

Cisco CCNA Discovery

4.1

Hálózati feladatok kis- és középvállalatoknál
vagy internetszolgáltatóknál

(2. szemeszter)



1. Az internet és használata

1.1 Mi az internet?

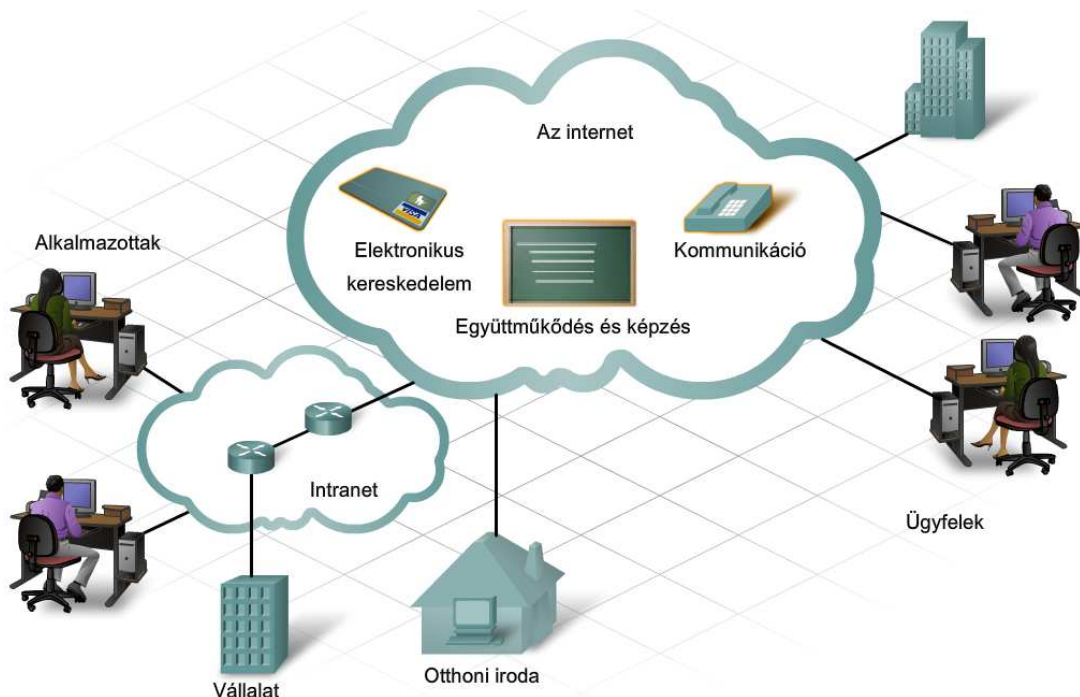
1.1.1 Az internet és a szabályok

Az internet világszerte nyilvánosan hozzáférhető hálózatok összessége. Lehetővé teszi mind magánszemélyek mind vállalatok számára, hogy egymással összekapcsolt számítógép-hálózatokon keresztül információt, erőforrásokat és szolgáltatásokat osszanak meg.

Kezdetben az internetet kizárólag tudományos, oktatási és katonai kutatásokhoz használták. 1991-ben a szabályok megváltozása tette lehetővé a vállalatok és felhasználók számára is a csatlakozást. Az internet gyorsan növekedett és ma már világméretű. A folyamatosan megjelenő új technológiák egyre könnyebbé és vonzóbbá teszik használatát. A felhasználók számára on-line alkalmazásokat biztosít, mint például az elektronikus levelezés, webböngészés, zene- és videofolyamok továbbítása, játékok és az azonnali üzenetküldés.

Az internet folyamatos fejlődésének megfelelően változik az emberek közti kapcsolattartás, a kommunikáció és üzleti élet is. Az internet nagyobb érdeklődést és fogyasztói bázist teremt a hálózaton nyújtható üzenetek, termékek és szolgáltatások iránt. Számos vállalat számára az internetkapcsolat nem csak a kommunikáció, hanem a mindennapi működés szempontjából is nélkülözhetetlen. A vállalatok egy része az internet alábbi felhasználási területeit használja:

- e-kereskedelem
- Kommunikáció
- Együttműködés és képzés



Elektronikus kereskedelem
Minden weben keresztül lebonyolítható üzleti tevékenységre vonatkozik. Magában foglalja a webes hirdetéseket, kiadványokat, katalógusokat, valamint a megrendelési és értékesítési szolgáltatásokat. A vállalatok termékeiket és szolgáltatásait interneten keresztül saját aukciós oldalakon vagy társoldalakon keresztül értékesíthetik.
Együttműködés és képzés
Dokumentumok, prezentációk és táblázatok megosztásához szükséges környezet létrehozására utal. Lehetővé teszi felhasználók egy virtuális csoportjának, hogy távoli helyszínekről üzleti és oktatási céllal együttműködjenek. Ilyen felhasználások például a videokonferencia, virtuális tárgyalók, virtuális tantermek, on-line oktatás, FTP oldalak és jelszóval védett adatbázisok és alkalmazások.
Kommunikáció
Ide tartozik a kommunikáció minden elektronikus formája, mint például az elektronikus levelezés, azonnali üzenetküldés és az on-line csevegés. Azonkívül, sok vállalat a telefonköltségek csökkentése érdekében, internetes telefonszolgáltatáson alapuló (VoIP - Voice over IP) belső telefonos rendszert használ.

Az on-line elérhető új technológiák és eszközök számának növekedése mellett hogyan lehet a változásokat követni, és olyan megbízható szolgáltatásokat nyújtani, mint például az elektronikus levelezés? A felelet az, hogy az internetszabványok segítségével.

Egy szabvány a működéshez szükséges szabályok gyűjteménye. A hálózati és az internetszabványoknak köszönhetően a hálózathoz csatlakozó minden eszközre ugyanazon szabályok érvényesek. Szabványok használatával lehetővé válik különböző típusú eszközök kommunikációja az interneten keresztül. Egy elektronikus levél formázása, továbbítása és vétele például szintén egy szabvány alapján történik. Egy személyi számítógépről elküldött elektronikus levelet a címzett mindaddig képes mobil telefonján fogadni és elolvasni, amíg a telefon és a számítógép ugyanazt a szabványt használja.

Egy internet szabvány minden részletre kiterjedő vita, problémamegoldás és tesztelés eredményeként jön létre. Új szabvány ajánlásakor a fejlesztési és jóváhagyási folyamat minden lépését rögzítik egy számozott RFC (Request for Comments) dokumentumban, melyben a szabvány fejlődése nyomonkövethető.

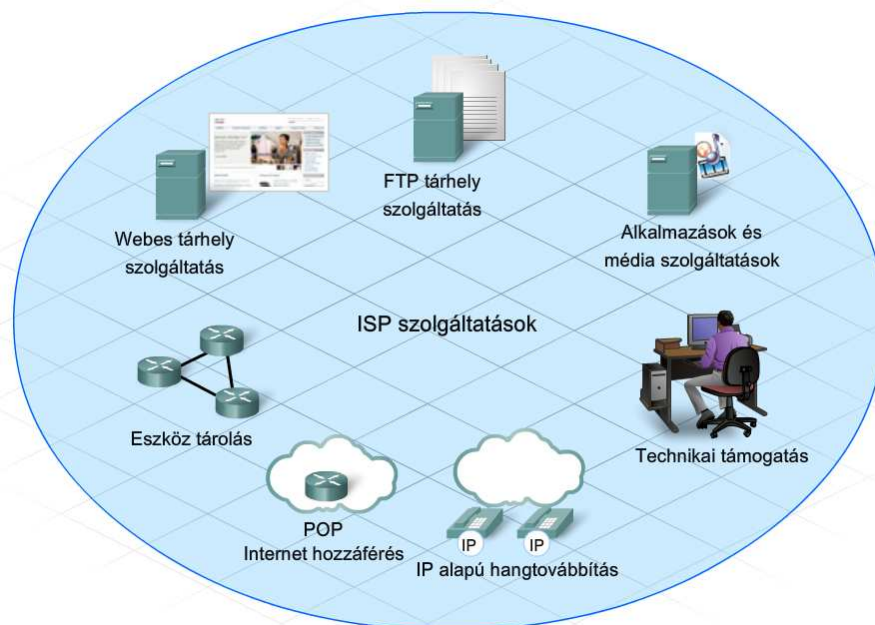
Az internetszabványok ezrei határozzák meg a hálózati eszközök kommunikációjának szabályait. Ezeket a különböző szabványokat több különböző szervezet készíti, teszi közzé és tartja karban. Az ilyen szervezetek által készített és karbantartott szabványok teszik lehetővé, hogy számos különböző eszközt használva, mint például a személyi számítógépek, mobiltelefonok, PDA-k, MP3 lejátszók és televíziók, emberek milliói kapcsolódjanak az internethez.

1.1.2 ISP és ISP szolgáltatások

Függetlenül attól, hogy egy magánszemély vagy vállalat milyen eszköz segítségével kapcsolódik az internethez, az eszköznek internetszolgáltatóhoz (ISP - Internet service provider) kell csatlakoznia. Az ISP egy vállalat vagy szervezet, amely az előfizetők számára az internet hozzáférést biztosítja. Előfizető lehet vállalat, magánszemély, kormányzati testület vagy akár egy másik ISP.

Az internet kapcsolat biztosítása mellett egy ISP további szolgáltatásokat is nyújthat az előfizetők számára, beleértve:

- **Eszköztárolás (Equipment co-location)** - A vállalatok kérhetik néhány vagy az összes hálózati eszközüknek az ISP területén történő tárolását.
- **Webes tárhely szolgáltatás** - Az ISP biztosítja a kiszolgálót és az alkalmazást a vállalat weboldalainak tárolásához.
- **FTP** - Az ISP biztosítja a kiszolgálót és az alkalmazást a vállalat FTP oldalainak tárolásához.
- **Alkalmazások és médiaszolgáltatások** - Az ISP bocsájtja rendelkezésre a kiszolgálót és a szoftvert egy vállalatnak, hogy az biztosíthasson média adatfolyam, mint például a zene és a video, vagy alkalmazásokat, mint például az on-line adatbázisok.
- **IP alapú hangtovábbítás** - Az egymástól fizikailag távol eső telephelyek közötti kommunikációra használva, az IP alapú hangátvitel költségmegtakarítással jár.
- **IP alapú hangtovábbítás** - sok vállalat nem rendelkezik olyan szakértelemmel, amely egy nagy belső hálózat karbantartásához kell. Számos internetszolgáltató nyújt fizetett technikai támogatást.
- **Szolgáltatási pont (POP - Point of Presence)** - Egy vállalat egy megjelenési ponton keresztül, különböző elérési technológiát használva kapcsolódhat az internetszolgáltatóhoz.



1.2 ISP-k

1.2.1 Az internet-szolgáltatások eljuttatása a végfelhasználókhoz

Az internethez történő kapcsolódáshoz elsődlegesen egy internetszolgáltatóval kell kapcsolatot teremteni. Az internetszolgáltatók a csatlakozások széles választékát kínálják. Otthoni és kisvállalati felhasználók által leggyakrabban használt kapcsolódási formák:

Betárcsázásos hozzáférés

A betárcsázás egy nem túl költséges, telefonvonal és modem használatával megvalósított internet elérési módszer. Az internetszolgáltatóhoz való kapcsolódáshoz a felhasználó felhívja a szolgáltató elérési számát. A leglassabb kapcsolódási forma, és jellemzően akkor használják, ha nagyobb sebességű kapcsolat nem építhető ki, illetve a több helyszín között ingázó dolgozók között elterjedt.

DSL

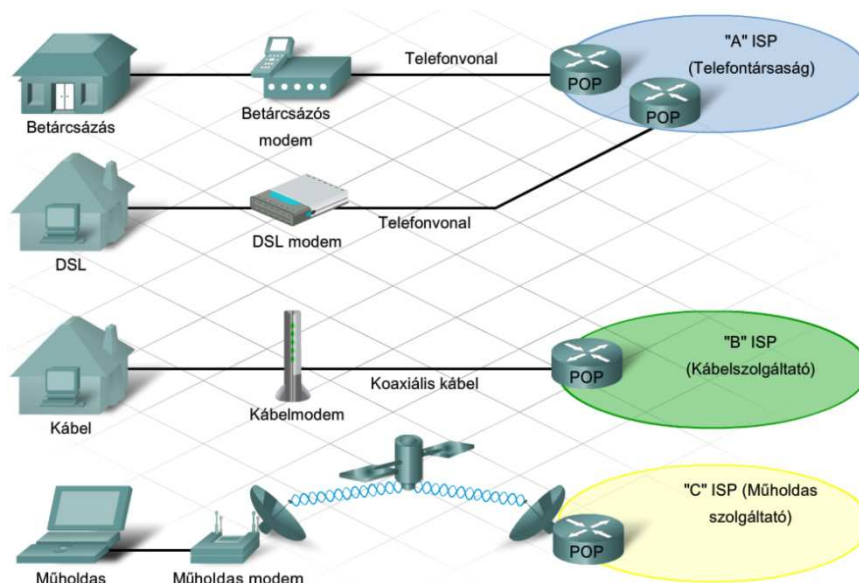
A digitális előfizetői hurok vagy DSL a betárcsázásnál költségesebb, de gyorsabb kapcsolatot biztosít. Szintén telefonvonalat használ, de a betárcsázásos hozzáféréssel ellentétben állandó internet kapcsolatot nyújt. Ez a kapcsolódási megoldás speciális nagysebességű modem segítségével választja szét a DSL jelet a telefon jeltől, és szolgáltat ethernetkapcsolatot egy számítógép vagy LAN számára.

Kábelmodem

A kábelmodem a televíziós társaságok által nyújtott kapcsolódási lehetőség. A hálózati kommunikációhoz szükséges jeleket ugyanaz a koaxiális kábel továbbítja, mint a televízióműsort. Egy speciális kábelmodem különválasztja a hálózati jeleket a többitől, és ethernetkapcsolatot biztosít egy számítógép vagy számítógéphálózat számára.

Műholdas

Műholdas kapcsolódást a műholdas szolgáltatók biztosítanak. A felhasználó számítógép ethernethálózattal kapcsolódik a műholdas modemhez, mely a műholdas hálózat legközelebbi szolgáltatási pontjához (POP) közvetíti a jeleket.



A betárcsázásos hozzáférés körülbelül 56 Kb/s sebességgel a leglassúbb kapcsolódási lehetőség. Egy 5 MB-os fájl letöltése például megközelítőleg 12 percet vesz igénybe.

A szélessávú technológián alapuló, nagysebességű átvitelre alkalmas DSL kapcsolat legalább 512 Kb/s sebességre képes, így egy 5 MB-os fájl letöltése megközelítőleg egy percet vesz igénybe. A letöltési és feltöltési sebesség a földrajzi helytől, az ISP-től való távolságtól és az ISP szolgáltatásaitól függően változhat.

A DSL kapcsolatnak több különböző fajtája létezik. Otthoni felhasználó esetén legáltalánosabban használt az Aszimmetrikus Digitális Előfizetői Vonal (ADSL - Asymmetric Digital Subscriber Line), melynél a letöltési sebesség nagyobb, mint a feltöltési sebesség. Egy másik típus a Szimmetrikus Digitális Előfizetői Vonal (SDSL - Symmetric Digital Subscriber Line), amelynél a feltöltési és letöltési sebesség azonos, így alkalmasabb lehet a kis- és középvállalatok számára.

A kábelkapcsolat a DSL-hez hasonló sebességű szélessávú technológia. Az internetszolgáltatótól és az elhelyezkedéstől függően, 512 Kb/s vagy nagyobb sebességű kapcsolatot biztosít, amely a DSL-lel ellentétben az ISP-től mért távolságtól független. A kábeles szolgáltatás osztott sáv szélességgel működik, így egy adott területen az internetet használók száma befolyásolja a sebességet.

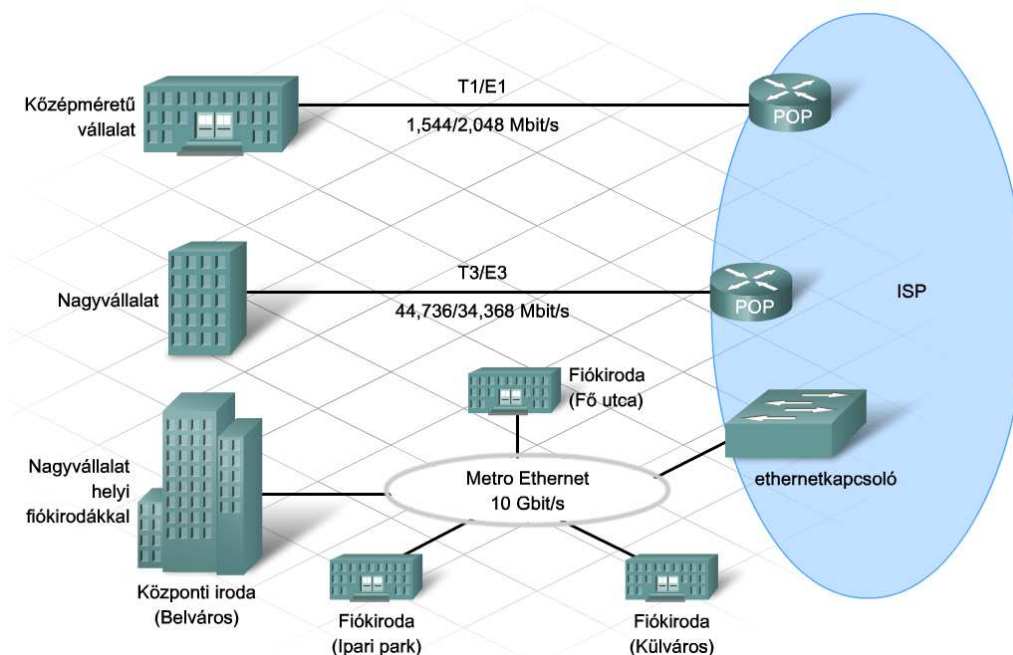
A műholdas internet-hozzáférés sebessége az előfizető igényétől függően 128 Kb/s és 512 Kb/s között mozog.

Sávszélesség mértékegysége a bit/s. Nagyobb sávszélességek megadására a Kbit/s, Mbit/s, illetve a Gbit/s mértékegységeket használjuk.

A vállalatok által leggyakrabban használt három nagysávszélességű kapcsolódási forma a következő:

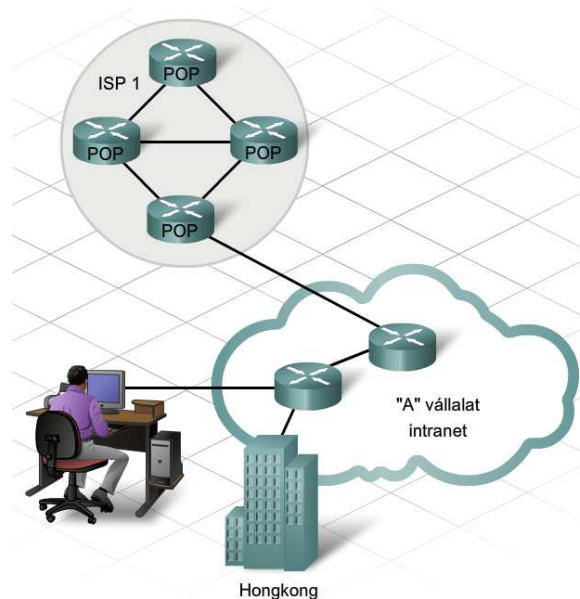
- **T1 kapcsolat**, mely 1,544 Mbit/s -os adatátvitelre képes. Ez egy szimmetrikus kapcsolat, abban az értelemben, hogy a feltöltési és letöltési sebesség azonos. Egy közepeméretű vállalatnak összesen egy T1 kapcsolatra van szüksége. Az E1 kapcsolat egy Európai szabvány, mely képes akár 2,048 Mbit/s-os adatátviteli sebességre is.
- A **T3 kapcsolat** maximálisan 45 Mbit/s-os adatátvitelt biztosít. Habár meglehetősen nagyobb költségekkel jár a T3 kapcsolat, mint a T1, nagyobb vállalatok esetén mégis megfelelőbb az alkalmazottak igényeinek kielégítésére. Többtelephelyű nagyvállalatok számára a T1 és T3 kapcsolatok együttes használata ajánlott. Az E3 kapcsolat egy Európai szabvány, mely képes akár 34,368 Mbit/s-os adatátviteli sebességre is.
- A **Metro Ethernet** a nagysávszélességű lehetőségek széles választékát kínálja, beleértve a Gbit/s-os kapcsolatot. Olyan nagyobb vállalatok, melyek egy városon belül több helyszínnel is rendelkeznek, mint például a bankok, Metro Ethernetet használnak. A Metro Ethernet a

telephelyeket kapcsolt technológiával köti össze. Nagymennyiségű adat olcsóbb és gyorsabb átvitelét teszi lehetővé, mint más nagysebességű kapcsolat.



A kapcsolat típusának meghatározása után az interneteléshez szükség van az ISP-hez történő kapcsolódásra. Egyéni számítógépek és vállalati hálózatok a szolgáltatási pontnál (POP) kapcsolódnak az internetszolgáltatóhoz. A szolgáltatási pontok (POP) általában az internetszolgáltatók hálózatának szélén találhatók és egy meghatározott földrajzi területet szolgálnak ki. A végfelhasználók számára helyi csatlakozási pontot és hitelesítést (jelszó védelem) biztosítanak. Egy internetszolgáltatónak több szolgáltatási pontja is lehet, attól függően, hogy mekkora a POP mérete és az a terület, melyet a POP kiszolgál.

Az ISP hálózatán belül nagysebességű forgalomirányítók és kapcsolók továbbítják az adatokat a szolgáltatási pontok között. Több útvonal is összeköti a szolgáltatási pontokat, hogy alternatív útvonalat szolgáltatassanak forgalom túlterhelés vagy kiesés esetén.

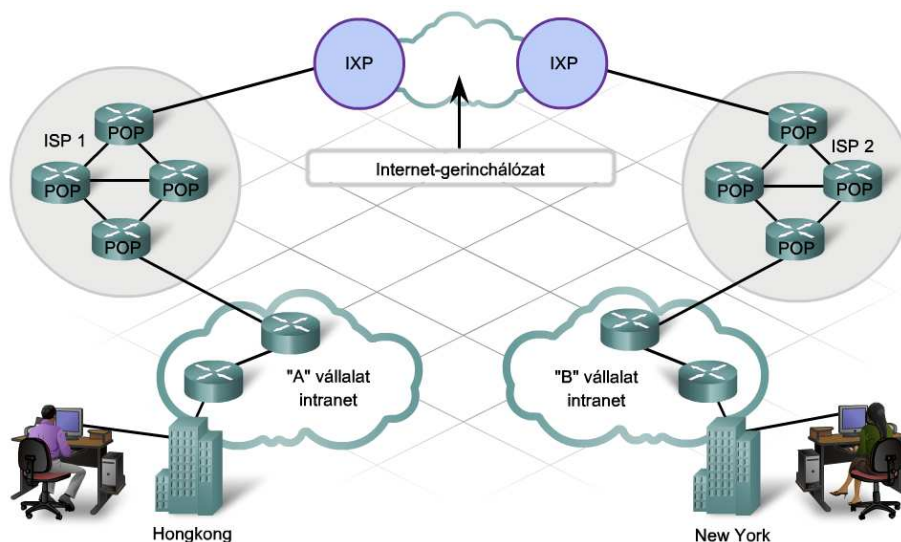


1.2.2 Internet hierarchia

Az internet hierarchikus felépítésű. A hierarchia csúcsán az internetszolgáltató szervezetek találhatók. Az internetszolgáltatók szolgáltatási pontjai (POP) egy internetcsatlakozási ponthoz csatlakoznak (IXP - Internet Exchange Point). Bizonyos országokban ezt hálózatelérési pontnak (NAP - Network Access Point) nevezik. Egy IXP vagy NAP az a pont, ahol több internetszolgáltató csatlakozik egymáshoz, hogy elérjék egymás hálózatát és információt továbbítsanak. Jelenleg több, mint 100 fő csatlakozási pont (IXP) található világszerte.

Az internet-gerinchálózatát a különböző szervezetek hálózatainak csoportja alkotja, melyeket IXP pontokon keresztül magán társkapcsolat köt össze.

Az internet-gerinchálózat olyan, mint egy információs szupersztráda, amely nagysebességű adatkapcsolatokat biztosít, hogy összekösse a POP-okat és az IXP-eket a világ nagyvárosaiban. Az elsődleges átviteli közeg, mely az internet gerinchálózatát összeköti, az üvegszálas kábel. Ezeket a kábeleket általában földfelszín alatt vezetik a városok összekötéséhez. Üvegszálas kábeleket a tenger alatt is vezetnek a kontinensek, országok és városok összekötésére.

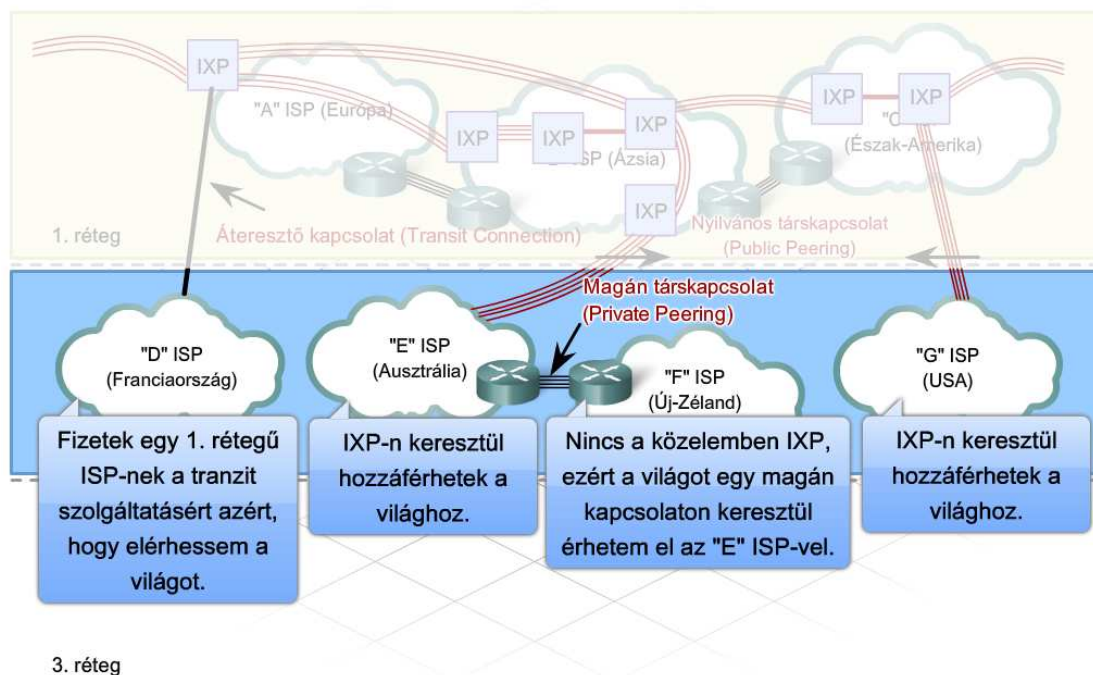
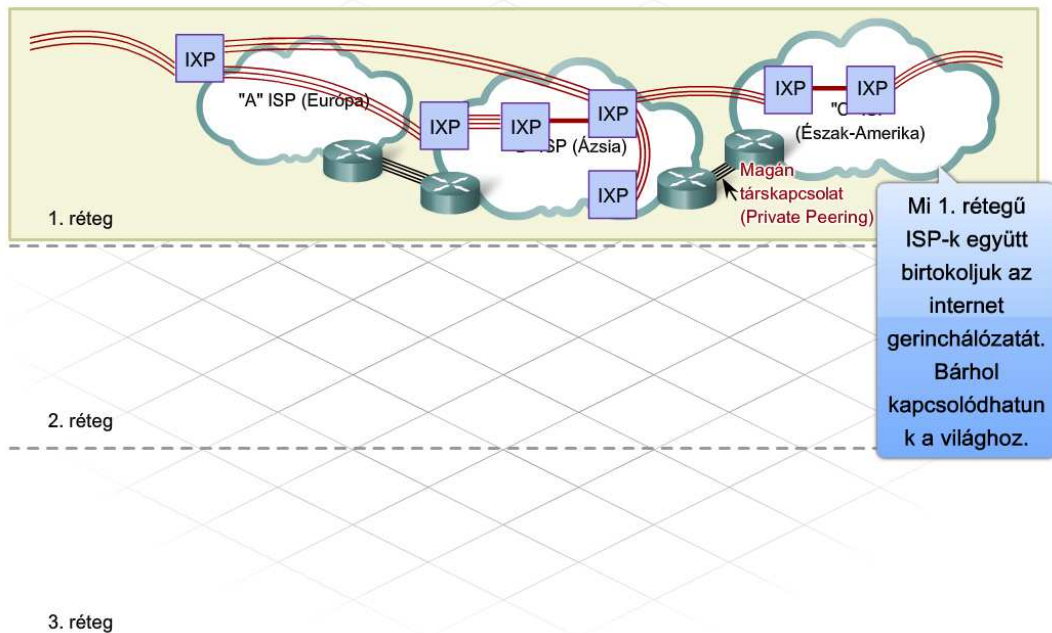


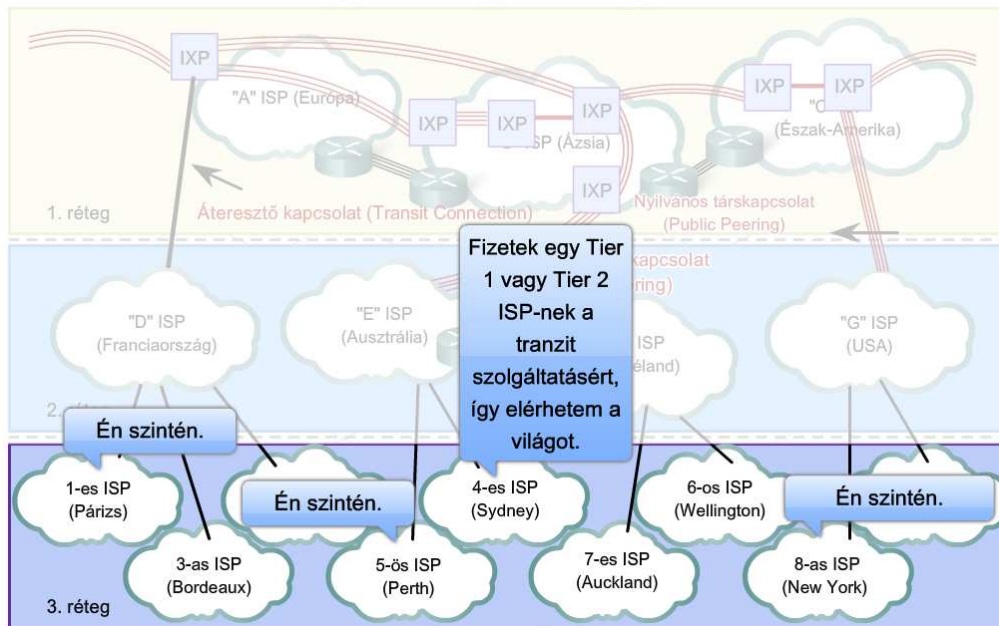
Az internetszolgáltatókat különböző osztályokba sorolják annak megfelelően, hogy hogyan érik el az internet gerinchálózatát.

- Az 1. rétegű (Tier 1) internetszolgáltatók a hierarchia csúcsát képezik. Az 1. rétegű internetszolgáltatók olyan óriásszervezetek, melyek magán társkapcsolaton keresztül kapcsolódnak egymáshoz, fizikailag összekötve az önnálló gerinchálózataikat, hogy egy globális internet-gerinchálózatot hozzanak létre. A saját hálózatukon belül ezek az 1. rétegű internetszolgáltatók saját forgalomirányítókkal, nagysebességű adatkapcsolatokkal és más olyan eszközökkel rendelkeznek, melyek lehetővé teszik számukra a többi 1. rétegű internetszolgáltatóhoz történő kapcsolódást. Ide tartoznak a kontinenseket összekötő, tengeralatti kábelek is.
- A 2. rétegű internetszolgáltatók a következő osztályt alkotják az internet gerinchálózatának elérésében. 2. rétegű ISP-k lehetnek nagyon nagyok, akár több országra is kiterjedők, bár igen kevésnek van egy egész földrészre kiterjedő, vagy kontinenseken átívelő hálózatuk. Vannak 2. rétegű internetszolgáltatók, akik, hogy az ügyfeleiknek globális internethozzáférést

biztosítsanak, fizetnek az 1. rétegű ISP-knek a forgalmuknak a világ más részei felé történő továbbításáért. Más 2. rétegű ISP-k a globális forgalmat kevésbé költséges magán társkapcsolatokon keresztül továbbítják más ISP-k felé. Egy hatalmas IXP egy központi fizikai helyszínen akár többszáz ISP-t is összehozhat azért, hogy több hálózathoz hozzáférjen egy megosztott csatlakozáson keresztül.

- A 3. rétegű internetszolgáltatók vannak legtávolabb a gerinchálózattól. 3. rétegű internetszolgáltatók általában nagyobb városokban találhatóak, és helyi internet elérést biztosítanak a felhasználóknak. 3. rétegű ISP-k fizetnek az 1 és 2. rétegű ISP-knek a globális internetelérésért és az internetszolgáltatásokért.





1.2.3 Az internet feltérképezéséhez használható eszközök

A hálózati eszközök segítségével az internetszolgáltatók hálózatainak csatlakozásairól és a kapcsolódási pontok elérési sebességéről kaphatunk információt.

A ping parancs egy megadott IP-cím elérhetőségét teszteli. A ping parancs egy ICMP (Internet Control Message Protocol) visszhangkérés csomagot küld a célállomásnak és várja, hogy a visszhangválasz csomagok megérkezzenek. Az ICMP a kommunikáció ellenőrzésére szolgáló internet protokoll. Méri a kérés-csomag elküldése és a válaszcsoport megérkezése között eltelt időt. A ping parancs kimenetéből leolvasható, hogy a válasz sikeresen megérkezett-e, valamint megmutatja az oda-vissza átviteli időt.

A ping használatához gépelje be a Cisco parancsoros felületén (CLI) a forgalomirányító vagy a Windows parancssor promptja után a következő parancsot:

ping <IP-cím>,

ahol az <IP-cím> a célállomás IP-címét jelöli.

Például: ping 192.168.30.1

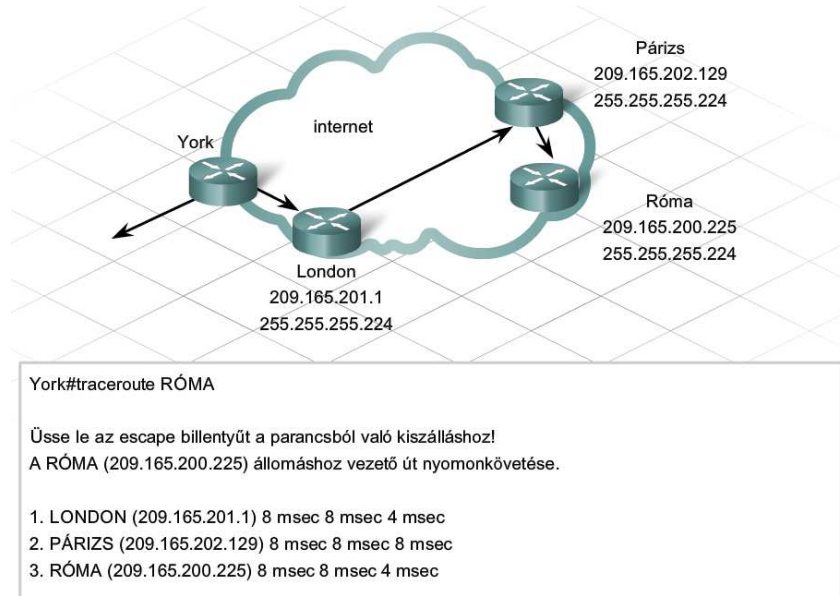
Ha a csomag nem éri el a célállomást, vagy a csomag útvonalán késés lép fel, hogyan határozható meg a probléma helye, illetve az, hogy mely forgalomirányítókra keresztül haladt a csomag?

A traceroute paranccsal egy csomagnak a forrástól a célállomásig tartó útvonala jeleníthető meg. Minden, a csomagtovábbításban résztvevő forgalomirányító egy ugrásnak (hop) felel meg. A traceroute parancs az útvonal egymás utáni ugrásait jeleníti meg és minden közbenső forgalomirányítónál kiszámolja, hogy mennyi idő telik el kérés elküldése és a válasz megérkezése között.

Ha probléma történik, használja a traceroute parancs kimenetét, hogy segítségével megállapíthassa, hol veszett el a csomag, vagy hol történik a késleltetés! A kimenetből az is leolvasható, hogy a

forrástól a célállomásig terjedő úton egy csomag mely internetszolgáltatók hálózatán utazik keresztül.

A Windows tracert parancsa hasonlóan működik. Számos vizuális nyomkövető (traceroute) program is létezik, melyek grafikusan is megjelenítik a csomag útját.



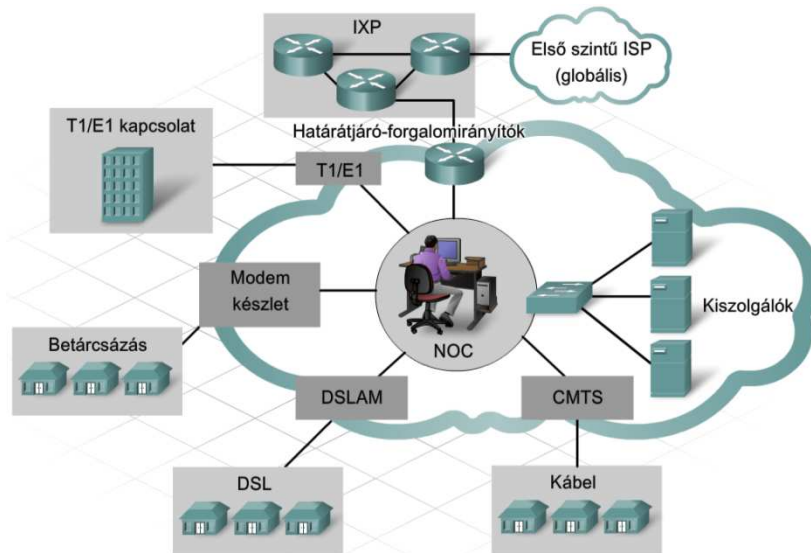
1.3 ISP kapcsolat

1.3.1 ISP követelmények

Egy internetszolgáltatónak számos különböző eszközzel kell rendelkeznie a felhasználók adatainak továbbításához és szolgáltatások nyújtásához. Ahhoz, hogy részt vegyen egy szállítási hálózatban, tudnia kell kapcsolódni más internetszolgáltatókhoz, illetve képesnek kell lennie nagymennyiségű adat kezelésére.

A következő eszközök szükségesek a szolgáltatások biztosításához:

- Elérési eszközök, melyek segítségével a felhasználók kapcsolódhatnak az internetszolgáltatóhoz. Ide tartoznak a DSL hozzáférési multiplexer (DSLAM - DSL Access Multiplexer) a DSL kapcsolathoz, a kábelmodem lezáró rendszer (CMTS - Cable Modem Termination System) a kábelmodemes kapcsolathoz, modemek a betárcsázáshoz és vezeték nélküli hidakra a vezeték nélküli kapcsolathoz.
- Határátjáró-forgalomirányítók, amelyek az internetszolgáltatók számára kapcsolódást és adatátvitelt biztosítanak más internetszolgáltatókhoz, internet-csatlakozási pontokhoz, ügyfél nagyvállalati hálózatokhoz.
- Kiszolgálók, melyek a levelezésért, a hálózati címfordításért, webes tárhelyért, FTP oldalakért és multimédia anyagok tárolásáért felelősek.
- Áramellátási berendezés tartalék tápegységekkel a folyamatos szolgáltatás biztosításához áramkimaradás esetén.
- Nagyteljesítményű légkondicionáló berendezések a folyamatosan ellenőrzött hőmérséklet biztosításához.



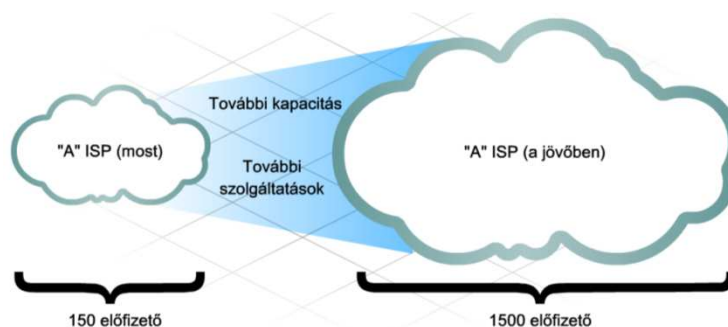
Az internetszolgáltatók más vállalatokhoz hasonlóan terjeszkedni szeretnének a bevételek növelése érdekében. A terjeszkedési képesség azon múlik, hogy tudnak-e újabb előfizetőt szerezni és több szolgáltatást értékesíteni. Azonban az előfizetők számának növekedésével az ISP hálózatának a forgalma is nő.

Végül, ez a megnövekedett forgalom túlterhelheti a hálózatot, ami a forgalomirányítók meghibásodásához, csomagvesztéshez és túlságosan nagy késleltetéshez vezethet. Egy túlterhelt hálózatban az előfizetők akár percekig is várhatnak egy weboldal letöltésére, sőt a hálózati kapcsolatot is elveszíthetik. Ezek a felhasználók választhatnak egy másik alkalmas ISP-t a jobb teljesítmény érdekében.

A felhasználók elvesztése azonban bevétel kieséssel jár, így az internetszolgáltatónak az az érdeke, hogy megbízható és skálázható hálózatot biztosítsanak.

A skálázhatóság a hálózat növekedésének képessége. Skálázható hálózatok gyorsan növekedhetnek újabb és újabb felhasználók és alkalmazások támogatására anélkül, hogy veszélyeztetnék a már létező felhasználóknak nyújtott szolgáltatások minőségét.

A skálázhatóságot leginkább támogató eszközök moduláris felépítésűek és a bővítésre szolgáló modulok beilleszthetősége érdekében bővítőhelyekkel rendelkeznek. A különböző modulok akár különböző számú interfésszel rendelkezhetnek. A moduláris forgalomirányítók (chassis router) megfelelő bővítő modulokkal többféle interfészt használhatnak, így többféle kapcsolat létesítésére is alkalmassá válnak.



1.3.2 Az ISP feladatai és kötelezettségei

Az ISP szervezetek több csoportból és részlegből állnak, amelyek felelősek a hálózat problémamentes működéséért és a szolgáltatások eléréséért.

A hálózati szolgáltatások a hálózat működtetésének minden összetevőjére kiterjednek, beleértve az új berendezések és vonalak megtervezését és kiépítését, új előfizetők felvételét, a hálózat javítását és karbantartását, illetve a felhasználók hálózati csatlakozásának üzemeltetését.

Amikor egy új vállalati előfizető ISP szolgáltatásokat igényel, a különböző szolgáltatásokat támogató csoportok együttes munkával biztosítják a megrendelés feldolgozásának kifogástalan folyamatát, valamint a szolgáltatásokhoz történő lehető leggyorsabb hozzáférést

Minden csoport saját feladatkörrel és kötelezettségekkel rendelkezik:

- A **vevőszolgálat** fogadja az előfizetők megrendeléseit és biztosítja, hogy a felhasználók különböző igényei pontosan kerüljenek be a rendeléseket nyomonkövető adatbázisba.
- A **tervezés és beszerzés** részleg megvizsgálja, hogy vajon az új előfizető rendelkezik-e meglévő hálózati berendezésekkel vagy újakat kell telepíteni.
- A **helyszíni telepítés (On-site Installation)** csoportja javaslatot tesz a szükséges felszerelés és vonal kiépítésére a felhasználói oldalon.
- A **hálózat üzemeltető központ (Network Operations Center, NOC)** felügyeli és teszteli az új kapcsolatot és biztosítja a megfelelő működést.
- Az **ügyfélszolgálatot** a NOC értesíti, amikor a vonal működőképes, majd kapcsolatba lép az ügyféllel, hogy segítse a jelszó és egyéb felhasználói paraméter beállításában.

1.4 A fejezet összefoglalása

- Számos vállalat használja az internetet e-kereskedelem, kommunikáció, együttműködés és továbbképzés céljából.
- A hálózati és internet szabványok biztosítják, hogy a hálózathoz csatlakozó minden eszköz egyazon szabályokat használjon, a szabványok létezése teszi lehetővé a különböző típusú eszközök kommunikációját az interneten keresztül.
- Függetlenül attól, hogy egy magánszemély vagy vállalat milyen eszköz segítségével szeretne kapcsolódni az internethez, az eszköznek internetszolgáltatón (ISP - Internet service provider) keresztül kell csatlakoznia.
- Az internet elérésén túl az internetszolgáltatók további szolgáltatásokat is nyújthatnak: eszköz tárolás (equipment co-location), webes és FTP tárhelyszolgáltatás (Web és FTP hosting), műszaki ügyfélszolgálat, hálózati hangátvitel, alkalmazások és média tárolás.



- A nagyobb vállalatoknak általában nagyobb sávszélesség és sebesség szükséges, mint például a T1/E1, T3/E3 és a Metro Ethernet.
- Az internetszolgáltató szolgáltatási pontjai (POP - Point of Presence) egy internetcsatlakozási ponthoz (IXP - Internet Exchange Point) csatlakoznak, ahol az ISP-k egymás hálózatához hozzáférhetnek és információt cserélhetnek.
- Az internet gerinchálózata különböző szervezetek tulajdonában levő hálózatokból áll, amelyek IXP-n vagy magán társkapcsolaton keresztül kapcsolódnak össze.
- Az ISP-k 1, 2 vagy 3 rétegű osztályozása a gerinchálózat elérése alapján történik.
- Egy internetszolgáltatónak a végfelhasználóktól jövő igények elfogadásához és szolgáltatások nyújtásához számos különböző eszközzel kell rendelkeznie, mint például az elérési eszközök, határátjáró-forgalomirányítók, nagyteljesítményű légkondicionáló és az áramellátást szabályozó berendezések.
- Az internetszolgáltató megbízható és skálázható hálózatot biztosít.
- Egy skálázható hálózat a meglévő teljesítmény veszélyeztetése nélkül képes gyorsan növekedni újabb felhasználók és alkalmazások támogatásához.
- Az internetszolgáltató szervezetek több csoportból és részlegből állnak, melyeknek együttes kötelezettsége a hálózat problémamentes működése.
- Ilyen hálózati szolgáltatást támogató csoportok: előfizetők kiszolgálásáért felelős csoport, NOC csoport, helyszíni telepítők, tervezési és beszerzési csoport és az ügyfélszolgálati csoport.

2. Ügyfélszolgálat

2.1 Ügyfélszolgálati szakemberek

2.1.1 Az internetszolgáltató ügyfélszolgálati szervezete

A helyi hálózat és az internetkapcsolat ma már a legtöbb vállalat üzleti tevékenységében komoly szerepet játszik. Ezért különösen fontos a hálózati hibák gyors elhárítása.

Az internetszolgáltató (Internet Service Provider – ISP) biztosítja az internetkapcsolatot a vállalkozások számára, és támogatást biztosít ügyfeleinek az internetkapcsolat zavarainak elhárításában. Ez a támogatás rendszerint kiterjed a felhasználó eszközeire is. Az internetszolgáltató támogatása általában az ügyfélszolgálaton (help desk) keresztül valósul meg. Ha van valami probléma az internetkapcsolattal vagy az elektronikus levelezéssel, az ügyfél először rendszerint az internetszolgáltató ügyfélszolgálatához fordul.

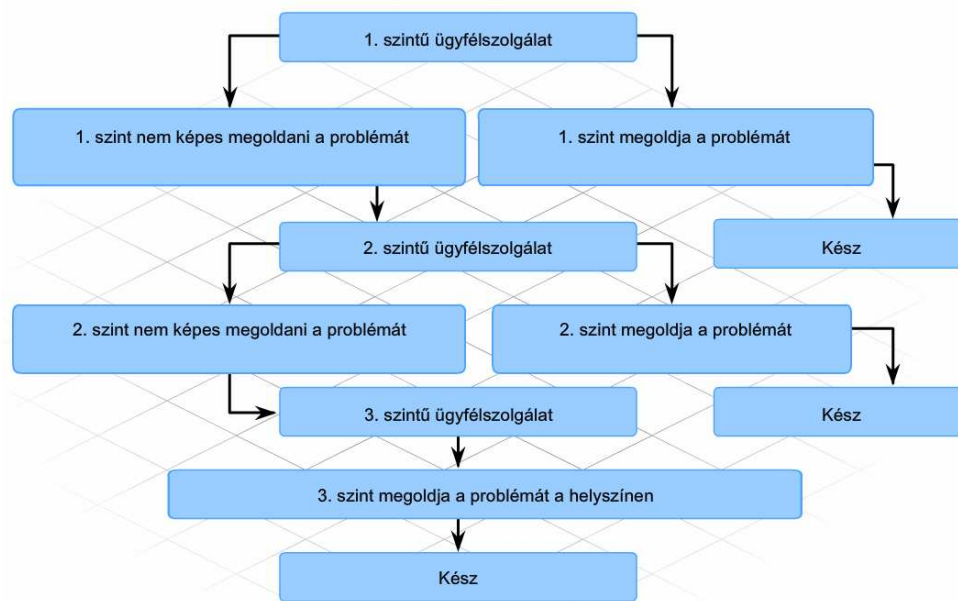
Az internetszolgáltató ügyfélszolgálati szakemberei kellő ismerettel és jártassággal rendelkeznek a problémák megoldásához, és biztosítják a felhasználók hálózati csatlakozását. Az ügyfélszolgálati szakemberek biztosítják a megoldást az ügyfelek problémáira, azzal a céllal, hogy optimalizálják a hálózat működését és megtartsák az ügyfeleket.

Egy jó ügyfélszolgálati csapat gyorsan elhárítja a hibákat az ügyfelek megalégedésére. Az internetszolgáltatásban igen nagy a verseny, ezért egy silány ügyfélszolgálat az ügyfelek elvesztését okozhatja.

Az internetszolgáltatónál rendszerint 3 szintű ügyféltámogatás van.

- szint: Közvetlen támogatás, amit rendszerint alacsonyabb beosztású ügyfélszolgálati szakemberek látnak el.
- szint: Ide kerülnek a tapasztaltabb ügyfélszolgálati szakemberek beavatkozását igénylő hívások.
- szint: Telefonon nem oldható meg a probléma, ki kell küldeni a helyszínre egy szakembert.

Az internet-szolgáltatókon kívül, sok más ágazatba tartozó közepes és nagy cég tart fenn ügyfélszolgálatot, vagy fogyasztóvédelmi csoportot. Az egyes szintek megnevezése természetesen eltérhet a fentiektől, de általában a három szintű struktúrát alkalmazzák. Az ügyfélszolgálat állhat egyetlen személyből, aki mindhárom szinten elvégzi a szükséges támogatást, de a szervezet nagyságától függően, akár egy minden részletre kiterjedő tevékenységet folytató hívásközpont is lehet, bonyolult telefonos berendezéssel és szabályokkal, amelyek meghatározzák, hogy melyik szint végezze a probléma megoldását. Van olyan internetszolgáltató és üzleti szervezet is, amelyik az 1. és 2. szintű támogatást egy másik, saját hívásközponttal rendelkező cégre bízta.



2.1.2 Az ügyfélszolgálati szakemberek feladatai

Amikor egy felhasználó először fordul az ügyfélszolgálatához, kérése rendszerint egy 1. szintű ügyfélszolgálati szakemberhez kerül. Az 1. szintű ügyfélszolgálat egy belépő szintű pozíció, ahol egy fiatal szakember értékes tapasztalatokat gyűjthet. Számos ügyfélkérést megold az 1. szintű ügyfélszolgálati szakember.

Azok a problémák, amelyeket nem tudtak megoldani, a 2. szintű ügyfélszolgálatához kerülnek, ahol jellemzően kevesebb szakember van. A 2. szintű ügyfélszolgálati szakember funkciói és kötelezettségei az 1. szintű ügyfélszolgálati szakemberéhez hasonlóak, azonban munkaköre nagyobb felkészültséget igényel. Ő a nagyobb kihívást jelentő, nagyobb tudást igénylő feladatokat oldja meg.

Az 1. szintű támogatással járó kötelezettségek:

- Az alapvető hálózati problémák megállapítása.
- A hardver-, szoftver- és rendszerhibák tüneteinek megállapítása és feljegyzése.
- A felhasználó által tapasztalt alapvető hibák megoldása és dokumentálása.
- A felhasználóknak nyújtott segítség azoknak az online űrlapoknak a kitöltésében, amelyek a különböző rendszerek, szolgáltatások, hardverek, szoftverek, jelentések és jogosultságok megszerzéséhez szükségesek.
- A megoldatlan feladatok eskalálása.

A 2. szintű támogatással járó kötelezettségek:

- A bonyolultabb hálózati hibák diagnosztizálása és elhárítása.
- Diagnosztikai eszközök és távoli megosztás alkalmazása a hibák azonosítására és elhárítására.
- Annak meghatározása, hogy mikor kell a hibajavításhoz a helyszínre küldeni egy szervizest.

Több nagyobb szolgáltató terjesztette ki tevékenységét felhasználói hálózatok helyszíni szervizelésére és menedzselésére. Ezeket általában felügyelt szolgáltatást nyújtó szolgáltatóknak Managed Service Providers (MSP) szokás nevezni. Ilyen szolgáltatást nyújthat az internetszolgáltató, a távközlési

szolgáltató vagy más számítástechnikai és számítógép-hálózati szervezet. Amikor az internetszolgáltató ilyenfajta szervizt vállal, munkatársai installálás és támogatás céljából gyakran keresik fel a felhasználót a telephelyén. Ez a 3. szintű támogatás.

A 3. szintű szolgáltatás gyakran van összhangban egy szolgáltatási szint megállapodással (Service Level Agreement – SLA). Az SLA olyan mint egy biztosítási kötvény, amely közvetítést vagy beavatkozást biztosít hálózati vagy számítógép hiba esetére.

A 3. szintű támogatás kötelezettségei:

- Olyan problémák felderítése és megoldása, amelyeket 1. és 2. szintű munkatársak adtak tovább.
- A hálózat állapotának szemléje vezető hálózati szakember általi elemzés céljából.
- Új eszközök telepítése és beállítása, szükség esetén beleértve a felhasználó oldali berendezések (CPE) újabbra való cseréjét is.

2.1.3 Tárgyalás az ügyféllel

Az ügyfélszolgálati szakember feladata, hogy telefonon, e-mail-ben, világhálón, on-line chat-en, de ha szükséges, akkor a helyszínen is nyújtson támogatást. Velük találkozik először a gyakran csalódott és nyugtalan ügyfél. Egy probléma megoldása során az ügyfélszolgálati szakember - a probléma pillanatnyi állását és elhárításának várható határidejét illetően - folyamatosan kaphat telefonhívásokat és leveleket.

A gyakori félbeszakítások ellenére az ügyfélszolgálati szakember tudjon a feladatra koncentrálni és egyszerre több problémát is tudjon hatékonyan és pontosan kezelni. Ilyen körülmények között elég nehéz dolog következetesen fenntartani a pozitív hozzáállást, és színvonalas szolgáltatást nyújtani. Az ügyfélszolgálati szakembernek kiváló kapcsolatteremtő és hatásos kommunikációs készséggel kell rendelkeznie, mind a szóbeli mind pedig az írásbeli kapcsolatot illetően. Az ügyfélszolgálati szakembertől elvárják, hogy tudjon önállóan dolgozni, de elengedhetetlen az is, hogy képes legyen a csoportmunkára is.

Fontos, hogy az ügyfélszolgálati szakember rátermetten, gyorsan és szakszerűen kezelje a felhasználók kéréseit. Az ügyfélszolgálati szakember a vállalat ügyfélszolgálati filozófiájával összhangban dolgozzon. Az ügyfélszolgálati filozófia egy etikai norma, mely áthatja az egész vállalatot a csúcavezetéstől a beosztottakig.

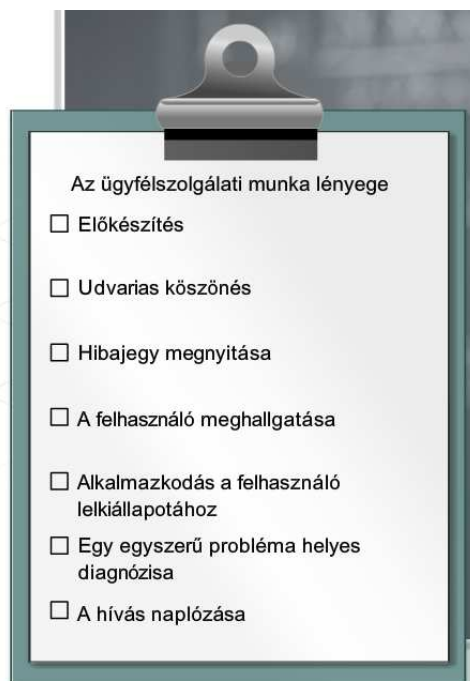
Ha az ügyfélszolgálati szakember hibabejelentő hívást kap, mindig egy alapvető hibaelhárítási folyamatot kell, hogy kövessen. A hibaelhárítás a „hibajegy” kiállítását és a hibaelhárító stratégia követését foglalja magában. A probléma-megoldó technika a hibaelhárítási folyamatára használatát, a hiba helyének behatárolására szolgáló kérdéssorozatot űrlapot, valamint a megfelelő hibajegy-továbbítási (eszkálálási) eljárások kezelését tartalmazza.

Az ügyfélszolgálati szakember a hibajegyen vezetett feljegyzések segítségével gyűjti össze a felhasználónál jelentkező hibára vonatkozó adatokat és írja le a hiba elhárításával kapcsolatos fontos tényeket.

Műszaki képességein felül az ügyfélszolgálati szakember üdvözlje barátságosan a hozzá forduló felhasználót, s az egész hívás során során tanúsítson hozzáértést és érdeklődést.

Nehéz ügyfelek és bonyolult problémák esetén különösen fontos az ügyfélszolgálat szerepe és a kapcsolatteremtési képességek megléte. Az ügyfélszolgálati szakembernek tudnia kell, hogyan oldja az ügyfél feszültségét, és hogyan válaszoljon az esetleg goromba ügyfélnek a hibaelhárítási folyamat során.

A hibajegy-indítás és ezzel az információ naplózása kritikus fontosságú az ügyfélszolgálati tevékenység szempontjából. Ha ugyanazzal a hibával vagy ugyanolyan hibajelenségekkel kapcsolatosan több hívás fut be a vevőszolgálathoz, nagy segítséget jelent annak ismerete, hogy miként oldották meg az adott problémát korábban. Ez azért is fontos, hogy az ügyfélszolgálati szakember közölhesse az ügyféllel, hogy mit is tesznek most éppen a probléma-elhárítás érdekében. A nyitott hibajegy kellőképpen jó információ segítséget nyújt abban, hogy a pontos állapotról tájékoztathassuk mind az ügyfelet, mind pedig az ISP többi dolgozóját.



Amellett, hogy sok problémát távolról lehet kezelni, az is előfordul, hogy installálás és az eszközök vizsgálata céljából helyszíni beavatkozás szükséges a hiba elhárításához. Amikor egy ügyfélszolgálati szakember kiszáll az ügyfélhez, akkor fontos, hogy professzionálisan képviselje szervezetét. Egy szakember képes arra, hogy a szaktudása tekintetében bizalmat ébresszen az ügyfélben.

Az első látogatás alkalmával fontos, hogy az ügyfélszolgálati szakember jó benyomást keltsen az ügyfélben. Személyes ápoltsága és öltözködése az, amit az ügyfél először észrevesz. Ha az első benyomás rossz, nagyon nehéz azt megváltoztatni, és az ügyfél bizalmát visszanyerni. Számos munkaadó egyenruhát biztosít a helyszínen megjelenő szakemberei számára, vagy előírja az öltözködésük módját.

Az ügyfélszolgálati szakember hozzáállása és nyelvhasználata alapján is megítélik azt a szervezetet, amelyet a munkatárs képvisel. Egy ügyfél nyugtalankodhat egy új berendezés használhatósága miatt.

Miközben az ügyféllel beszél, az ügyfélszolgálati szakember legyen udvarias és tisztelettudó. Válaszoljon az ügyfél valamennyi kérdésére. Ha az ügyfél kérdésére nem tud válaszolni, vagy ha további információra van szükség, jegyezze fel az ügyfél kérdését, és amint lehet, válaszoljon.

2.2 Az OSI modell

2.2.1 Az OSI modell használata

Amikor egy hálózati kapcsolat hibáját jelzik az ügyfélszolgálatnak, többféle módszer létezik a hiba behatárolására. A rétegzett hálózati modell használata egy ilyen tipikusan használható módszer. A rétegzett megközelítés megkívánja a vevőszolgálati szakembertől, hogy legyen jártas a hálózaton kialakuló folyamatokban. Ilyenek: az üzenet létrehozása, kézbesítése és értelmezése a hálózati eszközökben és a munkaállomásokban.

A hálózaton kialakuló adatmozgást legjobban a hétrétegű (Open Systems Interconnection – OSI) modell szemlélteti. Az OSI modell több részfolyamatra bontja a hálózati adatáramlást. Mindegyik folyamat a nagyobb feladat egy részlete.

Például egy járműveket gyártó üzemben sem egy személy szerel össze egy járművet. Inkább állomásról - állomásra mozgatják a járművet, miközben az egyes elemeket az arra szakosodott csoportok beszerelik. A jármű összeszerelésének összetett feladatát szétbontják könnyebben elvégezhető, logikus feladatokra. Ez az eljárás a hibaelhárítást is megkönnyíti. Amikor a gyártási folyamatban keletkezik egy hiba, be lehet határolni azt a helyet, ahol a hiba létrejött, és aztán azt ki lehet javítani.

Hasonlóképpen az OSI modell segítségével a hibásan működő rétegre lehet koncentrálni, és a hibát meg lehet szüntetni.



(Az ábráról bővebben az első. szemeszter anyagában.)

Az OSI modell hét rétegét két részre osztjuk: felső rétegekre és alsó rétegekre.

A felső réteg kifejezéssel néha, az OSI modell szállítási réteg feletti, bármelyik rétegét jelölhetik. A felső rétegek tipikusan az alkalmazásokkal foglalkoznak, és általában szoftveresen valósulnak meg. A legfelső, az alkalmazási réteg, ez van legközelebb a végfelhasználóhoz.

Az alsó réteg kifejezéssel az OSI modell viszony (együttműködési) réteg alatti rétegeit jelölik. Az adatszállítást az alsó rétegek összetett működése kezeli. A fizikai és az adatkapcsolati réteget hardveresen és szoftveresen is meg kell valósítani. A fizikai réteg van legközelebb a hálózati adatátvivő közegehez, vagy a kábelezéshez. A fizikai réteg adja át az információt az adatátviteli közegeknek.

A végkészülékek mint a szerver, vagy a kliens, általában mind a hét réteget használják. A hálózati eszközök csak az alacsonyabb rétegekben működnek. Hubok csak az 1. rétegben, a kapcsolók (switches) az 1. és 2. rétegben, a forgalomirányítók (routers) az 1. 2. és 3. rétegben, a tűzfalak (firewalls) az 1. 2. 3. és 4. rétegben.

Csoport	#	A réteg neve	Tipikus protokollok és technológiák	A réteg tipikus hálózati komponensei
Felső rétegek	7	Alkalmazás	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Hálózaton futó alkalmazások, e-mail, web-böngészők és -szerverek, fájl átvitel, névfeloldás
	6	Megjelenítési	SSL, shell-ek és átirányítók, MIME	
	5	Viszony	NetBIOS, alkalmazási program-illesztés (API), távoli eljárshívások	
Alsó rétegek	4	Szállítási	TCP és UDP	A lejátszással egyidejű videó- és hangletöltési mechanizmusok, tűzfalak szűrőlistái
	3	Hálózati	IPv4, IPv6, IP NAT	IP-címzés, forgalomirányítás
	2	Adatkapcsolati	Ethernet család, WLAN, Wi-Fi, ATM, PPP	Hálózati kártyák és meghajtók, hálózati kapcsolók, WAN kapcsolat
	1	Fizikai	Elektromos jelfeldolgozás, fényhullám minta, rádióhullám minta	Fizikai közegek, (réz csavart érpár, üvegszálas optikai kábel, vezeték nélküli átjátszók), hubok és ismétlők.

2.2.2 OSI modell protokollok és technológiák

Mikor az OSI modellt hibaelhárító eszközként alkalmazzuk, fontos tudni azt, hogy az egyes rétegekben melyik funkció valósul meg, és hogy a funkció megvalósítása közben milyen hálózati információt ér el az adott eszköz, vagy szoftver. Például ahhoz, hogy egy elektronikus levél eljusson a kientstől a szerverig, számos eljárásnak kell megvalósulni. Az OSI modell az e-mail küldését és fogadását felosztja kisebb elkülönített lépésekre a hét rétegnek megfelelően.

1. lépés: A felsőbb rétegek elkészítik az adatot.

Amikor a felhasználó egy alfa-numerikus karaktereket tartalmazó e-mail üzenetet küld, azt olyan adatokká kell konvertálni, amelyeket a hálózaton lehet továbbítani. A 7., 6., és 5. réteg felel azért, hogy az üzenet olyan formájú legyen, amelyet a célállomáson futó alkalmazás megért. Ez az eljárás a kódolás. Ez után a felsőbb rétegek átadják a kódolt üzenetet az alsóbb rétegeknek, hogy azok továbbítsák azt a hálózaton keresztül. A felhasználó által nyújtott konfigurációs információ alapján kell az e-mailt a megfelelő szerverre továbbítani. Az alkalmazási rétegnél előforduló hibák gyakran a felhasználói szoftverprogramok konfigurációjában rejlő hibákkal kapcsolatosak.

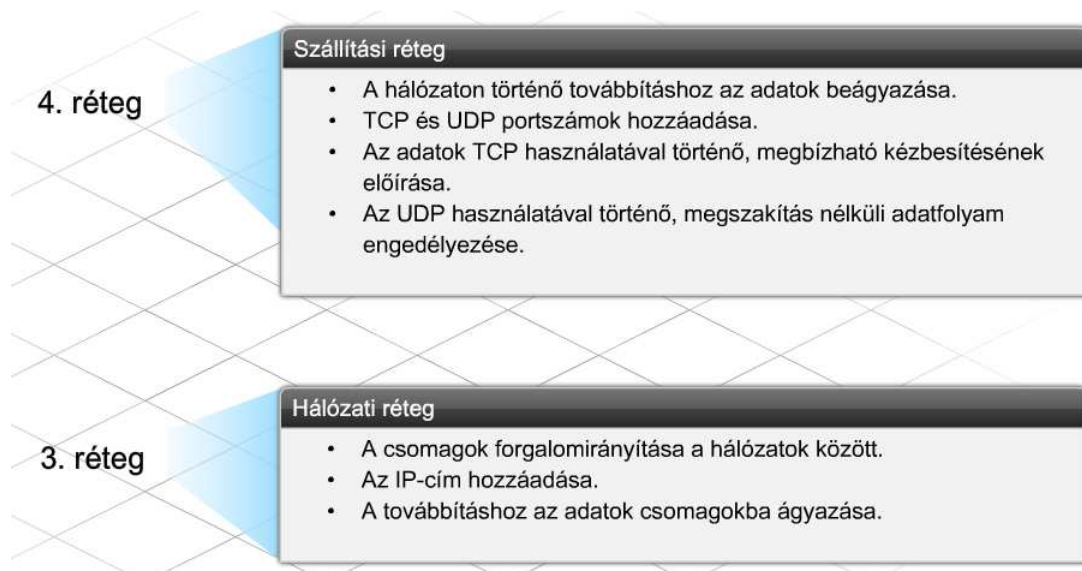


2. lépés: A 4. réteg az adatokat (üzenetet) a végponttól végpontig történő szállításhoz beágyazza.

Az e-mail üzenet tartalmát képező adatokat a 4. réteg a hálózati továbbítás céljából becsomagolja. A 4. réteg kisebb darabokra, úgynevezett szegmensekre bontja az üzenetet és olyan fejléccel látja el ezeket, amelyek magukban foglalják az alkalmazási rétegben működő végpontokat azonosító TCP vagy UDP, portszámokat is. Emellett a 4. rétegbeli fejléc azt is jelzi, hogy az adott szegmens milyen szállítási réteg-szolgáltatás típust használ. Az e-mail alkalmazás például TCP szállítási réteg-szolgáltatást használ, ezért e-mail szegmensek megérkezését a célállomás nyugtázza. A 4. réteg funkcióit a forrás- és a cél-állomáson futó szoftver valósítja meg. Mivel a tűzfalak a forgalom szűrésére gyakran használják a TCP és UDP port-számokat ezért a 4. réteg problémáit a helytelenül beállított tűzfal szűrő-lista is okozhatja.

3. lépés: A 3. réteg hozzáadja az IP-cím információt.

A szállítási rétegtől kapott szegmenseket a 3. réteg a forrás- és a célállomás hálózati IP-címét is magában foglaló 3. rétegbeli (IP) fejléccel egészíti ki, IP csomagokba ágyazza. A csomag cél-IP címét a forgalomirányítók arra használják, hogy a csomagot a hálózat legmegfelelőbb útvonalán továbbítsák. A forrás- vagy célállomás hibásan beállított IP-címe 3. rétegbeli működési hibát idézhet elő. Mivel az IP-címet a forgalomirányítók is használják, a forgalomirányítóban lévő hibás konfiguráció is okozhat 3. rétegbeli hibát.

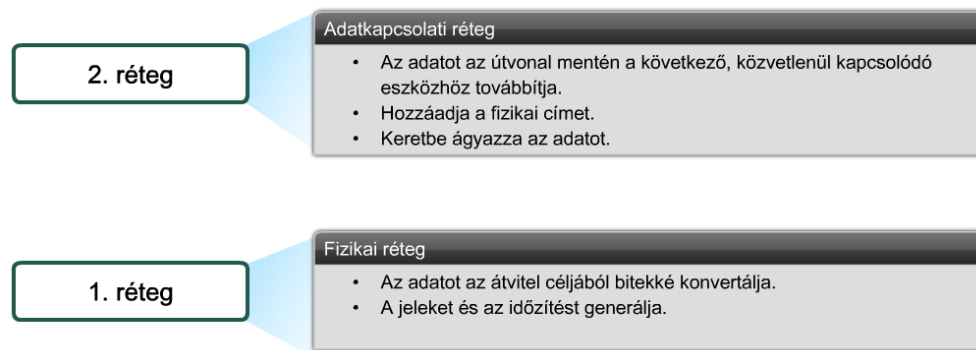
**4. lépés: A 2. réteg hozzáadja a keret fej- és láblécét.**

A hálózati egységek mindegyike a forrástól a célig, beleértve a küldő állomást is, a csomagot keretbe ágyazza. A keret-fejléc tartalmazza a közvetlenül csatlakozó adatvonalon át elérhető hálózati egység fizikai (Media Access Control - MAC) címét. A kiválasztott hálózati útvonalon minden hálózati egység újrakeretezi a csomagot, úgy, hogy az a következő közvetlenül csatlakozó adatvonalon át eljuthasson a következő hálózati egységhez. A keretekben található információt a kapcsolók és a hálózati kártyák használják fel arra, hogy az üzenet a megfelelő célállomáshoz kerülhessen. A hibás hálózati kártya, a nem megfelelő kártya-meghajtó és a kapcsolók hardverhibái 2. rétegbeli hibát okozhatnak.

5. lépés: Az 1. réteg alakítja át az adatot átvihető bitekké.

Az adatátviteli közegen való továbbításhoz a keretet 1-ekből és 0-ákból (bitek) álló sorozattá alakítják át. Egy szinkronizáló funkció teszi lehetővé, hogy az egységek a közegen való áthaladásuk során meg tudják különböztetni az egyes biteket. A forrástól a célig vezető útvonal mentén az átviteli közeg változhat. Például: egy e-mail üzenet származhat eredetileg egy Ethernet LAN hálózathoz, majd áthaladhat a campus üvegszálalás gerincén és egy soros WAN kapcsolaton, végül egy Ethernet LAN hálózaton célba érhet. Az 1. rétegben hibát okozhat a laza vagy hibás kábelezés, a hibás hálózati kártya, vagy valamilyen elektromos zavar.

A vevő állomáson a fenti lépések az 1. lépéstől az 5. lépésig fordított sorrendben megismétlődnek, ahogy az üzenet a rétegeken áthaladva elér a megfelelő alkalmazáshoz.



2.2.3 Hibakeresés az OSI modellel

Elméleti modellként az OSI modell meghatározza a protokollokat, hardver és egyéb előírásokat, amelyek a hét rétegnél működnek.

A hétrétegű OSI modell ugyanakkor a hálózati hibaelhárításhoz is biztosít egy szisztematikus alapot. Bármilyen hibaelhárítási forgatókönyvben, az alapvető probléma-megoldó eljárás a következő lépéseket tartalmazza:

1. A probléma azonosítása.
2. A probléma okának körülhatárolása.
3. A hiba elhárítása.
 - Az alternatív megoldások megkeresése és prioritási sorba állítása.
 - Egy alternatív megoldás kiválasztása.
 - A kiválasztott megoldás megvalósítása.
 - A megoldás kiértékelése.

Ha a kiválasztott megoldás nem oldotta meg a problémát, vissza kell vonni a változtatásokat, és át kell térni a következő lehetséges megoldásra! A lépéseket addig kell ismételni, míg egy megoldás működni nem fog!

Az alapvető probléma-megoldási eljáráson felül, a hétrétegű referenciamodell hibaelhárítási irányelvként is használható. Rétegelt modell használata esetén az ügyfélszolgálati szakember három különböző megközelítéssel határozhatja be a hiba helyét:

- **Bottom - Up** – Az alulról felfelé megközelítés a hálózat fizikai összetevőinél kezdi a hibakeresést, majd felfelé halad az OSI modell rétegein. Az alulról felfelé eljárás a fizikai hiba gyanúja esetén a hibaelhárítás hatékony eszköze.
- **Top – Down** – A felülről lefelé megközelítés az alkalmazásoknál kezdi a hibakeresést, ezután lefelé halad az OSI modell rétegein. Ez a megközelítés abból indul ki, hogy a probléma az alkalmazásnál van, nem a hálózati infrastruktúrában.
- **Divide-and-Conquer** – Az oszd meg és uralkodj megközelítést általában a tapasztaltabb ügyfélszolgálati szakemberek alkalmazzák. Megcélazzák azt a réteget, amelyekben a hibát feltételezik, majd ez alapján folytatják a hibakeresést felfelé, vagy lefelé haladva az OSI modell rétegein.

Az OSI modellt útmutatóként alkalmazva az ügyfélszolgálati szakember kérdéseket intézhet a felhasználóhoz a hiba meghatározására és az okának felderítésére.



Az ügyfélszolgálati szakembernek rendszerint van egy általános ellenőrző listája vagy forgatókönyve, amit a hiba feltárása során követ. A leírás gyakran az alulról felfelé megközelítésen alapul. Ennek oka az, hogy a fizikai hibákat rendszerint könnyebb diagnosztizálni és javítani, az alulról felfelé megközelítés pedig a fizikai réteggel kezd.

1. réteg hibakeresése

Az ügyfélszolgálati szakember az 1. rétegre vonatkozó kérdésekkel kezd. Emlékezzünk arra, hogy az 1. réteg a hálózati eszközök fizikai kapcsolataival foglalkozik. Az 1. réteg hibái gyakran a kábelezés és az elektromosság hibáiból adódnak, és ezek nagyon sok ügyfélszolgálati hívást eredményeznek. Néhány a gyakoribb fizikai réteg hibákból:

- Az egység ki van kapcsolva
- Az egység tápkábelét kihúzták
- Hibás a hálózati kábel csatlakozója
- Hibás a kábel típusa
- Hibás a hálózati kábel
- Hibás a vezeték nélküli hozzáférési pont
- Helytelen a vezeték nélküli beállítás, mint például az SSID

Az 1. réteg hibakeresésénél először ellenőrizzük le, hogy minden egységnél meg van-e a megfelelő elektromos tápellátás, valamint, hogy az egységek be vannak-e kapcsolva. Ez ugyan nyilvánvaló dolognak tűnik, de a hibát bejelentő személy gyakran átsiklik ezen valamilyen olyan egység esetében, mely a forrástól a célig tartó útvonal mentén helyezkedik el. Ha vannak állapotjelző LED-ek, ellenőriztessük a felhasználóval, hogy helyesen jeleznek-e. A helyszíni munka során szemrevételezéssel ellenőrizzük az egész kábelezést, és a kábelek újracsatlakoztatásával biztosítjuk a megfelelő kapcsolatot. Ha vezeték nélküli eléréssel van probléma, ellenőrizzük le, hogy a vezeték nélküli elérési pont működik-e, valamint helyes-e az egység konfigurációja.

Amikor távoli hibaelhárítást végez az ügyfélszolgálati szakember, minden lépésnél meg kell mondani a felhasználónak, hogy mit keressen, és mit tegyen a hiba elhárítására. Ha megállapítást nyert, hogy az összes 1. rétegre vonatkozó kérdést megbeszélték, tovább kell lépni az OSI modell 2. rétegére.

A 2. réteg hibakeresése

A hálózati kapcsolók és az állomások hálózati kártyái (NIC) 2. rétegbeli feladatokat látnak el. A 2. rétegben hibát okozhat a hibás berendezés, a helytelen eszközmeghajtó vagy a nem megfelelően konfigurált kapcsoló. Mikor távoli hibakeresést hajtunk végre, komplikált lehet a 2. réteg hibájának behatárolása.

Egy helyszíni ügyfélszolgálati szakember ellenőrizni tudja, vajon helyesen van-e konfigurálva, és megfelelően működik-e a hálózati kártya. A hálózati kártya újra bedugása, vagy a hibásnak feltételezett kártya kicserélése egy biztosan hibátlan kártyára, segíthet a hiba behatárolásában. Bármely hálózati kapcsolón (switch) hajtjuk végre ugyanez az eljárást végezhető el.

A 3. réteg hibakeresése

A 3. rétegben az ügyfélszolgálati szakembernek a hálózaton használt logikai címezést kell felderíteni, mint amilyen az IP-címzés. Ha a hálózat IP-címzést használ, ellenőrizni kell az egységek helyes beállítását, például a következőket.

- Az IP-cím a kijelölt hálózaton belül van-e?
- Helyes-e az álhálózati maszk?
- Helyes-e az alapértelmezett átjáró?
- Egyéb szükséges beállítások, mint a DHCP vagy a DNS.

A 3. réteg hibakeresésében számos segítség áll rendelkezésre. Íme három, a leggyakrabban használt parancssori eszközök közül:

ipconfig – megmutatja a számítógép IP beállításait

ping – ellenőrzi a hálózati kapcsolatot

tracert – ellenőrzi a forgalomirányítási útvonalat a forrástól a célállomásig

A legtöbb hálózati probléma megoldható az 1. 2. és 3. rétegek fenti hibakeresési technikáinak alkalmazásával.

A 4. réteg hibakeresése

Amennyiben az 1. rétegtől a 3. rétegig valamennyi normálisan működik, és a ping sikeresen elmegy a távoli szerverig, itt az ideje, hogy a magasabb rétegeket ellenőrizzük. Például, ha az útvonalon tűzfal van, fontos ellenőrizni azt, hogy az alkalmazás TCP vagy UDP portja nyitva van-e és, hogy a tűzfal szűrőlistája nem blokkolja-e a port forgalmát.

Az 5. rétegtől a 7. rétegig való hibakeresés.

Az ügyfélszolgálati szakembernek az alkalmazások konfigurációját is ellenőrizni kell. Például, ha egy e-mail hibát keresünk, ellenőrizni kell hogy a küldő és a fogadó szerverre vonatkozó információk helyesek-e. Azt szintén ellenőrizni kell, hogy a tartománynév feloldása az elvárt módon működik-e.

Távoli ügyfélszolgálati szakemberek, a magasabb rétegek hibáit más hálózati segédeszközökkel is ellenőrizhetik, egy packet sniffer-el a teljes hálózati forgalom ellenőrizhető. Egy olyan hálózati alkalmazás mint a Telnet szintén felhasználható a konfiguráció ellenőrzésére.

2.3 ISP hibaelhárítás

2.3.1 Ügyfélszolgálati hibaelhárítási forgatókönyv

Az ügyfélszolgálatához érkező hívások mennyisége és fajtája nagyon változatos lehet. A leggyakoribb hívások egy része e-mail-ekkel, az állomás-konfigurációval és a hálózati csatlakozással függ össze.

E-mail kérdések

- Fogadni tud, de küldeni nem
- Küldeni tud, de fogadni nem
- Sem küldeni nem tud, sem fogadni nem tud
- Senki sem tud válaszolni az üzenetekre

Számos e-mail probléma közös oka a rossz POP, IMAP, vagy SMTP szerver név. A legjobb az, ha ellenőriztetik az e-mail adminisztrátorral a pontos POP, vagy IMAP és az SMTP szerver nevét. Néha azonos a POP/IMAP és SMTP szerver név. Azt is ellenőrizni kell, hogy helyes-e a felhasználói név és a jelszó. Mivel a jelszó nem jelenik meg a képernyőn, célszerű a gondos újra belépés.

Mikor ezen kérdések telefonon keresztül hibaelhárítását végezzük, fontos, hogy az ügyfél körültekintően haladjon végig a konfigurációs paramétereken. Sok ügyfél számára ismeretlen a terminológia, és idegenek a konfigurációs adatok. Amennyiben lehetséges, egy távoli menedzsment szoftverrel csatlakozzunk az ügyfél készülékéhez. Ez lehetővé teszi, hogy az ügyfélszolgálati szakember végezze el az ügyfél számára szükséges lépéseket.

Állomás-konfigurációs kérdések

Egy tipikus probléma, hogy a helytelenül beállított állomáscím-információ megakadályozza az internethez vagy más hálózati erőforráshoz való csatlakozást. Ez következik be, ha hibás az IP-cím, az alhálózati maszk vagy az alapértelmezett átjáró.

Olyan környezetben, ahol az IP-cím információkat kézzel adják meg, lehetséges, hogy egyszerűen az IP-cím konfiguráció begépelése hibás. Olyan környezetben, ahol az állomás dinamikusan kapja az IP-címet egy kinevezett szervertől, mint amilyen a DHCP szerver, a szerver elromolhat vagy hálózati hiba következtében elérhetetlenné válhat.

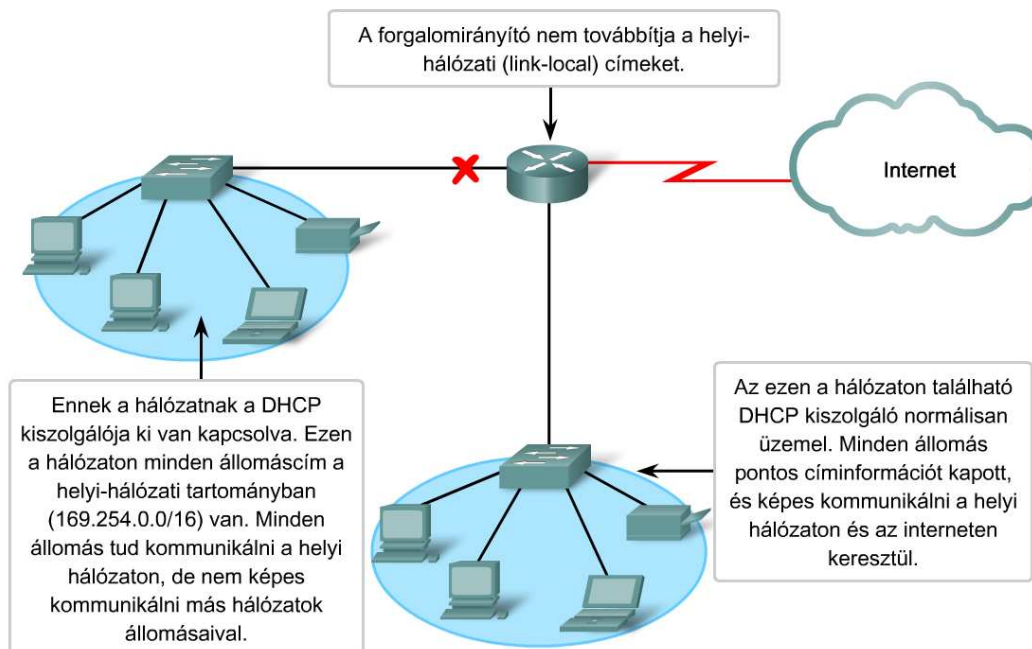
Amikor egy állomás dinamikus IP-cím fogadásra van konfigurálva, de a címkiosztó szerver elérhetetlen vagy hozzáférhetetlen, akkor az operációs rendszer automatikusan generál az állomás számára egy speciális (link-local) helyi-hálózati címet. Az IPv4 címeket a 169.254.0.1-től

169.254.255.254-ig terjedő címblokkban (169.254.0.0/16) adatkapcsolati szinten helyi (link-local) címnek nevezik. Az állomás operációs rendszere a címet véletlenszerűen adja ki a 169.254.0.0/16 címtartományban. De mi akadályozza meg azt, hogy két állomás ugyanazt a címet válassza?

Amikor az operációs rendszer generál egy ilyen címet, akkor küld egy ARP kérést ezzel a címmel a hálózatra, és megnézi, hogy használja-e valamelyik eszköz ezt a címet. Ha válasz nincs, akkor a címet az eszközhöz rendeli, egyébként másik IP-címet választ, és az ARP kérést megismétli. Microsoft hivatkozásokban ez az önműködő privát IP-címzés (Automatic Private IP Addressing – APIPA).

Ha ugyanazon a hálózaton több állomás kapott ilyen automatikusan kiosztott címet, akkor a kliens/szerver és a peer-to-peer alkalmazások az ilyen állomások között rendben működnek. Mivel az így kiosztott cím a B osztályú privát címtartományban van, a helyi hálózaton kívül nem működik a kapcsolat.

Amikor dinamikusan és manuálisan konfigurált állomások között keresünk hibát, használjuk az `ipconfig /all` parancsot annak ellenőrzésére, hogy az állomás megfelelő IP konfigurációt használ-e.



A felhasználói kapcsolódás kérdései

A kapcsolódási problémák az új felhasználók körében a fordulnak elő leggyakrabban az első csatlakozás idején. Előfordul meglevő felhasználók kapcsolati hibája is. Először kapcsolódó felhasználóknál gondot okozhat a hardver és a szoftver helytelen konfigurációja. Meglevő felhasználók akkor jelzik a kapcsolati hibákat, mikor nem tudnak megnyitni egy weboldalt, nem tudnak e-mailt vagy üzenetet küldeni, vagy fogadni.

Sok oka lehet annak, hogy a felhasználó nem tud kapcsolódni, beleértve az alábbiakat is:

A szolgáltatások kifizetésének elmulasztása

- Hardver hibák
- Fizikai réteg hibái

- Helytelenül beállított alkalmazások
- Hiányzó alkalmazási bővítmény-modulok
- Hiányzó alkalmazások

Sok esetben a hibát egy elromlott vagy rossz helyre dugott kábel okozza. Az ilyen hiba elhárítható a kábel-kapcsolat ellenőrzésével vagy a kábel cseréjével.

Másfajta, mint például a szoftver hibát, sokkal bonyolultabb behatárolni. Egy ilyen példa: A hibásan betöltött TCP/IP készlet megakadályozza az IP helyes működését. A TCP/IP készlet ellenőrizhető a visszacsatolási cím használatával. A visszacsatolási cím egy speciális IP-cím. Az IPv4 rendszerben erre a célra fenntartott cím: 127.0.0.1, melyen az állomás közvetlenül önmagával forgalmaz. A visszacsatolási hurok rövidre zárja a TCP/IP alkalmazások és szolgálatok közötti kommunikációt egy eszközön belül.

A saját állomás TCP/IP beállítása ellenőrizhető a ping 127.0.0.1 parancs kiadásával. Ha nem érkezik válasz a visszacsatolási cím pingelésére, akkor a hiba oka a TCP/IP készlet beállítása vagy installálása lehet.

A 127.0.0.1–től a 127.255.255.254–ig terjedő címtartomány az ellenőrzések céljára van fenntartva. Ezen belül minden cím visszacsatol, az adott helyi állomáson van. A fenti tartományon belüli cím sohasem jelenhet meg a hálózaton. Annak ellenére, hogy a 127.0.0.0/8 tartomány van fenntartva a visszacsatolós ellenőrzésre, jellemzően csak a 127.0.0.1 címet használjuk.

2.3.2 Ügyfélszolgálati feljegyzések készítése és alkalmazása

Amikor az 1. szintű ügyfélszolgálati szakemberhez befut egy ügyfélkérelem, azonnal megkezdődik az információ-gyűjtés. A híváshoz tartozó információk tárolására és visszakeresésére egy speciális rendszer szolgál. Nagyon fontos a pontos adatgyűjtés abban az esetben, amikor 2. szintű ügyfélszolgálati szakember igénybevétele, vagy helyszíni látogatás szükséges.

Az információ-gyűjtő és rögzítő eljárás abban a pillanatban indul, amikor az ügyfélszolgálati szakember válaszol a telefonban. Amikor a felhasználó azonosítja önmagát, az ügyfélszolgálati szakember hozzáfér a hozzá tartozó felhasználói információkhoz. A felhasználói információk menedzseléséhez adatbázis kezelőt szoktak használni.

Az információ átkerül egy hibajegyre, vagy egy incidensjelentésre. Ez a dokumentum lehet egy papírlap egy papíralapú eseménykövető rendszerben vagy egy bejegyzés egy elektronikus adattároló rendszerben, mely az elejétől a végéig kíséri a hibaelhárítási folyamatot. A probléma megoldásán dolgozó valamennyi munkatárs feljegyzi a hibajegyre azt, amit az ügyel kapcsolatban elvégzett. Amikor helyszíni beavatkozás szükséges, a hibajegyen lévő információk egy munkalappá alakíthatók, amit a helyszínre látogató ügyfélszolgálati szakember magával vihet.

A probléma megoldása után, dokumentálni kell a tevékenységet a hibajegyen vagy a munkalapon és az ismeretbázis dokumentumban is. Ez a később előforduló, hasonló hibák elhárítását segítheti.

Időnként az 1. szintű ügyfélszolgálati szakember olyan hívást kap, amely nem oldható meg gyorsan. Az ő felelőssége az, hogy a hívás eljusson a 2. szintű ügyfélszolgálati szakemberhez, aki a hibaelhárításban tapasztaltabb. Ez a híváskiterjesztés (eszkaláció) néven ismeretes eljárás, a feladat átadása a tapasztaltabb szakembernek.

Mind az 1. szintű, mind pedig a 2. szintű ügyfélszolgálati szakember megkísérli a felhasználó problémájának megoldását a telefon, a web eszközök és a lehetséges távoli asztalmegosztási alkalmazás használatával.

Ha az ügyfélszolgálati szakemberek nem tudják távolról megoldani az ügyfél problémáját, akkor 3. szintű ügyfélszolgálati szakembert kell küldeni a felhasználó telephelyére. A helyszíni látogatást végrehajtó ügyfélszolgálati szakember feladata, hogy meglátogassa a felhasználói telephelyet és fizikailag, magán a problémás eszközön dolgozzon. Az ügyfélszolgálati szakember egyeztethet egy találkozót a felhasználóval a helyszíni kiszálló szakember számára, de a helyszíni szakember maga is egyeztethet a felhasználóval a találkozást illetően.

A hibakeresés megkezdése előtt a helyszíni szakember áttekinti a hibajegyet, hogy lássa mit tettek korábban a hiba elhárítása érdekében. Ez az áttekintés háttér információkat ad egy logikus kiindulási pont megtalálásához. Abban is segít dönteni a szakembernek, hogy milyen szerszámokat és anyagokat vigyen magával azért, hogy később anyagbeszerzés miatt ne kelljen a helyszínt elhagyni.

A helyszíni ügyfélszolgálati szakember jellemzően a felhasználó telephelyén szokott a számítógépes hálózaton tevékenykedni, bár előfordul, hogy némelyik készüléket nem tudja a helyszínen megjavítani. Az ilyen eszközt vissza kell vinnie az internetszolgáltató telephelyére további hibaelhárításra.

2.3.3 A helyszíni eljárás

Mielőtt a helyszíni ügyfélszolgálati szakember megkezdi a hiba elhárítását vagy a javítást négy feladata van:

1. lépés Bemutatkozik a felhasználónak és azonosítja magát.

2. lépés Áttekinti az ügyféllel a hibajegy vagy a munkalap feljegyzéseit és ellenőrzik, hogy az eddigi információk megállják-e a helyüket.

3. lépés Közli az ügyféllel az azonosított problémák aktuális állapotát, valamint azt, hogy mit akar aznap tenni.

4. lépés Engedélyt kér a felhasználótól a munka megkezdésére.

Az ügyfélszolgálati szakembernek ellenőriznie kell a hibajegy minden tételét. Amint az összes körülménnyel megismerkedett, kezdődhet a munka. Ő a felelős az összes eszköz és hálózati beállítás ellenőrzéséért, és a szükséges segédprogramok (utilities) futtatásáért. Szükséges lehet a hibával gyanúsított hardver cseréjére egy jól működő hardverrel, a hardverhibák felderítésére.

Bármilyen helyszíni hibaelhárítás során, különösen új eszközök beszerelése vagy meglevők cseréje esetén, fontos a biztonságos munkakörülmények biztosítása a balesetek elkerülésére, követve az alábbi bevált biztonsági előírásokat. Sok munkáltató tart biztonságtechnikai gyakorlatot munkavállalói számára.

Létrák

A létrákat akkor használjuk, amikor a hálózati kábelt magas helyen kell vezetni, vagy amikor a vezeték nélküli hálózat elérési pontját nehezen hozzáférhető helyre kell telepíteni vagy ilyen helyen kell

javítani. A létráról való leesés vagy mászás közben egy készülék elejtése veszélyének csökkentésére, dolgozzunk együtt egy munkatárssal, ha lehet.

Magas vagy veszélyes helyek

Előfordul, hogy a hálózat készülékeit vagy kábelezését magas vagy nehezen megközelíthető helyen kell elhelyezni. Ilyen az épületek külső falsíkja, az épület tetőszerkezete, vagy olyan belső szerkezet, mint a liftakna, ami létráról nem érhető el. Ilyen esetekben különösen körültekintően kell eljárni. A leesés kockázatának mérséklésére használjunk biztonsági övet.

Villamos berendezések

Amikor egy készülék kezelése közben fennáll egy villamos vezeték megsértésének vagy érintésének lehetősége, fel kell venni a kapcsolatot a felhasználó villamos szakemberével az áramütés veszélyének csökkentése érdekében követendő óvintézkedések miatt. Egy áramütés súlyos személyi sérüléssel végződhet.

Kellemetlen helyek

A hálózati berendezések gyakran vannak szűk, kellemetlen, nehezen hozzáférhető helyen. Gondoskodni kell a megfelelő megvilágításról és a szellőzésről. A baleset veszélyének csökkentéséhez meg kell határozni az eszköz emelésének, szerelésének és eltávolításának legcélravezetőbb módját.

Nehéz berendezések

A hálózati eszközök lehetnek nehezek és terjedelmesek. Terjedelmes és nehéz berendezések helyszíni telepítése vagy mozgatása során gondoskodni kell a megfelelő munkaeszközökről és gyakorlott személyzet alkalmazásáról.

Az ügyfélszolgálati szakembernek bármilyen konfigurációs változtatás vagy új berendezés telepítése után ellenőrizni kell a helyes működést. Amikor befejezte a munkát, közölnie kell az ügyféllel az azonosított hiba természetét, a választott megoldást és minden azt követő eljárást. Mielőtt a problémát megoldottnak tekinthetné az ügyfélszolgálati szakember, az ügyfélnek át kell vennie a munkát. A hibajegyet csak ezután zárhatja le, és a megoldást is dokumentálnia kell.

A dokumentáció egy példányát át kell adni az ügyfélnek. A dokumentációnak tartalmaznia kell az eredeti ügyfélszolgálat-hívási problémát és az összes eljárást, amit a hiba elhárítása érdekében végrehajtottak. Az ügyfélszolgálati szakember feljegyezi a megoldást, és a hibajegyre rávezetik az ügyfél ellenjegyzését is. A jövőre való útmutatásul az ügyfélszolgálati szakember az ügyfélszolgálati dokumentációban rögzíti a problémát a megoldásával együtt, és felveszi ezeket a gyakran feltett kérdések (FAQ) közé.

Néhány esetben a helyszíni látogató ügyfélszolgálati szakember olyan hálózati problémákat tár fel, melyek a hálózati eszközök frissítését vagy újrakonfigurálását kívánják meg. Az ilyen eset az eredeti hibajegy hatáskörén kívül esik. A további lépések meghatározása érdekében mindezt mind az ügyféllel, mind pedig az internet-szolgáltatóval közölni kell.

2.4 A fejezet összefoglalása

- A felhasználók hálózati problémáit az ügyfélszolgálati szakemberek oldják meg.
- A felhasználói támogatás általában 3 szintű: ez az 1., a 2. és a 3. szint.
- Az ügyfélszolgálati szakember a szabványos problémamegoldási folyamat során alapvető eljárásként az incidensmenedzsment előírásai szerint jár el.
- Az ügyfélszolgálati eljárás a nyitott hibajegyen és a naplózási adatokon nyugszik.
- A nehéz ügyfelek és a bonyolult incidensek kezelése során az ügyfélszolgálat és a kapcsolatteremtő képesség kulcsfontosságú.
- A sikeres kommunikáció érdekében az ügyfélszolgálati szakemberek a következő képességekkel kell rendelkeznie:
 - Felkészültség
 - Udvarias magatartás
 - Odafigyelés az ügyfélre
 - Alkalmazkodás az ügyfél kedélyállapotához
 - Egy egyszerű probléma helyes diagnosztizálása
 - Naplózza a hívást
 - A hibaelhárításra a réteges modell megközelítést alkalmazzák.
 - Az OSI modell a hálózati kommunikációs feladatot több folyamatra bontja. Minden folyamat az egész feladatnak csak egy kis része.
 - A hét rétegű OSI modellt két részre oszthatjuk: felső és alsó rétegre.
 - A felső rétegekbe tartoznak a szállítási réteg feletti és ezt szoftverrel valósítják meg.
 - Az alsó rétegek: a szállítási, a hálózati, az adatkapcsolati és a fizikai réteg. A feladatuk az adattovábbítási funkciók kezelése.
 - Az ügyfélszolgálati szakemberek az OSI modell felhasználásával három különböző módon kereshetik meg a hiba helyét: alkalmazhatják a fentről-le, a lentől-fel és az oszd meg és uralkodj megközelítést.
 - A leggyakoribb ügyfélszolgálati hívások közül néhány az e-mailről és a kapcsolódási kérdésekről szól.
 - A felhasználótól begyűjtött információ átkerül a hibajegyre.
 - Az 1. szintű és a 2. szintű ügyfélszolgálati szakemberek a felhasználók problémáit telefonon, web-en, vagy távoli asztalmegosztási alkalmazásokkal oldják meg.
 - Néha szükséges a 3. szintű helyszíni ügyfélszolgálati szakember kiküldése.
 - Fontos az, hogy az ügyfél problémájának megoldási módját a jövőbeli hibaelhárításokhoz útmutatásul, a hibajegyen és a tudásbázisukban dokumentálják.

3. Egy hálózat továbbfejlesztésének tervezése

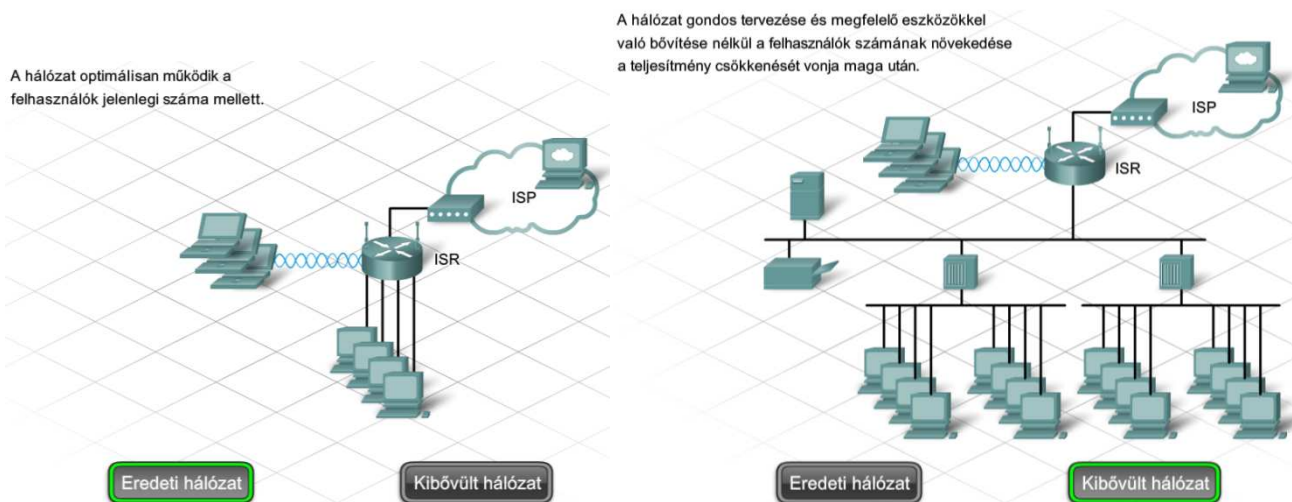
3.1 A létező hálózat dokumentálása

3.1.1 A helyszín felmérése

Amikor egy kisebb vállalkozás hirtelen növekedésnek indul, hálózata általában nem képes tartani a lépést a bővüléssel. Előfordulhat, hogy a vállalat dolgozói nem ismerik fel, milyen fontos a hálózati fejlesztések tervezése. Elképzelhető, hogy a vállalkozás az újonnan alkalmazott munkaerő hálózatra történő csatlakoztatásához különböző gyártóktól származó, eltérő minőségű és technológiájú hálózati eszközöket vásárol és illeszt a meglévő hálózathoz. Amint újabb felhasználókat adnak a meglévő hálózathoz, teljesítménye egyre csökken, míg végül már nem lesz képes kezelni a felhasználók által keltett hálózati forgalmat.

Miután a vállalati hálózat képtelen lesz elfogadhatóan működni, a kisvállalkozások nagy része szeretné áttervezni az új igényeknek megfelelően. Ehhez általában külső segítséget vesznek igénybe. Általában egy internetszolgáltatót vagy valamilyen támogatott szolgáltatást nyújtó céget bízhatnak meg tanácsadással, a fejlesztések kivitelezésével és felügyeletével.

Mielőtt hálózati fejlesztés megfelelően megtervezhető lenne, egy szakembert küldenek, aki helyszíni felmérés keretében dokumentálja a meglévő hálózati struktúrát. Ezen kívül az új berendezések telepítési helyének meghatározásához fel kell mérni és dokumentálni kell az épület fizikai elrendezését.



Az elvégzett helyszíni felmérés fontos információkat szolgáltat a hálózati tervezőknek, megfelelő kiindulási pontot biztosít a projekt elkezdéséhez, megmutatja a telephely jelenlegi állapotát, és jól jelzi a jövőbeni szükségleteket.

A helyszíni felmérések során gyűjthető fontosabb információk közé tartoznak a következők:

- Felhasználók száma és a berendezések típusa
- Tervezett növekedés mértéke
- Jelenlegi internet hozzáférés típusa

- Alkalmazásokra vonatkozó követelmények
- Meglévő hálózati infrastruktúra és fizikai elhelyezkedése
- Új szolgáltatásokra vonatkozó követelmények
- Biztonsági és titoktartási megfontolások
- Megbízhatósági és rendelkezésre állási elvárások
- Költségvetési megszorítások

Amennyiben lehetséges, szerezzük be a telephely alaprajzát. Ha az alaprajz nem áll rendelkezésre, a szakemberek rajzolhatnak egy a helyiségek méretére és elhelyezkedésére vonatkozó ábrát. Nagy segítséget nyújthat a fejlesztési alapkövetelmények megfogalmazásában a meglévő hálózati hardverekről és szoftverekről készült leltári lista.

A helyszíni felmérést végző szakember mellett egy értékesítési képviselő is részt vehet az ügyféllel való találkozó során. Az értékesítési képviselő az üzletvitel szükségleteit kielégítő hálózati fejlesztések felől tehet fel kérdéseket.

Állomások és felhasználók száma: Összesen hány hálózati felhasználót, nyomtatót és kiszolgálót fog ellátni a hálózat? A hálózat által támogatandó felhasználók számának meghatározásához ne felejtkezzen el az elkövetkező 12 hónapban hozzáadandó felhasználók számba vételéről, és hogy összesen hány hálózati nyomtatót és kiszolgálót kell befogadnia a hálózatnak.

Internet szolgáltatás és berendezések: Milyen módon kapcsolódik a vállalkozás az internethez? A kapcsolódáshoz szükséges eszközt az ISP biztosítja vagy saját tulajdonában áll? Nagy sebességű, például DSL vagy kábeles internetes kapcsolatok esetén gyakran előfordul, hogy a kapcsolathoz szükséges berendezések a szolgáltató tulajdonában vannak (DSL forgalomirányító vagy kábelmodem). Ha a csatlakozást korszerűsítik, az internet kapcsolatot biztosító eszköz fejlesztése vagy cseréje is szükséges lehet.

Meglévő hálózati eszközök: Hány hálózati eszköz van telepítve hálózatában? Mely funkciók ellátására szolgálnak ezek az eszközök? A hálózat fejlesztési tervének elkészítéséhez feltétlenül ismernünk kell az aktuálisan telepített eszközök számát és típusát. Valamint szükség van a jelenleg telepített eszközök konfigurációjának dokumentálására is.

Biztonsággal kapcsolatos elvárások: Rendelkeznek jelenleg a hálózat védelmét szolgáló tűzfallal? Amikor egy magánhálózat csatlakozik az internethez, fizikai kapcsolat jön létre több mint 50000 ismeretlen hálózat és ezek ismeretlen felhasználói felé. Miközben e kapcsolódások az információ-megosztás izgalmas lehetőségét biztosítják, egyúttal veszélynek tesszük ki a nem megosztásra szánt információkat is. A többfunkciós forgalomirányítók egyéb szolgáltatásaik mellett tűzfal képességgel is rendelkeznek.

Alkalmazottakra vonatkozó követelmény: Mely alkalmazásokat kell támogatnia a hálózatnak? Szükség van az alkalmazásokhoz például IP-telefon vagy video-konferenciaszolgáltatásra? Fontos, hogy megjelöljük a különleges alkalmazások iránti igényünket, főként a hang és video alapú alkalmazásokat. E felhasználási módok további hálózati eszköz konfigurációt igényelhetnek, és új szolgáltatásokra lehet szükség az ISP részéről a megfelelő minőségű szolgáltatás biztosításához.

Vezeték nélküli követelmények: Vezetékes, vezeték nélküli vagy mindkét technológiát használó helyi hálózatot szeretne (LAN)? Összesen hány négyzetmétert kell lefednie a vezeték nélküli helyi

hálózatnak? A számítógépek, nyomtatók és egyéb eszközök hálózatra történő csatlakoztatásához lehetőség van hagyományos vezetékes hálózat (10/100 kapcsolt Ethernet), csak vezeték nélküli hálózat (802.11x), illetve ezek kombinációjának használatára. Minden egyes vezeték nélküli hozzáférési pont, mely asztali számítógépek és laptopok csatlakoztatására szolgál, meghatározott hatótávolsággal rendelkezik. Ahhoz, hogy megbecsüljük a szükséges hozzáférési pontok számát, ismernünk kell a lefedendő terület nagyságát négyzetméterben és a helyszín fizikai jellemzőit.

A szemlét végző szakembernek mindenre fel kell készülnie a munkája során. A hálózatok nem mindig felelnek meg a helyi villamos és építészeti gyakorlati előírásoknak vagy biztonsági szabályozásoknak. Gyakran semmilyen szabványnak sem felelnek meg.

Előfordulnak olyan hálózatok, melyeken az idők folyamán rendszertelen bővítéseket végeztek, így különböző technológiákat és protokollokat használnak. A szakembereknek óvatosságnak kell lenniük, nehogy megsértsék az ügyfelet a meglévő hálózatról alkotott negatív véleményük kifejtésével.

Az ügyfél telephelyének meglátogatása alkalmával mélyreható vizsgálat alá kell venni a hálózati és számítógépes rendszert. Előfordulhatnak olyan nyilvánvaló esetek, mint jelöletlen kábelek, a hálózati eszközök gyenge védelme, tartalék áramforrás vagy a munkához nélkülözhetetlen eszközöket ellátó szünetmentes tápegységek (UPS) hiánya. E körülményeket, valamint a szemle és az ügyféllel való találkozó során szerzett további információkat le kell jegyezni a telephelyi felmérés beszámolójában.

