Cisco CCNA Discovery

4.0

Számítógép-hálózatok tervezése és támogatása

(4. szemeszter)

edited by Nono – 2012

Figyelem! A jegyzet csak a tananyag szöveges részeit tartalmazza. A teljes tananyaghoz olvasd el az interaktív anyagot is! (videók, mellékletek stb.)

1. Bevezetés a hálózattervezési koncepciókba

1.1 A hálózattervezés alapjainak feltárása

1.1.1 A hálózattervezés áttekintése

A nagy- és a kisvállalatok szempontjából egyaránt kulcsfontosságú a megfelelő számítógépes és információs hálózat, amely biztosítja az emberek közötti összeköttetést, támogatja az alkalmazásokat és a szolgáltatásokat, valamint biztosítja az üzletvitelhez szükséges erőforrások elérését. A vállalatok napi igényeit csak az egyre összetettebbé váló hálózatok képesek kielégíteni.

Hálózati igények

Napjainkban az internet-alapú gazdaság gyakran megköveteli az ügyfelek számára nyújtott szolgáltatások biztosítását a nap 24 órájában, ami azt jelenti, hogy a vállalati hálózatoknak csaknem az idő 100%-ában rendelkezésre kell állniuk. Kellő intelligenciával kell rendelkezniük, hogy automatikus védelmet nyújtsanak a váratlan biztonsági problémákkal szemben, valamint a változó forgalmi terhelés esetén is biztosítsák az alkalmazások közel állandó válaszidejét. Gondos tervezés és előkészítés nélkül, csupán sok-sok számítógép összekapcsolásával létrehozott hálózat ma már nem nyújt megfelelő megoldást.

A jó hálózat létrehozása

A jó hálózat nem magától jön létre, hanem olyan hálózattervezők és technikusok kemény munkájának eredménye, akik a hálózati igények meghatározását követően választják ki a vállalat szükségleteinek leginkább megfelelő megoldásokat.

1. lépés: A pénzügyi és a műszaki feltételek ellenőrzése
2. lépés: Az 1. lépésben meghatározott feltételekhez szükséges szolgáltatások és funkciók meghatározása
3. lépés: A hálózat készenlétének felmérése
4. lépés: A megoldás és a helyszínen történő átvételi vizsgálat megtervezése
5. lépés: A projektterv elkészítése

A hálózati felhasználók általában nem gondolnak a háttérben működő hálózat összetettségére. A hálózatot olyan dolognak tekintik, amely hozzáférést biztosít bármely időben a számukra szükséges alkalmazásokhoz.

Hálózati igények

A legtöbb vállalat csupán néhány követelményt támaszt a hálózatával szemben:

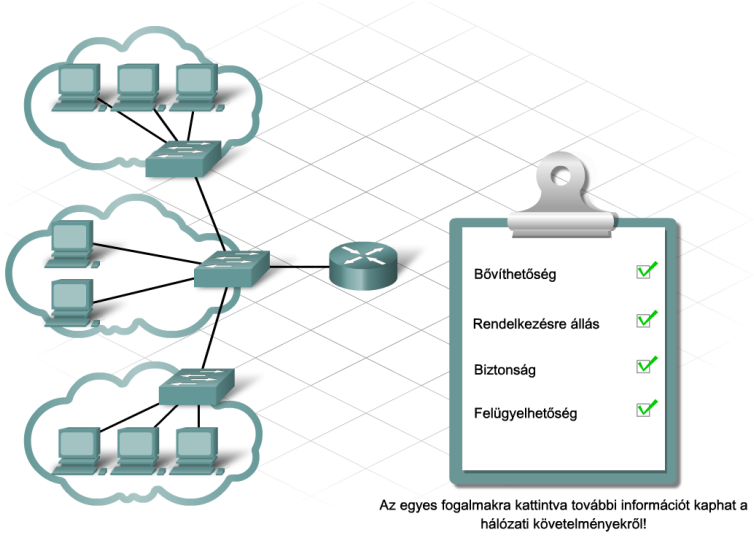
- A hálózat – még meghibásodott összeköttetések és berendezések, valamint túlterhelés esetén is – folyamatosan üzemeljen.
- A hálózaton megbízhatóan fussanak az alkalmazások, és elfogadható legyen a válaszidő bármely két állomás között.

- A hálózat legyen biztonságos. Védje a rajta áthaladó adatokat, csakúgy, mint a hozzá csatlakoztatott eszközökön tárolt adatokat.
- A hálózat legyen könnyen módosítható, ha a hálózat növekedése vagy az üzleti jellegű változások ezt kívánják.
- Mivel meghibásodások időnként előfordulnak, a hibaelhárítás legyen könnyű. A problémák megtalálása és kijavítása ne vegyen igénybe túl sok időt!

Alapvető tervezési célkitűzések

Ha jobban szemügyre vesszük, a fenti követelmények az alábbi négy alapvető hálózattervezési célkitűzésnek feleltethetők meg:

- bővíthetőség
- rendelkezésre állás
- biztonság
- felügyelhetőség



Bővíthetőség: A bővíthető hálózati tervben nem okoz gondot új felhasználói csoportok és távoli telephelyek hozzáadása, valamint oly módon támogatja az új alkalmazásokat, hogy eközben nem befolyásolja a meglévő felhasználók szolgáltatási szintjét.

Rendelkezésre állás: A nagy rendelkezésre állásúra tervezett hálózat következetes, megbízható teljesítményt nyújt a nap 24 órájában, a hét minden napján. Ezen felül egyetlen összeköttetés vagy berendezés meghibásodása sem befolyásolhatja számottevően a hálózat teljesítményét.

Biztonság: A biztonsági funkciókat bele kell tervezni a hálózatba, nem pedig a kész hálózathoz utólagosan hozzáadni azokat. A biztonsági eszközök, szűrők és tűzfal funkciók helyének megtervezése kulcsfontosságú a hálózati erőforrások védelméhez.

Felügyelhetőség: Nem számít, hogy a kiinduló hálózati terv mennyire jó, a rendelkezésre álló hálózati személyzetnek képesnek kell lennie a hálózat karbantartására és támogatására. A túlságosan bonyolult vagy nehezen felügyelhető hálózat nem képes eredményesen és hatékonyan működni.

1.1.2 A hierarchikus hálózattervezés előnyei

A négy alapvető tervezési célkitűzés megvalósításához a hálózatnak olyan architektúrára kell épülnie, amely a rugalmasságot és a növekedést egyaránt lehetővé teszi.

A hierarchikus hálózattervezés

Hálózatépítés során a hierarchikus tervezés segítségével az eszközök több, különböző hálózatba sorolhatók. A hálózatok egymásra épülő rétegekre tagolódnak. A hierarchikus tervezési modell három alapréteget különböztet meg:

- **Központi réteg** – összeköttetést biztosít az elosztási rétegbeli eszközök között
- **Elosztási réteg** – összeköttetést biztosít a kisebb, helyi hálózatok között
- **Elérési réteg** – összeköttetést biztosít a hálózati állomások és a végberendezések számára

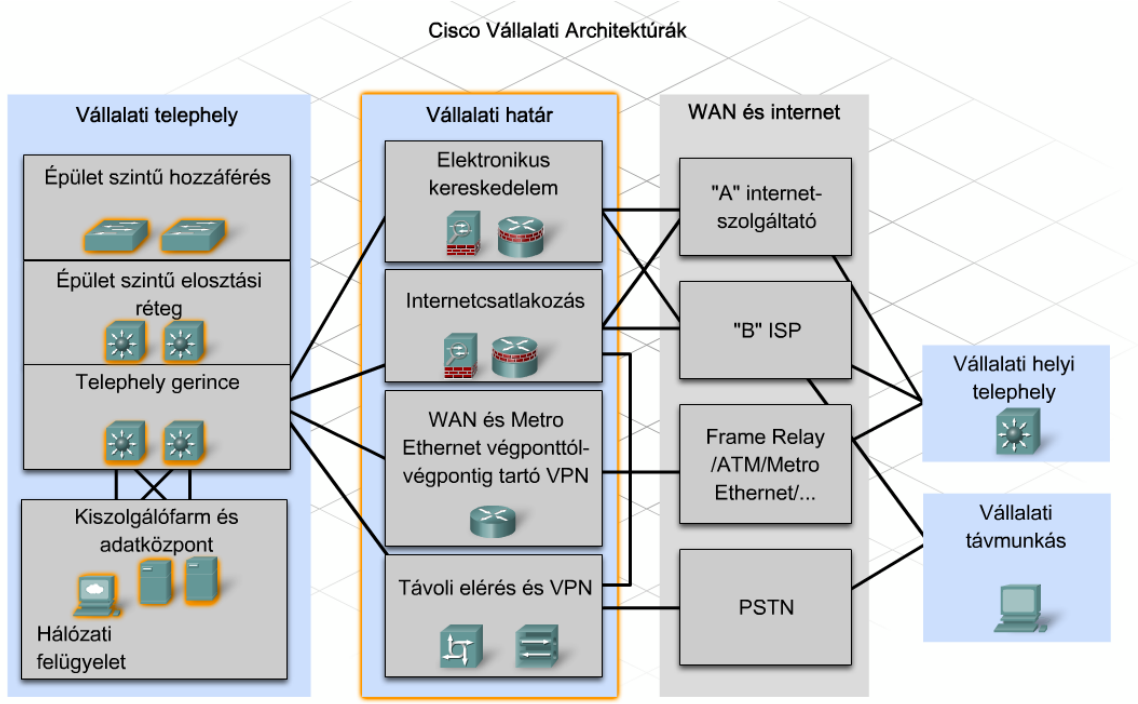
Az egyszintű hálózatokkal szembeni előnyök

A hierarchikus hálózatok számos előnnyel rendelkeznek az egyszintű hálózattervezéssel szemben. Ha egy egyszintű hálózatot kisebb, jobban felügyelhető egységekre tagolunk, a helyi forgalom helyi marad, kizárólag a más hálózatokba irányuló forgalom kerül a magasabb rétegekbe.

Az egyszintű hálózatokban a második rétegbeli eszközök kevés lehetőséget kínálnak a szórások korlátozására vagy a nem kívánt forgalom szűrésére. Ahogy egyre több eszköz és alkalmazás válik az egyszintű hálózat részévé, a válaszidő egyre romlik, mígnem a hálózat használhatatlanná válik.

A Cisco nagyvállalati architektúra (Cisco Enterprise Architecture) használatával a három rétegből álló hierarchikus terv további moduláris részekre tagolható, ahol az egyes modulok eltérő fizikai vagy logikai összeköttetéssel rendelkező területeknek felelnek meg. Ezek a modulok egyúttal a hálózatban elérhető különféle funkciókat is kijelölik. A modularitás biztosítja a hálózati terv rugalmasságát, valamint elősegíti a megvalósítás és a hibaelhárítás folyamatát. A moduláris hálózati terv fókuszában az alábbi három terület áll:

- **Vállalati telephely** – Ez a terület tartalmazza az egy telephelyen vagy fiókirodán belüli független működéshez szükséges hálózati elemeket.
- **Kiszolgálófarm** – A vállalati telephely összetevőjeként az adatközpont kiszolgálófarmja védelmet nyújt a kiszolgálók erőforrásai számára, valamint redundáns, megbízható és nagysebességű összeköttetést biztosít.
- **Vállalati határ** – Ahogy a forgalom a telephely hálózatára érkezik, ezen a területen zajlik a külső forrásokból származó forgalom szűrése és a forgalomirányítás a vállalati hálózat irányába. Tartalmazza a vállalati telephely, valamint a távoli telephelyek, felhasználók és az internet közötti hatékony és biztonságos kommunikációhoz szükséges összes elemet.



Épület szintű hozzáférés: Ez a hozzáférési réteg 2. rétegbeli vagy 3. rétegbeli kapcsolókkal valósítja meg a szükséges portsűrűséget. Itt kerülnek megvalósításra a VLAN-ok és az épület elosztási rétege felé vezető trönkvonalak. Az épület elosztási régegében elhelyezett kapcsolók fontos jellemzője a redundancia.

Épület szintű elosztási réteg: Ez az elosztási rétegbeli modul 3. rétegbeli eszközökkel valósítja meg az épület szintű hozzáférést. Ebben a rétegben kerül megvalósításra a forgalomirányítás, a hozzáférés-vezérlés és a szolgáltatásminőség (QoS). A redundancia elengedhetetlen ebben a rétegben is.

Telephely gerince: Ez a gerincrétegbeli modul nagy sebességű kapcsolatot biztosít az elosztási réteg modulja, az adatközpont kiszolgálófarmja és a vállalati határ között. Ebben a rétegben a redundancia, a gyors konvergencia és a hibatűrés áll a tervezés középpontjában.

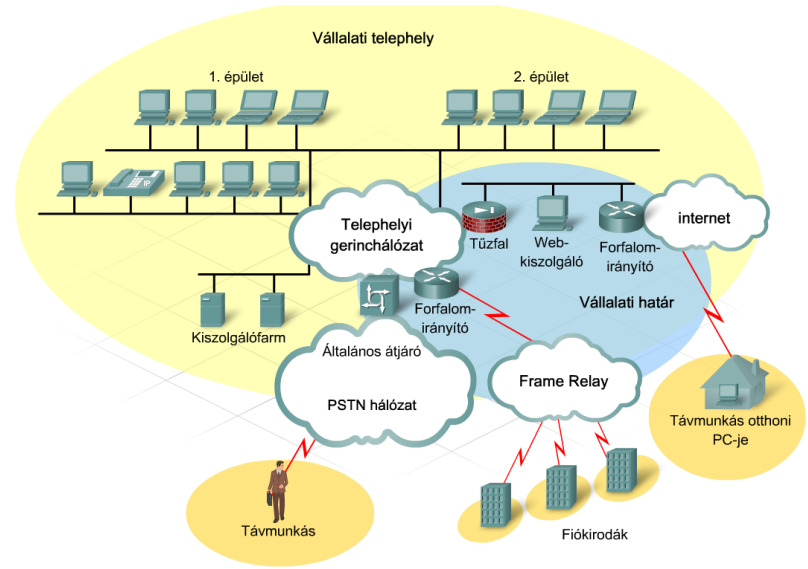
Felügyelet: Ez a fontos terület felügyeli a teljesítményt azáltal, hogy monitorozza az eszközöket és a hálózat elérhetőségét.

Kiszolgálófarm: Ez a modul biztosítja a gyors kapcsolatot és a védelmet a kiszolgálóknak. Ezen területen a biztonság, a redundancia és a hibatűrés a legfontosabbak.

Vállalati határ: Ez a modul terjeszti ki a vállalati szolgáltatásokat a távoli webhelyek felé, és teszi lehetővé, hogy a vállaltat elérje az internetet és a partnerek szolgáltatásait. Ez a modul biztosítja a szolgáltatásminőséget (QoS), a hálózati szabályok betartását, a szolgáltatási szinteket és a biztonságot.

A Cisco nagyvállalati architektúra moduláris keretrendszere az alábbi tervezési előnyöket nyújtja:

- Olyan determinisztikus hálózatot hoz létre, amely egyértelmű határokat definiál az egyes modulok között. Az így létrejövő egyértelmű határpontok segítségével a hálózat tervezője mindig pontosan tudja, hogy a forgalom honnan származik és merre halad.
- Azzal, hogy az egyes modulokat egymástól függetlenné teszi, a tervezés folyamata is könnyebbé válik, mivel a tervező külön-külön tud foglalkozni az egyes területek igényeivel.
- Ahogy a hálózat egyre összetettebbé válik, a tervező új funkciókat ellátó modulokkal bővítheti azt. A keretrendszer a vállalat számára a modulok egyszerű hozzáadásával biztosítja a bővíthetőséget.
- A háttérben működő hálózat megváltoztatása nélkül lehetséges új szolgáltatások és megoldások hozzáadása.



1.1.3 Hálózattervezési módszerek

A nagyméretű hálózatok tervezési munkái normál esetben három különálló lépésre tagolhatók:

1. lépés: A hálózati igények meghatározása

2. lépés: A meglévő hálózat feltérképezése

3. lépés: A hálózati topológia és a megoldások megtervezése

A hálózati igények meghatározása

A hálózattervező az ügyféllel szorosan együttműködve dokumentálja a projekt célkitűzéseit. A célok általában két kategóriába sorolhatók:

- Üzleti célok – Itt a fókusz arra helyeződik, hogy a hálózat miként teheti a vállalatot még sikeresebbé.
- Technikai követelmények – Itt a fókuszban az áll, hogy a technológia miként alkalmazható a hálózatban.

A meglévő hálózat feltérképezése

Ebben a lépésben történik a jelenleg meglévő hálózattal és szolgáltatásokkal kapcsolatos információk összegyűjtése és elemzése. Szükség van a meglévő hálózat funkcionalitásának és az új projektben rögzített célkitűzések összevetésére. A tervező határozza meg, hogy bármely berendezés, infrastruktúra vagy protokoll továbbra is hasznosítható-e, valamint azt, hogy milyen új berendezések és protokollok szükségesek a terv megvalósításához.

A hálózati topológia megtervezése

Az egyik közkedvelt hálózattervezési stratégia a fentről lefelé haladó megközelítés, melyben először a hálózati alkalmazások és szolgáltatások körét határozzuk meg, majd a hálózatot ennek megfelelően tervezzük meg.

Amikor egy terv elkészül, a fentről lefelé haladó módszer segítségével egy prototípus létrehozása vagy egy alapos vizsgálat szükséges. Ezzel már a tényleges megvalósítást megelőzően tesztelhető, hogy az új tervben szereplő funkciók az elvárásoknak megfelelően működnek-e.

A hálózattervezők által elkövetett gyakori hiba, hogy rosszul mérik fel a hálózattervezési projekt méretét.

A projekt méretének meghatározása

Az igények összegyűjtése során a tervező meghatározza az egész hálózatot érintő, valamint annak csak egy-egy részével kapcsolatos kérdéseket. Annak, hogy egy projekt volumene meghaladja az eredeti becsléseket gyakran az az oka, hogy egy konkrét igény hatásait nem jól mérte fel a tervező. Egy ilyen tévedés nagymértékben megnövelheti az új terv megvalósításának költségét és idejét.

A hálózat egészét érintő kérdések

Az egész hálózatot érintő hálózati igények között szerepel:

- Új hálózati alkalmazások hozzáadása, valamint a meglévő alkalmazások nagymértékű módosítása. Ilyen változás lehet például az adatbázis- és DNS-szerkezet módosítása.
- A hálózati címzés hatékonyságának növelése és az irányítóprotokoll megváltoztatása.
- Új biztonsági intézkedések bevezetése.
- Új hálózati szolgáltatások (pl. hangátvitel, tartalomszolgáltató hálózat vagy tárolóhálózat) hozzáadása.
- Kiszolgálók áthelyezése az adatközpont kiszolgálófarmjába.

A hálózatnak csak egy részét érintő kérdések

A hálózatnak csupán egy részét érintő igények között szerepel:

- Az internetkapcsolat javítása és a sávszélesség bővítése.
- Az elérési réteg LAN kábelezésének korszerűsítése.
- Redundancia biztosítása a kulcsfontosságú szolgáltatásokhoz.
- Vezetéknélküli hozzáférés biztosítása a kijelölt területeken.
- A WAN sávszélességének bővítése.

A fenti igények nem feltétlenül érintenek sok felhasználót vagy igényelnek túl sok változtatást a már üzemelő berendezésekben. Előfordulhat, hogy a meglévő hálózaton tervezett változtatások egyáltalán nem zavarják a normál hálózati működést a felhasználók döntő többségénél. Ez a módszer csökkenti a leállással járó költségeket, valamint felgyorsítja a hálózati bővítés megvalósítását.

1.2 A mag réteg (Core Layer) tervezési koncepcióinak feltárása

1.2.1 Mi történik a központi rétegben?

A központi réteget gerinchálózatnak is nevezzük. A központi réteghez tartozó forgalomirányítók és kapcsolók nagysebességű összeköttetést biztosítanak. A vállalati LAN-okban a központi réteg biztosítja az összeköttetést több épület és telephely között, valamint a kiszolgálófarm irányába. A központi réteg részét képezi egy vagy több olyan kapcsolat a vállalati határ eszközeivel, melyek az internethez, a virtuális magánhálózatokhoz (VPN-ekhez), az extranet-ekhez és a WAN-hoz történő hozzáférést biztosítják.

A központi réteg alkalmazása csökkenti a hálózat komplexitását, könnyebbé teszi a felügyeletet és a hibaelhárítást.

A központi réteg céljai

A központi réteg lehetővé teszi a hálózat két szegmense közötti hatékony, nagysebességű adatáramlást. A központi réteg elsődleges tervezési céljai az alábbiak:

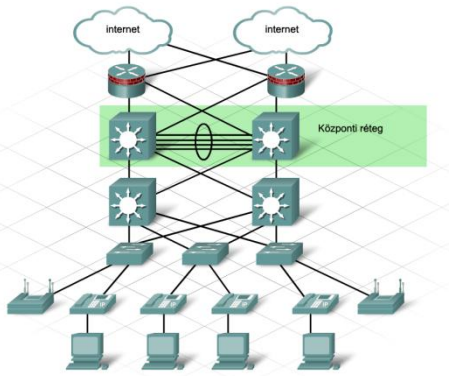
- 100%-os rendelkezésre állás biztosítása
- Az átviteli teljesítmény maximalizálása
- A hálózat növekedésének elősegítése

A központi réteg technológiái

A központi rétegben alkalmazott technológiák között szerepelnek az alábbiak:

- Forgalomirányítók vagy olyan többrétegű kapcsolók, amelyek egy eszközben valósítják meg a forgalomirányítást és a kapcsolást.
- Redundancia és terheléselosztás.
- Nagysebességű és összevont kapcsolatok.

- Olyan jól méretezhető és gyorsan konvergáló irányítóprotokollok, mint például az EIGRP (Enhanced Interior Gateway Routing Protocol, továbbfejlesztett belső átjáró irányító protokoll) és az OSPF (Open Shortest Path First, legrövidebb út) protokoll.

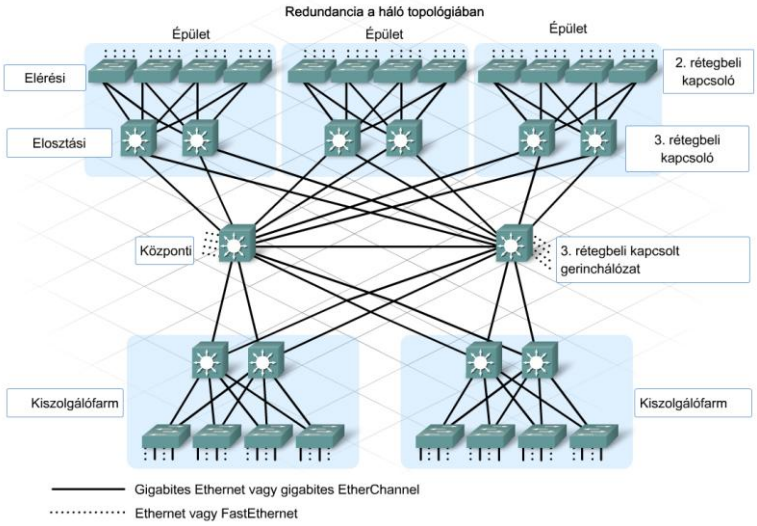


Redundáns összeköttetések

A redundáns összeköttetések alkalmazása a központi rétegben lehetővé teszi, hogy hiba esetén a hálózati eszközök alternatív útvonalat találjanak az adatküldéshez. Amennyiben 3. rétegbeli eszközök kerülnek a központi rétegbe, a redundáns összeköttetések terheléselosztásra is használhatók a tartalékútvonal funkció biztosítása mellett. Az egyszintű, csak a 2. rétegre korlátozódó hálózati tervben az STP (Spanning Tree Protocol, feszítőfa protokoll) egészen addig letiltja a redundáns összeköttetéseket, amíg egy elsődleges kapcsolat meg nem hibásodik. Az STP ilyen viselkedése nem teszi lehetővé a terheléselosztást a redundáns összeköttetéseken.

A háló topológia

A legtöbb hálózat központi rétege teljes háló vagy részleges háló topológia szerint van kábelezve. Teljes háló topológia esetében minden eszköz össze van kötve az összes többivel. Habár a teljes háló topológia egy teljesen redundáns hálózat előnyeit kínálja, kábelezésük és felügyeletük nehézkes, és általában sokba kerül. Nagyobb telepítések esetében egy módosított részleges háló topológiát használnak. Részleges háló topológia esetében minden eszköz legalább két másikkal van összekötve, így elegendő redundanciát biztosít a teljes háló túlzott összetettsége nélkül.



1.2.2 Prioritások a hálózati forgalomban

A meghibásodások elkerülése

A hálózattervezőnek törekednie kell arra, hogy hálózat ellenálló legyen a meghibásodásokkal szemben, és egy esetleges meghibásodás esetén gyorsan helyreálljon a normál működés. A központi forgalomirányítók és kapcsolók tartalmazhatnak:

- kettős tápellátást és hűtést
- moduláris kialakítású készülékházat
- további felügyeleti modulokat

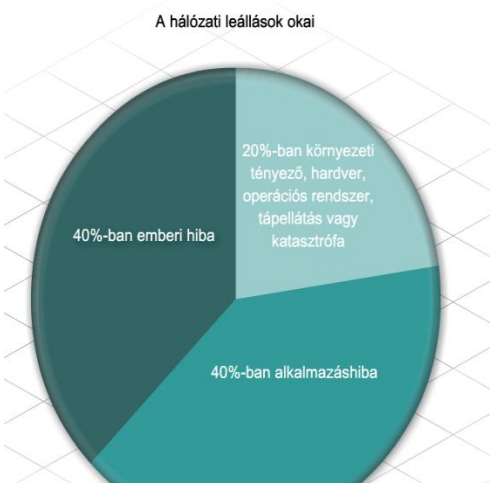
A redundáns összetevők növelik a költségeket, de általában megérik a befektetést. A központi rétegbeli eszközöknek lehetőség szerint üzem közben cserélhető (hot-swappable) összetevőkkel kell rendelkezniük. Az üzem közben cserélhető összetevők az eszköz áramtalanítása nélkül telepíthetők vagy távolíthatók el. Az ilyen összetevők használta csökkenti a javítási időt és a hálózati szolgáltatásokban bekövetkező zavart.

A nagyvállalatok gyakran alkalmaznak generátorokat és nagy teljesítményű szünetmentes tápegységeket (UPS), amelyek jelentős hálózati meghibásodásokat akadályoznak meg a kisebb áramkimaradások esetén.

Az emberi hibalehetőség csökkentése

A hálózati meghibásodásokhoz emberi hibák is hozzájárulnak. Sajnos, a redundáns összeköttetések és berendezések alkalmazása nem küszöböli ki ezt a problémát. Számos hálózati hiba oka az új berendezések nem kellő alapossággal megtervezett, tesztelés nélküli hozzáadása és frissítése. Laboratóriumi környezetben történő előzetes tesztelés nélkül soha ne végezzünk módosításokat egy működő hálózat konfigurációjában!

A központi réteg meghibásodásai széleskörű leállásokhoz vezethetnek, ezért kulcsfontosságú, hogy előzetesen elkészüljenek a változtatások jóváhagyásának, tesztelésének, telepítésének és dokumentálásának miként jét rögzítő írásos irányelvek és cselekvéstervek. Mindig legyen egy visszalépési stratégiánk, amellyel a sikertelen változtatások esetén a hálózat az előző állapotba visszaállítható!



1.2.3 A hálózati konvergencia

A központi réteg irányítóprotokolljának kiválasztása a hálózat méretétől, valamint a rendelkezésre álló redundáns összeköttetésektől és útvonalaktól függ. A protokoll kiválasztásának egyik fő szempontja, hogy kapcsolat- vagy eszközhiba esetén mennyi idő alatt képes a helyreállításra.

Konvergencia

Egy hálózat akkor van konvergált állapotban, ha az összes forgalomirányító teljes és pontos információval rendelkezik a hálózatról. Minél kisebb a konvergenciaidő, a hálózat annál gyorsabban tud reagálni a topológiában bekövetkezett változásokra. A konvergenciához szükséges időt befolyásoló tényezők között szerepel:

- Az a sebesség, amellyel az útvonalfrissítések elérik a hálózat összes forgalomirányítóját.
- Az egyes forgalomirányítók által a legjobb útvonal meghatározásához elvégzett számítások ideje.

Az irányítóprotokoll kiválasztása

A legtöbb dinamikus irányítóprotokoll elfogadható konvergenciaidőt kínál a kisebb hálózatokban. A nagyobb hálózatokban a RIPv2-höz hasonló protokollok túlságosan lassan konvergálnak egy összeköttetés meghibásodása esetén, így nem tudják megakadályozni a hálózati szolgáltatásokban bekövetkező zavart. Általánosságban elmondható, hogy a nagyobb hálózatok esetében az EIGRP és az OSPF nyújtja a legstabilabb forgalomirányítási megoldást.

Tervezési szempontok

A legtöbb hálózat dinamikus és statikus útvonalak kombinációját használja. A hálózattervezőnek mérlegelnie kell, hogy mennyi útvonal szükséges annak biztosításához, hogy az összes célhálózat elérhető legyen. A nagyméretű irányítótáblák jelentősen megnövelik a konvergenciához szükséges időt. A hálózati címkiosztás tervezése és a különböző szinteken történő címösszevonási stratégiák befolyásolják, hogy az irányítóprotokoll mennyire jól reagál egy esetleges meghibásodásra.

1.3 Az elosztási réteg (Distibution Layer) tervezési koncepcióinak feltárása

1.3.1 Mi történik az elosztási rétegben?

Az elosztási réteg irányítási határt képez a hozzáférési és a központi réteg között, ugyanakkor kapcsolódási pontként is szolgál a távoli telephelyek és a központi réteg között.

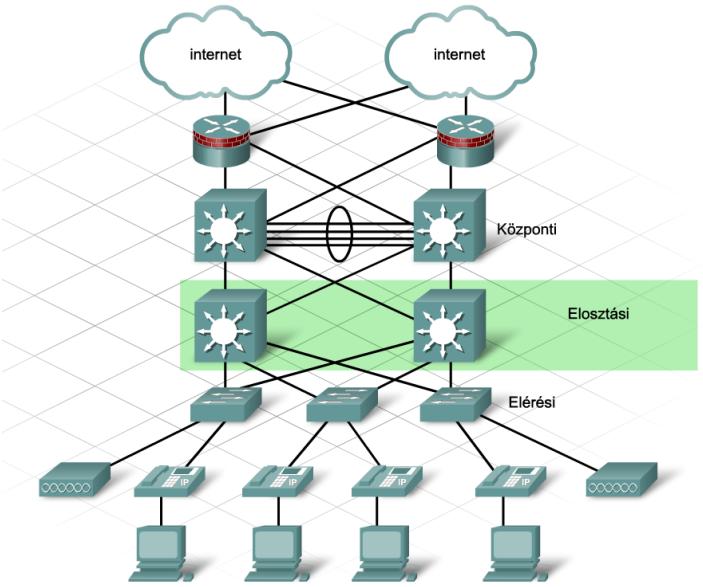
Az elosztási rétegben történő forgalomirányítás

Az elérési réteg általában 2. rétegbeli kapcsolási technológiát alkalmaz, míg az elosztási réteg általában 3. rétegbeli eszközöket használ. Az elosztási rétegben található forgalomirányítók és a többrétegű kapcsolók számos kulcsfontosságú funkciót biztosítanak, amelyek segítenek a hálózati célkitűzések megvalósításában. Ilyen cél lehet:

- Az adatfolyamok szűrése és felügyelete.
- Hozzáférés-vezérlési irányelvek érvényesítése.

- Útvonal-összevonás, mielőtt az útvonalak hirdetése megtörténne a központi réteg felé.
- A központi réteg elszigetelése az elérési rétegben bekövetkező meghibásodásoktól és zavaroktól.
- Az elérési réteg VLAN-jai közötti forgalomirányítás.

Az elosztási rétegbeli eszközök végzik a várakozási sorok kezelését, valamint a forgalom prioritás szerinti várakozási sorokba rendezését, még a telephely gerincén történő átvitel előtt.



Trönkök

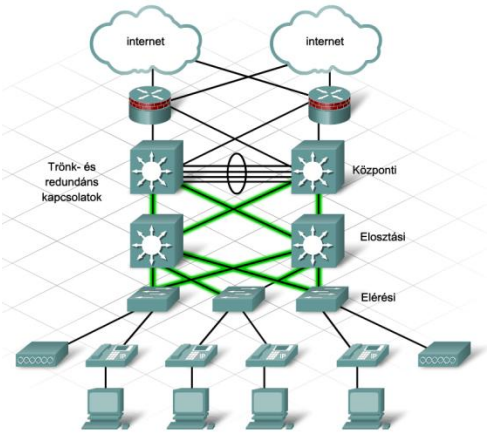
Trönkvonalakat általában az elérési és az elosztási réteg eszközei között kell beállítani. A trönkök használatának célja, hogy ugyanazon az összeköttetésen keresztül több VLAN-hoz tartozó forgalom haladhasson át. A trönkvonalak tervezésekor a hálózattervezőnek figyelembe kell vennie az általános VLAN stratégiát, valamint a hálózati fogalom összetevőit.

Redundáns összeköttetések

Amennyiben az elosztási réteg eszközei között vannak redundáns összeköttetések, az eszközökön beállítható, hogy a forgalmi terhelést szét lehessen osztani az összeköttetések között. A terheléselosztás megnöveli az alkalmazások számára rendelkezésre álló sávszélességet.

Az elosztási réteg topológiája

Az elosztási réteg kábelezése általában részleges háló topológia szerint történik, amely elegendő redundáns útvonalat biztosít ahhoz, hogy a hálózat kibírjon egy kapcsolat- vagy eszközhibát. Az elosztási réteg egyazon huzalozási központjában vagy adatközpontjában elhelyezett eszközei között általában gigabites összeköttetéseket használnak. Az egymástól nagyobb távolságra lévő eszközök esetében optikai kábelt használnak. A több, nagy sebességű optikai kapcsolatot támogató kapcsolók ára magas lehet, így gondos tervezés szükséges, hogy a kívánt sávszélesség és redundancia biztosításához elegendő optikai port álljon rendelkezésre.



1.3.2 A hálózati hiba hatásának korlátozása

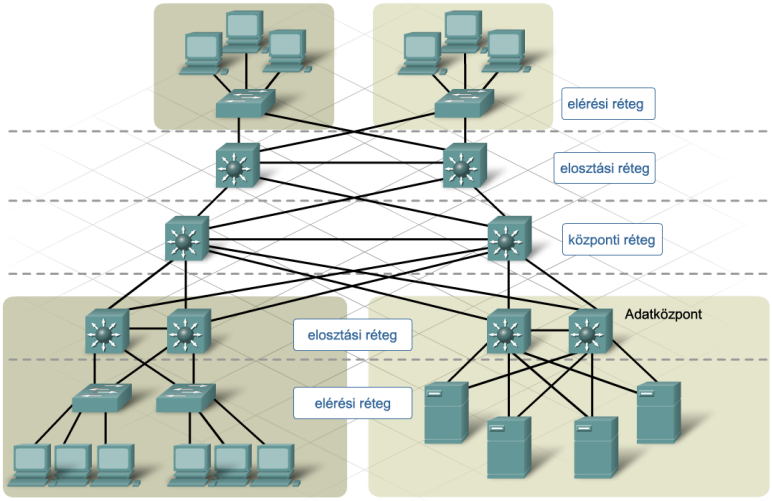
Hibatartomány alatt a hálózatnak azt a részét értjük, amely érintett egy eszköz vagy hálózati alkalmazás meghibásodásakor.

A hibatartomány méretének behatárolása

Mivel a hálózat központi rétegében bekövetkező hibák hatása a legnagyobb, a hálózattervező gyakran inkább a hibamegelőzésre helyezi a hangsúlyt. Ez a hozzáállás azonban nagymértékben megnövelheti a hálózat megépítésének költségeit. A hierarchikus tervezési modell szerint a legegyszerűbb és legolcsóbb megoldás a hibatartomány elosztási rétegben történő kontrollálása, mivel ott a hibák kisebb területet, ennél fogva kevesebb felhasználót érintenek. Amennyiben az elosztási rétegben 3. rétegbeli eszközöket alkalmazunk, mindegyik forgalomirányító átjáróként szolgál az elérési réteg korlátozott számú felhasználója számára.

Kapcsolóblokkok használata

A forgalomirányítók és a többrétegű kapcsolók általában párosával vannak telepítve, az elérési réteg kapcsolói pedig egyenletesen oszlanak el közöttük. Ezt az elrendezést épületi- vagy csoport-kapcsolóblokknak is nevezzük. Minden kapcsolóblokk egymástól függetlenül működik, megakadályozva ezzel a hálózat leállását egy eszköz meghibásodása esetén. Ebben az esetben még egy teljes kapcsolóblokk hibája sem érint jelentős számú végfelhasználót.



1.3.3 Redundáns hálózatok építése

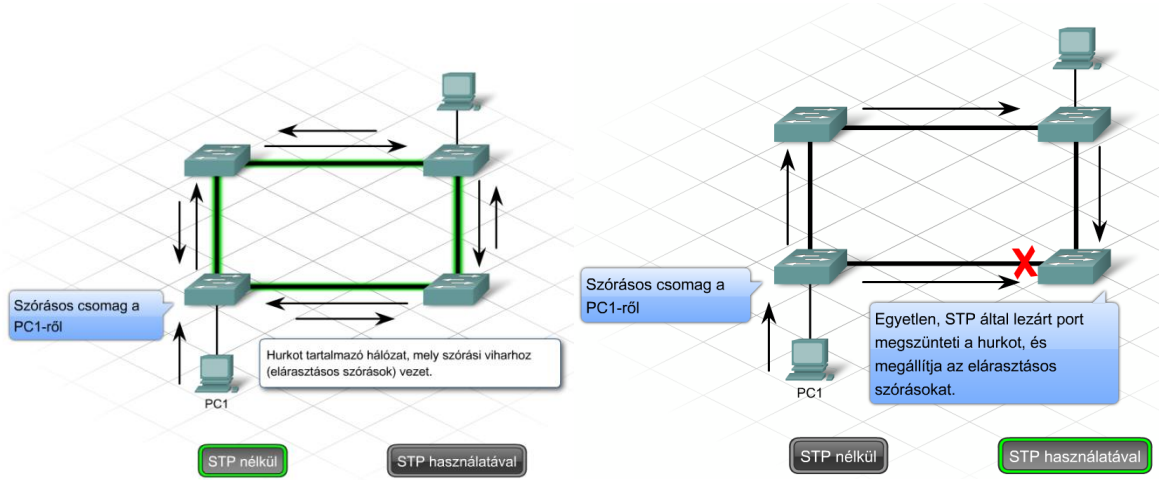
A leállási idő csökkentése érdekében a hálózattervezőnek redundanciát kell alkalmaznia a hálózatban.

Redundancia az elosztási rétegben

Az elosztási réteg eszközei redundáns összeköttetésekkel rendelkeznek az elérési réteg kapcsolói és a központi réteg eszközei felé. Kapcsolat- vagy eszközhiba esetén ezen összeköttetések alternatív útvonalat biztosítanak. Az elosztási rétegben alkalmazott megfelelő irányítóprotokoll esetén a 3. rétegbeli eszközök gyorsan reagálnak a kapcsolathibákra, így nem befolyásolják a hálózat működését.

Amíg az STP nincs engedélyezve, a 2. rétegbeli kapcsolók felé biztosított többszörös kapcsolat instabil viselkedést eredményezhet. STP nélkül egy 2. rétegbeli hálózat redundáns összeköttetései szórási vihart okozhatnak, mivel a kapcsolók nem képesek megjegyezni az érintett portokat, így végül a forgalom szétárad a kapcsolókon keresztül. Az STP az a redundáns összeköttetések tiltásával garantálja, hogy két eszköz között csak egyetlen aktív útvonal legyen. Amennyiben az egyik kapcsolat meghibásodik, a kapcsoló újraszámolja a feszítőfa-topológiát, majd automatikusan használni kezdi a tartalék összeköttetést.

Az IEEE 802.1w szabványban definiált gyors feszítőfa protokoll (Rapid Spanning Tree Protocol, RSTP) az IEEE 802.1d technológián alapul, és jelentősen felgyorsítja a feszítőfa újraszámolását.



Ha nagy forgalmat bonyolító vállalati kiszolgáló csatlakozik a kapcsoló egyik portjához, és az STP újraszámolásra kényszerül, a kiszolgáló 50 másodpercig elérhetetlenné válik. Elképzelni is nehéz, hogy az adott időszakban mennyi tranzakció vész el.

Stabil hálózatokban az STP újraszámolások nem túl gyakoriak. Instabil hálózatban fontos a kapcsolók stabilitásának és konfiguráció változásainak ellenőrzése. Az STP újraszámolások egyik leggyakoribb oka a kapcsoló hibás tápellátása. A hibás tápellátás az eszköz váratlan újraindulását eredményezheti.

1.3.4 Forgalomszűrés az elosztási rétegben

A hozzáférési lista (ACL) az elosztási rétegben használható eszköz, amellyel korlátozható a hozzáférés, és megakadályozható a nem kívánt forgalom központi hálózatba jutása. Az ACL olyan feltételellista, amellyel ellenőrizhető a forgalomirányító valamelyik interfészén áthaladó hálózati forgalom. Az ACL-utasításokkal azonosíthatók az engedélyezni vagy elutasítani kívánt csomagtípusok.

A hálózati forgalom szűrése

A hálózati forgalom szűréséhez a forgalomirányító minden csomagot megvizsgál, majd az ACL-ben meghatározott feltételek alapján továbbítja vagy törli azt. A különböző célokra eltérő típusú ACL-ek léteznek. A normál ACL kizárólag a forráscím alapján képes szűrni, míg a kiterjesztett ACL több feltétel alapján is végezhet szűrést. Ilyen feltétel például:

- a forráscím
- a célcím
- a protokollok
- a portszámok vagy alkalmazások
- a csomag egy már felépült TCP adatfolyam része-e

Mind a normál, mind pedig a kiterjesztett ACL megadható számozott vagy nevesített hozzáférési listaként.

Összetett ACL-ek

A normál és kiterjesztett ACL-ek szolgálhatnak más, sokkal összetettebb ACL típusok alapjául. A Cisco IOS szoftver használatával három összetett ACL-működési mód állítható be: dinamikus, reflexív és idő alapú.

