíg a nyomtatót csak helyben használják, addig nincs szükség alapértelmezett átjáróra. Azáltal, hogy egy nyomtatón nincs beállítva alapértelmezett átjáró, az internet hozzáférés sem lehetséges, ami adott esetben biztonsági szempontból jó döntés lehet. Ha nincs internet hozzáférés, akkor nincs biztonsági fenyegetettség sem. Amikor egy eszköz, mint például egy nyomtató, automatikusan képes frissíteni

önmagát az interneten keresztül, akkor rendszerint könnyebb és biztonságosabb ezt egy védett helyi állomásról megtennie.

Egy Windows állomáson a **`route print`** vagy a**`netstat -r`** parancs jeleníti meg az állomás irányítótábláját. A két parancs kimenete megegyezik. Bár a kimenet első ránézésre bonyolultnak tűnhet, mégis könnyen megérthető.

A **`netstat -r`** vagy a vele megegyező **`route print`**parancs az aktuális TCP/IP hálózati kapcsolatokra vonatkozóan az alábbi három információt tartalmazza:

- **Interfész lista -** Megadja az állomás minden hálózati interfészének (Ethernet, Wi-Fi és Bluetooth) MAC címét és hozzárendelt interfész azonosítóját.
- **IPv4-irányítótábla -** Tartalmazza az állomás által ismert összes IPv4-útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.
- **IPv6-irányítótábla -** Tartalmazza az állomás által ismert összes IPv6 útvonalat, közöttük a közvetlen kapcsolatokat, a helyi hálózatot és az alapértelmezett útvonalat.

Megjegyzés: A parancs kimenete az állomás beállításaitól és interfészeinek típusától függően változhat.

Az ábrán az IPv4 irányítótábla látható. Figyeljük meg, hogy a tábla a következő őt oszlopból áll:

- **Célhálózat -** Elérhető hálózatok listája.
- **Hálózati maszk -** Az állomás a hálózati maszk segítségével határozza meg az IP-cím hálózati és állomás részét.
- **Átjáró -** A helyi állomás által egy távoli célhálózat eléréséhez használt cím. Ha egy célhálózat közvetlenül kapcsolódó, akkor ebben az oszlopban a "Kapcsolaton belüli" (on-link) érték látható.
- **Interfész -** Annak a fizikai interfésznek a címe, amin a csomagot a távoli célhálózat eléréséhez szükséges átjáró felé ki kell küldeni.
- **Mérték -** Az útvonal költsége, amit a célhoz vezető legjobb útvonal meghatározásához használnak.

Az irányítótábla bejegyzések könnyebb megértése érdekében a célhálózatokat az ábrán látható kiemeléseknek megfelelően az alábbi öt csoportra oszthatjuk:

0.0.0.0

Helyi alapértelmezett útvonal. Ide továbbít az állomás minden olyan csomagot, melynek célhálózata nem egyezik meg az irányítótábla egyetlen más címével sem. A példában minden nem egyező célhálózat esetén az állomás a csomagokat a 192.168.10.10 interfészén küldi ki a 192.168.10.1 (R1) IP-című átjáróhoz. Jegyezzük meg, hogy a csomagban lévő célcím nem változik, az állomás ebből tudja, hogy a csomagot további feldolgozás érdekében az átjárónak kell továbbítania.

127.0.0.0 - 127.255.255.255

A loopback címek mind közvetlenül csatlakozónak tekinthetők és a helyi állomásnak biztosítanak szolgáltatásokat.

192.168.10.0 - 192.168.10.255

Ezek az állomáshoz vagy a helyi hálózathoz tartozó címek. Minden csomag, melynek célcíme ebbe a tartományba esik, a 192.168.10.10 interfészen kerül továbbításra.

- **192.168.10.0 -** A helyi hálózat címe, ami az összes számítógépet jelöli a 192.168.10.0 hálózaton.

- **192.168.10.10 -** Az állomás címe.

- **192.168.10.255 -** A hálózat szórási címe, amivel a helyi hálózat összes állomásának lehet üzenetet küldeni.

224.0.0.0

Speciális célra fenntartott D osztályú csoportcímek, melyek a loopback (127.0.0.1) vagy az állomás (192.168.10.10) interfészen használhatók.

255.255.255.255

A két utolsó limitált szórási címek, melyek a loopback (127.0.0.1) vagy az állomás (192.168.10.10) interfészen használhatók. Ezek segítségével kereshető meg például egy DHCP-szerver még mielőtt az állomás helyi IP-címmel rendelkezne.

Ha PC1 csomagot szeretne küldeni a 192.168.10.20 állomásnak, akkor:

1. Megnézi az IPv4-irányítótábláját.

2. Mivel egyezést talál a cél IP-cím és a 192.168.10.0 célhálózat bejegyzés között, így megállapítja, hogy a célállomás ugyanazon a hálózaton van, mint saját maga (On-link).

3. PC1 elküldi a csomagot a célhoz a helyi interfészén keresztül. (192.168.10.10)

Az 1. ábrán kiemelve látható az egyező útvonal.

Ha PC1 a távoli 10.10.10.10. című állomásnak szeretne üzenetet küldeni, akkor:

1. Megnézi az IPv4-irányítótábláját.

2. Megállapítja, hogy nincs egyezés a célhálózattal.

3. A helyi alapértelmezett útvonal (0.0.0.0) alapján eldönti, hogy a csomagot a 192.168.10.1 átjáró címre kell küldenie.

4. PC1 a helyi interfészén (192.168.10.10) kiküldi a csomagot az átjárónak. Az átjáró ezután meghatározza a következő ugrást a 10.10.10.10 IP-című célállomás felé.

A 2. ábrán kiemelve látható az egyező útvonal.

Az IPv6-irányítótábla kimenet oszlopfejlécei és formátuma is különböző a hosszabb IPv6-címek miatt.

Az IPv6-iránytótábla a következő négy oszlopból áll:

- **If -** A `netstat -r` parancs kimenetében szereplő interfész azonosítók, mely az állomás hálózati interfészeinek felel meg, ide értve az Ethernet, Wi-Fi és Bluetooth adaptereket.

- **Mérték -** A célhoz vezető útvonal költsége. A kisebb érték jobb útvonalat jelöl.

- **Célhálózat -** Elérhető hálózatok.

- **Átjáró -** A helyi számítógép által használt cím egy távoli célhálózat eléréséhez. A "Kapcsolaton belüli" ("on-link") bejegyzés azt jelöli, hogy az állomás közvetlenül kapcsolódik az adott hálózathoz.

Az ábrán a `netstat -r` parancs kimenet IPv6-irányítótáblájában szereplő alábbi célhálózatok láthatók:

- **::/0 -** IPv6 helyi alapértelmezett útvonal.

- **::1/128 -** Az IPv4-nek megfelelő IPv6 loopback cím, ami a helyi állomás tesztelését teszi lehetővé.

- **2001::/32 -** A globális egyedi címek hálózati előtagja.

- **2001:0:9d38:953c:2c30:3071:e718:a926/128 -** Az állomás globális egyedi IPv6-címe.

- **fe80::/64 -** A helyi érvényű (link local) hálózat címe, ami a helyi hálózaton elérhető összes eszközt jelöli.

- **fe80::2c30:3071:e718:a926/128 -** A számítógép helyi érvényű (link local) IPv6-címe.

- **ff00::/8 -** Speciális célra fenntartott csoportcímek, a D osztályú 224.x.x.x IPv4-címekhez hasonlóan.

Megjegyzés: IPv6 esetén egy interfésznek gyakran két IPv6-címe van: egy helyi érvényű link local cím és egy globális egyedi cím. Megjegyzendő, hogy az IPv6-ban nincsenek üzenetszórási címek. Az IPv6 címekről bővebben a következő fejezetben lesz szó.

Amikor egy állomás csomagot küld egy másik állomásnak, akkor az irányítótáblája segítségével dönti el, hogy hova továbbítsa azt. Ha a célállomás egy távoli hálózaton van, akkor a csomagot egy átjárónak kell küldeni.

Mi történik, amikor egy csomag érkezik egy forgalomirányító interfészére? A forgalomirányító megnézi az irányítótábláját és annak segítségével dönti el, hogy a csomagot merre kell küldenie.

Egy forgalomirányító irányítótáblája az alábbiakról tárol információkat:

- **Közvetlenül csatlakozó útvonalak -** A forgalomirányító aktív interfészein lévő hálózatok. A forgalomirányító akkor jegyez be a táblájába egy közvetlenül csatlakozó útvonalat, ha a megfelelő interfésze aktív és van IP-címe. A forgalomirányító minden interfésze külön hálózathoz tartozik. Az irányítótáblában minden csatlakoztatott és aktív hálózati szegmens információi megtalálhatók.

- **Távoli útvonalak -** Más forgalomirányítókhoz csatlakozó hálózatokra mutató útvonalak. Konfigurálhatók kézzel a helyi forgalomirányítón a hálózati rendszergazda által, vagy dinamikusan a helyi és a távoli forgalomirányítók közötti irányító protokollok segítségével.

Az ábrán az R1 forgalomirányító közvetlenül csatlakozó és távoli hálózatai láthatók.

Egy állomás irányítótáblájában csak a közvetlenül csatlakozó hálózatok szerepelnek, így egy távoli célállomás eléréséhez alapértelmezett átjáróra van szüksége. Egy forgalomirányító irányítótáblája hasonló információkat tartalmaz azzal a különbséggel, hogy távoli hálózatok azonosítására is képes.

A forgalomirányító és az állomás irányítótáblája is tartalmazza a következőket :

- célhálózat
- célhálózathoz tartozó mérték (metrika)
- célhálózat eléréséhez szükséges átjáró

Egy Cisco IOS forgalomirányítón a **`show ip route`**parancs jeleníti meg az irányítótáblát. Ebben további útvonal információk is találhatók arról, hogy milyen módon tanulta meg és mikor frissítette utoljára a forgalomirányító az adott útvonalat, és melyik interfészen keresztül érhető el a kívánt célhálózat.

A forgalomirányító az interfészére érkező csomag fejlécéből olvassa ki a célhálózat címét. Ha a célhálózat szerepel az irányítótábla útvonalai között, akkor a forgalomirányító a táblában szereplő információk alapján továbbítja a csomagot. Ha két vagy több útvonal is vezet ugyanahhoz a célhálózathoz, a mérték alapján dől el, hogy melyik kerül az irányítótáblába.

Az ábrán egy egyszerű hálózatban lévő R1 forgalomirányító irányítótáblája látható. Ellentétben az állomás irányítótáblájával, itt nincsenek oszlopfejlécek, amik a bejegyzésekben szereplő információkat azonosítják. Éppen ezért fontos megtanulni a sorokban szereplő különböző típusú információk jelentését.

Amikor egy forgalomirányító aktív interfészén IP-címet és maszkot konfigurálunk, két irányítótábla bejegyzés kerül automatikusan a táblába. Az ábrán az R1 forgalomirányító 192.168.10.0 közvetlenül csatlakozó hálózatának irányítótábla bejegyzése látható. Ez automatikusan került be az irányítótáblába a GigabitEthernet 0/0 interfész konfigurálását és aktiválását követően. A bejegyzés a következő információkat tartalmazza:

Útvonal forrása

Az útvonal forrását az ábrán az "A" jelöli. Ez azonosítja, hogyan tanulta meg a forgalomirányító az adott útvonalat. Közvetlenül csatlakozó interfészek esetén két lehetséges kód létezik.

- **C -** Közvetlenül csatlakozó hálózatot jelöl. A közvetlenül csatlakozó hálózatok automatikusan létrejönnek, amint az interfészen IP-címet konfigurálunk és aktiváljuk azt.
- **L -** A forgalomirányító interfészére mutató útvonalat jelöl. Ezek az útvonalak is automatikusan kerülnek az irányítótáblába, amikor az interfészen IP-címet konfigurálunk és aktiváljuk azt.

Célhálózat

A célhálózatot az ábrán a "B" jelöli. Ez adja meg a távoli hálózat címét.

Kimenő interfész

A kimenő interfészt az ábrán a "C" jelöli. Ez azonosítja azt az interfészt, amelyen a csomagokat a célhálózat felé továbbítani kell.

Megjegyzés: A forgalomirányító interfészekre mutató irányítótábla bejegyzések (L) a 15-ös IOS-nél korábbi verziók esetén nem jelennek meg az irányítótáblában.

Egy forgalomirányítón jellemzően több konfigurált interfész is van. A forgalomirányító nem csak ezekről, hanem a távoli útvonalakról is tárol információkat. A közvetlenül csatlakozó hálózatokhoz hasonlóan itt is az útvonal forrása azonosítja, hogyan tanulta meg a forgalomirányító az adott útvonalat. Távoli hálózatok esetén használt gyakori kódok:

- **S -** Az útvonalat a rendszergazda kézzel hozta létre egy adott hálózat elérése érdekében. Ezt hívjuk statikus útvonalnak.

- **D -** Az útvonalat a forgalomirányító dinamikusan tanulta meg más forgalomirányítótól az EIGRP (Enhanced Interior Gateway Routing Protocol) segítségével.

- **O -** Az útvonalat a forgalomirányító dinamikusan tanulta meg más forgalomirányítótól az OSPF (Open Shortest Path First) protokoll segítségével.

Megjegyzés: A további kódokat ez a fejezet nem tárgyalja.

Az ábrán az R1 forgalomirányító 10.1.1.0 távoli hálózatra vonatkozó irányítótábla bejegyzése látható. A bejegyzés az alábbi információkat tartalmazza:

- **Útvonal forrása -** Megmutatja, hogyan tanulta meg az adott útvonalat a forgalomirányító.

- **Célhálózat -** Megadja a távoli hálózat címét.

- **Adminisztratív távolság -** Az útvonal forrásának megbízhatóságát adja meg.

- **Mérték -** A távoli hálózat eléréséhez rendelt érték. A kisebb érték jobb útvonalat jelöl.

- **Következő ugrás -** A csomagtovábbítás során a következő forgalomirányító IP-címe.

- **Útvonal időbélyeg -** Az utolsó útvonalfrissítés óta eltelt idő.

- **Kimenő interfész -** Az az interfész, amelyen a csomagokat a célhálózat felé továbbítani kell.
  - A következő ugrás annak az eszköznek a címe, amelyik a csomagot következőben fogja feldolgozni. A hálózat egy állomása esetén az alapértelmezett átjáró (forgalomirányító interfész) címe lesz a következő ugrás minden távoli hálózatba küldendő csomag esetében. A forgalomirányító irányítótáblájában minden távoli hálózathoz vezető útvonalhoz tartozik egy következő ugrás.
  - Amikor egy távoli hálózatba címzett csomag érkezik, akkor a forgalomirányító egyezést keres a célhálózat és az irányítótábla egy útvonala között. Ha talál egyezést, akkor a csomagot a következő ugrás IP-címére küldi a bejegyzésben meghatározott interfészén keresztül.
  - A következő ugrással megadott forgalomirányító jelenti az átjárót a távoli hálózatokhoz.
  - Példaként, ha az ábrán látható hálózatban egy csomag érkezik az R1 forgalomirányítóhoz a 10.1.1.0 vagy a 10.1.2.0 hálózat felé, akkor a forgalomirányító a Serial 0/0/0 interfészén keresztül a 209.165.200.226 következő ugrás címre továbbítja azt.
  - A közvetlenül csatlakozó hálózatok esetében nincs következő ugrás cím, mivel a forgalomirányító a kijelölt interfészén egyenesen az adott hálózaton lévő állomásoknak tudja a csomagokat továbbítani.
  - A csomagokat a forgalomirányító csak akkor tudja továbbítani, ha a célhálózat szerepel az irányítótáblájában. Ha a célhálózat nem szerepel a táblában, a csomagot a forgalomirányító eldobja.
  - Ahogyan egy állomás az alapértelmezett átjárót használja egy ismeretlen célnak küldött csomag esetén, úgy a forgalomirányítón is beállítható egy statikus útvonal, ami végső átjáróként (Gateway of Last Resort) működik. A végső átjáróról bővebben a CCNA Routing and Switching Essentials kurzusában lesz szó.
  - Vegyük azt a példát, hogy a 192.168.10.10 IP-című PC1 állomás csomagot szeretne küldeni a saját hálózatán belül egy másik állomásnak. Ebben az esetben PC1 először ellenőrzi a cél IP-címet az IPv4-irányítótáblájában. Ebből kiderül számára, hogy a célállomás ugyanazon a hálózaton van, mint ő, így a csomagot egyszerűen kiküldi a megfelelő interfészén (On-link).
  - **Megjegyzés**: Az R1 forgalomirányító nem vett részt a csomagtovábbításban. Ha a PC1 állomás nem helyi hálózatába küld csomagot, akkor már szüksége van az R1 forgalomirányítóra és ilyenkor a csomagot a helyi alapértelmezett útvonal (192.168.10.1) felé továbbítja.

- A következő példák azt mutatják be, hogy egy állomás és egy forgalomirányító miként hozza meg csomagtovábbítási döntését saját irányítótáblája alapján:
- 1. példa: A PC1 állomás ellenőrizni szeretné a kapcsolatát a helyi alapértelmezett átjáróval a 192.168.10.1 IP-címen.
- 1. PC1 ellenőrzi a cél IP-címet az IPv4 irányítótáblájában.
- 2. Ebből kiderül számára, hogy a célállomás ugyanazon a hálózaton van, mint ő, így a csomagot egyszerűen kiküldi a megfelelő interfészén (On-link).
- 3. R1 forgalomirányító a Gigabit Ethernet 0/0 (G0/0) interfészén fogadja a csomagot és kiolvassa belőle a cél IP-címet.
- 4. R1 megvizsgálja az irányítótábláját.
- 5. R1 egyezést talál a cél IP-cím és az **L 192.168.10.1/32**irányítótábla bejegyzés között. Ebből tudja, hogy ez az útvonal saját helyi interfészére mutat (lásd 1. ábra).
- 6. R1 megnyitja a csomagot és annak megfelelően válaszol.
- 2. példa: A PC1 állomás csomagot szeretne küldeni a PC2 állomásnak (182.168.11.10)
- 1. PC1 megvizsgálja az IPv4-irányítótábláját és nem talál teljes egyezést.
- 2. PC1 így a csomagot az alapértelmezett útvonal (0.0.0.0) alapján az alapértelmezett átjárónak küldi el (192.168.10.1).
- 3. R1 forgalomirányító a Gigabit Ethernet 0/0 (G0/0) interfészén fogadja a csomagot és kiolvassa belőle a cél IP-címet.
- 4. R1 megvizsgálja az irányítótábláját és egyezést talál a cél IP-cím és a **C 192.168.11.0/24** irányítótábla bejegyzés között (lásd 2. ábra).
- 5. R1 ez alapján a csomagot a közvetlenül csatlakozó Gigabit Ethernet 0/1 (G0/1) interfészén küldi ki.
- 6. A PC2 állomás megkapja a csomagot és megvizsgálja az IPv4 irányítótábláját.
- 7. PC2 meggyőződik arról, hogy a csomagot neki küldték, így megnyitja a csomagot és annak megfelelően válaszol.
- 3. példa: A PC1 állomás csomagot szeretne küldeni a 209.165.200.226 IP-című állomásnak:
- 1. PC1 megvizsgálja az IPv4-irányítótábláját és nem talál egyezést.
- 2. PC1 így a csomagot az alapértelmezett útvonal (0.0.0.0) alapján az alapértelmezett átjárónak küldi el. (192.168.10.1)
- 3. R1 forgalomirányító a Gigabit Ethernet 0/0 (G0/0) interfészén fogadja a csomagot és kiolvassa belőle a cél IP-címet. (209.165.200.226)
- 4. R1 megvizsgálja az irányítótábláját és egyezést talál a cél IP-cím és a **C 209.165.200.224/30** irányítótábla bejegyzés között (lásd 3. ábra).
- 5. R1 ez alapján a közvetlenül csatlakozó Serial 0/0/0 (S0/0/0) interfészén továbbítja a csomagot.
- 4. példa: A PC1 állomás csomagot szeretne küldeni a 10.1.1.10 IP-című állomásnak:
- 1. PC1 megvizsgálja az IPv4-irányítótábláját és nem talál pontos egyezést.
- 2. PC1 így a csomagot az alapértelmezett útvonal (0.0.0.0) alapján az alapértelmezett átjárónak küldi el. (192.168.10.1)
- 3. R1 forgalomirányító a Gigabit Ethernet 0/0 (G0/0) interfészén fogadja a csomagot és kiolvassa belőle a cél IP-címet (10.1.1.10).
- 4. R1 megvizsgálja az irányítótábláját és egyezést talál a cél IP-cím és a **D 10.1.1.0/24** irányítótábla bejegyzés között (lásd 4. ábra).
- 5. R1 ebből tudja, hogy a csomagot a 209.165.200.226 következő ugrás címre kell küldenie.
- 6. R1 ismét megvizsgálja az irányítótábláját és egyezést talál a cél IP-cím és a **C 209.165.200.224/30** irányítótábla bejegyzés között (lásd 4. ábra).
- 7. R1 ez alapján a közvetlenül csatlakozó Serial 0/0/0 (S0/0/0) interfészén továbbítja a csomagot.

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

- 1. rész: Állomás irányítótáblájának megjelenítése.
- 2. rész: Állomás IPv4 irányítótábla bejegyzéseinek vizsgálata.
- 3. rész: Állomás IPv6 irányítótábla bejegyzéseinek vizsgálata.

Laborgyakorlat - Viewing Host Routing Tables

Különböző felépítésű forgalomirányítók léteznek. A Cisco forgalomirányítókat az alábbi igényeknek megfelelően tervezték:

- **Vállalati telephely (branch) -** Távmunkások, kisebb vállalatok és közepes méretű telephelyek részére tervezett forgalomirányítók. Ide tartoznak: Cisco 800, 1900, 2900 és 3900-as sorozatú 2. generációs ISR (Integrated Series Router, G2).

- **WAN -** Nagyobb vállalatok és szervezetek által használt forgalomirányítók. Ide tartoznak: Cisco Catalyst 6500-as sorozatú kapcsolók és a Cisco ASR (Aggregation Service Router) 1000.

- **Szolgáltató -** Nagy szolgáltatók számára készült forgalomirányítók. Ide tartoznak: Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 (Carrier Routing System) és a 7600-as sorozatú forgalomirányítók.

A CCNA tananyag a vállalati telephelyek számára alkalmas forgalomirányítókat tárgyalja. Az ábrán a Cisco 1900, 2900 és 3900-as sorozatú, 2. generációs ISR család látható.

Működésüktől, méretüktől és összetettségüktől függetlenül minden forgalomirányító összességében egy számítógép. Mint ahogy a számítógépeknek, a táblagépeknek és az okos eszközöknek, úgy a forgalomirányítóknak is a következőkre van szükségük:

- Operációs rendszer (OS)

- Központi feldolgozó egység (CPU)

- Véletlen elérésű memória (RAM)

- Csak olvasható memória (ROM)

A forgalomirányító speciális memóriával is rendelkezik, ilyenek például a flash és a nemfelejtő véletlen hozzáférésű memória (NVRAM).

Mint minden számítógépnek, táblagépnek és okos eszköznek, úgy a Cisco eszközöknek is szükségük van egy CPU-ra, ami végrehajtja az operációs rendszer utasításait, mint például a rendszerindítást vagy a forgalomirányítási és kapcsolási feladatokat.

A CPU-nak a forgalomirányítási és kapcsolási funkciók ellátásához operációs rendszerre van szüksége. Mérettől és típustól függetlenül szinte minden Cisco eszköz a Cisco Internetwork Operating System (IOS) szoftvert használja. Ezzel működnek a forgalomirányítók, a LAN kapcsolók, a kisebb hozzáférési pontok, a tucatnyi interfésszel rendelkező nagy forgalomirányítók és számos egyéb eszköz is.

Az ábrán bejelölt összetevő egy 1941-es forgalomirányító CPU-ja hűtőbordával.

Egy forgalomirányító négyféle memóriát használ: RAM, ROM, NVRAM és flash.

RAM

A RAM-ban tárolódnak a különböző alkalmazások és folyamatok, mint például:

- **Cisco IOS -** Az IOS az indítási folyamat során a RAM-ba másolódik.

- **Aktív konfigurációs fájl -** Ez tartalmazza a forgalomirányító operációs rendszere által aktuálisan használt konfigurációs utasításokat. Gyakori elnevezése még: running-config.

- **IP irányítótábla -** Ebben a fájlban információk találhatók a közvetlenül csatlakozó és a távoli hálózatokról. A forgalomirányító a célhoz vezető legjobb útvonal meghatározásához használja.

- **ARP gyorsítótár (cache) -** Ez tartalmazza az IPv4- és a MAC-cím összerendeléseket, hasonlóan az állomásokon használt ARP (Address Resolution Protocol) tárhoz. Az ARP cache-re a LAN (Ethernet) interfésszel rendelkező forgalomirányítók esetében van szükség.

- **Csomagpuffer -** A csomagok az interfészre érkezéskor vagy egy interfészen történő kiküldés előtt átmenetileg egy pufferben kerülnek tárolásra.

A számítógépekhez hasonlóan a Cisco forgalomirányítók dinamikus, véletlen hozzáférésű memóriát (dynamic random-access memory, DRAM) használnak. A DRAM egy gyakran használt RAM típus, ami a CPU által végrehajtandó utasításokat és adatokat tartalmazza. A ROM-mal ellentétben a RAM felejtő memória, így a benne lévő adatok megtartásához állandó tápellátásra van szükség. A forgalomirányító kikapcsolásakor vagy újraindításakor teljes tartalmát elveszíti.

Az 1941-es forgalomirányítók alapértelmezés szerint 512 MB alaplapra integrált DRAM-mal és további maximum 2 GB memóriát kezelni tudó DIMM (dual in-line memory modul) bővítőhellyel rendelkeznek. A Cisco 2901, 2911 és 2921-es modellek is 512 MB integrált DRAM-ot tartalmaznak. Jegyezzük meg, hogy az 1. generációs ISR-ekben és a régebbi Cisco forgalomirányítókban nincsen alaplapra integrált RAM.

ROM

A Cisco forgalomirányítók a ROM-ban tárolják a következőket:

- **Indítási utasítások -** Az indulási folyamathoz szükséges utasítások.

- **Alap diagnosztikai szoftver -** Minden összetevőn végrehajtja a bekapcsolási önellenőrzést (power-on self-test, POST).

- **Csökkentett IOS -** Csökkentett szolgáltatáskészletű, tartalék IOS, ha a teljes értékű IOS nem töltődik be.

A ROM egy beégetett firmware-t tartalmazó integrált áramkör a forgalomirányító belsejében, ami áramtalanításkor vagy újraindítás során nem veszti el tartalmát.

NVRAM

A Cisco IOS az NVRAM-ban tárolja az indító konfigurációs fájlt (startup-config). A ROM-hoz hasonlóan az NVRAM sem veszíti el a tartalmát, ha áramtalanítjuk a forgalomirányítót.

Flash memória

A flash egy nem felejtő memória, amit az IOS és más rendszerfájlok állandó tárolására használnak. Az IOS az indítási folyamat során a RAM-ba másolódik.

A Cisco 1941-es forgalomirányítók két külső Compact Flash (CF) bővítőhelyet tartalmaznak. Mindegyik bővítőhely nagy sebességű, maximum 4 GB kapacitású kártyát támogat.

Az ábra a négy különböző típusú memória jellemzőit foglalja össze.

Bár számos különböző típusú és felépítésű forgalomirányító létezik, mégis mindegyik ugyanazokat az alapvető hardver elemeket tartalmazza.

Az ábrán egy 1. generációs Cisco 1841-es forgalomirányító belseje látható. Az összetevőkre kattintva egy rövid leírást kapunk mindegyikről.

Az ábrán megjelölt forgalomirányító összetevők között vannak olyanok is, amelyeket nem ez a fejezet tárgyal. Ilyen például a tápegység, a hűtőventilátor, a hűtőborda és a fejlett integrációs modul (advanced integration modul, AIM), .

Megjegyzés: Egy hálózati szakembernek fontosabb ismerni a forgalomirányító belső összetevőit és azok feladatát, mint tudni azok tényleges elhelyezkedését egy adott készülékben. Az egyes forgalomirányító modellektől függően ezek az összetevők különböző helyeken lehetnek.

A Cisco 1941-es forgalomirányítón a következő csatlakozók találhatók:

- **Konzol portok -** Egy RJ-45 és egy B típusú USB csatlakozóval (mini-B USB) szerelt konzol port a kezdeti konfigurációhoz és a parancssori (command line interface, CLI) hozzáféréshez.

- **AUX port -** A konzol porthoz hasonló RJ-45 port a távoli hozzáféréshez.

- **Két LAN-interfész -** Két Gigabit Ethernet interfész a LAN hozzáféréshez.

- **Kiterjesztett, nagy sebességű WAN-interfész kártya bővítőhelyek (Enhanced high-speed WAN Interface Card, EHWIC) -** A modularitást és a sokrétű felhasználhatóságot teszi lehetővé ez a két bővítőhely, melyek segítségével a forgalomirányítóba különböző típusú, mint például soros, DSL (Digital Subscriber Line), kapcsolóport és vezeték nélküli interfész modulok tehetők.

A Cisco 1941 ISR háttértár bővítőhelye további tárolási lehetőséget biztosít. A két CF kártya bővítőhely mindegyike 4 GB kapacitású flash kártyát támogat. A két USB port is a tárolókapacitást növeli és külső biztonsági kulcs használatát teszi lehetővé.

A compact flash tárolja a Cisco IOS képfájlt, a naplófájlokat, a hang konfigurációs és HTML fájlokat, a biztonsági konfigurációt és további, a rendszer működéséhez szükséges fájlokat. Gyárilag csak a 0. bővítőhelyben van CF kártya és alapértelmezetten innen indul a forgalomirányító.

Az ábra a fent említett csatlakozókat és bővítőhelyeket mutatja.

A Cisco eszközök, forgalomirányítók és kapcsolók különféle berendezéseket kapcsolnak össze. Ezért különböző típusú portokkal és interfészekkel rendelkeznek, melyekhez kábelek segítségével csatlakoztathatók az eszközök.

Egy Cisco forgalomirányító csatlakozói két csoportba sorolhatók:

- **Felügyeleti portok -** Ezek a konzol és az AUX-portok, melyek használatával konfigurálható, felügyelhető és probléma estén javítható a forgalomirányító. A LAN és WAN-interfészekkel ellentétben ezeket a portokat csomagtovábbításra nem használják.

- **Sávon belüli interfészek -** Ezek a LAN és WAN-interfészek, melyek IP-címmel rendelkeznek a felhasználói forgalom továbbításához. A LAN-kapcsolatok leggyakrabban az Ethernet interfészeket, míg a WAN összeköttetések a soros és DSL-interfészeket támogatják.

Az ábrán a 2. generációs Cisco 1941 ISR portjai és interfészei vannak megjelölve.

A hálózati eszközökhöz hasonlóan a Cisco eszközök is fénykibocsátó diódát (Light Emitting Diode, LED) használnak az állapotinformációk megjelenítéséhez. Egy interfész LED a hozzá tartozó csatoló működéséről ad információt. Ha egy aktív és megfelelően csatlakoztatott interfész LED-je nem világít, akkor az interfésszel probléma lehet. Ha egy interfész terhelése nagy, akkor a LED folyamatosan világít.

A Cisco kapcsolóhoz hasonlóan a Cisco forgalomirányító parancssorának elérése is többféleképpen történhet. A leggyakoribb megoldások:

- **Konzol** - Kis sebességű soros vagy USB kapcsolat segítségével biztosítja a közvetlen, sávon kívüli hozzáférést egy Cisco eszközhöz.

- **Telnet vagy SSH** - Alkalmazások a parancssor távoli eléréséhez aktív hálózati interfészen keresztül.

- **AUX-port** - A forgalomirányító távoli felügyeletéhez használható telefonvonalon keresztüli elérés modem segítségével.

A konzol és az AUX-port a forgalomirányítón található.

Ezeken a portokon kívül a forgalomirányítók az IP-csomagok fogadásához és továbbításához különböző hálózati interfészekkel is rendelkeznek, melyekkel sokféle hálózathoz képesek csatlakozni. A különböző típusú hálózatokhoz csatlakozó interfészek eltérő kábelt és csatlakozót használnak.

A forgalomirányító minden interfésze egy-egy IP-hálózat része, így mindegyikhez különböző hálózathoz tartozó IP-címet és maszkot kell beállítani. Következésképpen egy Cisco IOS forgalomirányító két aktív interfésze nem tartozhat ugyanahhoz a hálózathoz.

A forgalomirányító interfészei két csoportba sorolhatók:

- **Ethernet LAN-interfészek** - LAN-eszközök, mint például számítógépek és kapcsolók csatlakoztatásához, valamint forgalomirányítók összekötésére használhatók. Az Ethernet interfészek elnevezésére számos változat használatos: Ethernet, FastEthernet és GigabitEthernet. Az alkalmazott elnevezés függ az eszköz típusától és a modelltől.

- **Soros WAN interfészek** - Forgalomirányítók külső hálózathoz csatlakoztatásához használják, általában nagyobb földrajzi távolságok esetén. A LAN-interfészekhez hasonlóan a WAN-interfészek is egyedi IP-címmel és alhálózati maszkkal rendelkeznek, ami egyértelműen megadja, hogy melyik hálózathoz tartoznak.

Az ábrán a forgalomirányító LAN és WAN-interfészei láthatók.

A Cisco IOS működése eltérő lehet a különböző hálózati eszközök jellemzőitől és felhasználási körétől függően, de minden esetben biztosítja a következőket:

- Címzés
- Interfészek
- Forgalomirányítás
- Biztonság
- QoS
- Erőforrás felügyelet

A forgalomirányítón lévő IOS egy több megabájt méretű fájl, mely a kapcsolókhoz hasonlóan a flash memóriában található . A flash jellegéből fakadóan az IOS frissíthető vagy új szolgáltatásokkal bővíthető. A rendszerindítási folyamat során az IOS a RAM-ba másolódik, mely lényegesen gyorsabb a flash-nél, ezzel növeli az eszköz teljesítményét.

Ahogy az ábrán is látható, a forgalomirányító induláskor az alábbi két fájlt tölti be a RAM-ba:

- **IOS-képfájl -** Az IOS felelős az eszköz hardver összetevőinek alapvető működéséért. Az IOS-képfájl a flash memóriában található.

- **Indító konfigurációs fájl -** Az indító konfigurációs fájlban található utasítások végzik a forgalomirányító kezdeti beállítását és a RAM-ban tárolt aktív konfigurációs fájl létrehozását. Az indító konfigurációs fájl az NVRAM-ban található. Minden változtatás az aktív konfigurációs fájlba mentődik és az IOS azonnal végrehajtja azt.

A hálózati rendszergazda által elvégzett konfigurációs módosításoknak megfelelően változik az aktív konfigurációs fájl is. A módosításokat követően az aktív konfigurációs fájlt (running-config) indító konfigurációs fájlként (startup-config) az NVRAM-ba kell menteni, hogy a forgalomirányító újraindításakor vagy áramkimaradás esetén az adatok ne vesszenek el.

Az 1. ábrán a rendszerindítási folyamat három alapvető szakasza látható:

1. Az önellenőrzés (POST) és a rendszerindító program (bootstrap) betöltése.

2. A Cisco IOS szoftver megkeresése és betöltése

3. Az indító konfigurációs fájl megkeresése és betöltése, vagy belépés beállítási (setup) módba.

1. Az önellenőrzés (POST) és a rendszerbetöltő program (bootstrap) futtatása (2. ábra)

Az önellenőrzés (Power-On Self Test, POST) egy gyakori folyamat, ami szinte minden számítógépen lefut induláskor. A forgalomirányító bekapcsolásakor a ROM chipben lévő program elindítja a POST folyamatot, ami leellenőrzi a forgalomirányító hardver elemeit. A teszt során a forgalomirányító ROM-ban tárolt hibakereső programokat futtat le a hardver összetevőkön, mint például a CPU-n, a RAM-on és az NVRAM-on. A POST befejezését követően a forgalomirányító betölti a rendszerindító programot.

Miután a rendszerindító program a ROM-ból a RAM-ba töltődött, a CPU végrehajtja a program utasításait. A rendszerindító program legfontosabb feladata a Cisco IOS megkeresése és betöltése a RAM-ba.

Megjegyzés: Konzol kapcsolat esetén innentől kezdve minden kimenet megjelenik a képernyőn.

2. A Cisco IOS megkeresése és betöltése (3. ábra)

Az IOS jellemzően a flash memóriában található, és onnan másolódik a RAM-ba. Az IOS-képfájl önkicsomagolási folyamata alatt a képernyőn kettős keresztekből álló jelsorozat jelenik meg.

Ha az IOS nincs a flash memóriában, akkor a forgalomirányítónak TFTP-szerver segítségével kell megkeresnie azt. Ha a forgalomirányító egyáltalán nem talál teljes értékű IOS-t, akkor egy csökkentett IOS-verzió töltődik be a ROM-ból a RAM-ba. Ez az IOS segít a hiba megkeresésében és adott esetben a teljes IOS-verzió RAM-ba töltésében.

3. A konfigurációs fájl megkeresése és betöltése (4. ábra)

A rendszerindító program az NVRAM-ban keresi az indító konfigurációs, más néven startup-config fájlt. Ebben a fájlban vannak a korábban elmentett konfigurációs parancsok és paraméterek. Ha létezik ilyen fájl, akkor aktív konfigurációs fájlként betöltődik a RAM-ba. A running-config fájl interfész címeket tartalmaz, forgalomirányítási folyamatokat indít el, jelszavakat állít be és a forgalomirányító egyéb jellemzőit adja meg.

Ha az NVRAM nem tartalmaz startup-config fájlt, akkor a forgalomirányítónak egy TFTP (Trivial File Transfer Protocol) szervert kell keresnie. Ha a forgalomirányító egy interfészén aktív kapcsolatot érzékel egy másik forgalomirányítóval, akkor szórásos üzenet küldésével keres konfigurációs fájlt az aktív összeköttetésen keresztül.

Ha a forgalomirányító nem talál TFTP-szervert, akkor alapbeállítási (setup) módban indul el. Alapbeállítási módban a felhasználó kérdésekre adott válaszok segítségével tudja a legfontosabb konfigurációs lépéseket elvégezni. Mivel ez a mód nem alkalmas összetett konfiguráció megadására, így a hálózati rendszergazdák jellemzően nem is használják.

Megjegyzés: Ebben a kurzusban a forgalomirányítót nem fogjuk beállítási módban konfigurálni. Amikor a rendszer a setup módba lépésre kérdez rá, mindig válaszoljuk azt, hogy **no**. Ha mégis belépünk setup módba, akkor a beállítási folyamat a **Ctrl**+**C** billentyűkombináció lenyomásával bármikor megszakítható.

A **`show version`** parancs használható a forgalomirányító alapvető hardver- és szoftverkomponenseinek ellenőrzésére és az esetleges hibák megkeresésére. A parancs információkat jelenít meg a forgalomirányítón éppen futó Cisco IOS szoftver és a rendszerindító program verziójáról, valamint a hardver konfigurációról, például a rendszer memória méretéről.

A **`show version`** parancs kimenete a következőket tartalmazza:

- **IOS-verzió -** A RAM-ba betöltött, a forgalomirányító által használt Cisco IOS szoftver verziója.
- **ROM rendszerindító program -** A ROM-ban tárolt, a forgalomirányító indításához használt rendszerindító program (System Bootstrap) verziója.
- **Az IOS helye -** A Cisco IOS teljes fájlneve és helye, ahonnan a rendszerindító program betöltötte.
- **CPU típus és RAM mennyiség -** A sor elején a forgalomirányító CPU-jának típusa, a végén pedig a DRAM mennyisége látható. Bizonyos forgalomirányítók, mint például a Cisco 1941 ISR a DRAM memória egy részét a csomagok átmeneti tárolására használja. A tényleges DRAM mennyiség meghatározásához ilyenkor a kimenetben szereplő, "/" jellel elválasztott két értéket össze kell adni.
- **Interfészek -** A forgalomirányító fizikai interfészei. A példánkban a Cisco 1941 ISR két Gigabit Ethernet és két lassabb soros interfésszel rendelkezik.
- **Az NVRAM és a flash memória mennyisége -** A forgalomirányítóban lévő NVRAM és flash memória mennyisége. Az NVRAM tárolja a startup-config fájlt, a flash pedig a Cisco IOS-t.

A **`show version`** parancs utolsó sorában található a konfigurációs regiszter aktuális értéke hexadecimális formában. Ha zárójelben egy második érték is szerepel, akkor az a forgalomirányító következő indulásakor érvénybe lépő konfigurációs regiszter érték.

A konfigurációs regiszternek különféle felhasználási területei vannak, ilyen például a jelszó helyreállítás. A regiszter gyári alapértelmezett értéke 0x2102, ami azt jelenti, hogy a forgalomirányító induláskor a Cisco IOS szoftvert a flash-ből, az indító konfigurációs fájlt pedig az NVRAM-ból próbálja betölteni.

A Cisco forgalomirányítók és kapcsolók sok hasonlóságot mutatnak. Hasonló operációs rendszert futtatnak, melyek parancsszerkezete és parancskészlete is majdnem azonos. Ezen felül mindkét eszköztípus azonos kezdeti konfigurációt igényel a hálózathoz való csatlakoztatás előtt.

A kapcsolóhoz hasonlóan a forgalomirányító kezdeti konfigurációjának lépései a következők:

1. Az eszköz nevének megadása a **`hostname`** globális konfigurációs paranccsal. (1. ábra)

2. Jelszavak beállítása. (2. ábra)

- A privilegizált EXEC mód jelszava az **`enable secret`** paranccsal adható meg.
- A felhasználói EXEC mód jelszava a konzol porton kiadott **`login`** és **`password`** parancsokkal állítható be.
- A virtuális hozzáférést az EXEC módhoz hasonlóan védhetjük le a virtuális terminál (vty) porton.
- A **`service password-encryption`** globális konfigurációs parancs megakadályozza a jelszavak egyszerű szövegként való megjelenítését a konfigurációs fájlban.

3. Jogos használatra vonatkozó üzenet írása a **`banner motd`** (message of the day) globális paranccsal. (3. ábra)

4. A konfiguráció elmentése a **`copy run start`**paranccsal. (4. ábra)

5. A konfiguráció ellenőrzése a **`show run`** paranccsal.

Az 5. ábrán gyakorolhatjuk a konfigurációs lépéseket.

Ebben a feladatban a forgalomirányító alapbeállítását végezzük el. Biztonságos hozzáférést állítunk be a parancssorhoz és a konzol porthoz titkosított és egyszerű szöveges jelszavak segítségével. Ezenkívül megtanuljuk, hogyan kell üzenetet küldeni a forgalomirányítóba bejelentkező felhasználóknak és egyben figyelmeztetni a jogosulatlan belépőket a tiltott hozzáférésről. Végezetül ellenőrizzük és elmentjük az aktív konfigurációt.

Packet Tracer - Configure Initial Router Settings - instructions

Packet Tracer - Configure Initial Router Settings - PKA

A forgalomirányítók eléréséhez annak interfészeit konfigurálni kell. Egy adott interfész beállításához interfész konfigurációs módba kell lépni az **`interface`** *`típus-és-szám`* globális konfigurációs paranccsal.

A Cisco forgalomirányítók számos különböző típusú interfésszel rendelkezhetnek. A példában a Cisco 1941-es forgalomirányító két Gigabit Ethernet és két WAN interfész kártyán (WIC) lévő soros interfésszel rendelkezik. Az interfészek elnevezései a következők:

- Gigabit Ethernet 0/0 (G0/0)
- Gigabit Ethernet 0/1 (G0/1)
- Serial 0/0/0 (S0/0/0)
- Serial 0/0/1 (S0/0/1)

Egy forgalomirányító interfészének engedélyezéséhez a következőket kell beállítani:

- **IPv4-cím és alhálózati maszk -** Az IP-cím és az alhálózati maszk az **`ip address`** *`alhálózati maszk`* interfész konfigurációs paranccsal adható meg.

- **Interfész aktiválása -** Alapértelmezetten a LAN és WAN-interfészek inaktív állapotban vannak. Az interfész a **`no shutdown`** paranccsal aktiválható. Ez tulajdonképpen az interfész bekapcsolása, mely csak abban az esetben lesz aktív, ha fizikailag egy másik eszközhöz (pl:. hubhoz, kapcsolóhoz, forgalomirányítóhoz) kapcsolódik.

Bár nem kötelező, a hálózat megfelelő dokumentálása érdekében ajánlott az interfészekhez leírást is megadni. Ez a szöveg maximálisan 240 karakter lehet. Valódi hálózatokban a leírásban található információk, mint például az adott interfészhez csatlakozó hálózat típusa vagy a hálózatban lévő egyéb forgalomirányítók jelenléte, segíthetnek az esetleges hibaelhárításban. Ha az interfész egy szolgáltatóhoz (pl.: ISP) csatlakozik, hasznos lehet megadni a szolgáltatói kapcsolat információit és a kapcsolattartó adatait is.

Az 1. ábrán az R1 forgalomirányító LAN-interfészeinek beállítása látható, a 2. ábrán pedig a LAN-interfészek konfigurálását gyakorolhatjuk.

Megjegyzés: Az 1. ábrán a Gigabit Ethernet 0/1 interfész beállításai parancs rövidítések segítségével történtek.

Számos olyan parancs létezik, amivel egy interfész konfigurációját ellenőrizhetjük. Ezek közül a leghatékonyabban a **`show ip interface brief`**utasítás használható. A parancs kimenete megjelenít minden interfészt, azok IP-címét és aktuális állapotát. A beállított és csatlakoztatott interfészeknél a Status (állapot) és a Protocol (protokoll) oszlopokban is "up" értéknek kell szerepelni. Bármilyen egyéb érték azt jelzi, hogy a konfigurációval vagy a kábelezéssel probléma van.

Az interfész összeköttetésének ellenőrzése a **`ping`**paranccsal történhet. A Cisco forgalomirányítók öt egymást követő ping üzenetet küldenek és mérik a minimális, átlagos és maximális válaszidőt (round trip time). A felkiáltójelek a kapcsolat működőképességét jelzik.

Az 1. ábrán a **`show ip interface brief`** parancs kimenete látható, ahol a LAN-interfészek és az egyik WAN-kapcsolat aktív és működik. Figyeljük meg, hogy a**`ping`** parancs kimenetében látható öt felkiáltójel az R1 és R2 közötti kapcsolat működését jelzi.

További, ellenőrzésre szolgáló parancsok:

- **`show ip route`** **-** Megjeleníti a RAM-ban tárolt IPv4 irányítótáblát.
- **`show interfaces`** **-** Megjeleníti az eszköz interfészeire vonatkozó statisztikai adatokat.
- **`show ip interface`** **-** Megjeleníti a forgalomirányító interfészeinek IPv4 statisztikai adatait.

A 2. ábrán a **`show ip route`** parancs kimenete látható. Figyeljük meg a három közvetlenül csatlakozó hálózatra és a hozzájuk tartozó forgalomirányító interfészekre vonatkozó bejegyzéseket.

Ne felejtsük elmenteni a konfigurációt a **`copy running-config startup-config`** paranccsal.

A legtöbb forgalomirányítónak legalább két interfésze van. Mindegyik interfész külön hálózathoz tartozik és egyedi IP-címmel rendelkezik.

Egy végberendezés hálózati működéséhez megfelelő IP-cím információt, köztük alapértelmezett átjáró címet kell az eszközön beállítani. Az alapértelmezett átjáróra csak abban az esetben van szükség, ha egy állomás egy másik hálózaton lévő eszköznek szeretne csomagot küldeni. Az alapértelmezett átjáró címe rendszerint az állomás helyi hálózatához csatlakozó forgalomirányító interfész címe. A forgalomirányító interfészének beállítása tetszőleges lehet, de az állomás és a router interfész IP-címét ugyanabból a hálózatból kell választani.

Az ábrán egy két interfésszel rendelkező forgalomirányító hálózata látható. Mindegyik interfész egy-egy külön hálózathoz tartozik. A G0/0 interfész a 192.168.10.0, a G0/1 pedig a 192.168.11.0 hálózathoz csatlakozik. Minden állomáson a megfelelő alapértelmezett átjáró van beállítva.

Az 1. ábrán a PC1 állomás csomagot küld a PC2-nek. Ebben az esetben nincs szükség alapértelmezett átjáróra, hiszen PC1 a PC2-nek címzett csomagot a kapcsolón keresztül közvetlenül a PC2-nek továbbítja.

A 2. ábrán a PC1 állomás csomagot küld a PC3-nak. Ebben az esetben PC1 a PC3-nak megcímzett csomagot a forgalomirányítónak továbbítja. A forgalomirányító fogadja a csomagot, az irányítótáblájában a célcím alapján megkeresi a megfelelő kimenő interfészt, majd ezen továbbítja a csomagot.

Minden olyan eszköznek alapértelmezett átjáróra van szüksége, amely egy távoli hálózatban lévő célállomással akar kommunikálni, és az oda vezető legjobb útvonal meghatározásához forgalomirányítót használ. Ehhez a közvetítő eszközök, mint például a kapcsolók is alapértelmezett átjáró címet használnak, hasonlóan a végberendezésekhez.

A kapcsoló IP-cím információi csak a távolról történő hozzáféréshez szükségesek. Más szóval, egy kapcsolóra csak akkor tudunk Telnet-tel bejelentkezni, ha van hova csatlakoznunk, azaz a kapcsoló IP-címmel rendelkezik. Ha a kapcsolót csak a helyi hálózat eszközeiről szeretnénk elérni, akkor elegendő rajta IP-címet beállítani.

Az IP-cím megadása a kapcsoló virtuális interfészén (Switch Virtual interface, SVI) történik az alábbiak szerint:

```
S1(config)# interface vlan1

S1(config-vlan)# ip address 192.168.10.51 255.255.255.0

S1(config-vlan)# no shut
```

Abban az esetben, ha a kapcsolónak más hálózatokból is elérhetőnek kell lenni, akkor alapértelmezett átjáróra van szükség, mivel a kapcsoló által küldött csomagokat ugyanúgy kell kezelni, mint egy állomástól küldötteket. Míg a kapcsolóval egy hálózaton belül lévő eszköznek küldött csomagok közvetlenül az adott eszközhöz kerülnek továbbításra, addig a távoli hálózatba küldött csomagokat a kapcsoló az alapértelmezett átjárójának továbbítja.

A kapcsoló alapértelmezett átjárójának megadásához az alábbi globális konfigurációs parancs használható:

```
S1(config)# ip default-gateway 192.168.10.1
```

Az 1. ábrán a rendszergazda távoli hálózatból csatlakozik a kapcsolóhoz. A rendszergazdának küldött válaszcsomagok továbbításához a kapcsolón alapértelmezett átjárót kell konfigurálni.

Gyakori félreértés, hogy a kapcsolók az alapértelmezett átjáró címet arra használják, hogy a hozzájuk csatlakozó állomás által küldött csomagokat egy távoli hálózatban lévő állomásnak továbbítsák. Valójában a kapcsoló az IP-címet és az alapértelmezett átjárót csak a saját maga által létrehozott és kiküldött csomagok esetén használja. A kapcsolóhoz csatlakozó állomás által küldött csomagok már rendelkeznek a távoli hálózatok eléréséhez szükséges alapértelmezett átjáró információval. A 2. ábrán a kapcsoló alapértelmezett átjárójának beállítását gyakorolhatjuk.

Egy eszköz hálózati működéséhez IP-címet, alhálózati maszkot és alapértelmezett átjárót kell rajta beállítani. Alapértelmezett átjáróra csak abban az esetben van szükség, ha egy állomás egy másik hálózaton lévő eszköznek szeretne csomagot küldeni. Az alapértelmezett átjáró címe rendszerint az állomás helyi hálózatához csatlakozó forgalomirányító interfész címe. Ebben a feladatban befejezzük

a hálózat dokumentálását, majd ellenőrizzük azt a végpontok közötti kapcsolatok tesztelésével és a felmerülő hibák kijavításával. A hibaelhárítás lépései a következők lesznek:

- A dokumentáció ellenőrzése és a problémák felfedése tesztek segítségével.
- Alkalmas megoldás keresése egy adott problémára.
- A megoldás megvalósítása.
- A megoldás ellenőrzése teszteléssel.
- A megoldás dokumentálása.

Packet Tracer - Troubleshooting Default Gateway Issues - Instructions

Packet Tracer - Troubleshooting Default Gateway Issues - PKA

Tudunk olvasni a térképről?

Megjegyzés: Ajánlott, hogy a tanulók párokban dolgozzanak, de a feladatot megoldhatják egyedül is.

Az oktatótól egy forgalomirányító által generált **`show ip route`** parancs kimenetet kapunk. A forgalomirányítási információk alapján kell elkészítenünk a topológiát Packet Tracer-ben.

A topológiának minimálisan az alábbiakat kell tartalmazni:

- 1 Catalyst 2960-as kapcsoló
- 1 Cisco 1941-es forgalomirányító HWIC-4ESW 4 portos kapcsolómodullal, és legalább 15.1 verziójú IOS-szel.
- 3 PC (lehetnek szerverek, általános számítógépek, laptopok, stb.)

Használjuk a Packet Tracer megjegyzés (note) funkcióját a forgalomirányító interfészek és a topológiában szereplő végberendezések címeinek feltüntetésére. Jelöljünk meg minden olyan eszközt, portot és címet, ami a **`show ip route`** parancs kimenetéből, vagyis az irányítótáblából meghatározható. Végül mentsük el a munkánkat, és beszéljük meg a megoldást az osztállyal.

Csoportos feladat - Can you read this map? - Instructions

A hálózati vezető elégedett a LAN rendszergazdai teljesítményünkkel. Szeretné, ha megmutatnánk, hogy képesek vagyunk olyan forgalomirányító konfigurálására is, mely két LAN-hoz csatlakozik. Feladatunk egy Cisco IOS forgalomirányító és egy kapcsoló alapbeállítása, majd a végpontok közötti kapcsolatok tesztelésével az eszközök konfigurációjának ellenőrzése.

Packet Tracer Skills Integration Challenge - Instructions

Packet Tracer Skills Integration Challenge - PKA

A hálózati réteg, vagy más néven az OSI 3. rétege, olyan szolgáltatásokat biztosít, amelyek lehetővé teszik a végberendezések közötti kommunikációt a hálózaton. A végpontok közötti adattovábbításhoz a hálózati réteg négy alapvető folyamatot használ: végberendezések címzése, beágyazás, forgalomirányítás és kicsomagolás.

Az internet elsősorban az IPv4-protokollra épül, ami a legszélesebb körben használt hálózati rétegbeli protokoll. Az IPv4-csomag egy IP-fejlécből és egy adatrészből áll. A korlátozott számú egyedi nyilvános IPv4-cím vezetett az IPv6 kifejlesztéséhez. Az IPv6 az egyszerűbb fejlécének köszönhetően számos előnnyel rendelkezik az IPv4-gyel szemben. Ilyen például a hatékonyabb forgalomirányítás, az egyszerűsített kiterjesztett fejlécek és a folyamatonkénti feldolgozás. Az IPv6-címek 128 bites hierarchikus felépítésűek, ellentétben a 32 bites IPv4-címekkel, melynek köszönhetően nagyságrendekkel több IP-címet biztosítanak.

A hierarchikus címzésen kívül a hálózati réteg feladata a forgalomirányítás is.

Az állomásoknak helyi irányítótáblát kell fenntartani, hogy a hálózati rétegbeli csomagokat a megfelelő célhálózatba tudják küldeni. Ez a helyi tábla jellemzően a közvetlenül csatlakozó hálózatokat és a helyi alapértelmezett útvonalat tartalmazza. A helyi alapértelmezett útvonal az alapértelmezett átjáróhoz vezető út.

Az alapértelmezett átjáró a forgalomirányító helyi hálózatra csatlakozó interfészének IP-címe. Ha egy állomás egy másik hálózatban lévő célállomásnak szeretne csomagot küldeni, akkor azt az alapértelmezett átjárónak küldi további feldolgozásra.

Amikor egy forgalomirányító, például az alapértelmezett átjáró csomagot fogad, akkor a célcímből meghatározza a célhálózatot. A forgalomirányító irányítótáblája mind a közvetlenül csatlakozó, mind a távoli hálózatokhoz vezető útvonalakról tárol információkat. Ha a forgalomirányító irányítótáblájában szerepel a célhálózat, akkor a csomag ennek alapján kerül továbbításra. Ha nincs megfelelő bejegyzés, akkor a forgalomirányító saját alapértelmezett útvonalát használja, vagy annak hiányában eldobja a csomagot.

Az irányítótábla bejegyzések konfigurálhatók kézzel (statikus forgalomirányítás), vagy a forgalomirányítók között irányító protokollokkal (dinamikus forgalomirányítás).

A forgalomirányítók elérhetőségéhez konfigurálni kell azok interfészeit. Egy adott interfész beállításához interfész konfigurációs módba kell lépni az **`interface`** *`típus szám`* globális konfigurációs paranccsal.

Az adathálózatok és az internet az emberek közötti megbízható kommunikációt, vagyis a humán hálózat működését segítik. Már egyetlen eszközön is számos alkalmazást és szolgáltatást veszünk igénybe. Ilyen például az e-mail, a világháló, valamint az üzenetküldésre és információszerzésre egyaránt használható azonnali üzenetküldés. Az e-mail kliensekhez, webböngészőkhöz és azonnali üzenetküldő kliensprogramokhoz hasonló alkalmazások lehetővé teszik, hogy a számítógépek és hálózatok segítségével üzeneteket küldjünk vagy információt szerezzünk.

A fenti alkalmazásokból származó adatokat be kell csomagolni, majd leszállítani és kézbesíteni a célkészüléken futó megfelelő alkalmazás részére. Az OSI szállítási rétegében működő folyamatok fogadják az alkalmazási rétegből származó adatokat, majd előkészítik a hálózati rétegben használatos címzésre. A szállítási réteg **előkészíti** az adatok hálózaton keresztül történő átvitelét. A küldő számítógép párbeszédet folytat a fogadó számítógéppel annak érdekében, hogy eldöntsék, miként bonthatók az adatok **szegmensekre**, hogyan lehet megbizonyosodni arról, hogy egyetlen szegmens sem veszik el, és milyen módon ellenőrizhetők a megérkezett szegmensek. Ha a szállítási rétegre gondolunk, képzeljünk magunk elé egy fuvarozási osztályt, amely egy több csomagból álló rendelést készít elő kézbesítésre.

Ebben a fejezetben megvizsgáljuk, hogy a szállítási réteg milyen szerepet tölt be az alkalmazások adatainak - hálózati rétegbeli felhasználásra történő - beágyazásában. A szállítási réteg az alábbi feladatokat is magában foglalja:

- Lehetővé teszi, hogy egyetlen eszközön egyszerre több alkalmazás (pl.: e-mail és közösségi média használata) kommunikáljon a hálózaton keresztül.

- Szükség esetén megbizonyosodik arról, hogy minden adat megérkezett és sorrendben eljutott a megfelelő alkalmazáshoz.

- Hibajavító módszereket használ.

Tanulási célkitűzések

A fejezetben a következő témaköröket tekintjük át:

- A szállítási réteg szükségességének ismertetése.