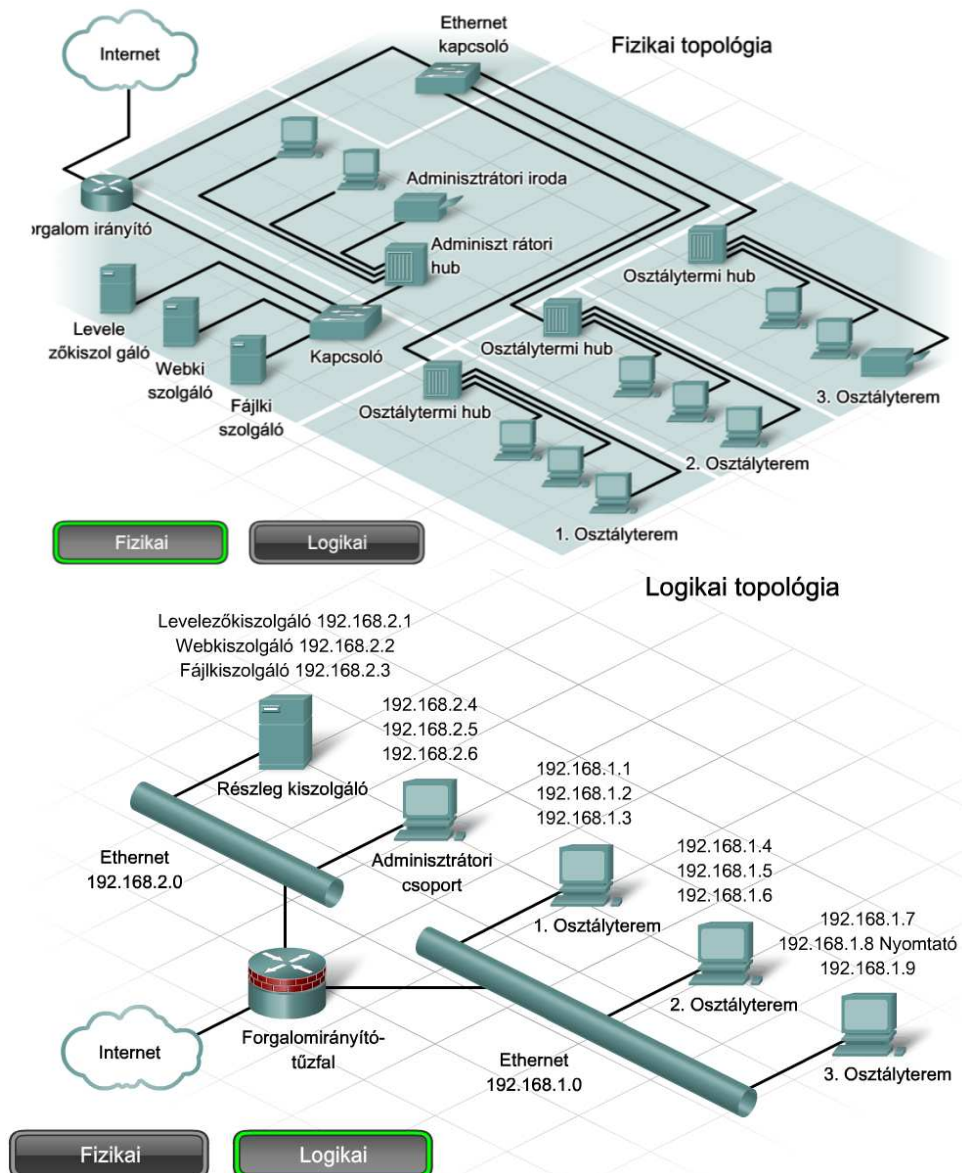
A felmérés befejeztével az ügyféllel együtt át kell nézni a kapott eredményeket, nehogy valami kimaradjon, vagy hiba kerüljön a felmérésbe. Ha mindent pontosan rögzítettek, a helyszíni felmérés kitűnő alapul szolgál az új hálózat terv elkészítéséhez.

3.1.2 Fizikai és logika topológiák

A hálózat fizikai és logikai topológiáját is dokumentálni kell. A fizikai topológia a kábelek, számítógépek és egyéb perifériák tényleges elhelyezkedéséből áll. A logikai topológia a hálózaton átmenő adatok által megtett útvonalat és a hálózati feladatok, például forgalomirányítás ellátásának helyét tartalmazza. A topológia térképek létrehozásához szükséges információkat a helyszíni felmérés során gyűjtik össze a szakemberek.

Vezetékes hálózatok esetében a fizikai topológia a kábelszekrényből és a végfelhasználói állomásokhoz vezető kábelekből áll. Ezzel szemben a vezeték nélküli hálózatoknál a kábelszekrény és a hozzáférési pontok alkotják a fizikai topológiát. Mivel ebben az esetben nincsenek kábelek, ezért a fizikai topológiához tartozik a vezeték nélküli jelek lefedettségi területe is.

A logikai topológia többnyire megegyezik a vezetékes és vezeték nélküli hálózatok esetén. Tartalmazza a végfelhasználói állomások, a forgalomirányítók és egyéb hálózati eszközök neveit és 3. rétegbeli címeit (IP), tekintet nélkül a fizikai elhelyezkedésükre. Jelzi a forgalomirányítás, hálózati címfordítás és tűzfalas szűrés helyét.



A logikai topológiai térkép létrehozásához szükség van az eszközök és a hálózat viszonyának megértésére, függetlenül a fizikai kábelezés elhelyezkedésétől. Számos topológiai elrendezés lehetséges. Ezek közé tartoznak például a csillag, kiterjesztett csillag, részleges háló és háló topológiák.

Csillag topológiák

Csillag topológia esetében az egyes hálózati eszközök önálló összeköttetésen keresztül kapcsolódnak a központi berendezéshez. A központi berendezés szerepét általában egy kapcsoló vagy vezeték nélküli hozzáférési pont látja el. A csillag topológia előnye, hogy ha egy kapcsolódó eszköz meghibásodik, a hiba csak ezt az eszközt érinti. Ha viszont a központi berendezés, például a kapcsoló hibásodik meg, akkor minden csatlakozó eszköz elveszti a kapcsolatot.

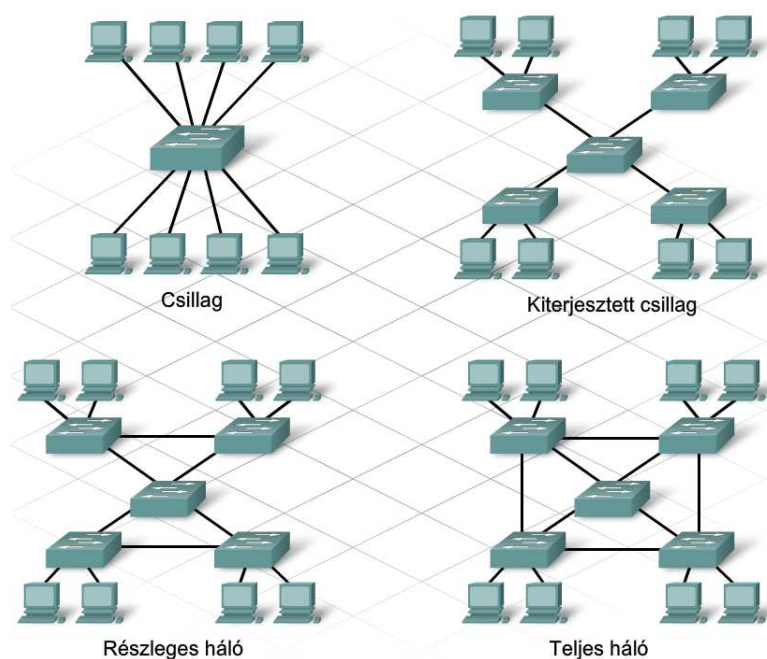
Kiterjesztett csillag topológia akkor jön létre, ha az egyik csillag központi eszköze egy másik csillag központi berendezésével kerül kapcsolatba. Ilyen topológia jön létre például, amikor több kapcsoló van összekötve, vagy lánckapcsolásban van egymással.

Háló Topológiák

A hálózatok központi (mag) rétegének kábelezése általában teljes háló vagy részleges háló topológiájú. Teljes háló topológia esetében minden hálózati eszköz közvetlen összeköttetésben áll a többi eszközzel. Bár a teljes háló topológiák a teljesen redundáns hálózat előnyeit nyújtják, hátrányaik közé tartozik a körülményes huzalozás és felügyelet, valamint a magas költségek.

Nagyobb méretű telepítések esetén módosított, részleges háló topológiát alkalmaznak. A részleges háló topológiáknál minden eszköz legalább két másikkal áll összeköttetésben. Ez a fajta elrendezés többnyire elegendő redundanciát biztosít a teljes háló topológiák bonyolultsága nélkül.

A részleges vagy teljes háló segítségével megvalósított redundáns topológiák biztosítják, hogy a hálózati eszközök meghibásodás esetén is képesek legyenek alternatív útvonalak használatával elküldeni az adatokat.



3.1.3 Hálózati követelmények dokumentálása

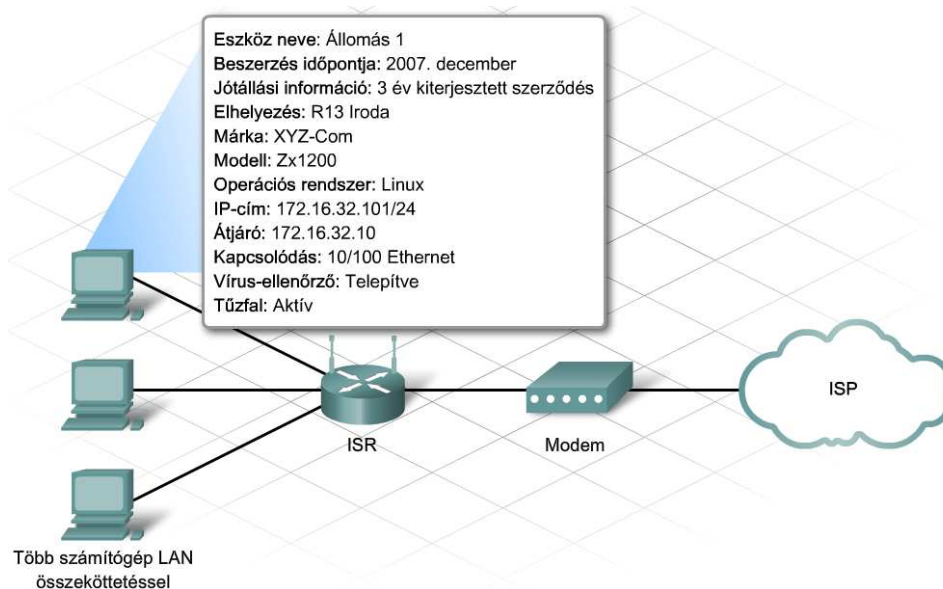
A meglévő hálózat alapján készített topológiai térképek mellett szükség van a jelenleg telepített állomásokról és eszközökről szerzett további információkra. Ezeket az adatokat leltári íveken szokás rögzíteni. Ezen kívül dokumentálják a vállalat közeljövőben várható növekedést is.

A fenti ismeretek birtokában a hálózat tervezője meghatározhatja a szükséges új eszközök számát, és a cég várható növekedéséhez legjobban illeszkedő hálózati struktúrát.

A telepített eszközökről felvett leltárnak a következő adatokat kell tartalmaznia:

- Eszköz neve
- Beszerzés időpontja
- Jótállási információk
- Hely
- Márka és modell megnevezése

- Operációs rendszer
- Logikai címzési információk
- Átjáró
- Kapcsolódás típusa
- Telepített víruskereső szoftverek
- Biztonsági információk



3.2 Tervezés

3.2.1 Hálózati korszerűsítés tervezési fázisai

A hálózat korszerűsítését gondos tervezésnek kell megelőznie. Bármely más projekthez hasonlóan először meg kell határozni a szükségleteket, majd egy terv készül, amely körvonalazza a fejlesztés folyamatát az elejétől a végéig. Egy jó projektterv segít felismerni a gyenge pontokat, az erősségeket, a kihasználható lehetőségeket és a veszélyforrásokat (SWOT). A terv pontosan meghatározza az elvégzendő feladatokat, és azok végrehajtási sorrendjét.

Néhány jó tervezési példa:

- A sportjátékok csapatai megfelelő terv alapján játszanak
- Az építések követik a tervrajzokat
- A szertartások vagy találkozók napirendet követve zajlanak le

Az olyan hálózat, mely mindössze többféle technológia és protokoll felhasználásával, egymással összekötött eszközök halmaza, általában a silány kezdeti tervezésről árulkodik. Az ilyen módon felépített hálózatok hajlamosabbak a leállásra, karbantartásuk és hibáik elhárítása nehezen megvalósítható.

Egy hálózati korszerűsítés tervezése a helyszíni szemle és az eredményeket tartalmazó jelentés elkészülte után kezdődhet meg. Öt fázist különböztetünk meg.

1. fázis: Követelmények összegyűjtése

Miután elvégezték a helyszíni szemlét, és minden szükséges információt összegyűjtöttek az ügyféltől, az adatok elemzésével meghatározhatók a hálózat követelményei. Az elemzést az ISP tervező csoportja végzi, amely az elemzés eredményét egy Elemzési jelentésben foglalja össze.

2. fázis: Kiválasztás és tervezés

Az Elemzési jelentésben megfogalmazott követelmények alapján kiválasztják a szükséges eszközöket és kábeleket. Többféle tervezési alternatívát készítenek, melyeket rendszeresen megosztanak a projekt többi tagjával. Ez a fázis lehetőséget teremt arra, hogy a tervező csapat tagjai még a dokumentáció szintjén áttekinthessék a hálózatot és kompromisszumot teremtsenek a teljesítmény és a költség között. Ez az a fázis, melynek során lehetőség van a terv gyenge pontjainak feltárására és kiküszöbölésére.

Szintén e fázis során készítik el és tesztelik a hálózat prototípusát. A prototípus jó indikátora az új hálózat várható működésének.

Miután az ügyfél jóváhagyta a tervet, megkezdődhet az új hálózat kivitelezése.

3. fázis: Kivitelezés

Ha az első két lépést megfelelően végezték el, a kivitelezés valószínűleg problémamentes lesz. Ha olyan feladatok merülnek fel, amelyeken a korábbi fázisokban átsiklottak, a kivitelezési fázisban kell korrigálni. Egy váratlan események megoldására tartalék időt biztosító kivitelezési ütemterv segítségével a szolgáltatás kiesése az ügyfél számára minimálisra szorítható. A projekt sikerének előfeltétele az ügyféllel való folyamatos kapcsolattartás a kivitelezési folyamat során.

4. fázis: Üzemeltetés

A hálózatot az úgynevezett termelési környezetben fogják üzembe helyezni. E lépést megelőzően a hálózat még az ellenőrzési vagy kivitelezési fázisban van.

5. fázis: Áttekintés és értékelés

Miután a hálózatot üzembe helyezték, sort kell keríteni a tervezési és kivitelezés áttekintésére és értékelésére. E folyamat végrehajtásához a következő lépések elvégzése ajánlott:

1. lépés: Hasonlítsuk össze a felhasználók tapasztalatait a dokumentációban foglalt célokkal, és mérlegeljük, hogy a terv megfelelő-e a feladatok elvégzéséhez!

2. lépés: Vessük össze az előírányzott terveket és költségeket a ténylegesen megvalósítottal! Ez az értékelés teszi lehetővé, hogy a most elvégzett projekt során szerzett tapasztalatok a jövőbeni projektek előnyére váljanak.

3. lépés: A működés megfigyelése és a változások rögzítése. Nagyon fontos, hogy a rendszer mindig teljes körűen dokumentált és ellenőrizhető legyen.

A különböző fázisok gondos tervezése biztosítja a projekt zökkenőmentes lezajlását és a megvalósítás sikerességét. A helyszínen dolgozó szakembereket gyakran bevonják a tervezésbe, mivel ők a korszerűsítés minden fázisában részt vesznek.

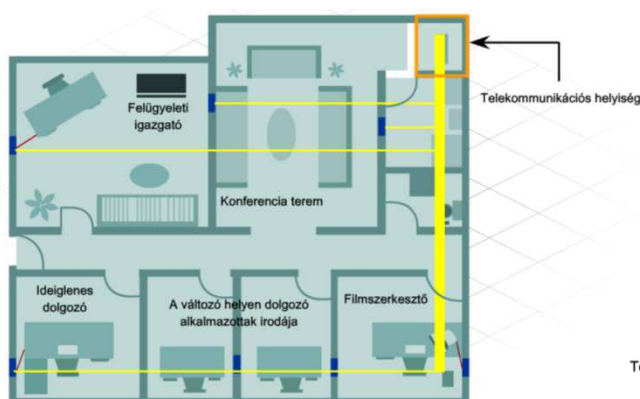
3.2.2 Fizikai környezet

Az egyik első dolog, melyet a hálózat tervezőjének el kell végeznie az új hálózathoz szükséges berendezések kiválasztása és a tervek elkészítése előtt, a meglévő hálózati felszerelések és a kábelezés megvizsgálása. A felszerelések közé tartozik a fizikai környezet egésze, a telekommunikációs helyiség és a meglévő hálózati kábelezés. A telekommunikációs helyiséget vagy a kábelszekrényt egy kisméretű, egy szintre kiterjedő hálózat esetén általában Központi kábelrendezőnek (MDF) nevezzük.

Az MDF jellemzően több hálózati eszközt, például kapcsolókat, hubokat, forgalomirányítókat és hozzáférési pontokat tartalmaz. Ezen a helyen fut össze egy pontban az összes hálózati kábel. Sokszor az MDF tartalmazza az internetszolgáltató szolgáltatás-elérési pontját (POP) is. Itt kapcsolódik a hálózat az internethez egy távközlési szolgáltatón keresztül.

Amennyiben további kábelszekrényekre is szükség van, azokat közbenső kábelrendezőknak (IDF) nevezik. Az IDF-ek jellemzően kisebbek a központi kábelrendezőnél, és kapcsolatban állnak vele.

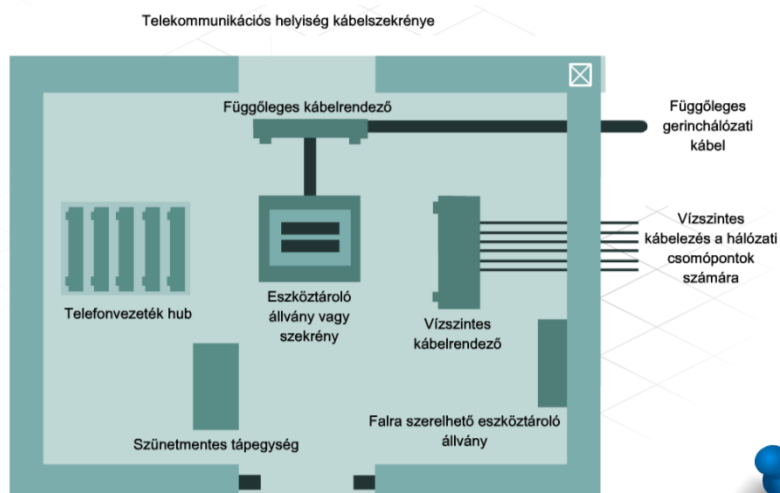
Sok kisvállalkozás nem rendelkezik telekommunikációs helyiséggel vagy kábelszekrénnyel. Ilyen esetekben a hálózati eszközök általában egy íróasztalon vagy más bútordarabon helyezkednek el, és a kábelek csak úgy a földön fekszenek. A hálózati berendezéseket mindig biztonságban kell tartani! A hálózat növekedésével egy telekommunikációs szoba meglete kritikus fontosságú lesz a biztonság és a hálózat megbízhatósága szempontjából.



A különböző ISO szabványok eltérő terminológiát használnak az MDF és IDF szakkifejezésekre. A kábelszekrény kifejezés utalhat az MDF-re és az IDF-re is.

MDF = Épületek közötti elosztó

IDF = Szintek közötti elosztó



3.2.3 Kábelezési megfontolások

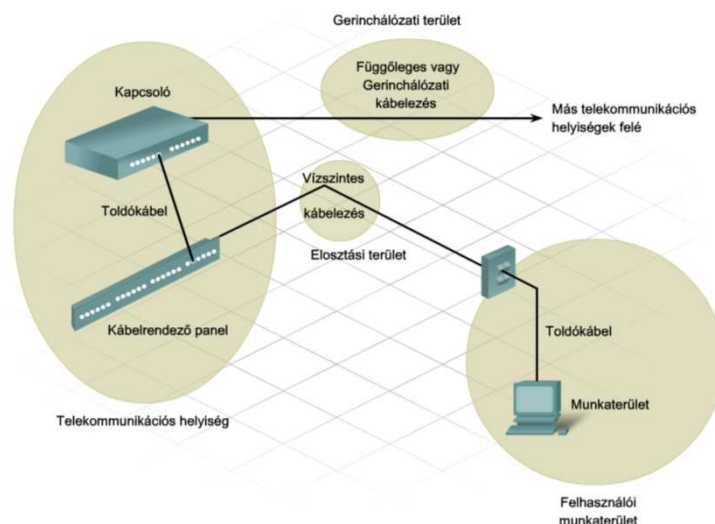
Ha a meglévő kábelezés nem felel meg az új berendezések előírásainak, új kábelezést kell tervezni és kiépíteni. A meglévő kábelek állapota gyorsan megállapítható a hálózat fizikai megtekintésével a helyszíni szemle során. Hálózati kábelek telepítésének tervezésekor négy fizikai környezetet kell figyelembe venni:

- Felhasználók munkaterülete
- Telekommunikációs helyiség
- Gerinchálózati terület
- Elosztási terület

Sokféle kábeltípus megtalálható a hálózati környezetekben, némelyek gyakrabban előfordulnak, mint mások:

- **Árnyékolt csavart érpár (STP)** - Rendszerint 5-ös, 5e vagy 6-os kategóriájú kábel, mely fémfólia segítségével védett a külső elektromágneses interferenciával (EMI) szemben. Ethernet hálózatokban a kábel által áthidalható maximális távolság körülbelül 100 méter (328 láb).
- **Árnyékolatlan csavart érpár (UTP)** - Jellemzően 5-ös, 5e vagy 6-os kategóriájú kábel, mely nem biztosít külön védelmet az EMI-vel szemben, viszont olcsó. A kábelek vezetése során el kell kerülni az elektromosan zajos területeket. Ethernet hálózatokban a kábel által áthidalható maximális távolság körülbelül 100 méter (328 láb).
- **Optikai szál kábel** - Elektromágneses interferenciára érzéketlen átviteli közeg, mely a réznél nagyobb sebességgel és távolabbra képes továbbítani az adatokat. Az üvegszál típusától függően az áthidalható távolság több kilométer is lehet. Az optikai szál kábelek gerinchálózati összeköttetések és nagysebességű kapcsolatok létrehozására használhatók.

E három gyakran használt kábeltípuson kívül a koaxiális kábelt is használják a hálózatokban. A koaxiális kábeleket általában nem LAN-okban használják, inkább a kábelmodemes internet szolgáltatói hálózatokban elterjedtek. A koaxiális kábel magja szilárd, körülötte több védőréteg található, melyek polivinilkloridból (PVC), fonott árnyékoló vezetékből és műanyag burkolatból állnak. A kábellel áthidalható távolság több kilométer. Az áthidalható távolsági a kapcsolat rendeltetésétől függ.



Világszerte több szervezet is bocsát ki LAN kábelezési specifikációkat.

A Telecommunications Industry Association (TIA) és az Electronic Industries Alliance (EIA) együttműködésének eredménye a LAN hálózatok számára létrehozott TIA/EIA kábelezési előírás. A két leggyakrabban használt TIA/EIA kábelezési specifikáció az 568-A és 568-B szabvány. Mindkét szabvány ugyanolyan 5-ös vagy 6-os kategóriájú kábelt használ, viszont a csatlakozók bekötése eltérő színmintát követ.

A hálózatokban három különböző típusú csavart érpáras kábelt használnak:

- **Egyeneskötésű** - Egymástól eltérő eszközök összekapcsolására használható, például kapcsoló és számítógép vagy kapcsoló és forgalomirányító.
- **Keresztkötésű** - Hasonló eszközök összekapcsolására szolgál, mint például két kapcsoló vagy két számítógép.
- **Konzol** (vagy Rollover) - Kapcsolatot teremt egy számítógép és egy forgalomirányító vagy kapcsoló konzol portja között a kezdeti konfigurálás elvégzéséhez.

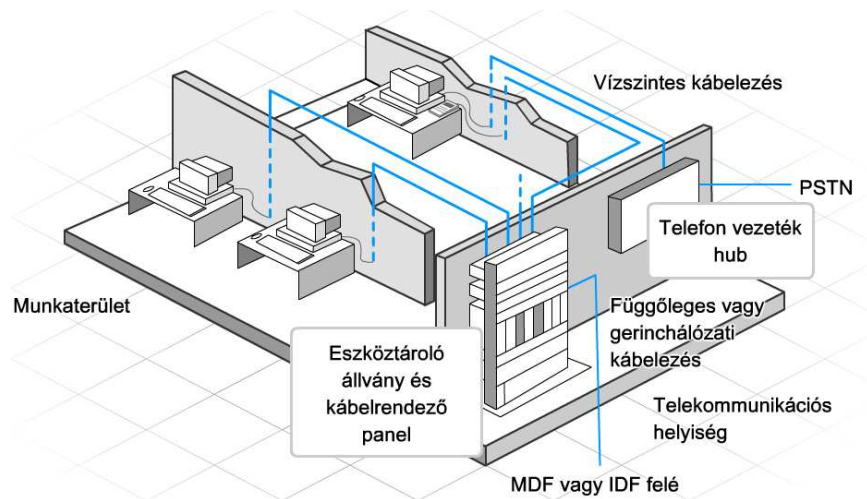
Hálózatokban gyakran előforduló egyéb kábeltípus a soros kábel. Soros kábelt jellemzően forgalomirányítók internetre történő csatlakozásához használnak. Ezt az internet kapcsolatot egy telefonszolgáltató, egy kábelszolgáltató vagy valamilyen magán ISP is biztosíthatja.

3.2.4 Strukturált kábelezés

Strukturált kábelezési projekt tervezése során az első lépés egy pontos alaprajz beszerzése. A tervrajz segítségével a szakembereknek lehetősége nyílik a kábelszekrények, kábelvezeték-csatornák és az elkerülendő elektromos területek lehetséges helyzetének meghatározására.

Miután a szakemberek meghatározták és jóváhagyták a hálózati eszközök helyét, felrajzolják a hálózat vázlatát az alaprajzra. Az alábbi tételeket feltétlenül rögzíteni kell a rajzon:

- **Toldókábel** - A számítógép és a fali csatlakozóaljzat között elhelyezkedő rövid kábel a felhasználók munkaterületén.
- **Horizontális kábel** - A fali csatlakozó és valamelyik IDF között található kábel az elosztási területen.
- **Vertikális kábel** - Az IDF-et és az MDF-et összekötő kábel a vállalat gerinchálózati területén.
- **Gerinchálózati kábel** - A legtöbb hálózati forgalmat bonyolító hálózati terület.
- **Kábelszekrény helye** - A végfelhasználók felől érkező kábeleket egy hub vagy kapcsoló segítségével koncentráló terület.
- **Kábelfelügyeleti rendszer** - Kábelek vezetését és védelmét ellátó sínek és pántok összessége.
- **Kábeljelölő rendszer** - A kábelek azonosítására használható jelölési rendszer vagy séma.
- **Elektromos rendszerekkel kapcsolatos megfontolások** - A hálózati berendezések elektromos követelményeit biztosító csatlakozókat és az ezekhez kapcsolódó felszereléseket foglalja magában.



3.3 Eszközök beszerzése és karbantartása

3.3.1 Eszközök beszerzése

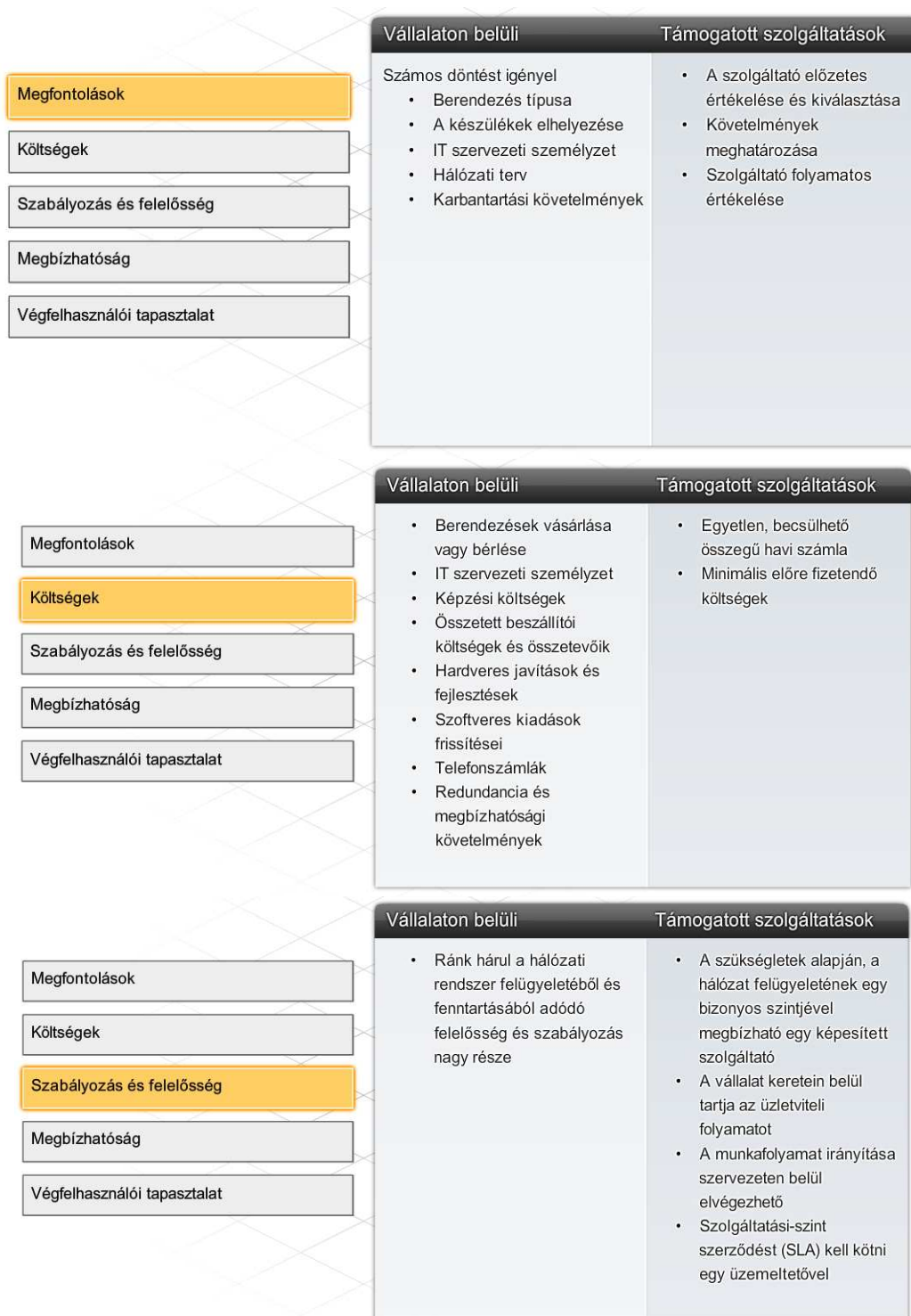
A hálózat korszerűsítésének tervezésekor az ISP csapatának válaszolnia kell az új eszközök vásárlásával valamint az új és meglévő eszközök karbantartásával kapcsolatban felmerülő kérdésekre. Az új eszközök beszerzésére alapvetően két lehetőség van:

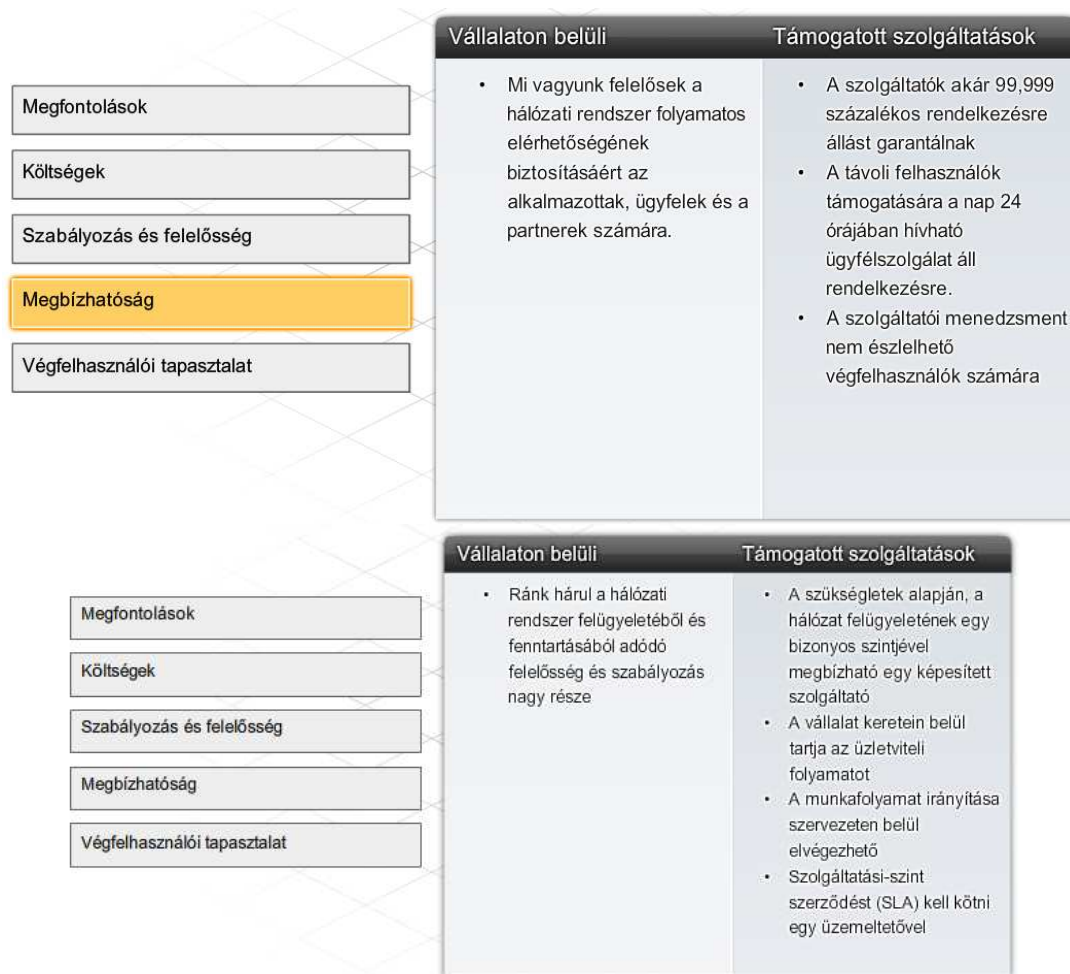
- **Támogatott szolgáltatás** - A berendezést az internet szolgáltató biztosítja bérleti vagy egyéb szerződés keretében. Ekkor az ISP felelős az eszköz fejlesztéséért és karbantartásáért.
- **Házon/Vállalaton belüli** - A berendezést az ügyfél vásárolja meg, és ő maga felelős az eszköz frissítéséért, karbantartásáért és a jótállás érvényesítéséért.

Eszközök beszerzésekor a költség mindig jelentős döntést befolyásoló tényező. A különböző lehetőségekről készített gondos költségelemzés jó alapot biztosít a végső döntés meghozatalához.

Ha a támogatott szolgáltatásra esett a választás, számolni kell a bérleti díjjal és a szolgáltatási szint szerződésben (SLA) felvázolt egyéb szolgáltatási költségekkel.

Ha pedig a vásárlásra esett a választás, az ügyfélnek figyelembe kell vennie a készülék árát, a jótállás időtartamát, a meglévő berendezésekkel való kompatibilitást, valamint a fejlesztési és karbantartási kérdéseket. E tényezők mindegyikét elemezni kell a költséghatékony beszerzés érdekében.





3.3.2 Hálózati eszközök kiválasztása

Az igények elemzése után a tervező csoport javaslatot tesz az új hálózati összekötés és szolgáltatás biztosítására alkalmas hálózati eszközök beszerzésére.

A korszerű hálózatokban számos eszköztípust használnak az összeköttetés megteremtésére. A különböző eszközök más-más képességekkel rendelkeznek a hálózaton keresztül átmenő adatfolyam vezérléséhez. Létezik az az általános szabály, mely szerint egy eszköz minél magasabb OSI modell rétegbe tartozik, annál intelligensebb. Ez azt jelenti, hogy egy magasabb szintű eszköz az adatforgalom jobb elemzésére képes, és olyan információk alapján továbbítja, melyek az alacsonyabb rétegekben nem érhetők el. Például, egy 1. rétegbeli hub kizárólag minden portját felhasználva képes az adatok továbbítására, míg egy 2. rétegbeli kapcsoló meg tudja szűrni az adatokat és csak azon a porton küldi ki, amely a megfelelő MAC című célállomáshoz kapcsolódik.

A kapcsolók és forgalomirányítók fejlődésével a köztük lévő különbségek egyre elmosódottabbakká válnak. Egy alapvető különbség azért megmarad: a LAN kapcsolók legfeljebb az adott szervezeten belüli helyi hálózatok összeköttetését biztosítják, míg a forgalomirányítók összekapcsolják a helyi hálózatokat, és a nagyterjedésű hálózatoknak is nélkülözhetetlen elemeik.

A kapcsolókon és forgalomirányítókön kívül más összekapcsolási lehetőségek is léteznek LAN-ok számára. A vezeték nélküli hozzáférési pontok segítségével a számítógépek és egyéb eszközök, például hordozható IP telefonok számára lehetőség adódik a hálózathoz való vezeték nélküli

csatlakozásra vagy a szélessávú kapcsolat megosztására. A tűzfalak védelmet jelentenek a hálózati fenyegetésekkel szemben, illetve biztonságot, hálózat vezérlést és elszigetelést biztosítanak.

A többfunkciós forgalomirányítók (ISR) olyan hálózati eszközök, melyek egy készülékben egyesítik a kapcsolók, forgalomirányítók, hozzáférési pontok és tűzfalak adottságait.

3.3.3 LAN eszközök kiválasztása

Bár mind a hubok, mind a kapcsolók biztosítják az összeköttetést a hálózat hozzáférési rétegében, mégis inkább a kapcsolókat érdemes választani a helyi hálózatban található eszközök összeköttetésére. A kapcsolók jóval költségesebbek a huboknál, azonban a nagyobb teljesítményük jóval gazdaságosabbá teszi őket. Hubra általában nagyon kisméretű helyi hálózatoknál kerül a választás, olyan esetekben, amikor nincs igény nagy átbocsátóképességre, vagy korlátozott pénzügyi keretek állnak rendelkezésre.

Amikor egy helyi hálózathoz kapcsolót kell választani, számos tényezőt kell fontolóra venni. E tényezők közé tartoznak többek között a következők:

- Portok, interfészek típusa és sebessége
- Bővíthetőség
- Felügyelhetőség
- Költség

Portok, interfészek típusa és sebessége

Olyan 2. rétegbeli eszközt választva, amely a megnövekedett sebesség követelményt is képes ellátni, lehetőség lesz a hálózat fejlesztésére a központi berendezések cseréje nélkül.

A kapcsoló kiválasztásakor alapvető szempont a portok száma és típusa.

A hálózati tervezőknek körültekintően kell meghatározniuk a csavart érpáras (TP) és az optikai szálak portok számát. Meg kell becsülni az esetleges hálózatbővítésekhez szükséges tartalék portok számát is.

Bővíthetőség

A hálózati eszközök moduláris és rögzített fizikai összeállításban is kaphatók. A rögzített konfigurációjú eszközök meghatározott típusú és számú porttal vagy interfésszel rendelkeznek. A moduláris berendezések bővítőhelyekkel rendelkeznek, így új modulok hozzáadásával rugalmasan lehet követni az igényeket. A legtöbb moduláris eszközt minimális számú rögzített porttal és bővítőhelyekkel szállítják.

A bővítőhely felhasználásának tipikus példája, amikor egy eredendően csak néhány rögzített csavart érpáras porttal konfigurált eszközt optikai szálak kábelek csatlakoztatására alkalmas modullal bővítik. Moduláris kapcsolók segítségével költséghatékonyan követhető a LAN méretnövekedése.

Felügyelhetőség

Egy alsó kategóriás, olcsó kapcsoló nem konfigurálható. Egy olyan felügyelhető kapcsoló esetén viszont, amely Cisco IOS szolgáltatáskészletet használ, lehetőség van az egyes portok vagy akár az

egész kapcsoló forgalmának szabályozására. A szabályozás lehetőségei közé tartozik többek között az eszköz beállításainak megváltoztatása, a port biztonság bevezetése, valamint a teljesítmény felügyelet.

Így például egy felügyelhető kapcsoló portjai különállóan be, illetve kikapcsolhatók. Továbbá a rendszergazda azt is megszabhatja, mely számítógépek csatlakozhatnak egy adott porthoz.

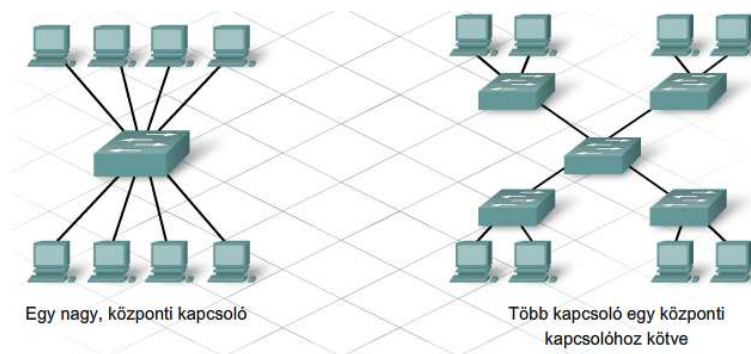
Költségek

Egy kapcsoló árát a teljesítménye és szolgáltatásai határozzák meg. A teljesítményt a portok száma és típusa, valamint a teljes átbocsátóképesség jellemzi. A költségeket befolyásoló egyéb tényezők például a hálózatfelügyeleti lehetőségek, a beágyazott biztonsági technológiák és más fejlett kapcsolási technológiák megléte.

Egy egyszerű ár/port számítást használva először úgy tűnhet, hogy a legjobb választás egy nagyméretű kapcsoló valamilyen központi helyre történő telepítése. A látszólagos megtakarításokat azonban ellensúlyozhatják a hosszabb kábelek miatt felmerülő többletköltségek, amelyek a központi kapcsoló és a többi eszköz között teremtik meg a kapcsolatot. Ezért ezt a lehetőséget érdemes összevetni azzal a megoldással, amikor több kisebb kapcsolót telepítünk egy központi kapcsoló köré kevesebb számú, hosszabb kábellel összekötve.

Egyetlen nagy központi helyett, több kisebb eszköz elhelyezése azzal az előnnyel is jár, hogy csökken a hibatartomány mérete. Egy hibatartomány a hálózat azon területe, amelyet egy hálózati berendezés hibás működése vagy meghibásodása befolyásolhat.

A LAN kapcsolók kiválasztása után kerülhet sor az ügyfél számára megfelelő forgalomirányító kiválasztására.



3.3.4 Hálózati eszközök kiválasztása

A forgalomirányító 3. rétegbeli készülék. Képes végrehajtani az alacsonyabb rétegekben elhelyezkedő eszközök feladatait, valamint 3. rétegbeli információk alapján meghatározni a célhoz vezető legjobb útvonalat. Hálózatok összekapcsolására elsődlegesen forgalomirányítókat használnak. Egy forgalomirányító minden egyes portja különböző hálózathoz csatlakozik és az ezek között áramló csomagok irányításáért felel. A forgalomirányítók képesek az üzenetszórás és az ütközési tartományok felosztására.

A forgalomirányító kiválasztásakor, a készülék jellemzőit és a hálózat követelményeit kell összeegyeztetni. A kiválasztáskor a következő tényezőket kell figyelembe venni:

- A kapcsolódás típusa
- Rendelkezésre álló szolgáltatások
- Költség

Kapcsolódás

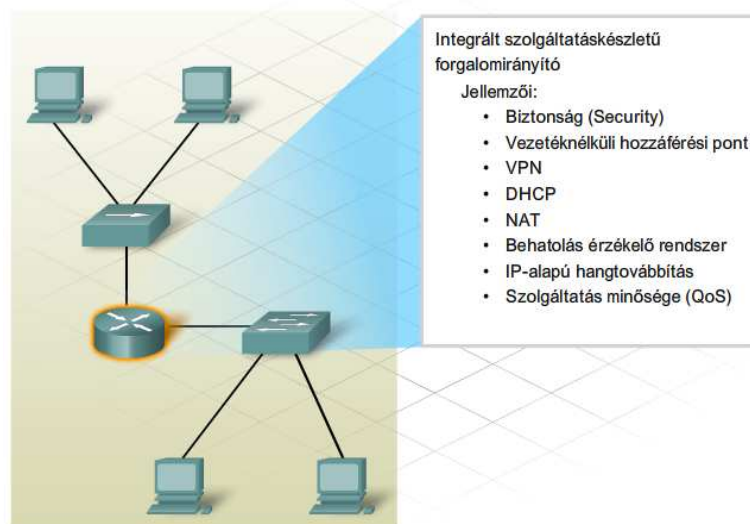
A forgalomirányítók képesek különböző technológiával rendelkező hálózatok összekapcsolására. Rendelkezhetnek LAN és WAN interfészekkel is.

A forgalomirányító LAN interfésze a helyi hálózat átviteli közegéhez csatlakozik. Ez leggyakrabban UTP kábeleztést jelent, de modulok hozzáadásával optikai kábelek használatára is nyílik lehetőség. A forgalomirányító sorozatától vagy modelljétől függően több interfész típus használható LAN, illetve WAN kábelek csatlakoztatására.

Jellemzők

A forgalomirányító jellemzőinek összhangban kell lenniük a hálózat követelményeivel. A vizsgálat után, az üzletvezetés meghatározhatja, hogy pontosan milyen funkciókkal rendelkező forgalomirányítóra lesz szükség. Az alapvető forgalomirányítási funkciókon kívül a következő szolgáltatások álnak rendelkezésre:

- Biztonság (Security)
- Szolgáltatás minősége (QoS)
- IP-alapú hangátvitel (VoIP)
- Hálózati címfordítás (NAT)
- Dinamikus állomáskonfiguráló protokoll (DHCP)
- Virtuális magánhálózat (VPN)



Költségek

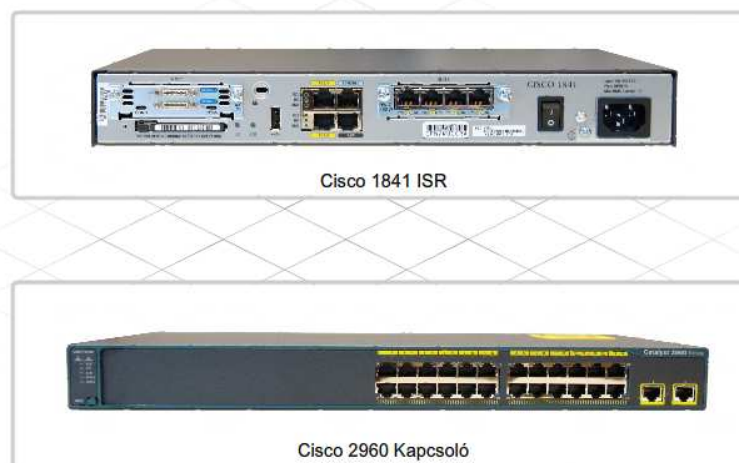
Hálózati eszközök kiválasztásakor mindig fontos szempont a költségvetés. A forgalomirányítók drága berendezések, és a bővítő modulok, például optikai szálmodulok hozzáadása tovább növeli a költségeket.

Viszonylag új technológiát képviselnek az integrált szolgáltatású forgalomirányítók (ISR), melyek egy eszközben számos szolgáltatást ötvöznek. Az ISR eszközök bevezetése előtt számos berendezés használatára volt szükség az adat, a vezetékes, a vezeték nélküli, a hang, a videó, a tűzfal és a VPN technológiák teremtette követelmények biztosításához. Az ISR eszközöket több szolgáltatás ellátására tervezték, hogy kielégítsék a kis és közepes méretű vállalkozások, illetve a nagyobb szervezetek kirendeltségeinek igényeit. ISR-ek segítségével egy szervezet gyorsan és könnyen képes végponttól végpontig kiterjedő védelmet nyújtani felhasználók, alkalmazások, hálózati végpontok és vezeték nélküli helyi hálózatok számára. Ráadásul egy ISR eszköz költsége jóval kisebb is lehet, mintha az egyes szolgáltatásokat biztosító készülékeket külön-külön vásárolnánk meg.

3.3.6 Hálózati berendezések fejlesztése

Számos kisméretű hálózatot kezdetben alsó kategóriás integrált forgalomirányító segítségével építettek meg a vezetékes és vezeték nélkül felhasználók csatlakoztatására. E forgalomirányítókat kisebb, rendszerint néhány vezetékes és esetleg négy-öt vezeték nélküli eszközt tartalmazó hálózatok létrehozására tervezték. Mihelyt a kisvállalkozás kinövi a meglévő hálózati berendezések nyújtotta lehetőségeket, a vállalatnak nagyobb teljesítményű, robosztusabb eszközökre lesz szüksége. Ilyen eszközök például a Cisco 1841 ISR és a Cisco 2960 kapcsoló, melyekkel jelen tanfolyam keretein belül megismerkedünk.

A Cisco 1841-et kirendeltségek vagy közepes méretű vállalkozások forgalomirányítási feladatainak ellátására tervezték. Belépő szintű többcélú forgalomirányítóként, számos különböző kapcsolódási lehetőséget kínál. Moduláris felépítésű eszköz, és többféle biztonsági szolgáltatás használatára is lehetőséget ad.



Az alábbiakban a Catalyst 2960 kapcsolók néhány jellemzőjét mutatjuk be:

- Belépő szintű, vállalati felhasználásra tervezett, fix konfigurációjú kapcsoló, melyet a hozzáférési rétegben történő felhasználásra optimalizáltak
- Fast és Gigabit Ethernet portokkal rendelkezik munkaállomások csatlakoztatására
- Használata elsősorban kis-, középvállalati és kirendeltségi környezetben előnyös
- Kompakt mérete kábelszekrényen kívüli használatra is alkalmassá teszi

Ezek a kapcsolók a kisebb, beépített kapcsolófunkcióval is rendelkező ISR berendezésekkel ellentétben sok porttal rendelkeznek, és nagy kapcsolási sebességet biztosítanak. Jó választás lehet olyan hálózati fejlesztések esetén, melyekben hubokat vagy kis ISR eszközöket használnak.

A Cisco Catalyst 2960 Series Intelligent Ethernet Switches család tagjai fix kiépítésű, önálló eszközök, amelyek munkaállomások Fast és Gigabit Ethernet csatlakozását biztosítják.

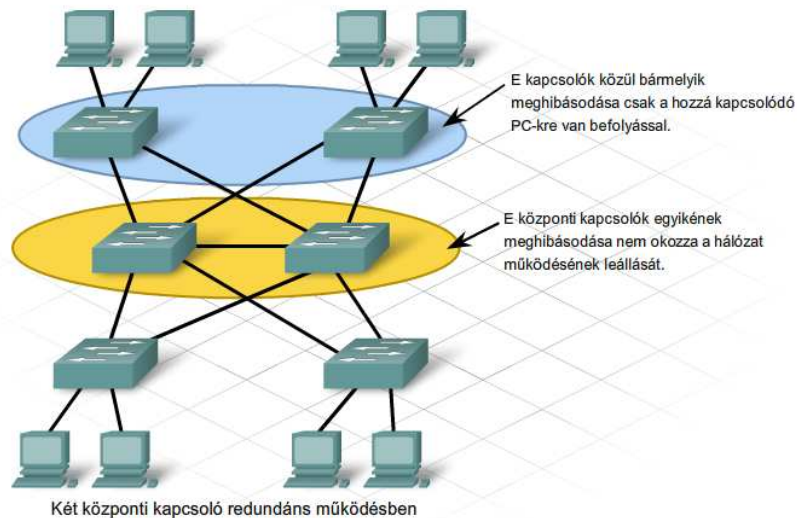


3.3.6 Tervezési megfontolások

A hálózati eszközök beszerzése és a kábelhálózat kiépítése csak a korszerűsítési folyamat kezdetét jelentik. A hálózatoknak azonban megbízhatóknak és folyamatosan rendelkezésre állóknak kell lenniük. A megbízhatóság redundáns hálózati összetevők, például egy helyett két forgalomirányító használatával, megvalósítható. Ebben az esetben alternatív útvonalak jönnek létre, így ha az egyik forgalomirányító esetében problémák lépnek fel, az adatok egy másik útvonalon juthatnak el a célállomáshoz.

A megbízhatóság növelése nagyobb rendelkezésre állást biztosít. Például a távbeszélő rendszerektől öt-9-es rendelkezésre állást várnak el. Ez azt jelenti, hogy a távbeszélő rendszernek az idő 99,999%-ában rendelkezésre kell állnia. A távbeszélő rendszer nem állhat, vagy lehet elérhetetlen az idő 0,001%-ánál tovább.

A hálózat megbízhatóságát általában a hibatűrő kialakításával javítják. A hibatűrő rendszerek tartozékai a szünetmentes tápegységek (UPS), a redundáns váltakozó áramú tápegységek, a menet közben cserélhető eszközök, a kettőzött illesztőkártyák és a tartalék rendszerek. Amikor valamelyik eszköz meghibásodik, a redundáns vagy tartalék rendszer átveszi a meghibásodott eszköz szerepkörét, hogy a megbízhatóság lehető legkisebb mértékben sérüljön. A hibatűrő rendszerek közé tartoznak a tartalék kommunikációs kapcsolatok is.



IP címzési terv

A hálózattervezés folyamatának részét képezi a logikai címzés tervezése is. Hálózatok fejlesztése során a 3. rétegbeli címzési séma megváltoztatása komoly feladat. Ha a korszerűsítés a hálózat szerkezetének a megváltozásával jár, valószínűleg elkerülhetetlen az IP címzési séma megváltoztatása.

Az IP címzési tervnek számolnia kell minden IP-címet igénylő eszközzel, és a jövőbeni növekedéssel is. IP-címet igénylő állomások és hálózati eszközök:

- Felhasználói számítógépek
- Adminisztrátori számítógépek
- Kiszolgálók
- Egyéb végponti eszközök, például nyomtatók, IP telefonok, IP kamerák
- Forgalmirányító LAN interfészek
- Forgalmirányító WAN (soros) interfészek

Vannak más eszközök, amelyeknek a konfigurálásukhoz és felügyeletükhöz van szükségük IP-címre. Ilyen eszközök:

- Egyedülálló kapcsolók
- Vezeték nélküli hozzáférési pontok

Ha például egy új forgalmirányítót telepítenek a hálózatra, a forgalmirányító minden interfésze további hálózatok vagy alhálózatok létrehozására használható. Ezekhez az új alhálózatokhoz megfelelő IP hálózati cím és alhálózati maszkot kell rendelni. Néha ez csak egy teljesen új címzési rendszer elkészítésével oldható meg.

A tervezési fázis befejezése után a korszerűsítési folyamat a kivitelezési fázissal folytatódik, melyben megkezdődik a tényleges hálózattervezés.

3.4 A fejezet összefoglalása

- A hálózati fejlesztések tervezése előtt helyszíni felmérést kell végezni a meglévő hálózat szerkezetének dokumentálásához.
- A dokumentációnak tartalmaznia kell a hálózat fizikai és logikai topológiatérképét és az eszköztárat.
- Felmérések és beszélgetések segítségével össze kell gyűjteni az ügyfélnek a hálózattal szembeni elvárásait.
- Amennyiben nélkülözhetetlenné válik egy hálózat korszerűsítése, rendelkezni kell az ehhez szükséges tervvel, melyhez figyelembe kell venni a hálózat telepítése során felmerülhető erősségeket, gyenge pontokat, lehetőségeket és veszélyforrásokat (SWOT).
- A hálózati fejlesztés folyamat öt fázisból áll: követelmények gyűjtése, kiválasztás és tervezés, megvalósítás, működés, áttekintés és kiértékelés.
- A hálózati felszerelések vizsgálata során érinteni kell a fizikai környezetet, a telekommunikációs helyiségeket (MDF és IDF), valamint a meglévő hálózati kábelezést.
- Kábelezés során négy különböző fizikai területet kell figyelembe venni: munkaterület, elosztási terület, telekommunikációs helyiség területe és a gerinchálózati terület.
- A kábelezési munkálatok meghatározásakor figyelembe kell venni a munkaterületet, a felhasznált kábelek típusát és a kábel rendeltetését.
- A strukturált kábelezési munkálatok során a kábelek lefektetésével, a kábelszekrények elhelyezésével, a kábelek nyilvántartásával és különböző villamossági kérdésekkel kell foglalkozni.
- Abban az esetben, ha a továbbfejlesztés során új hálózati eszközre van szükség, kétféle beszerzési módra nyílik lehetőség: felügyelt szolgáltatás és házon/vállalaton belüli vásárlás.
- A magasabb OSI rétegben működő eszköz általában intelligensebb eszköznek tekinthető.
- Hálózati eszközök továbbfejlesztése során a költséget és a bővíthetőséget mindenképpen figyelembe kell venni.

4. A címezési struktúra tervezése

4.1 IP-címzés LAN-okba

4.1.1 IP-címek áttekintése

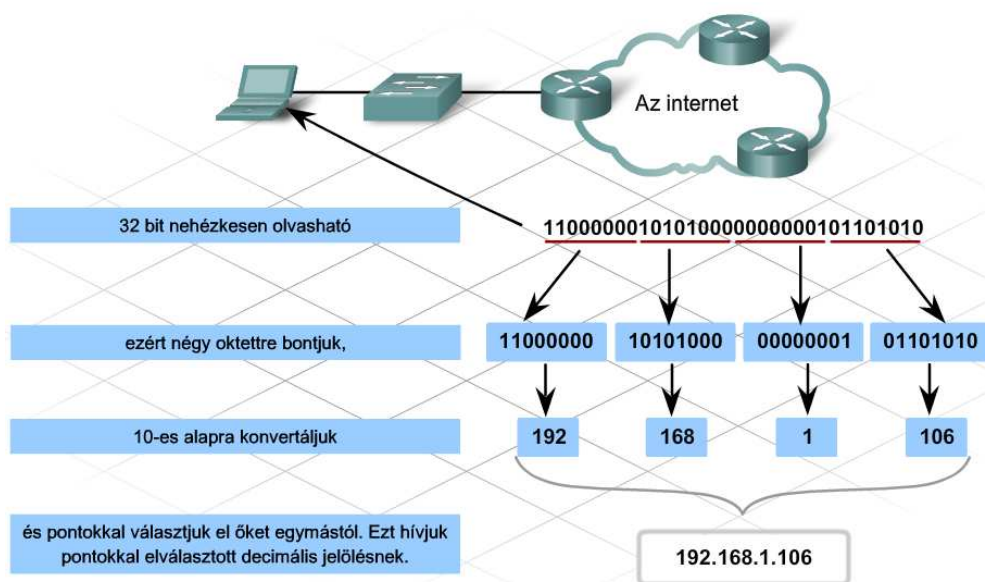
A számítógépes hálózatokon történő kommunikáció egyik legfontosabb eleme az IP-címzés rendszere.

Az IP-címzés egy eljárás, amelynek célja az állomások és a hálózatok azonosítása. Az idő előrehaladásával az internet folyamatosan növekedett, a bekötött állomások száma nőtt, az IP-címzés rendszerének pedig alkalmazkodnia kellett a növekedéshez.

Bár az IP-címzés rendszere folyamatosan változik, az IPv4 alapvető IP-cím struktúrája változatlan. Az IP hálózaton történő üzenetküldéshez és üzenetfogadáshoz minden hálózati állomáshoz hozzá kell rendelni egy egyedi 32 bites IP-címet. Mivel az emberek számára a hosszú bináris számok nehezen olvashatók és értelmezhetők, az IP-címetek rendszerint pontokkal elválasztott tízes számrendszerbeli számokkal ábrázoljuk. Ennél a jelölésnél a négy darab, nyolc bináris számjegyből álló blokkot (oktetet) átváltjuk tízes számrendszerbe, és pontokkal választjuk el egymástól őket. Például, a következő IP-címet:

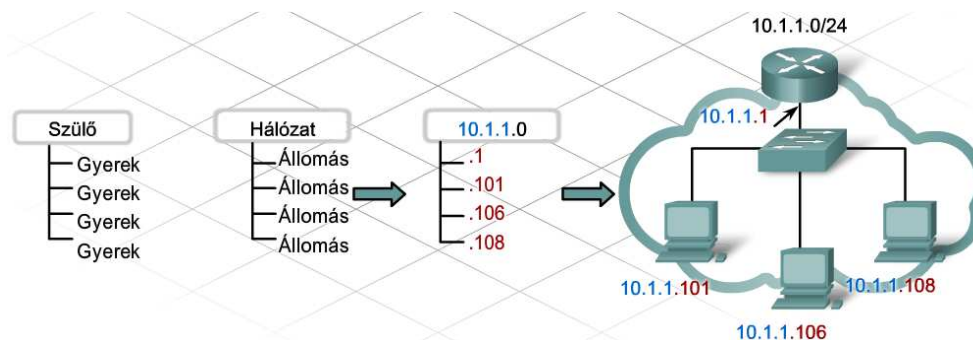
11000000.10101000.00000001.01101010

tízes számrendszerben, pontokkal elválasztva, 192.168.1.106 alakban ábrázolunk.



Az IP-címek hierarchikusak. A hierarchiát úgy képzeljük el, mint egy családfát, ahol a szülők a fa tetején helyezkednek el, és a gyerekek alulról csatlakoznak hozzájuk. A hálózatonál ez úgy néz ki, hogy a 32 bites szám egy része a hálózatot (a szülőket), míg a maradék az állomásokat azonosítja (gyerekek). Az internet hőskorában olyan kevés szervezetnek volt szüksége internetcsatlakozásra, hogy a hálózatokat az IP-cím első 8 bitje (első oktet) jelölte. A fennmaradó 24 bitből képezték a helyi állomások címeit.

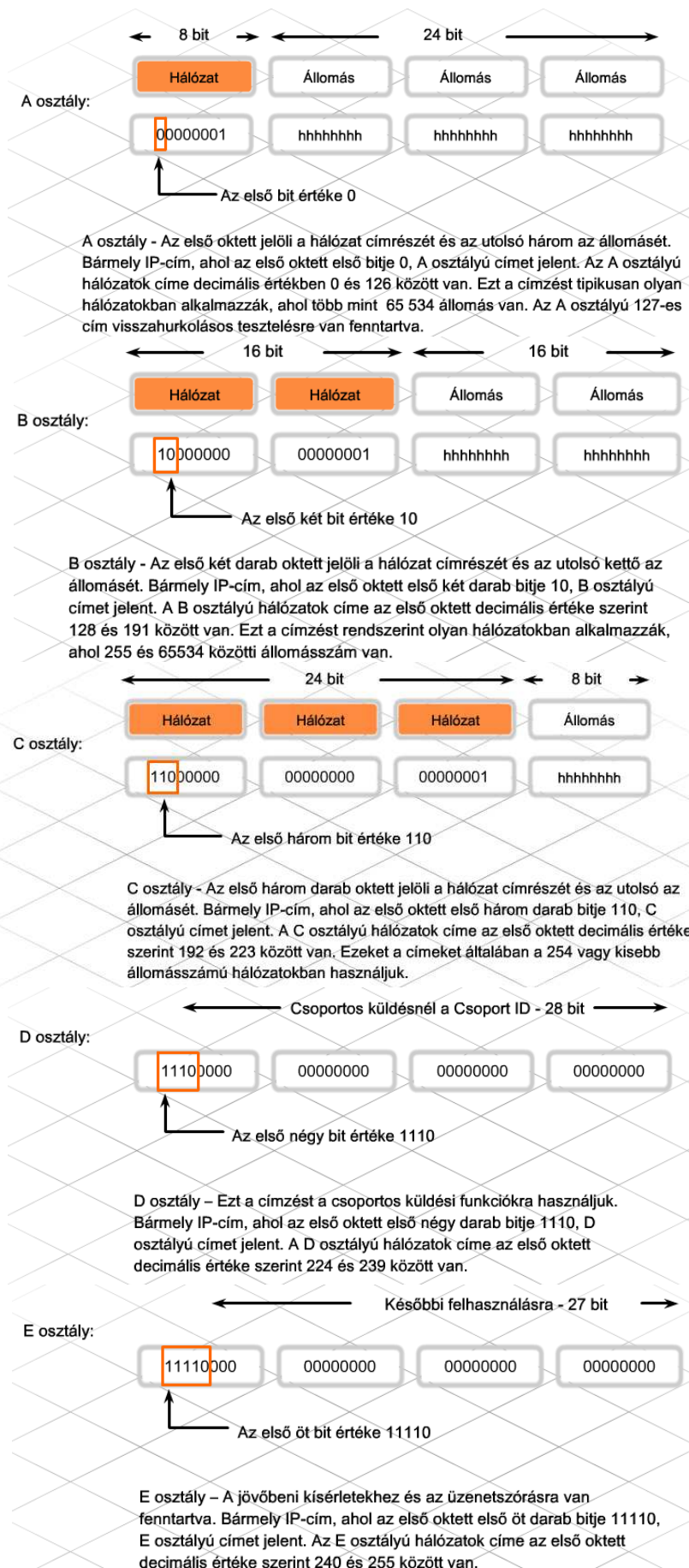
A 8 bites hálózati jelölés logikusnak tűnt, mivel eredetileg mindenki úgy gondolta, hogy az internet néhány nagy egyetemből, a kormányból, és katonai szervezetekből fog állni. A 8 bites hálózati azonosítóval 256 különböző hálózatot lehetett létrehozni, darabonként 16 millió állomással. Hamar kiderült, hogy jóval több szervezet illetve magánszemély végez kutatómunkát az interneten, vagy kommunikál másokkal. Több hálózatra volt szükség, és több hálózati azonosító létrehozását kellett megoldani.



A nagyszámú hálózat azonosításához a 32 bites címtartományt öt cím-osztályra bontották fel. Ezek közül három, az A, B és C osztályok az állomások vagy hálózatok egyedi azonosítására használható, míg a maradék két osztály, a D és az E csoportos címzés (multicast), illetve kísérleti célokra használható.

Az IP címtartomány cím-osztályokra bontása előtt a forgalomirányítók a hálózatok azonosítására csak az IP-címek legmagasabb helyiértékű 8 bitjét használták. Ezzel szemben a B osztályú hálózati címek 16 legmagasabb helyiértékű bitje azonosítja a hálózatokat, a C osztályú hálózati címek esetén pedig a cím 24 legmagasabb helyiértékű bitje szolgál ugyanerre a célra. A cím-osztályokra bontás után a forgalomirányítókat át kellett programozni azért, hogy azok figyelembe vegyék az első 8 biten túli tartományt is, és így a B és C osztályú hálózatokat is tudják kezelni.

Úgy döntöttek, hogy a hálózatokat olyan módon osztják fel, hogy a forgalomirányítók és az állomások könnyen és helyesen állapíthassák meg a hálózatot azonosító (hálózati ID) bitek számát. A hálózati osztályt az IP-cím első pár bitje adja meg, ezek a legmagasabb helyiértékű bitek. Ha az első bit 0, a hálózat A osztályú, és az első 8 bit (első oktet) azonosítja a hálózatot. Ha az első bit 1, a forgalomirányító megvizsgálja a második bitet. Ha a második bit 0, akkor a hálózat B osztályú, és a forgalomirányító az első 16 bittel azonosítja a hálózatot. Ha az első három bit 110, akkor az C osztályt jelent. A C osztályú címek az első 24 bitet, azaz három oktetet használnak a hálózat azonosítására. Az eredeti 8 bites hálózati mezőt kisebb osztályokra bontva a lehetséges hálózatok száma az eredeti 256-ról két milliónál is többre növekedett.



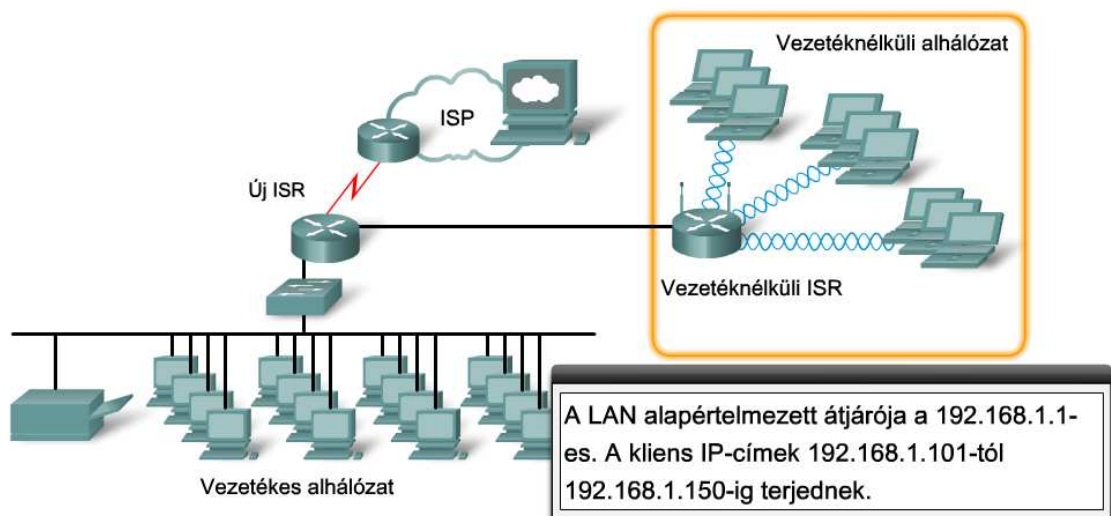
A különféle osztályok létrehozásán túlmenően az Internet Engineering Task Force (IETF) úgy döntött, hogy az internetes címtartomány egy részét a magánhálózatoknak tartja fenn. A magánhálózatok nem csatlakoznak a nyilvános hálózatokhoz. A magánhálózati címek nem alkalmasak forgalomirányításra az interneten. Így több hálózat, több különböző helyen használhatja ugyanazt a magánhálózati címezést címütközés nélkül.

A magánhálózati címtartomány használatával csökkent a szervezetek számára kijelölt egyedi IP-címek száma.

Egyetlen A osztályú cím, a 10.0.0.0 van magáncélokra fenntartva. Ezenkívül, a B és a C osztályokban is kijelöltek erre a célra fenntartott címtartományokat.

A legtöbb mai hálózat a magánhálózati címezési módot használja. A legtöbb, kereskedelemben kapható hálózati eszköz alapbeállításként magánhálózati címeket oszt ki a DHCP-n keresztül. Csupán az internethez közvetlenül kapcsolódó eszközökhöz van regisztrált, az interneten forgalomirányíthatásra alkalmas cím hozzárendelve.

Osztály	Privát IP-címek (RFC 1918)	Az alapértelmezett alhálózati maszk	A hálózatok száma	Állomások hálózatonként	Az összes állomás
A	10.0.0.0-től 10.255.255.255-ig	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0-től 172.31.255.255-ig	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0-től 192.168.255.255-ig	255.255.255.0	256	254	65,024



4.1.2 Alhálózatok a hálózatban

Az 1980-as és 90-es években a hálózatok folyamatosan növekedtek, egyre több hálózat csatlakozott az internetre, sok szervezet több száz, sőt több ezer állomással bővítette a hálózatát. Egy több ezer állomással rendelkező szervezet kiszolgálására tulajdonképpen jól megfelelne egy B osztályú hálózat, de azért ezzel akadtak problémák.

Először is, alig fordult elő olyan, hogy a több ezer állomással rendelkező szervezeteknél az állomások egy helyen lettek volna. Néhány szervezet biztonsági vagy irányítási okok miatt akarta szétválasztani a különböző részlegeket egymástól. Másodszor, a hálózaton küldött csomagok közül az



üzenetszórásos az egyik fő típus. Az üzenetszórási csomagokat minden állomáshoz elküldjük az adott logikai hálózaton belül. Ha több ezer állomás bonyolít üzenetszórásos forgalmat egy hálózaton, és a hálózat sávszélessége korlátozott, a hálózat teljesítménye további állomások hozzáadásakor jelentősen csökken.

Az internet fejlődésében vezető szerepet betöltő szervezetek a problémát úgy oldották meg, hogy hálózataikat kisebb minihálózatokra vagy alhálózatokra bontották az úgynevezett alhálózatokra való bontás (subnetting) felhasználásával. Hogyan lehetséges egy adott IP hálózatot több hálózatra osztani úgy, hogy ezek az alhálózatok mind önállóként viselkedjenek?

Az RFC 917, az internet-alhálózatok szabványa az alhálózati maszkot egy olyan eljárásként definiálja, amelyet a forgalomirányítók arra használnak, hogy a teljes IP-címből meghatározzák a hálózatazonosításra szolgáló címrészt. Amikor a forgalomirányító egy csomagot fogad, a benne levő cél IP-címet és a forgalomirányító táblájában levő útvonalakkal társított alhálózati maszkot használja arra, hogy a csomag helyes útvonalát meghatározza.

A forgalomirányító balról-jobbra, bitről-bitre kiolvassa az alhálózati maszkot. Ha egy bit értéke az alhálózati maszkban 1-re van állítva, akkor az azt jelzi, hogy a hozzátartozó pozícióban található érték a hálózati azonosító része. Az alhálózati maszk 0 értéke jelzi, hogy a kérdéses pozícióban levő érték az állomás azonosításához tartozik.

IP-címosztályok						
Címosztály	Az első oktet tartománya (decimálisan)	Az első oktet bitei (a zöld bitek nem változnak)	A cím hálózati (N) és az állomást azonosító (H) részei.	Az alapértelmezett alhálózati maszk (decimális és bináris).	A lehetséges hálózatok és hálózatonkénti állomások száma.	Megjegyzés és az állomáscímek tartománya**.
A	1 - 127*	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	128 hálózat (2 ⁷) 16 777 214 állomás hálózatonként (2 ²⁴⁻²)	Kereskedelmi 1.0.0.1 - 126.255.255.254
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.1111.00000000.00000000	16 384 hálózat (2 ¹⁴) 65 534 állomás hálózatonként (2 ¹⁶⁻²)	Kereskedelmi 128.0.0.1 - 191.255.255.254
C	192-223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.1111.11111111.00000000	2 097 152 hálózat (2 ²¹) 254 állomás hálózatonként (2 ⁸⁻²)	Kereskedelmi 192.0.0.1 - 223.255.255.254
D	224- 239	11100000 - 11101111	Nem használható fel kereskedelmi célra, mint állomás.			Adatszórás (lefoglalt) 224.0.0.1 - 239.255.255.254
E	240 - 255	11110000 - 11111111	Nem használható fel kereskedelmi célra, mint állomás.			Kísérleti célokra (lefoglalt) 240.0.0.1 - 255.255.255.255

* Az A osztályú 127.0.0.0-es cím a visszacsatolás tesztelésére van fenntartva.

** A csupa nulla (0) és csupa egyes (1) érvénytelen állomás címek.

Az eredeti IP-cím hierarchiában két szint létezik: a hálózat és az állomás szintje. Az osztályalapú rendszerben az első három kezdőbit az IP-cím A, B, vagy C osztályba tartozását hivatott jelölni. Ha egy címet már osztályba soroltunk, a hálózatot és az állomásokat azonosító (állomás ID) bitek száma jól ismert. A hálózati osztályokhoz tartozó alapértelmezett maszkok a következők:

A osztály 255.0.0.0

B osztály 255.255.0.0

C osztály 255.255.255.0

Egy adott osztályba tartozó hálózat tovább bontása új szintet hoz létre a hálózati hierarchiában. Három szinttel dolgozunk: egy hálózati, egy alhálózati és egy állomás szinttel. Hogyan kell az alhálózati maszkot beállítani, hogy az jelezze a hierarchia új szintjét?

Az egyes A, B, vagy C osztályú hálózati címtartományok sok alhálózatra bonthatók az állomás címtartományát meghatározó biteknek az alhálózat azonosítására történő felhasználásával. Nézzünk

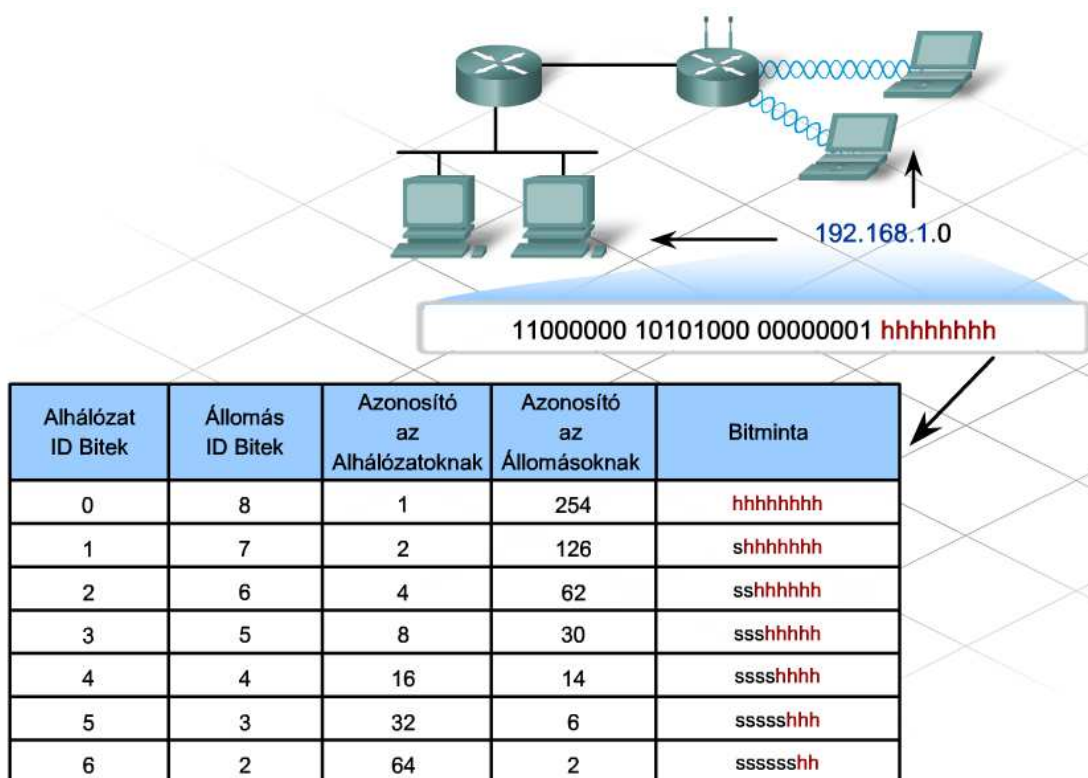
egy példát! Egy szervezet C osztályú címtartományt használ, két irodája van két különböző épületben. A könnyebb menedzselhetőség érdekében a hálózati adminisztrátor mindegyik helyszínt logikailag egy külön hálózatnak szeretné látni. Ha az állomások címtartományából két bitet felhasználunk, az alhálózati maszk 24-ről 26 bitre növekszik, vagyis 255.255.255.192 lesz.

Ha az állomásokhoz tartozó címrészből veszünk kölcsön biteket a hálózat azonosításához, kevesebb bit marad szabadon az egyéni állomásoknak. Ha az alhálózat ID két bitet használ fel, akkor csak hat bit marad a címből az állomások részére.

A hagyományos osztály alapú alhálózatokra bontáskor az egyazon osztályból létrehozott alhálózatok azonosítására szigorúan azonos számú biteket használunk. Ez a fajta alhálózatokra bontás ezért mindig azonos méretű, azonos számú állomást kezelni tudó alhálózatot eredményez. Ezért ezt a módszert azonos méretű alhálózatokra bontásnak nevezzük.

Komoly tervezést igényel eldönteni, hogy hány állomás biteket használjunk az alhálózat azonosítására. Két dolgot kell figyelembe venni: a hálózatokon levő állomások számát, és hány darab különálló hálózatra van szükség. A 192.168.1.0 hálózat alhálózati lehetőségeit bemutató táblázatból kiderül, hogyan befolyásolja az alhálózati azonosító bitek számának kiválasztása mind a lehetséges alhálózatok számát, mind pedig az azokban lévő állomások számát.

Egy dolgot azonban nem szabad elfelejteni: minden IPv4 hálózatban a csak nullából, illetve a csupa egyesből álló állomáscím más célra van fenntartva. Az a cím, amely az állomás részénél csupa nullából áll, érvénytelen állomáscím, és rendszerint az egész hálózatot vagy alhálózatot jelöli. Az a z állomást jelölő résznél a csupa egyesből álló cím a helyi hálózat üzenetszórásos címe. Ha egy hálózatot alhálózatra bontunk, minden alhálózat tartalmaz egy csak nullából, illetve csak egyesekből álló állomás címet, amelyeket nem használhatunk fel egyéni állomások címeként.



4.1.3 Egyedi alhálózati maszkok

Ha egy hálózatot alhálózatokra bontunk, a forgalomirányítónak megfelelően korrigált, egyedi alhálózati maszkra van szüksége, hogy az alhálózatokat egymástól meg tudja különböztetni.

Az alapértelmezett hálózati maszk és az alhálózati maszk abban különbözik egymástól, hogy az alapértelmezett maszkok csak oktetthatáron változnak. Például, egy A-osztályú hálózat alapértelmezett hálózati maszkja 255.0.0.0. Az alhálózati maszkok az állomás azonosító részből vesznek át biteket és hozzáadják őket az alapértelmezett alhálózati maszkhoz.

Ha egyedi alhálózati maszkot hozunk létre, az első kérdés: hány bitet vegyünk el az állomás azonosítóból és adjunk hozzá az alhálózati maszkhoz? Egy adott számú alhálózat létrehozásához szükséges kölcsönveendő bitek számát a következő matematikai egyenlőség fejezi ki: 2^n , ahol az n a kölcsönveendő bitek számával egyenlő.

Ha három alhálózatra van szükség, akkor elegendő bitnek kell lennie három egyedi alhálózati címhez.

Például, ha C-osztályú címből indulunk ki, mint például a 192.168.1.0, akkor csak 8 állomásbit van, amiből kölcsönvehetünk. A bitek mindegyike 1, vagy 0 lehet. A három alhálózat létrehozásához a nyolcból legalább két bitet kölcsön kell venni. Ebből összesen négy alhálózat áll elő:

00 - 1. alhálózat

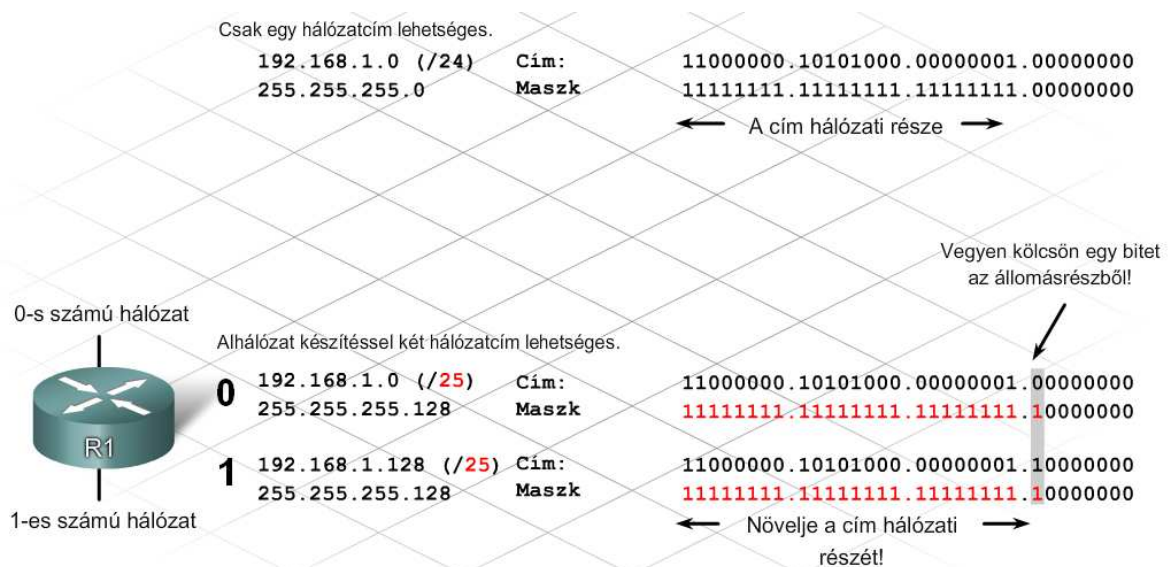
01 - 2. alhálózat

10 - 3. alhálózat

11 - 4. alhálózat

A fenti példában 2 bitet vettünk kölcsön, $2^2 = 4$ vagy $2 \times 2 = 4$, azaz négy alhálózat jött létre. Ha öt és nyolc közötti számú alhálózatra lenne igény, akkor három bitre lenne szükség ($2^3 = 8$ vagy $2 \times 2 \times 2$).

Az alhálózati azonosító számára felhasznált bitek száma mind a létrehozható lehetséges alhálózatok számát, mind az egyes alhálózatokban levő állomások lehetséges számát befolyásolja.



Címzési séma: példa két hálózatra

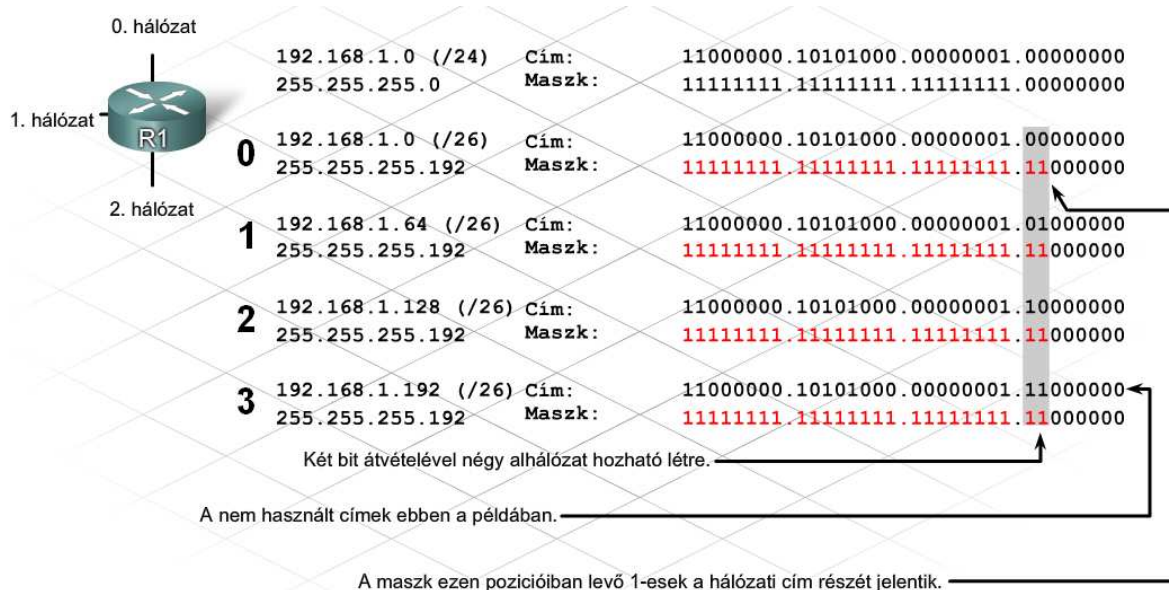
Alhálózat	Hálózati cím	Állomáscímek tartománya	Szórási cím
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Az osztály alapú alhálózatok létrehozásakor az alhálózati azonosítókhoz szükséges bitek száma két tényezőtől függ: a létrehozott alhálózatok számától és az alhálózatonkénti állomások számától.

Az osztály alapú, vagy rögzített hosszúságú alhálózatok létrehozásánál minden alhálózatnak egyforma méretűnek kell lennie, azaz az állomások száma, amelyet az alhálózatok tartalmazhatnak, ugyanakkora minden létrehozott alhálózaton. Minél több bitet használunk fel az alhálózat címéhez, annál kevesebb marad az állomások azonosítására.

Ugyanazzal az alapvető képlettel: 2^n , egy kis módosítás után meghatározhatjuk a rendelkezésre álló állomásazonosítók számát a fennmaradó állomásbitek alapján. A két, minden alhálózat által fenntartott állomás cím, a csupa 0 illetve a csupa 1 miatt, a támogatott állomások száma a következő módosított formulával számítható ki: $2^n - 2$.

Miután meghatároztuk, hogy hány bitből áll az alhálózati cím, az alhálózati maszk révén a hálózatba kapcsolt eszközök értesülnek az alhálózatokra bontásról. Az alhálózati maszkkal így megadható, hogy egy adott IP-cím melyik alhálózatban van, és ezáltal egyszerű, osztályalapú alhálózati IP-címzési sémákat lehet kialakítani.



Egy címzéstervezet: példa a négy hálózatról

Alhálózat	Hálózati cím	Állomáscím-tartomány	Szórási cím
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Több alhálózat áll rendelkezésre, de alhálózatonként kevesebb címmel.

Az eredeti osztályalapú hálózati címtartományok számos problémáját megoldotta az alhálózatokra bontás. Lehetővé tette az A, B vagy C-osztályú címtartománnyal rendelkező szervezeteknek, hogy a címtartományukat kisebb, helyi alhálózatokra osszák, és így hatékonyabban gazdálkodjanak a címekkel. Az alhálózatokra bontás azért is fontos, mert segítségével a forgalom okozta terhelést csökkenteni lehet, és biztonsági intézkedéseket lehet a hálózatok között foganatosítani.

Az alhálózatokra bontás szükségességének tipikus példája az az ügyfél, aki kinőtte az internetszolgáltatójától kezdetben telepített hálózatot. Ebben a hálózatban az eredeti kis, beépített vezeték nélküli forgalomirányítót túlterheli a vezetékes és a vezeték nélküli felhasználók forgalma. Mivel viszonylag kis kiterjedésű a hálózat, C osztályú címtartományt használnak a címek kiosztásához.

A túlterhelt hálózat problémájának egy lehetséges megoldása az, hogy egy második hálózati eszközt állítunk be, például egy nagyobb integrált szolgáltatású forgalomirányítót (ISR). Hálózati eszköz hozzáadásakor bevált taktika, hogy a biztonság növelése érdekében a vezetékes és a vezeték nélküli felhasználókat külön helyi alhálózatra teszik. Az eredeti vezeték nélküli forgalomirányítóval továbbra is biztonságosan kiszolgálhatjuk a vezeték nélküli felhasználókat. Hubok vagy kapcsolók segítségével a vezetékes felhasználók közvetlenül csatlakoztathatók az új, másik hálózatot használó ISR-hez. Az ISR és a vezeték nélküli forgalomirányító ezután közvetlenül csatlakoztatható egy harmadik hálózathoz.

Az új hálózati konfiguráció megkívánja, hogy a meglévő C osztályú hálózatot legalább három alhálózatra bontsuk. Az osztályalapú alhálózatokra való bontásnál legalább két bitet el kell vennünk az állomások címrészből, hogy az igényeket kielégíthessük. Ez az alhálózati séma végül négy egyedi alhálózat létrehozását fogja eredményezni, egyenként 62 szabad állomás címmel (64 lehetségesből leszámítva a csak nullából ill. csak egyesből álló címeket).

4.1.4 VLSM és osztályok nélküli tartományközi forgalomirányítás (CIDR)

Az eredeti, osztályalapú alhálózatokra bontás megkövetelte, hogy az egy hálózathoz kialakított alhálózatok mindegyike azonos méretű legyen. Ennek az az oka, hogy a forgalomirányítók útvonalfrissítései korábban nem tartalmaztak maszk információt. A forgalomirányítók az irányító tábla kitöltésekor a maszk-értékeket az interfészeiken beállított cím- és maszk-értékek alapján határozták meg és az azonos hálózathoz származó alhálózatok mindegyikénél az így meghatározott maszkot alkalmazták. Ez a megkötés az IP-kiosztás tervezésekor a rögzített hosszúságú alhálózati maszkok használatát igényelte.

Ugyanakkor a rögzített hosszúságú alhálózati maszkok miatt jelentős számú IP-cím vesztett kárba. Például, egy szervezet székhelyén 8000, míg máshol 1000, 400 és 100 állomás van helyszínenként. A rögzített hosszúságú alhálózati maszk alhálózatonként 8000 állomást támogatna, ott is, ahol csak 100-ra van szükség.

A változtatható hosszúságú alhálózati maszkolás (VLSM) segít a probléma megoldásában. A VLSM címezéssel ugyanis egy hálózat különböző méretű hálózatokra bontható, amit az alhálózatok újabb alhálózatokra való bontásával érünk el. Emiatt a ma használt forgalomirányítók olyan útvonal-leíró üzeneteket továbbítanak, amelyek a hálózatok IP-címei mellett az ezekhez tartozó maszkokat is tartalmazzák. Így az IP-címek hálózat-azonosító részét alkotó bitek száma pontosan meghatározható. A VLSM-mel az IP-címek ezrei lesznek megmenthetők, amelyek a hagyományos osztályalapú alhálózatokra bontással elvesznének.

Az RFC 1519-es szabványban javasolták és el is fogadták a VLSM mellett az osztályok nélküli tartományközi forgalomirányítást (CIDR) is. A CIDR a magasabb helyiértékű biteket alapul véve figyelmen kívül hagyja a hálózati osztályokat. A CIDR egyedül a hálózati előtag biteinek száma alapján azonosítja a hálózatokat, ez a szám az egyesek számának felel meg az alhálózati maszkban. Egy IP-cím CIDR átírása például így néz ki: 172.16.1.1/16 ahol a /16 a hálózati előtagban levő bitek számát jelenti.

A CIDR protollokat használó forgalomirányítók már nem csak az IP-címek legmagasabb helyiértékű bitei alapján képesek a hálózati címrészt meghatározni. A korábbi korlát feloldásával az a kényszer is megszűnt, hogy a regisztrált IP-címek kiosztása kizárólag címosztályok szerint lehetséges.

A CIDR használata előtt egy internetszolgáltatónak, ha 3000 állomáscímre volt szüksége, vagy egy teljes B osztályú címtartományt, vagy sok C osztályú hálózati címet kellett kérvényeznie az igények teljesítéséhez. A B osztályú címtartománnyal az internetszolgáltató a regisztrált címek ezreit pocskolná el. Ha sok C osztályú címet kérvényez, bonyolult lesz az internetszolgáltató hálózatot megtervezni úgy, hogy egyetlen egy hálózat se igényeljen 254-nél több állomáscímet. A sok C osztályt tartalmazó forgalomirányító táblák nagyok lesznek és a használatuk bonyolult.

A hagyományos címosztályok figyelmen kívül hagyásával a CIDR lehetővé teszi az internetszolgáltatónak, hogy a szükséges állomásszámnak megfelelő címblokkokat igényeljen. A mamuthálózatok, amelyek a C-osztályú címek nagy blokkokba kombinálásával jöttek létre, lehetővé teszik a címek hatékonyabb kiosztását. Például egy mamuthálózat (supernet) címe 192.168.0.0/19. Az IP-cím első 19 bitjét használja hálózati előtagnak, ami 8190 lehetséges állomáscímet tesz lehetővé számára. Az internetszolgáltató használhatja a mamuthálózatot mint egy nagy egészet, vagy annyi kisebb darabra bonthatja, ahányra igény van.

A mamuthálózat példában a magánhálózati C-osztályú 192.168.0.0 címet használtuk. A valóságban a legtöbb magáncímzést használó hálózat alhálózatokra bontott A-, vagy B-osztályú fenntartott címeket használ. Annak ellenére, hogy az osztály-alapú címzés és a rögzített hosszúságú alhálózati maszkolás egyre kevésbé szokványos, mégis fontos, hogy megértsük e címzési eljárások működését. Sok eszköz ma is alapértelmezett hálózati maszkot használ, ha nincs alhálózat specifikálva.

A CIDR (RFC 1519) a következőket biztosítja:

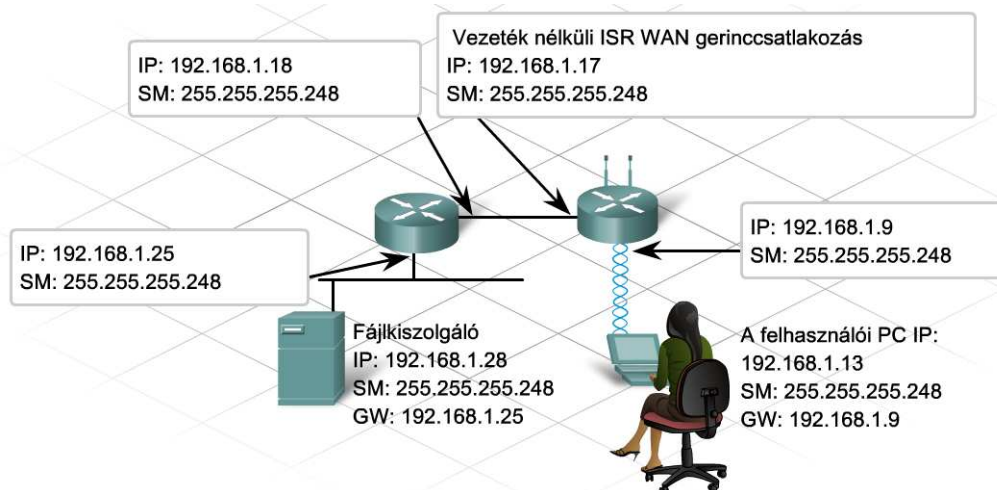
- hatékonyabban használja az IPv4 címeket,
- előtag-összefogást alkalmaz, ami csökkenti a forgalomirányító táblák méretét.

4.1.5 Az alhálózatok közötti kommunikáció

Ha egy hálózatot alhálózatokra bontunk, akkor valójában mindegyik alhálózat egy teljesen különálló hálózat lesz. Azért, hogy az egyik alhálózatban levő eszköz kommunikálni tudjon egy másik alhálózatban lévő eszközzel, forgalomirányítóra van szükség, mert hálózatokat összekötni forgalomirányítókkal tudunk.

Az alhálózatonkénti állomásszám meghatározásakor az érintett állomások mellett az alhálózat forgalomirányító interfészét (átjáróját) is figyelembe kell venni. Ezen a forgalomirányító interfészen olyan IP-címet kell beállítani amely az általa kiszolgált alhálózati címtartomány része.

Néhány esetben két forgalomirányító csatlakoztatása is szükségessé válhat, például, amikor a Linksys eszközt és az 1841-es ISR-t csatlakoztatjuk. Ez a konfiguráció megköveteli, hogy az egymáshoz csatlakozó forgalomirányítók interfészeihez rendelt IP-címek az adott hálózatban vagy alhálózatban legyenek. A szokványos csatlakoztatás két forgalomirányítót mutat, a 192.168.1.16/29-es alhálózathoz csatlakoztatva, a 192.168.1.17/29-es és a 192.168.1.18/29-es állomás IP-címekkel.



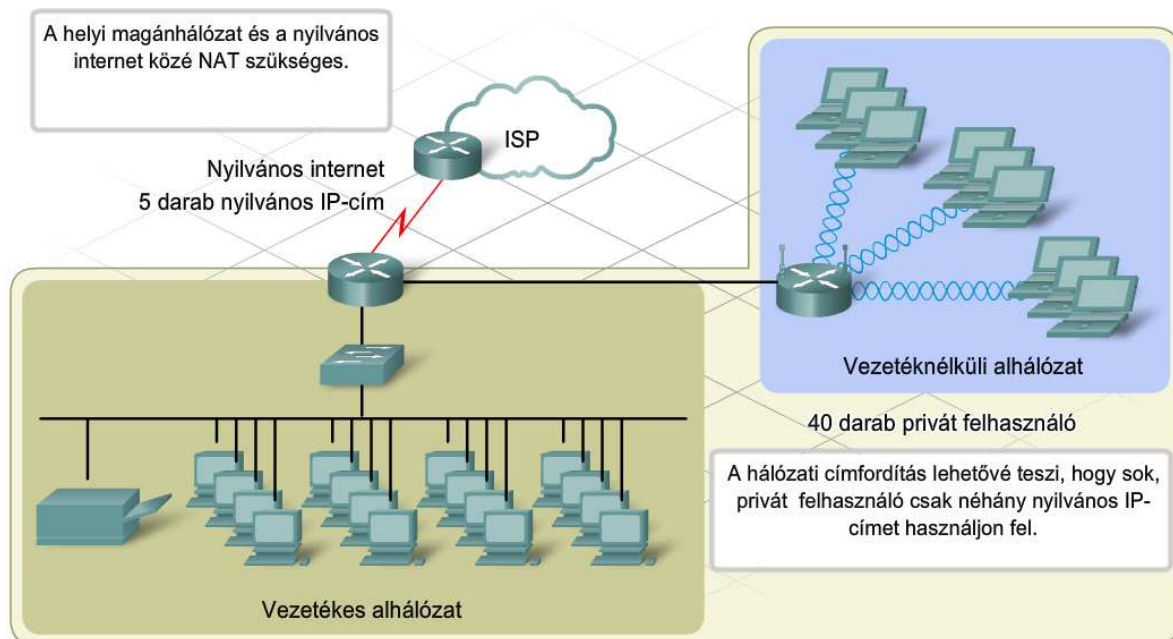
4.2 NAT és PAT

4.2.1 A hálózati címfordítás alapjai (NAT)

A forgalomirányító feladata az, hogy irányítsa a forgalmat a belső hálózat alhálózatai között, függetlenül attól, hogy az IP-címtartomány nyilvános vagy privát. Ugyanakkor, ha privát címtartományról van szó, a magánhálózatok nem vehetnek részt a forgalomirányításban a nyilvános internet felé. Vajon hogyan kommunikálnak a belső hálózaton levő, magáncímzési rendszert használó állomások az internettel? A magánhálózatot az internetszolgáltató hálózatával összekötő eszköznek a hálózati címfordítás (NAT) képességével kell rendelkezni.

A NAT lehetővé teszi, hogy egy nagy csoport egyéni felhasználó csatlakozzon az internetre, egy vagy több nyilvános IP-címen osztozva. A címfordítás hasonló a vállalati telefonrendszer működéséhez. Ahogy a cég folyamatosan veszi fel az embereket, egy ponton túl nem vezetnek minden dolgozó asztalához külön külső telefonvonalat. Ehelyett olyan rendszert használnak, amely lehetővé teszi, hogy a vállalat minden dolgozójához egy melléket rendel. A cég megteheti ezt, mert az összes dolgozó egyidejűleg nem akar telefonálni. A belső hívószámok használatával a cégnek kevesebb külső vonalat kell vásárolnia a telefontársaságtól.

A NAT a vállalati telefonhoz hasonlóan működik. A NAT kifejlesztésének legfőbb oka, hogy regisztrált IP-címeket takarít meg. Ezenkívül biztonságot is nyújt a PC-k, a szerverek és a hálózati eszközök számára, azok valódi állomás IP-címének a közvetlen, az internet felőli elérés elrejtésével.



A NAT fő előnye, hogy módot ad az IP-címek többszörös felhasználására, és ezzel sok, helyi hálózati állomás képes a globális egyedi IP-címek megosztott használatára. A NAT átlátszó módon működik, elfedi és ezzel megvédi a magánhálózat felhasználóit a nyilvános hálózatról felőli eléréstől.

Ezen túlmenően a NAT elrejtí a privát IP-címeket a nyilvános hálózat előtt. Ennek az az előnye, hogy a NAT egyfajta hozzáférési listaként működik, és nem engedi a külső felhasználókat a belső eszközökhöz hozzáférni. A hátránya, hogy külön beállítások szükségesek az erre jogosult külső felhasználók hozzáféréseinek biztosításához.

További hátrány még, hogy a NAT befolyásolja azon alkalmazások működését, amelyek IP-címeket tartalmazó üzenetekkel dolgoznak, mert ezeket a címeket is le kell fordítani. Ez a fordítás megnöveli az forgalomirányító terhelését, és visszafogja a hálózat teljesítményét.

A NAT előnyei	A NAT hátrányai
<ul style="list-style-type: none"> • A nyilvános IP-címek megosztása • Transzparens a végfelhasználók számára • Javított biztonság • A LAN bővíthetősége és skálázhatósága • Helyi vezérlés ISP kapcsolattal 	<ul style="list-style-type: none"> • Összeférhetetlenség bizonyos alkalmazásokkal • Elrejtí a jogosult távoli elérést. • A teljesítmény csökkenése a forgalomirányító megnövekedett feldolgozási tevékenysége miatt.

4.2.2 IP NAT alapfogalmak

A forgalomirányító IP-címfordítás opciójának beállításakor van néhány alapfogalom, amely segít megérteni a forgalomirányító címfordítását:

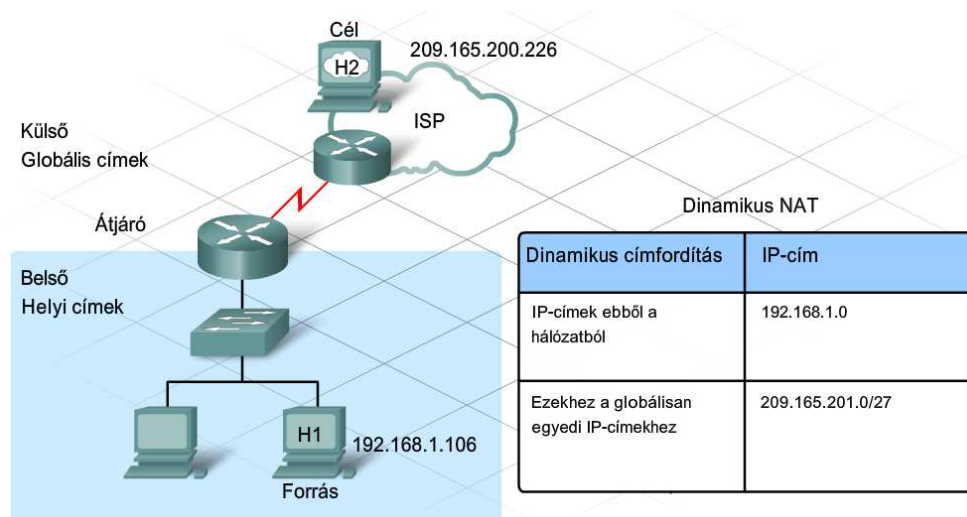
- **Belső helyi hálózat:** bármilyen, a forgalomirányítóhoz csatlakozó hálózat, amely a privát címezést használó helyi hálózat (LAN) része. A belső hálózaton levő állomások IP-címek fordításán megy át, mielőtt külső célpontokhoz továbbítják.
- **Külső globális hálózat:** bármilyen, a forgalomirányítóhoz csatlakozó hálózat, amely a helyi hálózaton kívül van, és nem ismeri fel a helyi hálózat állomásaihoz hozzárendelt privát címeket.

- **Belső helyi cím:** a belső hálózat egy állomásán beállított magánhálózati cím, privát IP-cím. A cím csak úgy kerülhet ki a helyi hálózati címzési struktúrából, ha előtte lefordítjuk.
- **Belső globális cím:** a belső hálózat állomásának címe a külső hálózatok felé. Ez a lefordított cím.
- **Külső helyi cím:** a helyi hálózaton tartózkodó adatcsomag célpontjának címe. Ez a cím rendszerint ugyanaz, mint a külső globális cím.
- **Külső globális cím:** egy külső állomás nyilvános IP-címe. A cím egy globálisan továbbítható címből, vagy hálózati tartományból van származtatva.

4.2.3 Statikus és dinamikus NAT

A címek dinamikusan is kioszthatók. A dinamikus címfordítás lehetővé teszi a magánhálózat privát IP-címmel rendelkező állomásainak a külső hálózatok, például, az internet elérését. Dinamikus címfordítás történik akkor, amikor a forgalomirányító a belső privát hálózati eszköz számára egy külső globális címet jelöl ki, egy előre meghatározott címet vagy címeket tartalmazó címtárból.

Amíg a kapcsolat él, a forgalomirányító érvényesnek tekinti a globális címet és a nyugtákat küld a kezdeményező eszköznek. Amint a kapcsolat véget ér, a forgalomirányító egyszerűen visszajuttatja a belső globális címet a címtárba.

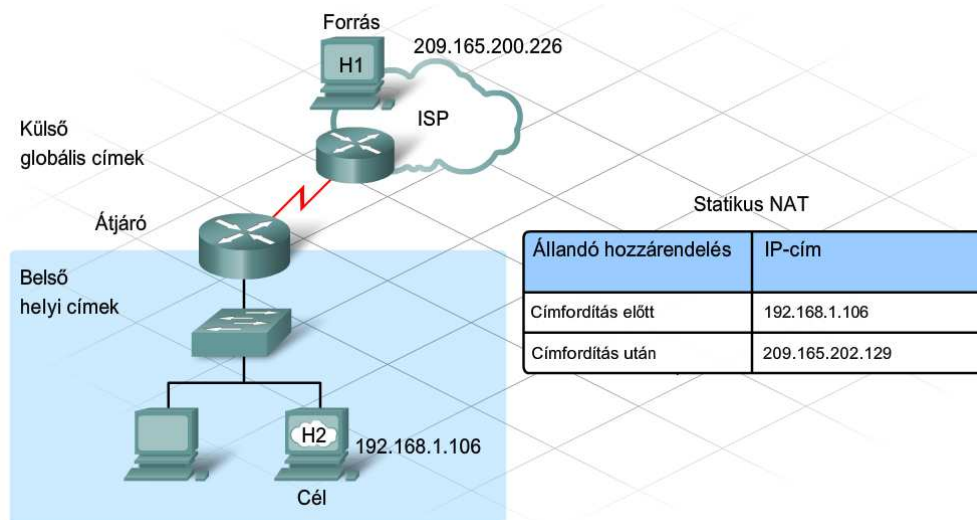


A NAT egyik előnye, hogy az egyéni állomások nem érhetők el közvetlenül az internetről. De mi a helyzet akkor, ha egy belső hálózati állomáson olyan szolgáltatások futnak, amelyeknek az internetre csatlakozó és a helyi privát hálózatra kötött eszközök számára is elérhetőeknek kell lenniük?

Egy helyi állomás internet felőli elérhetővé tételének egyik módja, hogy az eszköz számára egy állandó cím fordítását írjuk elő. A rögzített címre fordítás biztosítja, hogy az egyéni állomás privát IP-címe mindig ugyanarra a regisztrált globális IP-címre lesz lefordítva. Ezt a regisztrált címet más állomás garantáltan nem használja.

Az állandó NAT lehetővé teszi, hogy a nyilvános hálózaton levő állomások egy magánhálózaton levő kiválasztott állomásokhoz csatlakozzanak. Ha tehát egy belső hálózaton levő eszköznek kívülről is elérhetőnek kell lennie, akkor statikus NAT-ot használjunk.

Szükség esetén a statikus és a dinamikus NAT egyidejűleg is használható.

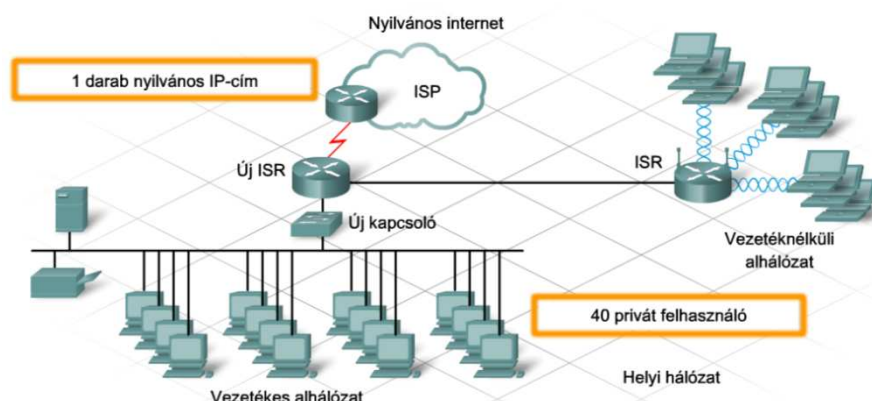


4.2.4 Port alapú hálózati címfordítás (PAT)

Amikor egy szervezet regisztrált IP-címlistája kicsi, akár csak egyetlen IP-címmel rendelkezik, a NAT akkor is képes több felhasználónak egyidejűleg biztosítani a nyilvános hálózat elérését az úgynevezett túlterheléses NAT-tal, vagy portcímfordítással (PAT). A PAT a különböző helyi címeket egyetlen globális IP-címre fordítja.