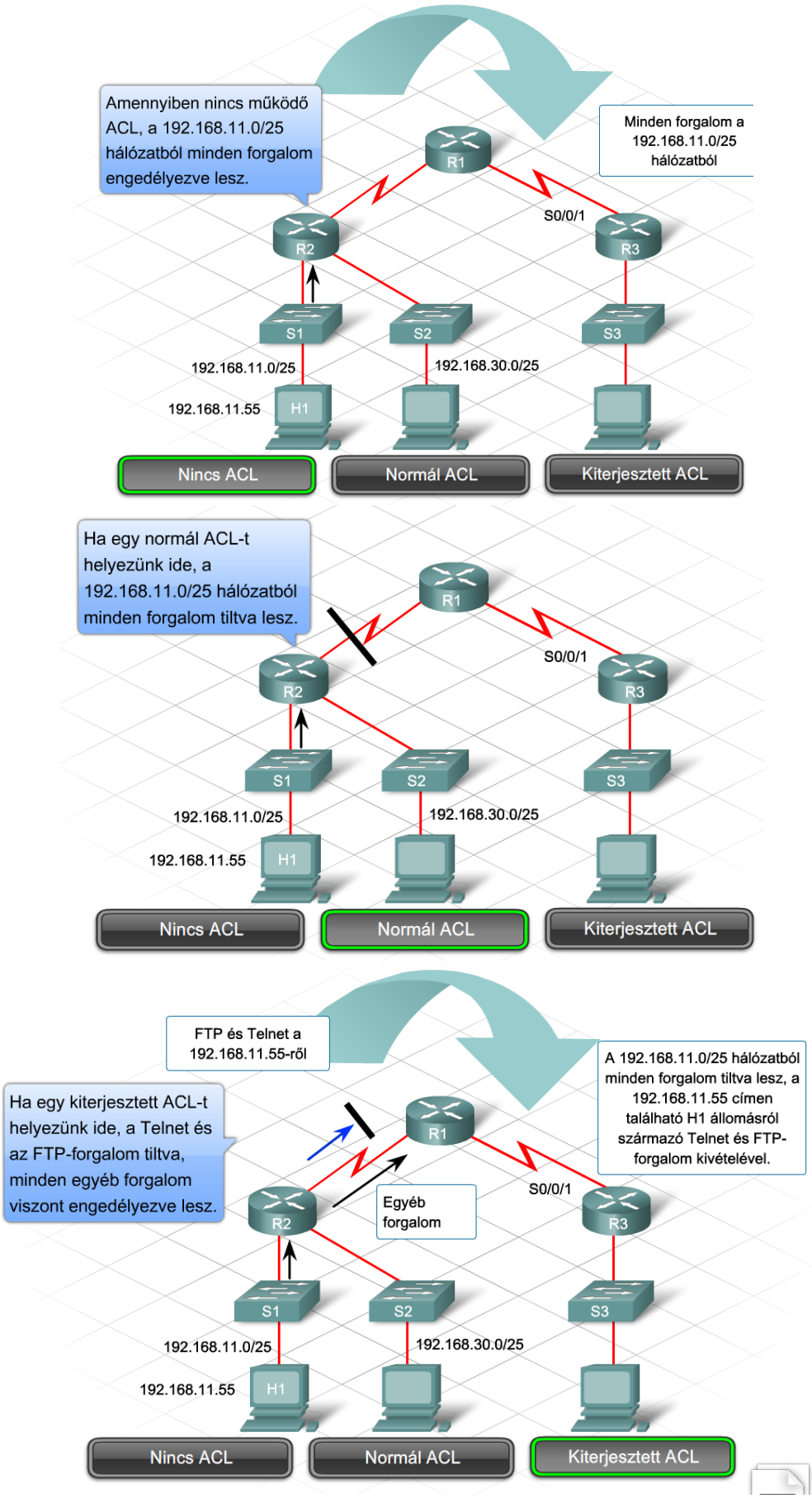
Dinamikus ACL – megköveteli a felhasználótól, hogy telnetkapcsolatot létesítsen a forgalomirányítóval és hitelesítse magát. A hitelesítést követően a felhasználótól származó forgalom engedélyezve lesz. A dinamikus ACL-t néha „zár és kulcs” névvel illetik, mivel a hozzáférés megszerzéséhez a felhasználónak be kell jelentkeznie.

Reflexív ACL – engedélyez minden kimenő forgalmat, ugyanakkor a bejövő forgalmat kizárólag az ezekre az engedélyezett kérésekre érkezett válaszokra korlátozza. Ez hasonló a kiterjesztett ACL-utasításokban használt established kulcsszóhoz azzal a különbséggel, hogy ez a típus a TCP-n kívül az UDP és ICMP forgalmat is vizsgálja.

Idő-alapú ACL – engedélyezi vagy tiltja a nap adott időszaka vagy a hét adott napja alapján meghatározott forgalmat.

Az ACL-ek elhelyezése

Egy adott interfészen a forgalomirányítóba beérkező forgalmat befelé irányított szűrő ACL-el, a kimenő forgalmat pedig kifelé irányított szűrő ACL-el szűrjük. A kívánt eredmények eléréséhez a hálózattervezőnek kell meghatározni az ACL-ek helyét hálózatban.


Amennyiben nincs működő ACL, a 192.168.11.0/25 hálózatból minden forgalom engedélyezve lesz.
Minden forgalom a 192.168.11.0/25 hálózatból
R1
R2
R3
S0/0/1
S1
S2
S3
192.168.11.0/25
192.168.30.0/25
192.168.11.55
H1
Nincs ACL
Normál ACL
Kiterjesztett ACL
Ha egy normál ACL-t helyezünk ide, a 192.168.11.0/25 hálózatból minden forgalom tiltva lesz.
R1
R2
R3
S0/0/1
S1
S2
S3
192.168.11.0/25
192.168.30.0/25
192.168.11.55
H1
Nincs ACL
Normál ACL
Kiterjesztett ACL
FTP és Telnet a 192.168.11.55-ről
A 192.168.11.0/25 hálózatból minden forgalom tiltva lesz, a 192.168.11.55 címen található H1 állomásról származó Telnet és FTP-forgalom kivételével.
Ha egy kiterjesztett ACL-t helyezünk ide, a Telnet és az FTP-forgalom tiltva, minden egyéb forgalom viszont engedélyezve lesz.
Egyéb forgalom
R1
R2
R3
S0/0/1
S1
S2
S3
192.168.11.0/25
192.168.30.0/25
192.168.11.55
H1
Nincs ACL
Normál ACL
Kiterjesztett ACL

Az alábbi lista röviden áttekinti a hozzáférési listák (ACL-ek) tervezési és alkalmazási szabályait.

- Interfészenként, irányonként és protokollonként csak egy ACL adható meg.
- A normál ACL-eket a célhoz a lehető legközelebb kell alkalmazni.
- A kiterjesztett ACL-eket a forráshoz a lehető legközelebb kell alkalmazni.
- A kimenő és a bejövő jelzőket úgy kell használni, mintha a forgalomirányító belsejéből néznénk a portokat.
- Az utasítások feldolgozása sorban, a lista tetejétől az alja felé haladva történik, amíg a forgalomirányító egyezést nem talál. Ha nincs egyezés, a forgalomirányító eldobja a csomagot.
- Minden ACL végén egy implicit "deny any" szabály található, amely nem jelenik meg a beállítások listázásakor.
- A hozzáférési listák utasításait a specifikusabbaktól az általánosabbak felé haladva kell megadni. Az egyes állomásokra vonatkozó tiltásokat kell először megadni, a csoportokra vonatkozó vagy általános szűrőket utolsóként kell elhelyezni.
- Elsőként az egyezési feltétel vizsgálata történik meg. Kizárólag egyezés esetén vizsgálja meg, hogy "engedélyezésről" vagy "tiltásról" van szó.
- Soha ne dolgozzunk aktívan működő ACL-lel!
- Először szövegszerkesztő segítségével készítsük el a működést felvázoló megjegyzéseket, a tényleges végrehajtó műveleteket csak ezt követően írjuk meg!
- Alapértelmezés szerint az új sorok mindig a hozzáférési lista végére kerülnek. A no access-list x parancs a teljes listát törli.
- Az IP alapú hozzáférési listák a célállomás elérhetetlenségét jelző ICMP-üzenetet küldenek az elutasított csomagok forrásainak, majd eldobják a csomagokat.
- Az ACL-ek törlésénél körültekintően kell eljárni, mivel a szűrési folyamat azonnal leáll.
- A kimenő szűrők nem vonatkoznak a helyi forgalomirányítóról kiinduló forgalomra.

1.3.5 Irányítóprotokollok az elosztási rétegben

Az elosztási rétegben végbemenő másik fontos feladat az útvonal összevonás, más néven útvonal összefogás vagy szuperhálózat-számítás.

Útvonal összevonás

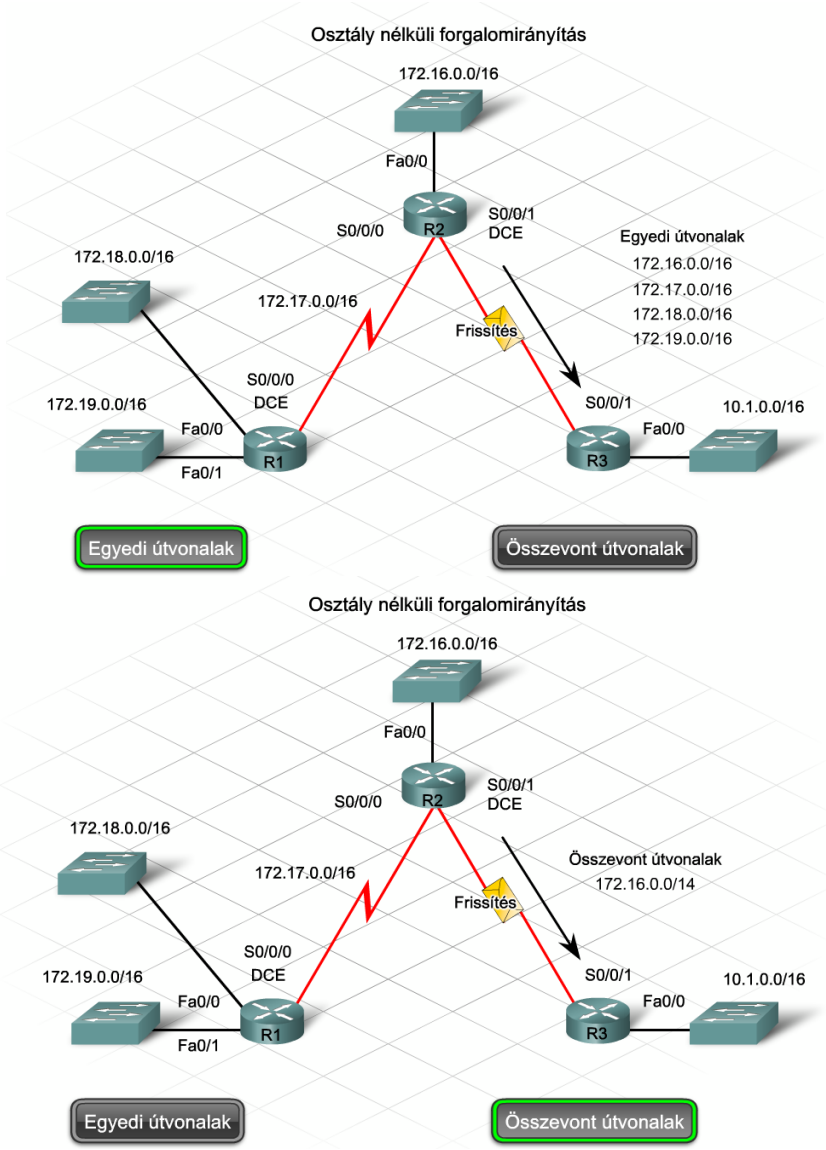
Az útvonal összevonás számos előnyt biztosít a hálózat számára. Ilyen például:

- Az irányítótáblába több más útvonalat képviselő egyetlen útvonal kerül, s így az irányítótábla kisebb méretű lesz.
- Kevesebb irányítási frissítésből származó forgalom jelenik meg a hálózaton.
- Csökken a forgalomirányító terhelése.

Az összevonás manuálisan és automatikusan is végezhető, a hálózatban használt irányítóprotokolloktól függően.

Az osztály nélküli irányítóprotokollok (pl. RIPv2, EIGRP, OSPF és IS-IS) útvonal-összevonásában szereplő hálózatcímek tetszőleges határra eshetnek.

Az osztály alapú irányítóprotokollok (pl. RIPv1) automatikusan összevonják az útvonalakat az osztályos hálózati határon, de nem támogatnak semmilyen egyéb határra eső összevonást.



1.4 Az elérési réteg (Access Layer) tervezési koncepcióinak feltárása

1.4.1 Mi történik az elérési rétegben?

Az elérési réteg képezi a hálózat határát, ahol a végberendezések csatlakoznak. Az elérési réteg szolgáltatásait és eszközeit a telephely, az összes távoli telephely és kiszolgálófarm, valamint a vállalati határ mindegyik épületében elérhetővé kell tenni.

Az elérési réteg kialakításának fizikai szempontjai

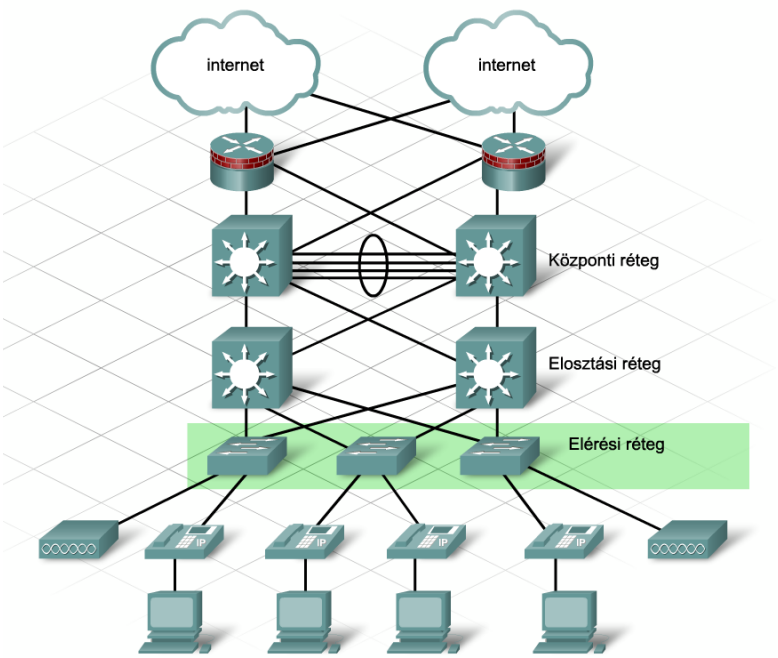
Egy telephely infrastruktúrájának elérési rétege 2. rétegbeli kapcsolási technológiát alkalmaz a hálózati kapcsolat biztosításához. Az elérés történhet állandó, vezetékes infrastruktúrán vagy vezetéknélküli hozzáférési pontokon keresztül. A rézvezetéken keresztüli Ethernet távolságbeli korlátokat szab, így egy telephelyi infrastruktúra hozzáférési rétegének tervezésénél az egyik elsődleges szempont a berendezések fizikai elhelyezése.

Huzalozási központok

A huzalozási központ lehet egy szekrény vagy egy kisméretű távközlési helyiség, amely az épületen vagy épületszinten belüli kábelezés végpontjául szolgál. A huzalozási központ helye és fizikai mérete a hálózat méretétől és bővítési terveitől függ.

A huzalozási központ berendezései biztosítják a tápellátást a végberendezések (pl. IP-telefonok és vezetéknélküli hozzáférési pontok) számára. Számos elérési rétegbeli kapcsoló támogatja az Ethernet hálózat által biztosított áramellátást (Power over Ethernet, PoE).

A tipikus huzalozási központtal ellentétben, a kiszolgálófarmon vagy adatközponton belül az elérési rétegbeli eszközök általában redundáns, többrétegű kapcsolók, amelyek kombinálják a forgalomirányítás és a kapcsolás képességét. A többrétegű kapcsolók a tűzfal és behatolásvédelmi funkciók mellett 3. rétegbeli funkciókat is biztosítanak.



A konvergált hálózatok hatása

A modern számítógépes hálózatok már nem csupán az elérési réteghez csatlakoztatott személyi számítógépekből és nyomtatókból állnak. Más, egyéb eszközök is csatlakoztathatók egy IP-hálózathoz, ide sorolva az alábbiakat:

- IP-telefonok
- videokamerák
- videokonferencia-rendszerek

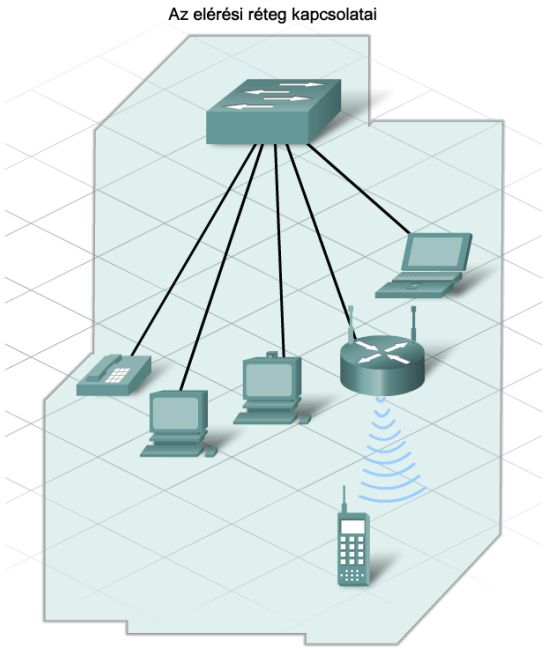
A fenti szolgáltatások mindegyike egyetlen fizikai elérési rétegbeli infrastruktúrában egyesíthető, ugyanakkor az ezeket támogató logikai hálózati terv sokkal összetettebbé válik a QoS, a forgalom-szétválasztás és -szűrés, valamint az ehhez hasonló szempontok miatt. A végberendezések ezen új típusai, valamint a hozzájuk tartozó alkalmazások és szolgáltatások megváltoztatják az elérési

réteg méretezhetőségével, elérhetőségével, biztonságával és felügyelhetőségével kapcsolatos követelményeket.

A rendelkezésre állás fontossága

A korábbi hálózatokban a magas rendelkezésre állás általában csak a hálózati magot, a vállalati határt és az adatközponti hálózatokat jellemezte. Az IP-telefonálás megjelenésével mára már elvárás, hogy minden egyes telefon legyen elérhető az idő 100%-ában.

Az elérési rétegben alkalmazott összetevők és hibakezelési stratégiák segítségével növelhető a végberendezések megbízhatósága és rendelkezésre állása.



Az elérési réteg felügyelete

A hálózattervező egyik kiemelt feladata az elérési réteg felügyelhetőségének javítása, amely kulcsfontosságú az alábbiak miatt:

- Az elérési réteghez csatlakoztatható eszközök egyre növekvő száma és egyre többféle típusa.
- A LAN részeként megjelenő vezetéknélküli hozzáférési pontok.

A felügyelhetőséggel kapcsolatos tervezési lépések

Az elérési réteg alapvető összeköttetéseinek biztosításán felül a tervezőnek az alábbi szempontokat is figyelembe kell vennie:

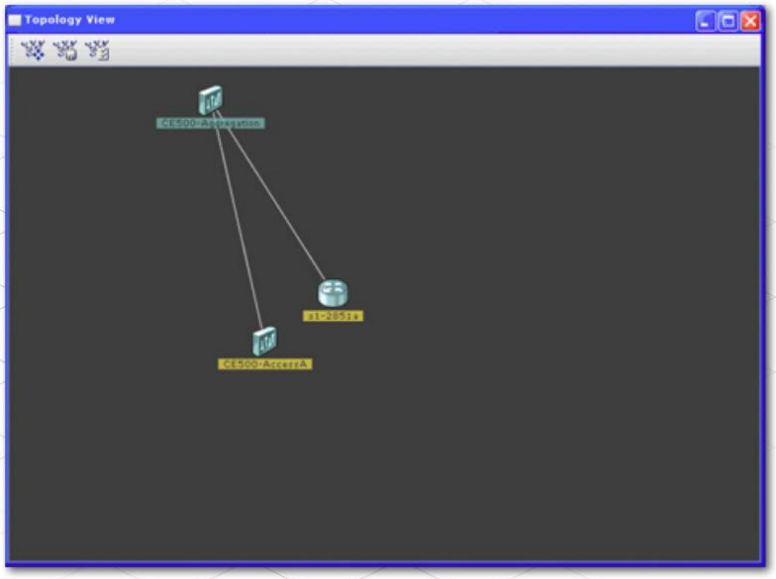
- elnevezési struktúrák
- VLAN architektúra
- forgalmi minták
- prioritással kapcsolatos stratégiák

Nagyméretű hálózatok esetében rendkívül fontos a hálózatfelügyeleti rendszerek beállítása és használata, valamint – ahol ez lehetséges – a beállítások és a berendezések szabványosítása.

A jó tervezési elvek követésével javul a hálózat felügyelhetősége és folyamatos támogatása az alábbiak miatt:

- Biztosítja, hogy a hálózat nem válik túlságosan összetetté.
- Probléma esetén egyszerű hibaelhárítást tesz lehetővé.
- Egyszerűsíti a jövőbeni új funkciók és szolgáltatások hozzáadását.

Hálózatfelügyeleti szoftver - A Cisco Network Assistant (Hálózati Segéd)



1.4.2 Az elérési réteg hálózati topológiái

A legújabb Ethernet hálózatok csillag topológiát használnak, amelyet kerékküllő topológiának is nevezünk. A csillag topológia szerint az összes végberendezés közvetlenül kapcsolódik egyetlen hálózati eszközhöz, amely általában egy 2. rétegbeli vagy többrétegű kapcsoló. Az elérési rétegben alkalmazott vezetékes csillag topológia jellemzően semmilyen redundanciát nem biztosít az egyes végberendezések és a kapcsoló között. Sok vállalat számára túl magas költségekkel jár a redundanciát biztosító kábelezés.

A csillag topológia előnyei közé tartoznak az alábbiak:

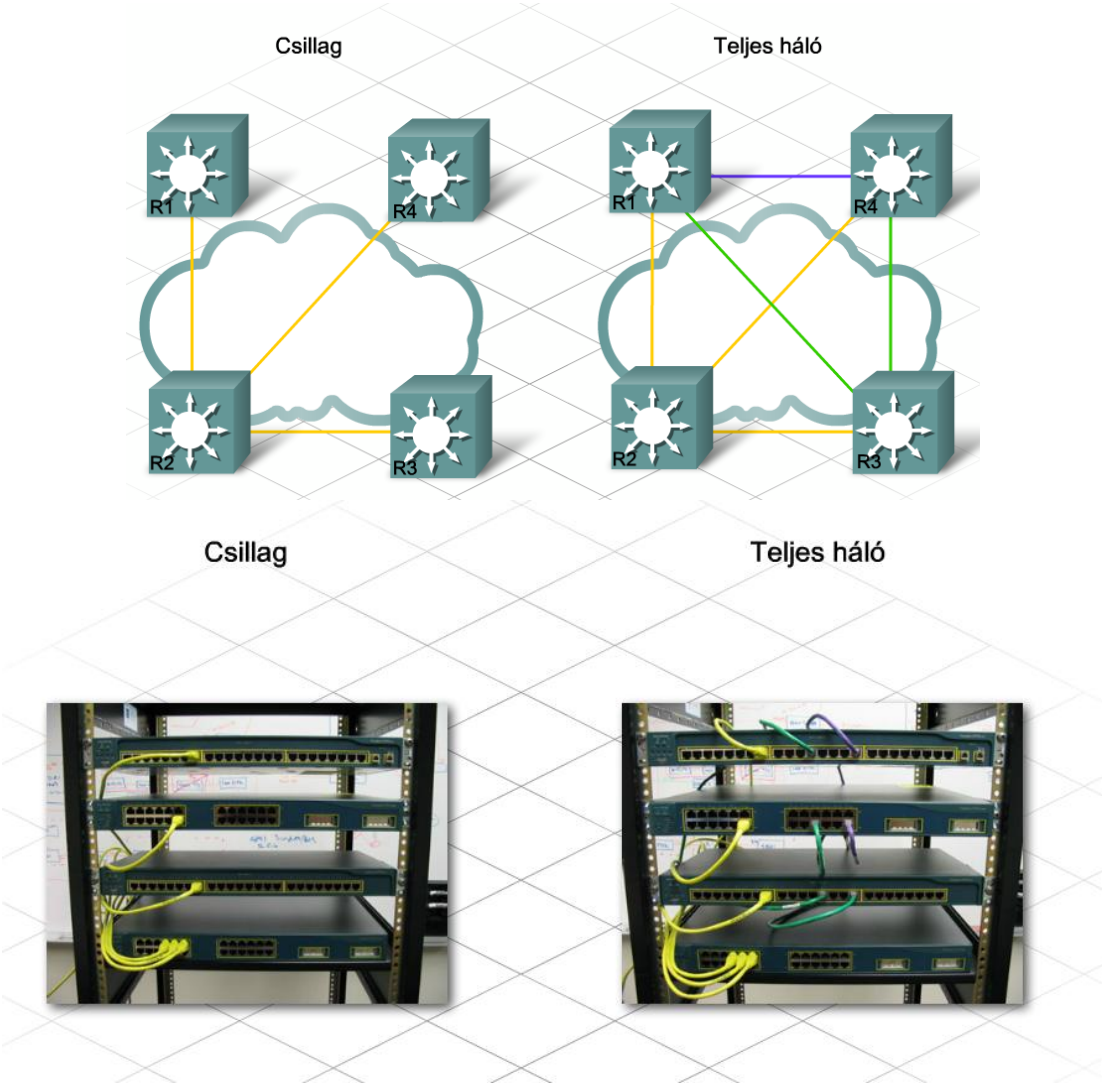
- könnyű telepíthetőség
- minimális konfigurálás

A csillag topológiának azonban komoly hátrányai is vannak:

- A központi eszköz kritikus hibaforrásként (single point of failure) jelenhet meg.
- A központi eszköz képességei korlátozhatják a hálózati elérés általános teljesítményét.
- A topológia nem képes helyreállni, amennyiben redundáns összeköttetések nélküli helyen következik be a hiba.

A csillag topológiájú Ethernet hálózatok általában az alábbi kábelezési kombinációt alkalmazzák:

- Csavart érpár a végberendezések csatlakoztatásához
- Optikai kábel az elérési réteg kapcsolói és az elosztási réteghez tartozó eszközök között



1.4.3 Hogyan választható szét és vezérelhető a hálózati forgalom a VLAN-okkal?

A forgalom VLAN használatával történő szétválasztása

A hálózat elérési rétegében a VLAN-ok és az IP alhálózatok alkalmazása a leggyakrabban használt eljárás a felhasználói csoportok és azok forgalmának egymástól történő elhatárolására.

VLAN-ok régen

A 2. rétegbeli kapcsolás megjelenésével a VLAN-okat végponttól végpontig terjedő munkacsoportos hálózatok létrehozására használták. Ezek a hálózatok épületek között vagy akár a teljes infrastruktúrán keresztül megvalósított összeköttetéseket is használtak. A végponttól végpontig terjedő VLAN-okat ma már nem használjuk. A felhasználók megnövekedett száma és az általuk generált adatforgalom már túl nagy ahhoz, hogy a fenti megoldást lehessen alkalmazni.

VLAN-ok napjainkban

A VLAN-okat napjainkban adatfolyamok szétválasztására és csoportosítására, valamint a szórások egyetlen huzalozási központon vagy épületen belül történő korlátozására használjuk. Bár az egész hálózaton átívelő, nagyméretű VLAN-ok használata már nem javasolt, speciális alkalmazásokhoz (pl. vezetéknélküli barangolás vagy vezetéknélküli IP-telefonok esetében) szükség lehet rájuk.

A jelenlegi ajánlás szerint a VLAN-okat egyetlen huzalozási központon belül kell tartani, így megnő az egy hálózatban lévő VLAN-ok száma, melynek eredményeként növekszik az egyéni IP-alhálózatok száma is. Jól bevált gyakorlat, hogy egy IP-alhálózatot egyetlen VLAN-hoz társítunk. Az elérési rétegben megvalósuló IP-címzés kulcsfontosságú tervezési kérdéssé válik, amely kihat a teljes hálózat bővíthetőségére.

1.4.4 A hálózati határ szolgáltatásai

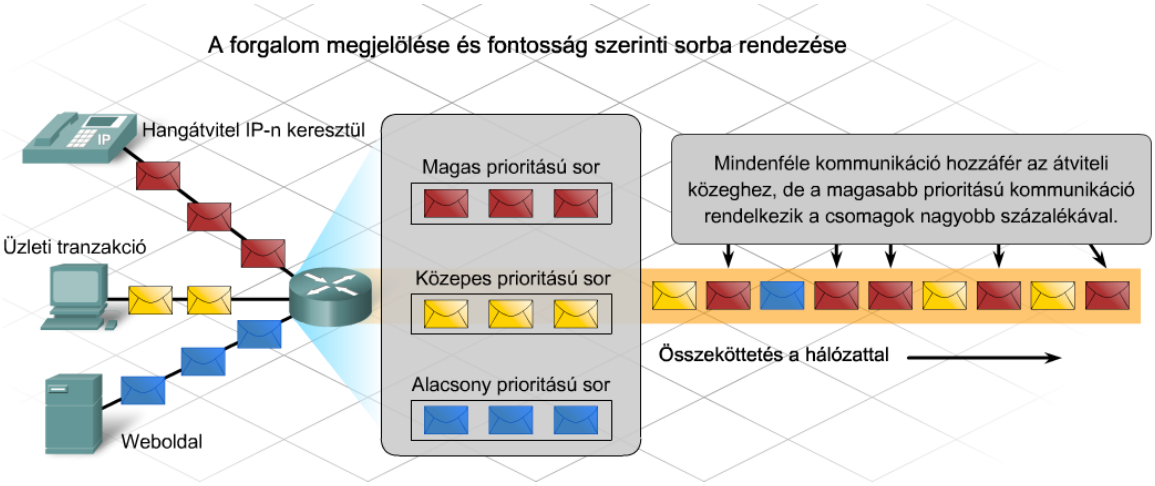
Szolgáltatásminőség biztosítása a hálózati alkalmazások számára

A hálózatnak biztonságos, kiszámítható, mérhető és estenként garantált szolgáltatásokat kell biztosítani. A hálózat számára olyan mechanizmusok is szükségesek, amelyekkel megnövekedett forgalom esetén kezelni tudja a torlódásokat. Torlódás akkor jöhet létre, amikor a hálózati erőforrásokra vonatkozó igények meghaladják a rendelkezésre álló kapacitást.

Minden hálózat korlátozott erőforrásokkal rendelkezik, ezért van szükség a QoS (Quality of Service – szolgáltatás minőség) mechanizmusokra. A QoS által biztosított szabályozás függ a forgalom osztályozásától és a beállított prioritástól.

Osztályozás

A QoS stratégiák megtervezése előtt el kell készíteni az alkalmazások konkrét kézbesítési igények alapján történő osztályozását. Az adatoknak a forrásnál vagy annak közelében történő osztályozása lehetővé teszi, hogy az adatokhoz a megfelelő prioritások legyenek rendelve, miközben keresztülhaladnak a teljes hálózaton. A hasonló jellemzőkkel bíró forgalom összetevők azonos osztályokba történő besorolása, majd megjelölése az elérési és az elosztási réteg eszközeinek feladata. A fenti stratégiára példa, amikor a hang alapú forgalom egy elérési rétegbeli kapcsolón azonos VLAN-ba kerül. Ezt követően a kapcsoló a „hang” VLAN-ból származó forgalomhoz a legmagasabb prioritást rendeli.



1.4.5 A hálózati határ biztonsága

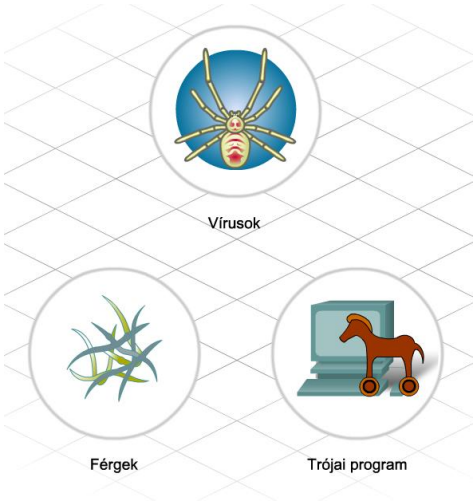
Az elérési réteg biztonsági kockázatai

A hálózat elérési rétegében előforduló biztonsági kockázatok nagyrészt a nem megfelelően védett végberendezésekből adódnak. Jelentős számú biztonsági rés származik felhasználói hibából és gondatlanságból.

Hogyan javíthat a hálózattervező a biztonságon?

A végberendezések megfelelő védelmének kialakítása meghaladhatja egy hálózattervezési projekt kereteit. Ettől függetlenül a tervezőnek ismernie kell egy végberendezésnél felmerülő biztonsági probléma (pl. egy féreg vagy egy trójai program) hálózatra gyakorolt hatását. A tervező így könnyebben el tudja dönteni, hogy milyen hálózatbiztonsági intézkedések szükségesek ahhoz, hogy a hálózatra gyakorolt hatás minimális legyen.

A kizárólag ismert és hitelesített berendezések számára engedélyezett hálózati hozzáférés korlátozza a támadó bejutási lehetőségeit a hálózatba. Az ajánlásokat követő vezetéknélküli biztonsági intézkedések alkalmazása szintén fontos szempont.



1.4.6 Biztonsági intézkedések

A fizikai védelem biztosítása

A hálózatok fizikai védelme rendkívül fontos, mivel a legtöbb támadó a hozzáférési rétegben szerzi meg a fizikai hozzáférést. A hálózati eszközök némelyikén (pl. a forgalomirányítókon és a kapcsolókon) a fizikai hozzáférés lehetőséget biztosít a jelszavak megváltoztatására, valamint az eszközökhöz való teljes hozzáférés megszerzésére.

A biztonsági rések megszüntetésének sokszor a leghatékonyabb módjai az olyan magától értetődő intézkedések, mint például a huzalozási központ zárva tartása vagy a hálózati eszközökhöz történő hozzáférés korlátozása. A nagy kockázatot jelentő vagy könnyen hozzáférhető helyeken szükséges lehet a huzalozási központ felszerelésére további védelemi eszközökkel (pl. kamerákkal, mozgásérzékelőkkel és riasztókkal). Néhány eszköz (pl. billentyűzár) rögzítheti a védett területekre történő belépéshez használt kódokat.

Az elérési réteg hálózati eszközeinek védelme

Az alábbi egyszerű biztonsági intézkedések további védelmet biztosíthatnak az elérési réteg hálózati eszközei számára:

- Erős jelszavak beállítása
- SSH használata az eszközök felügyeletéhez
- A használaton kívüli portok tiltása

A kapcsoló portbiztonság (port security) és a hálózati hozzáférés-vezérlés képes csak azt biztosítani, hogy csak az ismert és megbízható eszközök férhessenek hozzá a hálózathoz.

Biztonsági ajánlások

A biztonsági kockázatok nem szüntethetők meg teljesen. A kockázatok felmérésével és hatékony kezelésével jelentősen csökkenthetők a meglévő biztonsági kockázatok. A biztonsági intézkedések tervezésekor fontos tudni, hogy egyetlen termék sem képes önmagában biztonságossá tenni egy hálózatot. A valódi hálózatbiztonság a megfelelő termékek, szolgáltatások és folyamatok kombinációjából áll elő, de ugyanúgy a biztonsági rendszer részét képezik az alapos biztonsági irányelvek és azok betartása.

1.5 A szerver farmok és a biztonság feltárása

1.5.1 Mi az a kiszolgálófarm?

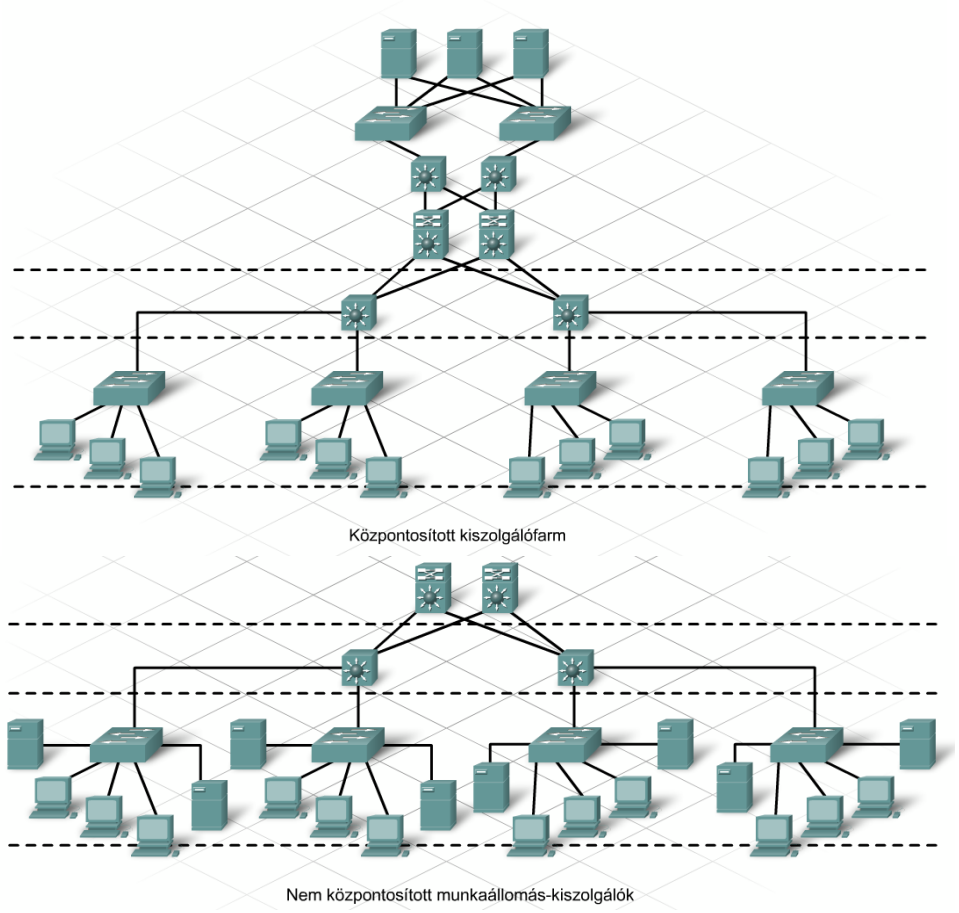
A legtöbb vállalati hálózat lehetővé teszi az internetelérést igénylő szolgáltatások (pl. e-mail és e-kereskedelem) biztosítását a felhasználók számára. A fenti szolgáltatások rendelkezésre állása és biztonsága kulcsfontosságú a vállalat sikeréhez.

Kiszolgálófarmok

A vállalati hálózat több különböző pontján elhelyezett nagyszámú kiszolgáló kezelése és védelme rendkívül nehézkes. Az ajánlások szerint a kiszolgálókat egy kiszolgálófarmra kell központosítani. A kiszolgálófarmok általában számítógépes helyiségekben vagy adatközpontokban vannak elhelyezve.

Egy kiszolgálófarm létrehozása az alábbi előnyökkel jár:

- A hálózati forgalom egy meghatározott ponton lép be a kiszolgálófarmra, és távozik onnan. Ez az elrendezés megkönnyíti a forgalom védelmét, szűrését és fontosság szerint történő sorba rendezését.
- Redundáns, nagy teljesítményű összeköttetések telepíthetők a kiszolgálókhoz, valamint a kiszolgálófarm és a központi LAN közé. Ez a felállás sokkal költséghatékonyabb, mintha a hálózaton elszórt kiszolgálókkal kellene hasonló szintű összeköttetést biztosítani.
- Terheléselosztás és hibakezelés egyaránt biztosítható a kiszolgálók és a hálózati eszközök között.
- A nagy teljesítményű kapcsolók és biztonsági eszközök száma csökken, ezzel hozzájárulva a szolgáltatások költségének csökkentéséhez.



1.5.2 Biztonság, tűzfal és DMZ-k

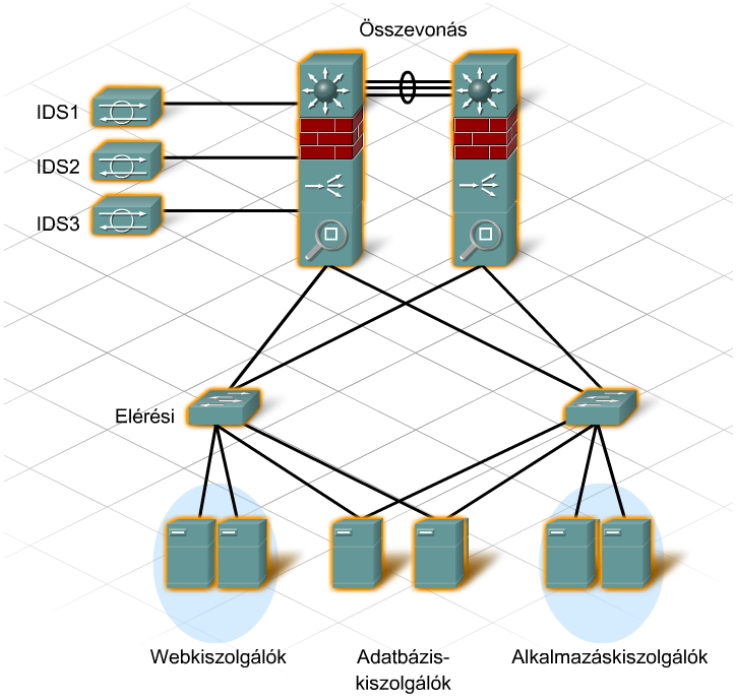
Az adatközponti kiszolgálók a rosszindulatú támadások célpontjai lehetnek, ezért meg kell védeni azokat.

A kiszolgálófarmok elleni támadások üzleti veszteséget okozhatnak az e-kereskedelmi vagy a vállalatok közötti (business-to-business, B2B) alkalmazások területén, de információlopás is történhet. A helyi hálózatokat (LAN-okat) és a tárolóhálózatokat (SAN-okat) egyaránt védeni kell, így csökkentve az ehhez hasonló támadások esélyeit. A támadók különféle eszközöket használnak a hálózat vizsgálatához, valamint a betöréses és szolgáltatásmegtagadásos (DoS) támadások indításához.

Kiszolgálófarmok védelme a támadásokkal szemben

Olyan helyeken, ahol a belső és külső felhasználók a kiszolgálófarmon keresztül érhetik el az internetet, gyakran alkalmaznak tűzfalakat az alapvető biztonság megteremtéséhez. A kiszolgálófarmok megfelelő védelmének megteremtése alapos körültekintést igényel, s ennek során az alábbi hálózati termékek fő erősségeire lehet építeni:

- Tűzfalak
- LAN kapcsolók védelmi funkciói
- Állomás- és hálózat-alapú behatolás érzékelő és -védelmi rendszerek
- Terheléselosztók
- Hálózatelemező és -felügyeleti eszközök



Demilitarizált zónák

A hagyományos, tűzfalat alkalmazó hálózati terv szerint a külső hálózati elérést igénylő kiszolgálókat egy ún. demilitarizált zónában (DMZ) kellett elhelyezni, így az internetről vagy más, megbízhatatlan külső hálózatból a kiszolgálókhoz hozzáférő felhasználók felől megakadályozta a belső LAN-ban található erőforrásokhoz történő hozzáférést. A LAN felhasználóit megbízható felhasználóknak tekintette, így rájuk kevés megszorítás vonatkozott a DMZ-ben lévő kiszolgálók elérésével kapcsolatban.

A belső támadások elleni védelem

A belső hálózatból származó támadások mára már sokkal gyakoribbak a külső forrásból eredő támadásoknál. Ennek eredményeképp a kiszolgálófarm védelmének terve is eltér a régebbi DMZ-modelltől. Szükség van egy tűzfalfunkciókat és behatolás védelmet biztosító rétegre a kiszolgálók és a belső hálózat, valamint a kiszolgálók és a külső felhasználók közé. A kiszolgálók között szükség lehet egy további biztonsági rétegre.

A kiszolgálófarm tervezésénél alkalmazott biztonsági irányelvek erősen függnek attól, hogy a kiszolgálókon tárolt és a tranzakciókban részt vevő adatok milyen mértékben tartalmaznak belső, védendő információt.