- A szállítási réteg szerepe az alkalmazások közötti, végponttól végpontig történő adatátvitel biztosításában.

- Két protokoll - a TCP és az UDP - szerepe a TCP/IP szállítási rétegében.

- A szállítási réteg alapvető feladatainak ismertetése, beleértve a megbízhatóságot, a portcímzést és a szegmentálást.

- Az alapvető feladatok megvalósításának módja a TCP és az UDP esetében.

- Mikor célszerű a TCP és az UDP használata, vagyis olyan alkalmazások példaként történő bemutatása, amelyek ezeket a protokollokat használják.

Beszélgessünk róla...

Megjegyzés: A feladat megoldása ideális esetben közepes méretű (6-8 fős) csoportokban történik.

Az oktató egy összetett üzenetet suttog a csoport első diákjának fülébe. Ilyen üzenet lehet például a következő: "A záróvizsga jövő kedden, azaz február 5-én 14:00-kor lesz az 1151-es teremben."

A diák ezután a soron következő diák fülébe suttogja az üzenetet. A folyamatot az egyes csoportok egészen addig ismétlik, amíg minden egyes tagjukhoz el nem jut a suttogott üzenet. Az alábbi szabályokat kell betartani:

- Az üzenetet csupán egyszer súghatjuk a szomszédunk fülébe.

- Az üzenet átadása személyről személyre történik, senki sem maradhat ki.

- Az oktatónak meg kell kérnie egy diákot, hogy mérje a feladat végrehajtásának idejét az első résztvevőtől az utolsóig. Erre a célra valószínűleg az első vagy az utolsó személy a legalkalmasabb.

- Az utolsó diák hangosan elmondja, hogy mit is hallott pontosan.

Ezután az oktató megismétli az eredeti üzenetet, így a csoport összehasonlíthatja az utolsó diák által mondott üzenettel.

Csoportos feladat - We Need to Talk Instructions

A szállítási réteg feladata, hogy két alkalmazás között ideiglenes kommunikációs munkamenetet létesítsen, valamint adatokat kézbesítsen. Az alkalmazások által generált adatokat a forrásállomáson futó alkalmazásból a célállomáson futó alkalmazáshoz kell elküldeni, függetlenül a célállomás típusától, az adatátvitelhez használt közegtől, az adatok által megtett útvonaltól, az előforduló

torlódástól, valamint a hálózat méretétől. Ahogy az ábrán is látható, a szállítási réteg egyfajta kapocs az alkalmazási réteg, valamint a hálózati átvitelért felelős alsóbb rétegek között.

A szállítási réteg olyan módot biztosít a hálózaton keresztül történő adatkézbesítéshez, amellyel a fogadó oldalon pontosan összeállíthatók az adatok. A szállítási réteg gondoskodik az adatok szegmentálásáról, valamint irányítja a szegmensek újbóli összeállítását adatfolyammá. A TCP/IP esetében a szegmentációs és újra-összeállítási folyamatok megvalósítását két roppant eltérő protokoll végzi: a TCP (Transmission Control Protocol) és az UDP (User Datagram Protocol).

A szállítási réteg protokolljai elsősorban az alábbiakért felelnek:

- A forrás- és célállomásokon futó alkalmazások közötti egyedi kommunikáció nyomon követése.

- Az adatok szegmentálása a jobb kezelhetőség céljából, valamint a szegmentált adatok ismételt összeállítása a rendeltetési helyen.

- A megfelelő alkalmazás azonosítása minden egyes kommunikációs folyamhoz.
  - **Az egyedi párbeszédek nyomon követése**
  - A szállítási rétegben a forrás- és a célalkalmazás között áramló minden egyes konkrét adathalmazt párbeszédnek nevezünk (lásd 1. ábra). Egy állomás számos alkalmazást futtathat, amelyek egyidejűleg kommunikálnak a hálózaton keresztül. Ezek mindegyike egy vagy több alkalmazással kommunikál, amelyek egy vagy több állomáson futnak. A szállítási réteg feladata, hogy fenntartsa és nyomon kövesse az ilyen többszörös párbeszédeket.
  - **Az adatcsomagok szegmentálása és ismételt összeállítása**
  - Az adatokat elő kell készíteni, hogy kezelhető darabokban lehessen átküldeni az átviteli közegen. A legtöbb hálózat korlátozza az egy csomag által szállítható adatmennyiséget. A szállítási réteg protokolljai olyan szolgáltatásokat nyújtanak, amelyekkel az alkalmazások adatai megfelelő méretű adatblokkokra szegmentálhatók. Ezek a szolgáltatások tartalmazzák az egyes adatszeleteken végrehajtandó beágyazást. Minden egyes adatblokkhoz -- az ismételt összeállítást megkönnyítendő -- hozzáadásra kerül egy fejléc. A fejléc segítségével nyomon követhető az adatfolyam útja.
  - A célban a szállítási rétegnek képesnek kell lennie az adatszeletek teljes adatfolyammá való visszaalakítására, amely használhatóvá teszi őket az alkalmazási réteg számára. A szállítási rétegben működő protokollok leírják, hogy a fejlécben szereplő információkat miként lehet felhasználni az adatszeletek - alkalmazási rétegnek átadandó - adatfolyammá történő ismételt összeállításához.
  - **Az alkalmazások azonosítása**
  - A hálózat minden egyes állomásán számos alkalmazás és szolgáltatás futhat. Az adatfolyamok megfelelő alkalmazásoknak történő átadásához a szállítási rétegnek azonosítania kell a célalkalmazást (lásd 3. ábra). Ennek érdekében a szállítási réteg mindegyik alkalmazáshoz egy azonosítót rendel. Ezt az azonosítót portszámnak nevezzük. Minden hálózati elérést igénylő szoftverfolyamathoz egy portszám van rendelve, amely egyedi az adott állomáson. A szállítási réteg a portok alapján azonosítja az alkalmazásokat, illetve szolgáltatásokat.
  - **Párbeszéd multiplexelése**
  - Bizonyos adattípusok (pl.: online videoközvetítés) teljes kommunikációs folyamként történő átküldése a hálózaton keresztül felemésztheti a rendelkezésre álló teljes sávszélességet, egyúttal megakadályozhat minden más egyidejű kommunikációt. Ez a hibajavítást és a sérült adatok újraküldését is megnehezíti.
  - Az ábrán látható, ahogy az adatok kisebb darabokra történő szegmentálása lehetővé teszi, hogy a különböző felhasználóktól származó, több különböző kommunikáció összefűzhető (multiplexelhető) legyen egyazon hálózaton. A szállítási rétegbeli protokollok által történő szegmentálás arra is módot kínál, hogy adatokat küldjünk, illetve fogadjunk, amikor több alkalmazást futtatunk egyidejűleg valamely számítógépen.
  - Szegmentáció nélkül mindössze egyetlen alkalmazás fogadhatna adatokat. Tekintsünk példaként egy online videoközvetítést, amely egyedüli kommunikációs folyamként teljes egészében felemésztené az átviteli közeget ahelyett, hogy megosztva használná. A videó

megtekintésének ideje alatt nem fogadhatnánk e-maileket, nem cseveghetnénk azonnali üzenetküldőn, és weboldalakra sem látogathatnánk el.

- Az egyes adatszegmensek azonosításához a szállítási réteg egy bináris adatokat tartalmazó fejléct ad minden szegmenshez. Ez a fejléc bitekből álló mezőket tartalmaz. A mezőkben szereplő értékek teszik lehetővé, hogy a szállítási rétegben működő protokollok különböző adatkommunikációs felügyeleti feladatokat lássanak el.
- A szállítási réteg felel a párbeszédek megbízhatósági feltételeinek biztosításáért. A különböző alkalmazások eltérő megbízhatósági feltételeket támasztanak.
- Az IP csak a struktúrával, a címzéssel és csomagok irányításával törődik. Az IP nem határozza meg, hogy miként történjen a csomagok szállítása és kézbesítése. A szállítási protokollok szabják meg, hogyan menjen végbe az üzenetek átvitele az állomások között. Ahogy az ábrán is látható, a TCP/IP két szállítási rétegbeli protokollt biztosít: a TCP-t (Transmission Control Protocol) és az UDP-t (User Datagram Protocol). A TCP/IP ezeket használja az állomások közötti kommunikáció biztosítására és az adatok átvitelére.
- A TCP-t egy megbízható, teljes körű szállítási rétegbeli protokoll, amely garantálja az összes adat célba érkezését. Ezzel szemben az UDP egy rendkívül egyszerű szállítási rétegbeli protokoll, amely semmilyen megbízhatóságot nem kínál.

Ahogy az már korábban is szerepelt, a TCP-t megbízható szállítási protokollnak tekintjük. Ez azt jelenti, hogy az alkalmazások közötti megbízható átvitel eléréséhez a TCP nyugtázott kézbesítést használ. A TCP-átvitel sok hasonlóságot mutat a forrástól a célig nyomon követhető postai csomagküldéssel. Ha egy FedEx (csomagküldő szolgálat) rendelést több szállítmányra bontanak szét, akkor az ügyfél online ellenőrizheti a kiszállítások sorrendjét.

A TCP esetében a megbízhatóságot három alapművelet biztosítja:

- Az adatszegmensek nyomon követése.
- A megérkezett adatok nyugtázása.
- A nem nyugtázott adatok újraküldése.

A TCP szegmensnek nevezett kis részekre darabolja szét az üzenetet. A szegmensek sorszámot kapnak, majd az IP-folyamathoz kerülnek csomagokká alakítás céljából. A TCP figyelemmel kíséri azokat a szegmens sorszámokat, melyeket az adott alkalmazástól már elküldött a célállomásnak. Ha a küldő nem kap nyugtát egy bizonyos időn belül, akkor feltételezi, hogy a szegmens elveszett, ezért azt újraküldi. Így az egész üzenetnek csak az elveszett része kerül újraküldésre, nem maga a teljes üzenet. A fogadó állomás esetében a TCP felelős az üzenetszegmensek összeillesztéséért és az alkalmazáshoz történő továbbításáért. Például az FTP (File Transfer Protocol) és a HTTP (Hypertext Transfer Protocol) is olyan alkalmazások, amelyek a TCP használatával gondoskodnak az adatok kézbesítéséről.

A küldőtől a fogadó állomásig továbbított TCP-szegmensek megtekintéséhez kattintsunk a Lejátszás gombra!

Ezek a folyamatok többletterhelést jelentenek a hálózati erőforrásokra nézve, a nyugtázás, a nyomon követés és az újraküldés miatt. A megbízhatóság biztosításához több vezérlési adat továbbítása szükséges a küldő és a fogadó állomások között. A vezérlési információk a TCP-fejlécben találhatók.

Mivel a TCP megbízhatóságot szolgáló funkciói sokkal robusztusabb kommunikációt folytatnak az alkalmazások között, így az átvitel során többletterhelést és lehetséges késést vonhatnak maguk után. Kompromisszumot kell találni a megbízhatóság, valamint a hálózati erőforrásokra rótt teher között. A megbízhatóság érdekében okozott többletterhelés csökkentheti bizonyos alkalmazások használhatóságát, vagy károsan befolyásolhatja a működésüket. Ilyen esetekben jobb választás lehet az UDP szállítási protokoll használata.

Az UDP csupán alapfunkciókat biztosít az adatszegmensek megfelelő alkalmazások között történő szállítása során, így nagyon csekély többletterhelést okoz és adatellenőrzést sem végez. Az UDP egy

"legjobb szándékú" (best-effort) szállítási protokollként ismert. Hálózatos környezetben a legjobb szándékú egyet jelent a megbízhatatlannal, mivel az adatok célba érkezésekor nincs semmiféle nyugtázás. Az UDP esetében nincs olyan szállítási rétegbeli folyamat, amely tájékoztatná a küldőt a sikeres kézbesítés tényéről.

Az UDP sokban hasonlít a normál, nem ajánlott postai levél kézbesítéséhez. A levél feladója ilyenkor nincs tisztában azzal, hogy tudja-e valaki fogadni az adott levelet, ugyanakkor a postahivatal sem felelős a levél nyomon követéséért vagy a feladó tájékoztatásáért, amennyiben a levél nem éri el végcélját.

A küldőtől a fogadó állomásig továbbított UDP-szegmensek megtekintéséhez kattintsunk a Lejátszás gombra!

Mind a TCP, mind pedig az UDP alkalmazott szállítási protokollok. Az alkalmazás által támasztott feltételektől függően valamelyik, esetenként mindkét szállítási protokoll használható. A fejlesztőknek kell kiválasztani, hogy melyik protokolltípus felel meg az alkalmazások által támasztott követelményeknek.

Némelyik alkalmazás esetében a sikeres feldolgozáshoz a szegmenseknek szigorúan meghatározott sorrendben kell megérkezniük. Más alkalmazások esetében az összes adatnak hiánytalanul meg kell érkezni, mielőtt annak bármely részét fel lehetne használni. Az előbbi két esetben a TCP szállítási protokollt kell alkalmazni. Például az adatbázisok, a webböngészők, az e-mail kliensek és a hasonló alkalmazások megkívánják, hogy minden adat az eredeti sorrendben és hiánytalanul érkezzen meg. Bármely elveszett adat sérülést okoz a kommunikációban, amely így hiányos és feldolgozhatatlan lesz. Épp ezért az ilyen alkalmazásokat úgy tervezték, hogy a TCP protokollt használják. Az így felmerülő hálózati többletterhelés ezekhez az alkalmazásokhoz szükségesnek tartják.

Megint más esetekben az alkalmazás elvisel ugyan bizonyos mértékű adatvesztést a hálózati átvitel során, de elfogadhatatlannak tekint bármilyen késést. Az ilyen alkalmazások számára a kisebb mértékű hálózati többletterhelés miatt az UDP jobb választás. Az UDP-t olyan alkalmazások részesítik előnyben, mint a videó- és audiofolyam, valamint az IP alapú hangtovábbítás (VoIP). Ezek esetében a nyugtázás lelassítaná a kézbesítést és az újraküldés sem kívánatos.

Például, ha a videofolyam egy vagy két szegmense nem érkezik meg, az csupán pillanatnyi zavart okoz a közvetítésben. Ilyenkor torzulhat a megjelenített kép, de a legtöbb esetben a felhasználó észre sem veszi. A másik esetben viszont az online videoközvetítés képe szét is esne, ha a céleszköznek minden elveszett adattal foglalkozni kellene, és így az újraküldésre történő várakozás kését okozna. Ilyenkor célravezetőbb lehet, ha a beérkezett szegmensek alapján előállítjuk a lehető legjobb képet, és lemondunk a megbízhatóságról.

Az UDP-t használó alkalmazásokra egy másik példa az internetrádió. Ha az üzenet egy része a hálózaton megtett út során elveszik, az nem kerül újratovábbításra. Ha néhány csomag hiányzik, a hallgató esetleg egy kis fennakadást hallhat a hangnál. Ha a TCP-t használnánk és az elvesztett csomagok újraküldésre kerülnének, az adattovábbítás szünetelne annak érdekében, hogy megkapjuk őket és ez a hangkimaradás még észrevehetőbb volna.

A TCP és az UDP közötti különbségek tényleges megértéséhez tisztában kell lenni azzal, hogy az egyes protokollok miként valósítanak meg bizonyos megbízhatóságot szolágló funkciókat, illetve hogyan követik nyomon a kommunikációt.

TCP (Transmission Control Protocol)

A TCP leírását először az RFC 793 szabványtervezetben adták meg. Ahogy az ábrán is látható, az adatok szegmentálását és ismételt összeállítását támogató alapfunkciókon felül a TCP az alábbiakat is biztosítja:

- Összeköttetés alapú párbeszéd, munkamenetek létesítésével.

- Megbízható kézbesítés.
- Adatok sorrendben történő újraépítése.
- Adatfolyam-vezérlés.

Munkamenet létesítése

A TCP egy összeköttetés alapú (connection-oriented, kapcsolatorientált) protokoll. Az összeköttetés alapú protokoll még a forgalom megkezdése előtt egyezteti, majd létrehozza a forrás- és céleszközök közötti állandó kapcsolatot (más néven munkamenetet). A munkamenet létrehozása felkészíti az eszközöket az egymással történő kommunikációra. A munkamenet létrehozása során az eszközök egyeztetik az adott idő alatt továbbítható forgalom mennyiségét, valamint szorosan felügyelik a két fél közötti adatkommunikációt. A munkamenet csak az összes kommunikáció befejeződése után szüntethető meg.

Megbízható kézbesítés

A TCP által használt módszer biztosítja az adatok megbízható szállítását. Hálózati szempontból a megbízhatóság azt jelenti, hogy a forrás által küldött minden egyes adatszelet célba érkezik. Számos oka lehet annak, hogy a hálózaton keresztül átvitt adatszeletek megsérülnek vagy teljesen elvesznek. A TCP azzal képes garantálni, hogy az összes szelet célba érjen, hogy a forráseszközzel újraküldeti az elveszett vagy megsérült adatokat.

A sorrend megtartásával történő kézbesítés

Mivel a hálózatok számos, különböző átviteli sebességgel rendelkező útvonalat kínálnak, előfordulhat, hogy az adatok rossz sorrendben érkeznek meg. A TCP a szegmensek megszámozásával és sorba rendezésével képes garantálni, hogy azok a megfelelő sorrendben legyenek újra összeállítva.

Adatfolyam-vezérlés (Flow Control)

A hálózati állomások korlátozott erőforrásokkal (pl.: memória, sávszélesség) rendelkeznek. Ha a TCP értesül ezen erőforrások túlzott mértékű igénybevételéről, kérheti, hogy a küldő alkalmazás csökkentse az adatátvitel sebességét. Ezt a TCP a forrás által küldött adatmennyiség szabályozásával éri el. Az adatfolyam-vezérléssel megelőzhető az adatszegmensek elvesztése a hálózaton, így elkerülhető az újraküldés.

Amint létrejön a TCP-kapcsolat, onnantól kezdve lehetséges a párbeszéd nyomon követése az adott munkameneten belül. Mivel a TCP képes az aktuális párbeszédek nyomon követésére, állapottartó protokollnak tekintjük. Az állapottartó protokoll olyan protokoll, amely nyomon követi a munkamenet minden változását. Például, ha TCP használatával történik az adatátvitel, a küldő arra számít, hogy a címzett majd nyugtázza az adatok fogadását. A TCP nyomon követi, hogy mely információk küldése, illetve nyugtázása történt meg. Ha az adatokat nem nyugtázták, a küldő feltételezi, hogy nem érkeztek meg, így újraküldi azokat. Az állapottartó kapcsolat a munkamenet létrehozásával indul, majd a munkamenet lezárásával ér véget.

Megjegyzés: Az állapotinformációk karbantartásához olyan erőforrásokra van szükség, amelyeket egy UDP-hez hasonló állapot nélküli protokoll nem igényel.

Ezen funkciók megvalósítása többletterhet jelent a TCP számára. Ahogy az ábrán is látható, minden egyes TCP-szegmens fejlécében 20 bájt szolgál az alkalmazási rétegbeli adatok beágyazása. Ez számottevően több, mint egy UDP-szegmens esetében, amely mindössze 8 bájt ilyen adatot tartalmaz. A többletteher az alábbiakat foglalja magában:

- **Sorszám (Sequence number, 32 bit)** - Az adatok ismételt összeállításához használják.

- **Nyugta sorszám (Acknowledgement number, 32 bit)** - Jelzi, hogy az adatok megérkeztek.

- **Fejléc hossza (Header length, 4 bit)** - "Adatkezdetként" is ismert, jelzi a TCP-szegmens fejlécének hosszát.

- **Fenntartott (Reserved, 6 bit)** - Ez a mező jövőbeli célokra van fenntartva.

- **Vezérlőbitek (Control bits, 6 bit)** - Olyan bitkódokat (más néven jelzőbiteket) tartalmaz, amelyek a TCP-szegmens célját és funkcióját jelzik.

- **Ablakméret (Window size, 16 bit)** - Jelzi az egyidejűleg fogadható szegmensek méretét.

- **Ellenőrzőösszeg (Checksum, 16 bit)** - A szegmens fejlécének és adattartalmának hibaellenőrzésére használják.

- **Sürgős (Urgent, 16 bit)** - Jelzi, ha az adatok sürgősek.

TCP-t használó alkalmazás például a webböngésző, az elektronikus levelezés vagy a fájlátvitel.

UDP (User Datagram Protocol)

Az UDP-t legjobb szándékú protokollnak tekintjük, amelynek leírását az RFC 768 szabványtervezetben adták meg. Az UDP egy "könnyűsúlyú" (lightweight) szállítási protokoll, amely az adatok szegmentálását és ismételt összeállítását kínálja ugyanúgy, mint a TCP, leszámítva ez utóbbi megbízhatóságát és adatfolyam-vezérlési képességét. Az UDP olyan egyszerű protokoll, amelyet gyakran azzal jellemeznek, hogy mit nem tud a TCP-hez képest.

Ahogy az ábrán is látható, az alábbi tulajdonságok jellemzik az UDP-t:

- **Összeköttetés-mentes (Connectionless)** - Az UDP nem létesít kapcsolatot az állomások között az adatok küldését és fogadását megelőzően.

- **Nem megbízható kézbesítés** - Az UDP nem kínál olyan szolgáltatásokat, amelyekkel garantálható lenne az adatok megbízható szállítása. Nincsenek benne olyan folyamatok, amelyek adatvesztés és -sérülés esetén az újraküldést kérnének a feladótól.

- **Az adatok helyreállítása nem sorrendben történik**- Esetenként előfordul, hogy az adatok nem a küldési sorrendben érkeznek meg. Az UDP semmilyen módszerrel nem rendelkezik az adatok eredeti sorrendjének helyreállításához. Az adatokat egyszerűen érkezési sorrendben kézbesíti az adott alkalmazásnak.

- **Nincs adatfolyam-vezérlés** - Az UDP semmilyen módszerrel nem rendelkezik a forrás által küldött adatmennyiség vezérléséhez, amellyel elkerülhető lenne a céleszköz túlterhelése. A forrás elküldi az adatokat. Ha ez a fogadó állomást túlságosan igénybe veszi, akkor az nagy valószínűséggel eldobja az adatokat, amíg nem szabadul fel elegendő erőforrás. Az UDP - a TCP-vel ellentétben - nem rendelkezik semmilyen módszerrel az eldobott adatok automatikus újraküldéséhez.
    - Ahogy az ábrán is látható, az UDP bár nem rendelkezik a TCP-nél alkalmazott megbízhatóságot segítő és adatfolyam-vezérlési módszerekkel, az alacsony többletterhet jelentő adatkézbesítés ideális szállítási protokollá teszi olyan alkalmazások számára, amelyek képesek elviselni némi adatvesztést. Az UDP-adategységeit datagramnak nevezik, melyeket a "legjobb szándékkal" továbbít. UDP-t használó alkalmazás például a DNS, az online videoközvetítés, valamint az IP-alapú hangátvitel (VoIP).
    - Az élő videó és hang hálózaton keresztüli továbbításával szemben támasztott egyik legfontosabb feltétel a gyors adatáramlás. A video- és hangalkalmazások képesek elviselni az adatvesztést úgy, hogy annak kicsi vagy egyáltalán nem érzékelhető hatása legyen, így tökéletesen illeszkednek az UDP-protokollhoz.

- Az UDP állapot nélküli protokoll, ami azt jelenti, hogy sem a kliens, sem pedig a szerver számára nem kötelező az adott munkamenet állapotának nyomon követése. Ahogy az ábrán is látható, az UDP nem foglalkozik a megbízhatóság és az adatfolyam-vezérlés kérdésével. Ha az adatok elvesznek vagy rossz sorrendben érkeznek, az UDP nem képes az adatok helyreállítására és sorbarendezésére. Amennyiben az UDP szállítási protokoll használata mellett mégis szükség van a megbízhatóságra, azt már az alkalmazásnak kell lekezelnie.
- A szállítási réteg feladata, hogy képes legyen több, egyidejűleg zajló, különböző szállítási igénnyel rendelkező kommunikáció szétválasztására és kezelésére. Vegyük példaként egy felhasználót, aki a számítógépén keresztül kapcsolódik a hálózatra. Ez a felhasználó egyidejűleg küld és fogad e-maileket, valamint azonnali üzeneteket, közben weboldalakat nézeget és IP-alapú (VoIP) telefonhívásokat is bonyolít. A futó alkalmazások mindegyike adatokat küld és fogad a hálózaton keresztül egyazon időben, pedig eltérő megbízhatósági elvárásaik vannak. Továbbá, a telefonhívás adatai nem kerülnek át a webböngészőbe, és az azonnali üzenetek szövege sem jelenik meg egy e-mailben.
- Megbízhatósági szempontból a felhasználók elvárják, hogy az e-mailek és a weboldalak hiánytalanul megérkezzenek, és teljes egészükben megjelenjenek, mivel csak így tekinthetők hasznos információnak. Az e-mailek és weboldalak betöltése során előforduló jelentéktelen késések általában elfogadhatók, ha a végeredmény egészben és hibátlanul jelenik meg. Ebben a példában a hálózat felügyeli a hiányzó információk újraküldését és pótlását, a végeredményt pedig egészen addig nem jeleníti meg, amíg meg nem érkezett minden, az összeállítás pedig nem hibátlan.
- Ezzel szemben, az esetenként előforduló kisebb hangkimaradásokat egy telefonbeszélgetés során elfogadhatónak tekintjük. Még ha el is veszik néhány szótöredék, a szövegkörnyezetből ki tudjuk következtetni a hiányzó hangokat, vagy megkérhetjük a másik személyt, hogy ismételje meg, amit mondott. Inkább ezt részesítjük előnyben, minthogy nagyobb késéseknek legyünk kitéve, ami a hiányzó szegmensek hálózat általi kezeléséből és újraküldéséből ered. Ebben a példában a felhasználó, nem pedig a hálózat végzi a hiányzó információk újraküldését és pótlását.
- Ahhoz, hogy a TCP és az UDP kezelje a változó feltételeket támasztó, egyidejűleg zajló párbeszédeket, mindkét szolgáltatásnak nyomon kell követni a különféle kommunikációt folytató alkalmazásokat (lásd ábra). Az alkalmazások adategységeinek megkülönböztetésére a TCP- és UDP-fejlécben találhatók olyan mezők, melyek azonosítják az alkalmazást. Ezek az egyedi azonosítók a portszámok.
- A forrás- és célport minden szegmens és datagram fejlécében szerepel. A forrásport egy szám, amely a helyi gépen futó, a kommunikációt kezdeményező alkalmazáshoz van rendelve. A célport pedig egy olyan, a kommunikációhoz tartozó szám, amely a távoli gépen futó célalkalmazáshoz van rendelve (lásd ábra).
- Ha egy üzenet kézbesítésre kerül TCP vagy UDP segítségével, a protokollok és a kért szolgáltatások azonosítása egy portszámmal történik. A port egy azonosítószám minden egyes szegmensben, amely a párbeszédek és a kért célszolgáltatások nyomon követésére szolgál. Minden üzenet, melyet az állomás elküld, tartalmaz egy forrás- és egy célportot.
- **Célport**
- A kliens elhelyez egy cél portszámot a szegmensben, hogy közölje a célszerverrel, milyen szolgáltatást kér. Például, a 80-as port a HTTP-t, vagyis a webszolgáltatást azonosítja. Amikor a kliens célportként a 80-as portot adja meg, az üzenetet fogadó szerver tudja, hogy webszolgáltatást kértek. Egy kiszolgáló egyidejűleg több szolgáltatást is kínálhat, például webszervert a 80-as porton, miközben FTP-kapcsolat létrehozását is engedélyezi a 21-es porton.
- **Forrásport**
- A forrás portszámot véletlenszerűen generálja a küldő a két eszköz közötti párbeszéd azonosítására. Ez egyidejűleg több párbeszédet tesz lehetővé. Például, egy eszköz számos HTTP-szolgáltatáskérést küldhet a webszervernek egyazon időben. Az elkülönített párbeszédek nyomon követése a forrásportokon alapszik.
- A forrás- és célportok a szegmensben kerülnek elhelyezésre. A szegmensek ezt követően egy IP-csomagba ágyazódnak be. Az IP-csomag tartalmazza a forrás és a cél IP-címét. A forrás- és célállomás IP-címének, valamint portszámainak kombinációját socket-nek vagy szoftvercsatornának nevezzük. A socket használatos a szerver és a kliens által kért szolgáltatás azonosítására. Naponta állomások ezrei kommunikálnak ezernyi különböző szerverrel. Ezeket a kommunikációkat a socket azonosítja.

- A szállítási réteg portszámai a hálózati réteg IP-címével kombinálva egyértelműen azonosítanak egy alkalmazást, mely egy meghatározott állomáson fut. A portszám és IP-cím kombinációt nevezzük socket-nek. Egy socket-pár, mely tartalmazza a forrás és a cél IP-címét, valamint portszámát, egyértelműen azonosítja a két állomás közötti párbeszédet.
- Egy kliens socket, 1099-es portszámmal például a következőképpen nézhet ki: 192.168.1.5:1099
- A webszerverhez tartozó socket pedig ilyen lehet: 192.168.1.7:80
- Ezek együttesen egy socket-párt alkotnak: 192.168.1.5:1099, 192.168.1.7:80
- A socket-ek létrehozásával a kommunikációs végpontok ismertté válnak, így így az adatok eljuthatnak az egyik állomás alkalmazásától egy másik állomás alkalmazásáig. A socket-ek teszik lehetővé, hogy a kliensállomáson futó folyamatokat, valamint hasonlóképpen egy szerverfolyamat kapcsolatait megkülönböztessük egymástól.
- Egy klienskérés forrásportjának generálása véletlenszerűen történik. A generált portszám a kérést indító alkalmazás címének felel meg. A szállítási réteg nyomon követi a forrásportot és a kérést kezdeményező alkalmazást, így a válasz a megfelelő alkalmazáshoz érkezik vissza. A kérést indító alkalmazás portszáma szerepel majd a szervertől visszaérkező válasz célportjaként.

A portszámok kiosztását az IANA (Internet Assigned Numbers Authority) végzi. Az IANA egy szabványügyi testület, amely a különféle címzési szabványok engedélyezéséért felel.

A portszámoknak különböző típusai vannak (lásd 1. ábra):

- **Jól ismert portok (0 és 1023 közötti számok)** - Ezek a szolgáltatások és alkalmazások részére fenntartott portszámok. Olyan, gyakran használt alkalmazásokhoz tartoznak, mint a HTTP (webszerver), az IMAP/SMTP (e-mail szerver), valamint a Telnet. Azzal, hogy a szerveralkalmazásokhoz jól ismert portokat rendelünk, a kliens oldali alkalmazásokat úgy lehet programozni, hogy a megadott porthoz kapcsolódva vegye igénybe a kapcsolódó szolgáltatást.

- **Bejegyzett portok (1024 és 49151 közötti számok)**- Ezek a felhasználói folyamatokhoz és alkalmazásokhoz rendelt portszámok. Főleg az ügyfél által telepített egyedi alkalmazások kapják, nem pedig olyan elterjedt programok, amelyekhez a jól ismert portszámok tartoznak. Ha ezek a portok nincsenek egy szerver erőforráshoz rendelve, akkor a kliens által dinamikusan kiválasztott forrásportként is használhatók.

- **Dinamikus vagy privát portok (49151 és 65535 közötti számok)** - Rövid életű portnak is nevezik, mivel általában akkor rendelik hozzá dinamikusan egy ügyfélalkalmazáshoz, amikor az kapcsolatot kezdeményez egy szolgáltatással. A dinamikus portot leggyakrabban a kliensalkalmazás azonosítására használják a kommunikáció során, míg az ügyfél a jól ismert port használatával kapcsolódik a szervertől igényelt szolgáltatáshoz. Szokatlan, ha a kliens a dinamikus tartományba eső célport használatával kapcsolódik egy szolgáltatáshoz (bár némelyik peer-to-peer fájlmegosztó programnál előfordul).

A 2. ábrán a TCP által használt néhány jól ismert és bejegyzett port látható. A 3. ábrán az UDP által használt néhány jól ismert és bejegyzett port látható.

TCP és UDP együttes használata

Némelyik alkalmazás TCP-t és UDP-t egyaránt használhat (lásd 4. ábra). Az UDP alacsony többletterhe teszi például lehetővé, hogy a DNS sok ügyfélkérést szolgáljon ki rendkívül rövid idő alatt. Ugyanakkor az is előfordulhat, hogy a kért információk megküldése a TCP megbízhatóságát igényli. A szolgáltatáshoz ebben az esetben az 53-as (jól ismert) portot használja mind a TCP, mind pedig az UDP.

Az alkalmazásokhoz rendelt portszámok aktuális listája megtalálható az IANA hivatalos weboldalán.

Néha szükséges tudni, hogy mely aktív TCP-kapcsolatok vannak nyitva, és melyek futnak egy hálózatba kötött állomáson. A netstat egy fontos hálózati segédprogram, mely ezen kapcsolatok

ellenőrzésére használható. A netstat kilistázza a használt protokollokat, a helyi címeket és portszámokat, a külső címeket és portszámokat, valamint a kapcsolatok állapotát.

A tisztázatlan TCP-kapcsolatok komoly biztonsági kockázatra utalhatnak, mivel azt jelezhetik, hogy valami vagy valaki csatlakozott a helyi állomáshoz. Továbbá a szükségtelen TCP-kapcsolatok értékes rendszererőforrásokat emészthetnek fel, így lerontják a számítógép teljesítményét. A netstat parancsot kell használni az állomás nyitott kapcsolatainak vizsgálatára, amennyiben a teljesítmény visszaesését érzékeljük.

Számos hasznos opció érhető el a **netstat** parancshoz. Kattintsunk az 1-5. ábrák gombjaira a **netstat** parancs különböző kimeneteinek megtekintéséhez.

Egy korábbi fejezet már ismertette, hogy miként lehet az alkalmazástól származó, a különböző rétegeken keresztül lefelé továbbított adatokból olyan PDU-kat létrehozni, amelyek ezt követően már továbbíthatók az átviteli közegen keresztül. A célállomásnál a folyamat megfordul, amíg az adatok fel nem érnek az alkalmazáshoz.

Némelyik alkalmazás rendkívül nagy mennyiségű adatot továbbít, amely egyes esetekben elérheti a több gigabájtot is. Ilyen nagy méretű adatokat nem lenne praktikus egy darabban továbbküldeni. Egyrészt amíg a fájl átküldése zajlana, semmilyen egyéb forgalom továbbítása nem lenne lehetséges. Másrészt, az ilyen nagy méretű fájlok átküldése percekig, vagy akár órákig is eltarthat. Ezen felül, bármilyen hiba előfordulásakor a teljes adatfájl elveszne, vagy újra kellene küldeni. A hálózati eszközök nem rendelkeznek olyan nagy méretű memóriapufferrel, amelyben tárolható lenne ilyen nagy mennyiségű küldött és fogadott adat. Ez a korlát az alkalmazott hálózati technológiától, valamint a használatban lévő átviteli közegtől függően eltérő lehet.

Az adatok szegmensekre történő szétbontásával biztosítható, hogy azok továbbítása az átviteli közeg korlátain belül maradjon. Továbbá garantálható, hogy a különböző alkalmazásokból származó adatok multiplexelhetők legyenek a közegen.

A TCP és az UDP eltérően szegmentál

Minden TCP-szegmens fejléce tartalmaz egy sorszámot, amely a szállítási réteg funkcióinak felhasználásával lehetővé teszi a szegmensek elküldési sorrendben történő összeállítását a célállomáson (lásd ábra). Ezzel garantálható, hogy a célalkalmazás a küldő szándékainak pontosan megfelelő formában kapja meg az adatokat.

Habár az UDP-t használó szolgáltatások szintén nyomon követik az alkalmazások közötti párbeszédeket, ezek egyáltalán nem foglalkoznak az információ átviteli sorrendjével, valamint a kapcsolat fenntartásával. Az UDP fejlécében nem szerepel sorszám. Az UDP egyszerűbb elgondoláson alapszik, így kisebb terhelést okoz a TCP-hez képest, ezért nagyobb adatátviteli sebességet eredményez.

Előfordulhat, hogy az információ nem sorrendben érkezik, mivel az egyes csomagok különböző útvonalakon juthatnak el a célhoz a hálózaton keresztül. Az UDP-t használó alkalmazásnak tolerálnia kell, ha az adatok nem az elküldés sorrendjében érkeznek meg.

A TCP és az UDP közötti alapvető különbség a megbízhatóság. A TCP-kommunikáció megbízhatóságát az összeköttetés alapú munkamenetek adják. Mielőtt egy TCP-t használó állomás adatokat küldene egy másik állomásnak, a TCP elindít egy kapcsolatlétesítési folyamatot a cél irányába. Az állapottartó kapcsolat lehetővé teszi a munkamenet, más néven az állomások közötti kommunikációs adatfolyam nyomon követését. Ez a folyamat garantálja, hogy mindegyik állomás tudatosan felkészüljön a kommunikációs adatfolyamra. A TCP-párbeszédhez kétirányú munkamenet létrehozására van szükség az állomások között, amit az ábrán is látható.

Miután a kapcsolat felépült, és az adatátvitel megkezdődik, a cél nyugtát küld a beérkezett szegmensekről a forrásnak. Ezek a nyugták adják a TCP-kapcsolat megbízhatóságának alapját. Ha a forrás megkap egy nyugtát, akkor tudja, hogy a kézbesítés sikeresen megtörtént, és befejezheti a

kérdéses adatok nyomon követését. Ha a küldő nem kap nyugtát egy előre meghatározott időn belül, akkor újraküldi az adatokat.

A TCP használatból fakadó többletteher egy része a nyugtázásokból és újraküldésekből származó hálózati forgalom. A kapcsolatok létrehozása további szegmensek cseréjét igényli, mely szintén többletterhelést okoz. Többletterhet jelent még az egyes állomásokra nézve annak nyomon követése, hogy mely szegmensek várnak nyugtázásra, valamint melyeket kell újraküldeni.

Az alkalmazási folyamatok futtatása szervereken történik. Egy önálló szerver is lehetővé teszi több alkalmazás egyidejű futtatását. Ezek a folyamatok egészen addig várnak, amíg egy kliens kommunikációt nem kezdeményez valamilyen információ vagy egyéb szolgáltatás igénybevételének céljából.

A szerveren futó minden egyes alkalmazási folyamat esetében be kell állítani egy portszám használatát, amely történhet alapértelmezés szerint, de végezheti a rendszergazda is. Egy szervernek nem lehet két olyan szolgáltatása, amely ugyanannak szállítási rétegbeli protokollnak (TCP vagy UDP) ugyanahhoz portjához van rendelve. Egy webszolgáltatást és fájlátvitelt egyaránt kínáló szerveren nem állítható be mindkét alkalmazás számára ugyanazon port használata (pl.: a TCP 8080-as portja). Az aktív szerver oldali alkalmazásokhoz rendelt konkrét portokat nyitott portnak tekintjük, ami azt jelenti, hogy a szállítási réteg elfogadja és feldolgozza az ezekre a portokra küldött szegmenseket. Bármely bejövő ügyfélkérés elfogadásra kerül, amelyet megfelelő socket címmel láttak el, az adatok pedig a szerveralkalmazáshoz lesznek továbbítva. Egy szerveren számos port lehet egyidejűleg nyitva, minden aktív szerveralkalmazáshoz egy. Gyakori, hogy egy kiszolgáló egyszerre több szolgáltatást is kínál, például FTP- és webszerverként is működik.

A szerverbiztonság javításának egyik módja, hogy hozzáférést kizárólag olyan portokhoz engedélyezünk, melyek szolgáltatásait csak jogosultsággal rendelkező felhasználók vehetik igénybe.

A TCP kliens/szerver műveleteiben érintett forrás- és célportok tipikus kiosztásához nézzük végig az ábrákat!

Egyes kultúrákban, ha két személy találkozik, kézfogással üdvözlik egymást. Ilyenkor mindkét fél tudja, hogy a kézfogás a baráti üdvözlés jele. A hálózati kapcsolatok is hasonlóan működnek. Az első kézfogás szinkronizálást kér. A második kézfogás nyugtázza az első szinkronizálási kérést, majd egyezteti az összeköttetés paramétereit az ellenkező irányban is. A harmadik kézfogási szegmens egy nyugta a célállomás számára, amely jelzi, hogy mindkét fél egyetért az összeköttetés létrejöttében.

Ha két állomás TCP használatával kommunikál egymással, még az adatcsere megkezdése előtt létre kell hozni a kapcsolatot. Miután a kommunikáció befejeződött, a munkameneteket le kell zárni, a kapcsolatot pedig bontani kell. A kapcsolathoz és munkamenethez tartozó mechanizmusok adják a TCP megbízhatóságát. A TCP kapcsolat létrehozásának és bontásának lépéseit megtekinthetjük az ábrán.

Az állomások nyomon követik az egyes adatszegmenseket egy munkameneten belül, valamint a TCP-fejlécben szereplő adatok alapján arról is információt cserélnek, hogy mely adatok érkeztek meg. A TCP egy full-duplex protokoll, ahol minden egyes kapcsolatnak két, egyirányú kommunikációs adatfolyam, más néven munkamenet felel meg. A kapcsolat létrehozásához az állomásoknak egy háromfázisú kézfogást kell végrehajtaniuk. A TCP-fejlécben lévő vezérlőbitek jelzik a kapcsolat állapotát és előrehaladását. A háromfázisú kézfogás:

- megállapítja a céleszköz jelenlétét a hálózaton
- ellenőrzi, hogy a céleszköz aktív szolgáltatással rendelkezik, amely elfogadja az olyan célportra érkező kéréseket, amelyet a kezdeményező kliens használni kíván a munkamenet idejére
- tájékoztatja a céleszközt arról, hogy a küldő kliens kapcsolatot kíván létrehozni az adott porton

A TCP-kapcsolatok esetében mindig a kliens számítógép kapcsolódik a szerverhez. A TCP-kapcsolat létrehozásának három lépése:

1. A kezdeményező ügyfél egy kliens-szerver irányú kapcsolat létrehozását kéri a kiszolgálótól.

2. A kiszolgáló nyugtázza a kliens-szerver irányú kapcsolat létrehozását, egyúttal kéri egy szerver-kliens irányú kapcsolat létrehozását is.

3. A kezdeményező ügyfél nyugtázza a szerver-kliens irányú kapcsolat létrehozását.

A TCP-kapcsolat létrehozásának megtekintéséhez kattintsunk az ábrán látható gombokra.

A háromfázisú kézfogás folyamatának megértéséhez vessünk egy pillantást a két állomás között átküldött különféle értékekre. A TCP-szegmens fejlécén belül hat olyan 1 bites mező szerepel, amely a TCP-folyamatok kezelésére használatos. Ezek az alábbi mezők:

- **URG** - sürgősségi jelző
- **ACK** - nyugtázás
- **PSH** - áttöltési funkció
- **RST** - a kapcsolat alaphelyzetbe állítása
- **SYN** - sorszámok szinkronizálása
- **FIN** - nincs több adat a küldőtől

A háromfázisú kézfogás elemzéséhez az ACK és a SYN mezők fontosak.

A háromfázisú kézfogás működése tanulmányozható például a Wireshark protokollelemző szoftver kimenetének felhasználásával.

1. A kezdeményező ügyfél egy kliens-szerver irányú kapcsolat létrehozását kéri a szervertől.

A háromfázisú kézfogást a TCP-kliens egy olyan szegmens elküldésével kezdeményezi, amelyben a SYN jelzőbit értéke 1, ezzel jelezve a fejlécben szereplő sorszám mező (sequence number) kezdőértékét. A kezdősorszám (ISN) kiválasztása véletlenszerűen történik, a kliens és szerver közötti adatáramlás nyomon követésének megkezdésére szolgál. Ahogy az adatkommunikáció folytatódik a kliens és a szerver között, az egyes szegmensek fejlécében szereplő ISN értéke az átküldött minden egyes adatbájt után eggyel növekszik.

Ahogy az ábrán is látható, a protokollelemző kimenetében látszik a SYN vezérlőbit, valamint a relatív sorszám.

A SYN vezérlőbit beállítása megtörtént, a relatív adatsorszám pedig 0. Az ábrán mutatott protokoll elemzőben decimális formában láthatók a relatív sorszám és a nyugta értékek, melyek igazából 32 bites bináris számok (a könnyebb olvashatóság érdekében hexadecimális formában).

2. A szerver nyugtázza a kliens-szerver irányú kapcsolat létrehozását, egyúttal kéri egy szerver-kliens irányú kapcsolat létrehozását is.

A kliens-szerver irányú munkamenet létrehozásához a TCP-szervernek nyugtáznia kell a klienstől jövő SYN szegmens beérkezését. Ennek érdekében a szerver visszaküld egy szegmenset a kliensnek, amelyben az ACK jelzőbit 1-es értéke mutatja, hogy a küldött nyugtasorszám érvényes. A

szegmensben szereplő jelzőbit segítségével a kliens felismeri a nyugtát, azaz, hogy a szerver megkapta a TCP-klienstől érkező SYN-t.

A nyugta számát tartalmazó mező értéke egyenlő az ISN + 1 értékkel. Ezzel létrejön a kliens-szerver irányú munkamenet. A kapcsolat egyensúlyának megőrzéséhez az ACK jelzőbit beállítva marad. Emlékezzünk vissza, hogy a kliens és szerver között zajló párbeszéd valójában két egyirányú munkamenet: az egyik a klienstől a szerver felé, a másik a szervertől a kliens felé. A háromfázisú kézfogás második lépésében a szervernek kell választ kezdeményeznie a kliens felé. Ennek a munkamenetnek a megkezdéséhez a szerver a klienshez hasonlóan egy SYN jelzőbitet használ, vagyis a szerver-kliens irányú munkamenet létrehozásához beállítja a fejlécben szereplő vezérlőbitet. A SYN jelzőbit 1-es értéke azt jelzi, hogy a sorszám mező kezdőértéke a fejlécben szerepel. Ez az érték használatos a munkamenetben zajló adatáramlás nyomon követésére, a szervertől vissza a kliens felé.

A protokollelemző kimenete mutatja, hogy az ACK és SYN vezérlőbit beállítása megtörtént, valamint megjeleníti a relatív sorszámot és nyugtaszámot (lásd ábra).

3. A kezdeményező kliens nyugtázza a szerver-kliens irányú kapcsolat létrehozását.

Végül a TCP-kliens egy ACK-t tartalmazó szegmenssel válaszol a szerver által küldött TCP SYN üzenetre. Ebben a szegmensben sem szerepel felhasználói adat. A nyugta számát tartalmazó mező értéke mindig eggyel több, mint a szervertől kapott ISN értéke. Miután mindkét munkamenet létrejött a kliens és a szerver között, minden további kiegészítő szegmens küldése esetén megtörténik az ACK jelzőbit beállítása.

A protokollelemző kimenete mutatja, hogy az ACK vezérlőbit beállítása megtörtént, valamint megjeleníti a relatív sorszámot és nyugtaszámot (lásd ábra).

Az adathálózat biztonsága növelhető az alábbi módszerekkel:

- a TCP-kapcsolatok létrehozásának megtagadásával
- csak meghatározott szolgáltatások igénybevételére létrehozott munkamenetek engedélyezésével
- kizárólag a már létrejött munkamenetek részét képező forgalom engedélyezésével

A fenti biztonsági intézkedések alkalmazhatók az összes TCP-kapcsolatra vagy csupán egy részükre.

A kapcsolat lezárásához be kell állítani a szegmens fejlécében található FIN vezérlőbit értékét. Az egyes, egyirányú TCP-munkamenetek megszüntetéséhez kétirányú kézfogást kell használnunk, amely egy FIN és egy ACK szegmensből áll. Ezért egy TCP által támogatott párbeszéd bontásához, mindkét munkamenetet meg kell szüntetni, amelyhez négy adatcsere szükséges (lásd 1. ábra).

Megjegyzés: A magyarázat során az egyszerűség kedvéért a kliens és szerver fogalmakat használjuk, de a bontás folyamatát bármely, nyitott munkamenettel rendelkező állomás kezdeményezheti.

1. Amikor már nincs több átküldendő adat, a kliens egy olyan szegmenset küld, amelyben a FIN jelzőbit beállítása megtörtént.

2. A kliens-szerver irányú munkamenet bontásához a szerver egy ACK üzenet küldésével nyugtázza a FIN üzenet megérkezését.

3. A szerver-kliens irányú munkamenet bontásához a szerver egy FIN üzenetet küld a kliensnek.

4. A kliens válaszként egy ACK üzenet küldésével nyugtázza a szervertől érkező FIN üzenetet.

Amikor már nincs szállítandó adat, a kliens beállítja a szegmens fejlécében szereplő FIN jelzőbitet. Ezután a kapcsolat szerver oldali vége egy normál, adatokat tartalmazó szegmenssel válaszol, amelyben az ACK jelzőbittel érvényesített nyugtaszám igazolja, hogy minden bájt megérkezett. Miután az összes szegmens nyugtázása megtörtént, a munkamenet is lezárul.

Az ellenkező irányú munkamenet bontása is ugyanígy történik. A fogadó fél a forrásnak küldött szegmens fejlécében szereplő FIN jelzőbit beállításával közli, hogy nincs több küldendő adat. A válaszként küldött nyugta igazolja, hogy az összes adatbájt megérkezett, a munkamenet pedig lezárul.

A szegmens fejlécében szereplő FIN és ACK vezérlőbitek beállítását, ezáltal egy HTTP-kapcsolat lebontását megtekinthetjük a 2. és 3. ábrán.

A kapcsolat háromfázisú kézfogással szintén megszüntethető. Amikor már nincs több átküldendő adat, a kliens egy FIN üzenetet küld a szervernek. Amennyiben a szervernél sincs több küldendő adat, küldhet olyan választ, amelyben mindkét vezérlőbit beállítása megtörtént, egyesítve ezzel két lépést (FIN, ACK). A kliens erre egy ACK üzenettel válaszol.

A szegmensek sorrendjének helyreállítása

Ha egy szolgáltatás TCP-vel küld adatokat, elképzelhető, hogy a szegmensek nem a megfelelő sorrendben érnek célba. Ahhoz, hogy a fogadó fél megértse az eredeti üzenetet, a szegmensekben lévő adatokat ismét az eredeti sorrendben kell összeállítani. Ennek érdekében minden egyes csomag fejlécében szerepel egy sorszám.

A kapcsolat felépítése során a kezdősorszám (ISN) is értéket kap. Az ISN tulajdonképpen a fogadó alkalmazásnak átvitt bájtok kezdőértéke az adott munkamenet során. A kapcsolat ideje alatt továbbított adatoknak megfelelően a sorszám értéke is növekszik az átvitt bájtok számával. Az adatbájtok ilyenfajta nyomon követése lehetővé teszi az egyes szegmensek egyedileg történő azonosítását és nyugtázását. Így a hiányzó szegmensek szintén azonosíthatók.

Ahogy az ábrán is látható, a megbízhatóságot a szegmensek sorszámai azzal garantálják, hogy jelzik, miként kell ismételten összeállítani és sorba rendezni a megérkezett szegmenseket.

A fogadó TCP-folyamat a szegmensek adatait egy vételi pufferbe helyezi át. A szegmensek a sorszámuknak megfelelő sorrendben kerülnek a pufferbe, majd onnan az ismételt összeállítást követően az alkalmazási rétegbe. A nem folytonos sorszámmal érkező szegmenseket későbbi feldolgozás céljából visszatartják. Amikor megérkeznek a hiányzó bájtokat tartalmazó szegmensek, akkor ezek is sorban feldolgozásra kerülnek.

A szegmensek beérkezésének nyugtázása

A TCP egyik feladata, hogy garantálja minden egyes szegmens célba érkezését. A célállomáson működő TCP-szolgáltatások nyugtázzák a forrásalkalmazás által küldött adatokat.

A sorszám (sequence number, SEQ) és a nyugtaszám (acknowledgement number, ACK) együttesen használatos az átvitt szegmensekben lévő adatbájtok beérkezésének nyugtázására. A SEQ értéke mutatja a munkamenet során továbbított bájtok relatív számát, beleértve a jelenlegi szegmens bájtjait is. A TCP az ACK szám visszaküldésével jelzi a forrásnak, hogy melyik bájt érkezésére számít legközelebb. Ezt várományos nyugtázásnak nevezzük.

A forrás értesül, hogy célba érkezett az adatfolyam összes bájtja, egészen az ACK szám által jelzett bájtig, de azt már nem beleértve. A forrás állomás várhatóan egy olyan szegmenset küld legközelebb, amelynek sorszáma megegyezik az ACK értékével.

Ne feledjük, hogy minden egyes kapcsolat valójában két egyirányú munkamenetnek felel meg! Ezért a SEQ és az ACK értéke mindkét irányban továbbításra kerül.

Az ábrán látható példában a bal oldali állomás adatokat küld a jobb oldali állomásnak. Jelen munkamenet során egy 10 adatbájtot tartalmazó szegmens átküldése zajlik, amelynek fejlécében az 1-es sorszám (Seq) szerepel.

A fogadó állomás a 4. rétegbe érkező szegmensről megállapítja, hogy a sorszáma 1, adattartalma pedig 10 bájt. Ezután visszaküld egy szegmenset a bal oldali állomásnak, amelyben nyugtázza az adatok beérkezését. Ebben a szegmensben az ACK értéke 11-re van állítva, jelezvén, hogy az állomás a 11-es számú adatbájt beérkezésére számít legközelebb. Amikor a küldő állomás megkapja a nyugtát, már indíthatja is a következő adatszegmens küldését, amely a 11-es bájttal kezdődik.

A példát szemügyre véve láthatjuk, hogy amennyiben a küldő állomásnak meg kellene várni a nyugtát minden beérkező 10 bájt után, az rengeteg többletterhet jelentene a hálózatra nézve. A nyugtázásból adódó többletterhelés csökkentésének érdekében számos adatszegmens átküldhető, de nyugtázásuk egyetlen TCP-üzenettel történik meg az ellenkező irányba. Az ilyen nyugta egy olyan ACK értéket tartalmaz, amely a munkamenet során beérkezett összes bájt számán alapul. Például, ha a sorszám 2000-rel kezdődik, és 10 egyenként 1000 bájt méretű szegmens érkezik, akkor a 12001-es ACK értéket kell visszaküldeni a forrásnak.

Azt az adatmennyiséget, amelyet a forrás átküldhet, mielőtt nyugtát kellene kapnia, ablakméretnek (window size) nevezzük. Az ablakméret a TCP-fejléc egyik mezője, amely lehetővé teszi az adatfolyam-vezérlést.

A szegmensvesztés kezelése

Bármennyire alaposan is van egy hálózat megtervezve, alkalmanként előfordul adatvesztés. Ezért a TCP módszereket biztosít a szegmensvesztések kezelésére. Ezek közé tartozik a nem nyugtázott adatszegmensek újraküldésének mechanizmusa is.

A célállomás TCP-t használó szolgáltatása rendszerint csak a folyamatos sorszámú bájtokat nyugtázza. Ha egy vagy több szegmens hiányzik, kizárólag az első folyamatos bájtsorozat nyugtázása történik meg. Például, ha a beérkezett szegmensek sorszáma 1500 és 3000, valamint 3400 és 3500 között van, az ACK értéke 3001 lesz. Ennek oka, hogy a 3001 és 3399 közötti SEQ számmal rendelkező szegmensek nem érkeztek meg.

Ha a forrásállomás TCP-je nem kap nyugtát egy előre megadott időn belül, akkor visszatér az utolsóként beérkező ACK értékéhez, és újraküldi az adatokat attól a ponttól kezdve. Az újraküldés folyamatát nem rögzíti a szabványtervezet, így az mindig a TCP konkrét megvalósításától függ.

A TCP egyik tipikus megvalósításában az állomás elküld egy szegmenset, a szegmens másolatát az újraküldési sorba helyezi, majd elindít egy időzítőt. Amikor megérkezik az adatok nyugtázása, a szegmens törlésre kerül a sorból. Ha nem érkezik meg a nyugta az időzítő lejártáig, megtörténik a szegmens újraküldése.

Az elveszett szegmensek újraküldését szemléltető animáció megtekintéséhez kattintsunk a Lejátszás gombra!

Az állomások manapság alkalmazzák a szelektív nyugtázásnak (SACK) nevezett opcionális lehetőséget is. Amennyiben mindkét állomás támogatja a szelektív nyugtázást, akkor a célállomás a nem folyamatos szegmensekben érkező bájtokat is nyugtázhatja, a másik oldalon pedig csak a hiányzó adatokat kell újraküldeni.

Adatfolyam-vezérlés

A TCP az adatfolyam-vezérléshez is kínál módszereket. Az adatfolyam-vezérlés azzal segíti a TCP-átvitel megbízhatóságának megőrzését, hogy mindig az adott munkamenethez igazítja az adatátvitel sebességét a forrás és a cél között. A megvalósítás része az is, hogy korlátozva van az egyszerre továbbítható adatszegmensek mennyisége, valamint az újabb adat küldése a kézbesítést igazoló nyugta visszaérkezéséig.

Az adatfolyam-vezérlés megvalósításának első lépéseként a TCP megállapítja a céleszköz által elfogadható adatszegmensek mennyiségét. Ennek céljából a TCP-fejléc tartalmaz egy 16 bites mezőt, amelynek ablakméret (window size) a neve. Ez nem más, mint egy adott TCP-munkamenet céleszköze által egyszerre fogadható és feldolgozható bájtok száma. A kezdeti ablakméret a beállítása a munkamenet felépítésekor, a forrás és cél közötti háromfázisú kézfogás alkalmával történik. Mihelyt megállapodik a két fél, a forráseszköznek az ablakméret alapján korlátoznia kell a céleszköznek küldött adatszegmensek mennyiségét. A forráseszköz kizárólag az adatszegmensek kézbesítését igazoló nyugta visszaérkezése után küldhet további adatokat az adott munkamenet során.

Amíg késik a nyugta visszaérkezése, addig a forrás nem küld további szegmenseket. Olyan időszakokban, amikor torlódik a hálózati forgalom, vagy a fogadó állomás erőforrásai túlságosan le vannak terhelve, nagyobb lehet a késés mértéke. Ahogy a késés egyre növekszik, úgy csökken az adott munkamenet tényleges adatátviteli sebessége. Ha mindegyik munkamenet adatátvitelét lassítjuk, az csökkenti az erőforrás-ütközések számát a hálózaton és a sok munkamenettel rendelkező céleszközön.

Az ábrán megtekinthető az ablakméret, valamint a nyugtázás egyszerűsített ábrázolása. A példában szereplő TCP-munkamenet kezdeti ablakmérete 3000 bájtra van állítva. Ha a feladó végzett 3000 bájt elküldésével, megvárja az ezekhez a bájtokhoz tartozó nyugta visszaérkezését, újabb adatokat csak ezt követően küld a munkamenet keretében. Miután a feladó megkapta a fogadó fél nyugtáját, további 3000 bájt küldését kezdheti meg.

A TCP azért használ ablakméreteket, hogy megpróbálja az átviteli sebességet a hálózat és a céleszköz által támogatott maximumra feltornászni, ugyanakkor minimalizálni a veszteségek és újraküldések számát.