Amikor a forrásállomás küld egy üzenetet a célállomásnak, akkor az IP-cím és a portszám kombinálását használja fel úgy, hogy biztosítani tudja az egyedi kommunikációt a célállomással. A PAT technológiában az átjáró a helyi cím és a portszám kombinációját fordítja le egyedi globális IP-címre és egy 1024-nél nagyobb egyedi port-számmra. Bár mindegyik állomáscím ugyanarra a globális IP-címre fordul le, a társított portszám egyedi.

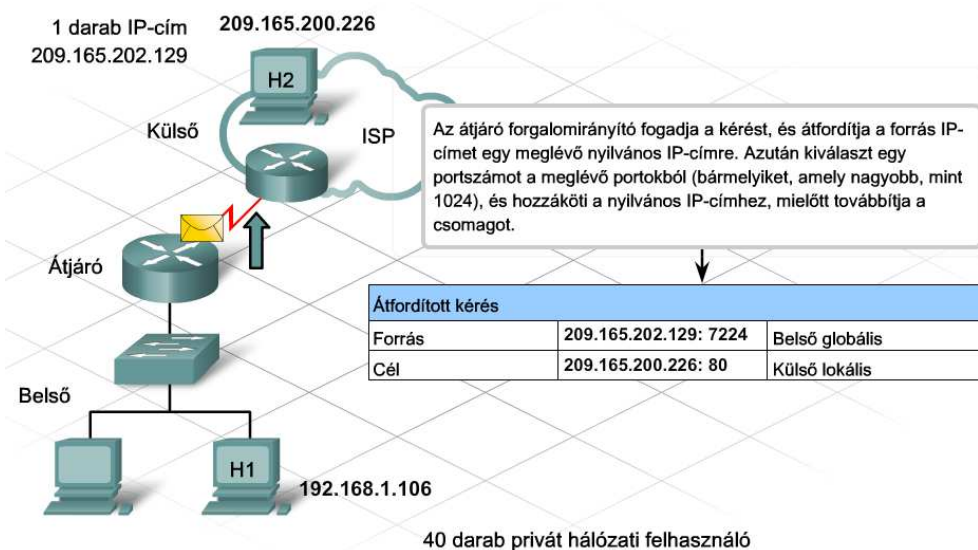
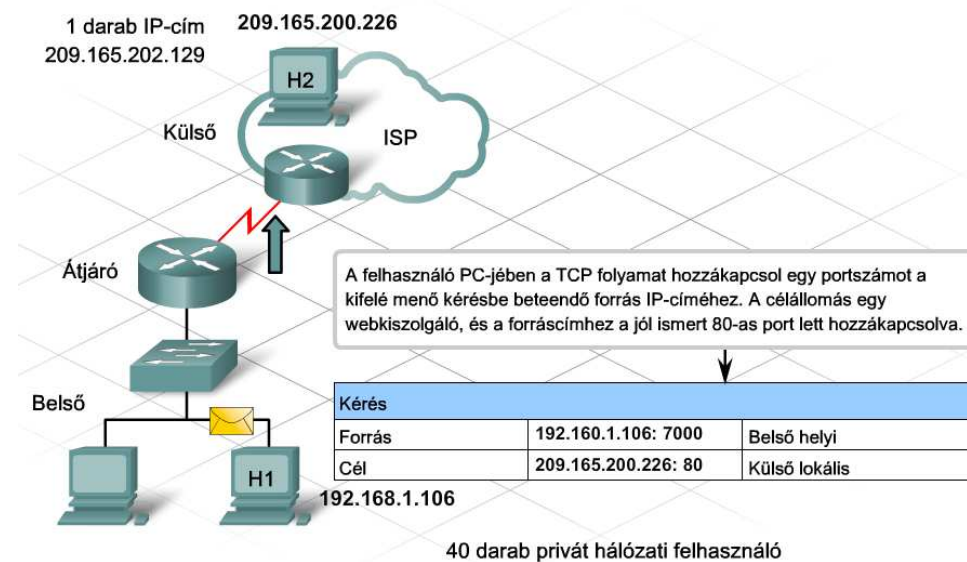
A válaszforgalom az állomás által használt címfordított IP-cím - portszám kombinációra érkezik. A forgalomirányítóban levő tábla tartalmazza azt a belső IP-címből és belső port-számból álló kombinációt, amelyet a külső címre fordított. Ennek felhasználásával a válaszforgalom a belső címre és portra továbbítható. Miután több mint 64 000 portszám lehetséges, valószínűtlen, hogy a forgalomirányító kifogy a portcímekből, ahogyan az a dinamikus NAT-nál nagyon is elképzelhető.

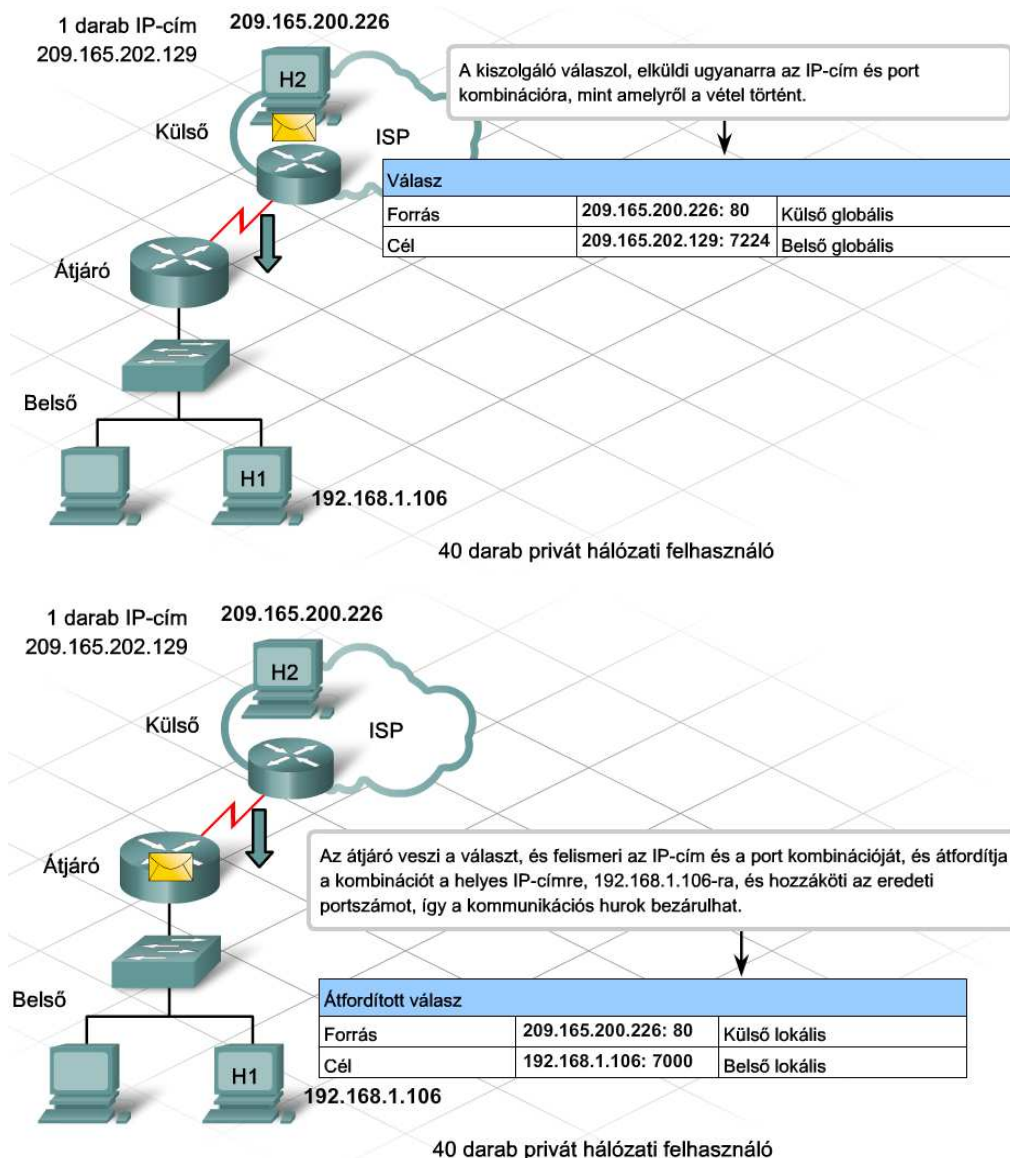


Mivel minden címfordítás egyedi a helyi címre és helyi portra vonatkozóan, minden kapcsolat, amely új forrásportot generál, külön fordítást igényel. Például, a 10.1.1.1:1025 egy különböző fordítás a 10.1.1.1:1026-tól.

A fordítás csak a kapcsolat idejéig áll fenn, így egy adott felhasználó nem tartja meg magának ugyanazt a globál IP-cím és portszám kombinációt a kapcsolat befejezése után.

A külső felhasználó nem tud megbízhatóan kapcsolatot létesíteni egy olyan állomással a hálózaton, amelyik PAT-ot használ. Nem csak lehetetlen megjósolni az állomás helyi vagy globális portszámát, hanem egy átjáró csak akkor végez címfordítást, ha a belső állomás kezdeményezi a kommunikációt.





4.2.5 További IP NAT kérdések

A felhasználók anélkül használják az internetet a privát hálózatról, hogy észrevennék, hogy a forgalomirányító NAT-ot használ. Ugyanakkor a NAT fontos jellemzője, hogy pluszterhelést jelent az IP-cím és a port fordítása.

Bizonyos alkalmazások növelik a forgalomirányító terhelését, mert a beágyazott adatsomagjaik részeként IP-címeket ágyaznak be. A forgalomirányítónak ki kell cserélnie azokat a forrás IP-címeket és a hozzájuk kapcsolódó portokat, melyek az adatfolyamban találhatók, és az IP-fejlécben lévő forráscímeket.

Mivel az egész folyamat a forgalomirányítóban megy végbe, a NAT alkalmazása jó hálózattervezést, az eszközök gondos kiválasztását és beállítását igényli.

A családi otthonunkban és a kisebb cégeknél használt integrált hálózati eszközökben a hálózati címfordítás annyira mindennapos dologgá vált, hogy egyeseknek a beállítás csupán annyit jelent, hogy néhány pipát tesznek a megfelelő helyre. Ahogy a vállalkozások nőnek és kifinomultabb

átjárókat és forgalomirányító megoldásokat igényelnek, az eszközök hálózati címfordítás-beállításai is sokkal bonyolultabbaká válnak.

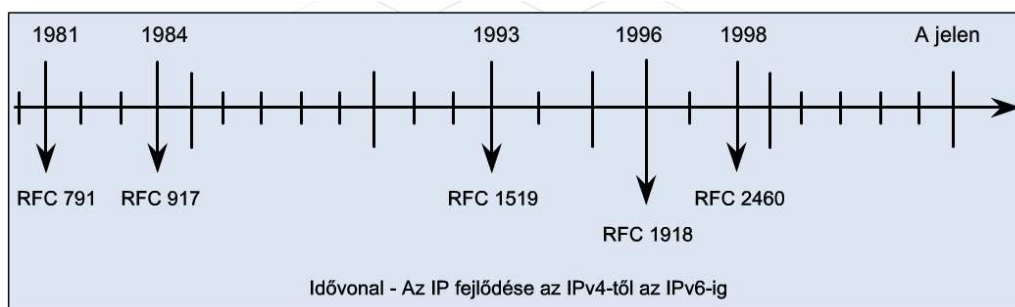
A hálózatok alhálózatokra bontása, a magánhálózati IP-címzés és a hálózati címfordítás kifejlesztése átmeneti megoldást jelent az IP-címek fogyására. Ezek az eljárások hasznosságuk ellenére sem hoznak létre több IP-címet. A címek elfogyására válaszul az RFC 2460 szabvány az IPv6-ot javasolta 1998-ban.

Habár az elsődleges cél a probléma megoldása volt, amit az IPv4 IP-címeinek elfogyása jelentett, más fontos okai is voltak a kifejlesztésének. Azóta hogy az IPv4-et először szabványosították, az internet jelentősen megnövekedett. Ezáltal láthatóvá váltak az IPv4 előnyei és hátrányai, és így az új képességekkel bíró utódra való áttérés lehetősége is.

Röviden az IPv6 legfontosabb fejlesztési tervei:

- több címtartomány
- jobb címtartomány kezelés
- könnyebb TCP/IP adminisztráció
- korszerűsített forgalomirányítási lehetőségek
- a csoportos adatszórás, mobilitás és biztonság jobb támogatása.

Az IPv6 fejlesztése arra irányul, hogy mindezeket a problémákat és elvárásokat a lehető legjobban figyelembe vegye.



RFC 791-ben definiálták az IP-t (IPv4)

RFC 917-ben definiálták az IP alhálózatra bontást

RFC 1519-ben definiálták a CIDR-t

RFC 1918-ben definiálták a privát IP-címzést

RFC 2460-ben definiálták az IPv6-ot

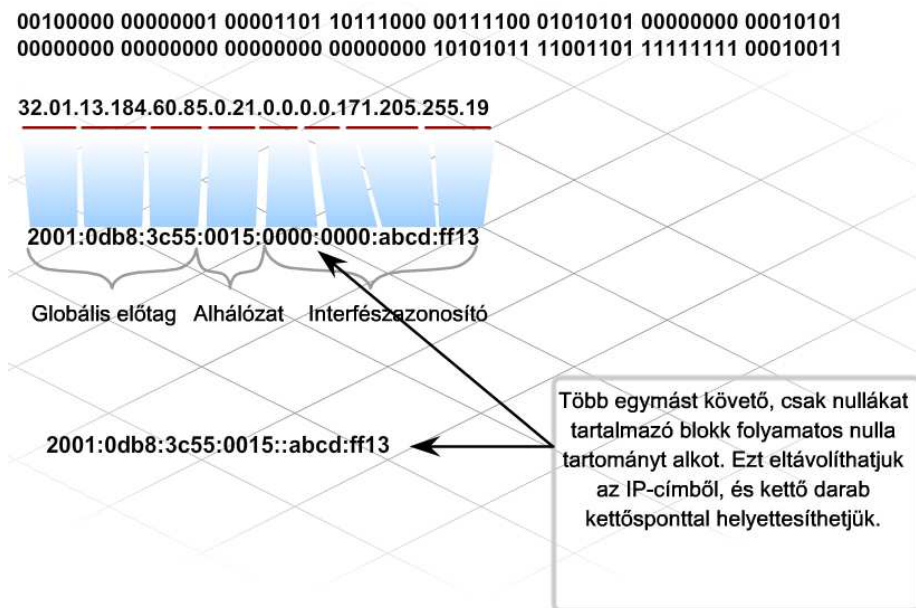
1998-tól a jelen-ig - átmenet az IPv4-ről az IPv6-ra (folyamatban)

Az IPv6-nál az IP-címek 128 bitesek, a lehetséges címtartomány 2^{128} . Tíztes számrendszerben jelölve, ez megközelítőleg egy hármast, amit 38 darab nulla követ. Ha az IPv4 címtartományát egy kis üveggolyónak tekintjük, akkor az IPv6 címtartománya körülbelül egy Szaturnusz nagyságú bolygó terjedelmének felel meg.

Mivel a 128-bites számokkal dolgozni bonyolult, az IPv6-cím számjegyei a 128 bitet 32 darab tizenhatos számrendszerbeli számjeggyel ábrázolják, amelyeket 8 darab, 4 hexadecimális

számjegyből álló csoportra bontunk, kettőspontot használva az elválasztáshoz. Az IPv6-cím-hierarchiája három részből áll. Az első három blokk a globális előtag, amely az internetes névadatbázisban levő szervezethez tartozik. Az alhálózat- és a csatlakozás-azonosító felett a hálózati adminisztrátor rendelkezik.

Egy darabig el fog tartani, amíg a rendszergazdák átállnak az új IPv6 címstruktúrára. Addig is, amíg az IPv6 széles körben elterjed, a rendszergazdáknak szükségük van az IPv4 privát címtartományok hatékonyabb felhasználását célzó módszerekre.



4.3 A fejezet összefoglalása

- Az internetre kötött hálózati eszközök interfészeinek egyedi IP-címmel kell rendelkezniük azért, hogy üzeneteket tudjanak küldeni és fogadni a hálózaton.
- Az IP-címek A, B, C, D és E hálózati osztályba csoportosíthatók és a privát IP-címtartomány létrehozásával tartalékolhatjuk őket.
- Egy hálózat több alhálózatra osztható.
- Az osztályalapú alhálózatképzés az alhálózati maszk kiterjesztését használja. Az osztályok nélküli IP-címhasználat, amely része az osztályok nélküli tartományok között megvalósuló forgalomirányítási módszernek (CIDR), egy rugalmas alhálózatképzést használ a változó hosszúságú alhálózati maszkok alkalmazásával (VLSM).



- Az alhálózati maszk használatával tovább oszthatjuk a hálózatokat a maszkbitek számának kiterjesztésével.
- Az alhálózati ID az eredeti állomás ID két részre osztásával keletkezik, egy alhálózati ID-re és egy új állomás ID-re.
- Az alhálózati ID biteinek száma meghatározza a hálózatban lévő alhálózatok számát.
- Az alhálózatok közötti kommunikáció forgalomirányítást igényel.
- A NAT lehetővé teszi az internetet használó privát felhasználók egy nagy csoportjának, hogy kevés számú publikus IP-címet megosztva használjanak, így csökkenteni lehet a globálisan egyedi IP-címek felhasználását.
- A belső címek a privát hálózati eszközök IP-címei számára vannak kijelölve. A külső címek a nyilvános hálózati eszközök IP-címei számára vannak kijelölve. A helyi címek azok az IP-címek, amelyeket a helyi hálózati csomagokban vannak. Globális címek azok az IP-címek, amelyek a külső hálózatok eléréséhez szükségesek.
- Egy csomag, amelyet át lett fordítva és a külső hálózatban van, egy belső globális IP-címet mint forráscímet és egy külső globális IP-címet, mint célcímet fog tartalmazni.
 - A statikus NAT egy egy az egyhez megfeleltetésű állandó címátalakítást végez, egy adott belső helyi IP-címhez egy adott belső globális IP-címet rendel hozzá.
 - A dinamikus NAT az "előbb jött, előbb szolgálják ki" alapon, egy belső globális IP-címet rendel a rendelkezésre álló címek listájából egy kijelölt hálózathoz vagy alhálózathoz.
 - A PAT-t arra használhatjuk, hogy az IP-címhez egy portszámot adjunk hozzá, hogy meghatározott kapcsolatot hozzunk létre.
 - A NAT-ot használó hálózati eszközök minden egyes csomagnál elvégzik a címfordítást. Ez jelentősen megnöveli a feldolgozási munka mennyiségét.
- Az IPv6 128 bites címzési struktúrát tartalmaz, míg a IPv4 csak 32 bitet használ.

5. Hálózati eszközök konfigurálása

5.1 Az ISR forgalomirányító első konfigurálása

5.1.1 ISR

Az integrált forgalomirányító (Integrated Services Router, ISR) az egyik legnépszerűbb hálózati eszköz a piacon, mely képes arra, hogy kielégítse a megnövekedett vállalati kommunikációs igényeket. Az ISR egy eszközben kínálja a forgalomirányítási, LAN kapcsolási, biztonsági, hangátviteli és WAN kapcsolódási funkciókat. Ezek a tulajdonságok ideálissá teszik az ISR-t a kis- és középvállalatok, valamint az internetszolgáltató által felügyelt ügyfelek számára.

Az opcionális integrált kapcsolómodul lehetővé teszi a kisvállalkozások számára, hogy az 1841-es ISR-hez közvetlenül csatlakoztassanak LAN eszközöket. Amennyiben a LAN állomások száma meghaladja a kapcsoló portjainak számát, az integrált kapcsolómodul segítségével további kapcsolók és hubok fűzhetők láncba, így módon bővítve az elérhető LAN portok számát. Ha kapcsolómodul nem áll rendelkezésre, a külső kapcsolók az ISR forgalomirányító interfészeihez csatlakoztathatóak.

Az ISR forgalomirányító funkciója lehetővé teszi, hogy a hálózatot alhálózatok segítségével több részre tagolja. Ezen felül biztosítja a LAN eszközök számára az internethez vagy a WAN-hoz történő csatlakozás lehetőségét.

A Cisco ISR forgalomirányítók családja



Cisco 800-as sorozatú ISR



Cisco 3800-as sorozatú ISR



Cisco 1800-as sorozatú ISR



Cisco 2800-as sorozatú ISR

Cisco 800-as sorozatú ISR

- Kisebb irodák és otthoni felhasználók számára fejlesztették
- 1 db. WAN kapcsolatot támogat
- 4 db. 10/100 Mb/s kapcsolatot támogat
- Adat, biztonsági és vezetékek nélküli szolgáltatások kombinációját nyújtja
- Széles sávú szolgáltatásokat biztosít

Cisco 3800-as sorozatú ISR

- Közepes és nagyméretű üzleti környezetek és vállalati kirendeltségek, fiókirodák számára fejlesztették
- LAN és WAN interfészeket támogató moduláris bővítőaljzattal rendelkezik
- Legfeljebb 2 db. 10/100 Mb/s sebességű forgalomirányító portot támogat
- Legfeljebb 112 db. 10/100 Mb/s sebességű kapcsolóportot támogat
- 240 db. Cisco IP telefonos felhasználót támogat
- Adat, biztonsági, hang és video alapú, valamint vezeték nélküli szolgáltatások kombinációját nyújtja
- Széles sávú szolgáltatásokat DSL, kábeles és T1/E1 kapcsolatok esetén biztosít

Cisco 1800-as sorozatú ISR

- Kis és közepes üzleti környezetek és kisebb vállalati kirendeltségek, fiókirodák számára fejlesztették
- LAN és WAN interfészeket támogató moduláris bővítőaljzattal rendelkezik
- Legfeljebb 8 db. 10/100 Mb/s sebességű forgalomirányító portot támogat
- 8 db. 10/100 Mb/s sebességű kapcsolóportot támogat
- Adat, biztonsági és vezeték nélküli szolgáltatások kombinációját nyújtja
- Széles sávú szolgáltatásokat, DSL, kábeles és T1/E1 kapcsolatok esetén biztosít

Cisco 2800-as sorozatú ISR

- Kis és közepes üzleti környezetek és kisebb vállalati kirendeltségek, fiókirodák számára fejlesztették
- LAN és WAN interfészeket támogató moduláris bővítőaljzattal rendelkezik
- Legfeljebb 2 db. 10/100 Mb/s sebességű forgalomirányító portot támogat
- Legfeljebb 64 db. 10/100 Mb/s sebességű kapcsolóportot támogat
- 96 db. Cisco IP telefonos felhasználót támogat
- Adat, biztonsági és vezeték nélküli szolgáltatások kombinációját nyújtja
- Széles sávú szolgáltatásokat, DSL, kábeles és T1/E1 kapcsolatok esetén biztosít

ISR-széria: 1841-es modell**Előlnézet:**

Az 1841-es készülék kis és közepes vállalkozások, valamint nagy cégek kis fiókirodái számára kifejlesztett, viszonylag olcsó ISR. Az adatátviteli és biztonsági szolgáltatásokon felül, megfelelő modul telepítése esetén vezeték nélküli szolgáltatásra is képes.

Bekapcsolt állapotot jelző LED (SYS-PWR)

Jelzi hogy a tápfeszültség megvan, és a belső tápegység működik. Bekapcsolt állapotban a LED folyamatos zöld fényű.

Rendszer aktivitást jelző LED (SYS ACT)

A LED villogása azt jelzi hogy a rendszer éppen adatcsomagokat továbbít.

**Hátulnézet:**

A 1841 ISR modulokat használ, ami különböző portkonfigurációk kialakítását teszi lehetővé.

Moduláris csatlakozóhely 1 db nagysebességű WAN interfész kártyával (HWIC):

A moduláris csatlakozó helyekre különböző típusú interfészkártyákat lehet illeszteni. Az itt látható HWIC soros csatlakozást biztosít nagytávolságú hálózatokhoz.

Compact Flash modul:

Ez a cserélhető modul tartalmazza a Cisco IOS-t és az egyéb szükséges szoftvereket az ISR számára.

Egyszerű USB port :

Az USB flash használata lehetővé teszi az operációsrendszer képfájlainak és konfigurációinak a tárolását, valamint az USB flash memóriából történő közvetlen rendszerbetöltést.

Fast Ethernet portok:

Ezek a portok 10/100 Mbit/sec-os kapcsolatot biztosítanak a helyi hálózatok irányába.

Konzolport:

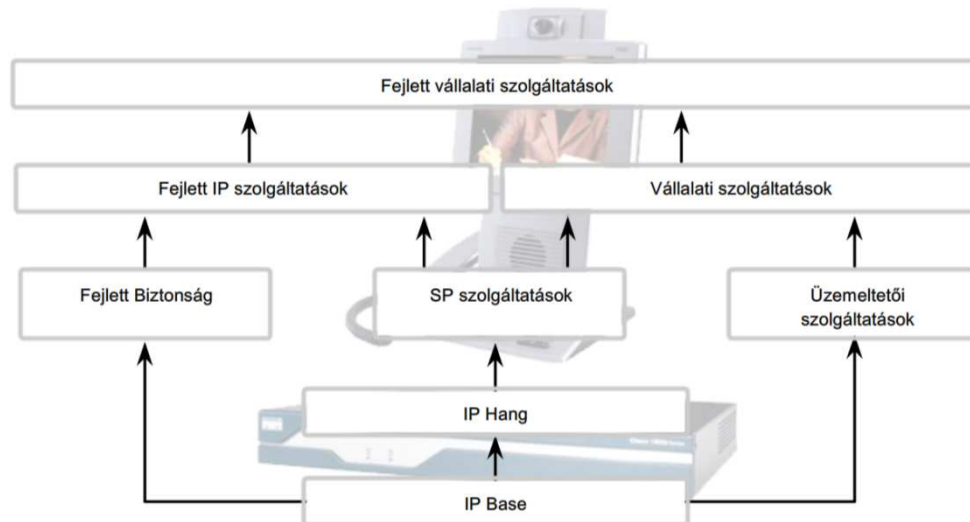
Ezen a porton keresztül az ISR beállítására használt állomást lehet közvetlenül csatlakoztatni.

Kiegészítő (AUX) port:

Ezt a portot az ISR beállítására használt modem csatlakozáshoz használják.

Moduláris csatlakozó 4 portos ethernet kapcsolóval:

A moduláris csatlakozó aljzatok különböző típusú interfészek használatát teszik lehetővé. Az itt látható 4 portos ethernet kártya LAN kapcsolatot biztosít több eszköz számára.



A Cisco Internetwork Operating System (IOS) szoftver funkciói lehetővé teszik a Cisco eszközök számára a vezetékes vagy vezeték nélküli hálózatokon keresztül történő hálózati forgalom bonyolítását (küldés és fogadás). A Cisco IOS szoftver rendszerkódnak (image) nevezett modulokban kapható. Ezek a rendszerkódok számos funkciót biztosítanak a különböző méretű vállalatok számára.

A belépő szintű Cisco IOS rendszerkódot IP Base-nek (IP Alap) nevezik. A Cisco IOS IP Base szoftver a kis- és középvállalkozások számára készült, és biztosítja a hálózatok közötti forgalomirányítást.

A többi Cisco IOS rendszerkód az IP Base szolgáltatásait bővíti. Az Advanced Security (Fejlett Biztonság) rendszerkód fejlett biztonsági funkciókat biztosít magánhálózatok és tűzfalak kialakításához.

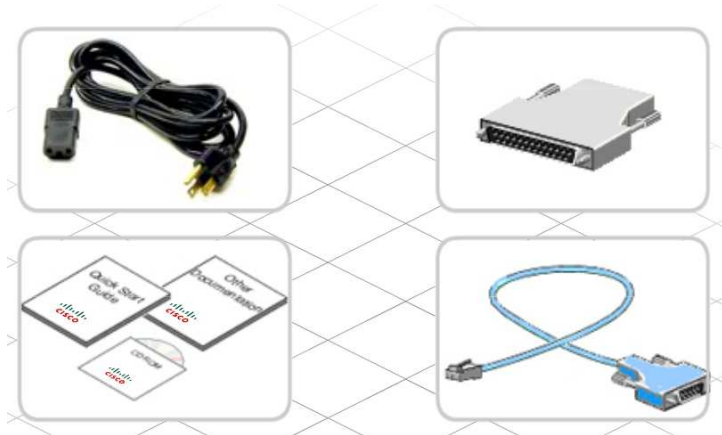
A Cisco IOS rendszerkód számtalan típusban és verzióban elérhető. Az egyes rendszerkódokat a forgalomirányítók, kapcsolók és ISR-ek konkrét modelljeihez tervezték és optimalizálták.

A készülék konfigurálásának megkezdése előtt fontos tudni, hogy milyen rendszerkód, illetve annak melyik verziója töltődik be.

5.1.2 Az ISR üzembehelyezése

Minden ISR-hez jár egy kábelkészlet, valamint a készülék bekapcsolásához és a telepítés megkezdéséhez szükséges dokumentáció. Új készülék vásárlása esetén csomagoljuk ki az eszközt és ellenőrizzük, hogy egyetlen hardverelem vagy kiegészítő sem hiányzik!

- Egy új Cisco 1841 típusú termék csomagolása az alábbiakat tartalmazza:
- RJ-45 -- DB-9 konzolkábel
- DB-9 -- DB-25 átalakító
- tápkábel
- termékregisztrációs kártya, más néven Cisco.com kártya
- a Cisco 1841 típusú forgalomirányító termékfelelősségi tanúsítványa
- a "Router and Security Device Manager" (SDM, biztonsági eszközközelő) angol nyelvű kezelési útmutatója (Quick Start Guide)
- a Cisco 1800-as sorozatú (moduláris) ISR angol nyelvű kezelési útmutatója



A Cisco 1841 ISR beüzemeléséhez szükséges minden speciális szerszám és felszerelés általában megtalálható az internetszolgáltatók és a hálózati szakemberek műhelyében. Az eszköz modelljétől és a megrendelt opcionális tartozékoktól függően szükség lehet egyéb felszerelésre is.

Az új eszköz beüzemeléséhez rendszerint az alábbi szerszámokra van szükség:

- terminálemulációs programmal (pl.: HyperTerminal) rendelkező PC
- kábelkötegelők és 2-es (méretű) csillagfejű csavarhúzó
- különböző interfészekhez (WAN, LAN, USB, stb.) tartozó kábelek

A WAN és a szélessávú kommunikációs szolgáltatások eléréséhez további felszerelésre és eszközökre (pl. modemre) is szükség lehet. Attól függően, hogy rendelkezésre áll-e integrált kapcsolómodul és hogy hány eszközt kell csatlakoztatni, elképzelhető, hogy egy vagy több Ethernet kapcsolót is be kell még szerezni.



Mindig olvassuk el a kezelési útmutatót és a többi dokumentációt, mielőtt bármilyen berendezés beüzemeléséhez hozzáfekszünk! A dokumentáció fontos biztonsági és végrehajtási információkat tartalmaz, amelyek segítségével elkerülhető, hogy az eszköz meghibásodjon.

Az 1841 típusú ISR üzembehelyezéséhez kövessük az alábbi lépéseket!

1. Rögzítsük és földeljük az eszközt megfelelően!
2. Helyezzük be a külső Compact Flash kártyát!
3. Csatlakoztassuk a tápkábelt!
4. Állítsuk be a PC-re telepített terminálemulációs programot, majd csatlakoztassuk a PC-t a konzolporthoz!
5. Kapcsoljuk be a forgalomirányítót!
6. Ellenőrizzük a forgalomirányító elindulásakor a PC-n megjelenő indítási üzeneteket!



1. lépés: Az eszköz megfelelő rögzítése és földelése

A Cisco forgalomirányítók és ISR eszközök rögzíthetők falra; tálcára illetve polcra helyezhetők vagy rack-szekrénybe szerelhetők.



2. lépés: A külső Compact Flash kártya behelyezése

Tegyük be a külső Compact Flash memóriakártyát az aljzatba! Bizonyosodjunk meg arról, hogy a kártya stabilan helyezkedik el az aljzatban és a kioldó gomb teljesen kiemelkedik! A kioldó nyomógomb általában az aljzat bal oldalán található.



3. lépés: A tápkábel csatlakoztatása

Csatlakoztassuk a tápkábel egyik végét az eszközhöz, majd a másik végét egy megbízható tápellátást biztosító áramforráshoz! Forgalmirányítókat és kapcsolókat általában akkumulátort tartalmazó szünetmentes tápegységhez csatlakoztatják. Ez biztosítja, hogy az eszköz ne álljon le váratlan áramkimaradás esetén.



4. lépés: A PC-re telepített terminálemulációs program beállítása és a PC csatlakoztatása a konzolporthoz

A számítógépen konfiguráljuk be a terminálemulációs szoftvert a Cisco forgalmirányítóval való kommunikációhoz szükséges beállításokkal! Az emulációs programot futtató számítógépet kössük össze az ISR konzolportjával az eszközhöz kapott konzolkábel segítségével.



5. lépés: A forgalomirányító bekapcsolása

Az eszköz hátulján található bekapcsológomb segítségével helyezzük áram alá az ISR-t!

```
1841 Router - HyperTerminal
File Edit View Call Transfer Help
[Icons]
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

    cisco Systems, Inc.
    170 West Tasman Drive
    San Jose, California 95134-1706

Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(4)T7, RELEASE S
FTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 28-Nov-06 17:31 by kellythw
Image text-base: 0x6008B70C, data-base: 0x61580000

Connected 0:01:41  Auto detect  9600 B-W-1  SCROLL  CAPS  NUM  Capture  Print echo
```

6. lépés: Az indítási üzenetek megfigyelése

Figyeljük meg a terminálemulációs program ablakában megjelenő indítási üzeneteket! Ezeket az üzeneteket a forgalomirányító operációs rendszere állítja elő.

5.1.3 Az indítási folyamat

A forgalomirányító elindítása három lépésből áll.

1. Az önellenőrzés (POST) és a rendszerindító program (bootstrap) betöltése.

A POST folyamat szinte minden számítógépen lefut az elindulás során. A POST ellenőrzi a forgalomirányító hardverét. A POST végrehajtása után a rendszerindító program töltődik be.

2. A Cisco IOS szoftver megkeresése és betöltése

A rendszerindító program megkeresi a Cisco IOS szoftvert, majd betölti a RAM-ba. A Cisco IOS fájl három helyen lehet: a flash memóriában, egy TFTP kiszolgálón vagy az indító konfigurációs fájlban

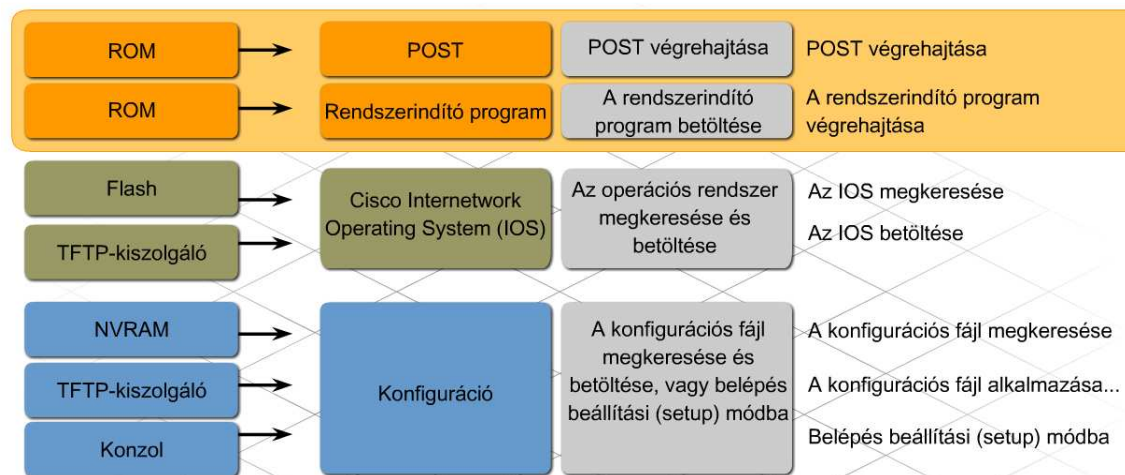
megadott egyéb helyen. A Cisco IOS szoftver alapértelmezés szerint a flash memóriából töltődik be. Egyéb helyről történő betöltése esetén a konfigurációs beállítások megváltoztatása szükséges.

3. Az indítási konfigurációt tartalmazó állomány megkeresése és betöltése, vagy beállítási módba váltás.

A Cisco IOS szoftver betöltése után a rendszerindító program az NVRAM-ban keresi az indító konfigurációs fájlt. Ez a fájl tartalmazza az előzőleg elmentett beállítási parancsokat és paramétereket, beleértve az interfészek címeit, a forgalomirányítási információkat, jelszavakat és egyéb konfigurációs paramétereket.

Ha a konfigurációs fájl nem érhető el, a forgalomirányító beállítási (setup) módba lép, ahol a felhasználónak meg kell adnia az alapkonfigurációt.

Ha az indító konfigurációs fájl elérhető, akkor tartalma a RAM-ba másolódik, és a képernyőn megjelenik egy, az állomásnevet tartalmazó prompt. A prompt jelzi, hogy a Cisco IOS szoftver és a konfigurációs fájl betöltése a forgalomirányítón sikeres volt.



Az adatvesztés elkerülése érdekében fontos tisztában lenni az indító konfigurációs fájl és az aktív konfigurációs fájl közötti különbséggel.

Az indító konfigurációs fájl

Az indító konfigurációs fájl olyan elmentett, konfigurációs állomány, amely az eszköz minden egyes indításakor beállítja az adott eszköz tulajdonságait. A fájl tárolása a nemfelejtő RAM-ban (NVRAM) történik, ami azt jelenti, hogy az eszköz kikapcsolása után is megőrzi tartalmát.

A Cisco forgalomirányítók az első bekapcsolásnál a Cisco IOS kódját a munkamemóriába, azaz a RAM-ba töltik be. Ezt követően az indító konfigurációs fájl tartalma az NVRAM-ból a RAM-ba másolódik. Amikor az indító konfigurációs fájl tartalma a RAM-ba töltődik, az lesz a kezdeti aktív konfiguráció.

Az aktív konfigurációs fájl

Az aktív konfiguráció kifejezés az eszköz memóriájában (RAM) jelenleg futó konfigurációra utal. A fájlban lévő parancsok határozzák meg az eszköz hálózati működését.



Az aktuális konfigurációs fájl tárolása az eszköz munkamemóriájában történik. A munkamemóriában lévő fájl lehetővé teszi a konfigurációs beállítások és számos eszközparaméter megváltoztatását. Ugyanakkor lényeges, hogy az aktív konfiguráció minden egyes leállításnál elveszik, amíg nincs elmentve az indító konfigurációs fájlba.

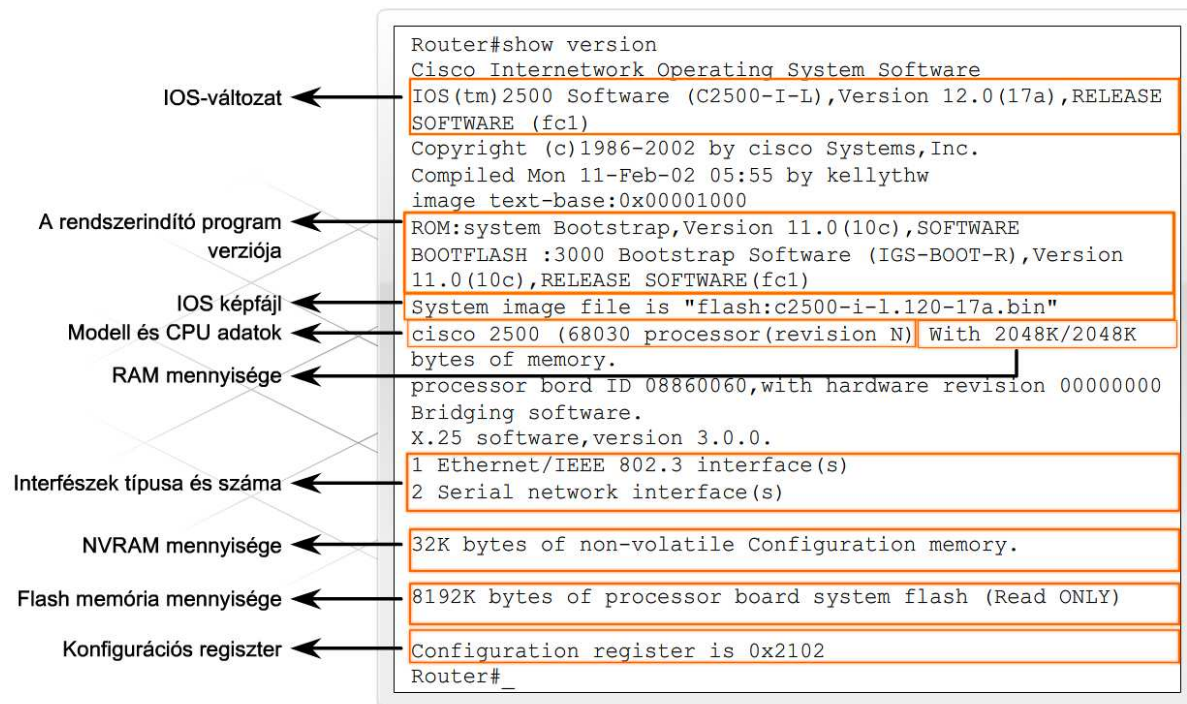
Az aktív konfiguráció változásai automatikusan nem kerülnek át az indító konfigurációs fájlba, a mentést manuálisan kell elvégezni.

Amennyiben az eszköz beállításához a Cisco parancssoros felületét (CLI) használjuk, a `copy running-config startup-config` vagy rövid alakban a `copy run start` parancs kiadásával az aktuális konfiguráció az indító konfigurációs fájlba menthető. Ha az eszköz beállításához a Cisco SDM grafikus felületét használjuk, minden végrehajtott parancs után lehetőség van a forgalomirányító aktuális konfigurációjának az indító konfigurációs fájlba történő mentésére.

Az indítási konfigurációt tartalmazó fájl sikeres 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 az alábbiakat jeleníti meg:

- A használatban lévő Cisco IOS verziója.
- A ROM-ban tárolt, a forgalomirányító első indításához használt rendszerindító program verziója.
- A Cisco IOS szoftver teljes fájlneve és az, hogy a rendszerindító program hol találta meg.
- A forgalomirányító által használt CPU típusa és RAM mennyisége. A Cisco IOS szoftver frissítésekor szükség lehet a RAM bővítésére.
- A forgalomirányító fizikai interfészeinek száma és típusa.
- Az NVRAM mennyisége. Az NVRAM az indító konfigurációs fájlt tárolja.
- A rendelkezésre álló flash memória mennyisége. A flash memória végzi a Cisco IOS szoftver folyamatos tárolását. A Cisco IOS szoftver frissítésekor szükség lehet a flash memória bővítésére.
- A konfigurációs regiszter jelenlegi, hexadecimális formában megadott értéke.

A konfigurációs regiszter adja meg az indítási folyamat módját a forgalomirányító számára. A gyári beállítás szerinti értéke `0x2102`, amely azt jelzi, hogy a forgalomirányító a Cisco IOS szoftvert a flash-ből, az indító konfigurációs fájlt pedig az NVRAM-ból tölti be. 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 megjelenik egy második érték zárójelben, az a forgalomirányító következő újraindításánál használt konfigurációs regiszter értéket mutatja.



A konfigurációs regiszter közli a forgalomirányító számára az indítási folyamat módját. Többféle lehetséges konfigurációs regiszter beállítás létezik. A leggyakoribbak az alábbiak:

0x2102 - A Cisco forgalomirányítók gyári alapértelmezett beállítása (az IOS rendszerkód betöltése a flash memóriából, az indító konfigurációs fájl betöltése az NVRAM-ból)

0x2142 - A forgalomirányító figyelmen kívül hagyja a nemfelejtő RAM (NVRAM) tartalmát

0x2120 - A forgalomirányító ROMmon módban indul

Előfordulhat, hogy a forgalomirányító nem indul el. Ennek oka lehet többek között a sérült vagy hiányzó Cisco IOS fájl vagy annak a konfigurációs regiszterben rosszul megadott helye, esetleg az új Cisco IOS rendszerkód betöltéséhez nem elegendő memória. Ha a forgalomirányító nem tudja betölteni a Cisco IOS-t, akkor ROM monitor (ROMmon) módban indul el. A ROMmon szoftver a csak olvasható memóriában (ROM) tárolt egyszerű parancskészlet, amely az indítási hibák elhárításához vagy – hiányzó IOS esetén – a forgalomirányító helyreállításához használható.

Amennyiben a forgalomirányító ROMmon módban indul el, a hibaelhárítás egyik első lépéseként keressünk egy érvényes IOS rendszerkódot a flash memóriában a `dir flash:` parancs kiadásával. Ha találunk érvényes rendszerkódot, akkor próbáljuk betölteni a `boot flash:` parancs kiadásával.

rommon 1>boot flash:c2600-is-mz.121-5

Ha a parancs kiadása után a forgalomirányító megfelelően elindul, akkor két ok lehetséges, amiért elsőre nem töltötte be a Cisco IOS rendszerkódot a flash-ből. Első lépésként a `show version` parancssal ellenőrizzük, hogy a konfigurációs regiszter értéke az alapértelmezett rendszerindítási sorrendet írja-e elő. Amennyiben a konfigurációs regiszter értéke helyes, a `show startup-config` parancs segítségével nézzük meg, hogy az indítási konfigurációt tartalmazó fájlban szerepel-e a `boot system` parancs, amely arra utasítja a forgalomirányítót, hogy más helyen keresse a Cisco IOS szoftvert.

5.1.4 A Cisco IOS segédprogramok

Ahhoz, hogy a PC-ről konfigurálhassunk és figyelemmel kísérjünk egy hálózati eszközt, kétféle csatlakoztatási mód létezik: a sávon-kívüli, illetve a sávon-belüli felügyelet.

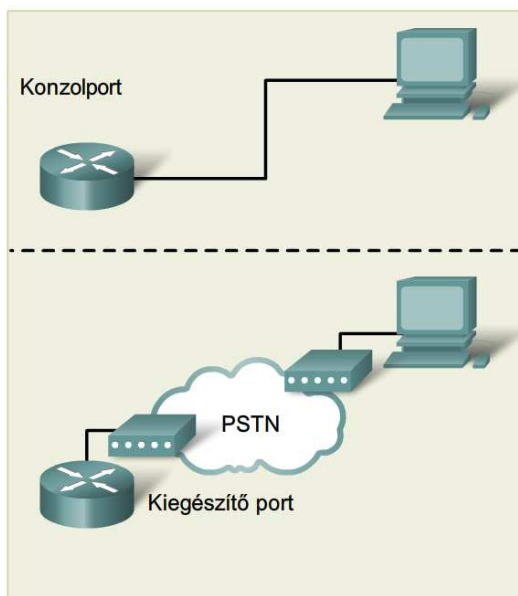
A sávon-kívüli felügyelet

A sávon-kívüli felügyelet esetében a számítógépet közvetlenül a konfigurálandó hálózati eszköz konzol- vagy AUX-portjához kell csatlakoztatni. Ebben az esetben nincs szükség aktív helyi hálózati kapcsolatra az eszközön. A sávon-kívüli felügyeletet a hálózati eszköz első beállításánál használjuk, mivel a még nem megfelelően konfigurált eszköz nem képes részt venni a hálózati kommunikációban. A sávon-kívüli felügyelet akkor is hasznos lehet, ha a hálózati kapcsolat nem működik megfelelően, és az eszköz nem érhető el a hálózaton keresztül. A sávon-kívüli felügyelettel kapcsolatos feladatok végrehajtásához szükség van egy, a PC-re telepített terminálemulációs ügyfélprogramra.

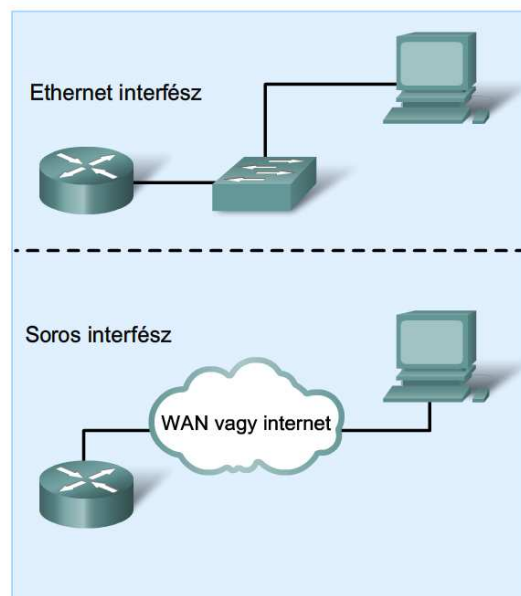
A sávon-belüli felügyelet

A hálózati eszközök működésének figyelemmel kíséréséhez, illetve a konfigurációjuk megváltoztatásához használunk hálózaton keresztül történő sávon-belüli felügyeletet! Ahhoz, hogy egy számítógép csatlakozzon az eszközhöz, és azon sávon-belüli felügyeleti feladatokat hajtsunk végre, legalább az eszköz egyik hálózati portjának csatlakoztott és működőképes állapotban kell lennie. A Telnet, a HTTP és az SSH egyaránt használható a Cisco eszközök sávon-belüli felügyelettel történő eléréséhez. A hálózati eszközök működésének figyelemmel kíséréséhez és konfigurációjuk megváltoztatásához webböngésző és Telnet ügyfélprogram egyaránt használható.

Forgalomirányító sávon-kívüli konfigurációja



Forgalomirányító sávon-belüli konfigurációja



A Cisco IOS parancssoros felülete (CLI) egy karakteres segédprogram, amely lehetővé teszi olyan Cisco IOS parancsok bevitelét és végrehajtását, amelyekkel figyelemmel kísérhető és karbantartható a Cisco eszközök működése. A Cisco CLI sávon-belüli és sávon-kívüli feladatok végrehajtásához egyaránt használható.

Az eszközök konfigurációjának megváltoztatásához és a forgalomirányítón futó folyamatok jelenlegi állapotának megjelenítéséhez használjuk a CLI parancsait! Akár egyszerű, akár összetett konfigurációról van szó, a tapasztalt felhasználók számára számos időtakarékos megoldást kínál a CLI. A Cisco hálózati eszközök szinte mindegyike hasonló CLI-t használ. Miután a forgalomirányító elindult és a Router> parancssor megjelenik, a CLI készen áll a Cisco IOS parancsok fogadására.

A parancsokat és a CLI működését jól ismerő szakember számára könnyű a különféle hálózati eszközök beállítása, és működésük nyomon követése. A CLI részletes súgója segít a felhasználóknak ebben a munkában.

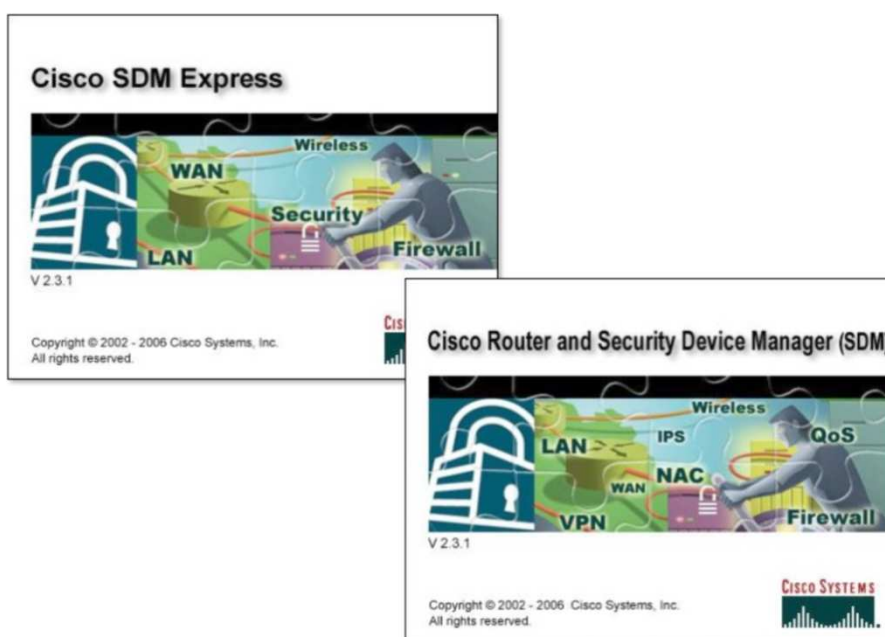
A Cisco IOS parancssoros felületén kívül más eszközök is segítenek a Cisco forgalomirányítók és ISR-ek konfigurálásában. A Security Device Manager (SDM, biztonsági eszközkezelő) egy web-alapú grafikus felügyeleti eszköz. A CLI-vel ellentétben az SDM kizárólag sávon-belüli felügyeleti feladatokra használható.

Az SDM Express leegyszerűsíti a forgalomirányító első beállítását, mivel gyors és könnyen használható formában, lépésről lépésre végigvezet az alapvető konfiguráció megadásának menetén.

A teljes SDM csomag még fejlettebb lehetőségeket kínál:

- további LAN és WAN kapcsolatok beállítása
- tűzfalak létrehozása
- VPN kapcsolatok beállítása
- biztonsági feladatok végrehajtása

Az SDM a Cisco IOS szoftverkiadások széles skáláját támogatja, és ingyenesen elérhető számos Cisco forgalomirányítón. Az SDM előtelepítve megtalálható például a Cisco 1800-as sorozatú ISR flash memóriájában. Amennyiben az SDM telepítve van a forgalomirányítón, akkor érdemes azt használni a forgalomirányító első beállításához. A konfiguráció ilyen esetben a forgalomirányító egyik előre beállított hálózati portján keresztül történik.



Nem minden Cisco eszköz támogatja az SDM-et, és az SDM sem támogatja a parancssoros felületen elérhető összes parancsot. Ebből kifolyólag előfordulhat, hogy az SDM használatával megkezdett eszközbeállítást a CLI segítségével kell befejezni. A Cisco eszközök sikeres támogatásához elengedhetetlen mindkét fenti módszer ismerete.

	Cisco IOS CLI	Cisco SDM
Felhasználói felület	<ul style="list-style-type: none"> • Terminálemulációs szoftver • Telnet-kapcsolat 	Web alapú böngésző
Forgalomirányító konfigurációs módja	Szöveges alapú Cisco parancsok	GUI gombok és szövegdobozok
Cisco eszközök konfigurációjához szükséges szakértelem	A konfigurációs feladattól függ	Nem szükséges a CLI parancsok ismerete
Súgó lehetőségek	Parancssor alapú	Grafikus felületű on-line súgó és oktatási segédlet
Flash memória követelmények	Az IOS képfájl tartalmazza	6 MB szabad memória
Elérhetőség	Minden Cisco eszközönél	A Cisco 830-as sorozattól kezdődően a Cisco 7301-ig
Mely esetben használják?	<ul style="list-style-type: none"> • SDM-et nem támogató Cisco eszközök esetén • Cisco SDM által nem támogatott konfigurációs feladatok esetén 	<ul style="list-style-type: none"> • SDM-mel ellátott eszköz esetén a kezdeti konfiguráció elvégzéséhez • CLI ismeretek nélkül történő konfiguráláshoz

5.2 A Cisco SDM Express és az SDM használata

5.2.1 A Cisco SMD Express

A hálózat új eszközzel történő bővítésekor alapvető fontosságú, hogy meggyőződjünk az eszköz megfelelő működéséről. A hálózat bővítése egy rosszul konfigurált eszközzel az egész hálózat működésképtelenségéhez vezethet.

A hálózati eszközök (pl. egy forgalomirányító) beállítása a konfigurálásra használt eszköztől függetlenül rendkívül összetett feladat lehet. A bevált módszereket követése az új eszköz beüzemelése során biztosítja, hogy megfelelően végezzük el az eszközbeállításokat és a beállítások dokumentálását.

Bevált módszer	Részletek
1. Szerezzünk be és dokumentáljunk minden információt a konfiguráció megkezdése előtt!	<ul style="list-style-type: none"> • Az eszközhöz rendelt név • A helyszín, ahová majd telepítésre kerül • Felhasználói nevek és jelszavak • Szükséges kapcsolattípusok (LAN és WAN) • IP-cím információk minden hálózati interfészről, beleértve az IP-címet, az alhálózati maszkot és az alapértelmezett átjárót • DHCP-kiszolgáló beállítások • Hálózati címfordítás beállításai • Tűzfal beállítások
2. Hozzunk létre egy hálózati diagramot, amely bemutatja, hogyan fognak csatlakozni a kábelek!	<ul style="list-style-type: none"> • Jelöljük be a diagramon az interfészek rendeltetését és a címinformációkat!
3. Hozzunk létre egy ellenőrző jegyzéket a konfigurációs lépésekről!	<ul style="list-style-type: none"> • Jelöljük meg minden egyes lépést, amint az sikeresen befejeződött!
4. Ellenőrizzük a konfigurációt egy hálózati szimulátor segítségével!	<ul style="list-style-type: none"> • Próbáljuk ki, mielőtt az éles hálózatban alkalmaznánk!
5. Frissítsük a hálózat dokumentációját és egy példányt tartsunk belőle biztonságos helyen!	<ul style="list-style-type: none"> • Mentsük le egy kiszolgálóra! • Nyomtassuk ki, és tartsuk irattároló szekrényben!

A Cisco SDM Express a "Cisco Router and Security Device Manager" csomag részét képezi, amely megkönnyíti a forgalomirányító alapkonfigurációjának kialakítását. Az SDM Express használatának megkezdéséhez a PC hálózati csatlóját kábellel kössük össze a beállítandó forgalomirányító vagy ISR kezelési útmutatójában megadott Ethernet portjával!

Az SDM Express nyolc konfigurációs képernyőn vezeti végig a felhasználót a forgalomirányító alapkonfigurációjának kialakításához.

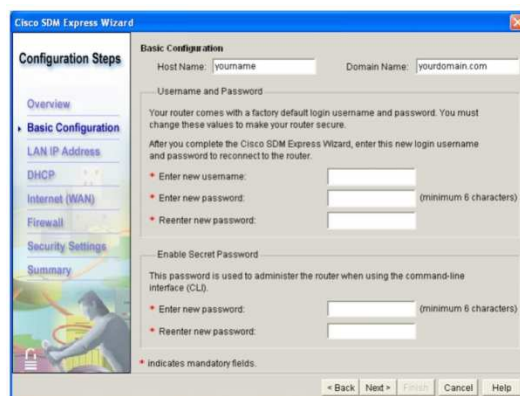
- Overview (Áttekintés)
- Basic Configuration (Alapbeállítások)
- LAN IP Address (LAN IP-cím)
- DHCP
- Internet (WAN)
- Firewall (Tűzfal)
- Security Settings (Biztonsági beállítások)
- Summary (Összefoglalás)

Az SDM Express grafikus felülete lépésről lépésre vezet végig bennünket a forgalomirányító kezdeti konfigurációjának kialakítása során. Miután a kezdeti konfiguráció elkészült, a forgalomirányító elérhetővé válik a LAN hálózaton. A forgalomirányító ezen kívül rendelkezhet WAN kapcsolattal, tűzfallal, és közel 30 beállítást kínál a hálózati biztonság fokozásához.

5.2.2 Az SDM Express beállítási lehetőségei

Az SDM Express "Basic Configuration" képernyőjén a forgalomirányító beállításához szükséges alapvető beállítások adhatók meg. Az alábbi adatok megadására van szükség:

- **Hostname** (állomás név) - A beállítandó forgalomirányítóhoz rendelt név.
- **Domain name for the organization** (a szervezet tartományneve) - A vállalat tartományneve (pl. cisco.com). A tartománynév többféleképpen végződhet (pl. .org, .net).
- **Username and password** (felhasználói név és jelszó) - Az SDM Express-ben a forgalomirányító beállításához és figyelemmel kíséréséhez szükséges felhasználói név és jelszó. A jelszónak legalább hat karakter hosszúságúnak kell lennie.
- **Enable secret password** (privilegizált üzemmódú titkos jelszó) - A forgalomirányítóhoz való (parancssoros felületen, telneten vagy konzolporton keresztül történő) hozzáférést szabályozó titkos jelszó. A jelszónak legalább hat karakter hosszúságúnak kell lennie.

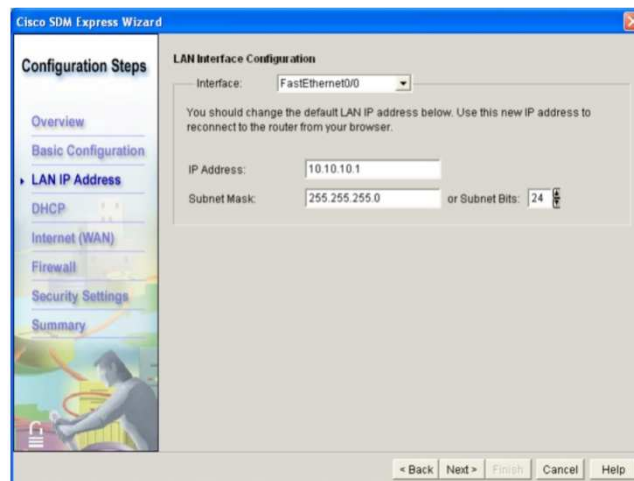


A LAN konfigurációs beállítások lehetővé teszik, hogy a forgalomirányító interfésze részt vegyen a csatlakoztatott helyi hálózatban.

- **IP address** (IP-cím) - A LAN interfész pontokkal tagolt, decimális számjegyekkel megadott IP-címe. Ez lehet privát IP-cím is, amennyiben az eszköz hálózati címfordítást (NAT) vagy portcímfordítást (PAT) alkalmazó hálózaton van telepítve.

Fontos, hogy lejegyezzük ezt a címet! Amikor a forgalomirányító újraindul, az SDM Express ezen a címen, nem pedig a kezelési összefoglalóban megadott címen érhető el.

- **Subnet mask** (alhálózati maszk) - Az IP-cím hálózati részét azonosító alhálózati maszk.
- **Subnet bits** (alhálózati bitek) - Az IP-cím hálózati részét meghatározó bitek száma. Az alhálózati maszk helyett használható.
- **Wireless parameters** (vezeték nélküli paraméterek) - Opcionális vezeték nélküli paraméterek. Akkor jelenik meg, ha a forgalomirányító rendelkezik vezeték nélküli interfésszel, és a "Yes" gombra kattintottunk a "Wireless Interface Configuration" ablakban. Megadja a vezeték nélküli hálózat SSID-jét.



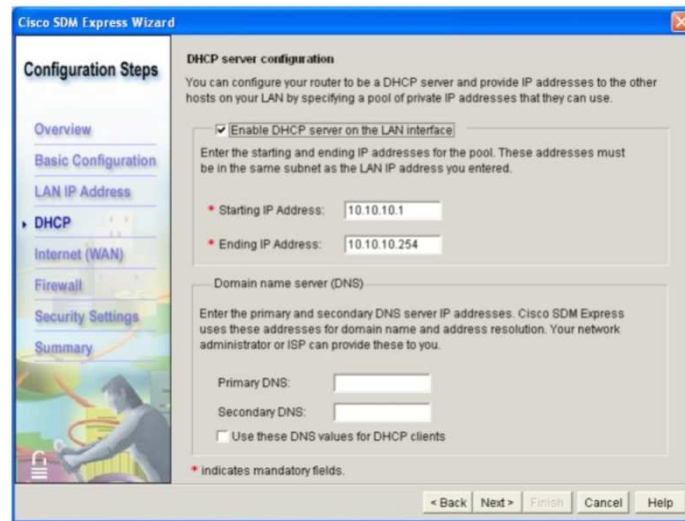
A DHCP az IP-címek állomásokhoz és eszközökhöz rendelésének egyszerű módja. A DHCP egy állomás bekapcsolásakor dinamikusan kioszt egy IP-címet, majd az állomás kikapcsolásakor visszaveszi azt. Ily módon a már nem használt IP-címek újból kioszthatók. Az SDM Express használatával a forgalomirányító beállítható DHCP-kiszolgálóként, amely címeket rendel a belső helyi hálózat egyes eszközeihez (pl. a PC-khez).

Egy eszköz DHCP-kiszolgálóként történő beállításához jelöljük be az **Enable DHCP Server on the LAN Interface** jelölőnégyzetet! Ez a beállítás lehetővé teszi, hogy a forgalomirányító privát IP-címeket rendeljen a LAN eszközökhöz. Az IP-címek lejáratí ideje egy nap.

A DHCP a megengedett IP-címek egy tartományát használja. Az érvényes címtartomány alapértelmezés szerint a LAN interfész esetében megadott IP-címen és alhálózati maszkon alapul.

A kezdőcím az IP-címtartomány legalacsonyabb címe. A kezdő IP-cím megváltoztatható, de ugyanabba a hálózatba vagy alhálózatba kell esnie, mint a LAN interfész címének.

A legmagasabb IP-cím megváltoztatásával csökkenthető a címtartomány mérete, de ugyanabba a hálózatba vagy alhálózatba kell esnie, mint a LAN interfész címének.



A DHCP konfiguráció további paramétereit:

- **Domain name for the organization** (a szervezet tartományneve) - Ezt a nevet kapják az állomások a DHCP konfiguráció részeként.
- **Primary domain name server** (elsődleges tartománynév-kiszolgáló) - Az URL-ek és hálózati nevek feloldásához használt elsődleges tartománynév-kiszolgáló IP-címe.
- **Secondary domain name server** (másodlagos tartománynév-kiszolgáló) - A másodlagos DNS-kiszolgáló IP-címe, amennyiben elérhető. Abban az esetben használható, ha az elsődleges DNS-kiszolgáló nem válaszol.

A **Use these DNS values for DHCP clients** lehetőség kiválasztásával a DHCP-kiszolgáló a DHCP-ügyfelekhez rendelheti a megadott DNS beállításokat. Ez a lehetőség akkor érhető el, ha a DHCP-kiszolgáló engedélyezve van a LAN interfészen.

5.2.3 A WAN kapcsolatok beállítása az SDM Express használatával

A nagy földrajzi távolságokkal elválasztott hálózatok összekötéséhez soros kapcsolatot használunk. Az ilyen WAN-kapcsolatok megvalósításához szükség van egy távközlési szolgáltatóra (TSP).

A soros összeköttetés általában lassabb az Ethernet kapcsolatnál, és további beállításokat igényel. Még az összeköttetés létrehozása előtt meg kell határoznunk a szükséges kapcsolattípust és a beágyazási protokoll típusát!

A soros összeköttetés mindkét végén ugyanolyan beágyazási protokoll használata szükséges. A beágyazási protokoll némelyikének szüksége lehet hitelesítési paraméterek (pl. felhasználói név és jelszó) beállítására. Beágyazási típusok:

- felső szintű adatkapcsolat-vezérlés (HDLC)
- Frame Relay
- pont-pont protokoll (PPP)

Add Serial0/1/0 Connection

Interface: Serial0/1/0
Note: Enter the WAN parameters that your service provider gave you.

Encapsulation: HDLC

Address Type: No IP Address

There is no IP address configured on the interface.

OK Cancel Help

Felső szintű adatkapcsolat-vezérlés (HDLC)

Az International Standards Organization (ISO) által kifejlesztett bit-orientált adatkapcsolati rétegbeli protokoll.

Add Serial0/1/0 Connection

Interface: Serial0/1/0
Note: Enter the WAN parameters that your service provider gave you.

Encapsulation: FrameRelay

Address Type: No IP Address

There is no IP address configured on the interface.

DLCI: 205

LMI Type
☐ ANSI ☐ Cisco ☐ ITU-TQ.933 ☒ autosense

☐ Use IETF Frame Relay encapsulation

OK Cancel Help

Frame Relay

Csomagkapcsolt adatkapcsolati rétegbeli protokoll, mely képes több virtuális áramkört is kezelni, abban az értelemben, hogy igény szerint ideiglenesen felépíti, majd lebontja a kommunikációs áramköröket. A DLCI egy olyan szám, melyet a szolgáltató biztosít és a virtuális áramkör azonosításához szükséges.

Add Serial0/1/1 Connection

Interface: Serial0/1/1
Note: Enter the WAN parameters that your service provider gave you.

Encapsulation: PPP

Address Type: IP Negotiated

This interface will obtain IP address using PPP/IPC (IP Control Protocol) address negotiation.

Authentication
Enter a valid username and password for CHAP and/or PAP authentication.

Authentication Type: ☐ CHAP ☐ PAP

Username:

Password:

Confirm Password:

OK Cancel Help

Pont-pont protokoll (PPP)

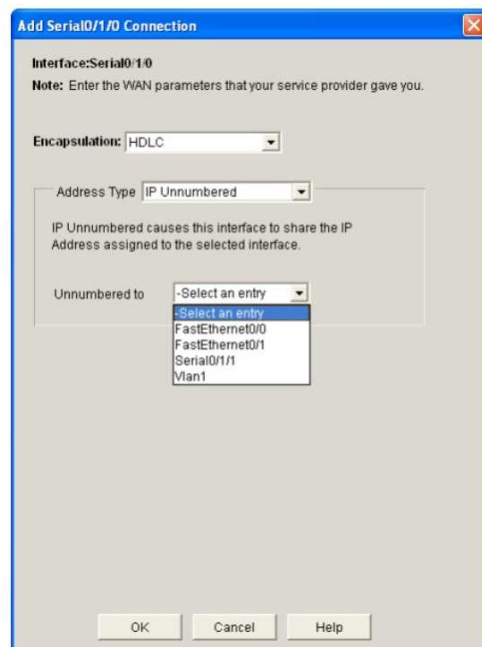
Gyakran használják két eszköz közötti, közvetlen kapcsolat kialakítására. Segítségével számítógépek kapcsolhatóak össze soros kábel, telefonvonal, gerincvonal, mobiltelefonos hálózat, speciális rádiós kapcsolat vagy optikai szál összeköttetés használatával. A legtöbb internetszolgáltató PPP-t használ, az előfizetői betárcsázós (dial-up) internet hozzáférések esetén. A PPP olyan jellemzőkkel is rendelkezik, melyek lehetővé teszik a kapcsolat létrejötte előtti hitelesítést. A PPP felhasználói neveket és jelszavakat SDM segítségével is be lehet állítani.

A WAN konfigurációs ablak további WAN paraméterek megadását teszi lehetővé.

Az "Address Type" (címtípusok) listája

A kiválasztott beágyazástól függően a soros interfészen az IP-címek kérésének különböző módjai érhetők el.

- **Static IP address** (statikus IP-cím) - Frame Relay, PPP és HDLC beágyazásokhoz egyaránt használható. A statikus IP-cím beállításához az IP-cím és az alhálózati maszk megadása szükséges.
- **IP unnumbered** (számozatlan IP) - a soros interfész címét a forgalomirányító egy másik, működő interfészének címére állítja be. Frame Relay, PPP és HDLC beágyazásokhoz egyaránt használható.
- **Egyeztetett IP** - Az IP-címet a forgalomirányító automatikusan, a PPP-n keresztül kapja.
- **Easy IP (IP negotiated)** (Egyeztetett IP) - Az IP-címet a forgalomirányító automatikusan, a PPP-n keresztül kapja.



5.2.4 A NAT beállítása a Cisco SDM használatával

A forgalomirányító beállításához mind a Cisco SDM Express, mind pedig a Cisco SDM használható.

Az SDM az SDM Express számos funkcióját támogatja, ugyanakkor sokkal összetettebb konfigurációs lehetőségeket is kínál. Ennek köszönhetően, számos felhasználó a forgalomirányító alapkonfigurációját az SDM Express segítségével adja meg, majd később, például a NAT engedélyezéséhez, átvált az SDM-re.

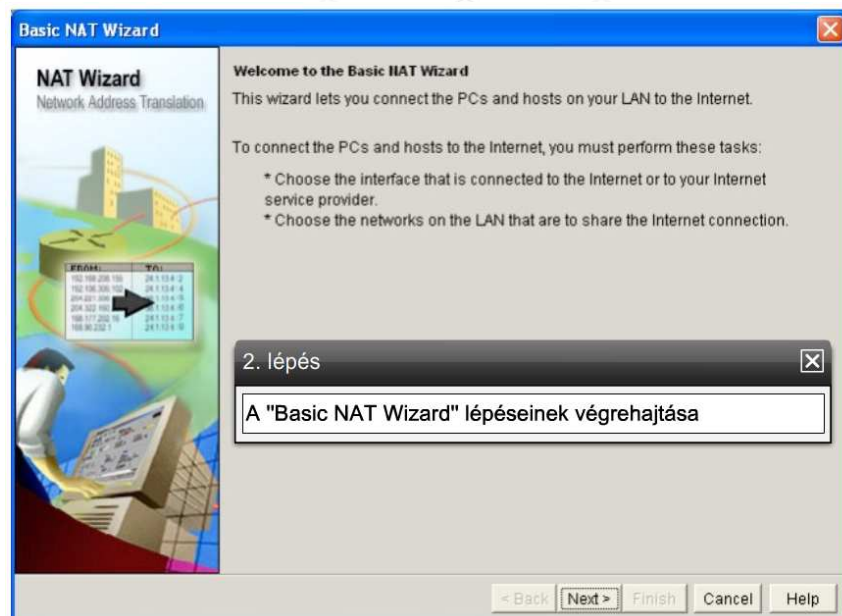
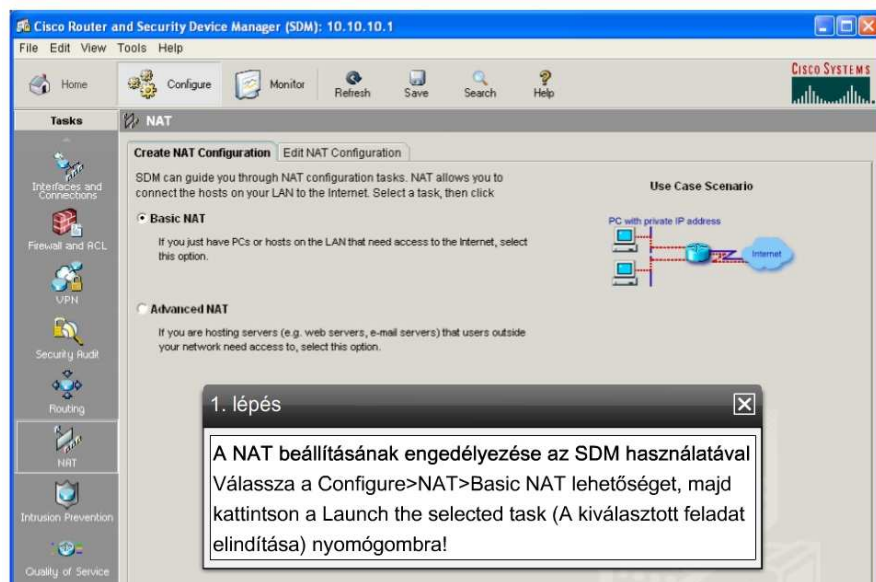
A "Basic NAT Wizard" (alapszintű NAT varázsló) alapértelmezés szerint a dinamikus NAT-ot és PAT-ot állítja be. A PAT lehetővé teszi a belső helyi hálózat állomásai számára, hogy a WAN-interfészhez

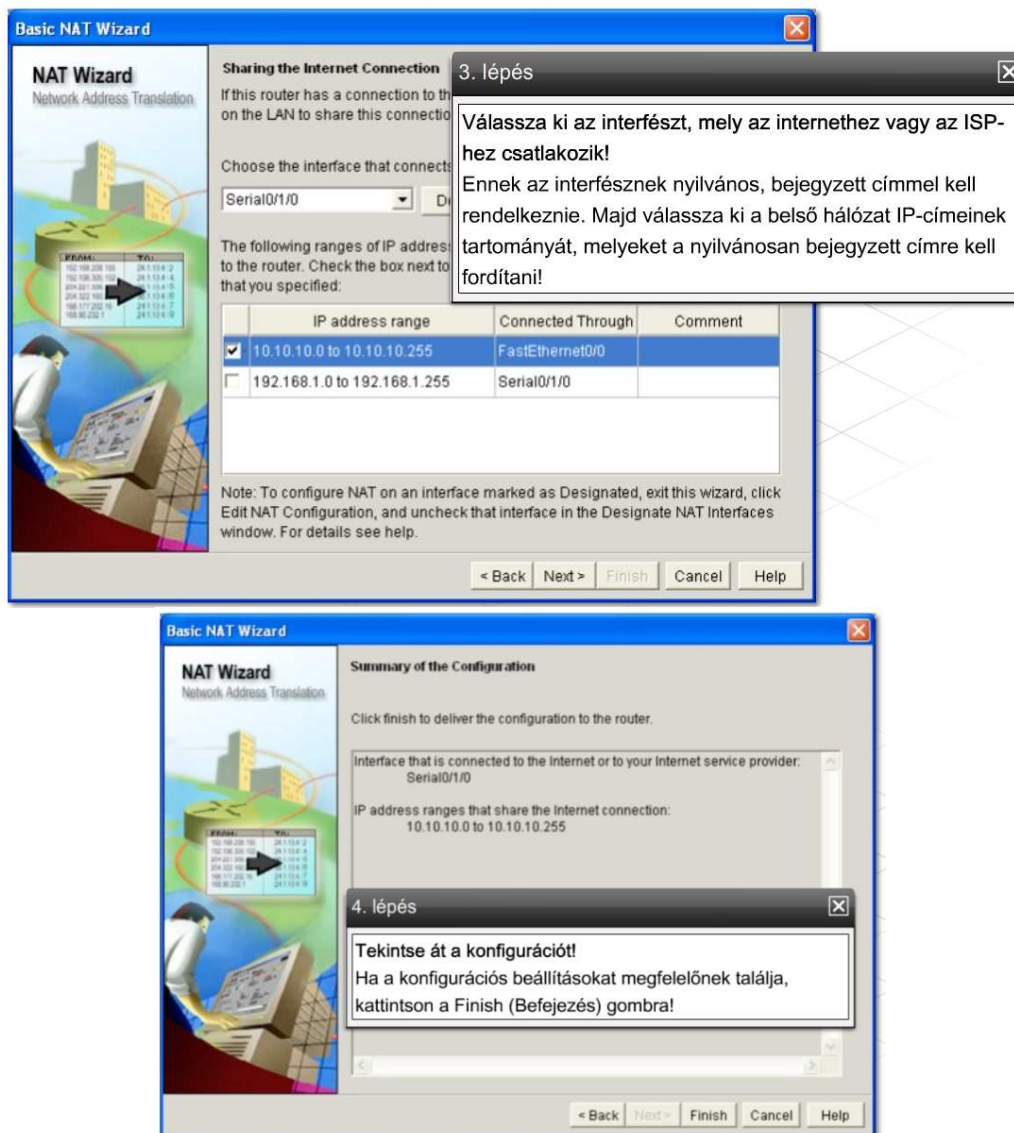
társított egyetlen IP-címen osztozzanak, így módon a belső privát címmel rendelkező állomások is elérhetik az internetet.

Kizárólag az SDM konfigurációjában megadott belső címtartományból származó ügyfelek címeinek fordítása történik meg. Fontos annak ellenőrzése, hogy az internetelérést igénylő összes címtartomány szerepeljen itt!

A NAT beállításának lépései:

- 1. lépés:** A NAT beállításának engedélyezése az SDM használatával
- 2. lépés:** A "Basic NAT Wizard" lépéseinek végrehajtása
- 3. lépés:** Az interfész kiválasztása és az IP-címtartományok megadása
- 4. lépés:** A konfiguráció ellenőrzése





5.3 A forgalomirányító IOS parancssori (CLI) konfigurálása

5.3.1 A parancssoros felület üzemmódjai

Egy eszköz beállítása és figyelemmel kísérése a Cisco IOS parancssorából teljesen eltér az SDM használatától. A CLI nem segít a konfiguráció lépésről lépésre történő megadásában, így a használata több tervezést és nagyobb szaktudást igényel.

CLI parancsmódok

A Cisco IOS a parancssorhoz történő hozzáférés két szintjét különbözteti meg: a felhasználói EXEC módot, valamint a privilegizált EXEC módot.

A forgalomirányító vagy más Cisco IOS-t használó eszköz elindulásakor az alapértelmezés szerinti hozzáférési szint a felhasználói EXEC mód, amelyet a parancssor készenléti jele (prompt) az alábbi módon jelez:

Router>

A felhasználói EXEC módban végrehajtható parancsokkal információ kérhető az eszköz működéséről, valamint hibaelhárítás is végezhető a show parancsok, a ping és a traceroute segédprogramok segítségével.

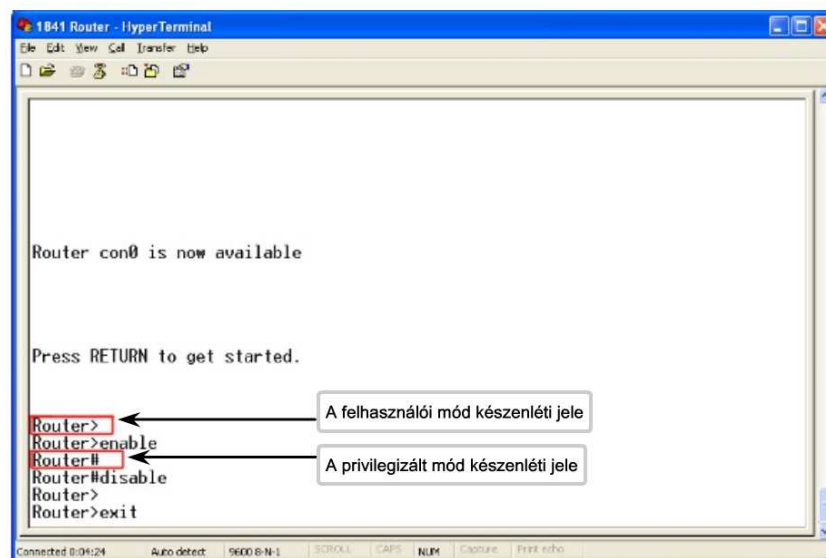
Az eszköz működését megváltoztató parancsok kiadásához privilegizált szintű hozzáférés szükséges. A privilegizált EXEC mód engedélyezése az enable parancsnak a parancssorba történő begépelésével és az Enter leütésével történik.

A parancssor készenléti jele a módváltást követően megváltozik. A privilegizált EXEC mód promptja:

Router#

A privilegizált EXEC módból való kilépéshez és a felhasználói EXEC módba való visszatéréshez adjuk ki a disable vagy az exit parancsot!

Mindkét mód jelszóval, vagy felhasználói név és jelszó párosával védhető.



Egy eszköz beállításához számos konfigurációs mód áll rendelkezésre. A Cisco IOS eszközök beállítása a privilegizált EXEC módba történő belépéssel kezdődik. Az egyéb konfigurációs módok innen érhetők el.

A legtöbb esetben a terminálkapcsolaton keresztül kiadott parancsok az aktuális konfigurációs fájl tartalmát módosítják. Ezen parancsok kiadásához a felhasználónak be kell lépnie a globális konfigurációs módba.

A globális konfigurációs módba történő belépéshez gépeljük be a configure terminal vagy a conf t parancsot! A parancssor promptja a módváltást követően megváltozik:

Router(config)#

Az ebben a módban kiadott parancsok hatása azonnal érvényre jut, és megváltoztatja az eszköz működését.

Az adminisztrátor a globális konfigurációs módból különböző alüzemmódokba léphet.

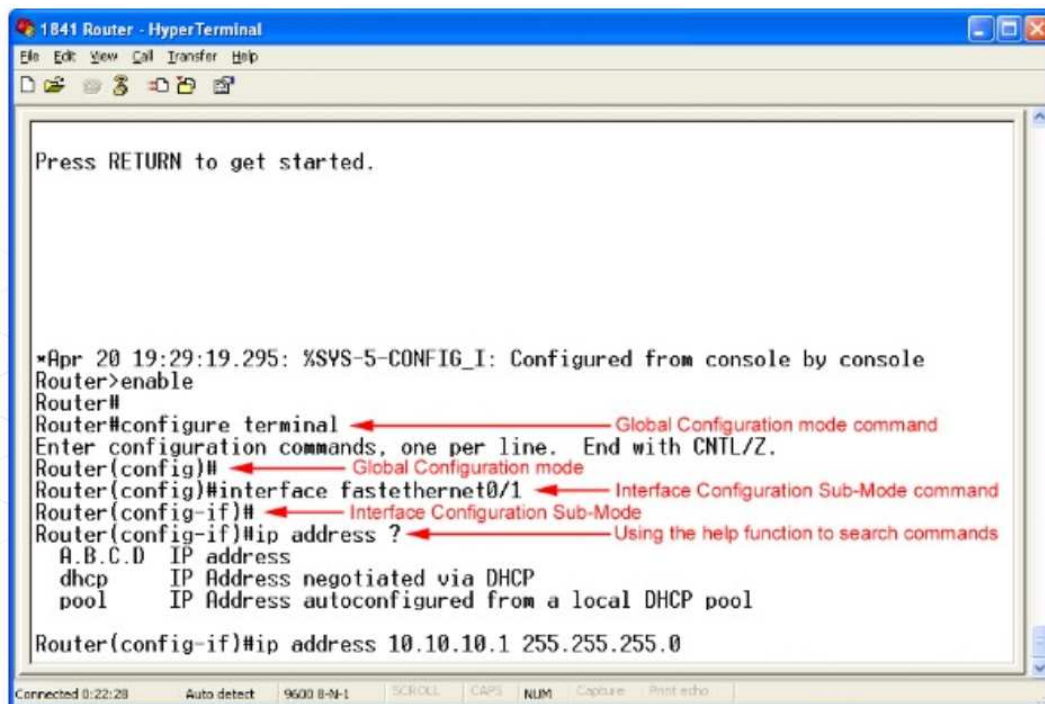
A LAN- és WAN-interfészek beállításához az interfészkonfigurációs mód használható. Az interfészkonfigurációs módba történő belépéshez gépeljük be az interface [típus] [szám] parancsot! A parancssor promptja a módváltást követően megváltozik:

```
Router(config-if)#
```

Szintén gyakran használt alüzemmód a forgalomirányító-konfigurációs üzemmód, amely a parancssorban így látszik:

```
Router(config-router)#
```

Ez a mód a forgalomirányítási paraméterek beállításához használható.



5.3.2 A Cisco IOS parancssoros felületének használata

A Cisco IOS parancssoros felülete számtalan olyan lehetőséget kínál, amely segít az eszközök beállításához szükséges parancsok felidézésében. Ez az egyik oka annak, hogy a hálózati szakemberek a Cisco IOS parancssoros felületét részesítik előnyben a forgalomirányítók konfigurálásához.

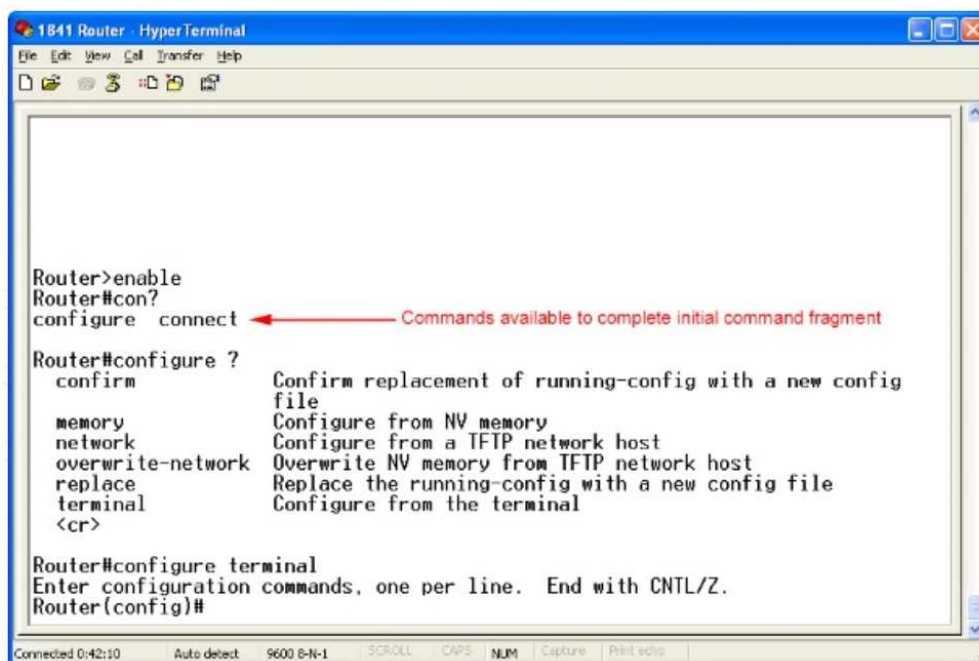
A környezetérzékeny súgó különösen hasznos az eszközök beállítása során. A parancssorba gépelt help vagy ? megjeleníti a súgó rövid leírását.

```
Router# help
```


A környezetérzékeny súgó javaslatokat tehet egy parancs kiegészítésére. Ha csak a parancs első néhány karakterére emlékszünk, de a teljes alakot nem ismerjük, akkor írjuk be a parancs bevezető karaktereit, majd a végére tegyünk egy ? karaktert. Ügyeljünk arra, hogy a ? előtt ne legyen szóköz!

Ahhoz, hogy egy konkrét parancs paraméterlistáját megkapjuk, gépeljük be a parancs egy részét, majd egy szóközt, ezt követően pedig egy ? karaktert! Például a configure parancs begépelése után tett szóköz, majd ? megjeleníti a lehetséges variációk listáját. A parancs kiegészítéséhez válasszunk egyet a felkínált lehetőségek közül! Amikor a parancs elérte a teljes alakját, a <cr> jelenik meg. Ekkor az Enter lenyomásával adjuk ki a parancsot!

Amennyiben a ? begépelése után nincs találat, a súgólista üres marad. Ez azt jelzi, hogy a rendszer nem ismer ilyen kezdetű parancsot.



```
Router>enable
Router#con?
configure connect
Router#configure ?
confirm          Confirm replacement of running-config with a new config
memory          Configure from NV memory
network         Configure from a TFTP network host
overwrite-network Overwrite NV memory from TFTP network host
replace         Replace the running-config with a new config file
terminal        Configure from the terminal
<cr>
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Előfordul, hogy a felhasználók elgépelik a kiadni kívánt parancsot. A CLI jelzi, ha nem ismert vagy befejezetlen parancsot vittünk be. A % jel a hibaüzenet kezdetét jelöli. Ha az interface parancsot például paraméterek nélkül adjuk ki, a parancs befejezetlenségére utaló hibaüzenet jelenik meg:

% Incomplete command

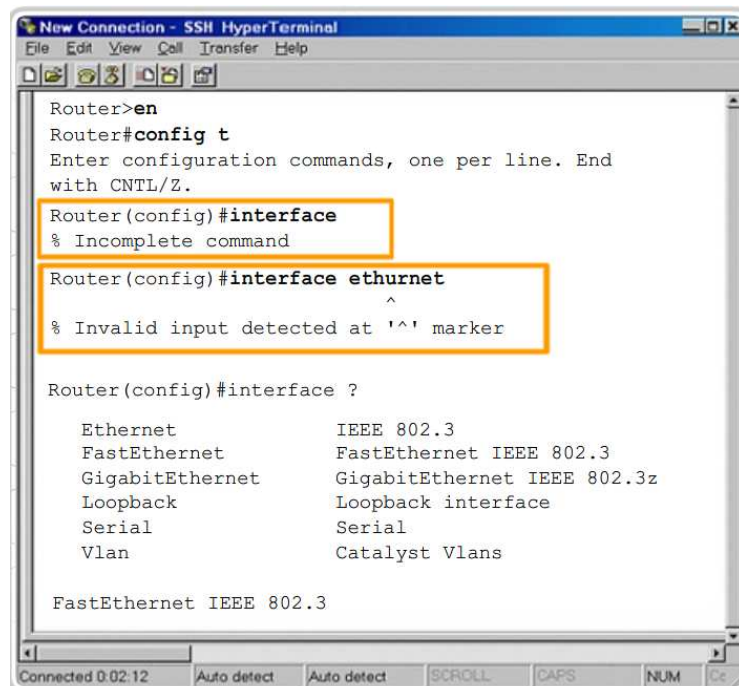
Használjuk a ? karaktert, hogy megkapjuk az elérhető paraméterek listáját!

Ha hibás parancsot gépelünk be, az alábbi hibaüzenet jelenik meg:

% Invalid input detected

Előfordul, hogy a rosszul begépelte parancsban nehezen találjuk meg a hibát. Szerencsére a CLI rendelkezik hibajelzővel. A beszúrási jel (^) a begépelte parancs első hibás vagy nem felismert

karakterénél jelenik meg. A felhasználó így visszatérhet a hiba helyéhez, és a súgó segítségével meghatározhatja a helyes parancsot.



```
Router>en
Router#config t
Enter configuration commands, one per line. End
with CNTL/Z.
Router(config)#interface
% Incomplete command
Router(config)#interface ethurnet
^
% Invalid input detected at '^' marker

Router(config)#interface ?

Ethernet                IEEE 802.3
FastEthernet            FastEthernet IEEE 802.3
GigabitEthernet         GigabitEthernet IEEE 802.3z
Loopback                Loopback interface
Serial                  Serial
Vlan                    Catalyst Vlans

FastEthernet IEEE 802.3
```

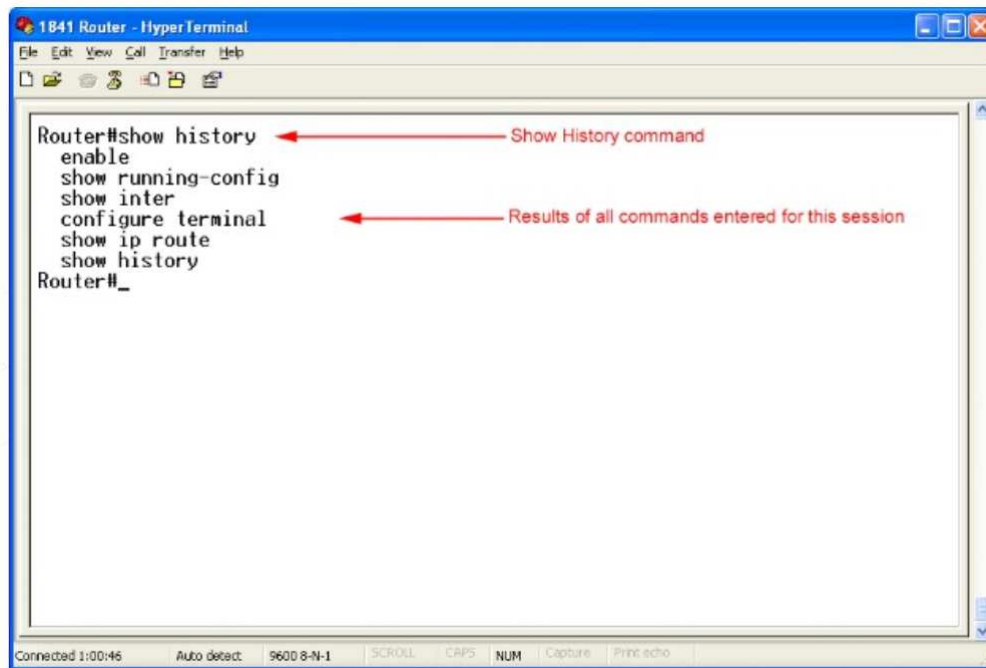
A Cisco IOS parancssoros felületének másik funkciója az előzőleg begépelte parancsok megjegyzése. A szolgáltatás különösen a hosszú és bonyolult parancsok előhívásánál hasznos.

A parancselőzmény funkció alapértelmezés szerint engedélyezett, és a 10 előzőleg kiadott parancsot a parancselőzmény-pufferben tárolja. A terminálkapcsolat eltárolt parancssorai számának megváltoztatásához a terminal history size és a history size parancs használható. A maximálisan eltárolható parancssorok száma 256.

Ahhoz, hogy a legutóbbi parancsot előhívjuk a parancselőzmény-pufferből, nyomjuk le a Ctrl-P billentyűkombinációt vagy a felfelé nyilat! A fenti folyamat ismételtetésével az egyre korábbi parancsok előhívása lehetséges. Amennyiben a tárolt legrégebbi parancsot akarjuk előhívni, nyomjuk le a Ctrl+N billentyűkombinációt vagy a lefelé nyilat! A fenti folyamat ismételtetésével az egyre későbbi parancsok előhívása lehetséges.

A CLI felismeri a részlegesen begépelte parancsokat az első egyedi karakter alapján. Az "interface" helyett például gépeljük be az "int" rövidítést! Ezután a Tab billentyű lenyomásával a parancsrészlet automatikusan kiegészül a teljes "interface" parancsra.

A legtöbb számítógépen megfelelő funkcióbillentyűk segítségével a vágólap kijelölési és másolási funkciója is használható. Egy korábbi parancsot például vágólapra lehet másolni, majd beilleszteni az éppen beírt parancs sorába.



```
Router#show history
enable
show running-config
show inter
configure terminal
show ip route
show history
Router#_
```

5.3.3 A Show parancsok használata

A Cisco IOS parancssoros felülete a show parancsot használja az eszközök konfigurációjával és működésével kapcsolatos információk megjelenítésére.

A hálózati szakemberek sokszor használják a show parancsokat a konfigurációs fájlok megtekintéséhez, az eszközök interfészeinek és folyamatainak állapotellenőrzéséhez és az eszköz működőképességének vizsgálatához. A show parancsok attól függetlenül használhatók, hogy az eszköz konfigurálásához a CLI-t vagy az SDM-et használtuk.

A forgalomirányító szinte minden folyamatának és funkciójának állapota megjeleníthető valamelyik show parancs segítségével. A leggyakrabban használt show parancsok közül néhány:

- *show running-config*
- *show interfaces*
- *show arp*
- *show ip route*
- *show protocols*
- *show version*

5.3.4 Az alapkonzfiguráció

A Cisco IOS eszközök kezdeti konfigurációjának megadásához hozzátartozik az eszköznév és a különféle funkciókhoz való hozzáférést szabályozó jelszavak beállítása.

Első lépésben adjunk egyedi nevet az eszköznek, amely a globális konfigurációs módban az alábbi parancs kiadásával lehetséges:

```
Router(config)# hostname <név>
```

Az Enter billentyű lenyomását követően a prompt az alapértelmezés szerinti Router-ről az újonnan beállított állomásnévre változik.

A következő lépésben állítsunk be az illetéktelen személyek hozzáférését megakadályozó jelszavakat!

Az *enable password* és az *enable secret* parancsokkal korlátozható a privilegizált EXEC módba történő belépés, így az illetéktelen felhasználók nem változtathatják meg a forgalomirányító beállításait.

```
Router(config)# enable password <password>
```

```
Router(config)# enable secret <password>
```

A fenti két parancs közötti különbség az, hogy az *enable password* alapértelmezés szerint nincs titkosítva. Amennyiben az "enable password" paranccsal megadott jelszót az "enable secret" paranccsal megadott jelszó követi, akkor az *enable secret* parancs felülírja az *enable password* parancsot.



A forgalomirányító alapbeállításai közé tartozik még a bejelentkezési üzenet beállítása, az egyidejű naplózás engedélyezése és a tartománynév-kiszolgáló keresésének tiltása is

Bejelentkezési üzenetek

A bejelentkezési üzenet olyan szöveg, amelyet a felhasználó a forgalomirányítóra történő bejelentkezés kezdetén lát. Egy jó biztonsági tervnek ki kell terjednie a megfelelő bejelentkezési üzenet meghatározására is. Az a legkevesebb, hogy a bejelentkezési üzenet figyelmeztessen arra, hogy az illetéktelen hozzáférés nem megengedett. Soha ne állítsunk be illetéktelen felhasználót üdvözlő bejelentkezési üzenetet!

A bejelentkezési üzeneteknek két típusa van: a nap üzenete (MOTD, message-of-the-day) és a bejelentkezési információk. Azért van szükség két, egymástól független üzenetre, hogy az egyik esetleges megváltoztatása ne legyen hatással az egész bejelentkezési üzenetre.

A bejelentkezési üzenetek beállításához a *banner motd* és a *banner login* parancsok használhatók. Mindkét típusnál valamilyen elválasztó karakter -- ilyen például a # -- szerepel az üzenet elején és végén. Az elválasztó karakter segítségével a felhasználó akár több soros üzenetet is beállíthat.

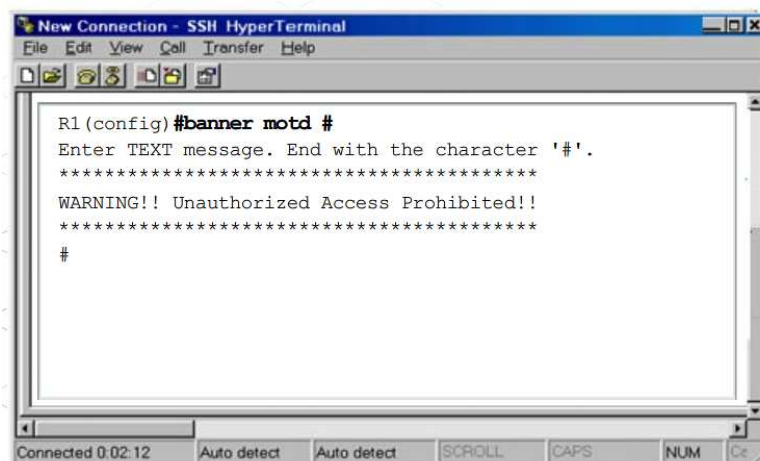
Amennyiben mindkét bejelentkezési üzenet be van állítva, a bejelentkezési információk a nap üzenetét követően jelennek meg.

Egyidejű naplózás

A Cisco IOS szoftver gyakran küld kéretlenül üzeneteket a képernyőre, például egy konfigurált interfész állapotváltozásáról. Előfordul, hogy ezek az üzenetek éppen gépelés közben jelennek meg. Habár az üzenetnek nincs hatása a parancsra, mégis megzavarhatja a felhasználót gépelés közben. A kéretlenül érkező üzenetek elválaszthatók a begépelte adatoktól a globális konfigurációs módban kiadott *logging synchronous* paranccsal.

A tartomány-kiszolgáló keresésének tiltása

A privilegizált (enable) módban bevitt állomásnevek esetében a forgalomirányító alapértelmezés szerint azt feltételezi, hogy a felhasználó telnet segítségével próbál kapcsolódni az eszközhöz. A privilegizált (enable) módban begépelte állomásnevek esetében a forgalomirányító alapértelmezés szerint azt feltételezi, hogy a felhasználó telnet segítségével próbál kapcsolódni egy eszközhöz. A privilegizált (enable) módban bevitt ismeretlen neveket a DNS-kiszolgálóhoz irányítva próbálja a forgalomirányító feloldani. Ez vonatkozik a forgalomirányító által fel nem ismert bármilyen bevitt szóra, beleértve az elgépelte parancsokat is. Amennyiben nincs szükségünk erre az alapértelmezés szerint bekapcsolt funkcióra, kikapcsolhatjuk a *no ip domain-lookup* parancs kiadásával.



Egy eszközhöz többféle módon kapcsolódhatunk, ha konfigurációs feladatokat akarunk végrehajtani. Ennek egyik módja, ha a PC-t csatlakoztatjuk az eszköz konzolportjához. Ez a módszer gyakran használatos az eszközök első beállításánál.

A konzolkapcsolaton keresztül történő hozzáférés a globális konfigurációs módban megadott jelszóval korlátozható. Az alábbi parancsok megakadályozzák, hogy illetéktelen felhasználók a konzolport használatával beléphessenek a felhasználói módba.

```
Router(config)# line console 0
```

```
Router(config)# password <password>
```

```
Router(config)# login
```

Amennyiben az eszköz csatlakoztatva van a hálózathoz, a hálózati kapcsolaton keresztül is elérhető. Az eszköz hálózaton keresztül történő elérése vty kapcsolatnak számít, ezért a jelszót a vty portra kell beállítani.

```
Router(config)# line vty 0 4
```

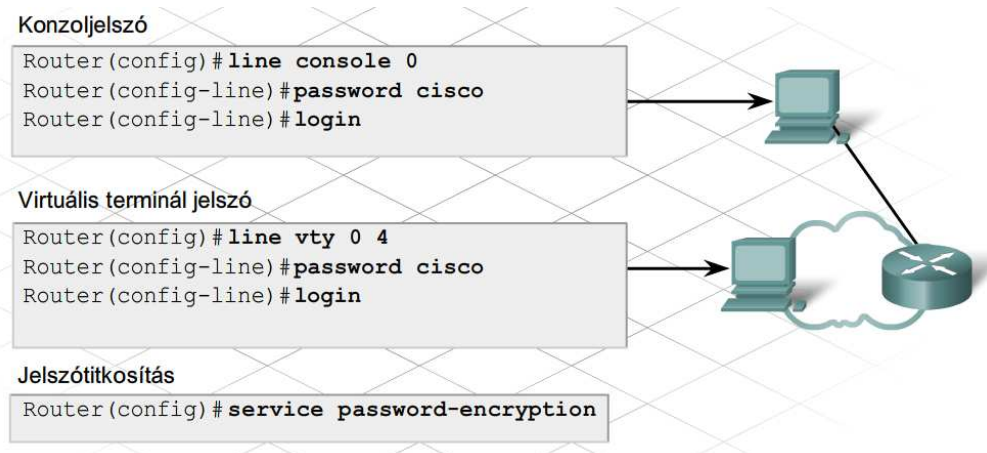
```
Router(config)# password <password>
```

```
Router(config)# login
```

A 0 4 öt egyidejű sávon-belüli kapcsolatot jelöl. Minden kapcsolathoz külön jelszó állítható be a konkrét vonalkapcsolat számának megadásával (pl.: *line vty 0*).

A jelszavak beállításának helyességét ellenőrizhetjük a `show running-config` parancs segítségével. Ezeket a jelszavakat az aktív konfiguráció tárolja egyszerű szöveg formájában. Lehetőség van a forgalomirányítón tárolt összes jelszó titkosítására, hogy az illetéktelenek ne tudják könnyen kiolvasni azokat. A globális konfigurációs módban kiadott `service password-encryption` parancs garantálja, hogy az összes jelszó titkosítva legyen.

Ne feledkezzünk meg arról, hogy a megváltozott aktív konfigurációt az indító konfigurációs fájlba másoljuk, máskülönben az eszköz kikapcsolásakor elvesznek a változtatásaink. Az aktív konfiguráció változásai az indító konfigurációs fájlba a `copy run start` paranccsal menthetők el.



5.3.5 Az interfészek beállítása

A forgalom egyik hálózathoz egy másikba történő irányításához a forgalomirányító interfészeit úgy kell beállítani, hogy mindegyik szóban forgó hálózathoz tartozzon egy-egy interfész. A forgalomirányító egy hálózathoz csatlakozó interfésze általában az adott hálózat állomásai által használt IP-tartományba tartozó IP-címet és alhálózati maszkot használ.

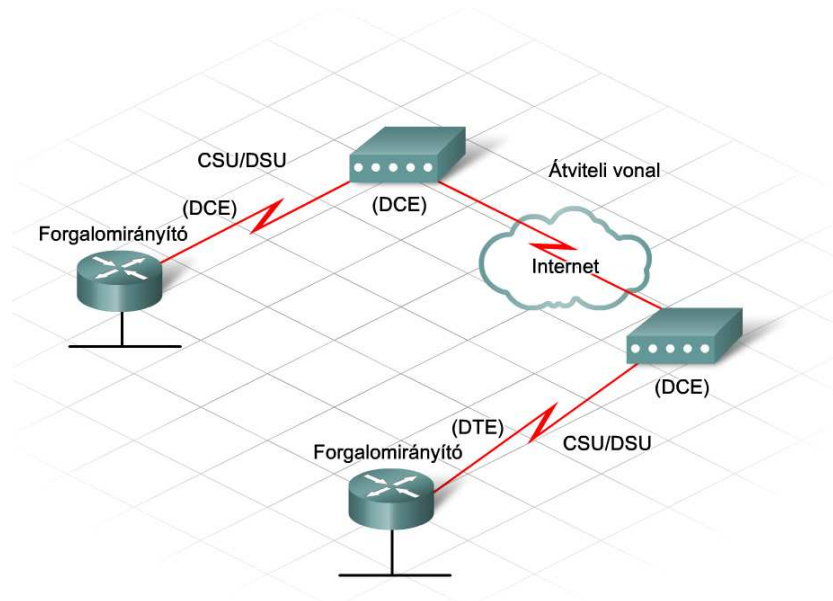
A forgalomirányítón különböző típusú interfészek vannak, amelyek közül a leggyakoribb a soros és az Ethernet interfész. A helyi hálózati kapcsolatok Ethernet interfészt használnak.

Egy WAN-összeköttetéshez az ISP-n keresztülhaladó soros kapcsolat szükséges. Az Ethernet interfészekkel szemben a soros interfészeknél a kommunikáció időzítésének kezeléséhez órajelre van szükség. A legtöbb esetben az órajelet egy adatkommunikációs berendezés (data communications equipment, DCE), például egy modem vagy egy CSU/DSU egység biztosítja.

Ha a forgalomirányító soros kapcsolaton keresztül kapcsolódik az ISP hálózatához, digitális WAN esetében egy CSU/DSU egység használata szükséges. Analóg WAN esetében modem használata szükséges. A fenti eszközök végzik a forgalomirányítóról érkező adatok átalakítását a WAN számára

elfogadható formára, valamint a WAN felől érkező adatok átalakítását a forgalomirányító számára elfogadható formára. Alapértelmezés szerint a Cisco forgalomirányítók adat-végberendezések (data terminal equipment, DTE). Mivel a DCE berendezések vezérlik a forgalomirányítóval történő kommunikáció időzítését, a Cisco DTE berendezések elfogadják a DCE berendezéstől érkező órajelet.

Habár nem túl gyakori, lehetőség van két forgalomirányító soros kapcsolaton keresztül történő, közvetlen összekötésére. Ebben az esetben nincs szükség CSU/DSU egység vagy modem használatára; az egyik forgalomirányítót kell DCE berendezésként konfigurálni, hogy biztosítsa az órajelet. Amennyiben a forgalomirányító DCE berendezésként van csatlakoztatva, az interfészen be kell állítani a DCE/DTE kapcsolat időzítését vezérlő órajelet!



A forgalomirányító interfészeinek beállítása a globális konfigurációs módból lehetséges. Az Ethernet interfészek beállítása nagyban hasonlít a soros interfészek beállításához. Az egyik fő különbség, hogy a DCE berendezésként működő soros interfészen be kell állítani az órajelet.

Az interfészek beállításának lépései

- 1. lépés:** Adjuk meg az interfész típusát és portszámát!
- 2. lépés:** Adjuk meg az interfész leírását!
- 3. lépés:** Állítsuk be az interfész IP-címét és alhálózati maszkját!
- 4. lépés:** DCE-ként működő soros interfész esetében állítsuk be az órajelet!
- 5. lépés:** Engedélyezzük az interfészt!

Az interfész engedélyezését követően karbantartás vagy hibaelhárítás miatt szükséges lehet az interfész leállítása. Ebben az esetben használjuk a shutdown parancsot!

Az 1841-es ISR soros interfészének beállítása során az interfészt három számjegy (C/S/P) azonosítja, ahol a C a vezérlő (controller) számát, az S a bővítőhely (slot) számát, a P pedig a port számát jelöli. Az 1841-es ISR két moduláris bővítőhellyel rendelkezik. A Serial0/0/0 jelölés arra utal, hogy a soros

interfész a 0. vezérlőn, a 0. bővítőhelyen található első (0.) port. A második interfészt a Serial0/0/1 jelöli. A soros modul normál esetben a 0. bővítőhelyre kerül, de telepíthető az 1. bővítőhelyre is. Ez utóbbi esetben az első soros interfészt a Serial0/1/0, míg a másodikat a Serial 0/1/1 jelöli.

Az olyan beépített portokat, mint például a FastEthernet port, két számjegy (C/P) azonosítja, ahol a C a vezérlő számát, a P pedig a port számát jelöli. Az Fa0/0 a 0. vezérlőt és a 0. interfészt jelöli.