1.5.3 Magas rendelkezésre állás

A magas rendelkezésre állás biztosítása

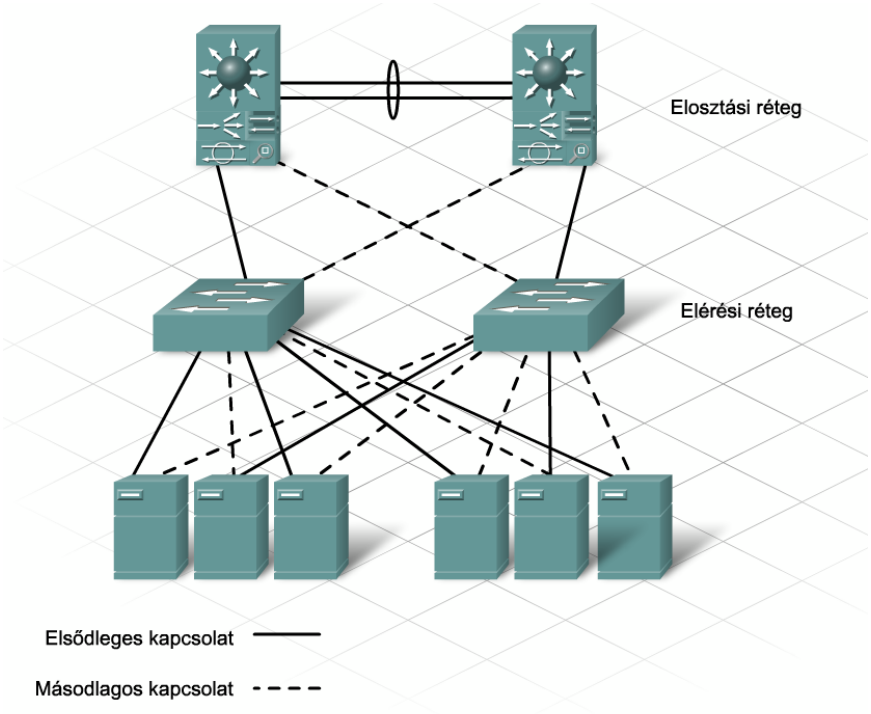
Az extra védelmi vonal biztosításán túlmenően a kiszolgálófarmnak magas rendelkezésre állást kell biztosítania a hálózati alkalmazások és szolgáltatások számára. A magas rendelkezésre állású hálózat kiküszöböli vagy lecsökkenti a hibák lehetséges hatásait. Ez a védelem lehetővé teszi a hálózat számára, hogy az alkalmazásokhoz, rendszerekhez és adatokhoz történő hozzáférési igényeket bárhonnan és bármikor teljesítse.

Redundáns építkezés

A magas rendelkezésre állás eléréséhez a kiszolgálók redundáns módon, az elérési réteg két különálló kapcsolójához vannak csatlakoztatva. Ez a redundancia biztosít egy tartalék útvonalat a kiszolgáló és a másodlagos kapcsoló között, amennyiben az elsődleges kapcsoló meghibásodik. A kiszolgálófarm elosztási és központi réteghez tartozó eszközei is redundáns kapcsolatokkal rendelkeznek. A feszítőfa-protokollok (pl. továbbfejlesztett gyors feszítőfa protokoll, RSTP+) felügyelik a 2. rétegbeli redundáns kapcsolatokat. A HSRP (Hot Standby Router Protocol – virtuális alapértelmezett átjáró protokoll) és más irányítóprotokollok biztosítják a 3. rétegbeli redundancia és hibakezelés támogatását.

Virtualizáció

Számos különálló logikai kiszolgáló lehet egyetlen fizikai kiszolgálón, amely kimondottan erre a célra, vagyis több virtuális gép támogatására tervezett operációs rendszert futtat. Ezt a képességet nevezzük virtualizációnak. Ez a technológia csökkenti a kritikus hálózati szolgáltatások számára biztosított redundáns szolgáltatások, terheléselosztás és hibakezelés költségeit.



1.6 A WLAN-ra vonatkozó egyedi szempontok

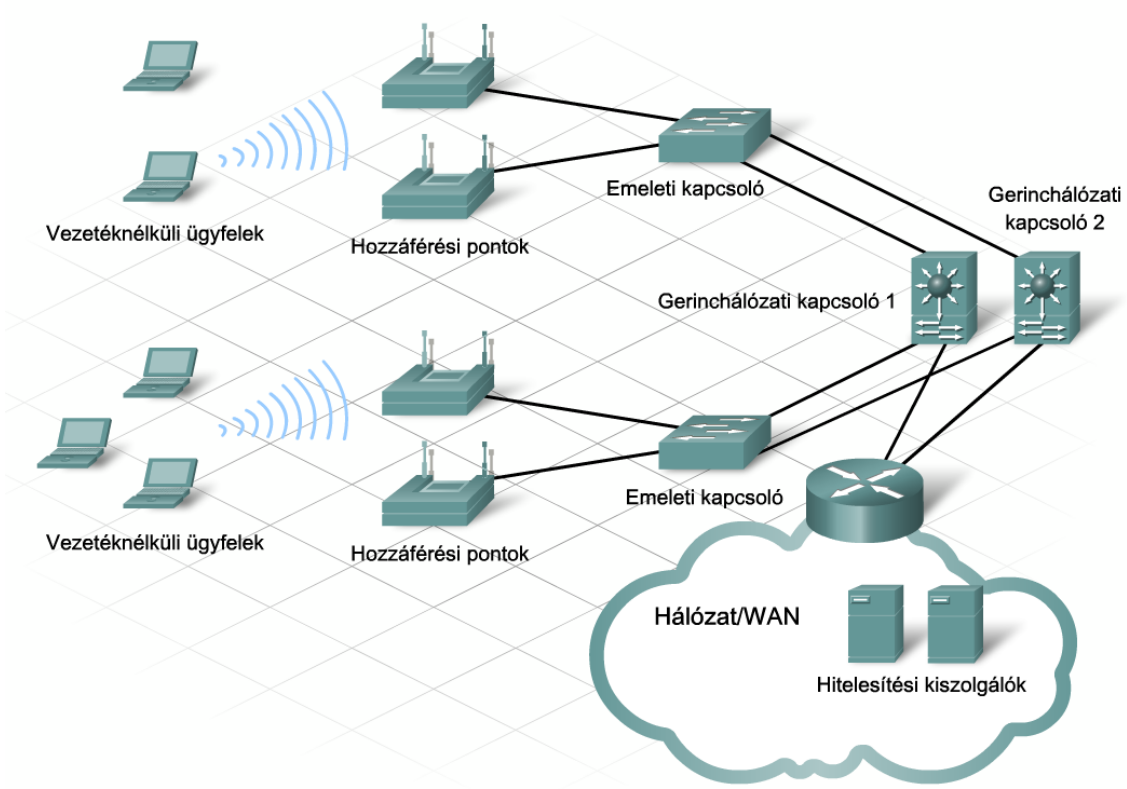
Az ügyfél igényeinek megismerése

Beltéri vezetéknélküli LAN (WLAN) megoldások tervezése előtt a hálózattervezőnek meg kell tudnia, hogy az ügyfél hogyan kívánja használni a vezetéknélküli hálózatot.

A tervező az ügyfélhez intézett kérdések segítségével ismeri meg a hálózati követelményeket, és az ezekre adott válaszok befolyásolják a vezetéknélküli hálózat kialakítását. Íme néhány példakérdés:

- Szükség van-e vezetéknélküli barangolásra?
- A felhasználók számára milyen hitelesítés szükséges?
- A vendégek számára kell-e nyílt csatlakozási pontot (hotspot) biztosítani?
- A vezetéknélküli felhasználók számára milyen hálózati szolgáltatások és alkalmazások legyenek elérhetők?
- Milyen titkosítási technika alkalmazható?
- Tervezik-e vezetéknélküli IP-telefonok használatát?
- Mely területekre kell lefedettséget biztosítani?
- Hány felhasználó lesz lefedettségi területenként?

Ha a tervező nem kap választ a fenti kérdésekre, vagy nem ismeri meg az ügyfél igényeit teljesen, a vezetéknélküli LAN kialakítása nehéz, majdhogynem lehetetlen vállalkozás lesz. A nem biztonságos csatlakozási pontok követelményei például nem olyan összetettek, mint a védett belső kiszolgálókhoz történő hitelesített hozzáférés megtervezése.



A hálózat fizikai terve

A vezetéknélküli hálózatok tervezésekor a hangsúly általában a hálózat által fizikailag lefedett területeken van.

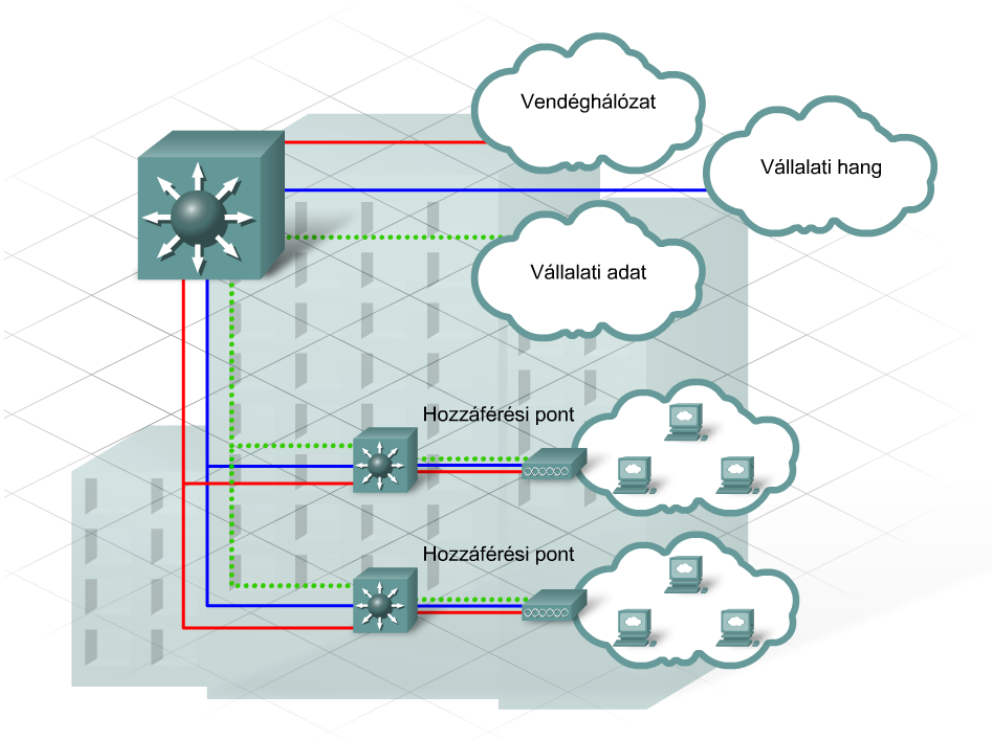
A hálózattervező egy helyszíni felmérés során határozza meg a lefedett területeket és a hozzáférési pontok telepítésének optimális helyét. A helyszíni felmérés a hozzáférési pont hardverét, az antennák típusát és a kívánt vezetéknélküli funkciókat is segít meghatározni. A tervező dönti el azt is, hogy lehet-e barangolni az egymással átfedésben lévő lefedett területek között.

A hálózat logikai terve

Általában a logikai hálózat megtervezése okozza a legnagyobb nehézséget a hálózattervezők számára. A megrendelők gyakran különböző szintű hozzáférést akarnak biztosítani a különböző vezetéknélküli felhasználók számára. A vezetéknélküli hálózatoknak ezen felül egyszerre kell könnyen kezelhetőnek és biztonságosnak lenniük. A vezetéknélküli LAN-ok megtervezésével és beállításával kapcsolatos elvárások és kötöttségek egyidejű teljesítése több különböző módon lehetséges.

Az összetett vezetéknélküli hálózat megtervezésére példa egy olyan vállalat, amelynek az alábbi szolgáltatásokat kell nyújtania:

- Nyílt vezetéknélküli hozzáférés a vendégek és a partnerek számára.
- Biztonságos vezetéknélküli hozzáférés azon alkalmazottak részére, akik rendszeresen változtatják a helyüket a telephelyen belül.
- Megbízható kapcsolat a vezetéknélküli IP-telefonok számára.



1.6.2 A WLAN-ra vonatkozó egyedi szempontok

A vezetéknélküli hozzáférés minden egyes típusa egyedi tervezési szempontokat igényel.

A vendégek nyílt hozzáférése

Amikor látogatók vagy partnerek érkeznek egy telephelyre, gyakran szeretnének hozzáférni a levelezésükhöz és különböző weboldalakhoz. Az ilyen típusú hozzáférésnek kényelmesnek kell lennie, jellemzően nincs titkosítva vezetékessel egyenértékű titkosítással (Wired Equivalent Privacy, WEP) vagy Wi-Fi védett hozzáféréssel (Wi-Fi Protected Access, WPA). A vendég felhasználók hálózathoz történő csatlakozását megkönnyítendő, a hozzáférési pont szolgáltatáskészlet azonosítója (service set identifier – SSID) hirdetve van.

Számos vendéghozzáférést biztosító csatlakozási pont DHCP-t és naplókiszolgálót használ a vezetéknélküli használat nyilvántartásához és rögzítéséhez. A vendégfelhasználók általában úgy érik el a vezetéknélküli hálózatot, hogy megnyitnak egy böngészőablakot, majd elfogadnak bizonyos felhasználási irányelveket. A vendégnyilvántartó rendszer rögzíti a felhasználó adatait és a fizikai címét, majd naplózni kezdi az IP-forgalmat. Az ilyen rendszerekben szükség van egy alkalmazás-kiszolgálóra, amelynek a hozzáférési pontokkal megegyező hálózatban vagy VLAN-ban kell lennie.

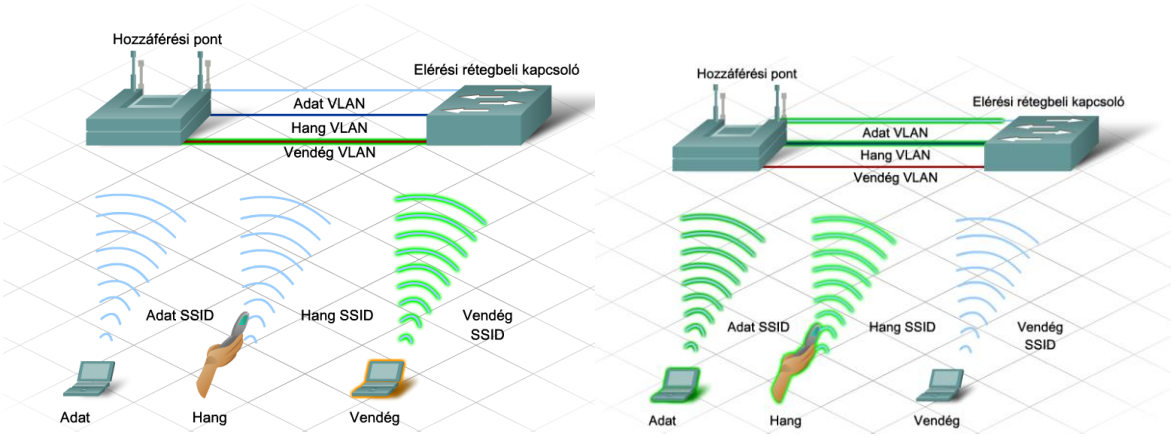
Az alkalmazottak biztonságos hozzáférése

A WLAN eszközök némelyike nem támogatja az elkülönített vendéghozzáférést. Ilyen esetben az alkalmazottak hozzáférésének védelméhez egy teljesen különálló, vendéghozzáféréssel nem rendelkező WLAN infrastruktúrát érdemes alkalmazni. Az ajánlások szerint a belső felhasználókat egy másik VLAN-ban kell elhelyezni.

A vezetéknélküli megoldásokhoz kapcsolódó további ajánlások:

- Az SSID elrejtése
- Erős titkosítás
- Felhasználói hitelesítés
- VPN alagúttechnika az érzékeny adatokhoz
- Tűzfal és behatolás-érzékelés

Azokon a területeken, ahol a védett vezetéknélküli hálózat tiltott néhány eszköz számára, ott MAC cím szűrés is alkalmazható a hozzáférések korlátozására.



A vezetéknélküli hálózatok egyik legnagyobb előnye, hogy az eszközök egyszerű és kényelmes csatlakozását teszik lehetővé. Sajnos a könnyű kapcsolódás és a rádióhullámokkal átvitt információ sebezhetővé teszi a vezeték nélküli hálózatokat az adatelfogásokkal és támadásokkal szemben.

A vezetéknélküli hozzáférési pontok és a hozzájuk tartozó vezeték nélküli átvitel védelmének jól bevált módszerei közé tartoznak az alábbiak:

- Az alapértelmezett SSID megváltoztatása, szórásának tiltása (amíg nem szükséges)
- Erős titkosítás használata

- Az ügyfél és a hálózat közötti kölcsönös hitelesítés bevezetése
- A VPN-ek vagy a WPA MAC-cím alapú hozzáférési listákkal történő kombinációja az üzleti célú eszközök védelméhez
- A hálózati erőforrásokhoz történő hozzáférés korlátozása VLAN-ok használatával
- A felügyeleti portok védelmének ellenőrzése
- Egyszerű vezetéknélküli hozzáférési pontok alkalmazása, amelyek nem tárolják helyben a biztonsági információkat
- A rongálások megelőzése a hozzáférési pontok fizikai elrejtésével és védelmével
- A külső épületek és helyszínek körül zajló gyanús tevékenységek megfigyelése

A fenti tényezők némelyike hatással van a hálózati tervre is; a hitelesítési kiszolgálók és VPN végpontok helye és típusa mellett például az egyszerű hozzáférési pontok választása is.

A WLAN-ok tervezésekor figyelembe veendő további szempontok:

- A vezetéknélküli berendezések biztonságos helyének meghatározása
- A WLAN-okhoz csatlakoztatott vezetékes hálózatok védelme

1.7 A WAN és a távmunkások támogatása

1.7.1 A vállalati határral kapcsolatos tervezési szempontok

A vállalati határ a hálózat azon része, ahol a vállalati hálózat külső hálózatokhoz kapcsolódik. A vállalati határon elhelyezett forgalomirányítók kapcsolják össze a telephely belső infrastruktúráját az internettel, és ezek biztosítják az összeköttetést a távoli WAN felhasználók és szolgáltatások felé. A vállalati határ tervezési szempontjai különböznek a telephelyi hálózatoknál használtaktól.

A sávszélesség költségei

A legtöbb telephelyi hálózat Ethernet technológiára épül, ugyanakkor a vállalati határ WAN kapcsolatait külső távközlési szolgáltatótól bérlik. Mivel az ilyen bérelt szolgáltatások sokba kerülhetnek, a WAN kapcsolatokhoz rendelkezésre álló sávszélesség gyakran lényegesen alacsonyabb a LAN-ban elérhetőnél.

QoS

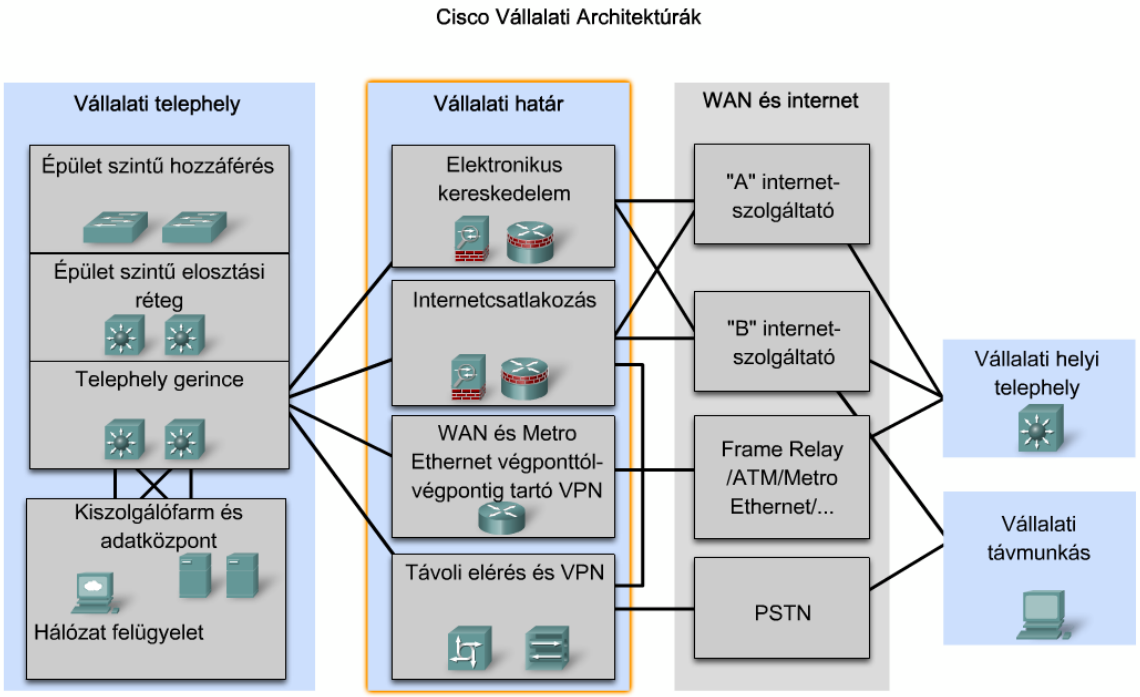
A LAN és a WAN közötti sávszélesség-különbség „üvegnyak-effektust” eredményezhet, amely arra kényszeríti határ-forgalomirányítókat, hogy az adatokat várakozási sorokba rendezzék. Az adatok sorba állításával kapcsolatos becslések és felügyeleti teendők szolgáltatásminőségi (QoS) stratégiát igényelnek. Ennek eredményeképp a WAN összeköttetések tervezése és kivitelezése bonyolult lehet.

Biztonság

Mivel a határ-forgalomirányítókon keresztül elért felhasználók és szolgáltatások nem mindig ismertek, a vállalati határ biztonsági követelményei kulcsfontosságúak. A telephely belső hálózatának a potenciális veszélyektől történő megóvásához behatolás-érzékelést és állapot alapú tűzfalat (stateful firewall) kell alkalmazni.

Távoli elérés

Számos esetben ki kell terjeszteni a telephelyi LAN szolgáltatásait a vállalati határon kívül eső távoli irodákba vagy távmunkásokhoz. Az ilyen típusú hozzáférés követelményei különböznek az internet felől érkező felhasználók számára biztosított nyilvános LAN hozzáférés szintjétől.



1.7.2 Távoli telephelyek integrálása a hálózati tervbe

Egy fiókirodákat és távmunkásokat támogató hálózat megtervezéséhez a hálózattervezőnek ismernie kell a különféle WAN technológiák képességeit. A hagyományos WAN technológiák közé tartoznak az alábbiak:

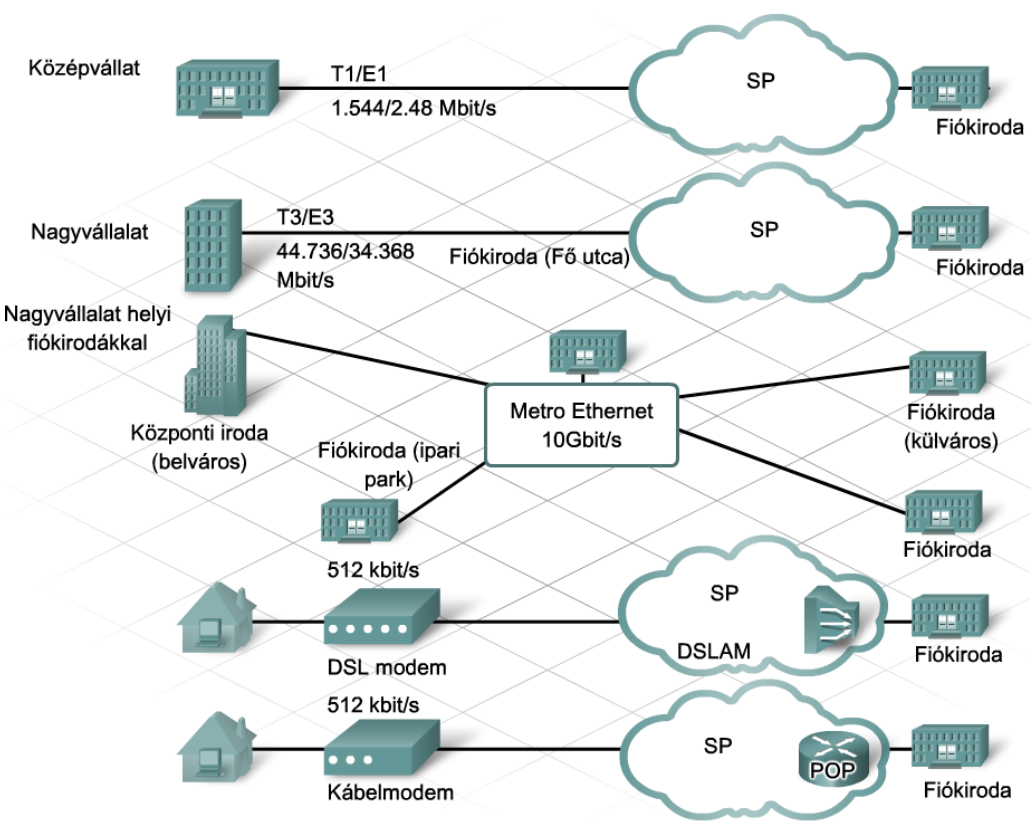
- bérelt vonalak
- vonalkapcsolt hálózatok
- csomagkapcsolt (pl. Frame Relay) hálózatok
- cellakapcsolt (pl. aszinkron átviteli módú – ATM) hálózatok

Sok helyen már az alábbiakhoz hasonló, újabb WAN technológiák állnak rendelkezésre:

- Digitális Előfizetői Vonal (DSL)
- Metro Ethernet
- Kábelmodem
- Nagy távolságú vezeték nélküli techológia
- Többprotokollos címkekapcsolás (MPLS)

A legtöbb WAN vonalat havidíj ellenében távközlési szolgáltatótól bérlik. A távolság függvényében az ilyen típusú összeköttetés meglehetősen sokba kerülhetnek. A WAN szerződések gyakran tartalmaznak egy szolgáltatói szerződést (SLA), amely garantálja a szolgáltató által nyújtott szolgáltatási szintet. A szolgáltatói szerződés támogatja az olyan kritikus üzleti alkalmazásokat,

mint például az IP-telefonálást vagy a távoli helyszínekre történő nagy sebességű tranzakció-feldolgozást.



Számos olyan cég van, ahol nem minden alkalmazott dolgozik a központi telephelyen. A máshol dolgozó alkalmazottak közé tartoznak az alábbiak:

- távmunkások
- folyamatosan mozgásban lévő dolgozók
- fiókirodai alkalmazottak

A távmunkások általában heti egy vagy több napot dolgoznak otthonról vagy más helyszínről. A folyamatosan mozgásban lévő dolgozók állandóan utaznak, vagy az ügyfelek telephelyére vannak kirendelve. Az alkalmazottak némelyike kis fiókirodákban dolgozik. A fenti esetek bármelyike is áll fenn, az alkalmazottaknak el kell tudniuk érni a vállalati hálózatot. Ahogy az internet egyre nőtt, a vállalatok egyre inkább felfedezték a saját hálózataik kiterjesztésének lehetőségét.

A virtuális magánhálózatok

Az interneten keresztül létrehozott virtuális magánhálózat (VPN) rendkívül népszerű kapcsolódási forma, különösen a távmunkások körében. A VPN olyan magánhálózat, amely egy nyilvános hálózat segítségével köt össze telephelyeket vagy felhasználókat egymással. Dedikált, valós kapcsolt (pl. bérelt vonal) helyett a VPN az interneten keresztül irányított virtuális kapcsolatokat használ a vállalat belső hálózata és a távoli forgalomirányító vagy PC között.

1.7.3 Redundancia és tartalék összeköttetések

Redundáns összeköttetések

A redundancia nélkülözhetetlen a WAN összeköttetéseknél, és életbevágóan fontos a távoli telephelyekkel és felhasználókkal történő megbízható kapcsolattartáshoz.

Az üzleti alkalmazások némelyike megköveteli, hogy minden csomag időben legyen kézbesítve. Az ilyen alkalmazások számára nem elfogadható, ha a kapcsolat néha megszakad. A WAN és a külső hálózatok által biztosított redundancia garantálja a magas rendelkezésre állást a végpontok közötti alkalmazások számára.

A WAN számára a tartalék összeköttetések biztosítják a szükséges redundanciát. A tartalék összeköttetések gyakran az elsődleges kapcsolattól eltérő technológiát alkalmaznak, így egy esetleges hiba nem feltétlenül hat ki a tartalék rendszerre.

Egy, a távoli telephelyekkel pont-pont WAN összeköttetést használó vállalat tartalék stratégiaként alkalmazhat például interneten keresztül létrehozott VPN-eket a redundancia biztosításához. Egy esetleges WAN hiba esetén a DSL, ISDN és betárcsázós modemek további lehetőséget kínálnak a tartalék összeköttetések biztosításához. Habár a tartalék összeköttetések rendszerint lassabbak az elsődleges kapcsolatoknál, beállítható, hogy kizárólag a magas prioritású adatokat és tranzakciókat továbbítsák.

Terheléselosztás

A tartalék stratégián felül a WAN összeköttetések további sávszélességet biztosíthatnak terheléselosztás segítségével. Beállítható, hogy a tartalék összeköttetés állandóan vagy csak csúcsidőben biztosítson további sávszélességet.

1.8 A fejezet összefoglalása

- A jó hálózat nem magától jön létre, hanem olyan hálózattervezők és technikusok kemény munkájának eredménye, akik a hálózati igények meghatározását követően kiválasztják a vállalat szükségleteinek leginkább megfelelő megoldásokat.
- A hálózattervezés négy alapvető műszaki feltétele: bővíthetőség, rendelkezésre állás, biztonság, felügyelhetőség.
- A Cisco nagyvállalati architektúra (Cisco Enterprise Architecture) használatával a három rétegből álló hierarchikus terv további moduláris részekre tagolható, ahol az egyes modulok eltérő fizikai vagy logikai összeköttetéssel rendelkező területeket jelképeznek.
- A nagyméretű hálózattervezési munkák normál esetben három különálló lépésre tagolhatók:
  1. lépés: A hálózati igények meghatározása
  2. lépés: A meglévő hálózat feltérképezése
  3. lépés: A hálózati topológia és a megoldások megtervezése
- A hálózatfejlesztési projekt nagyságrendjére vonatkozó helytelen becslés nagymértékben megnövelheti az új terv megvalósításának költségét és idejét.
- A központi réteg tervére vonatkozó célok között szerepel:
  - 100%-os rendelkezésre állás biztosítása

    - Az átviteli teljesítmény maximalizálása
    - A hálózat növekedésének elősegítése
- A központi réteg redundanciája lehetővé teszi, hogy a hálózat egy eszköz vagy kapcsolat meghibásodása esetén is tovább működjön.
- Harmadik rétegbeli eszközöket, a többrétegű kapcsolókat is ideértve, általában a hálózat központi rétegében használnak.
- A legtöbb hálózat központi rétege teljes vagy részleges háló topológia szerint van kábelezve.
- A központi rétegbeli eszközök általában redundáns tápellátással és üzem közben cserélhető összetevőkkel rendelkeznek.
- A központi réteg esetében a megfelelő választás az OSPF-hez és az EIGRP-hez hasonló, gyorsan konvergáló irányítóprotokollok használata.
- Az elosztási réteg irányítási határt képez a hozzáférési és a központi réteg között.
- Az elosztási réteggel kapcsolatos tervezési célok:
    - Az adatfolyamok szűrése és felügyelete
    - Hozzáférés-vezérlési irányelvek érvényesítése
    - Útvonal-összevonás, mielőtt az útvonalak hirdetése megtörténne a központi réteg felé
    - A központi réteg elszigetelése az elérési rétegben bekövetkező meghibásodásoktól és zavaroktól
    - Az elérési réteg VLAN-jai közötti forgalomirányítás
- A hierarchikus tervezési modell szerint a legegyszerűbb és legolcsóbb megoldás a hibatartomány méretének az elosztási rétegben történő beállitása.
- Az elosztási réteg redundanciája teszi lehetővé, hogy a hibatartomány kisméretű maradjon.
- Amíg az STP nincs engedélyezve, a 2. rétegbeli kapcsolók felé biztosított többszörös kapcsolat instabil viselkedést eredményezhet.
- A hálózati forgalom szűréséhez a forgalomirányító minden csomagot megvizsgál, majd az ACL-ben meghatározott feltételek alapján továbbítja vagy törli azt. A döntés az alábbi feltételek alapján történhet:
    - a forráscím
    - a célcím
    - a protokollok
    - a felsőbb rétegbeli portszámok
    - a csomag egy már felépült TCP adatfolyam része-e
- Az elérési réteg alapvető összeköttetéseinek biztosításán felül a tervezőnek az alábbi szempontokat is figyelembe kell vennie:
    - elnevezési struktúrák
    - VLAN architektúra
    - forgalmi minták
    - prioritással kapcsolatos stratégiák
- Ma az Ethernet hálózatok csillag topológiát használnak, amelyet kerékküllő topológiának is nevezünk.

- A hálózat hozzáférési rétegében a VLAN-ok és az IP alhálózatok alkalmazása a leggyakrabban használt eljárás a felhasználói csoportok és azok forgalmának egymástól történő elhatárolására.
- A hálózat számára olyan mechanizmusok is szükségesek, amelyekkel megnövekedett forgalom esetén vezérelheti torlódásokat.
- Torlódást az okozhat, amikor a hálózati erőforrásokra vonatkozó igények meghaladják a rendelkezésre álló kapacitást.
- Az adatoknak a forrásnál vagy annak közelében történő osztályozása lehetővé teszi, hogy az adatokhoz a megfelelő prioritások legyenek rendelve, ahogy keresztülhaladnak a teljes hálózaton.
- A hálózati eszközök némelyikén (pl.: forgalomirányítókon és kapcsolókon) a fizikai hozzáférés lehetőséget biztosít a jelszavak megváltoztatására, valamint az eszközökhöz való teljes hozzáférés megszerzésére.

2. A hálózati igények összegyűjtése

Ebben a fejezetben bemutatásra kerül a sportlétesítményeket kezelő Stadion Kht., amely egy nagyváros külterületén található stadiont kezel. A Stadion Kht. meglévő számítógépes hálózata fejlesztésre szorul, hogy modern szolgáltatásokat nyújtson. Ennek megvalósításához a Stadion Kht. vezetősége egy három lépésből álló projektet vázol fel. Első lépésben a Stadion Kht. szerződést köt a Hálózat Kft.-vel, amely a Cisco helyi üzleti partnere, és megbízást ad a hálózat tervezési dokumentációjának előkészítésére. A második lépésben a stadion vezetősége a részletes hálózati terv elkészítéséről szóló szerződés megkötését tervezi. Mihelyt a terv elkészült, a harmadik lépésben megtörténik a továbbfejlesztett hálózat beüzemelése és megvalósítása.

A Stadion Kht. jelenleg egy közeli nagyvárosban található filmkészítő céggel, a Film Rt.-vel is tárgyalásokat folytat egy szerződésről. A Film Rt. feladata a stadion weboldaláról letölthető jó minőségű videók készítése, filmezése és leszállítása. A Stadion Kht. vezetőségének további elvárása a Film Rt.-vel szemben, hogy a stadionban megrendezett sportesemények és koncertek élő közvetítését lehetővé tegye.

Ön a Hálózat Kft. gyakornokaként el fogja sajátítani a Stadion Kht. hálózatfejlesztési tervének elkészítéséhez szükséges készségeket. Az új tervezési készségei lehetővé teszik, hogy segítsen a Hálózat Kft. csapatának megtervezni a Film Rt. kisebb hálózatának bővítését. A feladat során elvégzett hálózattervezési portfólió lehetővé teszi, hogy kidolgozza és bemutassa a Film Rt. vezetősége számára készített hálózatbővítési tervét.

A Stadion Kht.-hez kapcsolódó tervezési projekt általában a törzsszövegben, a médiatartalmakban és a PT feladatokban szerepel. A Film Rt.-hez kapcsolódó tervezési projekt pedig a laborgyakorlatok során valósul meg.

2.1 A Cisco életciklus szolgáltatások bevezetése

2.1.1 A hálózat életciklusa

A hálózati világ folyamatosan fejlődik, már nem csupán számítógépek összekapcsolását jelenti. A hálózatkezelés ma már intelligens folyamat, amely kulcsfontosságú szerepet játszik az üzleti teljesítmény javításának elősegítésében. A vállalatok szívesen bővítik a hálózataikat, hisz a technológia vívmányainak kihasználásával új szolgáltatásokat vezethetnek be, és növelhetik a termelékenységüket.

A Cisco életciklus-szolgáltatás (Cisco Lifecycle Service)

A Cisco életciklus-szolgáltatást a fejlődő hálózatok támogatására tervezték. Ez egy hat szakaszból álló megközelítésmód, melynek minden szakaszához definiáltak a Cisco technológiák sikeres kiépítéséhez és üzemeltetéséhez szükséges tevékenységek. Emellett azt is részletezi, hogy a hálózat teljes életciklusa során miként lehet annak teljesítményét optimális szinten tartani.

A Cisco életciklus-szolgáltatás hat szakasza:

- Az előkészítési szakasz (Prepare Phase)
- A fejlesztési terv készítésének szakasza (Plan Phase)
- A műszaki terv készítésének szakasza (Design Phase)
- A megvalósítási szakasz (Implement Phase)
- Az üzemeltetési szakasz (Operate Phase)
- Az optimalizációs szakasz (Optimize Phase)

A fenti folyamatra gyakran a PPDIOO betűszóval hivatkoznak, amely az egyes szakaszok angol elnevezéseinek kezdőbetűin alapul.

Az előkészítési szakasz

A szervezetek az életciklus előkészítési szakaszában készítik el a hálózat továbbfejlesztésére vonatkozó üzleti tervet, amely tartalmazza, hogy a hálózat miként segítheti a szervezet céljait, valamint az új technológiák és szolgáltatásának üzleti alapját. Az előkészítési szakasz a tervezett architektúrára vonatkozó üzleti terv kiértékelésével igazolhatja a hálózati stratégia üzleti megalapozottságát.

A fejlesztési terv készítésének szakasza

A fejlesztési terv készítésének részét képezi a kezdeti hálózati igények meghatározása a célok, telephelyek, felhasználói igények és egyéb tényezők alapján. Ide tartozik továbbá a telephelyek jellemzőinek meghatározása és a meglévő hálózatok felmérése, valamint az eltéréselemzés elvégzése, melynek során kiderül, hogy a meglévő rendszer infrastruktúrája, a telephelyek és a működési környezet alkalmas-e a tervezett rendszer támogatására. A projektterv hasznos segítség a feladatok, felelősségek, kulcsfontosságú mérföldkövek és a hálózati változtatásokhoz szükséges erőforrások kezelésében. A projekttervnek összhangban kell lennie az eredeti üzleti igényekben meghatározott nagyságrenddel, költségekkel és erőforrásokkal.

A műszaki terv készítésének szakasza

A hálózattervező szakemberek munkáját a fejlesztési terv készítésének szakaszából származó kiindulási feltételek határozzák meg. A hálózat műszaki terve egy olyan átfogó és részletes terv, amely eleget tesz a jelenlegi üzleti és műszaki feltételeknek. A specifikációban szerepel a méretezhetőség, rendelkezésre állás, biztonság és felügyelhetőség támogatása. Ez a specifikáció lesz a megvalósítás alapja.

A megvalósítási szakasz

A megvalósítás (és az ellenőrzés) a műszaki terv elfogadása után kezdődik. A műszaki tervnek megfelelően történik a hálózat kiépítése vagy az új összetevők beépítése. A cél az, hogy az eszközök beépítése a meglévő hálózat megzavarása és sebezhetőségek létrehozása nélkül történjen.

Az üzemeltetési szakasz

Az üzemeltetés a terv megfelelőségének végső vizsgálata. Az üzemeltetési szakasz részét képezi a hálózat napi szinten végzett műveletekkel történő karbantartása, beleértve a magas rendelkezésre állás biztosítását és a költségek csökkentését. A napi szinten végzett hibakeresés és -elhárítás, valamint a teljesítmény nyomon követése adja a kiindulási adatokat az optimalizációs szakasz számára.

Az optimalizációs szakasz

Az optimalizációs szakasz részét képezi a hálózat előrelátó (proaktív) felügyelete. A proaktív felügyelet célja, hogy a problémákat még a szervezetre kifejtett hatásuk előtt meghatározza és megszü A PPDIOO folyamat során az optimalizációs szakaszban felmerülhet a hálózat újratervezésének javaslata. Az újratervezés akkor válhat szükségessé, ha túl sok hálózati probléma és meghibásodás fordul elő, a teljesítmény elmarad a várakozásoktól vagy csak új alkalmazásokkal biztosíthatók a szervezeti és műszaki feltételek.

Esettanulmány: Egy sportstadion hálózata

Egy stadion vezetősége a Hálózat Kft-t bízta meg hálózatának felújításával és fejlesztésével. Az évek során a stadion hálózata egyre nőtt, viszont nem nagyon gondolták át az általános üzleti célokat, és az infrastruktúra tervezésére sem fordítottak gondot. Néhány új projektbe ugyan belefogtak, de a hálózati rendszergazdák ténylegesen nem ismerték az ilyen fejlett és az üzletmenet szempontjából kritikus hálózat sávszélesség-, forgalmi prioritáskezelés- és egyéb követelményeit. A stadion vezetősége most további új, fejlett technológiájú funkciók bevezetését tervezi, de ezek támogatását a meglévő hálózat már nem képes biztosítani.

A hálózat életciklusának szakaszai

A Hálózat Kft. képviselői találkoznak a stadion vezetőségével, hogy megvitassák az új hálózat megtervezéséhez általuk javasolt folyamatot. Habár a tervezési szakasz csupán egy a hálózat életciklusának szakaszai közül, mégis az összes PPDIOO szakasz kihat a tervezési döntésekre.

Az előkészítési és a fejlesztési terv készítésének szakaszában a hálózattervezők és a stadion vezetősége meghatározzák az üzleti célokat, és a stadion szervezeti felépítését szolgáló műszaki feltételeket, csakúgy, mint a tervezési megszorításokat.

Az igényeknek a fenti szakaszokban történő összegyűjtése hatással van a tervezési szakaszban meghozott döntésekre. A megvalósítási szakasz a terv jóváhagyása után kezdődik, és az új tervnek a meglévő hálózatba történő integrációját foglalja magában.

Az üzemeltetési és az optimalizációs szakaszban a stadion munkatársai elemzik és figyelemmel kísérik a hálózat teljesítményét.

2.1.2 A hálózat életciklusának előkészítési szakasza

Az előkészítési szakasz

Az előkészítési szakasz során a stadion vezetősége és a Hálózat Kft. munkatársai az alábbi üzleti célokat határozzák meg:

- az ügyfél elégedettségének növelése
- a költségek csökkentése
- új szolgáltatások bevezetése
- a szervezet növekedésének támogatása

A fenti célkitűzések adják az üzleti terv alapját. Az üzleti terv a technológiai változtatásokba történő befektetetés szükségességét hivatott igazolni. A vállalat mérlegeli az esetleges üzleti korlátokat pl. a keretösszeg, a személyi állomány, a cégpolitika és az ütemezés vonatkozásában.