Az ablakméret csökkentése

Az adatfolyam-vezérlés egy másik módja, ha dinamikus ablakméretet használunk. Amikor a hálózati erőforrások túl vannak terhelve, a TCP csökkenti az ablakméretet, így sokkal gyakrabban igényli a beérkezett szegmensek nyugtázását. Ez ténylegesen lassítja az átviteli sebességet, mivel a forrásnak is sokkal gyakrabban kell várnia a nyugták visszaérkezésére.

A fogadó állomás az ablakméret értékének elküldésével jelzi a feladónak, hogy mennyi bájt fogadására áll készen. Ha a fogadónak le kell lassítania a kommunikáció sebességét, például a korlátozott puffermemória miatt, a nyugtázás részeként kisebb ablakméretet küld vissza a forrásnak.

Ha a fogadó állomásnál torlódás lép fel, válaszolhat a feladónak egy csökkentett ablakméretet meghatározó szegmens elküldésével (lásd ábra). A képen az látszik, hogy egy szegmens elveszett. A fogadó fél csökkentette a válasz üzenet TCP-fejlécben szereplő ablak mező értékét (window size) 3000-ről 1500-ra a jelenlegi párbeszéd során. Ebből kifolyólag a feladó is 1500-ra csökkentette az ablakméretet.

Ha a további átvitel során nem történik adatvesztés és az erőforrások sincsenek korlátozva, a fogadó fél elkezdi növelni az ablak mező értékét. Ez csökkenti a hálózat többletterhelését, mivel így kevesebb nyugta elküldésére van szükség. Az ablakméret folyamatosan növekszik, amíg nem történik adatvesztés, az viszont az ablakméret csökkenését vonja maga után.

Az ablakméret dinamikus növelése, illetve csökkentése a TCP egyik állandó folyamata. A kimagaslóan jól működő hálózatokban egészen nagy ablakméretek is előfordulhatnak, mivel nem történik adatvesztés. Az olyan hálózatokban viszont, ahol az alapvető infrastruktúra komoly igénybevételnek van kitéve, az ablakméret valószínűleg kicsi marad.

Az UDP egyszerű protokoll, amely a szállítási réteg alapfeladatait látja el. Mivel nem összeköttetés-alapú és nem használja a TCP kifinomult sorszámozási, újraküldési és folyamatszabályozási mechanizmusait, sokkal kisebb többletterhelést okoz.

Ez persze nem jelenti azt, hogy az UDP-t használó alkalmazások megbízhatatlanok vagy maga a protokoll alsóbbrendűbb. Csak annyit jelent, hogy a többlet funkciókat nem a szállítási réteg biztosítja, hanem szükség esetén valahol máshol kell megvalósítani.

Bár egy tipikus hálózat összes UDP forgalma viszonylag kicsi a többihez képest, a következő alkalmazási rétegbeli protokollok mind az UDP-t használják:

- Domain Name System (DNS)
- Simple Network Management Protocol (SNMP)
- Dynamic Host Configuration Protocol (DHCP)
- Routing Information Protocol (RIP)
- Trivial File Transfer Protocol (TFTP)
- Voice over IP (VoIP)
- Online játékok

Néhány alkalmazás elvisel kismértékű adatvesztést, ilyenek például az online játékok vagy a VoIP. Ha ezek a programok TCP-t használnának, nagymértékű késéseket tapasztalnánk, amíg a TCP észleli az adatvesztést és újraküldi azokat. Az ilyen késések sokkal károsabban hatnak az alkalmazás teljesítményére, mint a kisebb adatvesztések. Némelyik alkalmazás, például a DNS, egyszerűen újraküldi a kérést, ha nem érkezik válasz, ezért nincs is szükség a TCP által garantált üzenetkézbesítésre.

Az ilyen alkalmazások számára rendkívül kívánatos az UDP alacsony többletterhelése.

Mivel az UDP összeköttetés nélküli protokoll, ezért a kommunikáció megkezdése előtt nem jönnek létre munkamenetek, mint a TCP esetében. Az UDP-ről azt is mondják, hogy tranzakció alapú, vagyis ha egy alkalmazás adatot szeretne küldeni, akkor egyszerűen elküldi azokat.

Sok UDP-t használó alkalmazás olyan kicsi adatmennyiséget küld, amely belefér egyetlen szegmensbe. Ugyanakkor, néhány alkalmazás lényegesen nagyobb adatmennyiséget továbbít, amelyet több szegmensre kell szétbontani. Az UDP adategységét datagramnak nevezzük, bár a szállítási réteg adategységeinek leírásánál a szegmens és a datagram fogalmakat felváltva használjuk.

Amikor több datagramot küldünk egy célállomásnak, azok különböző útvonalat választhatnak, így előfordulhat, hogy az adatok rossz sorrendben érkeznek meg. Az UDP nem követi nyomon a sorszámokat, mint a TCP. Ahogy az ábrán is látható, az UDP semmilyen módszerrel nem rendelkezik a datagramok eredeti sorrendjének helyreállításához.

Ezért az UDP a kapott sorrendben állítja össze az adatokat, majd továbbküldi azokat az alkalmazásnak. Ha az adatsorrend lényeges az alkalmazás szempontjából, akkor az alkalmazásnak kell meghatározni a helyes sorrendet, valamint az adatok feldolgozásának módját.

Hasonlóan a TCP-hez, az UDP-t használó szerveralkalmazásokhoz is jól ismert vagy bejegyzett portszámok vannak hozzárendelve. Amikor ezek az alkalmazások és folyamatok futnak egy szerveren, akkor csak a hozzájuk rendelt portszámra illeszkedő adatokat fogadják el. Ha olyan datagram érkezik, amelyet ezen portok egyikének címeztek, az UDP a portszám alapján továbbítja az adatokat a megfelelő alkalmazáshoz. A TCP-hez hasonlóan, a kliens/szerver kommunikációt itt is egy kliensalkalmazás kezdeményezi, amely adatokat kér egy szerverfolyamattól. Az UDP kliensfolyamat véletlenszerűen választ egy portszámot a dinamikus portszámok tartományából, amelyet később a

párbeszéd forrásportjaként használ. A célport általában egy szerverfolyamathoz rendelt jól ismert vagy bejegyzett portszám.

A biztonsághoz a véletlenszerűen választott portszámok is hozzájárulnak. Ha a port kiválasztása kiszámítható minta alapján történik, a támadók lényegesen egyszerűbben szerezhetnek a klienshez hozzáférést úgy, hogy megpróbálnak a legnagyobb valószínűséggel nyitva lévő porthoz kapcsolódni.

Mivel az UDP esetében nem jön létre munkamenet, ezért a datagramok létrehozása rögtön azután megkezdődhet, ahogy készen állnak az adatok és megvannak a portok is. A datagramokat ezután továbbítani kell a hálózati rétegbe, hogy címzés után kiküldésre kerüljenek a hálózatba.

Miután a kliens kiválasztotta a forrás- és célportot, a tranzakció során végig ugyanaz a portpár szerepel az összes datagram fejlécében. Ami a szervertől a klienshez visszaérkező adatokat illeti, a datagramok fejlécében szereplő forrás- és célportok felcserélődnek.

Az UDP kliensfolyamatok részleteinek megvizsgálásához nézzük meg az 1-5 ábrákat!

A TCP megbízhatóságát és egyéb szolgáltatásait számos alkalmazás megköveteli. Ezek olyan alkalmazások, amelyek elviselik a TCP által okozott többletterhelésből adódó kisebb mértékű késést vagy teljesítménycsökkenést.

Emiatt a TCP leginkább olyan alkalmazások esetében használható, ahol fontos a megbízható szállítás és megengedett némi késés. A TCP kiváló példája annak, hogy a TCP/IP protokollkészlet különböző rétegeinek milyen konkrét szerepe van. Mivel a TCP kezeli az adatfolyam szegmensekre bontásához kapcsolódó összes feladatot, a megbízhatóságot, az adatfolyam-vezérlést, valamint a szegmensek sorrendjének helyreállítását, ezt a terhet leveszi az alkalmazások válláról. Az alkalmazás egyszerűen átküldheti az adatfolyamot a szállítási rétegbe, majd használja a TCP szolgáltatásait.

Az ábra néhány példát tartalmaz a TCP-t használó, jól ismert alkalmazásokra:

- HTTP
- FTP
- SMTP
- Telnet

Az alkalmazásoknak három olyan típusa létezik, amelyek számára az UDP a legjobb választás:

- Alkalmazások, amelyek elviselnek némi adatvesztést, de megkövetelik, hogy alig vagy egyáltalán ne legyen késés.
- Alkalmazások, amelyek egyszerű kérés-válasz tranzakciókat használnak.
- Egyirányú kommunikáció, ahol a megbízhatóságot vagy meg sem követeljük, vagy le tudja kezelni az alkalmazás.

Számos videó- és multimédiás alkalmazás használja az UDP-t, ilyen például a VoIP és az IPTV. Ezek az alkalmazások oly módon képesek elviselni az adatvesztést, hogy annak nincs vagy csak minimálisan érzékelhető hatása van. A TCP megbízhatósági funkciói némi késést eredményeznek, ami érzékelhető lehet a beérkező hang és videó minőségében.

Az egyszerű kérés-válasz tranzakciókat használó alkalmazások számára szintén jó választás lehet az UDP. Ilyenkor az állomás elküld egy kérést, aztán vagy kap rá választ, vagy nem. Ide tartoznak az alábbi alkalmazások is:

- DHCP
- DNS (TCP-t is használhat)
- SNMP
- TFTP

Némelyik alkalmazás maga gondoskodik a megbízhatóságról. Ezeknek nincs szüksége a TCP szolgáltatásaira, szállítási protokollként jobban ki tudja használni az UDP-t. A TFTP is ezek közé tartozik, mivel saját módszert kínál az adatfolyam-vezérlésre, hibakeresésre, nyugtázásra, valamint a hibajavításra. Ezeket a szolgáltatásokat nem kell igénybe vennie a TCP-től.

Beszélgessünk róla ismét ...

Megjegyzés: Fontos, hogy a diákoknak már be kellett fejezniük a fejezethez tartozó, bevezető modellezési feladatot. A feladat megoldása ideális esetben közepes méretű (6-8 fős) csoportokban történik.

Az oktató egy összetett üzenetet suttog a csoport első diákjának fülébe. Az üzenet valami ilyesmi lehet: "Holnap hóviharra számítunk. Valamikor reggel ér ide, ezért az első két óra elmarad. Hozzátok magatokkal a házi feladatot!"

A diák ezután a soron következő diák fülébe suttogja az üzenetet. A folyamatot az egyes csoportok egészen addig folytatják, amíg a csoportok minden egyes tagjához el nem jut a suttogott üzenet.

Az alábbi szabályokat kell betartani:

- Az üzenetet apró részletekben súghatjuk a szomszédunk fülébe, ÉS megismételhetjük az egyes részleteket, miután ellenőriztük, hogy a szomszédunk a megfelelő üzenetet hallotta.
- Az üzenet apró részletei suttogással ellenőrizhetők és (az óramutató járásával megegyező VAGY azzal ellentétes irányban) megismételhetők a pontosság kedvéért. Egy diák az időt méri a feladat teljesítése alatt.
- Amikor az üzenet elért a csoport végéhez, az utolsó diák hangosan elmondja, hogy mit is hallott. Az üzenet apró részletei megismételhetők (vagyis újraküldhetők), és a folyamat újrakezdhető annak érdekében, hogy az üzenet MINDEN részlete egészben és helyesen legyen kézbesítve.
- Ezután az oktató megismétli az eredeti üzenetet, hogy ellenőrizze a kézbesítés minőségét.

Csoportos feladat - We Need to Talk, Again Instructions

Ennek a szimulációs feladatnak az a célja, hogy megalapozza a TCP és az UDP részletekbe menő megértését. A szimulációs mód lehetőséget biztosít a különböző protokollok funkcionalitásának megtekintésére.

Ahogy az adatok áthaladnak a hálózaton, kisebb darabokra bontják szét őket és meg is jelölik, hogy a darabokat újra egyesíteni lehessen. Minden darabhoz egy adott nevet rendelünk: protokoll adategység (Protocol Data Unit, PDU) és egy speciális réteghez kötjük. A Packet Tracer szimulációs módja lehetővé teszi, hogy megtekintsük az egyes protokollokat és a kapcsolódó PDU-kat. A következő lépések végigvezetik a felhasználót azon a folyamaton, ahogy szolgáltatásokat kérünk le a kliens PC-n elérhető különféle alkalmazások segítségével.

Ez a feladat lehetőséget biztosít a TCP- és az UDP-protokoll funkcionalitásának, a multiplexelésnek, valamint a portszámok (helyi alkalmazások meghatározásában betöltött) szerepének tanulmányozására.

Packet Tracer feladat - TCP and UDP Communications Instructions

Packet Tracer feladat - TCP and UDP Communications - PKA

A szállítási réteg szállításhoz kapcsolódó szolgáltatásokat biztosít:

- Az alkalmazásoktól érkező adatok szegmensekre bontása.
- Fejléc hozzáadása az egyes szegmensek azonosításához és kezeléséhez.
- A szegmensek - alkalmazási adatokká történő - ismételt összeállítása a fejléc információk alapján.
- Az összeállított adatok továbbítása a megfelelő alkalmazáshoz.

A TCP és az UDP a leggyakoribb szállítási rétegbeli protokollok.

Az UDP-datagram és a TCP-szegmens egyaránt rendelkezik az adatrész elé helyezett fejléccel, amely tartalmazza a forrás- és a célport számát. Ezen portszámok teszik lehetővé, hogy az adatokat a célszámítógépen futó megfelelő alkalmazáshoz irányítsuk.

A TCP addig semmilyen adatot nem továbbít a hálózatra, amíg nem tudja, hogy a célállomás készen áll-e a fogadásukra. A TCP felügyeli az adatok áramlását is, és újraküld minden olyan adatszegmenset, amelynek a célállomáshoz történő beérkezését nem nyugtázták. A megbízhatóság eléréséhez a TCP kézfogást, időzítőket, nyugtázást, valamint dinamikus ablakkezelést alkalmaz. A megbízhatósági folyamat azonban többletterhelést okoz a hálózaton, a lényegesen nagyobb méretű szegmens-fejléc, valamint a forrás és a cél közötti megnövekedett forgalom által.

Amennyiben az alkalmazás adatait gyorsan kell a hálózaton keresztül kézbesíteni, vagy a hálózati sávszélesség nem támogatja a vezérlési üzenetek forrás- és célrendszer közötti cseréjéből adódó többletterhelést, a fejlesztő által előnyben részesített szállítási protokoll az UDP. Mivel az UDP nem követi nyomon, és nem is nyugtázza a datagramok célállomáshoz történő beérkezését, így az elveszett datagramokat sem küldi újra, csupán érkezési sorrendben továbbítja a beérkezett adatokat az alkalmazási rétegbe. Ez ugyanakkor nem jelenti szükségszerűen azt, hogy maga a kommunikáció nem lenne megbízható. Léteznek ugyanis olyan mechanizmusok az alkalmazási réteg protokolljaiban és szolgáltatásaiban, amelyek foglalkoznak az elveszett vagy késve érkező datagramokkal, amennyiben ezt az alkalmazás megköveteli.

Az alkalmazásfejlesztő dönti el, hogy melyik szállítási rétegbeli protokoll tesz a legjobban eleget a programmal szemben támasztott követelményeknek. Fontos megjegyezni, hogy az összes többi réteg is szerepet játszik az adathálózatok kommunikációjában, és kihat a teljesítményükre is.

A címzés a hálózati réteg protokolljainak kulcsfeladata, ez teszi lehetővé, hogy az állomások attól függetlenül kommunikálhassanak egymással, hogy azonos, vagy különböző hálózatokon helyezkednek-e el. Az Internet Protokoll 4-es (IPv4) és 6-os verziója (IPv6) egyaránt hierarchikus címzési módot biztosít az adatokat szállító csomagok számára.

Az IP-cím kiosztás hatékony tervezése, megvalósítása és karbantartása biztosítja a hálózatok hatékony és eredményes működését.

Ez a fejezet részletesen foglalkozik az IP-címek felépítésével, valamint a használatukkal IP-hálózatok és alhálózatok létrehozása és tesztelése során.

Minden a hálón (The Internet of Everything, IoE)

Ha a természet, a közlekedés, a szállítás, a hálózatok és az űrkutatás mind az információk digitális megosztásától függenek, akkor hogyan azonosítsuk az információt míg eljut a forrástól a céljáig?

Ebben a feladatban nem csak azon kezdünk el gondolkodni, hogy mit kell azonosítanunk az IoE világban, de azon is, hogy hogyan fogjuk ezeket a dolgokat azonosítani, megcímezni.

- Olvassuk el a blog illetve újságcikk forrást, amelyet John Chambers írt a Minden a hálón (IoE) jelenségről. http://blogs.cisco.com/news/internet-of-everything-2. Tekintsük meg az oldal közepe táján levő videót.

- Ezután látogassuk meg az IoE főoldalát - http://www.cisco.com/web/tomorrow-starts-here/index.html. Kattintsunk egy érdekesnek hangzó kategóriára.

- Nézzük meg a videót, blogot vagy pdf-et a választott kategóriából.

- Írjunk 5 hozzászólást vagy kérdést arról, amit láttunk vagy olvastunk és ezt osszuk meg osztályunkkal is.

Csoportos feladat - The Internet of Everything (IoE) Instructions

Ahhoz, hogy megértsük az eszközök hálózaton való működését, meg kell néznünk az általuk használt címeket és az egyéb adatokat - méghozzá bináris alakban. Bináris ábrázolás esetén az információ megjelenítése csak egyesek és nullák segítségével történik. A számítógépek bináris adatokkal kommunikálnak. Bináris adatokkal sok más formátumú adat is megjeleníthető. Például ha billentyűzeten gépelünk, a betűk a képernyőn számunkra olvasható és érthető formában jelennek meg, de a számítógép számára binárisan tárolódnak és továbbítódnak. A betűket a számítógép az ASCII (American Standard Code for Information Exchange) kódtábla segítségével fordítja le.

Az ASCII táblában az "A" betűt binárisan a 01000001 jelenti, a kisbetűs "a" pedig 01100001. Az 1. ábra ASCII fordítójával próbáljuk ki a karakterek binárissá alakítását.

Habár a betűk bináris formájával általában nem szükséges foglalkoznunk, az IP-címzéshez mégis fontos értenünk a bináris ábrázolást. Egy hálózat minden eszközét egyedi bináris címmel kell azonosítani. IPv4 hálózatokon ez a cím egy 32 bitből (egyesekből és nullákból) álló sorozat. A hálózati rétegben a csomagoknak ezt az egyedi azonosítót kell tartalmazniuk a forrás- és célrendszerek azonosítására is. Ezért egy IPv4 hálózatban minden csomag tartalmaz egy 32 bites forrás és egy 32 bites célcímet a harmadik réteg fejlécében.

Legtöbbünknek egy 32 bites bitsorozatot nagyon nehéz értelmezni és még nehezebb megjegyezni. Ezért az IPv4-címeket bináris helyett pontokkal elválasztott (pontozott) decimális formátumban használjuk. Ez azt jelenti, hogy minden byte (oktett) egy-egy 0 és 255 közé eső decimális szám lesz. Ennek megértéséhez a binárisból decimálisba történő átalakítással kell megismerkednünk.

A helyiérték

A binárisból decimálisba történő átalakításhoz szükség van a számrendszerek egyik matematikai alapjának, a helyiérték fogalmának megértésére. A helyiérték azt jelenti, hogy egy számjegy különböző értékeket képvisel attól függően, hogy melyik helyen áll a számon belül. A helyiértéket használó rendszerben a számrendszer alapszámát időnként radixnak is hívják. A tízes számrendszer radixa a 10. Kettes számrendszerben pedig 2 a radix. A radix és az alapszám kifejezések egyenértékűek, vegyesen használhatjuk őket. Pontosabban fogalmazva egy számjegy által jelölt számérték azt jelenti, hogy az alapszámot annyiadik hatványon vesszük, ahányadik helyen a számjegy áll, majd megszorozzuk a számjegy értékével. A következő példák segítenek megérteni a rendszer működését.

A decimális 192 esetén az 1-es szám által képviselt számérték 1*10^2 (1 szorozva 10 a másodikon). Ez az 1-es a hétköznapi szóhasználatban "százasoknak" nevezett helyiértéken áll. A helyiérték ezt alap^2 helynek nevezi, mert az alap, vagy radix a 10, a hatvány pedig a 2. A 9 értéke 9*10^1 (9 szorozva 10 az első hatványon). A 192 szám helyiértékei a 2. ábrán láthatók.

A helyiérték rendszer szerint a 10-es számrendszerben a 192 így néz ki:

192 = (1 * 10^2) + (9 * 10^1) + (2 * 10^0)

vagy

192 = (1 * 100) + (9 * 10) + (2 * 1)

Az IPv4-címek 32 bites bináris számok. Azonban azért, hogy emberek számára könnyebben legyen használható, az IPv4-címeket jelentő bináris sorozatokat pontokkal elválasztott decimális alakban használjuk. Először a 32 bites sort byte-onként (8 bitenként) pontokkal elválasztjuk, ezeket oktettnek is hívjuk. Azért hívják oktettnek, mert mindegyik decimális szám egy byte-ot vagy 8 bitet képvisel.

A bináris cím:

```
11000000 10101000 00001010 00001010
```

pontokkal elválasztott decimális alakban:

192.168.10.10

Az első ábrán a gombokat sorban kiválasztva megláthatjuk, hogy a 32 bites bináris cím hogyan áll össze pontozott decimális oktettekből.

De hogyan határozzuk meg a decimális megfelelőiket?

A kettes (bináris) számrendszer

Bináris számrendszerben a radix 2. Emiatt minden helyiérték a 2 egyre növekvő hatványát jelenti. 8 bites bináris számoknál a helyiértékek az alábbiak:

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

A 2-es alapú számrendszer csak két számjegyet használ: 0 és 1.

Amikor egy bájtot decimális számként értelmezünk, a helyének megfelelő értékkel számolunk a bit 1-es állásánál, 0-ás bit esetén pedig nem számolunk vele, amint az első ábrán is látható.

A 2. ábra a 192 decimális szám bináris megfelelőjét mutatja. Egy adott pozícióban az 1-es azt jelenti, hogy azt az értéket hozzáadjuk az összeghez. A 0 pedig azt jelenti, hogy azt az értéket nem adjuk hozzá. Az 11000000 bináris számban 1-es van a 2^7 helyen (decimálisan 128) és 1 van a 2^6 helyen (decimálisan 64). A többi bit nulla, az ő decimális értéküket nem számoljuk bele az összegbe. Az eredmény 128+64, ami 192, ez az 11000000 decimális megfelelője.

Még két példa:

1. példa: A csupa 1-est tartalmazó oktett: 11111111

A minden 1-es azt jelenti, hogy az összes általa képviselt érték beleszámít az összegbe. Mivel itt minden helyen 1-es van, mindent össze kell adnunk, a csupa 1-esből álló oktett értéke 255.

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

2. példa: A csupa nullás oktett: 00000000

A nulla azt jelenti, hogy az azon a helyen levő értéket nem kell beleszámolnunk az összegbe. Ha minden pozíción nulla van, az összeg is 0.

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

A nullák és egyesek egyéb kombinációi más decimális értékeket eredményeznek.

Minden oktett 8 bitből áll, és minden bit értéke 0 vagy 1. A négy darab 8 bites csoport értéke egyenként 0 és 255 közé eshet (0 és 255 is lehet). Minden bit értéke jobbról balra 1, 2, 4, 8, 16, 32, 64, és 128.

Az oktett értékét úgy állapítjuk meg, hogy összeadjuk a helyiértékeket azokban a pozíciókban, ahol bináris 1 van.

- Ha 0 szerepel egy pozíción, akkor ott nem adjuk hozzá a helyiértéket.
- Ha minden bit 0, tehát 00000000, akkor az oktett értéke 0.
- Ha mind a 8 bit 1-es, tehát 11111111, akkor az oktett értéke 255 (128+64+32+16+8+4+2+1).
- Vegyes bitértékek esetén a megfelelő értékeket összeadjuk. Például a 00100111 oktett értéke 39 (32+4+2+1).

Tehát a négy oktett mindegyikének értéke 0 és a maximális 255 közé esik.

A 11000000101010000000101000001010 32 bites IPv4-címet a következő lépésekben alakítjuk binárisból pontozott decimális formátumba:

1. lépés A 32 bit 4 oktettre osztása.

2. lépés Minden oktett decimálissá alakítása.

3. lépés A számok közé pont kerül.

Kattintsunk a Lejátszásra (Play) az ábrán, hogy megnézzük egy bináris szám pontozott decimálissá konvertálását.

A binárisból decimálissá konvertálás mellett szükséges annak a megértése is, hogy decimálisból binárisba hogyan alakítunk át.

Mivel az IPv4-címeket pontokkal elválasztott decimális alakban ábrázoljuk, elég a 8 bit nagyságú bináris számok 0 és 255 közé eső decimális értékekké alakításával foglalkoznunk az IPv4-címek oktettjeinek megfelelően.

A konvertálás első lépéseként megvizsgáljuk, hogy a decimális szám egyenlő-e vagy nagyobb, mint a legnagyobb helyiértékű bit által képviselt decimális érték. A legnagyobb helyiértéket tekintve megnézzük, hogy a szám egyenlő-e vagy nagyobb, mint 128. Ha az oktett értéke kisebb, mint 128, nullát írunk a 128 bitpozíciójához és tovább megyünk a 64-es értékhez.

Ha az oktett értéke nagyobb vagy egyenlő, mint 128, akkor 1-et írunk a bit pozíciójára és levonunk 128-at a konvertálás alatt levő számból. Majd összehasonlítjuk a maradékot a következő, eggyel kisebb hatványértékkel, ami a 64. Ezt a folyamatot folytatjuk az összes hátralevő bitértékre.

Kövessük végig az 1-6. ábrákat, hogy megfigyeljük a 168-as szám 10101000 bináris értékékké alakítását.

Kövessük az ábrákon az IP-cím bináris alakba történő átalakításának lépéseit.

1. ábra: A 192 binárissá konvertálása.

2. ábra: A 168 binárissá alakítása.

3. ábra: A 10 binárissá alakítása.

4. ábra: A 10 binárissá alakítása.

5. ábra: A konvertált oktettek összefűzése az elsőtől kezdődően.

A bináris ábrázolás megértése fontos, amikor azt szeretnénk meghatározni, hogy két állomás azonos hálózaton van-e. Idézzük fel, hogy az IP-cím hierarchikus cím, amely két részből áll: a hálózati és az állomás rész. Amikor a hálózat és állomás részt szeretnénk meghatározni, nem a decimális, hanem a bináris értékét kell vizsgálnunk. A 32 bit egy része adja a hálózatot, maradék része az állomást azonosító részt.

Szükséges, hogy a hálózati részt adó bitek minden olyan eszköznél azonosak legyenek, amelyek ugyanazon a hálózaton tartózkodnak. Az állomás rész bitjeinek az alhálózaton belül egyedinek kell lenniük, hogy az állomást azonosítani tudják. A decimális értékek egyezésétől függetlenül ha két állomás 32 bites címének hálózati része megegyezik, akkor az állomások ugyanazon a hálózaton vannak.

De honnan tudják az állomások, hogy a 32 bit melyik része a hálózati és melyik az állomás rész? Ennek meghatározása az alhálózati maszk feladata.

Amikor egy IP alapú állomás beállítását végezzük, alhálózati maszkot is rendelünk az IP-cím mellé. Ahogy az IP-cím, az alhálózati maszk is 32 bit hosszú. Az alhálózati maszk jelöli ki, hogy az IP-cím melyik része a hálózatcím és melyik az állomáscím.

Az alhálózati maszkot összevetjük az IP-címmel balról jobbra, bitről bitre. Az egyesek az alhálózati maszkban a hálózati részt jelentik, a nullák pedig az állomás részt. Ahogy az 1. ábra is mutatja, az alhálózati maszk úgy jön létre, hogy 1-est állítunk be a hálózati részhez és bináris 0-t az állomás részhez. Figyeljük meg, hogy az alhálózati maszk nem tartalmazza a cím hálózati vagy állomás részét, csak azt mondja meg a számítógépnek, hogy egy adott IPv4-címben hol találhatóak ezek a részek.

Az IPv4-címekhez hasonlóan az alhálózati maszkot is pontokkal elválasztott decimális formában használjuk a könnyebb olvashatóság érdekében. Az alhálózati maszkot az IPv4-címmel együtt állítjuk be az eszközön, ez amiatt szükséges, hogy az állomás meg tudja határozni melyik hálózathoz tartozik. A 2. ábra egy IPv4 oktetthez tartozó lehetséges maszkokat mutatja.

A hálózat előtag (prefix, prefixum)

A prefix hosszának megadása az alhálózati maszk egy másik formája. Az előtag hossza az alhálózati maszk egyeseinek száma. "Peres" jelöléssel írjuk, a "/" után az 1-es bitek számát kell írni. Például ha az alhálózati maszk 255.255.255.0, akkor 24 bit van 1-esre állítva a maszk bináris alakjában, tehát a prefix hossza 24 bit, avagy /24. A prefix és az alhálózati maszk ugyanannak a dolognak - a cím hálózati részének - különböző megadási módja.

Nem minden hálózat előtagja /24-es. A hálózat állomásainak számától függően a prefix különböző is lehet. Az eltérő prefix szám más állomáscím tartományt és szórási címet eredményez.

Az ábrák a 10.1.1.0 címet mutatják különböző prefix méretekkel. Az első ábra /24-től /26-ig ábrázolja az előtagokat. A második ábra pedig a /27 és /28 prefixeket mutatja.

Figyeljük meg, hogy azonos hálózat cím esetén a különböző prefixekhez különböző állomáscím tartományok és szórási címek tartoznak. Az ábrákról látható, hogy a megcímezhető állomások száma szintén változik.

Egy IPv4 alhálózat címtartományán belül háromféle cím van:

- hálózatcím
- állomáscímek
- üzenetszórási cím

Hálózatcím

A hálózatcím a hálózatra hivatkozás egyik szokásos módja. Az alhálózati maszkot vagy az előtag hosszát is használhatjuk erre. Például az első ábrán levő hálózatot hívhatjuk 10.1.1.0 hálózatnak, 10.1.1.0 255.255.255.0 hálózatnak, vagy 10.1.1.0/24 hálózatnak is. A 10.1.1.0/24 hálózat minden állomása esetén a címeik hálózat része ugyanaz lesz.

Ahogy a második ábra mutatja, egy IPv4 hálózaton az első cím a hálózatcímnek van fenntartva. Ez a cím az állomás részen csupa nullákat tartalmaz. A hálózat minden állomása ugyanazt a hálózatcímet használja.

Állomáscím

Minden végberendezésnek egyedi címmel kell rendelkeznie a hálózati kommunikációhoz. IPv4-címek esetén a hálózatcím és a szórási cím közötti címeket rendelhetjük hozzá a végberendezésekhez. A 3. ábra azt mutatja, hogy a cím nullák és egyesek bármely kombinációját tartalmazhatja az állomás részen, kivéve a csupa nulla és a csupa egyes címet.

Szórási cím

Az IPv4 szórási cím egy speciális címe az alhálózatoknak, amelynek segítségével minden állomással egyszerre kommunikálhatunk. Ehhez a küldőnek egyszerűen egy csomagot kell küldenie a hálózat szórási címére, ezt a hálózat minden állomása megkapja és feldolgozza.

A szórási cím a hálózat tartományának legmagasabb címe. Ez az a cím, ahol az állomás részben minden bit 1-es. Ha egy oktett bináris alakban csupa 1-eseket tartalmaz, akkor a decimális értéke 255. Ezért, ahogy a negyedik ábra is mutatja, a 10.1.1.0/24 hálózat esetén, ahol az utolsó oktett az állomás rész, a szórási cím 10.1.1.255 lesz. Ne feledjük, hogy az állomás rész nem mindig egész oktett. Ezt a címet irányított szórásnak is hívják.

Annak érdekében, hogy a hálózat minden állomása egyedi IP-címet kapjon a tartományon belül, fontos az első és utolsó állomáscím megállapítása. A hálózat állomásai ezen a tartományon belül kaphatnak IP-címet.

Az első állomáscím

Ahogy az első ábrán is látható, az első állomáscím állomás része csupa nullákat tartalmaz, kivéve a jobb szélső, legkisebb értékű bitet, ami 1-es. Ez a cím eggyel nagyobb a hálózatcímnél. Ebben a

példában a 10.1.1.0/24 hálózat első állomáscíme 10.1.1.1. Sok helyen az első állomáscímet használják a forgalomirányító vagy alapértelmezett átjáró címének.

Az utolsó állomáscím

Az utolsó állomáscím állomás része csupa egyeseket tartalmaz, csak a jobb szélső, legkisebb értékű bitje nulla. Ez a cím eggyel kisebb, mint a szórási cím. A második ábrán látható, hogy a 10.1.1.0/24 hálózat utolsó állomáscíme a 10.1.1.254.

Amikor egy eszköznek IP-címet adunk, az eszköz az alhálózati maszk segítségével állapítja meg, hogy melyik hálózat tagja. A hálózatcím az a cím, amely egy hálózat minden eszköze számára azonos.

Amikor az eszköz adatot küld a hálózaton, ezt az információt használja annak a megállapítására, hogy a csomagot helyileg kell küldenie, vagy az alapértelmezett átjárónak, amely a távoli hálózatba továbbítást végzi. Amikor az állomás elküldi a csomagot, összehasonlítja a saját IP-címének és a cél IP-címnek a hálózat részét az alhálózati maszk segítségével. Ha a hálózati bitek egyeznek, akkor mind a forrás, mind a cél azonos hálózaton van, a csomag helyileg kézbesíthető. Ha nem egyeznek, a küldő állomás a csomagot az alapértelmezett átjárónak küldi, hogy az egy távoli hálózat felé továbbítsa.

Az ÉS művelet

Az ÉS a digitális logikában használt három alapvető bináris művelet egyike. A másik kettő a VAGY és a NEM. Míg az adathálózatokban mindhármat használják, a hálózatcím meghatározására csupán az ÉS szolgál. Emiatt a fejezet keretei között csak az ÉS műveletet tárgyaljuk. A logikai ÉS művelet elvégzése után két bitből a következő eredményeket kapjuk:

1 ÉS 1 = 1 (1. ábra)

0 ÉS 1 = 0 (2. ábra)

0 ÉS 0 = 0 (3. ábra)

1 ÉS 0 = 0 (4. ábra)

Az IPv4 állomáscímet bitenként logikailag ÉS kapcsolatba hozva az alhálózati maszkkal megtudhatjuk az állomás alhálózatát. Vagyis a bitenkénti ÉS művelet elvégzése után a hálózatcímet kapjuk eredményül.

Minden címbit, amit ÉS kapcsolatba hozunk az alhálózati maszkban található 1-es bitekkel az eredeti bitet adja vissza. Így 0 (az IPv4-címből) ÉS 1 (az alhálózati maszkból) 0-t eredményez. 1 (az IPv4-címből) ÉS 1 (az alhálózati maszkból) pedig 1. Bármi, amit 0-val hozunk ÉS kapcsolatba 0-t eredményez. Az ÉS művelet ezen tulajdonságai miatt tudja az alhálózati maszk az IPv4-cím állomás részét "elmaszkolni". A cím minden bitjét ÉS kapcsolatba kell hozni a hozzá tartozó alhálózati maszkkal.

Mivel az alhálózati maszk állomás részén levő bitek nullák, a művelet után előálló hálózatcím állomás része is nullákat fog tartalmazni. Emlékezzünk rá, hogy az az IPv4-cím, amely az állomás részen csak nullákat tartalmaz, maga a hálózatcím.

Hasonlóképpen az alhálózati maszk hálózat részén levő bitjei 1-esek. Ha ezeket a cím megfelelő bitjeivel ÉS kapcsolatba hozzuk, az eredmény megegyezik az eredeti címmel.

Amint az ábrán látható, az alhálózati maszk 1-es bitjeinek hatására az alhálózat hálózati része megegyezik az állomás címének hálózati részével. A hálózatcím állomás része csupa nullából fog állni.

Adott IP-cím és maszkja esetén az ÉS művelettel meghatározhatjuk, hogy melyik alhálózathoz tartozik a cím és azt is, hogy mely egyéb címek tartoznak ebbe az alhálózatba. Ne feledjük, hogy ha két cím ugyanabba a hálózatba vagy alhálózatba tartozik, akkor ők helyi viszonyban vannak egymással, vagyis közvetlenül tudnak kommunikálni. Azokat a címeket, amelyek nem ugyanabba a hálózatba vagy alhálózatba tartoznak távolinak hívjuk, a köztük zajló kommunikációhoz 3. rétegbeli eszközre (forgalomirányító vagy 3. rétegbeli kapcsoló) van szükség.

A hálózatok ellenőrzése vagy hibaelhárítása közben gyakran meg kell határoznunk hogy két állomás azonos hálózaton van-e. Ezt az eszközök szemszögéből kell vizsgálnunk. Helytelen konfiguráció miatt előfordulhat, hogy egy állomás másik hálózatra "gondolja" magát, mint ahova tervezték. Ez kiszámíthatatlan működéshez vezethet, ha nem derítjük fel az állomás által végzett ÉS műveletek vizsgálatával.

Felhasználói eszközök címei

A legtöbb adathálózatban a leggyakoribb végberendezések közé a számítógépek, táblagépek, okostelefonok, nyomtatók és IP-telefonok tartoznak. Mivel ezek képezik az eszközök legnagyobb részét, a legtöbb címet is az ilyesfajta állomásoknak kell kiosztanunk. A hálózat szabad címtartományából fogunk címet adni nekik. A címeket statikusan vagy dinamikusan rendelhetjük hozzájuk.

Statikus hozzárendelés

Statikus hozzárendelésnél a hálózati rendszergazdának kell kézzel beállítania a hálózati információkat az állomáson. Az 1. ábra a hálózati kártya tulajdonságainak ablakát mutatja. Statikus IPv4-cím beállításához válasszuk az IPv4-et a tulajdonságok ablakban, írjuk be a statikus címet, az alhálózati maszkot és az alapértelmezett átjárót. A 2. ábra a minimális statikus beállításokat mutatja: az állomás címe, maszkja és az átjárója.

A statikus címkiosztásnak számos előnye van. Hasznos nyomtatók, szerverek, és olyan eszközök számára, amelyek nem változtatják gyakran a helyüket, és a rögzített IP-címük alapján kell elérhetőnek lenniük a kliensek részéről. Ha az állomások egy bizonyos IP-cím alapján érik el a szervert, akkor ennek a címnek a megváltozása gondokat okozhat. Továbbá a statikus címkiosztással a hálózati erőforrások jobban ellenőrizhetők. Például alkothatunk hozzáférési szabályokat bizonyos IP-címekre vagy címekről érkező forgalom alapján. Azonban a statikus cím beállítása minden állomáson időigényes feladat.

Statikus IP-cím kiosztás esetén fontos, hogy pontos listánk legyen az eszközöknek kiosztott címekről. Mivel ezek állandó címek, normális esetben nem használhatjuk fel őket újra.

Dinamikus címhozzárendelés

A helyi hálózatokon a felhasználók száma változó lehet. Új felhasználók érkeznek laptoppal és hálózati kapcsolatra van szükségük. Mások új munkaállomást kapnak vagy egyéb, hálózati kapcsolatot igénylő eszközt hoznak, például okostelefont. Ahelyett, hogy a hálózati rendszergazda rendelne minden állomáshoz IP-címet, sokkal könnyebb, ha ezeket automatikusan osztjuk ki. Ezt a DHCP (Dynamic Host Configuration Protocol) protokoll segítségével tehetjük meg, amint az 1. ábrán látható.

A DHCP lehetővé teszi a címzési információk - IP-cím, alhálózati maszk, alapértelmezett átjáró és egyéb konfigurációs paraméterek - automatikus kiosztását. A DHCP-szerver beállításainál meg kell adni egy címtartományt (címkészletet, angolul address pool), amelyből a DHCP a kliensekhez rendel címeket. A címkészletet úgy kell megtervezni, hogy az ne tartalmazza a más eszközök által használt statikus címeket.

Nagyobb hálózatokon a DHCP a legjobb módszer az állomáscímek kiosztására, csökkenti a hálózatfelügyeleti személyzet terheit és gyakorlatilag megszünteti az adatbeviteli hibákat.

A DHCP másik előnye, hogy egy címet nem állandó használatra, hanem csak bizonyos időtartamra "bérelnek" az állomások. Ha az állomást kikapcsolják vagy eltávolítják a hálózatról, a cím visszakerül az elérhető címek közé újrafelhasználásra. Ez a funkció különösen hasznos mobil eszközöknél, amelyek jönnek-mennek a hálózatokon.

Ha a DHCP engedélyezve van egy állomáson, az **`ipconfig`** parancs segítségével nézhetjük meg a DHCP-szerver által hozzárendelt IP-címet, ez a 2. ábrán látható.

Egy IPv4 hálózaton az állomások három módon kommunikálhatnak:

- **Egyedi címzés (unicast)** Az állomás egyetlen másik állomásnak küld csomagot.
- **Szórás** Egy állomás a hálózat összes állomásának küld csomagot.
- **Csoportos címzés (multicast)** Az állomás egy bizonyos csoportba tartozó, akár különböző hálózatokon levő állomásoknak küldi a csomagot.

Ez a háromféle kommunikációs módszer különböző célokra használatos. Mindhárom esetben a küldő állomás IPv4-címe kerül a csomag fejlécébe, mint forráscím.

Egyedi címzéses forgalom

Állomások egymás közötti kommunikációjának általános módja az egyedi címzéses továbbítás, akár kliens-szerver akár egyenrangú (peer-to-peer) hálózatról van szó. Az egyedi címzésű csomagok célcímként a cél eszköz címét használják, ezek a csomagok hálózatok között is továbbíthatók.

Az animáció lejátszásával egyedi címzéses átvitelre láthatunk példát.

IPv4 hálózaton állomáscímnek hívjuk a végberendezés egyedi címzésű címét. Egyedi címzésű kommunikációnál a két végberendezéshez rendelt cím lesz a forrás és cél címe. A beágyazás folyamata során a forrás állomás a saját címét az egyedi címzésű csomag fejlécének forráscím mezőjében, a cél állomás címét pedig a csomag célcím mezőjében helyezi el. Függetlenül attól, hogy a csomag célja egyedi cím, szórási cím vagy csoportcím, a csomag forráscíme mindig a küldő állomás egyedi címe.

Megjegyzés: Ebben a kurzusban az eszközök közti kommunikáción, ha nem jelezzük külön egyedi címzésű átvitelt értünk.

Az IPv4 állomáscímek egyedi címzésű címek, a 0.0.0.0 és 223.255.255.255 közé esik a tartományuk. Azonban ebben a tartományban is számos cím van, amik speciális célra vannak fenntartva. Ezekről a speciális célú címekről később lesz szó a fejezet során.

Szórásos átvitel

A szórásos forgalom arra való, hogy egy hálózat minden állomásának elküldjük a csomagot a hálózat szórási címének használatával. Üzenetszóráskor a csomag olyan cél IP-címet tartalmaz, amelyben az állomásazonosító csupa bináris 1-esből áll. Ez azt jelenti, hogy a helyi hálózat összes állomása (szórási tartomány) megkapja és megvizsgálja a csomagot. Sok hálózati protokoll használ szórásos átvitelt, ilyen például a DHCP. Ha egy állomás a hálózatának szórási címére küldött csomagot fogad, ugyanúgy feldolgozza, mintha a saját egyedi címére érkezett volna.

Néhány példa szórásos kommunikációra:

- Felsőbb rétegű címek alsóbb rétegű címekhez társítása.
- Cím kérése.

- Az egyedi címzésű csomagok hálózatok közt is továbbíthatók, ezzel ellentétben a szórásos üzenetek legtöbbször a helyi hálózaton belülre korlátozottak. Ez a korlátozás az átjáró forgalomirányító konfigurációjától és a szórásos üzenet típusától függ. Két fajta szórásos üzenet létezik: irányított szórás és korlátozott szórás.

Irányított szórás

Az irányított szórás egy bizonyos hálózat minden állomásának küldött üzenetet jelenti. Ez a fajta szórás akkor hasznos, ha szórásos üzenetet szeretnénk küldeni egy nem helyi hálózat minden állomásának. Például ha egy a 172.16.4.0/24 hálózaton kívüli állomás szeretne kommunikálni ezen hálózat minden állomásával, a csomag célcímeként a 172.16.4.255-t kell megadnia. Bár a forgalomirányítók alapértelmezés szerint nem továbbítják az irányított szórást, beállíthatjuk őket úgy, hogy mégis megtegyék azt.

Korlátozott szórás

A korlátozott szórás a helyi hálózat állomásaival való kommunikációra szolgál. Ezeknek a csomagoknak a cél IPv4-címe 255.255.255.255. A forgalomirányítók nem továbbítják a korlátozott szórást. Ezért az IPv4 alhálózatot szórási tartománynak is hívjuk. A szórási tartomány határain forgalomirányítók vannak.

Például a 172.16.4.0/24 hálózat egy állomása a saját hálózatán belül úgy tud minden állomásnak szórt csomagot küldeni, hogy a cél címnek a 255.255.255.255-öt állítja be.

Az animáción a korlátozott szórásos átvitelre láthatunk példát.

A szórt üzenet a hálózat erőforrásait is használja és minden fogadó állomást a csomag feldolgozására kényszeríti. Emiatt a szórásos forgalmat korlátozni kell annak érdekében, hogy ne rontsa le a hálózat vagy a többi eszköz teljesítményét. Mivel a forgalomirányítók elkülönítik egymástól a szórási tartományokat, a túl sok szórást forgalmazó hálózatok felosztásával növelni tudjuk a hálózat teljesítményét.

Csoportos küldés (multicast)

A csoportos küldést (multicast) arra tervezték, hogy takarékosan bánjon az IPv4 hálózat sávszélességével. A forgalmat azáltal csökkenti, hogy lehetővé teszi az állomás számára egyetlen csomag egyszerre több, a csoportcímre feliratkozott állomásnak történő elküldését. Egyedi címzés használatával az állomásnak külön-külön csomagot kellene minden cél állomás számára elküldenie. Csoportos címzéssel a forrás állomás egyetlen csomagja több ezer cél állomáshoz is eljuthat. A köztes hálózatok feladata az, hogy a multicast üzenetek folyamát hatékony módon többszörözzék úgy, hogy azok csak a tényleges címzettekhez jussanak el.

Néhány példa a csoportos küldéses átvitelre:

- Videó és audió adások.
- Forgalomirányító protokollok forgalomirányító információinak cseréje.
- Szoftver terjesztés.
- Távoli játék.

Csoportos küldéses címek (multicast cím, csoport cím)

Az IPv4 egy címtartományt tart fenn a multicast csoportok számára. Ez a tartomány 224.0.0.0 és 239.255.255.255 közé esik. A multicast címtartományt felosztották különböző címtípusok számára:

fenntartott link-local (adatkapcsolati szinten helyi) címek és globális hatókörű címek. Egy további multicast címtípus az adminisztratív hatókörű címek, más néven korlátozott hatókörű címek.

A 224.0.0.0 és 224.0.0.255 közé eső multicast címek a fenntartott link-local címek. Ezeket a címeket a helyi hálózatban levő multicast csoportok használják. A helyi hálózatban működő forgalomirányító felismeri, hogy a csomagokat link-local multicast csoportnak címezték és nem továbbítja őket. A fenntartott link-local címek használatának tipikus példája a forgalomirányítók kommunikációja, amelyek multicast átvitellel cserélnek forgalomirányítási információkat.

A globális hatókörű címek 224.0.1.0 és 238.255.255.255 közé esnek. Interneten keresztüli multicast forgalomra használhatók. Például a 224.0.1.1 a Hálózati Idő Protokoll (Network Time Protocol, NTP) számára van fenntartva, hálózati eszközök pontos idejének szinkronizálására használatos.

Multicast kliensek

Azokat az állomásokat, amelyek adott multicast kommunikációt fogadnak multicast klienseknek nevezzük. A multicast kliensek a kliens program által igényelt szolgáltatások segítségével iratkoznak fel a multicast csoportba.

Minden multicast csoportot egyetlen IPv4 multicast célcím képvisel. Amikor egy IPv4 állomás feliratkozik egy multicast csoportba, az állomás a multicast címre érkező csomagokat éppúgy feldolgozza, mint az ő saját egyedi címére érkezőket.

Az animáció bemutatja, amint kliensek multicast csomagokat fogadnak.

A feladatban az egyedi, szórásos és multicast átvitel viselkedését vizsgáljuk meg. A hálózatok legtöbb forgalma egyedi címzésű. Amikor egy számítógép ICMP válasz kérés (echo request) üzenetet küld egy távoli gépnek, az IP csomag fejlécének forrás mezője a számítógép IP-címe. Az IP-csomag fejlécének célcím mezőjébe a távoli forgalomirányító IP-címe kerül. A csomagot csak a valódi címzett kapja meg.

A **`ping`** parancs, vagy a Packet Tracer Add Compex PDU funkciója segítségével közvetlenül pingelhetünk szórási címet, hogy meglássuk a szórásos forgalmat.

A multicast tulajdonságait az EIGRP forgalmán keresztül nézhetjük meg. Az EIGRP a Cisco forgalomirányítók protokollja, melynek segítségével forgalomirányítási információkat cserélnek az eszközök. Az EIGRP-t használó forgalomirányítók a 224.0.0.10 multicast címre küldik üzeneteiket, amely az EIGRP forgalomirányítók csoportját jelenti. Ezeket a csomagokat más eszközök is megkapják, viszont az EIGRP forgalomirányítókkal ellentétben ők a 3. rétegben eldobják azokat, mert nincs dolguk velük.

Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic Instructions

Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic - PKA

Bár a legtöbb IPv4 állomáscím publikus cím, melyet internetre kötött hálózatokban való használatra jelöltek ki, vannak olyan címtartományok is, amelyeket azokban a hálózatokban használnak, ahol nincs, vagy korlátozott internethozzáférésre van csak szükség. Ezeket a címeket privát címeknek hívjuk.

Privát címek

A privát címtartományok a következők:

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

A privát címeket az RFC 1918 (Address Allocation for Private Internets - Privát Hálózatok Címkiosztása) definiálja, ezért időnként RFC 1918 címeknek is hívják őket. Az ábrán is látható privát címtartományokat magánhálózatokban használják. Azok az állomások, melyeknek nem szükséges internethozzáférés, privát címet kaphatnak. Ugyanakkor a magánhálózaton belül is egyedi címre van szükség a privát tartományon belül.

Különböző hálózatok állomásai használhatják ugyanazt a privát címet. Azok a csomagok, amelyeknek a forrás vagy cél címe ilyen cím, nem kerülhetnek ki a nyilvános internetre. A magánhálózat határán levő forgalomirányítónak vagy tűzfalnak blokkolni vagy lefordítania kell ezeket a címeket. Még ha ki is kerülnének ilyen csomagok az internetre, a forgalomirányítók úgysem találnák meg az utat a megfelelő magánhálózat felé.

Az IANA az RFC 6598-ban még egy fenntartott címtartományt kijelölt, amelyet megosztott vagy közös címtartománynak hívnak. Az RFC 1918 privát címteréhez hasonlóan a megosztott tartomány címei sem továbbíthatók globálisan. Azonban ezeket a címeket kizárólag szolgáltatói hálózatokban való használatra tervezték. Az osztott vagy közös címtartomány a 100.64.0.0/10.

Nyilvános címek

Az IPv4 egyedi címzésű címtartományának túlnyomó többsége nyilvános cím. Olyan állomások használják őket, amelyek nyilvános internethozzáféréssel rendelkeznek. Ám még ezeken a blokkokon belül is számos speciális célokra fenntartott cím van.

Vannak olyan címek, amelyek nem rendelhetők állomásokhoz. Vannak olyan speciális címek is, amelyeket kioszthatunk ugyan állomásoknak, de ezek az állomások csak bizonyos korlátozásokkal kommunikálhatnak a hálózaton.

Hálózat- és szórási címek

Ahogy korábban említettük, minden egyes hálózatban az első és utolsó cím nem rendelhető hozzá állomásokhoz. Ezek sorrendben az alhálózat hálózatcíme és szórási címe.

Visszacsatolás (loopback)

Egy tipikus fenntartott cím az IPv4 visszacsatolási (loopback) címe, a 127.0.0.1. A visszacsatolási cím olyan speciális cím, amelyet az állomások arra használnak, hogy a forgalmat visszairányítsák saját maguknak. A loopback cím egy rövid, egyszerűsített módot biztosít arra, hogy az ugyanazon gépen futó TCP/IP-t használó alkalmazások és szolgáltatások kommunikálhassanak egymással. Két ugyanazon az állomáson futó szolgáltatás megkerülheti a TCP/IP alsóbb rétegeit azzal, hogy nem a beállított IP-címet, hanem a loopback címet használják egymás között. A loopback cím meg is pingelhető, így ellenőrizhetjük a helyi gép TCP/IP beállításait.

Bár csak a 127.0.0.1 címet használjuk, a 127.0.0.0 és 127.255.255.255 közti összes cím fenntartott. Ezen tartomány minden címe a helyi gépre irányítódik vissza. A fenti tartományon belüli cím sohasem jelenhet meg a hálózaton.

Link-local (adatkapcsolati szinten helyi) címek

Az 169.254.0.1 és 169.254.255.254 közötti (169.254.0.0/16) IPv4-címblokk címeit adatkapcsolati szinten helyi (link-local) címnek nevezzük. Ezeket a címeket az operációs rendszer automatikusan a helyi géphez rendeli akkor, amikor nincs beállított vagy elérhető IP konfiguráció. Kis méretű egyenrangú hálózatban, vagy olyan állomások esetén használhatjuk, amelyek nem tudtak címet szerezni DHCP-szervertől.

Ahogy az ábrán is látható, pusztán IPv4 link-local címekkel csak olyan eszközök között lehetséges a kommunikáció, amelyek ugyanazon a hálózaton vannak. Az állomások nem küldhetnek forgalomirányítónak továbbításra olyan csomagot, amelynek IPv4 link-local cím a célcíme, valamint az ilyen csomagok TTL (élettartam) mezőjét 1-re kell állítani.

A link-local címek a helyi hálózaton kívül nem használhatók. Azonban számos kliens-szerver vagy peer-to-peer alkalmazás ilyen címekkel is működőképes.

Teszt-net címek

A 192.0.2.0 és 192.0.2.255 (192.0.2.0/24) közé eső címeket oktatási és tanulási célokra különítették el. E címeket dokumentációban és hálózati példákban használjuk. A kísérleti címekkel ellentétben a hálózati eszközök elfogadják beállításként ezeket a címeket. Gyakran találkozhatunk ezekkel a címekkel RFC-kben, gyártói- és protokoll dokumentációkban, sokszor az example.com és example.net domain nevekkel együtt használják őket. Ennek a blokknak a címei nem jelenhetnek meg az interneten.

Kísérleti célú címek

A 240.0.0.0 és 255.255.255.254 közti címeket későbbi használatra tartották fenn (RFC 3330). Jelenleg ezek a címek csak kutatási vagy kísérleti célra használhatók, de élő IPv4 hálózatban nem. Az RFC 3330 azonban lehetővé teszi, hogy a jövőben használható címekké alakítsák őket.

Eredetileg az RFC 1700 (Assigned Numbers, Hozzárendelt Számok) az egyedi címzéses tartományokat méret szerint A, B és C osztályokba sorolta. Ebben definiálták a D (multicast) és E (kísérleti) osztályú címeket is, amelyeket korábban már bemutattunk. Az A, B és C osztályok adott méretű hálózatokat jelentenek és meghatározott címtartományokat jelöltek ki ezen hálózatok számára. Egy cég vagy szervezet egy egész alhálózatot kaphat az A, vagy B, vagy C címtartományok egyikéből. A címek ezt a fajta használatát osztály alapú címzésnek vagy címkiosztásnak hívjuk.

"A" osztályú blokkok

Az A osztályú blokkokat rendkívül nagy hálózatokhoz tervezték, amelyek több, mint 16 millió állomással rendelkeznek. Az A oszályú IPv4-címek hálózat címét az első oktett rögzítése jelöli /8-as prefixummal. A fennmaradó 3 oktettet használják állomáscímekre. Minden A osztályú cím első oktettjének legnagyobb értékű bitje nulla. Eszerint legfeljebb 128 darab A osztályú hálózat lenne lehetséges 0.0.0.0/8 és 127.0.0.0/8 között. Habár az A osztályú hálózatok a teljes címtartomány felét elfoglalják, a 128 lehetséges hálózat miatt nagyjából csak 120 vállalat vagy szervezet kaphat belőle.

"B" osztályú blokkok

A B osztályú tartományt közepes- és nagyvállalatok számára alkották meg, ahol nagyjából 65000 állomás üzemel. A B osztályú IP-cím két legnagyobb értékű oktettje a hálózat rész. A másik két oktett pedig természetesen az állomás rész. Ahogy az A osztály esetén is, a további osztályok számára is szükség van címekre. A B osztályú címek két legnagyobb helyiértékű bitje 10. A B osztály számára kijelölt blokk a 128.0.0.0/16-191.255.0.0/16. A B osztály kissé hatékonyabban osztja ki a címeket, mint az A osztály, a teljes IPv4-tartomány 25%-a egyenlően oszlik el a kb. 16000 hálózat között.

"C" osztályú blokkok

A történelmi címosztályok közül a legszélesebb körben a C osztály használatos. A címtartományt kis, legfeljebb 254 állomással rendelkező hálózatok címeinek biztosítására találták ki. A C osztályú blokkok /24-es prefixumot használnak. Ez azt jelenti, hogy a C osztályú hálózat utolsó oktettje az állomás részt, a három legmagasabb értékű oktett pedig a hálózat részt alkotja. A C osztályú blokkokban található címek legnagyobb értékű oktettjének három legmagasabb értékű bitje 110. A C osztály blokkja 192.0.0.0/24-től 223.255.255.255.0/24-ig tart. Bár a teljes IPv4-tartománynak csak a 12,5%-át fedi le, 2 millió alhálózat címeit biztosítja.

Az 1. ábra a címosztályok eloszlását mutatja.

Az osztály alapú címzés korlátai

Nem minden szervezet szükséglete sorolható bele ebbe a három osztályba. A címek osztály alapú kiosztása miatt nagyon sok cím pazarlódik el, ami hozzájárul az IPv4-címek kimerüléséhez. Például egy 260 állomással rendelkező cégnek már B osztályú, 65000 címet biztosító alhálózatot kell adni.

Habár az osztály alapú rendszert az 1990-es évek végén elhagyták, a maradványaival még ma is találkozhatunk. Például amikor egy számítógépnek IPv4-címet adunk, az operációs rendszer a beírt címből megállapítja, hogy A, B vagy C osztályba tartozik-e, és ennek megfelelően ajánlja fel a beírandó alhálózati maszkot.