```
Router(config)#interface fastethernet 0/0
Router(config-if)#description connection to Admin LAN
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#description connection to Router2
Router(config-if)#ip address 192.168.1.125 255.255.255.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
```

A közvetlenül csatlakoztatott soros kapcsolatoknál - ilyenek a laborgyakorlatok összeköttetései is - valamelyik oldalt ki kell jelölni DCE-nek; ez fogja biztosítani az órajelet. Az órajel engedélyezése és értékének megadása a `clock rate` paranccsal történik. A rendelkezésre álló órajelek bit/másodpercben megadva a következők: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 és 4000000. Néhány bitsebesség érték nem használható bizonyos soros interfészek esetén. Ez az egyes interfészek kapacitásától függ. Az ábrán bemutatott parancsokat kell használni az órajel beállításához és a soros interfész engedélyezéséhez.

5.3.6 Az alapértelmezett útvonal beállítása

A forgalomirányító a célállomás IP-címe alapján egyik hálózatból egy másikba továbbítja a csomagokat. A forgalomirányító az irányítótábla segítségével dönti el, hogy merre továbbítsa a csomagot, hogy az elérje a célhálózatot. Arra az esetre, ha az irányítótáblában nem szerepel egy adott hálózatba vezető útvonal, megadható egy alapértelmezett útvonal. Ezt akkor használja a forgalomirányító, ha nem tudja, hogy merre kell a csomagot továbbítani.

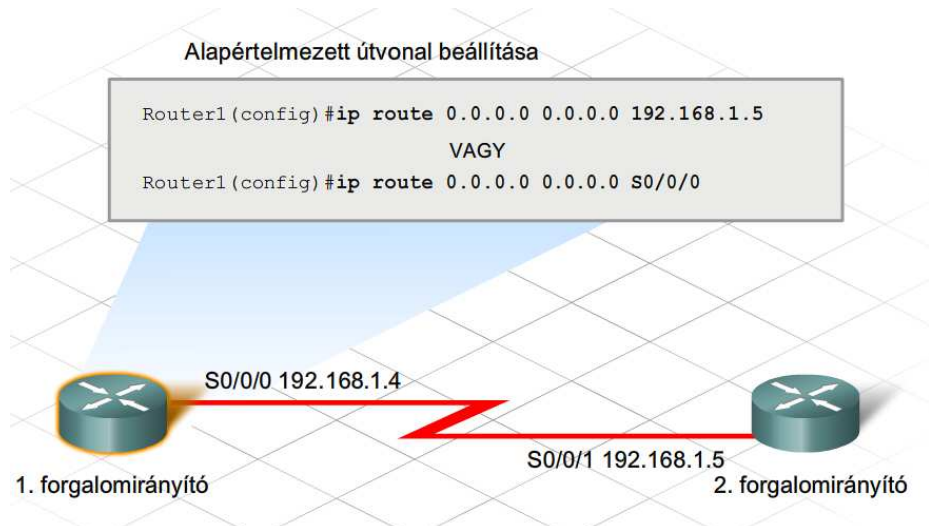
Az alapértelmezett útvonal általában az internet felé vezető, következő ugrást jelentő forgalomirányítóra mutat. Az alapértelmezett útvonal megadásához szükséges a következő ugrást jelentő forgalomirányító IP-címe vagy a helyi forgalomirányítónak az ismeretlen célhálózatba irányuló forgalom továbbítására használt interfész azonosítója.

A Cisco ISR-eken az alapértelmezett útvonal megadása a globális konfigurációs módban történik.

```
Router(config)# ip route 0.0.0.0 0.0.0.0 <next-hop-IP-address>
```

vagy

```
Router(config)# ip route 0.0.0.0 0.0.0.0 <interface-type> <number>
```



5.3.7 A DHCP-szolgáltatás beállítása

A Cisco IOS parancssoros felületén beállítható, hogy a forgalomirányító DHCP-kiszolgálóként működjön.

A DHCP-kiszolgálóként konfigurált forgalomirányító leegyszerűsíti az IP-címek kezelését a hálózaton. Az IP-konfiguráció paramétereinek megváltozása esetén a rendszergazdának csupán egyetlen helyen, a forgalomirányítón kell változtatnia. A DHCP parancssoros felületről történő beállítása némileg összetettebb az SDM használatával történő beállításnál.

A DHCP parancssoros felületről történő beállítása nyolc lépésből áll:

- 1. lépés:** A DHCP címkészlet létrehozása
- 2. lépés:** A hálózat vagy alhálózat megadása
- 3. lépés:** Bizonyos IP-címek kizárása
- 4. lépés:** A tartománynév megadása
- 5. lépés:** A DNS-kiszolgáló IP-címének megadása
- 6. lépés:** Az alapértelmezett átjáró beállítása
- 7. lépés:** A bérlet időtartamának beállítása
- 8. lépés:** A beállítások ellenőrzése

```
Router(config)# ip dhcp pool LAN-cimek
Router(dhcp-config)#
```

1. lépés: A DHCP címkészlet létrehozása

Lépjen be privilegizált EXEC módba, írja be a jelszót, ha szükséges, majd lépjen globális konfigurációs módba! Most nevezze el a DHCP-kiszolgáló címkészletét! Egy forgalomirányítón egynél több címkészlet is létezhet. A Cisco IOS be fog lépni a DHCP címkészlet konfigurációs módba. Használja ezeket a parancsokat:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp pool LAN-cimek
```

Ebben a példában "LAN-cimek" néven került létrehozásra egy címkészlet.

```
Router(dhcp-config)# network 172.16.0.0 255.255.0.0
```

A hálózat vagy alhálózat megadása

Adja meg a DHCP címkészlet hálózati vagy alhálózati azonosítóját és az alhálózati maszkját! Használja ezt a parancsot:

```
Router(dhcp-config)# network 172.16.0.0 255.255.0.0
```

Az IOS verziójától függően, az alhálózati maszk megadható a prefix konvenció használatával is (/16).

```
Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103
```

3. lépés: Bizonyos IP-címek kizárása

A DHCP-kiszolgáló feltételezi, hogy a DHCP-címkészletben lévő összes IP-cím kiosztható a DHCP-ügyfeleknek. Tiltson le bizonyos címeket a címkészletből, így a DHCP-kiszolgáló nem fogja kiosztani azokat! Amennyiben címek tartományát szeretné kizárni, csupán annak kezdő és utolsó címét kell megadnia. Használja ezt a parancsot:

```
Router(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.103
```

Ebben a példában négy cím van kizárva. A 172.16.1.100, 172.16.1.101, 172.16.1.102, és 172.16.1.103 címeket nem osztja ki a DHCP kiszolgáló az állomásoknak. Ezek a címek statikusan megadhatóak a rendszergazda által.

```
Router(dhcp-config)# domain-name cisco.com
```

4. lépés: A tartománynév megadása

Most adja meg az ügyfelek tartománynévét! Használja ezt a parancsot:

```
Router(dhcp-config)# domain-name cisco.com
```

Ebben a példában az ügyfelek a cisco.com tartománynévet kapják meg a DHCP konfiguráció részeként. A tartománynév elhagyható konfigurációs paraméter, nem feltételenül szükséges a DHCP működéséhez. A hálózati rendszergazdától megtudhatja, hogy szükség van-e tartománynév használatára.

```
Router(dhcp-config)# dns-server 172.16.1.103 172.16.2.103
```

5. lépés: A DNS-kiszolgáló IP-címe

Adja meg a DHCP-ügyfél számára elérhető DNS-kiszolgáló IP-címét! Egy IP-címre van szükség. Egy sorban maximálisan nyolc IP-cím adható meg. Amennyiben több, mint egy DNS kiszolgálót szeretne beállítani, fontossági sorrendben írja be a címeket. Használja ezt a parancsot:

```
Router(dhcp-config)# dns-server 172.16.1.103 172.16.2.103
```

Ebben az esetben két DNS kiszolgálót használhatnak az ügyfelek, egy elsődlegeset és egy másodlagosat. Legalább egy DNS kiszolgálót be kell állítani az állomások számára, mely feloldja az állomásneveket és URL címeket a hálózat szolgáltatásainak eléréséhez.

```
Router(dhcp-config) # default-router 172.16.1.100
```

6. lépés: Az alapértelmezett átjáró megadása

A hálózaton található DHCP ügyfelek számára állítsa be az alapértelmezett átjáró címét! Ez tipikusan a forgalomirányító LAN IP-címe. Ez a parancs be fogja állítani az alapértelmezett átjárót a hálózaton található, DHCP-t használó ügyfél eszközök számára. Miután egy DHCP ügyfél elindult, elkezd csomagokat küldeni az elsődleges forgalomirányító felé. A megadott IP-címnek ugyanazon az alhálózaton kell lennie, mint az ügyfeleknek kiosztott címeknek. Egy IP-címre van szükség. Használja ezt a parancsot:

```
Router(dhcp-config) # default-router 172.16.1.100
```

Példánkban a kliensek a forgalomirányító 172.16.1.100 című interfészét használják alapértelmezett átjáróként.

```
Router(dhcp-config) # lease {nap[óra] [perc] | infinite}  
Router(dhcp-config) # end
```

7. lépés: A bérleti időtartam beállítása

A DHCP minden olyan esetben ellátja IP-cím információkkal az állomásokat, amint azokat bekapcsolják vagy csatlakoztatják a hálózatra. Az alapértelmezett időtartam, ameddig egy ügyfél lefoglalhat egy címet, egy nap. Amennyiben egy állomás nem újítja meg címét, a címfoglalás időtartama lejár, és az IP-cím újra kioszthatóvá válik a DHCP szolgáltatáson keresztül. Ha szükséges, meg lehet változtatni a bérleti időt hosszabb időtartamra. Ez az utolsó lépése a DHCP szolgáltatás beállításának egy forgalomirányítón. Az end parancs használatával befejezhető a DHCP konfigurálása és visszatérhet globális konfigurációs módba. Használja ezeket a parancsokat:

```
Router(dhcp-config) # lease {nap[óra] [perc] | infinite}  
Router(dhcp-config) # end
```

```
Router# show running-config
```

8. lépés: A konfiguráció ellenőrzése.

Az aktív konfiguráció megtekintésével ellenőrizze le a DHCP konfigurációt. Ehhez használja a következő parancsot:

```
Router# show running-config
```

Az alábbiakban egy DHCP-t futtató forgalomirányító DHCP konfigurációs beállításai láthatóak:

```
!  
ip dhcp pool LAN-címek  
domain-name cisco.com  
network 172.16.0.0 255.255.0.0  
ip dhcp excluded-address 172.16.1.100  
dns-server 172.16.1.103 172.16.2.103  
default-router 172.16.1.100  
lease infinite  
!
```

Amennyiben a konfiguráció helyesnek bizonyult, másolja át az aktív konfigurációt az indító konfigurációs fájlba.

5.3.8 Statikus NAT beállítása a Cisco IOS parancssoros felületén

A NAT lehetővé teszi a belső privát címmel rendelkező állomások számára az internetes kommunikációt. A NAT beállításakor legalább az egyik interfészt belső interfészként kell konfigurálni. A belső interfész csatlakozik a belső, magáncélú hálózathoz. Egy másik – általában a külső, internethez kapcsolódó – interfészt külső interfészként kell beállítani. Amikor a belső hálózat eszközei a külső interfészen keresztül kifelé kommunikálnak, a belső címeket egy vagy több bejegyzett (publikus) IP-címre kell lefordítani.

Előfordulhat, hogy a belső hálózat egyik kiszolgálójának az internetről elérhetőnek kell lennie. Ehhez a kiszolgálónak a külső felhasználók számára ismert, publikus címmel kell rendelkeznie. A statikus címfordítás az egyik módja annak, hogy ilyen címet biztosítsunk a belső kiszolgáló számára.

A statikus NAT biztosítja, hogy a belső hálózat állomásaihoz rendelt címek mindig ugyanarra a bejegyzett (publikus) IP-címre legyenek lefordítva.

A NAT és a statikus NAT beállítása a Cisco IOS parancssoros felületéről számos lépésből áll:

- 1. lépés:** A belső interfész megadása
- 2. lépés:** A belső interfész elsődleges IP-címének beállítása
- 3. lépés:** A belső interfész azonosítása az ip nat inside paranccsal
- 4. lépés:** A külső interfész megadása
- 5. lépés:** A külső interfész elsődleges IP-címének megadása
- 6. lépés:** A külső interfész azonosítása az ip nat outside paranccsal
- 7. lépés:** A statikus címfordítás megadása
- 8. lépés:** A beállítások ellenőrzése

```
Router(config)# interface fastethernet 0/0
```

1. lépés: A belső interfész megadása

Cisco forgalomirányítón a NAT szolgáltatás beállításához először lépjen be privilegizált EXEC módba, kérésre adja meg az ehhez szükséges jelszót, majd váltson át globális konfigurációs módba! Adja meg, mely interfész csatlakozik belülről a helyi hálózathoz! Ezzel automatikusan interfész konfigurációs módba kerül. Használja ezeket a parancsokat:

```
Router> enable
Router# configure terminal
```

```
Router(config)# interface fastethernet 0/0
```

```
Router(config-if)# ip address 172.31.232.182 255.255.255.0
```

2. lépés: A belső interfész elsődleges IP-címének beállítása

Az alábbi parancs segítségével beállíthatja a belső interfész elsődleges IP-címét:

```
Router(config-if)# ip address 172.31.232.182 255.255.255.0
```

```
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit
```

3. lépés: A belső interfész azonosítása az ip nat inside paranccsal

Azonosítsa a belső hálózathoz csatlakoztatott interfészt, majd interfész-konfigurációs módból lépjen vissza globális konfigurációs módba! Használja ezeket a parancsokat:

```
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit
```



```
Router(config)# interface serial 0/0
```

4. lépés: A külső interfész megadása

Állítsa be a külső interfészt! Válassza ki az internetszolgáltatóhoz csatlakozó interfészt, majd lépjen be annak interfész-konfigurációs módjába! Használja ezt a parancsot:

```
Router(config)# interface serial 0/0
```

```
Router(config-if)#ip address 209.165.201.1 255.255.255.252
```

5. lépés: A külső interfész elsődleges IP-címének megadása

Azonosítsa a hálózathoz kívülről csatlakoztatott interfészt, majd interfész-konfigurációs módból lépjen vissza globális konfigurációs módba! Használja ezeket a parancsokat:

```
Router(config-if)#ip address 209.165.201.1 255.255.255.252
```

```
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit
```

6. lépés: A külső interfész azonosítása az ip nat outside paranccsal

Azonosítsa a külső hálózathoz csatlakoztatott interfészt, majd interfész-konfigurációs módból lépjen vissza globális konfigurációs módba! Használja ezeket a parancsokat:

```
Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit
```

```
Router(config)# ip nat inside source static 172.31.232.14 209.165.202.130
Router(config)# exit
```

7. lépés: A statikus címfordítás megadása

Az alábbi paranccsal létrehozható a hálózati címfordítás:

```
Router(config)# ip nat inside source static 172.31.232.14 209.165.202.130
```

Ebben a példában a kiszolgáló belső címe (172.31.232.14) mindig átfordításra kerül a külső címre (209.165.202.130). Használja ezt a parancsot a címfordításhoz! Ha végzett, lépjen ki globális konfigurációs módból!

```
show running-config
```

8. lépés: A beállítások ellenőrzése

Ellenőrizze a statikus NAT konfigurációt! Használja ezt a parancsot:

```
show running-config
```

Következzen egy példa:

```
!
interface fastethernet 0/0
ip address 172.31.232.182 255.255.255.0
ip nat inside
!
interface serial 0/0
ip address 209.165.201.1 255.255.255.252
ip nat outside
ip nat inside source static 172.31.232.14 209.165.202.130
```

Ne felejtse el az aktív konfiguráció tartalmát elmenteni az indító konfigurációs fájlba!

A NAT működés ellenőrzéséhez és hibaelhárításához számos CLI parancs áll rendelkezésre.

Az egyik leghasznosabb parancs a *show ip nat translations*, amely a NAT hozzárendelések részleteit jeleníti meg. A parancs megjelenít minden beállított statikus és a forgalom által generált dinamikus fordítást. Minden címfordításnál szerepel a protokoll, valamint a belső és külső lokális, illetve globális cím.

A *show ip nat statistics* parancs megjeleníti az aktív címfordítások teljes számát, a NAT konfiguráció paramétereit, valamint a címkészlet kiosztható és kiosztott elemeinek számát.

A fentiekén túl a *show run* parancs segítségével is megtekinthetők a NAT beállítások.

Alapértelmezés szerint a dinamikus NAT címfordítási bejegyzései 24 óra elteltével évülnek el, de esetenként ennél hamarabb is érdemes lehet törölni azokat. Ez különösen igaz lehet a NAT beállítások ellenőrzésénél. A dinamikus bejegyzések elévülés előtti törléséhez használjuk a privilegizált (enable) módban kiadott *clear ip nat translation ** parancsot! Ez kizárólag a dinamikus címfordításokat távolítja el a táblázatból, a statikus címfordítások nem törölhetők a címfordítási táblázatból.

```
R1# show ip nat translations
Pro   Inside global      Inside local      Outside local      Outside global
---   -
icmp   209.165.202.130       172.31.232.14     -----
      209.165.202.131:512 172.31.232.1:512  209.165.200.1:512 209.165.200.1:512
udp    209.165.202.131:1067 172.31.232.2:1067 209.165.200.2:53   209.165.200.2:53
tcp    209.165.202.131:1028 172.31.232.2:1028 209.165.200.3:80   209.165.200.3:80

R1# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial 0/0/0
Inside interfaces:
  FastEthernet 0/0
Hits: 47 Misses: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pub-addr refcount 4
  pool pub-addr: netmask 255.255.255.0
    start 209.165.202.131 end 209.165.202.140
    type generic, total addresses 10, allocated 2 (20%), misses 0
Queued Packets: 0
```

5.3.9 A Cisco forgalomirányítók konfigurációjának biztonsági mentése

A forgalomirányító beállítását követően az aktív konfigurációt el kell menteni az indító konfigurációs fájlba. Szintén hasznos a konfigurációs fájl másik helyre (pl. egy hálózati kiszolgálóra) történő mentése. Így a rendelkezésünkre áll egy másolat, ha az NVRAM meghibásodik vagy megsérül, és a forgalomirányító nem tudja betölteni az indító konfigurációs fájlt. A konfigurációs fájl elmentésének számos módja van.

Ezek egyike, hogy a konfigurációs fájlokat TFTP használatával egy hálózati kiszolgálóra mentjük. A TFTP-kiszolgálónak elérhetőnek kell lennie a hálózaton keresztül a forgalomirányító számára.

1. lépés: A *copy startup-config tftp* parancs kiadása

2. lépés: A konfigurációs fájl tárolását végző állomás (TFTP-kiszolgáló) IP-címének megadása

3. lépés: A konfigurációs fájlhoz hozzárendelni kívánt név megadása, vagy az alapértelmezés szerinti elfogadása

4. lépés: Az egyes választások jóváhagyása a "Yes" beírásával

Az aktív konfiguráció szintén eltárolható egy TFTP-kiszolgálón a *copy running-config tftp* parancs kiadásával.

A konfigurációs fájl biztonsági mentésének visszaállításához a forgalomirányítónak rendelkeznie kell legalább egy beállított interfésszel, amin keresztül képes elérni a TFTP-kiszolgálót.

1. lépés: A *copy tftp running-config* parancs kiadása

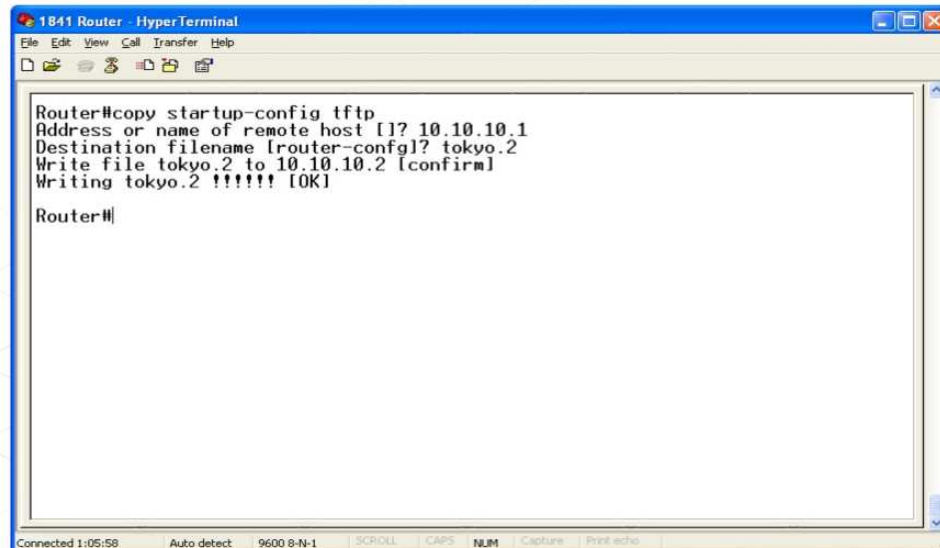
2. lépés: A TFTP-kiszolgálót futtató távoli állomás IP-címének megadása

3. lépés: A konfigurációs fájl nevének megadása, vagy az alapértelmezés szerinti elfogadása

4. lépés: A konfigurációs fájl nevének, valamint a TFTP-kiszolgáló IP-címének jóváhagyása

5. lépés: Az aktív konfiguráció mentése az indító konfigurációs fájlba a *copy run start* parancs segítségével, hogy a visszaállított konfiguráció megmaradjon

A visszaállítás egy lehetséges módja, ha a TFTP-fájl tartalmát az indító konfigurációs fájlba másoljuk. Ekkor azonban az új indító konfigurációs fájl betöltéséhez szükség van a forgalomirányító újraindítására.

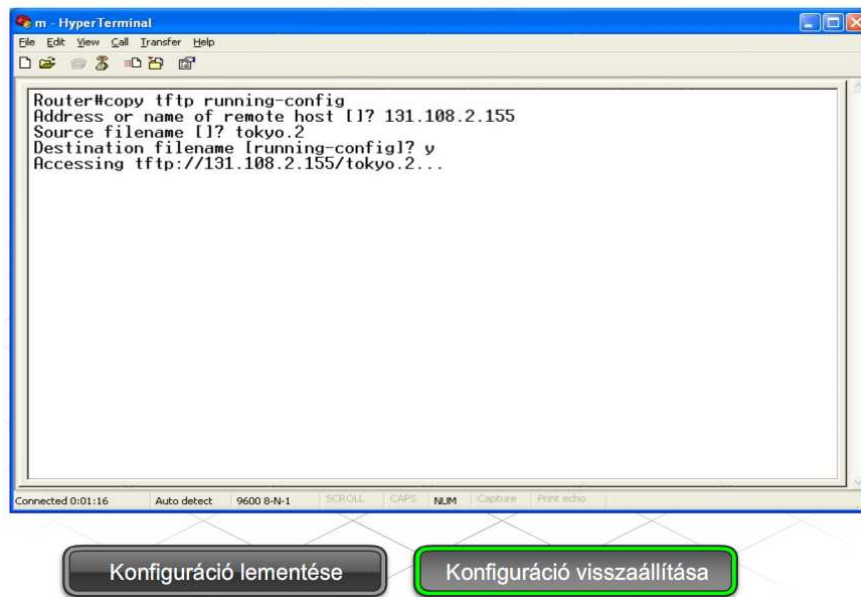


```
Router#copy startup-config tftp
Address or name of remote host [1]? 10.10.10.1
Destination filename [router-config]? tokyo.2
Write file tokyo.2 to 10.10.10.2 [confirm]
Writing tokyo.2 !!!!! [OK]

Router#
```

Konfiguráció lementése

Konfiguráció visszaállítása



A biztonsági másolat készítésének egy másik módja a `show running-config` parancs képernyőkimenetének rögzítése. Terminálkapcsolat esetén másoljuk ki a képernyőkimenetet (a vágólapra), majd illesszük be egy szövegfájlba, végül mentjük el a szövegfájl!

A konfiguráció rögzítése a HyperTerminal képernyőjéről az alábbi lépésekből áll:

1. lépés: A **Transfer (Átvitel)** menü kiválasztása
2. lépés: A **Capture Text (Szöveg rögzítése)** menüpont kiválasztása
3. lépés: A rögzített konfigurációt tároló szövegfájl nevének megadása
4. lépés: A **Start** lehetőség kiválasztása a rögzítés elindításához
5. lépés: A `show running-config` kiadása a konfiguráció képernyőn történő megjelenítéséhez
6. lépés: A szóköz billentyű lenyomása minden, a képernyő alján megjelenő "-More-" felirat esetén

A teljes konfiguráció megjelenítését követően az alábbi lépésekkel leállítható a rögzítés:

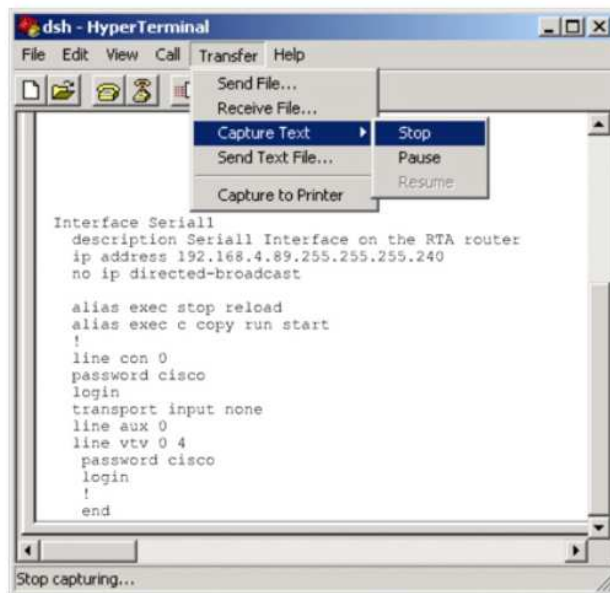
1. lépés: A **Transfer (Átvitel)** menü kiválasztása
2. lépés: A **Capture Text (Szöveg rögzítése)** menüpont kiválasztása
3. lépés: A **Stop** lehetőség kiválasztása

A rögzítés befejezését követően a konfigurációs fájl szerkesztésével el kell távolítani a felesleges szövegrészeket (pl.: building configuration). Ezen felül minden interfészkonfigurációs rész végére oda kell tennünk a `no shutdown` parancsot! Kattintsunk a **File (Fájl) > Save (Mentés)** menüpontra a konfiguráció mentéséhez! A konfigurációs fájlt szövegszerkesztővel, például a Jegyzettömbbel lehet szerkeszteni.

A konfiguráció biztonsági másolata HyperTerminal-kapcsolat során állítható vissza. A konfiguráció visszaállítása előtt minden más konfigurációt el kell távolítani a privilegizált EXEC módban kiadott *erase startup-config* parancs segítségével! Ezután indítsuk újra a forgalomirányítót a *reload* paranccsal!

A konfiguráció biztonsági mentését az alábbi lépésekkel lehet a forgalomirányítóra másolni:

- 1. lépés:** Belépés a globális konfigurációs módba
- 2. lépés:** A HyperTerminal **Transfer (átvitel) > Send Text File (Szövegfájl küldése)** lehetőségének kiválasztása
- 3. lépés:** A konfiguráció biztonsági mentését tartalmazó fájl nevének kiválasztása
- 4. lépés:** Az indító konfiguráció visszaállítása a *copy run start* paranccsal



5.4 A CPE csatlakoztatása az ISP-hez

5.4.1 A CPE telepítése

A helyszíni támogatást végző szakember egyik legfontosabb feladata az ügyfél otthonában vagy egy vállalatnál található berendezések telepítése és fejlesztése. Az ügyfélnél telepített hálózati eszközöket előfizetői végberendezésnek (customer premises equipment, CPE) nevezzük, és ide értjük a forgalomirányítókat, modemeket, kapcsolókat és egyéb hasonló eszközöket.

A forgalomirányító telepítése vagy karbantartása komoly fennakadást okozhat egy vállalkozás működésében. Számos vállalat számára nélkülözhetetlen az internet a levelezéshez, és a cég által nyújtott e-kereskedelmi szolgáltatásnak is elérhetőnek kell lennie a nap folyamán. Ezért a megfelelő működés biztosításához kulcsfontosságú a telepítések és fejlesztések gondos megtervezése. A tervezés lehetővé teszi, hogy végiggondoljuk a lehetőségeket még a papíron, ahol könnyű és olcsó a hibák javítása.

A tervek elkészítéséhez az ISP technikai személyzete rendszerint találkozik a vállalati ügyfelekkel. A megbeszélések alkalmával a technikus meghatározza a forgalomirányítón az ügyfél igényeinek megfelelő beállításokat, valamint az új telepítéshez vagy fejlesztéshez szükséges hálózati szoftvert.

A technikus az ügyfél informatikai személyzetével együtt dolgozza ki a forgalomirányítón használni kívánt beállításokat, valamint a konfiguráció ellenőrzésének menetét. A fenti információk alapján a technikus összeállít egy ellenőrzőlistát.

Az ellenőrzőlista a leggyakrabban konfigurált összetevőket sorolja fel, rövid magyarázattal mindegyik elemhez és beállításhoz. A lista kiváló eszköz az újonnan beüzemelt forgalomirányítók konfigurációjának ellenőrzéséhez, de az előzőleg beállított forgalomirányítók hibaelhárításánál is hasznos lehet.

A konfigurációs ellenőrzőlista számos különböző formában létezhet. Ezek némelyike egészen összetett. Az internetszolgáltatónak meg kell bizonyosodni arról, hogy a helyszíni támogatást végző technikusok rendelkeznek ilyen ellenőrzőlistával, és használni is tudják azt.

Amikor új berendezésre van szükség, az eszközöket általában már az ISP telephelyén beállítják és tesztelik, még az ügyfélnél történő tényleges beüzemelést megelőzően. Bármilyen, ami nem az elvárt módon működik, azonnal kicserélhető vagy javítható. A beüzemelés előtt álló forgalomirányító esetében a hálózati technikusnak meg kell bizonyosodnia arról, hogy az eszköz konfigurációja teljes és ellenőrzött.

Amennyiben a forgalomirányítót megfelelően konfiguráltuk, össze kell készítenünk a hálózati és tápkábeleket, a gyártói dokumentációt, a gyári szoftvereket, a beállítási dokumentációt, valamint a forgalomirányító beüzemeléséhez szükséges speciális szerszámokat! Egy leltár-ellenőrzőlista segítségével megbizonyosodhatunk arról, hogy a forgalomirányító beüzemeléséhez szükséges minden eszköz megvan. Az ellenőrzőlistát a hálózati technikus írja alá, amennyiben mindent rendben talált. A dátummal és aláírással ellátott ellenőrzőlista az ügyfél telephelyére szállítandó csomagba kerül, a forgalomirányító mellé.

A csomag megérkezését követően a helyszíni támogató technikus megkezdheti a forgalomirányító telepítését. Fontos, hogy ez olyan időpontban történjen, amikor ez a lehető legkevesebb zavart

okozza. Előfordulhat, hogy a hálózati eszközök telepítése vagy fejlesztése csak a normál munkaidőn kívül lehetséges. Amennyiben a telepítés a hálózat leállításával jár, a hálózati technikus, az ISP értékesítője és a vállalat képviselője együtt készíti el a forgalomirányító üzembe helyezésének tervét. Ez biztosítja, hogy az ügyfél a lehető legkevesebb zavart érezhes a szolgáltatásban az eszköz telepítése során. A forgalomirányító üzembehelyezési terve ezen felül tartalmazza az ügyfél által kijelölt kapcsolattartó személy nevét, valamint a munkaterületre a munkaidő után történő bejutás részleteit. Az üzembehelyezési terv részét képezi a telepítési ellenőrzőlista elkészítése, amellyel megbizonyosodhatunk arról, hogy a berendezés üzembehelyezése megfelelően zajlott.

A helyszíni támogató technikusnak mindig az üzembehelyezési terv és a telepítési ellenőrzőlista alapján kell a forgalomirányítót beüzemelnie az ügyfélnél. Az előfizetői végberendezések telepítésénél fontos, hogy mindig professzionális módon végezzük el a munkát! Ez azt jelenti, hogy a kábeleket címkézzük fel, rögzítsük egymáshoz vagy bújtassuk kábelvezetőbe! A felesleges kábelszakaszokat csavarjuk fel, hogy ne akadályozzák a közlekedést!

A dokumentációba vegyük bele a forgalomirányító jelenlegi konfigurációját, a hálózati rajzon pedig jelöljük be az új berendezés és a hozzá tartozó kábelek helyét!

A forgalomirányító sikeres beüzemelését és tesztelését követően a hálózati technikus kitölti a telepítési ellenőrzőlistát, amelyet az ügyfél képviselője ellenőriz. A telepített forgalomirányító ellenőrzése gyakran magában foglal egy bemutatót, ami bizonyítja, hogy az eszközön megfelelőek a beállítások és a forgalomirányítótól függő szolgáltatások az elvárt módon működnek.

Amennyiben az ügyfél képviselője elégedett a forgalomirányító telepítésével és működésével, feldátumozza és aláírja az ellenőrzőlistát. Előfordul, hogy az ellenőrzőlistán kívül szükség van egy formális teljesítési igazolásra is. Ezt a folyamatot gyakran lezáró szakasznak is nevezik. Kulcsfontosságú, hogy az ügyfél képviselője lezárja a munkát, mert az ISP csak akkor állíthat ki számlát az elvégzett munkáról.

A telepítési dokumentáció

Amennyiben az előfizetői berendezés beüzemelése és beállítása az ügyfél telephelyén történik, fontos, hogy az egész folyamatot dokumentáljuk! A dokumentációnak tartalmaznia kell a berendezés konfigurációjának minden részletét, a telepítési rajzokat, valamint a kapcsolódó ellenőrzőlistákat. Amennyiben új konfigurációra van szükség, a dokumentációban szereplő előző konfigurációval összehasonlítva megállapíthatjuk, hogy a konfiguráció valóban változott-e, és ha igen, akkor hogyan. A módosítások és az eszközhez való hozzáférés nyomon követéséhez használhatunk tevékenységi naplót. A megfelelően karbantartott tevékenységi napló segít a problémák hibaelhárításában.

A technikus már a forgalomirányító telepítése során elkezdi a dokumentációt. A későbbi azonosítás megkönnyítése érdekében minden kábelt és eszközt megfelelően felcímkéz és megjelöl a hálózati rajzon.

A forgalomirányító beüzemelése során mindig követi a telepítési ellenőrzőlistát, amely tartalmazza az ügyfél telephelyén végrehajtandó feladatokat. Az ellenőrzőlista segít a hibák elkerülésében, és biztosítja az üzembehelyezés hatékony és megfelelő menetét.

A végleges dokumentáció egy példánya az ügyfélnél marad.

5.4.2 WAN-on keresztüli előfizetői kapcsolatok

Az internetszolgáltatás biztosításához az ügyfél telephelyén beüzemelt új berendezést csatlakoztatni kell az ISP-hez. Előfordulhat, hogy az előfizetői végberendezés fejlesztésekor az ISP által biztosított kapcsolattípus is fejlesztésre szorul.

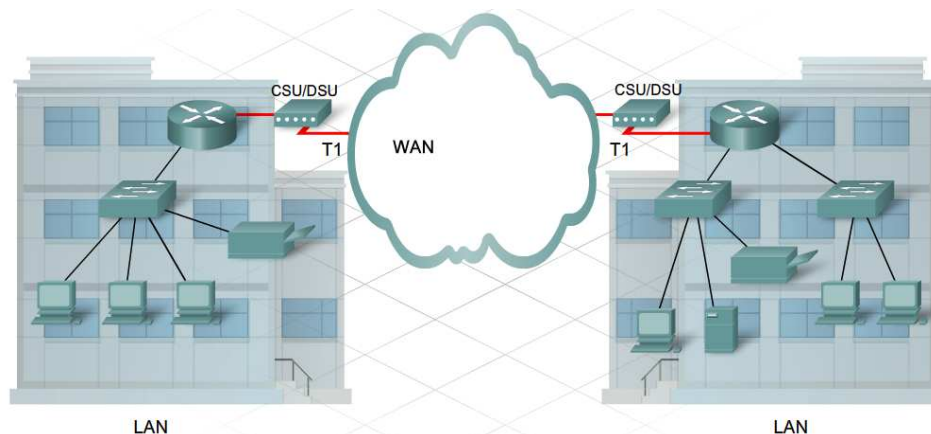
Nagytávolságú hálózatok

Ha egy vállalat több, egymástól földrajzilag távol eső telephellyel rendelkezik, szükség lehet egy távközlési szolgáltató (TSP) bevonására a különböző helyeken lévő LAN-ok összekapcsolásához. Az egymástól földrajzilag távol eső LAN-okat összekapcsoló hálózatokat nagytávolságú hálózatnak (WAN) nevezzük.

A távközlési szolgáltatók hatalmas, nagy területet lefedő regionális hálózatokat működtetnek. A távközlési szolgáltatók a hang- és adatkommunikációt hagyományosan külön hálózaton bonyolították, azonban egyre nagyobb számban kínálnak integrált információs szolgáltatásokat az előfizetők számára.

Az egyes szervezetek általában bérelt kapcsolattal rendelkeznek a TSP hálózatán keresztül. Habár a kapcsolat két végén lévő LAN-ok házirendjét és adminisztrációját teljes mértékben a szervezet felügyeli, a kommunikációs szolgáltatást nyújtó hálózat házirendjét az ISP szabályozza.

Az internetszolgáltatók a WAN-összeköttetések széles skáláját kínálják az ügyfelek számára. A WAN-összeköttetések eltérőek lehetnek a csatlakozó típusától, a sávszélességtől és a költségektől függően. A kisvállalkozások növekedésével egyre nő az igény a drágább WAN-összeköttetések által nyújtott sávszélességre. Az internetszolgáltatók és közép vállalatok egyik feladata, hogy felmérjék a szükséges WAN-összeköttetés típusát.



A soros WAN-összeköttetéseknek három típusa létezik.

Pont-pont

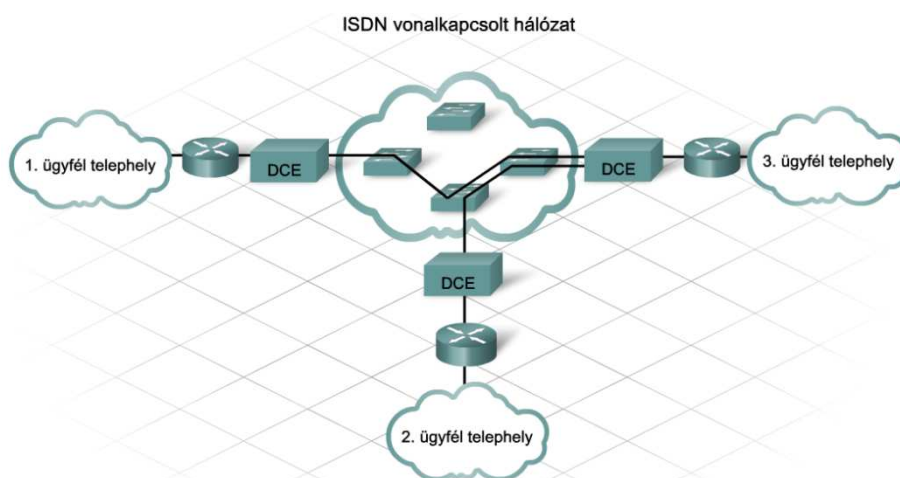
A pont-pont összeköttetés egy előre meghatározott kommunikációs útvonal az ügyfél telephelyétől a TSP hálózatán keresztül. Ez egy fix sávszélességgel rendelkező, állandóan rendelkezésre álló dedikált áramkör. A pont-pont összeköttetéseket általában a távközlési szolgáltatótól bérlik, ezért gyakran bérelt vonalnak is nevezik őket. A pont-pont összeköttetés általában a legdrágább WAN-

kapcsolattípus, melynek ára az igényelt sávszélesség és a két összekötött pont közötti távolság függvénye. A pont-pont típusú WAN-összeköttetésre példa a T1 és az E1 kapcsolat.



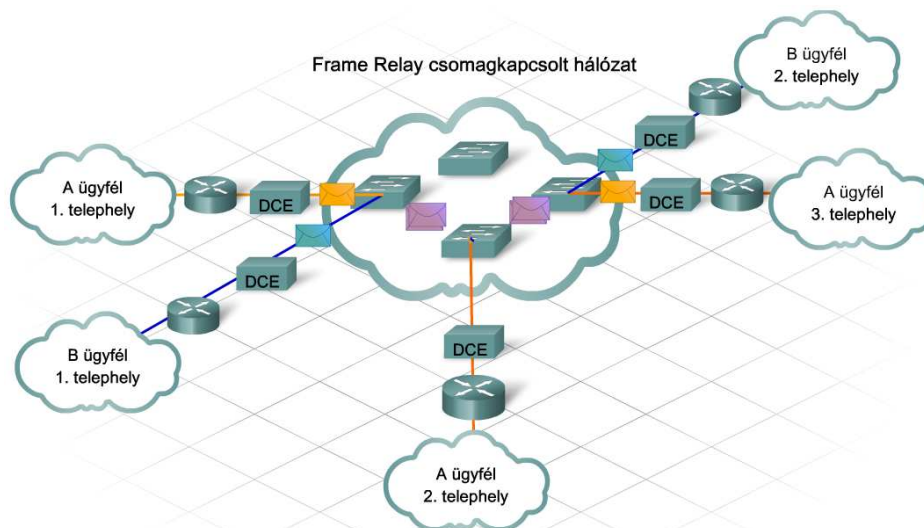
Vonalkapcsolt

A vonalkapcsolt összeköttetés a telefonhálózaton keresztül bonyolított telefonhíváshoz hasonló elven működik. Amikor felhívunk egy ismerőst, felemeljük a kagylót, létrehozuk az áramkört, majd tárcsázzuk a számot. A hívás befejezését követően lerakjuk a kagylót és lezárjuk az áramkört. A vonalkapcsolt WAN-összeköttetésre példa az ISDN és a betárcsázós kapcsolat.



Csomagkapcsolt

A csomagkapcsolt összeköttetésben minden hálózat a számos előfizető által közösen használt TSP hálózatba kapcsolódik. A vonalkapcsolt áramkör forrástól célig történő fizikai lefoglalása helyett, itt mindegyik előfizető saját virtuális áramkörrel rendelkezik. A virtuális áramkör egy, a küldő és a fogadó felet összekötő logikai – nem pedig fizikai – útvonal. A csomagkapcsolt hálózatra példa a Frame Relay.



5.4.3 A WAN-összeköttetés kiválasztása

A WAN-összeköttetés kiválasztásánál fontos szerepet játszik a sávszélesség és az ár. A kisebb vállalatok nem engedhetik meg a drágább (pl.: SONET vagy ATM típusú) WAN-összeköttetéseket, inkább a kevésbé drága DSL, kábeles vagy T1 típusú összeköttetéseket választják. Ezen felül a nagyobb sávszélességű WAN-összeköttetések nem biztos, hogy elérhetőek a földrajzilag távol eső helyeken. Amennyiben az irodák a városközpontokhoz közel esnek, több lehetőség áll rendelkezésre a WAN-kapcsolat kiválasztásánál.

A választásnál az is szerepet játszik, hogy a vállalat mire kívánja használni az összeköttetést. Amennyiben a vállalat interneten keresztül elérhető szolgáltatásokat nyújt, magasabb feltöltési sávszélességre lehet szüksége. Ilyen eset lehet például egy e-kereskedelmi szolgáltatásokat nyújtó webkiszolgáló üzemeltetése, amelynek elegendő feltöltési sávszélességet kell biztosítani a webhelyre látogató külső ügyfelek kiszolgálásához. Ugyanakkor, ha a vállalat e-kereskedelmi szolgáltatásokat nyújtó weboldalát az internetszolgáltató kezeli, nincs szükség túl nagy feltöltési sávszélességre.

Néhány vállalat döntésében az is szerepet játszik, hogy a WAN-összeköttetéshez tartozik-e a szolgáltatási szintet garantáló szerződés (SLA). A kevésbé drága (pl.: betárcsázós, DSL és kábeles) WAN-összeköttetésekhez általában nem tartozik ilyen szerződés, míg a drágábbakhoz igen.

Összeköttetés	Sávszélesség	Költségek
Betárcsázós elérés	56 Kbit/s-ig	Alacsony
Frame Relay	128 - 512 Kbit/s	Alacsony - Közepes
DSL	128 Kbit/s - 6+ Mbit/s ¹	Alacsony
Kábel	128 Kbit/s - 10+ Mbit/s ¹	Alacsony
Fractional T1	64 Kbit/sec - 1.544 Mbit/s	Alacsony - Közepes
T1/E1	1.544/2.048 Mbit/s	Átviteli közeg
Fractional T3	1.544 Mbit/s - 44.736 Mbit/s	Közepes - Magas
T3/E3	44.736/34.368 Mbit/s	Magas
SONET	51.840 Mbit/s - 9953.280 Mbit/s	Magas - Nagyon magas
ATM	622 Mbit/s	Nagyon magas

Ez a lista csak egy kis részhalmazát képezi az ISP-k és a telekommunikációs szolgáltatók által kínált lehetőségeknek.

Az elérhetőség függ a szolgáltatótól és a földrajzi elhelyezkedéstől.

¹A feltöltési sávszélesség jellemzően kisebb, mint a felsorolt letöltési sebesség.

A WAN továbbfejlesztésének tervezésekor számos szempontot kell figyelembe venni. Az internetszolgáltató az előfizetői igények elemzésével és a rendelkezésre álló lehetőségek áttekintésével indítja el a folyamatot. Ezután egy javaslatot dolgoz ki az ügyfél számára, amely tartalmazza a meglévő infrastruktúra leírását, az előfizetői igényeket és a szóba jöhető WAN lehetőségeket.

Meglévő infrastruktúra

Ez a vállalat által használt jelenlegi infrastruktúra leírása, amely segít a felhasználónak megérteni, hogy a meglévő WAN-összeköttetés miként nyújt szolgáltatásokat az otthona vagy a vállalata számára.

Előfizetői igények

A javaslat ezen része a WAN továbbfejlesztés szükségességének okait részletezi az ügyfél számára, valamint röviden felvázolja, hogy a jelenlegi WAN-összeköttetés hol nem felel meg az előfizetői igényeknek. Ezen felül tartalmazza az új WAN-összeköttetéssel szemben támasztott jelenlegi és jövőbeli elvárások listáját is.

WAN lehetőségek

Ez a választható WAN-kapcsolattípusok listája, a vonatkozó sávszélességgel, költségekkel és egyéb, a vállalat szempontjából lényeges paraméterekkel. A teljes listában az internetszolgáltató megjelöli az általa legmegfelelőbbnek tartott kapcsolattípust.

Ezután következik a WAN továbbfejlesztési javaslat bemutatása a vállalat döntéshozóinak, akik áttanulmányozzák a dokumentumot, és mérlegelik a lehetőségeket. Miután megszületett a döntés, az internetszolgáltató az ügyféllel együttműködve tervezi meg és koordinálja a WAN továbbfejlesztésének menetét.

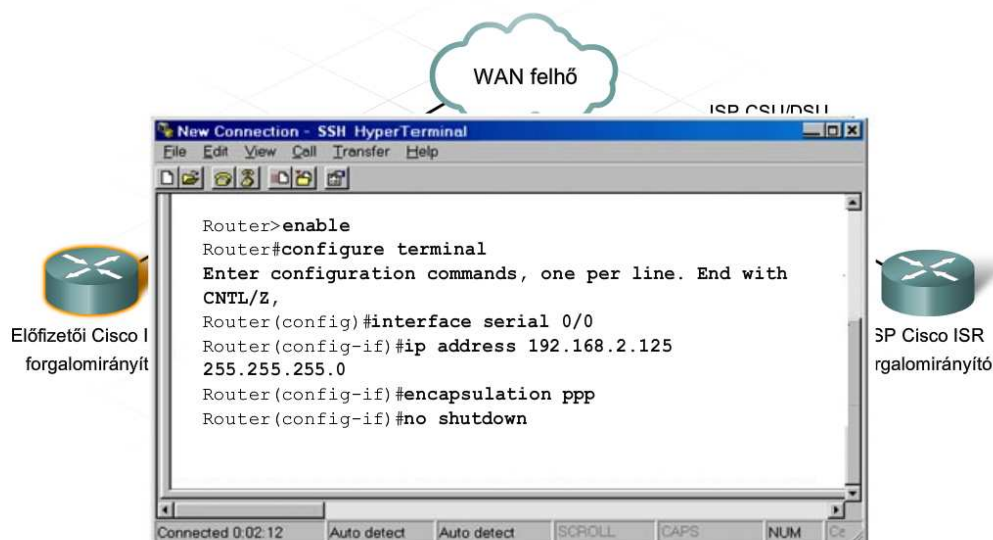
5.4.4 A WAN-összeköttetés beállítása

A WAN beállításának módja az igényelt WAN-összeköttetés típusától függ. Egyes WAN-összeköttetések az Ethernet interfészeket, mások pedig a soros interfészeket támogatják.

A bérelt vonalas WAN-kapcsolatok általában soros összeköttetést használnak, és szükségük van egy csatornaszolgáltató/adatszolgáltató egységre (CSU/DSU) az internetszolgáltató hálózatához történő kapcsolódáshoz. Az internetszolgáltató berendezését úgy kell beállítani, hogy a CSU/DSU-n keresztül kommunikálni lehessen az ügyfél telephelyén levő végberendezésekkel.

A soros összeköttetés szempontjából fontos, hogy a kapcsolat mindkét végén ugyanaz az órajelet legyen előre beállítva. Az órajelet általában a DCE berendezés (általában a CSU/DSU egység) állítja be, a DTE berendezés (általában a forgalomirányító) pedig fogadja.

A Cisco készülékek a soros vonalakon alapértelmezés szerint HDLC beágyazást alkalmaznak, de ez megváltoztatható PPP-re. A PPP nagyobb rugalmasságot nyújt, valamint támogatja a távoli berendezés általi hitelesítést.



5.5 A Cisco 2960 kapcsoló első konfigurálása

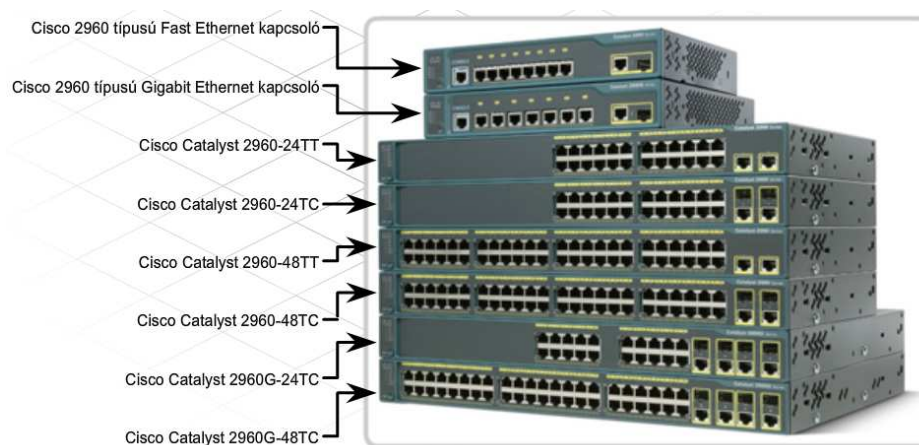
5.5.1 Önálló kapcsolók

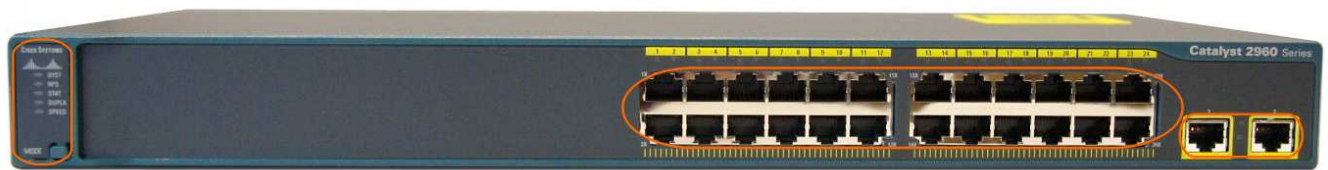
Habár az 1841-es típusú ISR integrált kapcsolómodulja alkalmas néhány állomás LAN-hoz történő csatlakoztatására, a hálózat növekedésével járó további felhasználók kiszolgálásához szükség lehet nagyobb, fejlettebb funkciókkal rendelkező kapcsolókra is.

A kapcsoló egy olyan eszköz, amely az egyik portján beérkező üzenetfolyamot egy másik portjára irányítja a célszámítógép MAC-címe alapján. A kapcsoló nem képes a két különböző helyi hálózat között zajló forgalom irányítására. A kapcsoló az OSI-modell második rétegében működik. A második réteg az adatkapcsolati réteg.

Az Ethernet kapcsolók számos, a különböző felhasználói igényekhez igazodó modellje kapható. A Cisco Catalyst 2960 típusú Ethernet kapcsolót a közepes méretű vállalatok és fiókirodák hálózataihoz tervezték.

A Catalyst 2960-as sorozat tagjai fix kiépítéssel rendelkező önálló kapcsolók, amelyek nem támogatják a külső modulok és flash kártyák használatát. Mivel a fix kiépítéssel rendelkező kapcsoló fizikai konfigurációja nem változtatható meg, mindig a szükséges számú és típusú port alapján kell kiválasztani. A 2960 sorozatú kapcsolók Fast Ethernet (10/100) és Gigabit Ethernet (10/100/1000) csatlakozást egyaránt biztosítanak. A fenti kapcsolók a Cisco IOS szoftvert használják, és a grafikus felületű Cisco Network Assistant (Hálózati Segéd) vagy a parancssoros felület használatával állíthatók be.





A Cisco Catalyst 2960 sorozatú intelligens Ethernet kapcsolók kis és közepes méretű hálózatok számára készültek. Támogatják a 10/100 sebességű Fast Ethernet és a 10/100/1000-es Gigabit Ethernet LAN kapcsolódást.

Állapotjelző LED-ek

SYST LED:

Visszajelzi, hogy a rendszer tápfeszültség alatt van és megfelelően működik.

- Zöld: Megfelelően működik a rendszer.
- Borostyán sárga: A rendszer tápfeszültség alatt van, de nem működik megfelelően.

RPS LED:

A redundáns rendszerű tápellátás (RPS) visszajelző LED, az RPS rendszer állapotáról tájékoztat.

- Zöld: Az RPS csatlakoztatva van és készen áll tartalék tápfeszültség biztosítására, amennyiben szükség van rá.
- Villogó zöld: Az RPS csatlakoztatva van, de nem elérhető, mivel más eszköz számára biztosít tápfeszültséget.
- Borostyán: Az RPS rendszer vagy készenléti állapotban van vagy meghibásodott.
- Villogó borostyán sárga: A kapcsolóban található belső tápegység meghibásodott, az RPS rendszer szolgáltat áramot a készüléknek.

Mode gomb és port-állapot LED-ek:

A port LED-ek információt szolgáltatnak a kapcsolóról és az egyes portokról.

Mode gomb:

A mode gombot a következő port-üzemmódok egyikének kiválasztására használják: állapot mód, duplex mód vagy sebesség mód. Üzem mód kiválasztásához vagy megváltoztatásához nyomja le a Mode gombot, amíg ki nem jelölődik a kívánt mód. A LED rendeltetése a port üzemmód beállításához van rendelve.

Port állapot vagy STAT, az alapértelmezett port mód

- Sötét: Nincs kapcsolat vagy a port adminisztratíván le lett tiltva.
- Zöld: Kapcsolatban van.
- Villogó zöld: A port éppen adatokat küld vagy fogad.



- Váltakozó zöld és sárga: Kapcsolati hiba. Kerethibák befolyásolhatják a kapcsolódást, ezért az olyan hibák bekövetkezése, mint a túl sok ütközés, CRC hibák, illetve az illesztési és az ún. jabber-hibák, folyamatos megfigyelés alatt állnak a kapcsolati hibák jelzése érdekében.
- Borostyán: A port működését blokkolja a Feszítőfa Protokoll (STP), és nem tovább adatokat.
- Villogó borostyán: A portot blokkolja az STP, viszont folytatja a kapcsolók közötti információs üzenetek küldését és fogadását.

Duplex LED:

Port duplex mód vagy DUPLEX, amely lehet duplex vagy fél-duplex.

- Sötét: A port fél-duplex módban üzemel.
- Zöld: A port duplex üzemmódban van.

Speed (Sebesség) LED

Speed mód: A 10/100-as portok, a 10/100/1000-es portok és az SPF modulportok működési sebességeit jelzi vissza.

10/100-as portok esetén:

- Sötét: A port 10 Mbit/s sebességgel üzemel.
- Zöld: A port 100 Mbit/s sebességgel üzemel.

10/100/1000-es portok esetén:

- Sötét: A port 10 Mbit/s sebességgel üzemel.
- Zöld: A port 100 Mbit/s sebességgel üzemel.
- Zölden villogó: A port 1000 Mbit/s sebességgel üzemel.

SFP portok esetén:

- Sötét: A port 10 Mbit/s sebességgel üzemel.
- Zöld: A port 100 Mbit/s sebességgel üzemel.
- Zölden villogó: A port 1000 Mbit/s sebességgel üzemel.

10/100-as és 10/100/1000-es portok:

A 10/100-as Ethernet portok beállíthatóak 10 vagy 100 Mbit/s sebesség támogatására.

A 10/100/1000-es portok képesek 10, 100 vagy 1000 Mbit/s sebességen üzemelni.

SFP portok:

Egy Gbabit sebességre alkalmas Ethernet SFP port használható optikai vagy réz alapú átalakító (transceiver) modulokkal. Az optikai átalakítók támogatják az optikai kábelek használatát. A réz alapú átalakítókkal RJ-45-ös csatlakozóval ellátott, 5-ös kategóriájú kábelek használhatók.

A Gigabit Ethernet SFP portok alkalmazásával lehetőség nyílik az optikai és réz alapú átalakítók könnyű felcserélhetőségére éles használat közben, amennyiben egy kapcsolat felmondaná a szolgálatot.



Minden Ethernet port a 2960-as típusú kapcsoló elején van. A készülék hátoldalán található a tápcsatlakozó, a konzolport és a hűtőventilátor szellőző nyílása.

Konzolport:

RJ-45-DB-9 kábel használatával a porton keresztül a kapcsoló összeköthető egy PC-vel.

Sávon kívüli felügyeleti feladatok elvégzésére használják.

Minden kapcsoló támogatja a fél-duplex és duplex átviteli üzemmódokat.

A fél-duplex módban működő port bármely adott pillanatban csak küldeni, vagy csak fogadni tudja az adatokat (egyszerre mindkettőt nem). A duplex módban működő port egyidejűleg tud adatokat küldeni és fogadni, megduplázva ezzel az áteresztőképességet.

Mind a portnak, mind pedig a csatlakoztatott eszköznek ugyanabban az átviteli üzemmódban kell működnie. Ha mégsem ugyanabban a módban működnek, nagyszámú ütközéssel, romló kommunikációval járó átviteli illesztetlenségi problémával számolhatunk.

A sebesség és a duplex üzemmód beállítható kézzel, de a kapcsoló portja automatikusan is egyeztetetheti azokat. Az automatikus egyeztetés lehetővé teszi a kapcsoló számára, hogy a portjára csatlakoztatott eszköz sebességét és duplex üzemmódját automatikusan detektálja. A legtöbb Cisco kapcsolón az automatikus egyeztetés alapértelmezés szerint engedélyezve van.

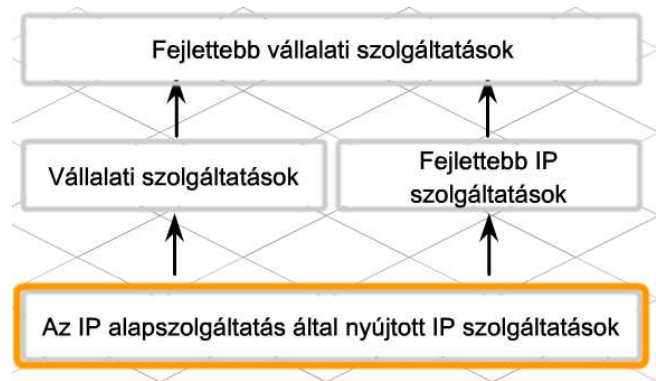
Ahhoz, hogy az automatikus egyeztetés működjön, ezt a funkciót mindkét résztvevőnek támogatnia kell. Amennyiben a kapcsoló automatikus egyeztetési módban van, de a csatlakoztatott eszköz nem támogatja azt, a kapcsoló a másik eszköz sebességét (10, 100 vagy 1000) fogja használni, és fél-duplex módba vált. A fél-duplex módra váltás problémákat okozhat, ha az automatikus egyeztetést nem támogató eszköz duplex módban működik.

Ha a csatlakoztatott eszköz nem támogatja az automatikus egyeztetést, kézzel állítsuk a kapcsoló duplex-beállításait a csatlakoztatott eszköz beállításaihoz megegyezőre! A sebesség-paraméter magától beállítódik, még akkor is, ha a csatlakoztatott port nem támogatja az automatikus egyeztetést.

A kapcsoló beállításai – beleértve a portok sebesség- és duplex-paramétereit – a Cisco IOS parancssoros felületéről is megadhatók. Amikor egy kapcsolót a Cisco IOS parancssoros felületéről

állítunk be, a felület és a parancsok szerkezete rendkívül hasonlít a Cisco forgalomirányítóknál megszokottakra.

Csakúgy, mint a forgalomirányítók esetében, a kapcsolók számára készült Cisco IOS rendszerkódnak is számtalan változata létezik. A Cisco Catalyst 2960 típusú kapcsolót az IP-Base (IP-Alap) rendszerkóddal szállítják, amely az alapvető kapcsolási funkciókat és IP-szolgáltatásokat biztosítja. A többi Cisco IOS rendszerkód az IP-Base szolgáltatásait bővíti.



5.5.2 A Cisco 2960 típusú kapcsoló üzembehelyezése

A Cisco 2960 típusú kapcsoló üzembehelyezése hasonlít a Cisco 1841 típusú ISR elindításához.

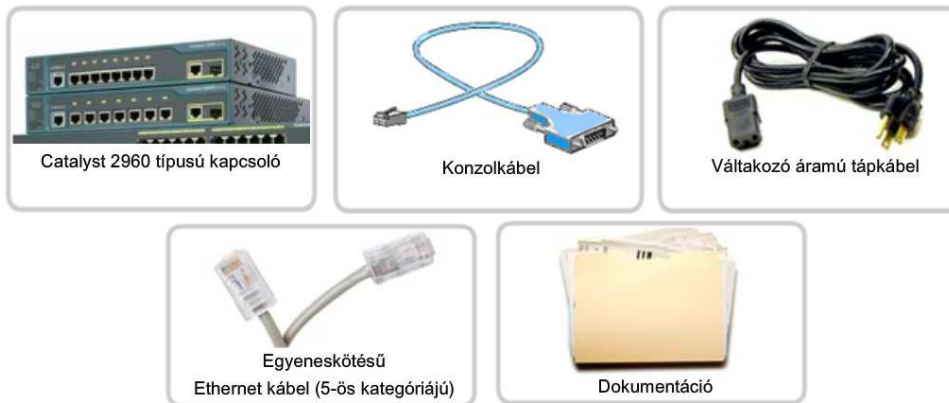
A kapcsoló üzembehelyezése három lépésben történik:

- 1. lépés:** Az összetevők ellenőrzése
- 2. lépés:** A kábelek összekötése a kapcsolóval
- 3. lépés:** A kapcsoló feszültség alá helyezése

Amint a kapcsoló áram alá kerül, elindul a bekapcsolási önteszt (POST). A POST ideje alatt a LED-ek villogása jelzi a kapcsoló megfelelő működését ellenőrző tesztek futását.

A POST sikeres befejezését a SYST LED gyors, zöld színű villogása jelzi. Amennyiben a POST nem volt sikeres, a SYST LED sárgára vált. Ilyenkor a kapcsolót vissza kell küldeni javításra.

Amennyiben minden indítási folyamat sikerrel zárul, megkezdődhet a Cisco 2960 típusú kapcsoló beállítása.



1. lépés - Az összetevők ellenőrzése

Ellenőrizze, hogy minden összetevő rendelkezésre álljon, amely a kapcsolóhoz tartozik! Ezek közé tartozik a konzolkábel, a tápkábel, az Ethernet kábel és a kapcsoló dokumentációja.



2. lépés - A kábelek összekötése a kapcsolóval

Csatlakoztassa a PC-t egy konzolkábel segítségével a kapcsolóhoz, majd indítson el egy terminálemulációs folyamatot. A kapcsoló tápkábelét csatlakoztassa a készülékhez és egy földelt, váltakozó áramú aljzathoz!



3. lépés - A kapcsoló elindítása

Néhány Cisco kapcsoló modell nem rendelkezik bekapcsoló gombbal. A 2960 típusú kapcsoló rögtön azután elindul, hogy a tápfeszültség kábelét energiaforráshoz csatlakoztatta.

5.5.3 A kapcsoló kezdeti konfigurációja

A Cisco LAN kapcsoló konfigurálásának és kezelésének számos módja van.

- A Cisco Network Assistant (Hálózati Segéd)
- A Cisco Device Manager (Eszközkezelő)
- A Cisco IOS parancssoros felülete
- A CiscoView felügyeleti szoftver
- Az SNMP hálózatfelügyeleti termékek

Mivel a fenti módszerek némelyike IP-kapcsolaton keresztül vagy valamilyen webböngésző segítségével használható, ezért a kapcsolónak IP-címre van szüksége. A forgalomirányító interfészeivel ellentétben a kapcsoló portjaihoz nem kell IP-címet rendelni. A Cisco kapcsolók IP-alapú felügyeleti szoftverrel vagy telnet-kapcsolaton keresztül történő kezeléséhez egy felügyeleti IP-cím beállítása szükséges.

Amennyiben a kapcsoló nem rendelkezik IP-címmel, a konfigurációs feladatok végrehajtásához közvetlenül a konzolportjára kell csatlakozni, és terminálemulációs programot kell használni.

Cisco Network Assistant

- PC-alapú hálózatfelügyeleti alkalmazás grafikus felhasználói felülettel (GUI), kis és közepes méretű üzleti LAN hálózatokra optimalizálva.
- Cisco kapcsolók központi felügyelhetőségének lehetőségét nyújtja, felhasználóbarát grafikus felületen keresztül.
- Egy kapcsoló vagy kapcsolók egy csoportjának beállítására és felügyeletére használják.
- Ingyenesen elérhető és letölthető a Cisco webhelyről.

Cisco Device Manager

- A kapcsoló memóriájában tárolt, webböngésző alapú szoftver.
- A webes felület az eszköz gyors konfigurálhatóságát és felügyeletét eredményezi.
- Kapcsolók teljes körű konfigurálásához és felügyeletéhez használható.
- Elérhető webböngészőn keresztül

Cisco IOS CLI

- A Cisco IOS szoftvernek a kapcsolási művelet kezelésére is alkalmas továbbfejlesztett változata.
- A parancssor segítségével a kapcsoló vagy a kapcsolók egy csoportja teljeskörűen konfigurálható és felügyelhető.
- A kapcsoló konzolportjához közvetlenül csatlakozó számítógépen keresztül érhető el, illetve távoli PC-ről telnet segítségével is használható.

CiscoView

- Megjeleníti a kapcsoló képét a konfigurációs paraméterek beállításához, valamint kijelzi a kapcsoló állapotára és teljesítményére vonatkozó információkat.
- Külön megvásárolható, használható kizárólagosan, vagy képezheti egy egyszerű hálózatfelügyeleti protokoll (SNMP) alapú rendszer részét.

Egyszerű hálózatfelügyeleti protokoll (SNMP)

- SNMP-kompatibilis felügyeleti állomásról kezelhető.
- SNMP-kompatibilis felügyeleti állomások például a HP OpenView vagy a SunNet Manager rendszerek.
- Jellemzően nagyméretű vállalatoknál használják.



A Cisco 2960 típusú kapcsoló előre konfigurálva érkezik, a hálózatra történő csatlakoztatás előtt csupán az alapvető biztonsági beállításokat kell megadni.

Az állomásnév és a jelszavak beállítása ugyanazokkal a parancsokkal történik, mint az ISR esetében. A Cisco kapcsolók IP-alapú felügyeleti szoftverrel vagy telnet-kapcsolaton keresztül történő kezeléséhez állítsunk be egy felügyeleti IP-címet!

Ahhoz, hogy egy IP-cím a kapcsolóhoz társítható legyen, a címet egy virtuális helyi hálózati (VLAN) interfészhez kell rendelnünk. A VLAN lehetővé teszi egyenél több fizikai port egyetlen logikai csoportként történő kezelését. A kapcsolón egy VLAN van előre konfigurálva, a felügyeleti feladatokat ellátó VLAN1.

A VLAN1 felügyeleti interfészéhez tartozó IP-cím beállításához lépünk be a globális konfigurációs módba!

```
Switch>enable
```

```
Switch#configure terminal
```

Ezután lépünk be a VLAN1 interfészkonfigurációs módjába!

```
Switch(config)#interface vlan 1
```

Adjuk meg a felügyeleti interfész IP-címét, alhálózati maszkját és alapértelmezett átjáróját! Az IP-címnek érvényesnek kell lennie a kapcsolót tartalmazó helyi hálózatban!

```
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
```

```
Switch(config-if)#exit
```

```
Switch(config)#ip default-gateway 192.168.1.1
```

```
Switch(config)#end
```

Mentsük el a beállításokat a *copy running-configuration startup-configuration* paranccsal!

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.1
Switch(config)#end
Switch#copy running-config startup-config
```

5.5.4 A LAN kapcsoló összekötése a forgalomirányítóval

A kapcsoló forgalomirányítóval történő összekötéséhez használjunk egyenes kötésű kábelt! A sikeres összeköttetést a két eszközön látható LED-ek jelzik.

A kapcsoló és a forgalomirányító összekötését követően ellenőrizzük, hogy a két eszköz tud-e üzenetet váltani egymással!

Először ellenőrizzük az IP-beállításokat! A `show running-configuration` parancs segítségével ellenőrizzük, hogy a kapcsoló VLAN1 felügyeleti portjához tartozó IP-cím és a közvetlenül csatlakoztatott forgalomirányító interfészehez tartozó IP-cím egyazon helyi hálózaton szerepel-e!

Ezután teszteljük az összeköttetést a `ping` parancs használatával! A kapcsolóról pingeljük meg a közvetlenül csatlakoztatott forgalomirányító interfészehez tartozó IP-címet! Ezután a forgalomirányítóról pingeljük meg a kapcsoló VLAN1 felügyeleti interfészehez tartozó IP-címet!

Ha a pingelés nem jár sikerrel, akkor ellenőrizzük újra az összeköttetést és a beállításokat! Bizonyosodjunk meg arról, hogy megfelelő kábelt használtunk, és a csatlakozóknál nincs-e illeszkedési probléma!

Miután a kapcsoló és a forgalomirányító megfelelően kommunikál egymással, egyenes kötésű kábel segítségével önálló PC-k is csatlakoztathatók a kapcsolóhoz. A kábel közvetlenül összekötheti a PC-t a kapcsolóval, de a strukturált kábelezés részeként vezethet egy fali aljzathoz is.

A kapcsoló portjai belépési pontként szolgálhatnak a hálózatba az illetéktelen felhasználók számára. Ennek megakadályozásához a kapcsolók a portbiztonság elnevezésű megoldást alkalmazzák. A portbiztonság portonként korlátozza az engedélyezett, érvényes MAC-címek számát. Az egyes portok nem továbbítják azokat a csomagokat, amelyeknél a forrás MAC-címe nincs az engedélyezett címek csoportjában.

A portbiztonság beállításának három módja van:

Statikus

A MAC-címek megadása manuálisan történik a `switchport port-security mac-address <mac-cím>` parancs segítségével. A statikus MAC-címeket a címtábla és az aktív konfiguráció is tárolja.

Cisco IOS CLI parancsok szintaxisa	
Lépjen be globális konfigurációs módba!	<code>S1#configure terminal</code>
Adja meg a beállítandó fizikai interfész típusát és számát, például FastEthernet 0/18, és lépjen be interfész konfigurációs módba!	<code>S1(config)#interface fastEthernet 0/18</code>
Az interfészt állítsa access (elérési) módba! Ha az interfész az alapértelmezett dinamikusan konfigurált elérési mód (dynamic desirable) üzemmódban van, akkor nem lehet biztonságos interfészként konfigurálni.	<code>S1(config-if)#switchport mode access</code>
Engedélyezze a portbiztonságot az interfészen!	<code>S1(config-if)#switchport port-security mac-address</code>

Dinamikus

A MAC-címek megtanulása dinamikusan történik, a megtanult címeket a címtábla tárolja. A megtanulható címek száma szabályozható, alapértelmezés szerint portonként legfeljebb egy. A megtanult címek a port lekapcsolása vagy a kapcsoló újraindítása esetén elvesznek.

Cisco IOS CLI parancsok szintaxisa	
Lépjen be globális konfigurációs módba.	S1# configure terminal
Adja meg a beállítandó fizikai interfész típusát és számát, például FastEthernet 0/18, és lépjen be interfész konfigurációs módba!	S1(config)# interface fastEthernet 0/18
Az interfészt állítsa access (elérési) módba! Ha az interfész az alapértelmezett dinamikusan konfigurált elérési mód (dynamic desirable) üzemmódban van, akkor nem lehet biztonságos interfészként konfigurálni.	S1(config-if)# switchport mode access
Engedélyezze a portbiztonságot az interfészen!	S1(config-if)# switchport port-security
Térjen vissza privilegizált EXEC módba!	S1(config-if)# end

Sticky

A dinamikusra hasonlító megoldás, amelyben a címeket az aktív konfiguráció is tárolja.

A portbiztonság alapértelmezés szerint nincs engedélyezve. A portbiztonság engedélyezését követően a biztonság megsértése a port leállítását eredményezi. Ha például a dinamikus portbiztonság van engedélyezve, és az engedélyezett MAC-címek maximális száma portonként egy, akkor az első megtanult cím lesz a biztonságos cím. Amennyiben egy másik számítógép eltérő MAC-címmel próbál csatlakozni a porthoz, az a biztonság megsértésének minősül.

Az alábbi esetek bármelyikének bekövetkezése a biztonság megsértésének minősül:

- A címtáblában szereplő címek száma elérte a biztonságos MAC-címek maximális számát, és egy -- a címtáblában nem szereplő MAC-címmel rendelkező -- eszköz próbál csatlakozni az interfészhez.
- A VLAN egyik biztonságos interfészén megtanult vagy beállított cím ugyanazon VLAN egy másik biztonságos interfészén látszik.

Cisco IOS CLI parancsok szintaxisa	
Lépjen be globális konfigurációs módba.	S1# configure terminal
Adja meg a beállítandó fizikai interfész típusát és számát!	S1(config)# interface fastEthernet 0/18
Az interfészt állítsa access (elérési) módba!	S1(config-if)# switchport mode access
Engedélyezze a portbiztonságot az interfészen!	S1(config-if)# switchport port-security
Állítsa be a biztonságos címek maximális számát 50-re!	S1(config-if)# switchport port-security maximum 50
Engedélyezze a MAC címek sticky megtanulási módját!	S1(config-if)# switchport port-security mac-address sticky
Térjen vissza privilegizált EXEC módba!	S1(config-if)# end

A portbiztonság aktiválása előtt a portot elérési módba kell állítani a *switchport mode access* parancs segítségével!

A kapcsoló vagy egy bizonyos interfész portbiztonsági beállításainak ellenőrzéséhez használjuk a *show port-security interface interface-id* parancsot! A képernyőkimeneten az alábbi információk jelennek meg:

- a biztonságos MAC-címek maximális száma portonként
- az interfészhez tartozó biztonságos MAC-címek száma
- a biztonságot megsértő események száma
- a biztonság megsértésének módja

Ezen felül a *show port-security address* parancs megjeleníti az összes porthoz tartozó biztonságos MAC-címet, a *show port-security* parancs pedig megjeleníti a kapcsoló portbiztonsági beállításait.

Amennyiben a statikus vagy a sticky portbiztonság van engedélyezve, az egyes portokhoz rendelt MAC-címek a *show running-config* paranccsal is megtekinthetők. Az aktív konfigurációban tárolt megtanult MAC-címek törlésének három módja létezik:

- A *clear port-security sticky interface <port száma> access* parancs segítségével töröljük ki a megtanult címeket! Ezután kapcsoljuk le a portot a *shutdown* paranccsal! Végül engedélyezzük újra a portot a *no shutdown* parancs segítségével!
- Tiltsuk le a portbiztonságot a *no switchport port-security* parancs segítségével! A letiltást követően engedélyezzük újra a portbiztonságot!
- Indítsuk újra a kapcsolót!

A kapcsoló újraindítása csak akkor működik, ha az aktív konfiguráció nincs elmentve az indító konfigurációs fájlba. Ellenkező esetben a kapcsolónak nem kell újratanulnia a címeket a rendszer újraindításakor. A megtanult MAC-cím egészen addig egy bizonyos porthoz lesz társítva, amíg a *clear port-security* paranccsal le nem tiltjuk a portbiztonságot. Ha ez megtörtént, ne felejtsük az aktív konfigurációt újra elmenteni az indító konfigurációs fájlba, máskülönben a kapcsoló az újraindítást követően ismét emlékezni fog az adott MAC-címre.

Amennyiben egy kapcsolón vannak használaton kívüli portok, ajánlott azokat letiltani. A kapcsoló portjainak letiltása igen egyszerű. Keressük meg az összes használaton kívüli portot, és mindegyiknél adjuk ki a *shutdown* parancsot! Amennyiben egy portot aktiválni kell, adjuk ki a *no shutdown* parancsot!

A portbiztonság engedélyezésén és a használaton kívüli portok letiltásán kívül a kapcsoló biztonsága tovább fokozható a vty vonalakra beállított jelszavakkal, a bejelentkezési üzenetek engedélyezésével és a jelszavak -- *service password-encryption* paranccsal történő -- titkosításával. A fenti beállításokhoz használjuk a forgalomirányítók esetében tanult parancsokat!

Terminál ablak

```
switch#show port-security interface fastEthernet 0/18
```

```
Port Security          : Enabled
Port Status            : Secure-down
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Portbiztonsági beállítások
ellenőrzése

Biztonságos MAC-címek
ellenőrzése

Terminál ablak

```
switch#show port-security address
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
99	0050.BAA6.06CE	SecureConfigured	Fa0/18	-

```
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Portbiztonsági beállítások
ellenőrzése

Biztonságos MAC-címek
ellenőrzése

5.5.5 A Cisco Discovery Protocol

A Cisco Discovery Protocol (CDP, Cisco felfedező protokoll) olyan, kapcsolók, ISR-ek és forgalomirányítók által használt információgyűjtő eszköz, amely más, közvetlenül csatlakozó Cisco eszközökkel oszt meg adatokat. A CDP alapértelmezés szerint az eszköz elindulásával egy időben kezd futni, melynek során rendszeresen üzeneteket (más néven CDP hirdetések) küld a közvetlenül csatlakozó hálózatokba.

A CDP kizárólag a második rétegben működik, és számos különböző helyi hálózattípuson használható, beleértve az Ethernet és a soros hálózatokat is. Második rétegbeli protokollról lévén szó, a CDP akkor is meg tudja határozni a közvetlenül csatlakozó kapcsolat állapotát, ha nincs IP-cím megadva vagy a megadott cím hibás.

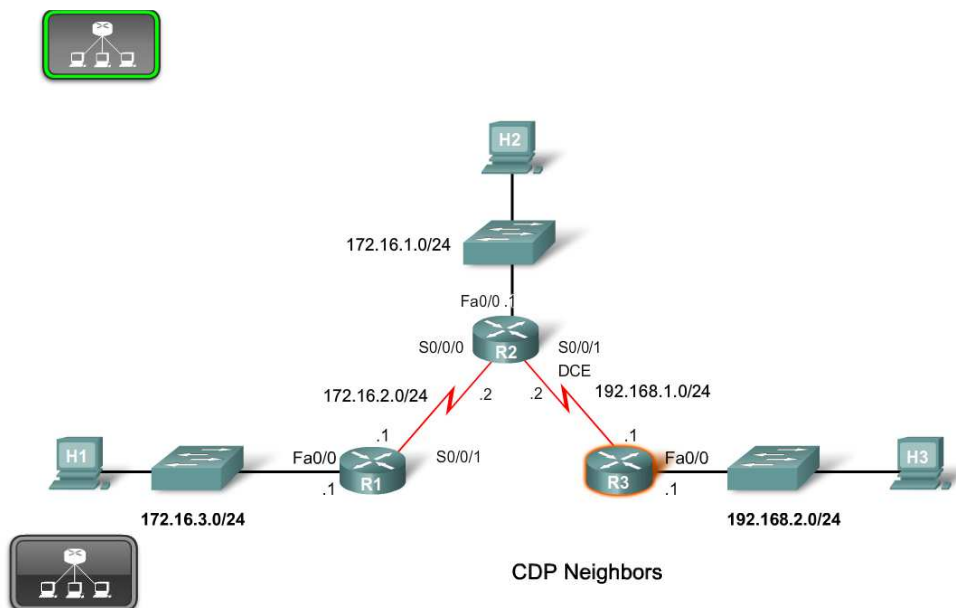
Az ugyanazon helyi hálózaton, egymáshoz közvetlenül csatlakozó Cisco eszközöket egymás szomszédjainak nevezzük. A szomszéd eszköz fogalmának megértése fontos a CDP parancsok kimenetének értelmezésénél.

A CDP által gyűjtött információk:

- Az eszköz azonosítója - a beállított állomásnév
- Címlista - a harmadik rétegbeli cím, ha meg van adva
- Portazonosító - a közvetlenül csatlakozó port (pl.: 0/0/0)
- Szolgáltatáslista - az eszköz által biztosított funkció(k)
- Platform - az eszköz hardverplatformja (pl.: Cisco 1841)

A *show cdp neighbors* és a *show cdp neighbors detail* parancsok kimenete megjeleníti az adott Cisco eszköz által a közvetlenül csatlakozó szomszédjairól szerzett információkat.

A CDP információk megjelenítéséhez nem szükséges a távoli eszközökre történő bejelentkezés. Mivel a CDP rengeteg adatot gyűjt és jelenít meg a közvetlenül csatlakozó szomszédokról, ráadásul bejelentkezést sem igényel, ezért az éles hálózatokban biztonsági okokból általában letiltják. Ezen felül a CDP sávszélességet köt le, így hatással lehet a hálózat teljesítményére.



```

R3#show cdp neighbors
Capability Codes: R - Router, T- Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Hose, I - IGMP, r - Repeater, P - Phone

Device ID      Local Intrfce    Holdtme    Capability    Platform    Port ID
Switch         Fas 0/0          133        S I           WS-C2950-2  Fas 0/11
R2             Ser 0/0/0        149        R S I         Cisco 1841  Ser 0/0/1
  
```



CDP neighbors detail

```
R3#show cdp neighbors detail
-----
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/1, Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''

-----
Device ID: S3
Entry address(es):
Platform: cisco WS-C2950-24, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/11
Holdtime : 148 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 24-Apr-02 06:57 by antonino

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFF0
10231FF00000000000000000AB769F6C0FF0000
VTP Management Domain: 'CCNA3'
Duplex: full

R3#
```

5.6 A fejezet összefoglalása

- Egy Cisco 1841 típusú ISR forgalomirányító fontosabb összetevői a következők:
 - HWIC bővítőaljzatok
 - Compact Flash modul
 - USB port
 - Kettő darab 10/100-as Fast Ethernet port
 - Konzol- és AUX port
 - Rendszer tápellátás visszajelző LED
 - A forgalomirányító indítási folyamata három részből áll:
 - 1. POST (önellenőrzés) végrehajtása
 - 2. Az IOS szoftver megkeresése és betöltése
 - 3. Az indító konfigurációs fájl megkeresése és feldolgozása
 - Cisco IOS rendszerkód állomány
- Két lehetséges eljárás létezik arra vonatkozóan, hogy egy számítógépet egy hálózati eszközzel, konfigurációs és felügyeleti feladatok céljából összekapcsoljanak: sávon-kívüli és sávon-belüli felügyelet.
- A Cisco Forgalomirányító és Biztonságos Eszközkezelő (SDM) egy grafikus felhasználói felülettel (GUI) rendelkező segédeszköz, mely Cisco eszközök beállításához, felügyeletéhez és karbantartásához használható. A Cisco SDM segítségével ajánlott konfigurálni egy új Cisco ISR forgalomirányítót.
- A Cisco IOS parancssoros felület (CLI) egy szöveges alapú program, mely lehetővé teszi Cisco IOS parancsok bevitelét és végrehajtását, Cisco eszközök konfigurálása, felügyelete és karbantartása céljából. A Cisco IOS parancssoros felületet általában a Cisco eszközök magasabb szintű konfigurálása esetén használják, illetve régebbi eszközöknél, melyek nem támogatják az SDM-et.
- A konfigurációs ellenőrzőlista segédeszköz fontos szerepet játszik abban, hogy az ügyfél az általa kívánt konfigurációhoz jusson hozzá.
- Az SDM Express a Cisco forgalomirányítóval együtt szállított segédeszköz, mely egyszerűvé teszi az alapvető forgalomirányító konfiguráció létrehozását.
- Az SDM egy fejlettebb grafikus felhasználói felület, több rendelkezésre álló konfigurációs beállítási lehetőséggel.
- Mind az SDM, mind az SDM Express grafikus-alapú konfigurációs varázslókat használ, a Cisco eszközök beállításának leegyszerűsítéséhez.
- Néhány konfigurálási folyamat, ami elvégezhető ezekkel: alapvető konfiguráció kialakítása, LAN IP konfiguráció, DHCP, WAN IP konfiguráció és NAT.



- A CLI nem nyújt lépésről-lépésre történő konfigurációs támogatást, így használata több tervezést és magasabb szaktudást igényel.
 - A privilegizált exec, globális konfigurációs és interfész konfigurációs módok mindegyikére szükség van egy forgalomirányító Cisco IOS parancssoros felületen történő konfigurálásához.
 - A környezetérzékeny sugó javaslatot adhat egy parancs kiegészítésére, valamint a további parancssori paraméterek meghatározására.
 - Az IOS **show** parancsok alapvető segédeszközei a forgalomirányítók beállításainak ellenőrzésével és hibaelhárításával kapcsolatos feladatoknak.
 - Az indító konfigurációs fájl az eszköz nemfelejtő memóriájában (NVRAM) található, és tartalma az eszköz működésének kezdetén a munkamemóriába másolódik.
 - Az aktív konfiguráció parancsoknak olyan halmaza, melyek aktuálisan az eszköz RAM-jában vannak működésben.
 - Az IOS parancssor használható alapvető forgalomirányító konfigurációs feladatokra, például a forgalomirányító nevének, jelszavaknak és üdvözlő üzeneteknek a beállítására. Ezen kívül alkalmazható soros és ethernet interfészek, illetve DHCP és NAT szolgáltatások beállítására is.
-
- A WAN összeköttetés egy olyan hálózati kapcsolódási típus, mely nagy távolságokon át képes küldeni a hálózati jeleket.
 - Három típusa létezik a soros WAN kapcsolatoknak: pont-pont, vonalkapcsolt és csomagkapcsolt. A megfelelő WAN kapcsolat kiválasztása gondos tervezést igényel.
 - A Cisco eszközök WAN kapcsolaton keresztül, Telnet vagy SSH szolgáltatás segítségével, távolról is konfigurálhatóak. Az SSH-t részesítik előnyben.
 - Némely WAN kapcsolat támogatja az Ethernet interfészeket. Más WAN kapcsolatok soros interfészeket igényelnek.
-
- Egy Cisco Catalyst 2960 sorozatú kapcsoló fontosabb összetevői a következők:
 - 24 darab 10/100-as Ethernet Port
 - Portállapot LED-ek
 - Mode gomb
 - Konzolport
 - Kétfunkciós 10/100/1000-es vagy SFP port
 - Cisco IOS LAN-alapú szoftver rendszerkód állomány
 - A 2960-as készülék támogatja a portok sebességének és duplex módjának automatikus egyeztetését.
-
- Amennyiben ellátjuk IP-címmel a VLAN 1 interfészt, lehetőség nyílik a kapcsoló távoli felügyeletére SSH vagy más TCP/IP alkalmazás, például hálózatfelügyeleti szoftver használatával.
 - Egy alapvető kapcsoló konfiguráció a kapcsoló nevét, a kapcsoló eléréséhez szükséges titkosított jelszavakat és Cisco CLI konfigurációs parancsokat tartalmazza.
 - Portbiztonság alkalmazásával korlátozható a portonként engedélyezett érvényes MAC-címek száma. A szolgáltatás beállítható statikus, dinamikus vagy dinamikus sticky üzemmódra.

6. Forgalomirányítás

6.1 Az irányító protokollok konfigurálása

6.1.1 A forgalomirányítás alapjai

Egy szervezet belső hálózatának növekedésével biztonsági és szervezeti okokból szükségessé válhat a hálózat kisebb egységekre bontása, amit gyakran alhálózatokra bontással valósítanak meg. Az alhálózatok közötti forgalom továbbításához forgalomirányítóra van szükség.

A forgalomirányítók az üzenetek megfelelő célba juttatása érdekében egy táblát használnak, melyben minden közvetlenül csatlakozó hálózat és a hozzájuk tartozó interfész szerepel. Minden interfész különböző IP hálózathoz tartozik.

A forgalomirányító az irányítótábla információi alapján határozza meg a megfelelő útvonalat. Az irányítótábla tartalmaz nem közvetlenül csatlakozó, távoli hálózatokra vonatkozó útvonalakat is.

A forgalomirányító útvonalbejegyzéseit létrehozhatja statikusan egy rendszergazda, vagy irányító protokoll segítségével küldheti egy másik forgalomirányító.

A forgalomirányító a csomagok megfelelő továbbításához útvonalakat tartalmazó irányítótáblát használ. Minden bejegyzés megadja, hogy egy adott hálózat melyik átjárón vagy interfészen keresztül érhető el.

Egy útvonalbejegyzésnek 4 alapvető összetevője van:

- Célhálózat címe
- Alhálózati maszk
- Átjáró vagy interfész címe
- Útvonal költsége vagy irányítási mértéke

Amikor beérkezik egy csomag, a forgalomirányító a csomagtovábbítás érdekében megvizsgálja a célállomás IP-címét, majd vele egyező bejegyzést keres az irányítótáblában.

Míg az irányítótábla minden bejegyzése egy célhálózat címe, addig a csomagban található cél IP-cím tartalmazza mind a hálózat mind az állomás címét. A forgalomirányító a célhálózathoz tartozó útvonal meghatározásához a hálózati cím és egy irányítótábla-bejegyzés között keres egyezést. Ehhez a forgalomirányítónak meg kell határoznia az IP-cím hálózatazonosító, illetve állomásonosító bitjeit.

A forgalomirányító kikeresi az irányítótábla összes lehetséges útvonalának hálózati maszkjait, alkalmazza azokat a csomag cél IP-címére, majd az így kapott hálózati címet hasonlítja össze a táblában lévő útvonalak hálózati címével. Egyezés esetén a megfelelő interfészre vagy a megadott átjáróhoz továbbítja a csomagot. Több lehetséges útvonal esetén a forgalomirányító a legspecifikusabb utat választja, vagyis azt, amelyiknél a hálózati címben a legtöbb bit megegyezik.

Előfordulhat, hogy több útvonal is létezik az adott célhálózat felé. Ilyen esetekben a választás irányító protokoll szabályok alapján történik.

Amennyiben egyetlen egyezés sincs, a forgalomirányító a csomagot az alapértelmezett útvonalként előre megadott átjáróhoz küldi, vagy annak hiányában eldobja azt.

```
Gateway of last resort is 172.16.3.1 to network 0.0.0.0 S
172.17.0.0/16 [1/0] via 172.16.3.1
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
S 172.16.236.0/24 [1/0] via 172.16.3.1
S 172.16.0.0/16 [1/0] via 172.16.3.1
C 172.16.1.0/24 is directly connected, FastEthernet0/0
C 172.16.3.0/24 is directly connected, FastEthernet0/1 [1/0]
via 172.16.3.1
    172.22.0.0/24 is subnetted, 1 subnets
S 172.22.1.0 [1/0] via 172.16.1.1
S* 0.0.0.0/0 [1/0] via 172.16.3.1
```

A forgalomirányító minden hálózati maszkot alkalmaz a cél IP-címre, hogy megtalálja azt a hálózati címet, ahol a leghosszabb az egyezés.

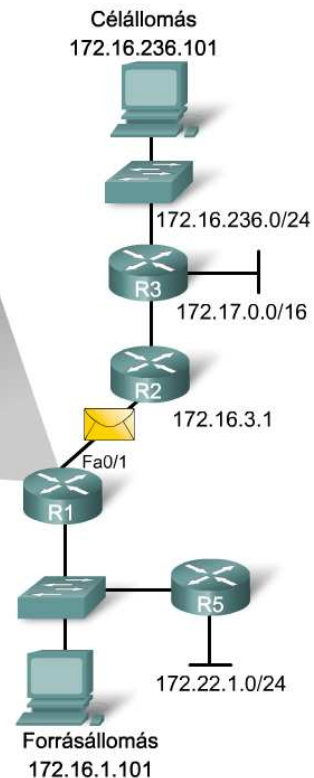
172.16.236.101 ----> leghosszabb egyezés: 172.16.236.0 255.255.255.0

A forgalomirányító az eredményül kapott hálózati címet összehasonlítja a forgalomirányító tábla bejegyzéseivel.

S 172.16.236.0/24 [1/0] via 172.16.3.1

A forgalomirányító kiküldi a csomagot a célállomáshoz vezető út következő ugrásának megfelelő interfészén.

C 172.16.3.0/24 is directly connected, FastEthernet 0/1



Cisco forgalomirányítók a *show ip route* IOS parancs jeleníti meg az irányítótábla tartalmát, amely számos különböző típusú útvonalat tartalmazhat.

Közvetlenül csatlakozó útvonalak

Egy forgalomirányító indulásakor a konfigurált interfészek engedélyezettek, és amint működőképessé válnak, a forgalomirányító a hozzá közvetlenül kapcsolódó hálózatok hálózati címét közvetlenül csatlakozott útvonalakként bejegyzi az irányítótáblába. Cisco forgalomirányítók irányítótáblájában ezeket az útvonalakat a C előtag jelöli. Az interfész újbóli konfigurálása vagy leállítása után automatikusan frissülnek az útvonalbejegyzések.

Statikus útvonalak

A hálózati rendszergazda manuálisan konfigurálhat egy adott hálózathoz statikus útvonalat. Ezeket az útvonalakat az S előtag jelöli az irányítótáblában, és mindaddig nem változnak, amíg a rendszergazda újra nem konfigurálja őket.

Dinamikusan frissített útvonalak (dinamikus útvonalak)

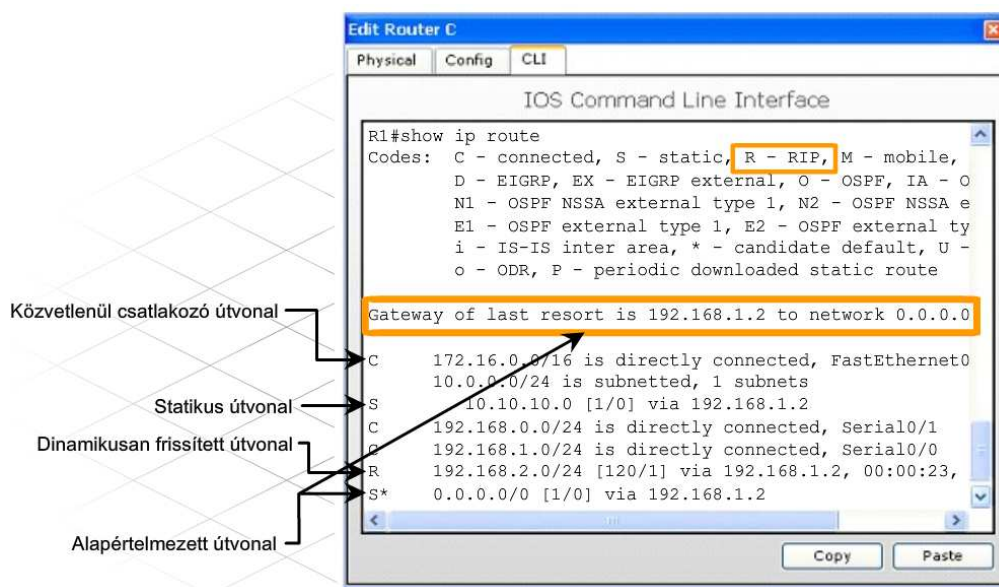
A dinamikus útvonalakat a forgalomirányító protokollok hozzák létre és tartják karban. Az forgalomirányító protokollok irányítási információkat cserélnek egymással a hálózaton. A dinamikus útvonalakat az irányítótáblában mindig az útvonalat létrehozó protokollra jellemző előtag jelöli. Például RIP (forgalomirányítási információs protokoll - Routing Information Protocol) esetén ez az R.

Alapértelmezett útvonal

Az alapértelmezett útvonal olyan statikus útvonal, amely meghatározza a használandó átjárót, ha az irányítótábla nem tartalmaz célhálózathoz vezető útvonalat. Ez gyakran az internetszolgáltató felé vezető útvonal következő forgalomirányítója. Egyetlen forgalomirányítót tartalmazó alhálózat esetén automatikusan az adott forgalomirányító lesz az alapértelmezett átjáró, mivel a helyi hálózat forgalma mindkét irányban csak rajta keresztül tud áthaladni.

Az irányítótáblák nem a forrás és célhálózat közötti teljes útvonalról, csupán a következő ugrásról tartalmaznak információt. Az irányítótáblában szereplő következő ugrás jellemzően egy közvetlenül csatlakozó hálózat.

Statikus útvonal esetén a következő ugrás a forgalomirányító által elérhető tetszőleges IP-cím lehet. A folyamat végén a csomag áthalad a célállomáshoz közvetlenül csatlakozó forgalomirányítón, majd céljához ér. Minden közbülső forgalomirányító esetében hálózati címek és nem konkrét állomáscímek alapján történik az irányítás. A célhálózat előtti utolsó forgalomirányító táblája az egyetlen, ahol a célcím nem egy hálózatra, hanem egy konkrét állomásra vonatkozik.



Statikus útvonalak konfigurálása

A statikus útvonalakat a hálózati rendszergazda manuálisan konfigurálja. Statikus útvonal létrehozásának lépései Cisco forgalomirányítókon:

- 1. lépés.** Csatlakozzon a forgalomirányítóhoz konzol kábel segítségével!
- 2. lépés.** Egy adott forgalomirányító konfigurálásához nyisson egy HyperTerminal ablakot!

3. lépés. Privilegizált módba lépéshez gépelje be az **enable** parancsot a **Router1>** parancssorba! Figyelje meg hogy a > jel helyett # jelöli a privilegizált módot!

```
Router1>enable
```

```
Router1#
```

4. lépés. Lépjen globális konfigurációs módba!

```
Router1#config terminal
```

```
Router1(config)#
```

5. lépés. Statikus útvonal létrehozásához használja a Cisco IOS **ip route** parancsát a következő formában:

```
ip route [célhálózat] [alhálózati_maszk] [átjáró_címe]
```

vagy

```
ip route [célhálózat] [alhálózati_maszk] [kimenő_interfész]
```

Példaként a 192.168.16.0 hálózat egy állomásának eléréséhez az R1 forgalomirányítón a rendszergazda egy statikus útvonalat konfigurál globális konfigurációs módban a következő Cisco IOS parancs segítségével:

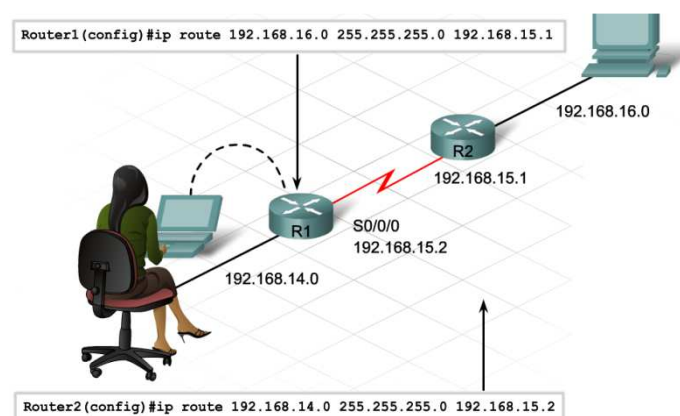
```
Router1(config)#ip route 192.168.16.0 255.255.255.0 192.168.15.1
```

vagy

```
Router1(config)#ip route 192.168.16.0 255.255.255.0 S0/0/0
```

A 192.168.16.0 hálózat egy állomásával kétirányú kommunikáció létrehozásához a rendszergazdának az R2 forgalomirányítón is definiálni kell egy statikus útvonalat.

Mivel a statikus útvonalakat a rendszergazda manuálisan hozza létre, így a hálózatban bekövetkező bármilyen változás esetén neki kell statikus útvonalat létrehozni vagy törölni. Kisebb hálózatokban kevesebb változás történhet, így a statikus útvonalak kezelése nem okoz gondot. Nagyobb hálózatokban viszont az irányítótáblák manuális kezelése jelentős adminisztrációs időt vehet igénybe, így ezekben a hálózatokban statikus útvonalak helyett dinamikus irányítást használnak.



6.1.2 Forgalomirányító protokollok

Az útvonalak gyorsan változhatnak. A kábelek és más hardverelemek meghibásodásai elérhetetlenné tehetik a célhálózatokat az addig használt interfészen keresztül. A forgalomirányítónak képesnek kell lenni az útvonalak gyors frissítésére a rendszergazda beavatkozása nélkül.

A forgalomirányítók forgalomirányító protokollok segítségével dinamikusan kezelik a saját interfészüktől, illetve más forgalomirányítóktól kapott információkat. A forgalomirányító protokollok konfigurálhatók úgy, hogy kezeljék a manuálisan beállított útvonalakat is.

Dinamikus irányítás használatával megtakarítható a statikus útvonalak kezeléséhez szükséges idő. Dinamikus irányítással a forgalomirányítók a rendszergazda beavatkozása nélkül képesek a hálózatban bekövetkező változások követésére, valamint forgalomirányító tábláik kezelésére.

A dinamikus irányító protokollok megtanulják az elérhető útvonalakat, a legjobbkat rögzítik a forgalomirányító táblában, az érvényteleneket pedig eltávolítják onnan. A forgalomirányító protokoll által a legjobb útvonal meghatározásához alkalmazott eljárást nevezzük forgalomirányító algoritmusnak, melynek két fő osztálya létezik: távolságvektor alapú és kapcsolatállapot alapú. A két megoldás különböző módon határozza meg a célhálózathoz vezető legjobb utat.

Konfiguráció vagy hiba következtében bekövetkező hálózati topológiaváltozás esetén az új hálózati topológia pontos képe érdekében minden forgalomirányító forgalomirányító táblája is meg kell, hogy változzon. Amikor a hálózat minden forgalomirányítója az új útvonalnak megfelelően frissítette forgalomirányító tábláját, akkor a hálózat konvergált.

Az alkalmazott forgalomirányítási algoritmus nagyon fontos szerepet játszik a dinamikus irányításban. Két forgalomirányító akkor tud forgalomirányítási információt cserélni, ha ugyanazt a forgalomirányítási protokollt és így ugyanazt a forgalomirányítási algoritmust használják.

Távolságvektor alapú forgalomirányító algoritmust használó forgalomirányítók rendszeres időközönként másolatot küldenek egymásnak forgalomirányító táblájukról, így informálva egymást a hálózati topológiában bekövetkező változásokról.

A távolságvektor alapú forgalomirányító algoritmus a más forgalomirányítóktól kapott útvonalinformációt két alapvető szempont alapján értékeli:

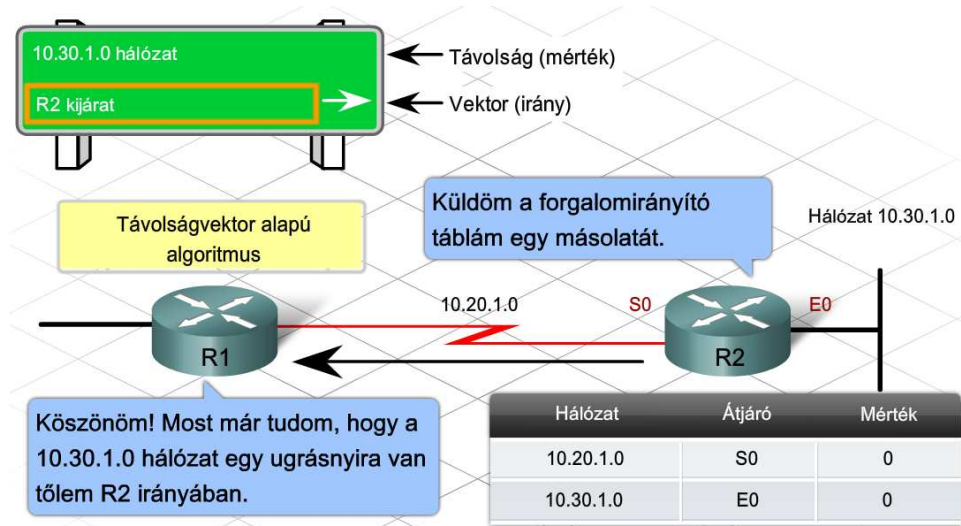
- Távolság - Milyen távolságra van a hálózat a forgalomirányítótól?
- Vektor – Milyen irányba kell a csomagot továbbítani a hálózat felé?

Az útvonal távolság összetevőjét az út költségének vagy mértékének nevezik, és a következőktől függhet:

- Ugrások száma
- Adminisztratív költség
- Sávszélesség
- Átviteli sebesség
- Késleltetések valószínűsége
- Megbízhatóság

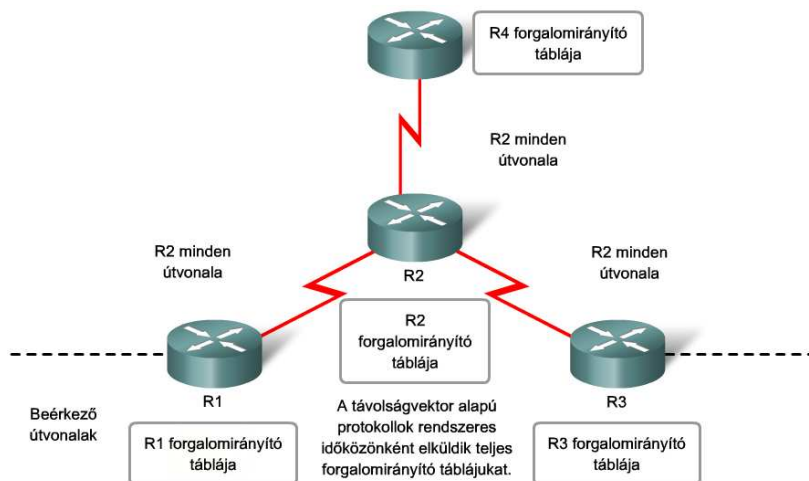
Az útvonal vektor vagy irány összetevője az adott útvonalban a következő ugrás IP-címe.

A távolságvektorok olyanok, mint a kereszteződésekben lévő jelzőtáblák. A tábla a cél irányába mutat, és jelzi a célhoz vezető út hosszát. Az út mentén további táblák mutatnak a cél felé, de a hátralévő távolság már egyre kevesebb. Amíg a távolság csökken, addig a forgalom a legjobb útvonalon halad.



Minden távolságvektor alapú forgalomirányítást használó forgalomirányító az irányítási információit elküldi szomszédainak. Szomszédos forgalomirányítóknak azokat nevezzük amelyeknek legalább egy közös, közvetlenül kapcsolódó hálózatuk van. A közvetlenül csatlakozó hálózatokhoz vezető interfészek távolsága 0.

Minden forgalomirányító forgalomirányító táblát kap a szomszédaitól. Például az R2 az R1-től kap



ilyen információt. R2 megnöveli a kapott táblában szereplő költségértékeket, jelen esetben az ugrásszámot, és ezzel jelzi, hogy az érintett célhálózatok innen már egy ugrásnyival hosszabb úton érhetők el. Ezt követően R2 is elküldi forgalomirányító tábláját szomszédainak, köztük R3-nak is. Lépésről lépésre ugyanez a folyamat zajlik le minden irányban a szomszédos forgalomirányítók között.

Végül minden forgalomirányító a távoli hálózatokat a szomszédos forgalomirányítók információi alapján tanulja meg. A forgalomirányító tábla minden bejegyzéséhez így egy összegzett távolságvektor tartozik, ami megadja a hálózat távolságát az adott irányban.