Az üzleti terv elfogadását követően a Hálózat Kft. munkatársai segítséget nyújtanak a magas szintű műszaki stratégia és megoldás kifejlesztésében.

A fenti stratégia meghatározza:

- az új hálózati megoldást támogató fejlett technológiákat
- a jelenlegi és a tervezett hálózati alkalmazásokat és szolgáltatásokat, valamint az üzleti célok alapján ezek prioritásait
- a műszaki megoldás üzemeltetésének és felügyeletének támogatásához szükséges személyeket, folyamatokat és eszközöket

Az előkészítési szakasz jellemzően még azelőtt befejeződik, hogy a vállalat kibocsátaná az ajánlatok (Request For Proposal, RFP), illetve az árajánlatok (Request For Quotation, RFQ) bekérésére vonatkozó dokumentumokat. Az RFP és az RFQ ismerteti az új hálózatra vonatkozó követelményeket, valamint a vállalat hálózati technológiák beszerzésére és beüzemelésére vonatkozó ügymenetét.

A projekt célja:

- A projekt milyen módon illeszkedik a vállalat üzleti céljaihoz
- Fő előnyök és veszélyek
- A siker mércéi

Költség/hozadék elemzés:

- Az üzleti célok megvalósításának lehetőségei
- Nem pénzügyi előnyök

Erőforrás-kezelési lehetőségek:

- A szolgáltatásokhoz szükséges források (külső gyártók, hálózattelepítő cégek, stb.)
- Beszerzési folyamatok

Költségkalkuláció

- A projekt egészének megfizethetősége, valamint a (belső és külső) források egyszerre vagy hosszabb idő alatt történő előteremtése

Projektvezetés

- Projektterv és -szerepek
- Ütemterv
- Főbb veszélyek és a következményeket minimalizáló terv
- Vészforgatókönyv, ha a projekt nem valósul meg
- A készségekre és a személyzetre vonatkozó követelmények

2.1.3 A hálózat életciklusának a fejlesztési terv készítésével foglalkozó szakasza

A fejlesztési terv elkészítésének szakasza

A fejlesztési terv készítésének szakaszában a hálózattervező átfogó, a helyszínt és a működési menetet vizsgáló felmérést végez, amely a meglévő hálózati-, működési- és hálózatfelügyeleti infrastruktúrát értékeli.

A Hálózat Kft. munkatársai meghatározzák az összes fizikai, környezeti és villamossági változtatást, valamint felmérik, hogy a jelenlegi működési és hálózatfelügyeleti infrastruktúra képes-e az új műszaki megoldás kiszolgálására. Az infrastruktúrára, a személyi állományra, a folyamatokra és az eszközökre vonatkozó összes változtatást végre kell hajtani az új műszaki megoldás megvalósítása előtt.

Az olyan egyedi alkalmazásokat, amelyek növelik az új hálózat jellemzőire és működési módjára vonatkozó követelményeket, szintén ebben a szakaszban kell meghatározni. A Hálózat Kft. munkatársai elkészítik az összes tervezési követelményt tartalmazó dokumentumot.

A projektterv

Ebben a szakaszban a Hálózat Kft. munkatársai és a stadion vezetősége készítenek egy, a projekt felügyeletét segítő tervet. A projektterv tartalmazza:

- a feladatokat
- az ütemtervet és a kritikus mérföldköveket
- a kockázatokat és a megszorításokat
- a felelősségi köröket
- a szükséges erőforrásokat

A tervnek az eredeti üzleti célkitűzésekben rögzített kereteken, költség- és erőforráskorlátokon belül kell maradnia. A projekt felügyeletére a stadion vezetősége és a Hálózat Kft. is kijelöl egy-egy személyt.

Példák a felmérendő területekre

Környezeti:

- *Lehetséges elektromos problémák*
- *A tartókerettel/huzalozási központtal kapcsolatban felmerülő helyproblémák*
- *A szünetmentes tápegység és a tartalék-tápellátás gondjai*
- *Az elektromos hálózat további berendezésekkel járó problémái*
- *A megfelelő kábelezési infrastruktúra*

Személyzeti:

- *A tervezett fejlesztés elvégzéséhez szükséges számú személyzet*
- *A személyzet műszaki tudásszintje megfelelő vagy képezni kell őket*

2.1.4 A hálózat életciklusának a műszaki terv készítésével foglalkozó szakasza

A műszaki terv készítésének szakasza

A műszaki terv készítésének szakaszában a Hálózat Kft. munkatársai a fejlesztési terv készítésének szakasza során meghatározott kiindulási követelményeket használják fel a munkájukhoz.

A tervezési követelményeket tartalmazó dokumentum támogatja az előkészítési és a fejlesztési terv készítésének szakaszában meghatározott specifikációkat:

- a rendelkezésre állással
- a bővíthetőséggel
- a biztonsággal
- a felügyelhetőséggel kapcsolatban.

A tervnek kellően rugalmasnak kell lennie ahhoz, hogy a felmerülő új célkitűzések vagy igények esetén változtatásokat vagy bővítéseket tegyen lehetővé. A technológiát harmonizálni kell a meglévő működési és hálózatfelügyeleti infrastruktúrával.

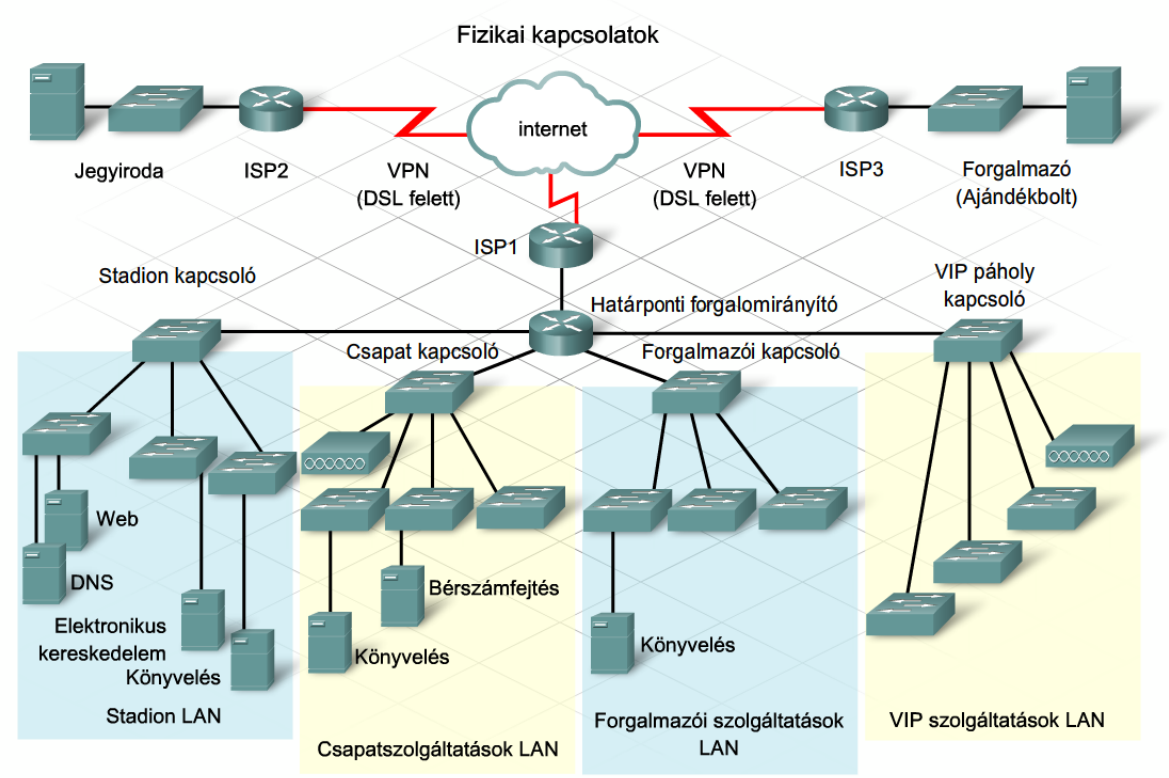
Az üzembe helyezés megtervezése

A tervezési szakasz végén a hálózattervező olyan terveket készít, amelyek útmutatóul szolgálnak az üzembe helyezés során, valamint biztosítják, hogy a végeredmény megegyezzen az ügyfél elvárásaival. A tervek az alábbiakat tartalmazzák:

- A kapcsolatok beállítása és ellenőrzése
- A tervezett rendszer megvalósítása
- A hálózat működőképességének bemutatása
- A hálózati alkalmazások lecserélése
- A hálózat működésének ellenőrzése
- A végfelhasználók és a karbantartó személyzet képzése

A stadion hálózatának fejlesztése során a tervezési szakaszban készül el a hálózat végleges terve. Ekkorra már az összes új berendezést és technológiát meg kell határozni, ellenőrzésüket el kell

végezni. A felvázolt terv áttekintése során kiderül, hogy az teljesíti-e az üzleti célokat. Elkészül a végső változat, amellyel tovább lehet lépni a hálózat fejlesztésének megvalósítási szakaszába.



2.1.5 A hálózati életciklus megvalósítási szakasza

A megvalósítási szakasz

A megvalósítási szakasz azután kezdődik, miután a Hálózat Kft. elkészült a végleges tervvel, és az ügyfél jóváhagyta azt. A hálózat kiépítése a jóváhagyott tervspecifikációnak megfelelően történik. A megvalósítási szakasz során derül ki, hogy a hálózati terv sikerre vagy kudarcra van-e ítélve.

Az új hálózat ellenőrzése

Az új hálózat egészének vagy egy részének meghatározott körülmények közötti ellenőrzése még a tényleges üzembe helyezés előtt segít a megvalósítási problémák meghatározásában és megoldásában.

A problémák megoldását követően a Hálózat Kft. munkatársai üzembe helyezik az új megoldást, és integrálják azt a meglévő hálózatba. Az üzembe helyezést követően további tesztek végrehajtása szükséges.

A rendszer-szintű átvételi vizsgálat ellenőrzi, hogy az új hálózat megfelel-e az üzleti céloknak és a tervezési követelményeknek. Ennek eredményeit rögzítik, és azok az ügyfélnek átadott dokumentáció részét fogják képezni. A stadion munkatársait érintő bármely képzésnek ebben a szakaszban le kell zárulnia.

2.1.6 A hálózat életciklusának üzemeltetési szakasza

Az üzemeltetési szakasz

Az üzemeltetési és az optimalizációs szakasz folyamatos, a hálózat napi műveleteit jelenti. A stadion munkatársai figyelemmel kísérik a hálózat működését, és méréssel meghatározott működési jellemzők segítségével létrehozzák a hálózat viszonyítási alapját (referencia). Ez segít abban, hogy a vállalat elérje a maximális bővíthetőséget, rendelkezésre állást, biztonságot és felügyelhetőséget.

Az új hálózat üzembe helyezését követően a stadion munkatársai felügyelik a hálózatot abból a célból, hogy az az előkészítési és a fejlesztési terv készítésének szakaszában körvonalazott tervspecifikációnak megfelelően teljesítsen.

Az irányelvek és az eljárások meghatározása

Az irányelvek és az eljárások az alábbi hálózati problémák kezeléséhez szükségesek:

- Biztonsági problémák
- Konfigurációs változtatások
- Berendezések beszerzése

A leállási idő, a működési költségek és a változtatásokkal kapcsolatos problémák száma csökkenthető, ha az irányelveket és az eljárásokat a fejlesztési folyamatot követően felülvizsgálják és módosítják. Amennyiben ilyen irányelvek és eljárások nincsenek rögzítve, létre kell hozni azokat!

2.1.7 A hálózat életciklusának optimalizációs szakasza

Az optimalizációs szakasz

A hálózat optimalizálása folyamatos, célja a hálózat teljesítményének és megbízhatóságának növelése. Ehhez a potenciális hálózati problémákat még a bekövetkezésük előtt meg kell határozni és meg kell oldani. Ezzel biztosítható, hogy a vállalat üzleti céljai és követelményei teljesüljenek. Az optimalizációs szakaszban felfedezhető tipikus problémák közé tartoznak:

- az egyes összetevők jellemzői közötti inkompatibilitás
- az elégtelen sávszélesség
- az eszközök teljesítményproblémái több funkció egyidejű használatakor
- a protokollok hangolhatósága

Előfordulhat, hogy a megváltozott üzleti céloknak nem felel meg az éppen alkalmazott technológiai stratégia és működési modell. Ilyenkor szükség lehet az újratervezésre, és a PPDIOO ciklus újra kezdődik.

2.2 Az értékelési folyamatok magyarázata

2.2.1 Az ügyfél által kért ajánlatra, illetve árajánlatra adott válasz

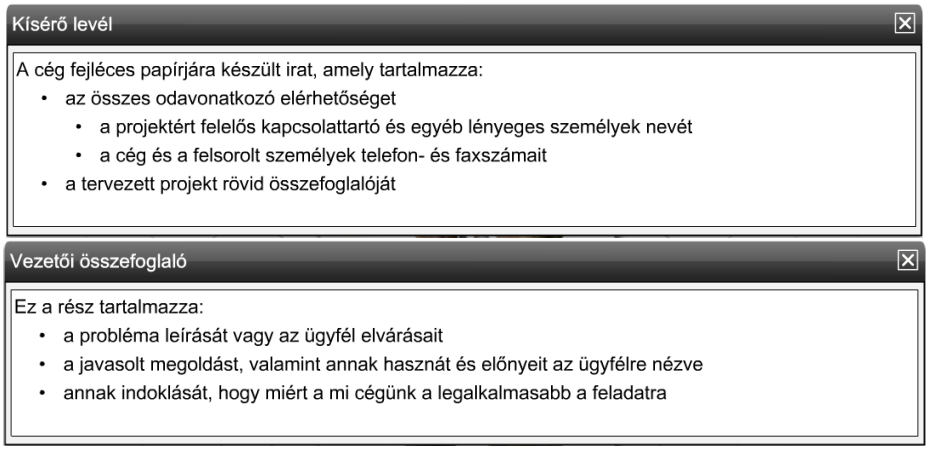
Amikor egy vállalat vagy szervezet úgy dönt, hogy továbbfejleszti vagy lecseréli a meglévő hálózatát, általában ajánlatokat (RFP) vagy árajánlatokat (RFQ) kérnek be. A PPDIOO modell szerint ez az előkészítési szakasz végén történik meg. Az RFP és az RFQ a potenciális kivitelezőktől várt ajánlatok formai és tartalmi követelményeit írja le. A kivitelező számára kulcsfontosságú, hogy a dokumentációban szereplő instrukciókat a lehető legpontosabban tartsa be. Az utasítások be nem tartása vagy a hiányosan benyújtott ajánlat ugyanis azt eredményezheti, hogy egy másik kivitelező nyeri meg a kiírást.

Az ajánlatra vonatkozó formai és tartalmi követelményeken kívül az RFP és az RFQ tartalmazza a betartandó ütemtervet is. A kiíró cég elutasíthatja a későn benyújtott ajánlatokat.

A kiírásra benyújtott ajánlat

Az ajánlatot tartalmazó dokumentum minden pontját a lehető legrészletesebben ki kell fejteni. Ha nincs külön jelölve, az ajánlat pontjait ugyanúgy kell számozni, mint a kiírás pontjait. Az ajánlatot mindig a célközönség szem előtt tartásával kell elkészíteni. A szakszavakat és szakkifejezéseket szükség esetén meg kell magyarázni.

Ahhoz, hogy az ajánlatot tartalmazó dokumentum könnyen követhető legyen, használjunk tartalomjegyzéket! Az anyag bemutatásához egy kísérőlevélre is szükség van.



Javasolt megoldás
Ez a rész tartalmazza, de nem csupán az alábbiakra korlátozódik:

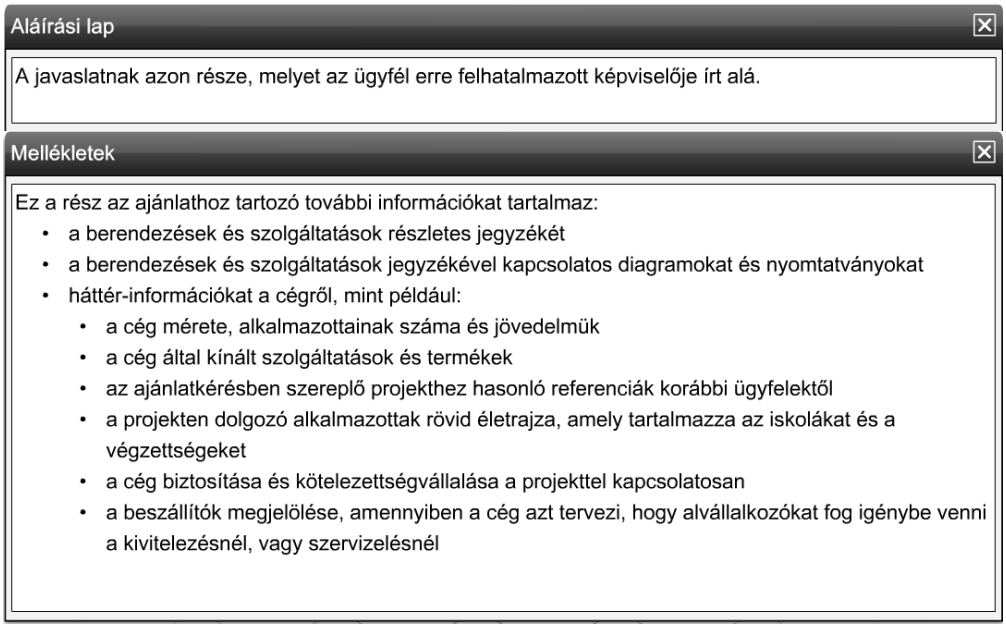
- a megoldás részletes kifejtését
- a projektet felügyelő csapatot és az ütemtervet (lehetőleg konkrét feladatokkal és dátumokkal)
  - az átmeneti időszak ütemezését
  - a helyszíni vagy távoli támogatás részleteit, a támogatás típusát és a rendelkezésre álló időt illetően
  - a jótállási információkat, amelyek meghatározzák:
  - azon elemeket, amelyekre a jótállás vonatkozik
  - a jótállási idő hosszát
  - a javítás és csere menetét
  - a válaszadási határidőt
  - az ismert problémákra vonatkozó javítási kötelezettséget
- leírást arról, hogy mi számít jelentős vagy jelentéktelen problémának

- a rendkívüli üzembe helyezés és válaszadás módjait katasztrófahelyzetben
- a cég feladatait az ISP-vel való kapcsolattartásra, illetve az ISP-vel kötött szolgáltatási szerződésre vonatkozóan
- a környezetet és a telephelyet érintő korszerűsítés feltételeit, illetve azok felelőseit
- a cég, a berendezések vagy a személyzet által az ügyfél telephelyén okozott kárral kapcsolatos összes feltételt és korlátozást

Javasolt ár

Ez a rész tartalmazhatja az alábbi felszámítható költségeket, de nem csak ezekre korlátozódik:

- szoftver- és alkalmazás-összetevők
- hardverösszetevők és azok interfészei
- a szükséges licencek
- díjak és engedélyezési költségek
- képzési díjak
- jótállási, karbantartási és támogatási költségek
- a projekten dolgozó személyek munkabérköltségei az óradíj vagy a projekt költsége szerint
- a felmerülő utazási költségek
- a távközlési szolgáltató változtatásokért és továbbfejlesztésekért felszámított díjai
- a munka elvégzéséhez szükséges konkrét eszközök és berendezések
- az eltávolítás és használaton kívül helyezés felmerülő költségei
- a megvalósításhoz használt villás-targonca vagy ahhoz hasonló berendezések bérleti díjai
- villanyszerelési költségek
- fizetési módok, beleértve a felmerülő lízinglehetőségeket
- az utolsó részlet kifizetése csak az átadás után



2.2.2 Az előkészítő megbeszélésen való részvétel

Az előkészítő tárgyalás

Az ügyfél még az ajánlatok benyújtásának határideje előtt szervezhet egy informális találkozót, amit előkészítő tárgyalásnak vagy az ajánlattételt megelőző konferenciának is neveznek. A találkozó célja, hogy biztosítsa:

- a projekt nagyságrendjének áttekintését
- az eredeti kiírásban nem szereplő információk és dokumentációk meghatározását
- az eredeti kiírásban nem szereplő formai és ütemezési részletek tisztázását.

A találkozó azt is lehetővé teszi, hogy a kivitelező megbecsülhesse a projekt iránt érdeklődő cégek számát. Amennyiben az előkészítő tárgyalásra nem kerül sor, a szükséges információkat és dokumentációt az RFP-ben kijelölt illetékestől lehet kérni.

2.2.3 Az ajánlatkérés (RFP)

Az RFP

A megrendelő általában elküldi az RFP egy-egy példányát a kivitelezőknek, de előfordul, hogy a cég weboldalára teszi ki azokat. A beérkezett ajánlatok segítségével az ügyfél összehasonlíthatja a különböző kivitelezők által kínált szolgáltatásokat, termékeket, árakat és támogatást.

Egy hálózati projekt RFP-je jellemzően az alábbiakat tartalmazza:

- A projekt üzleti céljai
- A projekt várható nagyságrendje
- A meglévő hálózattal és alkalmazásokkal kapcsolatos információk
- Az új hálózat követelményei
- Üzleti, műszaki vagy környezetvédelmi megszorítások
- A mérföldköveket és teljesítéseket tartalmazó előzetes ütemterv
- A szerződés jogi feltételei

Fontos, hogy az ajánlat az RFP-ben felsorolt összes elemre tartalmazzon választ, mert a kiíró cég elutasíthatja a hiányos anyagokat.

A Stadion Kht. ajánlatkérése

A pályázatok elfogadásának határideje: 200x. december 1. Az ajánlatok eljuttatása postán vagy személyesen történhet.

Küldjön el egy aláírt, eredeti példányt és egy másolatot az alábbi címre:

Szabó Úr
1234 Budapest, Bevásárlóközpont tér 1.
Település, irányítószám

Tárgy: Stadionfejlesztési projekt

További információért hívja a (99) 999-9999 számot!

Formai követelmények:

1. A cég fejléces papírjára készült borítónak tartalmaznia kell az összes odavonatkozó elérhetőséget, beleértve a kapcsolattartó nevét, a telefon- és faxszámait, valamint a tervezett projekt rövid összefoglalóját.

2. Az egyoldalas nyomtatással készült, egyszeres sortávolságú oldalakból álló anyagnak az alábbi részeket kell tartalmaznia:
   A. A végrehajtás összegzését tartalmazó rész
   B. A tervezett megoldás specifikációját tartalmazó rész
      - o Az üzleti célok
      - o A projekt nagyságrendje
      - o A tervezési követelmények
      - o A jelenlegi hálózat értékelése
      - o A logikai terv
      - o A fizikai terv
      - o A kivitelezési terv
      - o A megvalósíthatósági tanulmány

   C. A tervezett költségeket tartalmazó rész
   D. Aláírási oldal
   E. Mellékletek

3. A cég hátterét, elsődleges céljait és történetét is tartalmazó minősítések

4. Mellékletek (az alábbiak csatolása szükséges):
   - o Garanciák és biztosítási információk
   - o A legfrissebb üzleti eredmények, valamint a jelenlegi általános működési keret
   - o Ajánlólevelek az előző ügyfelektől

2.2.4 Az árajánlatkérés (RFQ)

Az RFQ

Amennyiben a projekt műszaki specifikációi már ismertek, a vállalatok az ajánlat helyett árajánlatot kérnek. Amennyiben a vállalat jól képzett hálózatüzemeltető személyzettel rendelkezik, a munkatársak maguk is kérhetnek árajánlatot a szükséges szolgáltatások és berendezések beszerzéséhez. Az árajánlatkérésre sokkal egyszerűbb válaszolni, mint egy normál ajánlatkérésre, mivel a kiírásnak megfelelő költségeket könnyebb meghatározni vagy megbecsülni.

Az RFQ tartalmát tekintve eltérő lehet, de általában három fő egységből áll. Az RFP-hez hasonlóan az RFQ esetében is lehetnek formai követelmények, a benyújtási határidőket pedig rendkívül szigorúan vehetik.

A benyújtott árajánlat esetében is érdemes az ajánlatok benyújtásánál alkalmazott irányelveket követni. Ahhoz, hogy biztosan mérlegeljék az árajánlatunkat, minden utasítást pontosan kövessünk, és az anyagot még a határidő lejárta előtt nyújtsuk be!

Szervezeti áttekintés

Az árajánlat ezen része háttérinformációkat tartalmaz az árajánlatot bekérő cégről, valamint belső információkat közöl a tervezett üzlet típusáról.

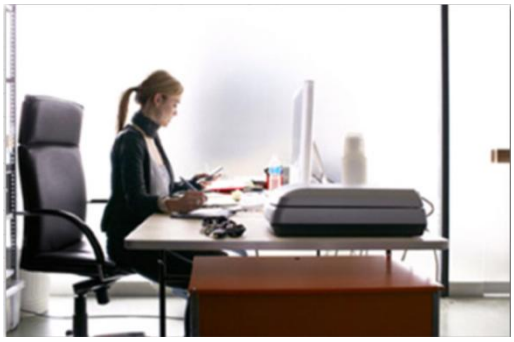
Elvárt teljesítések

Az árajánlat ezen része tartalmazza a projekt végtermékének leírását. Az árajánlatot bekérő cég például kereshet olyan partnert, amely elvégzi egy 1841-es forgalomirányító vagy ahhoz hasonló eszköz beüzemelését. Szükség esetén a teljesítések rész tartalmazza a szükséges eszközt és annak programozását (VLAN-ok, stb.).

Feltételezések/megállapodások

Ez a rész tartalmazza a projekt feltételeit, mint például a projekt költségvetését, a benyújtás időpontját, a cég által a kivitelező számára nyújtott támogatások típusait, a szolgáltatások és felhasznált anyagok jóváhagyásának folyamatát, stb. A bekért árajánlatra adott válaszával a kivitelező vagy a tervező elfogadja az ebben a részben szereplő feltételeket.

2.2.5 Az üzletkötő szerepe



Amikor a Hálózat Kft. megkapja a Stadion Kht. kiírását, az ajánlat elkészítését egy üzletkötőre bízzák. A Hálózat Kft. üzletkötőinek feladata a cég és az ügyfelek közötti folyamatos kapcsolattartás. A kapcsolat úgy indul, hogy az üzletkötő felkeresi a potenciális ügyfeleket, majd végighaladnak a PPDIOO hálózati életciklus összes szakaszán. A céges ügyfelek az üzletkötőjük ismereteire és szakértelmére támaszkodnak a hálózati követelmények meghatározásában. Az üzletkötő sikeréhez elengedhetetlen az ügyfél bizalmának elnyerése és megőrzése. A stadion projekttel

megbízott üzletkötő feladata a megfelelő üzleti kapcsolat kialakítása a Stadion Kht. és a Hálózat Kft. között.

Kommunikációs csatorna

A Hálózat Kft. részéről az üzletkötő fogja elsődlegesen tartani a kapcsolatot a stadion vezetőségével. A jó üzletkötő kiváló kommunikációs készséggel rendelkezik, és alaposan ismeri az ügyfél vállalatát. Az ügyfél igényeinek megfelelően személyes találkozók keretében, telefonbeszélgetéseken keresztül, e-mailben vagy ezek kombinációját használva tartja a kapcsolatot a stadion vezetőségével.

Az üzletkötő feladatai

Egyes cégeknél az üzletkötőknek egy adott terület vagy régió összes meglévő és potenciális ügyfelével, más cégek esetében csak bizonyos cégtípusokkal kell foglalkozniuk. Habár a konkrét teendők beosztásonként igencsak eltérőek lehetnek, a legtöbb üzletkötő feladata:

- a kitűzött értékesítési és bevételi célok elérése
- az új termékekkel és technológiákkal kapcsolatos információk eljuttatása az ügyfelekhez, illetve a potenciális ügyfelekhez
- a helyi értékesítési, szolgáltató és támogató csoportok irányítása
- az értékesítési és támogatási projektek megtervezése, valamint költségtervezetének elkészítése
- az ügyfél ajánlatokra, bemutatókra, árajánlatokra és információkra vonatkozó kéréseinek teljesítése
- értékesítési és szervizelési szerződések megkötése és megújítása

A Hálózat Kft. üzletkötőinek nem csupán az alapvető hálózati ismereteiket kell bizonyítaniuk, hanem ezen felül értékesítési és ügyfélkezelési képzésen is részt kell venniük.

2.2.6 Az értékesítési rendszermérnök szerepe

A Hálózat Kft. az értékesítés előtt és után egyaránt alkalmaz olyan műszaki munkatársakat, akik az üzletkötő munkáját segítve támogatást nyújtanak az ügyfelek számára.

Az értékesítési rendszermérnök

Az értékesítési rendszermérnök (esetenként értékesítés-támogató mérnöknek is nevezik) segít az üzletkötőnek és az ügyfélnek eldönteni, hogy milyen továbbfejlesztések, illetve

bővítések szükségesek az ügyfél hálózatán. Az üzletkötő az értékesítési rendszermérnök szakértelmére támaszkodik, hogy az új berendezések és szolgáltatások biztosan megfeleljenek az ügyfél hálózati igényeinek. A PPDIOO életciklusnak a fejlesztési terv, illetve a műszaki terv készítésével foglalkozó szakaszában az értékesítési rendszermérnök segít eldönteni, hogy megvalósíthatók-e a tervezett hálózati változtatások, és ha igen, milyen műszaki feltételekkel. Ezek a mérnökök, valamint a velük dolgozó hálózati szakemberek felelnek:

- az ügyfél meglévő hálózatának felméréséért, kiértékeléséért
- annak eldöntéséért, hogy a hálózat továbbfejlesztése vagy bővítése eleget tesz-e a műszaki feltételeknek
- azért, hogy a tervezett változtatásokat integrálni lehessen az ügyfél meglévő hálózatába
- a tervezett megoldások teszteléséért és kiértékeléséért

Az értékesítési rendszermérnök segít a hálózattervezőnek a meglévő hálózattal kapcsolatos, valamint a módosításokból eredő problémák meghatározásában. Egy hálózat továbbfejlesztése vagy üzembe helyezése szempontjából kulcsfontosságú a problémák korai felismerése és megoldása. Az értékesítési rendszermérnök kulcsszerepet játszik az ügyfél ajánlatkérésére benyújtott dokumentum elkészítésében.

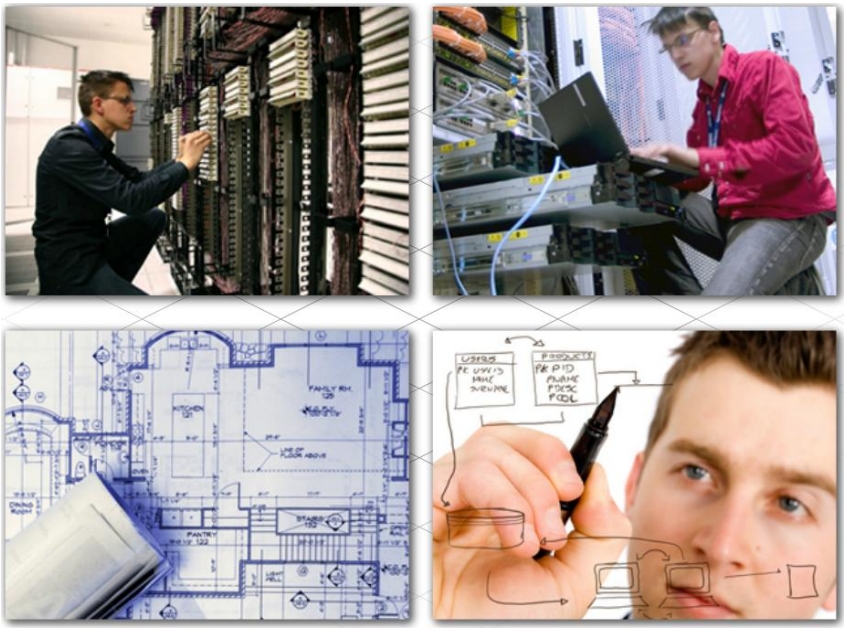
Az értékesítési rendszermérnököktől elvárják a hálózattervezési és hálózattechnológiai kurzusok elvégzését, de vannak olyan helyek, ahol a hálózattervezési minősítést is meg kell szerezniük. Ilyen például a Cisco Certified Design Associate (CCDA) minősítés.

2.2.7 A hálózattervező szerepe

A hálózattervezőnek átfogó ismeretekkel kell rendelkeznie a hálózati technológiák és berendezések összes típusát, illetve ezek képességeit illetően. Ezen képességek teszik lehetővé a tervező számára, hogy a hálózati terv skálázhatóság, rendelkezésre állás, biztonság és felügyelhetőség szempontjából is megfeleljen az ügyfél igényeinek. A tervező a PPDIOO hálózati életciklusnak a fejlesztési terv és a műszaki terv készítésével foglalkozó szakaszában is érintett. Kisebb vállalatoknál előfordulhat, hogy az értékesítési rendszermérnök a hálózattervező feladatát is ellátja, a nagyobb cégeknél viszont akár egy hálózattervezőkből álló csapat is dolgozhat egyetlen projekten. Ebben a tananyagban egyetlen hálózattervezőt feltételezünk.

Egy jó hálózat tervező fordít időt arra, hogy tanulmányozza az ügyfél tevékenységét a hálózati követelmények biztosítása végett. Ennek segítségével felkészülhet a vállalat növekedése, vagy egyre sikeresebbé válása során esetleg bekövetkező változásokra. A tervező feladatai:

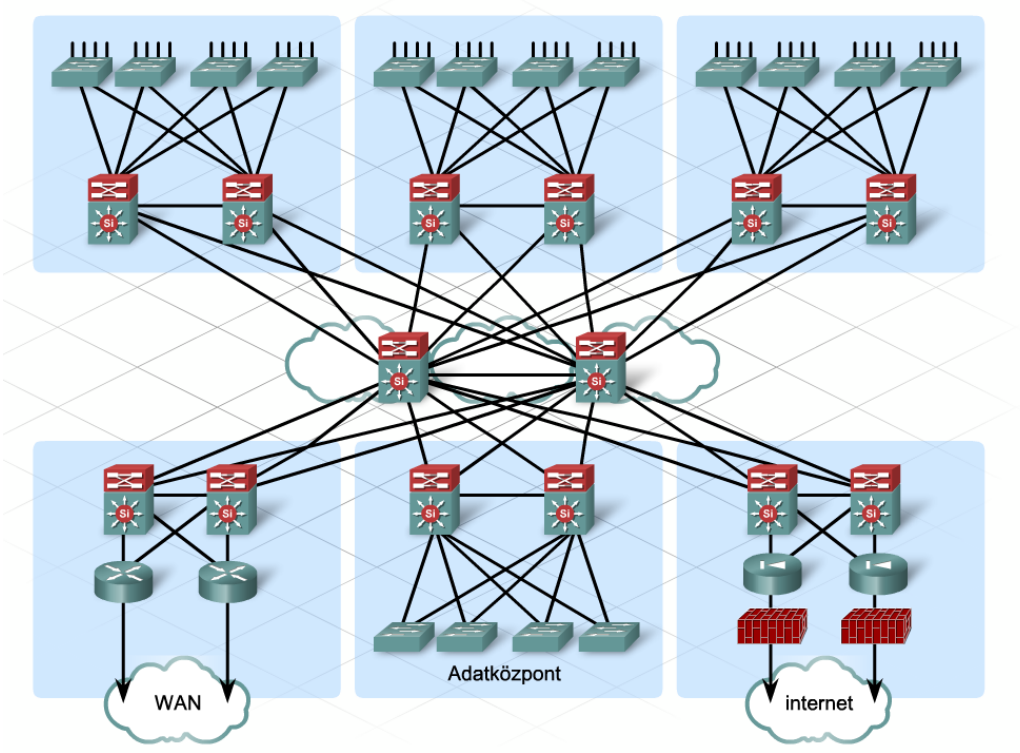
- Az ügyfél céljainak és kötöttségeinek elemzése az új terv műszaki feltételeinek meghatározásához
- Az üzemben lévő hálózat kiértékelése
- A megadott hálózati követelményeknek eleget tevő technológiák és berendezések kiválasztása
- A különféle hálózati eszközök és szolgáltatások elhelyezkedésének és összekapcsolódásának grafikus ábrázolása
- Az elméletet igazoló ellenőrzés megtervezése és felügyelete
- Segítségnyújtás az üzletkötőnek az ügyfél számára készülő bemutató összeállításában



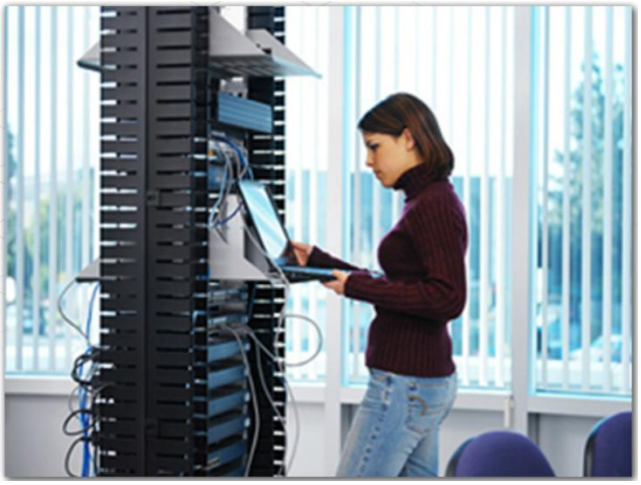
A Hálózat Kft. tervezőcsapata magasan képzett hálózati szakemberekből áll. A hálózattervezőnek naprakésznek kell lennie a technológiákat és az új tervezési eljárásokat illetően egyaránt.

A tervezőtől a műszaki hálózatkezelési szakmai minősítéseken kívül a hálózattervezési minősítések megszerzését is elvárják.

A stadion továbbfejlesztésével megbízott tervező Cisco Certified Design Professional (CCDP) minősítéssel rendelkezik. Egy ilyen komoly minősítés megszerzésével a tervező bizonyította, hogy rendelkezik a Stadion Kht. összetett hálózatának megtervezéséhez szükséges kompetenciákkal.



2.2.8 A rendszertámogató mérnök szerepe



A PPDIOO hálózati életciklus megvalósítási, üzemeltetési és optimalizációs szakaszában a rendszertámogató mérnök (esetenként műszaki támogató mérnöknek is nevezik) veszi át a műszaki segítségnyújtás feladatait. Általában a rendszertámogató mérnök feladata az új hálózati berendezések zökkenőmentes üzembe helyezése. Annak érdekében, hogy a hálózati továbbfejlesztés a tervezett módon történjen, a rendszertámogató mérnök együttműködik az ügyfelekkel.

A rendszertámogató mérnök feladatai

A rendszertámogató mérnök feladatai közé tartozik:

- Segítségnyújtás az üzembe helyezésnél, valamint az átvételi ellenőrzés biztosítása
- A rendszerekkel és azok összetevőivel kapcsolatos hibaelhárítás szervezése és támogatása
- Az ügyfél által jelzett műszaki problémák megoldása
- Az eszközök kezelésével és beállításával kapcsolatos képzés és segítségnyújtás biztosítása az ügyfelek számára

A rendszertámogató mérnök a teljes PPDIOO életcikluson keresztül segít a hálózati terv változtatásaira vonatkozó javaslatok kidolgozásában.

A rendszertámogató mérnökökkel szemben elvárás a hálózati technológiákkal foglalkozó alapfokú és haladó kurzusok elvégzése. Néhány technológia (pl. az IP-alapú hangátvitel) további haladó kurzusok elvégzését igényli. A legtöbb rendszertámogató mérnöki állás betöltéséhez a Cisco Certified Network Associate (CCNA) minősítés a minimális elvárás.

2.3 A tervezési folyamatok előkészítése

2.3.1 Az ügyféllel történő együttműködés

A stadion új hálózatának megtervezése során a Hálózat Kft. együttműködik a stadion irodai személyzetével. Amikor a hálózattervező és munkatársai találkoznak a stadion személyzetével, fontos, hogy szakemberként lépjenek fel.

A kommunikációs készségek fontossága

A jó kommunikációs készség kritikus az ügyféllel történő együttműködés során. A nyugodt, udvarias stílus bizalommal tölti el az ügyfelet, akinek így nem lesznek kétségei afelől, hogy a Hálózat Kft. tervezője és munkatársai el tudják végezni a szükséges feladatokat.

Az alábbi készségek alapvető fontosságúak az ügyféllel történő együttműködés során:

- Az információ meghallgatása és pontos összefoglalása
- A célközönség számára megfelelő stílus, forma és részletezettségi szint megválasztása a kapcsolattartásban
- A megfelelően rendszerezett műszaki tartalom logikus bemutatása

Az ügyféllel történő jó együttműködés kialakításának képessége döntő szerepet játszik. A bizalmon alapuló üzleti kapcsolat számos lehetséges problémát kiküszöböl, miközben mindkét fél számára nagymértékben hozzájárul a projekt sikeréhez.

2.3.2 Az ügyfél pontos ismerete

Egy átfogó fejlesztési terv elkészítéséhez a hálózattervezőnek meg kell ismernie, hogy a felhasználók miként használják a hálózati erőforrásokat és szolgáltatásokat. A tervező információt gyűjt a meglévő hálózati infrastruktúrához biztosított összes belső és külső hozzáférésről, mert ha nincs teljes körű ismerete arról, hogy kinek van hozzáférése a hálózathoz, néhány felhasználói igény elkerülheti a figyelmét. A csupán részleges helyzetkép következtében a tervező hiányos tervet készíthet, ami csúszásokhoz és a költségek növekedéséhez vezethet.

A releváns információk meghatározása

Az infrastruktúrára vonatkozó adatgyűjtés során a tervező a stadion munkatársaival együttműködve határozza meg az összes felhasználói csoportot. Sok egyéb mellett a tervezőnek az ügyfél szervezeti diagramját is be kell szereznie. Fontos azonban, hogy a szervezeti diagram

mögötti tényleges helyzet alapján határozza meg a hálózati hozzáféréssel rendelkező összes felhasználót és érintettet.