Osztály nélküli címzés

A ma használt rendszert osztály nélküli címzésnek hívjuk. A hivatalos neve Classless Inter-Domain Routing (Osztály nélküli tartományok közti forgalomirányítás, angol rövidítése CIDR, amelyet néha úgy ejtenek, mint az angol "cider" szót). Az IPv4-címek osztály alapú kiosztása egyáltalán nem volt hatékony, csak /8, /16 és /24-es prefixumot tett lehetővé és azokat is külön címtartományból. 1993-ban az IETF új szabványokat alkotott, amelyek lehetővé tették, hogy a szolgáltatók bármely bitnél határolt alhálózatokat használjanak az A, B és C osztály határai helyett.

Az IETF tudatában volt annak, hogy a CIDR csak egy átmeneti megoldás lehet, és hogy az új IP-protokollnak igazodnia kell az internet használók számának gyors növekedéséhez. 1994-ben az IETF elkezdett dolgozni az IPv4 utódján, ami végül az IPv6 lett.

A második ábra az osztályalapú címtartományokat mutatja.

Olyan cégnek vagy szervezetnek, amely internetről elérhető állomásokat (például webszerverek) szeretne üzemeltetni, nyilvános címtartománnyal kell rendelkeznie. Ne feledjük, hogy a publikus címeknek egyedinek kell lenniük, a címek használatát minden szervezet külön szabályozza. Ez az IPv4- és IPv6-címekre egyaránt igaz.

IANA és a RIR-ek

Az IANA (Internet Assigned Numbers Authority) (http://www.iana.org) kezeli az IPv4- és IPv6-címek kiosztását. Az 1990-es évek közepéig az egész IPv4-címtartományt közvetlenül az IANA kezelte. Akkor viszont az IPv4-címtartomány fennmaradó részét kiosztották meghatározott területekért vagy célokért felelős regisztrátorok között. Ezeket a regisztrátor cégeket Regionális Internet Regisztrátoroknak (RIR-ek) hívjuk, ezt mutatja az ábra.

A fő regisztrátorok:

- AfriNIC (African Network Information Centre) – Afrikai régió http://www.afrinic.net
- APNIC (Asia Pacific Network Information Centre) – Ázsia/Csendes-óceáni régió http://www.apnic.net
- ARIN (American Registry for Internet Numbers) – Észak-Amerikai régió http://www.arin.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin Amerika és a karibi szigetek http://www.lacnic.net
- RIPE NCC (Reseaux IP Europeans) - Európa, a Közel-Kelet és Közép-Ázsia http://www.ripe.net

Internetszolgáltatók (ISP-k)

A RIR-ek felelősek az IP-címek internetszolgáltatókhoz (ISP-k) rendeléséért. A legtöbb vállalat vagy szervezet az IPv4-címtartományát valamely internetszolgáltatótól kapja. Az ISP általában néhány (pl. 6 vagy 14) használható IPv4-címet biztosít az ügyfeleinek a szolgáltatás részeként. Nagyobb címtartományokhoz igazolniuk kell a jogos igényüket és további költségekbe is kerül.

Bizonyos értelemben az ISP a szervezetnek csak kölcsönzi, bérbe adja a címeket. Ha úgy döntünk, hogy az internetkapcsolatunkat másik ISP-hez költöztetjük, az új ISP a számukra kiosztott tartományból fog nekünk címeket biztosítani, az előző ISP pedig az általunk visszaadott címeket a más ügyfelek számára kioszthatók közé helyezi vissza.

Az IPv6-címeket szintén az ISP, bizonyos esetekben közvetlenül a RIR adja. Az IPv6-címeket és a tipikus tartomány méreteket a fejezet során később tárgyaljuk.

ISP szolgáltatások

Ha internetes szolgáltatásokat szeretnénk használni, a hálózatunkat internetszolgáltatón (Internet Service Provider, ISP) keresztül az internethez kell kapcsolnunk.

Az internetszolgáltatóknak saját belső hálózatuk van az internetkapcsolatok kezelésére és az ehhez tartozó szolgáltatások biztosítására. Az ISP sok más között például DNS- és e-mail szolgáltatást valamint weboldal elhelyezését biztosíthat az ügyfeleinek. A szükséges vagy elérhető szolgáltatási szintnek megfelelően az ügyfelek az ISP-k különböző szintjeit, rétegeit használhatják.

Az internetszolgáltatók rétegei (tier)

Az internetszolgáltatókat (ISP) az internet gerinchálózatához való kapcsolódásuk szintje szerint hierarchikus rendszerbe sorolhatjuk. Minden alacsonyabb rétegű ISP valamely felsőbb rétegű ISP-n keresztül kapcsolódik a gerinchálózathoz, amint az ábrákon is látható.

1. réteg

Amint az 1. ábrán látható, az ISP hierarchia tetején az 1. rétegű ISP-k vannak. Ezek nagy, országos vagy nemzetközi szolgáltatók, amelyek közvetlenül a gerinchálózatra kapcsolódnak. Az 1. rétegű szolgáltatók ügyfelei vagy az alacsonyabb rétegű szolgáltatók, vagy nagy cégek és szervezetek. Mivel az internet kapcsolódási rendszerének tetején helyezkednek el, nagy megbízhatóságú kapcsolatokat és szolgáltatásokat üzemeltetnek. A megbízhatóság elérésére egyebek között többszörös kapcsolatokat tartanak fenn az internet gerinchálózata felé.

Az 1. rétegű ISP-k legfontosabb előnyei az ügyfelek számára a megbízhatóság és a sebesség. Mivel ezek az ügyfelek mindössze egy kapcsolatnyira vannak az internettől, kevesebb számukra az esély a meghibásodásra vagy forgalmi dugókra. Az 1. rétegű ISP hátránya az ügyfél számára a magas költség.

2. réteg

A 2. rétegű ISP-k az 1. rétegű ISP-ktől szerzik az internetszolgáltatást, ezt a 2. ábrán láthatjuk. A 2. rétegű ISP-k célja általában az üzleti ügyfelek kiszolgálása. A 2. rétegű ISP-k több szolgáltatást biztosítanak a másik két rétegnél. A 2. rétegű ISP-k többnyire saját informatikai erőforrásokkal rendelkeznek a saját szolgáltatásaik üzemeltetéséhez, ilyenek például a DNS, az e-mail szerverek vagy webszerverek. A 2. rétegű ISP-k által nyújtott szolgáltatás lehet még weboldal fejlesztés és karbantartás, e-kereskedelem vagy VoIP.

A 2. rétegű ISP elsődleges hátránya az 1. réteghez viszonyítva a lassabb internetelérés. Mivel a 2. rétegű ISP legalább egy kapcsolatnyival távolabb van az internet gerinchálózatától, kissé alacsonyabb a megbízhatóságuk az 1. réteghez képest.

3. réteg

A 3. ábra is mutatja, hogy a 3. rétegű ISP-k 2. rétegű ISP-ktől vásárolják az internetszolgáltatásukat. Ezeknek a szolgáltatásoknak az elsődleges piacai a kiskereskedelem és az otthonok, mégpedig egy adott földrajzi területen belül. A 3. réteg ügyfeleinek általában nincs szükségük a 2. réteg által biztosított szolgáltatások nagy részére. A legfontosabb az internetkapcsolat és a támogatás.

Az ügyfeleknek gyakran alig, vagy szinte semennyi számítástechnikai vagy hálózati tapasztalatuk nincs. A 3. réteg az ügyfelei számára az internetkapcsolatot egy hálózati és számítógépes szolgáltatási szerződéssel egybekapcsolva adja. Habár kisebb a sávszélesség és a megbízhatóság, mint az 1. és 2. réteg szolgáltatói esetén, akár kis- vagy közepes vállalatok számára is megfelelő választás lehet.

Az IPv6-ot az IPv4 utódjának tervezték. Az IPv6 jóval nagyobb, 128 bites címtartományt használ, amely 340 szextillió címet jelent. (Ez a 340-es szám után 36 nullát takar.) Azonban az IPv6 jóval több, mint csak egy nagyobb címtér. Amikor az IETF elkezdte az IPv4 utódjának kidolgozását, ezt a folyamatot egyben arra is használta, hogy az IPv4 korlátait kijavítsa és további fejlesztéseket hozzáadjon. Egy példa erre az Internet Control Message Protocol version 6 (ICMPv6), amely az ICMP IPv4-es változatában (ICMPv4) még nem létező címfeloldást és cím autokonfigurációt is megvalósít. Az ICMPv4 és ICMPv6 a fejezet során később még elő fog kerülni.

Az IPv6 szükségessége

Az IPv6-ra történő átállás motiváló tényezője az IPv4-címtér kimerülése volt. Afrika, Ázsia és a világ más területei egyre nagyobb mértékben kapcsolódnak az internethez, ekkora mértékű növekedéshez nincs elég IPv4-cím. 2011 január 31-én, egy hétfői napon az IANA kiosztotta az utolsó két /8-as IPv4-címblokkot a Regionális Internet Regisztrátoroknak (RIR-ek). Különböző előrejelzések szerint az öt RIR valamikor 2015 és 2020 között fog kifogyni az IPv4-címeikből. Az internetszolgáltatóknak ekkorra kapják meg a maradék IPv4-címeket.

Az IPv4 elméleti maximuma 4.3 milliárd cím körül van. Az RFC 1918 privát címei a hálózati címfordítással (Network Address Translation, NAT) együtt használva valamelyest le tudták lassítani az IPv4-címtartomány kimerülésének folyamatát. De a NAT bizonyos korlátai erősen befolyásolják a végpontok közti kommunikációt.

Dolgok internete

A mai internet lényegesen különbözik attól, amilyen az elmúlt évtizedekben volt. Az internet ma több, mint e-mail, weboldalak és gépek közti fájlátvitel. A folyamatosan fejlődő internet a dolgok internetévé válik. Már nem csak a számítógépek, táblagépek és okostelefonok fogják használni az internetet. A holnap érzékelőkkel felszerelt internetképes eszközei közé fog tartozni minden az autóktól és orvosi eszközöktől kezdve egészen a háztartási gépekig és természetes ökoszisztémákig. Képzeljünk el egy találkozót az ügyfelünk irodájában, melyet a naptár alkalmazásunk automatikusan beidőzített a szokásos munkaidőnk előtt 1 órával való kezdésre. Ez jelentős probléma lehet, főleg ha elfelejtjük megnézni a naptárt vagy helyesen beállítani az ébresztőt. Most képzeljük el azt, hogy a naptár alkalmazás ezt automatikusan közli az ébresztőórával és az autónkkal is. Az autó automatikusan leolvasztja a jeget a szélvédőről mire beülünk és megtervezi az utat a találkozónkhoz.

A növekvő internetes populáció, az IPv4-címtartomány korlátozott mérete, a NAT problémái, a Dolgok internete mind azt bizonyítják, hogy itt az idő IPv6-ra váltani.

Az IPv6-ra váltásnak nincs lerögzített határideje. A belátható jövőben az IPv4 és az IPv6 együtt fog létezni. Az átmenet várhatólag évekig fog tartani. Az IETF különféle protokollokat és eszközöket fejlesztett ki a hálózati rendszergazdák számára, hogy elősegítsék az IPv6-ra történő átállást. Az áttérési technikákat három kategóriába soroljuk:

- **Kettős protokollkészlet (dual stack)** - Az 1. ábrán látható, hogy a kettős protokollkészlet lehetővé teszi az IPv4 és az IPv6 együttműködését azonos hálózaton. A dual stack eszközök egyszerre futtatják az IPv4 és az IPv6 protokollkészletet is.

- **Tunneling (alagút technika)** - Az alagút technika olyan megoldás, amely IPv6 csomagot szállít át IPv4 hálózaton (2. ábra). Az IPv6 csomagot pont ugyanúgy ágyazzák be egy IPv4 csomagba, mint bármely más adatot.

- **Címfordítás** - A 3. ábrán láthatjuk, hogy a Network Address Translation 64 (NAT64) lehetővé teszi az IPv6-képes eszközök számára, hogy az IPv4 NAT-jához hasonló fordítási technika használatával képesek legyenek más IPv4-es eszközökkel történő kommunikációra. Az IPv6 csomagot IPv4 csomaggá fordítják át és fordítva.
  - Ellentétben az IPv4-címekkel, melyeket pontokkal elválasztott decimális formában használunk, az IPv6-címeket hexadecimális formában írjuk. A Wireshark "Packets Byte" nézetében korábban már találkozhattunk hexadecimális számokkal. Wireshark-ban a hexadecimális értékek a keretek és csomagok bináris tartalmát mutatják. Az Ethernet Media Access Control (MAC) címeinél szintén hexadecimális ábrázolást használunk.
  - **Hexadecimális számok**
  - A hexadecimális (tizenhatos, "hexa") a bináris értékek ábrázolásának egy kényelmes módja. Amint a decimális számrendszer alapja a tíz, a binárisé a kettő, a hexadecimális alapszáma a tizenhat.
  - A 16 alapú számrendszer 0-tól 9-ig használja a számokat, majd A-tól F-ig a betűket. Az első ábra a megfelelő decimális, bináris és hexadecimális értékeket mutatja meg. Négy bitnek 16-féle kombinációja van 0000 és 1111 között. A 16 jegyű hexadecimális azért tökéletes számunkra, mert négy bitet pontosan egy hexadecimális számjegy írhat le.
  - **A byte fogalma**
  - Mivel 8 bit alkot egy bináris csoportot (vagy bájtot), a bináris 00000000-11111111 közti értékeket a hexadecimális 00-tól FF-ig terjedő tartománnyal lehet kifejezni. A teljes 8 bites ábrázoláshoz a vezető nullákat is használnunk kell. Például a 0000 1010 bináris értéket hexadecimális 0A-ként írjuk le.
  - **Hexadecimális értékek ábrázolása**
  - **Megjegyzés**: A 0 és 9 közé eső közös karakterek miatt nagyon fontos, hogy megkülönböztessük a hexadecimális és a decimális számokat egymástól.
  - A hexadecimális értékeket szövegesen vagy a számot megelőző 0x (például 0x73), vagy alsó indexbe írt 16-os számmal jelezzük. Ritkábban követheti H betű is, például 73H. Mivel parancssorban vagy programozási környezetben alsó indexet nem használhatunk, műszaki leírásban a hexadecimális értékeket a "0x" (nulla X) előzi meg. Ezért a fenti példák így jelennek meg: 0x0A és 0x73.
  - **Hexadecimális számok átváltása**
  - A decimális és hexadecimális számok közti átváltás nem bonyolult művelet, de gyorsan osztani vagy szorozni 16-tal nem mindig könnyű.
  - Egy kis gyakorlattal fel lehet ismerni a decimális és hexadecimális számoknak megfelelő bitmintákat. A 2. ábra néhány 8 bites értékhez tartozó mintát mutat.
  - Az IPv6-címek 128 bit hosszúak és hexadecimális értékek sorozataként írjuk fel őket. Mivel négy bit ad ki egy hexadecimális számjegyet, így a cím 32 hexadecimális számjegyből áll. Az IPv6-címek esetén nem különböztetjük meg a kis- és nagybetűket, bármelyiket használhatjuk.
  - **Preferált (előnyben részesített, elsődleges) formátum**
  - Ahogy az első ábrán látjuk, az IPv6-címek preferált formátuma x:x:x:x:x:x:x:x, ahol minden "x" négy hexadecimális értéket helyettesít. Az IPv4-címek 8 bites részeit oktettnek hívtuk. IPv6-ban egy 16 bites címrész vagyis négy hexadecimális érték nem hivatalos elnevezése hextett. Minden "x" egy-egy hextettet, azaz 16 bitet vagyis négy hexadecimális számjegyet jelent.
  - Az IPv6-címek preferált (előnyben részesített, elsődleges) formátuma az, amikor mind a 32 hexadecimális számjegyet kiírjuk. Ami nem feltétlenül jelenti azt, hogy ez egyben az IPv6-címek megjelenítésének ideális formátuma is lenne. A következő oldalakon megismerünk két szabályt, amelyeknek segítségével az IPv6-cím számjegyeinek száma lényegesen lerövidíthető.
  - A második ábra néhány példát mutat a preferált formátumú IPv6-címekre.

Az első szabály az IPv6-címek rövidítésekor az, hogy a 16 bites részek vagy hextettek vezető nulláit elhagyhatjuk. Például:

- a 01AB lehet 1AB

- a 09F0 lehet 9F0
- a 0A00 lehet A00
- a 00AB lehet AB

A szabály csak a vezető nullákra alkalmazható, a záró nullákra nem, különben a rövidítés nem lenne egyértelmű. Például az "ABC" hextettről nem tudnánk eldönteni, hogy "0ABC" vagy "ABC0" volt-e.

Az 1-8. ábrákon több példát láthatunk arra, hogy a vezető nullák elhagyása hogyan csökkenti az IPv6-címek méretét. Minden példához látható a teljes (preferált) forma is. Figyeljük meg, hogy a vezető nullák elhagyása a legtöbb példában kisebb címet eredményez.

Az IPv6-címek megjelenésének rövidítésére a második szabály az, hogy bármelyik, csak nullákat tartalmazó 16 bites szegmens (hextett) sorozat helyettesíthető dupla kettősponttal (::).

A dupla kettőspont (::) egy címen belül csak egyszer használható, különben több lehetséges cím rövidítése is ugyanaz lenne. A vezető nullák elhagyásával együtt használva az IPv6-címek mérete lényegesen lerövidül. Ezt időnként tömörített formátumnak hívják.

Egy helytelen cím:

- 2001:0DB8::ABCD::1234

A helytelen cím többféleképpen is bővíthető:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Az 1-7. ábrák több példát is mutatnak arra, hogy a dupla kettőspont és a vezető nullák elhagyása hogyan csökkenti az IPv6-címek méretét.

Az IPv6-címeknek három típusa van:

- **Egyedi címzés (unicast)** - Az IPv6 egyedi cím egyedileg azonosítja egy IPv6-képes készülék valamely interfészét. Amint az ábrán is láthatjuk, a forrás IPv6-címnek egyedi címnek kell lennie.
- **Csoportos címzés (multicast)** - Az IPv6 csoportcím arra való, hogy egyetlen IPv6 csomagot több címzettnek is elküldjünk.
- **Bárki címzés (Anycast)** - Az IPv6 anycast cím olyan IPv6-cím, amelyet több eszközhöz is hozzá lehet rendelni. Az anycast címre küldött csomagot ahhoz a legközelebbi eszközhöz irányítják, amelynek ez a címe. Az anycast címek használatát ebben a kurzusban nem részletezzük.

Az IPv4-gyel ellentétben IPv6-ban nincsenek szórási címek. Viszont van egy IPv6 minden állomás multicast cím (all-node multicast address), ami lényegében ugyanezt az eredményt adja.

Emlékezzünk rá, hogy az IPv4-cím előtagját (prefixumát) vagy hálózat részét pontokkal elválasztott decimális alhálózati maszk formájában vagy prefixummal (peres jelöléssel) azonosíthatjuk. Például a

192.168.1.10 IP-cím pontozott decimális alhálózati maszkja 255.255.255.0, amit így is írhatunk: 192.168.1.10/24.

Az IPv6 az előtag hosszát használja a cím előtag részének meghatározására. A pontozott decimális alhálózati maszk jelölést IPv6-nál nem használjuk. Az előtag hossz jelöli ki az IPv6-cím hálózat részét az IPv6-cím/előtag hossz jelöléssel.

Az előtag hossza 0 és 128 közé eshet. A tipikus IPv6 előtag hossz LAN-ok és a legtöbb egyéb hálózat esetén /64. Ez azt jelenti, hogy az előtag, avagy a cím hálózat része 64 bit hosszú, ami az interfész azonosító (állomás rész) számára szintén 64 bitet hagy.

Az IPv6 egyedi cím egy IPv6-képes eszköz interfészét azonosítja. Az egyedi címre küldött csomagot az az interfész fogadja, amelyhez a címet rendelték. Az IPv4-hez hasonlóan a forrás IPv6-címnek is egyedi címnek kell lennie. A cél IPv6-cím lehet akár egyedi, akár multicast cím is.

Hatféle IPv6 egyedi cím típust különböztetünk meg.

Globális egyedi cím (global unicast)

A globális unicast cím a publikus IPv4-címekre hasonlít. Az ilyen címek globálisan egyedi, interneten továbbítható címek. A globális unicast címeket konfigurálhatjuk statikusan, vagy kioszthatjuk dinamikusan is. Az IPv4 DHCP-hez képest néhány fontos különbség van abban, hogy az eszköz hogyan kapja meg dinamikusan az IPv6-címét.

Adatkapcsolati szinten helyi (link-local)

A link-local címeket az azonos helyi kapcsolaton levő eszközökkel történő kommunikációra használják. IPv6-nál a kapcsolat kifejezés az alhálózatra vonatkozik. A link-local címek csak egyetlen kapcsolatra korlátozódnak. Az egyediségüket csak a kapcsolaton belül kell biztosítani, mert azon túlra nem továbbítódnak. Vagyis a forgalomirányítók link-local forrás- vagy célcímekkel rendelkező csomagokat nem továbbítanak.

Visszacsatolás (loopback)

A loopback címet arra használja az állomás, hogy saját magának küldhessen csomagot, az ilyen címet fizikai interfészhez nem rendelhetjük. Az IPv4 loopback címhez hasonlóan egy IPv6 loopback címet is megpingelhetünk a helyi állomás TCP/IP konfigurációjának leteszteléséhez. Az IPv6 loopback cím az utolsó bit 1-esét kivéve csupa nulla, ami ::1/128 vagy tömörített formában csak ::1.

Meghatározatlan (unspecified) cím

A meghatározatlan cím csupa nullákból áll, tömörített formátumban ::/128 vagy csak simán ::. Nem rendelhető hozzá interfészhez és IPv6 csomagnak csak forráscíme lehet. Akkor láthatunk meghatározatlan címet forráscímként, amikor az eszköz még nem rendelkezik végleges IPv6-címmel, vagy ha a csomag forrása a cél számára lényegtelen.

Egyedi helyi (egyedi lokális, unique local)

Az IPv6 egyedi lokális címek mutatnak némi hasonlóságot az IPv4 RFC 1918 privát címeivel, de van néhány lényeges különbség is közöttük. Az egyedi lokális címeket helyi címzésre használják egy adott helyen vagy korlátozott számú helyszínek között. Az ilyen címeket a globális IPv6 hálózatba nem szabad továbbítani. Az egyedi lokális címek tartománya FC00::/7 és FDFF::/7 közötti.

IPv4-ben a privát címek használatát NAT/PAT megoldással kombinálva egyfajta több az egyhez címfordítást kapunk a privát és publikus címek között. Ezt a technológiát az IPv4-címtartomány korlátozott mérete miatt használjuk. Számos telephely az RFC 1918 címek privát tulajdonságát használja ki arra is, hogy biztonságosabbá tegye a hálózatát, vagy elrejtse azt a biztonsági támadások

elől. Ezeknek a technológiáknak azonban nem ez a célja, az IETF javaslata szerint a megfelelő biztonsági megoldásokat az internetre kapcsolódó forgalomirányítón kell megvalósítani. Bár az IPv6 helyspecifikus címzést is biztosít, az viszont nem arra való, hogy segítsen elrejteni IPv6-képes eszközeinket az internet elől. Az IETF továbbra is azt javasolja, hogy az eszközeink elérésének korlátozását a legjobb gyakorlat szerinti biztonsági módszerekkel valósítsuk meg.

Megjegyzés: Az IPv6 eredeti specifikációja tartalmazott helyen belüli (site-local) címeket hasonló célra, az FEC0::/10 tartományban. A specifikáció számos kétértelműsége miatt az IETF visszavonta a site-local címeket az egyedi lokális címek javára.

Beágyazott IPv4

Az utolsó egyedi címtípus a beágyazott IPv4-cím. Az ilyen címeket az IPv4-ről IPv6-ra történő átállás elősegítésére használjuk. A beágyazott IPv4-címek túlmutatnak a kurzus anyagán.

Az IPv6 link-local címek lehetővé teszik, hogy az eszköz kommunikáljon a vele közös kapcsolaton lévő más IPv6-képes eszközökkel, de csak ezen az egy kapcsolaton (alhálózaton) lévőkkel. Azok a csomagok, amelyeknek a forrása vagy célja link-local cím nem továbbíthatók a kiinduló kapcsolaton kívülre.

Az IPv4 link-local címekkel ellentétben az IPv6 link-local címeknek jelentős szerepük van a hálózat különböző vonatkozásaiban. A globális egyedi cím nem szükséges, link-local címmel viszont minden IPv6-képes hálózati interfésznek rendelkeznie kell.

Ha az interfészen nem állítunk be kézzel link-local címet, az eszköz automatikusan létrehoz magának egyet DHCP-szerver nélkül is. Az IPv6-képes állomások akkor is létrehoznak maguknak IPv6 link-local címet, ha globális egyed címet nem rendeltünk az eszközhöz. Ez lehetővé teszi azt, hogy azonos alhálózaton belül az IPv6-képes eszközök kommunikálhassanak egymással. Ebbe az alapértelmezett átjáróval (forgalomirányítóval) való kommunikáció is beletartozik.

Az IPv6 link-local címek az FE80::/10 tartományban vannak. A /10 azt jelenti, hogy az első 10 bit 1111 1110 10xx xxxx. Az első hextet tartománya 1111 1110 10**00 0000** (FE80) és 1111 1110 10**11 1111** (FEBF) közé esik.

Az első ábra egy IPv6 link-local címekkel zajló kommunikációra mutat példát.

A második ábra az IPv6 link-local cím formátumát mutatja.

Az IPv6 forgalomirányító protokollok is IPv6 link-local címeket használnak a következő ugrás címeként, amikor üzeneteket cserélnek egymással. A link-local címeket a kurzus folyamán később még részletesen tárgyaljuk.

Megjegyzés: Általában a forgalomirányító link-local címe az, amit az eszközök egy kapcsolatban alapértelmezett átjáróként használnak, nem pedig a globális egyedi címe.

Az IPv6 globális egyedi címzésű címek globálisan egyediek és továbbíthatók az interneten. Ezek a publikus IPv4-címek megfelelői. Az ICANN (Internet Committee for Assigned Names and Numbers) és az IANA (Internet Assigned Numbers Authority) üzemeltetői osztják ki az IPv6-címblokkokat az öt RIR számára. Jelenleg csak azokat a globális egyedi címeket osztják ki, amelyek első három bitje 001 (2000::/3). Ez az elérhető IPv6-címtartománynak csupán az 1/8 része, kivéve egy egészen kis részt, amit más típusú egyedi és csoportos címzés használ.

Megjegyzés: A 2001:0DB8::/32 címet dokumentációs célokra tartják fenn, beleértve a példákban való használatot is.

Az első ábra a globális egyedi címek szerkezetét és tartományát mutatja.

A globális egyedi cím három részből áll:

- globális forgalomirányító előtag
- alhálózat azonosító
- interfész azonosító

Globális forgalomirányító előtag

A globális forgalomirányító előtag vagy hálózat rész a cím azon része, amelyet a szolgáltató, például internetszolgáltató rendel hozzá egy ügyfélhez vagy telephelyhez. Jelenleg a RIR-ek /48-as globális előtagot adnak az ügyfeleknek. Ebbe a céges üzleti hálózatoktól az egyéni háztartásokig mindenki beletartozik. Ez a legtöbb ügyfél számára több, mint elég címet jelent.

A második ábra a globális egyedi cím szerkezetét mutatja /48-as globális forgalomirányító előtag használata esetén. A /48-as a leggyakrabban kiosztott globális előtag, a legtöbb példában ezt fogjuk használni a kurzus folyamán.

Például a 2001:0DB8:ACAD::/48 IPv6-cím azt jelenti, hogy az első 48 bit (3 hextett) (2001:0DB8:ACAD) a cím előtagja vagy hálózat része. A /48 előtag hossz előtti dupla kettőspont azt jelenti, hogy a cím további része csupa 0.

Alhálózat azonosító

Az alhálózat azonosítót a szervezet a saját telephelyén belüli alhálózatok azonosítására használhatja.

Interfész azonosító

Az IPv6 interfész azonosító az IPv4-cím állomás részének felel meg. Azért interfész azonosítónak hívjuk, mert egyetlen állomásnak lehet több interfésze és mindegyik interfésznek lehet egy vagy akár több IPv6-címe is.

Megjegyzés: Az IPv4-gyel ellentétben IPv6-ban a csupa nullás címet is kiadhatjuk állomásnak, mert nincsenek szórási címek. A csupa nulla cím viszont fenntartott, ez az alhálózat forgalomirányító anycast címe, ezt csak forgalomirányítóknak lehet kiosztani.

Az IPv6-címek olvasásának egyszerű módja, ha megszámoljuk a hextetteket. Ahogy a harmadik ábra mutatja, a /64-es globális egyedi címben az első négy hextett a cím hálózat része, amiből a negyedik az alhálózat azonosító. A maradék négy hextett pedig az interfész azonosító.

Forgalomirányító konfigurálása

A legtöbb konfigurációs és ellenőrző parancs IPv6 megfelelője Cisco IOS alatt hasonló az IPv4-es változathoz. Sok esetben mindössze annyi a különbség, hogy az **`ipv6`** kulcsszót használjuk az **`ip`** helyett a parancsokban.

A(z) **`interface`** parancs IPv6 globális egyedi cím konfigurálására egy adott interfészen: **ipv6 address** *ipv6-address/előtag-hossz*.

Figyeljünk rá, hogy nincs szóköz közöttük: *ipv6-address*és *előtag-hossz*.

A minta konfiguráció az 1. ábra topológiáját használja a következő IPv6 alhálózatokkal:

- 2001:0DB8:ACAD:0001:/64 (*vagy*2001:DB8:ACAD:1::/64)

- 2001:0DB8:ACAD:0002:/64 (*vagy*2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (*vagy*2001:DB8:ACAD:3::/64)

A második ábrán látható, hogy az R1 Gigabit Ethernet 0/0 interfészének globális egyedi IPv6-címét beállító parancsok a következők:

```
Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ipv6 address 2001:db8:acad:1::1/64

Router(config-if)#no shutdown
```

Állomás konfiguráció

Egy állomás IPv6-címének beállítása hasonló, mintha IPv4-címet adnánk meg.

Ahogy a harmadik ábrán is látható, a PC1 alapértelmezett átjárója a 2001:DB8:ACAD:1::1, ami az R1 forgalomirányító ugyanezen a hálózaton levő Gigabit Ethernet interfészének globális egyedi címe.

Konfiguráljunk IPv6 globális egyedi címet a 4. ábra szimulált parancssorával!

Ugyanúgy, mint az IPv4-nél, nagyobb hálózatokban nem praktikus a klienseknek statikusan adni a címeket. Emiatt a legtöbb IPv6-hálózat rendszergazdája az IPv6-címek dinamikus hozzárendelését alkalmazza.

Két módja van annak, hogy egy eszköz hogyan szerezheti be automatikusan IPv6 globális egyedi címét:

- Állapotmentes Cím Autokonfiguráció (Stateless Address Autoconfiguration, SLAAC)
- DHCPv6

Állapotmentes Cím Autokonfiguráció (Stateless Address Autoconfiguration, SLAAC)

Az Állapotmentes Cím Autokonfiguráció (SLAAC) olyan módszer, ami lehetővé teszi az eszköz számára, hogy beszerezze a prefixumot, a prefixum hosszát és az alapértelmezett átjáró címét egy *IPv6 forgalomirányító*eszköztől DHCPv6 szerver nélkül is. SLAAC használatakor az eszköz a helyi forgalomirányító ICMPv6 forgalomirányító hirdetés (Router Advertisement, RA) üzeneteiből szerzi be a szükséges információkat.

Az IPv6 forgalomirányítók rendszeres időközönként küldenek ki ICMPv6 forgalomirányító hirdetés (Router Advertisement, RA) üzeneteket a hálózat minden IPv6-képes eszközének. Alapértelmezésben a Cisco forgalomirányítók minden 200. másodpercben kiküldik ki az RA üzeneteiket az IPv6 minden állomás multicast címre. Az IPv6 eszköznek viszont nem kell kivárnia a következő RA üzenetet. Küldhet egy forgalomirányító keresés (Router Solicitation, RS) üzenetet a routernek a minden router (multicast) csoportcímre. Ha egy IPv6 forgalomirányító RS üzenetet kap, azonnal válaszolni fog egy forgalomirányító hirdetéssel.

Attól, hogy egy Cisco forgalomirányító interfésznek IPv6-címet állítunk be, még nem lesz azonnal "IPv6 forgalomirányító". Az IPv6 forgalomirányító olyan forgalomirányító, amely:

- IPv6 csomagokat továbbít hálózatok között.
- Statikus IPv6 útvonalakat, vagy dinamikus IPv6 forgalomirányító protokollt lehet beállítani rajta.

- ICMPv6 RA üzeneteket küld.

Az IPv6 forgalomirányítás alapértelmezés szerint nincs engedélyezve. Egy forgalomirányítót IPv6 forgalomirányítóvá tehetünk az **`ipv6 unicast-routing`**globális konfigurációs parancs kiadásával.

Megjegyzés: A Cisco forgalomirányítók alapértelmezés szerint IPv4 forgalomirányítóként üzemelnek.

Az ICMPv6 RA üzenete tartalmazza a prefixumot, a prefixum hosszát és további információkat az IPv6 eszközök számára. Az RA üzenet arról is tájékoztatja az IPv6 eszközt, hogy a címzési információt milyen módon szerezheti be. Az ábrán látható háromféle lehetőség közül választhat:

- **1. lehetőség - Csak SLAAC** - Az eszköznek az RA üzenetben lévő előtagot, előtag-hosszot és átjáró címet kell használnia. Egyéb információt a DHCPv6 szervertől sem fog kapni.

- **2. lehetőség - SLAAC és DHCPv6 együtt** - Az eszköznek az RA üzenetben lévő előtagot, előtag-hosszot és alapértelmezett átjáró címet kell használnia. A DHCPv6 szervertől viszont egyéb információt is kaphat, ilyen lehet például a DNS-szerver címe. Az eszköz végig futtatja a DHCPv6 szerver keresésének és lekérdezésének normális folyamatát azért, hogy ezt a plusz információt megkapja. Ezt állapotmentes DHCPv6-nak hívják, mert a DHCPv6 szervernek nem kell címeket kiosztania és követnie a hozzárendelt címeket, csak kiegészítő információkat biztosít, mint például a DNS-szerver címe.

- **3. lehetőség - Csak DHCPv6** - Az eszköz nem használhatja az RA üzenet információit a címének beállításához. Ehelyett a címzési információit normál módon, DHCPv6 szerver keresése és lekérdezése útján kell, hogy beszerezze. IPv6 globális egyedi címet, prefixum hosszot, alapértelmezett átjáró címet és DNS-szerver címeket fog kapni. Ebben az esetben a DHCPv6-szerver ugyanolyan állapottartó (állapotkövető) DHCP-szerverként fog üzemelni, mint amilyen az IPv4 DHCP szolgáltatása is. A DHCPv6 szerver kiosztja és nyomon követi az IPv6-címeket, hogy több eszköz ne kapja ugyanazt a címet.

A forgalomirányítók ICMPv6 RA üzeneteinek forrás IPv6-címe a link-local címük. Az SLAAC-t használó eszközök a router link-local címét használják alapértelmezett átjárónak.

DHCPv6

Az IPv6 Dinamikus Hoszt Konfigurációs Protokollja (DHCPv6) hasonló az IPv4 DHCP-hez. Az eszköz automatikusan megkaphatja a címzési információkat (globális egyedi cím, előtag hossz, alapértelmezett átjáró, DNS-szerverek címei) egy DHCPv6 szerver szolgáltatásainak segítségével.

Az eszköz minden IPv6-címzési információt vagy csak egy részét a DHCPv6 szervertől kapja meg attól függően, hogy a második (SLAAC és DHCPv6) vagy a harmadik (csak DHCPv6) lehetőséget adták meg az ICMPv6 RA üzenetben. Ezen felül az állomás operációs rendszere figyelmen kívül hagyhatja a forgalomirányító RA üzenetének tartalmát és dönthet úgy, hogy az IPv6-címét és információit közvetlenül DHCPv6 szervertől szerzi be.

Az IPv6-képes eszközök hálózatba kapcsolása előtt hasznos lehet ellenőrizni, hogy az állomás figyelembe veszi-e a forgalomirányító ICMPv6 RA üzeneteinek beállításait.

Az eszköz dinamikusan is beszerezheti az IPv6 globális egyedi címét, valamint több statikus IPv6-címet is beállíthatunk ugyanazon az interfészen. Az IPv6 több IPv6-címet is megenged beállítani egy interfésznek ugyanabból az IPv6 hálózatból.

Az eszköznek egynél több alapértelmezett átjáró címet is meg lehet adni. Az RFC 6724-ben (Alapértelmezett Cím Kiválasztása IPv6-ban, Default Address Selection for IPv6) további információkat találhatunk arról, hogy milyen módon dönt az eszköz a forráscímének és alapértelmezett átjárójának megválasztásáról.

Az interfész azonosító

Ha a kliens nem használja az RA üzenet információit és csak a DHCPv6-ra támaszkodik, akkor a DHCPv6 szerver fogja az egész IPv6 globális egyedi címet adni, beleértve az előtagot és az interfész azonosítót is.

Azonban az 1. (csak SLAAC) vagy a 2. lehetőség (SLAAC DHCPv6 segítségével) használata esetén a kliens nem fogja megkapni a tényleges interfész azonosítót. Saját magának kell meghatároznia a 64 bites interfész azonosítóját akár az EUI-64 művelettel, akár egy 64 bites véletlen szám generálásával.

Az EUI-64 módszer

Az IEEE meghatározott egy Kiterjesztett Egyedi Azonosító (Extended Unique Identifier, EUI) vagy módosított EUI-64 nevű folyamatot. A művelet a kliens 48 bites Ethernet MAC-címének közepébe beszúr további 16 bitet, így állítja elő a 64 bites interfész azonosítót.

Az Ethernet MAC-címeket legtöbbször hexadecimális formában ábrázoljuk és a címek két részből állnak:

- **Szervezeti Egyedi Azonosító (Organizationally Unique Identifier, OUI)** - Az OUI az IEEE által kiosztott 24 bites (6 hexadecimális számjegy) gyártói kód.
- **Eszközazonosító** - Az eszközazonosító szintén 24 bit (6 hexadecimális számjegy), az OUI-n belül egyedi.

Az EUI-64 interfészazonosítót binárisan ábrázoljuk és három részből áll:

- A kliens MAC-címének 24 bites OUI része, amelyben a hetedik bit (az univerzális/helyi (U/L) bit) invertált. Tehát ha a hetedik bit 0, akkor 1 lesz és fordítva.
- A 16 bites FFFE (hexadecimális) érték közbeszúrva.
- A MAC-cím 24 bites eszközazonosító része.

Az EUI-64 folyamatát az 1. ábra mutatja be az R1 Gigabit Ethernet MAC-címével, ami FC99:4775:CEE0.

1. lépés: A MAC-cím kettéosztása az OUI és az eszközazonosító között.

2. lépés: A hexadecimális FFFE beszúrása, ami binárisan 1111 1111 1111 1110.

3. lépés: Az OUI első 2 hexadecimális számjegyének binárissá alakítása, az U/L bit (7. bit) invertálása. Ebben a példában a hetedik bit 0, amiből tehát 1 lesz.

Az eredmény az EUI-64 generált interfész azonosító: FE99:47FF:FE75:CEE0.

Megjegyzés: Az U/L bit szerepét és az invertálásának okát az RFC 5342 tárgyalja.

Az EUI-64 előnye az, hogy egy interfész azonosító generálható az Ethernet MAC-cím segítségével. Lehetővé teszi a hálózat rendszergazdáinak azt is, hogy az egyedi MAC-cím alapján az IPv6-címet egészen a végberendezésig követhessék. Azonban ez sok felhasználóban adatvédelmi aggályokat ébresztett. Attól tartanak, hogy a csomagjaikat a tényleges fizikai számítógépükig követhetik. Ezen aggályok miatt használhatunk véletlenszerűen generált interfész azonosítót is.

Véletlenszerűen generált interfész azonosító

Operációs rendszertől függően az eszköz a MAC-cím és az EUI-64 algoritmus helyett véletlenszerűen generált interfész azonosítót is használhat. Például a Windows operációs rendszerek a Vista verzióval kezdődően az EUI-64 helyett már véletlenszerűen generált interfész azonosítót használnak. A Windows XP és a korábbi Windows operációs rendszerek az EUI-64-et alkalmazták.

A második ábrán egy egyszerű módszert láthatunk annak megállapítására, hogy egy cím nagy valószínűséggel EUI-64-gyel készült vagy sem, csak meg kell néznünk, hogy az interfész azonosító közepén megtalálható-e az FFFE rész.

Miután az EUI-64, vagy a véletlen generálás eredményeképpen előállt interfész azonosítót az IPv6 előtaggal összekombináljuk létrejön egy globális egyedi cím, vagy egy link-local cím:

- **Globális egyedi cím** - SLAAC használata esetén az eszköz az ICMPv6 RA üzenetből megkapott előtagot kombinálja az interfész azonosítójával.

- **Link-local cím** - A link-local előtag FE80::/10-zel kezdődik. Általában FE80::/64-es előtagot/előtag hosszot használnak, ami után az interfész azonosító következik.

SLAAC használata esetén (akár csak SLAAC, akár SLAAC DHCPv6-tal együtt) az eszköz az előtagot és az előtag hosszát az ICMPv6 RA üzenetből szerzi. Mivel a cím előtagját az RA üzenet már meghatározta, az eszköznek csak a cím interfész azonosító részét kell biztosítania. Amint korábban említettük, az interfész azonosítót generálhatjuk az EUI-64 művelettel, vagy az operációs rendszertől függően véletlenszerűen. Az RA üzenet információiból és az interfész azonosítóból az eszköz már meg tudja határozni a globális egyedi címét.

Miután az interfészhez hozzárendeltük a globális egyedi címet, az IPv6-képes eszköz automatikusan generál egy link-local címet. MInden IPv6-képes eszköznek legalább link-local címének lennie kell. Emlékezzünk vissza arra, hogy az IPv6 link-local cím lehetővé teszi az IPv6-képes eszközök számára az alhálózatukon belüli kommunikációt egymással.

Az IPv6 link-local címeket különböző célokra használjuk:

- Az állomás a helyi forgalomirányító link-local címét használja az alapértelmezett átjáró címeként.

- A forgalomirányítók link-local címek segítségével cserélik ki a dinamikus forgalomirányító protokollok üzeneteit.

- A routerek forgalomirányító táblái az IPv6 csomag továbbításakor használt következő ugrás címnél link-local címet tartalmaznak.

A link-local cím beállítható dinamikusan vagy konfigurálhatjuk kézzel is, mint statikus link-local cím.

Dinamikusan hozzárendelt link-local cím

A link-local címet dinamikusan hozzuk létre FE80::/10 előtaggal és az interfész azonosítóval.

A Cisco IOS-t futtató forgalomirányítók IPv6 interfészein alapértelmezésben az EUI64-gyel generálják a link-local címek interfész azonosítóját. Soros interfészek esetén a forgalomirányító egy Ethernet interfész MAC-címét fogja használni. Ne feledjük, hogy a link-local címnek csak ezen a kapcsolaton vagy hálózaton belül kell egyedinek lennie. A dinamikusan kiosztott link-local címek hátrányaként a hosszukat lehet megemlíteni, ami miatt nehéz felismerni és emlékezni a kiosztott címekre.

Statikus link-local cím

A link-local címek manuális konfigurálása lehetővé teszi, hogy olyan címet alkossunk, ami felismerhető és könnyen megjegyezhető.

A link-local címet ugyanúgy állítjuk be manuálisan, mint ahogy IPv6 globális egyedi címet adunk meg, de egy további paramétert kell használnunk az interfész parancs után:

```
Router(config-if)#ipv6 address link-local-address link-local
```

Az első ábrán látható, hogy a link-local cím előtagja az FE80 és FEBF közé eső tartományban van. Ha a cím ezzel a hextettel (16 bites rész) kezdődik, a címet a link-local paraméternek kell követnie.

A második ábra a link-local cím konfigurációját mutatja az**`ipv6 address interface`** paranccsal. Azért használjuk az FE80::1 link-local címet, hogy könnyebben megjegyezhessük, hogy az R1 forgalomirányítóhoz tartozik. Ugyanezt az IPv6 link-local címet beállíthatjuk R1 összes interfészén is. Sőt akár minden kapcsolatra is beállítható lenne ugyanez az FE80::1 cím, mert csak a kapcsolaton belül kell egyedinek lennie.

Az R1-hez hasonlóan R2 minden interfészére beállítjuk az FE80::2 IPv6 link-local címet.

Amint az első ábrán is láthatjuk, az IPv6 interfész konfiguráció ellenőrzésének parancsa hasonló az IPv4-nél használt parancshoz.

A **`show interface`** parancs kiírja az Ethernet interfészek MAC-címeit. Az EUI-64 ezt a MAC-címet használja a link-local cím interfész azonosítójának előállításához. Továbbá a **`show ipv6 interface brief`** parancs egy rövidített kimenetet jelenít meg minden interfészhez. Az interfésszel azonos sorban megjelenő `[up/up]` rész az interfész első/második rétegbeli állapotát jelenti. Ez a megfelelő IPv4 parancs Status és Protocol oszlopainak felel meg.

Figyeljük meg, hogy minden interfésznek két IPv6-címe van. Az interfészek esetén a második cím az a globális egyedi cím, amit beállítottunk neki. Az FE80-nal kezdődő első cím pedig az interfész link-local egyedi címe. Emlékezzünk vissza, hogy a link-local címet automatikusan kapja meg az interfész, ha globális egyedi címet rendelünk hozzá.

Figyeljük meg azt is, hogy az R1 soros 0/0/0 interfészének link-local címe ugyanaz, mint a Gigabit Ethernet 0/0 interfészé. A soros interfészeknek nincs Ethernet MAC-címük, ezért a Cisco IOS az első elérhető Ethernet interfész MAC-címét használja. Ez azért lehetséges, mert a link-local interfésznek csak a kapcsolaton belül kell egyedinek lennie.

A forgalomirányító interfész link-local-címe lesz a kapcsolaton vagy hálózaton levő eszközök alapértelmezett átjárója.

Ahogy a 2. ábrán látható, a **`show ipv6 route`** parancs használható az IPv6 forgalomirányító táblában levő IPv6 hálózatok és IPv6 interfészcímek ellenőrzésére. A **`show ipv6 route`** parancs csak az IPv6 hálózatokat jeleníti meg, az IPv4 hálózatokat nem.

A forgalomirányító táblában az útvonal melletti C a közvetlenül csatlakoztatott hálózatot jelenti. Ha egy forgalomirányító interfész globális egyedi címmel konfigurált és "up/up" állapotban van, az IPv6 előtag és előtag hossz is bekerül az IPv6 forgalomirányító táblájába mint csatlakoztatott (connected) útvonal.

Az interfészen konfigurált IPv6 globális egyedi cím szintén bekerül a forgalomirányító táblába mint helyi útvonal. A helyi útvonal előtagja /128. A helyi útvonalakat a forgalomirányító tábla arra használja, hogy hatékonyabban dolgozza fel azokat a csomagokat, melyeknek a célcíme a forgalomirányító interfészének címe.

A **`ping`** parancs IPv6 esetén is ugyanúgy használható, mint IPv4-ben, csak itt IPv6-címet adunk meg. A harmadik ábrán is látható, hogy a parancsot az R1 és PC1 közti harmadik rétegbeli kapcsolat ellenőrzésére használjuk. Ha egy forgalomirányítóról link-local címet pingelünk, a Cisco IOS megkérdezi a kimenő interfészt. Mivel a cél link-local cím a forgalomirányító egy vagy több kapcsolatán vagy hálózatán is előfordulhat, az eszköznek tudnia kell, hogy melyik interfészen küldje ki a pinget.

Elenőrizzük az IPv6-cím konfigurációját a 4. ábra parancsszimulátorának segítségével.

Az IPv6 csoportcímek hasonlóak az IPv4 csoportcímekhez. Emlékezzünk vissza a csoportcímre (multicast cím), amely arra való, hogy egyetlen csomagot küldhessünk egy vagy több célhoz (multicast csoportnak). Az IPv6 csoportcímek előtagja FF00::/8.

Megjegyzés: Csoportcím csak célcím lehet, forrás sosem.

Kétfajta IPv6 csoportos cím létezik:

- Assigned (kiosztott vagy kijelölt) multicast
- Solicited (kérelmezett vagy kért) node multicast

Kiosztott multicast

A kiosztott (hozzárendelt) multicast címek bizonyos előre definiált eszközcsoportok számára fenntartott multicast címek. A kijelölt multicast cím olyan egyetlen cím, amellyel közös protokollt vagy szolgáltatást futtató eszközök csoportját érhetjük el. A kijelölt multicast címeket meghatározott protokollokkal kapcsolatban használjuk, ilyen például a DHCPv6.

Két gyakori IPv6 assigned multicast csoport:

- **FF02::1 Minden állomás (all-nodes) multicast csoport** - Ennek a multicast csoportnak minden IPv6-képes eszköz a tagja. A csoportnak küldött csomagot a kapcsolaton vagy a hálózaton lévő összes IPv6 interfész megkapja és feldolgozza. Ennek ugyanaz a hatása, mint az IPv4 szórási címnek. Az ábra egy példát mutat a minden állomás multicast cím használatával történő kommunikációra. Az IPv6 forgalomirányító a minden állomás multicast csoportnak küldi el az ICMPv6 (Internet Control Message Protocol version 6) RA üzeneteket. Az RA üzenetben az IPv6-képes eszközök számára találhatók címzési információk, mint például az előtag, az előtag hossza és az alapértelmezett átjáró.
- **FF02::2 Minden router (All-routers) multicast csoport** - Ez egy olyan multicast csoport, amelynek minden IPv6 forgalomirányító a tagja. A router akkor válik a csoport tagjává, amikor IPv6 routerként engedélyezzük azt neki az **`ipv6 unicast-routing`** globális konfigurációs paranccsal. A csoportnak küldött csomagokat a kapcsolaton vagy hálózaton lévő minden IPv6 router megkapja és feldolgozza.

Az IPv6-képes eszközök az ICMPv6 forgalomirányító keresés (RS) üzeneteket a minden router multicast címre küldik. Az RS üzenet RA üzenetet kér az IPv6 forgalomirányítótól, hogy segítséget kapjon a cím konfigurációjának beállításához.

A solicited-node multicast hasonló a minden állomás (all-nodes) multicast címhez. Emlékezzünk rá, hogy a minden állomás multicast cím lényegében az IPv4 szórással egyenértékű. A hálózat minden eszköze feldolgozza a minden állomás címre küldött forgalmat. Hogy lecsökkentsük azon állomások számát, amelyeknek fel kell dolgozniuk a forgalmat, solicited-node multicast címet használhatunk.

A solicited-node multicast cím olyan cím, amely az eszköz IPv6 globális egyedi címének csak az utolsó 24 bitjével egyezik meg. Csak azoknak az eszközöknek kell feldolgozniuk ezeket a csomagokat, amelyek interfész azonosítójának legkisebb helyiértékű, jobb oldali részén levő 24 bitje megegyezik vele.

Az IPv6 solicited-node multicast cím automatikusan létrejön, amikor globális egyedi vagy link-local egyedi címet állítunk be. Az IPv6 solicited-node multicast cím a speciális FF02:0:0:0:0:FF00::/104 előtag után fűzött 24 bitből (az egyedi cím jobb szélső bitjei) áll.

A solicited-node multicast cím tehát két részből áll:

- **FF02:0:0:0:0:FF00::/104 multicast előtag** - Ez a solicited-node multicast cím első 104 bitje.

- **Legkisebb helyiértékű 24 bit** - Ez a solicited-node multicast cím utolsó (jobb szélső) 24 bitje. Ezek a bitek az eszköz globális egyedi vagy link-local egyedi címéből másolódnak át.

Lehetséges, hogy több eszköznek is ugyanaz lesz a solicited-node multicast címe. Ritkán ugyan, de előfordulhat, hogy az eszközök interfész azonosítójának jobb szélső 24 bitje megegyezik. Ez azonban nem jelent problémát, mert az eszköz a beágyazott üzenetet is feldolgozza, amelyben viszont az eszköz teljes IPv6-címe szerepel.

Habár maga az IP nem megbízható protokoll, a TCP/IP protokollcsalád tartalmaz olyan üzeneteket, amelyek bizonyos hibák előfordulása esetén küldhetők. Ezeket az üzeneteket.az ICMP protokoll szolgáltatásaival küldik el. A céljuk nem az, hogy megbízhatóvá tegyék az IP protokollt, inkább az IP csomagok feldolgozása során felmerült jelenségekről küldenek visszajelzést bizonyos esetekben. Az ICMP üzenetek nem szükségesek, bizonyos hálózatokon belül biztonsági okokból sokszor nem is engedélyezettek.

Az ICMP IPv4 és IPv6 esetén egyaránt rendelkezésre áll. Az IPv4 üzenetküldő protokollja az ICMPv4. Az ICMPv6 ugyanezeket a szolgáltatásokat nyújtja az IPv6 felé, de további funkciókat is tartalmaz. Ha ebben a kurzusban az ICMP kifejezést használjuk, akkor azt egyaránt értjük az ICMPv4-re és az ICMPv6-ra is.

Az ICMP üzenetek száma és az ok, ami miatt kiküldik őket, nagyon kiterjedt. Most csak a leggyakoribbak egy részét tárgyaljuk.

Az ICMPv4 és ICMPv6 közös ICMP üzenetei például:

- állomás visszaigazolás (host confirmation)

- cél vagy szolgáltatás nem elérhető (Destination vagy Service Unreachable)

- időtúllépés (Time exceeded)

- útvonal átirányítás (Route redirection)

Állomás megerősítés

Az ICMP visszhang kérés üzenetet annak a megállapítására használhatjuk, hogy egy állomás üzemel-e. A helyi gép ICMP visszhang kérés üzenetet küld az állomásnak. Ha az állomás elérhető, visszhang válasz üzenettel válaszol. Játsszuk le az ábra animációját az ICMP visszhang kérés/visszhang válasz üzenetek megtekintéséhez. Az ICMP visszhang üzenetei képezik a ping segédprogram alapját is.

Cél vagy szolgáltatás nem elérhető (Destination vagy Service Unreachable)

Ha egy állomás vagy átjáró olyan csomagot kap, amelyiket nem tud kézbesíteni, az ICMP cél nem elérhető üzenetét használhatja arra, hogy a küldőt értesítse a cél vagy a szolgáltatás elérhetetlenségéről. Az üzenet tartalmaz egy kódot, amely leírja, hogy a csomagot miért nem sikerült kézbesíteni.

Az ICMPv4 cél nem elérhető üzenetének néhány kódja és jelentésük:

- 0 - hálózat nem elérhető

- 1 - állomás nem elérhető

- 2 - protokoll nem elérhető

- 3 - port nem elérhető

Megjegyzés: Az ICMPv6 hasonló, de kissé más kódokat használ a cél nem elérhető üzenetekben.

Időtúllépés

Az ICMPv4 időtúllépés üzenetet forgalomirányítók használják akkor, ha a csomagot nem továbbíthatják, mert az élettartam (Time To Live, TTL) mezőjének értéke nullára csökkent. Ha egy forgalomirányító elfogad egy csomagot, és a TTL érték csökkentése után az új érték nulla lesz, eldobja a csomagot, majd időtúllépés üzenetet küld a küldőnek.

Az ICMPv6 szintén időtúllépés üzenetet küld, ha a forgalomirányító nem tudja továbbítani az IPv6 csomagot, mert az élettartama lejárt. Az IPv6-nál nem TTL mezőt használnak, hanem az ugrás korlát (hop limit, ugrás limit) nevű mező jelzi, ha a csomag élettartama lejárt.

Útvonal átirányítás

Ha egy bizonyos cél felé egy jobb útvonal is elérhető a forgalomirányító az ICMP átirányítás üzenetét használhatja arra, hogy a hálózat állomásait értesítse erről. Ezt az üzenetet csak akkor használják, ha a küldő állomás ugyanazon a fizikai állomáson van, mint a két átjáró.

Az ICMPv4 és ICMPv6 egyaránt használ útvonal átirányítás üzeneteket.

Az ICMPv6 információs- és hibaüzenetei nagyon hasonlóak az ICMPv4-ben megvalósított vezérlő- és hibaüzenetekhez. Azonban az ICMPv6 olyan funkciókat és fejlesztéseket is tartalmaz, melyek az ICMPv4-ben még nincsenek jelen.

Az ICMPv6 négy új protokollt tartalmaz a Szomszéd Felderítő Protokoll (Neighbor Discovery Protocol, ND, NDP) részeként:

- forgalomirányító keresés üzenet (Router Solicitation)
- forgalomirányító hirdetés üzenet (Router Advertisement)
- szomszéd keresés üzenet (Neighbor Solicitation)
- szomszéd hirdetés üzenet (Neighbor Advertisement)

Forgalomirányító keresés és forgalomirányító hirdetés üzenetek

Az IPv6-képes eszközöket két kategóriába sorolhatjuk: forgalomirányítók és állomások. A forgalomirányító keresés és a forgalomirányító hirdetés üzenetek állomások és forgalomirányítók között zajlanak.

- **Forgalomirányító keresés (Router Solicitation, RS) üzenet:** Az állomás akkor fog RS üzenetet küldeni a forgalomirányítónak, amikor úgy állítjuk be, hogy a címzési információját automatikusan szerezze be állapotmentes cím autokonfiguráció (SLAAC) segítségével. Az állomás ezt az RS üzenetet az IPv6 minden router multicast címre küldi el.
- **Forgalomirányító hirdetés (Router Advertisement, RA) üzenet:** Az RA üzeneteket a forgalomirányítók küldik, hogy címzési információt biztosítsanak az SLAAC-t használó állomások számára. Az RA üzenet olyan címzési információkat adhat az állomásnak, mint az előtag és az előtag hossza. A forgalomirányító rendszeresen, vagy egy RS üzenetre válaszolva küld ki az RA üzeneteket. Alapértelmezés szerint a Cisco forgalomirányítók 200 másodpercenként küldenek RA üzenetet. Az RA üzeneteket az IPv6 minden állomás multicast címre küldik. Az SLAAC-t

használó állomás az alapértelmezett átjáróját az RA üzenetet küldő forgalomirányító link-local címére állítja be.

Az ICMPv6 Szomszéd Felderítő Protokoll (Neighbor Discovery Protocol) két további üzenettípust tartalmaz: szomszéd keresés (Neighbor Solicitation) és szomszéd hirdetés (Neighbor Advertisement).

A Neighbor Solicitation és a Neighbor Advertisement üzeneteket az alábbiakra használják:

- Címfeloldás
- Duplikált Cím Felderítés (Duplicate Address Detection, DAD)

Címfeloldás

Címfeloldásra akkor van szükség, ha a LAN egy eszköze ismeri a cél egyedi IPv6-címét, de nem tudja a hozzá tartozó Ethernet MAC-címet. A cél MAC-címének meghatározásához az eszköz egy NS üzenetet küld a keresett csomópont címére. Ez az üzenet az ismert (cél) IPv6-címet fogja tartalmazni. Az eszköz, amelynek a címe megegyezik a cél IPv6-címmel, egy NA üzenettel fog válaszolni, amely a saját Ethernet MAC-címét tartalmazza.