A távolságvektor felderítő folyamat alapján a forgalomirányító a szomszédoktól kapott információk segítségével megkeresi a célhálózat felé vezető legjobb útvonalat, ami a legkisebb távolságú vagy mértékű út.

A forgalomirányítók minden topológiaváltozáskor frissítik forgalomirányító táblájukat, vagyis bármikor, ha egy új hálózat jelenik meg, vagy egy útvonal elérhetetlenné válik pl. egy forgalomirányító meghibásodása miatt. A forgalomirányító táblák másolatainak forgalomirányítóról forgalomirányítóra történő küldése eredményeként a topológia frissítése a hálózatfelderítési folyamathoz hasonlóan lépcsről lépésre történik.

6.1.3 A leggyakoribb belső forgalomirányító protokollok

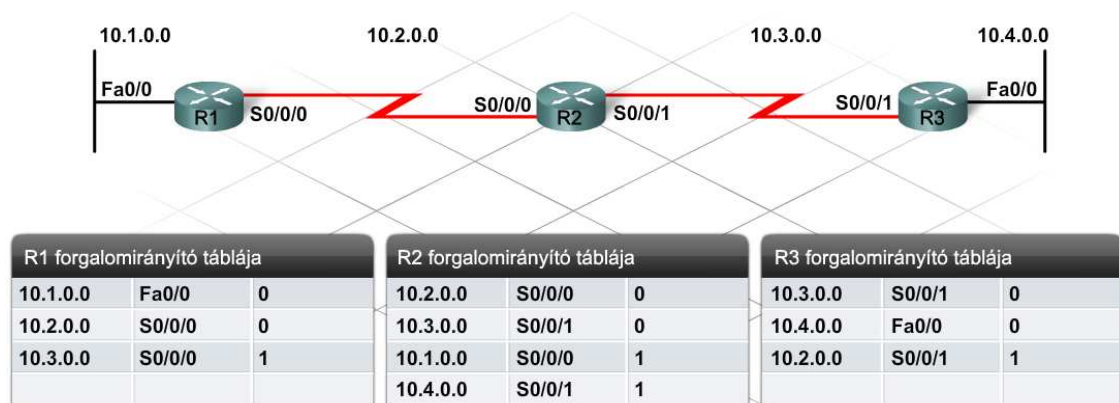
A forgalomirányítási információs protokoll (RIP - Routing Information Protocol) a világ több ezer hálózatában alkalmazott, az RFC 1058 dokumentumban definiált távolságvektor alapú protokoll.

A RIP jellemzői:

- Távolságvektor alapú forgalomirányító protokoll.
- Az útvonal kiválasztáskor az ugrásszámot használja mértéknek.
- A 15 ugrásnál hosszabb útvonalakat elérhetetlennek tekinti.
- 30 másodpercenként elküldi teljes irányítótábláját a szomszédainak.

Útvonalfrissítés fogadásakor a forgalomirányító a változásoknak megfelelően módosítja forgalomirányító tábláját. Amennyiben új útvonalról szerez tudomást a frissítésből, a kapott ugrásszámot eggyel megnövelve tárolja az útvonalat a forgalomirányító táblájában. Következő ugrásként a frissítést küldő, közvetlenül csatlakozó forgalomirányító helyi hálózati címét használja.

Saját forgalomirányító táblájának frissítését követően a forgalomirányító azonnal útvonalfrissítésekkel tájékoztatja a hálózat forgalomirányítóit a változásokról. Ezeknek az úgynevezett eseményvezérelt frissítéseknek (triggered update) a küldése a RIP által küldött rendszeres frissítésektől független.



RIP (Routing Information Protocol - forgalomirányítási információk protokoll)

A RIP egyszerűségének és könnyű telepíthetőségének köszönhetően széles körben használt és népszerű forgalomirányító protokoll.

A RIP hátrányai:

- A maximum 15 ugrásnak köszönhetően csak olyan hálózatokban alkalmazható, ahol 16 forgalomirányítónál több nem kapcsolódik sorban egymáshoz.
- Mivel rendszeres időközönként teljes forgalomirányító táblákat küld a közvetlenül csatlakozott szomszédoknak, így nagyobb hálózat esetén minden frissítés jelentős hálózati forgalmat jelent.
- Nagy hálózatok változása esetén lassan konvergál.

Jelenleg a RIP két verziója elérhető: RIPv1 és RIPv2. A RIPv2 számos előnnyel rendelkezik és rendszerint csak abban az esetben nem alkalmazzák, ha valamelyik eszköz nem támogatja. A legjelentősebb különbség a két verzió között, hogy a RIPv2 támogatja az osztály nélküli irányítást, mivel frissítései tartalmazzák az alhálózati maszkot. A RIPv1 nem küld hálózati maszk információt, és így - jobb híján - az egyes osztályok alapértelmezett maszkjait használja.

EIGRP - Enhanced Interior Gateway Routing Protocol

Az EIGRP a Cisco saját fejlesztésű, továbbfejlesztett távolságvektor alapú forgalomirányító protokollja, melyet a többi távolságvektor alapú protokoll, mint például a RIP, hiányosságainak megoldására hoztak létre. Ilyen hiányosság például az ugrásszám mértékként való használata, valamint a maximum 15 ugrás méretű hálózatok kezelése.

Az EIGRP összetett mértéket használ, többek között a konfigurált sávszélességet és a csomag adott útvonalra vonatkozó késleltetését.

Az EIGRP jellemzői:

- Egy útvonal költségének kiszámításához többféle mértéket használ.
- A távolságvektor alapú protokollok következő ugrás szerinti mérték tulajdonságait ötvözi további adatbázisokkal és frissítési jellemzőkkel.
- Maximum 224 ugrást engedélyez.

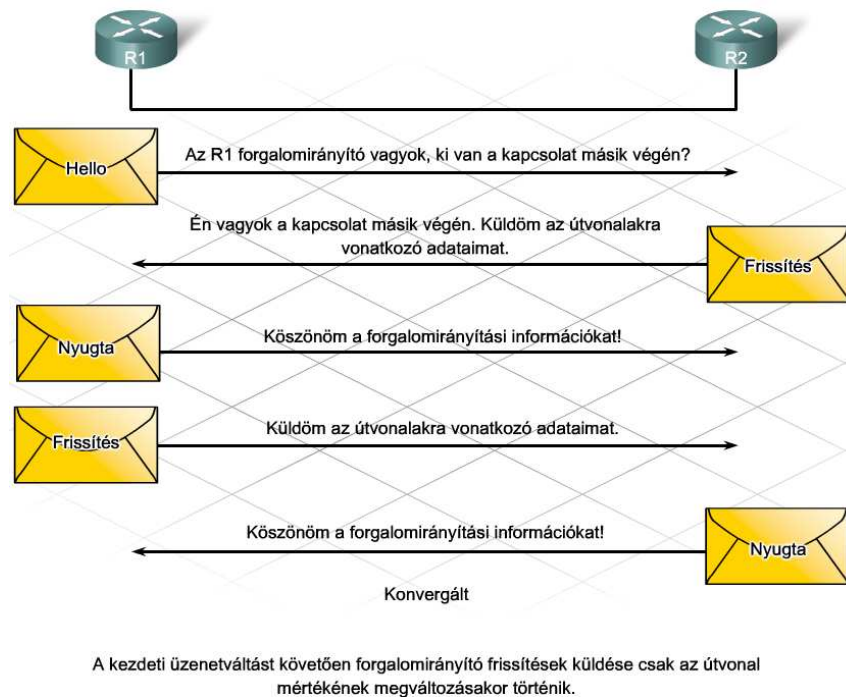
A RIP-pel szemben az EIGRP nem csak a forgalomirányító táblájában tárolja a működéséhez szükséges információkat, hanem két további adatbázis táblát is létrehoz: a szomszéd- és a topológiatáblát.

A szomszéd táblában található a közvetlenül csatlakozó helyi hálózatokon lévő forgalomirányítók adatai, mint például interfész IP-címe, típusa és sávszélessége.

Az EIGRP topológiatábla a szomszédos forgalomirányítók hirdetményei alapján épül fel, és tartalmaz minden szomszéd által hirdetett útvonalat. Az EIGRP a DUAL (Diffused Update Algorithm) algoritmust használja egy hálózaton belül a célhoz vezető legrövidebb útvonal meghatározására és bejegyzésére a forgalomirányító táblába. A topológiatábla segítségével a hálózat megváltozásakor a forgalomirányító gyorsan képes a legjobb alternatív útvonal meghatározására. Amennyiben a

topológiatábla nem tartalmaz alternatív útvonalat, akkor a forgalomirányító a szomszédait lekérdezve keres új útvonalat a célhoz.

Míg a RIP hálózatok egyszerűek és maximum 15 ugrás méretűek lehetnek, addig az EIGRP ideális összetettebb, maximum 224 ugrás méretű és gyors konvergenciát igénylő nagyobb hálózatok kezelésére.



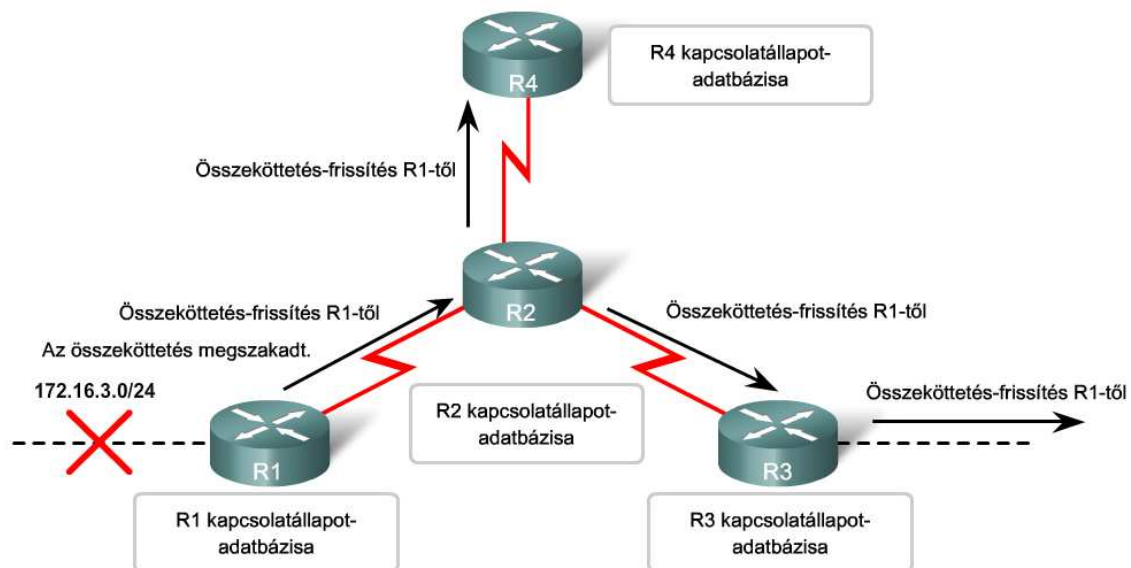
Kapcsolatállapot alapú protokollok

A távolságvektor alapú irányító algoritmust futtató forgalomirányítók a távoli hálózatokról kevés, a távoli forgalomirányítókról pedig semmi információval sem rendelkeznek. Ezzel szemben a kapcsolatállapot alapú irányító algoritmus a távoli forgalomirányítókról és azok összeköttetéseiről minden forgalomirányítóban teljes topológiai adatbázis nyilvántartást vezet.

A kapcsolatállapot alapú forgalomirányítás jellegzetes összetevői:

- Forgalomirányító tábla - az ismert útvonalak és interfészek listája.
- Kapcsolatállapot-hirdetés (LSA - Link-state advertisement) -forgalomirányítók között küldött, forgalomirányítási információkat tartalmazó, kisméretű csomag. Az LSA-k tartalmazzák egy forgalomirányító interfészeinek (összeköttetéseinek) állapotát és egyéb információit, mint például minden összeköttetés IP-címét.
- Topológiai adatbázis – egy forgalomirányítóhoz beérkező LSA-kból összegyűjtött információkat tartalmazza.
- Legrövidebb utat kereső algoritmus (SPF - Shortest Path First algorithm) - az adatbázison végzett számítások, melyek eredményeként előáll az SPF-fa. Az SPF-fa a hálózat egy térképe a forgalomirányító szemszögéből. A fában található információk alapján épül fel a forgalomirányítótábla.

Az LSA-csomagok megérkezését követően az SPF algoritmus a forgalomirányító topológiai adatbázisa alapján felépíti az SPF fát. Az SPF algoritmus meghatározza a hálózatokhoz vezető legjobb útvonalakat. Minden esetben, amikor egy LSA-csomag megváltoztatja a kapcsolatállapot adatbázist, az SPF algoritmus újraszámítja a legrövidebb útvonalakat, és ennek megfelelően frissíti a forgalomirányító táblát.



A kapcsolatállapot-alapú protokollok egy összeköttetés állapotának megváltozásakor küldenek frissítéseket.

OSPF

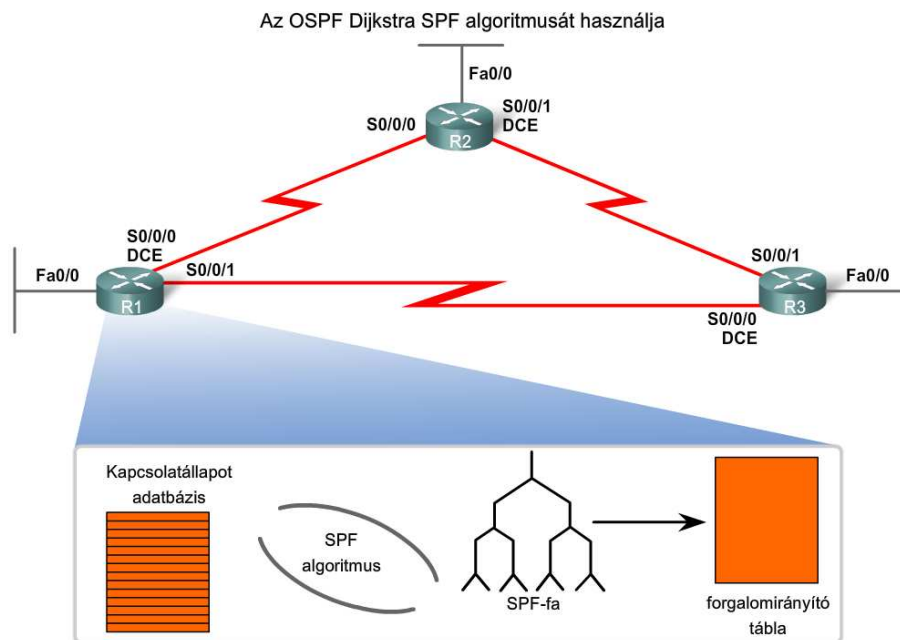
Az OSPF (Open Shortest Path First) egy nyílt szabványú, kapcsolatállapot alapú forgalomirányító protokoll, melyet az RFC 2328 dokumentum definiál. Az OSPF jellemzői:

- A célhoz vezető legkisebb költségű útvonal kiszámításához az SPF algoritmust használja.
- Forgalomirányító frissítéseket csak a hálózati topológia megváltozásakor küld; vagyis nem küldi el rendszeres időközönként a teljes irányítótáblát.
- Gyors konvergenciát tesz lehetővé.
- Támogatja a változó hosszúságú alhálózati maszkok (VLSM – Variable Length Subnet Mask) és a nem folytonos hálózatok használatát.
- Útvonal hitelesítést biztosít.

OSPF hálózatokban a forgalomirányítók abban az esetben küldenek egymásnak kapcsolatállapot-hirdetményeket, ha a hálózatban valamilyen változás történik, például egy új szomszédos forgalomirányító kerül a hálózatba, egy összeköttetés kiesik vagy éppen helyreáll.

A hálózati topológia megváltozásakor az érintett forgalomirányítók LSA frissítéseket küldenek a hálózat többi forgalomirányítójának. Minden forgalomirányító frissíti a topológia-adatbázisát, és újraépíti az SPF-fáját, hogy meghatározza az egyes hálózatokhoz vezető legrövidebb útvonalat, majd végül a megváltozott útvonalakkal frissíti a forgalomirányító tábláját.

Az OSPF több erőforrást, például RAM-ot és CPU teljesítményt igényel a forgalomirányítóban, és - mint minden fejlett hálózati protokoll - gyakorlott üzemeltető személyzetet igényel.



6.1.4 Szervezeten belüli forgalomirányítás

Minden forgalomirányító protokoll más és más mértéket használ, így két különböző forgalomirányító protokoll által használt mérték általában nem összehasonlítható. Adott esetben két forgalomirányító protokoll ugyanahhoz a célhoz eltérő útvonalat adhat meg, köszönhetően a különböző mértékeknek. Míg a RIP például a legkevesebb ugrást tartalmazó útvonalat használja, addig az EIGRP a legnagyobb sávszélességi és legkisebb késleltetésűt.

IP forgalomirányító protokollok által használt mértékek:

- Ugrásszám - egy csomag által érintett forgalomirányítók száma.
- Sávszélesség - egy adott összeköttetés sávszélessége.
- Terhelés - egy adott összeköttetés forgalmi kihasználtsága.
- Késleltetés - egy csomag célba jutásához szükséges idő.
- Megbízhatóság - egy összeköttetés meghibásodásának valószínűsége az interfészhez tartozó hibaszámláló vagy a korábbi hibák alapján.
- Költség - melyet vagy a Cisco IOS alkalmazás vagy a rendszergazda határoz meg az adott útvonal preferáltságát tükrözve. A költség lehet egyszerű vagy összetett mérték, szabályozhatja helyi irányelv.

Egy forgalomirányítón egyszerre több irányító protokoll is engedélyezhető, valamint a rendszergazda is konfigurálhat bizonyos hálózatokhoz statikus útvonalakat. Amennyiben egy forgalomirányító két különböző forgalomirányító protokoll alapján eltérő útvonallal rendelkezik egy célhálózat felé, hogyan dönti el, melyik útvonalat használja?

Ilyenkor a forgalomirányító az úgynevezett adminisztratív távolság (AD - administrative distance) alapján dönt. Az adminisztratív távolság egy útvonal "hihetőségének" mértéke. Minél kisebb az adminisztratív távolság, annál megbízhatóbb forrásból származik az útvonal. Például egy statikus útvonal adminisztratív távolsága 1, míg egy RIP által feltárt útvonalé 120. Ugyanahhoz a célhálózathoz vezető két különböző útvonal esetén a forgalomirányító a kisebb adminisztratív távolságút használja. Így a statikus útvonal elsőbbséget élvez a RIP által meghatározott útvonallal

szemben, csakúgy, mint a 0 adminisztratív távolsággal rendelkező, közvetlenül csatlakozó útvonal, a statikus útvonallal szemben.

Az útvonal forrása	Adminisztratív távolság	Alapértelmezett mérték(ek)
Csatlakoztatva	0	0
Statikus	1	0
EIGRP összevont útvonal	5	
Külső BGP	20	Rendszergazda által megadott érték
Belső EIGRP	90	Sávszélesség, késleltetés
IGRP	100	Sávszélesség, késleltetés
OSPF	110	A kapcsolat költsége (sávszélesség)
IS-IS	115	A kapcsolat költsége (rendszergazda által megadott érték)
RIP	120	Ugrásszám
Külső EIGRP	170	
Belső BGP	200	Rendszergazda által megadott érték

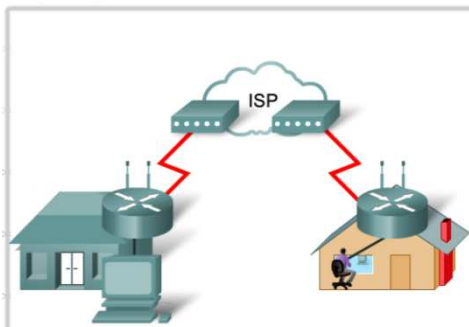
Bizonyos esetekben, mint például két meglévő hálózat egyesítésekor, szükségessé válhat egyszerre több forgalomirányító protokoll használata. Ugyanakkor egy új hálózat megtervezésekor érdemes egyetlen forgalomirányító protokoll használatára szorítkozni, mivel az megkönnyíti a hálózat karbantartását és hibaelhárítását. A megfelelő protokoll kiválasztása még a gyakorlott hálózattervező szakemberek számára sem egyszerű feladat.

Az internethez egyetlen átjáróval csatlakozó, kisebb hálózatok esetén várhatóan használhatók a statikus útvonalak. Dinamikus irányítást ezek a hálózatok ritkán igényelnek.

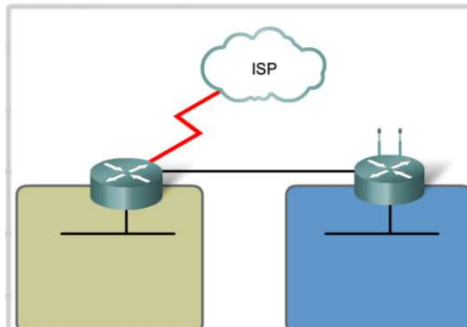
A szervezet növekedtével, ahogy néhány újabb forgalomirányító csatlakozik a topológiához, a RIPv2 lehet a megfelelő választás. A RIPv2 könnyen konfigurálható és megfelelően működik kisebb hálózatokban mindaddig, míg a hálózat nem éri el a 15 ugrásnyi méretet.

Nagyobb hálózatok esetében a leggyakrabban alkalmazott protokollok az EIGRP és az OSPF, de semmilyen egyszerű szabállyal nem lehet eldönteni, hogy melyiket válasszuk. Minden hálózat esetében a választás külön megfontolást igényel. Három alapvető kritériumot érdemes átgondolni:

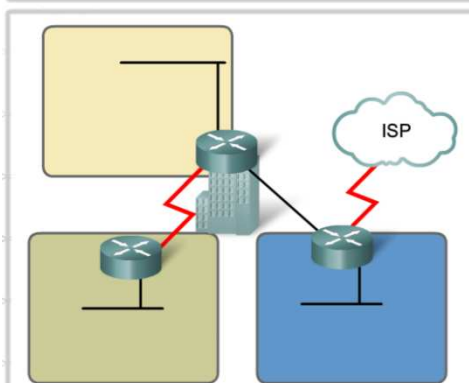
- **Egyszerű felügyelhetőség** - Milyen információkat vezet magáról a protokoll? Milyen show parancsok érhetők el?
- **Egyszerű konfigurálás** - Hány parancsra van szükség egy átlagos konfiguráció kialakításához? Lehetséges-e a hálózat több különböző forgalomirányítójához ugyanazt a konfigurációt használni?
- **Hatékonyság** - Mennyi sávszélességet igényel a forgalomirányító protokoll alapállapotban, illetve, amikor egy hálózati eseményre válaszolva konvergál?



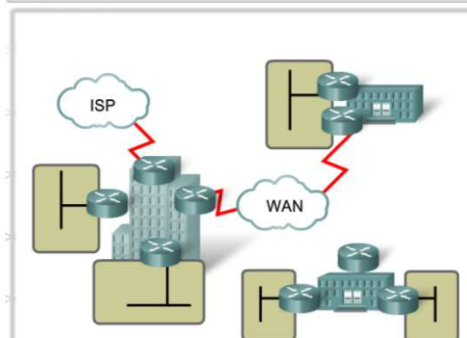
Kisvállalatok általában egyáltalán nem használnak forgalomirányítást, mivel legtöbbször csak az internetkapcsolathoz van szükségük forgalomirányításra.



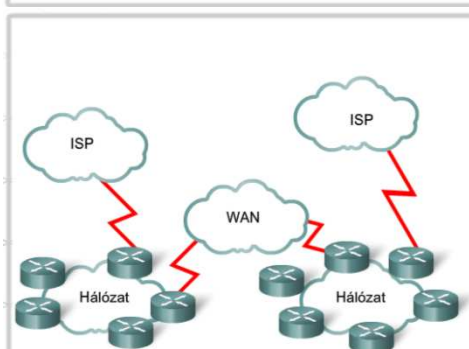
Kis- és középvállalat statikus útvonalat használhat. Ebben a példában, egy Linksys forgalomirányító és egy Cisco 1841-es ISR között van statikus útvonal.



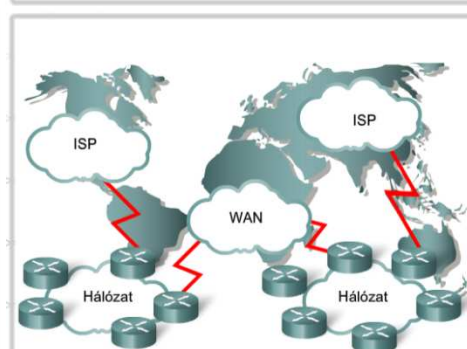
Az ábrán láthatóhoz hasonló közepes méretű vállalat esetében RIPv2 és néhány statikus útvonal beállítása jó választás lehet.



Nagyvállalatok EIGRP vagy OSPF protokollokat alkalmazhatnak.



Több gyártótól származó eszközökkel rendelkező óriás vállalatok OSPF-et alkalmaznak. Az EIGRP a Cisco saját fejlesztésű protokollja.



A multinacionális vállalatok alkalmazhatnak az ISP által használt forgalomirányítási megoldásokhoz hasonlókat.

6.1.5 A RIP konfigurálása és ellenőrzése

A RIP a legtöbb forgalomirányító által támogatott, népszerű távolságvektor alapú protokoll, amely megfelelő választás több forgalomirányítót tartalmazó kisebb hálózatok esetében. Konfigurálása előtt érdemes számba venni a forgalomirányító által kezelt hálózatokat, valamint a forgalomirányítónak az adott hálózatokhoz csatlakozó interfészeit.

Az ábrán három forgalomirányító látható, melyek mindegyike egy külön privát helyi hálózatot, azaz LAN-t kezel. A forgalomirányítók is külön hálózaton keresztül csatlakoznak egymáshoz, így a topológia összesen hat hálózatot tartalmaz.

Ebben a hálózati topológiában az R1 forgalomirányító alapesetben nem ismeri a 10.0.0.0/8 és 192.168.4.0/24 hálózatokhoz vezető útvonalat. Az R1 forgalomirányító csak a RIP megfelelő konfigurálását követően lesz képes elérni ezeket a hálózatokat, amikor az R2 és R3 elküldi neki a 10.0.0.0/8 és a 192.168.4.0/24 hálózatok elérhetőségét tartalmazó frissítéseket.

A RIP konfigurálása előtt az irányításban résztvevő minden fizikai interfészt engedélyeznünk kell, illetve IP-címet kell hozzájuk rendelnünk!

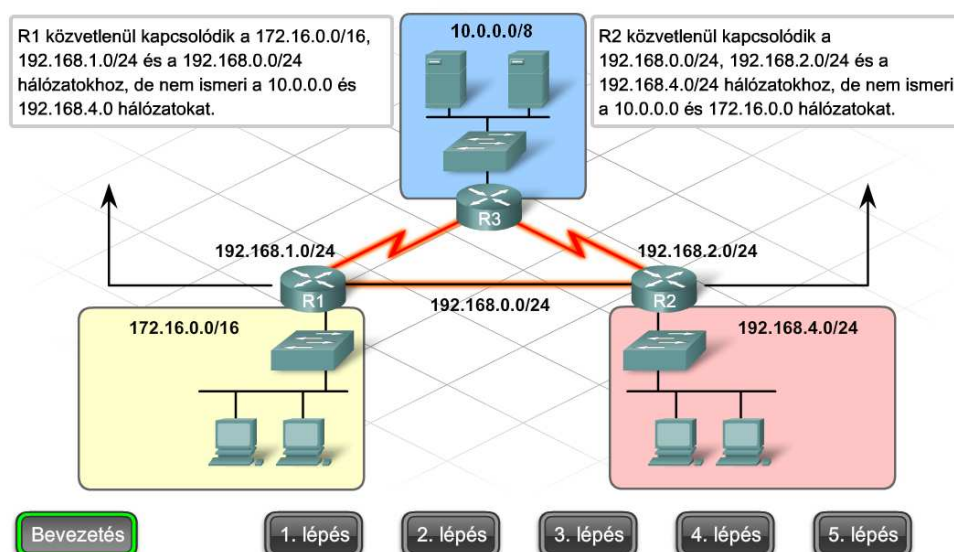
A RIPv2 konfiguráció három megjegyzendő utasítása:

*Router(config)#**router rip***

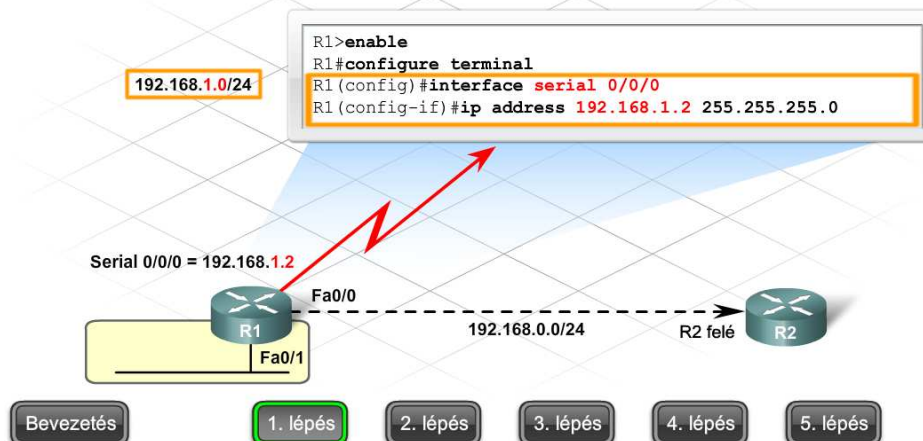
*Router(config-router)#**version 2***

*Router(config-router)#**network** [hálózatazonosító]*

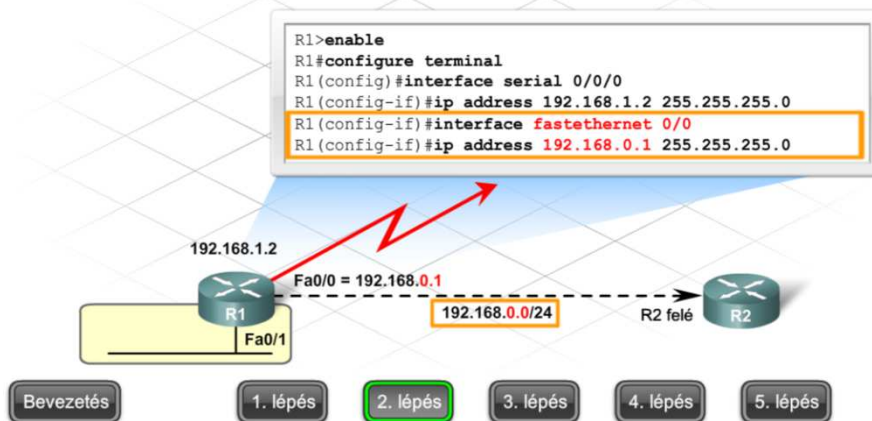
A forgalomirányítón a globális konfigurációs módban kiadott **router rip** paranccsal engedélyezhető a RIP forgalomirányítás. Az irányításban résztvevő hálózatok megadásához használjuk forgalomirányító konfigurációs módban a **network** parancsot! A forgalomirányítási folyamat a megadott hálózatazonosítók alapján azonosítja az interfészeket, és megkezdí rajtuk keresztül a RIP frissítések küldését és fogadását.



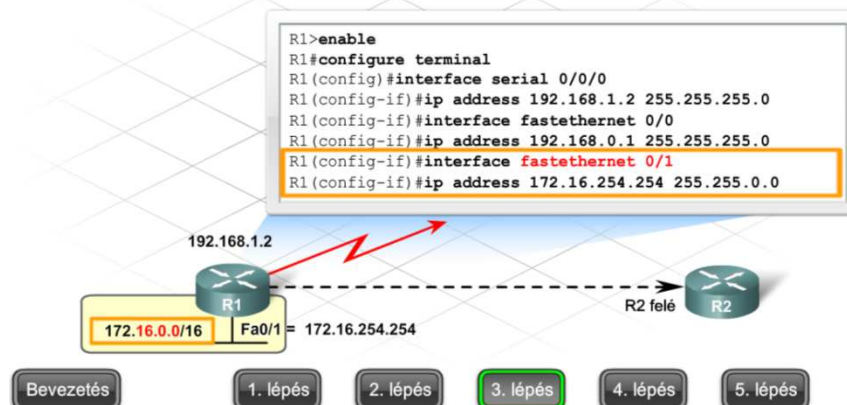
Az R1 forgalomirányítónak három interfészét kell konfigurálni. A Serial 0/0/0 az R3 forgalomirányítóhoz, a FastEthernet 0/0 az R2 forgalomirányítóhoz, és a FastEthernet 0/1 a 172.16.0.0/16 hálózathoz vezet. Először a Serial 0/0/0-t konfigurálja!

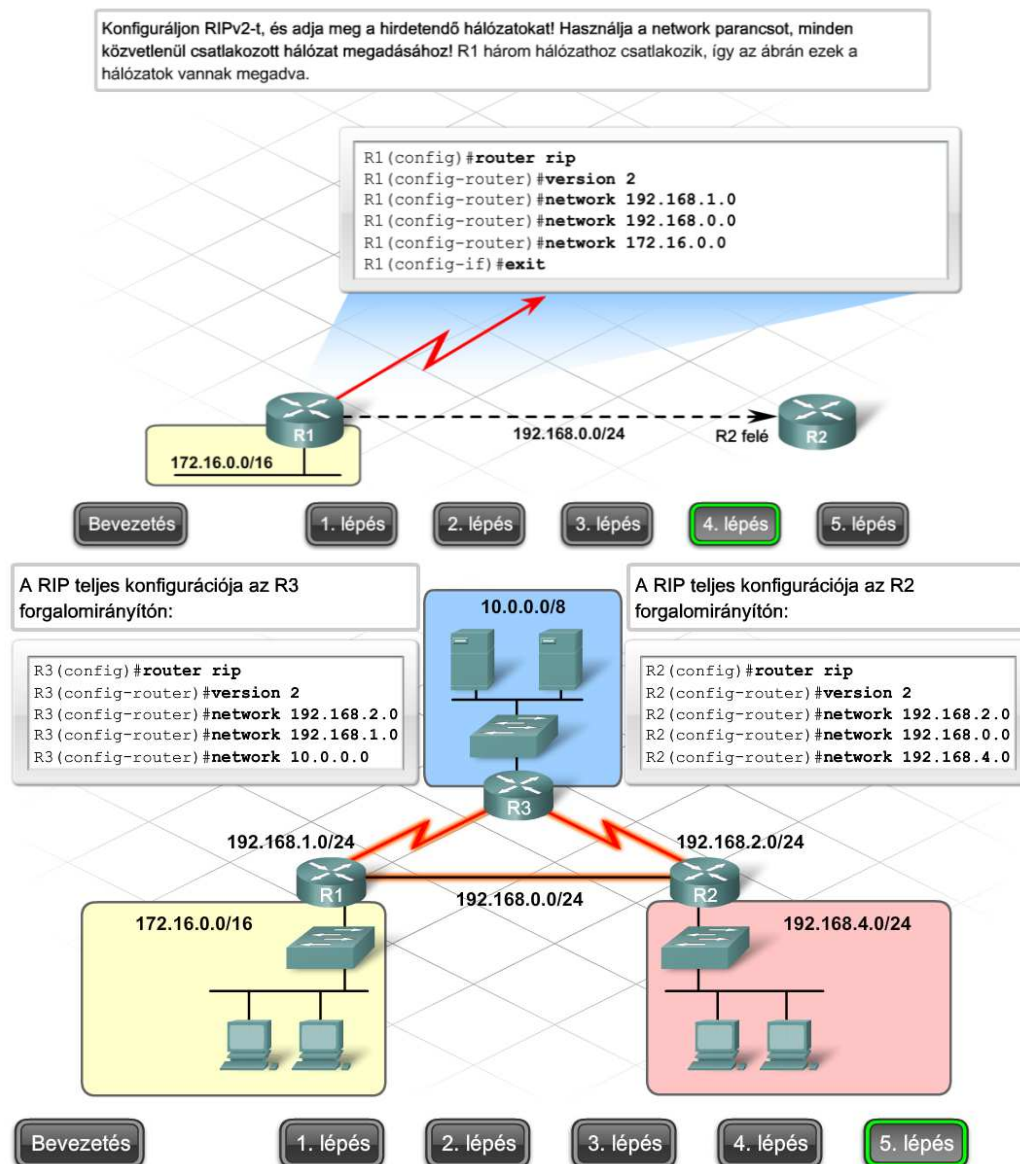


Mindhárom interfészhez rendeljen egy korábban nem használt IP-címet, az interfészhez csatlakozó hálózathoz! A FastEthernet0/0 az R2 felé vezet és a 192.168.0.0/24-es hálózathoz tartozik. Rendelje ehhez az interfészhez, a hálózat első használható IP-címét!



Konfigurálja az utolsó interfészt is az R1 forgalomirányítón!





A konfigurációt követően érdemes a hálózatazonosítókat és az interfészek IP-címeit ellenőrizni az aktív konfigurációs fájl és a pontos topológia-diagramm összehasonlításával. Ezt azért érdemes megszokni, mert könnyen követhetünk el adatbeviteli hibát.

Számos lehetőség van a RIP helyes működésének ellenőrzésére egy hálózatban. Az irányítás megfelelő működésének egyik ellenőrzési módja a távoli hálózat eszközeinek megpingelése. Sikeres ping esetén feltehetően a forgalomirányítás működik.

Másik módszer az IP forgalomirányítást ellenőrző **show ip protocols** és **show ip route** parancsok használata.

A **show ip protocols** paranccsal ellenőrizhető, hogy a RIP konfigurálva van, a megfelelő interfészek küldenek és fogadnak frissítéseket, és a forgalomirányító a megfelelő hálózatokat hirdeti.

A **show ip route** parancs megjeleníti az irányítótáblát, és így ellenőrizhető, hogy a RIP szomszédoktól kapott útvonalak bekerültek a forgalomirányító táblába.

A **debug ip rip** utasítás használható a küldött és fogadott frissítésekben hirdetett hálózatok megfigyelésére. A debug parancsok mindig valós időben jelenítik meg a forgalomirányító működését. Mivel a debug működése processzor erőforrásokat igényel a forgalomirányítón, így használata működő hálózatokban körültekintést igényel.

```
R1#show ip route
Codes: C - connected, R - RIP

R 10.0.0.0/8 [120/1] via 192.168.1.1, 00:00:17, Serial0/0/0
C 172.16.0.0/16 is directly connected, FastEthernet0/1

R 172.17.0.0/16 [120/1] via 192.168.0.2, 00:00:20, FastEthernet0/0
C 192.168.0.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/0
R 192.168.2.0/24 [120/1] via 192.168.0.2, 00:00:20, FastEthernet0/0
    [120/1] via 192.168.1.1, 00:00:17, Serial0/0/0
```

```
R1#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 23 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send 2, receive version 2
    Interface Send Recv Triggered RIP Key-chain
    FastEthernet0/0 2 2
    FastEthernet0/1 2 2
    Serial0/0/0 2 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.0.0
    192.168.1.0
  Routing Information Sources:
    Gateway Distance Last Update
  Distance: (default is 120)
```

```
R1#debug ip rip
RIP protocol debugging is on
R1#
*Sep 12 21:08:51.959: RIP: build update entries
*Sep 12 21:08:51.959: 192.168.1.0/24 via 0.0.0.0, metric 1, tag 0
*Sep 12 21:09:16.399: RIP: received v2 update from 172.16.1.2 on
Serial0/0/0
*Sep 12 21:09:16.399: 192.168.2.0/24 via 0.0.0.0 in 1 hops
*Sep 12 21:09:18.575: RIP: sending v2 update to 224.0.0.9 via
Serial0/0/0 (172.20.1.1)
```

6.2 Külső forgalomirányító rendszerek

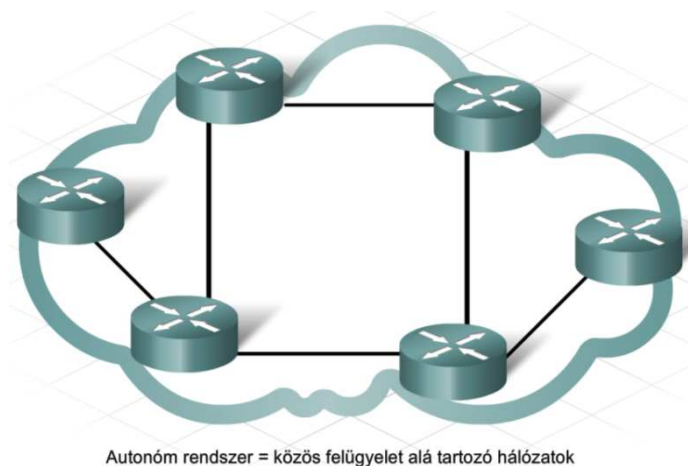
6.2.1 Autonóm rendszerek

Az internet forgalomirányítási architektúrája az évek során összekapcsolt hálózatok elosztott rendszerévé fejlődött. Az internet napjainkban olyan hatalmas és olyan sok hálózatot foglal magában, hogy egy szervezet önmagában képtelen a világ tetszőleges pontjának eléréséhez szükséges forgalomirányítási információk kezelésére.

Éppen ezért az internet olyan hálózatok, vagy más néven autonóm rendszerek (AS – Autonomous Systems) összessége, melyeket különböző szervezetek és vállalatok egymástól függetlenül felügyelnek.

Egy autonóm rendszer ugyanazon felügyelet alá tartozó és ugyanazokat a belső irányítási stratégiákat használó hálózatok együttese. Minden AS-t egyedi AS szám (ASN) azonosít, melyeket az interneten lehet regisztrálni és ellenőrizni.

Leggyakrabban egy autonóm rendszer egy internetszolgáltatót takar. A legtöbb vállalat internetszolgáltatón keresztül csatlakozik az internetre és így az adott szolgáltató irányítási tartományához tartozik. Az AS-t az internetszolgáltató felügyeli, és így nem csak saját útvonalait, hanem minden hozzá csatlakozó vállalat és más felhasználói hálózat útvonalait is kezeli.



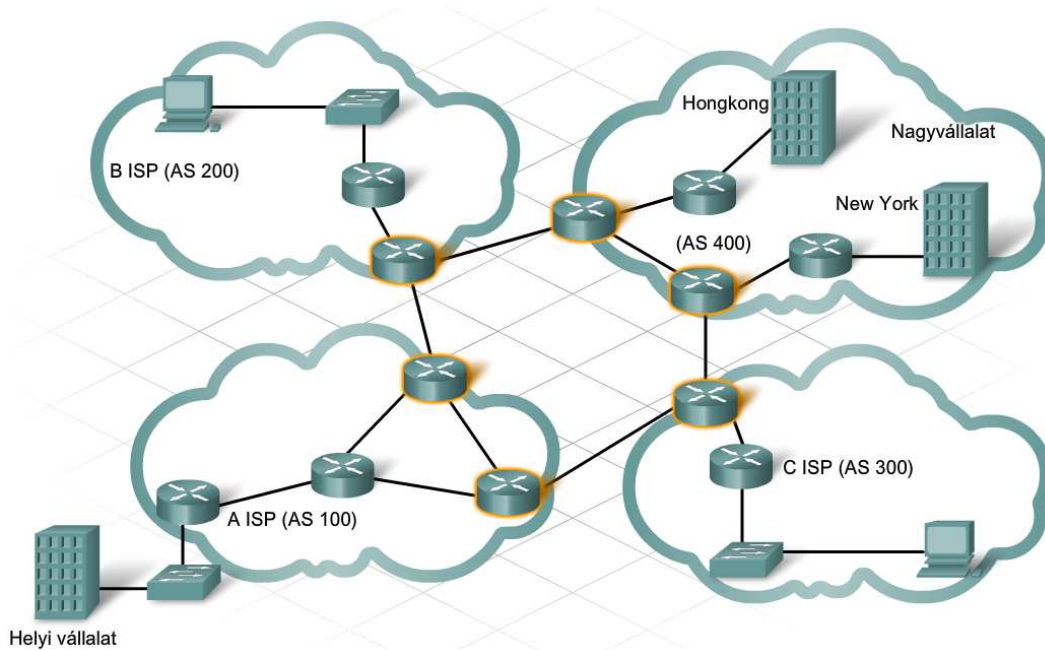
Egy autonóm rendszer irányítási tartományán belül minden hálózati eszközhöz ugyanaz az AS szám tartozik.

Az A ISP egy olyan autonóm rendszer, amelynek irányítási tartományához az ISP-hez közvetlenül csatlakozó helyi vállalat tartozik. A vállalat nem rendelkezik saját AS számmal, hanem az ISP AS számát használja (ASN 100).

Az ábrán látható továbbá egy Hong Kong-ban és New York-ban központi irodával rendelkező nagyvállalat is. Mivel az irodák különböző országokban vannak, így mindkettőnek a helyi ISP szolgáltatója az internetet, azaz a vállalat két ISP-hez is csatlakozik. Ebben az esetben a vállalat melyik AS-hez tartozik, és melyik AS számot használja?

Mivel a vállalat a B és a C ISP-n keresztül is kommunikál, az összeköttetések tekintetében irányítási problémák adódhatnak. Az internet felől érkező forgalom esetében nem egyértelmű, hogy melyik

autonóm rendszeren keresztül érhető el a vállalat. A probléma megoldásaként a vállalat önálló AS-ként regisztrálja magát és a 400-as AS számot használja.



6.2.2 Interneten keresztüli forgalomirányítás

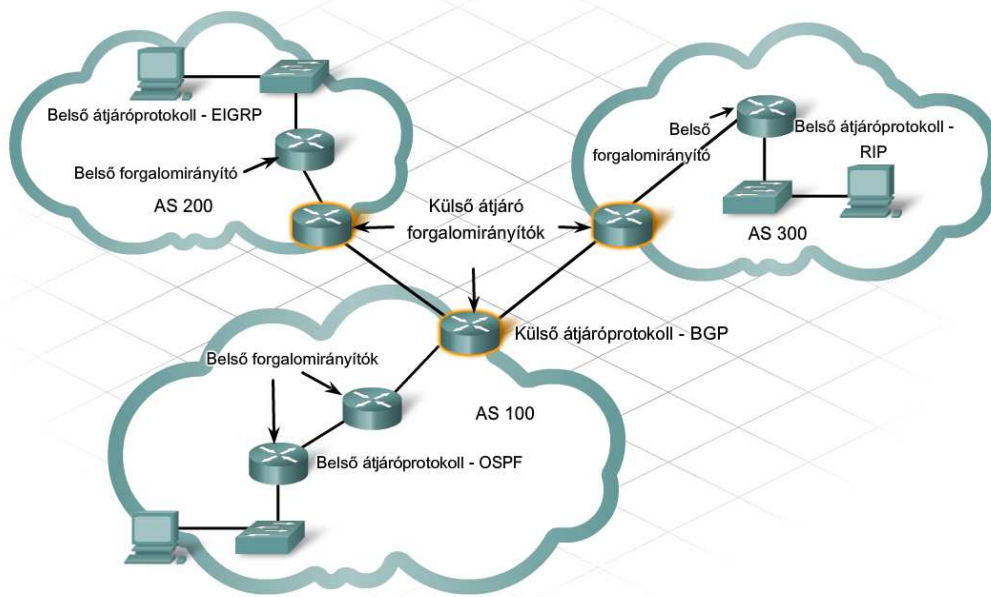
Egy autonóm rendszeren vagy önálló szervezeten belüli forgalomirányítási információk cseréjére belső átjáróprotokollok (IGP – Interior Gateway Protocol) szolgálnak. Feladatuk a belső hálózaton keresztüli legjobb útvonal megkeresése. Az IGP-k egy szervezet belső forgalomirányítóin futnak. Ilyen IGP például a RIP, az EIGRP és az OSPF.

Ezzel szemben egy külső átjáróprotokoll (EGP – Exterior Gateway Protocol) különböző autonóm rendszerek közötti irányítási információk cseréjére alkalmas. Mivel az AS-ek különböző felügyelet alá tartoznak, és eltérő belső protokollokat használhatnak, így a különféle rendszerek közötti kommunikációhoz külön protokollra van szükség. Az EGP egyfajta fordítási feladatot lát el annak érdekében, hogy a külső irányítási információk megfelelően értelmezve jussanak el minden AS belső hálózatához.

A külső átjáróprotokollok az AS határán elhelyezkedő úgynevezett külső (exterior) forgalomirányítókon futnak, melyeket határátjáróknak vagy határ-forgalomirányítóknak is neveznek.

Míg a belső forgalomirányítók IGP-k segítségével egyedi útvonalinformációkat cserélnek egymással, addig a külső forgalomirányítók közötti adatcsere a hálózatok külső protokollok segítségével történő elérhetőségéről szól. A külső forgalomirányító protokollok az interneten keresztüli legjobb útvonalat autonóm rendszerek sorozataként adják meg.

Napjainkban az internet legelterjedtebb külső forgalomirányító protokollja a határátjáró-protokoll (BGP – Border Gateway Protocol). Becslések szerint az autonóm rendszerek 95%-a ezt használja. A BGP legújabb verziója a BGP-4, melynek legfrissebb leírása az RFC 4271 dokumentumban található.

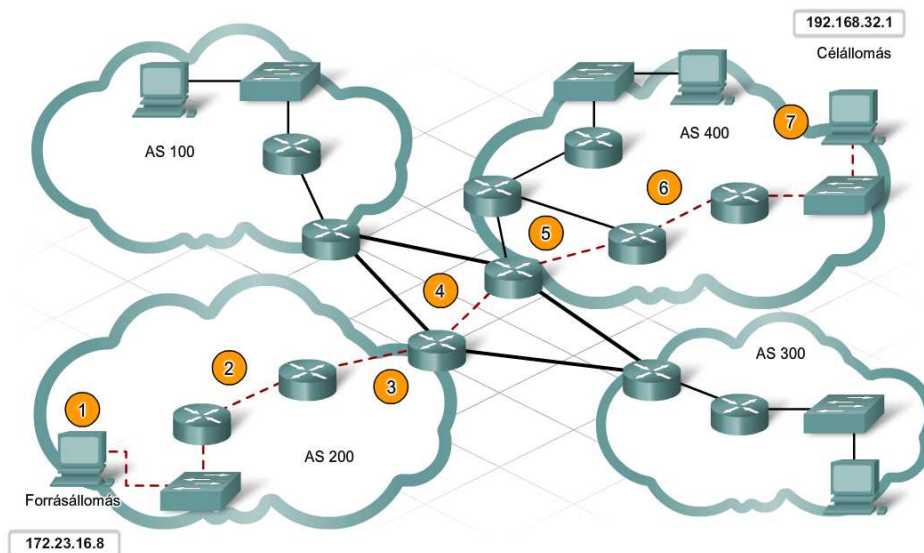


Minden autonóm rendszer felelős azért, hogy a rajta keresztül elérhető hálózatokról informálja a többi autonóm rendszert. Ezeknek az úgynevezett elérhetőségi információknak a cseréje speciális határátjárókon futó külső forgalomirányító protokollok segítségével történik.

A csomagok továbbítása az interneten a következő lépésekben történik:

1. A forrásállomás csomagot küld egy másik AS-ben lévő távoli állomásnak.
2. Mivel a csomagban szereplő cél IP-cím nem egy helyi hálózatra mutat, így a belső forgalomirányítók a csomagot az alapértelmezett útvonalaik alapján továbbítják mindaddig, míg az a helyi autonóm rendszer határán lévő külső forgalomirányítóhoz nem ér.
3. A külső forgalomirányító minden hozzá csatlakozó autonóm rendszert nyilvántart az adatbázisában. Ebből az úgynevezett elérhetőségi adatbázisból tudja a forgalomirányító, hogy a célhálózathoz vezető út számos autonóm rendszeren keresztül vezet, és az útvonal következő ugrása egy szomszédos autonóm rendszer közvetlenül csatlakozó külső forgalomirányítója.
4. A külső forgalomirányító a csomagot az útvonal következő ugrásához irányítja, ami egy szomszédos autonóm rendszer külső forgalomirányítója.
5. A szomszédos autonóm rendszer külső forgalomirányítója a saját elérhetőségi adatbázisa alapján továbbítja a csomagot az útvonal következő ugrásához.
6. A folyamat mindaddig folytatódik az autonóm rendszereken keresztül, amíg a cél autonóm rendszer külső forgalomirányítója a csomagban szereplő cél IP-címet fel nem ismeri, mint az egyik hozzá kapcsolódó belső hálózat címét.

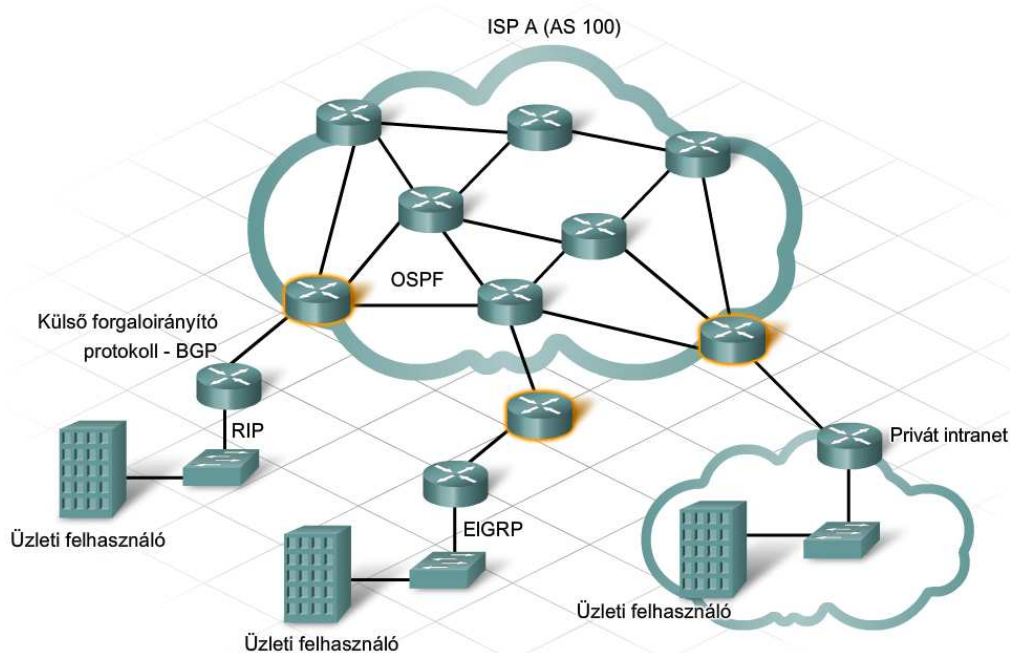
Az útvonal utolsó külső forgalomirányítója a forgalomirányító táblája alapján a következő belső forgalomirányítóhoz továbbítja a csomagot. Innentől kezdve a csomagot ugyanúgy kezeli a hálózat, mint bármilyen más helyi csomagot, és belső forgalomirányító protokollok segítségével halad a belső forgalomirányítókön keresztül a célállomásig.



6.2.3 Külső forgalomirányító protokollok és az ISP

A külső forgalomirányító protokollok (EGP) számos fontos szolgáltatást biztosítanak az ISP számára, mellyel lehetővé teszik például a forgalom távoli célhoz való eljuttatását az interneten keresztül. Továbbá olyan megoldásokat is nyújtanak, amelyekkel egy ISP képes házirendek és előnyben részesített helyi paraméterek beállítására és érvényesítésére annak érdekében, hogy az ISP forgalma hatékony legyen, és egyetlen belső forgalomirányítót se terheljen túl az átmenő forgalom.

Az üzleti felhasználók ragaszkodnak internetszolgáltatásuk megbízhatóságához, így számukra az internetszolgáltatóknak mindig elérhető internetkapcsolatot kell biztosítaniuk. Ennek érdekében tartalék útvonalakat és forgalomirányítókat alkalmaznak az esetleg kieső elsődleges útvonalak pótlására. A hálózat rendes működésekor az ISP-k az állandó útvonalakat hirdetik a többi autonóm rendszer felé. Ezek kiesésekor az ISP egy külső protokollfrissítő üzenetet küld, melyben a tartalék útvonalat hirdeti.

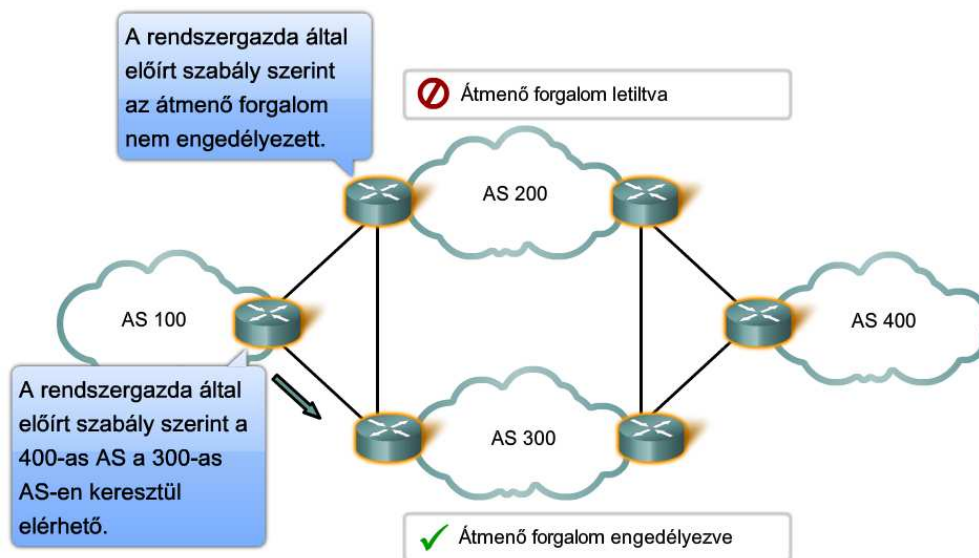


Az interneten küldött üzenetek folyamatát forgalomnak nevezzük, és két csoportba sorolhatjuk:

- Helyi forgalom - Egy autonóm rendszeren belüli forgalom, amely vagy az adott autonóm rendszerben keletkezett, vagy a célállomás az adott autonóm rendszerben található. Hasonló az utcai helyi forgalomhoz.
- Átmenő forgalom - Az adott autonóm rendszeren kívül keletkezett forgalom, ami az autonóm rendszeren kívüli célállomás elérése érdekében halad át az adott autonóm rendszer belső hálózatán. Hasonló az utcai átmenő forgalomhoz.

Az autonóm rendszerek közötti forgalom általában gondosan ellenőrzött forgalom. Biztonsági okokból vagy a túlterhelés elkerülése érdekében fontos az ilyen típusú forgalom korlátozása vagy adott esetben letiltása.

Számos autonóm rendszer hálózati rendszergazdája dönt úgy, hogy nem engedélyezi az átmenő forgalmat. Az átmenő forgalom a nagyobb terhelésre nem alkalmas forgalomirányítók túlterheléséhez és kieséséhez vezethet.



6.2.4 BGP konfigurálása és ellenőrzése

A szolgáltató által a felhasználóhoz kihelyezett forgalomirányítóban általában egy előre konfigurált statikus útvonal vezet az ISP hálózata felé. Bizonyos esetekben a szolgáltató akarhatja, hogy ez a forgalomirányító az autonóm rendszerének része legyen, és vegyen részt a BGP-ben, és így szükséges rajta a BGP engedélyezése.

A BGP engedélyezésének első lépése az AS szám konfigurálása, amire a következő parancs szolgál:

```
router bgp [AS_száma]
```

Ezt követően azonosítani kell azt az ISP forgalomirányítót, amelyik az előfizetői végberendezés (CPE - customer premises equipment) BGP szomszédja lesz, és amelyikkel információt cserél. A szomszédos forgalomirányító a következő paranccsal definiálható:

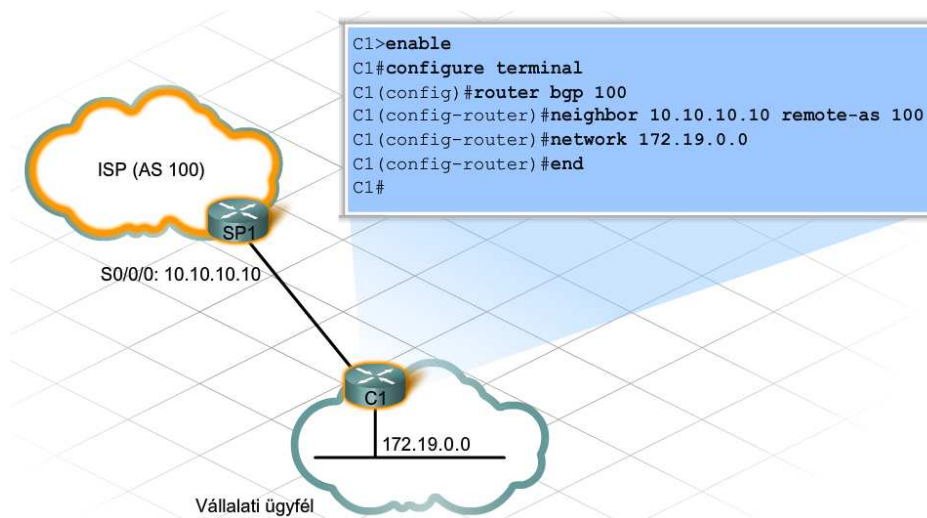
```
neighbor [IP-cím] remote_as [AS_száma]
```

Amennyiben egy ISP felhasználó saját regisztrált IP-címtartománnyal rendelkezik, akkor előfordulhat, hogy néhány belső hálózatának útvonalát szeretné nyilvánossá tenni az interneten. Ahhoz, hogy a BGP hirdesse a belső útvonalakat, a hálózati címeket kell megadni a következő paranccsal:

network [hálózati_cím]

A CPE installálása és a forgalomirányító protokollok konfigurálását követően a felhasználó helyi és internet kapcsolattal is rendelkezik, és képes teljes mértékben használni az ISP által nyújtott egyéb szolgáltatásokat.

A BGP forgalomirányításhoz használt IP-címek egyedi szervezeteket azonosító, hagyományosan regisztrált és irányítható címek. Nagy szervezetek esetében a BGP folyamat során privát címek is használhatók, de az interneten a BGP nem használható privát hálózati cím hirdetésére!



6.3 A fejezet összefoglalása

- A forgalomirányítást az üzenetek megfelelő célba juttatásához használják.
- A forgalomirányítás lehet dinamikus vagy statikus.
- Dinamikus forgalomirányítás esetén, a forgalomirányítók közti forgalomirányító információk cseréjéhez, forgalomirányító protokollokra van szükség. Dinamikus forgalomirányító protokollok például a távolságvektor alapú és kapcsolatállapot alapú forgalomirányító protokollok.
- A távolságvektor alapú forgalomirányító protokollok minden hálózathoz megadnak egy irányt és egy távolságot. A forgalomirányító táblákat és frissítéseket rendszeres időközönként elküldik a szomszédos forgalomirányítóknak.
- A kapcsolatállapot alapú protokollok, az összeköttetések állapotáról küldenek frissítéseket. Ezek a protokollok csökkentik a forgalomirányítási hurok kialakulásának valószínűségét, és kisebb hálózati forgalmat generálnak.
- Egy szervezet irányító protokolljának kiválasztásakor a legfontosabb szempontok a könnyű kezelhetőség, könnyű konfigurálás és hatékonyság.



- Az internet a hálózatok, más néven autonóm rendszerek, összessége.
- Egy autonóm rendszeren belül belső átjáró forgalomirányító protokollokat használnak, olyanokat mint például RIP, EIGRP és OSPF.
- Autonóm rendszerek között külső átjáró protokollok (EGP – Exterior Gateway Protocol) szükségesek. Ezek egy AS határán található külső, vagy más néven, határ-forgalomirányítókon futnak. A leggyakoribb külső forgalomirányító protokoll, a határatjáró-protokoll (BGP – Border Gateway Protocol).
- A BGP, egy távolságvektor alapú protokollhoz hasonlóan működik. Adatbázisában a célhálózatra vonatkozóan egy irány és egy távolság található.
- A külső protokollok lehetővé teszik a forgalom távoli célhoz való eljuttatását az interneten keresztül.
- A külső protokollok olyan szolgáltatásokat biztosítanak, melyekkel egy ISP képes házirendek és előnybe részesített paraméterek beállítására és érvényesítésére, a forgalom hatékonysága érdekében.

7. ISP szolgáltatások

7.1 Az ISP szolgáltatások bevezetése

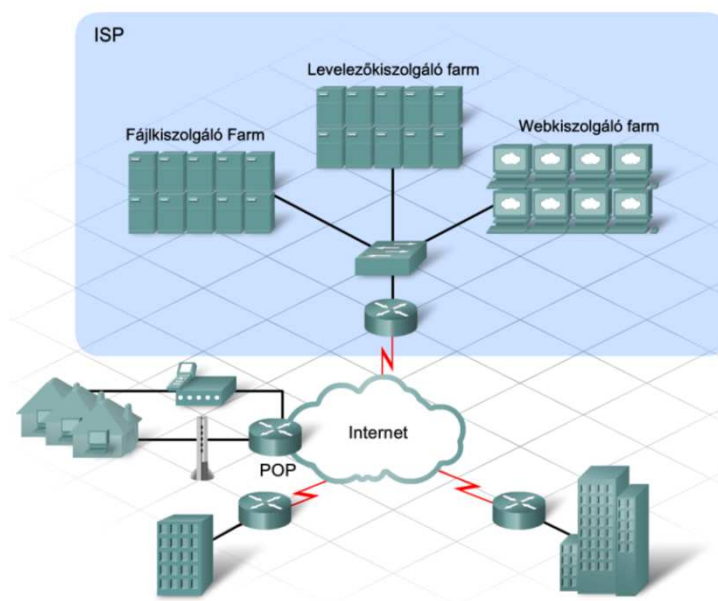
7.1.1 Felhasználói követelmények

Miután sikerült az ISP-vel kapcsolatba lépni, az egyéni felhasználónak vagy a vállalatnak el kell döntenie, milyen szolgáltatásokat igényelnek a szolgáltatótól.

Az internetszolgáltatók számos piacot szolgálnak. Az otthoni felhasználók alkotják a felhasználói piacot. Hatalmas multinacionális vállalatok képezik a vállalati piacot. Ezeken felül léteznek még olyan kisebb piacok, mint a kis- és középvállalatok, vagy nagyobb nonprofit szervezetek. Mindegyik, más és más szolgáltatás igényekkel rendelkezik.

A felhasználók növekvő igényei és az erősödő piaci verseny hatására az internetszolgáltatóknak újabb és újabb szolgáltatásokat kell nyújtani, amelyek lehetővé teszik, hogy bevételüket növelve megkülönböztethessék magukat versenytársaiktól.

Az elektronikus levelezés, a weboldalak tárolása, az adatfolyamok továbbítása, az IP telefonia és a fájlátvitel mind olyan fontos szolgáltatás, amit a szolgáltatók minden felhasználónak rendelkezésére bocsátanak. Ezek a szolgáltatások elengedhetetlenek az ISP felhasználói, valamint az olyan kis- és középvállalatok számára, amelyek nem rendelkeznek saját szakemberekkel e feladatok biztosítására.



Nagyon sok szervezet, kis és nagyvállalat, túl drágának tartja a legújabb technológiák beszerzését, vagy egyszerűen csak saját üzleti tevékenységi körükre szeretnék erőforrásaikat fordítani. Az ISP-k az ilyen szervezeteknek felügyelt szolgáltatásokat nyújtanak, amelyekkel a legújabb technológiákat és alkalmazásokat anélkül használhatják, hogy nagyobb összegeket fektetnének be akár a felszerelésbe, akár a szakértői támogatásba.

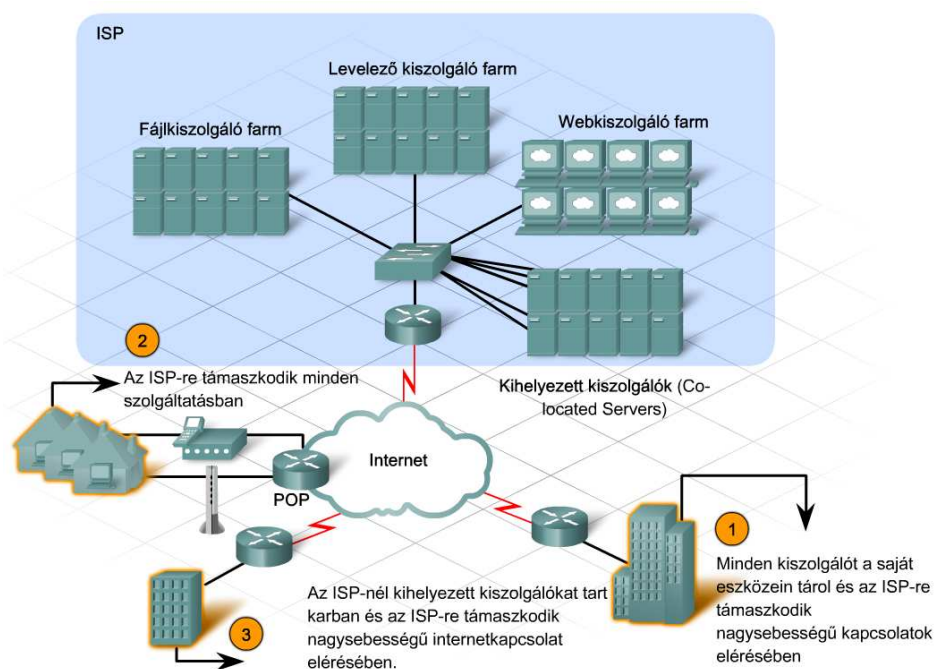
Amikor egy vállalat egy ilyen felügyelt szolgáltatásra előfizet, akkor a szolgáltató biztosítja az eszközöket és az alkalmazást a szolgáltatói szerződésnek (SLA – Service Level Agreement) megfelelően. Bizonyos felügyelt szolgáltatások esetén az alkalmazást magát is a szolgáltatói oldalon, nem pedig a felhasználói berendezéseken tárolják.

A következő három eset különböző felhasználói kapcsolatokat mutat:

1. eset - A felhasználó tulajdonában van és ő felügyeli a saját hálózati eszközeit és a szolgáltatásokat. Ezek a felhasználók csak a megbízható internet kapcsolatot várják az internetszolgáltatótól.

2. eset - Az ISP szolgáltatja az internet kapcsolatot, és tartja karban a felhasználói oldalon telepített hálózati eszközöket. Az ISP felelőssége kiterjed a telepítésre, az eszközök karbantartására és adminisztrációjára. A felhasználó kötelessége a hálózat és az alkalmazások állapotának megfigyelése, és fogadni a hálózat teljesítményére vonatkozó rendszeres jelentéseket.

3. eset - A felhasználó tulajdonában vannak a hálózati eszközök, de a kiszolgálók, melyeken az alkalmazások futnak az internetszolgáltatónál találhatók meg. A kiszolgálók lehetnek akár a felhasználó, akár az ISP tulajdonában, de mindkét esetben az ISP tartja karban a kiszolgálókat és az alkalmazásokat is. A kiszolgálókat általában a kiszolgálófarmon, az ISP hálózat üzemeltető központjában (NOC – Network Operations Center) helyezik el.



7.1.2 Megbízhatóság és elérhetőség

Egy új szolgáltatás bevezetése kihívást jelenthet. Egyrészt az internetszolgáltatóknak meg kell érteniük a felhasználói igényeket, másrészt rendelkezniük kell az adott szolgáltatásnak megfelelő erőforrásokkal és képességekkel. Mióta az internet alkalmazások egyre összetettebbek, egyre többen hagyatkoznak az ISP által felügyelt szolgáltatásokra.

Az ISP-k bizonyos díj ellenében a szolgáltatói szerződésben (SLA) meghatározott szintű szolgáltatást nyújtanak. A felhasználó követelményeinek megfelelően a biztosított szolgáltatásnak elérhetőnek és megbízhatóknak kell lennie.

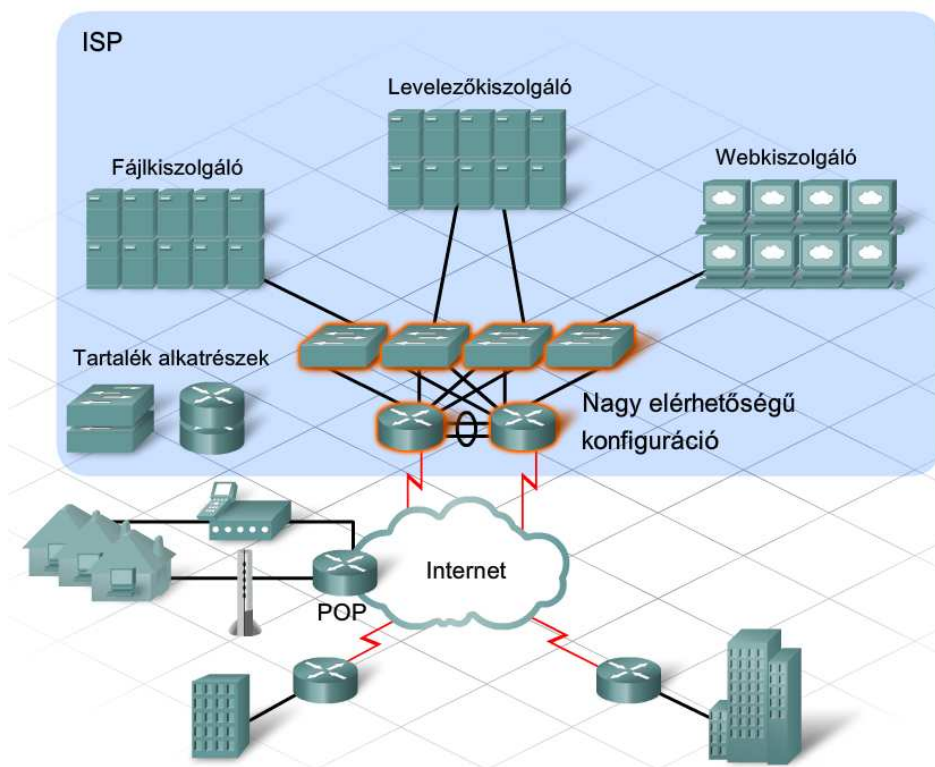
Megbízhatóság

A megbízhatóságnak két mértéke van: a meghibásodások közötti átlagos idő (MTBF – mean time between failure) és a működőképesség helyreállításához szükséges átlagos idő (MTTR – mean time to repair). Az eszközök gyártói a gyártás során végzett tesztek alapján megadják a várható meghibásodási időt (MTBF). Egy eszköz robusztusságának mértékét a hibatűrése adja meg. Minél hosszabb a várható meghibásodási idő (MTBF), annál nagyobb a hibatűrése. A helyreállításához szükséges időt a garancia vagy szolgáltatói egyezmény szabja meg.

Egy eszköz meghibásodása miatt bekövetkező hálózat- vagy szolgáltatáskiesés befolyásolhatja az internetszolgáltatót a szolgáltatói szerződésben (SLA) foglaltak betartásában. Ennek megelőzésére az ISP a kritikus hardverelemekre költséges szolgáltatói egyezményeket köthet a gyártókkal vagy az eladókkal a gyors hibaelhárításra. Az ISP választhatja azt a megoldást is, hogy tartalék hardverelemeket vásárol és saját telephelyén tárolja.

Elérhetőség

Az elérhetőséget általában az erőforrás üzemidejének és rendelkezésre állásának időarányaként adjuk meg százalékos formában. A tökéletes elérhetőséget a 100% jelenti, amikor a rendszer mindig működik és elérhető. A hagyományoknak megfelelően a telefonszolgáltatásoknál 99.999%-os elérhetőség az elvárás. Ez az ún. "5 kilences elérhetőség". Ilyenkor csak az üzemidő nagyon kis százalékában (0,001%) lehet a hálózat elérhetetlen. Mivel az internetszolgáltatók kritikus üzleti szolgáltatásokat is támogatnak, mint például az IP telefónia vagy nagy mennyiségű kereskedői tranzakció, így felhasználóik magasabb szintű elvárásainak is meg kell felelniük. Az internetszolgáltatók az elérhetőséget a hálózati eszközök és kiszolgálók megduplázásával, valamint nagy rendelkezésre állást biztosító technológiák alkalmazásával érik el. Redundáns konfiguráció esetén, ha egy eszköz kiesik, akkor a másik automatikusan átveheti a szerepét.



7.2 Az ISP szolgáltatásokat támogató protokollok

7.2.1 A TCP/IP protokollkészlet áttekintése

Ma az ISP-k ügyfelei mobiltelefonon néznek tv-t, PC-n telefonálnak és televízión játszanak interaktív játékokat. A hálózati szolgáltatások egyre fejlettebbé válásával az internetszolgáltatóknak lépést kell tartani, hogy kielégíthessék felhasználóik igényeit. Az ún. "konvergált IP hálózatok" kifejlesztése teszi lehetővé, hogy az összes szolgáltatás egyetlen közös hálózaton legyen elérhető.

Több TCP/IP-n alapuló végfelhasználói alkalmazás támogatásához az internetszolgáltatók ügyfélszolgálatát ellátó személyzetnek is tisztában kell lennie a protokollkészlet működésével.

Az ISP szervereinek számtalan alkalmazást kell szolgáltatniuk a különböző előfizetői igények kielégítésére. Ehhez szükség van a TCP/IP két szállítási rétegbeli protokolljára, a TCP-re és az UDP-re szolgáltatásaira. A szolgáltatók által biztosított közismert alkalmazások, mint például: webkiszolgálók és levelezői fiókok szintén a TCP/IP protokolljaira támaszkodva biztosítják a megbízható kézbesítést. Ezen felül minden IP szolgáltatás az ISP tartománynév kiszolgálóján alapszik, amely az IP-címzési rendszer és a felhasználók által használt URL-ek közötti kapcsolatot biztosítja.

Az ügyfelek és a kiszolgálók meghatározott protokollokat használnak az információcserére. A TCP/IP protokolljai egy négyrétegű modell segítségével reprezentálhatók. Nagyon sok ISP nyújtotta szolgáltatás a TCP/IP rétegmodell alkalmazási és szállítási rétegének protokolljaira támaszkodik.

Alkalmazási rétegbeli protokollok

Alkalmazási réteg protokolljai határozzák meg a formátumot és szabályozzák a legismertebb internetes kommunikációs folyamatokhoz szükséges információt. Ilyen protokollok:

- Tartománynév rendszer (DNS – Domain Name System) - internet neveket feloldja IP címekre.
- Hiperszöveg átviteli protokoll (HTTP - HyperText Transfer Protocol) – A világháló weboldalait képező fájlok átvitelét valósítja meg.
- Egyszerű levéltovábbító protokoll (SMTP - Simple Mail Transfer Protocol) – E-mailek és csatolt állományainak átvitelére szolgál.
- Telnet - Terminál-emulációs protokoll, mely hálózati eszközök és kiszolgálók távoli elérését biztosítja.
- Fájltáviteli protokoll (FTP- File Transfer Protocol) - rendszerek közötti interaktív fájltávitelt valósít meg.

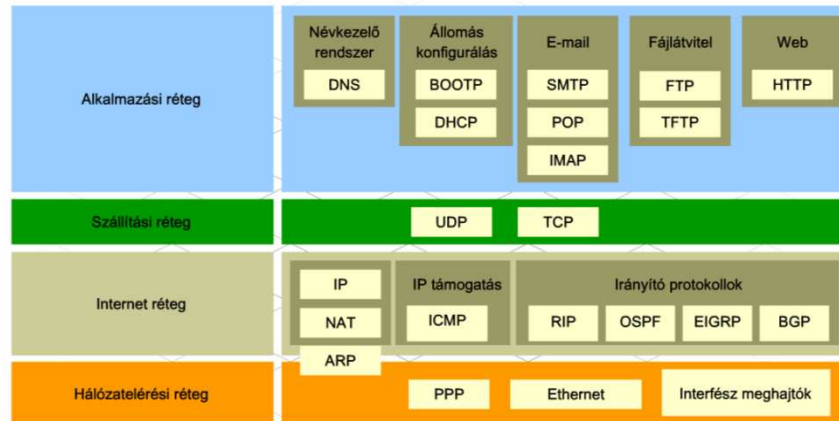
Szállítási rétegbeli protokollok

Különböző típusú adatoknak egyedi követelményeik lehetnek. Bizonyos alkalmazások esetén a kommunikációs adatszegmenseknek meghatározott sorrendben kell megérkezniük a megfelelő feldolgozás érdekében. Más esetben az összes adatnak meg kell érkeznie a felhasználás előtt. Az is előfordul, hogy az alkalmazás kis mennyiségű adatvesztésre nem reagál érzékenyen.

A modern konvergált hálózatokon a különböző alkalmazások jelentősen eltérő szállítási igényeik ellenére ugyanazon a hálózaton kommunikálhatnak. A különböző szállítási rétegbeli protokollok különböző szabályokat használva biztosítják az eltérő követelményeket támaztó adatátviteli igények kielégítését.

Általában az alsóbb rétegek nem veszik észre, hogy több alkalmazás adatait küldik a hálózaton. Az ő felelősségük csak az, hogy az adatot eljuttassák az eszközhöz. A szállítási réteg feladata, hogy az adatot a megfelelő alkalmazáshoz juttassa.

A két legfőbb szállítási rétegbeli protokoll a TCP és az UDP.



A TCP/IP rétegmodell és az OSI modell hasonlóságokat és különbségeket is mutat.

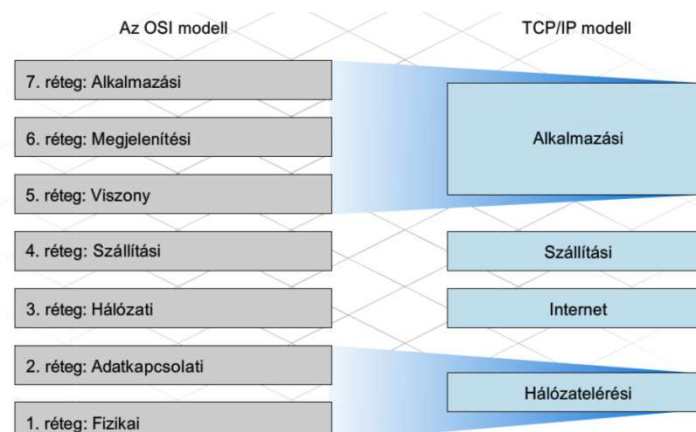
Hasonlóságok

- Mindkettő rétegek segítségével szemlélteti a protokollok és szolgáltatások együttműködését.
- A szállítási és hálózati rétegek megfeleltethetők egymásnak az egyes modellekben.
- Mindkettőt a hálózatok témakörében használják a protokollok együttműködésének bemutatására.

Különbségek

- Az OSI modell a TCP/IP modell alkalmazási rétegét három külön rétegre osztja. Ez a három legfelső réteg ugyanazt a feladatot látja el, mint a TCP/IP modell alkalmazási rétege.
- A TCP/IP nem határoz meg külön protokollokat a fizikai összekapcsolódáshoz. Az OSI modell két alsó rétege a fizikai hálózat elérésével és a helyi hálózatok állomásai közötti bitek küldésével foglalkozik.

A TCP/IP modell a ténylegesen kidolgozott protokollokra és szabványokra épül, míg az OSI modell inkább egy elméleti útmutató a protokollok együttműködéséhez



7.2.2 Szállítás réteg protokollok

Különböző alkalmazásoknak különböző szállítási igényeik vannak. Két szállítási rétegbeli protokoll létezik: TCP és UDP

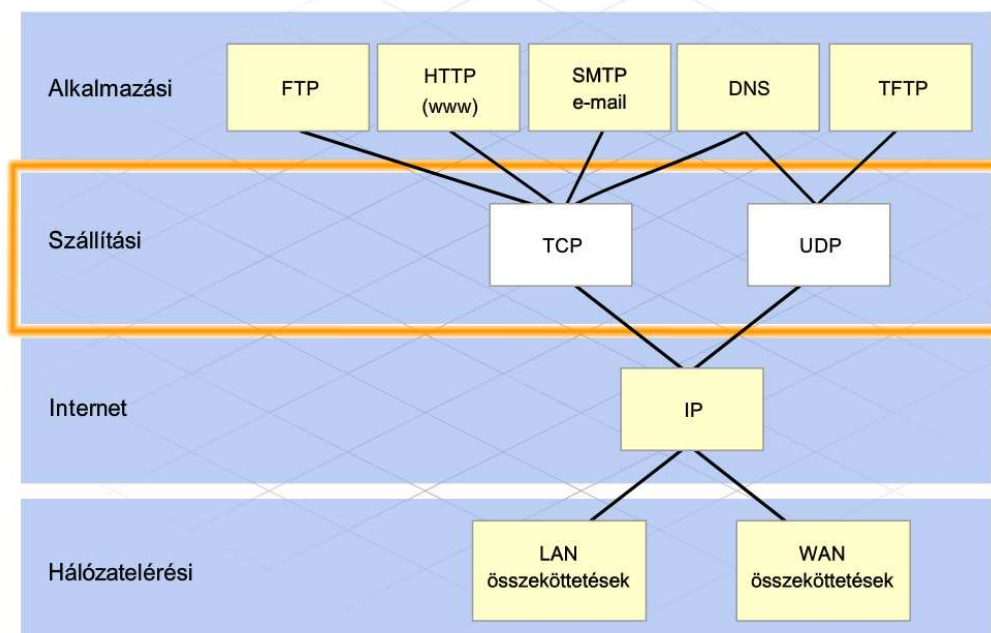
TCP

A TCP egy megbízható, garantált átvitelt biztosító protokoll. A TCP meghatározza az állomások által használt csomagnyugtázási módszert, és arra készíti a forrás állomást, hogy újraküldje a nem nyugtázott csomagokat. Irányítja az üzenetek cseréjét a forrás és célállomás között, amellyel kommunikációs viszonyt alakít ki köztük. A TCP-t gyakran egy csőhöz, vagy állandó kapcsolathoz hasonlítják, ezért is nevezik összeköttetés alapú protokollnak.

A TCP többletterheléssel jár, mind a sávszélesség, mind a feldolgozási idő tekintetében az egyes viszonyok nyomonkövetése, valamint a forrás és célállomás közötti nyugtázási és újraküldési mechanizmusok megvalósítása miatt. Bizonyos esetekben e többletterhelés okozta késleltetés már nem elfogadható az alkalmazások számára. Az ilyen alkalmazások számára az UDP jobb megoldást jelent.

UDP

Az UDP egy nagyon egyszerű összeköttetésmentes protokoll, mely kevés többletterhelést biztosító adatküldést nyújt. Az UDP-t „legjobb szándékú” szállítási rétegbeli protokollnak tartják, mert nem biztosít hibaellenőrzést, garantált adatkézbítésítést, vagy adatfolyam-vezérlést. Mivel az UDP egy legjobb szándékú protokoll, így az UDP adataegységek elveszhetnek az út folyamán vagy esetleg nem a megfelelő sorrendben érkeznek meg a célállomáshoz. Azok az alkalmazások, melyek UDP-t használnak, a kis mennyiségű adatvesztésre nem reagálnak érzékenyen. Ilyen alkalmazás például az internet rádió. Ha egy adataegység nem érkezik meg, annak csak kisebb hatása van a üzenetszórás minőségére.



Az olyan alkalmazások, mint az adatbázisok, weboldalak és az elektronikus levelezés minden adat eredeti sorrendben történő, hibátlan megérkezését igénylik. Minden hiányzó adat az üzenet feldolgozhatatlanságát eredményezheti, ezért ezek az alkalmazások megbízható szállítási rétegbeli protokollt használnak. Az a hálózati többletterhelés, amely ezt a megbízhatóságot lehetővé teszi, elfogadható árat jelent egy sikeres kommunikációért.

A szállítási rétegbeli protokollt az alkalmazás adattípusa határozza meg. Például egy elektronikus levél nyugtázott adatküldést igényel, így TCP-t használ. Egy levelező ügyfél, mely SMTP-t használ, az elektronikus üzenetet bájtfolyamként továbbítja a szállítási rétegnek. A szállítási rétegben a TCP feladata a folyam szegmensekre osztása.

Minden szegmensen belül a TCP minden egyes bájtot vagy oktetet egy sorszámmal azonosít. Az így kapott szegmenseket az internet réteg kapja meg, mely csomagba helyezi őket az adatküldéshez. Ez a folyamat a beágyazás. A célállomásnál ez a folyamat megfordul és a csomagot kicsomagolják. A beágyazott szegmensek a TCP folyamaton mennek keresztül, amely visszaalakítja a szegmenseket bájtfolyammá, és azt a levelező kiszolgálónak kézbesíti.

Egy TCP viszony használata előtt az összeköttetés felépítéséhez a forrás és célállomás üzenetet váltanak egymással. Ehhez egy háromlépéses folyamatot használnak.

Az első lépésben a forrásállomás küld egy szinkronizációs üzenetet (SYN – Synchronization Message) a TCP viszony felépítéséhez. Az üzenet két célt szolgál:

- Jelzi a forrásállomás szándékát a célállomással történő kapcsolat felépítéséről.
- Szinkronizálja a TCP sorszámokat a két állomás között, hogy a beszélgetés folyamán mindkét fél nyomkövethesse az elküldött és megérkezett szegmenseket.

A második lépésben a célállomás válaszol a SYN üzenetre egy szinkronizációs nyugtával (SYN-ACK).

Az utolsó lépésben a küldő állomás megkapja a SYN-ACK üzenetet és egy ACK üzenetet küld vissza a kapcsolatfelépítés befejezéséhez. Az adatok küldése most már megbízható módon történik.

Ezt a TCP folyamatok közötti háromlépéses metódust háromfázisú kézfogásnak nevezik.

Amikor egy állomás TCP protokollt használva küld egy üzenetszegmenst, akkor a TCP folyamat elindít egy időzítőt. Az időzítő elég időt hagy az üzenet kézbesítésére, valamint a nyugta visszaérkezésére. Ha a forrásállomás nem kapja meg a nyugtát a célállomástól az időzítő lejárt előtt, akkor a forrás az üzenetet elveszítettnek tekinti. Az üzenet nem nyugtázott részeit újraküldi a forrás.

A nyugtázás és újraküldés mechanizmusa mellett a TCP azt is meghatározza, hogyan történik az üzenet összeállítása a célállomásnál. Minden TCP szegmens tartalmaz egy sorszámot. A célállomásnál a TCP folyamat egy ideiglenes tárolóba rakja a megérkezett szegmenseket. A szegmensek sorszámának kiértékelése lehetőséget nyújt a TCP folyamat számára a hiányzó szegmensek meghatározására. Ha az adatok nem sorrendben érkeznek, a TCP újra tudja sorrendezni őket.

7.2.3 Különbségek a TCP és UDP között

Az UDP egy nagyon egyszerű protokoll. Mivel ez nem összeköttetés-alapú és nem használja a TCP kifinomult sorszámozási, újraküldési és adatfolyam szabályozási mechanizmusait, sokkal kisebb többletterheléssel jár.

Az UDP-re gyakran úgy hivatkoznak, mint nem megbízható szállítási protokoll, hiszen nincsen semmi garancia az üzenet megérkezésére. Ez persze nem jelenti azt, hogy az UDP-t használó alkalmazások megbízhatatlanok. Csak annyit jelent, hogy ezeket a funkciókat nem a szállítási réteg biztosítja, hanem szükség esetén valahol máshol kell implementálni.

Bár egy tipikus hálózat összes UDP forgalma relatív kicsi a többihez képest, a következő alkalmazási rétegbeli protokollok mind az UDP-t használják:

- Tartománynév rendszer (DNS - Domain Name System)
- Egyszerű hálózatfelügyeleti protokoll (SNMP - Simple Network Management Protocol)
- Dinamikus állomáskonfigurálási protokoll (DHCP - Dynamic Host Configuration Protocol)
- RIP irányító protokoll
- Triviális fájlátviteli protokoll (TFTP - Trivial File Transfer Protocol)
- On-line játékok

A TCP és UDP közti fő különbség a protokollok által megvalósított funkciókban és az ezzel együttjáró többletterhelésben van. A két protokoll fejrészének tanulmányozásával jól látható ez a különbség.

Minden TCP szegmens fejrészében 20 bájtnyi extra adat található az alkalmazási réteg adatai mellett. Ez az extra adat a hibaellenőrző mechanizmus eredménye.

Az UDP adategységeit datagramnak nevezik. Ezeket a datagramokat „legjobb szándékkal” továbbítják, összesen 8 bájtnyi extra információval kiegészítve.

TCP-szegmens

Bit (0)	Bit (15)	Bit (16)	Bit (31)
Forrásport (16)		Célport (16)	
Sorszám (32)			
Nyugta sorszám (32)			
Fejrész hossza (4)		Foglalt (6)	Kódolási bitek (6)
Ablak (16)			
Ellenőrző összeg (16)		Sürgős (16)	
Opciók (0 vagy 32, ha van)			
Alkalmazási rétegbeli adat (méret változó)			

↑

20 bájt

↓

UDP datagram

Bit (0)		Bit (15)	Bit (16)	Bit (31)	
Forrásport (16)			Célport (16)		
Hossz (16)			Ellenőrző összeg (16)		
Alkalmazási rétegbeli adat (méret változó)					

8 bájt

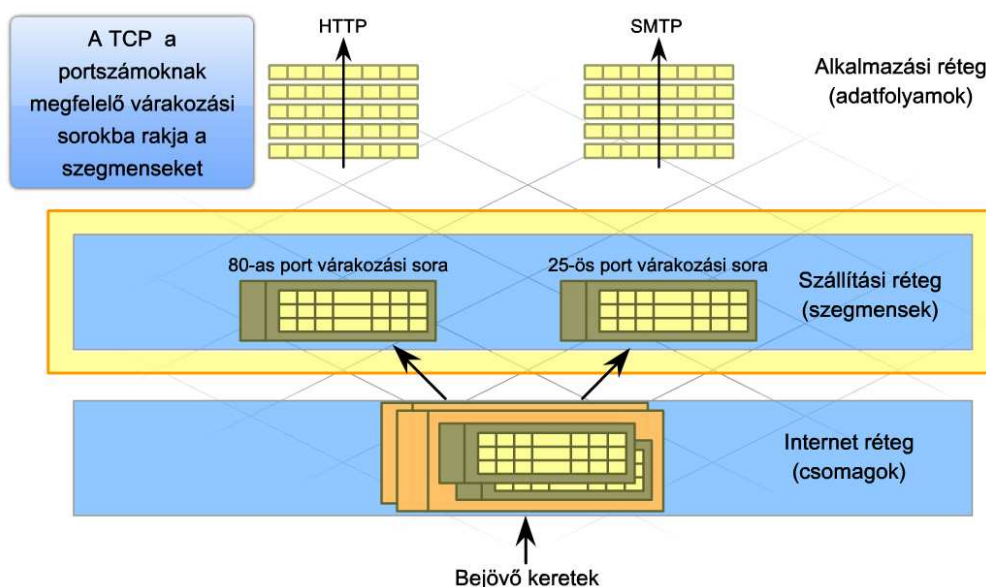
7.2.4 Több szolgáltatás támogatása

Több egyidejű kommunikációs folyamat kezelése a szállítási rétegben történik. A TCP és UDP szolgáltatások nyomonkövetik a különböző, hálózaton kommunikáló alkalmazásokat. Az alkalmazások adategységeinek a megkülönböztetésére, mind a TCP, mind az UDP fejrészében található olyan mezők, melyek azonosítják az alkalmazást.

A forrásport és célport minden szegmens vagy datagram fejrészében jelen van. Portszoamokat nagyon sokféleképp lehet alkalmazásokhoz rendelni, például attól függően is, hogy kérésről vagy válaszról van-e szó. Ha egy ügyfél állomás kérést küld egy kiszolgálónak, akkor a fejrészben megtalálható célport a kiszolgálón az alkalmazáshoz rendelt portszoam. Például, ha egy webböngésző kérést küld egy webkiszolgálónak, a kommunikáció TCP-vel történik a 80-as porton. Ez az alapértelmezett port webes alkalmazások esetén. Számos közismert alkalmazásnak vannak alapértelmezett port hozzárendeléseik. SMTP-t használó levelező kiszolgálók a TCP 25-ös portját használják.

Az alkalmazás-specifikus portokra érkező szegmenseket a TCP és az UDP is a megfelelő várakozási sorba rakja. Például, HTTP kérés esetén a webkiszolgálón a TCP folyamat a beérkező csomagokat a webkiszolgáló várósorába rakja. Ezek a szegmensek aztán, amilyen gyorsan csak lehet, a HTTP alkalmazáshoz kerülnek.

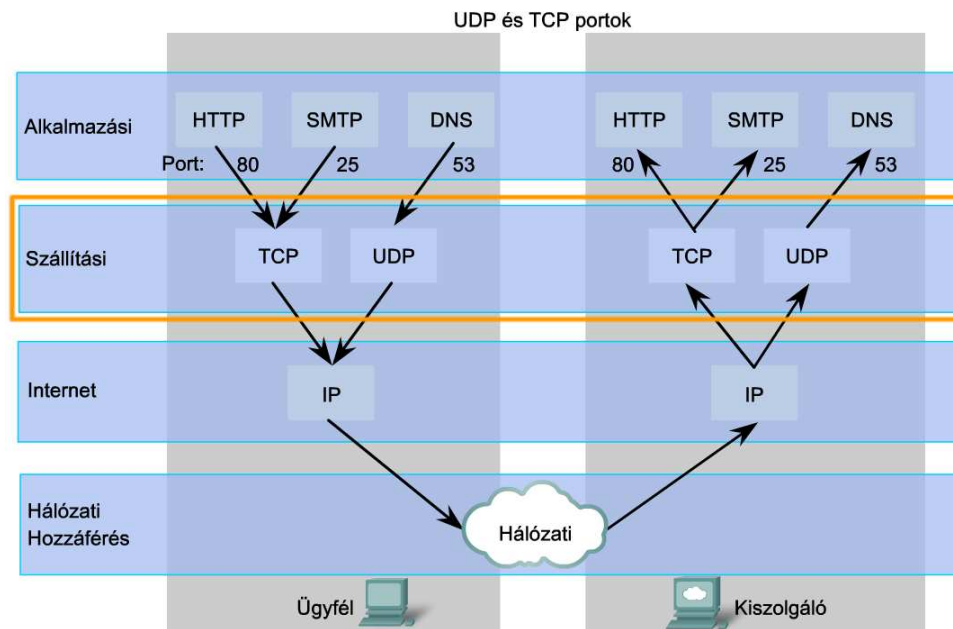
25-ös portot megjelölő szegmensek egy külön sorba, a levelező szolgáltatások sorába kerülnek. Így támogatják a szállítási rétegbeli protokollok az ISP kiszolgálókat több különböző alkalmazás és szolgáltatás egyidejű biztosításában.



Minden internetes alkalmazás esetén létezik egy forrásállomás és egy célállomás, általában egy ügyfél és egy kiszolgáló. A TCP folyamatok a küldő és fogadó állomáson némiképp különböznek. Az ügyfelek aktívak és kapcsolatot kérnek, míg a kiszolgálók passzívan viselkednek, figyelik és elfogadják a kapcsolatkérdéseket.

Kiszolgáló folyamatokhoz általában statikusan a jól ismert portokat rendelik 0-tól 1023-ig. A jól ismert portok segítik az ügyfél alkalmazásokat a helyes célport hozzárendelésében egy szolgáltatáskérés létrehozásakor.

Az ügyfeleknek a kérést indító ügyfél alkalmazás azonosításához is szükségük van egy portszámmra. A forrásportok hozzárendelése dinamikusan történik az 1024-től 65535-ig terjedő tartományból. Ez a porthozzárendelés a kérést indító alkalmazás címének felel meg. A szállítási rétegbeli protokollok nyomonkövetik a forrásportot és a kérést kezdeményező alkalmazást, így a válasz a megfelelő alkalmazásnak továbbítható.



A szállítási réteg portszámából és a hálózati réteg IP-címéből álló páros egy adott állomáson futó alkalmazás azonosít. A portszám - IP-cím együttest socket-nek nevezik. Egy forrás- és cél-oldali socket pár két állomás közötti párbeszéd egyedi azonosítójaként használható.

Egy ügyfél socket, 7151-es portszámmal például a következőképpen nézhet ki:

192.168.1.1:7151

Egy socket egy webkiszolgálón például:

10.10.10.101:80

Ezek együttesen egy socket párt alkotnak:

192.168.1.1:7151, 10.10.10.101:80

A socketek segítségével a kommunikációs végpontok ismertek, így az adatok eljuthatnak az egyik állomás alkalmazásától egy másik állomás alkalmazásáig. Ez teszi lehetővé egy ügyfél állomáson futó több alkalmazás, valamint egy kiszolgáló több kapcsolatának megkülönböztetését.

7.3 Tartománynév rendszer (DNS)

7.3.1 TCP/IP állomás név

A forrás és célállomás közti internetes kommunikációhoz mindkét állomásnak érvényes IP címre van szüksége. Az IP-címek, sőt az IP-címek ezrei azonban az emberek számára nehezen megjegyezhetők.

Az olyan könnyen olvasható tartománynevek, mint cisco.com az emberek számára sokkal használhatóbbak. A hálózati névfeloldó-rendszerek ezeknek a könnyen megjegyezhető neveknek a gépek számára feldolgozható, hálózati kommunikációhoz szükséges IP-címekre történő fordítását végzik.

Webböngészés, vagy elektronikus levelezés közben nap mint nap használjuk a névfeloldó rendszereket, anélkül, hogy tudnánk róla. A névfeloldó rendszerek rejtett, de szerves részét alkotják a hálózati kommunikációnak. Például a Cisco Systems weboldalának megtekintéséhez a böngésző címezőjébe a <http://www.cisco.com> címet kell beírni. A www.cisco.com egy hálózati név, mely egy meghatározott IP-címhez van rendelve. Ha a kiszolgáló IP címét íránk a böngésző címezőjébe, akkor ugyanazt a weboldalt látnánk.

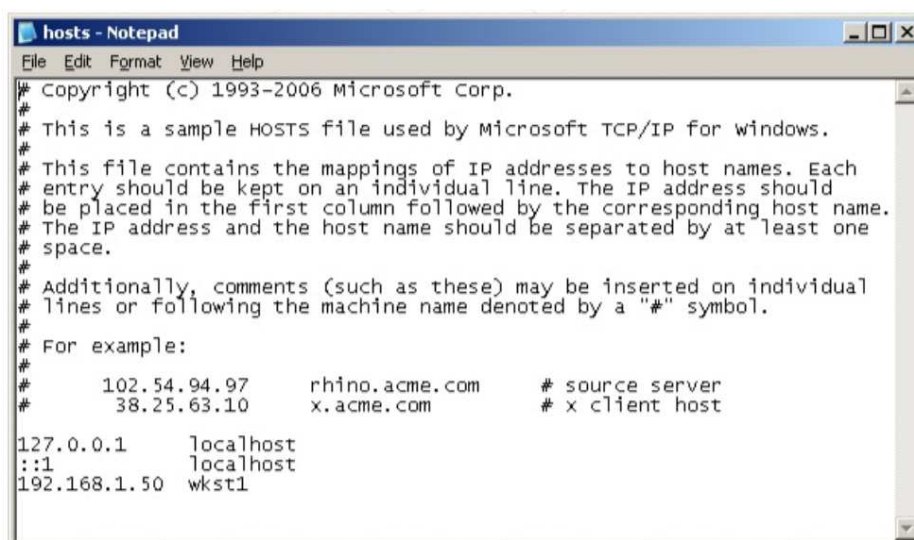
A hálózati névfeloldó-rendszerek az emberek számára fontos eszközök, melyek segítenek abban, hogy összetett IP-címek megjegyzése nélkül is elérhessük ugyanazokat az erőforrásokat.

Az internet első napjaiban az IP-címek és állomásnevek egy adminisztrációs kiszolgálón központilag tárolt HOSTS nevű állományban voltak megtalálhatók.

Ez a központi HOSTS állomány tartalmazta a korai internetre csatlakozott összes állomás nevének és IP-címének összerendelését. Mindenholnan elérhető volt az állomásnevek feloldása céljából. Az állomásnév megadása után a küldő állomás a letöltött HOSTS állományból kikereshette a célállomás IP-címét.

Eleinte a HOSTS állomány megfelelő volt az internet korlátozott számú számítógépei számára, azonban a hálózat növekedésével, a név-IP-cím hozzárendelést igénylő állomások száma nagyon megnőtt, ezáltal lehetetlenné vált a HOSTS frissítése. Új névfeloldó-rendszert kellett kifejleszteni. Ez a DNS, amely tartomány-nevek IP-címekre történő fordítására szolgál. A DNS kiszolgálók elosztott működéssel végzik a névfeloldást, központilag karbantartott HOSTS állományra már nincs szükség.

Ennek ellenére, ugyan csak virtuálisan, de minden állomás karbantart egy HOSTS állományt, amit a TCP/IP elindulásakor hoznak létre. A névfeloldási folyamat részeként a DNS szolgáltatás kérés előtt a helyi HOSTS fájl átvizsgálása történik. Ez a fájl használható hibakereséskor, vagy a DNS kiszolgálón található bejegyzések törlésekor.



```
# Copyright (c) 1993-2006 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a "#" symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com   # source server
#       38.25.63.10      x.acme.com       # x client host

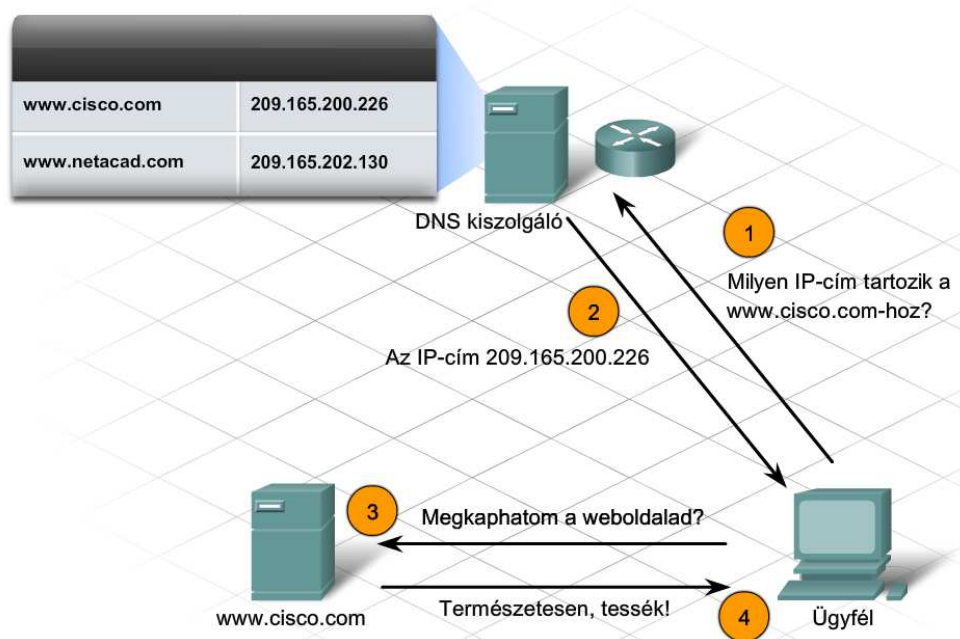
127.0.0.1    localhost
:::1        localhost
192.168.1.50 wkst1
```

7.3.2 DNS hierarchia

A DNS a HOSTS fájlra alapuló névfeloldás hiányosságait pótolja, felépítése hierarchikus és az egész világra kiterjedően elosztott adatbázist használ az állomásnév – IP-cím összerendelésekhez. Ezzel ellentétben a HOSTS fájl egyetlen kiszolgálón tárolt.

A DNS tartományneveket használ a hierarchiához, amely kisebb, könnyen kezelhető zónákra van osztva. Minden DNS kiszolgáló egy meghatározott adatbázist kezel és csak a DNS struktúra kis részének név – IP-cím hozzárendeléséért felelős. Amikor egy DNS kiszolgáló egy olyan névre kap feloldási kérést, mely nem található meg saját zónájában, akkor egy másik, a megfelelő zónát kezelő DNS kiszolgálónak továbbítja a kérést.

A DNS egy jól bővíthető szolgáltatás, mivel a névfeloldás több kiszolgálóra támaszkodik.



A szolgáltatásnak három összetevője van.

Erőforrás bejegyzések és domainnév-tartomány

Az erőforrás bejegyzés egy adatbejegyzés a DNS zóna adatbázis állományában. Az állomás típusának, IP-címének vagy a DNS adatbázis paraméterének azonosítására szolgál.

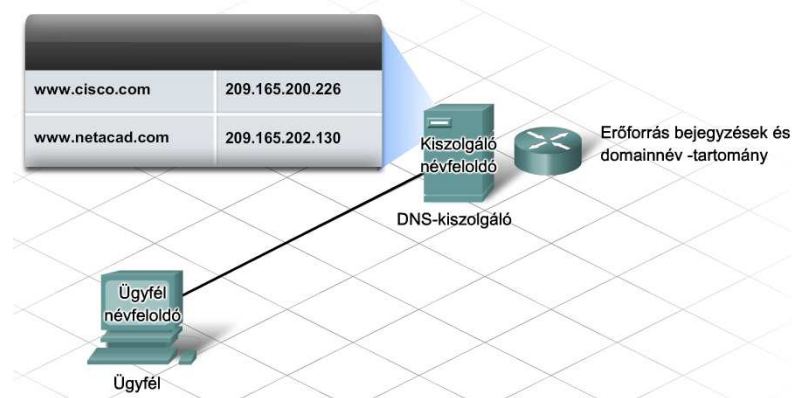
A domainnév-tartomány az erőforrások rendszerezésének hierarchikus névstruktúrájára utal. Több tartományból vagy csoportból és a csoportokon belüli erőforrás bejegyzésekből áll.

Tartománynév-kezelő rendszer kiszolgálói

A tartománynév-kezelő rendszer kiszolgálói tartják karban az erőforrás bejegyzéseket és a domainnév-tartomány információit tároló adatbázist. A DNS kiszolgálók megpróbálják a saját zónájuk adatbázis állományában tárolt információk alapján feloldani az ügyfelek kéréseit. Ha a kiszolgáló nem rendelkezik a kért információval, akkor további, előre meghatározott névkiszolgálók segítségével oldja meg a kérést.

Névfeloldó (resolver)

A névfeloldók olyan alkalmazások vagy operációs rendszerfunkciók, melyek a DNS ügyfeleken és kiszolgálókon egyaránt futnak. Amikor egy tartománynév használatban van, a névfeloldó a DNS ügyfélen betöltődik, és létrehoz egy DNS kérést a kiszolgáló felé. Ha a kiszolgáló nem rendelkezik a kért név – IP-cím hozzárendeléssel, akkor a névfeloldó segítségével továbbítja a kérést egy másik DNS kiszolgáló felé.



A DNS egy hierachikus rendszer segítségével biztosítja a névfeloldást. Ez a hierarchia egy fordított fához hasonlít, melynek a gyökere van felül és az ágak alul.