A stadion vezetősége az alábbi lehetséges végfelhasználókat adta meg:

- a fiókirodák munkatársai
- a távmunkások
- a terepen dolgozó értékesítési és támogató személyzet
- a kereskedők, beszállítók és partnerek
- a bizottsági tagok
- a tanácsadók és kivitelezők
- az ügyfelek

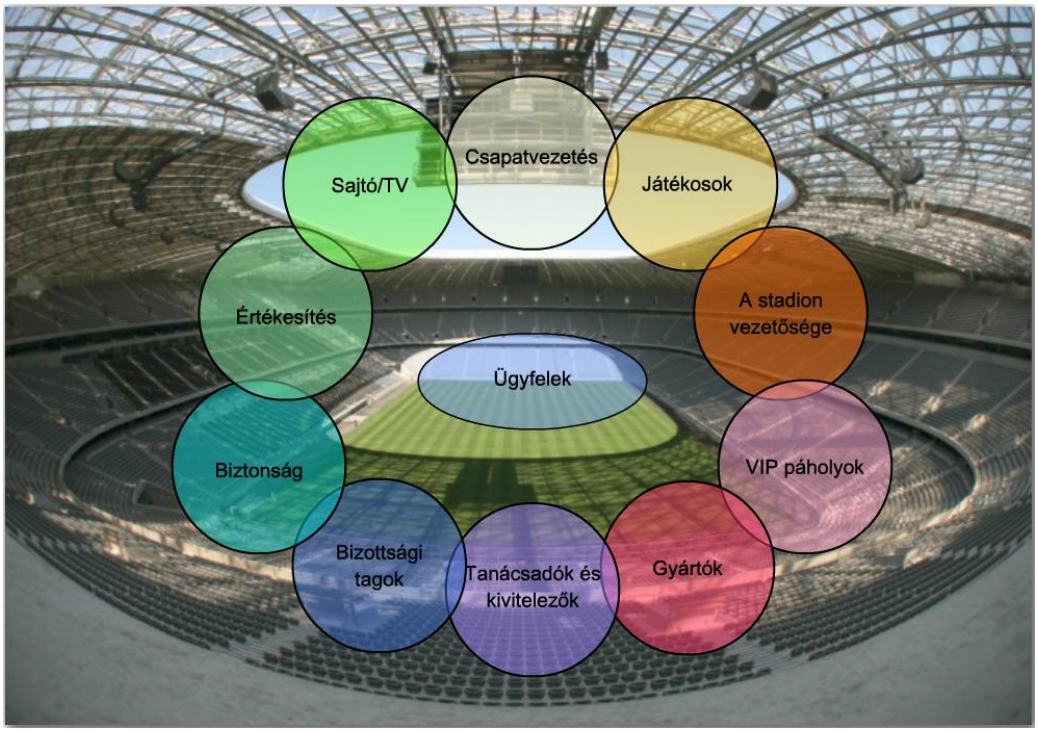
A felhasználói hozzáférés bővítése

A tervezőnek fel kell mérnie, hogy az új felhasználói csoportok hozzáadása a hálózathoz milyen következményekkel jár. Egyes, hálózati hozzáféréssel jelenleg nem rendelkező felhasználói csoportoknak a jövőben szükségük lehet a stadion új hálózati erőforrásaihoz történő hozzáférésre.

A tervező a stadion vezetőségével együttműködve határozza meg:

- az új felhasználói csoportokat
- a szükséges hozzáférés típusát
- azt, hogy a hozzáférés honnan legyen lehetséges
- a biztonságot érintő általános következményeket

A fenti információk birtokában már a fejlesztési terv készítésének szakaszában, illetve az előkészítési szakaszban biztosítható, hogy az új terv pontos és sikeres legyen.



2.3.3 Az üzleti célok és prioritások meghatározása

Minden vállalkozás célja az, hogy sikeres legyen. Egy hálózati projekt megkezdése előtt az üzletvezetők elemzik a projekt megvalósíthatóságát abból a szempontból, hogy az mennyiben járul hozzá a vállalat sikeréhez. Mérlegelniük kell az alábbiakat:

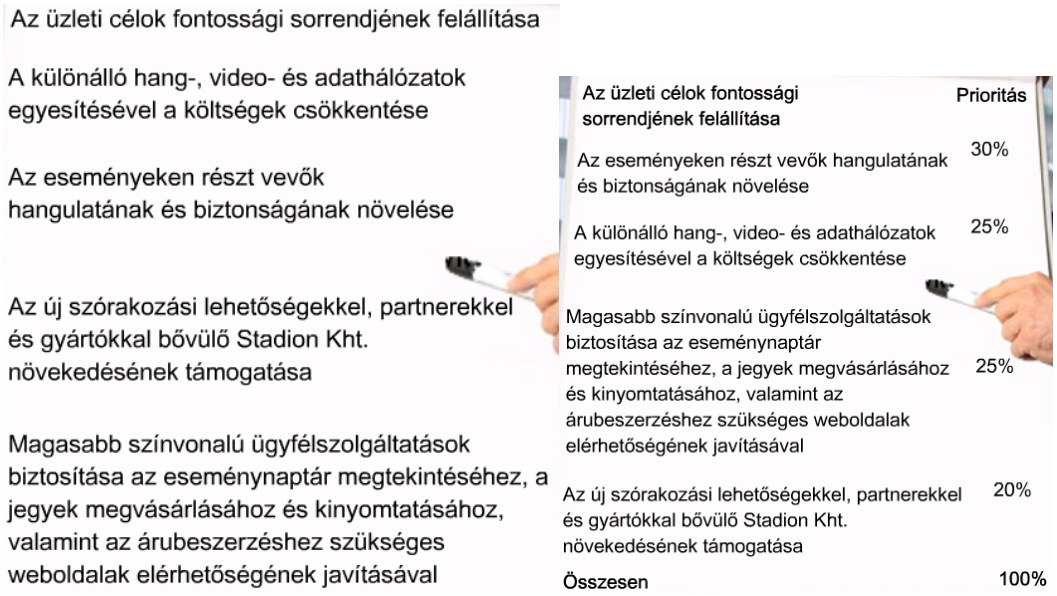
- Jövedelmezőség – Segíthet-e a projekt a költségek csökkentésében vagy megtakarításában a jövőben?
- Vállalati növekedés és piaci részesedés – Segíthet-e a projekt a vállalat hatékonyabb növekedésében, illetve képes-e versenyelőnyhöz juttatni a céget?
- Vásárlói elégedettség – Képes-e a projekt az ügyfelek elégedettségét és hűségét fokozni?

A fenti megvalósíthatósági elemzés lehetővé teszi, hogy az üzletvezetők megfogalmazzák a hálózati projekt magas szintű célkitűzéseit. A hálózattervező tudomásul veszi ezeket, és feljegyzi az esetlegesen megemlített problémákat és aggodalmakat is.

A célok fontossági sorrendjének felállítása

A stadion vezetőségével történő egyeztetések után a hálózattervező felállítja az üzleti célok fontossági sorrendjét. A fontossági sorrend alapját az adja, hogy mely célok kínálják a legjobb lehetőséget a vállalat sikeréhez. Az egyes célok egymáshoz viszonyított fontosságát például százalékos arányban adhatjuk meg a 100 százalékot véve alapul.

Miután a Hálózat Kft. munkatársai felállítják az üzleti célok fontossági sorrendjét, a tervezési fázis munkálataihoz kezdenek hozzá.



2.4 A műszaki követelmények és korlátok beazonosítása

2.4.1 A műszaki feltételek megadása

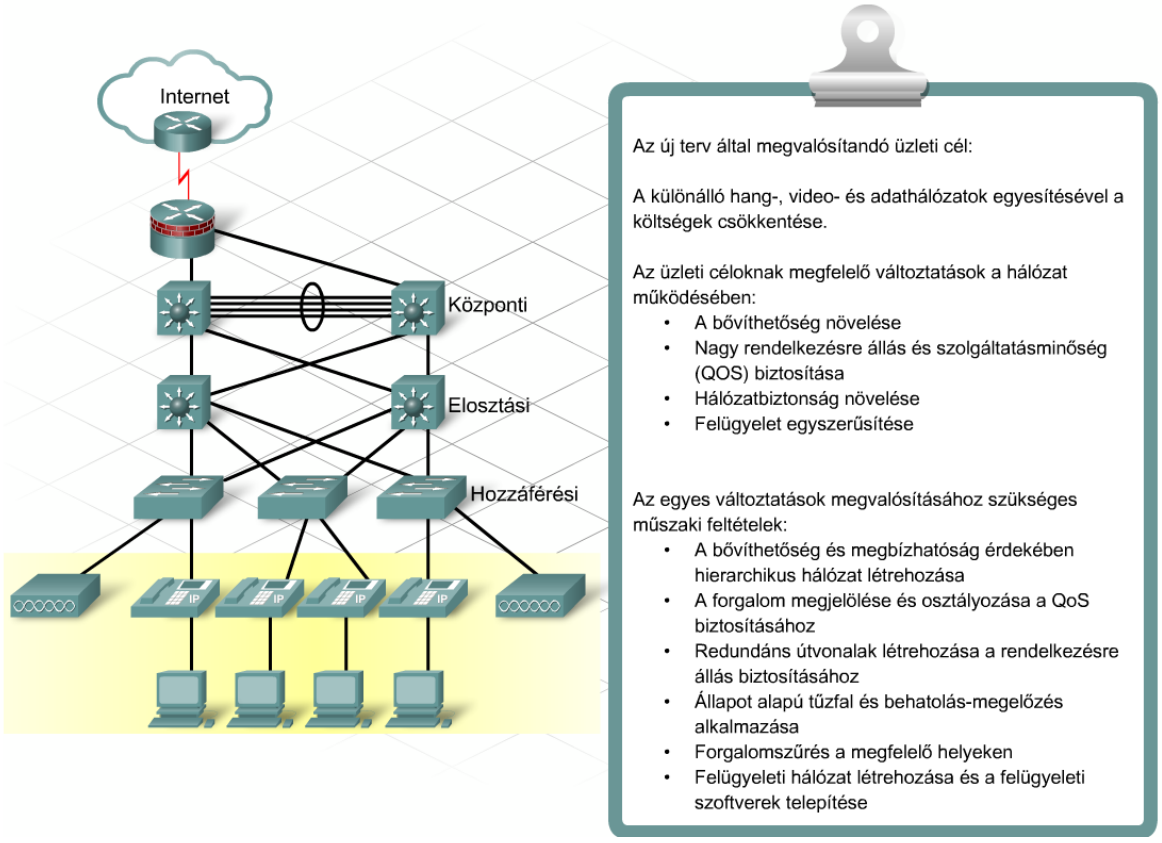
Az üzleti célok fontossági sorrendjének felállítása után a hálózattervező meghatározza az egyes célok megvalósításához szükséges hálózati funkciókat. A tervező felsorolja az új terv által

megvalósítandó üzleti célokat, majd meghatározza, hogy az egyes változtatások végrehajtásához milyen műszaki feltételek szükségesek.

A műszaki követelmények meghatározása lehetővé teszi a tervező számára a projekt nagyságrendjének megadását. Ezen követelmények alapján történik a technológiák, berendezések és a felügyeleti szoftver kiválasztása.

A műszaki feltételek az alábbiakat tartalmazzák (de nem kizárólag ezekre korlátozódnak):

- A hálózat bővíthetőségének garantálása
- A hálózat rendelkezésre állásának és teljesítményének növelése
- A hálózatbiztonság javítása
- A hálózatfelügyelet és a hálózati támogatás egyszerűsítése



A hálózattervező az ügyféllel együttműködve készíti el a műszaki feltételek fontossági sorrendjét amely az alábbi döntésekhez ad iránymutatást:

- A hálózati berendezések kiválasztása
- A protokollok kiválasztása
- A hálózati szolgáltatások megtervezése

A fenti projektlista határozza meg a projekt nagyságrendjét.

Amikor a tervező a műszaki feltételeket beszéli meg az ügyféllel, mérlegelnie kell a hallgatóság műszaki tudásszintjét, ugyanis az ügyfél nem feltétlenül érti a műszaki kifejezéseket és a

szakzsargont. Ezeket vagy kerülni kell, vagy az ügyfél tudásszintjének megfelelő részletességgel és mélységben kell leírni.

Rendelkezésre állás és teljesítmény:

- A webes alkalmazások 24 órás elérhetőségének támogatása a hét minden napján
- A biztonsági alkalmazások 24 órás elérhetőségének támogatása a hét minden napján
- A telefonrendszer 24 órás elérhetőségének támogatása a hét minden napján
- Egy tranzakció végrehajtási idejének 3 másodperc alá szorítása
- Magas színvonalú hang- és videofolyamok biztosítása
- A szolgáltatásminőség garantálása

Biztonság:

- Biztonság javítása szűrők, tűzfalak és behatolás-érzékelő rendszerek (IDS) alkalmazásával
- Központi kiszolgálók és felügyelet
- Vezeték nélküli hálózat védelme

Bővíthetőség:

- A tervezett hálózatban az elkövetkező két év folyamán 50%-os növekedés támogatása a felhasználók és telephelyek számában
- A tervezett hálózatban 75%-os növekedés támogatása a vezeték nélküli hálózat lefedettségében
- A tervezett hálózatban az elektronikus kereskedelem forgalmát tekintve 75%-os növekedés támogatása

Felügyelhetőség:

- Hálózat-karbantartási feladatok végrehajtása a meglévő személyzettel.
- Jelentéseket küldő és felügyelő eszközök biztosítása.

2.4.2 A kötöttségek meghatározása

Minden vállalat a lehető legfejlettebb és leghatékonyabb hálózattal szeretne rendelkezni, a valóságban azonban számos kötöttség befolyásolja a hálózati tervet. A leggyakoribb kötöttségek:

- **Keretösszeg** – A korlátozott erőforrások kompromisszumokat eredményezhetnek a tervben, a berendezések, a szoftver vagy egyéb összetevők árát illetően.
- **Cégpolitika** – A tervnek figyelembe kell vennie az ügyfél meglévő – protokollokra, szabványokra, gyártókra és alkalmazásokra vonatkozó – politikáját.
- **Ütemezés** – A projekt időkeretét az ügyfél időbeosztásához kell igazítani.
- **Személyi állomány** – A megvalósítási és az üzemeltetési szakaszban a tervezés során figyelembe kell venni, hogy lehet-e megfelelően képzett személyzetre számítani.

A kötöttségek kihathatnak a hálózati tervre, ezért még a PPDIOO életciklus folyamat elején meg kell határozni azokat. A kötöttségek relatív fontossága projektenként eltérő lehet. Az óriásprojekteknél nem mindig a költségkeretet érintő kötöttségek a leglényegesebbek.

A stadion vezetősége például nem szeretné, ha a hálózatfejlesztési projekt megvalósítása a sportszezon idejére esne.

2.5 A tervezési vonatkozások menedzselhetőségek azonosítása

2.5.1 A felülről lefelé történő tervezési módszer használata

Két gyakori megközelítési móddal történhet a hálózattervezés: fentről lefelé vagy lentről felfelé.

Fentről lefelé

A fentről lefelé történő tervezés során a hálózati infrastruktúrát kell a szervezet igényeihez igazítani. A fentről lefelé történő tervezés tisztázza a tervezési célokat, majd a tervet a szükséges alkalmazások és hálózati szolgáltatások (pl. IP-telefon, tartalomszolgáltató hálózat és videokonferencia) szemszögéből indítja. A PPDIOO módszer a fentről lefelé megközelítésmódot alkalmazza.

Lentről felfelé

A lentről felfelé tervezési mód gyakori, ám nem javasolt módszer. Ebben a megközelítésben a hálózattervező a szervezet megismerése helyett korábbi tapasztalatai alapján választja ki a hálózati eszközöket és technológiákat. Mivel ez a megközelítésmód figyelmen kívül hagyja az üzleti célokra vonatkozó információt, a tervezett hálózat esetleg nem lesz képes a szükséges alkalmazások támogatására.

A két tervezési stratégia összehasonlítása

	Fentről lefelé módszer	Lentről felfelé módszer
Előnyök	• Tartalmazza a szervezeti igényeket. • Teljes képet ad mind a szervezet, mind pedig a tervező számára.	• Lehetővé teszi a gyors válaszadást a tervezési kérésekre. • Elősegíti a korábbi tapasztalatokon alapuló tervezést.
Hátrányok	• Több időt igényel a hálózati terv elkészítése előtt. • A legtöbb hálózattervező számára nem igazán ismert stratégia.	• A tényleges szervezeti igényeket kismértékben vagy egyáltalán nem veszi figyelembe a megoldás megvalósítása során. • Nem megfelelő hálózati tervet eredményezhet.

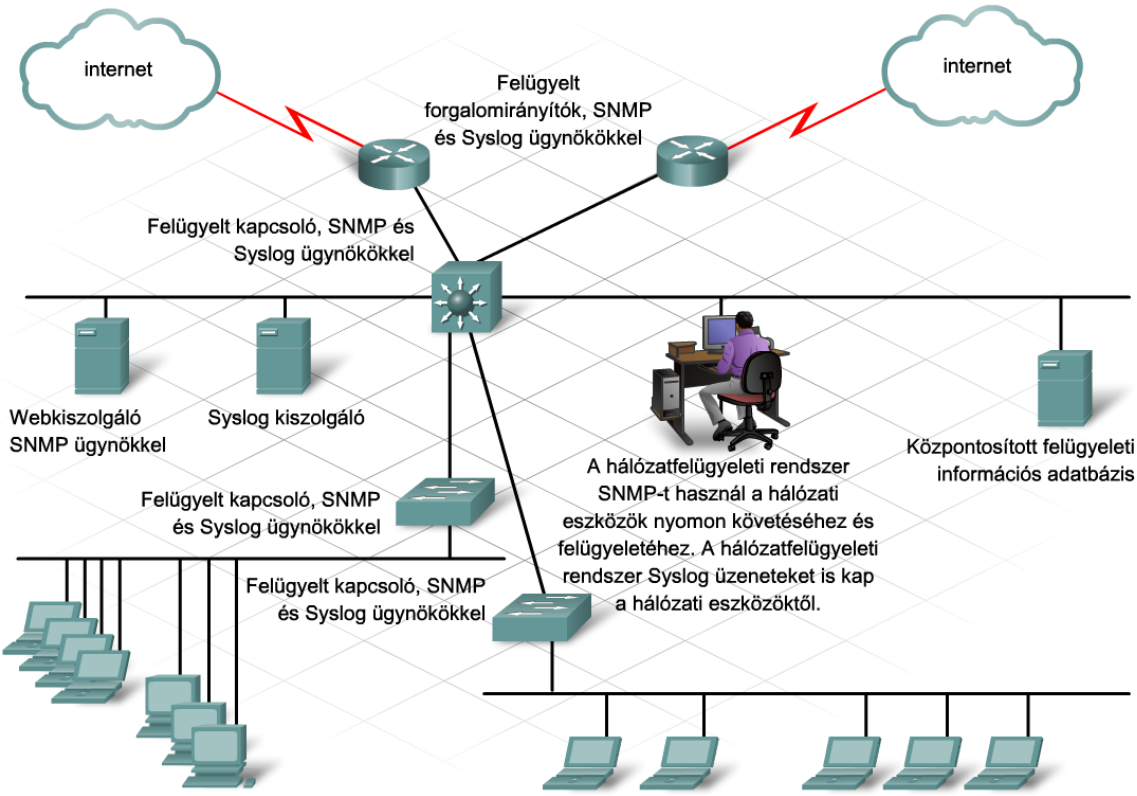
2.5.2 A hálózati műveletek nyomon követése

A megvalósítást követően fontos megbizonyosodni arról, hogy a hálózati terv specifikációi teljesültek-e. A stadion hálózati személyzete ezért nyomon követi és felügyeli a hálózat teljesítményét. A hálózatfelügyelet az alábbi feladatokat tartalmazza:

- A hálózatban bekövetkező változások felügyelete
- A hálózati hibák meghatározása
- A teljesítményszintek nyomon követése
- Biztonsági és jogosultság-kezelési felügyelet biztosítása a hálózat egyéni vagy csoportos használatához

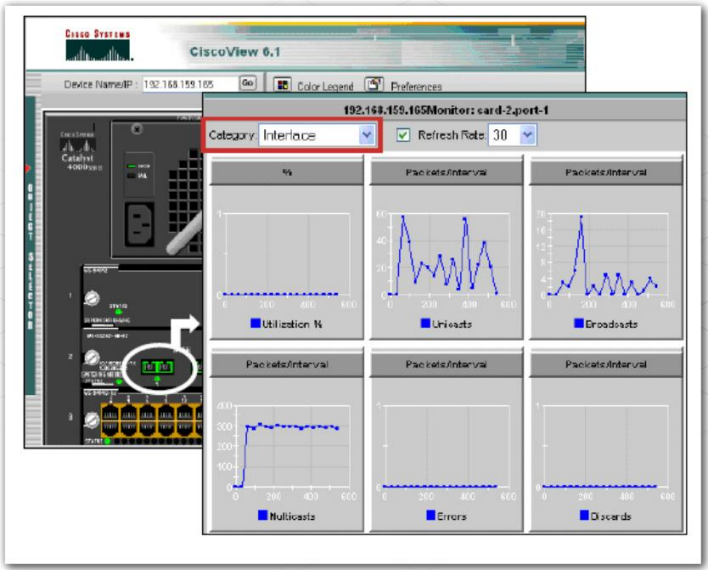
A tipikus hálózatfelügyeleti architektúra az alábbi elemekből áll:

- Hálózatfelügyeleti rendszer (Network Management System - NMS) – Olyan rendszer, amely egy alkalmazás segítségével nyomon követi és irányítja a felügyelt hálózati eszközöket. Ilyen alkalmazás például a CiscoWorks.
- Hálózatfelügyeleti protokoll – Olyan protokoll, amely elősegíti a hálózati eszközök és az NMS között zajló információcserét. Ilyen például az egyszerű hálózatfelügyelő protokoll 3-as változata (SNMPv3).
- Felügyelt eszközök – Az NMS által felügyelt hálózati eszközök. Ilyenek például a forgalomirányítók és a kapcsolók.
- Felügyeleti ügynökök – A felügyeleti ügynök egy a felügyelt eszközökön futó program, amely gyűjti és tárolja a hálózatfelügyeleti adatokat.
- Felügyeleti információ – Az NMS által összegyűjtött adatok.



A CiscoWorks LAN Management Solution (LMS) olyan erőteljes nagyteljesítményű felügyeleti eszközkészlet, amely egyszerűsíti a Cisco hálózatok beállítását, adminisztrációját, nyomon követését és hibaelhárítását. A CiscoWorks ezeket a képességeket integráló megoldása a kategóriája egyik legjobbjának számít, és az alábbi előnyöket kínálja:

- Növeli a hálózatüzemeltetési munkatársak pontosságát és hatékonyságát.
- A beállítások egyszerűsítésével, valamint a hálózati problémák gyors meghatározásával és elhárításával növeli a hálózat általános rendelkezésre állását.
- A hozzáférés-vezérlési szolgáltatások és a hálózatszintű változások naplózásának integrálásával maximalizálja a hálózatbiztonságot.



2.5.3 Hálózatfigyelő eszközök

A leggyakrabban használt hálózatfelügyeleti protokoll az SNMP, amely lehetővé teszi a hálózati rendszergazdák számára a hálózatról és a vonatkozó eszközökről történő adatgyűjtést. Az SNMP felügyeleti rendszerprogram a CiscoWorks és a hozzá hasonló eszközök részét képezi. Az SNMP felügyeleti ügynök program gyakran a kiszolgálók, forgalomirányítók és kapcsolók operációs rendszerébe van beágyazva.

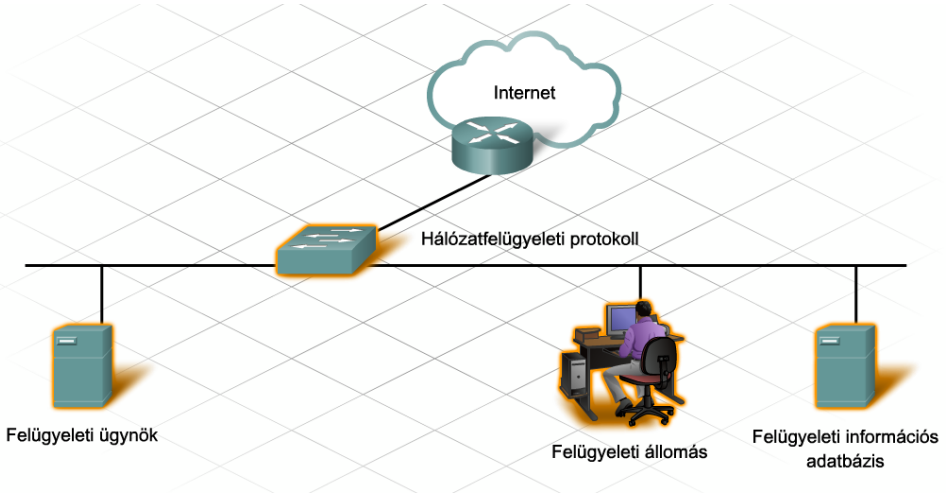
Az SNMP négy fő összetevőt tartalmaz:

- Felügyeleti állomás
- Felügyeleti ügynökök
- Felügyeleti információs bázis (Management Information Base, MIB)
- Hálózatfelügyeleti protokoll

A hálózatfelügyeleti rendszer részeként az SNMP eszközök számos módon reagálhatnak a hálózati hibákra vagy zavarokra. Általánosságban elmondható, hogy a hálózati hibák előfordulásakor vagy előre megadott küszöbértékek elérésekor az SNMP eszközök az alábbi módokon reagálhatnak:

- Figyelmeztetés küldése a hálózaton
- Üzenet küldése egy személyi hívóra
- E-mail küldése a rendszergazdának

Mivel elképzelhető, hogy a stadion vezetősége szolgáltatási szerződést kíván kötni a beszállítóival, valamilyen hálózatfelügyeleti szoftvert mindenképpen be kell szereznie.



2.6 A fejezet összefoglalása

- A Cisco Életciklus Szolgáltatás egy hat szakaszból álló megközelítésmód a Cisco technológiák sikeres kiépítéséhez és üzemeltetéséhez.

- A hálózat életciklusának hat szakasza:

    - Az előkészítési szakasz
    - A fejlesztési terv készítésének szakasza
    - A műszaki terv készítésének szakasza
    - A megvalósítási szakasz
    - Az üzemeltetési szakasz
    - Az optimalizációs szakasz

- Az előkészítési szakaszban történik a projekt üzleti céljainak meghatározása, valamint a hálózat továbbfejlesztésének szükségességét igazoló üzleti terv elkészítése.

- A fejlesztési terv készítésének szakaszában a hálózattervező átfogó helyszíni és műveleti felmérést végez, amely a jelenlegi hálózatot értékeli.

- Elkészül a projektterv, amely tartalmazza a a hálózattervezési projekt elvégzéséhez szükséges feladatokat, az ütemtervet, a kockázatokat, a felelősségeket és a szükséges erőforrásokat.

- A műszaki terv készítésének szakaszában a tervező kellően rugalmas műszaki tervet készít, hogy az új technológiákat integrálni lehessen a jelenlegi műveleti és hálózatfelügyeleti infrastruktúrába.

- A megvalósítási szakaszban a hálózat kiépítése a jóváhagyott tervspecifikációnak megfelelően történik. Ekkor kell tesztekkel megbizonyosodni arról, hogy az új hálózat megfelel-e az üzleti céloknak és a tervezési követelményeknek.

- Az üzemeltetési és az optimalizációs szakasz folyamatos, mindkettő a hálózat napi műveleteit takarja.

- A hálózat optimalizálása vég nélküli folyamat, amelynek során a potenciális gyengeségeket még a bekövetkezésük előtt meg kell határozni és meg kell oldani.

- Az ajánlatok és árajánlatok bekérésének célja, hogy a hálózati kivitelezők tegyék meg a tervezési szolgáltatásokra, berendezésekre, üzembe helyezésre és támogatásra vonatkozó ajánlataikat.

- Az ajánlatok és árajánlatok bekérése a kiíró céggel kapcsolatban az alábbi információkat tartalmazza: az üzleti célok, az új technológiákra vonatkozó követelmények, az ajánlat benyújtásához követendő folyamat vázlata.

- Ahhoz, hogy a hálózati szolgáltatásokat biztosító ajánlatunk sikeres legyen, kulcsfontosságú az előírt formátum és határidő betartása.

- Az ügyfél kiírására a hálózati kivitelező üzletkötőből, értékesítési rendszermérnökökből, hálózattervezőkből és rendszertámogató mérnökökből álló csapata válaszol.

- Az üzletkötő szolgál elsődleges kapcsolódási pontként az ügyfelek és a hálózati kivitelező között.
- Az értékesítési rendszermérnök feladata, hogy segítsen az üzletkötőnek eldönteni, hogy milyen továbbfejlesztések, illetve bővítések szükségesek a jelenlegi hálózaton. Az értékesítési rendszermérnök segít a hálózattervezőnek, hogy az új berendezések és szolgáltatásokat integrálni lehessen a meglévő hálózatba.
- A tervező olyan hálózati tervet készít az ügyfél számára, amely skálázhatóság, rendelkezésre állás, biztonság és felügyelhetőség szempontjából is megfelel az ügyfél igényeinek.
- A rendszertámogató mérnök feladata, hogy a továbbfejlesztett hálózatot zökkenőmentes üzembe helyezze, valamint meggyőződjön arról, hogy a hálózat a terveknek megfelelően működik.
- A hálózati kivitelező minden munkatársának jó kommunikációs készséggel kell rendelkeznie, hogy bizalmat sugározzon, hogy a cég munkatársai biztosítani tudják a szükséges hálózati szolgáltatásokat.
- A vállalat új technológiákat
- A megszorítások hatással lehetnek/vannak a hálózati tervre, így már a tervezési folyamat elején figyelembe kell venni azokat.
- A legjobb eséllyel a fentről lefelé történő hálózattervezési stratégiák használhatók, mivel a tervezők figyelembe veszik az ügyfél üzleti céljait még a technológiai megoldások kiválasztása előtt.
- A lentről felfelé történő tervezési stratégiák a berendezések és technológiák kiválasztásával kezdődnek, majd ezek hálózatba történő beépítésének miként jét határozzák meg.
- Bármely hálózat esetében az egyik elsődleges műszaki feltétel a minősített támogató személyzet rendelkezésre állása. A folyamatban lévő hálózati műveletek egyszerűsítésének érdekében a hálózatfigyelő és hálózatfelügyeleti szoftver legyen a hálózati terv része!

3. Egy létező hálózat jellemzése

3.1 A létező hálózat dokumentálása

3.1.1 Hálózati diagram készítése

Egy új hálózat telepítése során az első lépés általában a meglévő hálózat részletes áttekintése. A Hálózat Kft. tervezője a következő szempontok alapján vizsgálja a hálózatot:

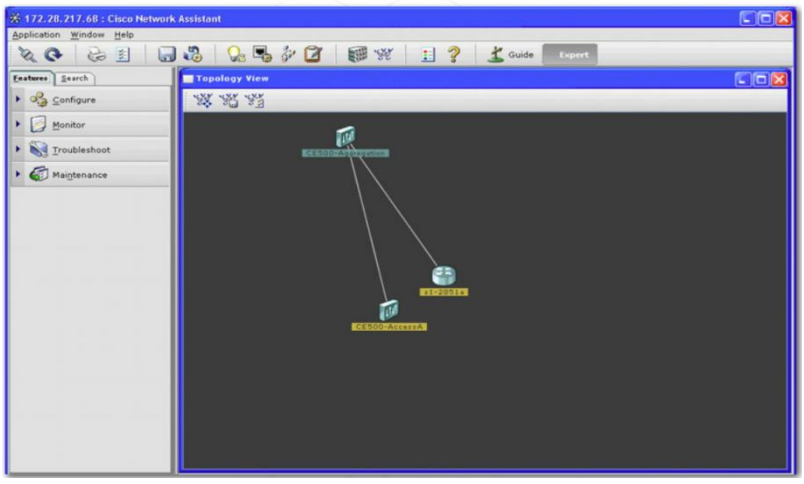
- Mennyire reálisak és kivitelezhetőek a tervezési célok
- A meglévő hálózat mennyire felel meg a méretezhetőséggel, a rendelkezésre állással, a biztonsággal és a felügyelhetőséggel kapcsolatos elvárásoknak.
- Hol van szükség új eszközökre, infrastruktúrára és szolgáltatásokra
- Hogyan biztosítható a régi és új eszközök, átviteli közegek, illetve hálózati funkciók együttműködése

A stadion hálózatának korszerűsítése

Mint a legtöbb szervezetnek, a stadionnak is van már működő hálózata. A vezetőség egy olyan új hálózatot szeretne, melyben:

- jobban felügyelhető a meglévő hang-, video-, és adathálózat
- fejlettebbek az ügyfelek számára nyújtott szolgáltatások
- kisebb a költség

A Cisco Network Assistant (Hálózati Segéd)



A Hálózat Kft. tervezője átnézi a meglévő hálózat dokumentációját. A stadion informatikai részlegének hálózati dokumentációja a legtöbb olyan információt tartalmazza, amelyre a tervezőnek a hálózat felépítésével és szolgáltatásaival kapcsolatosan szüksége lehet.

A hálózati dokumentációnak tartalmaznia kell:

- A hálózat logikai és fizikai diagramját
- Az egyes épületszintek alaprajzát a kábelek és a huzalozási központok feltüntetésével
- A telepített hálózati eszközökről készített nyilvántartási listát

- Az aktuális konfigurációs fájlokat
- A hálózati alkalmazásokról készített nyilvántartási listát

A hálózat topológiai térképének elkészítése

Ahogy ez más vállalatnál is előfordul, a Stadion Kht. hálózati dokumentációja nem a legfrissebb adatokat tartalmazza. A hálózat egészéről, valamint a hálózatot alkotó szegmensekről is új diagramot kell készíteni.

A hálózatfelügyeleti szoftverek segítségével információt lehet gyűjteni és diagramot lehet készíteni a jelenlegi hálózatról. A hálózatfelügyeleti programok közé tartozik például a Cisco Network Assistant és a CiscoWorks alkalmazás.

A stadion hálózatánál a Cisco Network Assistant programot használják a hálózati diagramhoz szükséges információk begyűjtésére.

Információgyűjtés az eszközökről és az adatútvonalakról

A Hálózat Kft. szakemberei hozzáférési jogosultságot kaptak a stadion hálózati eszközeihez. A hálózattervező mérnök a hagyományos Cisco IOS parancsok segítségével szerzi meg a szükséges információkat az eszközökről és a hálózaton zajló adatforgalom útvonalairól.

A Cisco IOS szoftver hasznos parancsokat biztosít a hálózati diagram elkészítéséhez szükséges információk megszerzéséhez. Ilyen parancsok például a:

- `show version`
- `show running-config`
- `show ip route`
- `show cdp neighbors detail`
- `show controllers`
- `show tech-support`

A show tech-support parancs segítségével forgalomirányítókról lehet nagy mennyiségű információt begyűjteni. A parancs kimenete a forgalomirányító vagy a kapcsoló konfigurációjától és platformjától függően eltérő lehet.

A felsorolt parancsok többsége Cisco kapcsolókon is alkalmazható. További hasznos, kapcsolókon alkalmazható parancsok:

- `show vlan`
- `show vtp`
- `show spanning-tree`

3.1.2 A logikai architektúra diagramjának elkészítése

Az információgyűjtés után a következő feladat a logikai hálózati diagramok elkészítése vagy frissítése.

Egy létező hálózat áttekintő diagramjának elkészítése

A stadion hálózati projektjének első diagramjaként, a hálózattervező mérnök elkészíti a stadion hálózatának összes helyszínét magában foglaló áttekintő vázlatot. A diagram a következőket tartalmazza:

- A stadion fő hálózatát
- Az ajándékboltot
- A jegyárusító helyeket
- A távoli helyszínek kapcsolódását
- Az üzleti partnerek kapcsolódását

A tervező felvázolja a fő hálózat és a külső helyszínek végberendezései közötti WAN-kapcsolatokat.

Ez a hálózati diagram azt ábrázolja, hogyan áramlik az információ az egyik helyszínről a másikra, s ez segítséget nyújt a tervező számára a problémás területek azonosításához.

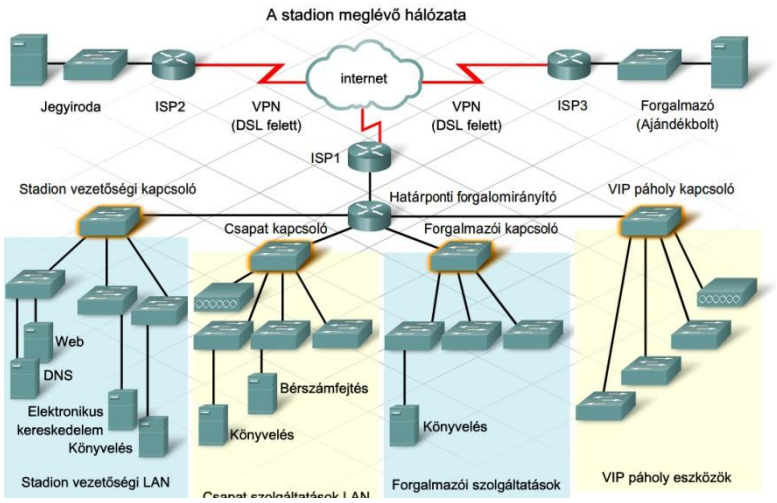
A hálózati szegmensek diagramjának elkészítése

A tervező ezt követően elkészíti a különböző helyszínek fizikai és logikai diagramját.

Mindegyik diagram tartalmazza az alábbiakat:

- A hálózati eszközök és huzalozási központok helyét
- A logikai címzést
- Az elnevezéseket

Ezeket a diagramokat felhasználva a tervező azonosítja azokat a pontokat, ahol topológia változtatásra vagy eszközcserére van szükség, majd ezt követően kiértékeli az adatforgalom áramlásáról és a címzési rendszerről szerzett információkat.



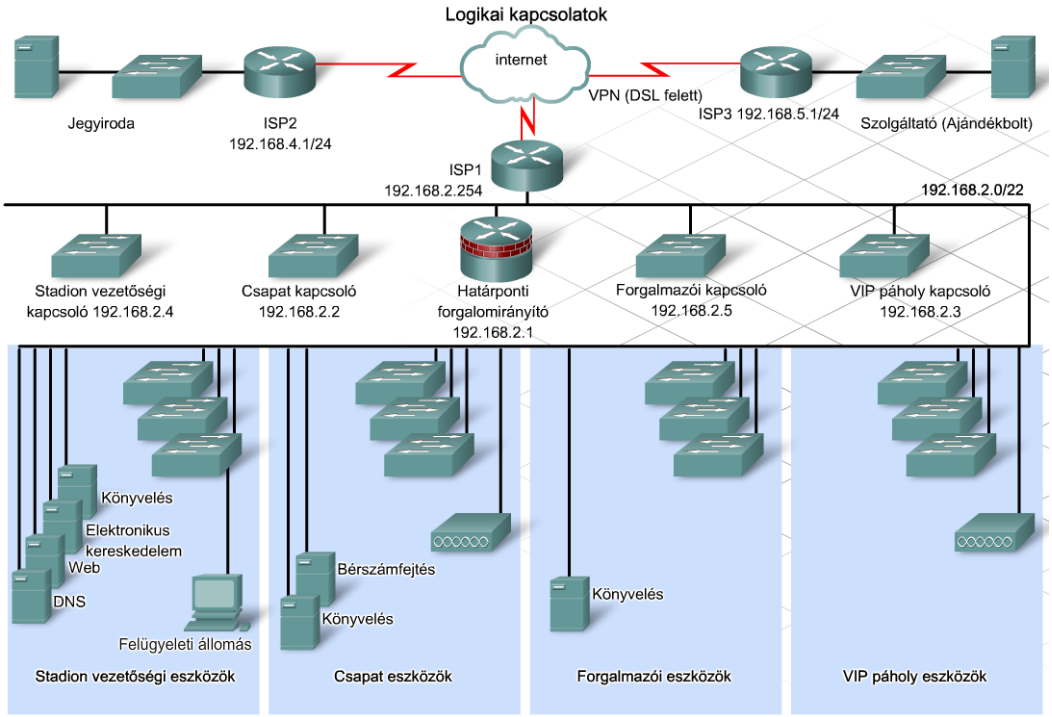
A stadion központi helyszínén telepített hálózat összetettebb, mint a távoli helyszíneken lévők. A hálózattervező egy különálló logikai diagramot készít a LAN különböző összetevőinek és topológiáinak bemutatására. A diagram megmutatja a felhasználók és a kiszolgálók közötti adatfolyam áramlást.

A stadion fő LAN-ját ábrázoló logikai diagram elkészítése

A tervező elkészít egy logikai hálózati diagramot, mely a jelentősebb hálózati eszközöket és azok összeköttetéseit ábrázolja. A diagram tartalmazza:

- a forgalomirányítókat és kapcsolókat
- a vezetéknélküli hozzáférési pontokat
- a kritikus távközlési berendezéseket (CSU/DSU, modemek, stb.)
- a tűzfalakat és a behatolás érzékelő eszközöket (IDS)
- a felügyeleti állomásokat
- a kiszolgálókat és a kiszolgálófarmokat

A diagram a kiszolgálókat szolgáltatásaikkal együtt azonosítja, mivel a kiszolgálók elhelyezkedése befolyásolhatja a forgalommintákat, a sávszélesség használatot és a biztonságot. A tervező az egyes összeköttetések mellé a sávszélességet, a használt kábeltípust, vezetéknélküli eszköznél az eszköz jellemzőit is felírja.



3.1.3 Moduláris diagram készítése

A stadion hálózata a kezdeti tervekhez képest jelentős mértékben növekedett. A Hálózat Kft. tervezője a logikai diagram alapján moduláris blokkdiagramba szervezi a hálózatot.

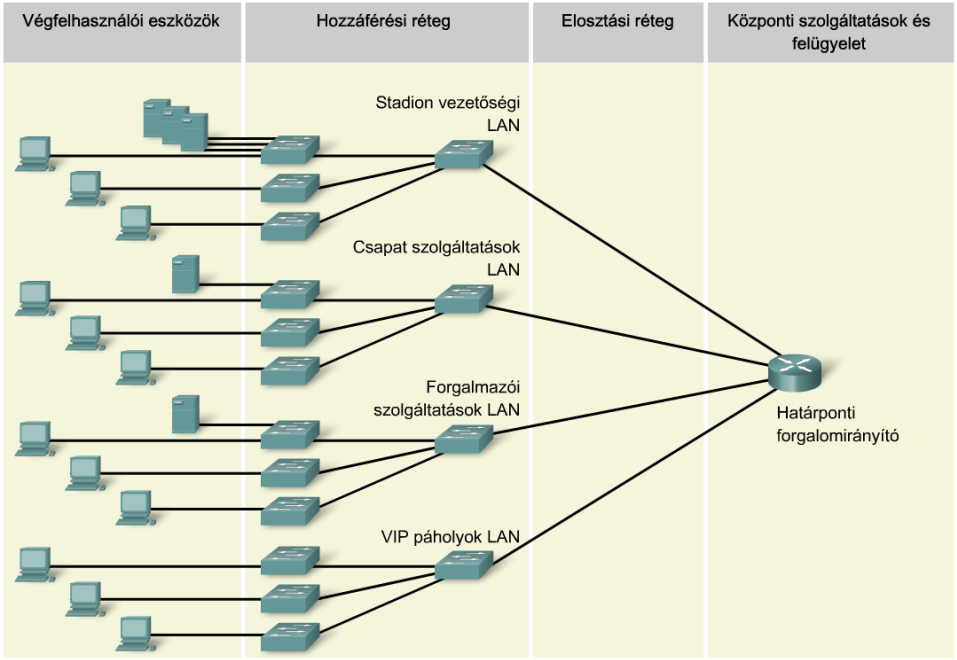
A moduláris blokkdiagram tulajdonképpen a hálózat egyszerűsített képe, mely moduláris formában mutatja be a hálózat főbb funkcióit. A hálózattervező mérnök ennek alapján határozza meg a hálózat alapját képező architektúrát.

A tervező összehasonlítja a blokkdiagramot a Cisco Enterprise Network Architectures szerinti ideális hálózati tervvel, és azonosítja azokat a területeket, ahol mindenképpen újratervezés vagy bővítés szükséges.

A stadion hálózatának eredeti felépítése egy hatalmas egyszintű hálózatnak felel meg. A kapcsolók mindössze két rétegben működnek: bizonyos kapcsolók a végfelhasználók csatlakozását biztosítják a hálózathoz, míg a többi csak kapcsolókat köt össze. Mindkét réteg második rétegbeli kapcsolókból épül fel, és egyik réteg sincs VLAN-okkal szegmentálva.