Duplikált Cím Felderítés

Amikor egy eszköz globális egyedi vagy link-local egyedi címhez jut, egy DAD művelet elvégzése javasolt a számára, hogy megbizonyosodjon a címének egyediségéről. A cím egyediségét úgy ellenőrzi, hogy egy NS üzenetet küld ki a saját IPv6-címével, mint célcímmel. Ha a hálózat más eszköze is birtokolja ugyanezt a címet, egy NA üzenettel fog válaszolni. Ez az NA üzenet jelzi a küldőnek, hogy a cím használatban van. Ha egy bizonyos ideig nem érkezik vissza NA üzenet, akkor az egyedi cím valóban egyedi és használható.

Megjegyzés: A DAD művelet elvégzése nem kötelező, de az RFC 4861 ajánlja az egyedi címekre történő végrehajtását.

A ping egy olyan tesztelési segédprogram, amely ICMP visszhang kérés és visszhang válasz üzeneteket használ az állomások közti kapcsolatok ellenőrzésére. A ping IPv4 és IPv6 állomások esetén is működik.

A hálózat egy másik állomásával úgy ellenőrizhetjük a kapcsolatot, hogy egy visszhang kérés üzenetet küldünk neki a **`ping`** paranccsal. Ha a megadott című állomás megkapja a visszhang kérést, egy visszhangkérés válasz (vagy visszhang válasz) üzenettel fog válaszolni. A visszhang válasz fogadásakor a ping kiírja a kérés elküldése és a válasz megérkezése közt eltelt időt. Ebből következtethetünk a hálózat teljesítményére is.

A ping a válaszra csak egy bizonyos ideig vár. Ha az adott időn belül nem érkezik válasz, a ping egy üzenetben közli, hogy nem érkezett válasz. Ez általában valamilyen probléma jele, de jelentheti azt is, hogy a hálózatban valamilyen biztonsági beállítás blokkolja a ping üzeneteit.

Az összes kérés elküldése után a ping segédprogram egy összegzést is ad, amelyben kiírja a sikerességi arányt valamint a céltól mért oda-vissza terjedési idő átlagát.

A helyi loopback pingelése

A ping néhány speciális tesztelési és ellenőrzési célra is használható. Az egyik ilyen eset, amikor a helyi gép IPv4- vagy IPv6-konfigurációját ellenőrizzük. Ezt a helyi loopback cím pingelésével végezhetjük el, ami IPv4 esetén 127.0.0.1 (és ::1 IPv6-nál). Az ábrán egy IPv4 loopback tesztelése látható.

Ha választ kapunk a 127.0.0.1- ről (IPv4) vagy a ::1-ről (IPv6), akkor az állomáson megfelelően van telepítve az IP protokoll . A választ a hálózati réteg adja. Ez a válasz azonban nem azt jelenti, hogy a címek, maszkok vagy átjárók helyesen vannak beállítva. Az alsóbb rétegek állapotáról sem kapunk információt. Egyszerűen csak a hálózati rétegig teszteli az IP-t. Ha hibaüzenetet kapunk, az azt jelenti, hogy a TCP/IP nem megfelelően működik az állomáson.

A ping az állomás helyi hálózattal való kommunikációjának ellenőrzésére is használható. Ezt legtöbbször úgy végezzük el, hogy megpingeljük az állomás átjárójának IP-címét. Az átjáró sikeres pingelése azt jelenti, hogy az állomás és a forgalomirányító átjáró funkciót betöltő hálózati interfésze egyaránt képes kommunikálni a helyi hálózaton.

Azért az átjáró címét használjuk leggyakrabban, mert a forgalomirányítónak normális esetben működnie kell. Ha az átjáró nem válaszol, megpróbálhatjuk egy másik, működőnek sejtett állomás IP-címét pingelni a helyi hálózaton belül.

Ha az átjáró, vagy egy másik állomás válaszol, biztosak lehetünk benne, hogy az állomásunk képes kommunikálni a helyi hálózaton. Ha az átjáró nem, de egy másik állomás válaszol, ez az átjáróként funkcionáló forgalomirányító problémáját jelezheti.

Az egyik lehetőség az, hogy az állomáson helytelen átjáró cím van beállítva. Egy másik lehetőség pedig, hogy a forgalomirányító interfész teljesen működőképes, viszont biztonsági szabályokat állítottak be rajta, amelyek megakadályozzák a ping kérések feldolgozását vagy megválaszolását.

A ping arra is jó, hogy egy helyi állomás távoli hálózatok irányába történő kommunikációját teszteljük. A helyi állomás megpingel egy távoli hálózaton üzemelő IPv4 állomást, amint az ábrán is látható.

Ha a ping sikeres, a köztes hálózat nagy részének működését igazoltuk. A sikeres ping megerősíti a helyi hálózat, az átjáróként használt forgalomirányító, minden egyéb köztünk levő forgalomirányító és a távoli állomás hálózatának működését.

Továbbá a távoli állomás működését is leellenőriztük. Ha a távoli gép nem tudna kommunikálni a saját hálózatán kívülre, válaszolni sem tudott volna.

Megjegyzés: Sok hálózati rendszergazda korlátozza vagy tiltja az ICMP üzenetek belépését a vállalat hálózatába, emiatt lehet, hogy a válasz a biztonsági korlátozások miatt nem érkezik meg.

A ping két állomás közti kapcsolat tesztelésére való, de a köztes eszközökről semmilyen információval nem tud szolgálni. A traceroute (tracert) olyan segédprogram, amely listát ad az útvonal sikeres ugrásairól is. Ez a lista fontos ellenőrzési és hibakeresési információkat tartalmazhat. Ha az adat eléri a célját, a nyomkövetés felsorolja az állomások közti útvonalon érintett forgalomirányítókat. Ha az adat elakad valamelyik ugrásnál, az utolsóként választ adó forgalomirányító címe fontos információ lehet a probléma vagy biztonsági korlátozás helyére vonatkozóan.

Körülfordulási idő (Round Trip Time, RTT)

A traceroute megmutatja az útvonal minden ugrásának körülfordulási idejét és jelzi, ha valamelyik közbülső eszköz nem válaszol. A körülfordulási idő az az idő, ami alatt a csomag eléri a cél állomást, majd a válasz visszaér. Csillag (*) jelzi az elveszett, vagy megválaszolatlan csomagot.

Ezeket az információkat az útvonalon lévő problémás forgalomirányító megtalálásához használhatjuk. Ha a program kimenetében egy bizonyos ugrásnál magas válaszidőket vagy adatvesztést látunk, az annak a jele, hogy a forgalomirányító vagy a kapcsolatai leterheltek.

IPv4 élettartam (Time-to-Live, TTL) és IPv6 ugrás korlát (Hop Limit)

A traceroute az IPv4 TTL és az IPv6 ugrás korlát harmadik rétegbeli fejléc mezőjét használja az ICMP időtúllépés üzenetével együtt.

Az animáció lejátszásával megnézhetjük hogyan használja a traceroute TTL-t.

A traceroute által kiküldött első üzenetsorozat TTL értéke 1 lesz. Emiatt az első forgalomirányítónál a csomag TTL értéke lejár, időtúllépést eredményez. A forgalomirányító erre egy ICMPv4 üzenettel válaszol. A traceroute ebből tudta meg az első ugrás címét.

A traceroute ezután fokozatosan növeli a TTL mező értékét (2, 3, 4...) üzenetsorozatonként. Így sorban megkapja az útvonal minden ugrását, ahogy a csomag egyre tovább jut az úton. A TTL mezőt addig növeli, amíg a célt vagy a meghatározott maximum értéket el nem éri.

Ha elértük a végső célt, az állomás az ICMP időtúllépés üzenet helyett ICMP port nem elérhető vagy ICMP visszhangkérés válasz üzenetet küld.

Ugyanazon a hálózaton az IPv4 és IPv6 együtt is létezhet. A PC parancssorának használata közben néhány különbséget fedezhetünk fel a parancsok használatában és a kimenet formátumában.

Packet Tracer - Verifying IPv4 and IPv6 Addressing Instructions

Packet Tracer - Verifying IPv4 and IPv6 Addressing - PKA

Minden a hálón... Természetesen!

Ebben a fejezetben megtanultuk, hogy a kis- és közepes vállalatok milyen módon csatlakoznak hálózatok csoportjaihoz. A bevezető feladatban a Minden a hálón elmélettel is megismerkedtünk.

Ehhez a feladathoz válasszunk a következők közül:

- online banki műveletek
- hírek a nagyvilágból
- időjárás előrejelzés, klíma
- közlekedés és feltételei

Dolgozzunk ki egy IPv6-címzési sémát a választott témára. A címzési sémának tartalmaznia kell, hogyan terveznénk meg a címzést a következőkre:

- alhálózatok
- egyedi címzés
- csoportos címzés
- szórás

A saját sémánk másolatát osszuk meg az osztállyal vagy a tanulócsoportunkkal. Készüljünk fel az alábbiak elmagyarázására:

- Hogyan valósulna meg az alhálózatokra bontás, az egyedi, a csoportos és a szórt átvitel használata?
- Hol lehetne ezt a címzési rendszert használni?
- Milyen hatással lenne a terv a kis- és közepes vállalatokra?

Csoportos feladat - The Internet of Everything...Naturally Instructions

Az IP-címek hierarchikusan hálózati, alhálózati és állomás részekből állnak. Egy IP-cím a teljes hálózatot, egy állomást, vagy egy hálózat szórási címét is képviselheti.

A bináris ábrázolás megértése fontos, amikor azt szeretnénk meghatározni, hogy két állomás azonos hálózaton van-e. Ugyanazon a hálózaton lévő eszközök IP-címében a hálózati rész bitjeinek azonosnak kell lenniük. Az alhálózati maszk vagy előtag (prefix, prefixum) határozza meg az IP-cím hálózati részét. Az IP-címek statikusan és dinamikusan is hozzárendelhetők. A DHCP lehetővé teszi a címzési információk - IP-cím, alhálózati maszk, alapértelmezett átjáró és egyéb konfigurációs paraméterek - automatikus kiosztását.

Az IPv4 állomások háromféle módon kommunikálhatnak: egyedi címzéssel, szórással vagy csoportos címzéssel. Privát címeknek hívjuk azokat a címtartományokat, amelyeket olyan hálózatokban használnak, ahol korlátozott kapcsolatra vagy egyáltalán semmilyen internetkapcsolatra nincsen szükség. A privát IPv4-címtartományok a következők: 10.0.0.0/8, 172.16.0.0/12 és 192.168.0.0/16.

Az IPv4-címtartomány kimerülése az IPv6-ra átállás fő motiváló faktora. Az IPv6-címek 128 bitesek, míg az IPv4-címek csak 32. A pontozott decimális alhálózati maszk jelölést IPv6-nál nem használjuk. Az előtag vagy prefix hossza jelzi az IPv6-cím hálózati részét a következő alakban: ipv6-cím/prefix hossz.

Háromféle IPv6-címet különböztetünk meg: egyedi (unicast), csoportos (multicast) és anycast cím. Az IPv6 link-local címek lehetővé teszik, hogy az eszköz más IPv6-képes eszközökkel kommunikáljon ugyanazon a kapcsolaton, de csak azon az egy kapcsolaton (alhálózaton). Azok a csomagok, melyeknek a forrás vagy célja link-local cím nem továbbíthatók a kiinduló kapcsolaton kívülre. Az IPv6 link-local címek az FE80::/10 tartományban vannak.

Az ICMP IPv4 és IPv6 esetén egyaránt rendelkezésre áll. Az IPv4 üzenetküldő protokollja az ICMPv4. Az ICMPv6 ugyanezeket a szolgáltatásokat biztosítja IPv6 esetén, de további funkciókat is tartalmaz.

Megvalósítás után az IP-hálózatokat tesztelni, a kapcsolatokat ellenőrizni és a működés teljesítményét is ellenőrizni kell.

Az IP-címzési terv megfelelő kialakítása, megvalósítása és karbantartása biztosítja a hálózat hatékony és eredményes működését. Ez azért különösen igaz, mert a hálózatra csatakozó állomások száma egyre növekszik. Az IP-címek hierarchikus felépítésének, valamint annak megértése, hogy ezt a hierarchiát hogyan kell a hatékonyabb forgalomirányítás követelményeinek megfelelően módosítani, elengedhetetlenül fontos egy IP-címzési séma tervezésekor.

Az eredeti IPv4-es címek hierarchiája kétszintű, a címek hálózat- és állomás részekre tagozódnak. A címzés ezen két szintje teszi lehetővé az alapvető hálózatcsoportosítások esetén a csomagok célhálózathoz való eljuttatását. A forgalomirányító az IP-cím hálózati része alapján továbbítja a csomagokat, majd ahogy azok elértek a célhálózathoz, a cím állomás része azonosítja a cél eszközt.

Mindamellett a hálózatok növekedésével számos szervezet állomások százait, vagy akár ezreit adta a hálózatához, ezért ez a kétszintű hierarchia elégtelené vált.

A hálózatok tovább bontása egy újabb szintet ad a hierarchiához, amely tulajdonképpen így már háromszintűvé válik: hálózat, alhálózat és állomás. Egy újabb hierarchiaszint bevezetése alcsoportokat hoz létre egy IP-hálózaton belül, amely elősegíti a gyorsabb csomagtovábbítást és további szűrések hozzáadásával segíti a „helyi” hálózati forgalom minimalizálását.

A továbbiakban a fejezet részletesen taglalja az IP-hálózatok és alhálózatok címeinek alhálózati maszk alapján történő meghatározását és kiosztását.

Hívj fel!

Ebben a fejezetben egy nagyobb hálózat eszközeinek alhálózatokba, vagy kisebb hálózat csoportokba szervezéséről lesz szó.

Ebben a modellezési feladatban az a kérés, hogy gondoljunk egy olyan számra, amit nap mint nap használunk, például a telefonszámunkra. A feladat elvégzése közben gondoljuk át, hogy miben hasonlít a telefonszám azokhoz a hatékony adatkommunikációs stratégiákhoz, amit a hálózati rendszergazdák az állomások azonosításához használhatnak.

Válaszoljuk meg az alábbi két kérdést írásban! Majd tegyük félre a válaszokat, hogy a későbbiekben a csoportban megvitathassuk azokat!

- Magyarázzuk el, hogyan osztható a mobil- vagy a vezetékes telefonszámunk azonosítást végző számcsoportokra! A telefonszámunk tartalmaz-e terület azonosítót? Vagy szolgáltató azonosítót? Város, megye, vagy országkódot?

- Hogyan osztható fel a telefonszámunk a kapcsolást, vagy az egymás közti kommunikációt segítő azonosító részekre?

Csoportos feladat - Call me! Instructions

A korai hálózati alkalmazásokban általános megoldás volt, hogy a szervezeti egység összes számítógépe, vagy hálózati eszköze egyetlen IP-hálózatba tartozott. A szervezeti egység valamennyi eszköze azonos hálózatazonosítójú IP-címet kapott. Az ilyen konfigurációt egyszintű hálózatszervezésnek nevezzük. Kisebb hálózatban, vagy kevés hálózati eszköz esetén az egyszintű hálózatszervezés is megfelelő lehet. Ugyanakkor a hálózat növekedésével az ilyen hálózatszervezés komoly problémákat okozhat.

Gondoljunk bele, hogy egy Ethernet LAN eszközei hogyan használják az üzenetszórást a kívánt szolgáltatások vagy eszközök megkeresésére. Emlékezzünk rá, hogy egy szórás egy IP-hálózat valamennyi állomásához eljut. A dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP) jó példa egy üzenetszórásra épülő hálózati szolgáltatásra. Az eszközök a hálózatukban üzenetszórással keresik meg a DHCP-szervert. Nagy hálózat esetében ez a hálózati funkciók sebességét csökkentő jelentős mértékű forgalmat is generálhat. Mindemellett, mivel az üzenetszórás valamennyi eszközre vonatkozik, valamennyi eszköznek fogadnia és feldolgoznia is kell ezen üzeneteket, amely jelentősen megnövelheti az eszközök feldolgozási terheltségét. Ha egy eszköznek jelentős mennyiségű szórásos üzenetet kell feldolgoznia, az más eszközfunkciókat is lelassíthat. Az ilyen okok indokolják a nagy hálózatok kisebb alhálózatokra, kisebb eszköz- és szolgáltatás-csoportokra szegmentálását.

A hálózat szegmentálását, több kisebb részre osztását alhálózatokra bontásnak (subnetting) nevezzük. Az így nyert kisebb hálózatokat alhálózatoknak nevezzük. A hálózati rendszergazdák az eszközök és szolgáltatások alhálózatokba csoportosítását a földrajzi elhelyezkedés (pl. harmadik emelet), a szervezeti egység (pl. kereskedelmi osztály), az eszköztípus (pl. nyomtatók, szerverek, WAN), vagy bármilyen más a hálózat szempontjából ésszerű módon is elvégezheti. Az alhálózatokra bontás a teljes hálózat forgalmának csökkentésével növelheti a hálózat teljesítményét.

Megjegyzés: Egy alhálózat valójában önmaga is egy hálózat, így a két szakkifejezés egymással felcserélhető. A legtöbb hálózat valamely nagyobb címtartományú hálózat alhálózata.

Különböző hálózatokon lévő eszközök kommunikációjához egy forgalomirányító szükséges. A hálózat eszközei a forgalomirányító helyi hálózatukra csatlakozó interfészét alapértelmezett átjáróként használják. Egy távoli hálózaton lévő eszköz felé irányuló forgalmat a forgalomirányító dolgozza fel és továbbítja célja felé. Azt, hogy a forgalom helyi vagy távoli, a forgalomirányító az alhálózati maszk alapján dönti el.

Egy alhálózatokra bontott hálózatban ez a dolog ugyanígy történik. Ahogy az ábra is mutatja, egy címtartomány, vagy egy hálózati cím alhálózatokra bontása több logikai hálózatot eredményez.

Minden alhálózat egy külön hálózati tartomány lesz. Az egyazon alhálózaton lévő eszközöknek a saját alhálózatuknak megfelelő címet, alhálózati maszkot és az alapértelmezett átjárót kell használniuk.

Az alhálózatok között forgalomirányító használata nélkül nem tudunk forgalmat továbbítani. A forgalomirányító egyes interfészeinek mindig abból a hálózatból vagy alhálózatból kell IPv4-címet kapniuk, amelyhez kapcsolódnak.

Ahogy azt az ábra is mutatja, az alhálózati terv elkészítéséhez az intézményi hálózat használatának és a struktúrájának az elemzése egyaránt szükséges. Az első lépés a hálózattal szemben támasztott igények felmérése. Ez a teljes hálózat főbb részeinek és azok tagolódásának meghatározását jelenti. A címzési tervben el kell dönteni, hogy mekkorák az egyes alhálózatok méretei, hány állomás van bennük és hogyan lesznek a címek kiosztva, mely állomások igényelnek statikus IP-címeket és mely állomások esetén lehet DHCP-t használni a címzési információk megszerzéséhez.

Az alhálózatok méretének tervezése a felosztani kívánt magánhálózat valamennyi alhálózatában az IP-címet igénylő állomások számának átgondolását igényli. Például egy kampusz hálózati tervében előre el kell tervezni, hogy hány állomás lesz az adminisztratív LAN-ban, hány a kari LAN-ban és hány a hallgatói LAN-ban. Egy otthoni hálózat esetében ez a ház központi és az otthoni irodai LAN állomásszámainak meghatározását jelenti.

Ahogy arról már korábban volt szó, egy LAN magánhálózati IP-címtartományainak kiosztása a hálózati rendszergazdák döntése alapján kellő körültekintéssel történik úgy, hogy elegendő cím jusson a már meglévő és a jövőben tervezett állomások számára is. Ne feledjük, hogy a magánhálózati IP-címtartományok az alábbiak:

- 10.0.0.0 a 255.0.0.0 alhálózati maszkkal
- 172.16.0.0 a 255.240.0.0 alhálózati maszkkal
- 192.168.0.0 a 255.255.0.0 alhálózati maszkkal

Az IP-cím igények ismeretében kell a telepítendő állomáscím tartományt, vagy tartományokat meghatározni. A kiválasztott magánhálózati IP-címtartomány alhálózatokra bontása biztosítja a hálózat igényeinek megfelelő állomáscímeket.

Az internetre csatlakozáshoz szükséges nyilvános címeket általában a szolgáltató biztosítja. Ezért bár az alhálózatokra bontás szabályai itt is ugyanazok, az nem tartozik bele a szervezet hálózati rendszergazdájának általános feladatkörébe.

Alakítsunk ki szabályokat az alhálózatok IP-címkiosztására. Például:

- A nyomtatók és szerverek statikus IP-címeket kapnak.
- A felhasználók a DHCP-szerverektől /24 alhálózatú IP-címeket kapnak.
- A forgalomirányítók az egyes tartományok első kiosztható állomáscímét kapják.

A megfelelő magánhálózati IP-címtartomány kiválasztásának két nagyon fontos szempontja, hogy mennyi a kialakítandó alhálózatok száma, valamint hogy mekkora az egyes alhálózatokra eső maximális állomásszám. Ezen címtartományok teszik lehetővé az állomások megfelelő címkiosztását mind a már meglévő, mind pedig a közeljövőben tervezett állomásszámot szem előtt tartva. Az IP-cím igények határozzák meg az állomások címtartományát, vagy tartományait.

A következőkben 255.0.0.0, 255.255.0.0 és 255.255.255.0 alhálózati maszkú alhálózati címtartományok kialakítására látunk példát.

Minden hálózati címhez egy érvényes állomáscím tartomány tartozik. Az ugyanazon hálózathoz kapcsolódó állomások ugyanabból a hálózati címtartományból kapnak IPv4-es címet, ezért megegyezik az alhálózati maszkjuk, illetve a hálózati előtagjuk (prefixumuk) is.

Az előtag és az alhálózati maszk ugyanannak a dolognak - a cím hálózati részének - különböző megadási módjai.

Az IPv4 alhálózatok egy vagy több állomásbit hálózati bitként való értelmezésével keletkeznek. Ez a maszk kiegészítésével történik, kibővítve a cím hálózati részét az állomás részéből kölcsönvett bitekkel. Minél több állomásbitet veszünk kölcsön, annál több alhálózat kialakítására van lehetőség. Minden egyes elvett bit megduplázza a lehetséges alhálózatok számát. Egy bit kölcsönvételével például két alhálózat kialakítására van lehetőség. Ha két bitet veszünk el, akkor négy, ha hármat akkor nyolc alhálózat jön létre és így tovább. Ugyanakkor a kölcsönvett állomásbitek az alhálózatban kioszthatő állomáscímek számát is csökkentik.

Bitek csak a cím állomás részéből kölcsönözhetők. A hálózati részt a szolgáltató osztja ki és így az nem változtatható.

Megjegyzés: Az ábra példájában azért csak az utolsó oktett van bináris formában, mert csak az állomásbitek kölcsönözhetők.

Amint az 1. ábrán látszik, a 192.168.1.0/24 hálózat címeinek a hálózati része 24, míg az állomás része 8 bites, ahogy azt a 255.255.255.0 maszk, vagy a /24 előtag is jelzi. Alhálózatokra bontás nélkül ez a hálózat egyetlen LAN interfészt szolgál ki. Amennyiben több LAN-ra lenne szükség, akkor szükségessé válhat a hálózat alhálózatokra bontása.

A 2. ábrán, a legmagasabb helyértékű bitet (a balszélső bit) vesszük kölcsön az állomás részből, 25 bitessé téve ezzel a hálózati részt. Két alhálózat jön így létre, az egyik a kölcsönvett bit 0-ás értékénél, a másik az 1-es értékénél. A kölcsönvett bit pozíciójában mindkét hálózat alhálózati maszkja 1-est használva jelöli azt, hogy ez a bit most már a cím hálózati részéhez tartozik.

Ahogy az a 3. ábrán látszik, amikor a bináris oktettet decimálissá konvertáljuk, az első alhálózat címének a 192.168.1.0, míg a másodiknak a 192.168.1.128 adódik. A kölcsönvett bit miatt az alhálózati maszk mindkét alhálózat esetében 255.255.255.128, vagy /25.

Az előző példában a 192.168.1.0/24 hálózat két alhálózatra lett osztva:

192.168.1.0/25

192.168.1.128/25

Az 1. ábrán vegyük észre, hogy az R1 forgalomirányítónak két LAN szegmense van, amelyek a GigabitEthernet interfészeihez kapcsolódnak. Az alhálózatok ezekhez az interfészekhez kapcsolódó szegmenseket fogják használni. Ahhoz, hogy a LAN-ok eszközeinek átjárója lehessen, a forgalomirányító mindkét interfészének a saját alhálózatában érvényes címtartományból kell IP-címet kapnia. Általános gyakorlat, hogy egy címtartománynak az első vagy az utolsó címét választjuk ki a forgalomirányító interfészének.

Az első 192.168.1.0/25 alhálózat a GigabitEthernet 0/0 interfészhez kapcsolódó hálózatot, míg a második 192.168.1.128/25 a GigabitEthernet 0/1 interfészhez kapcsolódó hálózatot szolgálja ki. Ahhoz, hogy az interfészekhez IP-címeket rendeljünk, meg kell határoznunk az egyes alhálózatok érvényes IP-címtartományát.

Az alhálózatokra az alábbi szabályok vonatkoznak:

- **Hálózatcím** – A cím állomás részének minden bitje 0-ás.

- **Első állomáscím** - A cím állomás részének bitjei 0-ák, kivéve a jobbszélső bitet, amely 1-es.
- **Utolsó állomáscím** - A cím állomás részének bitjei 1-ek, kivéve a jobbszélső bitet, amely 0-ás.
- **Üzenetszórási cím** - A cím állomás részének minden bitje 1-es.

Ahogy azt a 2. ábra is mutatja, a 192.168.1.0/25 hálózat első állomáscíme 192.168.1.1, az utolsó pedig a 192.168.1.126. Ahogy azt a 3. ábra is mutatja a 192.168.1.128/25 hálózat első állomáscíme 192.168.1.129, az utolsó pedig a 192.168.1.254.

Ahhoz, hogy a forgalomirányító interfészéhez mindegyik alhálózatban az első állomáscímet rendeljük, használjuk az interfész konfigurációs mód **`ip address`** parancsát a 4. ábra szerint. Vegyük észre, hogy a címek 25 bites hálózati résznek megfelelően mindegyik alhálózat a 255.255.255.128 alhálózati maszkot használja.

A 192.168.1.128/25 hálózat állomásának konfigurációját az 5. ábra mutatja. Figyeljük meg, hogy az átjáró IP-címe az R1 G0/1 interfészén beállított 192.168.1.129 cím, az alhálózati maszk pedig a 255.255.255.128.

Az alhálózatok számítása

Az alhálózatok számításához használjuk az alábbi összefüggést:

2^n (ahol n = a kölcsönvett bitek számával)

Ahogy azt az 1. ábra is mutatja, a 192.168.1.0/25 példát alapul véve, a számítás az alábbiaknak megfelelően alakul:

2^1 = 2 alhálózat

Az állomások számítása

A hálózatok állomásainak számítására használjuk az alábbi összefüggést:

2^n (ahol n = a maradék állomásbitek számával)

Ahogy azt az 2. ábra is mutatja, a 192.168.1.0/25 példát alapul véve, a számítás az alábbiaknak megfelelően alakul:

2^7 = 128

Mivel az alhálózatban a hálózat címet és az üzenetszórás címet nem használhatják az állomások, ez a két cím nem osztható ki állomáscímnek. Ez azt jelenti, hogy mind a két hálózatra 126 (128-2) érvényes állomáscím jut.

Ebben a példában tehát egy állomásbit hálózati részhez adása két alhálózatot eredményez, alhálózatonkénti 126 állomáscímmel.

Tegyük fel, hogy a belső hálózatunk három alhálózatot igényel.

Újból a 192.168.1.0/25 címtartományt használva, most legalább 3 alhálózatnak megfelelő mennyiségű állomásbitet kell kölcsönvennünk. Egyetlen bit kölcsönvétele 2 alhálózatot eredményez. Ennél több hálózathoz több bit kölcsönvétele szükséges. Az alhálózatok számát 2 kölcsönvett bit esetén a 2^n összefüggéssel számolhatjuk, ahol a n a kölcsönvett bitek számát jelenti:

2^2 = 4 alhálózat

Ahogy azt a 1. ábra mutatja 2 bit kölcsönvétele 4 alhálózatot eredményez.

Ne feledjük, hogy a kölcsönvett biteknek megfelelően az alhálózati maszk is változik! Ebben a példában, amikor 2 bitet vettünk kölcsön, az utolsó oktettben a maszk két bittel lett hosszabb. Bináris formában az utolsó oktett 1100 0000, ezért a maszk decimális formában 255.255.255.192.

Az állomások számítása

Az állomások számításához meg kell vizsgálnunk az utolsó oktettet. Az alhálózatok számára 2 bit kölcsönvétele 6 maradék állomásbitet eredményez.

A 2. ábrának megfelelően alkalmazzuk az állomáscím kiszámítására az összefüggést.

2^6 = 64

De ne feledjük, hogy a csupa 0-ás bitet tartalmazó állomásazonosító rész a hálózat címét, a csupa 1-es bitet tartalmazó állomásazonosító rész pedig az üzenetszórási címet jelöli. Ezért az egyes alhálózatokban csak 62 állomáscím osztható ki.

Ahogy azt a 3. ábra is mutatja, az első alhálózat első állomáscíme 192.168.1.1, az utolsó pedig 192.168.1.62. A 4. ábra az első három alhálózat címtartományát mutatja. Ügyeljünk rá, hogy valamennyi állomás a hálózati szegmensének megfelelő érvényes IP-címet kapjon. A forgalomirányító interfészéhez rendelt alhálózat határozza meg, hogy az állomás melyik szegmenshez tartozik.

Az 5. ábra egy példakonfigurációt mutat. Ebben a konfigurációban az első hálózat a GigabitEthernet 0/0 interfészhez van rendelve, a második hálózat a GigabitEthernet 0/1 interfészhez, a harmadik hálózat pedig a Serial 0/0/0 hálózathoz.

A szokásos címzési tervnek megfelelően az alhálózat első állomáscíme a forgalomirányító interfészéhez van hozzárendelve. Az alhálózat állomásai a forgalomirányító interfészének címét használják alapértelmezett átjárónak.

- A PC1 (192.168.1.2/26) a 192.168.1.1 (az R1 G0/0 interfész címe) címet használja alapértelmezett átjárónak.
- A PC2 (192.168.1.66/26) a 192.168.1.65 (az R1 G0/1 interfész címe) címet használja alapértelmezett átjárónak.

Megjegyzés: Egy alhálózat valamennyi eszközének IPv4 állomáscíme ugyanazon címtartományába esik és az alhálózati maszkjuk is megegyezik.

A következőkben tegyük fel, hogy a belső hálózatunk öt alhálózatot igényel, ahogy azt az 1. ábra is mutatja.

Újból a 192.168.1.0/24 címtartományt használva, most legalább 5 alhálózatnak megfelelő mennyiségű állomásbitet kell kölcsönvennünk. Ahogy azt az előző példában láttuk 2 bit kölcsönvétele 4 alhálózatot eredményez. Ennél több hálózathoz több bit kölcsönvétele szükséges. A 3 bit kölcsönvétele esetén keletkező alhálózatok száma az alábbi összefüggéssel számítható:

2^3 = 8 alhálózat

Ahogy azt a 2. és 3. ábra mutatja, 3 bit esetén 8 alhálózat keletkezik. Amikor 3 bitet veszünk kölcsön, az alhálózati maszk az utolsó oktettben 3 bittel bővül (/27), ami 255.255.255.224 alhálózati maszkot eredményez. Az alhálózat valamennyi eszköze ezt a 255.255.255.224 (/27) alhálózati maszkot fogja használni.

Az állomások számítása

Az állomások számításához meg kell vizsgálnunk az utolsó oktettet. Az alhálózatok számára 3 bit kölcsönvétele 5 maradék állomásbitet eredményez.

Az állomáscím számításának összefüggését alkalmazva:

2^5 = 32, de ebből még lejön 2 cím, a csupa 0-ás állomásazonosító részű (hálózatcím) és a csupa 1-es állomásazonosító részű (üzenetszórási cím).

Az alhálózatok topológiának megfelelő hálózati szegmensekhez rendelését a 4. ábra szemlélteti.

Ismét a szokásos címzési tervet használva az alhálózat első állomáscímét a forgalomirányító interfésze kapja, ahogy azt az 5. ábra is mutatja. Az alhálózat állomásai a forgalomirányító interfészének címét használják alapértelmezett átjárónak.

- A PC1 (192.168.1.2/27) a 192.168.1.1 címet használja alapértelmezett átjárónak.
- A PC2 (192.168.1.34/27) a 192.168.1.33 címet használja alapértelmezett átjárónak.
- A PC3 (192.168.1.98/27) a 192.168.1.97 címet használja alapértelmezett átjárónak.
- A PC4 (192.168.1.130/27) a 192.168.1.129 címet használja alapértelmezett átjárónak.
    - Az előzőekben egy 3 és egy 5 alhálózatot igénylő hálózatra láttunk példát. Annak érdekében, hogy négy alhálózatot hozzunk létre, 2 bitet vettünk kölcsön egy IP-címben az alapértelmezett 255.255.255.0 maszk, vagy /24 előtag esetén rendelkezésre álló 8 állomásbitből. Az így kapott 255.255.255.192 alhálózati maszkkal összesen 4 lehetséges alhálózatot hoztunk létre. Az állomáscím számításának 2^6-2 összefüggését alkalmazva meghatároztuk, hogy mind a 4 alhálózat esetében hálózatonként 62 állomáscímet rendelhetünk a csomópontokhoz.
    - 5 alhálózat létrehozásának érdekében, 3 bitet vettünk kölcsön egy IP-címben az alapértelmezett 255.255.255.0 maszk, vagy /24 előtag esetén rendelkezésre álló 8 állomásbitből. Az állomás rész 3 bitjének kölcsönvételét követően 5 állomásbit marad. Az eredő alhálózati maszk így 255.255.255.224, mely 8 darab, alhálózatonként 30 állomáscímet tartalmazó alhálózat kialakítását teszi lehetővé.
    - Vegyünk egy nagy intézményt vagy kampuszt, ahol a hálózat 100 alhálózatot igényel! Pont úgy, mint az előző példákban, annak érdekében, hogy 100 alhálózatot hozhassunk létre, a meglévő hálózat IP-címének állomásazonosító részéből kell biteket kölcsönvennünk. Ugyanúgy mint korábban, az alhálózatok számának meghatározásához most is meg kell vizsgálnunk a rendelkezésre álló állomásbitek számát és alkalmaznunk kell a 2^n (n=kölcsönzött bitek száma) összefüggést. Az utolsó példa 192.168.10.0/24 IP-címét használva 8 állomásbitünk van, melyből 7 bitet kell kölcsönvennünk.
    - Az alhálózatok száma 7 bit kölcsönvétele esetén: 2^7=128 alhálózat.
    - Ellenben ha 7 bitet veszünk kölcsön, akkor csak egyetlen állomásbit marad, melyre ha alkalmazzuk az állomáscím számítási összefüggést, egyetlen állomáscím sem marad ezekben az alhálózatokban. Az állomáscímek száma egy állomásbit esetén: 2^1=2, melyből le kell vonni 2-őt a hálózat címének és az üzenetszórási címnek, így 0 állomáscím marad (2^1-2=0).
    - Magasabb számú alhálózati igény esetén olyan IP-hálózat szükséges, amely például olyan IP-címmel rendelkezik, amelynél az alapértelmezett alhálózati maszk /16, vagy 255.255.0.0, így ebből több állomásbitet lehet kölcsönvenni. A 128-191 tartományba eső első oktettű címek alapértelmezett maszkja 255.255.0.0, vagy /16. Az ebbe a tartományba eső címeknek 16 bites hálózati és 16 bites állomás része van. Ez a 16 bit áll rendelkezésre az alhálózatok kialakítására szolgáló bitek kölcsönvételére.
    - Az új 172.16.0.0/16 IP-címtartományt használva kell most a legalább 100 alhálózat kialakításához szükséges állomásbiteket kölcsönvennünk. Balról jobbra haladva az első használható állomásbittel kezdve egyesével fogjuk a biteket kölcsönvenni, míg el nem érjük a kívánt 100 alhálózatot biztosító bitszámot. 1 bit kölcsönvétele 2 alhálózatot, 2 bit

kölcsönvétele 4 alhálózatot, 3 bit 8 alhálózatot, stb. eredményez. Az alhálózatok száma 7 bit kölcsönvétele esetén a 2^n (n=kölcsönvett bitek száma) összefüggés alapján:

- 2^7 = 128
- 7 bit kölcsönvétele 128 alhálózatot eredményez, ahogy azt az ábra is mutatja.
- Ne feledjük, hogy a kölcsönvett biteknek megfelelően az alhálózati maszk is változik! A példánkban 7 bitet vettünk kölcsön, így a maszk a harmadik oktettben 7 bittel bővült. A harmadik oktett binárisan 11111110, a negyedik oktett pedig 00000000, ezért a maszk decimális formában 255.255.254.0, vagy előtaggal felírva /23. Az alhálózatok kialakítása a harmadik oktettben történik, így az állomásbitek a harmadik és negyedik oktettre esnek.
- **Az állomások számítása**
- Az állomások számának meghatározásához meg kell vizsgálnunk a harmadik és negyedik oktettet. Az alhálózatok számára 7 bit kölcsönvételét követően 1 állomásbit marad a harmadik, és 8 állomásbit marad a negyedik oktettben.
- Az állomáscím számítási összefüggést alkalmazva, ahogy azt az 1. ábra is szemlélteti:
- 2^9 = 512
- De ne feledjük, hogy a csupa 0-ás bitet tartalmazó állomásazonosító rész a hálózat címét, a csupa 1-es bitet tartalmazó állomásazonosító rész pedig az üzenetszórási címet jelöli. Ezért az egyes alhálózatokban csak 510 állomáscím osztható ki.
- Ahogy azt a 2. ábra szemlélteti, az első alhálózat első állomáscíme a 172.16.0.1, az utolsó pedig a 172.16.1.254. Ügyeljünk rá, hogy valamennyi állomás a hálózati szegmensének megfelelő érvényes IP-címet kapjon. A forgalomirányító interfészéhez rendelt alhálózat határozza meg, hogy az állomás melyik szegmenshez tartozik.
- **Emlékeztető:**
- Bitek csak a cím állomás részéből kölcsönözhetők. A hálózati részt a szolgáltató osztja ki, ezért az nem változtatható. Így a magas alhálózatszámot igénylő intézményeknek az internetszolgáltatójukkal kell egyeztetniük, hogy kellő méretű alapértelmezett maszkú IP-címet kapjanak, mely elegendő bitet biztosít az alhálózatok kialakítására.
- Vannak intézmények, például a kisebb szolgáltatók, amelyeknek 100-nál is több alhálózat kialakítására van szükségük. Vegyünk például egy 1000 alhálózatot igénylő szervezetet. Mint mindig, az alhálózatok létrehozásának érdekében most is biteket kell kölcsönvennünk a meglévő hálózathoz rendelt IP-cím állomásazonosító részéből. Ahogy korábban is, az alhálózatok számának meghatározásához meg kell vizsgálnunk a rendelkezésre álló állomásbitek számát. Az ilyen helyzetekben az internetszolgáltató által biztosított IP-címnek kell elegendő állomásbitjének lennie az 1000 alhálózat kiosztásához. Azon IP-címeknek, melyeknek az első oktettje 1-126 közé esik, az alapértelmezett maszkja 255.0.0.0, vagy /8. Ez azt jelenti, hogy 8 bitjük van a hálózat részben és 24 állomásbit áll rendelkezésre a további alhálózati bitek kölcsönvételére.
- A 10.0.0.0/8 címtartományt használva kell most legalább 1000 alhálózat kialakításához szükséges állomásbiteket kölcsönvennünk. Balról jobbra haladva az első használható állomásbittel kezdve egyesével fogjuk a biteket kölcsönvenni, míg el nem érjük a kívánt 1000 alhálózatot biztosító bitszámot. Az alhálózatok számát 10 kölcsönvett bit esetén a 2^n összefüggéssel számolhatjuk, ahol a n a kölcsönvett bitek számát jelenti:
- 2^10 = 1024 alhálózat
- 10 bit kölcsönvétele 1024 alhálózatot eredményez, ahogy azt az 1. ábra is mutatja.
- Ne feledjük, hogy a kölcsönvett biteknek megfelelően az alhálózati maszk is változik! A példánkban 10 bitet vettünk kölcsön, így a maszk a harmadik oktettben 10 bittel bővült. A harmadik oktett binárisan 11000000, a negyedik oktett pedig 00000000, ezért a maszk decimális formában 255.255.192.0, vagy előtaggal felírva /18. Az alhálózatok kialakítása a harmadik oktettben történik, de ne feledjük, hogy így az állomásbitek a harmadik és negyedik oktettre esnek.
- **Az állomások számítása**
- Az állomások számának meghatározásához meg kell vizsgálnunk a harmadik és negyedik oktettet. Az alhálózatok számára 10 bit kölcsönvételét követően 6 állomásbit marad a harmadik, és 8 állomásbit marad a negyedik oktettben. Összesen 14 állomásbit marad.
- A 2. ábrának megfelelően alkalmazzuk az állomáscím kiszámítására az összefüggést.
- 2^14 - 2 = 16382
- Az első alhálózat első állomáscíme a 10.0.0.1, az utolsó pedig a 10.0.63.254. Ügyeljünk rá, hogy valamennyi állomás a hálózati szegmensének megfelelő érvényes IP-címet kapjon. A

forgalomirányító interfészéhez rendelt alhálózat határozza meg, hogy az állomás melyik szegmenshez tartozik.

- **Megjegyzés:** Egy alhálózat valamennyi eszközének IPv4 állomáscíme ugyanazon címtartományába esik és az alhálózati maszkjuk is megegyezik.
- Az alhálózatok kialakításához kölcsönvett állomásbitek számának meghatározása fontos tervezői döntés. Az alhálózatok tervezésekor két szempontot kell megfontolnunk: az egyes hálózatokban szükséges állomásszámot és az igényelt független alhálózat számot. Az animáció a 192.168.1.0 hálózat lehetséges alhálózatokra bontását mutatja be. Az alhálózati bitek számának megválasztása egyaránt érinti a lehetséges alhálózatok számát és a hálózatokra eső állomáscímek számát.
- Vegyük észre, hogy az alhálózatok száma és az állomások száma fordított arányban áll egymással! Minél több bitet veszünk kölcsön az alhálózatok számára, annál kevesebb állomásbit marad, ezért csökken az egyes alhálózatokban az állomások száma is. Ha több állomáscímre van szükségünk, akkor több állomásbit kell, így kevesebb alhálózat kialakítására van lehetőség.
- **Az állomások száma**
- Az alhálózatok kialakításánál a bitek kölcsönvételekor elegendő állomásbitet kell hagyni a legnagyobb alhálózat számára is. A legnagyobb alhálózat állomásainak száma határozza meg, hogy hány bitnek kell maradnia az állomásazonosító részben. A 2^n összefüggéssel (ahol n a megmaradó állomásbitek száma) határozható meg az egyes alhálózatokban rendelkezésre álló címek száma. Ne feledjük, hogy ezen címekből 2 nem osztható ki, így a használható címek száma 2^n-2!
- Egyes esetekben az alhálózatok száma a lényegesebb, háttérbe szorítva az alhálózatonkénti állomások számát. Ez lehet egy olyan eset, amikor egy intézmény a hálózati forgalmát szeretné a belső struktúrájának, vagy az osztályok szerinti felosztásának megfelelően szétválasztani. Például egy intézmény szeretné a mérnöki részleg által használt valamennyi eszközét az egyik, míg a menedzsment által használt eszközöket egy másik, különálló hálózathoz kapcsolni. Ebben az esetben az alhálózatok száma a meghatározó a kölcsönvett bitek számát illetően.
- Ne feledjük, hogy a létrehozott alhálózatok száma a 2^n (ahol n a kölcsönzött bitek száma) összefüggés alapján számítható! Az így kapott valamennyi alhálózat használható, ezért ezt a számot nem kell csökkenteni.
- A megoldás kulcsa az alhálózatok száma és a legnagyobb alhálózat által igényelt állomásszám közötti egyensúly megtalálása. Több bit kölcsönvétele újabb alhálózatok létrehozásának érdekében kisebb alhálózatonkénti állomásszámot eredményez.
- Minden intézményi hálózat véges sok állomás befogadására alkalmas. Az alhálózatokra bontás alapelvei szerint a belső hálózatok számának megfelelő mennyiségű alhálózatot kell kialakítani úgy, hogy azok alhálózatonként elegendő számú állomáscímet is biztosítsanak.
- Néhány hálózat, mint például a pont-pont WAN kapcsolatok, csak két állomást tartalmaznak. Más hálózatok, mint például a nagy épületek, vagy részlegek felhasználói LAN-jai, állomások százait tartalmazhatják. A hálózatadminisztrátornak kell alkalmas belső címzési struktúrát kialakítania annak érdekében, hogy a hálózatok fogadni tudják a maximális állomásszámot. Emellett mindegyik részlegben lehetőséget kell biztosítani az állomásszámok bővítésére.
- **Az összállomásszám meghatározása**
- Első lépésként vizsgáljuk meg a teljes intézményi belső hálózat összállomásszámát! A címtartománynak elég nagynak kell lennie az intézményi hálózat valamennyi eszközének befogadására. Ezen berendezések a felhasználók eszközei, a szerverek, a közvetítő eszközök és a forgalomirányító interfészek.
- Vegyünk például egy intézményi hálózatot, amelynek öt telephelyen összesen 800 állomást kell befogadnia (lásd 1. ábra). Ebben a példában a szolgáltató a 172.16.0.0/22 (10 állomásbit) hálózatcímet osztotta ki. Ahogy azt a 2. ábra is mutatja, ez 1,022 állomáscímet jelent, ami bőven fedezi a belső hálózat címigényét.
- **A hálózatok számának és méretének meghatározása**
- A következőkben vizsgáljuk meg a szükséges alhálózat számot és az alhálózatonként igényelt állomáscím számot! Az 5 LAN-szegmenst és a forgalomirányítók közötti 4 kapcsolatot tartalmazó hálózati topológia alapján 9 alhálózat kialakítása szükséges. A legnagyobb alhálózat 40 állomást tartalmaz. A címzési struktúra tervezésekor figyelemmel kell lenni a hálózat bővülésére, mind az alhálózatok számát, mind az alhálózatonkénti állomásszámot illetően.

- A 172.16.0.0/22 hálózatcím 10 állomásbitet tartalmaz. Mivel a legnagyobb hálózatban 40 állomást van, legalább 6 állomásbitet kell kölcsönvennünk. Ezt a 2^6 – 2 = 62 összefüggéssel határozhatjuk meg. A maradék 4 állomásbitet használhatjuk az alhálózatok kijelölésére. Ez az alhálózatok számát meghatározó összefüggés alapján 16 alhálózat: 2^4 = 16. Mivel a példa hálózat 9 alhálózatot igényel, ez pont megfelelő és még némi bővítési lehetőséget is tartalmaz.
- Amikor 4 bitet veszünk kölcsön, az új előtag hossza /26, az alhálózati maszk pedig 255.255.255.192.
- Ahogy azt a 1. ábra mutatja a /26 előtag hossz 16 alhálózat kialakítását teszi lehetővé. A címnek csak az alhálózati részét növeljük. Az eredeti 22 bites hálózati cím nem változik, a állomás rész pedig csupa 0-ás bitekből áll.
- **Megjegyzés:** Figyeljük meg, hogy az alhálózati rész a harmadik és negyedik oktettre is kiterjed, ezért az egyik vagy akár mindkettő változhat az alhálózat címekben!
- Ahogy azt a 2. ábra mutatja, az eredeti 172.16.0.0/22 hálózat egyetlen 10 állomásbites hálózat volt, mely 1,022 használható állomáscímet tartalmazott. 4 állomásbit kölcsönvételével 16 alhálózat keletkezett (0000-tól 1111-ig). Valamennyi alhálózatnak 6 állomásbitje és 62 használható állomáscíme van.
- Ahogy azt a 3. ábra szemlélteti, az alhálózatok LAN szegmensekhez és forgalomirányító-forgalomirányító kapcsolatokhoz rendelhetők.
- Hagyományos alhálózatok kialakításánál az egyes alhálózatokhoz rendelt címek száma megegyezik. Ha valamennyi alhálózat állomásszám igénye ugyanaz lenne, az ilyen a rögzített méretű címtartományok használata hatékony lenne. Az esetek jelentős részében azonban ez nem teljesül.
- Például az 1. ábrán bemutatott topológia hét alhálózatot igényel, mind a négy LAN és a forgalomirányítók közötti mindhárom WAN-kapcsolat egyet-egyet. A hagyományos alhálózatokra bontást alkalmazva az adott 192.168.20.0/24 hálózatcím utolsó oktettjének állomásazonosító részéből 3 bitet kölcsönvéve alakítható ki a hét alhálózat. Ahogy azt a 2. ábra mutatja, a 3 bit kölcsönvétele 8 alhálózatot eredményez, melyekben alhálózatonként a maradék 5 állomásbitnek köszönhetően 30 állomás lehet. Ez a módszer előállítja a kívánt alhálózatokat és teljesíti a legnagyobb LAN állomásszám igényét is.
- Bár a hagyományos alhálózatkialakítási módszer teljesíti a legnagyobb LAN állomásszám igényét és kellő számú alhálózatra osztja a címtartományt, jelentős számú kihasználatlan címet eredményez.
- Például mindössze két-két címre van szükség a három WAN kapcsolat alhálózatain. Mivel mindegyik alhálózat 30 címet tartalmaz, így ezen alhálózatok mindegyikén 28 kihasználatlan cím marad. Ahogy ezt a 3. ábra is szemlélteti, ez 84 kihasználatlan (28x3) címet eredményez.
- Mindemellett csökkenti a jövőben kiosztható alhálózatok számát is. Ez a címpazarló alhálózat kiosztás a jellemzője az osztály alapú hálózatok hagyományos alhálózatokra bontásának.
- Ebben a helyzetben a hagyományos alhálózatkialakítási módszer nem túl hatékony és pazarló. Valójában a példa jól mutatja, hogyan lehetne az alhálózatok további alhálózatokra bontásával javítani a címkihasználtságot.
- Az alhálózatok további alhálózatokra bontása, vagy más néven a változó hosszúságú alhálózati maszk (Variable Length Subnet Mask, VLSM)) alkalmazása elkerülhetővé teszi a címveszteséget.
- Vegyük észre, hogy az összes korábbi példában ugyan azt az alhálózati maszkot alkalmaztuk valamennyi alhálózatban. Ez azt eredményezi, hogy valamennyi alhálózatban ugyan annyi állomáscím kerülhet kiosztásra.
- Ahogy az az 1. ábrán is látszik, hagyományos alhálózatokra bontás azonos méretű alhálózatokat eredményez. A hagyományos módszer szerint valamennyi alhálózatban ugyan azt az alhálózati maszkot használjuk. Ahogy az a 2. ábra mutatja, a VLSM lehetővé teszi a hálózati tartomány egyenlőtlen felosztását. VLSM esetén az alhálózati maszk az egyes alhálózatokban kölcsönvett bitek számától függően változik, ez jelenti a „változót” a VLSM nevében.
- A VLSM-et használó alhálózatok kialakítása a bitek kölcsönvételét illetően nagyon hasonló a hagyományos alhálózatok kialakításához. Az állomáscímek és az alhálózatok számának meghatározására szolgáló összefüggések itt is érvényesek. A különbség az, hogy az alhálózatok kialakítása nem egy lépésben történik. VLSM esetén a hálózatot először alhálózatokra osztjuk, majd az alhálózatokat újból alhálózatokra bontjuk. Ezt a folyamatot a változó méretű alhálózatok kialakításának érdekében többször is megismételhetjük.

- A VLSM-folyamat jobb megértésének érdekében vegyük újból az előző példát.
- Ahogy azt az 1. ábra is mutatja, az előző példában a 192.168.20.0/24 hálózat lett nyolc egyenlő méretű alhálózatra bontva, melyekből hét került kiosztásra. Négy alhálózat LAN-okhoz lett felhasználva és három alhálózat a forgalomirányítók közötti WAN-kapcsolatokhoz. Emlékeztetőül, a jelentős címveszteség a WAN-kapcsolatok alhálózatain volt, mert ott csak két címre volt szükség: egy-egy a két forgalomirányító interfészre. Ennek a veszteségek elkerülésére használhatunk VLSM-et, hogy a WAN-kapcsolatokhoz kisebb méretű alhálózatokat rendeljünk.
- Ahhoz, hogy a WAN-kapcsolatokhoz kisebb méretű alhálózatokat hozzunk létre, az egyik alhálózatot bontjuk tovább. A 2. ábrán a 192.168.20.224/27 az utolsó alhálózat, ezt fogjuk most továbbosztani.
- Ne feledjük, hogy amikor a szükséges állomáscímek száma az ismert, akkor a 2^n-2 (ahol n a megmaradó állomásbitek száma) összefüggést használhatjuk. Ahhoz, hogy két kioszthatóó címünk legyen, 2 állomásbitnek kell maradnia az állomásazonosító részben.
- 2^2 – 2 = 2
- Mivel a 192.168.20.224/27 címtartományban 5 állomásbit van, ezért 3 bitet vehetünk kölcsön, így az állomás részben 2 bit marad.
- Itt a számítások teljesen megegyeznek a hagyományos alhálózatok kialakításánál látottakkal. Biteket veszünk kölcsön és meghatározzuk az alhálózati tartományokat.
- Ahogy azt a 2. ábra mutatja, a VLSM alhálózatszámítási módszer a WAN igényeinek megfelelően csökkenti le az alhálózatonkénti állomáscímek számát. A 7. alhálózat további alhálózatokra bontása létrehozza még a 4., 5. és 6. alhálózatokat, melyek további hálózatok, vagy WAN-kapcsolatok kialakítására alkalmasak.

A VLSM alhálózatok használatával a LAN és WAN szegmensek fölösleges pazarlás nélkül címezhetők.

A LAN-ok állomásai a /27-es maszkú alhálózatukból kapnak érvényes állomáscímeket. Mind a négy forgalomirányító LAN interfészéhez /27-es, míg az egy vagy több soros interfészükhöz /30-as alhálózat kapcsolódik.

A szokásos címzési mód szerint valamennyi alhálózat első IPv4 állomáscímét a forgalomirányító LAN interfésze kapja. A forgalomirányítók WAN interfésze a /30-as alhálózatból kap IP-címet és maszkot.

Az 1-4. ábrák a forgalomirányítók interfész konfigurációit mutatják.

Valamennyi alhálózat állomásai saját alhálózatukból kapnak érvényes állomáscímet és maszkot. Az állomások a kapcsolódó forgalomirányító LAN interfészének címét használják alapértelmezett átjáró címként.

- Az A épület állomásai (192.168.20.0/27) a forgalomirányító 192.168.20.1 címét használják alapértelmezett átjáróként.

- Az B épület állomásai (192.168.20.32/27) a forgalomirányító 192.168.20.33 címét használják alapértelmezett átjáróként.

- Az C épület állomásai (192.168.20.64/27) a forgalomirányító 192.168.20.65 címét használják alapértelmezett átjáróként.

- Az D épület állomásai (192.168.20.96/27) a forgalomirányító 192.168.20.97 címét használják alapértelmezett átjáróként.

A címzési terv elkészítését számos segédeszköz támogatja. Az egyik lehetséges módszer a foglalt és szabad blokkok nyilvántartására a VLSM-diagram alkalmazása. Használatával elkerülhető a már foglalt blokkok újrakiosztása. Az előző feladat hálózatának példáját alapul véve, a VLSM-diagrammal elkészíthetjük a címkiosztási tervet.

A /27 hálózatok vizsgálata

Ahogy azt az 1. ábra mutatja, amikor hagyományos alhálózatkiosztást használunk, az első hét címtartományt osztjuk ki a LAN-ok és WAN-ok számára. Emlékezzünk rá, hogy ez 8 (/27-es) alhálózatot és hálózatonként 30 érvényes állomáscímet eredményezett. Addig, amíg ez a módszer megfelelő volt a LAN-szegmensekre, jelentős címveszteséget okozott a WAN-szegmenseken.

Amikor az új hálózat címkiosztási tervét készítjük, a címtartományokat úgy kell kiosztanunk, hogy minimalizáljuk a veszteséget és egyben tartsuk a fel nem használt címtartományokat.

A VLSM címtartományok kijelölése

Ahogy azt a 2. ábra szemlélteti, annak érdekében, hogy a címtartományt hatékonyan használjuk, a WAN kapcsolatokhoz /30-as alhálózatokat hoztunk létre. Azért, hogy a kihasználatlan címtartományokat egyben tartsuk, az utolsó /27-es alhálózatot osztottuk tovább /30-as alhálózatokra. Az első három alhálózatot a WAN kapcsolatokhoz rendeltük.

- A .224 /30 állomáscím tartomány 225 és 226 címe: az R1 és R2 közötti WAN-kapcsolat.
- A .228 /30 állomáscím tartomány 229 és 230 címe: az R2 és R3 közötti WAN-kapcsolat.
- A .232 /30 állomáscím tartomány 233 és 234 címe: az R3 és R4 közötti WAN-kapcsolat.
- A .236 /30 állomáscím tartomány 237 és 238 címe: Szabadon felhasználható.
- A .240 /30 állomáscím tartomány 241 és 242 címe: Szabadon felhasználható.
- A .244 /30 állomáscím tartomány 245 és 246 címe: Szabadon felhasználható.
- A .248 /30 állomáscím tartomány 249 és 250 címe: Szabadon felhasználható.
- A .252 /30 állomáscím tartomány 253 és 254 címe: Szabadon felhasználható.

Az ilyen módon kialakított címzési terv 3 szabad /27-es és 5 szabad /30-as alhálózatot hagy.

Ahogy azt az ábra is mutatja, egy intézményi hálózat hálózati réteg címtartományának kiosztását alaposan meg kell tervezni. A címkiosztás nem lehet véletlenszerű. Három elsődleges szempont játszik szerepet a címkiosztásban.

- **A címduplikáció megakadályozása -** Egy hálózat valamennyi állomáscímének egyedinek kell lennie. Megfelelő tervezés és dokumentáció nélkül egy cím többször is kiosztásra kerülhet, amely mindkét állomás esetén hozzáférési problémákat okozhat.
- **A hozzáférés biztosítása és szabályozása -** Néhány állomás, például a kiszolgálók, mind belső, mind külső állomások számára nyújtanak szolgáltatásokat. A kiszolgálóhoz rendelt 3. rétegbeli cím alkalmas lehet a kiszolgálóhoz való hozzáférés szabályozása. Ha ellenben a címeket véletlenszerűen és rosszul dokumentáltan osztják ki, a hozzáférés szabályozása nehézkessé válhat.
- **Biztonsági és teljesítmény felügyelet -** Hasonlóképpen a hálózat állomásainak és a hálózat egészének biztonságát és teljesítményét felügyelnünk kell. A felügyeleti rendszer részeként a hálózat forgalmát vizsgálnunk kell olyan címek után kutatva, melyek túlzott csomagforgalmat generálnak, vagy fogadnak. Megfelelő hálózati címzési terv és dokumentáció esetén a problémás hálózati eszközök könnyen megtalálhatóak.