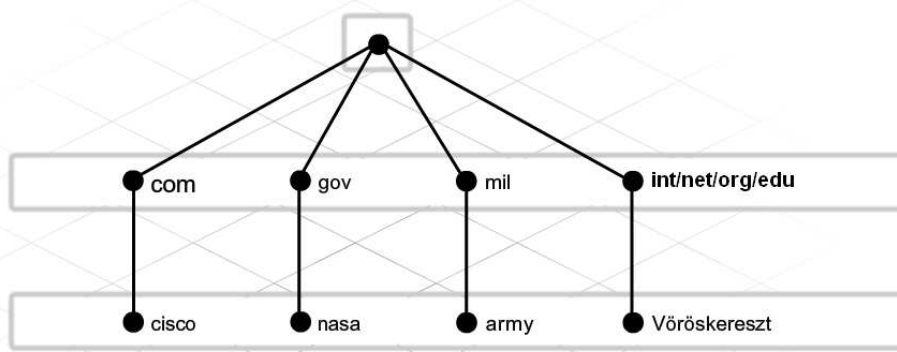
A hierarchia csúcán a gyökér (root) kiszolgálók tartják karban a legmagasabb szintű (top-level) kiszolgálók eléréséről tárolt információt, melyek visszamutatnak a második szintű (second level) tartomány kiszolgálókra.

A különböző legmagasabb szintű tartományok a szervezetek típusát vagy a származó országot reprezentálják. Példák a legmagasabb szintű tartományokra:

- .au - Ausztrália
- .co - Kolumbia
- .com – ipari vagy üzleti vállalat
- .jp - Japán
- .org – nonprofit szervezet

A legmagasabb szintű tartományok alatt a második szintű tartományok helyezkednek el, melyek alatt további, alacsonyabb szintű tartományok találhatók.

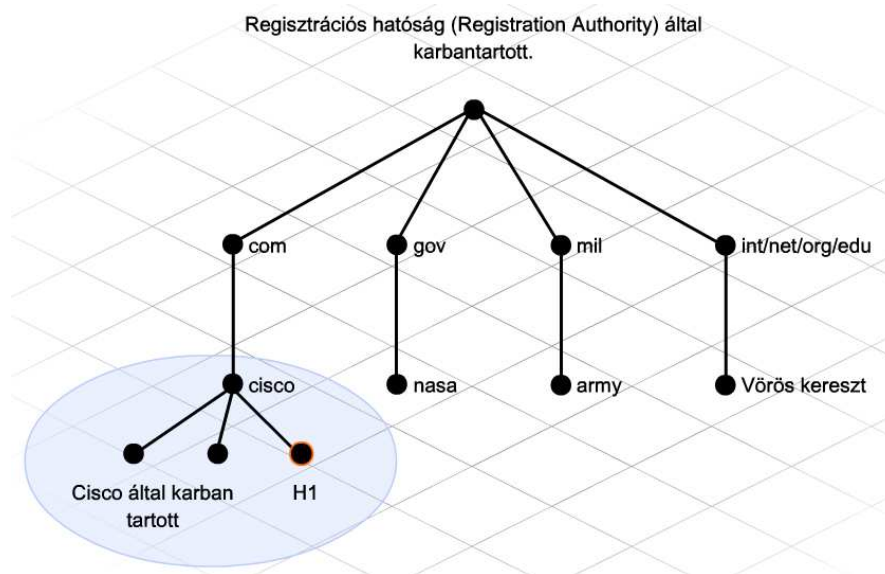
Regisztrációs hatóság (Registration Authority) által karbantartott.



A gyökérben található (root) DNS kiszolgáló nem feltétlenül tudja pontosan merre található a H1.cisco.com, de van egy bejegyzése a .com legmagasabb szintű tartományról. Hasonlóan a .com tartományba tartozó kiszolgálók nem feltétlenül tudják merre van a H1.cisco.com, de van bejegyzése a cisco.com tartományról. A cisco.com tartománynak van bejegyzése a H1.cisco.com-ról és fel tudja oldani az IP-címet.

A DNS szolgáltatás nem centralizált kiszolgáló hierarchián alapszik. Az erőforrás bejegyzések tartalmaznak tartományneveket, melyeket a kiszolgálók feloldanak és ezt más kiszolgálók szintén lekérdezhetik.

A H1.cisco.com egy teljesen minősített tartománynév (FQDN – Fully Qualified Domain Name), mivel megadja a számítógép pontos helyét a hierarchikus DNS névtartományban.



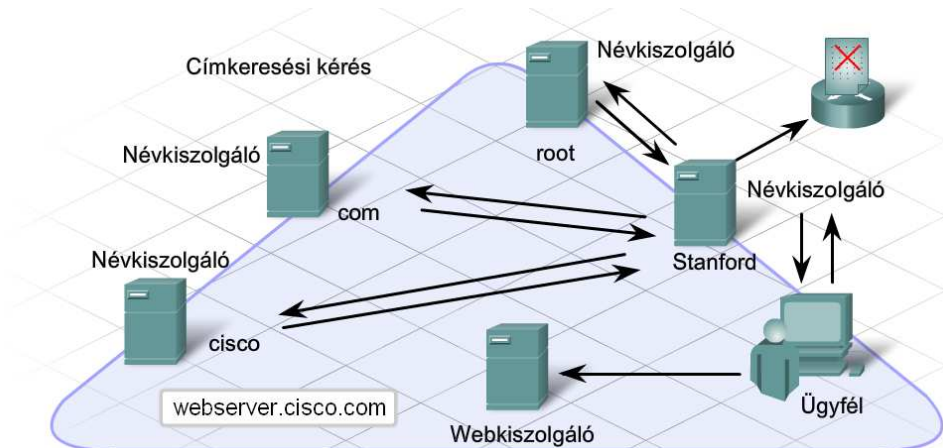
7.3.3 DNS névfeloldás

Amikor egy állomásnak DNS névfeloldásra van szüksége, akkor a névfeloldó segítségével lép kapcsolatba a tartományán belüli DNS kiszolgálóval. A resolver ismeri a DNS kiszolgáló IP-címét, mert ez része az állomás IP-cím konfigurálásának.

Amikor a DNS kiszolgáló kérést kap egy ügyfél névfeloldójától, akkor az először ellenőrzi a helyi DNS bejegyzések cache tárolóját. Ha ott nem oldható fel az IP cím, akkor a kiszolgáló névfeloldója közvetíti a kérést egy másik DNS kiszolgáló felé. Ez a folyamat addig folytatódik amíg az IP-cím nincs feloldva. A névfeloldási információ visszakerül az eredeti kiszolgálóhoz, mely az információt felhasználva válaszol a kérésre.

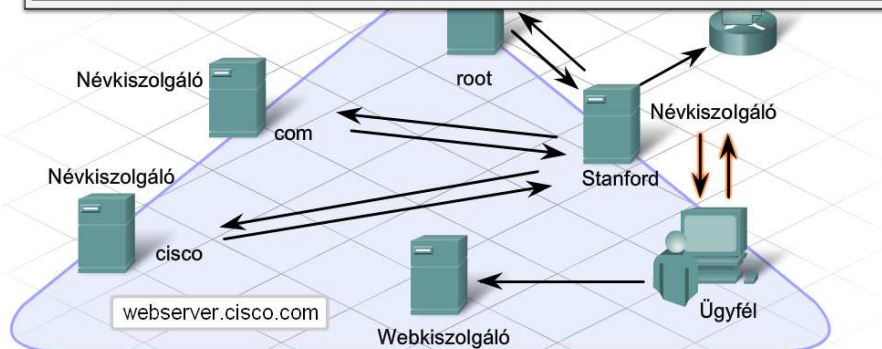
A DNS név feloldási folyamata alatt minden DNS kiszolgáló eltárolja a kérésre válaszul érkezett információt egy gyorsítótárban (cache). A cache-ben tárolt információ segítségével a DNS kiszolgáló sokkal gyorsabban tud válaszolni az egymást követő feloldási kérésekre, mert a kiszolgáló először a gyorsítótárban lévő információt ellenőrzi.

A DNS kiszolgálók csak egy meghatározott időre tárolják az információt a cache-ben. Nem tárolhatja hosszú ideig az információt, mert az állomásnév bejegyzések időről időre változnak, és egy régebbi bejegyzéssel esetleg rossz IP-címet adna meg.



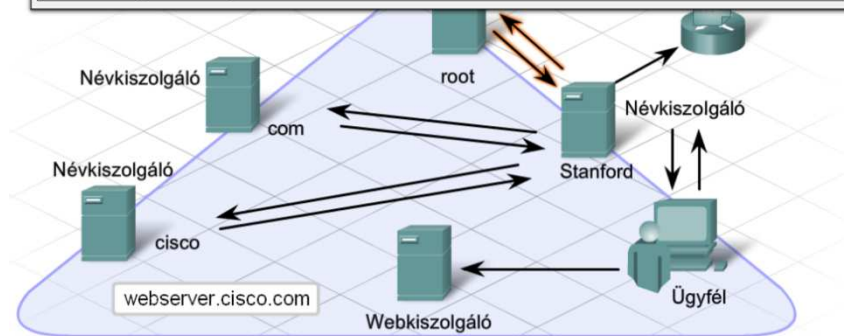
1. lépés: Helyi rekurzív kérés

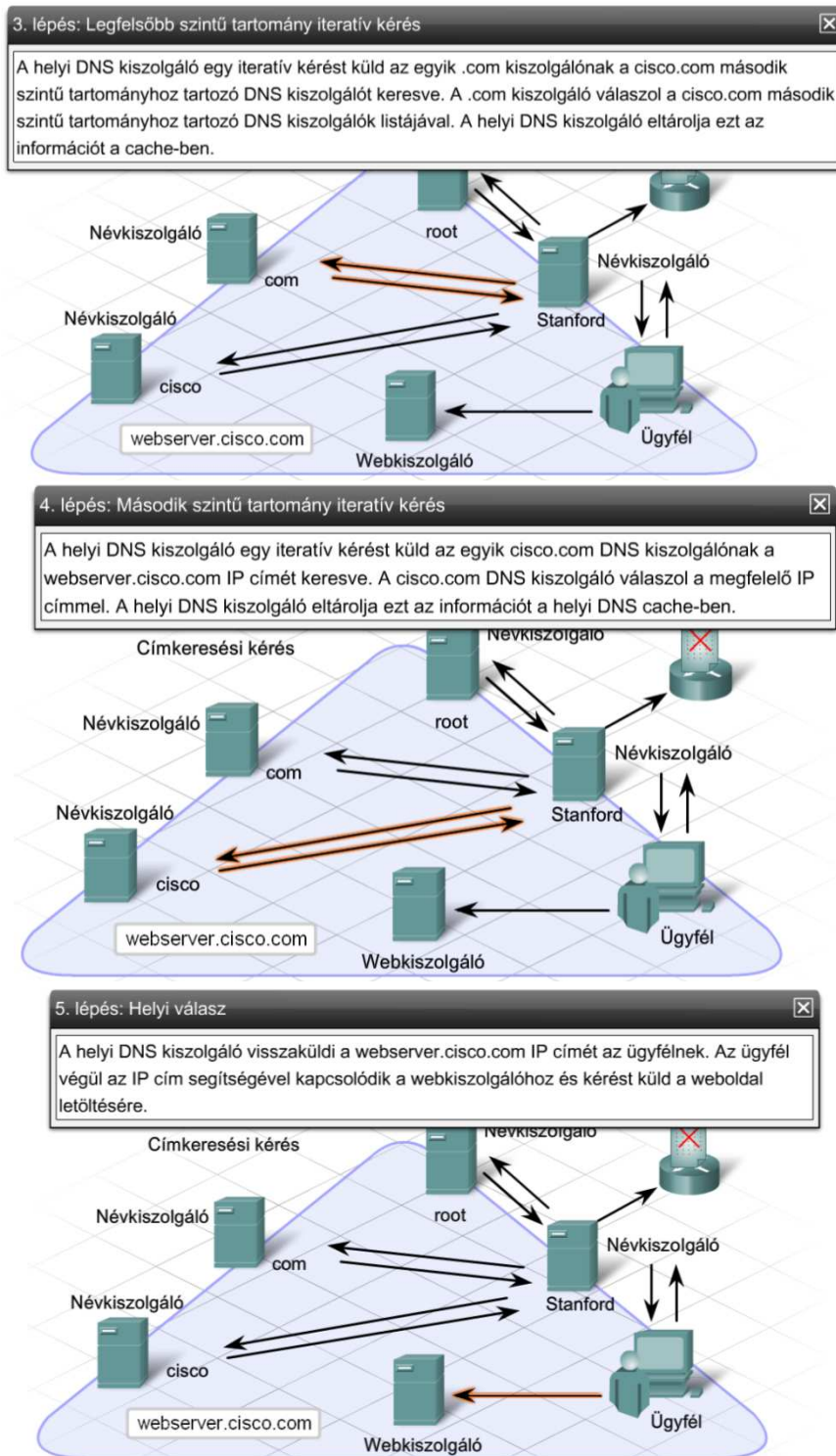
A névfeloldó (resolver) egy rekurzív DNS kérést küld a helyi DNS kiszolgálónak a webkiszolgáló IP-címének lekérdezésére. Cisco.com a távoli állomás teljesen minősített tartományneve. A helyi DNS kiszolgáló megnézi a zóna adatbázisában és a gyorsítótárban a keresett névhozzárendelést. Nem találja.



2. lépés: Root tartomány iteratív kérés

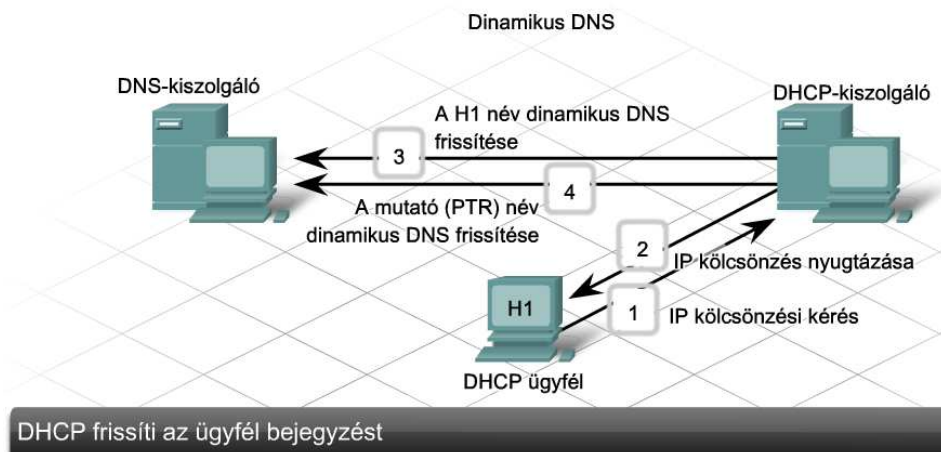
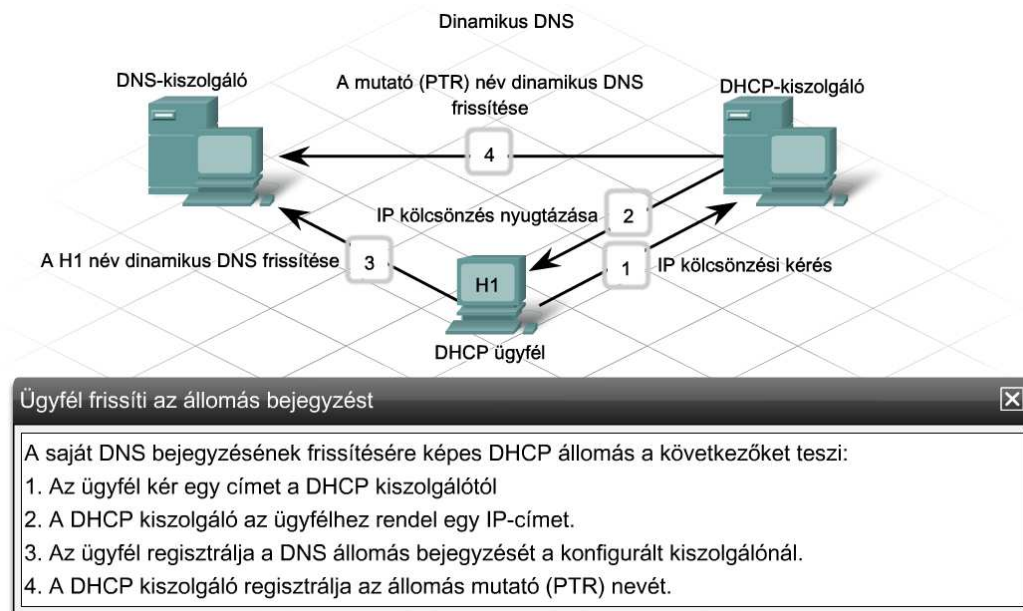
A helyi DNS kiszolgáló küld egy iteratív DNS kérést a .com tartományhoz tartozó legfelsőbb szintű kiszolgálót keresve az egyik előrekonfigurált root kiszolgálónak. A root DNS kiszolgáló visszaküldi a .com tartományhoz tartozó legfelsőbb szintű DNS kiszolgálók listáját. A helyi DNS kiszolgáló eltárolja ezt az információt a cache-ben.





A DNS korai megvalósításaiban az erőforrás bejegyzések hozzáadása és frissítése manuálisan történt. A hálózat és a számon tartott állomások számának növekedésével már nem lehetett tovább hatékonyan megoldani a manuális karbantartást. Továbbá a DHCP használatával az egy DNS zónán belüli erőforrás bejegyzéseket sokkal gyakrabban kellett frissíteni. A DNS zónák karbantartásának könnyítésére, a DNS protokollt megváltoztatták úgy, hogy a számítógép a saját bejegyzéseit dinamikusan frissíthesse.

Dinamikus frissítéssel a DNS ügyfélszámítógép bármilyen változás esetén azonnal regisztrálhatja és frissítheti saját bejegyzéseit. A dinamikus frissítéshez a DNS kiszolgálónak, a DNS ügyfélnek és a DHCP kiszolgálónak egyaránt támogatnia kell a dinamikus frissítéseket. z alapértelmezetten tiltva van, így engedélyezni kell. A legtöbb, napjainkban használatos operációs rendszer már támogatja a dinamikus frissítést.



Némely régebbi operációs rendszer nem támogatja a dinamikus DNS frissítést. Ilyen esetben a DHCP kiszolgálót kell úgy konfigurálni, hogy dinamikusan frissítse a DNS-t az ügyfél nevében. DNS frissítése DHCP használatával a következőképpen történik:

1. Az ügyfél kér egy címet a DHCP kiszolgálótól
2. A DHCP kiszolgáló az ügyfélhez rendel egy IP-címet.
3. A DHCP kiszolgáló regisztrálja a DNS állomás bejegyzést az előre konfigurált kiszolgálónál az ügyfél nevében.
4. A DHCP kiszolgáló regisztrálja az állomás mutató (PTR) nevét.

A DNS kiszolgálók a teljes DNS hierarchia egy meghatározott részének zóna adatbázisát tartják karban. Az erőforrás bejegyzéseket a DNS zónában tárolják.

A DNS zónák címkeresési (forward lookup) vagy névkeresési (reverse lookup) zónák lehetnek. Ezen belül elsődleges vagy másodlagos címkeresési, illetve névkeresési zóna lehet. Minden zóna típusnak speciális szerepe van az egész DNS infrastruktúrában.

Címkeresési zóna

A címkeresési zóna egy hagyományos DNS zóna, mely egy teljesen meghatározott tartománynevet egy IP-címre old fel. Az internet böngészése közben ezzel a típussal lehet leggyakrabban találkozni. Egy weboldal címének, mint például `www.cisco.com` begépelése után egy rekurzív kérés érkezik a helyi DNS kiszolgálóhoz a név feloldására.

Névkeresési zóna

A névkeresési zóna egy speciális zóna típus, mely IP címeket old fel teljesen meghatározott tartománynevekre. Bizonyos alkalmazások névkeresést használnak a velük kommunikáló számítógép rendszer azonosítására. Az interneten megtalálható egy teljes névkeresési DNS hierarchia, melynek segítségével bármely nyilvánosan regisztrált IP cím feloldható. Sok magánhálózat saját maga implementálja a helyi névkeresési zónáját a hálózat számítógéprendszerének azonosítására. Névkeresést használ a `ping -a [IP-cím]` parancs is.

Elsődleges zónák

Az elsődleges DNS zóna módosítható. Ha egy új erőforrás bejegyzést hozzá kell adni vagy egy létező bejegyzést frissíteni, törölni kell, akkor a módosítást az elsődleges zónában végzik. Ha egy elsődleges zóna található a DNS kiszolgálón, akkor a kiszolgáló a felelős azért a zónáért, ő rendelkezik a zóna bejegyzéseit érintő kérésekre adható válaszokkal. Minden DNS tartományban egyetlen elsődleges zóna lehet, illetve egy elsődleges címkeresési és egy elsődleges névkeresési zóna.

Másodlagos zónák

A másodlagos zóna egy olvasható tartalék (backup) zóna, melyet az elsődleges zónától külön kiszolgálón kell tárolni. Ez tulajdonképpen az elsődleges zóna másolata és az elsődleges zónától kapja a frissítéseket. Mivel a másodlagos zóna csak egy olvasható backup zóna, így minden bejegyzés frissítést a megfelelő elsődleges zónán kell elvégezni. Másodlagos zónából is lehet címkeresési és névkeresési zóna is. A DNS zóna elérhetőségi követelményeitől függően több másodlagos zóna is lehet szétszórva.



```
Command Prompt
C:\>ping netacad.net

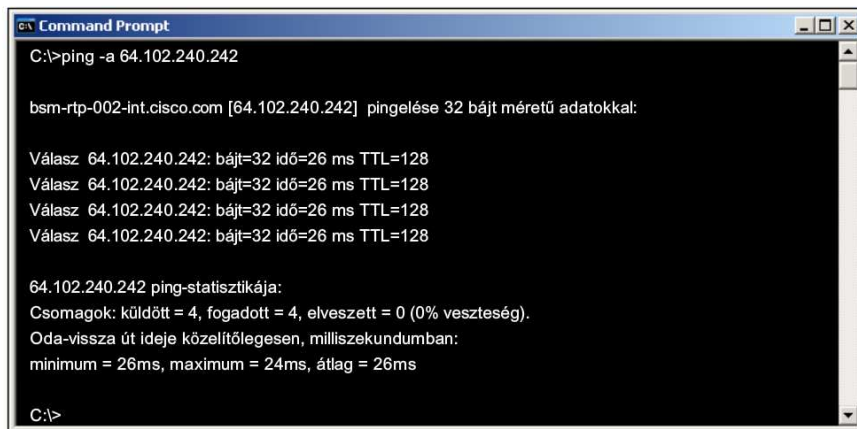
netacad.net.esxi.loc [64.102.240.242] pingelés 32 bájt méretű adatokkal:

Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=247
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=247
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=247
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=247

64.102.240.242 ping-statisztikája:
Csomagok: küldött = 4, fogadott = 4, elveszett = 0 (0% veszteség).
Oda-vissza út ideje közelítőlegesen, milliszekundumban:
minimum = 26ms, maximum = 24ms, átlag = 26ms
```

Címkeresési (Forward lookup) zóna

Névkeresési (Reverse lookup) zóna



```
C:\>ping -a 64.102.240.242

bsm-rtp-002-int.cisco.com [64.102.240.242] pingelése 32 bájtt méretű adatokkal:

Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=128
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=128
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=128
Válasz 64.102.240.242: bájt=32 idő=26 ms TTL=128

64.102.240.242 ping-statisztikája:
Csomagok: küldött = 4, fogadott = 4, elveszett = 0 (0% veszteség).
Oda-vissza út ideje közelítőlegesen, milliszekundumban:
minimum = 26ms, maximum = 24ms, átlag = 26ms

C:\>
```

Címkeresési (Forward lookup) zóna

Névkeresési (Reverse lookup) zóna

7.3.4 DNS implementálása

Több módja is létezik a DNS implementálásának.

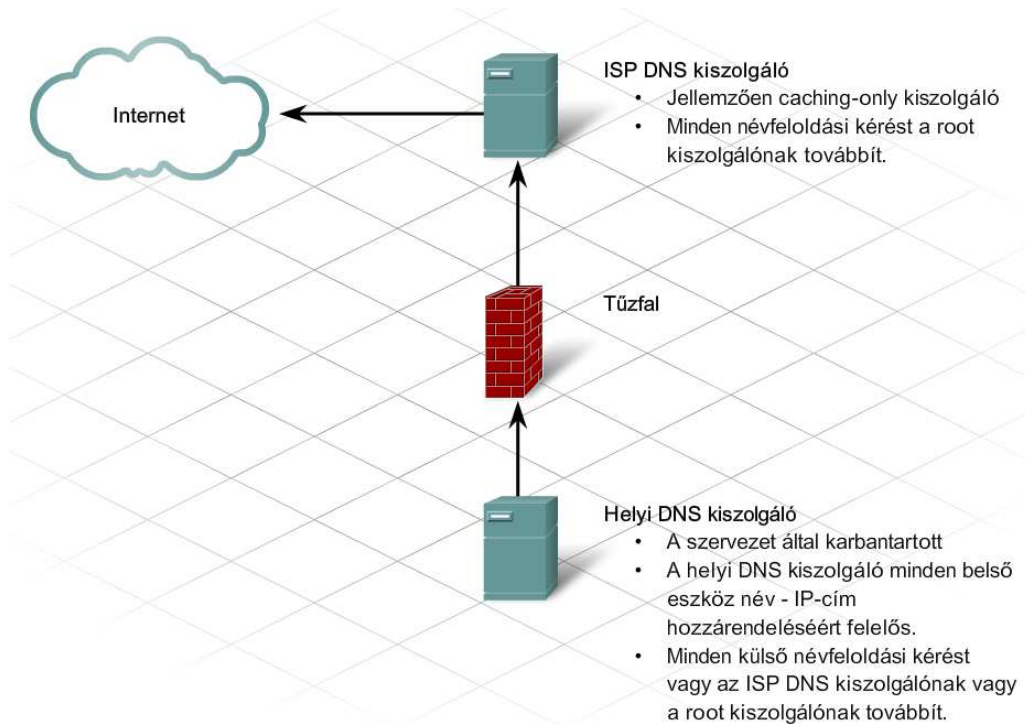
ISP DNS kiszolgálók

Az internetszolgáltatók általában gyorsítótáras (caching-only) DNS kiszolgálókat tartanak karban. Ezeket a kiszolgálókat úgy konfigurálják, hogy minden feloldási kérést az interneten a root kiszolgálóknak továbbítsanak. Az eredményeket a cache-ben tárolják és későbbi kérésekhez használják. Mivel a szolgáltatóknak általában sok felhasználójuk van, így az eltárolt DNS bejegyzések száma igen nagy. A hatalmas gyorsítótár csökkenti a hálózati sávszélesség igénybevételét a gyökér kiszolgálóknak továbbított DNS kérések gyakoriságának csökkentésével. A caching-only kiszolgálók nem tartanak kézből semmilyen hiteles (authoritative) zóna információt, azaz nem tárolnak egyetlen név – IP-cím hozzárendelést sem az adatbázisukban.

Helyi DNS kiszolgálók

Egy vállalat saját maga is üzemeltetheti a DNS kiszolgálóját. Ilyenkor a hálózaton lévő ügyfélszámítógépeket úgy konfigurálják, hogy a helyi és nem az ISP DNS kiszolgálójára mutasson. A helyi DNS kiszolgáló tartalmazhat hiteles zónabejegyzéseket a szóbanforgó zónára, azaz név – IP-cím hozzárendeléseket a zónáján belüli összes állomásra. Ha a DNS kiszolgáló olyan kérést kap, amit nem tud feloldani, akkor továbbítja. A helyi DNS kiszolgáló gyorsítótára viszonylag kicsi az ISP DNS kiszolgálójáéhoz képest, mivel a feloldási kérések száma jóval kevesebb.

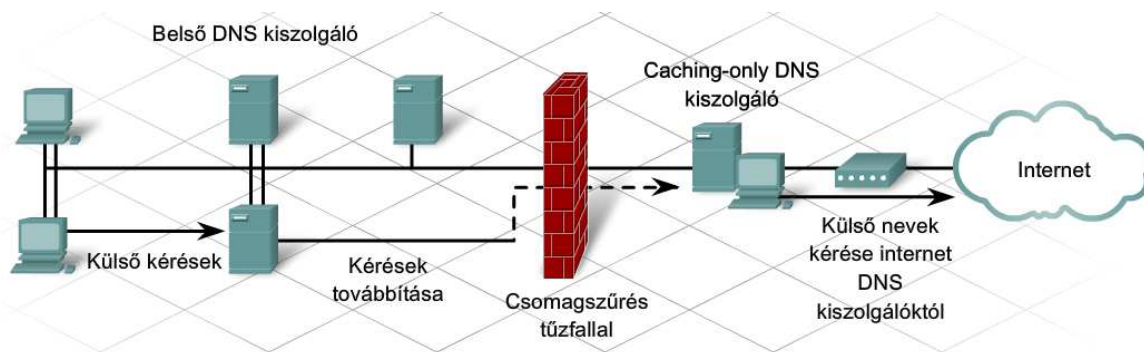
A helyi DNS kiszolgálót úgy is lehet konfigurálni, hogy a kéréseket közvetlenül a root DNS kiszolgálónak továbbítsa. Sok rendszergazda a DNS kiszolgálót mégis úgy konfigurálja, hogy a kéréseket a hierarchián eggyel magasabb szinten álló kiszolgálónak, például az ISP DNS kiszolgálójának továbbítsa. Ilyenkor a helyi DNS kiszolgáló előnyt élvez az ISP DNS kiszolgálójának gyorsítótárában eltárolt nagyszámú bejegyzésből, és így nem kell a root kiszolgálótól kezdődő egész keresési folyamaton végigmenni.



A DNS kiszolgáló elérhetőségének elvesztése veszélyeztetheti a nyilvános erőforrások láthatóságát. Ha a felhasználók olyan tartománynevet gépelnek be, melyet nem lehet feloldani, akkor nem tudják elérni az erőforrást. Ezért amikor egy szervezet regisztrál egy tartománynevet az interneten, akkor legalább két DNS kiszolgálónak el kell küldeni a regisztrációt. Ezek a kiszolgálók tárolják a DNS zóna adatbázist. Tartalék DNS kiszolgálók biztosítják, hogy az egyik kiesése esetén a másik elérhető legyen névfeloldásra. Ez adja a rendszer hibatűrő képességét. Ha a hardver erőforrások lehetővé teszik egy zónán belül két vagy több DNS kiszolgáló elhelyezését, akkor nagyobb védelmet és szervezettséget lehet elérni.

Szintén hasznos, ha a zóna információt tároló DNS kiszolgálói fizikailag külön hálózaton vannak. Például az elsődleges DNS zónainformáció tárolható a vállalat helyi DNS kiszolgálóján. Általában az ISP-nél tárolható egy másodlagos DNS kiszolgáló a kiesés elkerülésére.

A DNS kritikus hálózati szolgáltatás, ezért tűzfalakkal és más biztonsági módszerekkel kell védeni. Kiesése esetén a webszolgáltatások elérhetetlenek lesznek.



7.4 Szolgáltatások és protokollok

7.4.1 Szolgáltatások

Az internetkapcsolat és DNS szolgáltatás mellett az internetszolgáltatók nagyon sok üzleti-célú szolgáltatást biztosítanak a felhasználóknak. Ezek a szolgáltatások a kiszolgálón található programmal engedélyezhetők. Az ISP által nyújtott szolgáltatásokhoz tartozik:

- e-mail tárolás
- weboldalak tárolása
- elektronikus kereskedelmi oldalak
- fájl tárolás és átvitel
- üzenőfalak és blog-ok
- video – és audiofolyam szolgáltatások

A TCP/IP alkalmazás rétegbeli protokollok ezen ISP szolgáltatások és alkalmazások többségét lehetővé is teszik. A legismertebb TCP/IP alkalmazási rétegbeli protokollok a HTTP, FTP, SMTP, POP3 és IMAP4.

Sok felhasználó biztonsággal szembeni elvárásai nagyobbak, ezért az alkalmazási rétegbeli protokollok biztonságos verziói is rendelkezésre állnak, mint például az FTPS és a HTTPS.

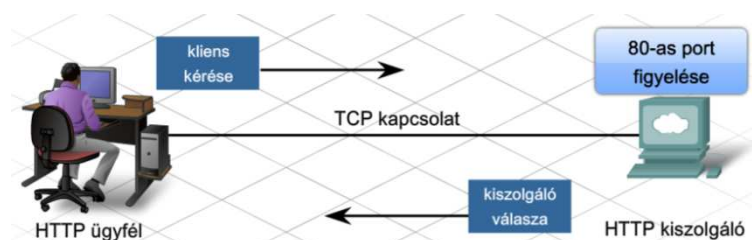
7.4.2 HTTP és HTTPS

A HTTP-t, a TCP/IP modell egyik protokollját eredetileg HTML formájú weboldalak lehívására tervezték. Ma már elosztott, együttműködéssel létrehozott információ megosztásra használják. A HTTP-nek sok verziója létezik. A legtöbb ISP a HTTP 1.1-es verzióját használja web-hosting szolgáltatások biztosítására. A korábbi verzióktól eltérően az 1.1-es verzió lehetővé teszi a webkiszolgáló számára több weboldal tárolását is. Megengedi az állandó kapcsolatokat, így több kérés- és válaszüzenet használhatja ugyanazt a kapcsolatot, csökkentve ezáltal új TCP viszonyok létesítésének idejét.

A HTTP egy kérés/válasz alapú protokoll. Amikor egy ügyfél, általában egy webböngésző kérést küld a webkiszolgálónak, akkor a HTTP meghatározza az ügyfél által küldött kérés, valamint a kiszolgáló által küldött válasz üzenettípusát.

A HTTP rugalmassága ellenére nem biztonságos protokoll. A kérésüzenetek és a kiszolgálóválaszok titkosítás nélküli információt szállítanak, amely könnyen elfogható és olvasható mások számára is.

Az internet feletti biztonságos kommunikációra, a webkiszolgáló elérésére a biztonságos HTTP-t (HTTPS – Secure HTTP) használják. A HTTPS hitelesítést és titkosítást is használhat az adatok biztonságos átviteléhez az ügyfél és a kiszolgáló között. További szabályokat is meghatároz az alkalmazási és szállítási réteg közötti adatáramlás szabályozására.



Ha kapcsolatba lépünk egy HTTP kiszolgálóval egy weboldal letöltése céljából, az egységes erőforrás azonosító (URL – uniform resource locator) segítségével történik a kiszolgáló és a meghatározott erőforrás helyének meghatározása. Az URL meghatározza:

- A használt protokollt
- Az elérni kívánt kiszolgáló tartománynevét
- A kiszolgálón található erőforrás helyét, mint például
`http://example.com/example1/index.htm`

Sok webkiszolgáló alkalmazás megengedi a rövid URL-eket. A rövid URL-ek azért is népszerűek, mert könnyű megjegyezni, leírni vagy továbbadni őket. Egy rövid URL-lel az erőforrás alapértelmezett oldala jeleníthető meg. Amikor a felhasználó begépel egy rövidített URL-t, mint például: `http://example.com`, akkor az alapértelmezett oldalt kapja meg, ami tulajdonképpen a `http://example.com/example1/index.htm` weboldal.

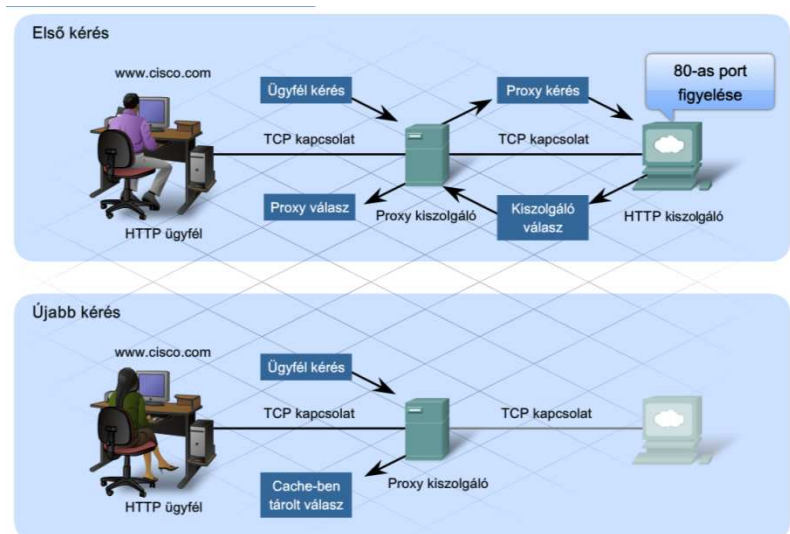
A HTTP proxy szolgáltatásokat is támogat. A proxy kiszolgáló lehetővé teszi az ügyfelek számára, hogy közvetett hálózati kapcsolatokat alakítsanak ki más hálózati szolgáltatásokkal. A kommunikációs folyam közbülső eszköze, mely az ügyfél felé úgy viselkedik, mint egy kiszolgáló, a kiszolgáló felé pedig, mint egy ügyfél.

Az ügyfél kapcsolódik a proxy kiszolgálóhoz és kér egy másik kiszolgálón található erőforrást a proxy-tól. A proxy kapcsolódik a meghatározott kiszolgálóhoz és lehívja a kért erőforrást, majd továbbítja az ügyfél felé.

A proxy kiszolgáló egy előrekonfigurált időre eltárolhatja az oldalt vagy az erőforrást a cache-ben, így későbbi ügyfélkérések esetén lehetővé teszi a gyors weboldal letöltést a távoli kiszolgáló elérése nélkül. A proxy-kat három szempont miatt is használják:

- Gyorsaság – A cache-ben eltárolt információ lehetővé teszi az ügyfél által kért erőforrás más ügyfelek számára történő gyors letöltését a tényleges kiszolgáló elérése nélkül.
- Biztonság – A proxy kiszolgálók felhasználhatók számítógépes vírusok és más rosszindulatú programok felfogására és az ügyfeleknek való továbbítás megakadályozására.
- Szűrés – A proxy kiszolgálók látják a bejövő HTTP üzeneteket és szűrik a nem megfelelő vagy támadó tartalmú weboldalakat.

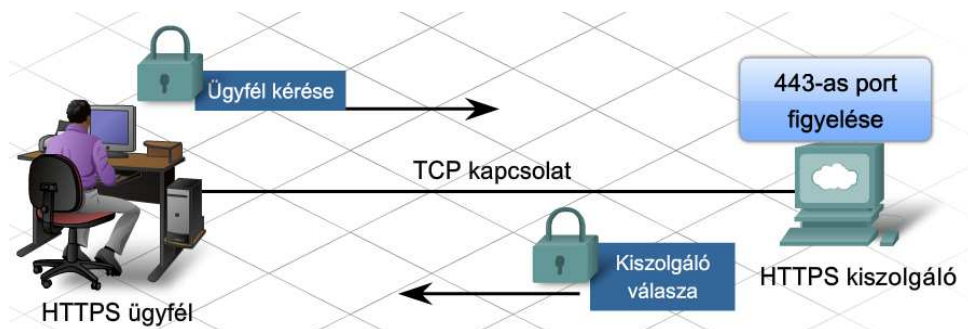
A HTTP titkosítatlan szöveget küld az ügyfél és a kiszolgáló között. Ezek az üzenetek könnyen elfoghatók és olvashatók jogosulatlan felhasználók számára. Az adatok, főleg a bizalmas információ védelmére, sok ISP nyújt biztonságos webszolgáltatást HTTPS segítségével. A HTTPS tulajdonképpen



HTTP, egy biztonságos csatoló réteg (SSL – secure socket layer) felett. A HTTPS ugyanazt az ügyfélkérés – kiszolgálóválasz üzeneteket használja mint a HTTP, de az adatokat a hálózaton történő átvitel előtt SSL használatával titkosítja.

Amikor a HTTP adatfolyam megérkezik a kiszolgálóhoz, akkor a TCP réteg átadja a kiszolgáló alkalmazási rétegében lévő SSL-nek dekódolásra.

A HTTPS kiszolgáló kevesebb egyidejű kapcsolatot tud ellátni, mint a HTTP kiszolgáló. A HTTPS többletterhelést ró a kiszolgálóra az adatforgalom titkosítása és dekódolása érdekében. A kiszolgáló teljesítményének javítására a HTTPS-t csak indokolt esetben érdemes használni, például bizalmas adatok küldése esetén.



7.4.3 FTP

Az FTP egy összeköttetés-alapú protokoll, mely TCP-t használ az ügyfél folyamat és a kiszolgáló folyamat közötti kommunikáció lebonyolítására. Az FTP implementációk a protokoll értelmező (PI – Protocol Interpreter) és az adatátviteli folyamat (DTP – data transfer process) funkciókat is tartalmazzák. A PI és a DTP két külön folyamatot határoznak meg, melyek együtt dolgoznak a fájlátvitelben. Ennek eredményeképpen az FTP két kapcsolat meglétét igényli az ügyfél és a kiszolgáló között. Egyet a vezérlő információk és parancsok küldéséhez, egyet pedig az aktuális adatátvitelhez.

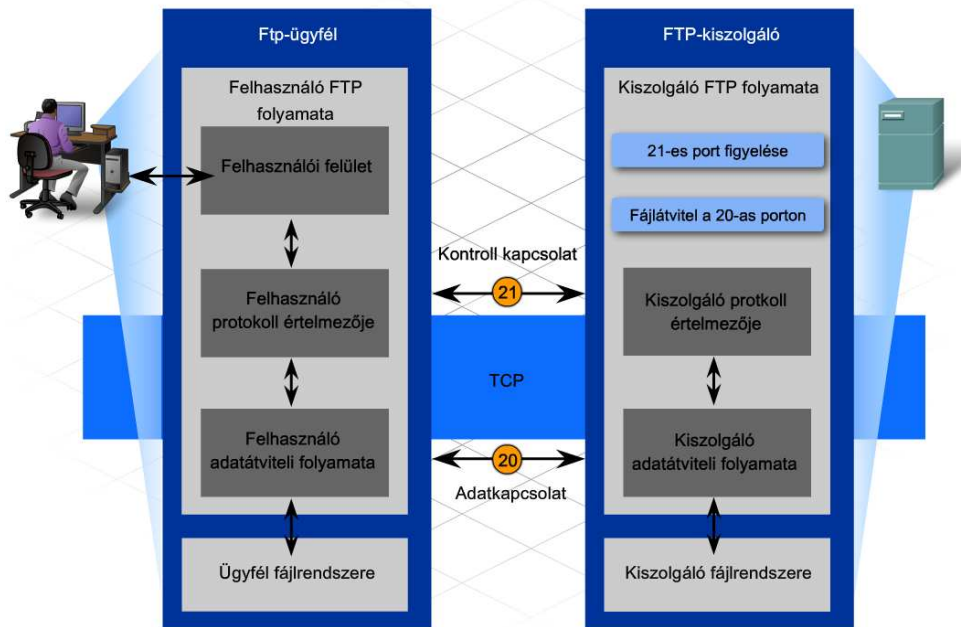
Protokoll értelmező (PI - Protocol Interpreter)

A PI a fő vezérlő kapcsolat az FTP ügyfél és az FTP kiszolgáló között. Létrehozza a TCP kapcsolatot és továbbítja a vezérlő információt a kiszolgálónak, amely a fájl hierarchián történő navigáláshoz, átnevezéshez vagy fájlmozgatáshoz szükséges parancsokat is magába foglalja. A vezérlő kapcsolat vagy vezérlő folyam addig nyitva marad, míg a felhasználó be nem zárja. Amikor egy felhasználó kapcsolódni akar egy FTP kiszolgálóhoz, akkor ez öt lépésben történik:

- 1. lépés:** A felhasználó PI kapcsolat felépítés kérést küld a kiszolgáló PI-nek a 21-es porton.
- 2. lépés:** A kiszolgáló PI válaszol és a kapcsolat felépült.
- 3. lépés:** Miután a TCP vezérlő kapcsolat megnyílt, a kiszolgáló PI megkezd a bejelentkezési folyamatot.
- 4. lépés:** A felhasználó a felhasználói interfészen keresztül megadja a személyi adatait, és elvégzi a hitelesítést.
- 5. lépés:** Megkezdődik az adatátvitel.

Adatátviteli folyamat (DTP – Data Transfer Process)

A DTP egy különálló adatátviteli funkció. Ez a funkció csak akkor engedélyezett, ha a felhasználó akar ténylegesen állományokat le – vagy feltölteni az FTP kiszolgálóra. A PI kapcsolattól eltérően, mely nyitva marad, a DTP kapcsolat automatikusan bezárul a fájlátvitel befejezése után.



Az FTP által támogatott kétfajta adatkapcsolat az aktív és a passzív kapcsolat.

Aktív adatkapcsolatok

Aktív adatkapcsolat esetén az ügyfél kezdeményezi a kérést a kiszolgáló felé és megnyit egy portot a várt adatnak. A kiszolgáló aztán kapcsolódik az ügyfélhez a megadott porton és megkezdődik a fájlátvitel.

Passzív adatkapcsolatok

Passzív adatkapcsolat esetén az FTP kiszolgáló nyit meg egy véletlenszerűen kiválasztott portot (nagyobb, mint 1023). A kiszolgáló elküldi az FTP ügyfélnek az IP címét és a megnyitott port számát egy vezérlő folyamaton. A kiszolgáló várja az FTP ügyfél kapcsolódását és a fájlátvitel megkezdését.

Az ISP-k az FTP kiszolgálóknak általában passzív adatkapcsolatokat szolgáltatnak. A tűzfalak gyakran nem engedélyezik az aktív FTP kapcsolatokat a belső hálózaton lévő állomások számára.

Aktív kapcsolat

Kiszolgáló kezdeményezi az adatátviteli kapcsolatot. A felhasználó kéri az adatátvitelt, a kiszolgáló-PI arra utasítja a kiszolgáló-DTP-t, hogy kapcsolódjon a felhasználó-DTP-hez. A felhasználó-DTP várja a kiszolgáló-DTP kapcsolódását.

Passzív kapcsolat

Az ügyfél kezdeményezi az adatátviteli kapcsolatot. A ügyfél-PI kapcsolódik a kiszolgáló-PI-hez és utasítja a kiszolgáló-DTP-t, hogy legyen passzív. A kiszolgáló-PI az IP címével és egy dinamikus portszámmal válaszol, melyet a felhasználó az adatátvitelre felhasznál. A kiszolgáló-DTP várja az ügyfél-DTP kapcsolódását.

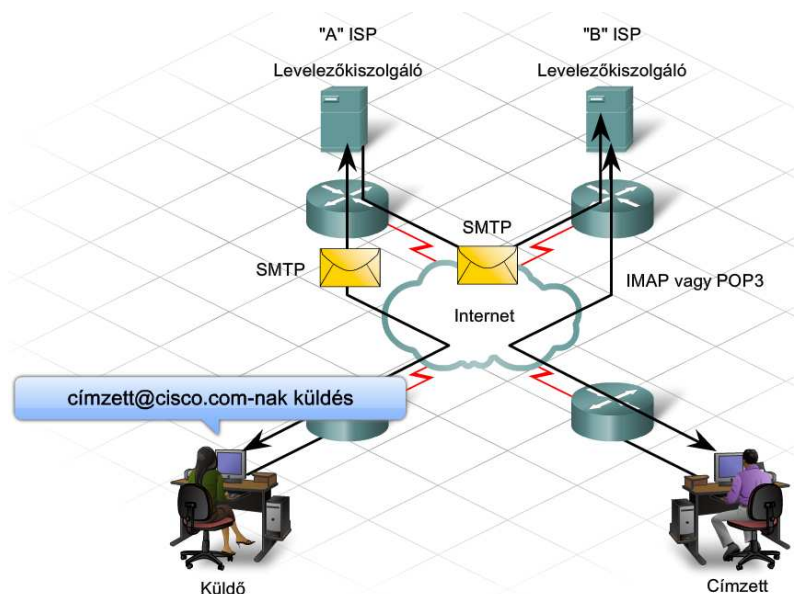
7.4.4 SMTP, POP3 és IMAP4

Az ISP által támogatott elsődleges szolgáltatások egyike az email-hosting (e-mail szolgáltatás). Az elektronikus levelezés szolgáltatás a tárol és továbbít módszert alkalmazza az üzenetek hálózaton történő küldésére, tárolására és elérésére. Az elektronikus leveleket a levelezőkiszolgálók adatbázisokban tárolják. Az internetszolgáltatók gyakran alkalmaznak olyan levelezőkiszolgálókat, melyek több különböző felhasználói fiókot is támogatnak.

A levelező ügyfelek a kiszolgálóknak küldik és tőlük kapják a leveleket. Levelezőkiszolgálók más kiszolgálókkal is kommunikálnak, hogy egyik tartományból a másikba küldjék az üzeneteket. Levélküldés esetén az ügyfelek nem kommunikálnak egymással közvetlenül, helyettük a kiszolgálók végzik az üzenettovábbítást még akkor is, ha a küldő és fogadó állomás ugyanabban a tartományban van.

A levelező ügyfelek a kiszolgálónak az alkalmazás beállításainak megfelelően küldik az üzeneteket. Amikor a kiszolgáló megkapja az üzenetet, akkor először ellenőrzi, hogy a címzett a helyi adatbázisában van-e. Ha nem, akkor egy DNS kérést küld a célállomás tartományában megtalálható levelezőkiszolgáló meghatározására. Ha a célállomás levelezőkiszolgálójának IP-címe már ismert akkor a levelet továbbítja ennek a kiszolgálónak.

Az elektronikus levelezés három különböző protokollt támogat: SMTP, POP3 és IMAP4. Az az alkalmazási rétegbeli folyamat, amely az ügyféltől a kiszolgálóig, vagy két kiszolgáló között továbbítja a leveleket, az SMTP protokollra épül. Az ügyfél pedig a POP3 vagy IMAP4 alkalmazási rétegbeli protokoll valamelyikével hívja le az e-maileket.



Az SMTP megbízhatóan és hatékonyan továbbítja a leveleket. Az SMTP alkalmazások megfelelő működéséhez az üzenetnek megfelelő formájúnak kell lennie, és az SMTP folyamatoknak mind az ügyfél, mind a kiszolgáló állomáson futnia kell.

Az SMTP üzenetnek van egy fejrésze és adatrésze. Míg az üzenet adatrésze tetszőleges mennyiségű szöveges információt tartalmazhat, addig a fejrésznek megfelelő formátumú címzett és feladó címet kell tartalmaznia. A többi fejrész információ nem kötelező.

Amikor az ügyfél e-mailt küld, akkor az SMTP folyamata kapcsolódik a kiszolgáló SMTP folyamatához a jól ismert 25-ös porton. A kapcsolat felépítése után az ügyfél megkísérli a kapcsolaton keresztül az e-mail küldését. Ha a kiszolgáló megkapja az üzenetet, akkor vagy elhelyezi egy helyi levelezőfiókban vagy továbbítja egy másik kiszolgálónak ugyanazon az SMTP folyamaton keresztül.

A célállomás e-mail kiszolgálója lehet, hogy nem elérhető az üzenetküldés idejében, ezért az SMTP eltárolja az üzeneteket egy sorban a későbbi küldéshez. A kiszolgáló periódikus időközönként ellenőrzi az üzenetsort és újra megpróbálja elküldeni. Ha az üzenetet nem sikerült egy előre meghatározott lejárati időn belül kézbesíteni, akkor visszakerül a feladóhoz kézbesítetlenül.

Az e-mail üzenet fejrészének egyik szükséges mezője a címzett e-mail címe. Az e-mail cím felépítésében megtalálható az e-mail fiók neve vagy egy fedőnév a levelező kiszolgáló tartomány neve mellett. Példa az e-mail címre:

címzett@cisco.com

A @ szimbólum a kiszolgáló tartomány nevét és a levelező fiók nevét választja el egymástól. Ha a DNS kiszolgáló egy olyan kérést kap, amiben megtalálható a @ szimbólum, akkor tudja, hogy egy levelező kiszolgáló IP-címét kell keresnie.

Ha az üzenet a címzett@cisco.com-nak szól, akkor a tartománynevet elküldik a DNS kiszolgálónak, hogy a tartomány levelező kiszolgálójának IP-címét megszerezzék. A levelező kiszolgálókat a DNS-en belül egy MX bejegyzés jellel különböztetik meg. Az MX egy erőforrás bejegyzés típus, mely a DNS kiszolgálókon megtalálható. Ha a célállomás levelező kiszolgálója megkapja az üzenetet, akkor eltárolja a megfelelő levelesládában. A levelesláda helye az e-mail cím első részében meghatározott előfizetői fiókon alapszik, jelen esetben ez a "címzett" előfizetői fiók. Az üzenet addig a levelesládában marad, amíg a címzett nem kapcsolódik a kiszolgálóhoz és le nem tölti az e-mailt.

Ha a levelező kiszolgáló kap egy e-mail üzenetet, ami egy ismeretlen előfizetői fióknak szól, az e-mailt kézbesítetlenül visszaküldi a feladónak.

Postafiók protokoll – 3-as verzió (POP3 – Post Office Protocol) lehetővé teszi egy munkaállomás számára az e-mailek levelező kiszolgálóról történő lehívását. POP3 esetén az e-mailek letöltés után törlődnek a kiszolgálóról.

A kiszolgáló a POP3 szolgáltatást a 110-es TCP port passzív figyelésével teszi elérhetővé az ügyfelek számára. Ha az ügyfélnek szüksége van a szolgáltatásra, akkor kérést küld a TCP kapcsolat felépítésére. A kapcsolat felépítése után a POP3 kiszolgáló egy üdvözlő üzenetet küld. Az ügyfél és a POP3 kiszolgáló utasításokat és válaszokat váltanak egymással, addig amíg a kapcsolat nem zárul vagy meg nem szakad.

Mivel az e-mail üzeneteket az ügyfelek letöltik és aztán a kiszolgálóról törlődnek, így az üzenetek nincsenek egyetlen központi helyen tárolva. Mivel a POP3 nem tárolja az üzeneteket, ezért kis vállalatok számára nem ajánlott, mert központosított mentési megoldást igényelnek.

POP3 az ISP-k számára megfelelő választás, mivel nem szükséges a levelezőkiszolgálókon nagyméretű tárolóterület fenntartása és karbantartása.

Internetes üzenetelérési protokoll (IMAP4 – Internet Message Access Protocol) egy másik e-mail hozzáférési módszert definiál. A POP3-tól eltérően azonban, amikor a felhasználó az IMAP kiszolgálóhoz kapcsolódik, az ügyfél alkalmazás az e-mail üzeneteknek csak egy másolatát tölti le. Az eredeti üzenetek kezelői törlésig a kiszolgálón maradnak. A felhasználók a levelező ügyfélprogram segítségével tekinthetik meg az üzenetek másolatát.

Az ügyfelek a kiszolgálón fájlhierarchiát hozhatnak létre a levelek tárolására és rendszerezésére. A fájlhierarchia másolata az e-mail ügyfélen is megtalálható. Ha az ügyfél töröl egy üzenetet, akkor a kiszolgáló szinkronizálja a műveletet és törli az üzenetet a kiszolgálóról.

Kis- és középvállalatok szempontjából sok előnye van az IMAP szolgáltatásnak. Az IMAP hosszútávú e-mail tárolást, és központosított mentést tesz lehetővé. Az alkalmazottak számára az e-mailek több helyszínről, különböző eszközökkel és ügyfélprogrammal történő elérését is támogatja. A levelesláda könyvtárszerkezetének megtekintése független a levelesláda elérési módjától.

Egy ISP számára az IMAP nem megfelelő választás. Nagyon költséges lenne az e-mailek tárolásához szükséges tárhely kapacitás megvásárlása és karbantartása. Ezen felül az ügyfelek postafiókjainak rendszeres mentése tovább növelné az ISP költségeit.

7.5 A fejezet összefoglalása

- A TCP egy összeköttetés alapú protokoll. Nyugtázott, garantált kézbesítést igénylő alkalmazások használnak TCP-t.
- Az UDP egy összeköttetés-mentes protokoll. Nem garantált kézbesítést igénylő alkalmazások UDP-t használnak.
- A TCP és UDP protokollok portszámokat használnak egy meghatározott alkalmazás adatainak, vagy a kiszolgálón futó folyamat azonosítására.
- A TCP és UDP portok teszik lehetővé, hogy a hálózati kiszolgálók egyidejűleg több különböző alkalmazás által kezdeményezett adatátviteli kérésre gyorsan és megbízhatóan válaszoljanak.
- Az eredeti TCP/IP névrendszer a HOSTS állományon alapult, mely tartalmazta az ismert állomások nevét és IP címét.
- A DNS egy névfeloldási rendszer, mely a HOSTS állomány hiányosságait hivatott pótolni.
- A DNS hierarchikus felépítésű és a DNS adatbázis fel van osztva a root, a legfelsőbb szintű, a második szintű és az altartományok között.
 - Dinamikus frissítések segítségével a DNS ügyfelek regisztrálhatják magukat a kiszolgálónál és változás esetén frissíthetik az erőforrás bejegyzéseiket.
- A DNS zónák lehetnek címkeresési (Forward lookup) és névkeresési (reverse lookup) zónák. Ezen felül lehetnek elsődleges vagy másodlagos zónák.
- Sok ISP nyújt gyorsítótáras (caching-only) DNS szolgáltatást.
- Egy szervezet úgy is futtathatja a DNS kiszolgálóját, hogy vagy a caching-only kiszolgálóra vagy rögtön a root kiszolgálóra mutasson.



- Az interneten nyújtott leggyakoribb szolgáltatások az FTP, FTPS, SMTP, POP3, IMAP4, HTTP és HTTPS.
- A HTTP és a HTTPS webkiszolgáló szolgáltatások. A HTTPS a biztonságos változata a HTTP-nek, mely SSL-t használ.
- Az ISP a HTTPS támogatásához nagyteljesítményű webkiszolgálókat használ, hogy ellássa a titkosítási és visszafejtési feladatokat.
- Az FTP-t fájlátviteli szolgáltatásokra használják. Az ISP támogatja az aktív és passzív FTP kapcsolatokat is. Aktív kapcsolat esetén a kiszolgáló kezdeményezi a összeköttetést. Passzív kapcsolat esetén az állomás kezdeményezi az összeköttetést.
- Az elektronikus levelezés három különböző protokollt használ. Email küldése SMTP-vel történik. Email letöltésére a POP3 és IMAP protokollok szolgálnak.

8. ISP felelősség

8.1 ISP biztonsági megfontolások

8.1.1 ISP biztonsági szolgáltatások

Bármilyen internet kapcsolat esetén a számítógép rosszindulatú támadások célpontjává válhat. A károkozó vagy rosszindulatú programok, mint a számítógépes vírusok, férgek vagy kémprogramok levélben, illetve weboldalak letöltésével érkezhettek. Az általuk keletkezett, változó mértékű hibák, gyakran az ISP hálózatának nem biztonságos előfizetői asztali gépeiről származnak.

Ha az ISP webhelyek és e-kereskedelmi oldalak tárolásával is foglalkozik, bizalmas kereskedelmi és bankszámlákkal kapcsolatos adatokat is tárolhat, minek következtében az előfizetők adatainak biztonságos tárolása elengedhetetlen követelmény.

Az internetszolgáltatók fontos szerepet játszanak az otthoni és üzleti felhasználók védelmében, továbbá biztonsági szolgáltatásaikkal védik a náluk elhelyezett kiszolgálókat is. A felhasználók gyakran kérik segítségüket hálózataik és munkaállomásaik védelme érdekében a veszély kockázatának csökkentésére.

Számos lehetőség áll rendelkezésre mind a helyi, mind a szolgáltatói oldalon az operációs rendszer, a benne tárolt és a rendszerek között szállított adatok védelmére.

Ha egy internetszolgáltató tárhely és levelező szolgáltatást nyújt, fontos feladata az adatok védelme a rosszindulatú támadásokkal szemben. A védelem megteremtése bonyolult lehet, mert az egyetlen vagy néhány kiszolgálón tárolt adatok több felhasználóhoz tartozhatnak.

A sebezhető felületek elleni támadások megelőzésére a szolgáltatók könnyen kezelhető, asztali lehetőségeket nyújtanak. A helyszíni telepítő munkájának fontos részét képezi az alapvető biztonsági lehetőségek telepítése és beállítása az ügyfél számítógépén, melyek az alábbiak lehetnek:

- Segítségnyújtás az eszközök biztonságos jelszavainak beállításához.
- Alkalmazások javítási és frissítési lehetőségekkel történő védelme.
- A támadási felületet jelentő, ám nem használt programok és szolgáltatások eltávolítása.
- Felhasználók által hozzáférhető és kizárólag a számukra szükséges alkalmazások biztosítása.
- Asztali tűzfal és vírusellenőrző program beállítása.
- Biztonsági tesztek elvégzése a programokon és szolgáltatásokon a sebezhető pontok felderítése és fokozott védelme érdekében.

Jelszówédelem

Válasszon összetett jelszót! Az összetett jelszavak nagybetűk, kisbetűk, számok és szimbólumok keveréke. Legalább nyolc karakter hosszú, és nem alapulhat szótári szavakon vagy személyes információn, amelyet valaki kitalálhat.

Szintén javasolt a jelszó rendszeres megváltoztatása. Léteznek programok, amelyek lehetővé teszik a támadóknak a jelszavak feltörését a betűk, számok és szimbólumok összes lehetséges kombinációjának próbálgatásával.

A jelszó változtatgatásával a "nyers erő" szerinti jelszófeltörés valószínűsége eltörpül, mivel a próbálgatás rengeteg időt vesz igénybe, miközben a jelszó folyton módosul.

Felesleges szolgáltatások

A számítógéprendszer veszélyeztetésének egyik legáltalánosabb módszere a nem, vagy rosszul konfigurált szolgáltatások kiaknázása. A szolgáltatás természetéből adódóan figyelni a külső számítógépes rendszerekből érkező kéréseket. Ha a szolgáltatásnak kiismerhető és jól kiaknázható forgalma van a rossz konfiguráció eredményeként, a támadó vagy egy féreg veszélyeztetheti, és hozzáférést szerezhet a szolgáltatást futtató számítógéphez.

Bevált módszerként az összes nem használt szolgáltatás eltávolítása vagy kikapcsolása javasolt. A szükséges vagy nem eltávolítható szolgáltatások esetén meg kell győződni a helyes konfigurációról.

Javítások kezelése

Szinte naponta, folyamatosan azonosítanak új, kiaknázható biztonsági hézagokat az operációs rendszerekben. Egyszerű böngészéssel ezek megkereshetők, bárki rátalálhat a napjainkban használt összes operációs rendszer kiaknázható felületeinek listáját tartalmazó oldalakra.

A programfejlesztők rendszeresen hoznak forgalomba frissítéseket - bizonyos esetekben naponta. Az operációs rendszerek frissítéseinek rendszeres figyelemmel kísérése és telepítése elengedhetetlen. A legtöbb támadás, ami egy hekkertől, vagy egy vírus vagy féreg által okozott fertőzéstől indul ki, az operációs rendszer folyamatos javításával megakadályozható.

Alkalmazásbiztonság	Biztonsági vizsgálat
<p>A szükségtelen és javítatlan alkalmazások telepítése növelheti az operációs rendszer támadásainak kockázatát. Az operációs rendszerek folyamatos javításához hasonlóan az alkalmazásoknál is szükséges ez az eljárás.</p> <p>Az internetalapú alkalmazások, mint a böngészők és levelező programok esetén legfontosabb a frissítések folyamatos figyelése, mivel ezek az alkalmazások a legkiszolgáltatottabbak.</p>	<p>Számos eszköz létezik, mely segít az operációs rendszer védelmében. A legtöbb biztonsági ellenőrző program sok más rendszerbiztonsági gyengeség felülvizsgálata után tájékoztatást ad a talált programhibák helyreállításának lehetőségeiről.</p> <p>Némely fejlettebb programcsomag túlmegy a tipikus operációs rendszerbeli biztonsági vizsgálaton, és átvizsgál olyan programokat és szolgáltatásokat is, amelyek a számítógépen futnak és lehetőséget adnak az egész rendszernek a támadás elleni védelmére.</p>

Felhasználó jogosultságok

Egy korszerű operációs rendszerben több hozzáférési szint létezik. Ha a felhasználóknak rendszergazdai, azaz korlátlan hozzáférésük van a rendszerhez, a károkozók könnyebben árthatnak a számítógépnek.

A normál felhasználói azonosító nem jogosítja fel tulajdonosát új alkalmazások telepítésére, mivel nincs hozzáférése sem a legtöbb alkalmazás telepítéséhez szükséges állományrendszerhez, sem a

rendszer állományokhoz. Ennek eredményeként a normál felhasználó nem annyira érzékeny rosszindulatú fertőzésekre, melyek az állományrendszer bizonyos részeihez próbálnak hozzáférni vagy telepíteni rá valamit.

Legjobb megoldásként a felhasználóknak csak azt a hozzáférési szintet szabad engedélyezni, amely a mindennapi munkájukhoz elengedhetetlen. Rendszergazdai hozzáférés csak abban az esetben alkalmazható, amikor olyan műveletek elvégzésére van szükség, melyek a normál felhasználók számára nem megengedettek.

Tipp

A Microsoft szabadon letölthető segédeszköze a Microsoft Baseline Security Analyzer (MBSA) (Microsoft alap biztonsági elemző) program, amely megvizsgál minden, normál felhasználói hozzáféréssel telepített Windows szolgáltatást, és még az operációs rendszer jelenlegi javítási szintjét is ellenőrzi.

Másik népszerű átvizsgáló segédprogram a Nessus Vulnerability Scanner, amely nem csak Windows-on, hanem más, különböző platformon is fut. Számos további eszköz érhető el interneten. Rendszerint a legjobb megoldást az adja, ha legalább egy (de inkább több) program vizsgálja át a rendszer biztonságát.

8.1.2 Biztonsági intézkedések

Az felhasználók adatainak védelmében tett szolgáltató oldali intézkedések elengedhetetlenek a rosszindulatú támadásokkal szemben. A leggyakrabban alkalmazott lehetőségek és eljárások a következők:

- A kiszolgáló merevlemezén tárolt adatok titkosítása.
- Jogosultságok alkalmazása állományok és könyvtárak elérése esetén.
- Felhasználói azonosító vagy csoporttagság alapján történő hozzáférés engedélyezése illetve megtagadása.
- Többszintű hozzáférési jogosultságok használata felhasználói azonosító vagy csoporttagság alapján.

Állományok és könyvtárak jogosultságainak beállításakor a "lehető legkevesebb előjog elve" alapján érhető el a legnagyobb biztonság. Ez annyit jelent, hogy a felhasználóknak csak annyi jogosultságot szabad adni az erőforrások eléréséhez, amennyi a munkájuk elvégzéséhez elengedhetetlenül szükséges. Azaz a megfelelő jogosultsági szintet kell hozzájuk rendelni, például hozzáférés csak olvasásra vagy írásra.

Hitelesítés, Jogosultság ellenőrzés és Naplózás (AAA - Authentication, Authorization, Accounting) a rendszergazdák által használt három lépéses eljárás, amely megnehezíti a támadók hálózathoz történő hozzáférését.

A hitelesítés során a felhasználónak azonosítania kell magát





egy felhasználónévvel és egy jelszóval. A hitelesítési adatbázisokat általában RADIUS vagy TACACS protokollt használó kiszolgálókon tárolják.

A jogosultságok kezelésével a felhasználók megfelelő jogokat kapnak az erőforrások eléréséhez és bizonyos feladatok elvégzéséhez.

Naplózással nyomonkövethetők a felhasználók által használt alkalmazások és használati idejük.

Például a hitelesítési folyamat része a "tanuló" nevű felhasználó felismerése és a rendszerbe történő bejelentkezésének engedélyezése. Az jogosultság ellenőrzés meghatározza a "tanuló" felhasználó jogait az XYZ kiszolgáló eléréséhez Telnet segítségével. A naplózás nyomonköveti a "tanuló" felhasználó hozzáféréseit az XYZ kiszolgálóhoz és a Telnet használatát egy bizonyos napon 15 percen keresztül.

Az AAA különböző hálózati kapcsolatokban használható. Adatbázis alkalmazásával tartja nyilván a felhasználói azonosítókat, jogosultságokat és hozzáférési statisztikákat. A helyi hitelesítés a legegyszerűbb megoldás, ebben az esetben a helyi adatbázist az átjáró forgalomirányítón lehet elhelyezni. Ha egy szervezetnek több tucat felhasználót kell hitelesítenie az AAA segítségével, külön kiszolgálón kell az adatbázist fenntartania.

8.1.3 Adattitkosítás

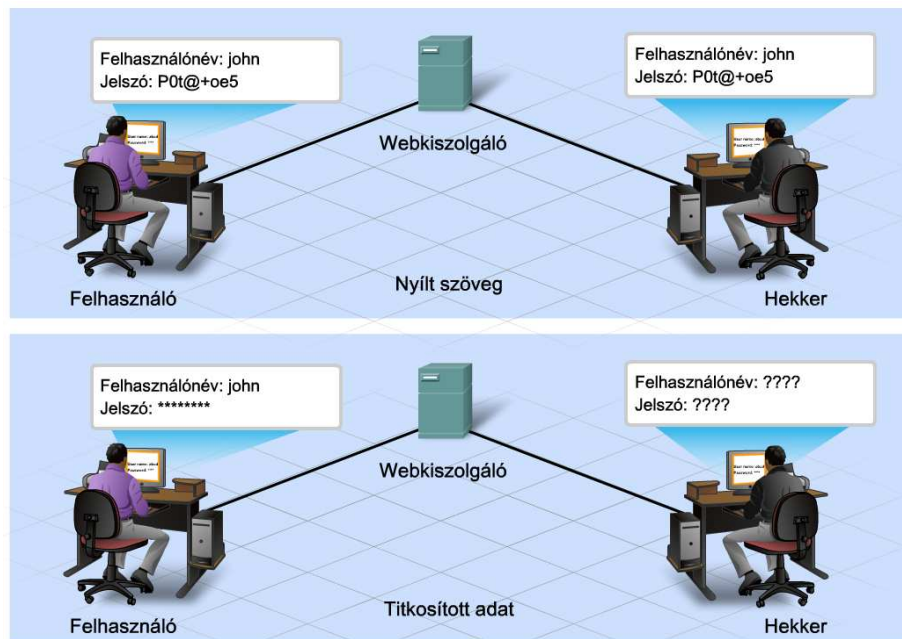
Az internetszolgáltatóknak a kiszolgálók közötti adatforgalom védelmét is biztosítaniuk kell. A hálózatok alapértelmezett adattovábbítása nem biztonságos, nyílt szövegben történik, amelyet illetéktelen felhasználók lehallgathatnak. Az átmenő forgalom adatainak elfogása során az összes, az adatokon beállított állományrendszerbeli védelmet elkerülik. Vannak módszerek a biztonsági problémák elleni védelemre.

Titkosítás

A digitális titkosítás az ügyfél és a kiszolgáló közötti forgalom titkosítását teszi lehetővé. Számos protokoll, amelynek biztonságos változatát használják az adattovábbításhoz, digitális titkosítást alkalmaz. Legjobb minden esetben a protokoll biztonságos változatát használni, valahányszor bizalmas adatokat kell továbbítani állomások között.

Például, amikor egy felhasználó a bejelentkezése során megerősíti a felhasználónevét és jelszavát egy e-kereskedelemmel foglalkozó oldalon, biztonságos protokoll szükséges az adatok védelme érdekében. Szintén elengedhetetlen a biztonságos protokollok használata a hitelkártyával és bankszámlával kapcsolatos adatok használatánál.

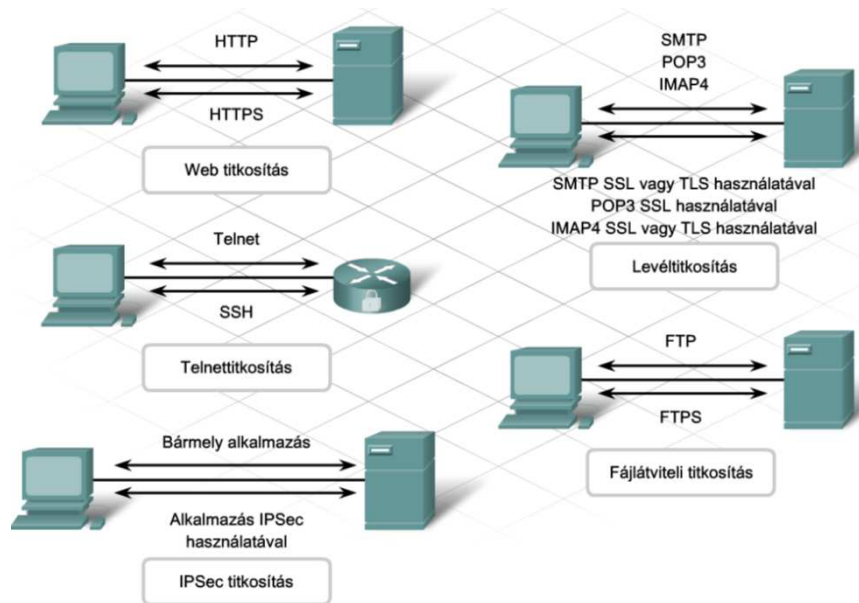
Az internet böngészése és nyilvános honlapok nézegetése közben az adatok biztonságos továbbítása nem szükséges, sőt, felesleges számítási többletet és lassabb válaszidőt eredményezhet.



Az alkalmazások számos hálózati protokollt használnak, melyek közül némelyiknek van biztonságos változata, némelyiknek azonban nincs:

- **Web kiszolgálók** - A Web kiszolgálók HTTP protokollt használnak, amely nem biztonságos. A HTTPS, Biztonságos átviteli protokoll (SSL - Secure Socket Layer) alkalmazásával azonban lehetővé válik a biztonságos adattovábbítás.
- **Levelező kiszolgálók** - Különböző protokollokat használnak, például SMTP, POP3 és IMAP4. A felhasználó bejelentkezése során a POP3 és az IMAP4 felhasználónevet és jelszót kér a hitelesítéshez, amelyeket nem biztonságos módon küldenek. A POP3 SSL segítségével biztonságossá tehető. Az SMTP és az IMAP4 SSL-t és Szállítási rétegbeli biztonság (TLS - Transport Layer Security) protokollt is használhat a védelem érdekében.
- **Telnet kiszolgálók** - Cisco forgalomirányítóra vagy kapcsolóra történő Telnet bejelentkezés esetén a kapcsolat nem biztonságos. A Telnet program a hitelesítő adatokat és a parancsokat nyílt szöveggént küldi a hálózaton keresztül, de a Biztonságos Parancshéj (SSH - Secure Shell) protokoll használatával a hitelesítés és a munka biztonságos módon történik.
- **FTP kiszolgálók** - Az FTP szintén nem biztonságos protokoll, a bejelentkezéshez és a hitelesítéshez kért adatokat nyílt szöveggént továbbítja. SSL használatával a biztonságos adatküldés megvalósítható, és némely verzió SSH alkalmazására is képes.
- **Állománykiszolgálók** - A számítógép operációs rendszerétől függően több különböző protokollt is használhatnak adattovábbításra, de az esetek többségében ezek nem biztonságosak.

Az IP Biztonság (IPSec - IP Security) egy hálózati rétegbeli protokoll, amellyel bármely alkalmazás rétegbeli protokoll használata biztonságos kommunikációt eredményez. Ez magában foglal állománykiszolgáló protokollokat, amelyeket semmilyen más biztonsági protokollverzió nem kínál.



8.2 Biztonsági eszközök

8.2.1 Hozzáférési listák és portszűrés

Még az AAA és a titkosítás használata esetén is, sok különböző típusú támadás ellen kell az ISP-nek védekeznie. Különösen sebezhetők a Szolgáltatásmegtagadási támadásokkal (DoS - denial-of-service) szemben, mivel számos különböző, regisztrált tartománynévvel rendelkező oldalt tárolhatnak, amelyek némelyike igényel hitelesítést, más részük viszont nem. Jelenleg három kulcsfontosságú DoS támadás létezik:

DoS

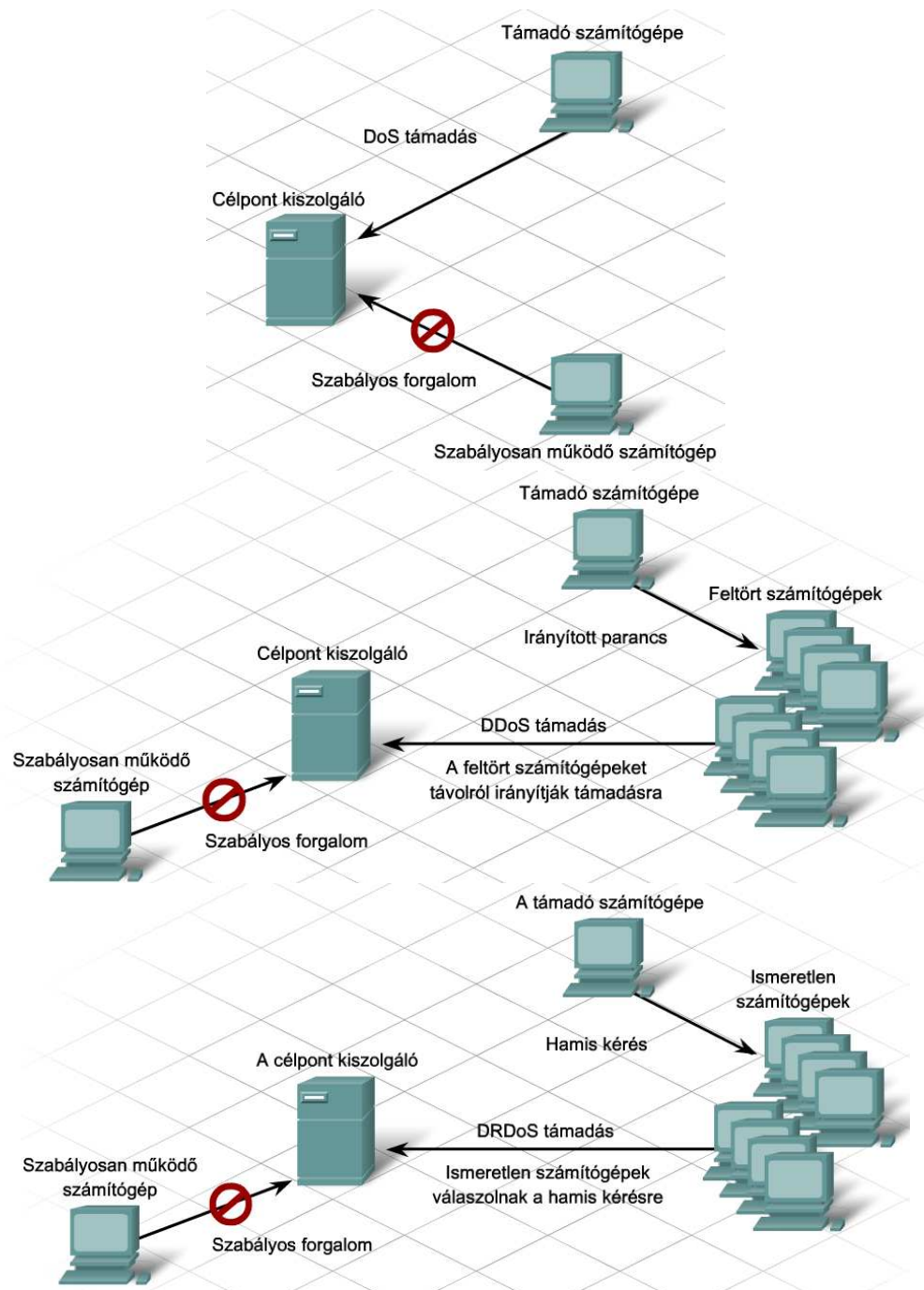
A DoS támadások alapformája a kiszolgáló vagy szolgáltatás elleni támadás a jogos felhasználók hozzáféréseinek megakadályozására. Ilyen például a SYN elárasztás, ping elárasztás, Land támadás, sávszélességet leterhelő támadás és buffer túlcsordulási támadás.

DDoS

Az elosztott szolgáltatásmegtagadási támadás (DDoS - distributed denial-of-service) esetén több számítógép egyszerre lép fel egy meghatározott célpont ellen. A támadó sok feltört számítógéphez fér hozzá, általában interneten keresztül, így módon távolról indíthatja a támadást. A DDoS támadások az alap DoS támadásokhoz hasonlítanak, leszámítva, hogy egyszerre több számítógépről, párhuzamosan indulnak.

DRDoS

Az elosztott reflektált szolgáltatásmegtagadási támadás (DRDoS - distributed reflected denial-of-service) alkalmával a támadó ál- vagy látszatüzenetkérést küld egyszerre több számítógépnek az interneten keresztül, módosítva a forrás címet a célpont számítógép címére. Azok a számítógépek, amelyek a kérést megkapják, mind válaszolnak a célpont számítógép címére. Mivel a támadás reflektált, a támadó kezdeményezőjét nagyon nehéz meghatározni.



Az internetszolgáltatóknak képesnek kell lenniük az olyan hálózati forgalom kiszűrésére, mint például a DoS támadás, amely veszélyezteti a hálózatuk vagy a kiszolgálók működését. A Portsűrítés (Port filtering) és a hozzáférési lista (ACL - access control list) segítségével a kiszolgáló és más hálózati eszközök felé menő adatforgalom szabályozható.

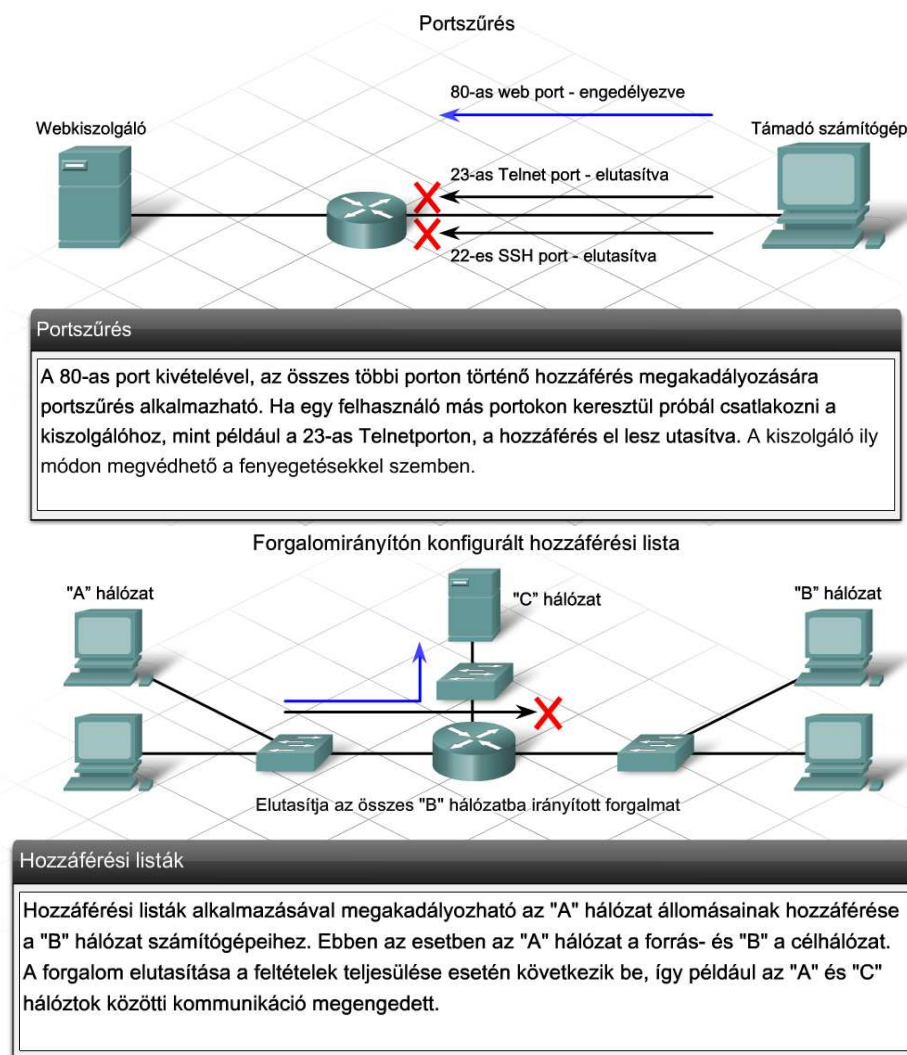
Portsűrítés

Meghatározott TCP vagy UDP portok alapján ellenőrzi az adatforgalmat. Számos kiszolgáló operációs rendszerében van lehetőség a hozzáférések korlátozására portsűrítés segítségével. Hálózati forgalomirányítók és kapcsolók is gyakran használják a forgalom ellenőrzésére és az eszközökhöz való biztonságos hozzáféréshez.

Hozzáférési listák

A hozzáférési listákkal definiálható a tiltott vagy engedélyezett hálózati forgalom a forrás és cél IP-címek alapján, valamint a használt protokoll forrás- és célportjai alapján. Továbbá az ICMP üzenetek és a forgalomirányító protokollok frissítései is ellenőrizhetők. A rendszergazda ACL-eket hoz létre olyan hálózati eszközökön, mint például a forgalomirányító, annak eldöntésére, vajon a forgalom átengedhető-e vagy sem.

Az ACL-ek a védelemnek csak az első lépései, önmagukban nem elégségesek a hálózat biztonságához. Csupán megelőzik a hálózathoz történő hozzáférést, de nem védik meg a rosszindulatú támadások minden fajtájától.



8.2.2 Tűzfalak

A tűzfal olyan hálózati hardver vagy szoftver, amely meghatározza, melyik forgalom jöhet be vagy távozhat a hálózat bizonyos részeiből, illetve hogyan kell az adatokat kezelni.

Az ACL mechanizmus egy a tűzfalak által használt eszközök közül, amelyek szabályozzák, mely forgalom haladjon át a tűzfalon. Az engedélyezett forgalom iránya is szabályozható. Egy közepes méretű hálózatban az ellenőrizni kívánt forgalom, illetve a szabályozandó hálózati protokollok mennyisége igen nagy lehet, így a tűzfalon elhelyezett ACL-ek túl bonyolulttá válhatnak.

A tűzfalak hozzáférési listákat használnak az átengedhető és a letiltandó forgalom ellenőrzésére. Állandóan fejlődnek, ahogy új képességeket fejlesztenek ki, és új fenyegetéseket fedeznek fel.

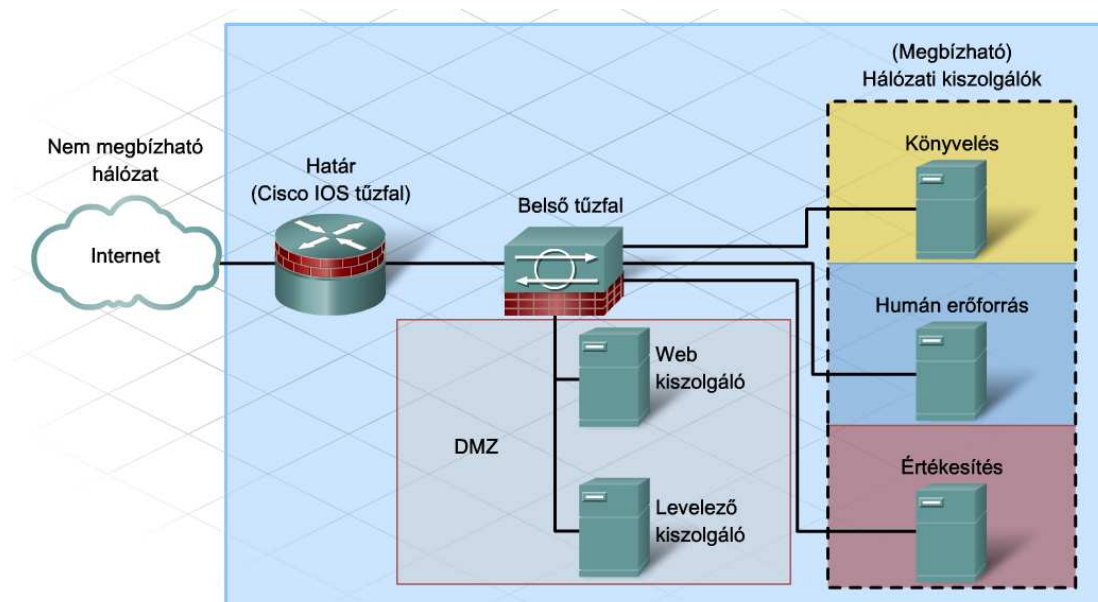
A különböző tűzfalak különböző jellemzőkkel rendelkeznek. Az állapotalapú tűzfalként is ismert dinamikus csomagszűrő tűzfalak állapotábra alkalmazásával képesek a forrás- és céleszközök közötti kommunikáció követésére. Ezek adott adatfolyamok engedélyezését követően csak az azokhoz tartozó forgalom áthaladását engedik a tűzfalon. A Cisco IOS-be ágyazott Cisco IOS tűzfal használatával a forgalomirányítók hálózati rétegbeli dinamikus, állapotalapú csomagszűrő tűzfalként is használhatók.

A tűzfalak állandóan fejlődnek, ahogy új képességeket fejlesztenek ki, és új fenyegetéseket fedeznek fel. Minél több beágyazott funkcióval rendelkeznek, annál több időt vesz igénybe a csomagok feldolgozása.

A tűzfalak a hálózat egész területének határbiztonságát és a belső, helyi szegmensek, például kiszolgáló-farmok, védelmére is jól használhatók.

Egy ISP hálózaton belül vagy egy közepes méretű vállalat hálózatában a tűzfalakat általában több rétegben valósítják meg. A nem megbízható hálózatról bejövő forgalom először egy határforgalomirányító csomagszűrőjén halad át, amelynek belső tűzfala az engedélyezett csomagokat egy demilitarizált zóna felé (DMZ - demilitarized zone) irányítja. A DMZ az internet felől érkező felhasználók számára hozzáférhető kiszolgálókat tárolja és kizárólag az a forgalom érkezik ide, amelyeknek engedélyezett ezekhez a kiszolgálókhoz történő hozzáférése. A tűzfalak a védett, belső hálózatba érkező forgalom típusát is ellenőrzi. Általában a belső eszközök meghatározott kéréseire érkező válaszok engedhetők be a belső hálózatba. Például, ha egy belső eszköz egy külső kiszolgálótól kér egy weboldalt, a tűzfal beengedi.

Némely szervezet belső tűzfalat alkalmaz az érzékeny területek védelmére. Ezek a tűzfalak a fokozott védelmet igénylő területek elérésének korlátozására használhatók. Elkülönítik és védik a kiszolgálókon elhelyezett vállalati erőforrásokat a szervezeten kívüli felhasználóktól, megakadályozzák a külső és belső véletlenszerű vagy akár rosszindulatú támadásoktól.



8.2.3 IDS és IPS

Szintén az internetszolgáltató kötelezettsége, hogy amennyire lehetséges akadályozza meg a saját, és az olyan előfizetők hálózatába történő behatolást, akik fizetnek a szervezett szolgáltatásokért. Ennek érdekében két, gyakran használt megoldás közül választhatnak a szolgáltatók.

Behatolásérzékelő rendszer (IDS - Intrusion Detection System)

Az IDS a hálózati forgalmat passzívan figyelő szoftver- vagy hardver alapú megoldás. Az IDS eszköz a hálózati interfészeken áthaladó forgalmat figyeli, amely az IDS-en nem halad át. Amint rosszindulatú forgalmat észlel, vészüzenetet küld egy előre konfigurált felügyelő állomásnak.

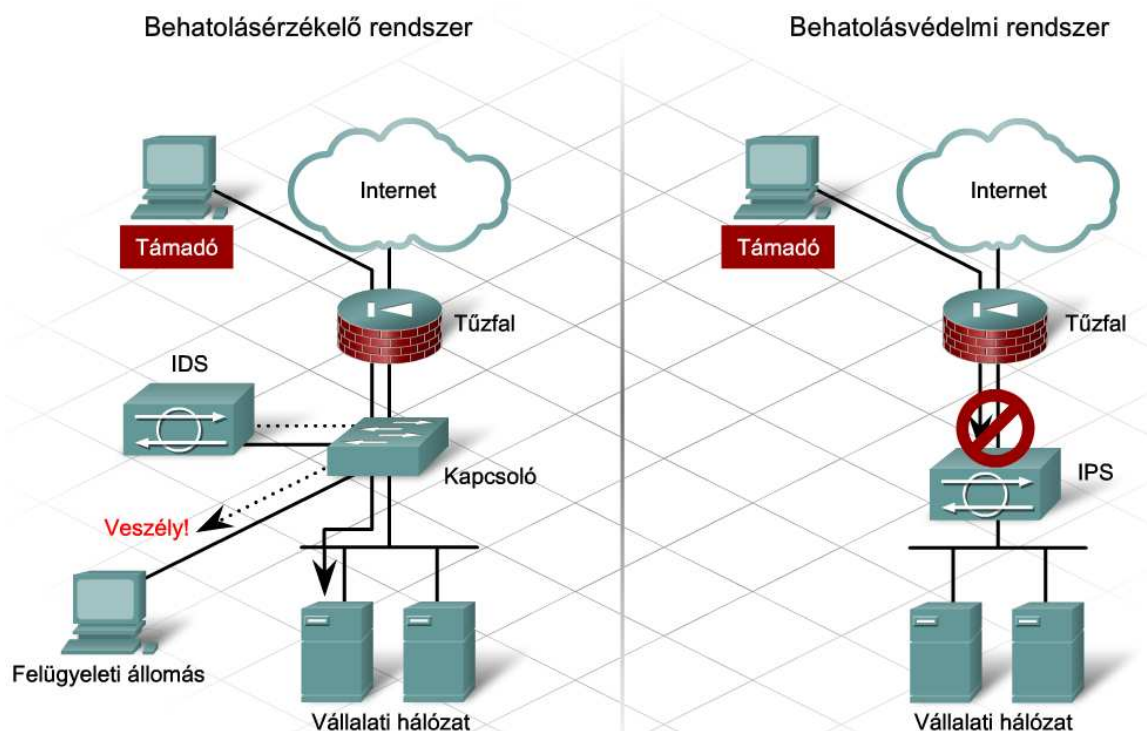
Behatolás megelőző rendszer (IPS - Intrusion Prevention System)

Az IPS aktív fizikai eszköz vagy szoftver. A forgalom az IPS egyik interfészen megy be és a másikon megy ki. Az IPS megvizsgálja a hálózati forgalomban résztvevő aktuális adatsomagokat, és valós időben működve engedi vagy tiltja a hálózatot elérni kívánó csomagokat.

Az IDS és IPS technológia szenzorokon alapul, amelyek az alábbiak lehetnek:

- Cisco IOS IPS-sel ellátott verziójával konfigurált forgalomirányító.
- IDS vagy IPS szolgáltatásra tervezett speciális (hardver) berendezés.
- Adaptív biztonsági berendezésbe (ASA - adaptive security appliance), forgalomirányítóba vagy kapcsolóba épített hálózati modul.

Az IDS és IPS szenzorok különböző módon válaszolnak a hálózatban észlelt, nem megszokott eseményekre, de mindegyiknek saját szerepe van a hálózatban.



Az IDS megoldások reaktívak, a behatolás észlelésekor riasztanak. A behatolást a jellemző hálózati forgalom vagy a számítógép jellemző tevékenységének ismeretében, az attól való eltérés alapján

detektálják. A kezdeti forgalmat nem tudják leállítani a célpont elérése előtt, csak reagálnak a detektált eseményre.

A rosszindulatú forgalom észlelését követően egy helyesen konfigurált IDS meg tudja akadályozni a következő támadásokat az olyan hálózati eszközök újrakonfigurálásával, mint a biztonsági berendezések vagy a forgalomirányítók. Megjegyzendő, hogy a kezdeti támadás keresztülhalad a hálózaton az érintett célpont felé, leállítani nem lehet, csak a további rosszindulatú forgalom akadályozható meg. Ebben a tekintetben, az IDS nem tudja teljes mértékben megakadályozni a sikeres támadást.

Gyakran a hálózatok nem megbízható határvonalában alkalmazzák, a tűzfalon kívül. Itt az IDS tudja elemezni a tűzfal felé haladó forgalom típusokat és meghatározza milyen a végrehajtott támadás. A tűzfallal blokkolható a legtöbb rosszindulatú forgalom. IDS a tűzfalon belül is elhelyezhető a tűzfal félrekonfigurálásának felismerésére. Amikor az IDS itt van elhelyezve, bármely felbukkanó vészjel azt mutatja, hogy rosszindulatú forgalom lett átengedve a tűzfalon. Ezek a vészjelek a tűzfal helytelen konfigurációját jelzik.

IPS

Az IDS megoldásaival ellentétben, melyek reaktívak, az IPS megoldásai proaktívak. Minden gyanús eseményt azonnal blokkolnak. Az IPS majdnem a teljes adatcsomagot képes megvizsgálni az OSI modell második rétegétől a hetedikig. Amikor rosszindulatú forgalmat észlel, azonnal blokkolja, majd vészjelet küld a felügyelő állomásnak a behatolásról. A kiinduló és a rákövetkező támadásokat egyaránt megakadályozza.

Megjegyzendő, hogy az IPS egy behatolás detektáló berendezés, nem pedig egy program. Általában a tűzfalon belül helyezik el, ezért tudja megvizsgálni a teljes adatcsomagot és megvédeni a kiszolgáló alkalmazásokat támadás esetén. A tűzfal általában nem vizsgálja meg a teljes csomagot, mint az IPS, hanem a legtöbb nem engedélyezett csomagokat eldobja, de még így is átengedhet rosszindulatú csomagokat. Mivel az IPS-nek kevesebb számú adatcsomagot kell megvizsgálnia, ellenőrizheti az egész csomagot, így azonnal blokkolhatja az újabb támadásokat, amelyek a tűzfal eredeti konfigurációjában még nem voltak tiltva. Az IPS olyan támadásokat is képes megállítani, amelyeket a tűzfal, saját korlátaiból kifolyólag, nem tud.

4.2.4 Vezeték nélküli hálózatok biztonsága

Némely ISP lehetőséget ad vezeték nélküli hozzáférési pontok (hot spot) létesítésére, amelyeken az előfizetők elérhetik a vezeték nélküli helyi hálózatokat (WLAN - wireless local-area network). WLAN-okat könnyű implementálni, ám könnyen is sebezhetőek rossz konfiguráció esetén. Mivel a vezeték nélküli jelek áthaladnak a falakon, a vállalat területén kívülről is elérhetők. Az alapértelmezett beállítások megváltoztatásával, hitelesítés vagy MAC-cím szűrés beállításával a vezeték nélküli hálózatok védhetők.

Az alapértelmezett beállítások megváltoztatása.

Az SSID, a felhasználónév és a jelszó alapértelmezett beállításait ajánlott megváltoztatni, illetve az SSID üzenetszórását kikapcsolni.

A hitelesítés beállítása

A hitelesítés az a folyamat, mely során hitelesítő információk alapján dől el a belépés engedélyezése. A kapcsolódni kívánó eszközök megbízhatóságának eldöntésére használják. Három hitelesítési módszer használható:

- **Nyílt hitelesítés** - Személytől függetlenül, bármely felhasználó kaphat hozzáférést. Általában nyilvános vezeték nélküli hálózatokban használják.
- **Előre megosztott kulcs (PSK - Pre-shared key)** - A kiszolgálónak és az ügyfélnek egyaránt, egy megegyező, előre konfigurált kulcsra van szüksége. Kapcsolódás esetén, a hozzáférési pont egy véletlen bájtsorozatot küld a felhasználónak, amelyet az titkosít (vagy összekever) a kulcs alapján, majd visszaküld. A hozzáférési pont a titkosított karaktersorozatot a kulcs segítségével visszafejti (vagy visszakeveri). Egyezés esetén a hitelesítés sikeres.
- **Kiterjeszthető hitelesítő protokoll. (EAP - Extensible Authentication Protocol)** - Kölcsönös vagy két-utas hitelesítést és felhasználóhitelesítést tesz lehetővé. Ha EAP-ot használó programot telepítettek egy állomásra, az ügyfél egy kiszolgáló oldali hitelesítő szerverrel kommunikál, mint például a RADIUS.

MAC-cím szűrés beállítása

A MAC-cím szűrés megakadályozza az illetéktelen számítógép hálózatra csatlakozását a MAC-címek korlátozásával. Bár a módszer működik, mégis, mivel a MAC-cím lemásolható, más biztonsági megoldásokkal együtt alkalmazandó!

A legfontosabb a vezeték nélküli hálózaton keresztül küldött adatok titkosítása. WLAN-ok esetén három fontos titkosítási eljárás létezik:

- **Vezetékessel egyenértékű titkosítás (WEP - Wired Equivalent Privacy)** - Vezeték nélküli csomópontok között küldött adatok titkosítására szolgál. 64, 128, vagy 256 bites, előre kiosztott kulcsokat alkalmaz. Legnagyobb hibája a kulcsok állandóságából adódik, azaz minden eszköznél ugyanazt a kulcsot használja az adatok titkosítására. Számos WEP feltörő eszköz érhető el az Interneten, ezért csak régebbi eszközökön használható, amelyek nem támogatják az újabb biztonsági protokollokat.
- **WiFi védett hozzáférés (WPA - Wi-Fi Protected Access)** - egy új vezeték nélküli titkosítási protokoll, amely egy továbbfejlesztett titkosítási algoritmust, az Átmeneti kulcsintegritás protokollt (TKIP - Temporal Key Integrity Protocol) használja. A TKIP egyedi kulcsot generál minden ügyfél számára, amelyeket egy konfigurálható intervallumon belül forgat. Kölcsönös hitelesítési eljárást nyújt, mivel a felhasználó és a hozzáférési pont egyaránt rendelkezik a kulccsal, amelyet sohasem küldenek át a hálózaton.
- **WPA2** - A WPA egy új, továbbfejlesztett változata. A WPA2 a biztonságosabb Fejlett titkosítási szabványt (AES - Advanced Encryption Standard) használja.

8.2.5 A munkaállomások biztonsága

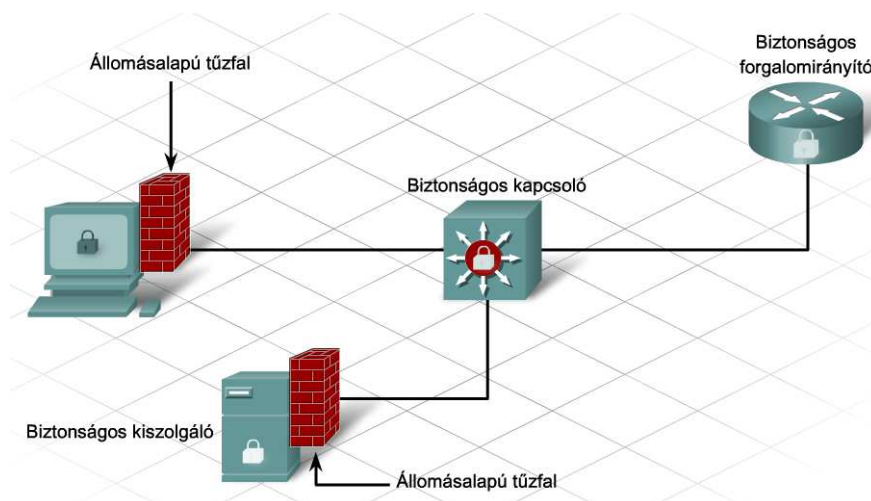
Függetlenül a hálózat védekezési rendszerében megvalósított rétegektől, minden kiszolgáló ki van téve támadásoknak a nem megfelelő biztonsági intézkedések esetén. Az ISP kiszolgálók különösen sebezhetők, mert általában az internetről elérhetőek. A kiszolgálóknak minden nap újabb és újabb sebezhetőségeit fedezik fel, így egy ISP számára kritikus, hogy szervereit védje az ismert és

ismeretlen sebezhetőségeikkel szemben, amikor csak lehetséges. Egy lehetséges megoldást jelentenek az állomásalapú tűzfalak.

Az állomásalapú tűzfal közvetlenül a munkaállomás operációs rendszerén futó program. Megvédi a számítógépet az olyan rosszindulatú támadástól, amelyik a védelem összes többi rétegén keresztüljutott. A hálózaton belüli és kívüli forgalmat egyaránt ellenőrzi. Lehetővé teszi a számítógép címe és portja szerinti szűrést, mely további védekezési lehetőséget ad a hagyományos portszűrésen túl.

Az állomásalapú tűzfalak általában előre meghatározott szabályokkal kaphatók, amelyek blokkolják az összes beérkező forgalmat. A szabályokhoz kivételeket hozzáadva válik engedélyezetté a bejövő és a kimenő forgalom megfelelő aránya. Az állomásalapú tűzfal alkalmazásakor fontos megtartani az egyensúlyt a feladatok elvégzéséhez szükséges erőforások hozzáférhetősége, és a rosszindulatú támadások célpontjait jelentő alkalmazások megelőzése között. Számos kiszolgáló operációs rendszerében egy korlátozott lehetőségű, egyszerű állomásalapú tűzfal található. Fejlettebb, külső gyártók által forgalmazott csomagok szintén elérhetők.

Az ISP-k állomásalapú tűzfalakat használnak arra, hogy korlátozzák egy kiszolgáló által ajánlott specifikus szolgáltatásokhoz való hozzáférést. Egy állomásalapú tűzfal használatával az ISP megvédi a szervereiket és az előfizetőik adatait, a meglévő, de felesleges portjai elérésének blokkolásával.



Az állomásalapú tűzfalakat alkalmazó ISP kiszolgálók védettek a támadások és sebezhetőségek különböző fajtáival szemben.

Ismert támadások

Az állomásalapú tűzfalak frissíthető aláírásoknak is nevezett jellemző aktivitásminták alapján ismerik fel a rosszindulatú tevékenységet, majd blokkolják a forgalmat a támadás által használt porton.

A kihasználható szolgáltatások

Az állomásalapú tűzfalak védik a kihasználható szolgáltatásokat nyújtó kiszolgálókat a szolgáltatás portjain történő elérés megakadályozásával. Némelyek a csomag tartalmát is képesek ellenőrizni a rosszindulatú kódok felismerése érdekében. A web és levelező kiszolgálók népszerű célpontjai a

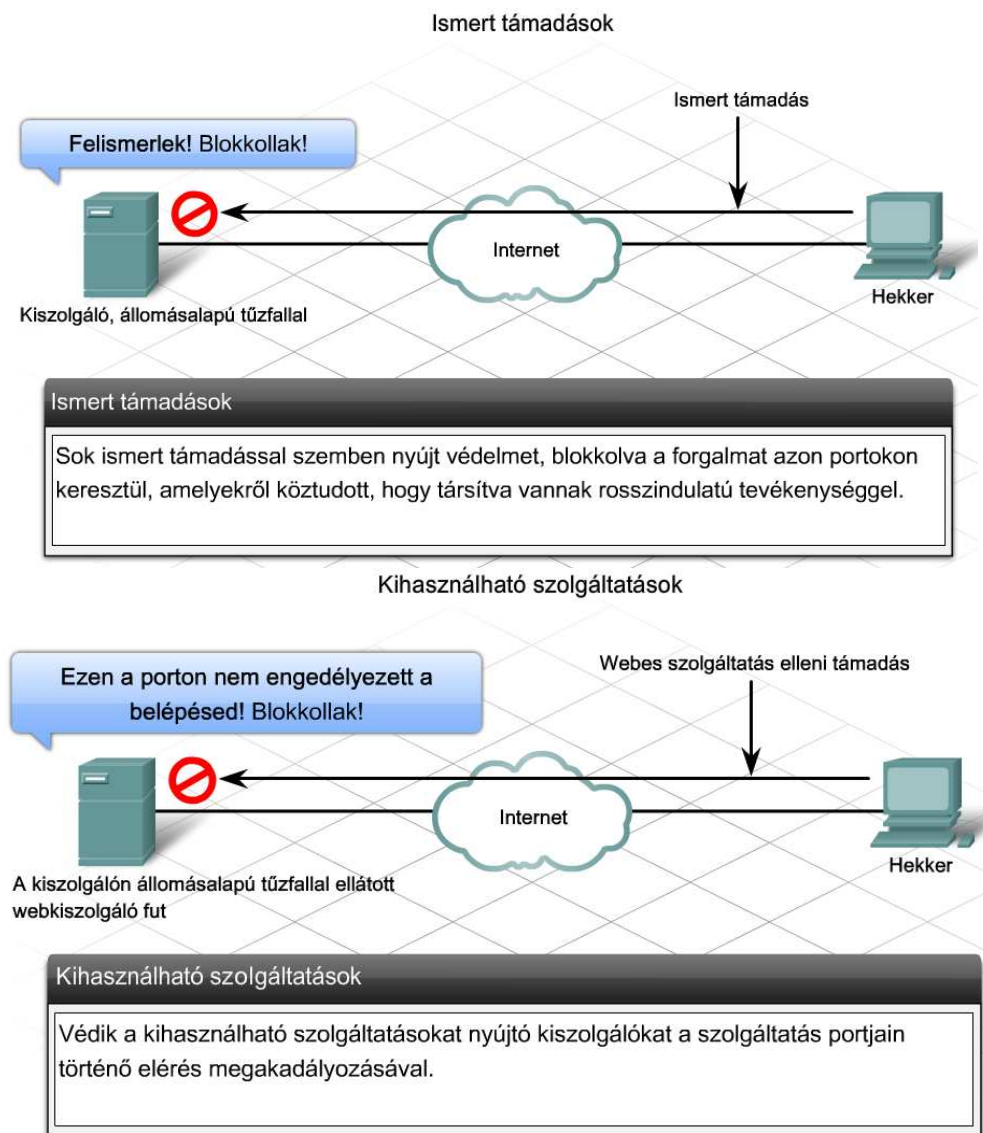
szolgáltatás támadásoknak, de csomagvizsgálatra alkalmas állomásalapú tűzfalak alkalmazásával megvédhetők.