A kiszolgálók a hálózat különböző pontjain találhatók.

Az internet-kapcsolatot egy különálló forgalomirányító biztosítja. A kapcsolatot tűzfal és behatolás-érzékelő rendszer (IDS) védi. Mindkét távoli telephely VPN kapcsolaton keresztül csatlakozik a stadion hálózatához. A VPN kapcsolatok végpontja az internet kapcsolatért felelős forgalomirányítónál található.



3.1.4 A meglévő hálózat erős és gyenge pontjai

A hálózattervező mérnök által készített diagramok lehetővé teszik a Hálózat Kft. dolgozói számára, hogy megkeressék a hálózat erős és gyenge pontjait.

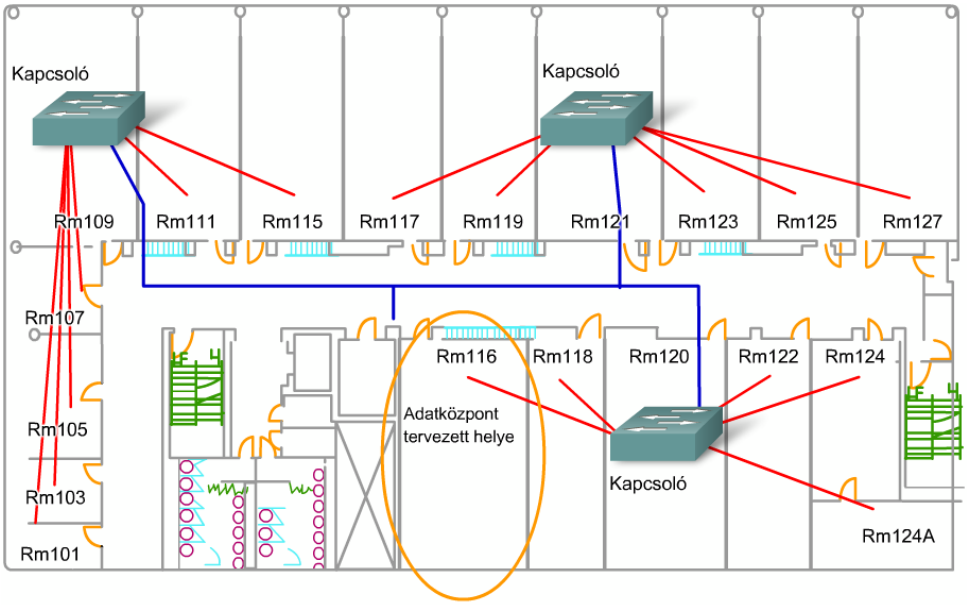
A stadion jelenlegi hálózatának erősségei

A tervező áttekinti a jelenlegi hang- és videohálózat dokumentációját az eszközök pontos helyének és a szolgáltatásokat igénybe vevő felhasználói csoportoknak a meghatározásához.

3. Egy létező hálózat jellemzése

Új, 5-ös kategóriájú kábelezést mostanában telepítettek a stadion hálózatában. Ezen felül új, egymódusú üvegszál köti össze a huzalozási központokat és a fő távközlési helyiséget. A meglévő kábelezés által biztosított nagy áteresztőképesség miatt nincs szükség a stadion hálózati infrastruktúrájának komolyabb módosítására. További kábelezésre is csak akkor van szükség, ha új vezetéknélküli hozzáférési pontokat (AP) kell telepíteni.

A huzalozási központ melletti terület megfelel a kiszolgálófarmot magában foglaló új adatközpont helyszínének.



A diagramok és a meglévő eszközök listájának áttekintése után a hálózattervező mérnök pontokba szedi a stadion jelenlegi hálózatának erős és gyenge pontjait:

Erősségek:

- Új kábelezés és megfelelő huzalozási központok
- Megfelelő helyszín az új adatközpont számára
- A kiszolgálók és PC-k korszerű modellek, cseréjük nem szükséges
- Néhány meglévő kapcsoló és forgalomirányító az új tervezetben is használható

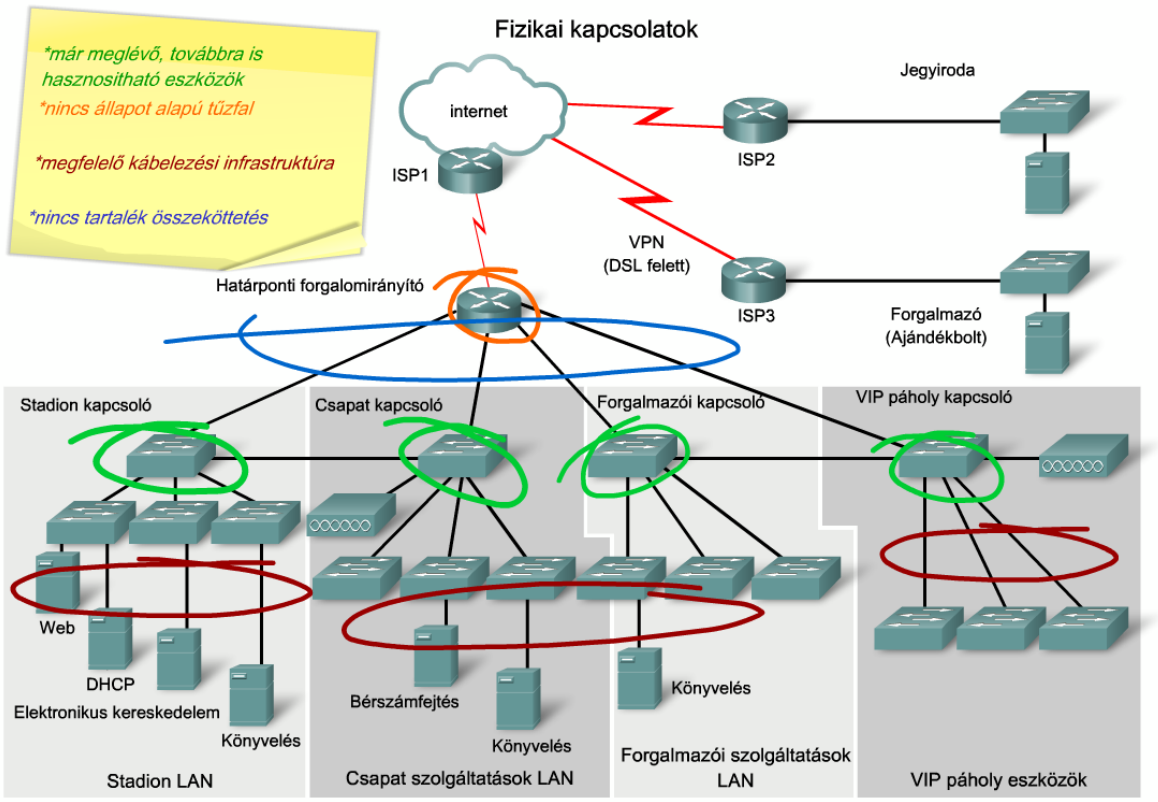
Gyenge pontok:

- Egyszintű hálózati terv
- Nincs elosztási réteg
- Nincs igazi központi réteg
- A kiszolgálók elhelyezése nem megfelelő
- Több hálózatból felépülő, nehezen karbantartható rendszer
- Nem megfelelő IP-címzési rendszer
- Nincs dedikált sávszélesség a WAN kapcsolaton
- Rosszul telepített vezetéknélküli hálózat
- Korlátozott biztonsági intézkedések

A hálózat korszerűsítése során a gyenge pontok kiküszöbölése

A tervező a létező hálózat gyenge pontjainak kiküszöbölésére összpontosít, és javasolja a hálózati terv frissítését a szükséges fejlesztésekkel.

Azokat a meglévő eszközöket, melyeket továbbra is hasznosítanak, ugyancsak át kell vizsgálni. Az új eszközök és funkciók problémamentes együttműködéséhez fontos ellenőrizni, hogy minden hardver megfelelően működik-e és, hogy ezeken a legfrissebb szoftver van-e telepítve.



3.2 A meglévő Cisco IOS frissítése

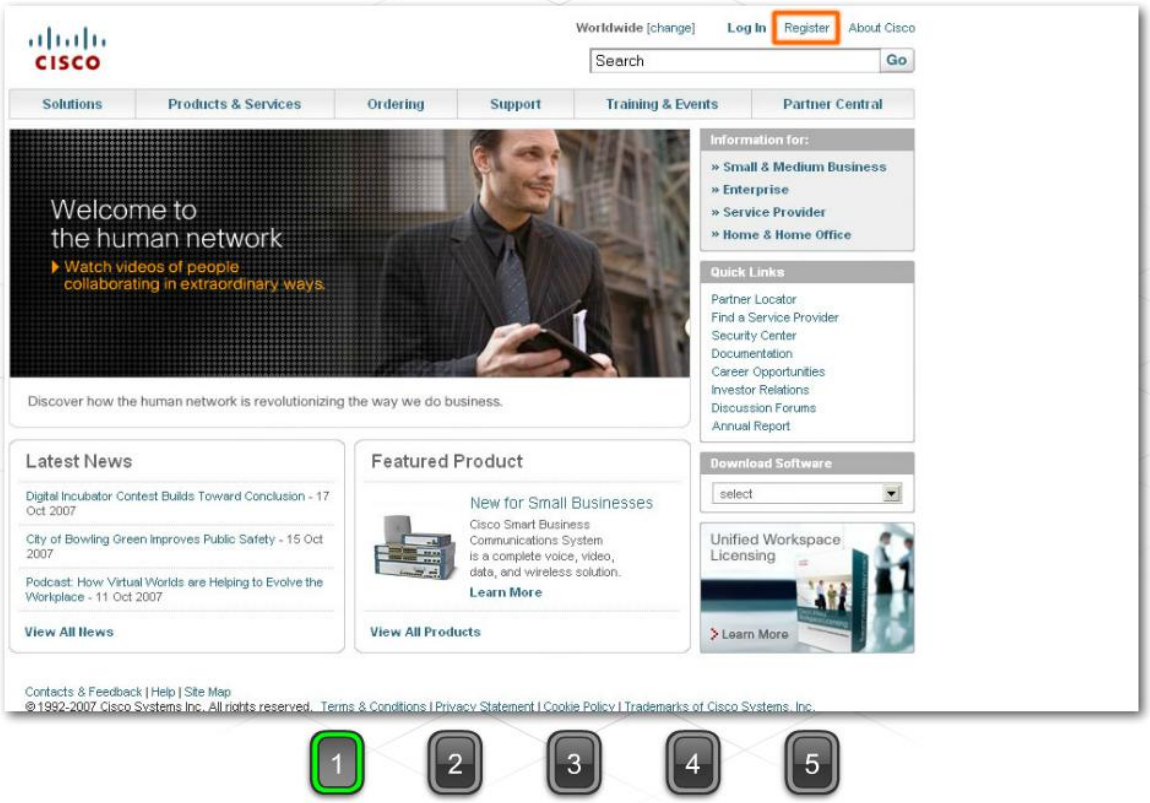
3.2.1 A Cisco CCO jellemzői és felépítése

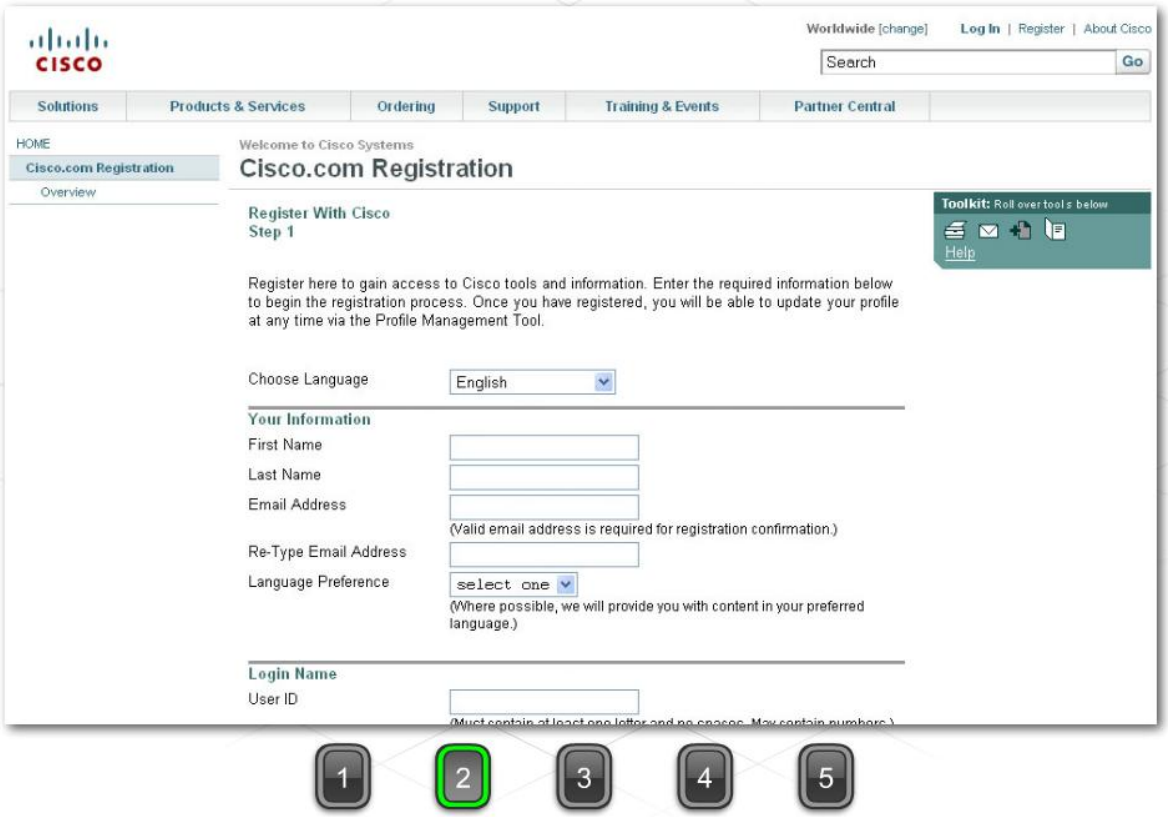
A Cisco.com weboldal olyan eszközöket és on-line erőforrásokat nyújt a Hálózat Kft. dolgozói számára, amelyek segítségével a stadion hálózatának eszközeiről szerezhetnek információt. A weboldal általános technikai problémák megoldásában is segít. Az erőforrások és eszközök közé tartoznak a következők:

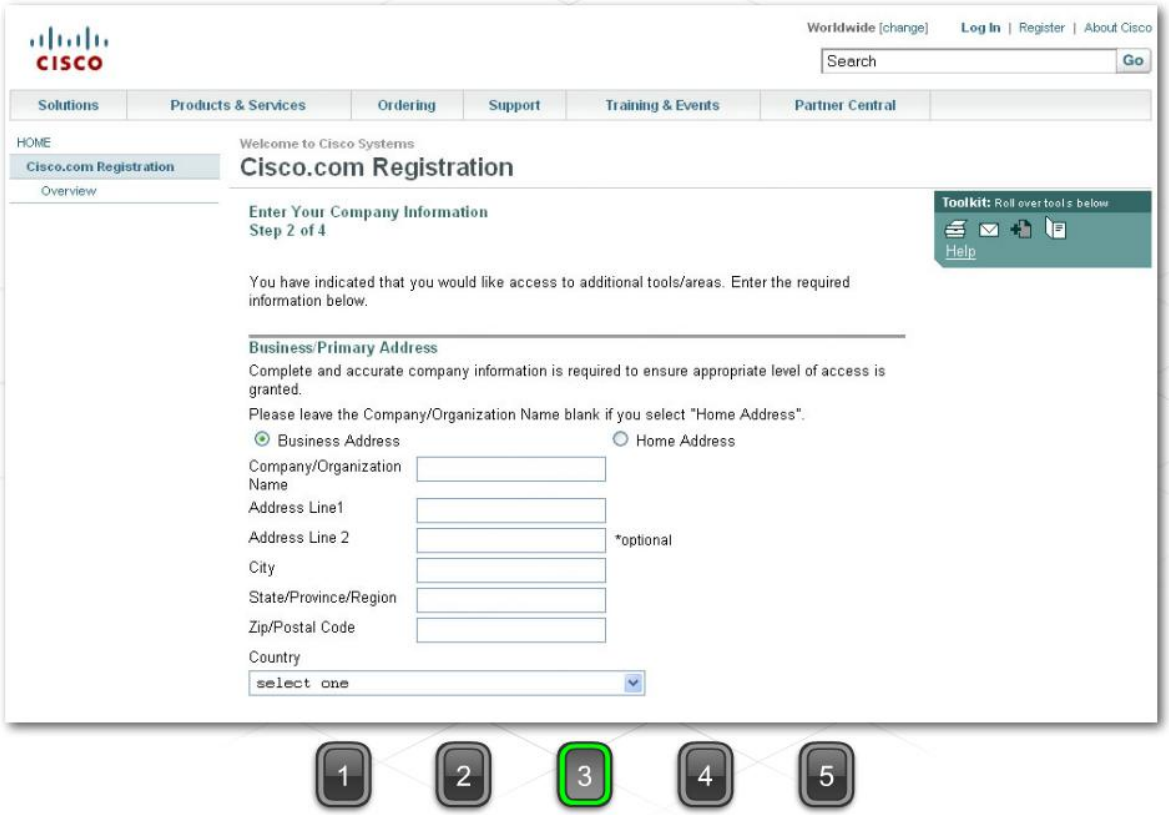
- **Dokumentáció** – Hardver és szoftver konfiguráció és ellenőrzés, valamint hibafeltárásra alkalmas Cisco termékek és technológiák
- **Eszközök** – Hibaelhárítás, telepítés, vizsgálat- és szolgáltatáskérés
- **Letöltések** – Szoftver, speciális fájl változatok, technikai támogatást nyújtó alkalmazások
- **Közösségek és képzés** – Információ a hálózati szakmai kapcsolatokról, a technikai támogatásra felkészítő tanfolyamokról, és más képzési lehetőségekről
- **Hírek** – A Cisco Technical Support hírlevélben megjelenő aktuális témák

A Cisco.com oldal által nyújtott szolgáltatások eléréséhez regisztrált felhasználói jogosultság létrehozása szükséges. A hozzáférés szintje függ a felhasználói jogosultság típusától, valamint attól, hogy a felhasználó rendelkezik-e érvényes SMARTnet karbantartási szerződéssel.

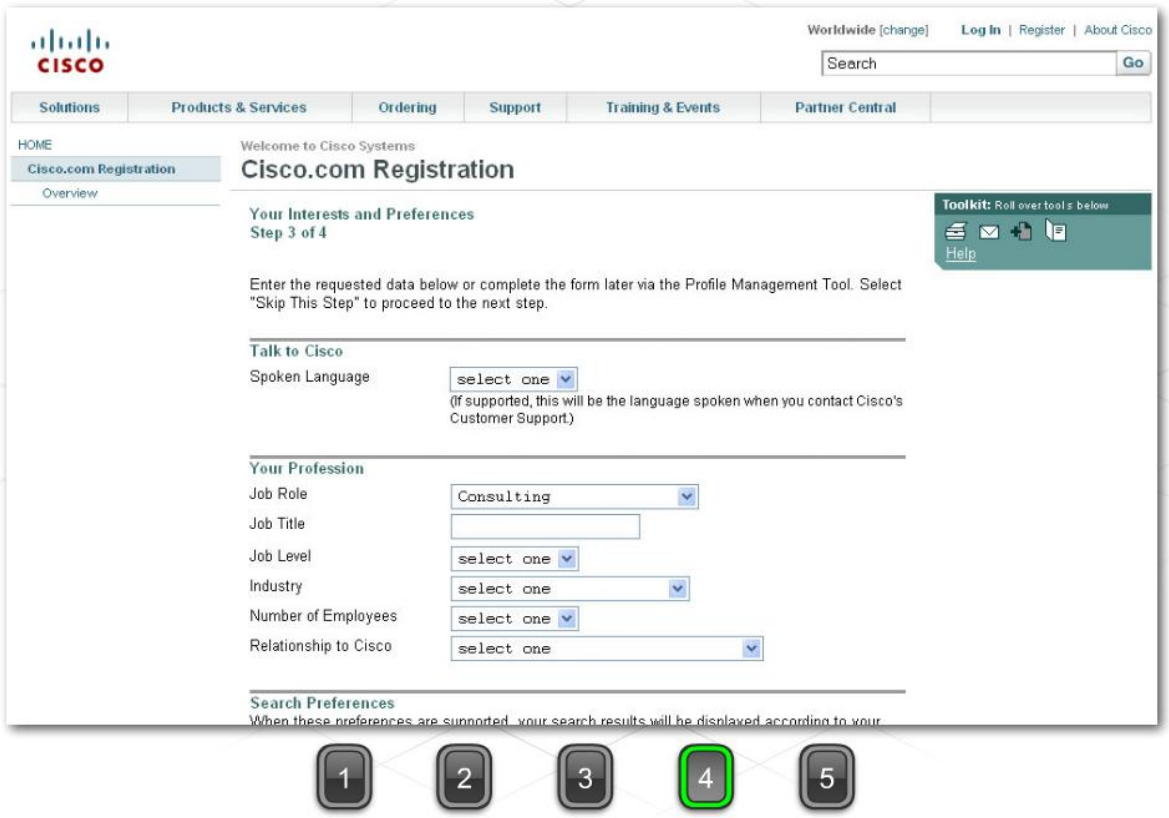
Regisztráció a Cisco.com weboldalon



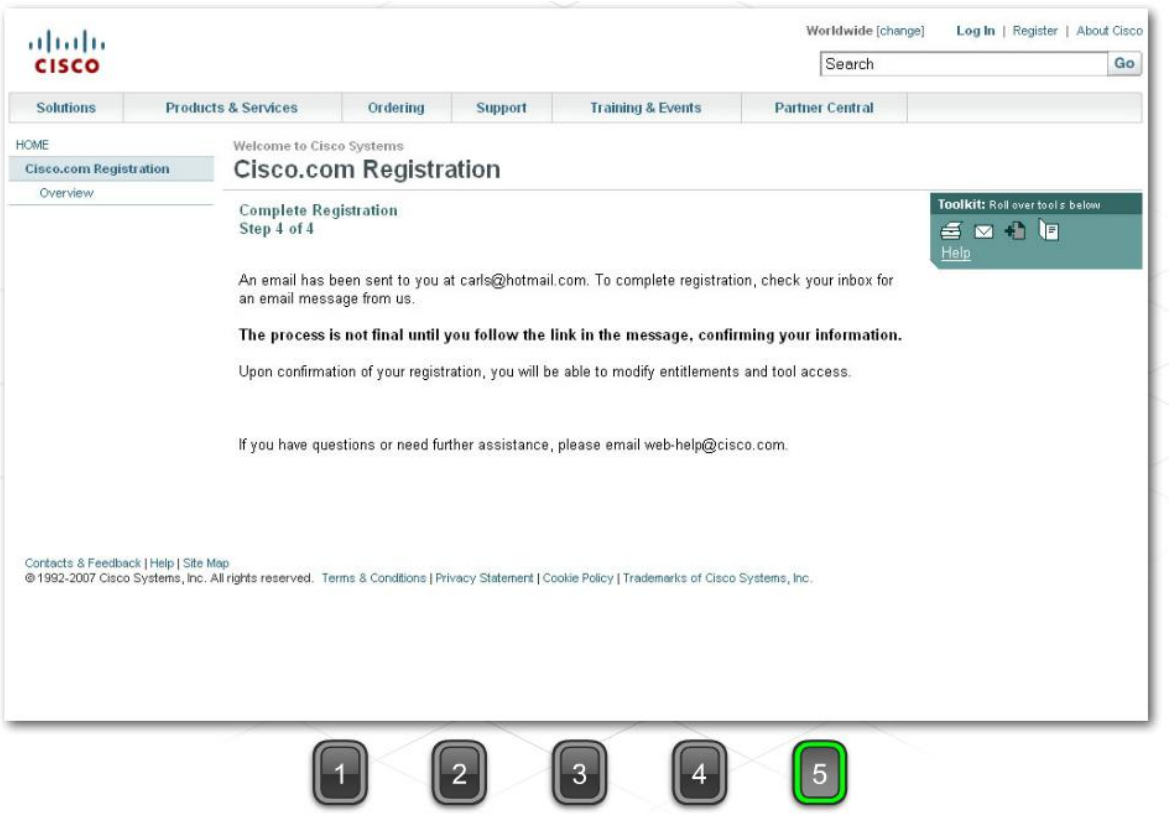



Worldwide [change]
Log In | Register | About Cisco
Search
Go
Solutions
Products & Services
Ordering
Support
Training & Events
Partner Central
HOME
Cisco.com Registration
Overview
Welcome to Cisco Systems
Cisco.com Registration
Toolkit: Roll over tools below
Help
Enter Your Company Information
Step 2 of 4
You have indicated that you would like access to additional tools/areas. Enter the required information below.
Business/Primary Address
Complete and accurate company information is required to ensure appropriate level of access is granted.
Please leave the Company/Organization Name blank if you select "Home Address".
Business Address
Home Address
Company/Organization Name
Address Line1
Address Line 2
*optional
City
State/Province/Region
Zip/Postal Code
Country
select one

1
2
3
4
5


Worldwide [change]
Log In | Register | About Cisco
Search
Go
Solutions
Products & Services
Ordering
Support
Training & Events
Partner Central
HOME
Cisco.com Registration
Overview
Welcome to Cisco Systems
Cisco.com Registration
Toolkit: Roll over tools below
Help
Your Interests and Preferences
Step 3 of 4
Enter the requested data below or complete the form later via the Profile Management Tool. Select "Skip This Step" to proceed to the next step.
Talk to Cisco
Spoken Language
select one
(If supported, this will be the language spoken when you contact Cisco's Customer Support.)
Your Profession
Job Role
Consulting
Job Title
Job Level
select one
Industry
select one
Number of Employees
select one
Relationship to Cisco
select one
Search Preferences
When these preferences are supported, your search results will be displayed according to your

1
2
3
4
5



3.2.2 A telepített Cisco IOS szoftver vizsgálata

A Cisco.com weboldalon elérhető szolgáltatások használata előtt a Hálózat Kft. dolgozóinak szüksége van az eszközlista következő adataira:

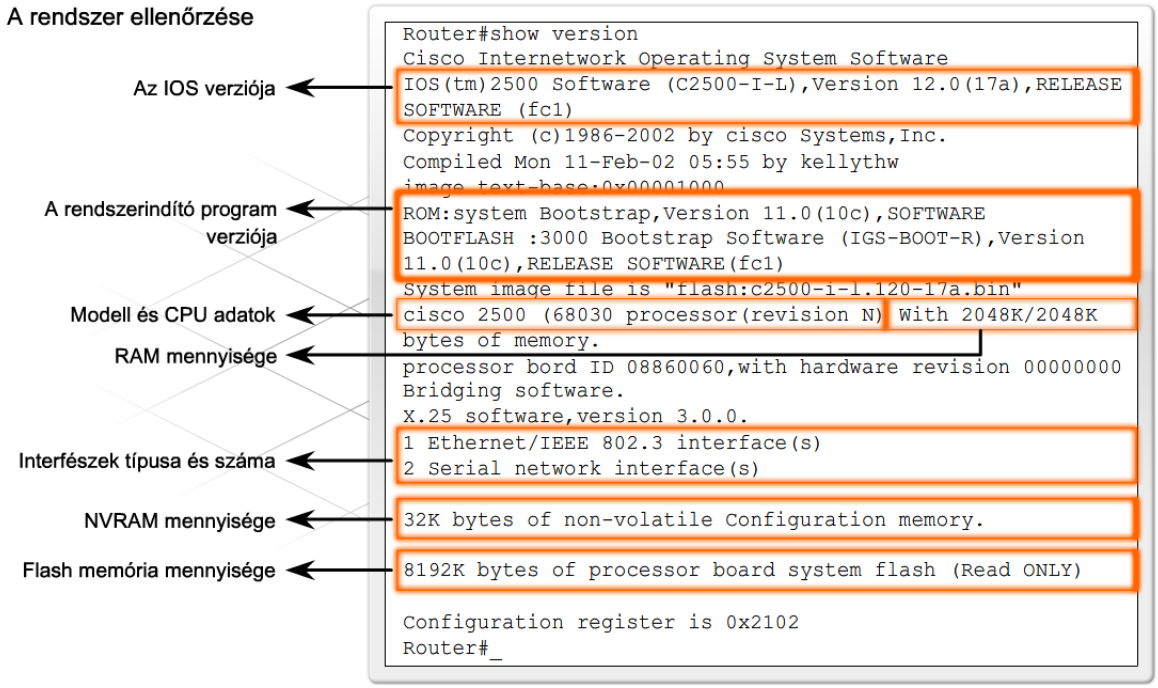
- Az eszközök típusa és modell azonosítója
- Telepített memória
- Interfészek és bővítő helyek
- Opcionálisan telepített modulok
- Jelenlegi IOS szoftver verzió és fájlnév

A Hálózat Kft. dolgozói ezen információk alapján határozzák meg, hogy melyik Cisco IOS szoftver verzió a megfelelő és milyen opcionális hardverelemek telepíthetők.

A `show version` parancshasználata

A szakemberek minden eszközön a show version parancs használatával ellenőrzik az eszközlista helyességét és pótolják a hiányzó információt.

A hálózattervező mérnök listát küld a dolgozóknak az új szolgáltatásokról. Ezek azok a szolgáltatások, amelyek a hálózattervező mérnök megítélése szerint mindenképp szükségesek a kibővített stadion hálózat különböző funkcióinak ellátására. A lista kiértékelése segíti a szakembereket az új hálózat megfelelő IOS szoftververziójának kiválasztásában.



A Hálózat Kft. szakemberei és a stadion informatikai vezetősége megvitatják, hogyan lehetne a jelenlegi hálózat bővítését a napi működés minimális mértékű megszakításával megoldani. Abban mindannyian egyetértenek, hogy a forgalomirányítók és kapcsolók frissítése a szokásos előre tervezett karbantartási időben (vasárnap hajnalban 2:00 –től 8:00-ig) megtehető. Az eszközök nagy száma miatt azonban ez valószínűleg egynél több vasárnapot fog igénybe venni.

A stadion hálózatának új tervezetében három különböző típusú hálózati eszköz szerepel:

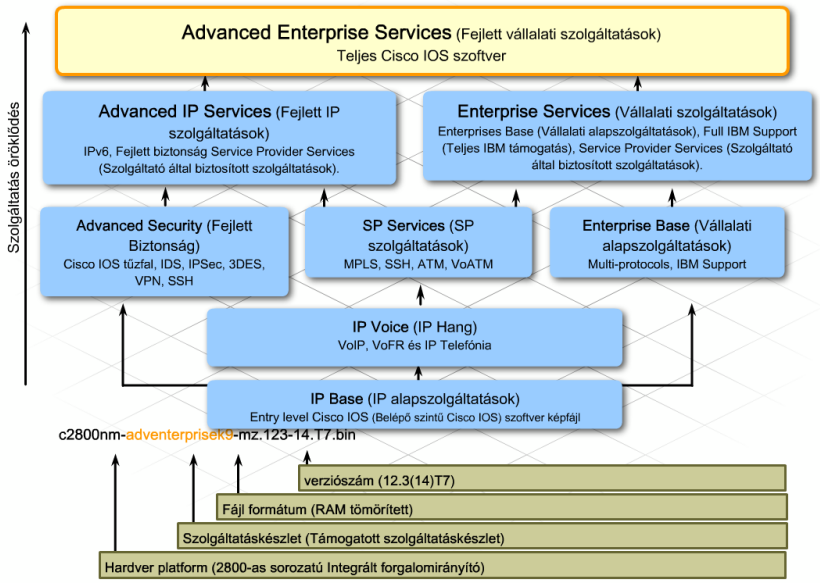
- 16 db Cisco 2960-as kapcsoló
- 1 db Cisco 1841-es forgalomirányító
- 3 db nem Cisco forgalomirányító

Miután megtörtént a Cisco IOS szoftver verziójának és a szükséges hardverelemeknek a kiválasztása, a Hálózat Kft. dolgozói már meg tudják becsülni a Cisco eszközök frissítéséhez szükséges időt. A nem Cisco-forgalomirányítókat egy későbbi időpontban frissítik.

IOS szoftver fájlnév konvenciók

Az IOS fájlokat mindig frissíteni kell a hibajavítások telepítése és a biztonsági kockázatok csökkentése érdekében. A stadion hálózatának néhány eszközén már elavult IOS verziók találhatók.

Az IOS fájlok elnevezése az IOS szolgáltatáskészletét és verziószámát mutatja.

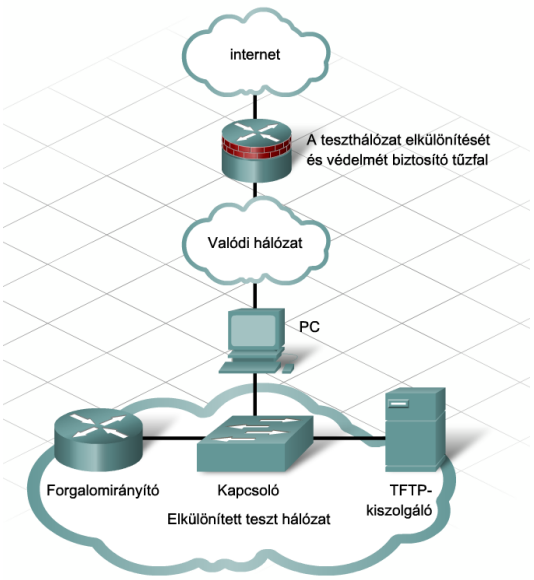


Ha egy forgalomirányítón vagy kapcsolón a Cisco IOS szoftvert frissítik, akkor az eszközt újra kell indítani, ami az eszköz rövid ideig tartó működéskiesését okozza. Mint minden frissítésnél, egy új hardverelem vagy az IOS telepítése során is előre nem látható problémák jelentkezhetnek. A frissítéseket jól meg kell tervezni, így elkerülhető, hogy a hálózat normális működési idejében kimaradás lépjen fel.

A frissítési eljárás tesztelése

A lehetséges problémák elkerülése érdekében a Hálózat Kft. beszerez egy 2960-as kapcsolót és egy 1841-es forgalomirányítót. Ezeken az eszközökön tesztelik a frissítési eljárást, mielőtt valóban belekezdenének a stadion eszközeinek frissítésébe. A tesztelés azért is jó módszer, mivel jelentős eltérések adódhatnak az egyes IOS verziók vagy hardver elemek között.

A teszteszközök használatával a Hálózat Kft. meggyőződhet arról, hogy a frissített rendszer valóban az elvárásoknak megfelelően fog működni. Az is jobban megbecsülhető lesz, hogy a frissítési folyamathoz mennyi idő szükséges.



3.2.3 Megfelelő Cisco IOS szoftverfájl kiválasztása

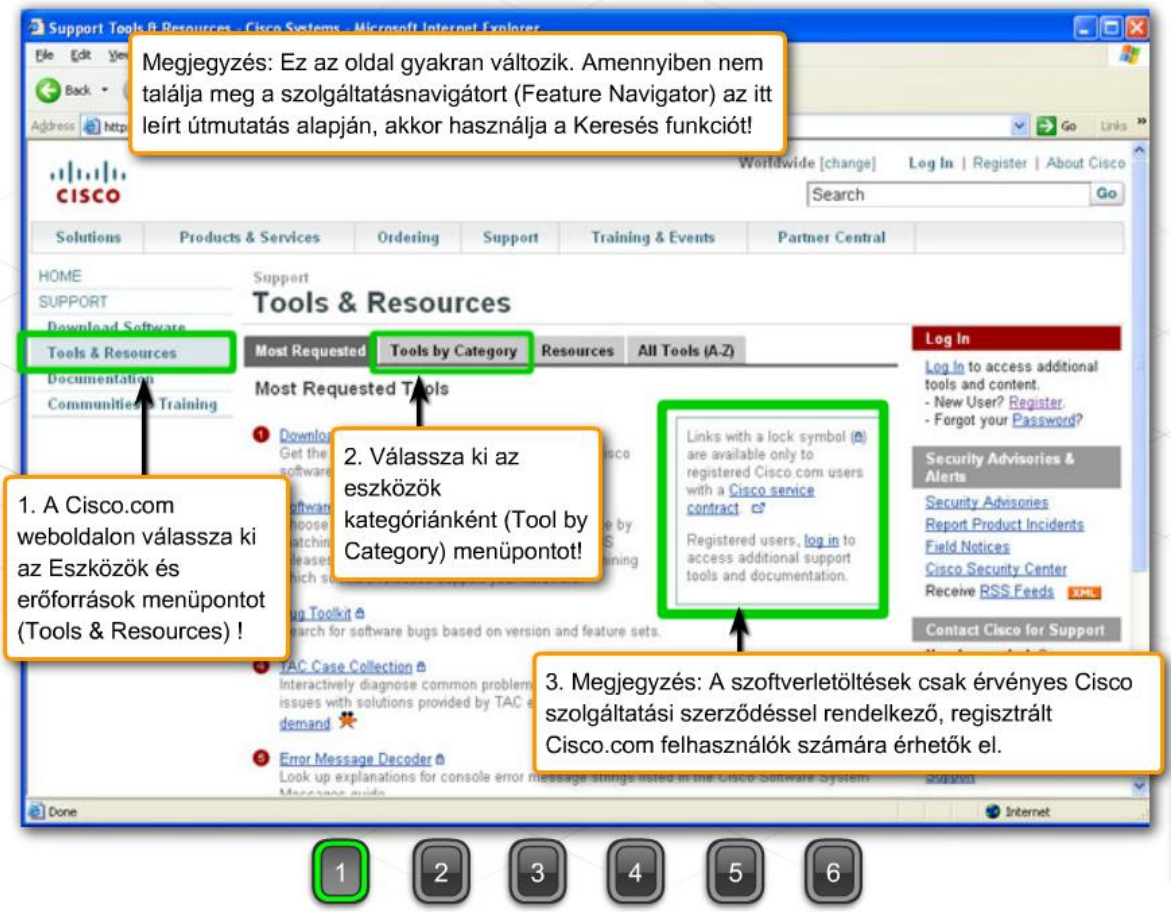
A Hálózat Kft. dolgozóinak meg kell határozniuk, hogy a jelenlegi eszközök megfelelőek-e a szükséges új szolgáltatásokat is támogató Cisco IOS verzió futtatására. Ez a frissítési folyamat fontos lépése.

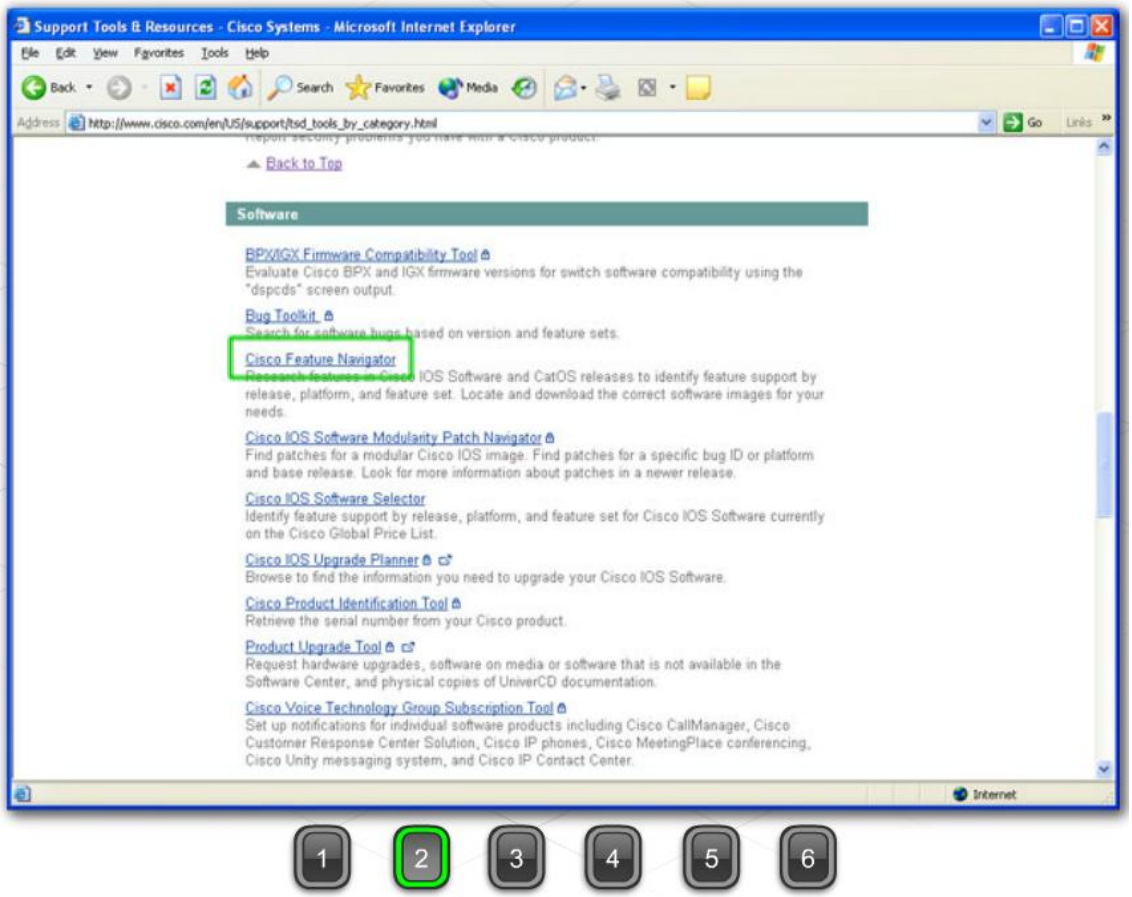
A szolgáltatásnavigátor (Feature Navigator) használata

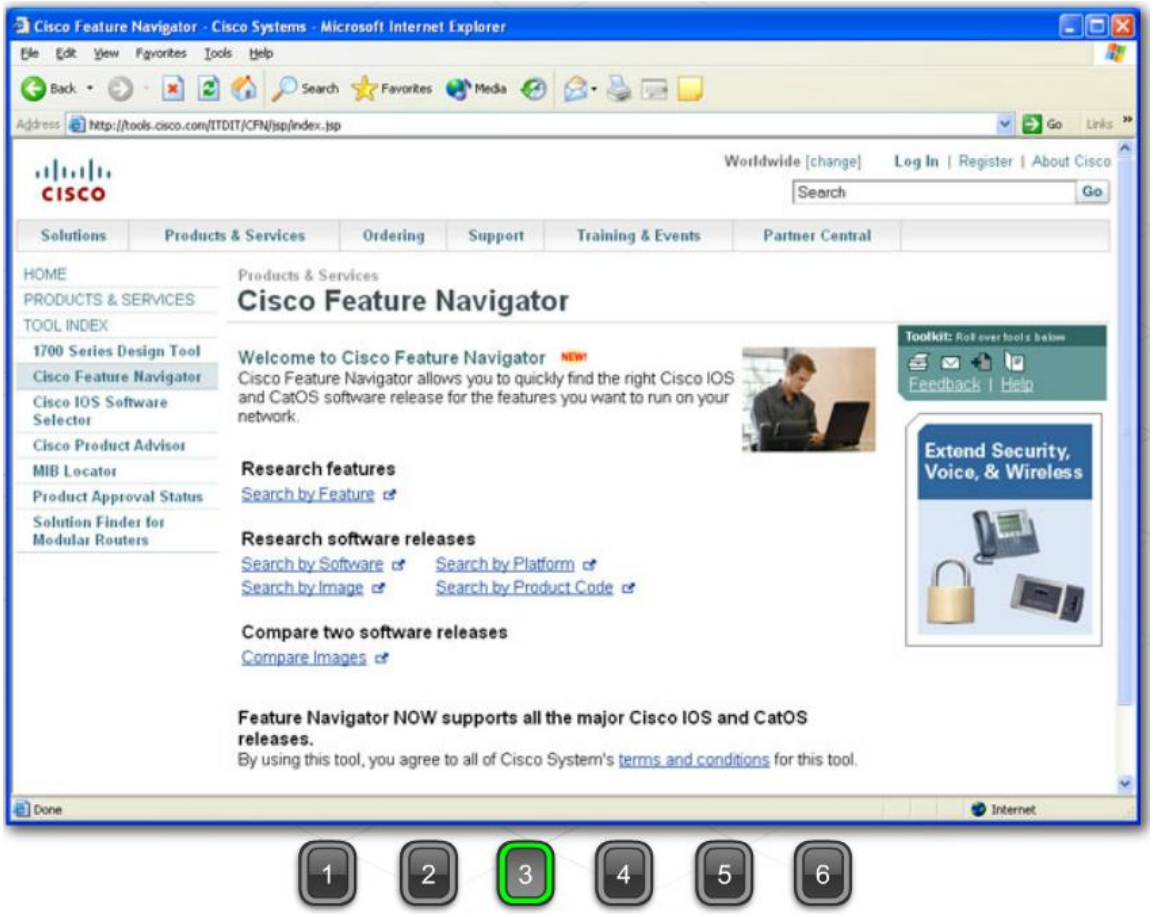
A Cisco.com weboldal olyan eszközöket is tartalmaz, melyek segítik a Hálózat Kft. dolgozóit a megfelelő IOS verzió kiválasztásában. A szolgáltatásnavigátor (Feature Navigator) egy olyan webalapú eszköz, mely megmutatja, hogy milyen szolgáltatásokat támogatnak az egyes IOS szoftverfájlok, illetve, hogy melyik IOS szoftverfájl támogat egy-egy meghatározott szolgáltatást.