Címek kiosztása a hálózatban

A hálózatban különböző eszköztípusok találhatók, például:

- végfelhasználó kliensek
- szerverek és perifériák
- az internet felől elérhető állomások
- közvetítő eszközök
- átjáró

Az IP-címzési terv kialakításakor célszerű egy mintát kialakítani arra, hogy hogyan osszuk ki a címeket az egyes eszköztípusokra. Ez hasznára van a rendszergazdának, amikor új eszközöket állít be, vagy távolít el, amikor IP alapon szűri a forgalmat, vagy egyszerűen csak megkönnyíti a dokumentációt.

A hálózat címzési terve kitérhet az egyes alhálózatok eszköztípusonkénti különböző címtartományaira.

A kliensek címei

A statikus címkiosztás adminisztrációs nehézségei miatt a végfelhasználói eszközök gyakran dinamikus, DHCP-vel (Dynamic Host Configuration Protocol) hozzárendelt címeket kapnak. A DHCP általánosan előnyben részesített IP-címkiosztási módszer a nagyobb hálózatok esetén, mert csökkenti a hálózatot üzemeltető személyzet terheit és gyakorlatilag megszünteti az adatbeviteli hibákat.

A DHCP másik előnye, hogy a címek nincsenek állandóan egy állomáshoz rendelve, hanem csak egy időtartamra bérlik azokat. Így ha meg kell változtatnunk a hálózatunk alhálózati tervét, nem kell statikusan az egyes állomásokhoz a címet újra hozzárendelni. DHCP használata esetén elég a DHCP-szervert újrakonfigurálni az új alhálózati adatokkal. Ezt követően az állomásoknak csak automatikusan meg kell újítaniuk IP-címeiket.

Szerverek és perifériák címei

Ahogy azt az ábra szemlélteti, bármely hálózati erőforrásnak, mint például a kiszolgálóknak és nyomtatóknak statikus IP-címeiknek kell lenniük. A kliens állomások ezen eszközök erőforrásait az IP-címeiket felhasználva érik el. Emiatt ezen szerverek és perifériák címeinek előre meghatározhatónak kell lenniük.

A szerverek és perifériák a hálózat forgalmának torlódási pontjai. Ezen eszközök IPv4-címére sok csomag érkezik és maguk is sokat küldenek. Amikor megfigyeljük a hálózat forgalmát, mint pl. a Wireshark program, a hálózati rendszergazdáknak gyorsan fel kell tudni ismerni ezen eszközöket. Egy következetes címzési rendszer megkönnyítheti az azonosításukat.

Az internet felől elérhető állomások címei

A legtöbb hálózatban csak néhány eszköz van, amely az intézményen kívülről is elérhető. A legtöbb ilyen eszköz általában valamilyen kiszolgáló. Ahogy a hálózat valamennyi szolgáltatást nyújtó eszközének, úgy ezeknek is statikus IP-címének kell lennie.

Valamennyi az internet felől elérhető kiszolgálóhoz egy publikus címtartományból kell címet rendelni. Mindemellett ha valamelyikük címe megváltozna, akkor az az internet felől elérhetetlenné válna. Sok esetben ezek az eszközök olyan hálózatban vannak, amely privát címeket használ. Ez azt jelenti, hogy a hálózat peremén lévő forgalomirányítót, vagy tűzfalat úgy kell konfigurálni, hogy az a kiszolgáló belső címét egy publikus címmé alakítsa. A peremen lévő közvetítő eszköz többletkonfigurációja miatt még inkább fontos, hogy ezek az eszközök előre meghatározható címet kapjanak.

A közvetítő eszközök címei

A közvetítő eszközök ugyancsak torlódási pontjai a hálózat forgalmának. Szinte az összes hálózaton belüli, vagy hálózatok közti forgalom áthalad valamely közvetítő eszközön. Ezért ezen hálózati eszközök megfelelő helyet biztosítanak a hálózat-menedzsmentnek, a monitorozó és biztonsági rendszereknek.

A legtöbb közvetítő eszköznek van harmadik rétegbeli címe akár az eszközmenedzsment, akár a működésük érdekében. Az olyan eszközök, mint a HUB-ok, a kapcsolók és a vezeték nélküli hozzáférési pontok közvetítő eszközként való működésükhöz nem igényelnek IPv4-címet. Ellenben ha állomásként szeretnénk konfigurálni, megfigyelni, vagy hálózati hibaelhárítást végezni rajtuk, rendelkezniük kell saját címmel.

Mivel a közvetítő eszközökkel tudnunk kell kommunikálni, ezeknek is rögzített címekkel kell rendelkezniük. Ezért általában manuálisan hozzárendelt címeket kapnak. Mindemellett, ezen eszközök címeinek a hálózati tartomány egy a felhasználói eszközöktől elkülönülő részében kell lennie.

Az átjáró címe (forgalomirányítók és tűzfalak)

A többi közvetítő eszközzel ellentétben a forgalomirányítók és tűzfalak mindegyik interfészéhez van IP-cím rendelve. Minden interfész más hálózaton van, és az érintett hálózat állomásainak az átjárójaként szolgál. A forgalomirányító interfésze általában a hálózat legalacsonyabb, vagy legmagasabb címét kapja. Ennek a hozzárendelésnek egységesnek kell lenni az egész intézményi hálózatban, így a hálózat karbantartói mindig tudni fogják a hálózat átjáróját függetlenül attól, hogy melyik hálózaton dolgoznak.

A forgalomirányítók és tűzfalak interfészei a hálózatba érkező és az azt elhagyó forgalom torlódási pontjai. Mivel valamennyi hálózat állomásai egy forgalomirányító, vagy tűzfal interfészét használják átjáróként a hálózaton kívüli kapcsolatokhoz, ezért ezeken az interfészeken nagyszámú csomag halad át. Emiatt ezek az eszközök a csomagok forrás- és/vagy célcím szerinti szűrésével fontos szerepet játszhatnak a hálózatbiztonságban. Az eszközök különböző logikai címcsoportokba rendezése hatékonyabbá teszi a csomagszűrés feladatkijelölését és működését.

Az IPv6 alhálózatok kialakítása az IPv4 alhálózatokétól eltérő módon történik. Ennek elsődleges oka az IPv6 címek igen magas száma, így az alhálózatok kialakításának célja is teljesen eltérő. Egy IPv6 címtartományt nem a címekkel való takarékoskodás miatt bontunk alhálózatokra, hanem a hierarchikus logikai hálózattervezés érdekében. Amíg az IPv4 alhálózattervezés a címtartomány szűkösségének kezeléséről szólt, addig az IPv6 alhálózattervezés egy a forgalomirányítókat és hálózatokat támogató címhiararchia építését tűzi ki célul.

Ne feledjük, hogy ahogy azt az 1. ábra is szemlélteti, a /48-as IPv6 címtartományhoz 16 bites alhálózat azonosító (Subnet ID) tartozik. A 16 bites alhálózat azonosítóval pedig 65,536 darab /64 alhálózat alakítható ki úgy, hogy egyetlen bitet sem kell kölcsönöznünk az interfész azonosító (Interface ID), vagy állomás részéből a címnek. Valamennyi /64-es IPv6 alhálózat durván tizennyolc trillió címet tartalmaz, jóval többet, mint egy IP hálózati szegmens valaha is igényelhet.

Az alhálózat azonosítóból képzett alhálózatokat egyszerű ábrázolni, mert nincs szükség bináris átalakításra. A következő szabad alhálózat meghatározásához elég eggyel növelni a hexadecimális értéket. Ahogy ezt a 2. ábra is mutatja, ez nem más, mint hexadecimális számolás az alhálózat azonosító részben.

A globális előtag azonos valamennyi alhálózatban. Csak az alhálózatot azonosító kvartettek értéke növekedik minden alhálózatban.

A több mint 65,000 rendelkezésre álló alhálózat mellett a hálózati rendszergazdák feladatává válik a hálózat logikai címtervének elkészítése.

Ahogy azt az 1. ábra mutatja, a példa topológián alhálózatokat kell kialakítani valamennyi LAN-ra és az R1, R2 közötti WAN-kapcsolatra. Az IPv4 példával ellentétben, az IPv6 esetében a WAN-kapcsolatot nem bontjuk további alhálózatokra. Ez ugyan „címpazarlásnak” tűnhet, de ennek IPv6 esetén nincs jelentősége.

Ahogy azt a 2. ábra szemlélteti, a példában 5 darab, 0001-től 0005-ig terjedő alhálózat azonosítójú IPv6 alhálózatot osztunk ki. Valamennyi /64-es alhálózat jóval több címet biztosít, mint amire valaha is szüksége lehet.

Ahogy azt a 3. ábra mutatja, valamennyi LAN-szegmenshez és WAN-kapcsolathoz /64-es alhálózatot rendelünk.

Az IPv4 konfigurációjához hasonlóan valamennyi forgalomirányító interfész különböző IPv6-alhálózatba esik (lásd 4 ábra).

Hasonlóan, mint az IPv4-cím állomásbitjeiből való kölcsönvétel esetén történt, az IPv6-cím interfész azonosító (Interface ID) bitjeiből is vehetünk kölcsön újabb IPv6-alhálózatok kialakítására. Ez általában biztonsági megfontolásokból történik azért, hogy csökkentsük az alhálózatonkénti állomásszámot és nem újabb alhálózatok létrehozására.

Amikor az alhálózat azonosítót az interfész azonosítóból kölcsönvett bitekkel kiterjesztjük, azt legjobb egy nibble határon megtenni. A „nibble” 4 bit, vagy egy hexadecimális számjegy. Ahogy azt az ábra szemlélteti, a /64 alhálózati előtagot 4 bittel, azaz 1 nibble-el terjesztjük ki /68-ra. Ennek hatására az interfész azonosító mérete 4 bittel, 64-ről 60-ra csökken.

Az alhálózatok nibble határokon történő kialakítása nem jelent mást, mint a nibble határokra illeszkedő alhálózati maszk választást. A /64-től indulva a nibble határokra illeszkedő alhálózati maszkok a /68, /72, /76, /80, stb.

Nibble határokra eső alhálózatok választása esetén az alhálózatok címei hexadecimális értékekkel nőnek. A példában az új alhálózat azonosító 5 hexadecimális értékből áll, 00000-tól FFFFF-ig.

Egy nibble határon azaz, a hexadecimális helyértéken belül is lehet alhálózatot kialakítani, de nem ajánlott, hacsak az nem feltétlenül szükséges. A nibble határon belüli alhálózat kialakítás elnehezíti az előtag interfész azonosítóból való meghatározását. Például, ha az előtag hossza /66, az első két bit az alhálózat azonosító része lesz, a második két bit pedig az interfész azonosítóé marad.

A hálózat rendszergazdája arra kér bennünket, hogy a topológia ábrán látható hálózatra osszunk ki 5 darab /64-es IPv6 alhálózatot. A feladatunk az IPv6 alhálózatok meghatározása, az IPv6-címek forgalomirányítókra való kiosztása, és a PC-k automatikus IPv6-cím konfigurációjának engedélyezése. Az utolsó lépés az IPv6 állomások közötti kapcsolatok ellenőrzése.

Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme Instructions

Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme - PKA

Ahogy azt az ábra is szemlélteti, a hálózatok kisebb tartományokra történő felosztásának folyamatát, alhálózatokra bontásnak nevezzük.

Minden hálózati címhez egy érvényes állomáscím tartomány tartozik. Az ugyanazon hálózathoz kapcsolódó állomások ugyanabból a hálózati címtartományból kapnak IPv4-es címet, ezért megegyezik az alhálózati maszkjuk, illetve a hálózati előtagjuk is. Az azonos alhálózaton lévő állomások közvetlenül képesek egymásnak forgalmat továbbítani. Az alhálózatok között forgalomirányító használata nélkül semmilyen forgalom nem továbbítható. Azt, hogy a forgalom helyi vagy távoli, a forgalomirányító az alhálózati maszk alapján dönti el. Az előtag (prefix vagy prefixum) és az alhálózati maszk ugyanannak a dolognak - a cím hálózati részének - különböző megadási módjai.

Az IPv4-alhálózatok egy vagy több állomásbit hálózati bitként való értelmezésével keletkeznek. A megfelelő magánhálózati IP-címtartomány kiválasztásának két nagyon fontos szempontja, hogy mennyi a kialakítandó alhálózatok száma, valamint hogy mekkora az egyes alhálózatokra eső maximális állomásszám. Az alhálózatok száma és az állomások száma fordított arányban áll egymással. Minél több bitet veszünk kölcsön az alhálózatok számára, annál kevesebb állomásbit marad, ezért csökken az egyes alhálózatokban az állomások száma is.

A 2^n összefüggéssel (ahol n a megmaradó állomásbitek száma) határozható meg az egyes alhálózatokban rendelkezésre álló címek száma. Ebből azonban a hálózat címe és az üzenetszórási cím nem használható, ezért a ténylegesen használható címek száma a 2^n-2 összefüggéssel számítható.

Az alhálózatok további alhálózatokra bontása, azaz a változó hosszúságú alhálózati maszk (VLSM) a címveszteségek csökkentése érdekében lett bevezetve.

Az IPv6-alhálózatok kialakítása az IPv4-alhálózatokétól eltérő módon történik. Egy IPv6-os címtartományt nem a címekkel való takarékoskodás miatt bontunk alhálózatokra, hanem a hierarchikus logikai hálózattervezés érdekében. Amíg az IPv4 alhálózattervezés a címtartomány szűkösségének kezeléséről szólt, addig az IPv6 alhálózattervezés egy a forgalomirányítókat és hálózatokat támogató címhierarchia építését tűzi ki célul.

A gondos tervezés elengedhetetlenül fontos a rendelkezésre álló címtartomány legjobb kihasználásának érdekében. A méret, a hely, a felhasználás és a hozzáférési követelmények, mind lényeges szempontjai a címtervezési folyamatnak.

Megvalósítás után egy IP-hálózatot tesztelni kell, ellenőrizni kell a kapcsolatokat és a működés teljesítményét.

Megtapasztaljuk az internetet, valahányszor a világhálón keresztül videókat nézünk, online játékokat játszunk, chatelünk, e-mailezünk a barátokkal, vagy a webes vásárláskor alkuszunk. Az említett szolgáltatásokat is biztosító alkalmazások nyújtják számunkra a mögöttes hálózat használatához szükséges felületet. Ezek az alkalmazások teszik lehetővé az adatok viszonylag egyszerű küldését és fogadását. Az egyes alkalmazások használatához általában nem kell ismernünk a tényleges működésüket. Egy hálózati szakembereknek ugyanakkor fontos tudnia, hogy egy alkalmazás hogyan formázza, továbbítja és értelmezi a hálózaton keresztül küldött és fogadott üzeneteket.

A hálózati kommunikáció működését egyszerűbb bemutatni, ha ahhoz az OSI modell rétegezett keretrendszerét használjuk.

Ebben a fejezetben megvizsgáljuk az alkalmazási réteg szerepét és azt, hogy az alkalmazási réteg alkalmazásai, szolgáltatásai és az ott szereplő protokollok hogyan biztosítják a hálózaton keresztül a megbízható adatkommunikációt.

Mi történne, ha...

Munkaadónk úgy dönt, hogy IP-telefonokat kell telepíteni a munkahelyünkre, és emiatt a hálózat egy hétig működésképtelenné válik.

A munkánkat ugyanakkor folytatnunk kell. E-maileket kell elküldenünk és meg kell írnunk egy árajánlatot, amit majd vezetőnknek kell jóváhagyni. A felmerülő biztonsági aggályok miatt a céges munkánk elvégzéséhez nem megengedett a személyes, külső vagy telephelyen kívüli számítógépes rendszerek és eszközök használata.

Oktatónk kérheti, hogy válaszoljuk meg mindkét témakör kérdéseit, vagy válasszunk egyet a témakörök közül (A. e-mailek, vagy B. vezetői jóváhagyásra váró árajánlat). A témakör(ök) összes kérdésére adjunk választ! Készüljünk fel rá, hogy válaszokat a csoportban is megvitassuk!

A. E-mailek

- Milyen módszert vagy módszereket lehet használni e-mailek küldésére?
- Hogyan lehet ugyanazt az e-mailt több címzettnek is elküldeni?
- Hogyan lehet egy nagyméretű csatolmányt szükség esetén több címzetthez is eljuttatni?
- Költséghatékonyak-e ezek a módszerek a vállalatunk számára?
- Sértik-e a vállalatunk valamely biztonsági házirendjét?

B. Vezetői jóváhagyásra váró árajánlat

- A számítógépünkre egy irodai alkalmazásokból álló szoftvercsomag lett telepítve. Egyszerű lesz-e elkészíteni a vezetői jóváhagyásra váró árajánlatot a hét végére? Milyen problémák merülhetnek fel az árajánlat elkészítése közben?
- Hogyan tudjuk az árajánlatot a jóváhagyásra bemutatni a vezetőnknek? Vajon hogyan fogja majd továbbküldeni az árajánlatot az ügyfélnek az ő jóváhagyására?
- Költséghatékonyak-e ezek a módszerek a vállalatunk számára? Indokoljuk a választ!

Csoportos feladat - What would happen if... Instructions

A hálózati szakemberek mind szóban, mind pedig az írott műszaki dokumentációban az OSI és a TCP/IP modelleket egyaránt alkalmazzák (lásd ábra). Ezeket a modelleket használhatják a protokollok és az alkalmazások viselkedésének leírására.

Az OSI-modellben az adat rétegről-rétegre halad, elindulva a forrásállomás alkalmazási rétegéből, haladva lefelé a hierarchiában a fizikai rétegig, át a kommunikációs csatornán egészen a célállomásig, ahol aztán elindul felfelé a hierarchiában egészen az alkalmazási rétegig.

Az alkalmazási réteg mind az OSI mind a TCP/IP-modellnek a legfelső rétege. A TCP/IP-modell alkalmazási rétege számos, a végfelhasználói alkalmazások szolgáltatásaihoz szükséges protokollt tartalmaz. A TCP/IP alkalmazási rétegbeli protokolljainak funkciói nagyjából az OSI-modell felső három rétegének, az alkalmazási-, megjelenítési- és viszonyrétegnek felelnek meg. Az alkalmazásfejlesztők és gyártók az OSI-modell 5., 6. és 7. rétegére hivatkoznak hálózati hozzáférést igénylő termékeik, pl. egy web böngésző kapcsán.

Az alkalmazási réteg

A végfelhasználóhoz az alkalmazási réteg van a legközelebb. Ahogy azt az ábra is mutatja, ez az a réteg, amely az interfészt biztosítja az általunk kommunikációra használt alkalmazások és a mögöttes hálózat között, amelyen üzeneteink továbbítódnak. Az alkalmazási rétegbeli protokollokat a forrás- és célállomásokon futó programok közötti adatcserére használjuk. Számos alkalmazási rétegbeli protokoll létezik, és mindig vannak új, fejlesztés alatt álló protokollok is. A legismertebb alkalmazási rétegbeli protokollok a HTTP (Hypertext Transfer Protocol), az FTP (File Transfer Protocol), a TFTP (Trivial File Transfer Protocol), az IMAP (Internet Message Access Protocol) és a DNS (Domain Name System) protokoll.

A megjelenítési réteg

A megjelenítési rétegnek három fő funkciója van:

- Megjeleníti a forrásállomásról származó adatokat, vagy átalakítja azokat a célállomás által igényelt formára.

- Tömöríti az adatokat egy a célállomás által kitömöríthető formátumban.

- Titkosítja az adatokat az átvitelhez, valamint a célállomáson visszafejti azokat.

Amint az ábrán látható, a megjelenítési réteg az alkalmazási réteg adatait alakítja át, valamint határozza meg az egyes fájlformátumokra vonatkozó szabványokat. Az ismertebb videó szabványok közé tartozik a QuickTime és az MPEG (Motion Picture Experts Group). A QuickTime egy videóra és hangra vonatkozó Apple Computer által jegyzett szabvány, míg az MPEG szintén egy videó- és hangtömörítésre, valamint kódolásra szolgáló formátum.

A hálózatokon használt ismertebb grafikus képformátumok közé tartozik a GIF (Graphics Interchange Format), a JPEG (Joint Photographic Experts Group) és a PNG (Portable Network Graphics). A GIF és a JPEG rasztergrafikus képek tömörítésére és kódolására szolgáló szabványok. A PNG-t a GIF formátum bizonyos korlátainak kiküszöbölésére, majd végül a formátum lecserélésére tervezték.

A viszonyréteg

Ahogy a neve is utal rá, a viszonyréteg feladatai a forrás- és célalkalmazások közötti párbeszédek (munkamenetek) létrehozása és fenntartása. A viszonyréteg kezeli a párbeszédek kialakításához, fenntartásához, valamint a megszakadó vagy hosszabb ideje tétlen viszonyok újraindításához szükséges információcserét.

Míg az OSI-modell megkülönbözteti az alkalmazási-, megjelenítési- és viszony funkciókat, addig a széles körben ismert és használt TCP/IP-alapú alkalmazások egyesítik a három réteg funkcionalitását.

A TCP/IP alkalmazási protokolljai számos népszerű internetes kommunikációs szolgáltatás formátumát és vezérlőinformációit határozzák meg. Ezen TCP/IP-protokollok közé tartoznak az alábbiak:

- **Tartománynév-kezelő rendszer (Domain Name System, DNS)** - Ez a protokoll az internetes nevek IP-címekhez történő hozzárendelését végzi.

- **Telnet** - Szerverekhez és hálózati eszközökhöz való távoli hozzáférésre használjuk.

- **Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol, SMTP)** - Ez a protokoll e-mail üzeneteket és csatolmányokat továbbít.

- **Dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP)** - A protokollt arra használjuk, hogy egy állomáshoz IP-címet, alhálózati maszkot, alapértelmezett átjárót és DNS szervert rendeljünk.

- **Hiperszöveg továbbító protokoll (Hypertext Transfer Protocol, HTTP)** - Ez a protokoll a világháló weboldalait felépítő fájlokat továbbítja.

- **Fájlátviteli protokoll (File Transfer Protocol, FTP)** - A protokollt rendszerek közötti interaktív fájlátvitelre használjuk.

- **Fájlátviteli protokoll (File Transfer Protocol, FTP)** - Ezt a protokollt kapcsolat nélküli aktív fájlátvitelre használjuk.

- **Rendszerbetöltő protokoll (Bootstrap Protocol, BOOTP)** - Ez a protokoll a DHCP protokoll előfutára. A BOOTP egy hálózati protokoll, amelyet a rendszerindítás során az IP-címzési információk megszerzésére használunk.

- **Postahivatal protokoll (Post Office Protocol, POP)**- A protokollt a levelezőkliensek az e-mailek távoli szerverről történő letöltésére használják.

- **Internetes levélhozzáférési protokoll (Internet Message Access Protocol, IMAP)** - Ez egy másik, szintén a levelek letöltését szolgáló protokoll.

A kommunikációs folyamat során az alkalmazási rétegbeli protokollokat mind a forrás-, mind pedig a célállomás egyaránt használja. Hogy a kommunikáció sikeres legyen, a forrás- és célállomásokon használt alkalmazási rétegbeli protokolloknak egymással kompatibilisnek kell lenniük.

Amikor egy hálózati eszközön - legyen az PC, laptop, tablet, okostelefon vagy bármilyen más hálózatra csatlakoztatott eszköz - hozzáférünk valamilyen információhoz, akkor nem biztos, hogy az fizikailag is az adott eszközön van tárolva. Ebben az esetben az információ eléréséhez egy kérést kell küldeni az adatokat tároló eszköznek. Az egyenrangú (P2P, peer-to-peer) hálózati modellben az adatok elérése dedikált szerver használata nélkül, egy társ eszközről (peer) történik.

A P2P hálózati modell két részre bontható: P2P-hálózatokra és P2P-alkalmazásokra. Mindkét résznek hasonlók a tulajdonságaik, de a gyakorlatban egészen másként működnek.

P2P-hálózatok

Egy P2P-hálózatban két vagy több számítógép csatlakozik egymáshoz a hálózaton keresztül úgy, hogy dedikált szerver nélkül oszthatják meg egymás között az erőforrásaikat (pl. nyomtatókat vagy fájlokat). Minden csatlakoztatott végberendezés (más néven peer) működhet szerverként és kliensként is egyben. Egy számítógép az egyik adatátviteli folyamatban betöltheti a szerver szerepkörét, míg egy másikban ezzel egyidejűleg kliens is lehet. A szerver és a kliens szerepköröket az egyes kérések határozzák meg.

Példa lehet erre egy egyszerű otthoni hálózat két számítógéppel, ahogy az az ábrán is látható. A példában Peer2-nek van egy hozzá USB-n közvetlenül csatlakoztatott nyomtatója és be van állítva a hálózati megosztása úgy, hogy azon Peer1 tudjon nyomtatni. Peer1 pedig egy meghajtó vagy egy mappa hálózati megosztására van beállítva. Ez Peer2-nek lehetővé teszi a megosztott mappához való hozzáférést és abba fájlok mentését. Egy ilyen hálózat a fájlok megosztásán kívül a felhasználóknak a hálózati játékok használatát, vagy egy internetkapcsolat megosztását is biztosíthatja.

A P2P-hálózatok decentralizálják a hálózat erőforrásait. Az adatok dedikált szerverek helyett bárhol és bármely csatlakoztatott eszközön megoszthatók. A legtöbb mai operációs rendszer további szerverszoftver igénye nélkül támogatja a fájl- és nyomtatómegosztást. A P2P-hálózatok a jogosultságok kezelésére nem alkalmaznak központosított felhasználói fiókokat vagy hozzáférési szervereket. Ezért a néhány számítógépnél többet tartalmazó hálózatok esetében is már bonyolult lehet a biztonsági és a hozzáférési házirendek érvényre juttatása. A felhasználói fiókokat és a hozzáférési jogosultságokat az egyes eszközön egyedileg kell beállítani.

Egy peer-to-peer (P2P) alkalmazás lehetővé teszi, hogy egy eszköz ugyanabban a kommunikációban egyszerre kliens és szerver is lehessen (lásd ábra). Ebben a modellben minden kliens szerver is és minden szerver kliens is egyben. Mindkettő kezdeményezhet kommunikációt és a kommunikációs folyamatban egyenrangúnak tekintendők. A P2P-alkalmazások megkövetelik azonban, hogy minden végberendezés biztosítson egy felhasználói felületet és egy háttérszolgáltatást is futtasson. Amikor elindítunk egy adott P2P-alkalmazást, az betölti a szükséges felhasználói felületet és a háttérszolgáltatásokat, majd ezt követően az eszközök már közvetlenül tudnak egymással kommunikálni.

Bizonyos P2P-alkalmazások úgynevezett hibrid rendszert használnak, ahol az erőforrások megosztása ugyan decentralizált, de az erőforrások helyeire mutató indexeket már egy központi címtárban tárolják. A hibrid rendszerekben minden csomópont (peer) hozzáfér egy indexszerverhez, ahonnan lekérdezheti a más csomópontokon tárolt erőforrások helyét. Az indexszerver segíthet a két csomópont összekapcsolásában, de azt követően a csomópontok közötti kommunikáció már a szervertől függetlenül zajlik.

P2P-alkalmazásokat használhatunk P2P-hálózatokban, kliens-szerver hálózatokban és az interneten keresztül is.

P2P-alkalmazást használva a hálózat valamennyi számítógépe kliensként és szerverként is szolgálhat a hálózat azon többi számítógépe számára, amelyek ugyanazt az alkalmazást futtatják. Az ismertebb P2P-alkalmazások közé tartoznak a következők:

- eDonkey
- eMule
- Shareaza
- BitTorrent
- Bitcoin
- LionShare

Bizonyos P2P alkalmazások a Gnutella protokollra épülnek. A Gnutella lehetővé teszi felhasználóinak, hogy megosszák egymással a merevlemezeiken lévő fájlokat. Amint az az ábrán is látható, egy Gnutella kompatibilis kliensszoftver lehetővé teszi a felhasználóknak, hogy az interneten Gnutella szolgáltatásokhoz kapcsolódjanak, és más Gnutella csomópontok által megosztott állományokat találjanak meg és érjenek el. A Gnutella hálózat elérésére számos kliensalkalmazás létezik, közöttük a BearShare, a Gnucleus, a LimeWire, a Morpheus, a WinMX és a XoloX.

Míg az alapprotokollt a Gnutella Fejlesztői Fórum (Gnutella Developer Forum) gondozza, addig az alkalmazásforgalmazók gyakran fejlesztenek hozzá kiterjesztéseket, hogy a protokollt az alkalmazásaikba illeszthessék.

Számos P2P alkalmazás nem használ központi adatbázist, valamennyi fájlt a peer-ek tartanak nyilván. Lekérdezésre a hálózat valamennyi eszköze elmondja a többieknek, hogy rajta keresztül mely fájlok érhetők el, majd a fájlmegosztó protokollt és a szolgáltatásokat használják az állományok megkeresésére.

A kliens-szerver modellben az információt kérő eszközt kliensnek, a kérésre válaszoló eszközt pedig szervernek vagy kiszolgálónak nevezzük. A kliens- és szerverfolyamatokat az alkalmazási réteghez soroljuk. A párbeszédet a kliens kezdeményezi azzal, hogy adatokat kér a szervertől, amely aztán a kliensnek egy vagy több adatfolyam elküldésével válaszol. A kliensek és szerverek közötti kérések és válaszok formátumát az alkalmazási rétegbeli protokollok határozzák meg. A tényleges adatátvitel mellett ez a párbeszéd a felhasználó hitelesítését, valamint az átvitt adatfájl azonosítását is megkövetelheti.

A kliens-szerver hálózat egy példája, amikor egy ISP e-mail szolgáltatását használjuk levelek küldésére, fogadására és tárolására. Egy otthoni számítógépen lévő levelezőkliens egy kérést intéz az ISP levelezőszerveréhez egy olvasatlan levélért. A szerver ezután a válaszüzenetében elküldi a kért levelet a kliensnek.

Bár az adatok általában a szerverről áramlanak a kliens felé, bizonyos adatok mindig a kliens felől haladnak a szerver irányába. Az adatáramlás lehet mindkét irányban lehet egyenlő mértékű, de lehet akár nagyobb is a klienstől a szerver irányába. A kliens például tárolási célból átmásolhat egy fájlt a szerverre. Ahogy az ábra is mutatja, a kliensről a szerverre történő adatátvitelt feltöltésnek (upload), míg a szerverről a kliensre történőt letöltésnek (download) nevezzük.

Több tucat alkalmazási rétegbeli protokoll létezik, de egy átlagos napon talán csak ha ötöt vagy hatot használunk. Három olyan alkalmazási rétegbeli protokoll van, amelyek a mindennapi munkánkat vagy játékainkat biztosítják:

- Hiperszöveg továbbító protokoll (Hypertext Transfer Protocol, HTTP)

- Egyszerű levéltovábbító protokoll (Simple Mail Transfer Protocol, SMTP)
- Postahivatal protokoll (Post Office Protocol, POP)

Ezek az alkalmazási rétegbeli protokollok teszik lehetővé a világháló böngészését, valamint az e-mailek küldését és fogadását. A HTTP-t internetes weboldalakhoz való kapcsolódásra használjuk. Az SMTP e-mailek küldését teszi lehetővé. A POP pedig az e-mailek fogadására szolgál.

A következő néhány oldal erre a három alkalmazási rétegbeli protokollra fókuszál.

Amikor egy webcímet vagy URL-t (Uniform Resource Locator) begépelünk egy webböngészőbe, a böngésző a HTTP-protokollt használva építi ki a kapcsolatot a szerveren futó web-szolgáltatással. Az URL-ek azok az egységes erőforrás-azonosító (URI, Uniform Resource Identifier) nevek, amelyeket a legtöbb ember a webcímekkel társít.

A http://www.cisco.com/index.html URL egy olyan példa, amely egy meghatározott erőforrásra, az **index.html** nevű weboldalra hivatkozik a **cisco.com**nevű szerveren. Kattintsunk az ábra melletti számokra a HTTP által használt lépések megtekintéséhez!

A webböngésző a kliensalkalmazásoknak egy típusa, amelyet egy számítógép a világhálóra történő csatlakozásra, és egy webszerveren tárolt állományok elérésére használ. Mint a legtöbb szerverfolyamat, a webszerver is háttérszolgáltatásként fut és különböző típusú fájlok elérését teszi lehetővé.

A tartalom elérésére a webes kliensek kapcsolatokat alakítanak ki a szerverrel, majd kérik tőle a kívánt állományokat. A szerver a kért állománnyal válaszol, majd a böngésző értelmezi a kapott adatokat és megjeleníti a felhasználó számára.

A böngészők számos adattípust képesek értelmezni és megjeleníteni (ilyenek például az egyszerű szöveg, vagy a hiperszöveg, a nyelv melyben a weboldalakat írják). Bizonyos adattípusok ugyanakkor egyéb szolgáltatást vagy programot is igényelhetnek, amelyeket általában beépülő modulnak (plug-in) vagy kiegészítőnek (add-on) neveznek. A kapott fájl típusának megállapításában a böngészőt a szerver az állomány adattípusának meghatározásával segíti.

A webböngésző és a webszerver interakciójának jobb megértése érdekében vizsgálhatjuk meg, hogy egy oldal hogyan nyílik meg a böngészőben. A példához használjuk a http://www.cisco.com/index.html URL-t!

Ahogy az 1. ábra mutatja, a böngésző az URL három részét vizsgálja:

1. **http** (az alkalmazott protokoll vagy séma)

2. **www.cisco.com** (a szerver neve)

3. **index.html** (a kért fájl neve)

Ahogy a 2. ábra mutatja, a böngésző ezek után a névszerverhez fordul, hogy a www.cisco.com nevet egy numerikus címmé alakítsa át, amit majd a szerverhez történő csatlakozáshoz használ. A böngésző egy a HTTP szabványának megfelelő GET-üzenet küldésével kéri a kiszolgálótól az **index.html** fájl elküldését. Majd ahogy a 3. ábra mutatja, a szerver elküldi a böngészőnek az oldal HTML kódját. Végül a böngésző értelmezi a HTML kódot és megjeleníti az oldalt a böngészőablakban (lásd 4. ábra).

A HTTP-t a világhálón keresztüli adatátvitelre használjuk és egyike a leggyakrabban használt alkalmazási protokolloknak. Eredetileg egyszerűen HTML oldalak közzétételére és letöltésére találták ki, ám a HTTP-t a sokoldalúsága az elosztott közösségi információs rendszerek egyik alapvető alkalmazásává tette.

A HTTP egy kérés/válasz protokoll. Amikor egy kliens, általában egy webböngésző, kérést küld a webszervernek, a kommunikációhoz HTTP-üzenettípusokat használ. A három leggyakoribb üzenettípus a GET, a POST és a PUT (lásd ábra).

A GET a kliens adatkérése. A kliens (webböngésző) egy GET-üzenetet küld a webszervernek a HTML oldalak lekérésére. Amikor a szerver megkapja a GET-kérést, egy állapotkóddal (mint például a " HTTP/1.1 200 OK "), valamint magával az üzenettel válaszol. A kiszolgáló üzenete lehet maga a kért HTML fájl amennyiben az elérhető, vagy tartalmazhat egy hiba-, illetve információs üzenetet, mint például "A kért oldal nem található".

A POST és PUT-üzeneteket az adatfájlok webkiszolgálóra történő feltöltésére használjuk. Amikor egy felhasználó például kitölt egy weblapba ágyazott űrlapot (mint amikor egy megrendelést töltünk ki), a webszervernek egy POST-üzenet lesz elküldve. A felhasználó űrlapon beküldött adatait a POST-üzenet tartalmazza.

A PUT állományokat vagy egyéb tartalmakat tölt fel a webszerverre. Ha egy felhasználó például megpróbál egy fájlt vagy képet feltölteni a weboldalra, a kliens egy PUT üzenet küld a szervernek a csatolt fájllal vagy képpel.

Bár a HTTP rendkívül rugalmas, de nem egy biztonságos protokoll. A kérésüzenetek az információt kódolatlan szövegként továbbítják a szerverhez, amely így elfogható és mások által is elolvasható. A kiszolgálói válaszok, jellemzően HTML oldalak, ugyancsak titkosítatlanok.

A biztonságos internetes kommunikáció érdekében a webkiszolgáló eléréséhez vagy adatok közzétételéhez a HTTPS (HTTP Secure) protokollt használjuk. Az adatbiztonság megvalósítására a HTTPS a kliens és a szerver közötti adatforgalomra hitelesítést és titkosítást is alkalmazhat. Az adatok alkalmazási- és szállítási rétegek közötti továbbítására a HTTPS további szabályokat határoz meg. A HTTPS ugyanazt a kliens kérés és szerver válasz folyamatot használja mint a HTTP, csak a hálózati átvitelt megelőzően az adatfolyamot SSL-el (Secure Socket Layer) titkosítja. A forgalom titkosítása és visszafejtése miatt a HTTPS használata egy szerveren többletterhelést és feldolgozási időnövekedést okoz.

Az elektronikus levelezés az ISP-k által nyújtott egyik elsődleges szolgáltatás. Egyszerűsége és gyorsasága révén az e-mail forradalmasította az emberek kommunikációját. Az e-mail használata egy számítógépen vagy más végberendezésen különböző alkalmazásokat és szolgáltatásokat is igényel.

Az elektronikus levelezés egy tárol és továbbít (store-and-forward) módszer az üzenetek hálózaton keresztüli küldésére, tárolására és letöltésére. Az elektronikus leveleket a levelezőszervereken adatbázisokban tárolják. Az internetszolgáltatók gyakran olyan levelezőszervereket üzemeltetnek, amelyek egyszerre több előfizető fiókjait is kezelik.

A levelezőkliensek a szervereken keresztül küldik és fogadják a leveleket. Az üzeneteket egyik tartományból egy másikba történő továbbítása esetén a levelezőszerverek más levelezőszerverekkel is kapcsolatba kerülnek. Levélküldéskor a kliensek nem közvetlenül egymással kommunikálnak. Ehelyett mindkét kliens a levelezőszervert bízza meg az üzenetek továbbításával. Ez még abban az esetben is így történik, ha mindkét felhasználó ugyanabban a tartományban van.

Az levelezőkliensek az alkalmazás beállításaiban megadott levelezőszervernek küldik el az üzeneteket. Amikor a szerver megkapja az üzenetet, ellenőrzi hogy a címben szereplő tartomány megtalálható-e a helyi adatbázisában. Amennyiben nem, akkor egy DNS-kérést küld a címzett tartományért felelős levelezőszerver IP-címének meghatározására. Az e-mailt ezek után már a megfelelő szerverhez továbbítja.

Az e-mail három különböző protokollt használ a működéséhez: SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) és IMAP (Internet Message Access Protocol). A levelet elküldő alkalmazási rétegbeli folyamat az SMTP-t használja. Ez az az eset, amikor egy kliens a szervernek, vagy egy szerver egy másik szervernek küldi az üzenetet.

Ugyanakkor a levelek letöltéséhez a kliens a POP vagy az IMAP alkalmazási rétegbeli protokollok valamelyikét használja.

Az SMTP (Simple Mail Transfer Protocol) megbízhatóan és hatékonyan továbbítja a leveleket. Az SMTP alapú alkalmazások megfelelő működéséhez a levélüzenetnek megfelelő formátumúnak kell lenni, valamint az SMTP-folyamatnak mind a kliensen, mind pedig a szerveren futnia kell.

Az SMTP üzenetformátuma egy üzenetfejlécből és egy üzenettörzsből áll. Míg az üzenet törzse tetszőleges mennyiségű szöveget tartalmazhat, addig a fejlécnek megfelelő formátumban meg kell tartalmaznia a címzett és a feladó e-mail címét. A fejléc minden más része opcionális.

Amikor egy kliens e-mailt küld, akkor az SMTP-folyamata a jól ismert 25-ös porton kapcsolódik a szerver SMTP-folyamatához. A kapcsolat létrejötte után a kliens megpróbálja a levelet elküldeni a szervernek. Amikor a szerver megkapja az üzenetet, helyi címzett esetén azt egy helyi postafiókban helyezi el, vagy további kézbesítésre egy ugyanilyen SMTP-folyamattal átadja azt egy másik szervernek.

Előfordulhat, hogy az üzenetek küldésekor a címzett levelezőszervere nem elérhető. Ilyenkor az SMTP várakoztatja az üzeneteket, hogy azokat egy későbbi időpontban elküldhesse. A szerver rendszeresen ellenőrzi, hogy vannak-e üzenetek a várakozási sorában, és megpróbálja azokat újra elküldeni. Ha az üzenet egy előre meghatározott idő lejárta után sem kézbesíthető, akkor kézbesítetlenül visszakerül a feladóhoz.

A POP (Post Office Protocol) lehetővé teszi, hogy a munkaállomások e-mailek fogadjanak egy levelezőszervertől. POP használatakor a levelek a szerverről letöltődnek a kliensre, majd törlődnek a szerverről.

A szerver a POP-szolgáltatást a kliensek kapcsolódási kéréseire várva a 110-es TCP port passzív figyelésével indítja. Amikor a kliens a szolgáltatást igénybe kívánja venni, akkor egy kérést küld a szervernek a TCP kapcsolat felépítésére. A kapcsolat létrejötte után a POP-szerver egy üdvözlő üzenetet küld. Majd a kliens és a POP-szerver parancs- és válaszüzeneteket váltanak, amíg a kapcsolat le nem záródik, vagy meg nem szakad.

Mivel a kliensek letöltik az e-mail üzeneteket, majd azok eltávolításra kerülnek a szerverről, ezért a levelek nem egy központi helyen tárolódnak. A POP nem tárolja az üzeneteket, ezért használata nem előnyös olyan kisvállalkozások esetében, amelyeknek központosított biztonsági mentésre van szükségük.

A POP3 ugyanakkor megfelelő választás az ISP-k számára, mivel csökkenti a levelezőszervereiken kialakítandó nagyméretű tárolóterület kezelésének felelősségét.

Az IMAP (Internet Message Access Protocol) egy másik protokoll, amely ugyancsak az e-mail üzenetek letöltésére szolgál. A POP-al ellentétben, amikor a felhasználó egy IMAP-szerverhez csatlakozik, a kliensalkalmazáshoz csak az üzeneteknek egy másolata töltődik le. Az eredeti üzenetek továbbra is a szerveren maradnak, míg azokat külön le nem töröljük. A felhasználók az üzeneteknek csak a másolatát látják a levelezőprogramjukban.

A felhasználók a szerveren a levelek tárolására és rendszerezésére egy fájlhierarchiát hozhatnak létre. A fájlhierarchia másolata a levelezőkliensen is létrejön. Amikor a felhasználó egy üzenet törléséről dönt, a szerver szinkronizálja a műveletet és törli azt a szerverről is.

Kis- és középvállalkozások szempontjából számos előnye van az IMAP használatának. Az IMAP támogatja az e-mailek hosszú távú tárolását és központosított biztonsági mentéstét is. Több helyről, különböző eszközökről és különböző kliensprogramokkal is biztosítja az alkalmazottak hozzáférését e-mailjeikhez. A postafiók mappaszerkezetének megtekintése független annak elérési módjától.

Egy ISP számára az IMAP nem biztos, hogy a legmegfelelőbb választás. Költséges lehet a nagyszámú e-mail tárolásához szükséges lemezterület megvásárlása és karbantartása. Ezenkívül

amennyiben az előfizetők elvárják postafiókjainak rendszeres biztonsági mentését, az tovább növelheti az ISP költségeit.

Az adathálózatok eszközei a hálózaton keresztüli adatküldéséhez és fogadáshoz numerikus IP-címeket használnak. A legtöbb ember azonban nem képes megjegyezni ezeket a számokat. A numerikus címek egyszerű, megjegyezhető nevekké alakítására tartományneveket hoztak létre.

Ezek az internetes tartománynevek, mint például a http://www.cisco.com, sokkal könnyebben megjegyezhetők, mint mondjuk a 198.133.219.25, ami ennek a szervernek a tényleges numerikus címe. Ha a Cisco úgy dönt, hogy megváltoztatja a www.cisco.comnumerikus címét, azt a felhasználók nem is veszik észre, mivel a tartománynév ugyanaz marad. Az új címet egyszerűen a meglévő tartománynévhez kötik és így az elérhetőség továbbra is fennmarad. Amíg kisméretűek voltak a hálózatok, egyszerű feladat volt a címek és a hozzájuk tartozó tartománynevek egymáshoz rendelésének a karbantartása. Ahogy a hálózatok mérete és az eszközök száma növekedett, ez a kézi megoldás kezelhetetlenné vált.

A hálózatok tartományneveinek címekké fordítására a tartománynév-kezelő rendszert (Domain Name System, DNS) hozták létre. A DNS a címekhez tartozó nevek meghatározására egy elosztott szerverhálózatot használ. Kattintsunk az ábrán lévő gombokra a DNS címfeloldás lépéseinek megtekintéséhez!

A DNS-protokoll egy automatikus szolgáltatást definiál, amely erőforrásneveket társít a kért numerikus hálózati címhez. Tartalmazza még a lekérdezések, a válaszok és az adatok formátumát. A DNS-protokollra épülő kommunikációk egyetlen, üzenetnek nevezett formátumot használnak. Ezt az üzenetformátumot használják a klienslekérdezések és a szerverválaszok minden fajtájához, a hibaüzenetekhez, valamint az erőforrásrekordok szerverek közötti továbbításához.

A számok 1-től 5-ig a DNS névfeloldás lépéseit mutatják.

Egy DNS-szerver a névfeloldást a *BIND*(Berkeley Internet Name Domain) vagy ahogy gyakran nevezik a névfeloldó démon (name daemon vagy named) segítségével biztosítja. A BIND-ot eredetileg a kaliforniai Berkeley Egyetem négy diákja fejlesztette ki még az 1980-as évek elején. Ahogy az az ábrán is látható, a BIND által használt üzenetformátum a legszélesebb körben alkalmazott DNS-formátum az interneten.

A DNS-szerver a nevek feloldásához különböző típusú erőforrásrekordokat tárol. Ezek a bejegyzések a rekord nevét, címét és típusát tartalmazzák.

Néhány rekordtípus a következő:

- **A** – Egy állomás címe.
- **NS** - Egy mérvadó névkiszolgáló.
- **CNAME** - A kanonikus név (vagy teljes tartománynév, FQDN) egy álnév (alias). Akkor alkalmazzuk, amikor egyetlen hálózati címen több szolgáltatás fut, de ugyanakkor minden szolgáltatásnak saját DNS-bejegyzése van.
- **MX** – Levelezőszerver rekord (Mail Exchange). Az adott tartományhoz tartozó levelezőszerverekhez rendel egy nevet.

A kliens lekérdezésére a szerver BIND-folyamata a névfeloldáshoz először saját rekordjait vizsgálja meg. Ha a tárolt rekordjai alapján nem tudja a nevet feloldani, más szerverekkel lép kapcsolatba annak meghatározásához.

A kérés számos szerveren haladhat át, ami külön időt vesz igénybe és sávszélességet emészt fel. Miután keresés eredményre vezetett, és a válasz is visszajutott az eredeti kérelmező szerverhez, az a névhez tartozó címet átmenetileg egy cache memóriában tárolja.

Ha ismét ugyanazt a nevet kérik, az első szerver már a cache memóriájában tárolt értéket használva is képes a címet visszaadni. A gyorsítótárazás csökkenti mind a DNS-lekérdezések okozta adathálózati forgalmat, valamint a hierarchiában feljebb lévő szerverek terhelését. A Windows-os PC-k DNS-kliense a névfeloldás teljesítményét úgy optimalizálja, hogy a korábban feloldott neveket a saját memóriájába is eltárolja. A **ipconfig /displaydns** utasítás egy Windows-os számítógép gyorsítótárának DNS-bejegyzéseit mutatja meg.

A DNS-protokoll a névfeloldásra egy hierarchikusan felépített adatbázist használ. A hierarchia úgy néz ki, mint egy fordított fa, tetején a gyökérrel és alatta ágakkal (lásd ábra). A hierarchiát a DNS által használt tartománynevek alkotják.

Az elnevezési struktúra kisebb, könnyen kezelhető zónákra lett osztva. Minden DNS-szerver egy meghatározott adatbázisfájlt tart karban, és a teljes DNS-struktúra csak egy kis részének név-IP-cím hozzárendeléséért felelős. Amikor egy DNS-szerver egy olyan névfeloldási kérést kap, amely nincs benne a zónájában, akkor azt a szerver egy másik, a megfelelő zónához tartozó DNS-szerverhez továbbítja.

Megjegyzés: A DNS jól méretezhető, mivel az állomásnevek feloldása számos szerver között oszlik meg.

A legfelső szintű tartományok a szervezet típusát vagy a származási országot jelölik. Példák a legmagasabb szintű tartományokra:

- **.hu -** Magyarország
- **.co -** Kolumbia
- **.com -** kereskedelem vagy ipar
- **.jp -** Japán
- **.org -** egy non-profit szervezet

A legfelső szintű tartományok után a második szintű tartománynevek következnek, azok alatt pedig az egyéb alacsonyabb szintű tartományok vannak. Minden tartománynév egy a gyökértől kiinduló lefelé vezető út ebben a fordított fában. Ahogy az ábra példája mutatja, a gyökér (root) DNS-szerver nem feltétlenül tudja, hogy a mail.cisco.com levelezőszerver rekordja hol van tárolva, de fenntart egy rekordot a .com legfelső szintű tartományhoz. Hasonlóképpen a .com tartományba tartozó szerverek nem biztos hogy rendelkeznek a mail.cisco.com rekorddal, de van egy bejegyzésük a cisco.com tartományhoz. A cisco.com tartományba tartozó szervereknek pedig már van egy rekordjuk (egész pontosan egy MX rekordjuk) a mail.cisco.com-ra.

A DNS az erőforrásrekordok decentralizált szerverek hierarchiáján történő tárolására és karbantartására épül. Az erőforrásrekordok a szerver által feloldani képes tartományneveket és a kérések feldolgozásának további szervereit tartalmazzák. Ha egy szervernek a tartományhierarchia szintjének megfelelő erőforrásrekordjai vannak, akkor ezekre a bejegyzésekre vonatkozóan őt mérvadónak mondjuk. Például a cisco.netacad.net tartományban egy névszerver nem lehet mérvadó a mail.cisco.com rekordra, mert ezt a rekordot egy magasabb tartományi szintű szerver tartja nyilván, konkrétan a cisco.com tartomány névszervere.

A DNS egy kliens-szerver szolgáltatás, ámbár különbözik egyéb kliens-szerver szolgáltatásoktól. Míg más szolgáltatások egy kliensalkalmazást (például böngészőt, levelezőprogramot) használnak, addig

a DNS-kliens egyidejűleg maga is szolgáltatásként fut. A DNS-klienst gyakran DNS-feloldónak (resolver) nevezik. Névfeloldást biztosít az azt igénylő alkalmazások és szolgáltatások számra.

Egy hálózati eszköz konfigurálásakor általában egy vagy több DNS-szerver címét is megadjuk, melyeket a DNS-kliens a névfeloldáskor használ. A DNS-szerverek címeit rendszerint az internetszolgáltató (ISP) biztosítja. Amikor a felhasználó alkalmazása név alapján szeretne egy távoli eszközhöz csatlakozni, a kérelmező DNS-kliens ezen névszerverek egyikét kérdezi le, hogy a nevet numerikus címmé alakítsa.

A számítógépes operációs rendszereknek van egy nslookup nevű segédprogramja is, amely lehetővé teszi egy adott állomásnév feloldásához a névszerverek manuális lekérdezését. Ezt a segédprogramot névfeloldási problémák hibakereséséhez és a névszerverek pillanatnyi állapotának ellenőrzésére is használhatjuk.

Amikor kiadjuk az **nslookup** parancsot, az állomásunkon alapértelmezettként beállított névszerver jelenik meg (lásd ábra). Ebben a példában a DNS-szerver a dns-sj.cisco.com, aminek a címe 171.70.168.183.

Az **nslookup** parancssorába egy állomás vagy tartomány nevét írhatjuk be. Az ábrán az első lekérdezés a `www.cisco.com` lekérdezése. A válaszoló névszerver a `198.133.219.25` címet adja rá vissza.

Az ábrán látható lekérdezések csak egyszerű próbák. Az nslookup számos lehetőséget biztosít a DNS-folyamat átfogó tesztelésre és ellenőrzésére. Befejezéskor az **exit**parancs begépelésével léphetünk ki az nslookup segédprogramból.

A dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol, DHCP) szolgáltatás a hálózaton lévő eszközök számára biztosítja, hogy egy DHCP-szervertől IP-címeket és egyéb információkat kaphassanak. A szolgáltatás automatizálja az IP-címek, alhálózati maszkok, átjárók és egyéb IP-hálózati paraméterek kiosztását. Ezt dinamikus címzésnek nevezzük. A dinamikus címzés alternatívája a statikus címzés. Statikus címzés alkalmazásakor a rendszergazda manuálisan állítja be az IP-címzési információkat a hálózat állomásain.

A DHCP lehetővé teszi, hogy egy állomás a hálózatra csatlakozásakor dinamikusan kaphasson IP-címet. Kapcsolatba lép egy DHCP-szerverrel és kér tőle egy IP-címet. A DHCP-szerver választ egy címet a hatókörnek (pool) nevezett, előre konfigurált címtartományból és egy meghatározott időtartamra kiutalja (bérbe adja) azt az állomásnak.

Nagyobb helyi hálózatokban, vagy ahol a felhasználók gyakran változnak, a DHCP a javasolt címkiosztási módszer. Új felhasználók jöhetnek, akiknek csatlakozásra van szükségük a laptopjaik számára, mások új munkaállomásokat kaphatnak, amiket ugyancsak csatlakoztatni kell. Ahelyett, hogy minden munkaállomáshoz a hálózati rendszergazdának kellene IP-címeket rendelnie, sokkal hatékonyabb, ha azok kiosztása dinamikusan, a DHCP használatával történik.

A DHCP által kiosztott címek nem végérvényesen vannak az állomásokhoz rendelve, csak egy adott időtartamra adják bérbe azokat. Ha az állomást kikapcsolják vagy eltávolítják a hálózatról, a cím újrafelhasználásra visszakerül a készletbe. Ez különösen a mobil felhasználók esetében hasznos, akik csak úgy jönnek-mennek a hálózaton. A felhasználók szabadon mozoghatnak egyik helyről a másikra és hozhatnak létre újra hálózati kapcsolatokat. Az állomás a hardveres kapcsolat létrejötte után kap IP-címet, akár vezetékes- akár vezeték nélküli LAN-on keresztül csatlakozik.

A DHCP lehetővé teszi, hogy repülőtereken vagy kávézókban vezeték nélküli hotspot-okon keresztül csatlakozzunk az internetre. Amikor egy vezeték nélküli eszköz csatlakozik a hotspot-hoz, a DHCP-kliense a vezeték nélküli kapcsolaton keresztül kapcsolatba lép a helyi DHCP-szerverrel, ami kioszt egy IP-címet az eszköznek.

Ahogy az ábra mutatja, különböző típusú eszközök lehetnek DHCP-szerverek, amennyiben DHCP-szerverszoftvert futtatnak. A legtöbb közepes- és nagyméretű hálózatban a DHCP-szerver általában

dedikáltan egy helyi PC-alapú szerver. Otthoni hálózatokban a DHCP-szerver általában azon a helyi forgalomirányítón található, amely az otthoni hálózatot az ISP-hez csatlakoztatja. A helyi állomások közvetlenül ettől a helyi forgalomirányítótól kapják az IP-címzési információkat. A helyi forgalomirányító pedig az ISP DHCP-szerverétől kap egy saját IP-címet.

A DHCP biztonsági kockázatot is jelenthet, mivel bármely a hálózatra csatlakozó eszköz kaphat egy címet. Ez a kockázat meghatározó tényezővé teszi a fizikai biztonságot, akár dinamikus, akár manuális címzést használunk. Mind a dinamikus-, mind a statikus címzésnek helye van a hálózatterezésben. Sok hálózat használ egyszerre DHCP-t és statikus címzést is. DHCP-t használunk általában az általános célú állomásokon, mint a végfelhasználói berendezéseken, és statikus címzést használunk a hálózati eszközökön, mint az átjárókon, kapcsolókon, szervereken és nyomtatókon.

DHCP nélkül a felhasználóknak hálózatra csatlakozáskor manuálisan kellene megadniuk az IP-címet, az alhálózati maszkot és egyéb hálózati beállításokat. A DHCP-szerver egy IP-címkészletet kezel, és ad bérbe belőle egy címet bekapcsoláskor bármely DHCP-képes kliensnek. Mivel az IP-címek dinamikusak (béreltek), ellentétben a statikus címzéssel (állandó hozzárendelés), a már nem használt címek újbóli kiosztásra automatikusan visszakerülnek a készletbe. Amint az ábra mutatja, amikor egy DHCP-re konfigurált eszköz elindul vagy csatlakozik a hálózatra, a kliens egy szórásos DHCP-felfedező (DHCPDISCOVER) üzenetet küld szét, hogy egy a hálózaton elérhető DHCP-szervert találjon. A DHCP-szerver egy DHCP-ajánlás (DHCPOFFER) üzenettel válaszol, amely a kliensnek felajánl egy címbérletet. Az ajánlat tartalmazza a kiosztott IP-címet és alhálózati maszkot, a DNS-szerver IP-címét, valamint az alapértelmezett átjáró IP-címét. Az ajánlott címbérlet tartalmazza még bérlet időtartamát is.

A kliens több DHCPOFFER üzenetet is kaphat, amennyiben egynél több DHCP-szerver is van a helyi hálózaton. Ezért választania kell közülük, majd a kliens egy DHCP-igénylés (DHCPREQUEST) üzenetet küld az elfogadott bérleti ajánlatra az azt kibocsátó szervernek. Egy kliens dönthet úgy is, hogy egy olyan címet kér, amelyet a szerver egyszer korábban már kiosztott neki.

Abban az esetben, ha a kliens által megigényelt vagy a szerver által kiajánlott IP-cím továbbra is rendelkezésre áll, a szerver egy DHCP-nyugta (DHCPACK) üzenettel válaszol, amely visszaigazolja a kliensnek a bérlet véglegesítését. Ha az ajánlat már nem érvényes egy esetleges időtúllépés miatt, vagy mert egy másik kliens már megkapta a címbérletet, akkor a kiválasztott szerver egy negatív DHCP-nyugta (DHCPNAK) üzenettel válaszol. Amennyiben egy DHCPNAK-üzenet érkezik vissza, akkor a kérelmezési folyamatot újra kell kezdeni egy DHCPDISCOVER üzenet kiküldésével. Miután a kliens megszerezte a címbérletet, a bérleti idő lejártakor azt egy újabb DHCPREQUEST üzenettel meg kell újítania.

Az IP-címek egyediségét a DHCP-szerver biztosítja (ugyanazt az IP-címet nem lehet párhozamosan két hálózati eszközhöz hozzárendelni). A DHCP használata lehetővé teszi, hogy a hálózati rendszergazdák a kliensek IP-címeit könnyen, a kliensek manuális módosítása nélkül újrakonfigurálhassák. A legtöbb internetszolgáltató DHCP-t használ a statikus címet nem igénylő előfizetőik címkiosztásához.