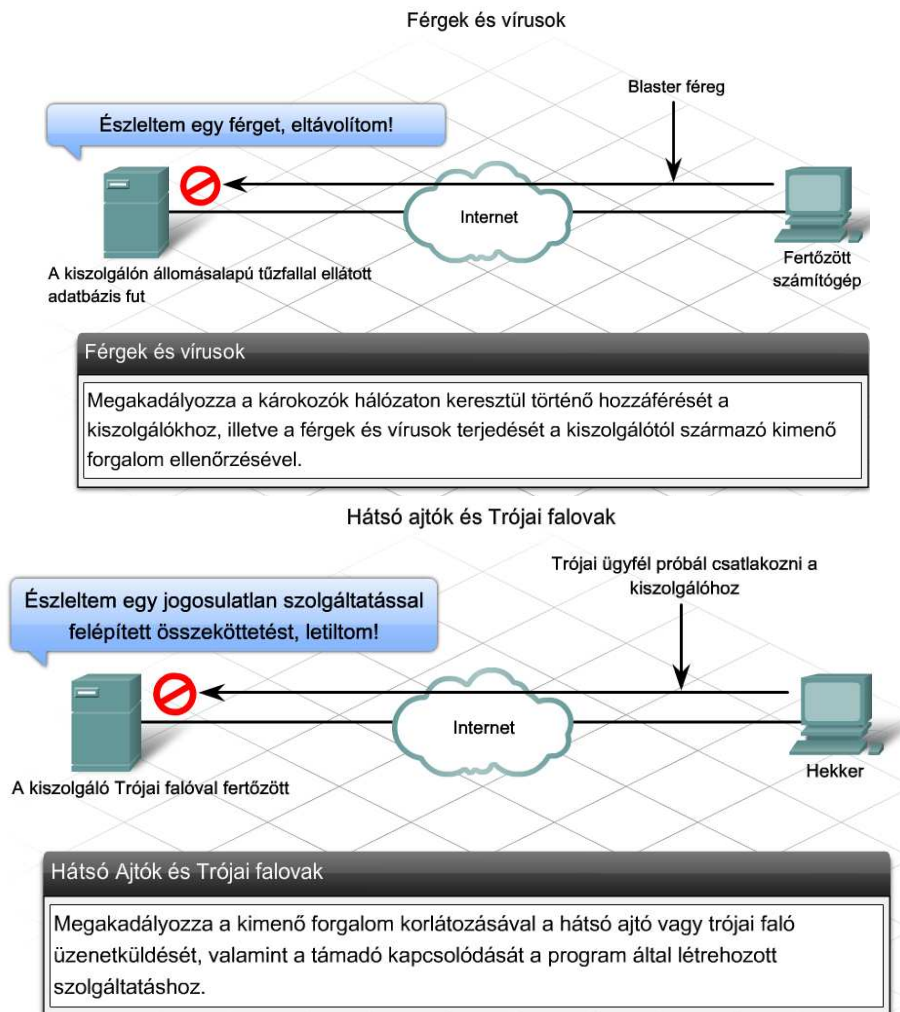
Férgek és vírusok

Férgek és vírusok a szolgáltatások sebezhetőségének kiaknázásával és az operációs rendszerek más gyengeségeivel terjednek. Az állomásalapú tűzfalak megakadályozzák az ilyen rosszindulatú programok hozzáférését a kiszolgálókhoz. Megakadályozhatják a férgek és vírusok terjedését is a kiszolgálótól származó kimenő forgalom ellenőrzésével.

Back Doors és Trójai falovak

A Back door-ok (hátsó ajtó) és Trójai falovak lehetővé teszik a hekkerek távoli hozzáférését a hálózat kiszolgálóihoz. A program általában üzenetet küld a hekkernek, tudatva vele a behatolás sikerességét, majd lehetőséget ad a rendszerhez való hozzáféréséhez. Az állomásalapú tűzfal a kimenőforgalom korlátozásával megakadályozhatja a trójai faló üzenetküldését és a támadó bármely szolgáltatáshoz való kapcsolódását.





Az anti_X program telepítésével még átfogóbb biztonsági szint érhető el. Az anti_X segít a számítógép védelmében a vírusok, férgek, kémprogramok, rosszindulatú programok, adathalászat és még a spam támadásokkal szemben is. Több internetszolgáltató nyújt anti_X programot a teljeskörű biztonsági szolgáltatásaik részeként. Nem minden anti-X szoftver véd meg ugyanazokkal a fenyegetésekkel szemben. Az ISP-nek állandóan szemmel kell tartania, hogy az anti-X szoftver valójában mely veszélyek ellen véd, és a veszélyek elemzése alapján kell javaslatokat tennie.

Számos anti_X programcsomag tesz lehetővé távoli felügyeletet, azaz tartalmaz megfigyelő rendszert, amely elektronikus levélben vagy személyi hívón figyelmezteti az adminisztrátort vagy műszaki szakembert az illetéktelen behatolásról. A megfelelő személy azonnali tájékoztatása jelentősen csökkenti a támadások következményeit. Anti_X használatával a rosszindulatú események száma nem csökkenthető, viszont a fertőzések kockázata igen.

Alkalmanként a fertőzések és támadások erősen romboló hatásúak lehetnek, ezért fontos az esetek felügyelete és a megfelelő megoldások nyomkövetése a fertőzések újból való bekövetkezésének elkerülése érdekében. Az eseményfelügyelethez a felhasználók adatait nyilván kell tartani, mert az internetszolgáltató az előfizetői felé kötelezi magát a védelem és az adatok sértetlenségének biztosítására. Például, ha egy hekker a támadásával hitelkártyaszámok százait lopta el a szolgáltató által felügyelt adatbázisból, értesítenie kell előfizetőit, hogy azok értesíthessék a kártyatulajdonosokat.

8.3 Az ISP megfigyelése és felügyelete

8.3.1 Szolgáltatói szerződés

Az internetszolgáltató és az előfizető között rendszerint szolgáltatói szerződés (SLA - Service Level Agreement) jön létre, mely meghatározza a felek elvárásait és kötelességeit. Általában az alábbi részeket tartalmazza:

- Szolgáltatásleírás
- Költségek
- Megfigyelés és tájékoztatás
- Problémakezelés
- Biztonság (Security)
- Végződtetés
- Kártérítés szolgáltatáskimaradás esetén
- Rendelkezésre állás, teljesítmény és megbízhatóság

Az SLA fontos dokumentum, mely egyértelműen vázolja a hálózat felügyeletét, megfigyelését és fenntartását.



Kártérítés szolgáltatáskimaradás esetén	Költségek
<ul style="list-style-type: none">Leírja a kártérítést a hálózati szolgáltatások meghibásodása esetén. Ez különösen fontos, ha az ISP a vállalat működéséhez elengedhetetlen szolgáltatásokat nyújt.	<ul style="list-style-type: none">Inkább a szolgáltatások, mint a felszerelések meghatározásával, leírja a felhasználó költségeit. Az internetszolgáltatónak lehetősége van a szükséges szolgáltatásokat számlázni, és az előfizető csak a használt szolgáltatásokért fizet.

8.3.2 A hálózati összeköttetések teljesítményének megfigyelése

Az internetszolgáltató köteles figyelemmel kísérni és ellenőrizni az eszközök közötti kapcsolatot. A felelősség magában foglalja az ISP-hez tartozó bármely berendezést, és a felhasználói oldalon lévő azon felszereléseket, amelyeknek az ISP az SLA-ban elvállalta a megfigyelését. A felügyelet és a beállítások történhetnek sávon kívül, közvetlen konzol kapcsolaton keresztül, vagy sávon belül, hálózati kapcsolaton keresztül.

A sávon kívüli felügyelet a kezdeti konfigurációnál hasznos, amikor az eszköz még nem érhető el hálózaton keresztül, vagy ha az eszköz helyszíni megtekintést igényel.

A legtöbb szolgáltatónak nem áll módjában fizikai kapcsolatot teremteni minden eszközzel vagy megtekinteni azokat. A sávon belüli felügyeleti eszközök könnyebb adminisztrációra adnak módot, mert a szakembernek nincs szüksége fizikai kapcsolatra. Emiatt azon felügyeleti kiszolgálók és hálózati eszközök számára, amelyek a hálózatról elérhetőek, a sávon belüli felügyeletet részesítik előnybe a sávon kívülivel szemben. Ráadásul a sávon belüli eszközök hagyományosan több felügyeleti funkciót tesznek lehetővé, mint amelyek a sávon kívüli felügyelettel megvalósíthatók, például egy hálózati eszköz teljes vizsgálatára is mód van. Hagyományos sávon belüli felügyeleti protokollok a Telnet, SSH, HTTP, és az Egyszerű hálózatfelügyeleti protokoll (SNMP - Simple Network Management Protocol).

Számos, ezeket a felügyeleti protokollokat használó beágyazott, kereskedelmi és ingyenes eszköz érhető el, például a web böngésző a HTTP eléréséhez. Néhány alkalmazás, mint a Cisco SDM is, sávon belüli felügyeletre használja e protokollokat.

8.3.3 Eszközfelügyelet sávon belüli eszközökkel

Előfizetői oldalon történő új hálózati eszköz telepítését követően, egy távoli ISP helyről kell a berendezést figyelemmel kísérni. Néha csak a kisebb beállítási változtatásokra van szükség a szakember fizikai jelenléte nélkül.

IP hálózatok esetén Telnet ügyfélprogrammal, sávon belül lehet az eszközhöz kapcsolódni a felügyeleti és adminisztrációs teendők elvégzése érdekében. A Telnet által használt kapcsolatot Virtuális terminál (VTY) kapcsolatnak hívják. A Telnet egy kiszolgáló/ügyfél protokoll. A kapcsolódó eszköz futtatja a Telnet ügyfélprogramot. Telnet ügyfélkapcsolat létesítéséhez a csatlakoztatott eszköznek vagy kiszolgálónak a Telnet démon nevű szolgáltatást kell futtatnia.

A legtöbb operációs rendszer tartalmaz alkalmazás rétegbeli Telnet ügyfélprogramot. A Microsoft Windowst használó számítógépeken a Telnet, parancssorból indítható. Más, közzismert Telnet ügyfelet futtató terminál-emulátor alkalmazások, a HyperTerminal, Minicom, és TeraTerm. A hálózati

eszközök, mint például a forgalomirányítók, a Telnet-démon és a Telnet-ügyfélprogramot egyaránt támogatják, ezért akár ügyfélként, akár kiszolgálóként használhatók.

Egy Telnet kapcsolat felépülését követően a felhasználók bármilyen engedélyezett műveletet végrehajthatnak a kiszolgálón, úgy, mintha magán a kiszolgálón használnák a parancssort. Megfelelő jogosultság esetén a felhasználó elindíthat és leállíthat folyamatokat, konfigurálhatja az eszközt, vagy akár a rendszert is leállíthatja.

Telnet kapcsolatot a forgalomirányító parancssorából a **telnet** parancs és azt követően egy IP-cím vagy egy domain név segítségével lehet kezdeményezni, egyszerre akár több kiszolgálóval is. Cisco forgalomirányítón a Ctrl-Shift-6 X billentyűkombinációval lehet a Telnet kapcsolatok között választani. Ráadásul egy Telnet kiszolgáló képes egyszerre több ügyféllel kommunikálni. Egy kiszolgálóként működő forgalomirányítón a **show sessions** paranccsal megjeleníthetők az ügyfélkapcsolatok.

Bár a telnet a felhasználók hitelesítését támogatja, a hálózaton átküldött adatok titkosítását nem. A telnetkapcsolat teljes adatforgalma nyílt szöveggént továbbítódik, az üzenetek a felhasználónévvel és jelszóval együtt könnyen lehallgathatók.

Amennyiben a biztonság is fontos szerepet játszik, a Secure Shell (SSH) protokoll teremt alternatív megoldást a kiszolgáló biztonságos eléréséhez. Az SSH biztonságos távoli bejelentkezést és más hálózati szolgáltatásokat nyújt, valamint a Telnetnél erősebb hitelesítési módszert és titkosított adatszallítást. A hálózati szakembereknek minden lehetséges esetben az SSH használata ajánlott Telnet helyett.

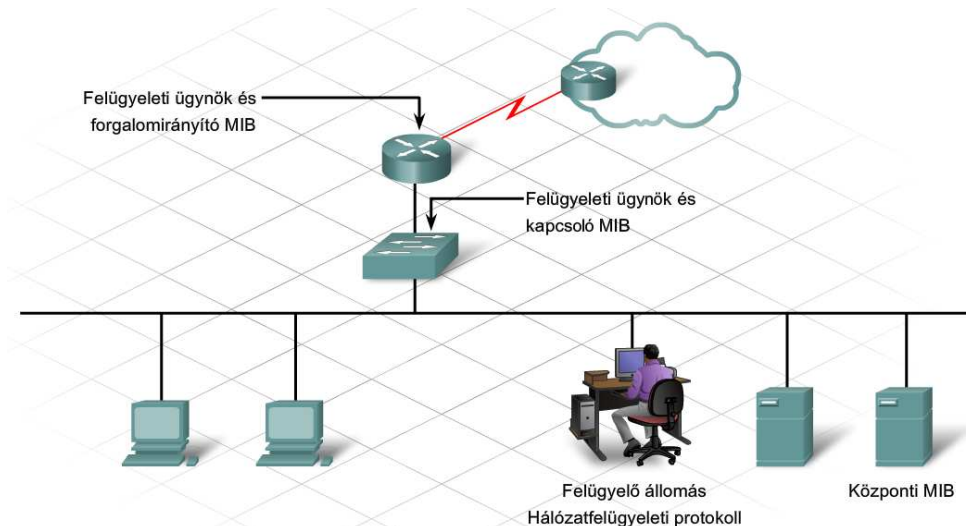
Az SSH kiszolgáló alkalmazásnak két változata létezik, a választás az eszközre betöltött Cisco IOS verziójától függ. Asztali gépen futtatható SSH ügyfél esetén több különböző programcsomag érhető el. Az SSH ügyfélnek támogatnia kell a kiszolgálón konfigurált változatot.

8.3.4 SNMP és Syslog használata

Az SNMP hálózatfelügyeleti protokoll, amely a rendszergazda számára lehetővé teszi hálózati és más eszközökről az adatok összegyűjtését. Az SNMP felügyeleti rendszerprogram elérhető olyan eszközökből, mint a CiscoWorks, melynek ingyenes változata letölthető az internetről. Az SNMP felügyeleti ügynök programokat gyakran a kiszolgálók, forgalomirányítók és kapcsolók operációs rendszerébe ágyazzák be.

Az SNMP négy fő összetevőből áll:

- **Felügyeleti állomás** - A rendszergazda által, a hálózat megfigyelésre és konfigurálására használt állomás, melyen SNMP felügyeleti alkalmazás fut.
- **Felügyeleti ügynök** (Management agent) - Az SNMP által felügyelt eszközön telepített program.
- **Felügyeleti információs adatbázis** (MIB - Management Information Base) - Adatbázis, amelyet az eszközök maguk vezetnek a hálózati teljesítmény paramétereiről.
- **Hálózatfelügyeleti protokoll** - A felügyeleti állomás és az ügynökök között használt kommunikációs protokoll.



A felügyelő állomás futtatja a rendszergazda által a hálózati eszközök konfigurálására használt SNMP alkalmazást. Itt tárolódnak az adatok ezekről az eszközökről. A felügyeleti állomás az eszközök lekérdezésével gyűjti az adatokat. Lekérdezés akkor következik be, amikor a felügyelő állomás meghatározott információkat kér egy ügynöktől.

Az ügynök tájékoztatást ad, válaszolva a lekérdezésre. Amikor a felügyelő állomás lekérdez egy ügynöket, az ügynök előveszi a MIB-ben összegyűjtött statisztikát.

Az SNMP ügynökök nem csak lekérdezhetők, trap-nek nevezett önálló riasztóüzenet elküldésére is konfigurálhatók. A trap egy eseményvezérelt jelzés. Bizonyos területeken az ügynökökön egy küszöb- vagy maximumértéket konfigurálnak, amely például egy meghatározott porton áthaladó adatforgalom mennyiségére vonatkozik. Ha a forgalom mennyisége a küszöböt eléri, az ügynök riasztóüzenetet küld a felügyelő állomásnak. A riasztóüzenetek megkímélik a felügyelő állomásokat a hálózati eszközök folyamatos lekérdezésétől.

A felügyelő állomások és a felügyelt eszközök hitelesítése egy közösségi azonosítónak nevezett karakterlánc alapján történik. Az SNMP ügynök és az SNMP állomás közösségi karakterláncának meg kell egyeznie. Amikor az ügynök egy lekérdezés vagy egy riasztóüzenetet generáló esemény hatására információt küld a felügyelő állomásnak, mindketten először a karakterláncot egyeztetik.

A hálózat megfigyelésének fontos része a device log (eszköz napló) tárolása és rendszeres időközönkénti felülvizsgálata. A Syslog a rendszeresemények naplózására kidolgozott szabvány. Az SNMP-hez hasonlóan egy alkalmazás-rétegbeli protokoll, amely lehetővé teszi az eszközök információküldését a felügyeleti állomáson telepített és futtatott syslog démon számára.

A Syslog rendszer egy kiszolgálóból és egy ügyfélből áll. Az előbbiek fogadják és feldolgozzák az ügyfelek naplózási üzeneteit, az utóbbiak az eszközök megfigyelését végzik, amiről tájékoztatják a Syslog kiszolgálót.

A naplózási üzenetek általában egy azonosítóból, az üzenet típusából, az elküldés időpontját jelölő időbélyegből (dátum, idő) és az üzenet szövegéből állnak. A küldő hálózati eszköztől függően, a felsoroltaknál több elemet is tartalmazhatnak.

8.4 Biztonsági mentések és katasztrófhelyzet helyreállítás

8.4.1 Archiválási hordozók

A hálózatfelügyeleti és megfigyelési programok segítenek az internetszolgáltatóknak és a vállalatoknak azonosítani és kijavítani a hálózatban előforduló problémákat. A olyan hálózati hibák helyreállításában szintén fontos szerepük van, mint a kártékony és rosszindulatú tevékenység, elromlott eszközök, vagy hibás működés okozta problémák.

A hiba okától függetlenül a felhasználók weboldalait és leveleit tároló ISP kötelessége biztosítani az adatvesztés elleni védelmet. A weboldalakon tárolt adatok elvesztése utáni helyreállítás több száz, vagy akár több ezer órát is igénybe vehet, nem beszélve a tartalom elvesztése és újratöltése közti üzleti forgalom kieséséről.

Az ISP levelező kiszolgálóján tárolt üzenetek adatainak elvesztése a vállalatok számára kritikus lehet. Némely vállalkozás számára törvény írja elő a levelezések adatainak megtartását, minek következtében azok megsemmisülése megengedhetetlen.

Az adatok mentése elengedhetetlen. Egy informatikai szakember munkaköréhez tartozik az adatvesztés kockázatának csökkentése, és egy esetleges helyreállítási eljárás megtervezése.

Hardver meghibásodás

A hardverek öregedésével a meghibásodások valószínűsége egyre nő, és vele az adatvesztés lehetősége is. Egy hardverhiba általában jelentős adatvesztéssel jár. A helyreállításhoz a hibás alkatrészt ki kell cserélni, és az adatokat a legutóbbi mentés alapján visszaállítani.

Felhasználói hiba

Felhasználói hiba történhet egy állomány véletlen felülírásával, letörlésével, helytelen szerkesztésével vagy állományon belüli adatok törlésével. Az adatvesztés ezen típusának a kihatása a felhasználóra nagyobb, mint a vállalatra, hiszen a vállalat rendszerint csak termelési időt veszít, mialatt a felhasználónak újra létre kell hoznia az elveszett adatokat. Felhasználói hiba esetén a helyreállítás általában egy meghatározott állomány vagy mappa biztonsági mentésen történő visszakereséséből áll.

Adatlopás

A tolvajok célpontjai laptopok, memóriakártyák, cd-k és dvd-k, szalagok vagy egyéb tárolóeszközök. Amikor egy társaság az adatokat külső telephelyre szállítja, az adatokról másolatot készít. A hordozható adatforrásokkal óvatosan kell bánni. Ajánlott az adatok titkosított formában történő szállítása, így a tolvaj számára használhatatlanná válik az információ.

Rosszindulatú tevékenység

A vírusok és támadók az adatokat megsemmisíthetik. Némely vírusnak meghatározott típusú állományok a célpontjai, mások az adatokat tároló hardverre lehetnek hatással, elérhetetlenné téve azokat. A hekkerek az adatokat módosíthatják is, például weboldalakat tozíthatnak el, hogy figyelmet keltsenek.

Operációs rendszer meghibásodás

Egy rossz javítás vagy egy driverfrissítés komoly operációs rendszerbeli hibákat eredményezhet, a szükséges adatok elérhetőségének megakadályozásával. Ementett rendszerállományokkal az operációs rendszer gyakran visszaállítható a megfelelő működési szintre. Mindazonáltal, az újratelepítés szükséges lehet az összes hiányzó adat helyreállításával együtt.

Amikor az ISP-nek adatai mentésére vagy archiválására van szüksége, a lehetőségek költségének és hatékonyságának egyensúlyban kell lennie. Az archiválási hordozók kiválasztása a számos befolyásoló tényező következtében összetett feladat.

Néhány tényező az alábbi lehet:

- Adat mennyisége
- Tárolóhely költsége
- Tárolóhely teljesítménye
- Tárolóhely megbízhatósága
- A külső tárolás egyszerűsége

Többféle archiválási hordozó létezik, például szalagok, optikai lemezek és félvezető alapú háttértárak.

A szalag máig a legközismertebb külső tárolók egyike, nagy kapacitású, és máig a piac leginkább költséghatékony tárolója. Ha az adatmennyiség meghaladja egyetlen szalag tárolóképességét, a mentési folyamat alatt az automatikus betöltők és könyvtárak cserélgethetik a szalagokat, lehetővé téve annyi adat eltárolását, amennyire szükség van. Az automatikus betöltők és könyvtárak igen költségesek lehetnek, amivel a kis- és középvállalatok általában nem is rendelkeznek, mindamellett nagyobb adatmennyiség esetén, lehetséges, hogy nincs más választásuk.

A szalag hibaérzékenysége nagy, a vezérlőeszközt rendszeresen tisztítani kell a hibátlan működés érdekében. Könnyen elkopik, ezért csak meghatározott ideig használható. A szalagoknak különböző fajtái léteznek:

- Digitális adattároló (DDS - Digital data storage)
- Digitális hangszalag (DAT - Digital audio tape)
- Digitális lineáris szalag (DLT - Digital linear tape)
- Nyílt (formátumú) lineáris szalag (LTO - Linear tape-open)

Mindegyik típus különböző kapacitás és teljesítmény jellemzőkkel rendelkezik.

Optikai lemezek

Az optikai lemez kis mennyiségű adat esetén a legkedveltebb tárolóeszköz. A cd 700 MB, az egyoldalas két rétegű dvd több, mint 8.5 GB adat tárolására képes, a HD-dvd és a Blue-Ray lemezek kapacitása a 25 GB-ot is meghaladhatja. A weboldalak tartalmának a felhasználók és az ISP kiszolgálók közötti hordozására mindkét fél egyaránt optikai tárolókat alkalmazhat. Az optikai hordozók bármely számítógépről könnyen elérhetők cd vagy dvd meghajtó segítségével.



Merevlemezek

A merevlemez alapú mentési rendszerek egyre közkedveltebbé válnak alacsony költségük és nagy tárolási kapacitásuk következtében. Mindamellett a merevlemezek másik helyen történő tárolása nehézkes. A hatalmas lemeztömbök, mint a közvetlenül csatlakoztatott tároló (DAS - direct attached storage), hálózathoz kapcsolt tároló (NAS - network attached storage) és a tároló hálózatok (SAN - storage area network) nem hordozhatók.

A merevlemez alapú mentési rendszerek különböző megvalósításai a szalagos mentési rendszerekkel együttműködnek a külső helyen történő tárolásban. Többszintű biztonsági mentés esetén a merevlemez és a szalagos lehetőségek egyaránt gyors helyreállítási időt tesznek lehetővé a merevlemezen helyileg elérhető adatok és a hosszútávú archiválási megoldások kombinálásával.

Félvezető alapú tároló rendszerek

A félvezető alapú tároló rendszerekközé sorolandó az összes nemfelejtő tárolóeszköz, amelyben nincsenek mozgó részek. A példák széles skálája az 1 GB tárolására képes, kicsi postai bélyeg méretű eszköztől az 1000 GB (1 TB) adat tárolására képes forgalomirányítónak megfelelő méretű eszközökig terjed.

Az adatok gyors tárolási és visszakereshetőségi igénye esetén kitűnő. A félvezető alapú tároló rendszerek alkalmazásai közé sorolhatók az adatbázisgyorsítók, a HD videó letöltők és szerkesztők, az információszolgáltatók és a tárolóhálózatok (Storage Area Network- SAN) A nagy teljesítményű, félvezető alapú tároló rendszerek kirívóan drágák lehetnek, de a technikai fejlődés természetéből fakadóan az árak folyamatosan csökkennek.



Merevlemez



Félvezető alapú tároló

8.4.2 Az állománymentés módszerei

Az archiválási közeg kiválasztása után a mentési módszer kiválasztása következik.

Normál

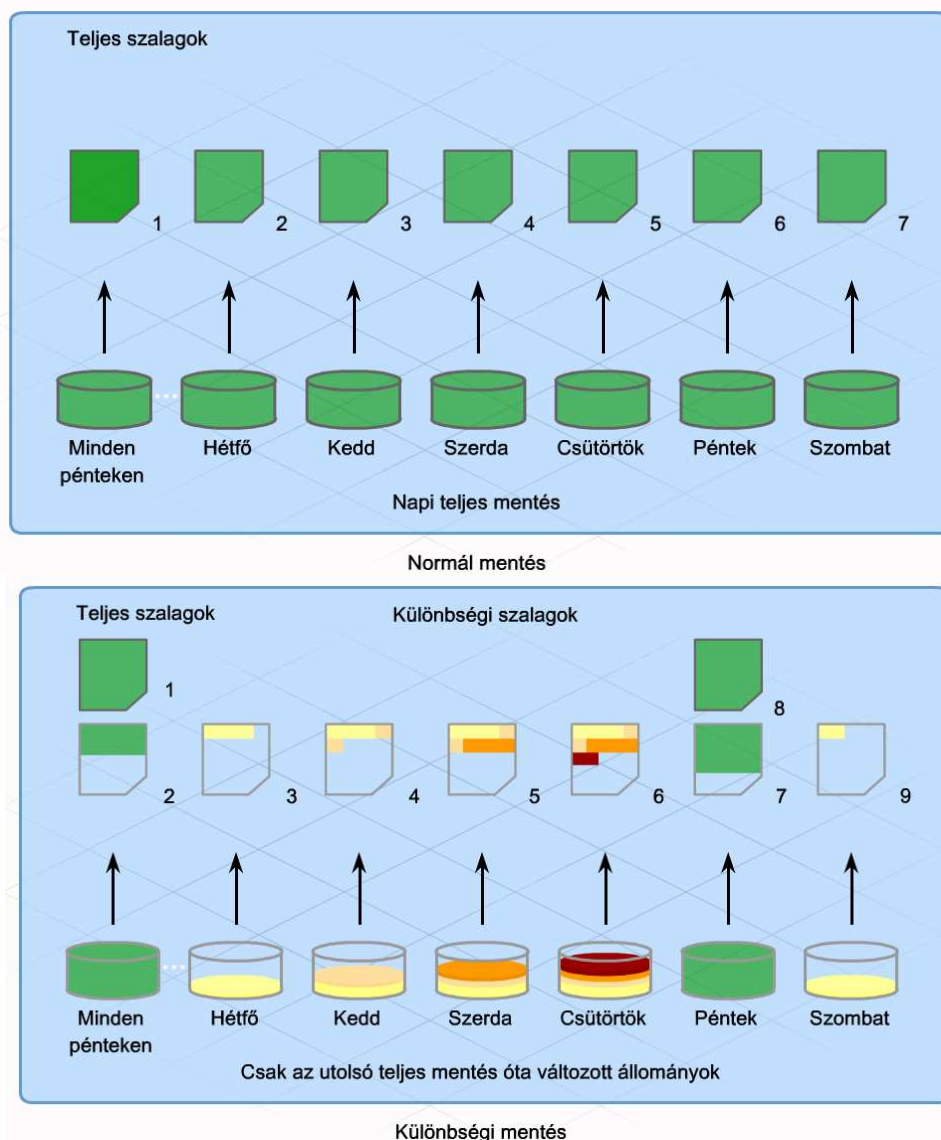
A normál vagy teljes biztonsági mentés során az összes kijelölt állományról másolat készül, teljes egészében. Utána mindegyik állomány kap egy "másolva" jelet. Normál mentések esetén elegendő mindig a legutolsó mentést megtartani, ami meggyorsítja és egyszerűsíti a helyreállítási folyamatot. Mindamellett, mivel mindig a teljes adatállomány mentésére kerül, ez a legidőigényesebb mentési módszer.

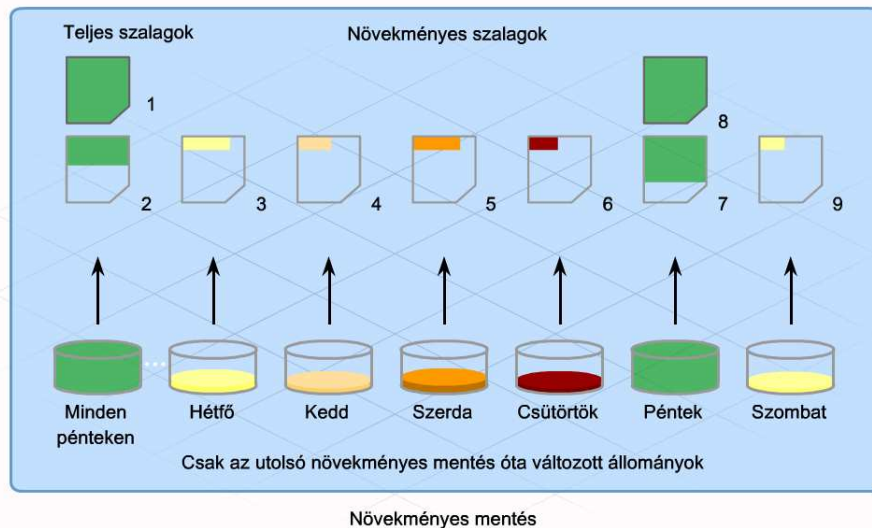
Különbségi

A különbségi mentés esetén, mindig csak a legutolsó teljes mentés óta keletkezett vagy változott állományokról készül másolat. Ennél a módszernél a mentési ciklus első napján teljes mentés szükséges, azt követően pedig mindig csak az ahhoz képest történt változásoké, egészen a ciklus végét jelentő legközelebbi teljes mentésig. Ezáltal a folyamat kevesebb időt vesz igénybe. Az adatok helyreállításához az utolsó teljes és az utolsó különbségi mentés szükséges.

Növekményes

A növekményes mentés egyetlen lényeges pontban tér el a különbségitől. Amíg a különbségi mentés során az utolsó teljes mentés után történt változásokról készül másolat, addig a növekményes esetben az utolsó növekményes mentés óta bekövetkezett változásokat kell elmenteni. Ha minden nap növekményes mentési eljárás történik, az archiválási közege mindig csak az aznapi változások tárolódnak. A növekményes mentési módszer a leggyorsabb, viszont a helyreállítási folyamata a legidőigényesebb, mivel az utolsó normál és az utána következő összes növekményes mentés szükséges hozzá.





A mentési rendszerek a helyes működés érdekében rendszeres karbantartást igényelnek. Léteznek a mentések sikerességét segítő eljárások:

- **Az adathordozók cseréje** - számos mentési módszer igényli az adathordozók napi cseréjét, az elmentett adatok előzményeinek fenntartására. Ha a szalagot vagy lemezt nem cserélik napi rendszerességgel, adatvesztés léphet fel. Mivel a szalagok cseréje kézzel végezhető feladat, ki van téve a hiba bekövetkezésének. A felhasználónak szükségük van egy feljegyzési módszerre, mint a naptár vagy határidőnapló.
- **A mentési naplózások áttekintése** - Jóformán az összes mentésre szolgáló program létrehoz naplózási állományokat. Ezek az állományok tájékoztatnak a művelet sikerességéről, vagy meghatározzák a hiba helyét. A mentési naplózások rendszeres felügyelete lehetővé teszi bármely olyan mentési probléma gyors azonosítását, amely megköveteli a figyelmet.
- **Helyreállítási folyamatok kipróbálása** - Mégha a naplók szerint a mentés sikeres is volt, felmerülhetnek a naplókban nem jelzett, más problémák. Az adatok rendszeres próbahelyreállításával ellenőrizhető az elmentett adatok használhatósága és a mentési eljárás megfelelő működése.
- **Az eszközezőlő karbantartása** - Sok archiválási rendszer speciális hardvereket igényel az eljárás végrehajtásához. A szalagos mentési rendszer a szalag olvasásához és írásához mágnesszalagos egységet használ, amely a használat során piszkolódik, és később mechanikai hibához vezethet. Ezért megfelelő tisztító szalagok segítségével rendszeres tisztítást kell rajta végezni. A merevlemez alapú archiváló rendszereken alkalmanként töredezettség-mentesítés ajánlott a teljesítmény növelése érdekében.

8.4.3 Cisco IOS mentése és helyreállítása

Az ISP számára a kiszolgálók állományainak mentésén túl a hálózati eszközeiken használt, az ISP tulajdonában lévő Cisco IOS és konfigurációs állományok védelmét is biztosítani kell. Ezekről az állományokról is készülhet másolat egy hálózati TFTP kiszolgálón a megfelelő copy parancs segítségével. Az IOS és a konfigurációs állományok mentése hasonló parancsal történik.

A Cisco IOS kód biztonsági mentése három alapvető lépésből áll:



A ROMmon környezeti változóinak beállításához be kell gépelni a változó nevét, majd az egyenlőség (=) jelet, és végül a változó értékét. Például az IP-cím 10.0.0.1-re történő beállításához be kell gépelni az `IP_ADDRESS=10.0.0.1` parancsot.

A szükséges környezeti változók a következők:

- `IP_ADDRESS` - a LAN interfész IP-címe
- `IP_SUBNET_MASK` - a LAN interfész alhálózati maszkja
- `DEFAULT_GATEWAY` - a LAN interfész alapértelmezett átjárója
- `TFTP_SERVER` - a TFTP kiszolgáló IP-címe
- `TFTP_FILE` - a Cisco IOS állományneve a kiszolgálón

A `set` parancs használatával a ROMmon környezeti változói megnézhetők és ellenőrizhetők.

A változók beállítása után a `tftpdnld` parancsot kell használni. Az Cisco IOS állomány összes adatcsomagjának megérkezése után egy felkiáltó jel (!) jelenik meg. Amint az IOS másolata elkészül, a Flash memória meglévő tartalma kitörlődik, melybe nem csak az aktuális IOS fájl, hanem az összes itt tárolt állomány is beletartozik. Ezért ezek megóvása és szükség esetén helyreállítása érdekében a másolatok TFTP kiszolgálón történő ideiglenes tárolása elengedhetetlen.

A ROMmon parancssorának (rommon1>) megjelenésekor a forgalomirányító a `reset` parancs, vagy az `i` begépelésével újraindítható. A forgalomirányító most a flash memóriában tárolt új Cisco IOS rendszerkód alapján fog indulni.

```
rommon1> IP_ADDRESS=192.168.1.2
rommon2> IP_SUBNET_MASK=255.255.255.0
rommon3> DEFAULT_GATEWAY=192.168.1.1
rommon4> TFTP_SERVER=192.168.1.1
rommon5> TFTP_FILE=c1841-ipbase-mz.123-14.T7.bin

rommon7> tftpdnld

      IP_ADDRESS: 192.168.1.2
      IP_SUBNET_MASK: 255.255.255.0
      DEFAULT_GATEWAY: 192.168.1.1
      TFTP_SERVER: 192.168.1.1
      TFTP_FILE: c1841-ipbase-mz.123-14.T7.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n:  [n]:
Do you wish to continue? y/n:  [n]: y <CR>

Receiving c1841-ipbase-mz.123-14.T7.bin from 192.168.1.1
!!!!!!!!!!(output omitted)!!!!!!!!!!
File reception completed.
Copying file c1841-ipbase-mz.123-14.T7.bin to flash.
Erasing flash at 0x607c0000
program flash location 0x605a0000
```

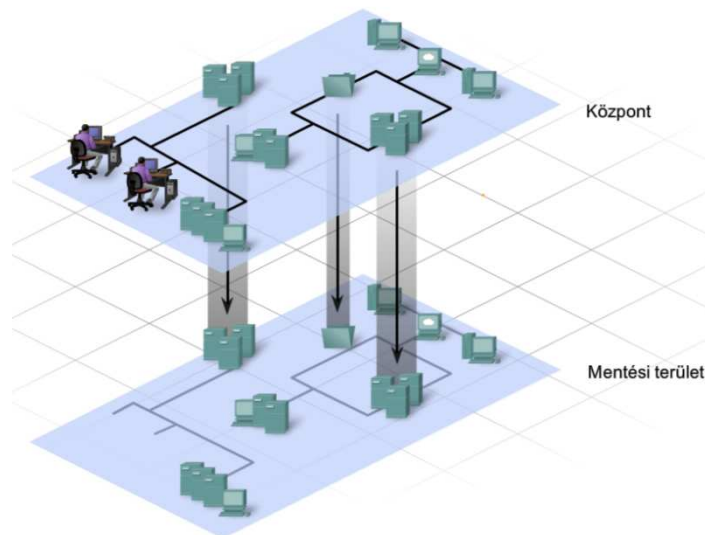
8.4.4 Katasztrófa-helyreállítási terv

A katasztrófa-helyreállítási tervének fontos része az adatok biztonsági mentése. A katasztrófa-helyreállítási terv egy mindent átfogó dokumentum a gyors tárolási folyamatokról, és a vállalat katasztrófa alatti és utáni folyamatos működésének fenntartási feltételeiről. Célja a

vállalat katasztrófa okozta fizikai és szociális változásokhoz történő alkalmazkodásának biztosítása. Katasztrófa lehet, a hálózat szerkezetét érintő természeti csapásoktól kezdve a hálózatot ért rosszindulatú támadásokig, bármi.

A katasztrófahelyzet-helyreállítási terv információkat tartalmazhat más telephelyekről, ahova a szolgáltatások áttehetők, a hálózati eszközök és kiszolgálók kikapcsolásáról, valamint a tartalék csatlakozási lehetőségekről. A terv elkészítése során elengedhetetlen a működés fenntartásához szükséges kritikus szolgáltatások teljes megértése. Katasztrófahelyzet esetén is elérhetőnek kell lennie az alábbi szolgáltatásoknak:

- Adatbázisok
- Alkalmazáskiszolgálók
- Rendszerfelügyeleti kiszolgálók
- Web
- Adattárolók
- Címtár



A katasztrófahelyzet-helyreállítási terv készítésénél fontos megérteni a szervezet igényeit és elnyerni a támogatását. Sok lépés kell egy hatékony helyreállítási terv elkészítéséhez.

- **Sebezhetőségfelmérés** - Fel kell mérni a kritikus vállalati folyamatok és alkalmazásaik sérülékenységeinek mértékét egy hétköznapi katasztrófa esetén.
- **Kockázatfelmérés** - Elemezni kell az esetleges katasztrófa és hatásainak kockázatát illetve költségét. A kockázati felmérés részeként össze kell állítani a tíz legvalószínűbb katasztrófa listáját a következményeikkel együtt, beleértve a vállalat teljes megsemmisülését is.
- **Szervezési tudatosság** - Használja fel a sebezhetőségekről és a kockázatokról összegyűjtött információkat, hogy elnyerje a felsőbb vezetés támogatását a katasztrófahelyzet-helyreállítási projekthez. A felszerelések és elhelyezkedések fenntartása egy esetleges katasztrófa helyzet helyreállításban igen költséges lehet, ezért a vezetőkkel fontos megértetni a lehetséges következményeket.
- **Tervező csoport felállítása** - Fel kell állítani egy tervező csoportot a katasztrófahelyzet-helyreállítási stratégia és terv kidolgozására és megvalósítására. Akár kis vagy közepes

mértékű katasztrófa esetén is fontos, hogy mindenki tisztában legyen a feladataival és kötelezettségeivel.

- **Elsőbbségi sorrend felállítása** - Prioritást kell rendelni minden, a vállalat hálózatát, alkalmazásait és rendszereit érintő lehetséges katasztrófahelyzethez, úgymint kritikus, fontos vagy kevésbé fontos.

A tervhez először a vezetőséget kell megnyerni, majd végül mindenkit, aki a kritikus vállalati folyamatokban dolgozik. A siker érdekében mindenkinek részt kell vennie benne, és támogatnia kell a tervet.

A vállalkozás számára legfontosabb alkalmazások és szolgáltatások meghatározását követően, a gyűjtött információk alapján el kell készíteni a katasztrófahelyzet-helyreállítási tervet. Öt fő lépés szükséges a terv megvalósításához:

1. lépés - Hálózathelyreállító stratégia

A hálózat tervének elemzése. A hálózat tervénél figyelembe vett katasztrófahelyreállítási szempontok a következők:

- Vajon a tervezett hálózat túlélne-e egy nagyobb katasztrófát? Léteznek-e tartalék kapcsolatok és redundanciák a hálózatban?
- Azok a nem helyszínen tárolt kiszolgálók, melyek olyan alkalmazásokat támogatnak, mint a levelezés vagy adatbázis-kezelés, elérhetők maradnak-e?
- Megszakadna-e a tartalék forgalomirányítók, kapcsolók és más hálózati eszközök elérhetősége?
- A hálózat számára szükséges erőforrások és szolgáltatások elhelyezkedése nagy földrajzi területre terjed-e ki?

2. lépés - Leltár és dokumentáció

Leltár készítése az összes helyről, az összes eszközről, gyártóról, a felhasznált szolgáltatásokról és a kapcsolatok neveiről! A kockázatfelmérési lépésben megbecsült költség ellenőrzése.

3. lépés - Ellenőrzés

Olyan tesztfolyamat létrehozása, melynek segítségével ellenőrizhető a katasztrófahelyreállítási stratégia működőképessége. Bevált katasztrófahelyzet-helyreállítási gyakorlat a terv korszerűségének és hatékonyságának biztosítására.

4. fázis - Jóváhagyás és megvalósítás

A felsővezetők jóváhagyásának elnyerése, és a terv megvalósítási költségvetésének elkészítése.

5. fázis - Felülvizsgálat

A katasztrófahelyreállítási tervzet megvalósítását követő első évben a terv felülvizsgálata.

8.5 A fejezet összefoglalása

- Előfizetők számára elérhető asztali szolgáltatások: biztonságos jelszó, biztonsági alkalmazások javításokkal és frissítésekkel, a nem használt alkalmazások eltávolítása, biztonsági vizsgálatok végzése és a megfelelő hozzáférési jogosultságok beállítása.
- Állományok és könyvtárak jogosultságainak beállításakor a "lehető legkevesebb előjog elve" alapján érhető el a legjobb biztonság.
- Hitelesítés, Jogosultságellenőrzés és Azonosítás (AAA) egy három lépéses eljárás a hálózati hozzáférések figyelemmel kísérésére és ellenőrzésére. Adatbázis alkalmazásával tartja nyilván a felhasználói jelszavakat, jogosultságokat és azonosító statisztikákat.
- A digitális titkosítás a kiszolgálók és ügyfelek közötti forgalom titkosítását teszi lehetővé. Számos protokollnak létezik biztonságos változata.
- Legjobb minden esetben a protokoll biztonságos változatát használni, valahányszor bizalmas adatokat kell továbbítani hálózaton keresztül.
- Számos biztonsági fenyegetés létezik, mint DoS, DDoS és DRDoS támadások.
- A portszűrés és hozzáférési listák használata védelmet nyújt az ilyen veszélyek ellen.
- A portszűrés alkalmazásával TCP és UDP port alapján a forgalom korlátozható vagy átengedhető.
- A hozzáférési listákkal IP-címek, vagy akár UDP és TCP portok alapján definiálható a tiltott vagy az engedélyezett forgalom.
- A tűzfal olyan hálózati hardver vagy szoftver, amely meghatározza melyik forgalom jöhet be vagy távozhat a hálózat bizonyos részeiből.
- Az IDS a hálózati forgalmat passzívan figyelő szoftver- vagy hardveralapú megoldás. Nem akadályozza meg a kezdeti támadó forgalom hálózaton történő áthaladását és a cél elérését.
- Az IPS aktív fizikai eszköz vagy szoftver. A forgalom ténylegesen áthalad az IPS interfészekén és az IPS képes valós időben blokkolni az összes gyanús forgalmat.
- Az állomásalapú tűzfal és az Anti-X program közvetlenül a munkaállomás operációs rendszerén futó program. Védi a számítógépet olyan rosszindulatú támadásokkal szemben, amelyek a védelem összes többi rétegén keresztüljutottak.



- A szolgáltatói szerződés (SLA) az internetszolgáltató és a felhasználó között létrejött szerződés, mely világosan dokumentálja a felek elvárásait és kötelelességeit.
- Az ISP-k figyelemmel kísérik és ellenőrzik az eszközök közötti kapcsolatot. Ezt sávon belüli és sávon kívüli kezeléssel hajtják végre. Sávon belüli felügyelet kedvezőbb a hálózaton keresztül elérhető kiszolgálók elérése esetén.
- Biztonsági mentések elvégzésére több megoldás kínálkozik, például szalag, optikai lemez vagy félvezető alapú tároló.
- Három módszer létezik az adatok mentésére: teljes mentés, különbségi mentés és növekményes mentés. Általában a három módszer kombinált használata ajánlott.
- A katasztrófa-helyzet-helyreállítási terv egy mindent átfogó dokumentum a gyors helyreállítási folyamatokról és egy vállalat katasztrófa alatti és utáni folyamatos működését lehetővé tevő feltételekről.
- Elkészítéséhez a sebezhetőségek és kockázatok felbecsülése, vezetői tudatosság, tervezési csoport felállítása és a prioritások meghatározása szükséges.

9. Hibaelhárítás

9.1 Hibaelhárítási módszerek és eszközök

A hálózati szakemberek egyik legfontosabb képessége a hálózati problémák megoldásának képessége. A jó problémamegoldó képességgel rendelkező hálózati szakemberek mindig keresettek. Éppen ezért a Cisco képesítések vizsgái a hálózati hibák felismerésére és megoldására helyezik a hangsúlyt.

A hálózati hibaelhárítás során a szakemberek általában az OSI referenciamodell vagy a TCP/IP hálózati modell segítségével határolják be a hiba lehetséges okát. A logikai hálózati modellek rétegekre bontják a hálózati működést. Az OSI és a TCP/IP modell rétegei jól meghatározott feladatokat látnak el adott protokollokkal. A hibaelhárítás során nagyban megkönnyíti a szakember munkáját, ha tisztában van az egyes rétegek feladataival, jellemzőivel, az azokhoz tartozó eszközökkel, illetve az adott réteg többi réteghez való viszonyával.

A fejezet során az OSI és a TCP/IP modell mentén épül fel a hálózati hibaelhárítás szerkezete. A fejezet elkezdése előtt érdemes átismételni a CCNA Discovery: Otthoni és kisvállalati hálózatok és CCNA Discovery: Hálózati feladatok kis- és középvállalatoknál vagy internetszolgáltatóknál tananyag OSI és TCP/IP modellre vonatkozó részeit!

Az OSI referenciamodell mint hibaelhárítási segédeszköz

Az OSI referenciamodell a hálózati technikusok és fejlesztőmérnökök közös nyelve. Fontos megérteni az OSI modell egyes rétegeiben felmerülő feladatokat, és megismerni e feladatok végrehajtását szolgáló hálózati eszközöket.

Az OSI modell felsőbb (5-7) rétegei jellemzően speciális alkalmazási funkciót látnak el, többnyire szoftveresen valósítják meg őket. A problémák gyökere általában az ügyfél vagy a kiszolgálói oldalon futó végfelhasználói szoftverek beállításáiban keresendő.

Az OSI modell alsóbb (1-4) rétegei elsősorban az adattovábbítási kérdésekért felelősek.

A 3. (hálózati) és 4. (szállítási) réteget általában teljesen szoftveresen valósítják meg. Egyúttal a végrendszerek szoftveres hibáit, és a forgalomirányítók és tűzfalak konfigurációs hibáit tartják felelősnek e két rétegben előforduló problémák többségéért. Az IP-címzési és a forgalomirányítási hibák a 3. rétegre jellemzőek.

Az 1. (fizikai) és a 2. (adatkapcsolati) réteg szoftveres és hardveres összetevőkből épül fel. A fizikai réteg az átviteli közeghez (mint például a kábelezés) áll legközelebb, és ez a réteg a felelős az adatok átviteli közegre juttatásáért. Az 1. és a 2. rétegben előforduló hibák zöméért hardveres vagy kompatibilitási problémák okolhatók.

9.1.2 Hibaelhárítási módszerek

A hálózati modellekkel végzett munka során három fő hibaelhárítási megközelítés alkalmazható:

- Fentről lefelé
- Alulról felfelé
- Oszd meg és uralkodj

Mindhárom megközelítés alapja a hálózati működés rétegekre bontása. Elsődleges céljuk, hogy a hibaelhárítást végző személy könnyen tudja az egyes rétegek működési funkcióit ellenőrizni, illetve a hibát egy adott rétegre behatárolni.

Fentről lefelé - Az alkalmazási réteggel kezd és rétegenként halad lefelé. A problémát a felhasználó és az alkalmazás szemszögéből nézi. Csak egy alkalmazás nem működik vagy egyik sem? A felhasználó például eléri a különböző weblapokat az interneten, de az elektronikus levelezést nem? A többi állomáson is tapasztalhatók hasonló problémák?

Alulról felfelé - A fizikai réteggel kezd és rétegenként halad felfelé. A fizikai réteg a kábelezésre és a fizikai összetevőkre koncentrál. Nem lazult meg egyik kábel sem? Amennyiben vannak kijelző fények az eszközön, azok világítanak vagy sem?

Oszd meg és uralkodj - Valamelyik közbülső réteggel kezd és onnan halad rétegenként felfelé vagy lefelé. A hibaelhárítást végző szakember kezheti például az IP-címzési beállítások ellenőrzésével.

Ezek a hibaelhárítási módszerek tökéletesek lehetnek kezdő hibaelhárító személyeknek. A tapasztaltabbak gyakran mellőzik ezeket a strukturált módszereket és ösztöneikben, illetve tapasztalataikban bízhatnak.

Hibaelhárítási módszer	Működése	Alkalmazhatósági esetek	Előnyök/Hátrányok
Fentről lefelé	Mindig az alkalmazási rétegnél kezdjük és addig haladunk lefelé, míg meg nem találjuk a hibás réteget.	Alkalmazható egyszerűbb problémák esetén vagy akkor, amikor gyanítható, hogy az alkalmazási/felhasználói vagy a felsőbb rétegek érintettek.	Ha kiderül, hogy a probléma az alsóbb rétegekhez kapcsolódik, sok idő és energia veszett el a felsőbb vagy az alkalmazási rétegekben.

Hibaelhárítási módszer	Működése	Alkalmazhatósági esetek	Előnyök/Hátrányok
Oszd meg és uralkodj	A körülményektől (a jelentett problémáktól) és tapasztalatunktól függően, valamelyik rétegnél kezdjük a hibaelhárítást, és lefelé vagy felfelé haladunk az OSI modell rétegeiben.	Akkor a legmegfelelőbb, amikor már tapasztalattal rendelkezünk, és egyértelmű jelek utalnak a problémára.	A módszer a problémás réteget célozza meg, így gyorsabb más megközelítésekénél. Hatékony alkalmazásához tapasztalat szükséges.

Hibaelhárítási módszer	Működése	Alkalmazhatósági esetek	Előnyök/Hátrányok
Lentről-felfelé	Mindig a fizikai rétegben kezdjük a hibaelhárítást, és addig haladunk felfelé, amíg meg nem találjuk a hibás réteget.	Bonyolult problémákra alkalmasabb.	Lassú, de biztos módszer. Amikor a probléma az alkalmazáshoz (vagy felsőbb rétegekhez) kapcsolódik, ez a módszer hosszadalmas lehet.

9.1.3 Hibaelhárítási eszközök

A hálózati kapcsolatok hibaelhárítását nagyban megnehezíti, ha nem áll rendelkezésre az IP-címeket, útvonalakat és eszközöket (tűzfalak, kapcsolók) pontosan feltüntető hálózati rajz. A hibaelhárítás során felbecsülhetetlen értéket képviselnek a pontos fizikai és logikai topológia-rajzok.

Fizikai topológiák

A fizikai topológia mutatja meg a hálózatba kötött eszközök tényleges, fizikai kapcsolódásait, melyek ismerete nélkülözhetetlen a fizikai réteg hibáinak - például a kábelezési és hardveres hibák - feltárása során. A rajz általában az alábbi részleteket tartalmazza:

- Az eszköz fajtája
- Az eszköz típusa és gyártója
- Helyszínek
- Az operációs rendszer verziója
- Kábeltípusok és azonosítók
- Kábelezési végpontok

Logikai topológiák

A logikai topológia mutatja meg, hogyan áramlanak az adatok a hálózatban. Az egyes hálózati eszközök (forgalomirányítók, kiszolgálók, hubok, állomások és biztonsági berendezések) külön jelölést kapnak. A rajz általában az alábbi részleteket tartalmazza:

- Eszköz azonosító
- IP-cím és alhálózati maszk
- Interfész azonosító
- Irányító protokollok
- Statikus és alapértelmezett útvonalak
- Adatkapcsolati rétegbeli protokollok
- WAN-technológiák

A hálózati diagram mellett számos további eszköz segítheti a hatékony hibaelhárítást a hálózati teljesítmény javítása és a rendszerhibák feltárása során.

Hálózati dokumentációs és alapszint-ellenőrző eszközök

Ilyen eszközök szép számban állnak rendelkezésre Windows, Linux és UNIX operációs rendszerekhez is. A CiscoWorks nevű szoftver kiválóan alkalmas a hálózati diagramok megrajzolására, a szoftver- és hardverdokumentáció naprakészen tartására, valamint a jellemző hálózati sávszélességigény költséghatékony felmérésére. A hálózati működés alapszintjének meghatározásához ezek a szoftverek általában monitorozó és jelentéskészítő eszközöket biztosítanak.

Hálózatfelügyeleti rendszereszközök

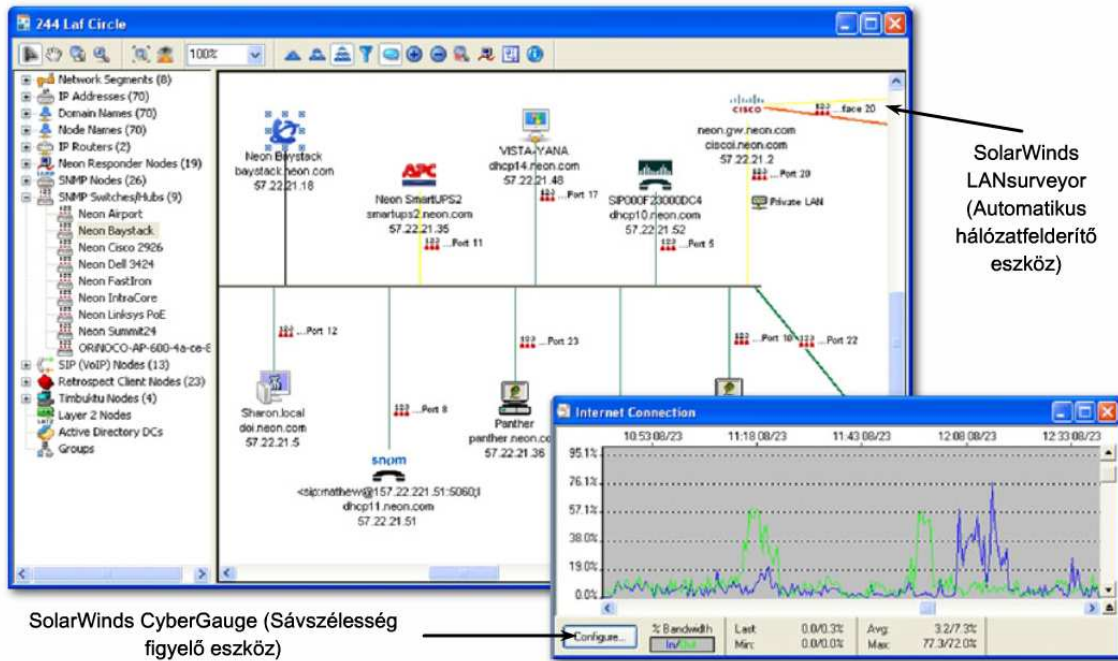
A hálózatfelügyeleti rendszereszközök (NMS - Network Management System tools) elsődleges feladata a hálózat teljesítményének követése. A hálózati eszközök fizikai elrendezését jelenítik meg grafikusán. Meghibásodás esetén ezekkel az eszközökkel meghatározható a hiba forrása, továbbá kideríthető, hogy rosszindulatú program, betörési kísérlet vagy egy eszköz meghibásodása okozta a hibát. A gyakran használt hálózatfelügyeleti eszközök közé tartozik a CiscoView, a HP Openview, a SolarWinds és WhatUp Gold.

Tudásbázis

Mára az egyes gyártók által gondozott tudásbázisok nélkülözhetetlen információforrásokká nőttek ki magukat. Az on-line tudásbázisok internetes keresőkkel történő kombinálása hatalmas mennyiségű tapasztalati alapokon nyugvó ismeret hozzáférését teszi lehetővé.

Protokollelemzők

A protokollelemzők a kereteket képesek hálózati rétegekre tagoltan dekódolni és viszonylag könnyen értelmezhető alakban megjeleníteni, és ezáltal a hálózati forgalmat további elemzés céljából rögzíteni. Az így rögzített kimenet különböző igények és kritériumok szerint szűrhető: megjeleníthető például csak egy adott eszközről indított és annak címzett forgalom. A Wireshark és a hasonló protokollelemző alkalmazások a hálózaton forgalmazott adatokról nyújtanak részletes hibaelhárítási információt. Jó példa a protokollelemzőkkel feltárható információra a két állomás között zajló TCP viszony felépítése és lezárása.



SolarWinds
LANsurveyor
(Automatikus
hálózatfelderítő
eszköz)

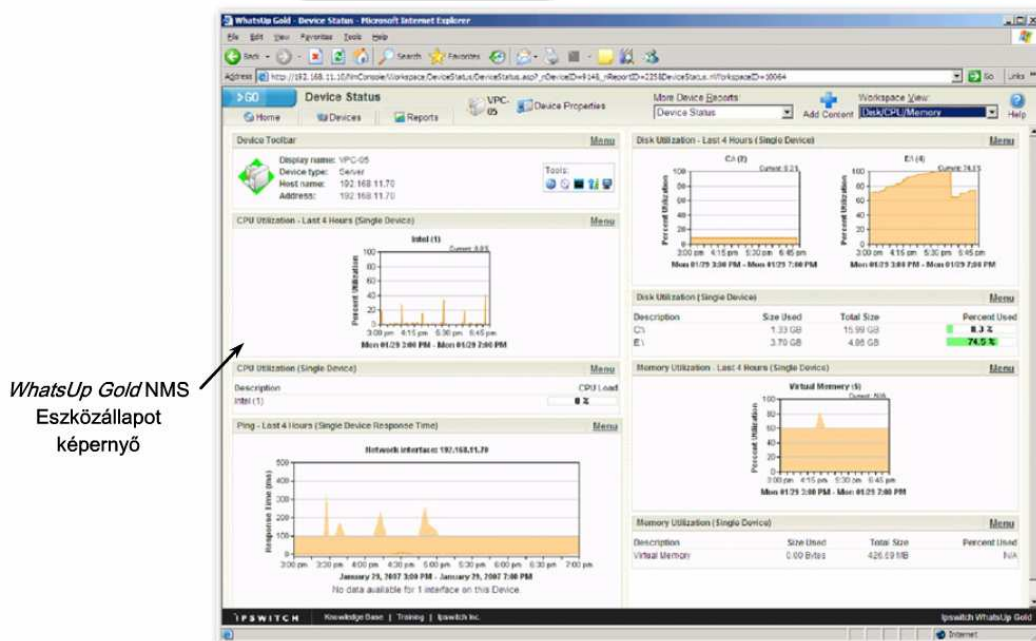
SolarWinds CyberGauge (Sávszélesség
figyelő eszköz)

Alapvető eszközök

Hálózatfelügyeleti
rendszer

Ismeretbázis

Protokollelemző



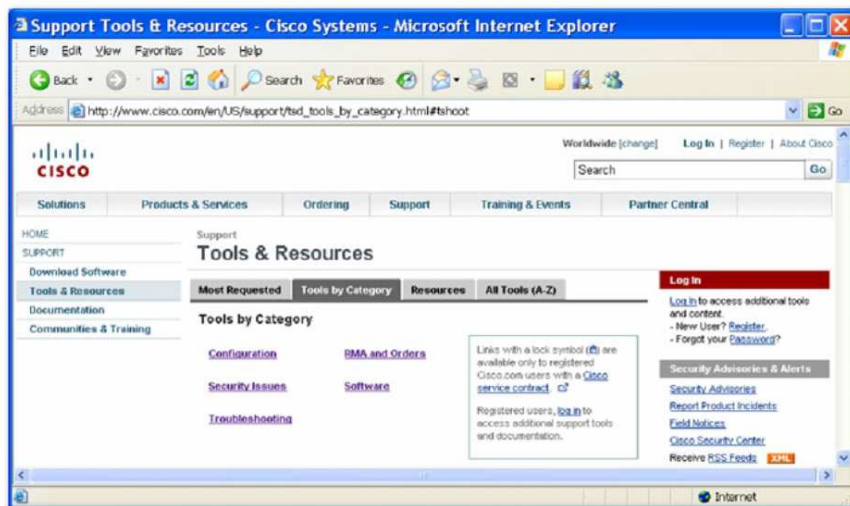
WhatsUp Gold NMS
Eszközállapot
képernyő

Alapvető eszközök

Hálózatfelügyeleti
rendszer

Ismeretbázis

Protokollelemző

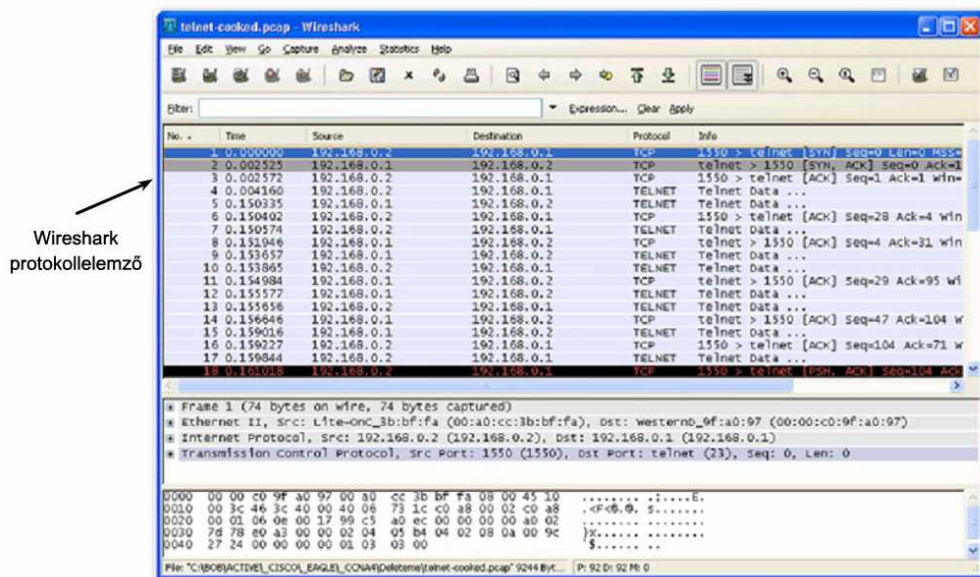


Alapvető eszközök

Hálózati felügyeleti
rendszer

Ismeretbázis

Protokollelemző



Alapvető eszközök

Hálózati felügyeleti
rendszer

Ismeretbázis

Protokollelemző

Szoftveres eszközökkel sokszor nem könnyű az OSI modell alsó rétegeiben jelentkező hibák felismerése. Ezekben az esetekben fontos segítséget nyújthatnak a hardveres hibaelhárító eszközök: a kábelteszter, a multiméter és a hálózatelemző.

Kábeltesztetek

A kábeltesztetek olyan kisméretű célműszerek, melyeket különböző kommunikációs kábelek ellenőrzésére terveztek. Alkalmazásukkal feltárhatók a törött kábelek, a hibás bekötések, a rövidzárlatok és a felcserélt kábelek. A fejlettebb eszközök, mint például a TDR kábelteszter (time-domain reflectometer - időtartományi reflektométer) képesek a kábelben a szakadás helyét is meghatározni. Kábelteszterrel meghatározható a kábel hossza is.

Digitális multiméterek

A digitális multiméterek olyan mérőműszerek, melyekkel közvetlenül mérhetünk bizonyos elektromos jellemzőket: feszültséget, áramerősséget és ellenállást. A hálózati hibaelhárításban a multiméter elsősorban az egyes áramforrások feszültségszintjeinek és az adott hálózati készülékek áramellátásának ellenőrzésekor hasznos.

Hordozható hálózatanalizátorok

A hálózat tetszőleges pontján egy hálózatanalizátor kapcsolóhoz csatlakoztatásával rögtön láthatóvá válik az adott szegmens átlagos és csúcskihasználtsága. Analizátorral az is könnyen kideríthető, hogy melyik eszköz generálja a legnagyobb hálózati forgalmat, de elemezhető vele a forgalom is protokollok szerint, vagy akár részletesen vizsgálhatók az egyes interfészek. A hálózatanalizátorok különösen jól használhatók rosszgindulatú programok, vagy szolgáltatásmegtagadási támadás okozta problémák felderítésekor.



Fluke 179 digitális multiméter



Fluke Networks LinkRunner Pro Tester



Fluke Networks CableIQ Qualification Tester



Fluke Networks OptiView™ Series III Integrated Network Analyzer

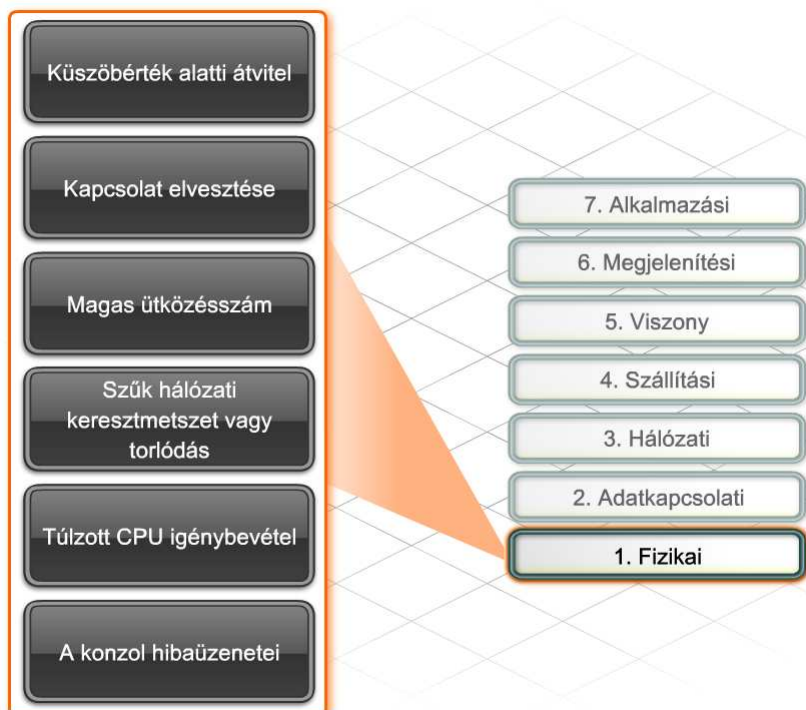
9.2. 1. és 2. rétegbeli problémák hibaelhárítása

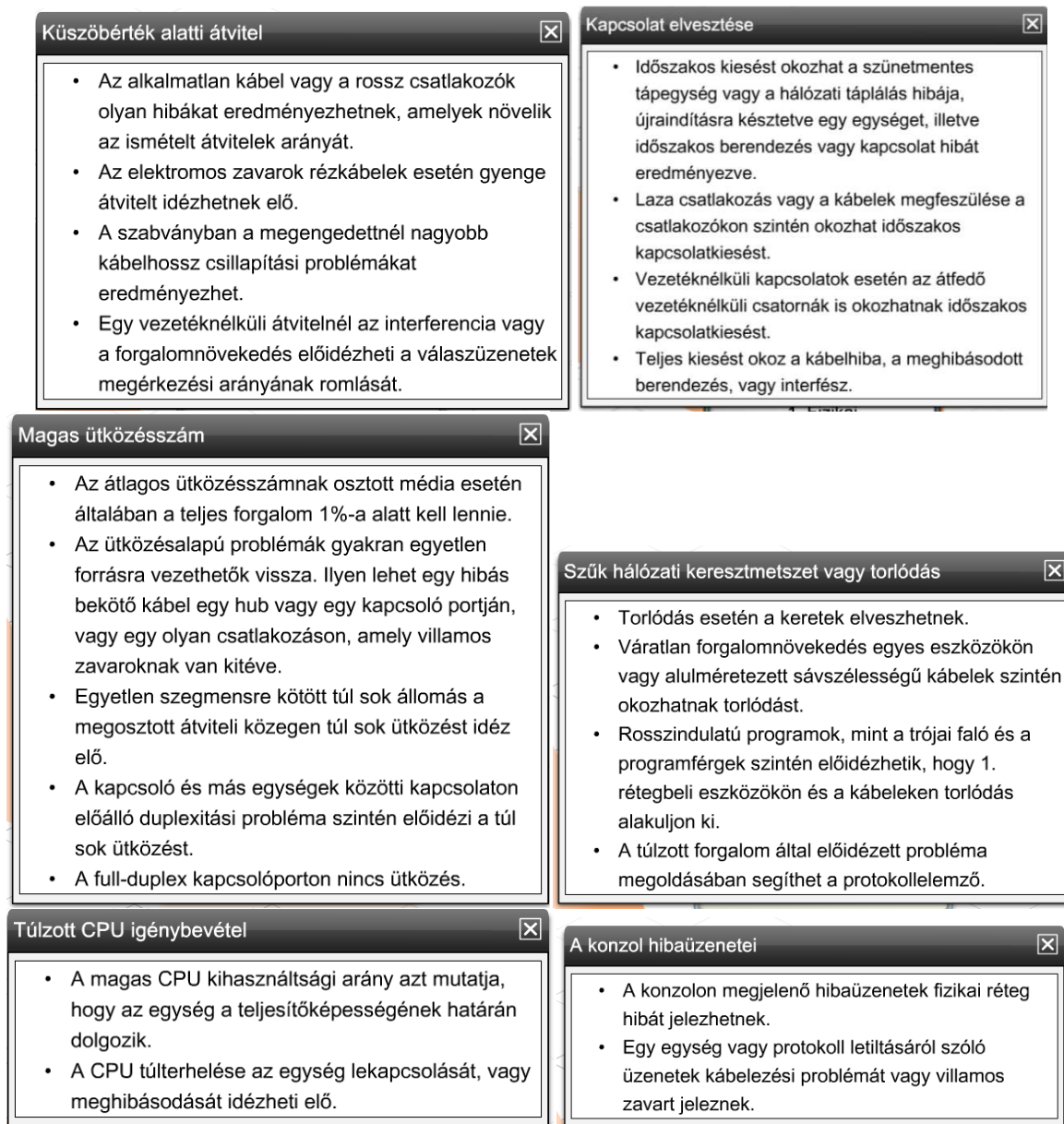
A fizikai és az adatkapcsolati réteg hardveres és szoftveres megvalósításokat is tartalmaz. Minden hálózati kommunikáció ebben a két rétegben alkalmazott technológiákon nyugszik. Éppen ezért roppant fontos, hogy a hálózati szakember gyorsan felismerje és javítani tudja az itt előforduló hibákat.

A fizikai réteg felelős az egyik állomásról a másik állomásra küldött bitek fizikai és elektromos jellemzőinek a definiálásáért függetlenül attól, hogy vezetékes vagy vezeték nélküli átviteli közeget alkalmaznak. Az 1. rétegben előforduló hibák a kapcsolat elvesztésével, vagy - egyszerűbb esetben - teljesítménycsökkenéssel járhatnak.

Az 1. rétegben előforduló hibák szorosan kapcsolódnak az alkalmazott technológiához. Az Ethernet például többszörös hozzáférésű technológia. Az Ethernet protokollban alkalmazott algoritmus alapja, hogy az egyes állomások érzékelik, hogy szabad-e a csatorna mielőtt adni kezdenek. Ennek ellenére előfordul, hogy két állomás ugyanabban az időpillanatban kezd adni, ezzel ütközés keletkezik. Minden ütközésnél az összes érintett eszköz abbahagyja a továbbítást, és véletlen ideig vár az újratekés előtt. Mivel az Ethernet észleli az ütközést és képes reagálni rá, ezért gyakran Vivőjel-figyeléses többszörös hozzáférésű ütközésérzékeléses (CSMA/CD - Carrier Sense Multiple Access with Collision Detection) technológiának nevezik.

Ugyanakkor a túl gyakori ütközések erősen ronthatják a hálózat teljesítményét. Osztott közegen, amilyen a hubokkal kialakított hálózat, az ütközések sokkal komolyabb problémát jelentenek, mint a kapcsolt hálózatokban.





Küszöbérték alatti átvitel

- Az alkalmatlan kábel vagy a rossz csatlakozók olyan hibákat eredményezhetnek, amelyek növelik az ismételt átvitelek arányát.
- Az elektromos zavarok rézkábelek esetén gyenge átvitelt idézhetnek elő.
- A szabványban a megengedettnél nagyobb kábelhossz csillapítási problémákat eredményezhet.
- Egy vezeték nélküli átvitelnél az interferencia vagy a forgalomműködés előidézhetheti a válaszüzenetek megérkezési arányának romlását.

Kapcsolat elvesztése

- Időszakos kiesést okozhat a szünetmentes tápegység vagy a hálózati táplálás hibája, újraindításra készítve egy egységet, illetve időszakos berendezés vagy kapcsolat hibát eredményezve.
- Laza csatlakozás vagy a kábelek megfeszülése a csatlakozókon szintén okozhat időszakos kapcsolatkiesést.
- Vezeték nélküli kapcsolatok esetén az átfedő vezeték nélküli csatornák is okozhatnak időszakos kapcsolatkiesést.
- Teljes kiesést okoz a kábelhiba, a meghibásodott berendezés, vagy interfész.

Magas ütközésszám

- Az átlagos ütközésszámnak osztott média esetén általában a teljes forgalom 1%-a alatt kell lennie.
- Az ütközésalapú problémák gyakran egyetlen forrásra vezethetők vissza. Ilyen lehet egy hibás bekötő kábel egy hub vagy egy kapcsoló portján, vagy egy olyan csatlakozáson, amely villamos zavaroknak van kitéve.
- Egyetlen szegmensre kötött túl sok állomás a megosztott átviteli közegen túl sok ütközést idéz elő.
- A kapcsoló és más egységek közötti kapcsolaton előálló duplexitási probléma szintén előidézi a túl sok ütközést.
- A full-duplex kapcsolóporton nincs ütközés.

Szűk hálózati keresztmetszet vagy torlódás

- Torlódás esetén a keretek elveszhetnek.
- Váratlan forgalomműködés egyes eszközökön vagy alulméretezett sávszélességű kábelek szintén okozhatnak torlódást.
- Rosszindulatú programok, mint a trójai faló és a programférgék szintén előidézhethetik, hogy 1. rétegbeli eszközökön és a kábeleken torlódás alakuljon ki.
- A túlzott forgalom által előidézett probléma megoldásában segíthet a protokollelemző.

Túlzott CPU igénybevétele

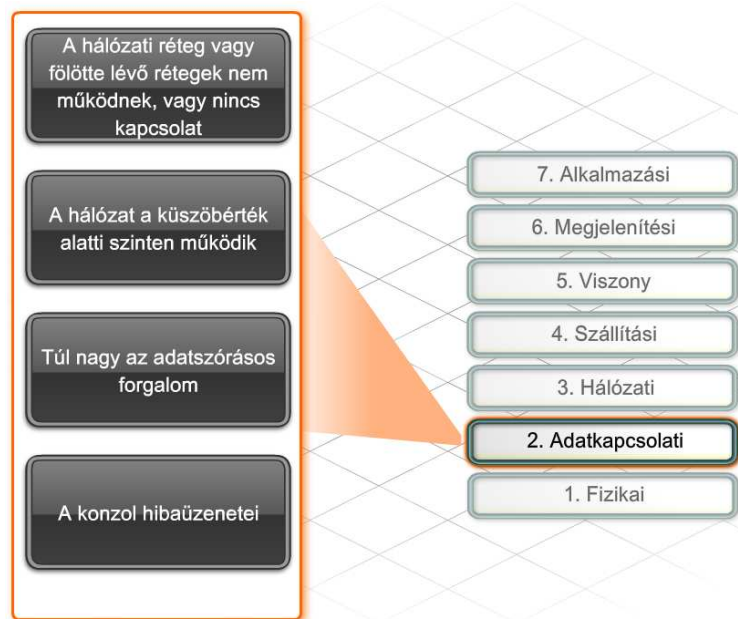
- A magas CPU kihasználtsági arány azt mutatja, hogy az egység a teljesítőképességének határán dolgozik.
- A CPU túlterhelése az egység lekapcsolását, vagy meghibásodását idézheti elő.

A konzol hibaüzenetei

- A konzolon megjelenő hibaüzenetek fizikai réteg hibát jelezhetnek.
- Egy egység vagy protokoll letiltásáról szóló üzenetek kábelezési problémát vagy villamos zavart jeleznek.

Az adatkapcsolati réteg (azaz a 2. réteg) definiálja az adott közegen történő továbbításra előkészített adatok formátumát. Ebben a rétegben kerül szabályozásra a közeghozzáférés is. A 2. réteg teremti meg a kapcsolatot a hálózati réteg szoftveres megvalósítása és az 1. réteg hardveres LAN és WAN technológiái között. Az 1. és 2. rétegben előforduló hibák hatékony kezeléséhez elengedhetetlen a kábelezési szabványok, a beágyazási folyamat és a keretformátumok ismerete.

Az 1. réteg működőképességének ellenőrzése után meg kell állapítani, hogy a hiba a 2. rétegben jelentkezik-e, vagy valamelyik felsőbb rétegben. Például, ha az állomás meg tudja pingelni a visszacsatolási hurok címét (127.0.0.1), de nem éri el a hálózati szolgáltatásokat, akkor a hiba jó eséllyel a 2. rétegbeli keretezésben, vagy a hálózati csatlakozó hibás beállításában keresendő. A hálózati analízátorok és más, hasonló on-line eszközök segítségével behatárolható a 2. rétegbeli hiba helye. Egyes esetekben az eszközök felismerhetik a 2. rétegben jelentkező hibát, melyről akár hibaüzenetet is küldhetnek a konzolra.



A hálózati réteg vagy fölötte lévő rétegek nem működnek, vagy nincs kapcsolat

- Rosszul beállított hálózati kártya vagy meghajtó szoftver le tudja állítani a keretek cseréjét a kapcsolaton keresztül.
- Beágyazási hibák a soros vagy WAN kapcsolatokon előidézhetik a kapcsolat leállítását a működő áramkörök ellenére is.

A hálózat a küszöbérték alatti szinten működik

- Az interfész eldobja a kapacitását meghaladó forgalomban érkező-, a CRC-, vagy keretezési hibával rendelkező kereteket silány hálózati működést eredményezve. Ez a probléma a hibaszámláló statisztika, vagy a kapcsoló és forgalomirányító konzoljának hibaüzenetei segítségével azonosítható.
- A leggyakoribb 1. rétegbeli hibák a hálózati kártyák, interfészek hibái, valamint a villamos zavarok, melyek 2. rétegbeli keretezési hibát idézhetnek elő a hálózaton.

A hálózat a küszöbérték alatti szinten működik

- Az interfész eldobja a kapacitását meghaladó forgalomban érkező-, a CRC-, vagy keretezési hibával rendelkező kereteket silány hálózati működést eredményezve. Ez a probléma a hibaszámláló statisztika, vagy a kapcsoló és forgalomirányító konzoljának hibaüzenetei segítségével azonosítható.
- A leggyakoribb 1. rétegbeli hibák a hálózati kártyák, interfészek hibái, valamint a villamos zavarok, melyek 2. rétegbeli keretezési hibát idézhetnek elő a hálózaton.

A konzol hibaüzenetei

- Konzol üzenet általában akkor keletkezik, amikor az eszköz azt tapasztalja, hogy a bejövő keretek beágyazási vagy keretezési hibával érkeznek.
- Akkor is keletkezik üzenet, amikor ébrenléti jel beérkezését várja de az nem érkezik meg.
- A leggyakoribb 2. rétegbeli hibát jelző üzenet a line protocol down üzenet.

9.2.2 Hardware-s eszközhibák és rendszerindítási problémák hibaelhárítása

A hálózati problémák gyakran egy eszköz újraindítását követően jelentkeznek. A rendszer újraindítása lehet szándékos (például egy eszközfrissítést követően), vagy váratlan (például áramkimaradás után). A hardveres eszközhibák és a rendszerindítási problémák kezelése megköveteli a Cisco IOS rendszerindítási folyamatának ismeretét. A rendszerindítási folyamat három szakaszból áll:

1. Az önellenőrzés (POST) és a rendszerbetöltő program (bootstrap) futtatása.



2. A Cisco IOS megkeresése és betöltése.

3. Az indítási konfigurációkat tartalmazó állomány megkeresése és betöltése, vagy beállítási módba váltás.

Tetszőleges Cisco hálózati eszköz elindításakor hasznos a rendszerindítás során megjelenő konzolüzenetek tanulmányozása. A Cisco IOS betöltődése után néhány paranccsal ellenőrizhető, hogy a hardver- és szoftverösszetevők valóban megfelelően működnek-e.

A *show version* parancs kimenetéből megállapítható a használatban levő operációs rendszer verziószáma, valamint megtudható, hogy a rendszer rendben felismerte-e a hardver interfészeket.

A *show flash* parancs a flash memória tartalmát listázza ki, beleértve az Cisco IOS fájlnevét is. A kimenetéből megállapítható a használatban levő és a szabad flash memória mérete.

A *show ip interfaces brief* parancs kimenetében az egyes fizikai interfészek állapota és a hozzájuk rendelt IP-címek láthatók.

A *show running-configuration* és a *show startup-configuration* parancsok kimenetéből megállapítható, hogy minden utasítást felismert-e a rendszer az indítási folyamat során.

Amikor egy eszköz nem indul el megfelelően, és ezzel hálózatlanállást okoz, az eszközt ki kell cserélni egy ellenőrzött működőképes készülékre a szolgáltatás helyreállítása érdekében. A szolgáltatás helyreállítását követően elegendő időt kell szánni a meghibásodott eszköz diagnosztizálására és javítására.

Ha a forgalomirányító rendben elindult, kigyulladnak a zöld jelzőfények. Ha hibát észlelnek a rendszerindítási folyamat során, a Cisco eszközök alapértelmezett műveletek segítségével (például ROMmon módba lépve) megpróbálnak helyreállni. A következőkben 5 gyakori rendszerindítási hiba hibaelhárítási stratégiáját tárgyaljuk meg.

Az eszköz nem jut át az önellenőrzésen

Ha az önellenőrzés sikertelen, nem jelennek meg üzenetek a konzolképernyőn. Az eszköz típusától függően a rendszer LED vagy villog, vagy más színre vált. A kijelző fények jelentése az eszköz leírásában megtalálható. Ha az önellenőrzés sikertelen, az eszközt ki kell kapcsolni, a hálózati áramforrásból ki kell húzni és el kell távolítani az összes interfészmodult. Ezek után az eszköz újraindítható. Ha az önellenőrzés még mindig sikertelen, az eszköz javításra szorul. Ha az interfészmodulok nélkül sikeres lesz az önellenőrzés, akkor valószínűsíthető, hogy az egyik modul okozta a hibát. Áramtalanítás után egyenként vissza kell szerelni az interfészmodulokat, és újraindítani a rendszert, hogy a hibás modul kiszűrhető legyen. A hibás modult egy ellenőrzött működőképes modulra ki kell cserélni, majd újra kell indítani a készüléket.

Sérült Cisco IOS rendszerkód a flash memóriában

Ha a flash memóriában tárolt rendszerkód megsérült, vagy hiányzik, a rendszerindító program nem talál érvényes, betölthető operációs rendszert. Egyes Cisco eszközökön van egy korlátozott képességű operációs rendszer is, melyet az eszköz betölt, ha nem talál operációs rendszert a flash memóriában vagy más meghatározott helyen. Ezt a limitált rendszerkódot nevezzük

betöltésssegítőnek (Boothelper). A betöltésssegítők sokszor nem rendelkeznek olyan szolgáltatáskészlettel, hogy sikeresen lehessen konfigurációs parancsokat futtatni, és ezáltal helyreállítani az eszköz helyes működését. Betöltésssegítő hiányában az eszköz általában ROMmon módba lép. A ROMmon mód parancsaival TFTP kiszolgálóról betölthető egy működőképes Cisco IOS fájl.

A rendszer nem ismeri fel a memóriát, vagy memóriahibát jelez

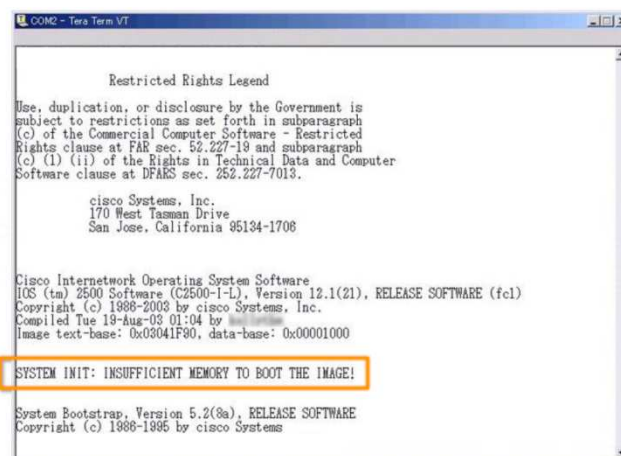
Előfordulhat, hogy nem áll rendelkezésre kellő méretű memória az operációs rendszer kicsomagolásához és betöltéséhez. Ilyenkor hibaüzenetek peregnek a konzolképernyőn, vagy a rendszer folyton újraindul. Lehet, hogy ROMmon módban elindítható ilyenkor is az eszköz. Ehhez a CTRL+Break billentyűkombinációt kell leütni rendszerindítás közben. ROMmon módban, a megfelelő parancs használatával megállapítható a memória állapota. A rendes működés helyreállításához elképzelhető, hogy ki kell cserélni, vagy ki kell bővíteni a memóriát.

A rendszer nem ismeri fel az interfészmodulokat

A hibás vagy helytelenül telepített interfészmodulokat a rendszer nem ismeri fel az önellenőrzés vagy az IOS betöltése során. Ilyenkor a show version parancs kimenetében listázott és használható interfészek nem egyeznek meg a fizikailag telepített interfészekkel. Új interfészmodulokat mindig ellenőrizni kell, hogy a készüléken futó IOS támogatja-e, illetve van-e elég memória a működéséhez. A hardver hiba biztonságos felismeréséhez a készülék áramtalanítása és a tápcsatlakozó kihúzása után az interfészmodult újra be kell szerelni a készülékbe. Ha újratelepítés után sem ismeri fel a rendszer a modult, ki kell cserélni egy ellenőrzöten jól működőre.

Hibás vagy hiányzó konfigurációs állomány

Egyes Cisco készülékek beépített automatikus telepítési segédprogramot futtatnak, ha nem találnak érvényes konfigurációs állományt. Ez a segédprogram szórással TFTP kérést küld ki, hogy konfigurációs állományt szerezzen. Más eszközök azonnal a kezdeti konfigurációs párbeszédbe lépnek, amit beállítási segédprogramnak vagy beállítási módnak is nevezünk. Az automatikus telepítési segédprogramot futtató készülékek is beállítási módba lépnek, ha 5 kérés után egyetlen TFTP kiszolgáló sem válaszol. A konfiguráció betöltése vagy létrehozása érdekében TFTP vagy kézi beállítás is alkalmazható. Az eszközök nem továbbítanak hálózati forgalmat, amíg helyes konfigurációhoz nem jutottak.



9.2.3 Kábelezési és interfészproblémák hibaelhárítása

A forgalomirányító interfész hibák gyakran az első tünetei az 1. és 2. rétegbeli kábelezési és kapcsolati hibáknak. A hibakeresést érdemes az adott interfész *show interfaces* parancs kimenetén található statisztikáinak az áttekintésével, valamint a *show ip interface brief* parancs kimenetén látható állapot információk ellenőrzésével kezdeni!

A *show ip interface brief* parancs kimenete tömör összefoglalást tartalmaz az összes interfészről, beleértve az interfészek állapotát és hozzárendelt IP-címét is.

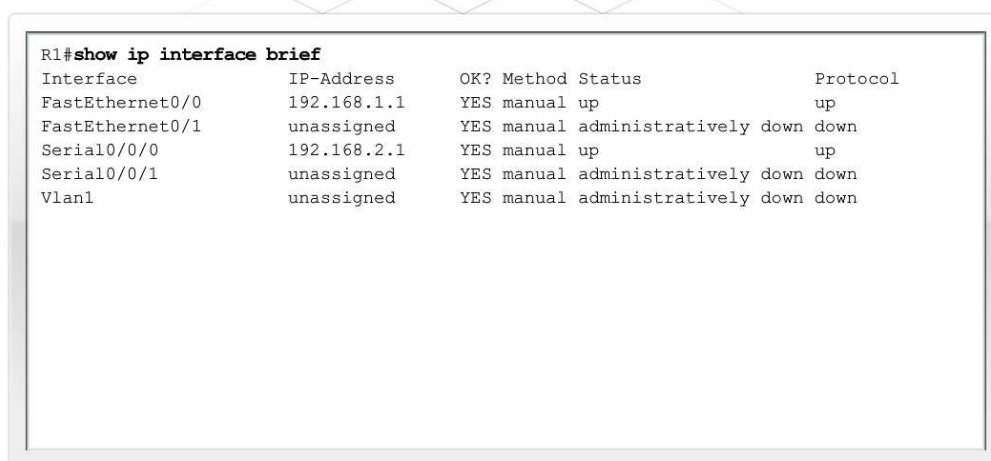
- **up/up állapot** - a normál működést jelzi, mind a közeg, mind a 2. rétegbeli protokoll üzemképes.
- **down/down állapot** - kapcsolati vagy átviteli közeg problémára utal.
- **up/down állapot** - azt jelzi, hogy az átviteli közeg megfelelően csatlakozik, de a 2. rétegbeli protokoll nem működik megfelelően, beállítási hibák lehetnek.

Down/down állapothoz vezető gyakori kábelezési vagy átviteli közeg hibák:

- Meglazult vagy megfeszülő kábel - akár egyetlen érintkező rossz csatlakozása az áramkör megszakadását okozhatja.
- Hibás végződtetés - ellenőrizni kell az érintkezők szabvány szerinti bekötését, és hogy az érintkezők helyesen vannak-e végződtetve a csatlakozóban.
- Sérült soros interfészcsatlakozó - a csatlakozó egyes érintkezői elgörbültek, vagy hiányoznak.
- Szakadás vagy rövidzár a vezetékben - ha hibák lépnek fel az áramkörben, az interfész nem érzékel megfelelő jeleket.

Up/down állapothoz vezető gyakori 2. rétegbeli problémák:

- Helytelen beágyazási beállítások.
- Az adott interfészen nem érkeznek ébrenléti jelek.



```
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	192.168.2.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down

Időnként az átviteli közeg hibái nem vezetnek az áramkör leállításához, hanem a csak hálózati teljesítmény csökkenését okozzák. A *show interfaces* parancs további információkkal szolgál, melyek segítenek az átviteli közeget érintő problémák azonosításában.

A *show interfaces* parancs kimenetében megtalálható:

- **Erős zaj** - Ethernet és soros interfészen érzékelhető sok CRC hiba és kevés ütközés erős zajra utal. A CRC hibák általában az átviteli közeg vagy a kábelezés hibájára utalnak. Jellemző hibák: elektromos interferencia, meglazult vagy sérült kapcsolatok, nem megfelelő kábeltípus alkalmazása.
- **Sok ütközés** - az ütközések a fél-duplex kommunikációra és az osztott közegre jellemzőek. A sérült kábelek az ütközések számának megnövekedéséhez vezethetnek.
- **Sok túl kicsi (runt) keret** - a túl kicsi keretek számának megemelkedését általában egy hibásan működő hálózati kártya okozza, de előidézhetheti a sok ütközéshez vezető állapot is.
- **Késői ütközés** - a helyesen megtervezett és kialakított hálózatokban soha nem fordulhat elő késői ütközés. Leggyakoribb előidézői a túl hosszú kábelek. A téves duplex egyeztetés is okozhat késői ütközést.

Erős zaj	
1. lépés	Az Ethernet interfészek állapotának meghatározására alkalmazza a show interface parancsot! A sok CRC hiba, de kevés ütközés megjelenése erős zajra utal.
2. lépés:	Vizsgálja meg a kábeleket és a zajforrásokat!
3. lépés	Ellenőrizze, hogy a használatban levő kábel és csatlakozó megfelel-e az interfész sebességének!
4. lépés	1000BASE-TX esetén győződjön meg arról, hogy a kábel legalább 5-ös kategóriájú!

Sok ütközés	
1. lépés	Használja a show interface parancsot az ütközések arányának meghatározásához! Az ütközések száma nem haladhatja meg a kimenő csomagok számának 1%-át.
2. lépés:	Használjon időtartománybeli reflexiómérőt (TDR) a hibás kábelek megkeresésére!

Sok túl kicsi (runt) keret	
1. lépés	Egy megosztott Ethernet környezetben majdnem mindig az ütközések idézik elő a túl kicsi keretek megjelenését. Ha nagy az ütközésszám, olvassa el a "Sok ütközés" részt!
2. lépés:	Ha túl kicsi keretek keletkeznek olyankor, amikor nincs számottevő mennyiségű ütközés, akkor az a hálózati kártya szoftverének hibájára utal.
3. lépés	Protokollelemző segítségével határozza meg a túl kicsi keretek forrásának címét!

Késői ütközések	
1. lépés	A késői ütközések felderítésére használjon protokollelemzőt! Egy megfelelően tervezett Ethernet hálózatban soha sem következhet be késői ütközés. Rendszerint akkor fordul elő, ha túl hosszú az Ethernet kábel vagy duplexitási probléma van.
2. lépés:	Ellenőrizze, hogy a hálózat kiterjedése megfelel-e a szabványnak!

9.2.4 LAN kapcsolati hibák elhárítása

A LAN hibaelhárítása szorosan kötődik a kapcsolók világához, mivel a LAN felhasználók többsége egy kapcsolóporton keresztül éri el a hálózatot. A Cisco kapcsolókon a hibaelhárítás során az eddig megismert *show* parancsok többsége használható információgyűjtésre. Ezen kívül minden egyes kapcsolóport saját LED kijelzővel rendelkezik, mely hasznos információt nyújt a hibakereséshez.

A LAN kapcsolati hibák elhárításának első lépése annak ellenőrzése, hogy a felhasználó csatlakozását biztosító kapcsolóport működik-e, és hogy a LED kijelzők világítanak-e. Ha a kapcsoló fizikailag hozzáférhető, akkor a legidőhatékonyabb megoldás rápillantani a LED kijelzőre, amiből kiderül, hogy

van-e kapcsolat (zöld fény), vagy hiba van (vörös vagy narancs fény). Az összeköttetés mindkét végén ellenőrizni kell a kapcsolat meglétét.

Ha a kapcsolatjelző nem világít, meg kell győződni a kábel helyes csatlakozásáról az összeköttetés mindkét végén, és hogy a kábel a megfelelő porthoz csatlakozik-e. Továbbá ellenőrizni kell, hogy mindkét eszköz be van-e kapcsolva, és hogy a rendszerindítási folyamat hiba nélkül befejeződött-e. A lengőkábeleket ki kell cserélni ellenőrzött jó kábelekre, és ellenőrizni kell a csatlakozók bekötését a kívánt kapcsolattípusnak megfelelően. Ha a kapcsolatjelző fény továbbra sem gyullad ki, ellenőrizni kell, hogy a port nincs-e adminisztratív módon kikapcsolva. A portok beállításainak megtekintéséhez a *show running-config interface* parancs használható.

```
Switch# sh run interface fastEthernet 4/2
```

```
!
```

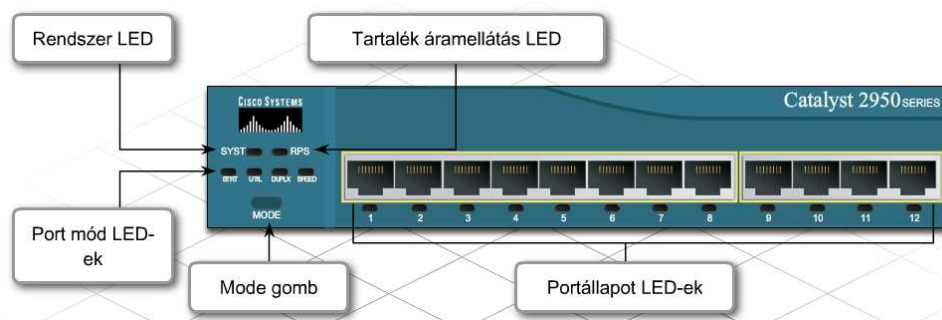
```
interface fastEthernet 4/2
```

```
shutdown
```

```
duplex full
```

```
speed 100
```

```
end
```



A világító kapcsolatjelző nem feltétlenül jelenti a kábel tökéletes működését. A kábel lehet sérült, ami időszakos teljesítményproblémákat okozhat. Az ilyen esetek általában feltárhatók a Cisco IOS *show* parancsaival: a kimenetekben nagy számú csomaghibát, és folyamatosan le-, illetve felkapcsolódó interfészeket érdemes keresni.

A kapcsolón kiadott *show version* és *show interfaces* parancsok kimenete hasonló információt szolgáltat a forgalomirányítón kiadott parancsokéhoz. A *show interface portazonosító counter errors* paranccsal egy adott interfész hibastatisztikái gyorsan megjeleníthetők.

A hibás duplexbeállítás sokkal jellemzőbb a kapcsolókra, mint a forgalomirányítókra. Sok eszköz automatikusan egyezteteti a sebesség- és duplexbeállításokat. Könnyen ellentmondó beállításhoz, és így csomagvesztéshez és ütközéshez vezethet, ha a kapcsolat egyik végén automatikus egyeztetést, míg a másik végén kézi beállítást alkalmaznak.

A *show interface portazonosító status* parancs segítségével megjeleníthető, hogy milyen duplex- és sebességbeállítások (kézi, vagy automatikus, illetve milyen konkrét érték) vannak érvényben egy adott porton.

Ha az egyeztetési hiba olyan Cisco eszközökön jelentkezik, melyeken a Cisco Discovery Protocol (CDP) engedélyezve van, mindkét eszköz konzolképernyőjén vagy a naplófájlokban hibaüzenetek jelennek meg. A CDP hasznos segítség a szomszédos Cisco eszközök hibáinak, port- és rendszerstatisztikáinak ellenőrzéséhez.

A duplex egyeztetési hibák kijavításának legegyszerűbb módja, mindkét eszköz automatikus egyeztetésre állítása. Ha az automatikus beállítás nem hozná meg a várt eredményt, akkor kézzel kell beállítani az egyező sebesség és duplex értékeket.

```
Jun  2 11:16:45 %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet6/2 (not half duplex), with TBA04251336 3/2 (half duplex).
```

Duplexitási problémára utaló hibaüzenet.