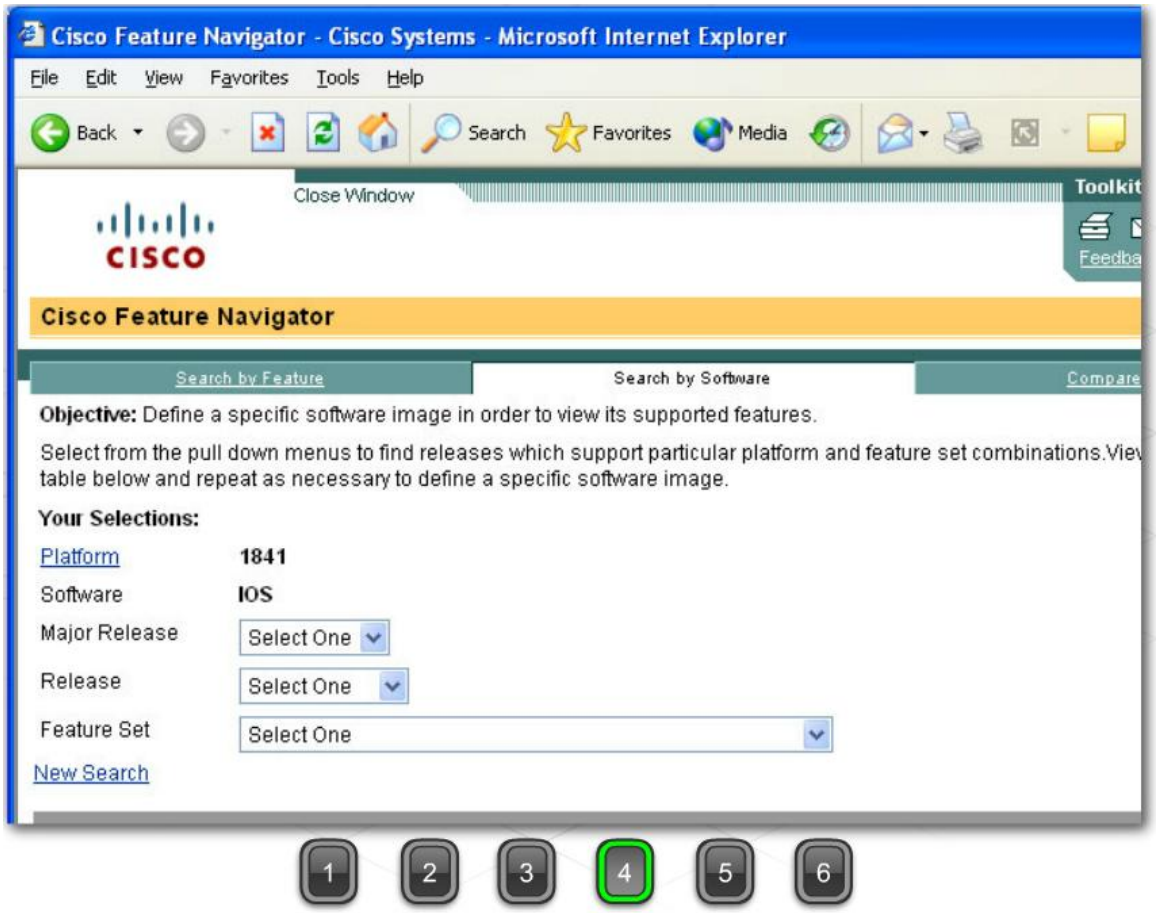
A szolgáltatásnavigátorral szolgáltatás és verziószám alapú keresésre is lehetőség van. A kiadási verziók (release version) részen belül a szakemberek egy oldalon belül tudják összehasonlítani az egyes változatokat. Regisztrált Cisco.com felhasználók a szolgáltatásnavigátort a http://www.cisco.com/go/fn címen érhetik el.

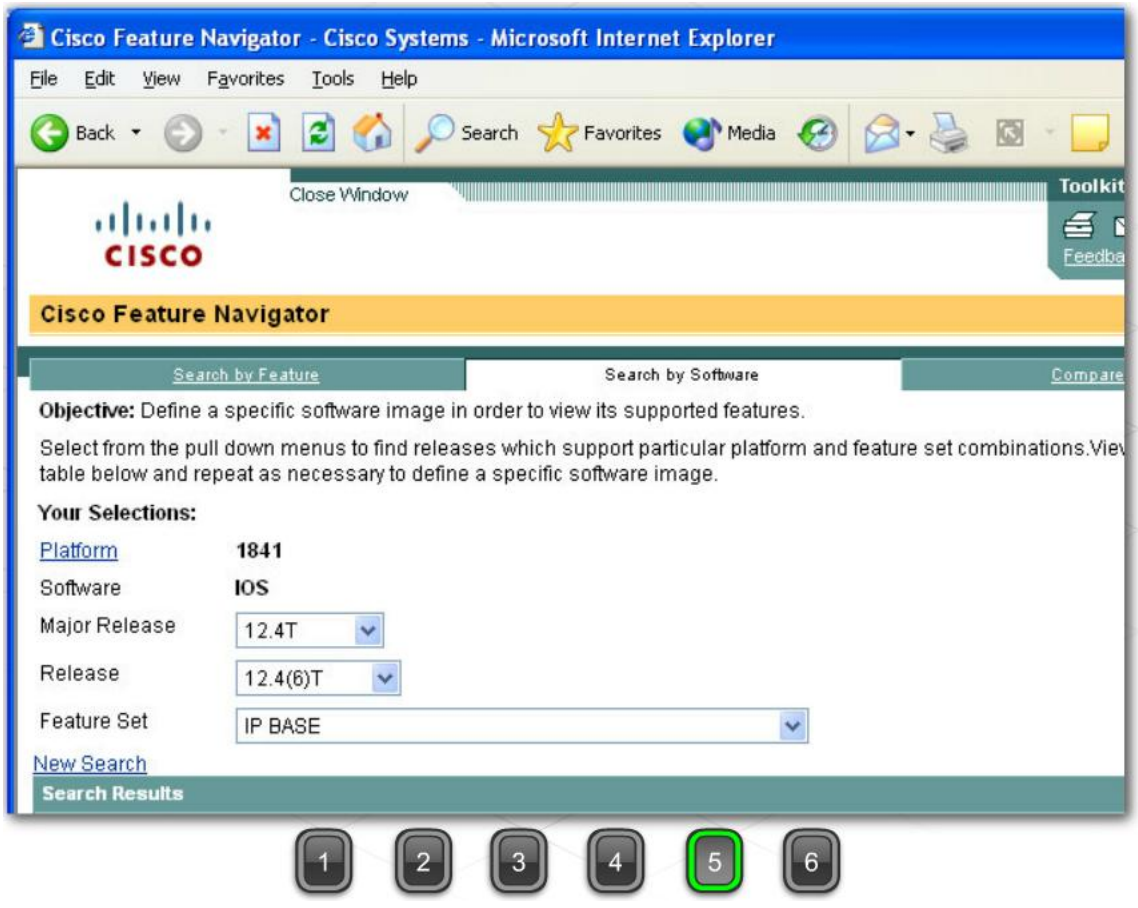
Az IOS szoftverek eltérő szolgáltatáskészlettel rendelkeznek a különböző kapcsoló és forgalomirányító platformok támogatására. A vállalat dolgozói a nyilvántartási lista és a szükséges szolgáltatások figyelembe vételével, a szolgáltatásnavigátor segítségével választják ki a telepített eszközökön alkalmazható IOS verziókat.

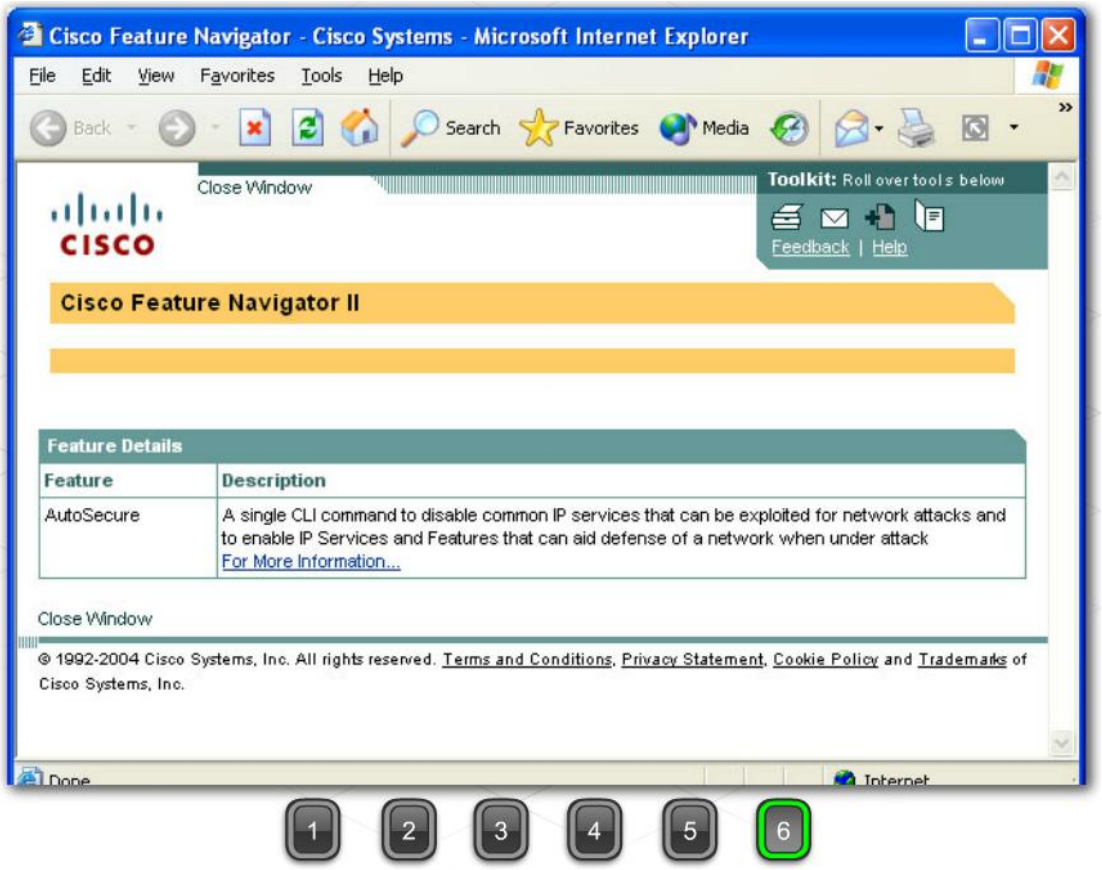



Support Tools & Resources - Cisco Systems - Microsoft Internet Explorer
Back to Top
Software
BPX/IGX Firmware Compatibility Tool
Evaluate Cisco BPX and IGX firmware versions for switch software compatibility using the "dspcds" screen output.
Bug Toolkit
Cisco Feature Navigator
IOS Software and CatOS releases to identify feature support by release, platform, and feature set. Locate and download the correct software images for your needs.
Cisco IOS Software Modularity Patch Navigator
Find patches for a modular Cisco IOS image. Find patches for a specific bug ID or platform and base release. Look for more information about patches in a newer release.
Cisco IOS Software Selector
Identify feature support by release, platform, and feature set for Cisco IOS Software currently on the Cisco Global Price List.
Cisco IOS Upgrade Planner
Browse to find the information you need to upgrade your Cisco IOS Software.
Cisco Product Identification Tool
Retrieve the serial number from your Cisco product.
Product Upgrade Tool
Request hardware upgrades, software on media or software that is not available in the Software Center, and physical copies of UniverCD documentation.
Cisco Voice Technology Group Subscription Tool
Set up notifications for individual software products including Cisco CallManager, Cisco Customer Response Center Solution, Cisco IP phones, Cisco MeetingPlace conferencing, Cisco Unity messaging system, and Cisco IP Contact Center.
1
2
3
4
5
6


Cisco Feature Navigator - Cisco Systems - Microsoft Internet Explorer
Worldwide [change]
Log In | Register | About Cisco
Search
Go
Solutions
Products & Services
Ordering
Support
Training & Events
Partner Central
HOME
PRODUCTS & SERVICES
TOOL INDEX
1700 Series Design Tool
Cisco Feature Navigator
Cisco IOS Software Selector
Cisco Product Advisor
MIB Locator
Product Approval Status
Solution Finder for Modular Routers
Products & Services
Cisco Feature Navigator
Welcome to Cisco Feature Navigator
Cisco Feature Navigator allows you to quickly find the right Cisco IOS and CatOS software release for the features you want to run on your network.
Toolkit:
Feedback | Help
Extend Security, Voice, & Wireless
Research features
Search by Feature
Research software releases
Search by Software
Search by Platform
Search by Image
Search by Product Code
Compare two software releases
Compare Images
Feature Navigator NOW supports all the major Cisco IOS and CatOS releases.
By using this tool, you agree to all of Cisco System's terms and conditions for this tool.
1
2
3
4
5
6


Cisco Feature Navigator - Cisco Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Close Window
Toolkit
Feedba
CISCO
Cisco Feature Navigator
Search by Feature
Search by Software
Compare
Objective: Define a specific software image in order to view its supported features.
Select from the pull down menus to find releases which support particular platform and feature set combinations.Viev
table below and repeat as necessary to define a specific software image.
Your Selections:
Platform 1841
Software IOS
Major Release Select One
Release Select One
Feature Set Select One
New Search
1 2 3 4 5 6


Cisco Feature Navigator - Cisco Systems - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Close Window
Toolkit
Feedba
CISCO
Cisco Feature Navigator
Search by Feature
Search by Software
Compare
Objective: Define a specific software image in order to view its supported features.
Select from the pull down menus to find releases which support particular platform and feature set combinations.Viev
table below and repeat as necessary to define a specific software image.
Your Selections:
Platform 1841
Software IOS
Major Release 12.4T
Release 12.4(6)T
Feature Set IP BASE
New Search
Search Results
1 2 3 4 5 6



Cisco IOS verzió kódok:

Korai kiadás (ED)

A korai kiadás (ED) az új szolgáltatásokat és platformot támogató szofververzióra utal. A kiadások hibajavítást is biztosítanak.

Korlátozott kiadás (LD)

A Cisco IOS és a Catalyst OS (CatOS) szoftverek sorozatának többsége általában az életciklusának ún. "Korlátozott kiadás" fázisában van, a korai kiadás és az általános kiadás mérdföldkövei között. Semmilyen új szolgáltatást vagy platformot nem nyújt ez a fázis, mindössze hibajavítást.

Általános kiadás (GD)

Az az időpont, amikor a szoftver eléri az életcilusának "Általános kiadás" mérdföldkövét. A Cisco IOS és a Catalyst OS (CatOS) szoftverek alapkiadás általában akkor éri el az "Általános kiadás" mérföldkövet, amikor a Cisco, úgy érzi, hogy minden olyan felhasználói hálózatban megfelelően működne a szoftver, ahol ezekre a szolgáltatásokra szükség van. A Cisco IOS alapkiadásának egy példája, mely elérte a GD-t a 12.2-es verzió. A CatOS kiadási sorozatának egy példája, mely elérte a GD-t a 7.x. Az Általános kiadás mérföldköve a felhasználói visszajelzéseken, teszthálózati alkalmazásokon, CE hibajelentéseken és tapasztalaton alapul, de más is befolyásolhatja.

A Hálózat Kft. dolgozói meghatározzák a megfelelő Cisco IOS szoftver-verziót. Ezt követően a szakembereknek meg kell győződniük arról, hogy az eszközökben van elegendő flash memória és RAM az új IOS futtatásához. Ha nincs, akkor a memóriabővítést még az IOS telepítése előtt el kell végezni.

A stadiont üzemeltető cég rendelkezik Cisco karbantartási szerződéssel, mely lehetővé teszi szakembereik számára az új IOS verziók letöltését. A stadion vezetőségének biztosítania kell a Hálózat Kft. dolgozóit, hogy a cég megfelelő Cisco licencszerződéssel rendelkezik. A Hálózat Kft. szakembereinek ellenőriznie kell, hogy minden Cisco eszközt belefoglaltak-e a karbantartási szerződésbe.

A Hálózat Kft. dolgozói letöltik az új IOS verziókat a Cisco.com weboldaláról, melyeket ezután már TFTP kiszolgálón is tárolhatnak. A TFTP kiszolgálón történő tárolás egyik nagy előnye, hogy a szoftver onnan könnyen letölthető a forgalomirányítókra és a kapcsolókra.

A letöltéshez a `copy` parancs használható.

3.2.4 Cisco IOS szoftver letöltése és telepítése

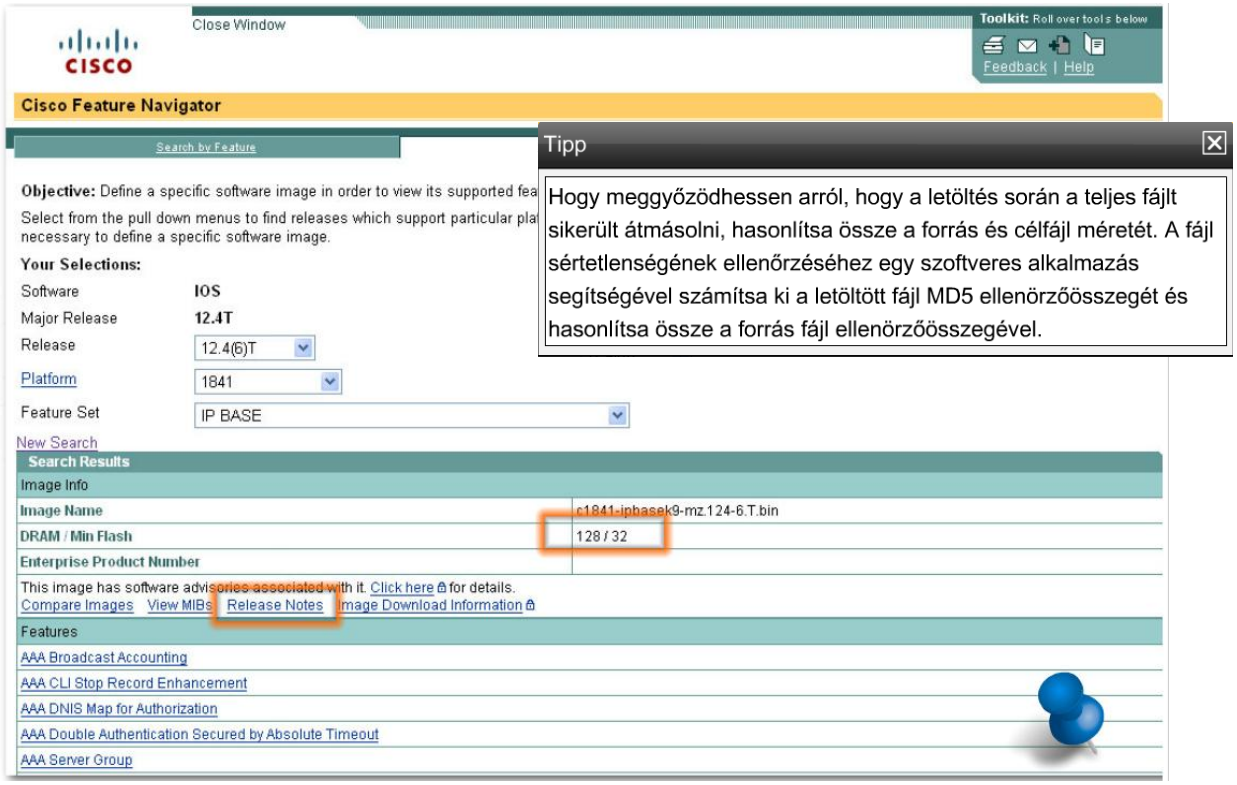
A stadion forgalomirányítója és kapcsolói nem rendelkeznek a legújabb Cisco IOS verzióval. A szükséges frissítést a következő lépések manuális végrehajtásával kell megoldani:

1. lépés: Az IOS szoftver kódfájl kiválasztása

A frissítési folyamat első lépése a megfelelő IOS szoftver verziójának és szolgáltatáskészletének kiválasztása a következő tényezők figyelembe vételével:

- **Memória szükséglet** – Biztosítani kell, hogy a forgalomirányító elegendő lemezterülettel vagy flash memóriával rendelkezzen az IOS tárolásához. A forgalomirányítónak elég memóriával (DRAM) kell rendelkeznie az IOS futtatásához is. Ha nincs elegendő memória, akkor problémák léphetnek fel az új IOS-sel történő indítás során.
- **Interfészek és modulok támogatása** – Ellenőrízni kell, hogy az új IOS valóban támogatja-e a jelenlegi és a telepítésre váró új interfészeket, modulokat.
- **Szoftver szolgáltatások támogatása** – Az új és a régi IOS tulajdonságainak összehasonlításával ellenőrízni kell, hogy a frissítés támogatja-e az összes régi és új szolgáltatást.

A Hálózat Kft. dolgozói a szolgáltatásnavigátor használatával választják ki a hálózat eszközein alkalmazható és a követelményeknek is megfelelő IOS állományokat. Letöltik és átmásolják az IOS fájlokat a TFTP kiszolgáló letöltési könyvtárába. A kiválasztott verzióval kapcsolatos megjegyzéseket is elolvassák, hogy a verziót érintő minden változással tisztában legyenek.



2. lépés: A kódfájl helyének meghatározása az eszköz fájlrendszerében

A Hálózat Kft. dolgozói a `show file systems` parancs kimenetéből határozzák meg a Cisco IOS fájlok és kódfájlok helyét. A show file systems vagy a `dir [file_system]` parancs használható annak megállapítására, hogy van-e megfelelő méretű szabad tárterület az új IOS fájl tárolásához. Ha az eszközökön nincs elegendő flash memória, akkor memóriabővítésre van szükség az új IOS telepítése előtt.

3. lépés: A TFTP kiszolgáló és az érintett eszköz közötti IP kapcsolat ellenőrzése

A TFTP kiszolgáló és a frissíteni kívánt eszköz között működő hálózati kapcsolatra van szükség, így a TFTP kiszolgálóról meg kell tudni pingelni az érintett eszköz IP-címét. Ehhez vagy az szükséges, hogy az eszköz kapcsolódó interfésze és a TFTP kiszolgáló IP-címe egy cimtartományban legyen, vagy az eszközön megfelelő alapértelmezett átjárót kell beállítani.

```
Press RETURN to get started.

Router>enable
Router#show file systems
File Systems:

     Size(b)     Free(b)      Type   Flags   Prefixes
           -           -    opaque      rw   archive:
           -           -    opaque      rw   system:
           -           -   network      rw   snmp:
           -           -    opaque      rw   null:
           -           -   network      rw   tftp:
      196600      194617      nvram      rw   nvram:
* 326071680     7380992       disk      rw   flash:#
           -           -    opaque      rw   xmodem:
           -           -    opaque      rw   ymodem:
           -           -   network      rw   rcp:
           -           -   network      rw   ftp:
           -           -   network      rw   http:
           -           -    opaque      ro   tar:
           -           -    opaque      ro   cns:

Router#_
```

4. lépés: Az aktuális konfiguráció elmentése a frissítés előkészítésére

A konfigurációs fájlokat és az IOS aktuális változatát el kell menteni a Cisco IOS frissítése előtt. Az aktív konfigurációt indító konfigurációként kell elmenteni, majd az aktuális IOS kódfájllal együtt egy TFTP kiszolgálóra kell másolni. Néhány IOS változat alapértelmezett konfigurációval rendelkezik. Ezek a beállítások megzavarhatják az aktuális konfiguráció beállításait.

5. lépés: Az IOS kódfájl átmásolása az eszközre

Amennyiben a TFTP kiszolgáló és az érintett eszköz között sikeres a ping, a Hálózat Kft. dolgozói készen állnak az IOS képfájl flash memóriába történő másolására. Mielőtt a másolást elkezdenék, ellenőrizni kell, hogy a TFTP kiszolgáló szoftver valóban fut, és a kiválasztott IOS kódfájl a TFTP kiszolgáló megfelelő könyvtárában található.

Az IOS átmásolása a `copy tftp flash` paranccsal történik.

A másolási folyamat eltart néhány percig. A `dir flash` paranccsal ellenőrizhető a fájlátvitel sikeressége.

A frissítés befejezéséhez szükség van az eszköz újraindítására és a rendszerindítási folyamat ellenőrzésére.

A szakemberek elvégzik a frissítést a hálózati teszteszközökön. A frissítés után összehasonlítják az elmentett és a frissítés eredményeként született konfigurációt, majd megbizonyosodnak arról, hogy a különbségek nem okoznak problémát a stadion hálózatának működésében.

3.2.5 A forgalomirányító rendszerindítási folyamata

A rendszerindítási folyamat három szakaszból áll.

1. Az önellenőrzés (POST) és a rendszerbetöltő program (bootstrap) futtatása.

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. A rendszerindító program megkeresi a Cisco IOS szoftvert, majd betölti a RAM-ba.

2. IOS szoftver megkeresése és betöltése

Az IOS kód pontos helyét a konfigurációs regiszter bitjeinek értéke határozza meg. A beállított bitek alapján az eszköz az IOS fájlt a következő helyekről töltheti be:

- Flash memória
- TFTP kiszolgáló
- Egy másik, az indító konfigurációban meghatározott hely

Az IOS flash-ből történő betöltéséhez a konfigurációs regiszter értékének 0x2102-nek kell lennie.

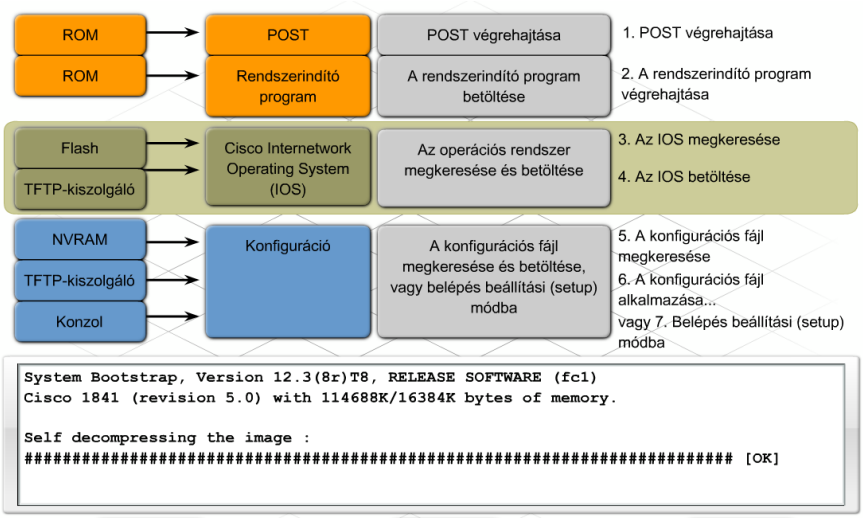
3. Az indítási konfigurációt tartalmazó állomány megkeresése és betöltése, vagy belépés beállítási módba

A Cisco IOS szoftver betöltése után a rendszerindító program az NVRAM-ban keresi az indító konfigurációs fájlt (startup-config). Ez a fájl tartalmazza az előzőleg elmentett beállítási parancsokat és paramétereket, beleértve:

- az interfészek címeit,
- a forgalomirányítási információkat,
- a jelszavakat
- és az egyéb konfigurációs paramétereket

Ha a konfigurációs fájl nem érhető el, akkor a forgalomirányító beállítási (setup) módba lép a konfigurációs folyamat megkezdéséhez.

Ha az indító konfigurációs fájl elérhető, akkor a képernyőn az állomásnevet tartalmazó prompt jelenik meg. Ez jelzi, hogy a Cisco IOS szoftver és a konfigurációs fájl betöltése a forgalomirányítón sikeresen megtörtént, és a Hálózat Kft. dolgozói megkezdhetik a forgalomirányítón az IOS parancsok használatát.



3.3 A meglévő hardver frissítése

3.3.1 A telepített hardver tulajdonságainak vizsgálata

A Cisco IOS verzió aktualizálása után a hálózattervező mérnöknek tudnia kell, milyen hardver változtatások hajthatók végre ahhoz, hogy a meglévő eszközök megfeleljenek az új követelményeknek. A bővítés nagysebességű vagy nagybonyolultságú modulokat, valamint olyan hardverelemeket is magában foglalhat amelyek állványba szerelhető eszközkészlet formájában használhatók.

A Cisco.com a stadion hálózatának minden eszközéhez tartalmaz adatlapot. A Hálózat Kft. dolgozói ezen adatlapok segítségével készítenek listát az egyes eszközökön végrehajtható lehetséges változtatásokról.

Az 1841-es forgalomirányító adatlapját a modellhez használható modulok és interfészek meghatározásához használják. Számos különböző típusú modul csatlakoztatható az 1841-es forgalomirányító két bővítőhelyéhez, például:

- WAN interfész kártyák (WIC)
- Nagysebességű WAN interfész kártyák (HWIC)
- Hang/WAN interfész kártyák (VWIC)
- Vezetéknélküli WIC-ek, melyek hozzáférési pontként (Access Point) is működhetnek
- Gigabit Ethernet HWIC-ek az üvegszálas összeköttetés biztosításához

A hálózattervező mérnök ezen lista alapján határozza meg, milyen összetevők szükségesek ahhoz, hogy az eszközök megfeleljenek az új hálózattal szemben támasztott elvárásoknak.

A forgalomirányító belső nézete

A forgalomirányító hátoldali nézete

A forgalomirányító belső nézete

A forgalomirányító hátoldali nézete

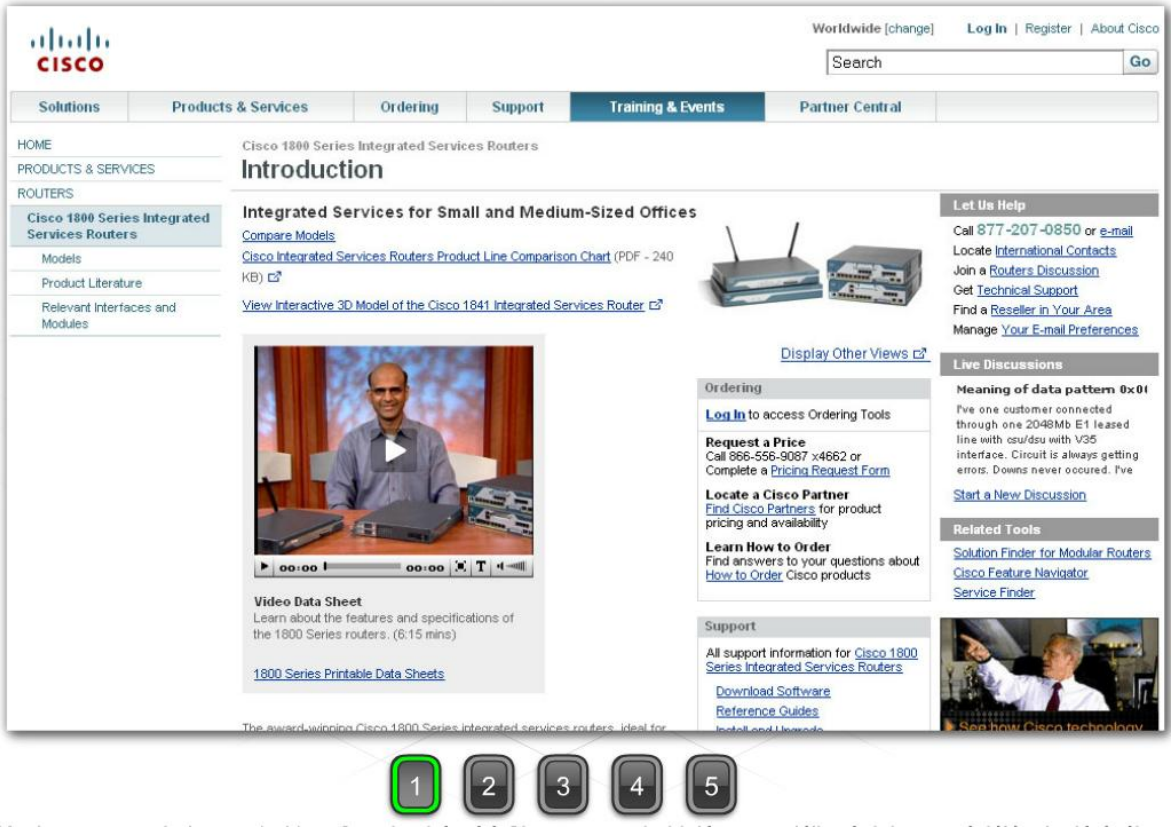
3.3.2 Az opcionálisan telepíthető hardverelemek vizsgálata

Az egyes hardvereszközök különböző tulajdonságokkal rendelkeznek. Fontos megvizsgálni, hogy egy adott forgalomirányító egy-egy modulja milyen technológiát és átviteli közeget támogat. A hálózattervező mérnök megállapítja, mely technológiákat lehet nagy valószínűséggel alkalmazni a stadion új hálózatában.

A hang-, video- és adatforgalom hálózaton történő átviteléhez a tervező a technológiák és átviteli közegek következő listáját állítja össze:

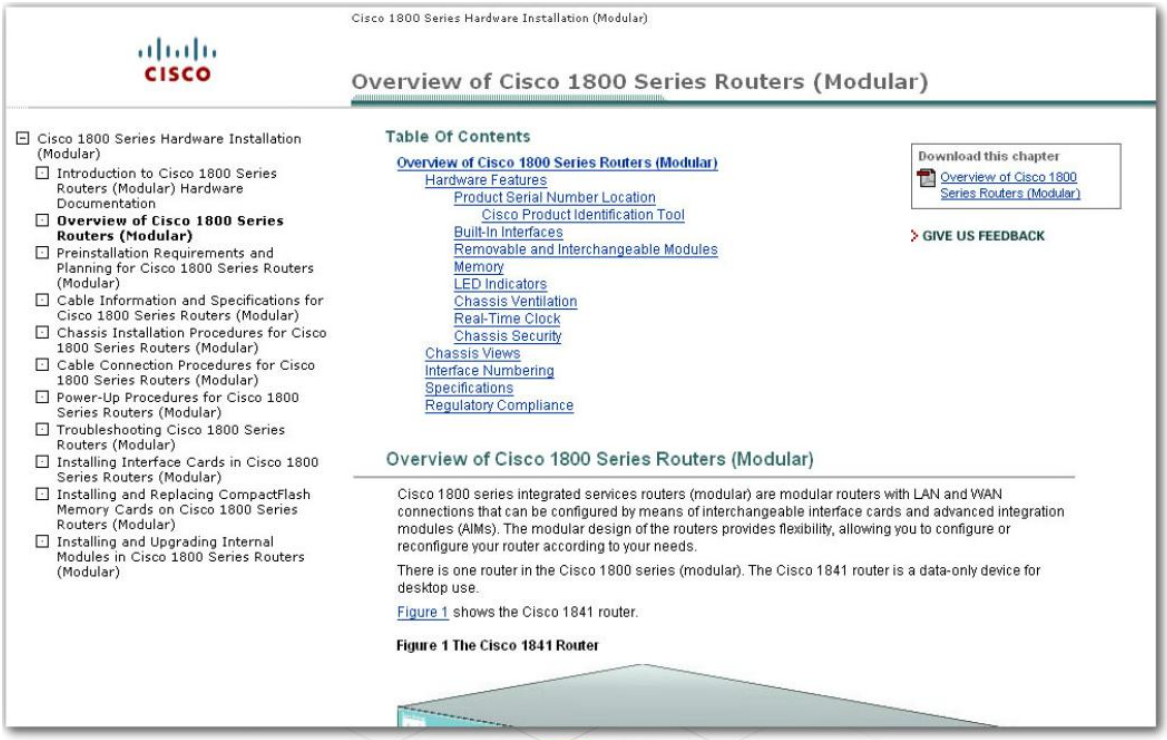
- Üvegszálas Gigabit Ethernet a központi és elosztási rétegekben
- 100 Mbit/sec-os rézkábeles összeköttetés a hozzáférési rétegben
- Gigabit Ethernet üvegszálon vagy rézkábelen az adatközpontban
- Nagysebességű soros kapcsolat a két WAN összeköttetésen
- Nagysebességű digitális előfizetői vonal (DSL) az internetcsatlakozáshoz

A tervező összehasonlítja ezt a listát az 1841-es forgalomirányítónak a Cisco.com weboldalán megtalálható dokumentációjában felsorolt opcionális hardverelemeivel. Lehet, hogy a már meglévő 1841-es forgalomirányító támogatja a WAN összeköttetésekhez és az internetcsatlakozáshoz szükséges modulokat.




Bekabeling en installatie voor Cisco 1801-, Cisco 1802- en Cisco 1803-routers met geïntegreerde services (PDF - 2 MB)
Bekabeling en installatie voor Cisco 1811- en Cisco 1812-routers met geïntegreerde services (PDF - 2 MB)
Cisco 1800 Series (Modular)
Cisco 1800 Series Integrated Services Routers (Modular) Quick Start Guide
Cisco 1800 Series Integrated Services Routers (Modular) Quick Start Guide - Simplified Chinese (PDF) (PDF - 3 MB)
Cisco 1800 Series Integrated Services Routers (Modular) Quick Start Guide - Spanish (PDF) (PDF - 1 MB)
Cisco 1800 Series Hardware Installation (Modular)
Regulatory Compliance and Safety Information for Cisco 1840 Routers
Cisco Interface Cards
Quick Start Guide: Interface Cards for Cisco Access Routers
Cisco Interface Cards Hardware Installation Guide
Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information


1
2
3
4
5


Cisco 1800 Series Hardware Installation (Modular)
Overview of Cisco 1800 Series Routers (Modular)
Cisco 1800 Series Hardware Installation (Modular)
Introduction to Cisco 1800 Series Routers (Modular) Hardware Documentation
Overview of Cisco 1800 Series Routers (Modular)
Preinstallation Requirements and Planning for Cisco 1800 Series Routers (Modular)
Cable Information and Specifications for Cisco 1800 Series Routers (Modular)
Chassis Installation Procedures for Cisco 1800 Series Routers (Modular)
Cable Connection Procedures for Cisco 1800 Series Routers (Modular)
Power-Up Procedures for Cisco 1800 Series Routers (Modular)
Troubleshooting Cisco 1800 Series Routers (Modular)
Installing Interface Cards in Cisco 1800 Series Routers (Modular)
Installing and Replacing CompactFlash Memory Cards on Cisco 1800 Series Routers (Modular)
Installing and Upgrading Internal Modules in Cisco 1800 Series Routers (Modular)
Table Of Contents
Overview of Cisco 1800 Series Routers (Modular)
Hardware Features
Product Serial Number Location
Cisco Product Identification Tool
Built-In Interfaces
Removable and Interchangeable Modules
Memory
LED Indicators
Chassis Ventilation
Real-Time Clock
Chassis Security
Chassis Views
Interface Numbering
Specifications
Regulatory Compliance
Download this chapter
Overview of Cisco 1800 Series Routers (Modular)
GIVE US FEEDBACK
Overview of Cisco 1800 Series Routers (Modular)
Cisco 1800 series integrated services routers (modular) are modular routers with LAN and WAN connections that can be configured by means of interchangeable interface cards and advanced integration modules (AIMs). The modular design of the routers provides flexibility, allowing you to configure or reconfigure your router according to your needs.
There is one router in the Cisco 1800 series (modular). The Cisco 1841 router is a data-only device for desktop use.
Figure 1 shows the Cisco 1841 router.
Figure 1 The Cisco 1841 Router


1
2
3
4
5

system software image from flash memory. It also stores the system configuration file and the virtual configuration register.

Table 2 lists the memory specifications for Cisco 1800 series routers.

Table 2 Router Memory Specifications

Description	Specification
SDRAM	128 MB, expandable to 384 MB; default is 128 MB
Flash memory	32, 64, or 128 MB; default is 32MB
Boot/NVRAM	2/4 MB flash memory

Note SDRAM and the flash memory are user-upgradable, but the boot/NVRAM is permanently soldered to the router's motherboard and is not upgradable.

LED Indicators

1 2 3 4 5

Table 1 WAN and LAN Connections

Port or Connection	Port Type, Color[1]	Connected to:	Cable
Fast Ethernet (FE)	RJ-45, yellow	Ethernet hub.	Crossover to connect to a router Straight-through to connect to a switch
T1/E1 WAN	RJ-48C	T1 or E1 network or CSU/DSU.	RJ-48 T1/E1 straight-through (Crossover to connect ot a PBX or any other equipment)
Cisco serial (1T)	60-pin D-sub, blue	CSU/DSU and serial network or equipment.	Cisco serial transition cable that matches the signaling protocol (EIA/TIA-232, EIA/TIA-449, V.35, X.21, or EIA/TIA-530) and the serial port operating mode (DTE or DCE). Refer to the *Cisco Modular Access Router Cable Specifications* document for information about selecting these cables.
Cisco Smart serial (2T)	Cisco Smart compact connector, blue	CSU/DSU and serial network or equipment. For WIC-2T and WIC-2A/S only.	
DSL	RJ-11C/RJ-14C	Network demarcation device for service provider's DSL interface.	RJ-11 straight-through for 2-wire RJ-14 straight-through for 4-wire

1 2 3 4 5

3.3.3 Új hardverelem telepítése

Opcionális interfészkártyák telepítése az 1841-es forgalomirányítókon

A Hálózat Kft. dolgozói a Cisco.com weboldalán keresik meg az opcionális interfészkártyák telepítési útmutatóját. A kártyák telepítésének folyamata a következő lépésekből áll:

1. lépés: A forgalomirányító áramtalanítása

Az 1841-es forgalomirányító bővítőhelyei nem támogatják az üzem közben cserélhető (hot-swappable) interfészkártyákat, melyek a forgalomirányító bekapcsolt állapotában is ki-, behelyezhetők.