Egy másik általánosan használt alkalmazási rétegbeli protokoll a fájlátviteli protokoll (File Transfer Protocol, FTP). Az FTP-t egy kliens és egy szerver közötti adatátvitelre fejlesztették ki. Az FTP-kliens egy FTP-démont (FTPd) futtató szerverről való adatletöltésre vagy arra történő adatfeltöltésre szolgáló alkalmazás.

Amint azt az ábra is mutatja, a kliens és a szerver közötti sikeres adatátvitelhez az FTP két kapcsolatot igényel. Egyet a parancsoknak és a válaszoknak, a másikat pedig a tényleges fájlátvitelhez.

- Az első kapcsolatot a szerverrel a kliens kezdeményezi a kliens parancsaiból és a szerver válaszaiból álló vezérlési forgalomnak.

- Szintén a kliens kezdeményezi a tényleges adatátvitelre szolgáló második kapcsolatot is a szerverrel. Ez a kapcsolat minden egyes adatátvitel alkalmával létrejön.

Az adatátvitel mindkét irányba megtörténhet. A kliens tölthet le adatokat a szerverről és oda tölthet is fel adatokat.

Az SMB (Server Message Block) egy az IBM által az 1980-as évek végén kifejlesztett kliens-szerver fájlmegosztó protokoll, amely olyan osztott hálózati erőforrások szerkezetét írja le, mint például könyvtárak, fájlok, nyomtatók és soros portok. Ez egy kérés-válasz protokoll.

Az SMB-protokoll leírja a fájlrendszer elérését, valamint azt, hogy a kliensek hogyan kérhetik le a fájlokat. Leírja továbbá az SMB-protokoll folyamatok közötti belső kommunikációját is. Minden SMB-üzenetnek közös a formátuma. Ez a formátum egy állandó hosszúságú fejlécet és egy azt követő változó méretű paraméter- és adatkomponenst használ.

Az SMB-üzenetek az alábbiakra alkalmasak:

- Párbeszédek indítása, hitelesítése és lezárása.
- Fájl- és nyomtatóelérés vezérlése.
- Egy alkalmazás és egy másik eszköz üzenetváltásainak biztosítása.

Az SMB alapú fájlmegosztás és nyomtatás a Microsoft legfőbb hálózati szolgáltatásaivá vált. A Windows 2000 szoftversorozat megjelenésével a Microsoft megváltoztatta az SMB által használt mögöttes struktúrát. A Microsoft termékek korábbi verzióiban az SMB-szolgáltatások névfeloldásra még nem TCP/IP-re épülő protokollt használtak. A Windows 2000-től minden Microsoft termék már DNS neveket használ, ami közvetlenül támogatja az SMB-erőforrások TCP/IP protokoll alapú megosztását (lásd 1. ábra). A 2. ábra két Windows PC közti SMB-alapú fájlcserefolyamatot szemlélteti.

A fájlátviteli protokollal (FTP) ellentétben a fájlmegosztásra a kliensek tartós kapcsolatokat építenek ki a szerverekkel. A kapcsolat létrejötte után a kliens felhasználója a szerveren lévő erőforrásokat helyi erőforrásként tudja elérni.

A Linux és Unix operációs rendszerek egy SAMBA nevű SMB-verzió alkalmazásával biztosítanak módszert a Microsoft hálózatokkal történő erőforrás-megosztásához. Az Apple Macintosh operációs rendszerek ugyancsak támogatják az SMB-protokoll alapú erőforrás-megosztást.

Az alkalmazási réteg felelős a hálózati kommunikációt kezelő és továbbító mögöttes folyamatok közvetlen eléréséért. Az adathálózat típusától függetlenül ez a réteg egyben a kommunikációk forrása és célja is. Valójában a hálózathasználat fejlődése egyben az alkalmazástípusok fejlesztésére is kihat.

Az olyan trendek, mint a „hozd a saját eszközöd” (Bring Your Own Device, BYOD), a bárhonnan történő hozzáférés lehetősége, a virtualizáció, valamint a gép-gép közti közvetlen kommunikáció (Machine-to-Machine, M2M) újfajta alkalmazásoknak nyitottak utat. A becslések szerint 2020-ra mintegy 50 milliárd eszköz lesz összekapcsolva. Egyedül 2010-ben több mint 350 000 alkalmazást fejlesztettek, több mint 3 millió letöltéssel. Mindez az emberek ösztönös kapcsolatainak, folyamatoknak, adatoknak és tárgyaknak a világát eredményezi a hálózaton.

Az "okos" címkék használata, valamint a hétköznapi eszközök – a kerékpároktól és palackoktól kezdve a hűtőszekrényeken át a járművekig – digitálissá tétele és internetre csatlakoztatása új és szinte elképzelhetetlen távlatokat nyit az emberek, de a vállalatok interakciójában is. A tárgyak képesek lesznek információt gyűjteni, fogadni és küldeni felhasználóiknak és más eszközöknek is. Ahogy azt az ábra is szemlélteti, az internet fejlődésének ez az új hulláma a tárgyak internete (Internet of Things, IoT) vagy "minden a hálón" néven vált ismertté.

Mára több mint 100 millió árusító automata, jármű, füstérzékelő és egyéb eszköz oszt meg automatikusan információkat, és ez szám a Berg Insight piackutató számításai szerint 2016-ra eléri a 360 milliót. Ma a fénymásolók egy M2M-modullal automatikusan képesek friss tonert és papírt

rendelni, vagy egy hiba miatt riasztani a technikust, akár a javításhoz szükséges alkatrészt is meghatározva.

Az alkalmazások számának robbanása nagyrészt a hálózati adatfeldolgozás hatékony réteges szemléletének köszönhető. Különösen az alkalmazási réteg és az adattovábbítás funkcióinak elkülönítése segít abban, hogy az alkalmazási protokollokat megváltoztathassuk, és új alkalmazásokat fejleszthessünk anélkül, hogy az adatok hálózaton keresztüli átjutásával külön foglalkozni kellene. Ez a feladat más rétegekre, azaz más fejlesztőkre hárul.

Ahogy azt az ábra mutatja, amikor egy alkalmazás egy kérést küld a szerveralkalmazásnak, akkor az alkalmazási réteg összeállítja az üzenetet, majd kézbesítésre továbbadja a kliens alsóbb rétegeinek. Ahogy az üzenet végighalad a protokoll-vermen, minden alsóbb réteg beágyazza azt, azaz ellátja a saját kommunikációs protokolljához tartozó fejléccel. Ezeknek a küldő- és fogadóállomáson is meglévő protokolloknak az együttműködése teszi lehetővé az alkalmazások végponttól végpontig terjedő hálózati adattovábbítását.

Protokollok - mint például a HTTP - teszik lehetővé a weboldalak állomásokhoz való eljutását. Miután már tanultunk a különböző rétegekről és funkcióikról, végigkövethetjük egy weboldal webszerverről történő lekérését, hogy lássuk ezen független funkciók teljes együttműködését.

A TCP/IP modellt szerint a teljes kommunikációs folyamat hat lépésből áll:

Az adatok létrehozása

Az első lépés az adatok létrehozása a kezdeményező forrásállomás alkalmazási rétegében. Ebben az esetben a webes kliens HTTP GET-kérésének összeállítása után az adatokat kódolják, tömörítik és szükség esetén titkosítják. A TCP/IP modellben ez az alkalmazási rétegbeli protokoll feladata, mivel az magába foglalja az OSI-modell alkalmazási-, megjelenítési- és viszonyrétegei funkcióit is. Az alkalmazási réteg ezeket az adatokat adatfolyam formájában küldi tovább a szállítási rétegnek.

Szegmentáció és kezdeti adatbeágyazás

A protokoll-vermen lefelé haladva a következő lépés az adatok szegmentációja és beágyazása. A szállítási rétegben a HTTP GET-üzenetet kisebb és kezelhetőbb darabokra tördelik, majd minden egyes darab egy szállítási rétegbeli fejlécet kap. A szállítási réteg fejlécében az üzenet újbóli összeállításához szükséges adatok vannak. Tartalmaz egy azonosítót is, a 80-as portszámot. Ez jelzi majd a célszervernek, hogy az üzenet a webszerver alkalmazásnak küldték. Hozzáadódik még egy véletlen generált forrásport azonosító is, hogy a kliens képes legyen a visszatérő kommunikációt a megfelelő kliensalkalmazásának továbbítani.

Címzés

A következő lépésben, ahogy azt az ábra is mutatja, a szegmensek címazonosítókat kapnak. Ahogyan az adatok célhoz történő továbbítását előkészítő protokolloknak is több rétege van, úgy a kézbesítést biztosító címzés is többrétegű. A hálózati réteg feladata az adatok forrástól a célállomásig történő eljutását biztosító címek hozzáadása. A hálózati réteg ezt a szegmensek IP-csomagba történő beágyazásával oldja meg. Az IP-csomag fejléce tartalmazza a forrás- és célállomások IP-címeit. (A célállomás IP-címét általában egy tartománynév DNS lekérdezéséből nyerjük.) A forrás és cél IP-cím, valamint a forrásport és a célport együttesét socket-nek nevezzük. A socket-et használjuk a kliens által kért kiszolgáló és szolgáltatás azonosítására.

Az átvitel előkészítése

Miután a csomag megkapta az IP-címzést, azt a hálózatelérési réteghez továbbítják, hogy az adatok az átviteli közegre kerülhessenek (lásd ábra). Azért hogy ez rendben megtörténhessen, a hálózatelérési rétegnek a csomagot egy fejléccel és egy utótaggal ellátott keretbe kell ágyaznia. Ez a keret tartalmazza a forrásállomás, valamint a célállomás felé vezető útvonal következő állomásának (next hop) fizikai címét. Ez megegyezik az OSI-modell második, azaz adatkapcsolati rétegének (Layer

2) funkciójával. A második réteg egy helyi hálózaton belüli végzi az üzenetek továbbítását. A második rétegbeli cím az adott helyi hálózaton egyedi és a végberendezés címét reprezentálja a fizikai közegen. Ethernetet használó LAN-okban ezt a címet közeghozzáférés-vezérlési címnek (MAC, Media Access Control) nevezik. A hálózatelérési réteg a forrás- és célcímekkel kiegészített keretet, bitekké, aztán pedig elektromos- vagy fényimpulzus jelekké alakítja, majd a fizikai közegen továbbítja.

Az adatok átvitele

Az adatokat átviteli közegekből és közvetítő eszközökből álló összekapcsolt hálózatokon keresztül továbbítjuk. Ahogy a beágyazott üzenet átjut a hálózaton, különböző közegeken és hálózattípusokon megy keresztül. A hálózatelérési réteg határozza meg a különböző közegek keretformátumát és a keretek küldési módját, amit közeghozzáférés-vezérlésnek nevezünk.

Ha cél- és a forrásállomás ugyanazon a hálózaton van, akkor a csomag a két állomás között a helyi közegen forgalomirányító szükségessége nélkül kerül kézbesítésre. Ha azonban a cél- és a forrásállomás nem ugyanazon a hálózaton vannak, akkor a csomag továbbítása számos hálózaton, különböző közegtípusokon és forgalomirányítókon keresztül történhet. Ahogy a keret áthalad a hálózaton, a benne lévő információ nem változik.

A helyi hálózatok határán egy közvetítő eszköz, általában egy forgalomirányító, kibontja a keretet, hogy a csomag fejlécéből kiolvashassa a célállomás címét. A forgalomirányítók ezen cím hálózatazonosító részét használják a célállomáshoz vezető út meghatározására. Ahogy a forgalomirányító az útvonalat meghatározta, a csomagot új keretbe ágyazza és elküldi a célállomáshoz vezető út következő ugrásának címére.

Az adatok kézbesítése a megfelelő alkalmazáshoz

Végül a keret megérkezik a célállomáshoz. Ahogyan az adat a célállomáson felfelé halad a protokoll-veremben, beágyazását visszafejtik, majd végül újból összeállítják. A hálózatelérési rétegtől, a hálózati rétegen és a szállítási rétegen keresztül az adat folytonosan halad felfelé míg végül el nem éri az alkalmazási réteget, ahol feldolgozásra kerül. De honnét tudja az eszköz, hogy az adatok a megfelelő alkalmazáshoz jutottak-e?

Emlékezzünk rá, hogy a szállítási rétegbeli PDU fejlécének adatai azonosítják a célállomáson azt a folyamatot vagy szolgáltatást, amelyhez az illető adat tartozik (lásd ábra). Az állomások, akár kliensek, akár szerverek az interneten, több hálózati szolgáltatást is képesek párhuzamosan futtatni. Egy PC-n gyakran egyszerre van megnyitva egy levelezőkliens, egy böngésző, egy üzenetküldő program, valamilyen média folyam, esetleg egy játék. Ezek az önállóan futó programok lehetnek példák az egyedi folyamatokra.

Egy weboldal megtekintése legalább egy hálózati folyamatot igényel. Egy hiperlinkre kattintáskor a böngésző egy kommunikációs folyamatot kezdeményez egy webszerver. A háttérben ugyanakkor egy levelezőkliens e-maileket küldhet és fogadhat, egy kolléga, vagy barát pedig chat-elhet.

Vegyünk egy olyan számítógépet, aminek csak egy hálózati interfésze van. A PC-n futó valamennyi alkalmazás adatfolyama ezen az egy interfészen keresztül lép be és távozik, ám a chat üzenetek mégsem jelennek meg az éppen szerkesztett dokumentum közepén és az e-mailek sem jelennek meg a játék felületén.

Ez azért van így, mert a forrás- és célállomásokon lévő egyes folyamatok egymással kommunikálnak. Minden alkalmazást, vagy folyamatot egy 4. rétegbeli portszám jelöl. Az egyedi párbeszédeket az egymással kommunikáló alkalmazások 4. rétegbeli forrás- és cél portszám párosa azonosítja. Adatok beérkezésekor megvizsgálják a portszámot, hogy az adatok céljául szolgáló alkalmazást vagy folyamatot kiválaszthassák.

A TNG Media Lab által készített "A hálózat harcosai" ("Warriors of the Net") című animációs film egy a hálózati fogalmak megértését segítő, szórakoztató segédlet. Mielőtt megnéznénk, érdemes előtte megfontolni egy pár dolgot. Először is a fejezetben tanult fogalmakat szem előtt tartva vegyük észre a

videót nézve, hogy mikor vagyunk a LAN-on, a WAN-on, az intraneten, vagy az interneten, és hogy mik a végberendezések illetve a közvetítő eszközök, hogy hogyan alkalmazzál az OSI és a TCP/IP-modelleket, és mely protokollok szerepelnek a filmben.

Másodsorban, míg a 21-es, 23-as, 25-ös, 53 és 80-as portszámokat a videó konkrétan említi, addig az IP-címekre csak utal. Észrevesszük hogy hol? Hol szerepelnek a videóban a MAC-címek?

Végül pedig, bár az animációk gyakran egyszerűsítenek, van benne egy leplezetlen hiba. Körülbelül az 5. percnél a következőt állítja: "Mi történik, amikor Mr. IP nem kap visszajelzést arról, hogy a csomag időben megérkezett? Egyszerűen küld egy másik csomagot helyette". Ez nem a 3. rétegbeli IP-protokoll feladata, amely egy "nem megbízható", legjobb szándékú (best effort) kézbesítést végző protokoll, hanem inkább a szállítási rétegbeli TCP-protokoll funkciója.

Töltsük le a videót a http://www.warriorsofthe.netweboldalról.

Tegyük meg!

Tekintsünk vissza a fejezet elején lévő modellezési feladatra, amely ennek feladatnak is az alapját képezi! IP-telefonjainkat a várt egy hét helyett már fél nap alatt felszerelték. A hálózatot teljes mértékben helyreállították és a hálózati alkalmazások is készen állnak a használatra. Ugyanazokat az e-maileket kell megválaszolnunk és ugyanazokat az árajánlatokat kell megírnunk vezetői jóváhagyásra.

Használjuk a bevezető modellezési feladatban elvégzett forgatókönyvet a következő kérdések megválaszolásához:

A. E-mailek

- Milyen módszert vagy módszereket tudnák használni az e-mailek küldésére most, hogy a hálózat már működik?
- Milyen formátumban lesznek elküldve e-mailjeink a hálózaton?
- Hogyan tudnánk ugyanazt az üzenetet több címzettnek is elküldeni?
- Hogyan tudnánk a hálózati alkalmazásokat felhasználva nagyméretű csatolmányokat több címzettnek is elküldeni?
- Bebizonyosodhat-e, hogy a hálózati alkalmazások használata költséghatékony kommunikációs módszer a vállalatunk számára?

B. Vezetői jóváhagyásra váró árajánlat

- Így, hogy számítógépünkre egy irodai alkalmazásokból álló szoftvercsomag lett telepítve, egyszerű lesz-e elkészítenünk azt az árajánlatot, amelyre vezetőnknek egy a hét végén esedékes új szerződéshez van szüksége? Magyarázzuk meg a választ!
- Miután végeztünk az árajánlat megírásával, hogyan fogjuk azt jóváhagyásra bemutatni a vezetőnknek? Ő vajon hogyan fogja majd az árajánlatot továbbküldeni elfogadásra az ügyfélnek?
- Költséghatékony-e az üzleti tranzakciók végrehajtásához a hálózati alkalmazások használata? Indokoljuk a választ!

Készítsünk nyomtatott vagy elektronikus másolatot válaszainkról! Készüljünk fel rá, hogy válaszainkat az osztályban is megvitassuk!

Modellezési feladat - Make it happen! Instructions

A Packet Tracer Multiuser eszköze pont-pont kapcsolatok kialakítását teszi lehetővé a Packet Tracer példányai között. Ez az első Packet Tracer Multiuser (PTMU) feladat egy gyors bemutató annak demonstrálására, hogy milyen lépésekben lehet a Packet Tracer egyazon LAN-on belüli két példánya között multiuser kapcsolatot létrehozni és ellenőrizni. Ideális esetben ez két tanulónak szánt feladat. Végrehajtható ugyanakkor egyéni feladatként is, amennyiben a két fájlt a helyi gépen egyszerűen a Packet Tracer két külön példányaként nyitjuk meg.

Packet Tracer Multiuser - Tutorial Instructions

Packet Tracer Multiuser - Tutorial - Client Side - PKA

Packet Tracer Multiuser - Tutorial - Server Side - PKA

Az alkalmazási réteg feladata az emberi kommunikációt felügyelő és továbbító háttérfolyamatok közvetlen elérése. Ez a réteg egyben a hálózati kommunikáció forrása és célja is. Az alkalmazási rétegbeli alkalmazások, szolgáltatások és protokollok biztosítják a felhasználók és az adathálózat ésszerű és hatékony kapcsolatát.

- Az alkalmazások azok a számítógépes programok, amelyekkel a felhasználó kapcsolatban áll, és amelyek a felhasználó kérésére az adatátviteli folyamatot kezdeményezik.

- A szolgáltatások olyan háttérprogramok, amelyek az alkalmazási réteg és a hálózati modell alsóbb rétegei között biztosítanak összeköttetést.

- A protokollok megállapodáson alapuló szabályoknak és folyamatoknak egy olyan struktúráját biztosítják, amely lehetővé teszi, hogy egy adott eszköz szolgáltatásai képesek legyenek különböző hálózati eszközöktől adatokat fogadni és azokra adatokat küldeni.

Az adatok hálózaton keresztüli átvitelét kérheti egy kliens egy szervertől, vagy történhet P2P elrendezésben működő eszközök között, ahol a kliens-szerver kapcsolat aszerint alakul, hogy az adott esetben melyik eszköz a forrás, illetve a cél. A kommunikáló eszközök alkalmazási rétegbeli szolgáltatásai közötti üzenetváltás ezeket a kapcsolatokat kialakító és használó protokoll előírásainak megfelelően történik.

Protokollok - mint például a HTTP - teszik lehetővé a weboldalak végberendezésekhez való eljutását. Az SMTP és a POP az e-mailek küldését és fogadását biztosítják. Az SMB és az FTP lehetővé teszik, hogy a felhasználók fájlokat osszanak meg. A P2P alkalmazások különböző médiatartalmak megosztását könnyítik meg a felhasználóknak. A DNS az emberek számára könnyen értelmezhető neveket alakítja át a hálózat által is használható numerikus címekké. A felhők távoli feltöltési helyek, amelyek adatokat és alkalmazásokat tárolnak, így a felhasználók nem igényelnek annyi helyi erőforrást és különböző eszközökről és helyekről is gond nélkül férhetnek hozzá a különböző tartalmakhoz.

Mindezek az elemek együtt dolgoznak az alkalmazási rétegben. Az alkalmazási réteg teszi lehetővé, hogy a felhasználók dogozzanak és játszanak az Interneten.

A kurzus során eddig áttekintettük az adathálózatoknak a humán hálózatok számra nyújtott szolgáltatásit, megvizsgáltuk az OSI-modell egyes rétegeinek tulajdonságait és a TCP/IP-protokollok működését, valamint foglalkoztunk a legnépszerűbb LAN-technológiával, az Ethernettel. Ebben a fejezetben következő lépésként megtanuljuk, miként lehet ezekből az elemekből egy működő és fenntartható hálózatot létrehozni.

Emlékszünk még ...?

Megjegyzés: A tanulók egyedül, párban, vagy osztály szinten is megoldhatják ezt a feladatot.

Figyeljük meg a két hálózati ábrát. Hasonlítsuk össze a két hálózatot, és keressük meg a különbségeket. Készítsünk feliratot az eszközökhöz mindkét hálózatban. Ha a címkézés elkészült, már tudni fogjuk, milyen közvetítő és végberendezések találhatók az egyes hálózatokban.

Miben különbözik a két hálózat? Csak abban, hogy a B-ben több eszköz van, mint az A-ban?

Válasszuk ki, melyiket használnánk egy kis- vagy középvállalat tulajdonosaként! Indokoljuk meg választásunkat a következő szempontok alapján: költség, sebesség, csatlakozás, bővíthetőség, felügyelet!

Csoportos feladat - Did You Notice Instructions

Az üzleti világ jelentős része kisvállalkozás, így nem meglepő dolog, hogy a hálózatok többsége kis hálózat.

A kis hálózatok tervezése viszonylag egyszerű, mivel lényegesen kevesebb számú és típusú eszközt tartalmaznak, mint a nagyméretű hálózatok. A kis hálózati topológiák jellemzően egyetlen forgalomirányítóból és legfeljebb néhány kapcsolóból épülnek fel. Tartalmazhatnak még vezeték nélküli elérési pontokat (forgalomirányítóval egybeépítve is) és IP-telefonokat. Internet kapcsolatuk általában egyetlen WAN-csatlakozás, amely DSL, kábel vagy Ethernet szolgáltatáson keresztül valósul meg.

Egy kis hálózat felügyelete nagyon hasonló képességeket igényel, mint egy nagy hálózaté. A munka többségét a meglévő berendezések karbantartása és hibaelhárítása, valamint a hálózat- és információbiztonság megvalósítása jelenti. A kis hálózatok felügyeletét elláthatja a vállalat egy alkalmazottja vagy egy szerződéssel megbízott személy, függően a vállalat méretétől és típusától.

Az ábrán egy tipikus kisvállalati hálózat látható.

A felhasználói igények kielégítése érdekében a kis hálózatok megvalósítása is átgondolást és tervezést igényel, mely magában foglalja az összes követelményt, költségelemet és fejlesztési lehetőséget.

A tervezés egyik első lépése a közvetítő eszközök típusának kiválasztása, melynek szempontjai az ábrán láthatók.

Költség

A költség az egyik legfontosabb szempont a kis hálózatok berendezéseinek kiválasztásakor. A kapcsolók és forgalomirányítók árát teljesítményük és képességeik határozzák meg. A teljesítmény magában foglalja a portok számát, típusát és az eszköz belső sebességét. A költséget befolyásoló tényezők még a hálózatfelügyeleti képességek, a beépített biztonsági funkciók és a választható bővítési lehetőségek. Figyelembe kell venni még a hálózati eszközök csatlakoztatásához szükséges kábelezés költségét is. Külön költségvetési elem, hogy milyen mértékű redundancia kerüljön beépítésre a hálózatba, beleértve az eszközöket és azok portjait, a réz vagy optikai kábeleket.

Portsebesség és interfész típus

A kapcsolók és forgalomirányítók portszámának és típusának kiválasztása kritikus döntés. Az ilyenkor felmerülő kérdések: "Válasszunk a jelenlegi kívánalmaknak megfelelő portszámot, vagy vegyük figyelembe a növekedési követelményeket is?", "Szükségünk van különböző UTP sebességekre?", "Kellenek UTP és optikai portok is?"

Az új számítógépek 1 Gbps-os hálózati kártyával rendelkeznek, 10 Gbps porttal csak néhány munkaállomás és szerver van felszerelve. Bár drágább, de érdemes nagyobb sebesség fogadására alkalmas Layer 2 eszközöket választani, megelőzve ezzel a hálózat fejlesztése során a központi eszközök cseréjét.

Bővíthetőség

A hálózati eszközök moduláris és rögzített fizikai összeállításban is kaphatók. Fix konfiguráció esetén adott a portok vagy interfészek száma és típusa. A moduláris berendezések bővítőhelyekkel rendelkeznek, így új modulok hozzáadásával rugalmasan lehet követni az igényeket. A legtöbb ilyen berendezés alap beépített portokkal és további üres bővítőhelyekkel kerül forgalomba. Kapcsolók esetében speciális kiegészítő portok szolgálják a nagy sebességű gerinchálózathoz való csatlakozást (uplink portok). Továbbá, mivel a forgalomirányítók több különböző típusú hálózatot kötnek össze, külön figyelmet kell fordítani az adott média számára megfelelő modul kiválasztására. A megfontolandó kérdések: "Válasszunk cserélhető modulokkal rendelkező eszközt?", "Kellenek WAN-interfészek a forgalomirányítóba, és ha igen, milyen típusúak?"

Az operációs rendszer jellemzői és szolgáltatásai

Az operációs rendszer verziójától függően a hálózati eszközök a következő jellemzőkkel és szolgáltatásokkal rendelkeznek:

- Biztonság
- QoS
- VoIP
- Layer 3 kapcsolás
- NAT
- DHCP

A forgalomirányítók költségeit megnövelhetik a szükséges interfészek és szolgáltatások, valamint a kiegészítő modulok, például a optikai kártyák is tovább növelik a hálózati eszközök költségét.

Egy kis hálózat megvalósításához is szükséges IP-címzési terv. Egy hálózat állomásai számára egyedi címet kell biztosítani, és ezek kiosztása még egy kis hálózatban sem lehet véletlenszerű. A címzési séma tervezését, dokumentálását és karbantartását a megcímzett eszközök típusának figyelembevételével kell elvégezni.

Példa néhány eszköztípusra, mely hatással van az IP-címzési tervre:

- Felhasználói végberendezések
- Szerverek és perifériák
- Az internet felől elérhető állomások
- Közvetítő eszközök

Az IP-címzés tervezése és dokumentálása segíti a rendszergazdát az eszközök közötti eligazodásban. Például, ha az összes szerver az 50-100 közötti tartományból kap címet, akkor a forgalmuk könnyen azonosítható IP-cím alapján. Ez nagyon hasznos a hálózati forgalom problémáinak protokoll elemzővel történő hibaelhárítása során.

Továbbá egy jól meghatározott IP-címzési rendszer használata esetén a rendszergazdák hatékonyabban képesek a hálózati erőforrásokat felügyelni. Ez különösen fontos lehet azon állomások esetében, melyek a belső és a külső hálózatnak is nyújtanak szolgáltatásokat. Ebbe a körbe tartoznak például a web és az e-kereskedelem szerverei. Ha a hozzájuk rendelt IP-címek nem tervezettek és

nem dokumentáltak, akkor az eszközök biztonsága és hozzáférhetősége nehezen ellenőrizhető. Ha egy szerver véletlenszerűen kap címet, akkor a szerverhez történő hozzáférés letiltása nehezen megoldható valamint az adott erőforrás a kliensek számára könnyen elérhetetlenné válhat.

A fenti eszköztípusokhoz különálló logikai címblokkot kell rendelni a hálózati címtartományból.

Kattintsunk a gombokra a hozzárendelési módszer megtekintéséhez!

A hálózattervezés másik fontos eleme a megbízhatóság. A kisvállalkozások üzleti folyamatai számára gyakran elengedhetetlen a hálózat működése, és annak hibája jelentős veszteséget okozhat. A hálózat megtervezésekor a magas szintű megbízhatóság fenntartásához és az elsődleges meghibásodási pontok kiküszöböléséhez redundanciára van szükség. A hálózati redundancia megvalósításának többféle módja közül az egyik a berendezések másodpéldányainak telepítése, a másik a hálózati összeköttetések többszörözése, ahogy az ábrán is látható.

Minél kisebb a hálózat, annál kisebb az esély arra, hogy a berendezések duplikálása kifizetődő lesz. Ezért gyakori megoldás, hogy csak a kapcsoló-kapcsoló és a kapcsoló-forgalomirányító közötti összeköttetéseket kettőzik meg.

A szerverek körében is elterjedt a több porttal rendelkező hálózati kártya, mely támogatja a redundáns csatlakozást egy vagy több kapcsolóhoz. A kis hálózatokban rendszerint web, fájl és e-mail szerverek találhatók.

A kis hálózatoknak általában egy kijáratuk van az internet felé egy vagy több alapértelmezett átjárón keresztül. Az egyetlen forgalomirányítót tartalmazó topológiában redundancia csak a 3. rétegbeli útvonalak tekintetében valósítható meg, mégpedig a forgalomirányítón több belső oldali Ethernet interfész használatával. Ilyenkor a forgalomirányító meghibásodása a teljes hálózat internet kapcsolatának elvesztését eredményezi. Éppen ezért a kisvállalkozások számára is kifizetődő lehet egy olcsó másodlagos összeköttetés előfizetése (backup).

A felhasználók állandó hozzáférést igényelnek elektronikus leveleikhez és osztott használatú állományaikhoz. A cél elérése érdekében a hálózat tervezőjének a következő feladatai vannak:

1. A fájl és levelező szerverek biztonságos elhelyezése egy központi helyiségben.

2. A helyiség védelme a jogosulatlan belépéstől fizikai és logikai eszközökkel.

3. Szerver redundancia létrehozása, mely biztosítja egy eszköz meghibásodása esetén a fájlok sértetlenségét.

4. Tartalék összeköttetések biztosítása a szerverekhez.

A modern hálózatokat gyakran használják a vásárlók és az üzleti partnerek közötti IP-alapú hang- és videokommunikációra. Az ilyen típusú konvergens hálózat beépített vagy kiegészítő lehetőségként tartalmazza a nyers adatok IP-hálózatba ágyazását. A hálózati rendszergazdának a rendszer tervezésekor tekintetbe kell vennie a különféle forgalomtípusokat és azok kezelésének módját. A kis hálózatok forgalomirányítóit és kapcsolóit úgy kell konfigurálni, hogy a valós idejű forgalmat, mint például a hang- és a videó átvitelt az egyéb adatforgalomtól elválasztva kezeljék. Egy jó hálózati tervben a forgalom prioritás alapján kerül osztályozásra, ahogy ez az ábrán is látható. Jellegzetes forgalmi osztályok lehetnek:

- Fájlátvitel
- E-mail
- Hang

- Videó
- Üzenetküldés
- Üzleti

Egy jó hálózati terv végső célja, kis hálózatok esetén is, a munka hatékonyságának növelése és a kiesési idő minimalizálása.

Egy hálózat csak olyan mértékben hasznos, mint amennyire a rajta lévő alkalmazások. Az alkalmazási rétegben kétféle szoftver vagy folyamat van, ami hozzáférést biztosít a hálózathoz: a hálózati alkalmazások és az alkalmazási rétegbeli szolgáltatások (lásd ábra).

Hálózati alkalmazások

A hálózati alkalmazások olyan szoftverek, melyek alkalmasak a hálózaton keresztüli kommunikációra. Néhány felhasználói program hálózat-tudatos, ami azt jelenti, hogy a beléjük ágyazott alkalmazási rétegbeli protokollok képesek közvetlenül kommunikálni az alsóbb rétegbeli protokollokkal. Ilyen alkalmazások például az email kliensek és a böngészőprogramok.

Alkalmazási rétegbeli szolgáltatások

Más programoknak az alkalmazási réteg szolgáltatásai nyújtanak segítséget az olyan hálózati erőforrások használatához, mint a fájl átvitel vagy a hálózati nyomtatás. Noha a felhasználó számára a szolgáltatások láthatatlanok, mégis ezek a programok teremtenek kapcsolatot a hálózattal és készítik elő az adatokat az átvitelre. A különféle adattípusok, legyenek azok szöveg, grafika vagy videó, különféle szolgáltatásokat igényelnek, hogy megfelelően elő legyenek készítve az OSI-modell alsóbb rétegeiben való feldolgozásra.

Minden hálózati alkalmazás vagy szolgáltatás protokollokat használ, melyek szabályokat és adatformátumokat tartalmaznak. Protokollok nélkül a hálózat képtelen lenne az adatok kezelésére és továbbítására. A különféle hálózati szolgáltatások funkcióinak megértéséhez szükség van az őket irányító legfontosabb protokollokban való jártasságra.

Egy szakember legtöbb feladatában valamilyen módon megjelennek a hálózati protokollok, legyen szó akár egy kis, akár egy nagy hálózatról. Kis hálózat felhasználói által használt alkalmazásokat és szolgáltatásokat támogató leggyakoribb hálózati protokollok a következők:

- DNS
- Telnet
- IMAP, SMTP, POP (email)
- DHCP
- HTTP
- FTP

Az ábrán lévő szerverekre kattintva azok hálózati szolgáltatásainak rövid leírását jeleníthetjük meg.

Ezek a hálózati protokollok tartalmazzák a hálózati szakember számára szükséges alapvető segédeszközöket is. A hálózati protokollokban meghatározásra kerülnek:

- A kommunikációs viszony kezdetének és végének folyamatai

- Üzenettípusok
- Az üzenetek szintaxisa
- Az információs mezők jelentése
- Az üzenetküldés módja és az arra adott válasz
- Az alsóbb rétegekkel való kölcsönhatás

Sok szervezet házirendje megköveteli e protokollok biztonságos változatainak használatát, ilyenek például a HTTPS, SFTP, SSH.

Az előzőekben ismertetett protokollokon túl a mai cégek, még a kicsik is, gyakran használnak valósidejű alkalmazásokat az üzleti partnerekkel való kapcsolattartásra. Mivel a kisvállalkozások nem képesek a Cisco Telepresence megoldás finanszírozására, ezért olyan valósidejű alkalmazásokat választanak, melyek megfizethetők számukra, lásd 1. ábra. A valós idejű alkalmazások más adattípusokhoz képest több tervezést és magasabb szintű szolgáltatásokat igényelnek a hang és a videó forgalom megfelelő prioritással történő továbbításához. Ezért a hálózati rendszergazdának gondoskodni kell a megfelelő berendezések telepítéséről és konfigurálásáról. A 2. ábrán a kis hálózatok valósidejű alkalmazásaihoz szükséges eszközök láthatók.

Infrastruktúra

Az infrastruktúrának illeszkedni kell a jelenlegi és a tervezett valósidejű alkalmazások adatforgalmának jellemzőihez. A hálózat tervezőjének feladata annak eldöntése, hogy a meglévő kapcsolók és kábelezés képes-e a megnövekedett forgalom fogadására. Egy gigabites átvitelre képes hálózat megfelel ezen követelményeknek és nem szükséges az infrastruktúra módosítása. Ha a régi kapcsolók nem támogatják a PoE (Power over Ethernet, Etherneten keresztüli tápellátás) technológiát, vagy a kábelezés nem felel meg a sávszélesség követelményeknek, akkor mindkét esetben fejlesztés szükséges.

VoIP

A VoIP a hagyományos telefont használó szervezeteknél valósítható meg. A VoIP működéséhez hangtámogatással rendelkező forgalomirányítók szükségesek, melyek a hagyományos telefonvonal hangjeleit IP-csomagokká alakítják. A jelek IP-csomaggá alakítása után a forgalomirányító továbbítja azokat a megfelelő helyre. A VoIP lényegesen olcsóbb megoldás, mint egy integrált IP-telefon megvalósítás, de a kommunikáció minősége meg sem közelíti azt. A kisvállalatok számára is megvalósítható IP alapú hang- és videótovábbítás például a Skype vagy a Cisco WebEx alapváltozatának alkalmazásával.

IP-telefónia

IP-telefónia esetén maga a telefonkészülék végzi a hang átalakítását IP-csomaggá, ezért nincs szükség hangtámogatással rendelkező forgalomirányítóra. IP-telefonok esetében egy dedikált szerver végzi a hívások kezelését és felügyeletét. Ma már sok gyártó kínál IP-telefon megoldásokat kis hálózatok számára.

Valósidejű alkalmazások

Az adatfolyamok eredményes továbbításához a hálózatnak támogatni kell a késleltetésérzékeny alkalmazások követelményeit. Az RTP (Real-time Transport Protocol) és az RTCP (Real-time Transport Control Protocol) két olyan protokoll, mely megfelel az előbbi elvárásoknak. Az RTP és az RTCP azáltal képes a hálózati erőforrások vezérlésére és elosztására, hogy beépített QoS (Quality of Service) mechanizmusokkal rendelkezik. Ez a QoS-technika hatékony eszközöket biztosít a késleltetési hibák minimalizálására a valósidejű adattovábbítás során.

A növekedés a kisvállalkozások természetes folyamata, melyet hálózataiknak is követni kell. A kis hálózat rendszergazdája dolgozhat visszahatóan vagy előrehatóan, függően a vállalati vezetéstől, melynek gyakran ő is tagja. Ideális esetben a hálózati rendszergazdának elegendő ideje van a hálózat növekedésével kapcsolatos döntések meghozatalára, melyek illeszkednek a vállalat növekedési folyamatába.

A hálózat méretezéséhez szükséges elemek:

- **Hálózati dokumentáció** - fizikai és logikai topológia
- **Eszközleltár** - a hálózatot alkotó és használó berendezések listája
- **Költségvetés** - részletes IT-költségvetés, mely tartalmazza az üzleti év eszközbeszerzésre fordítandó kiadásait
- **Forgalom elemzés** - protokollok, alkalmazások és szolgáltatások, valamint a hozzájuk tartozó forgalmi követelmények

Ezek az információk szükségesek a kis hálózatok bővítésével kapcsolatos döntéshozatalban.

A kis hálózatok felügyelete és fejlesztése jártasságot kíván a protokollok és hálózati alkalmazások tekintetében. Ha egy kis hálózat rendszergazdája nem tud időt szakítani minden hálózati eszköz kihasználtságának külön megfigyelésére, akkor jelentős segítséget nyújthat neki egy szoftver vagy hardver alapú protokollelemző használata.

Mint az ábrán is látható, protokollelemző segítségével a hálózati szakember gyorsan össze tud állítani egy statisztikát a hálózati forgalomról.

A hálózati forgalom kezeléséhez, különösen bővülő hálózat esetén, nagyon fontos a forgalom típusának és mennyiségének ismerete. Ha a forgalom típusa ismeretlen, a protokollelemző segíthet az azonosításban és a forrás felkutatásában.

A hálózat forgalmi mintáinak meghatározása érdekében fontosak az alábbiak:

- A hálózat használatának csúcsidejében rögzítsük a csomagokat, így megfelelően jó mintát nyerhetünk a különböző típusú forgalmakból.
- Mivel bizonyos forgalomtípusok adott helyhez köthetőek, mindig vegyünk mintát több hálózati szegmensről is.

Ezután a begyűjtött adatok rendszerezhetők az üzenetek forrása, célja és típusa szerint is. Az elemzés alapján meghozhatók azok a döntések, melyekkel hatékonyabban felügyelhető a hálózati forgalom. Ilyen lehet például a szükségtelen forgalom csökkentése vagy az adatfolyam szerkezetének megváltoztatása egy szerver áthelyezésével.

Néha csupán egyetlen szerver vagy szolgáltatás áttelepítése egy másik hálózati szegmensbe, képes megnövelni a hálózat teljesítményét és elsimítani a megnövekedett forgalmi igényeket. Máskor azonban csak a hálózat újratervezésével vagy komolyabb beavatkozással lehet a hálózati teljesítményt optimalizálni.

A forgalmi trendek változásának megértésén túl a hálózati rendszergazdának tisztában kell lennie a hálózat használatával kapcsolatos változásokkal is. A kis hálózat rendszergazdájának feladata egy személyre szóló IT "pillanatfelvétel" elkészítése a dolgozók egy meghatározott csoportjának programfelhasználásról. Ez a pillanatfelvétel rendszerint a következőket tartalmazza:

- Operációs rendszer és annak verziója

- Lokális alkalmazások
- Hálózati alkalmazások
- CPU-használat
- Meghajtók használata
- Memória használat

A kis hálózat felhasználóiról rendszeresen készített pillanatfelvételek elemzése olyan információkhoz juttatja a hálózati rendszergazdát, melyek alapján teljesíthetők a protokoll és a hozzá kapcsolódó forgalom által támasztott követelmények. Tegyük fel, hogy néhány alkalmazott külső forrásokat, például közösségi oldalakat használ a vállalat marketing helyzetének javításához. Amikor ezek a dolgozók a vállalathoz kerültek, kevésbé foglalkoztak a internet alapú reklámozással. A hálózat felhasználói szokásainak megváltozása a rendszergazdától a hálózati erőforrások megfelelő átcsoportosítását igényli.

Ezért a hálózati rendszergazda feladata a hálózat kihasználtságának és az adatforgalom követelményeinek nyomon követése, valamint a termelékenység javítása és az üzlet növekedése érdekében a szükséges módosítások végrehajtása.

A vezetékes vagy vezeték nélküli számítógép hálózatok mindennapi életünk fontos kellékei. Mind a magánszemélyek, mind a szervezetek egyaránt függenek számítógépeiktől és hálózatuktól. Egy jogosulatlan személy behatolása költséges hálózati leállást és a munka elvesztését eredményezheti. Egy hálózat elleni támadás lehet végzetes, valamint a fontos információk és eszközök megrongálása vagy ellopása okozhat idő- és pénzveszteséget.

A behatolók hozzáférést szerezhetnek a hálózathoz a szoftver sebezhető pontjain keresztül, hardver elleni támadással vagy egy felhasználó nevének és jelszavának kitalálásával. Azt a behatolót, akik a szoftver módosításával vagy sebezhető pontjainak kihasználásával jut hálózati hozzáféréshez gyakran hacker-nek (hekker, számítógépkalóz) nevezik.

A hacker hozzáférése a hálózathoz négyféle fenyegetést jelenthet:

- Információlopás
- Azonosító lopás
- Adatvesztés és manipuláció
- Szolgáltatás megszakítása

Bővebb információért kattintsunk a képekre!

Kis hálózatok tervezése és megvalósítása során is szükség van a biztonsági fenyegetések és sebezhetőségek áttekintésére.

Amikor hálózati vagy számítógép biztonságról beszélünk, általában a szoftverek sebezhetőségét kihasználó támadóra gondolunk. Ugyanennyire fontos azonban az eszközök fizikai biztonsága is, hiszen egy támadó megakadályozhatja a hálózati erőforrások használatát, ha azokat fizikailag képes veszélyeztetni.

A fizikai fenyegetések négy formája:

- **Hardver fenyegetések** - szerverek, munkaállomások, forgalomirányítók, kapcsolók és a kábelezés fizikai megrongálása.

- **Környezeti fenyegetések** - szélsőséges hőmérséklet (túl meleg vagy hideg) vagy szélsőséges páratartalom (túl nedves vagy száraz)

- **Elektromos veszélyek** - feszültség tüskék, alacsony feszültségszint (feszültségesés), szűrés nélküli tápellátás (zaj), áramszünet

- **Karbantartási veszélyek** - az elektromos összetevők hanyag kezelése (elektrosztatikus feltöltődés), kritikus alkatrészek hiánya, hibás kábelezés és hiányos feliratozás

Ezen problémák egy részének szerepelni kell a vállalat házirendjében, más részük megoldása a szervezet vezetőségének hatáskörébe tartozik.

A három fontos hálózatbiztonsági tényező: sebezhetőség, fenyegetés és támadás.

A sebezhetőség a gyengeség fokmérője, mely minden hálózatban és eszközben eredendően benne rejlik, beleértve a forgalomirányítókat, kapcsolókat, szervereket, munkaállomásokat, és még a biztonsági eszközöket is.

Fenyegetésekbe beleszámítanak azok az emberek, akik érdekeltek és kellőképpen képzettek is a biztonsági sebezhetőségek kihasználására. Az ilyen személyek folyamatosan keresik az új lehetőségeket és gyengeségeket.

A fenyegetések különféle segédeszközök, szkriptek és programok formájában jelennek meg, melyek alkalmasak a hálózatok és a hálózati eszközök megtámadására. Ezek a hálózati eszközök általában végberendezések, például szerverek vagy asztali számítógépek.

A három elsődleges sebezhetőségi pont:

- Technológiai (lásd 1. ábra)

- Konfiguráció (lásd 2. ábra)

- Biztonsági házirend (lásd 3. ábra)

Mindhárom sebezhetőség vagy gyengeség különféle támadásokra ad lehetőséget, ilyenek például a rosszindulatú programok vagy a hálózati támadások.

A rosszindulatú kód támadások (malicious code attack) közé azokat a számítógép programokat soroljuk, melyeket adatvesztés vagy sérülés okozása céljából hoztak létre. Három fő típusuk a vírusok, a trójai lovak és a férgek.

A vírus egy rosszindulatú szoftver, mely más programokba ágyazva nemkívánatos hatást okoz egy munkaállomáson. Vírus például egy program, amely beágyazódik a command.com állományba (ez a Windows rendszerek elsődleges parancsértelmezője), letöröl bizonyos fájlokat és megfertőz minden más command.com állományt, amit talál.

A Trójai ló annyiban különbözik ettől, hogy az alkalmazás egészen másnak látszik, mint ami valójában, miközben igazából egy támadási eszköz. Trójai ló például egy olyan alkalmazás, mely egyszerű játékként fut a munkaállomáson. Miközben a felhasználót lefoglalja a játék, a trójai elküldi saját másolatát a felhasználói címjegyzékben szereplő összes címre. A címzettek megkapják és futtatják a játékot, ezáltal tovább terjesztik a Trójai lovat a saját címjegyzékükben szereplőknek.

A vírusoknak a víruskód más rendszerbe való átviteléhez egy továbbító mechanizmusra, például egy levélhez csatolt zip vagy exe fájlra van szükségük. A vírusok és férgek közötti alapvető különbség az, hogy a vírus továbbterjedéséhez emberi közreműködés szükséges.

A férgek önálló programok, melyek megtámadják a rendszert és megpróbálják kihasználni annak sebezhető pontjait. A sikeres támadás után a féreg átmásolja önmagát a megtámadott rendszerbe, és a folyamat kezdődik elölről. Egy féregtámadás anatómiája a következő:

- **A sebezhetőség** - A féreg feltelepíti magát a rendszer egy ismert gyenge pontját kihasználva, például amikor egy naiv felhasználó megnyit egy futtatható email csatolmányt.

- **Terjesztési mechanizmus** - Az állomáshoz való hozzáférés megszerzése után a féreg másolatot készít önmagáról, majd új célpontot választ.

- **Hasznosítás** - A megfertőzött állomáshoz a támadó gyakran olyan jogosultságot szerez, mellyel a helyi lehetőségeket kihasználva adminisztrátorrá válhat.

A rosszindulatú szoftver támadásokon kívül a hálózat áldozatul eshet különféle hálózati támadásoknak is. A hálózati támadások három fő kategóriába sorolhatók:

- **Felderítéses támadások** - a rendszerek, szolgáltatások és sebezhetőségek jogosulatlan feltérképezése

- **Hozzáférési támadások** - adatok, rendszerhozzáférések és felhasználói jogok illetéktelen kezelése

- **Szolgáltatásmegtagadás** - hálózatok, rendszerek és szolgáltatások megbénítása vagy elrontása

Felderítéses támadások

Egy külső támadó internetes eszközöket használva, például nslookup vagy whois segédprogramok segítségével könnyen megállapíthatja egy adott szervezet IP-címtartományát. Ezután a támadó a tartomány publikus IP-címeinek megpingelésével ki tudja választani az aktív állomásokat. Ez a feladat egy "ping sweep" (ping pásztázás) segédprogrammal, mint például az fping vagy a gping automatizálható is, hiszen ezek a programok szisztematikusan végigpingelik a összes címet egy adott tartományban vagy alhálózatban. Ez pont olyan, mint egy telefonkönyvben végighívni az összes számot azt figyelve, hogy melyiket veszik fel.

Kattintsunk az ábrán lévő felderítéses támadás eszközökre és figyeljük meg az animációt!

Hozzáférési támadások

A hozzáférési támadások a hitelesítési, FTP és web szolgáltatások ismert sebezhetőségi pontjait használják ki a bejelentkezési adatok, bizalmas információk megszerzéséhez. Ennek eredményeképpen a támadó személy jogosulatlan hozzáférés által jut hozzá számára titkos adatokhoz. A hozzáférési támadások négy csoportba oszthatók. Az egyik leggyakoribb támadástípus a jelszó elleni támadás, amely egy protokollelemző segítségével is végrehajtható, elfogva az egyszerű szövegként továbbított felhasználóneveket és jelszavakat. Szintén ide sorolhatók a megismételt bejelentkezési próbálkozások, melyek osztott erőforrások, például szerverek vagy forgalomirányítók felhasználónevének és jelszavának megszerzésére irányulnak. Az ismétléses támadásokat nevezik még szótár (dictionary) vagy nyers erő (brute-force) támadásoknak is.

Kattintsunk az ábrán lévő gombokra a hozzáférési támadások néhány példájának megtekintéséhez!

Szolgáltatás megtagadás

A DoS (Denial of Service, szolgáltatás megtagadás) támadás a legismertebb és a legnehezebben kiküszöbölhető támadásforma. Még a hekker társadalomban is jelentéktelennek és helytelennek számítanak a DoS-támadások, mivel csekély erőfeszítés árán végrehajthatók. Ugyanakkor pontosan a könnyű megvalósítás és a lehetséges jelentős károkozás miatt követelnek kiemelt figyelmet a biztonsági szakemberek részéről.

Sokféle DoS-támadás létezik, de végeredményként mindegyik a rendszer erőforrásainak felemésztésével akadályoz meg jogosult felhasználókat egy szolgáltatás használatában.

Kattintsunk az ábrán lévő gombokra a DoS és DDoS (Distributed DoS, szétosztott szolgáltatás megtagadás) támadások néhány példájának megtekintéséhez!

A vírusirtó szoftverek felismerik a legtöbb vírust és trójai lovat, és megakadályozzák szétterjedésüket a hálózatban. Működhetnek helyi felhasználói vagy hálózati szinten is.

A legutóbbi fejlesztések eredményeinek folyamatos alkalmazása eredményesebb védekezést tehet lehetővé ezen támadások ellen. Amint egy új vírus vagy trójai megjelenik, a vállalkozásoknak frissíteniük kell víruskereső szoftvereik adatbázisát.

A féreg támadások elhárítása is odafigyelést igényel a hálózati adminisztrációval foglalkozó személyzettől. A védekezés javasolt lépései:

- **Elszigetelés** - A féreg terjedésének megakadályozása a hálózatban a fertőzésmentes részek leválasztásával.
- **Immunizálás** - Hibajavító csomagok telepítése és sebezhetőségi pontok keresése a rendszerben.
- **Karantén** - A fertőzött gépek azonosítása, majd leválasztása vagy eltávolítása a hálózatból.
- **Mentesítés** - A fertőzött rendszerek tisztítása és javítása, mely néhány féreg esetében teljes újratelepítést igényel.

A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch). Ennek megvalósítása nehézkes az ellenőrzés nélküli felhasználói rendszereket tartalmazó helyi hálózatban. Nagyszámú rendszer felügyelete maga után vonja egy általános szoftvercsomag, vagy más néven "image" létrehozását (operációs rendszer és kliens alkalmazások), amely telepítéskor vagy frissítéskor használható. Amennyiben a biztonsági követelmények változnak, a már üzemelő rendszereken is szükség van a biztonsági frissítések telepítésére.

Az egyik megoldás a kritikus biztonsági javítócsomagok kezelésére egy központi elosztó szerver létrehozása, mellyel időközönként minden rendszernek kommunikálni kell (lásd ábra). Az állomásról hiányzó frissítések automatikusan letöltődnek a patch szerverről és felhasználói beavatkozás nélkül települnek.

A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, melyek a hálózati eszközök hozzáférés-szabályozásának alapját alkotják. Az AAA vezérli, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultság), és nyomon követi a használat során végrehajtott műveleteket (naplózás). Az AAA jobb méretezhetőséget biztosít, mint az önmagukban használt konzol, AUX, VTY és privilegizált EXEC hitelesítési parancsok.

Hitelesítés

A felhasználóknak és az adminisztrátoroknak igazolniuk kell, hogy azok, akiknek mondják magukat. Erre a hitelesítés nyújt lehetőséget felhasználónév és jelszó, ellenőrző kérdés és válasz, belépőkártya,

vagy más módszer segítségével. Például: "Én a 'diák' nevű felhasználó vagyok. Igazolni tudom ezt azzal, hogy ismerem a hozzá tartozó jelszót."

Kis hálózatban gyakran használt megoldás a helyi hitelesítés, melynek során minden eszköz saját adatbázisában tárolja a hozzá tartozó felhasználónév/jelszó kombinációkat. Sok felhasználó esetén azonban a lokális adatbázisok karbantartása meglehetősen összetett művelet, a hálózat és az eszközök számának növekedésével pedig a helyi hitelesítés fenntartása bonyolult és követhetetlen. Például, ha 100 hálózati eszközünk van, akkor az összes felhasználói fiókot hozzá kell adnunk mind a 100 eszközhöz.

Nagyobb hálózatok számára jobban méretezhető megoldás a külső hitelesítés, mely a felhasználói bejelentkezések ellenőrzését egy távoli szerveren végzi el. A felhasználók külső hitelesítésére használt két legnépszerűbb módszer a RADIUS és a TACACS+.

- A RADIUS egy kis CPU és memóriaigényű nyílt szabvány, melyet főleg hálózati eszközök, például kapcsolók, forgalomirányítók és vezeték nélküli berendezések esetében alkalmaznak.

- A TACACS+ hitelesítési, jogosultság kezelési és naplózási szolgáltatást nyújtó biztonsági megoldás, amely kiszolgálói alkalmazásként egy szerveren fut.

Jogosultság kezelés

A hitelesítést követően a jogosultságokat kezelő szolgáltatás megállapítja, hogy a felhasználó mely erőforrásokat érheti el és milyen műveleteket végezhet. Például: "A 'diák' nevű felhasználó csak Telnet-en kapcsolódhat az XYZ szerverhez."

Naplózás

A naplózó szolgáltatás feljegyzést készít a felhasználó minden cselekedetéről, beleértve, hogy mihez kapcsolódott, mennyi ideig használta az erőforrást és milyen módosításokat hajtott végre. A naplózás nyomon követi, hogy miként történt a hálózati erőforrások használata. Például: "A 'diák' nevű felhasználó Telnet-en kapcsolódott az XYZ szerverhez 15 percen keresztül."

Az AAA fogalom a bankkártya használathoz hasonlítható. A kártya meghatározza, hogy ki használhatja, mennyit költhetnek el róla, és lekönyveli a felhasznált összeg sorsát. (lásd ábra)

A hálózatra kapcsolt személyi számítógépek és szerverek védelmén kívül fontos a hálózatba érkező és onnan kimenő forgalom ellenőrzése is.

A tűzfal az egyik leghatékonyabb biztonsági eszköz, amely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is. A tűzfal termékek változatos technikákat használnak annak meghatározására, hogy mely forgalom számára legyen engedélyezve vagy tiltva a hálózathoz való hozzáférés. Ezek a módszerek a következők:

- **Csomagszűrés** - Tiltja vagy engedélyezi a hozzáférést IP-cím vagy MAC-cím alapján.

- **Alkalmazás szűrés** - Tiltja vagy engedélyezi a hozzáférést bizonyos alkalmazások számára portszámuk alapján.

- **URL-szűrés** - Tiltja vagy engedélyezi weboldalak elérését adott URL vagy kulcsszó alapján.

- **Állapot-alapú csomagszűrés (Stateful Packet Inspection, SPI)** - A bejövő csomagok csak a belső hálózat állomásairól kezdeményezett kérések válaszcsomagjai lehetnek. A nemkívánatos csomagok külön engedély hiányában kiszűrésre kerülnek. Az SPI képes arra is, hogy felismerjen és kiszűrjön bizonyos támadástípusokat, például a szolgáltatás megtagadást (DoS).

A tűzfalak egyidejűleg többféle szűrési módszert is támogathatnak, és gyakran hálózati címfordítást (Network Address Translation, NAT) is végeznek. A NAT a belső privát IP-címeket lecseréli egy külső publikus IP-címre, amellyel a csomagok továbbküldésre kerülnek a hálózaton. Ez egyben lehetővé teszi a belső címek külső felhasználók elől való elrejtését.

A tűzfalak különféle formában kerülnek forgalomba, amint az ábrán is látható.

- **Eszköz-alapú tűzfalak** - Az eszköz-alapú tűzfal olyan biztonsági berendezés, melybe a tűzfal célhardverként van beépítve.

- **Szerver-alapú tűzfalak** - A szerver-alapú tűzfal egy speciális alkalmazást tartalmaz, amely hálózati operációs rendszeren fut, például UNIX-on vagy Windows-on.

- **Integrált tűzfalak** - Az integrált tűzfal egy meglévő eszköz, például egy forgalomirányító tűzfalszolgáltatással kiegészítve.

- **Személyes tűzfalak** - Személyes tűzfal a munkaállomásokon található és nem a LAN védelmére tervezték. Képezheti az operációs rendszer részét vagy származhat külső gyártótól.
  - Egy hálózat pontosan annyira biztonságos, mint amennyire a legsebezhetőbb összeköttetése. Bár a médiában leggyakrabban szereplő veszélyek a kívülről érkező fenyegetések, mint például az internetes férgek vagy DoS-támadások, de legalább ilyen jelentőséggel bír a belső és köztes hálózatok biztonsága is. A belső hálózat végpontokból, más néven állomásokból áll, melyek hálózati kliensként működő számítógépek vagy eszközök (lásd ábra). Gyakori végpont típusok a laptopok, asztali számítógépek, szerverek, okostelefonok és tabletek. Ha a felhasználók nem rendelkeznek gyakorlattal saját eszközeik biztonságával kapcsolatban, akkor nincs olyan óvintézkedés, mely garantálná a hálózat biztonságát.
  - Az állomások biztonsága az egyik legnagyobb kihívás a hálózati rendszergazda munkájában, mivel itt az emberi tényezőt is számításba kell venni. A vállalatnak rendelkezni kell jól dokumentált szabályzattal és a munkavállalóknak be kell tartaniuk az abban leírtakat. Ezenkívül az alkalmazottakat fel kell készíteni a hálózat megfelelő használatára is. A házirend szabályok gyakran tartalmazzák a víruskereső és behatolás megelőző szoftverek használatának módját. A minden részletre kiterjedő állomásbiztonsági megoldások a hálózati hozzáférés vezérlésén alapulnak.
  - A végpontok biztonsága megköveteli a hálózati infrastruktúra 2. rétegbeli eszközeinek védelmét is az olyan támadások ellen, mint például a MAC-cím hamisítás (MAC address spoofing), a MAC-címtábla túlcsordulás (MAC address table overflow), és a hálózati vihar (LAN storm). Ezt hívjuk támadás megelőzésnek.