```
Switch# sh interfaces fas 6/1 status
Port Name      Status      Vlan    Duplex  Speed  Type
Fa6/1          notconnect  1       auto    auto   10/100BaseTX
```

Show parancs kimenete, amely azt mutatja, hogy a duplexitás és a sebesség beállítása automatikus egyeztetéssel történik.

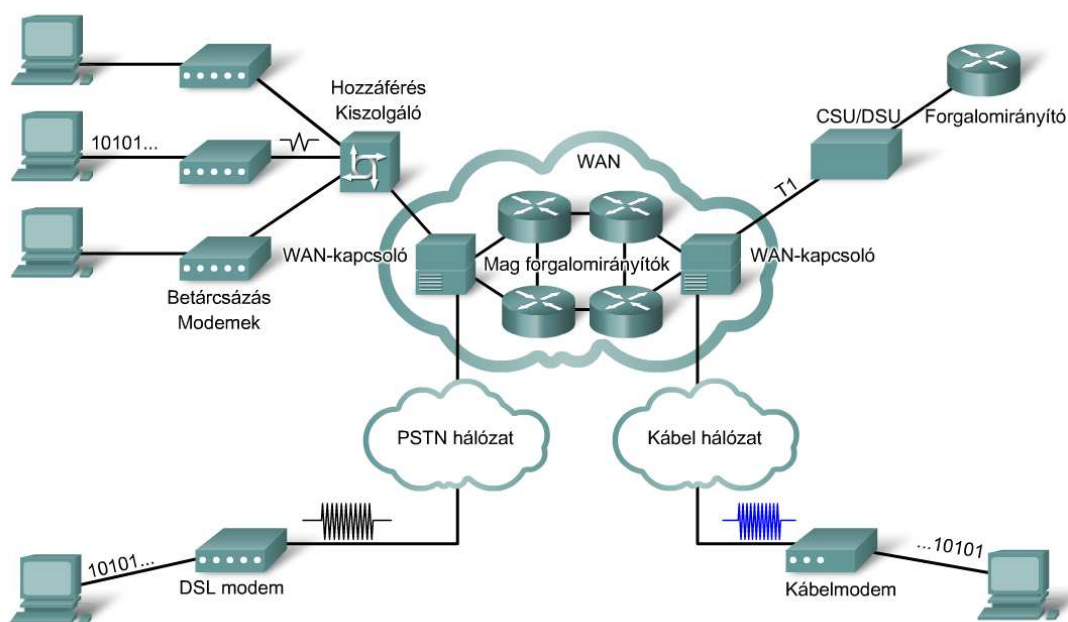
9.2.5 WAN kapcsolati hibák elhárítása

A soros WAN kapcsolatok hibaelhárítása eltér az Ethernet LAN kapcsolatokétól. A WAN kapcsolat jellemzően távközlési szolgáltató (TSP - telecommunications service provider) birtokában levő készülékek és az átviteli közeg működésétől függ. Ezért lényeges, hogy a technikus jártas legyen a felhasználói végberendezések hibaelhárításában, és az eredményeket érthetően tudja kommunikálni a szolgáltató felé.

A soros interfészek és vonali problémák többségének felismeréséhez és megoldásához elegendő a *show interfaces serial* parancs kimenetéből nyerhető információ. A soros összeköttetésekre általában csomaghibák, beállítási hibák, beágyazási eltérések vagy rossz időzítések jellemzők. Mivel a soros WAN összeköttetések az időzítési információt rendszerint CSU/DSU készülékektől vagy modemektől kapják, a soros vonalak hibaelhárításakor ezeket az eszközöket is érdemes számításba venni. Prototípus hálózatokban a forgalomirányítón beállítható a DCE órajel-szolgáltatás, ekkor nincs szükség CSU vagy modem használatára.

A hatékony WAN kapcsolati hibaelhárításhoz ismerni kell az alkalmazott CSU/DSU eszköz vagy modem típusát, és a visszahurkolási mód beállításának módját a teszteléshez.

WAN-készülékek



A *show interfaces serial* parancs kimenetén a soros vonal állapotát jelző sor hat különböző állapotot mutathat:

Serial x is down, line protocol is down (DTE mode) - amikor a forgalomirányító soros interfésze nem érzékel semmiféle jelet a vonalon, akkor mind a vonalat, mind a 2. rétegbeli protokollt leálltnak tekinti.

Lehetséges probléma:	A hiba megkeresése:
<ul style="list-style-type: none"> Azt mutatja, hogy a forgalomirányító nem érzékeli a hívőjelet. Telefonszolgáltatói probléma - A vonal nem csatlakozik a CSU/DSU-hoz. Helytelen vagy hibás kábelezés. Helytelen vagy hibás kábelezés. 	<ol style="list-style-type: none"> 1. lépés: Ellenőrizze, hogy a LED-ek a CSU/DSU-n aktívak-e! 2. lépés: Ellenőrizze, hogy a megfelelő kábelt és a megfelelő interfészt használja-e! 3. lépés: Vegye fel a kapcsolatot a bérelt vonali - vagy egyéb szolgáltatóval, és érdeklődjön, tudnak-e a hibáról! 4. lépés: Cserélje ki az interfész modult egy ellenőrzöten hibátlan példányra! 5. lépés: Helyettesítse a CSU/DSU-t egy ellenőrzöten hibátlan eszközzel.

Serial x is up, line protocol is down (DTE mode) - amennyiben a soros interfészre nem érkeznek ébrenléti jelek, vagy beágyazási hiba van, akkor a 2. rétegbeli protokollt tekinti leálltnak.

Lehetséges probléma:	A hiba megkeresése:
<ul style="list-style-type: none"> A helyi vagy a távoli forgalomirányító hibásan van beállítva. A távoli forgalomirányító nem küld ébrenléti üzeneteket. Hibás a távoli CSU vagy DSU. Hibás a helyi CSU vagy DSU. 	<ol style="list-style-type: none"> 1. lépés: Állítsa helyi loopback üzemmódba a modemet, a CSU vagy a DSU egységet, majd a <code>show interfaces serial</code> paranccsal ellenőrizze, hogy a vonali protokoll működni kezd-e! Ha a vonali protokoll működni kezd, akkor vagy a telefon vonal vagy a távoli forgalomirányító okozhatja a problémát. 2. lépés: Ha azt tapasztalja, hogy a hiba a kapcsolat túlsó végén jelentkezik, akkor az első lépést a távoli modemmel, CSU vagy DSU egységgel is ismételje meg! 3. lépés: Ellenőrizze a kábeleket! Ellenőrizze, hogy a kábel a megfelelő interfészhez, a megfelelő CSU/DSU egységhez és a megfelelő WAN-szolgáltató hálózati végpontjához csatlakozik-e! 4. lépés: Ellenőrizze a beágyazás helyességét mindkét végpontnál! 5. lépés: Ha a vonali protokoll nem működik helyi loopback üzemmódban és nincs beágyazási probléma, akkor cserélje ki a hibás hardvert!

Serial x is up, line protocol is down (DCE mode) - az olyan esetekben, amikor a forgalomirányító szolgáltatná az órajelet, és az interfészhez DCE kábel csatlakozik, de nincs beállítva órajel, akkor a 2. rétegbeli protokollt leálltnak tekinti.

Lehetséges probléma:	A hiba megkeresése:
<ul style="list-style-type: none"> Hiányzik a <code>clockrate</code> interfész konfigurációs parancs. Hibás a helyi CSU vagy DSU. Hibás vagy helytelen kábel. Forgalomirányító hardver hiba. 	<ol style="list-style-type: none"> 1. lépés: Adja ki a soros interfészen a <code>clockrate</code> interfész konfigurációs parancsot! 2. lépés: Ellenőrizze, hogy megfelelő kábelt használ-e! 3. lépés: Ha a vonali protokoll továbbra sem kezd el működni, valószínűleg hardver, vagy kábel hiba lépett fel. 4. lépés: A hibás darabokat cserélje ki hibátlanokra!

Serial x is up, line protocol is up (looped) - bevett gyakorlat, hogy a kapcsolat teszteléséhez visszacsatolási állapotba helyezik az áramkört. Amikor a soros interfész saját jelét kapja vissza az áramkörben, akkor hurkoltnak jelzi a vonalat.

Lehetséges probléma:	A hiba megkeresése:
Az áramkörben hurok keletkezett. A hurok első jele az, hogy az ébrenléti üzenetben lévő sorszám véletlenszerű értékre változik. Ha az összeköttetésen keresztül ugyanaz a véletlenszerű érték jön vissza, akkor hurok van a hálózatban.	<ol style="list-style-type: none"> 1. lépés: Adja ki a show running-config parancsot privilegizált EXEC üzemmódban! Ez megmutatja az összes loopback interfész konfigurációs bejegyzést. 2. lépés: Ha talál loopback interfész konfigurációs bejegyzést, akkor távolítsa el a hurkot a no loopback interfész konfigurációs paranccsal! 3. lépés: Ha nem talál loopback interfész konfigurációs bejegyzést, akkor vizsgálja meg nincs-e a CSU/DSU manuális loopback módra állítva! Ha igen, állítsa le a manuális loopback-et? 4. lépés: Hozza alapállapotba a CSU/DSU egységet, majd ellenőrizze a vonal állapotát! Ha a vonali protokoll működni kezd, akkor további beavatkozásra nincs szükség. 5. lépés: Ha a CSU/DSU nincs manuális loopback üzemmódba állítva, akkor vegye fel a kapcsolatot a szolgáltatóval, és kérjen segítséget a hiba elhárításához!

Serial x is up, line protocol is down (disabled) - a magas hibaarány arra készíti a forgalomirányítót, hogy az adott vonalat "protokoll üzenen kívül" állapotba helyezze. Az ilyen hiba általában hardveres hibára vezethető vissza.

Lehetséges probléma:	A hiba megkeresése:
<ul style="list-style-type: none"> • Távközlési szolgáltatói probléma okozta magas hibaarányt. • CSU/DSU hardver probléma. • Rossz a forgalomirányító hardver. 	<ol style="list-style-type: none"> 1. lépés: Lépjen kapcsolatba a távközlési szolgáltatóval! 2. lépés: Kösse hurok módba a CSU/DSU egységet (DTE hurok)! Ha a probléma továbbra is fennáll, valószínűleg hardver hibával állunk szemben. Ha a probléma nem áll fenn, valószínűleg a távközlési szolgáltató hibájával állunk szemben. 3. lépés: Szükség szerint cserélje ki a hibás hardvereszközöket (CSU, DSU, kapcsoló, helyi vagy távoli forgalomirányító)!

Serial x is administratively down, line protocol is down - egy interfész akkor van adminisztratív lezárt állapotban, ha a konfigurációjában szerepel a *shutdown* utasítás. A hiba kijavításához rendszerint csak az szükséges, hogy interfészkonfigurációs módban kiadjuk a *no shutdown* parancsot. Ha az interfész nem kapcsol fel a *no shutdown* parancs hatására, ellenőrizzük a konzolon, hogy nem jelent-e meg duplikált IP-címre utaló hibaüzenet. Duplikált IP-cím esetén ki kell javítani a hibát, majd újra ki kell adni a *no shutdown* parancsot.

Lehetséges probléma:	A hiba megkeresése:
<ul style="list-style-type: none"> A forgalomirányító beállítása a shutdown interfész konfigurációs parancsot is tartalmazza. Többszörös IP-cím. 	<ol style="list-style-type: none"> 1. lépés: Ellenőrizze, hogy a forgalomirányító beállításában nem szerepel-e a shutdown parancs! 2. lépés: Ha szerepel, akkor a no shutdown interfész konfigurációs paranccsal távolítsa el a shutdown utasítást! 3. lépés: Ellenőrizze, hogy nincs-e két azonos IP-cím a hálózaton a privilegizált EXEC módbeli show running-config, vagy az EXEC módbeli show interfaces paranccsal! 4. lépés: Ha talál két azonos IP-címet, akkor szüntesse meg az ütközést a két cím egyikének megváltoztatásával!

Serial x is up, line protocol is up - az interfész az elvárásoknak megfelelően működik.

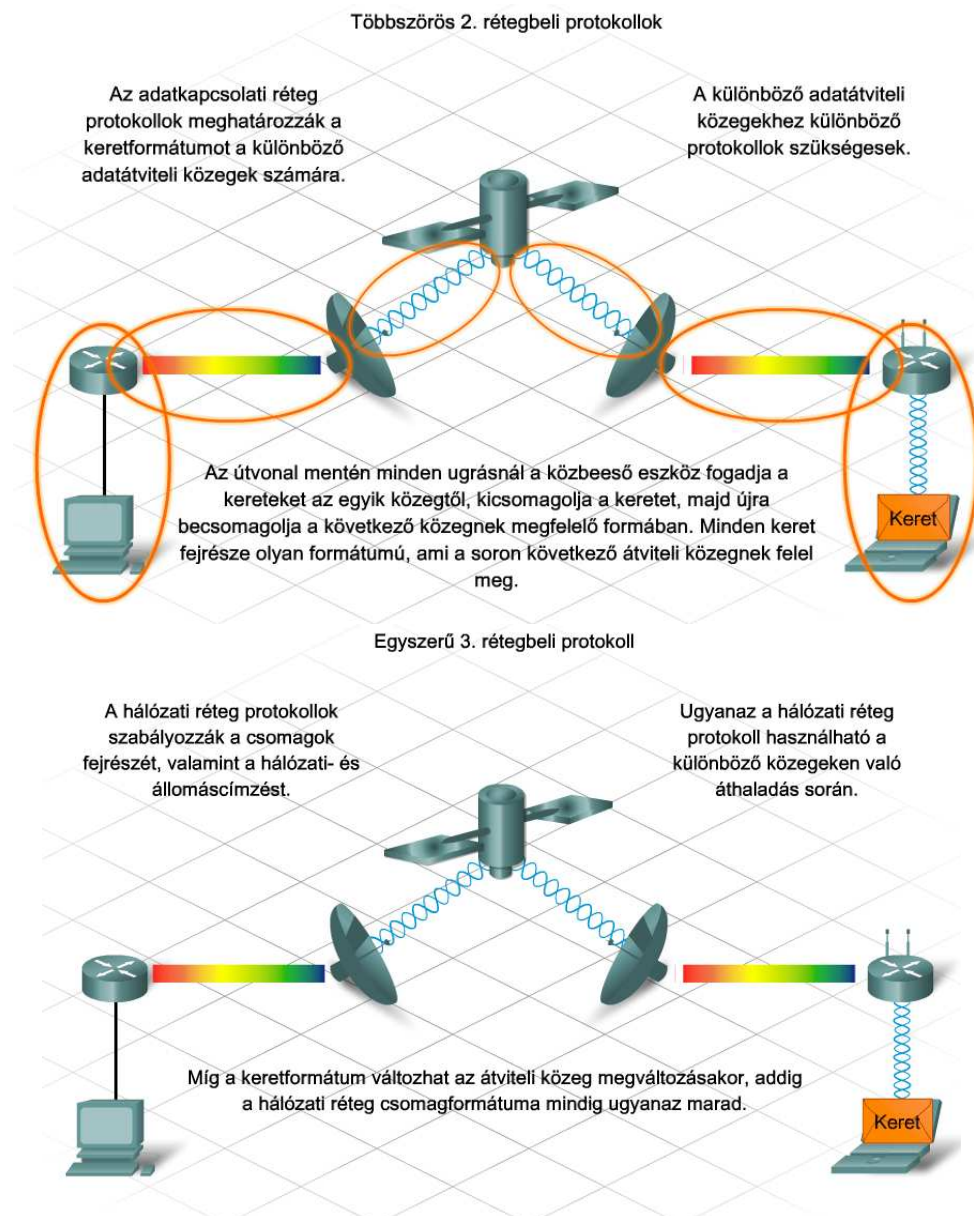
9.3 3. rétegbeli működés és IP-címzés - ismétlés

1. rétegbeli hálózat akkor jön létre, ha hálózati eszközöket pusztán fizikai átviteli közeggel kapcsolnak össze. A 2. rétegbeli protokollok hardverfüggőek. Az Ethernet nem képes soros vonalon üzemelni, ahogy soros kommunikáció sem létesíthető Ethernet hálózati kártyával.

A 3. rétegben (azaz a hálózati rétegben) működő protokollok nem kötődnek egy adott átviteli közeghez, sem a 2. rétegbeli keretformátumokhoz. Ugyanaz a 3. rétegbeli protokoll működhet Ethernet, vezeték nélküli, soros vagy bármi más 2. rétegbeli megvalósítás fölött is. Egyazon 3. rétegbeli hálózat állomásait többféle 1. és 2. rétegbeli technológia is összekötheti. Az OSI modell 3. rétegének elsődleges feladata a hálózati címzés és a forgalomirányítás megvalósítása. A 3. rétegbeli hálózatokat logikai hálózatoknak nevezzük, mivel megvalósításuk tisztán szoftver segítségével történik.

A mai hálózatok többsége a TCP/IP protokollkészlet megvalósításával oldja meg az állomások közti információcserét. Éppen ezért a 3. réteg hibaelhárítása főleg az IP-címzési problémákra és az irányítóprotokollokra koncentrál.

A 3. rétegbeli hibaelhárításhoz nélkülözhetetlen az IP-címzés és a hálózatok határainak alapos megértése. A hálózati teljesítményproblémák zöme rosszul megtervezett és kialakított IP-címzési sémákra vezethető vissza.



A 3. rétegben minden csomagnak hordoznia kell a forrás- és a célrendszer címét. Az IPv4 rendszer 3. rétegbeli fejrésze tartalmazza a forrás és a cél 32-bites címét.

Az IP-cím az egyedi állomásazonosítás mellett az állomás 3. rétegű hálózatát is azonosítja, amelyen kommunikálhat. Egy egyszerű IP-hálózat kialakításához elegendő, ha közvetlenül összekapcsolunk két állomást, melyekhez ugyanabból az alhálózatból rendelünk IP-címet, és azonos alhálózati maszkot adunk.

Az állomások csak akkor képesek egymással TCP/IP alapon üzeneteket váltani, ha rendelkeznek IP-címmel. A különálló 3. rétegbeli IP-hálózatok lényegében IP-címtartományokat jelentenek. A hálózatok határait a cím hálózati előtagját alkotó bitek száma határozza meg. Az ökölszabály egyszerű: minél hosszabb a hálózati előtag a címben, annál kevesebb egyedi címet lehet állomásoknak kiosztani az adott IP-hálózatban.

A 3. rétegbeli problémák megoldásához elengedhetetlen, hogy a rendszergazda meg tudja határozni azt az állomás címtartományt, amely egy adott IP-hálózathoz tartozik. A címtartomány az

állomáscímet alkotó bitek számától és pozíciójától függ. Tegyük fel például, hogy a 192.168.1.0/24 hálózatban 3 bitet kölcsönveszünk alhálózatok kialakítására. Így 5 bit marad az állomáscímezésre. 8 alhálózatot kapunk ($2^3=8$), mindegyikben 30 állomással ($2^5 - 2 = 30$).

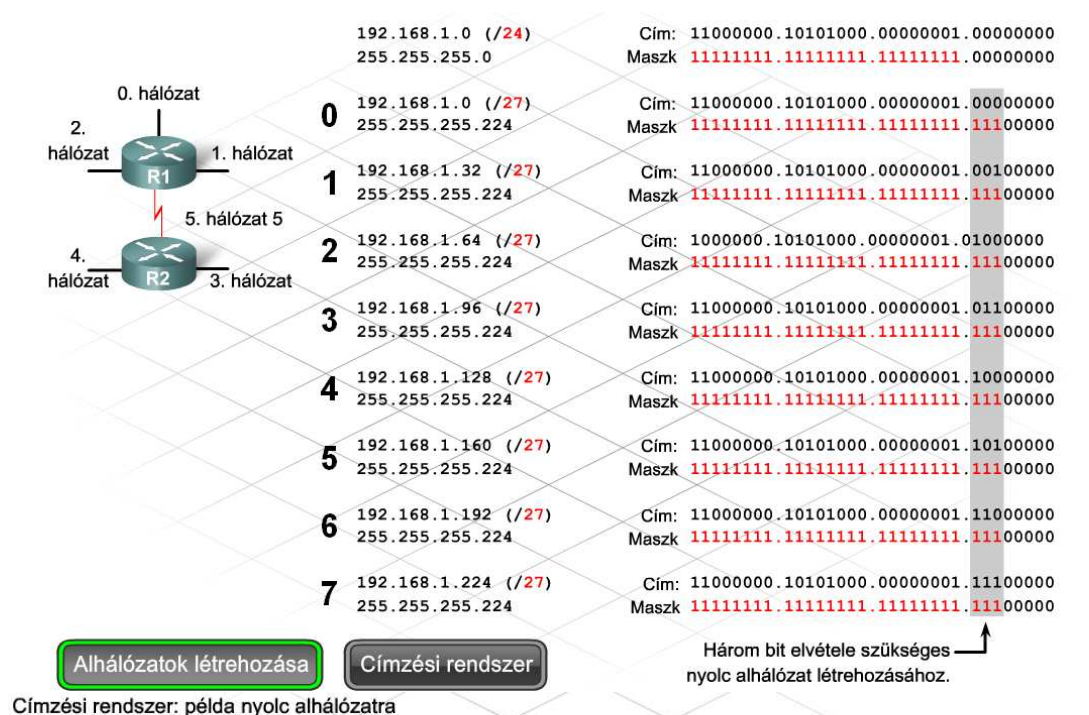
Tekintsük a 192.168.1.96/27 hálózatot, melyben az első kiosztható állomáscím a 192.168.1.97 lesz, míg az utolsó a 192.168.1.126. Az alhálózat szórási címe a 192.168.1.127. Mindez leolvasható az utolsó oktett bináris alakjából:

(011 az alhálózat) 96 + (00001 az első állomáscím) 1 = (01100001), ami decimálisan 97

(011 az alhálózat) 96 + (11110 az utolsó állomáscím) 30 = (01111110), ami decimálisan 126

(011 az alhálózat) 96 + (11111 szórás) 31 = (01111111), ami decimálisan 127

Ez egy C osztályú címet használó példa. Ugyanez a technika alkalmazható az A és a B osztályú címek esetében is. Nem szabad elfelejteni, hogy az állomásazonosító bitek átnyúlhatnak az oktetthatáron.

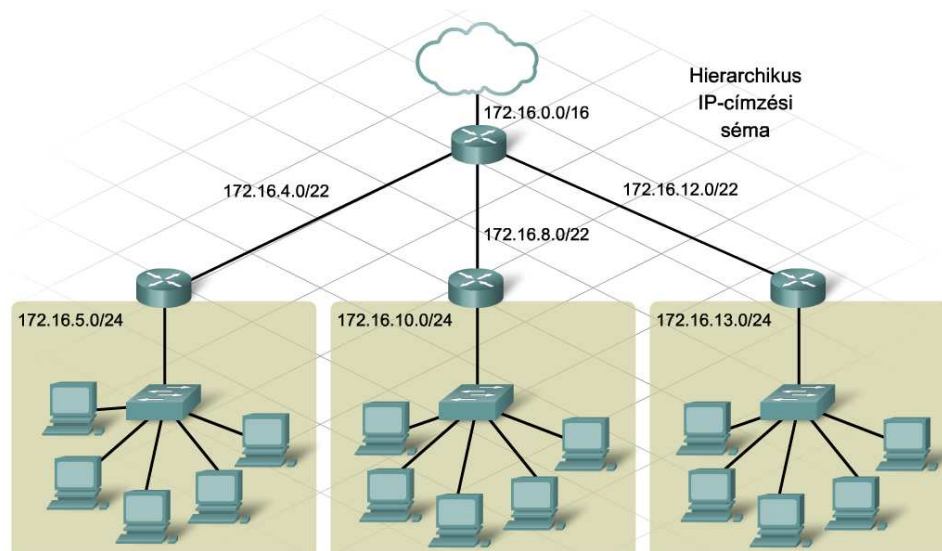


9.3.2 IP-címtér megtervezésének és beállításának kérdései

Az IP-címtér meggondolatlan kiosztása azt eredményezheti, hogy nehézkessé válik a forrás- és a célállomás helyének meghatározása. Manapság a legtöbb hálózat hierarchikus IP-cím kiosztást alkalmaz. A hierarchikus IP-címzési séma számos előnyt hordoz, beleértve a kisebb irányítótáblákat és az ezzel járó kisebb számításigényt is. A hierarchikus IP-címzés egyúttal jobban strukturált környezetet teremt, amelyben a dokumentálás, a hibaelhárítás és a bővítés is könnyebben elvégezhető.

Ugyanakkor a hanyagul megtervezett hierarchikus hálózat, vagy egy rosszul dokumentált terv olyan veszélyeket rejt magában, mint az átfedő alhálózatok kialakulása, vagy a helytelenül beállított alhálózati maszkok az eszközökben. Ebből a két típushibából számos IP-címzéssel és irányítással kapcsolatos probléma származhat.

Akkor beszélünk átlapolódó alhálózatokról, ha egyes IP-címek vagy szórási címek két különálló alhálózatnak is a tagjai. Az átlapolódás oka általában a rossz tervezés, vagy a véletlenül hibásan megadott alhálózati maszk, illetve hálózati előtag. Az átlapolódó címzés nem minden esetben vezet hálózatlanálláshoz. A hibásan beállított alhálózati maszk helyétől függően többnyire csak néhány állomást érint a probléma.



A Cisco IOS megengedi, hogy átlapolódó alhálózatokból rendeljünk IP-címeket a forgalomirányító két különböző interfészéhez, ilyenkor azonban nem aktiválja a második interfészt.

Például rendeljünk IP-címet és alhálózati maszkot az R1 nevű forgalomirányító FastEthernet 0/0 interfészéhez a 192.168.1.0/24 hálózathoz! Ezek után, ha a FastEthernet 0/1 interfészhez a 192.168.1.0/30 hálózathoz próbálunk meg IP-címet rendelni, hibaüzenet fog tájékoztatni az átlapolódó beállításokról. Ha megpróbáljuk felkapcsolni az interfészt a *no shutdown* paranccsal, újabb hibaüzenetet kapunk. Ezen az interfészen a forgalomirányító nem továbbít csomagokat. A *show ip interface brief* parancs kimenetéből is látható, hogy a másodikként a 192.168.1.0/24 hálózathoz konfigurált FastEthernet 0/1 interfész leállított állapotban van.

Mindig fontos az interfészek állapotának ellenőrzése a beállításaik megváltoztatása után. Ha egy interfész adminisztratív lezárt állapotban marad a *no shutdown* parancs kiadása után, az többnyire IP-címzési problémára utal.

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.1.2 255.255.255.252
192.168.1.0 overlaps with FastEthernet0/0

R1(config-if)#no shutdown
192.168.1.0 overlaps with FastEthernet0/0
FastEthernet0/1: incorrect IP address assignment
```

Konfigurációs hibaüzenetek

Show parancs kimenet

```
R1#show ip interface brief

<output omitted>

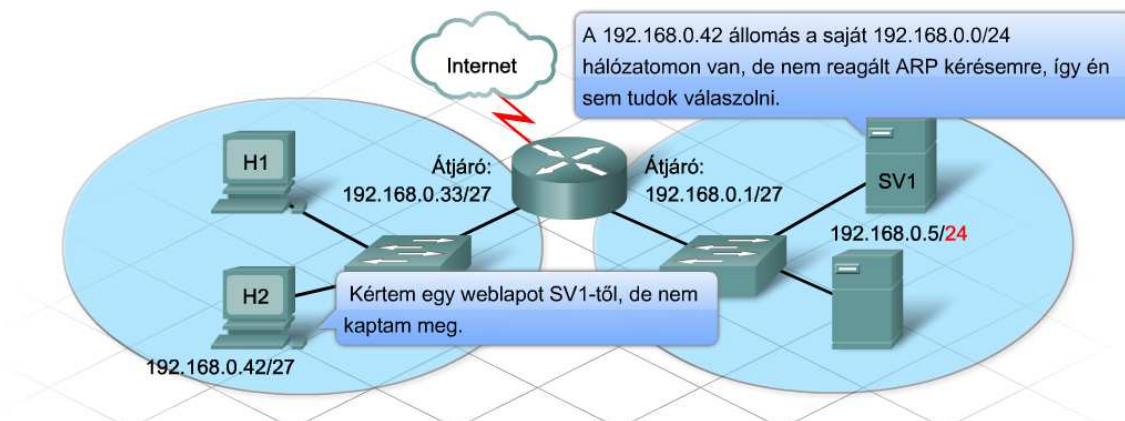
FastEthernet0/1 192.168.1.2 YES manual administratively down down
```

Konfigurációs hibaüzenetek

Show parancs kimenet

Ugyan a Cisco IOS szoftver rendelkezik beépített védelemmel az egy azon készülék különböző interfészein beállított átlapolódó IP-címek kivédésére, nem tudja megakadályozni a különböző készülékeken, illetve az állomásokon beállított átlapolódásokat.

Egyetlen rosszul beállított alhálózati maszk is okozhat néhány állomáson hálózatelérési nehézségeket. A rosszul beállított alhálózati maszkok különféle tüneteket mutathatnak, amelyek olykor nehezen azonosíthatók.



A kiszolgálót csak a vele azonos alhálózatban levő állomások érik el.

A kiszolgálót az alhálózatok egyikében kézzel állították be, az alapértelmezett /24-es hálózati előtaggal a /27-es előtag helyett. Ez a helytelen beállítás okozza, hogy a kiszolgáló az összes különböző alhálózaton lévő állomást a kiszolgálóval azonos alhálózaton lásson. A kiszolgáló nem küld forgalmat az alapértelmezett átjáróhoz egyetlen állomás számára sem /27-es alhálózatokon. Ilyen esetekben ellenőrizze a kiszolgáló beállításait!

1. Kérdéskör

2. Kérdéskör

3. Kérdéskör

4. Kérdéskör



Az állomások válaszokat kapnak az internet kiszolgálóktól, de más alhálózaton levő kiszolgálóktól nem.

Egy állomáson vagy az állomások egy csoportján /24-es alhálózati maszkot állítottak be, ami a kiszolgáló hálózatának alhálózati címeivel átfedésben van. Minden állomás helyesen állapítja meg, hogy az internetcímek nincsenek a saját 3. rétegbeli hálózatán, és a forgalmat az alapértelmezett átjáróhoz továbbítja. Az állomások helytelenül azt állapítják meg, hogy a belső kiszolgáló címek a helyi hálózatokon vannak, és az ARP segítségével keresik a kiszolgáló MAC-címét. Ilyen esetekben ellenőrizze a kiszolgáló és az állomások beállításait! Az ARP keretek megtekintéséhez hálózati sniffer használható.

1. Kérdéskör

2. Kérdéskör

3. Kérdéskör

4. Kérdéskör



Az állomások nem kapnak választ az internet és más alhálózatokon levő kiszolgálóktól, amikor az állomásneveket használják.

Egy állomáson vagy az állomások egy csoportján /24-es alhálózati maszkot állítottak be, ami a kiszolgáló hálózatának alhálózati címével átfedésben van. Az állomások alhálózati maszk hibái általában nem befolyásolják az internet kapcsolatát; eltekintve attól, amikor az alhálózati maszk átfedi a DNS kiszolgáló alhálózatát. Ilyenkor az állomás nem tud kapcsolatba lépni a DNS-kiszolgálóval.

DNS nélkül nincs IP címfeloldás, és egyetlen olyan szolgáltatás sem érhető el, amihez DNS-re van szükség.

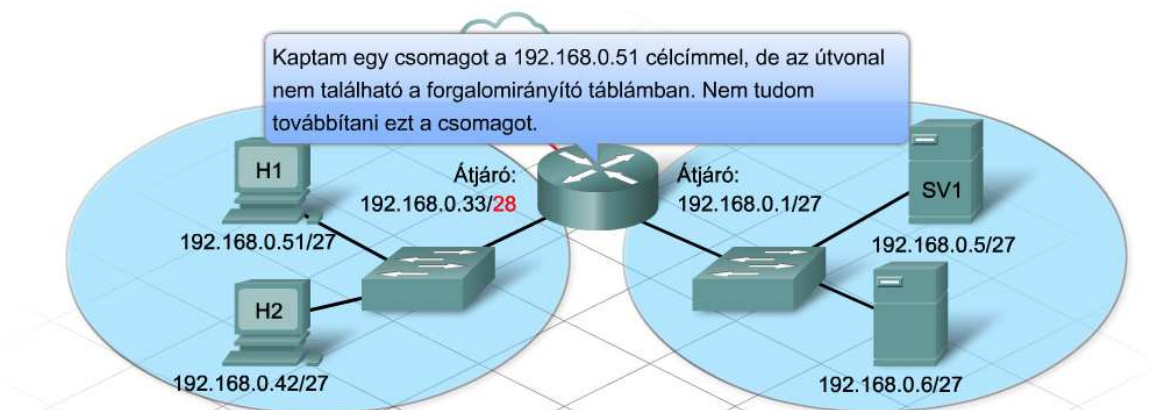
Ellenőrizze az állomás és a DNS beállításokat, ha az internet nem érhető el!

1. Kérdéskör

2. Kérdéskör

3. Kérdéskör

4. Kérdéskör



Egyes állomások el tudják érni az internet és más alhálózatok kiszolgálóit is, más állomások azonban nem.

A forgalomirányító interfész beállításában az alhálózati maszk helytelen konfigurációja okozza, hogy az alapértelmezett átjáró a /27-es alhálózatok egyikén van. Ha a forgalomirányító interfészén helytelenül beállított /28-as alhálózati maszk van, a forgalomirányító táblájában nem szerepel a /27-es alhálózat minden állomása. Az állomások kisebb része, amelyek a /28-as alhálózat tartományába esnek képesek lesznek az információ küldésére és fogadására. A címtartomány felső felébe eső IP-című állomások el tudják küldeni az üzeneteiket a távoli állomásoknak, de mikor a válaszüzenet megérkezik a forgalomirányítóra, nincs tovább út a célállomáshoz. Mindig ellenőrizze az összes forgalomirányító irányítótábláját a show IP route parancs segítségével!

1. Kérdéskör

2. Kérdéskör

3. Kérdéskör

4. Kérdéskör

9.3.2 IP-címtér megtervezésének és kiosztásának kérdései

A rosszul megtervezett IP-címkiosztás további bonyodalmakhoz vezethet. A rendszergazdák gyakran alábecsülik a lehetséges növekedést az alhálózatok tervezésekor. Ennek az a következménye, hogy az IP-alhálózati terv nem teszi lehetővé elegendő állomás címezését minden alhálózatban. Túl sok állomás jelenlétére utal az alhálózatban, ha egyes állomások nem kapnak IP-címet a DHCP kiszolgálótól.

Amikor egy Microsoft Windows operációs rendszert futtató számítógép nem kap IP-címet a DHCP kiszolgálótól, automatikusan választ magának egyet a 169.254.0.0 hálózathoz. A tünet jelentkezésekor ellenőrizni kell a *show ip dhcp binding* paranccsal, hogy van-e szabad, kiosztható cím a DHCP kiszolgálón.

A túl kevés IP-cím másik jellemző tünete a duplikált IP-címre utaló hibaüzenet az állomáson. Ha a DHCP bérleti ideje akkor jár le, amikor az azt birtokló állomás ki van kapcsolva, akkor a cím visszakérül a kiosztható címek készletébe, így kioszthatóvá válik egy másik számítógép számára. Amikor a cím eredeti bérlőjét újra bekapcsolják, az először megpróbálja megújítani a korábbi IP címét. Ebben az időpillanatban mindkét Microsoft Windows rendszert futtató állomás hibaüzenetet jelenít meg a duplikált címek miatt.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
192.168.10.10       0100.e018.5bdd.35    Oct 03 2007 06:14 PM    Automatic
192.168.10.11       0100.b0d0.d817.e6    Oct 03 2007 06:18 PM    Automatic
```

9.3.4 DHCP és NAT problémák

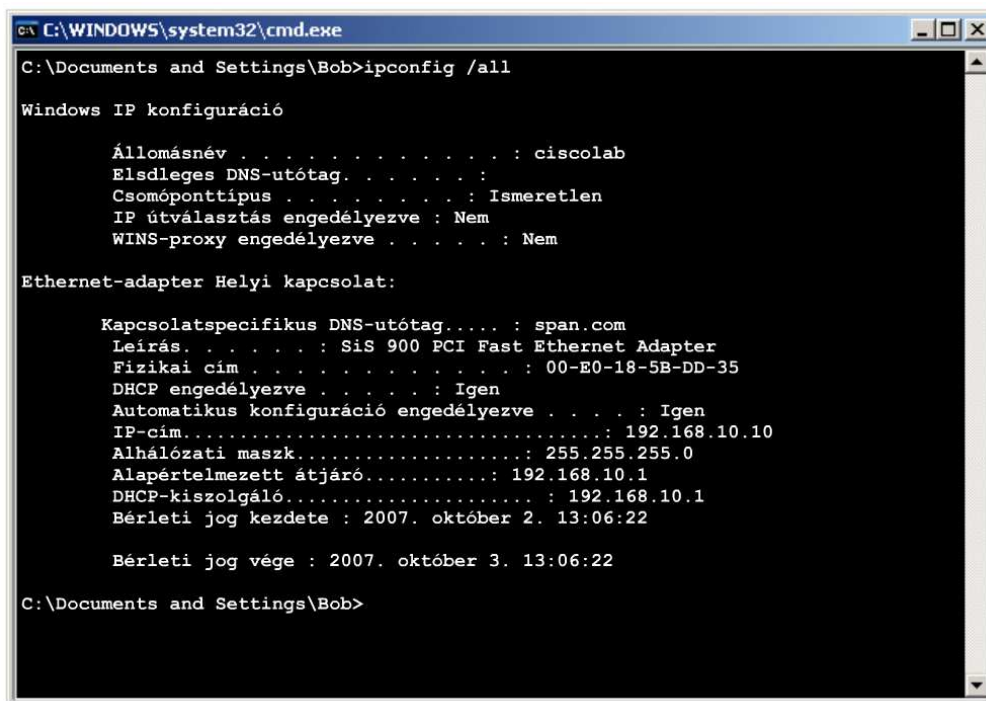
A DHCP további bonyodalmakat okozhat a hibaelhárítás során. Ha egy DHCP használatára beállított állomás nem tud kapcsolódni a hálózathoz, a Windows *ipconfig /all* paranccsal ellenőrizni kell, hogy kapott-e IP-címet. Ha nem kapott, valószínűleg a DHCP kiszolgálón kell keresni a hibát.

Függetlenül attól, hogy a DHCP szolgáltatás egy dedikált kiszolgálón, vagy a forgalomirányítón fut, a hibaelhárítás első lépése a fizikai kapcsolat ellenőrzése. Ha a szolgáltatás külön kiszolgálón fut, elsőként ellenőrizni kell, hogy a kiszolgáló fogad-e hálózati forgalmat. Ha a szolgáltatás a forgalomirányítón fut, a *show interfaces* paranccsal ellenőrizhető az interfész működése. A leállított állapotban levő interfészek nem továbbítanak semmilyen hálózati forgalmat, így DHCP kérésekre sem válaszolnak.

Következő lépés a DHCP kiszolgáló beállításainak ellenőrzése, különösen, hogy van-e elegendő kiosztható IP-címe. Ezek után a címütközések vizsgálat következik. Címütközés akkor is előfordulhat, ha van elegendő cím a DHCP címkészletben. Címütközés keletkezhet például, ha egy állomáson olyan cím van statikusan beállítva, mely szerepel a DHCP kiosztható címei közt is.

A *show ip dhcp conflict* paranccsal kilistáztatható az összes olyan címütközés, melyet a DHCP kiszolgáló regisztrált. Címütközés esetén az érintett cím kikerül a kiosztható címek halmazából, és mindaddig vissza sem kerül, amíg a rendszergazda fel nem oldja az ütközést.

Ha mindezek nem oldották meg a problémát, érdemes megvizsgálni, hogy valóban a DHCP szolgáltatásban van-e a hiba! Állítsunk be statikus IP-címet, alhálózati maszkot és az alapértelmezett átjárót az állomáson. Ha az állomás nem fér hozzá a hálózat erőforrásaihoz, akkor minden bizonnyal nem a DHCP szolgáltatás felelős a hibáért. Ezen a ponton a hálózati kapcsolat hibaelhárítására van szükség.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Bob>ipconfig /all

Windows IP konfiguráció

Állomásnév . . . . . : ciscolab
Elsődleges DNS-utótag. . . . . :
Csomóponttípus . . . . . : Ismeretlen
IP útválasztás engedélyezve : Nem
WINS-proxy engedélyezve . . . . . : Nem

Ethernet-adapter Helyi kapcsolat:

Kapcsolatspecifikus DNS-utótag . . . . : span.com
Leírás. . . . . : SiS 900 PCI Fast Ethernet Adapter
Fizikai cím . . . . . : 00-E0-18-5B-DD-35
DHCP engedélyezve . . . . . : Igen
Automatikus konfiguráció engedélyezve . . . . : Igen
IP-cím . . . . . : 192.168.10.10
Alhálózati maszk . . . . . : 255.255.255.0
Alapértelmezett átjáró . . . . . : 192.168.10.1
DHCP-kiszolgáló . . . . . : 192.168.10.1
Bérleti jog kezdete : 2007. október 2. 13:06:22

Bérleti jog vége : 2007. október 3. 13:06:22

C:\Documents and Settings\Bob>
```

A DHCP alapvetően üzenetszórást alkalmazó protokoll, ami azt jelenti, hogy a DHCP kiszolgálónak elérhetőnek kell lennie szórásos üzenetekkel. Tekintve, hogy a forgalomirányítók általában nem továbbítják a szórásos forgalmat, a DHCP kiszolgálónak vagy az állomással megegyező helyi hálózaton kell lennie, vagy a forgalomirányítón be kell állítani a szórásos üzenetek továbbítását.

A forgalomirányítók az *ip helper-address* parancs segítségével konfigurálhatók a szórásos üzenetek, így a DHCP kérések továbbküldésére is egy meghatározott kiszolgálóra. A parancs hatására a forgalomirányító egyedi címekre cseréli a szórásos célcímeket a csomagban:

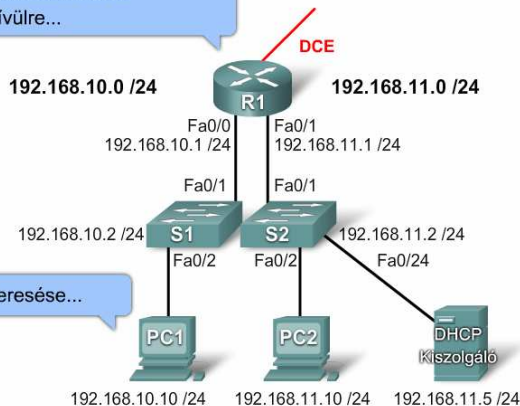
Router(config-if)# ip helper-address x.x.x.x

A parancs kiadása után az összes szórásos üzenet (köztük a DHCP kérések is) a parancsban megadott IP-címmel rendelkező kiszolgálóhoz kerülnek.

Amikor a forgalomirányító továbbküldi a címkéréseket, DHCP közvetítő ügynökként működik. A DHCP közvetítő szolgáltatás nélkül az állomások nem jutnának IP-címhez. Amikor egyik állomás sem kap IP-címet a másik hálózaton található DHCP kiszolgálótól, ellenőrizni kell az *ip helper-address* beállítás helyességét a forgalomirányítón.

Sajnálom, nem tudok továbbítani
semmilyen üzenetszórást az
alhálózaton kívülre...

DHCP kiszolgáló keresése...



DHCP probléma

Állomás probléma

Közvetítő (relay)
beállítás

Állomás
kapcsolatának
megújítása

Kattintson a gombokra a DHCP továbbítás működésének megismeréséhez!

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /release

Windows IP konfiguráció

Ethernet-adapter Helyi kapcsolat:

    Kapcsolatspecifikus DNS utótag, :
    IP-cím . . . . . : 0.0.0.0
    Alhálózati maszk . . . . . : 0.0.0.0
    Alapértelmezett átjáró . . . . . :

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP konfiguráció

Egy hiba keletkezett az interfész helyi hálózati kapcsolatának megújítása
során: nem jött létre kapcsolat a DHCP kiszolgálóval. A keresésre nem érkezett
válasz határidőn belül.
  
```

DHCP probléma

Állomás probléma

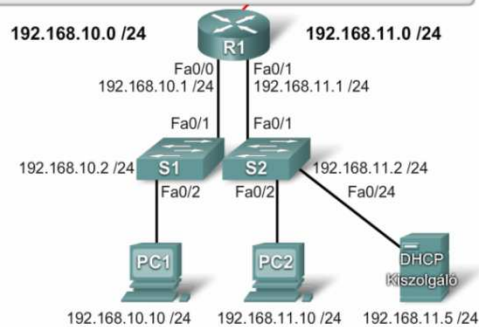
Közvetítő (relay)
beállítás

Állomás
kapcsolatának
megújítása

Kattintson a gombokra a DHCP továbbítás működésének megismeréséhez!

```

R1# config t
R1(config)# interface Fa0/0
R1(config-if)# ip helper-address 192.168.11.5
R1(config-if)# end
  
```



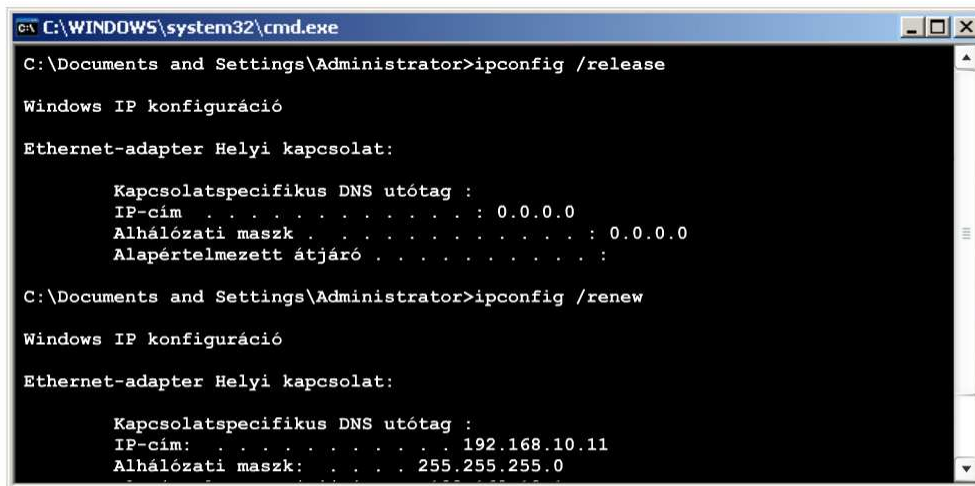
DHCP probléma

Állomás probléma

Közvetítő (relay)
beállítás

Állomás
kapcsolatának
megújítása

Kattintson a gombokra a DHCP továbbítás működésének megismeréséhez!



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /release

Windows IP konfiguráció

Ethernet-adapter Helyi kapcsolat:

    Kapcsolatspecifikus DNS utótag :
    IP-cím . . . . . : 0.0.0.0
    Alhálózati maszk . . . . . : 0.0.0.0
    Alapértelmezett átjáró . . . . . :

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP konfiguráció

Ethernet-adapter Helyi kapcsolat:

    Kapcsolatspecifikus DNS utótag :
    IP-cím: . . . . . : 192.168.10.11
    Alhálózati maszk: . . . . . : 255.255.255.0
```

DHCP probléma

Állomás probléma

Közvetítő (relay)
beállításÁllomás
kapcsolatának
megújítása

↳attintson a gombokra a DHCP továbbítás működésének megismeréséhez!

Ha a belső hálózat állomásai privát címmel rendelkeznek, az állomások csak NAT segítségével tudnak kommunikálni a nyilvános hálózattal. A NAT problémák legjellemzőbb tünete, hogy az állomások nem érik el az internetes oldalakat. Háromféle címfordítást különböztetünk meg: statikus, dinamikus és PAT (port address translation - port alapú címfordítás) A két legjellemzőbb beállítási hiba mindhárom fajtát érinti.

A belső és külső interfészek hibás kijelölése

A NAT működése szempontjából alapvető fontosságú, hogy a megfelelő interfészek legyenek belső és külső interfészként kijelölve. A legtöbb NAT megvalósításban a belső interfész kapcsolódik a privát címteret használó helyi hálózathoz. A külső interfész kapcsolódik a nyilvános hálózathoz, ami rendszerint egy internetszolgáltató hálózata. Ezek a beállítások a show running-config interface paranccsal ellenőrizhetők.

Helytelen IP-címbeállítás az interfészen vagy rossz NAT címtartomány

A legtöbb NAT megvalósításban a NAT címtartománynak és a statikus címfordításnak ugyanabból a tartományból származó IP-címeket kell használnia, mint amibe a külső interfész IP-címe esik. Ellenkező esetben a címfordítás megtörténik, de a rendszer nem talál útvonalat a lefordított címhez. Az összes lefordított cím elérhetőségét ellenőrizni kell. Amikor a címfordítás a külső interfész címét használja PAT esetén, ellenőrizni kell, hogy az interfész címe a megfelelő hálózathoz tartozik, és helyes alhálózati maszkkal rendelkezik.

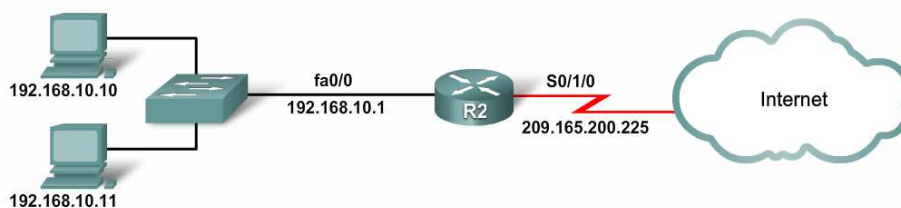
További problémát jelenthet, ha dinamikus NAT vagy PAT használata esetén a külső felhasználók nem érik el a belső erőforrásokat. Ha külső felhasználóknak el kell érniük bizonyos kiszolgálókat a belső hálózaton, akkor ezekhez statikus fordítást kell alkalmazni.

```
access-list 1 permit 192.168.0.0 0.0.255.255
! - Meghatározza, hogy mely címeket kell átfordítani.
ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240
! - Meghatároz egy NAT-POOL2 nevű címkészletet, mely a címfordítás során kerül használatra.
ip nat inside source list 1 pool NAT-POOL2 overload
! - Hozzárendeli a NAT címkészlethez az ACL 1-t
interface serial 0/0/0
ip nat inside
! - A Serial 0/0/0 interfészt belső NAT interfészként azonosítja.
interface serial 0/1/0
ip nat outside
! - A Serial 0/1/0 interfészt külső NAT interfészként azonosítja.
```

A NAT működésének ellenőrzését akkor is el kell végezni, ha a NAT beállítások helyessége bizonyos.

A NAT működés ellenőrzésében az egyik leghasznosabb parancs a *show ip nat translations*. Az érvényben levő fordítások megtekintése után a lista a *clear ip nat translation ** paranccsal törölhető. Megjegyzendő, hogy az érvényben levő IP címfordítások törlése fennakadásokat okozhat a felhasználói szolgáltatásokban. A törlést követően újból alkalmazni kell a *show ip nat translations* parancsot! Ha új címfordítások jelennek meg a listában, elképzelhető, hogy valami más hiba miatt nem érhető el az internet.

Ebben az esetben ellenőrizni kell, hogy van-e érvényes útvonalbejegyzés az internet felé a lefordított címekhez! A *traceroute* paranccsal megjeleníthető a lefordított csomagok útvonala. Ellenőrizni kell az útvonal helyességét. Ha van rá mód, ellenőrizni kell az útvonalat az egyik lefordított címre egy külső hálózaton található távoli számítógépről. Ez segíthet kiválasztani azt az eszközt, amely a hibát okozhatja. Elképzelhető, hogy forgalomirányítási probléma van azon a forgalomirányítón, ahol az útvonalkövetés elakadt.



```
access-list 1 permit 192.168.10.0 0.0.0.255
ip nat inside source list 1 interface serial 0/1/0 overload
interface fastethernet0/0
  ip nat inside
interface serial 0/1/0
  ip nat outside
```

[NAT túlterhelés](#)[NAT fordítások](#)[NAT törlése](#)

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
tcp 209.165.200.225:62452 192.168.10.11:62452 209.165.200.254:80 209.165.200.254:80

R2#show ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
   create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
   flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452 192.168.10.11:62452 209.165.200.254:80 209.165.200.254:80
   create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
   flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

NAT túllerhelés

NAT fordítások

NAT törlése

```
R2#clear ip nat translation *
R2#show ip nat translations
R2#
```

NAT túllerhelés

NAT fordítások

NAT törlése

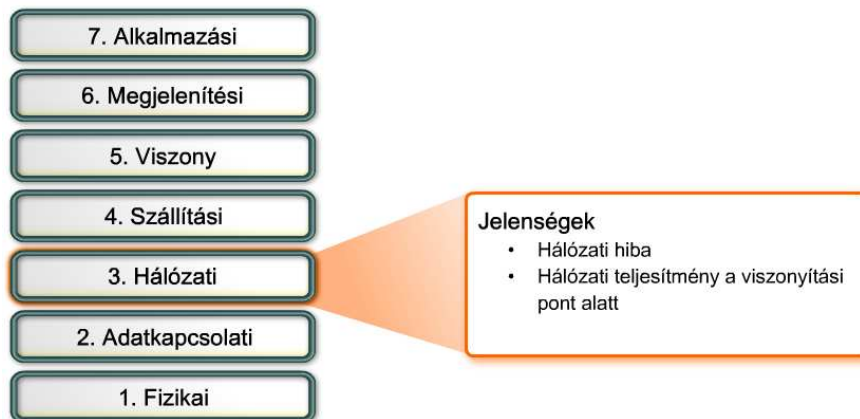
9.4 3. rétegbeli irányítási problémák

A 3. réteg gyakorlatilag az állomások és hálózatok címzését, valamint az ezek közti forgalomirányítást végző protokollokat definiálja.

A legtöbb hálózatban különböző típusú útvonalak vannak egyszerre jelen: statikus, dinamikus és alapértelmezett útvonalak. Az irányítási folyamat hibái hálózati leállást okozhatnak, és igen kedvezőtlenül érintik a hálózat teljesítményét. A hibák forrása sokféle lehet: rossz kézi útvonalbejegyzések, irányítóprotokollok beállítási és működési hibái, valamint az OSI alsóbb rétegeinek hibái.

A 3. rétegbeli problémák megoldása megköveteli az irányítási folyamatok, a különböző útvonaltípusok és azok működésének alapos ismeretét.

A folytatás előtt érdemes lehet átismételni a CCNA Discovery: Otthoni és kisvállalati hálózatok és CCNA Discovery: Hálózati feladatok kis- és középvállalatoknál vagy internetszolgáltatóknál tananyagok forgalomirányítással, irányítóprotokollokkal foglalkozó részeit.



Számos tényezőnek köszönhetően a hálózat állapota gyakran változhat:

- Egy interfész meghibásodik.
- A szolgáltató megszakítja az összeköttetést.
- A rendelkezésre álló sávszélesség túlterheltté válik.
- Egy rendszergazda helytelen konfigurációt készít.

Minden egyes hálózati változásnál előfordulhat, hogy útvonalak vesznek el, vagy téves útvonalak kerülnek az irányítótáblába.

A 3. rétegbeli problémák feltárásának legfontosabb eszköze a *show ip route* parancs, amely kilistázza az összes olyan útvonalat, amelyet a forgalomirányító felhasznál a csomagok továbbítására. A forgalomirányító-tábla az alábbi forrásokból származó bejegyzéseket tartalmaz:

- Közvetlenül kapcsolódó hálózatok
- Statikus útvonalak
- Dinamikus forgalomirányító protokollok

Az irányítóprotokollok az irányítási mérték alapján választják ki az előnyben részesített útvonalakat. A közvetlenül kapcsolódó hálózatok mértéke 0, csakúgy mint a statikus útvonalak alapértelmezett mértéke. A dinamikus útvonalak irányítási mértéke irányítóprotokollonként változó.

Ha egy célhálózat felé több útvonal is létezik, a legkisebb adminisztratív távolságú (administrative distance - AD) útvonal kerül be az irányítótáblába.

Ha irányítási probléma gyanúja merül fel, a *show ip route* paranccsal ellenőrizhető, hogy a remélt útvonal szerepel-e az irányítótáblában.

Az útvonal forrása	Adminisztratív távolság	Alapértelmezett mérték(ek)
Csatlakoztatva	0	0
Statikus	1	0
EIGRP összevont útvonal	5	
Külső BGP	20	Rendszergazda által megadott érték
Belső EIGRP	90	Sávszélesség, késleltetés
IGRP	100	Sávszélesség, késleltetés
OSPF	110	Összeköttetés költsége (sávszélesség)
IS-IS	115	Összeköttetés költsége (rendszergazda által megadott érték)
RIP	120	Ugrásszám
Külső EIGRP	170	
Belső BGP	200	Rendszergazda által megadott érték

Közvetlenül kapcsolódó hálózatok problémái

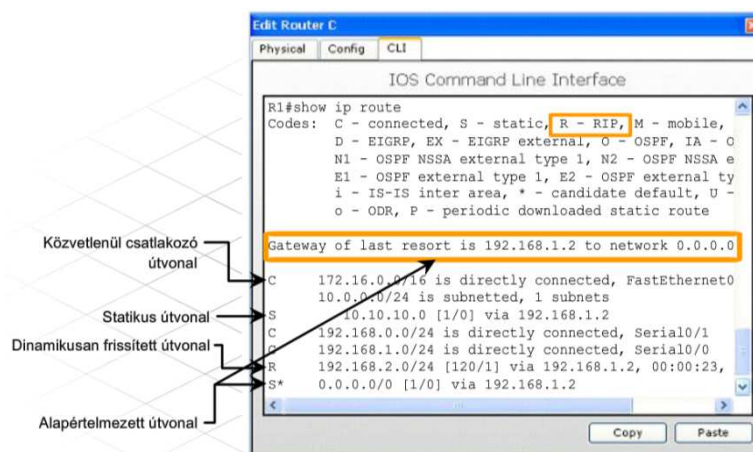
A közvetlenül kapcsolódó hálózatok automatikusan bekerülnek az irányítótáblába, mielőtt az interfész IP-címet kap, és a *no shutdown* parancs végrehajtódik. Ha egy közvetlenül kapcsolódó hálózat nem jelenik meg az irányítótáblában, a *show interfaces* vagy a *show ip interface brief* paranccsal ellenőrizhető, hogy rendben van-e az interfész IP-címe, illetve up/up állapotban van-e.

Statikus és alapértelmezett útvonalak problémái

Szinte mindig beállítási probléma van a háttérben, ha egy statikus vagy egy alapértelmezett útvonal nem jelenik meg az irányítótáblában. Statikus és alapértelmezett útvonalak megadhatók a kimenő interfész vagy a következő ugrás IP-címének megnevezésével. A statikus útvonalak hibája gyakran abból ered, hogy a megadott következő ugrás IP-címe nem esik egyik közvetlenül kapcsolódó hálózat tartományába sem. Mindig ellenőrizni kell a konfigurációs parancsok helyességét és hogy a használt kimenő interfészek up/up állapotban vannak-e.

Dinamikus útvonalak problémái

Több, különböző probléma okozhatja, hogy a dinamikus útvonalak nem épülnek be az irányítótáblába. Mivel a dinamikus irányítóprotokollok irányítási információkat cserélnek a hálózat többi forgalomirányítójával, a célhoz vezető útvonalon lévő bármelyik forgalomirányító hibás beállítása eredményezheti egy-egy útvonal kiesését.



9.4.2 A dinamikus forgalomirányítás hibái

A forgalomirányító tábla frissítéseket általában új hálózat belépése vagy egy hálózat elérhetetlenné válása idézi elő.

Közvetlenül kapcsolódó hálózatok megjelenésekor a forgalomirányító tábla csak akkor frissül, ha a közvetlenül csatlakozó interfész állapota megváltozik. Statikus és alapértelmezett útvonalak konfigurálása esetén a forgalomirányító tábla csak akkor változik, ha új útvonalat definiálnak, vagy ha az útvonal meghatározásában szereplő kimenő interfész állapota megváltozik.

A dinamikus forgalomirányító protokollok automatikusan frissítéseket küldenek a hálózat más forgalomirányítóinak. Ha a dinamikus forgalomirányítás engedélyezve van, a forgalomirányító mindig frissíti az irányítótábláját, amikor egy szomszédos forgalomirányítótól kapott frissítésben változást észlel.

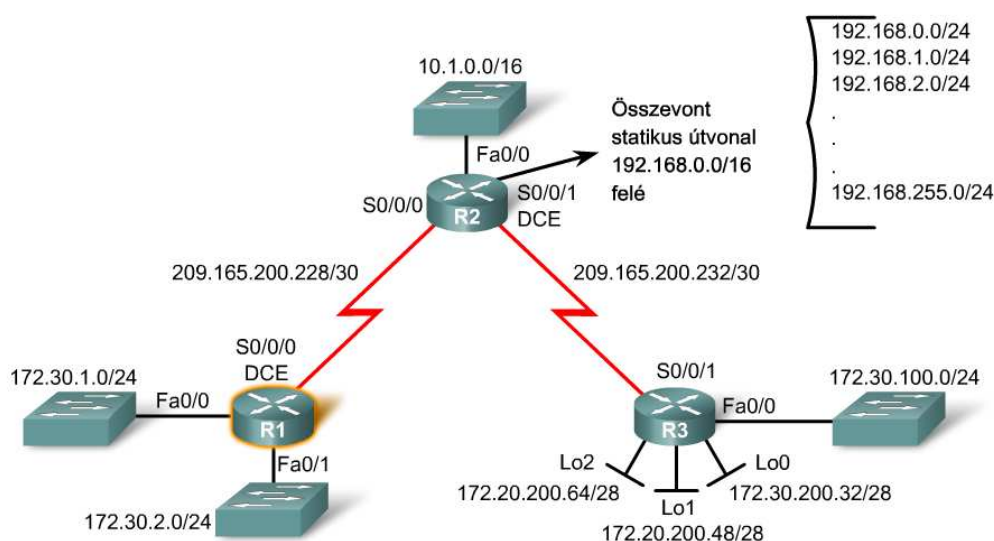
A RIP egy olyan dinamikus irányítóprotokoll, melyet kis és közepes helyi hálózatokban használnak. A RIP protokollal kapcsolatos hibák kijavításakor ellenőrizni kell a verzió beállítását és konfigurációs parancsokat.

Tanácsos a forgalomirányító protokollnak ugyanazt a verzióját használni az összes forgalomirányítón. Bár a RIPv1 és a RIPv2 kompatibilis, a RIPv1 nem tudja kezelni az osztály nélküli forgalomirányítást (CIDR) és a változó hosszúságú alhálózati maszkokat (VLSM). A RIPv1 és a RIPv2 egyidejű futtatása ugyanazon a hálózaton problémákat okozhat. Míg a RIPv2 automatikusan figyeli a RIPv1 és a RIPv2 frissítéseket is, a RIPv1 nem fogadja a RIPv2 frissítéseit.

Abból is forgalomirányítási problémák származhatnak, ha hiányoznak vagy hibásak a network utasítások. A network utasítások szerepe kettős:

- Engedélyezi, hogy az irányítóprotokoll minden olyan interfészen frissítéseket küldjön és fogadjon, melynek IP-címe a network parancs által megadott hálózatba esik.
- A kiküldött frissítéseiben feltünteti ezt a hálózatot.

A hiányzó, vagy hibás network utasítás, tehát hibás irányítási frissítéseket generálhat, illetve megakadályozhatja, hogy a forgalomirányító adott interfészén frissítéseket küldjön és fogadjon.



```
R1#show running-config
Building configuration...
!
hostname R1
!
interface FastEthernet0/0
 ip address 172.30.1.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.30.2.1 255.255.255.0
!
interface Serial0/0/0
 ip address 209.165.200.230 255.255.255.252
 clock rate 64000
!
router rip
 version 2
 network 172.30.0.0
 network 209.165.200.0
 no auto-summary
!
!
end
```

A dinamikus irányítás hibáinak feltárásában sok eszköz segíthet.

A TCP/IP **ping** és **tracert** segédprogramja használható a kapcsolat ellenőrzéséhez. A telnet segítségével egyrészt ellenőrizhető a kapcsolat, másrészt távoli eszközök is konfigurálhatók. A Cisco IOS show parancsai pillanatképet mutatnak a forgalomirányító beállításairól és az egyes összetevők állapotáról. A Cisco IOS parancskészlete számos debug parancsot is tartalmaz.

A debug parancsok dinamikus működésűek, valós idejű információt szolgáltatnak a hálózati forgalomról és a protokollok kommunikációjáról. Például a *debug ip rip* parancs a RIP irányítóprotokoll üzenetváltásait mutatja meg.

A debug parancsok komoly CPU erőforrásokat kötnek le, így lassíthatják, vagy akár meg is állíthatják a forgalomirányító normál működését. Éppen ezért a debug parancsokat csak a hibafeltárásban szabad használni, a forgalomirányító normál működésének monitorozására nem ajánlott.



9.5 A 4. és a felsőbb rétegek hibaelhárítása

9.5.1 4. rétegbeli forgalomszűrési hibák

A 4. (szállítási) réteget szokás átmenetnek tekinteni az OSI modell alsóbb és a felsőbb rétegei között. A 4. réteg felelős az adatcsomagok szállításáért, és definiálja az egyes alkalmazások eléréséhez használatos portszámokat. A 4. rétegbeli problémák a hálózat határán lépnek fel, ahol a biztonsági technológiák ellenőrzik és módosítják a forgalmat. Számos problémát okoznak a tűzfalak, amelyeket úgy konfigurálnak, hogy a portszámok alapján tiltsák a forgalmat, amelyet egyébként továbbítaniuk kellene.

A 4. réteg az UDP és a TCP forgalmat támogatja. Egyes alkalmazások kizárólag az egyiket használják, mások mindkettőt. Éppen ezért a portszámokon alapuló forgalomszűrésnél meg kell nevezni a protokollt is. Előfordul, hogy a TCP és az UDP protokollt is tiltják egy adott portszámhoz, pusztán mert bizonytalanok abban, hogy az adott alkalmazás melyiket használja. Ez a megoldás azonban olyan forgalmat is kiszűrhet, melynek kiszűrése nem volt cél.

A tűzfalakat gyakran úgy konfigurálják, hogy az explicit permit utasításokkal engedélyezett forgalom kivételével minden más forgalmat tiltsanak. Ha egy engedélyezett forgalomtípus nem szerepel a tűzfal utasításai között, vagy egy új alkalmazás jelenik meg a hálózaton anélkül, hogy a megfelelő engedélyek bekerülnének a tűzfal konfigurációjába, forgalomszűrési problémák keletkezhetnek.

A 4. rétegre jellemző hibajelenség, hogy a felhasználók bizonyos webes szolgáltatásokat (például video- és audioszolgáltatásokat) nem érnek el.

Ellenőrizni kell, hogy a tűzfalon engedélyezett ill. tiltott portok biztosítják-e az alkalmazások megfelelő működését. Az egyes alkalmazásokhoz tartozó portok jobb megértéséhez érdemes átismételni a CCNA Discovery: Otthoni és kisvállalati hálózatok és CCNA Discovery: Hálózati feladatok kis- és középvállalatoknál vagy internetszolgáltatónál tananyag TCP és UDP portokra vonatkozó részeit.



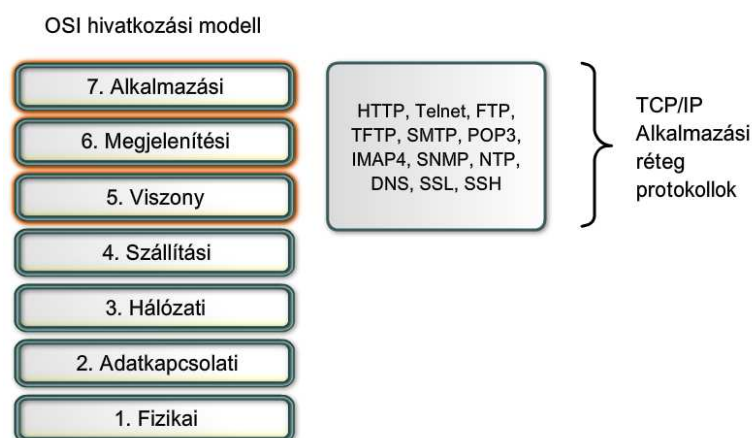
9.5.2 Felsőbb rétegek hibáinak elhárítása

A felsőbb rétegbeli protokollok többnyire olyan felhasználói szolgáltatásokat nyújtanak, mint a hálózatzfelügyelet, a fájlátvitel, az elosztott szolgáltatások, a terminálemuláció és az elektronikus levelezés. A felsőbb rétegekben működő protokollokat szokás TCP/IP alkalmazási rétegbeli

protokolloknak is nevezni, mivel a TCP/IP modell alkalmazási rétege az OSI modell felső 3 rétegét egyesíti.

Az alábbi listában láthatók a legismertebb, leggyakrabban megvalósított TCP/IP alkalmazási rétegbeli protokollok:

- Telnet - lehetővé teszi terminálkapcsolat kialakítását egy távoli állomással.
- HTTP - webes felületen történő adatcserét (szövegek, képek, hangok, videók és más multimédiás tartalmak) tesz lehetővé.
- FTP - TCP alapú, interaktív fájlátvitelt tesz lehetővé az állomások között.
- TFTP - egyszerű, de interaktív fájlátvitelt tesz lehetővé UDP fölött, jellemzően állomások és hálózati eszközök között.
- SMTP - alapvető levéltovábbítási szolgáltatást nyújt.
- POP3 - kapcsolatot teremt a levelező-kiszolgálóval és letölti a leveleket a levelezőprogramba.
- IMAP4 - lehetővé teszi, hogy a levelezőprogramok letöltsék a leveleket kiszolgálóról, és küldjenek leveleket a kiszolgálóra.
- SNMP - a felügyelt eszközökről gyűjt információt.
- NTP - pontos idő szolgáltatást nyújt a hálózati eszközöknek és állomásoknak.
- DNS - a hálózati neveket és az IP-címeket társítja.
- SSL - a HTTP tranzakciók titkosítását és biztonságát garantálja.
- SSH - kiszolgálók és hálózati eszközök biztonságos távoli elérését teszi lehetővé.



A felsőbb rétegek problémáit sokszor nem könnyű behatárolni, különösen, ha az ügyfél beállításai nem utalnak semmi hibára. A felsőbb rétegek hibaelhárítását is az alapvető kapcsolati hibák kiszűrésével érdemes kezdeni.

Az "oszd meg és uralkodj" elv alapján célszerű a 3. rétegbeli kapcsolat ellenőrzésével kezdeni a hibaelhárítást.

1. lépés Ping üzenet küldése az állomás alapértelmezett átjárójához.

2. lépés A végponttól-végpontig tartó kapcsolat ellenőrzése.

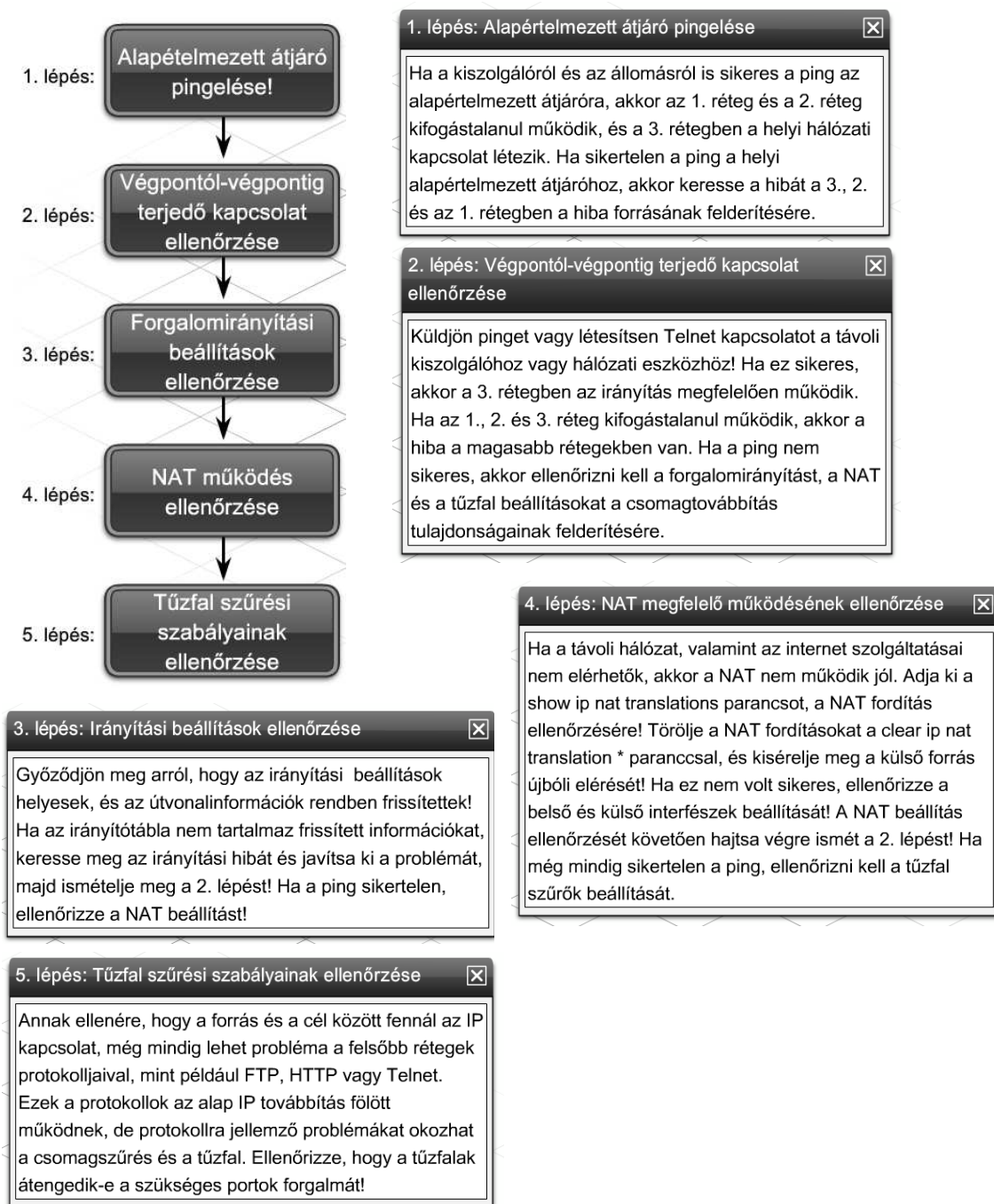
3. lépés Az irányítási beállítások ellenőrzése.

4. lépés A NAT megfelelő működésének ellenőrzése.

5. lépés A tűzfalszabályok ellenőrzése.

Ha a probléma egy távoli hálózatban jelentkezik, a végponttól-végpontig tartó kapcsolat nem ellenőrizhető, hiszen bizonyos kapcsolatok más felügyelet alá tartoznak. Ebből következően előfordulhat, hogy bár a helyi eszközökön minden rendben van, mégis problémák vannak a távoli hálózat elérésével. Ebben az esetben az internetszolgáltatóval kell ellenőriztetni, hogy a hálózati kapcsolatok működőképes-e.

Ha mindez megtörtént, és a végponttól-végpontig tartó kapcsolat működőképes, miközben a végberendezés még mindig nem működik megfelelően, akkor a hibát a felsőbb rétegekben kell keresni.



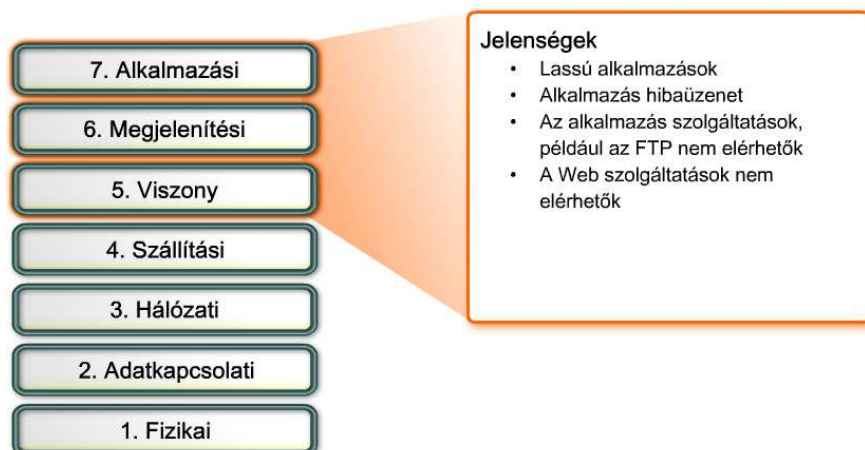
A felsőbb rétegek hibái miatt általában nem működhetnek az alkalmazói programok felé nyújtott szolgáltatások. Elérhetetlenné, vagy működésképtelenné tehetik az erőforrásokat, annak ellenére, hogy az alsóbb rétegek üzemképesek. Előfordulhat, hogy a hálózati kapcsolattal minden rendben van, az alkalmazás mégsem szolgáltat adatokat.

A felsőbb rétegek hibái sokszor csak néhány vagy csak egyetlen alkalmazást érintenek. Nem ritka, hogy olyan hívás fut be az ügyfélszolgálatra, hogy a felhasználó nem éri el a leveleit, miközben a többi hálózati szolgáltatás üzenszerűen működik.

A felsőbb rétegbeli hibákért legtöbbször a rossz ügyfélprogram-beállítások a felelősek. Az ügyfél nem jut hozzá a szükséges információhoz, ha rossz levelező- vagy az FTP kiszolgáló van megadva. Ha több alkalmazást is érintett, a felsőbb réteg hibáját a DNS szolgáltatás környékén érdemes kereseni.

A Windows *nslookup* segédprogramjával ellenőrizhető, hogy a DNS szolgáltatás hibátlanul működik-e, és fel tudja-e oldani a kiszolgálók IP-címeit. Ha a DNS szolgáltatás nem az elvárásoknak megfelelően működik, ellenőrizni kell az állomáson a DNS kiszolgáló címének beállítását. Ha az állomás a DNS kiszolgáló címét egy DHCP kiszolgálótól kapja, ellenőrizni kell a DHCP kiszolgálón a DNS kiszolgáló IP-címének beállítását.

Ha a DNS kiszolgáló üzemel és elérhető, ellenőrizni kell a DNS zónabeállítások hibáit. A hibát gyakran a címek és a tartománynevek elírása okozza a konfigurációs fájlokban.



A felsőbb rétegek a felelősek a titkosításért és a tömörítésért is. Alkalmazási hibákhoz vezethet, ha az ügyfél ill. a kiszolgáló nem ugyanúgy titkosítja és tömöríti az adatokat, mint ahogyan a másik fél elvárja.

Ha a probléma egyetlen állomásra korlátozódik, valószínű, hogy az adott számítógépen futó alkalmazás beállításai van a hiba. A böngészők különböző beépülő moduljai, mint például az Adobe Reader, gyakran felsőbb rétegbeli hálózati funkciókat is megvalósítanak. A weboldalak helyes megjelenítése érdekében ezeket a modulokat rendszeresen frissíteni kell.

Az adat lekérésekor használt nem megfelelő protokoll okozhatja, hogy a weboldal nem elérhető. Például előfordulhat, hogy az SSL-lel titkosított oldalak megtekintéséhez a **https://** kezdetű címet kell a böngésző címsorába írni a szokásos **http://** helyett.

9.5.3 Felsőbb rétegbeli kapcsolat ellenőrzése Telnettel

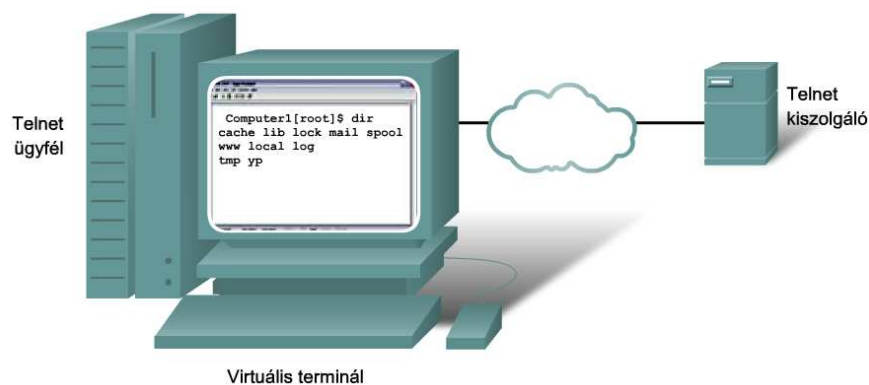
A Telnet jól használható a felsőbb rétegbeli problémák elhárításában. Segítségével a rendszergazdák úgy kapcsolódhatnak a hálózati eszközökhöz, és adhatnak ki parancsokat, mintha helyileg csatlakoznának. Sikeres bejelentkezés egy eszközre telnettel, egyúttal az alsóbb rétegek megfelelő működését is jelzi.

Mindazonáltal, a telnet nem biztonságos protokoll, vagyis minden továbbított információ könnyedén lehallgatható és olvasható. Ha a legkisebb esélye is megvan, hogy illetéktelenek lehallgatják a hálózati kommunikációt, akkor telnet helyett a Secure Shell (SSH) protokoll használata ajánlott. Az SSH lényegesen biztonságosabb módja a távoli eszközök elérésének.

A Cisco IOS újabb változatainak többsége már tartalmaz SSH kiszolgálót. Egyes eszközökben ez a szolgáltatás már alapértelmezésként fut, másokon külön engedélyezni kell.

A Cisco IOS csomagok tartalmaznak egy SSH ügyfelet is, hogy SSH kapcsolatot tudjanak létesíteni más eszközökkel. Hasonlóan, távoli számítógépek SSH ügyfél segítségével biztonságos parancssori kapcsolatot kezdeményezhetnek. Az SSH ügyfélprogram nem minden operációs rendszernek része, ebben az esetben a rendszergazdának külön kell beszereznie, telepítenie és konfigurálnia.

Érdemes átismételni az SSH konfigurálását és használatát a CCNA Discovery: Hálózati feladatok kis- és középvállalatoknál vagy internetszolgáltatóknál tananyagban.



A Telnet lehetővé teszi, hogy a hálózaton keresztül hozzáférhessen egy hálózati eszközhöz úgy, mintha a billentyű és a monitor közvetlenül az adott eszközhöz csatlakozna.

9.6 Felkészülés a Cisco képesítés megszerzésére

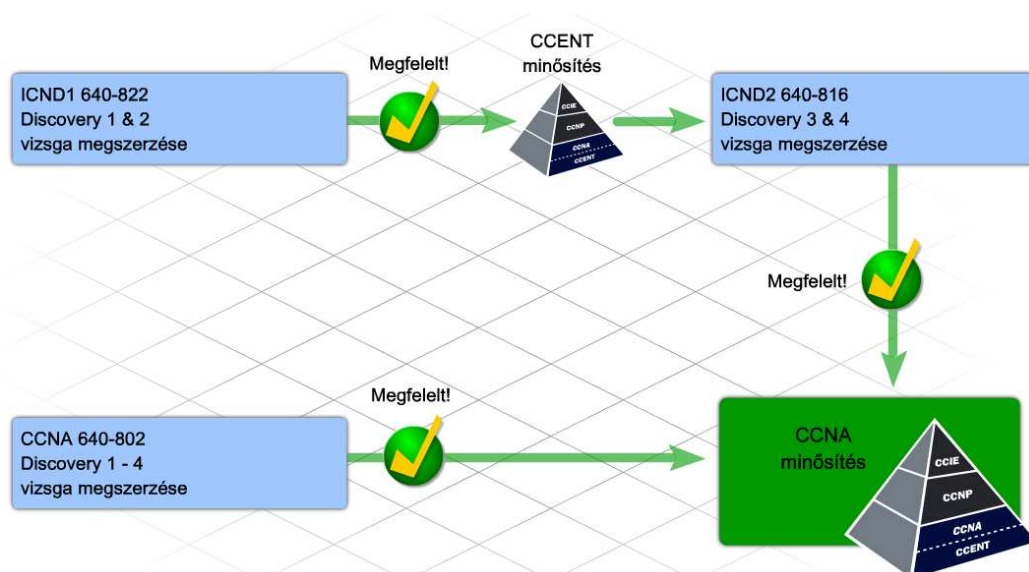
9.6.1 Tudás, készség és képesség

A CCENT (Cisco Certified Entry Networking Technician - Cisco belépő szintű hálózati technikus) minősítés igazolja, hogy a tulajdonosa rendelkezik a belépő szintű hálózat támogatási munkakörök ellátáshoz szükséges szakértelemmel, amely számos sikeres karrier kiindulópontja a számítógépes hálózatok területén. Megszerzése az első lépés a CCNA (Cisco Certified Network Associate - Cisco hálózati rendszergazda) képesítés felé vezető úton, amely a közepes méretű, bonyolultabb összeköttetésekkel bíró, vállalati kirendeltségek hálózatait foglalja magába. A CCENT képesítés megszerzéséhez a jelöltnek le kell tennie az ICND1 vizsgát a hivatalos Cisco vizsgaközpontok valamelyikében. (A CCENT vizsga jelenleg magyar nyelven nem érhető el.)

Az ICND1 (640-822) vizsgán a jelöltnek azt kell bizonyítania, hogy rendelkezik a kis irodai hálózatok telepítéséhez, üzemeltetéséhez és hibaelhárításához szükséges képességekkel. A vizsga részét képezik az alábbi hálózati alapismeretek:

- Csatlakozás egy WAN-hoz
- Alapvető hálózatbiztonsági és vezeték nélküli hálózati ismeretek
- Forgalomirányítás és kapcsolás
- A TCP/IP és az OSI modell
- IP-címzés
- WAN-technológiák
- Cisco IOS operációs rendszert futtató eszközök üzemeltetése és konfigurálása
- RIPv2, statikus és alapértelmezett forgalomirányítás konfigurálása
- NAT és DHCP alkalmazása
- Egyszerű hálózatok konfigurálása

A Cisco vizsgára való felkészülés komoly kihívás. A Cisco különös figyelmet fordít a CCNA vizsgák színvonalának megtartására, ezért rendszeresen frissíti az elvárásokat. Egyes jelöltek elsőre leteszik a vizsgát, mások többször nekifutnak, és olyanok is akadnak, akiknek nem sikerül megszerezniük a képesítést. Az alapos felkészülés a legjobb módszer ahhoz, hogy az első csoportba tartozzon valaki.



Mindig érdemes azzal kezdeni a vizsgafelkészülést, hogy az ember megérti a vizsga célját. A Cisco vizsgarendszerek célja, hogy egy adott szakterületen mérjék a jelölt tudását, szakértelmét és képességét. A vizsga többféle mérési technikát alkalmaz annak érdekében, hogy a jelölt bizonyíthassa rátermettségét, és a különböző hálózati feladatok megvalósításában szerzett jártasságát. A vizsga tartalmaz feleletválasztós feladatokat, különböző gyakorlatokat és szimulált hálózatkonfigurációs feladatokat is. Minden kérdésnek, feladatfajtának célja van. A Cisco képesítések honlapján megtalálhatók az ICND1 vizsga céljai.

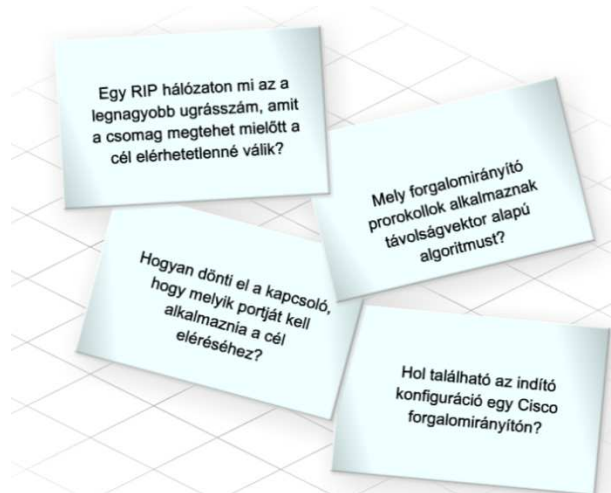
Ismeret
A természetben az ismeret általában tényekről vagy történetekről szól. Közvetlenül egy feladat elvégzésével kapcsolatos.

Készségek
A készség azt jelenti, hogy képesek vagyunk kézzel, szóval vagy szellemileg adatokat vagy tárgyakat kezelni a kívánt eredmény elérése érdekében. A készséget egy teljesítményvizsgálat mérheti, ahol mennyiségi és minőségi követelményeknek kell megfelelni adott időn belül. Készségeinkkel kapcsolatos feladat például egy szöveg gépelése vagy egy jármű vezetése.

Képességek
A képesség azt jelenti, hogy végre tud hajtani egy konkrét tevékenységet. Olyan tevékenységen keresztül bizonyítható, mint amelyet majd a munkavégzés során kell végrehajtani. Például képesség arra, hogy meg tudja tervezni és szervezni saját munkáját.

9.6.1 Hálózati tudás, készség és képesség

A hálózati feladatok megoldása általában megköveteli bizonyos háttérismeretek meglétét. Ez a fajta tudás legtöbbször tényeken alapul. A vizsgára készülés során mindig érdemes az adott számonkérési célhoz tartozó alapvető tényeket rendszerezni. Van, akinek segít, ha kis kártyákra felírja a tényeket, kulcsfogalmakat tanulás közben. Ugyan szerepelhet a vizsgán néhány olyan kérdés, amikor csak a lexikális tudást kell mozgósítani, de többségében a hálózati problémák feltárása és megoldása során lesz szükség ezekre az ismeretekre.

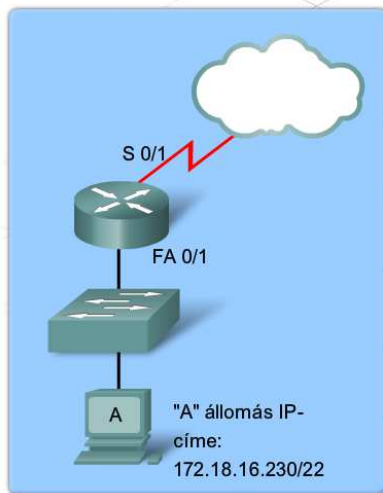


A hálózati feladatok megoldása sokrétű szakértelmet igényel. Egyes készségek roppant egyszerűek, mint például a keresztkötésű kábel készítése. Mások jóval összetettebbek, például az IP-hálózatok kialakítása.

A hálózattervezési feladatok elsajátítása sok gyakorlást igényel. A laborgyakorlatok és a Packet Tracer feladatok hivatottak a sokrétű tapasztalatszerzés lehetőségét biztosítani a hallgatók számára.

A Cisco vizsgák az alapján mérik a jelölt felkészültségét a számítógépes hálózatok tárgykörében, hogy miként tud a Cisco hálózati eszközökkel dolgozni. Ezért elengedhetetlenül fontos, hogy kellő tapasztalatot szerezzenek a hallgatók a Cisco IOS használatában. A vizsgafeladatok jelentős részének megoldásához szükség van a különböző IOS parancsok, elsősorban a *show* parancsok kimenetének értelmezésére.

Ez a mintakérdés annak ellenőrzésére szolgál, hogy a jelölt mennyire jártas az IP-címzésben és a Cisco IOS szoftver használatában.



Tanulmányozza az ábrát! Melyik Cisco IOS parancs rendeli hozzá az első felhasználható IP-címet az alhálózatban az RTA FastEthernet 0/1 interfészéhez?

- A. RTA(config-if)#ip address 172.18.13.1 255.255.254.0
- B. RTA(config-if)#ip address 172.18.14.1 255.255.252.0
- C. RTA(config-if)#ip address 172.18.14.1 255.255.255.252
- D. RTA(config-if)#ip address 172.18.16.1 255.255.252.0
- E. RTA(config-if)#ip address 172.18.16.1 255.255.255.252
- F. RTA(config-if)# ip address 172.18.16.229 255.255.255.252

A belépő szintű technikus számára a legfontosabb, hogy rendelkezzen a tervezés, a szervezés, a kivitelezés és a problémamegoldás képességével. Vizsgahelyzetben ezek meglétét leginkább konfigurációs és hibaelhárítási feladatokon keresztül lehet ellenőrizni. A vizsgafeladatok összeállításakor az a cél, hogy a vizsgahelyzetek minél jobban közelítsék a valós élethelyzetekben előforduló szituációkat. Ezek a körülmények szimulációkkal és esetleírásokkal közelíthetők legjobban.

Az esetleíráson alapuló és a szimulációs feladatokra nehezebb felkészülni, mint néhány adatot megjegyezni, vagy egy adott képességet begyakorolni. A kitűzött célok teljesítése és a probléma megoldása egyszerre követeli meg az ismeretek és a készségek mozgósítását.

A hibaelhárítási képességek fejlesztésének egyik legjobb módja, ha elsőként az adott hálózati probléma megoldásához szükséges ismeretek és képességek elemzésére kerül sor. A szükséges ismeretek feltárását követően érdemes eljátszani a gondolattal, hogy mi történne, ha azok nem lennének ismertek. Ajánlott egy lista készítése a lehetséges kimenetelekről, majd annak eldöntése, milyen készségeket igényelne egy-egy probléma felismerése és kijavítása, ha az bekövetkezne. Elsőre bonyolultnak hangozhat mindez, de az alábbi példák segíthetik az áttekintést:

- Mi történne, ha a technikus nem lenne tisztában az alhálózatban kiosztható állomáscímek számával adott alhálózati maszk használata esetén? Hogyan ismerhető fel a probléma, és mit lehet tenni a megoldása érdekében?
- Milyen problémák származhatnak abból, ha egy RIPv2 hálózatban van olyan útvonal a forrás és a cél között, amely hosszabb 15 ugrásnál? Milyen tünetek tapasztalhatók ilyen esetben? Hogyan oldható meg a probléma?

Feledat: Állítson be a RIPv2 protokollt a hálózati forgalom irányítására.

Szükséges információ

Lehetséges problémák, ha nincs meg a szükséges tudásom

A problémák lehetséges tünetei

Szükséges információ:

- RIPv2 protokoll konfigurálásának lépései.
 1. Jelentkezzen be a forgalomirányítóra!
 2. Lépjen be privilegizált módba!
 3. Lépjen be konfigurációs módba!
 4. Engedélyezze a RIP-et!
 5. Engedélyezze a 2. verziót!
 6. Adja ki a network parancsot a RIP-ben résztvevő kapcsolódó hálózatokra!
- Cisco IOS parancsok a RIPv2 irányítás engedélyezésére.
 1. Config t
 2. Router rip
 3. Version 2
 4. Network [cím]
 5. Copy running-config startup-config
- Hálózati címek az egyes csatlakoztatott hálózatokhoz
- Módszerek a RIPv2 protokoll helyes konfigurációjának és működésének ellenőrzésére.
 1. A show running-configuration parancs alkalmazása
 2. A show ip route parancs alkalmazása
 3. Ping parancs kiadása az állomásról egy másik hálózaton levő IP címre
 4. A forgalom nyomonkövetése a forgalomirányítón át a távoli IP-címig
 5. A debug használata annak ellenőrzésére, hogy a RIPv2 irányítási frissítések rendben megtörténnek-e.

Felmerülő problémák:

- Nem tudok belépni konfigurációs módba a beállítás megkezdéséhez.
- Elfelejtettem beállítani a 2. verziót vagy hozzáadni a network parancsokat.
- Nem tudom beállítani az összes hálózatot.
- Rossz IP-cím információt állítottam be.
- Nem tudom ellenőrizni, hogy a RIPv2 helyesen működik-e.

A problémák lehetséges tünetei:

- Sikertelen a ping más hálózat állomásaira
- A nyomkövetés nem tud átmenni a forgalomirányítón
- Nem jelentek meg útvonalak a forgalomirányító irányítótáblájában.

9.6.3 Elhatározás

Minősítő vizsgát tenni komoly elszántságot kíván. Rengeteg anyagot kell átismételni és feladatot kell megoldani. A vizsgára készülés is sikeresebb lesz – csakúgy, mint egy ügyfél hálózatának a kialakítása – ha kisebb részfeladatokra bontjuk:

1. Elhatározás
2. Tervkészítés
3. Vizsgarutin megszerzése

Ezután a pár lépés után megkezdődhet a tényleges felkészülés.

A Cisco képzés megszerzéséhez vezető út első lépése az elhatározás, a kellő idő és energia ráfordítása érdekében. Az elhatározásnak együtt kell járnia azzal, hogy a felkészülésnek maximális prioritást adunk, hiszen nyilván más tevékenységektől kell elvonni a ráfordítandó időt.

A ráfordított idő önmagában nem elegendő: megfelelő figyelmet is kell szentelni a felkészülésnek. Meg kell keresni azt a helyet otthon vagy az iskolában, ahol a zavartalan tanulás hosszabb ideig biztosított. A hálózati ismereteket és készségeket nem lehet úgy elsajátítani, ha folyton mindenféle zavaró tényezők hátráltatják a felkészülést.

Ugyanilyen fontos, hogy rendelkezésre álljanak a megfelelő készülékek és erőforrások. Gondoskodni kell róla, hogy elérhető legyen egy számítógép on-line tananyag hozzáféréssel és a Packet Tracer alkalmazással. Oktatói egyeztetés után a labor használata is ajánlott, valódi eszközökön szerzett tapasztalatok elsajátítása céljából. Érdeemes utána nézni, hogy van-e a környezetben internetes labor hozzáférés.

Segíthet a család és a barátok tájékoztatása is a CCENT bizonyítvány megszerzésére irányuló elhatározásról. Támogatásuk és segítségük fontos lehet a felkészülési időszakban. Emlékeztetőkártyákkal vagy gyakorlókérdésekkel akkor is segíthetnek a felkészülésben, ha ők nem járatosak a számítógép-hálózatokban. Az is könnyebbé tehető, ha tiszteletben tartják a nyugodt felkészülési időre való igényt. Érdeemes lehet tanulócsoportokat alakítani az osztály többi, szintén a vizsgára készülő tagjával.

9.6.4 Tervkészítés

Az elhatározás, majd az ICND1 vizsgára történő felkészülés megfelelő körülményeinek megteremtése és kialakítása után, következhet a tervkészítés. A felkészülési terv tartalmazza a felkészülés tervezett menetét, az ütemezést és a szükséges erőforrások listáját.

Alapvetően kétféleképp lehet felkészülni egy vizsgára: egyénileg vagy csoportosan. Sokan előnyben részesítik a csoportos felkészülést, mert az segíthet a tananyag alaposabb feldolgozásában és a határidők betartásában.

A csoportos felkészülés szempontjából lényeges többek között, hogy minden résztvevő tisztában legyen a kapcsolattartás módjával, a találkozások időpontjaival és helyszínével. Érdeemes lehet az egyes feladatokra felelőst kijelölni a csoportból:

- Tananyagok összegyűjtése és kiosztása
- Laboridő beosztása
- Fogyóeszközök biztosítása
- Csoport előmenetelének követése
- Felmerült problémák megoldása

Az egyéni felkészülés megkönnyítheti az erőforrásokkal való gazdálkodást, ami nem jelenti azt, hogy felesleges tervet készíteni.

A heti felkészülésre szánnak időmennyiség alapján reális időpontot kell kitűzni a vizsga letételére.

A rövidebb rendelkezésre álló időszetekek használhatók az elméleti felkészülésre, az egybefüggő, hosszabb időegységek pedig a gyakorlati tevékenységekre. Roppant bosszantó, ha egy laborfeladat vagy más gyakorlati tevékenység elkezdése után nem marad elég idő a befejezésre.

A Cisco Press gondozásában megjelent "31 Days to the CCENT" (31 nap alatt CCENT vizsgát) felkészülési útmutató kiadvány segíthet az időrend összeállításában (angol nyelven elérhető csak). A könyv vizsgacélok mentén haladva emeli ki a legfontosabb tanulnivalókat. Rendre jelöli a CCNA Discovery: Otthoni és kisvállalati hálózatok és CCNA Discovery: Hálózati feladatok kis- és középvállalatoknál vagy internetszolgáltatóknál tananyag vonatkozó fejezeteit, melyek alapján fel lehet készülni.

Az ütemterv készítésének első lépéseként rögzítsük a rendelkezésre álló időszakokat a naptárba. Ezután a rendelkezésre álló időblokkok rögtön konkrét feladatokhoz rendelhetők, például "az OSI modell rétegeinek és feladatainak áttekintése" vagy "IP-hálózatok kialakításának gyakorlása". Amikor sikerült minden feladathoz időpontot rendelni, a vizsga időpontjának kitűzése következhet.

Vizsgáljuk meg a felkészüléshez rendelkezésre álló eszközöket és erőforrásokat. Az ICND1 vizsgán a jelen kurzus, és a CCNA Discovery: Otthoni és kisvállalati hálózatok kurzus során elsajátítható ismereteket és készségeket ellenőrizzük. A sikeres felkészülés előfeltétele, hozzáférés az on-line tananyaghoz, a laborgyakorlatokhoz és a Packet Tracer alkalmazáshoz.

A Cisco CCNA minősítés weboldalán rengeteg további segédanyag található (jellemzően angol nyelven). A CCNA felkészülési központ weboldala:

CCNA Prep Center

A Cisco Press gondozásában számos kiadvány jelent már meg, mely feldolgozza a CCENT vizsga tartalmát. Ezek a kiadványok megvásárolhatók (angol nyelven) a Cisco Marketplace Bookstore elektronikus könyvtárában.

Cisco Marketplace Bookstore

Következő lépés az összegyűjtött anyagok rendszerezése. A CCENT vizsgához szükséges ismeretek és képességek mennyisége túl nagy ahhoz, hogy csapongva, kapkodva át lehessen őket tekinteni és kellőképpen be lehessen őket gyakorolni. Sokkal könnyebb olyan dolgokra emlékezni, melyeket rendszerezetten sajátított el az ember.

9.6.5 Vizsgarutin megszerzése

A hálózati készségek felidézése és teljesítése vizsgaszituációban teljesen más mint otthoni vagy osztálytermi környezetben. Lényeges a vizsga lebonyolításának és formájának ismerete.

Látogatás a vizsgaközpontban

A vizsga előtt ajánlott ellátogatni a vizsgaközpontba, és kérdésekkel tapasztalatot gyűjteni a vizsga menetéről. Egyes vizsgaközpontokban minden vizsgázó külön munkakörnyezetben dolgozik, míg másokban több vizsgázó tevékenykedik ugyanabban a térben. Mindenképpen tájékozodni kell a teremben engedélyezett és méginkább a tiltott eszközökről. A Cisco weboldalán megkereshető a lakóhelyhez legközelebbi vizsgaközpont.

A vizsga menete

A képesítővizsgákat ugyanúgy on-line kell letenni, mint a Hálózati Akadémia számonkéréseit. Van azonban néhány eltérés:

- Közvélemény-kutató kérdések előzhetik meg a tényleges vizsga megkezdését. Fontos az őszinte válasz. A közvélemény-kutató kérdések nincsenek kapcsolatban a tényleges vizsgával, és nem befolyásolják annak eredményét.
- A vizsga időre megy. A hátralevő idő a képernyő felső részén látható, így eldönthető, hogy egy-egy kérdésre mennyi idő számítható.
- A vizsgán belül sokféle kérdés és feladat fordulhat elő.
- Tovább lépés után már nem lehet a korábbi kérdésekre visszatérni.

Nincs mód egy kérdés kihagyására, vagy megjelölésére későbbi ellenőrzés céljából. Bizonytalanság esetén legjobb tippelni, és tovább lépni a következő kérdésre.

A Cisco vizsgaformák az alábbi kérdéstípusokat tartalmazzák:

- feleletválasztós kérdés, egy jó válasszal
- feleletválasztós kérdés, több jó válasszal
- fogd és vidd feladat
- üres mezők kitöltése
- kérdéscsoport
- szimulációs egység
- szimuláció

A vizsga előtt mindenképpen ajánlott megismerkedni az egyes feladatfajták működésével, különösen a kérdéscsoport (testlet), szimulációs egység (simlet) és a szimuláció (simulation tool) megismerése izgalmas. Ez a gyakorlat segíthet a vizsgán a tényleges feladatra összpontosítani a feladatfajta működése helyett. A Cisco CCNA felkészülési weboldalon található vizsgafelkészítő eszközök segítséget nyújtanak a gyakorlásban, és az összes feladatfajta megoldásáról szerzett pontos ismeretek kialakításában.

Bár semmi sem helyettesítheti igazán a tényleges vizsgarutint, mégis érdemes megoldani a gyakorlóvizsgát. A CCNA felkészülési weboldalon található feladatválasztós kérdéseket tartalmazó minta-feladatsorok is az ICND1 vizsgához. A csoportos felkészülés során gyakorlókérdések önálló kidolgozása is célszerű, melyek megoszthatók a csoporttársakkal. Az interneten kereskedelmi forgalomban levő vizsgakérdéssorok is megvásárolhatók vagy letölthetők.

A Cisco képesítővizsgák mindig tartalmaznak forgalomirányítók és kapcsolók működését szimuláló feladatokat is. Érdemes lehet újra végigcsinálni a laborgyakorlatokat és a Packet Tracer feladatokat a felkészülés során. A képesítővizsga összetett feladataira roppant nehéz pusztán a tananyagot olvasgatva és a laborokat kipróbálva felkészülni. Fontos próbálgatni, hogy mi történne, ha hiba lépne fel az adott eszköz telepítése vagy konfigurálása során. Sokat lehet tanulni szándékosan előidézett hibákból, melyek során megfigyelhetők az eszköz működésében és a parancsok kimenetében megjelenő változások. Az ICND1 vizsga esetleíráson alapuló feladatai túlnyomó többségben hálózati hibaelhárítási feladatok.

9.7 A fejezet összefoglalása

- Mind az OSI, mind a TCP/IP modell egyes rétegei jól meghatározott feladatokat látnak el adott protokollokkal. A hibaelhárítás során nagyban megkönnyíti a szakember munkáját, ha tisztában van az egyes rétegek feladataival, jellemzőivel, az azokhoz tartozó eszközökkel, valamint az adott réteg többi réteghez való viszonyával.
- Az OSI modell felsőbb (5-7) rétegei jellemzően speciális alkalmazási funkciót látnak el, többnyire szoftveresen vannak megvalósítva. Az alacsonyabb rétegek (1-4) az adatátviteli feladatokat és a hálózat fizikai megvalósítását látják el.
- A hálózati modellekkel végzett munka során három fő hibaelhárítási megközelítést követhetünk:
 - Fentről lefelé
 - Alulról felfelé
 - Oszd meg és uralkodj

Hálózati hibafelderítést elősegítő eszközök közé tartoznak:

- Hálózati diagramok és dokumentumok
- Hálózati dokumentációs és alapszint-ellenőrző eszközök
- Hálózatkezelési rendszerek
- Ismeret bázisok
- Protokollelemzők

Szoftveres eszközökkel sokszor nem könnyű az OSI modell alsó rétegeiben jelentkező hibák felismerése. Ezekben az esetekben nagy segítségünkre lehetnek a hardveres hibaelhárító eszközök: a kábelteszter, a multiméter és a hálózat-analizátor.

- A fizikai és az adatkapcsolati réteg hardveres és szoftveres megvalósításokat is tartalmaz.
- A fizikai réteg felelős az egyik állomásról a másik állomásra küldött bitek fizikai és elektromos jellemzőinek a definiálásáért függetlenül attól, hogy vezetékes vagy vezeték nélküli átviteli közeget alkalmazunk.
- 1. rétegbeli problémák közé tartoznak:
 - Kábeltípus, hossz és csatlakozó problémák
 - Duplexitási problémák
 - Az átvitelt megszakító interferencia és zaj
 - Hardveres eszközhibák és rendszerindítási problémák
- A forgalomirányító interfészének hibája gyakran az első tünete az 1. és 2. rétegbeli kapcsolati és kábelezési hibáknak.
- Az eszközök LED kijelzői hasznos hibaelhárítási információt tartalmaznak a kapcsolódási problémák kiszűrésére.



- Az adatkapcsolati réteg (azaz a 2. réteg) határozza meg az adott közegen történő továbbításra előkészített adatok formátumát. Ebben a rétegben kerül szabályozásra a közeghozzáférés is. A 2. réteg teremti meg a kapcsolatot a hálózati réteg szoftveres megvalósítása és az 1. réteg hardveres LAN és WAN technológiái között.
- 2. réteg problémái például:
 - Beágyazási problémák
 - Ébrenléti jelek küldésének vagy vételének hiánya
 - Időzítési problémák a WAN kapcsolatoknál
- A `show version`, `show interfaces` és a `show interface brief` parancsok hibaelhárítási adatokat tartalmaznak az 1. réteg és a 2. réteg hibáinak azonosítására és szétválasztására.
- Az OSI modell 3. rétegének elsődleges feladata a hálózati címzés és a forgalomirányítás megvalósítása.
- Legtöbb esetben a rosszul megtervezett és kialakított IP-címzési rendszer, jellegzetesen az átfedő alhálózati címek okozzák a hálózat teljesítményének problémáit.
- Alhálózati átfedést okozhat a nem kellő gondossággal kialakított címzés vagy a helytelenül megadott alhálózati maszk.
- A DHCP szervertől kapott címzés mellett előfordul, hogy az állomások automatikusan kapnak egy IP-címet a 169.254.0.0 (privát)hálózathoz.
- NAT beállítási és működési problémák előidézhetik, hogy internet lapok nem elérhetők privát címzésű LAN-okból.
- A legtöbb hálózatban különböző típusú útvonalak is létezhetnek. Többek között statikus, dinamikus és alapértelmezett útvonalak kombinációi.
- A hibák forrása sokféle lehet: manuális útvonalbejegyzési hibák, irányítóprotokollok beállítási és működési hibái, valamint az OSI alsóbb rétegeinek hibái.
- A 3. réteg problémáinak feltárására elsődleges eszköz a `show ip route` parancs. A forgalomirányító irányítótáblájának útvonalai a következő forrásokból származhatnak:
 - Közvetlenül kapcsolódó hálózatok
 - Statikus útvonalak
 - Dinamikus irányítási protokollok
- Probléma lehet a RIPv2 irányító protokollal többek között:
 - A verzió megadásának elmulasztása a verziók különbözőségét okozhatja a forgalomirányítók között.
 - Hibás vagy hiányzó network parancsok.
 - Helytelenül megadott interfész IP-címek.

- A 4. réteg felelős az adatcsomagok szállításáért, valamint definiálja az egyes alkalmazások eléréséhez használatos portszámokat.
- A tűzfalak és port-szűrő szabályok, amelyek átengedik vagy tiltják a nem megfelelő portok forgalmát, megakadályozhatják egyes szolgáltatások elérését az ügyfél gépéről.
- Felsőbb rétegek szolgáltatásai közé tartoznak a DNS névfeloldás, a titkosítás és a tömörítés. Az ilyen funkciók hibái a végfelhasználó gépén futó alkalmazásokat működésképtelenné tehetik.
- A Windows nslookup parancsa segíthet a DNS hibák felderítésében.
- A hivatalos CCENT (Cisco Certified Entry Networking Technician - Cisco belépő szintű hálózati technikus) minősítés megszerzése igazolja, hogy a tulajdonosa rendelkezik a belépő szintű hálózati támogatási munkakörök ellátáshoz szükséges képességekkel. Számos sikeres karrier kiindulópontja a számítógépes hálózatok területén.
- A CCENT tanúsítvány megszerzéséhez, a jelöltnek le kell tennie az ICND1 (640-822) vizsgát. Itt megvizsgálják, hogy képes-e egy fiókroda hálózatának telepítésére, üzemeltetésére és hibaelhárítására.
- A Cisco vizsgák az alapján mérik a jelölt felkészültségét a számítógépes hálózatok tárgykörében, hogy miként tud a Cisco hálózati eszközökkel dolgozni. A feladatok egy jelentős része arra kíváncsi, hogy tudja-e a jelölt a különböző IOS parancsok, elsősorban a show parancsok kimenetét értelmezni.
- A vizsgára készülés - csakúgy mint egy ügyfél hálózatának a kialakítása - szintén hatékonyabb, ha lebontjuk kisebb feladatokra:
 1. Elhatározás
 2. Tervkészítés
 3. Vizsgarutin megszerzése

1. Az internet és használata	0
1.1 Mi az internet?	1
1.1.1 Az internet és a szabályok	1
1.1.2 ISP és ISP szolgáltatások	3
1.2 ISP-k	4
1.2.1 Az internet-szolgáltatások eljuttatása a végfelhasználókhoz	4
1.2.2 Internet hierarchia	7
1.2.3 Az internet feltérképezéséhez használható eszközök	9
1.3 ISP kapcsolat	10
1.3.1 ISP követelmények	10
1.3.2 Az ISP feladatai és kötelezettségei	12
1.4 A fejezet összefoglalása	12
2. Ügyfélszolgálat	14
2.1 Ügyfélszolgálati szakemberek	14
2.1.1 Az internetszolgáltató ügyfélszolgálati szervezete	14
2.1.2 Az ügyfélszolgálati szakemberek feladatai	15
2.1.3 Tárgyalás az ügyféllel	16
2.2 Az OSI modell	18
2.2.1 Az OSI modell használata	18
2.2.2 OSI modell protokollok és technológiák	20
2.2.3 Hibakeresés az OSI modellel	22
2.3 ISP hibaelhárítás	25
2.3.1 Ügyfélszolgálati hibaelhárítási foratókönyv	25
2.3.2 Ügyfélszolgálati feljegyzések készítése és alkalmazása	27
2.3.3 A helyszíni eljárás	28
2.4 A fejezet összefoglalása	30
3. Egy hálózat továbbfejlesztésének tervezése	31
3.1 A létező hálózat dokumentálása	31
3.1.1 A helyszín felmérése	31
3.1.2 Fizikai és logika topológiák	33
3.1.3 Hálózati követelmények dokumentálása	35
3.2 Tervezés	36
3.2.1 Hálózati korszerűsítés tervezési fázisai	36
3.2.2 Fizikai környezet	38

3.2.3 Kábelezési megfontolások.....	39
3.2.4 Strukturált kábelezés.....	40
3.3 Eszközök beszerzése és karbantartása.....	41
3.3.1 Eszközök beszerzése.....	41
3.3.2 Hálózati eszközök kiválasztása.....	43
3.3.3 LAN eszközök kiválasztása.....	44
3.3.4 Hálózati eszközök kiválasztása.....	45
3.3.6 Hálózati berendezések fejlesztése.....	47
3.3.6 Tervezési megfontolások.....	48
3.4 A fejezet összefoglalása.....	50
4. A címezési struktúra tervezése.....	51
4.1 IP-címzés LAN-okba.....	51
4.1.1 IP-címek áttekintése.....	51
4.1.2 Alhálózatok a hálózatban.....	54
4.1.3 Egyedi alhálózati maszkok.....	58
4.1.4 VLSM és osztályok nélküli tartományközi forgalomirányítás (CIDR).....	60
4.1.5 Az alhálózatok közötti kommunikáció.....	61
4.2 NAT és PAT.....	62
4.2.1 A hálózati címfordítás alapjai (NAT).....	62
4.2.2 IP NAT alapfogalmak.....	63
4.2.3 Statikus és dinamikus NAT.....	64
4.2.4 Port alapú hálózati címfordítás (PAT).....	65
4.2.5 További IP NAT kérdések.....	67
4.3 A fejezet összefoglalása.....	69
5. Hálózati eszközök konfigurálása.....	71
5.1 Az ISR forgalomirányító első konfigurálása.....	71
5.1.1 ISR.....	71
5.1.2 Az ISR üzembehelyezése.....	75
5.1.3 Az indítási folyamat.....	78
5.1.4 A Cisco IOS segédprogramok.....	82
5.2 A Cisco SDM Express és az SDM használata.....	84
5.2.1 A Cisco SMD Express.....	84
5.2.2 Az SDM Express beállítási lehetőségei.....	85
5.2.3 A WAN kapcsolatok beállítása az SDM Express használatával.....	87

5.2.4 A NAT beállítása a Cisco SDM használatával	89
5.3 A forgalomirányító IOS parancssori (CLI) konfigurálása	91
5.3.1 A parancssoros felület üzemmódjai	91
5.3.2 A Cisco IOS parancssoros felületének használata	93
5.3.3 A Show parancsok használata	96
5.3.4 Az alapkonfiguráció	96
5.3.5 Az interfészek beállítása	99
5.3.6 Az alapértelmezett útvonal beállítása	101
5.3.7 A DHCP-szolgáltatás beállítása	102
5.3.8 Statikus NAT beállítása a Cisco IOS parancssoros felületén	104
5.3.9 A Cisco forgalomirányítók konfigurációjának biztonsági mentése	107
5.4 A CPE csatlakoztatása az ISP-hez	111
5.4.1 A CPE telepítése	111
5.4.2 WAN-on keresztüli előfizetői kapcsolatok	113
5.4.3 A WAN-összeköttetés kiválasztása	115
5.4.4 A WAN-összeköttetés beállítása	117
5.5 A Cisco 2960 kapcsoló első konfigurálása	118
5.5.1 Önálló kapcsolók	118
5.5.2 A Cisco 2960 típusú kapcsoló üzembehelyezése	122
5.5.3 A kapcsoló kezdeti konfigurációja	124
5.5.4 A LAN kapcsoló összekötése a forgalomirányítóval	126
5.5.5 A Cisco Discovery Protocol	129
5.6 A fejezet összefoglalása	132
6. Forgalomirányítás	134
6.1 Az irányító protokollok konfigurálása	134
6.1.1 A forgalomirányítás alapjai	134
6.1.2 Forgalomirányító protokollok	138
6.1.3 A leggyakoribb belső forgalomirányító protokollok	140
6.1.4 Szervezeten belüli forgalomirányítás	144
6.1.5 A RIP konfigurálása és ellenőrzése	147
6.2 Külső forgalomirányító rendszerek	151
6.2.1 Autonóm rendszerek	151
6.2.2 Interneten keresztüli forgalomirányítás	152
6.2.3 Külső forgalomirányító protokollok és az ISP	154

6.2.4 BGP konfigurálása és ellenőrzése.....	155
6.3 A fejezet összefoglalása.....	156
7. ISP szolgáltatások	158
7.1 Az ISP szolgáltatások bevezetése	158
7.1.1 Felhasználói követelmények	158
7.1.2 Megbízhatóság és elérhetőség.....	159
7.2 Az ISP szolgáltatásokat támogató protokollok.....	161
7.2.1 A TCP/IP protokollkészlet áttekintése	161
7.2.2 Szállítás réteg protokollok.....	163
7.2.3 Különbségek a TCP és UDP között.....	165
7.2.4 Több szolgáltatás támogatása.....	166
7.3 Tartománynév rendszer (DNS)	167
7.3.1 TCP/IP állomás név	167
7.3.2 DNS hierarchia.....	169
7.3.3 DNS névfeloldás.....	171
7.3.4 DNS implementálása	176
7.4 Szolgáltatások és protokollok.....	178
7.4.1 Szolgáltatások.....	178
7.4.2 HTTP és HTTPS.....	178
7.4.3 FTP	180
7.4.4 SMTP, POP3 és IMAP4.....	182
7.5 A fejezet összefoglalása.....	184
8. ISP felelősség	186
8.1 ISP biztonsági megfontolások.....	186
8.1.1 ISP biztonsági szolgáltatások	186
8.1.2 Biztonsági intézkedések	188
8.1.3 Adattitkosítás.....	189
8.2 Biztonsági eszközök	191
8.2.1 Hozzáférési listák és portszűrés	191
8.2.2 Tűzfalak.....	193
8.2.3 IDS és IPS	195
8.2.4 Vezeték nélküli hálózatok biztonsága	196
8.2.5 A munkaállomások biztonsága.....	197
8.3 Az ISP megfigyelése és felügyelete.....	201

8.3.1 Szolgáltatói szerződés.....	201
8.3.2 A hálózati összeköttetések teljesítményének megfigyelése	202
8.3.3 Eszközfelügyelet sávon belüli eszközökkel	202
8.3.4 SNMP és Syslog használata.....	203
8.4 Biztonsági mentések és katasztrófhelyzet helyreállítás	205
8.4.1 Archiválási hordozók	205
8.4.2 Az állománymentés módszerei.....	207
8.4.3 Cisco IOS mentése és helyreállítása	209
8.4.4 Katastrófa-helyreállítási terv	211
8.5 A fejezet összefoglalása.....	214
9. Hibaelhárítás.....	216
9.1 Hibaelhárítási módszerek és eszközök	216
9.1.2 Hibaelhárítási módszerek	217
9.1.3 Hibaelhárítási eszközök	218
9.2. 1. és 2. rétegbeli problémák hibaelhárítása	223
9.2.2 Hardware-s eszközhibák és rendszerindítási problémák hibaelhárítása	225
9.2.3 Kábelezési és interfészproblémák hibaelhárítása	228
9.2.4 LAN kapcsolati hibák elhárítása.....	229
9.2.5 WAN kapcsolati hibák elhárítása.....	231
9.3 3. rétegbeli működés és IP-címzés - ismételés.....	235
9.3.2 IP-címtér megtervezésének és beállításának kérdései.....	238
9.3.2 IP-címtér megtervezésének és kiosztásának kérdései	242
9.3.4 DHCP és NAT problémák	242
9.4 3. rétegbeli irányítási problémák	247
9.4.2 A dinamikus forgalomirányítás hibái.....	250
9.5 A 4. és a felsőbb rétegek hibaelhárítása	252
9.5.1 4. rétegbeli forgalomszűrési hibák	252
9.5.2 Felsőbb rétegek hibáinak elhárítása.....	252
9.5.3 Felsőbb rétegbeli kapcsolat ellenőrzése Telnettel	256
9.6 Felkészülés a Cisco képzés megszerzésére.....	257
9.6.1 Tudás, készség és képesség.....	257
9.6.1 Hálózati tudás, készség és képesség	258
9.6.3 Elhatározás	260
9.6.4 Tervkészítés	261



9.6.5 Vizsgarutin megszerzése	262
9.7 A fejezet összefoglalása.....	264