A hálózatbiztonságnak része a valódi eszközök, köztük a végberendezések és a hálózati eszközök védelme is.

Egy új operációs rendszer telepítése után az eszköz biztonsági beállításai az alapértelmezett értéket veszik fel, mely a védelem szempontjából nem megfelelő. Cisco forgalomirányítók esetében a Cisco AutoSecure szolgáltatás segít a rendszer biztonságossá tételében (lásd ábra). A beállítás néhány egyszerű lépésből áll, melyek alkalmazhatók a legtöbb operációs rendszer esetében:

- Az alapértelmezett felhasználóneveket és jelszavakat azonnal meg kell változtatni.

- A rendszer erőforrásaihoz való hozzáférést csak az erre jogosult személyek számára szabad engedélyezni.

- A szükségtelen szolgáltatásokat és alkalmazásokat lehetőség szerint ki kell kapcsolni vagy le kell törölni.

A biztonsági frissítéseket megjelenésük után azonnal telepíteni kell az összes eszközre. Mivel a gyártótól szállított berendezések hosszabb időt is tölthetnek raktárakban, így nincsenek naprakész állapotban. Fontos a beüzemelés során a szoftver és biztonsági frissítések telepítése.

A hálózati eszközök védelme érdekében fontos az erős jelszavak használata, melynek irányelvei a következők:

- Használjunk legalább 8, de inkább 10 vagy annál több karakterből álló jelszavakat. A hosszabb jelszó biztonságosabb.
- Készítsünk bonyolult jelszavakat. Legyenek bennük kis- és nagybetűk, számok, speciális karakterek és szóközök, minden, ami megengedett.
- A jelszavakban kerüljük az ismétlődéseket, gyakori szavakat, betű- vagy számsorozatokat, felhasználóneveket, rokonok vagy háziállatok neveit, életrajzi adatokat, mint például a születési dátumok, azonosító számok, elődök nevei, vagy bármely könnyen azonosítható információ.
- Írjuk szándékosan rosszul a jelszót. Például: Smith=Smyth=5mYth vagy Security=5ecur1ty.
- Cseréljük gyakran a jelszavakat. Így ha a jelszó mégiscsak kitudódik, a támadónak kevesebb ideje marad annak használatára.
- Ne hagyjuk a leírt jelszavakat látható helyen, például az asztalon vagy a monitoron.

Az ábrán példákat láthatunk erős és gyenge jelszavakra.

A Cisco forgalomirányítókon a vezető szóközök törlődnek a jelszavakból, de az első karakter után begépeltek megmaradnak. Éppen ezért erős jelszót kapunk, ha a szóköz billentyű segítségével több szóból álló kifejezést hozunk létre. A "password" mintájára ezt "pass pharse"-nek nevezik, és sokkal könnyebben megjegyezhető a jelszónál, ráadásul hosszabb és nehezebb megfejteni is.

A rendszergazdának gondoskodni kell arról, hogy a hálózatban erős jelszavak legyenek használatban. Ennek vizsgálatára használhatók például azok a segédprogramok, melyeket a hekkerek egy jelszó erősségének meghatározásához alkalmaznak a "nyers erő" (brute force) támadások során.

Egy eszköz telepítésekor nagyon fontos a szervezet által támasztott biztonsági előírások betartása. Ez vonatkozik az elnevezési konvencióra is, mely egyszerű dokumentálást és következetességet tesz lehetővé, de egyben a biztonságot is figyelembe veszi. Például nem helyes az állomásnévben az eszköz használatával kapcsolatosan túl sok információt megadni. Ezen kívül még számos alapvető biztonsági intézkedést kell megtenni.

További jelszóbiztonsági beállítások

Az erős jelszavak csak akkor hasznosak, ha titokban maradnak. A következő lépések segíthetik a jelszavak titokban tartását. A globális konfigurációs módban kiadott **service password-encryption** parancs megakadályozza a jogosulatlan személyeket abban, hogy megnézhessék a konfigurációs állományban lévő titkosítatlan jelszavakat (lásd ábra). A parancs titkosítja az összes kódolatlan jelszót.

A konfigurált jelszavak minimális hosszának biztosítására globális konfigurációs módban a **security passwords min-length** parancs használható.

Egy másik módja a jelszavak megfejtésének a brute-force támadás, melynek során a hekker addig próbálgatja a különböző jelszavakat, amíg rá nem talál a megfelelőre. Az ilyen típusú támadások megelőzhetők a bejelentkezés letiltásával, ha a sikertelen próbálkozások száma meghalad egy értéket egy adott időtartamon belül.

```
Router(config)# login block-for 120 attempts 3 within 60
```

A parancs letiltja a bejelentkezést 120 másodperc időtartamra, ha 3 sikertelen kísérletet érzékel 60 másodpercen belül.

Bejelentkezési üzenetek

A bejelentkezési üzenet hasonlatos a "Tilos az átjárás!" táblához. Ez fontos a hivatalos eljárás során, ha valakit a rendszer illetéktelen használatával vádolnak meg. A bejelentkezési üzenetnek illeszkedni kell a szervezet biztonsági rendszabályaihoz.

```
Router(config)# banner motd #message#
```

Időtúllépés

Ajánlott ezen felül a végrehajtási időtúllépés beállítása, melynek során megmondjuk a Cisco eszköznek, hogy egy adott tétlenségi idő lejárta után jelentkeztesse ki a felhasználót. Időtúllépés konfigurálható a konzol, VTY és AUX portokra.

```
Router(config)# line vty 0 4

Router(config-vty)# exec-timeout 10
```

A parancs 10 perc tétlenség után kijelentkezteti a felhasználót .

Távoli elérés SSH-n keresztül

Az eszközök távolról történő kezelésének hagyományos protokollja a Telnet, mely nem biztonságos. A Telnet csomagokban lévő adatok titkosítás nélkül kerülnek átvitelre. Ezért a Wireshark vagy egy hozzá hasonló segédprogram használatával elfogható a Telnet párbeszéd és a jelszó megszerezhető. Éppen ezért a biztonságos távoli eléréshez nagyon ajánlott az SSH engedélyezése az eszközön . Az SSH támogatás Cisco eszközön való konfigurálásának négy lépése, mely az ábrán is látható, a következő:

1. Győződjünk meg a forgalomirányító állomásnevének egyediségéről, majd állítsuk be a hálózat IP-tartománynevét. Erre szolgál az **ip domain-name***domain-name* parancs globális konfigurációs módban.

2. Szimmetrikus titkosító kulcspárt kell létrehozni a forgalomirányító SSH-folyamatának elindításához, az adatok kódolásához és dekódolásához. A kulcsgeneráláshoz globális konfigurációs módban a**crypto key generate rsa general-keys modulus** *modulus-size* parancs használható. A parancs egyes részeinek pontos jelentése összetett és túlmutat a kurzus keretein, így csak annyit jegyezzünk meg, hogy a modulus nagysága határozza meg a kulcs hosszát és értéke 360 és 2048 között lehet. A nagyobb modulus biztonságosabb kulcsot generál, de ekkor a titkosítási folyamat is több időt vesz igénybe. Az ajánlott minimális modulus hossz 1024 bit.

```
Router(config)# crypto key generate rsa general-keys modulus 1024
```

3. Hozzunk létre helyi felhasználót. Erre szolgál a**username** *"felhasználónév"* **secret** *"jelszó"*globális konfigurációs parancs.

4. Engedélyezzük vty vonali konfigurációs módban a bejövő SSH kapcsolódást a következő parancsokkal:**login local** és **transport input ssh**.

Ezután a forgalomirányító SSH szolgáltatása elérhető bármely SSH kliens alkalmazással.

A hálózat kiépítését követően a rendszergazda feladata a hálózati kapcsolatok megfelelő működésének ellenőrzése, továbbá a hálózati dokumentáció elkészítése.

A `ping` parancs

A **`ping`** parancs egy hatékony módja a kapcsolatok ellenőrzésének. Alkalmas a protokollkészlet vizsgálatára is, mivel a **`ping`** parancs működése a 3. rétegen túl az OSI-modell 2. és 1. rétegére is épül. A ping az ICMP-protokollt használja a kapcsolatok ellenőrzésére.

A **`ping`** parancs nem minden esetben tárja fel a probléma természetét, de segít a hibaforrás azonosításában. Ez egy nagyon fontos kezdeti lépés a hálózati hibaelhárításban.

A **`ping`** parancs nemcsak a protokollkészlet és az IP-konfiguráció ellenőrzésére, hanem a helyi és távoli állomásokkal való kapcsolat tesztelésére is alkalmas, amint az ábrán is látható. Léteznek olyan segédeszközök is, amelyek több információt szolgáltatnak, mint a **`ping`**parancs. Ilyen például a későbbiekben részletesen tárgyalásra kerülő Telnet és Trace.

Az IOS ping jelei

Az IOS parancssorában kiadott ping az általa küldött ICMP-üzenetekre kapott válaszokat különféle módon jelzi. A leggyakoribbak a következők:

- **!** - egy ICMP visszhang válasz (ICMP echo reply) megérkezését jelzi
- **.** - jelzi, hogy az ICMP visszhang (ICMP echo) üzenetre nem érkezett válasz a lejárati időn belül
- **U** - egy ICMP elérhetetlen (ICMP unreachable) üzentet érkezését jelzi

A "**!**" (felkiáltójel) azt jelenti, hogy a ping sikeresen befejeződött és a 3. rétegbeli kapcsolatok működnek.

A "**.**" (pont) azt jelenti, hogy hiba történt a kommunikáció során. Ez lehet kapcsolati probléma valahol az útvonalban, vagy jelezheti, hogy egy közbülső forgalomirányító nem talált útvonalat a cél felé és nem küldött "A cél nem érhető el" (ICMP destination unrechable) üzenetet. Továbbá mutathatja azt is, hogy a ping blokkolásra került egy eszköz biztonsági beállítása miatt.

Az "**U**" jelzi, hogy az útvonalon egy közbülső forgalomirányító nem rendelkezik elérési úttal a célcím felé, vagy a ping válasz blokkolásra került és feleletképpen egy ICMP unreachable üzenet érkezett.

A visszacsatolási cím (loopback) tesztelése

A **`ping`** parancs egy állomás belső IP-konfigurációjának ellenőrzésére is alkalmas. Emlékezzünk vissza, hogy ennek végrehajtásához a **`ping`** parancs mögé egy fenntartott, loopback címet írtunk (127.0.0.1). Ez a parancs leellenőrzi a protokollkészlet működését a hálózati rétegtől a fizikai rétegig és vissza, de nem küld jeleket a kommunikációs közegbe.

`Ping` utasításokat a parancssorban hajthatunk végre.

Gépeljük be a **`ping loopback`** parancsot a következő szintaxissal:

```
C:\> ping 127.0.0.1
```

A kapott válasz az alábbiakhoz hasonlóan fog kinézni:

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

```
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Az eredmény azt jelzi, hogy négy 32 bájtos teszt csomag került kiküldésre és a válaszok kevesebb, mint 1 ms alatt megérkeztek a 127.0.0.1 állomástól. A TTL (Time-To-Live, élettartam) érték azt határozza meg, hogy a ping csomag hány ugrás után kerül eldobásra.

A Cisco IOS ping parancsa rendelkezik egy "kiterjesztett" móddal is, mely az utasítás IP-cím nélküli beírásával érhető el. Ekkor az alább példában látható paraméter-bekérő üzenetek jelennek meg. Az Enter billentyű leütésének hatására a []-ben lévő alapértelmezett értékek kerülnek elfogadásra. A példa azt mutatja be, hogyan kényszeríthető a ping parancs a 10.1.1.1 forráscím használatára (lásd az ábrán R2-t); bár normál ping esetén a forráscím 209.165.200.226 lenne. Ezáltal a hálózati rendszergazda távolról (R2-ről) is ellenőrizni tudja, hogy az R1 irányítótáblájában van-e bejegyzés a 10.1.1.0/24 hálózat felé.

R2# **ping**

Protocol [ip]:

Target IP address: **192.168.10.1**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **10.1.1.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

Hosszabb időtúllépési (Timeout) periódus megadása lehetőséget ad a késleltetési hibák felderítésére. Ha a nagyobb értékkel sikeres a ping, akkor a kapcsolat él az állomással, de valamilyen késleltetési probléma van a hálózatban.

Figyeljük meg, hogy az "Extended commands" (Kiterjesztett utasítások) paraméternél beírt "y" további hasznos hibaelhárítási lehetőségeket nyit meg.

Az egyik leghatékonyabb eszköz a teljesítmény figyelésére és a hibaelhárításra a hálózat alapállapotának, más néven viszonyítási alapjának meghatározása. Az alapállapot meghatározásához a hálózat normál működés közbeni rendszeres vizsgálata szükséges. Ez több, mint egy szimpla beszámoló a hálózat adott időpontra vonatkozó állapotáról, mivel elkészítéséhez a teljesítmény hosszabb ideig történő megfigyelése szükséges. A különböző időpontokban történő mérések (lásd 1. és 2. ábra) segítenek teljesebb képet alkotni a hálózat összteljesítményéről.

A hálózat viszonyítási alapjához különféle parancsok kimenetei szolgáltatják az adatokat.

Az állapotfelmérés kezdőlépése lehet a ping, a trace és egyéb fontos parancsok eredményeinek elmentése egy időbélyeggel ellátott szövegállományba a későbbi visszakereshetőség céljából.

A tárolt információk tényleges használatára az aktuális eredményekkel való összehasonlításkor kerül sor (lásd 3. ábra). Figyelni kell a hibaüzeneteket és az állomások közötti válaszidőket, melyek növekedése késleltetési problémát jelenthet a címzett felé.

A dokumentáció elkészítésének fontosságát nem lehet elégszer hangsúlyozni. A végponttól végpontig tartó kapcsolatok ellenőrzésének adatai, a késleltetési hibák leírása, és az azonosított problémák megoldásai segíthetik a rendszergazdát a hálózat hatékony működtetésében.

A vállalati hálózatok fenntartásához széleskörű állapotfelmérés szükséges, sokkal bővebb, mint a jelen kurzusban leírtak. A viszonyítási információk kezelésére és tárolásához különféle professzionális alkalmazások állnak rendelkezésre. A kurzus keretében azonban csak az alapvető eljárásokat érintjük és a célokat tárgyaljuk meg.

A viszonyítási alap elkészítésének bevált gyakorlatait megtaláljuk itt.

A **`ping`** utasítás kimenetének rögzítése megvalósítható a 4. ábrán bemutatott módon, az IOS parancssorából is.

A nyomkövetés (trace) eredménye azon ugrások listája, melyek a csomagtovábbítás során a hálózati útvonalon történnek. A parancs formája az alkalmazott rendszertől függ. Windows számítógép esetében a **`tracert`**, míg egy forgalomirányító CLI esetén a **`traceroute`** parancs használható (lásd 1. ábra).

Hasonlóan a **`ping`** parancsokhoz, a **`trace`** utasítások is parancssorból használhatók és egy IP-címet használnak paraméterként.

Windows számítógépen használjuk a **`tracert`**parancsot az alábbiak szerint:

```
C:\> tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops

1 2 ms 2 ms 2 ms 10.0.0.254
```

```
2 * * * Request timed out.

3 * * * Request timed out.

4 ^C
```

Sikeres válasz csak a Router A helyi hálózat felőli kijáratától érkezett, míg a következő ugrás követése időtúllépéssel zárult. Ez azt jelenti, hogy a következő ugrásnál lévő forgalomirányító nem válaszolt. A nyomkövetés eredménye azt mutatja, hogy a hiba valahol a LAN-on kívül, a külső hálózatban van.

A 2. ábrán a forgalomirányítón kiadott traceroute parancs eredményének rögzítése látható.

A Cisco IOS parancssori felülete a **show** parancsokat használja az eszközök konfigurációjával és működésével kapcsolatos információk megjelenítésére.

A hálózati szakemberek gyakran használják a **show**parancsokat a konfigurációs fájlok megtekintéséhez, az eszközök interfészeinek és folyamatainak állapotellenőrzéséhez és a berendezés működőképességének vizsgálatához. A **show** parancsok az eszköz parancssorában vagy a Cisco Configuration Professional (CCP) segédprogramból érhetők el.

Szinte minden forgalomirányító folyamat és funkció állapotának megjelenítésére létezik **show** parancs. A leggyakrabban használt show parancsok közül néhány:

- **show running-config** (1. ábra)
- **show interfaces** (2. ábra)
- **show arp** (3. ábra)
- **show ip route** (4. ábra)
- **show protocols** (5. ábra)
- **show version** (6. ábra)

Az ábrán lévő gombokra kattintva részletes leírásukkal együtt jelennek meg a **show** parancsok.

Az indító konfigurációs fájl betöltése és a forgalomirányító sikeres elindulása után a **show version** parancs használható az indításnál szerepet játszó hardver- és szoftverkomponensek ellenőrzésére és az esetleges hibák megkeresésére. A **show version** parancs kimenete a következőket tartalmazza:

- A használatban lévő Cisco IOS szoftver verziója.
- A ROM-ban tárolt, a forgalomirányító indításához használt rendszerbetöltő program verziója.
- A Cisco IOS szoftver teljes fájlneve, valamint a háttértár neve, ahol a rendszerindító program azt megtalálta.
- A forgalomirányítóban lévő CPU típusa és RAM mennyisége. A Cisco IOS szoftver frissítésekor szükség lehet a RAM mennyiségének bővítésére.
- A forgalomirányító fizikai interfészeinek száma és típusa.

- Az NVRAM mennyisége. Az NVRAM tárolja az indító konfigurációs fájlt (startup-config).
- A forgalomirányító flash memóriájának mérete. A Cisco IOS szoftver frissítésekor szükség lehet a flash memória bővítésére.
- A konfigurációs regiszter aktuális értéke hexadecimálisan.

Az ábrán lévő lejátszás gombra kattintva egy animációt láthatunk, amely bemutatja a felsorolt elemeket a show parancs kimenetében.

A konfigurációs regiszter határozza meg a forgalomirányító számára az indítási folyamat módját . Például, a konfigurációs regiszter gyári alapértelmezett értéke 0x2102. Ez azt jelenti, hogy a forgalomirányító a Cisco IOS szoftvert a flash-ből, az indító konfigurációs fájlt pedig az NVRAM-ból próbálja betölteni. A konfigurációs regiszter értéke megváltoztatható, ezáltal az indítási folyamat során a forgalomirányító máshol fogja keresni a Cisco IOS kódot, valamint az indító konfigurációs fájlt. Amennyiben egy második érték jelenik meg zárójelben, az a forgalomirányító következő újraindításakor érvénybe lépő konfigurációs regiszter értékét mutatja.

A konfigurációs regiszterről további információt a jobb alsó sarokban lévő "Jegyzet" ikonra kattintva találunk.

A **`show version`** parancs információkat jelenít meg a kapcsolón aktuálisan betöltött szoftver verziójáról, valamint az eszköz hardver összetevőiről. Néhány ezek közül:

- **Cisco IOS Software** - Az IOS-szoftver verziója
- **ROM: Boot Loader** - A rendszerbetöltő program verziója
- **Switch uptime** - Az utolsó újraindulás óta eltelt idő
- **System returned to ROM** - Az újraindulás módja (pl.: áramkimaradás, rendszerösszeomlás)
- **System image file** - Az IOS-képfájl neve
- **Cisco "switch type" processor** - A készülék modell száma és a beépített processzor típusa
- **"main/shared" bytes of memory** - Alap processzor RAM és osztott I/O puffer memória mennyisége
- **Interfaces** - A kapcsolóban rendelkezésre álló interfészek
- **Configuration register** - Rendszertöltési beállítások, konzol sebesség, és ezek paraméterei

Az ábrán egy kapcsolón kiadott **`show version`** parancs kimenete látható.

Egy állomáson az alapértelmezett átjáró IP-címének lekérdezésére egy Windows-t futtató számítógép parancssorában az **`ipconfig`** utasítás használható. (lásd 1. ábra)

A MAC-cím megjelenítéséhez gépeljük be: **`ipconfig /all`**. Figyeljük meg a 2. ábrán, hogy a MAC-címen kívül kijelzésre került a számítógép néhány további 3. rétegbeli címinformációja is. Próbáljuk ki ezt a parancsot.

Ezen felül a MAC-cím alkalmas a számítógépben lévő hálózati kártya gyártójának azonosítására is. Erre a cím első 24 bitje (OUI) ad módot, mely visszakereshető az interneten.

A Windows PC DNS-kliens szolgáltatása a memóriában tárolja a korábban már meghatározott neveket és ezáltal javítja a névfeloldás teljesítményét. Az **ipconfig /displaydns** parancs megmutatja a rendszer DNS-gyorsítótárának bejegyzéseit.

Az **arp** parancs segítségével létrehozhatók, módosíthatók és megjeleníthetők a fizikai cím - IP-cím összerendelések. Az **arp** utasítás a Windows parancssorában futtatható.

Az **arp** végrehajtásához az állomás parancssorába gépeljük be:

```
C:\host1> arp -a
```

Amint az ábrán is látható, az **arp -a** parancs felsorolja az összes ARP-gyorsítótárban lévő eszközt, beleértve azok IPv4-címét, fizikai címét és a cím típusát (statikus/dinamikus).

A gyorsítótár az **arp -d** paranccsal törölhető, ha a hálózati rendszergazda szeretné friss információkkal újratölteni azt.

Megjegyzés: Az ARP-gyorsítótár csak azoknak az eszközöknek az információit tartalmazza, melyekhez mostanában történt hozzáférés. A cache feltöltéséhez pingeljük meg a kívánt eszközt, így biztosan lesz bejegyzés hozzá az ARP táblában.

Figyeljük meg a **show cdp neighbors** parancs kimenetét a 1. ábrán és vessük össze a 2. ábrán látható topológiával. Figyeljük meg, hogy az R3 milyen részletes információkat gyűjtött be az R2-ről és a FastEthernet interfészére csatlakoztatott kapcsolóról.

A CDP a Cisco saját protokollja, mely az adatkapcsolati rétegben működik. Ebből kifolyólag az egymással összekötött Cisco eszközök, például a különböző hálózati protokollt használó forgalomirányítók, képesek felismerni szomszédaikat még akkor is, ha 3. rétegbeli kapcsolat nincs is közöttük.

Egy Cisco eszköz elindulása után a CDP automatikusan betöltődik és felderíti a CDP-t futtató szomszédos Cisco berendezéseket, függetlenül attól, hogy milyen 3. rétegbeli protokoll vagy programcsomag fut rajtuk. A CDP hardverre és szoftverre vonatkozó adatokat cseré a közvetlenül csatlakozó szomszédok között.

A CDP által szolgáltatott információk:

- **Device ID** - Eszköz azonosítók, például a kapcsolón beállított állomásnév
- **Entry address(es)** - Hálózati rétegbeli cím, minden támogatott protokollhoz legfeljebb egy.
- **Local interface, Port ID** - A helyi és a távoli portok nevei ASCII formátumban, például Serial0/0/1
- **Capability** - Szolgáltatás lista, például, hogy a kapcsolódó eszköz forgalomirányító (R) vagy kapcsoló (S)
- **Platform** - Az eszköz hardver típusa, például Cisco 1841 sorozatú forgalomirányító

A **show cdp neighbors detail** parancs megmutatja a szomszéd eszköz IP-címét, még akkor is, ha pingelni sem tudjuk. Ez nagyon hasznos parancs, amikor két Cisco forgalomirányító nem talál egymásra a közös adatkapcsolaton. A **show cdp neighbors detail**parancs segítségével megállapítható a szomszédok IP-konfigurációs hibái.

Hálózatfelderítés esetén a CDP-szomszéd IP-címének ismerete elégséges információ az eszközbe való Telnet bejelentkezéshez.

Érthető okokból a CDP biztonsági kockázatot jelenthet. Mivel néhány IOS verzió alapértelmezett beállítása a CDP-hirdetések küldése, így fontos tudni a CDP kikapcsolásának módjait.

A CDP egész eszközre kiterjedő tiltásához használható globális konfigurációs parancs a **`no cdp run`**. A CDP egy adott interfészen történő tiltására a **`no cdp enable`**parancs szolgál.

Hasonlóan az állomások konfigurációjának vizsgálatához, a közvetítő eszközök interfészeinek ellenőrzéséhez is rendelkezésre állnak utasítások és segédprogramok. A Cisco IOS-ben számos parancs szolgál a forgalomirányító és a kapcsoló interfészeinek ellenőrzésére.

A forgalomirányító interfészeinek ellenőrzése

Az egyik leggyakrabban használt parancs a **`show ip interface brief`** . Ez az utasítás sokkal tömörebb kimenetet ad, mint a **`show ip interface`** parancs. Összegezve mutatja a forgalomirányító hálózati interfészeinek kulcsfontosságú információit.

Az 1. ábrán a példában használt hálózati topológia látható.

Kattintsunk a 2. ábrán lévő R1 gombra! A **`show ip interface brief`** kimenete felsorolja a forgalomirányító interfészeit, a hozzájuk rendelt IP-címet és a működési állapotukat.

Ennek alapján a FastEthernet 0/0 interfész IP-címe 192.168.254.254. Az utolsó két oszlop az interfész 1. és 2. rétegbeli állapotát mutatja. Az **`up`** a Status oszlopban azt jelzi, hogy az interfész 1. rétegbeli működése rendben van. Az **`up`** a Protocol oszlopban pedig azt mutatja, hogy a 2. rétegbeli protokoll is működik.

Ezenkívül figyeljük meg, hogy a Serial 0/0/1 interfész nincs engedélyezve. Ezt jelzi az **`administratively down`** bejegyzés a Status oszlopban.

A végberendezésekhez hasonlóan, a 3. rétegbeli kapcsolatok ellenőrzéséhez itt is használhatók a **`ping`**és **`traceroute`** parancsok. A példában mind a **`ping`** , mind a **`trace`** parancsok sikeres kapcsolódást mutatnak.

A kapcsoló interfészeinek ellenőrzése

Kattintsunk a 2. ábrán lévő S1 gombra! A **`show ip interface brief`** parancs a kapcsoló interfészeinek állapotáról ad jelentést. Kapcsoló esetében az IP-cím egy VLAN-interfészhez van hozzárendelve. Jelen esetben a VLAN1 címe 192.168.254.250, az interfész engedélyezett és működőképes.

A kimenetből az is látszik, hogy a FastEthernet0/1 interfész nem működik. Ez azt jelenti, hogy nincs hozzá eszköz csatlakoztatva, vagy a kapcsolódó eszköz hálózati interfésze nem működőképes.

Ezzel ellentétben a kimenet alapján a FastEthernet0/2 és a FastEthernet0/3 interfészek működőképesek, mivel mind a Status, mind a Protocol állapota **`up`**.

A kapcsolón is használhatók a 3. rétegbeli csatlakozás tesztelésére a **`show ip interface brief`** és a**`traceroute`** parancsok. Az ábrán látható példában mind a **`ping`** , mind a **`traceroute`** parancsok sikeres kapcsolódást mutatnak.

Nagyon fontos, hogy megjegyezzük: a kapcsolónak nincs szüksége IP-címre a 2. rétegbeli keretek továbbításához. Az IP-cím csupán a kapcsoló hálózaton keresztül történő kezeléséhez szükséges, ami történhet Telnet vagy SSH használatával. Ha a hálózati rendszergazda a helyi hálózaton kívülről szeretne a kapcsolóhoz csatlakozni, alapértelmezett átjárót is konfigurálnia kell.

Egy kis hálózat létrehozásán és a biztonság megvalósításán kívül a hálózati rendszergazda feladata a konfigurációs állományok kezelése is. Ennek fontos eleme a biztonsági mentés és eszközhiba esetén a helyreállítás.

A Cisco IOS File System (IFS) egyszerű hozzáférést biztosít a forgalomirányító összes fájlrendszeréhez, melyek a következők:

- Flash memória fájlrendszerek
- Hálózati fájlrendszerek (TFTP és FTP)
- További olvasható és írható adattárolók, például NVRAM, aktív konfiguráció, ROM stb.

A Cisco IFS segítségével minden fájl megtekinthető és rendezhető (képfájl, szöveges fájl stb.), beleértve a távoli szervereken lévő állományokat is. Például, ellenőrzés céljából lehetőség van a távoli szerveren tárolt konfigurációs fájl megtekintésére annak forgalomirányítóba való betöltése előtt.

A Cisco IFS-ben a rendszergazda szabadon mozoghat a különféle könyvtárak között, kilistázhatja a tartalmukat, valamint létrehozhat alkönyvtárakat a flash memóriában vagy a lemezen. A felhasználható könyvtárak száma eszközfüggő.

Az 1. ábrán a **`show file systems`** parancs látható, mely éppen kilistázza a Cisco 1941-es forgalomirányító elérhető fájlrendszereit. Az utasítás hasznos információkat nyújt például a teljes és a még felhasználható tárolóterület nagyságáról, a fájlrendszer típusáról és jogosultságairól. Az engedélyek a lista Flags oszlopában jelennek meg, jelentésük a következő: csak olvasható (read only, ro), csak írható (write only, wo), és írható-olvasható (read and write, rw).

Bár nagyon sokféle fájlrendszer létezik, bennünket a tftp, a flash és az nvram érdekel.

Figyeljük meg, hogy a flash fájlrendszer meg van jelölve egy csillaggal (*), mely azt jelzi, hogy ez az aktuális alapértelmezett fájlrendszer. Mivel a flash tartalmaz egy betölthető IOS-t, így kettőskereszt (#) kerül a sor végére, jelezve ezzel az indítólemezt.

A flash fájlrendszer

A 2. ábrán az alapértelmezett fájlrendszer tartalma látható, mely jelen esetben a flash, amint azt az előző ábrán lévő * is mutatta. Számos fájl található a flash-en, de külön figyelmet érdemel az utolsó, mivel ez az aktuálisan a RAM-ba betöltött Cisco IOS képfájl.

Az NVRAM fájlrendszer

Az NVRAM tartalmának megtekintéséhez meg kell változtatnunk az aktuális alapértelmezett fájlrendszert a **`cd`** (change directory, könyvtár váltás) parancs használatával, amint a 3. ábrán látható. A **`pwd`** (present working directory, jelenlegi munkakönyvtár) parancs ellenőrzi, hogy valóban az NVRAM-ot látjuk. Végül a **`dir`**(directory, könyvtár) parancs kilistázza az NVRAM tartalmát. Bár több konfigurációs állomány is látható, külön figyelmet a startup-config (indító konfigurációs) fájl érdemel.

A Cisco 2960-as kapcsoló flash fájlrendszerének segítségével másolhatók a konfigurációs állományok, valamint le- és feltölthetjük a szoftver képfájlokat.

A Catalyst kapcsoló fájlrendszerének megtekintésére a Cisco forgalomirányítókhoz hasonlóan a **`show file systems`** parancs használható (lásd ábra).

A Cisco kapcsolók és forgalomirányítók több alap UNIX parancsot is támogatnak, például: **`cd`** - fájlrendszer vagy könyvtár váltás, **`dir`** - könyvtár tartalmának megjelenítése, és **`pwd`** - aktuális munkakönyvtár megmutatása.

Konfiguráció mentése szöveg rögzítéssel (Tera Term)

A konfigurációs fájlok szövegfájlba menthetők (archiválhatók) Tera Term használatával.

Az ábrán is látható lépések a következők:

1. A File menüben kattintsunk a **Log** menüpontra.

2. Válasszunk elérési utat a mentéshez. A Tera Term megkezdi a szöveg rögzítését.

3. Ezután futtassuk a **`show running-config`** vagy a **`show startup-config`** parancsot privilegizált EXEC módban. A terminálablakban megjelenő szöveg a választott fájlba íródik.

4. A rögzítés befejezéséhez válasszuk a **Close**nyomógombot a Tera Term Log ablakában.

5. Nyissuk meg a fájlt és ellenőrizzük a sértetlenségét.

Szöveges konfiguráció visszatöltése

A konfigurációt átmásolhatjuk a fájlból az eszközre. Ha kimásolunk valamit egy szöveges állományból és beillesztjük a terminálablakba, akkor az IOS parancsként értelmezi a sorokat és végrehajtja azokat. Ezért a fájlt előzőleg meg kell szerkeszteni, azaz a titkosított jelszavakat egyszerű szöveggé kell alakítani és törölni kell a parancsként nem értelmezhető szövegeket, például a "-More-" és hozzá hasonló IOS-üzeneteket. A folyamatot a laborgyakorlatban tárgyaljuk részletesen.

Fontos még, hogy az eszköz parancssorában a globális konfigurációs módot kell kiválasztani a szövegfájl beillesztése előtt.

Tera Term esetén a lépések a következők:

1. A File menüben kattintsunk a **Send** file menüpontra.

2. Válasszuk ki az eszközre másolandó fájlt és kattintsunk az **Open** gombra.

3. A Tera Term beilleszti az állományt az eszközre.

A fájlban lévő szöveget a CLI parancsként értelmezi és bemásolja az eszköz aktív konfigurációjába. Ez egy kényelmes módja a forgalomirányító kézzel történő konfigurálásának.

Konfiguráció mentése TFTP használatával

A konfigurációs állományokról biztonsági másolatot kell lementeni, felkészülve ezzel a váratlan eseményekre. A konfigurációs fájlok, melyek a hálózati dokumentáció részét is képezik, tárolhatók TFTP-szerveren (Trivial File Transfer Protocol) vagy USB-meghajtón.

Az aktív vagy az indító konfiguráció TFTP-szerverre mentéséhez a **`copy running-config tftp`** vagy a**`copy startup-config tftp`** parancs használható. (lásd ábra) Az aktív konfiguráció TFTP-szerverre mentéséhez kövessük az alábbi lépéseket:

1. Gépeljük be a **`copy running-config tftp`**parancsot.

2. Írjuk be a konfigurációs fájlt tárolását végző állomás (TFTP-szerver) IP-címét.

3. Adjuk meg a konfigurációs fájl nevét.

4. Nyomjuk le az Enter billentyűt választásunk megerősítéséhez.

Konfiguráció visszaállítása TFTP használatával

Az aktív vagy az indító konfiguráció TFTP-szerverről történő visszaállítására a **`copy tftp running-config`** vagy a **`copy tftp startup-config`**parancs használható. Az aktív konfiguráció TFTP-szerverről történő visszaállításához kövessük az alábbi lépéseket:

1. Gépeljük be a **`copy tftp running-config`**parancsot.

2. Írjuk be a konfigurációs állomány tárolására szolgáló állomás IP-címét.

3. Adjuk meg a konfigurációs fájl nevét.

4. Nyomjuk le az Enter billentyűt választásunk megerősítéséhez.

Egyes Cisco forgalomirányítók támogatják az USB (Universal Serial Bus) tárolási szolgáltatást, mely lehetővé teszi az USB flash meghajtók használatát. Ezek másodlagos tárolóként és alternatív indítólemezként is szolgálhatnak. A képfájlok, konfigurációs állományok és egyéb fájlok ugyanolyan megbízhatóan használhatók és tárolhatók USB flash memórián, mint Compact Flash (CF) kártyán. Továbbá a moduláris ISR (Integrated Services Router) eszközök képesek indításkor egy USB flash memórián lévő IOS-képfájlt betölteni.

A Cisco USB flash modulok 64MB, 128MB és 256MB változatokban kaphatók.

A Cisco fogalomirányítón való használathoz az USB-meghajtót FAT16-szabvány szerint kell formázni. Amennyiben ez nem teljesül, a show file systems parancs "ismeretlen fájlrendszer" hibaüzenetet ad.

A következő példa a dir parancs használatát mutatja be USB-fájlrendszeren:

Router# dir usbflash0:

Directory of usbflash0:/

1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)

Az USB flash memórián egyszerre több Cisco IOS-fájl és konfigurációs állomány is tárolható. Így a rendszergazda egyszerűen át tudja másolni ezeket fájlokat az egyik forgalomirányítóról a másikra, sok esetben jelentősen rövidebb idő alatt, mint LAN-on vagy WAN-on keresztül. Figyeljünk arra, hogy az IOS nem minden esetben ismeri fel helyesen az USB flash méretét, de ez nem feltétlenül jelenti annak használhatatlanságát. Végül jegyezzük meg, hogy a forgalomirányítón általában USB 2.0 szabványú portok találhatók.

Konfiguráció mentése USB flash meghajtóra

USB-re való mentés előtt a meghajtó nevének ellenőrzése érdekében célszerű kiadni a **`show file systems`**parancsot. (lásd 1. ábra)

Ezt követően a **`copy run usbflash0:/`** utasítás használatával másoljuk át a fájlt az USB flash lemezre. Ügyeljünk a rá, hogy a fájlrendszerben lévő nevet használjuk. A per jel (/) nem kötelező, de jelzi, hogy a meghajtó gyökérkönyvtáráról van szó.

Ezután az IOS bekéri a fájlnevet. Ha a fájl már létezik az USB meghajtón, a forgalomirányító a 2. ábrán látható módon figyelmeztet a felülírás veszélyére.

Használjuk a **dir** parancsot az USB-meghajtón lévő fájlok megtekintéséhez, és a **more** parancsot az állomány tartalmának megjelenítésére (lásd 3. ábra).

Konfiguráció visszaállítása USB-meghajtóról

A fájlt visszamásolás előtt feltétlenül nyissuk meg egy szövegszerkesztővel, és győződjünk meg annak helyességéről; ellenkező esetben érvénytelen parancsokat és nemlétező interfészeket tartalmazó bejegyzések kerülhetnek a konfigurációba.

```
R1# copy usbflash0:/R1-Config running-config

Destination filename [running-config]?
```

Hálózatokat nem csak a kisvállalkozások és a nagy szervezetek használnak.

Otthoni környezetben is egyre jobban terjed a hálózati technológiák alkalmazása. Az otthoni hálózatok a lakásban található különféle számítógépeket és laptopokat kötik össze, valamint internet kapcsolatot biztosítanak számukra. Ezenkívül számos szolgáltatást nyújtanak a felhasználóknak, úgymint hálózati nyomtatás, képek, zenék és filmek központi tárolása NAS berendezésen (Network Attached Storage, hálózatba kötött tároló), valamint internetelérést biztosítanak számos végfelhasználói készüléknek, melyek lehetnek táblaszámítógépek, mobiltelefonok vagy háztartási eszközök, mint például egy televízió.

Egy otthoni hálózat nagyon hasonlít egy kisvállalati hálózathoz, mivel legtöbbször egyik sem igényel felső kategóriás eszközöket, például dedikált forgalomirányítókat és kapcsolókat. Számukra megfelelnek olyan kisebb eszközök, melyek rendelkeznek útválasztási és kapcsolási funkcióval. Ez az oka annak, hogy sok otthoni és kisvállalati hálózatban többfunkciós, más néven multifunkciós eszközt használnak.

A kurzus folyamán ezekre a multifunkciós eszközökre mint integrált forgalomirányítókra hivatkozunk.

Az integrált forgalomirányító olyan, mintha számos különböző eszközt csatlakoztatnánk és építenénk egybe. Például a kapcsoló és a forgalomirányító közötti összeköttetés a berendezésen belül valósul meg. Amikor egy csomag a helyi hálózat egy végpontjától egy másik felé kerül kiküldésre, akkor a beépített kapcsoló továbbítja azt a céleszköznek. Ha a csomag egy távoli hálózat felé irányul, akkor is a beépített kapcsoló továbbítja azt, de ilyenkor a szintén beépített forgalomirányítónak. A forgalomirányító meghatározza a legjobb útvonalat és aszerint küldi tovább a csomagot.

A legtöbb integrált forgalomirányító vezetékes és vezeték nélküli kapcsolódási lehetőséget is biztosít, azaz elérési pontként (Access Point, AP) viselkedik, amint az 1. ábrán látható. A vezeték nélküli kapcsolódás közkedvelt, rugalmas és költséghatékony módszer végberendezések hálózati kiszolgálására otthoni és kisvállalati környezetben.

A 2. és 3. ábra a vezeték nélküli kapcsolat használatának szempontjait és előnyeit mutatja be.

Az integrált forgalomirányító az útválasztáson, kapcsoláson és vezeték nélküli csatlakozáson kívül még számos, például DHCP-szerver, tűzfal és NAS szolgáltatást is nyújthat.

Az integrált forgalomirányítók kínálata az otthoni és kisvállalati felhasználásra tervezett eszközöktől egészen a nagy szervezetek igényeit is kielégítő berendezésekig terjed.

Egy tipikus példa integrált forgalomirányítóra az ábrán is látható Linksys vezeték nélküli forgalomirányító. Maga a készülék egyszerű kivitelű és általában egyetlen összetevőből áll, ami csökkenti a bekerülési költségét. Ebből következően hiba esetén nincs lehetőség a tönkrement alkatrész cseréjére. Mindezek miatt elsődleges meghibásodási pontnak tekinthető, ráadásul egyetlen beépített funkciója sincs optimalizálva.

Egy másik példa integrált forgalomirányítóra a Cisco ISR (Integrated Services Router, integrált szolgáltatású forgalomirányító). A Cisco ISR termékcsalád széles választékot kínál, ideértve az otthoni és kis irodai környezetbe tervezett eszközöket és a nagyobb hálózatokba valókat is. Számos ISR moduláris, azaz minden funkcióját különálló elemek valósítják meg, mint például egy kapcsoló és egy forgalomirányító modul. Ez szükség esetén lehetővé teszi egyedi összetevők hozzáadását, cseréjét és fejlesztését.

Minden integrált forgalomirányító azonos alapbeállításokra ad lehetőséget, mint például a jelszavak, IP-címek és DHCP-beállítások konfigurálása, melyek egyaránt vonatkoznak a vezetékkel és a vezeték nélkül csatlakozó állomásokra. A vezeték nélküli kapcsolódáshoz további paraméterek beállítása is szükséges, úgymint vezeték nélküli mód, SSID és vezeték nélküli csatorna.

Vezeték nélküli mód

A vezeték nélküli mód a hálózat által használt IEEE 802.11 szabvány szerinti beállítást jelenti. Az IEEE 802.11 szabványhoz több kiegészítés is tartozik, melyek leírják a különféle vezeték nélküli kommunikációk jellemzőit. Ezek a 802.11a, 802.11b, 802.11g és a 802.11n szabványok. (továbbá a 802.11ac,ad,af,ah stb., a fordító megjegyzése). Az ábrára kattintva láthatjuk a különféle beállítási lehetőségeket.

A legtöbb integrált forgalomirányító támogatja a 802.11b,g,n szabványokat. Ezek kompatibilisek egymással, de a hálózat minden eszközének egyazon szabvány szerint kell működni. Például: Ha egy 802.11n forgalomirányító egy 802.11n laptophoz kapcsolódik, akkor a hálózat 802.11n szabvány szerint fog működni. Ha viszont hozzáadunk egy 802.11b nyomtatót a hálózathoz, akkor a forgalomirányító és a laptop is visszaáll a lassabb 802.11b szabvány használatára. Tehát a régi eszközök az egész hálózat működését lelassítják. Ezt fontos észben tartani, amikor egy régebbi eszköz megtartásáról vagy cseréjéről döntünk.

SSID

Mivel sok vezeték nélküli hálózat lehet a környezetünkben, ezért fontos, hogy a vezeték nélküli eszközök a megfelelő WLAN-hoz csatlakozzanak. Erre való az SSID (Service Set Identifier, szolgáltatás készlet azonosító).

Az SSID a vezeték nélküli hálózat neve, mely legfeljebb 32 alfanumerikus karakterekből állhat és nagybetű-kisbetű érzékeny. Az SSID-t arra használjuk, hogy a vezeték nélküli eszközöknek megmondjuk, melyik WLAN-hoz tartoznak és mely más eszközökkel kommunikálhatnak. Tekintet nélkül arra, hogy milyen típusú WLAN-ról van szó, a kommunikáció érdekében egy hálózat minden vezeték nélküli eszközét ugyanarra az SSID-re kell beállítani.

Vezeték nélküli csatorna

A csatornák a rendelkezésre álló rádiófrekvenciás (RF) tartomány részekre bontásával jönnek létre. Minden egyes csatorna egy különböző párbeszéd lebonyolítására alkalmas. Ez hasonló ahhoz, amikor több televíziós csatornát szolgáltatnak egyetlen átviteli közegen keresztül. Így több hozzáférési pont is képes egymáshoz közel üzemelni, feltéve hogy eltérő csatornákat használnak a kommunikációra.

Biztonsági óvintézkedések megtervezése és beállítása is szükséges, mielőtt egy AP-t a hálózathoz vagy az internethez csatlakoztatnánk.

Néhány alapvető biztonsági rendszabály ezek közül, melyek az 1. ábrán is láthatók:

- Változtassuk meg az SSID, a felhasználó nevek és a jelszavak alapértelmezett értékeit
- Tiltsuk le az SSID-szórást
- Állítsunk be WEP vagy WPA titkosítást

A titkosítási folyamat az adatok olyan átalakítását jelenti, melynek eredményeként az elfogott információk használhatatlanok lesznek.

WEP

A WEP (Wired Equivalency Protocol, vezetékessel egyenértékű titkosítási protokoll) egy fejlett biztonsági lehetőség, mely a vezeték nélküli hálózati forgalom titkosítását végzi. Az adatok kódolására és dekódolására a WEP előre konfigurált kulcsokat használ (lásd 2. ábra).

A WEP-kulcsok szám- és betűkombinációból álló sorozatok, többnyire 64 vagy 128 bit hosszúsággal, mely egyes esetekben 256 bit is lehet. A kulcsok létrehozásának és beírásának egyszerűsítése érdekében számos eszköz felkínálja a Passphrase (jelmondat) lehetőséget. A passphrase egy könnyen észben tartható szó vagy kifejezés, melyet a kulcsok automatikus létrehozásához használhatunk.

A WEP megfelelő működéséhez a hozzáférési ponton és az összes engedélyezett állomáson ugyanazon WEP-kulcsot kell megadni. Ezen kulcs nélkül az eszközök nem tudják értelmezni az érkező vezeték nélküli jeleket.

A WEP használatának megvannak a hátrányai is, például, hogy az összes állomáson statikus (állandó érvényű) kulcsokat használ. Léteznek olyan interneten is fellelhető alkalmazások, melyek segítségével a támadók kideríthetik a WEP-kulcsot. Miután a támadó megfejtette a kulcsot, teljes hozzáférést szerez az összes továbbított információhoz.

A sebezhetőség elkerülésének egyik módja a WEP-kulcsok gyakori megváltoztatása. A másik módszer egy jóval fejlettebb és biztonságosabb titkosítási eljárás, a WPA (Wi-Fi Protected Access, Wi-Fi védett hozzáférés) alkalmazása.

WPA

A WPA (Wi-Fi Protected Access, Wi-Fi védett hozzáférés) is 64 és 256 bit közötti hosszúságú kulcsokat használ, de ellentétben a WEP-pel, automatikusan új kulcsokat hoz létre minden alkalommal, amikor egy kliens kapcsolódik a hozzáférési ponthoz. A dinamikus kulcsok használata miatt a WPA feltörése lényegesen nehezebb, így jóval biztonságosabb a WEP-nél.

Számos további biztonsági megoldás konfigurálható egy vezeték nélküli AP-n, például MAC-cím szűrés, hitelesítés és forgalomszűrés. Ezek megvalósítása azonban kívül esik a kurzus témakörén.

A Linksys vezeték nélküli forgalomirányító gyakori eszköz az otthoni és kisvállalati hálózatokban, ezért a kurzus során az integrált forgalomirányító konfigurálásának bemutatásához fogjuk használni. A Linksys eszköz általában 5-8 Ethernet porttal rendelkezik a vezetékes kapcsolódáshoz, és vezeték nélküli elérési pontként (AP) is működik. Ezenkívül tartalmaz egy DHCP-szervert és egy mini webszervert, amely a grafikus felhasználói felületet (Graphical User Interface, GUI) biztosítja.

Linksys forgalomirányító elérése és konfigurálása

A Linksys forgalomirányítóhoz való első kapcsolódáshoz kössük össze a számítógépet a forgalomirányító egyik LAN Ethernet portjával (lásd ábra). A csatlakozás után a számítógép automatikusan címinformációkat kap az integrált eszköztől, többek között az alapértelmezett átjáró címét, amely egyben a Linksys eszköz IP-címe is. Ellenőrizzük a számítógép beállításait és állapítsuk meg ezt címet az **`ipconfig /all`** parancs használatával. Ezután gépeljük be a kapott IP-címet egy böngészőprogramba, hogy hozzáférjünk a webes konfigurációs felülethez (GUI).

A Linksys eszköz gyári konfigurációja alapvető útválasztási és kapcsolási szolgáltatásokat, valamint egy DHCP-szervert tartalmaz. Mielőtt egy AP-t az élő hálózathoz csatlakoztatunk, néhány kezdeti konfigurációs feladatot végre kell hajtanunk. Ezek közé tartozik az alapértelmezett felhasználónév és jelszó megváltoztatása, a Linksys IP-címének lecserélése és DHCP-ímtartományának módosítása.

A vezeték nélküli kapcsolódás engedélyezéséhez be kell állítanunk a vezeték nélküli módot, az SSID-t, az RF-csatornát és a kívánt titkosítási eljárást.

Először válasszuk ki a megfelelő vezeték nélküli módot, ahogy az ábrán is látható. Bármelyik mód beállítása bizonyos többletterhelést jelent a forgalomirányító számára. Ha minden állomás ugyanazt a szabványt használja, akkor a forgalomirányítón is ezt konfigurálva csökkenthető a terhelés. Ezenfelül biztonságot növelő tényező is, ha a végberendezéseknek nem engedélyezzük a különböző módú csatlakozást. Ha az állomások mégis különféle szabványokat használnak a hálózat elérésére, akkor a "mixed" módot kell választanunk. Ebben az esetben a hálózat teljesítménye csökkenni fog a módok támogatása miatti többletterhelés miatt.

Ezután állítsuk be az SSID-t. A vezeték nélküli hálózatban (WLAN) lévő összes együttműködő eszköznek azonos SSID-vel kell rendelkezni. Biztonsági okokból változtassuk meg az alapértelmezett SSID-t. Az SSID-szórás gyárilag bekapcsolt állapotban van, hogy a WLAN kliensek könnyen felismerjék a hálózatot. Az SSID-szórás kikapcsolható, ilyenkor azonban a vezeték nélküli klienseken kézzel kell beállítani ezt az értéket.

Az RF-csatorna kiválasztásakor figyelembe kell venni az integrált forgalomirányító közelében működő más vezeték nélküli hálózatokat.

Az optimális átbocsátóképesség elérése érdekében a szomszédos hálózatoknak egymást át nem fedő csatornákat kell használni. Manapság a legtöbb AP-n megtalálható az a beállítás, amely automatikusan megkeresi a legkevésbé terhelt csatornát.

Végül válasszuk ki a kívánt titkosítási módszert, és adjuk meg a kulcsot vagy a jelszót (jelmondatot).

Vezeték nélküli kliens konfigurálása

Vezeték nélküli állomásnak, más néven kliensnek nevezünk minden olyan eszközt, amely rendelkezik vezeték nélküli hálózati kártyával és a hozzá tartozó szoftverrel. Ez a kliensszoftver teszi lehetővé, hogy a hardver a WLAN része legyen. Vezeték nélküli kliensek például: okostelefonok, laptopok, asztali számítógépek, nyomtatók, televíziók, játékkonzolok és táblaszámítógépek.

A WLAN-hoz való sikeres csatlakozás érdekében a kliens és a forgalomirányító beállításainak összhangban kell lenni. Ilyenek például az SSID, a biztonsági beállítások, és a csatorna adatok (ha manuálisan lettek konfigurálva). A beállítások a kliensszoftverben kerülnek megadásra.

A használt kliensszoftver lehet az eszköz operációs rendszerébe integrált, vagy lehet különálló, letölthető szoftver, melyet vezeték nélküli NIC kezelésére terveztek.

A szoftver beállítása után ellenőrizzük a kliens és az AP közötti kapcsolatot.

Nyissuk meg a vezeték nélküli kapcsolat információs ablakát, melyben a következők láthatók: adatátviteli sebesség, kapcsolat állapot és csatorna használat (lásd ábra). A Link Information menüpont, ha rendelkezésre áll, megjeleníti a vezeték nélküli jel erősségét és minőségét.

A kapcsolat további ellenőrzéséhez győződjünk meg arról, hogy továbbíthatók-e az adatok. Az egyik leggyakrabban használt módszer az adatátvitel tesztelésére a ping. Ha a ping sikeres, az adatátvitel lehetséges.

Capstone ("sarokkő") projekt

Kisvállalati hálózat tervezése és kivitelezése

A feladat megoldásához használjuk a Packet Tracer-t és egy szövegszerkesztő. Dolgozzunk 2-3 fős csoportokban.

Tervezzük meg és építsük fel a hálózatot a következő rövid vázlat alapján.

- A tervezetben legyen legalább egy forgalomirányító, egy kapcsoló és egy PC.
- Teljesen konfiguráljuk fel a hálózatot IPv4- vagy IPv6-címzést használva (alhálózatokra bontás is legyen a címzési tervben).
- Teszteljük a hálózatot legalább 5 **`show`** parancs kiadásával.
- Ügyeljünk a hálózatbiztonságra, használjunk SSH-t, jelszótitkosítást és védjük a konzol hozzáférést is. (Minimum elvárás)

Készítsünk táblázatot a munka értékeléséhez, vagy használjuk az oktató által biztosítottat.

Mutassuk be saját tervünket az osztálynak és készüljünk fel a felmerülő kérdések megválaszolására.

Csoportos feladat - Design and Build a Small Network Instructions

A felhasználói igények teljesítése érdekében a kisebb hálózatok is tervezést igényelnek (lásd ábra). Tervezéskor figyelembe kell venni az összes követelményt, költségelemet és fejlesztési lehetőséget, valamint biztosítani kell a megbízhatóságot, skálázhatóságot és a rendelkezésre állást.

A kis hálózatok felügyelete és fejlesztése jártasságot kíván a protokollok és hálózati alkalmazások tekintetében. A protokollelemzők segítségével a szakemberek gyorsan kaphatnak átfogó statisztikai információkat a hálózati forgalomról. Ezt követően a begyűjtött adatok rendszerezhetők az üzenetek forrása, célja és típusa szerint. A elkészült elemzés alapján a hálózati szakember döntést hozhat a forgalom hatékonyabbá tétele érdekében. A leggyakran vizsgált protokollok a következők: DNS, Telnet, SMTP, POP, DHCP, HTTP és FTP.

A hálózat tervezésekor figyelembe kell venni a biztonsági fenyegetéseket és sebezhetőségi pontokat. A hálózat összes készülékét védeni kell, beleértve a forgalomirányítókat, kapcsolókat és felhasználói eszközöket, sőt még a biztonsági berendezéseket is. A hálózatokat különféle kártékony szoftverek veszélyeztetik, például vírusok, trójai lovak és férgek. A vírusirtó szoftverek felismerik legtöbbjüket, és megakadályozzák szétterjedésüket a hálózatban. A féregtámadások elkerülésének leghatékonyabb módja az operációs rendszer biztonsági frissítéseinek telepítése és a sebezhető rendszerek hibajavítása (patch).

A hálózatokat védeni kell a hálózati támadásoktól is, melyek három fő csoportja: a felderítési és a hozzáférési támadások, valamint a szolgáltatás megtagadás. A hálózatok többféle módon is megóvhatók ezektől a támadásoktól.

- A hitelesítés, jogosultság kezelés és naplózás (Authentication, Authorization, and Accounting, AAA vagy tripla A) olyan biztonsági szolgáltatások, melyek a hálózati eszközök hozzáférés-szabályozásának alapját alkotják. Az AAA vezérli, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultság), és nyomon követi a használat során végrehajtott műveleteket (naplózás).
- A tűzfal az egyik leghatékonyabb olyan biztonsági eszköz, mely a belső hálózati felhasználók külső veszélyektől való megvédésére szolgál. A tűzfal két vagy több hálózat között helyezkedik el, ellenőrzi a köztes forgalmat, és véd a jogosulatlan hozzáféréstől is.
- A hálózati eszközök védelme érdekében fontos az erős jelszavak használata. valamint távoli bejelentkezés esetén az SSH engedélyezése a könnyen támadható Telnet helyett.

A hálózat kiépítése után a rendszergazda következő feladata a hálózati összeköttetések vizsgálata és karbantartása, melyhez számos módszer áll rendelkezésre. A helyi és távoli hálózatokkal való

kapcsolat tesztelésére leggyakrabban a **ping, telnet**és a **traceroute** parancsokat alkalmazzák.

A Cisco IOS eszközökön a **show version** parancs használható az indításnál szerepet játszó hardver- és szoftverkomponensek ellenőrzésére és az esetleges hibák megkeresésére. A forgalomirányító interfész információinak megtekintésére a **show ip interface**utasítás szolgál. A **show ip interface brief** egy tömörebb kimenetet jelenít meg, mint a **show ip interface** parancs. A CDP (Cisco Discovery Protocol) egy Cisco fejlesztésű protokoll, mely az adatkapcsolati rétegben működik. Ennek köszönhetően az egymással összekötött Cisco eszközök, például a különböző hálózati protokollt használó forgalomirányítók, képesek felismerni szomszédaikat még akkor is, ha 3. rétegbeli kapcsolat nincs is közöttük.

Az IOS konfigurációs állományait (pl.: startup-config vagy running-config) archiválni kell egy szövegfájlba vagy egy TFTP-szerverre. Néhány forgalomirányító típus rendelkezik USB-porttal, így a biztonsági mentés USB-meghajtóra is történhet. Szükség esetén a lementett fájlok a TFTP-szerverről vagy az USB-meghajtóról visszamásolhatók a forgalomirányítóra vagy kapcsolóra.

Hálózatokat nem csak kisvállalkozások és nagy szervezetek használnak. Otthoni környezetben is egyre jobban terjed a hálózati technológiák alkalmazása. Egy otthoni hálózat nagyon hasonlít egy kisvállalati hálózathoz, mivel egyik sem igényel felső kategóriás eszközöket, például dedikált forgalomirányítókat és kapcsolókat. Helyettük az otthoni hálózatokban multifunkciós eszközök működnek. A kurzus folyamán ezekre a multifunkciós eszközökre, mint integrált forgalomirányítókra hivatkozunk. A legtöbb integrált forgalomirányító vezetékes és vezeték nélküli kapcsolódási lehetőséget is biztosít, valamint vezeték nélküli elérési pontként (Access Point, AP) viselkedik. A vezeték nélküli kapcsolódás engedélyezéséhez be kell állítanunk a vezeték nélküli módot, az SSID-t, az RF-csatornát és a kívánt titkosítási eljárást.