2. lépés: A bővítő helyek előlapjának eltávolítása

1-es méretű Phillips csillagcsavarhúzó vagy egyszerű Egyélű csavarhúzó használható a rögzítő csavarok eltávolításához. Ezután a bővítő helyek előlapja levehető.

3. lépés: Az opcionális modul telepítése

- A telepítés alatt az elektrosztatikus kisülés kockázatának és károsító hatásának csökkentése érdekében az elektronikus eszközökön végzett munka során mindig használjunk megfelelően földelt antisztatikus csuklópántot, és a kártyát az élénél fogjuk meg.
- A kártyát a szélénél fogjuk meg, így elkerülhetjük a statikus kisülésekből fakadó meghibásodást.
- Igazítsuk a kártyát a bővítőhely sínjeihez majd finoman csúsztassuk be.
- Addig toljuk a kártyát, míg a sarokérintkezők bizonságosan nem csatlakoznak! Az előlapnak hozzá kell érnie a panel hátsó részéhez.
- Az előlap rögzítőcsavarjait helyezzük vissza és húzzuk meg!

4. lépés: A forgalomirányító bekapcsolása és az új konfiguráció ellenőrzése

- Csatlakoztassunk számítógépet a forgalomirányító konzol portjához, és figyeljük meg a rendszerindítási folyamatot!
- Ellenőrizzük, hogy a forgalomirányító valóban felismeri-e az új opcionális interfészkártyát!
- Jegyezzük fel az új eszköz interfészének jelölését a nyilvántartási listára és a meglévő topológiai diagramra!

3.4 A vezetéknélküli hálózatok jellemezése

3.4.1 A közönség által látogatható helyszínek megtekintése

A meglévő hálózat felmérésének következő lépése a vezetéknélküli LAN hálózat (WLAN) használatának kiértékelése. A konfigurációk különbözőségéből, a hozzáférési pontok elhelyezéséből és a fizikai környezetből adódóan minden WLAN megvalósítás egyedi.

A vezetéknélküli hálózat megtervezésének befejezése előtt a Hálózat Kft. dolgozói helyszíni felmérést végeznek a vezetéknélküli hálózati eszközök optimális használatának és elhelyezésének meghatározásához. Ez a felmérés nyújt megfelelő információt a WLAN hozzáférési pontok típusának, elhelyezésének, és lefedettségi területeinek megválasztásához.

A vezetéknélküli hálózat helyszíni felmérésénél a Hálózat Kft. dolgozóinak a nyilvános helyeket, az irodákat és az üzleti élet helyszíneit is végig kell látogatniuk.

Amikor a Hálózat Kft. dolgozói a stadionban megjelennek, akkor a vállalatukat képviselik, ezért a megfelelő viselkedés és megjelenés elengedhetetlen. A dolgozók szakmai hozzáértése és viselkedése pozitív visszajelzést ad a Hálózat Kft. által elvégzett bővítési folyamatról.

A vezetéknélküli hálózat helyszíni felmérésére készülve a Hálózat Kft. dolgozóinak a saját cégük irányelvei szerint kell eljárniuk.

A következő útmutató a sportstadion helyszíni felméréséhez készült:

Előkészítés

- Egyeztessük a helyszíni felmérés időpontját az ügyféllel!
- Öltözzünk megfelelően a feladathoz!
- Viseljük vagy vigyük magunkkal a vállalat igazolványát.
- Vigyük magunkkal a szükséges felszerelést! (Készítsünk listát, hogy minden szükséges kellék ott legyen!)
- Tájékoztassuk a stadion személyzetét, hogy mikor érkeznek a szakemberek és hogy körülbelül meddig tart a felmérés!

A helyszíni szemle

- Jelentkezzünk a megfelelő helyen a stadionba való belépéskor!
- Gyorsan és hozzáértéssel végezzük munkánkat, hogy bizalmat keltsünk az ügyfélben!
- Udvariasan és amennyire csak lehet, pontosan válaszoljunk a kérdésekre!
- Írjuk le azokat a kérdéseket, melyekre más dolgozóktól várjuk a választ!
- Tájékoztassuk az ügyfelet a helyszíni felmérés folyamatáról!
- A helyszín elhagyása előtt értesítsük az ügyfelet a felmérés sikeres befejezéséről!

Biztonság

Számos vállalatnak egyenruhás biztonsági emberei vannak, akiknek tudniuk kell minden látogatásról. Az üzleti életben általában elvárás, hogy a látogató először a központi irodánál jelentkezzen be, és csak utána lépjen más helyiségekbe. A fokozott biztonságot igénylő területek látogatásához engedély, és szükség esetén kíséret szükséges. Ilyenek a hadügy, a kormányzat és a légi közlekedés.

Biztonsági előírások

- Kövessük a biztonsági előírásokat a vezetéknélküli eszközök megfelelő működésének és biztonságos használatának eléréséhez.

- Kérjünk engedélyt, mielőtt a hálózati eszközökhöz nyúlnánk, vagy csatlakoztatnánk azokat a meglévő hálózati berendezésekhez.

Az ügyfél megadhatja a látogatásokkal kapcsolatos elvárásait, melyeket a vezetéknélküli hálózat helyszíni felmérését végző szakembereknek is be kell tartaniuk. Léteznek olyan vállalatok is, melyek a rendszeres látogatások hiányában előre nem fogalmaznak meg helyszíni követelményeket. Ebben az esetben a Hálózat Kft. szakembereinek az időpont egyeztetésekor kell célirányos kérdésekkel megtudakolniuk a látogatással kapcsolatos elvárásokat.

A helyszíni látogatások követelményei közé tartozhatnak:

- Hozzáférési megszorítások
- Ruházat
- Biztonsági felszerelés
- Azonosító kártya
- Felmérés időpontja
- Biztonság
- Tiltások

Az ügyfél elvárásai helyszínről helyszínre változhatnak. A felmérésre készülve a Hálózat Kft. szakembereinek tisztában kell lenniük az elvárásokkal.

3.4.2 A hálózat fizikai felépítésére vonatkozó megfontolások

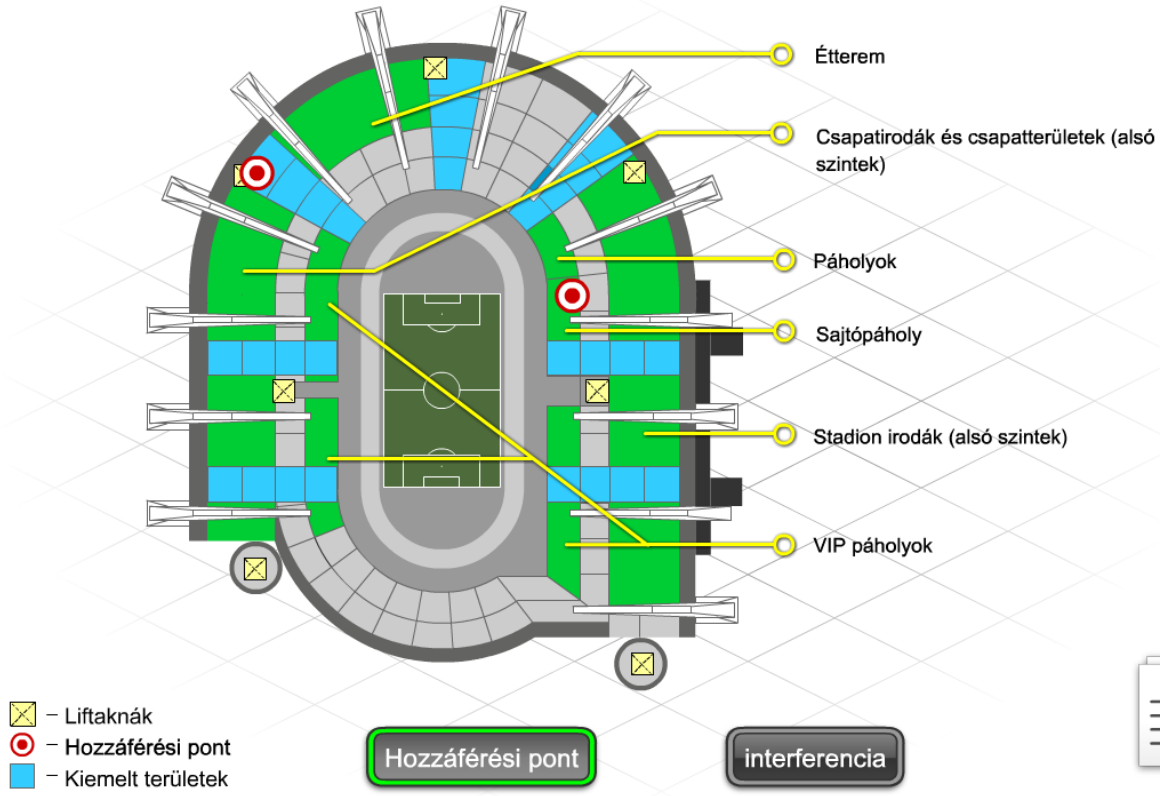
A stadion hálózata a jelenlegi két hozzáférési pontján keresztül csak korlátozott vezetéknélküli hozzáférést tud biztosítani. Az egyik hozzáférési pont, a csapat vezetősége által beszerzett kis vezetéknélküli forgalomirányító, a csoportirodában található. A másik egy olcsó, régebbi Cisco Aironet AP, melyet a stadion sajtópáholyában helyeztek el. Ez a hozzáférési pont biztosítja a riporterek számára a vezetéknélküli összeköttetést.

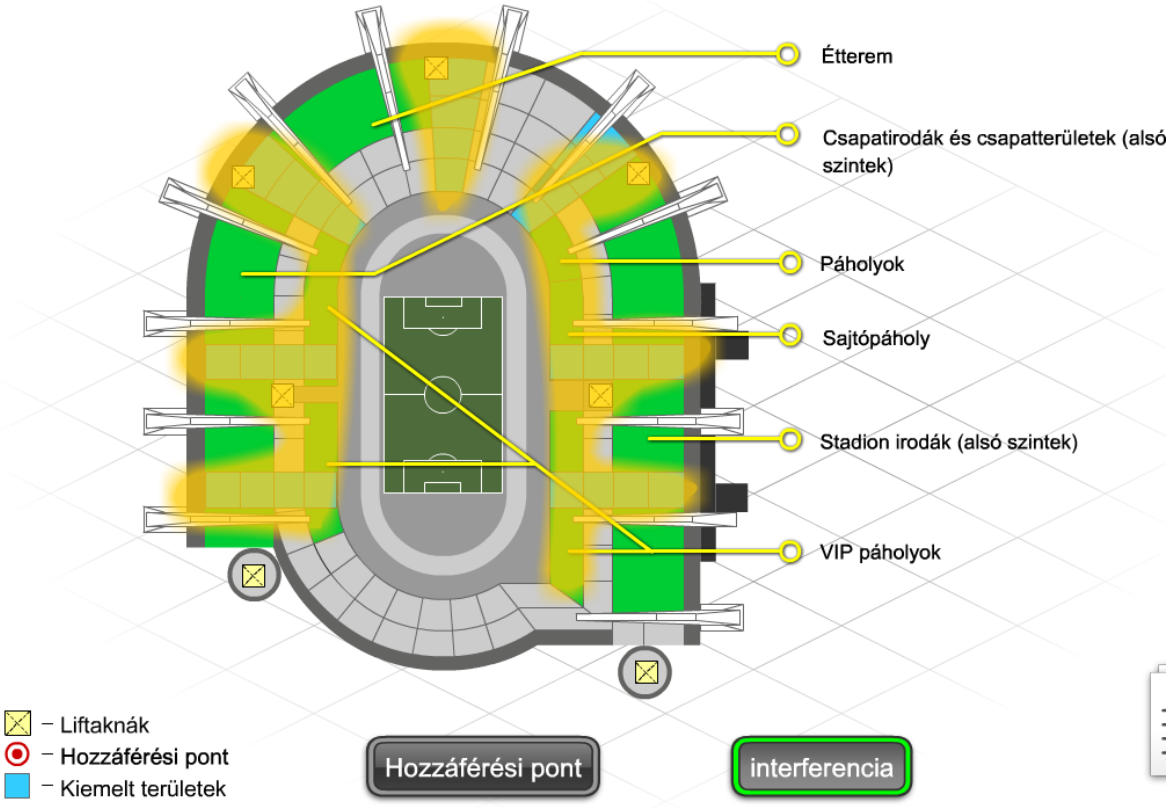
Az új hálózati terv szerint a stadion hálózatának további vezetéknélküli elérési pontokra van szüksége, melyeket az étteremben, illetve a VIP páholyoknál helyeznek el. A stadion vezetősége mindkét helyen biztonsági korlátozás nélküli internet elérést kíván nyújtani.

A hálózattervező mérnök listát készít a zavaró interferenciát okozó lehetséges forrásokról, valamint a rádiófrekvenciás lefedettségi területeket befolyásoló, az infrastruktúrával kapcsolatos problémákról. A helyszíni felmérés során a Hálózat Kft. dolgozói ellenőrizhetik ezeken a területeken a vezetéknélküli jelre gyakorolt hatásokat.

A tervező listáján megtalálható befolyásoló tényezők:

- Az étel- és italárusító területeken és a VIP páholyokban található mikrohullámú sütők
- A riporterek és újságírók által használt vezetéknélküli telefonok és fejhallgatók
- Az étterem és a VIP páholyok közelében található liftaknák
- Vastag betonoszlopok és falak a VIP páholyok között





3.4.3 A vezetéknélküli hálózat helyszíni felmérése

A helyszíni felmérés a következő lépésekből áll:

1. lépés: Felhasználói követelmények meghatározása

Előfordulhat, hogy a stadion szeretné publikussá tenni a vezetéknélküli elérési pontok elérhetőségét. A Hálózat Kft. dolgozóinak meg kell határozniuk az elvárt szolgáltatási színvonalat, és tisztázniuk kell, hogy szükség van-e fejlett vezetéknélküli technológiák (mint pl. vezeték nélküli IP telefonok) támogatására.

2. lépés: A lefedettségi területek meghatározása

A Hálózat Kft. dolgozói felbecsülik az egyes lefedettségi területekre eső felhasználók számát, és ami ennél is fontosabb, a nagyobb események alkalmával várható csúcskihasználtságot.

3. lépés: A hozzáférési pontok előzetes helyének meghatározása

A szakemberek a stadion tervrajzának áttekintése után kijelölik a hozzáférési pontok lehetséges helyeit, majd meghatározzák a lefedettség biztosításának feltételeit, az áramellátást igénylő területeket, valamint a hozzáférési pontok vezetékes hálózathoz történő kapcsolódásának módját.

4. lépés: A jelerősség mérése

A szakemberek átmeneti jelleggel hozzáférési pontot telepítenek egy kiválasztott helyszínre. Ennek segítségével mérik a vett rádiófrekvenciás jel erősségét és az interferencia lehetséges okait.

A Hálózat Kft. dolgozói az étterem közepén, a konyhától távol telepítik az átmeneti hozzáférési pontot, amelyet nem szükséges a stadion hálózatához csatlakoztatni, hiszen most még csak a vezetéknélküli lefedettséget tesztelik.

A szakemberek a helyszíni felmérés elvégzésére alkalmas, vezetéknélküli hálózati kártyát tartalmazó laptopot használnak a teszt végrehajtására.

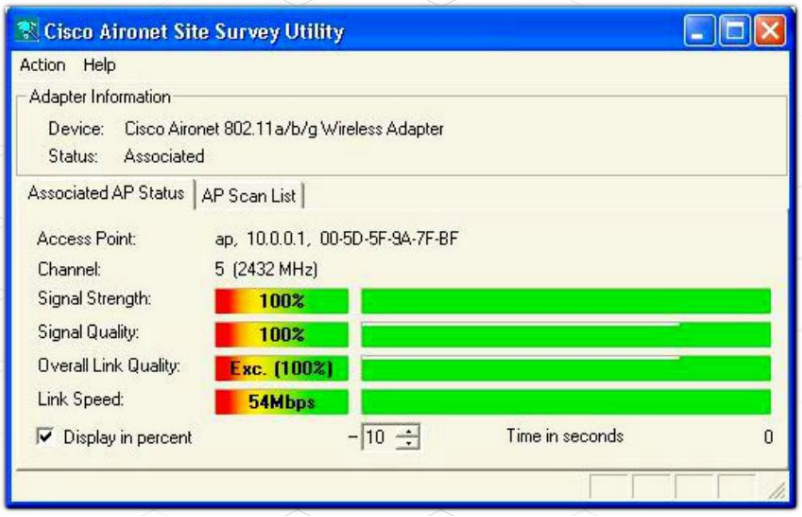
A Hálózat Kft. dolgozói a következő lépéseket hajtják végre:

1. lépés: A hozzáférési ponttól távolodva mérik a jelerősséget és a kapcsolat sebességét.

2. lépés: Rögzítik az eredményeket és a hozzáférési ponttól mért távolságot minden alkalommal, amikor a minőség vagy a kapcsolat sebessége változik.

3. lépés: Az alaprajzon megjelölik azokat a területeket, ahol a jel minősége elfogadható.

A hálózat tervezője a megjelölt alaprajz alapján határozza meg a hozzáférési pontok és a vezetékes hálózathoz való kapcsolódást biztosító csatlakozók helyét. A harmadik lépés teljesítése során be kell tartani a helyi és az országos rendeletekben előírt elektromos és tűzvédelmi előírásokat.



3.5 A hálózat-tervezési követelmények dokumentálása

3.5.1 A hálózattervezési követelmények dokumentációjának elkészítése

A Hálózat Kft. dolgozói befejezték a hálózat korszerűsítésének előkészületi és tervezési fázisait. Készen állnak a tervezési követelmények dokumentációjának elkészítésére és a tervező munka megkezdésére.

A Tervezési Követelmények című dokumentum az új hálózati terv összes számottevő üzleti és technikai követelményét magában foglalja.

A Tervezési Követelmények elkészítéséhez szükséges információk döntő része megtalálható az ajánlatkérésben (RFP - Request for Proposal). A Tervezési Követelmények dokumentuma a tervezett hálózatkorszerűsítés specifikációját is tartalmazza.

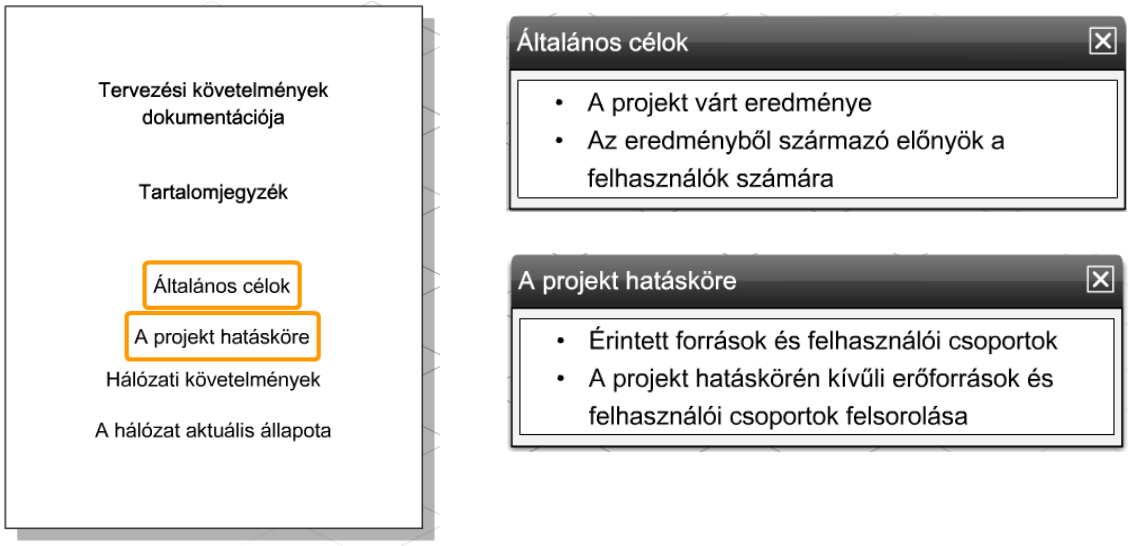
A dokumentum első két része az általános célokat és a projekt hatókörét tárgyalja.

Általános Célok

Ez a rész a bővítés általános céljait fogalmazza meg, valamint leírja, hogy a hálózat korszerűsítése révén hogyan válhat sikeresebbé a stadiont működtető cég.

A projekt Hatóköre

Ez a rész a korszerűsítés által érintett területeket, alkalmazásokat és felhasználói csoportokat vázolja fel. Tartalmazhat a korszerűsítés keretein túlmutató elemeket is, mint például a kiszolgálók és alkalmazások frissítése.



A dokumentum további két fontos része a hálózati követelményekkel és a hálózat aktuális állapotával foglalkozik.

Hálózati Követelmények

Ez a rész azokat az üzleti célokat, technikai követelményeket, korlátokat, felhasználói csoportokat és alkalmazásokat foglalja össze, amelyek befolyásolják a stadion hálózatának tervezetét.

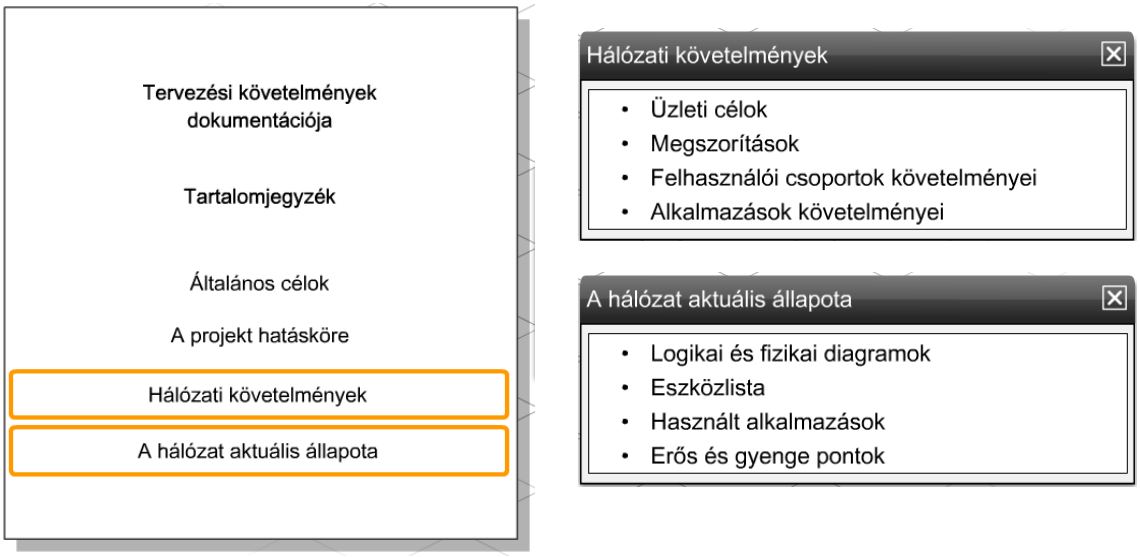
A hálózat Aktuális Állapota

A jelenlegi hálózatot a következő információkkal írja le:

- Logikai és fizikai diagramok
- Eszközlista
- Alkalmazások
- Erős és gyenge pontok

A hálózat tervezőjének jól kell ismernie a meglévő hálózatot a gyenge pontok kiküszöbölése és az erősségek hatékony kihasználása érdekében.

A félreértések elkerülése érdekében a Hálózat Kft. dolgozói a tervezési folyamat megkezdése előtt a stadion vezetőségével együtt átnézik a tervezési követelmények dokumentációját.

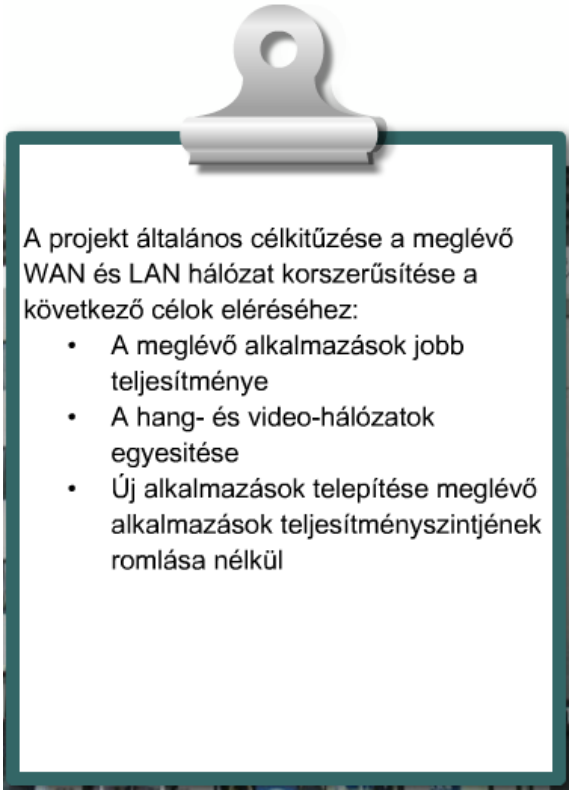


3.5.2 Általános célok

Az általános célok megfogalmazásakor a hálózat tervezésének elsődleges céljára kell elsősorban összpontosítani. Az általános céloknak összhangban kell lenniük a sikeresebb tevékenységet eredményező üzleti célokkal.

A dokumentáció ezen részében a Hálózat Kft. tervezője a stadion hálózati tervének általános céljait fogalmazza meg, alapul véve a Stadion Kht. elnökével és más dolgozókkal folytatott beszélgetések során szerzett információt.

A Hálózat Kft. megszerzi a stadion vezetőségének egyetértését a terv általános céljaira vonatkozóan.

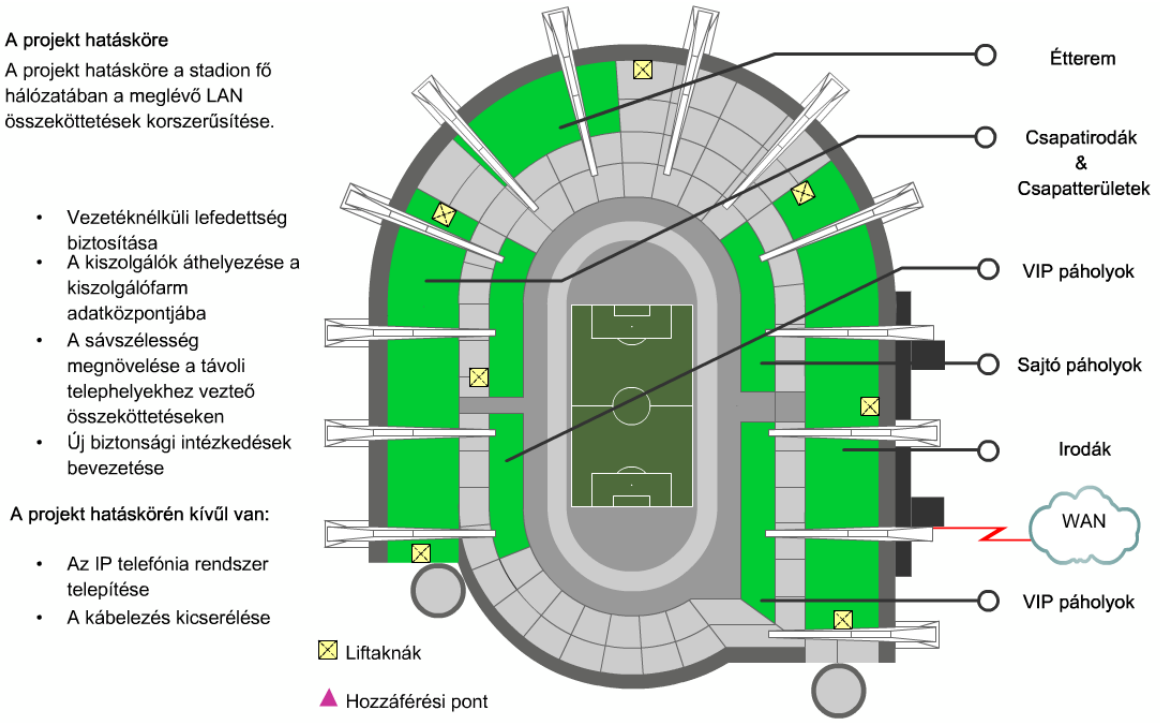


3.5.3 A projekt hatóköre

A Tervezési Követelmények dokumentumának második része a projekt hatókörét vázolja fel. Részletezi, hogy a projekt végrehajtása a hálózatnak mekkora részét érinti vagy változtatja meg.

A meglévő hálózat azon részeit is meghatározza, melyek nem tartoznak a projekt által érintett területek közé. Ezeket a nem érintett területeket úgy kell meghatározni, hogy ne lehessen félreértés a Hálózat Kft. és a stadion vezetősége között.

A Hálózat Kft. tervezője áttekinti a meglévő hálózat topológiáját és a jelenleg biztosított szolgáltatásokat. Az általános célkitűzések szerint mind a LAN, mind a WAN hálózatot korszerűsíteni kell. A projekt során így a stadion fő épületének és két távoli helyszínének felhasználói is érintettek lesznek.



3.5.4 Üzleti célok és technikai követelmények

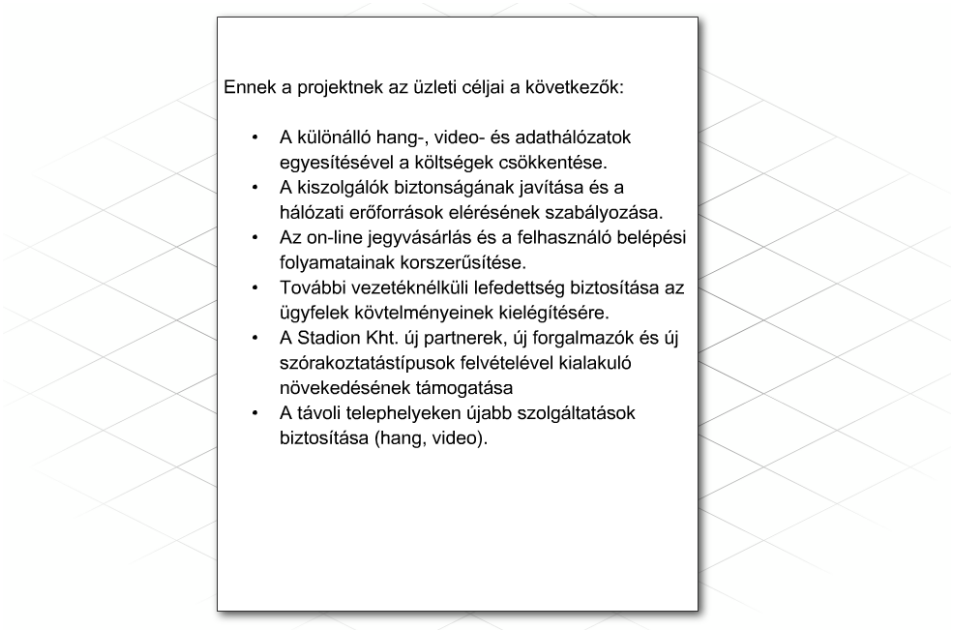
A tervezési követelmények dokumentációjának első két része általában rövid és nem tartalmaz túl sok részletet. Ezzel ellentétben a Hálózati Követelmények című rész, mely a hálózat tervezését és az új technológiák implementálását is irányítja, nagyon részletes.

A Hálózati Követelmények rész négy alfejezetből épül fel:

- Üzleti célok
- Technikai követelmények
- Felhasználók
- Alkalmazások

Üzleti Célok

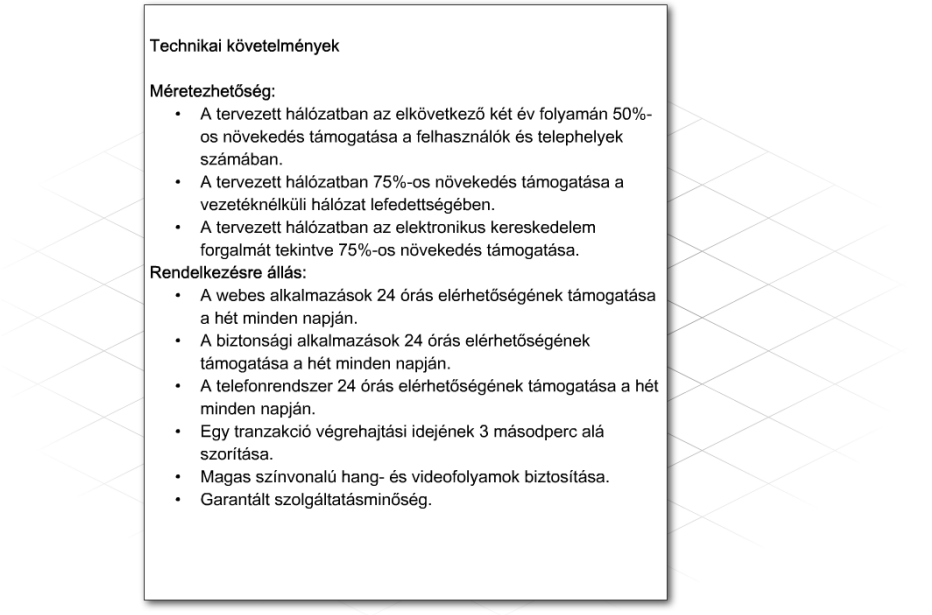
A Hálózat Kft. tervezője a legfontosabbal kezdve, fontossági sorrendben sorolja fel a célokat.



Technikai követelmények

A Hálózat Kft. tervezője kiértékeli az egyes üzleti célokat, majd meghatározza a célok eléréséhez szükséges technikai követelményeket. Ezeket a követelményeket a Technikai Követelmények rész tartalmazza a bővíthetőség, a rendelkezésre állás, a biztonság és a felügyelhetőség pontok alatt.

- **Bővíthetőség** – Az üzleti célok közé tartozik az új felhasználók bekapcsolása, új szolgáltatások bevezetése, valamint hang- és video átvitel támogatása a hálózatban. A hálózatnak jelentősebb későbbi újratervezés és szolgáltatás-kimaradás nélkül kell méretezhetőnek lennie. A tervező a stadion vezetőségével megvitatja és dokumentálja a lehetséges növekedést.
- **Rendelkezésre állás** – A hang-, video- és biztonsági szolgáltatások, valamint az on-line jegyvásárlás szükségessé teszi a hálózat 24 órás elérhetőségét. Az új szolgáltatásokat a távoli telephelyeken és a stadion fő telephelyén is elérhetővé kell tenni. Az új jegyvásárlási és beléptetési alkalmazások nagyon rövid tranzakciós időt igényelnek, a hang- és video szolgáltatások számára viszont QoS támogatás szükséges.



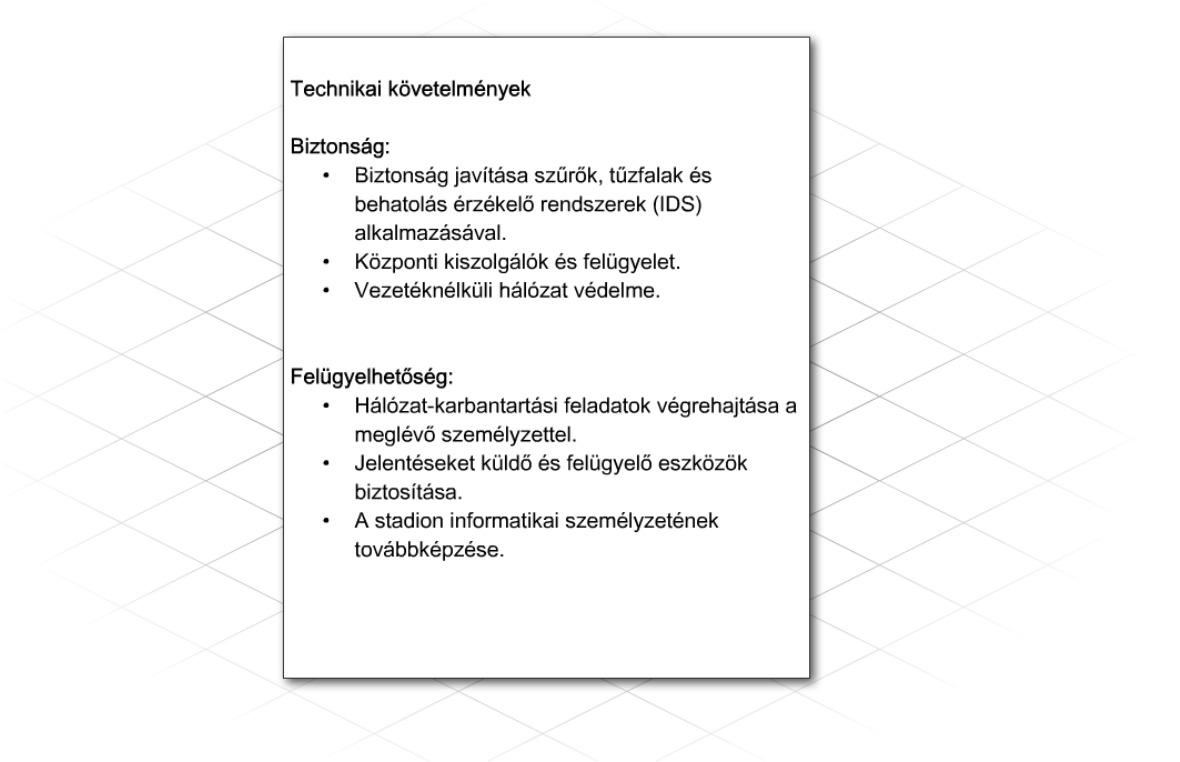
- **Biztonság** – Minden hálózati korszerűsítés egyik fő célja a biztonság javítása. A stadion tervezett hálózata tűzfalakat, csomagszűrést és behatolás-érzékelő rendszereket (IDS) is alkalmaz a jogosulatlan hozzáférés megakadályozására. A szolgáltatásokat egy adatközpont kiszolgálófarm fogja védeni.
- **Felügyelhetőség** – A stadion vezetősége nem kívánja növelni a stadion informatikai szakembereinek számát, így a hálózatnak könnyen kezelhetőnek és karbantarthatónak kell lennie. Egy hálózatot akkor könnyű felügyelni, ha a tervezés és telepítés a hálózati szabványoknak megfelelően történik. Egy felügyeleti alkalmazásra van szükség, mely jelentéseket és riasztásokat küld az informatikai személyzetnek tevékenységük segítésére. Ezen felül az informatikai személyzet továbbképzésére is szükség van ahhoz, hogy a tervezett hálózat karbantartását és felügyeletét el tudják majd végezni.

Felhasználók

A Tervezési Követelmények ezen része a különböző felhasználói csoportokat és hozzáférési követelményeiket tartalmazza. A Stadion Kht. az ügyfelek, a beszállítók, a személyzet, a távmunkások, valamint a cég helyszínen dolgozó munkatársai számára is szeretné biztosítani a hálózat elérhetőségét. Mindegyik felhasználócsoport azonban más és más hálózati szolgáltatást igényelhet. Fontos, hogy ezeket az elvárásokat is dokumentálják és a hálózat tervezése során figyelembe vegyék.

Alkalmazások

A hálózat forgalmi jellemzői és a különböző alkalmazások követelményei is befolyásolják a hálózat tervezését. Ez a rész azokat az alkalmazásokat jellemzi, melyeket a hálózatnak támogatnia kell. Természetesen a hálózat egyedi forgalmi igényeit is részletezni kell.



3.5.5 A létező hálózat jellemzése

A létező hálózat állapota

A Tervezési Követelmények dokumentumának utolsó része a következő információkat tartalmazza:

- A Hálózat Kft. által a létező hálózatról készített összes diagram
- A kiszolgálók és más fontos hálózati eszközök nevei és IP-címei
- A létező hálózat erős és gyenge pontjai, valamint az üzleti célokra kifejtett hatásuk

A hálózattervező mérnök egy táblázatot készít a felismert gyenge pontokról, az érintett üzleti és technikai célokról, valamint arról, hogy az új hálózatban a gyenge pontok kiküszöbölése milyen módon történhet.

A Hálózat Kft. dolgozói áttekintik az elkészült dokumentációt, majd egy megbeszéléshez időpontot egyeztetnek a stadion vezetőségével. A megbeszélés célja a hálózat korszerűsítésének folytatásához szükséges felhatalmazás és beleegyezés megszerzése.

Gyenge pont	Hatás	Lehetséges megoldás
Egyszintű hálózati terv	Nem méretezhető - a hálózat növekedése kihatással van a teljesítményre	Irányított hierarchia létrehozása
Egyszintű hálózati terv	Nincs hálózati szegmentáció - a forgalom nem szűrhető és Nem különíthető el, ami biztonsági kockázattal jár	Szegmentáció megvalósítása VLAN-okkal Forgalomszűrés alkalmazása
Nincs redundancia	Hatalmas hibatartományok - az esetleges összeköttetés - és eszköz meghibásodások a hálózat nagy területére vannak hatással	• kisebb hibatartományok létrehozása • ahol lehet redundancia használata
Elosztott kiszolgálók	Kiszolgálók veszélynek vannak kitéve - nincs ellenőrzött környezet, háttérmentés vagy tartalék összeköttetés	A kiszolgálók áthelyezése a kiszolgálófarm adatközpontjába
Elosztott kiszolgálók	Kiszolgálók nem elérhetők - nincs nagysebességű kapcsolat a kiszolgálókhoz	A kiszolgálókhoz gigabit sebességű összeköttetések telepítése és a kiszolgálók központi elhelyezése
Korlátozott üvegszálas hozzáférés	A lehetséges redundancia	Több kapcsoló és köztük nagysebességű összeköttetés használata
Nincs állapot alapú tűzfal	Csak forgalomszűrés, nem akadályozza meg a jogosulatlan és a nem kívánatos forgalmat	Állapot alapú IOS tűzfal használata
Tűzfal csak a hálózat határán	Belső eszközök sérülékenyek - nincs védelem a belső támadásokkal szemben	• Többrétegű tűzfal és szűrő mechanizmusok létrehozása • Behatolás érzékelő rendszerek alkalmazása az adatközpontban

3.6 A fejezet összefoglalása

- A hálózattervező a meglévő hálózat vizsgálatával határozza meg, hogy mennyire reálisak és kivitelezhetőek a tervezési célok, valamint a meglévő hálózat mennyire felel meg a méretezhetőséggel, a rendelkezésre állással, a biztonsággal és a felügyelhetőséggel kapcsolatos elvárásoknak.
- A hálózat jellemzése során a hálózattervező első feladatai közé tartozik, hogy megvizsgálja a hálózati dokumentációk és topológia diagramok naprakész információt tartalmaznak-e.
- A Cisco Network Assistant segítségével lehet információt szerezni a hálózatban telepített eszközökről.
- A hálózattervezők és mérnökök a show parancsok használatával gyűjtenek információt a hálózat eszközeiről és konfigurációikról.
- A meglévő hálózat moduláris blokkdiagramba szervezésével azonosítja a tervező azokat a területeket, ahol a tervezés javítására van szükség.
- A tervező a hálózat különböző elemeit az erős és gyenge pontok kategóriájába sorolja.
- Az új tervnek az újabb szolgáltatások és technológiák hozzáadása előtt minden azonosított gyenge pontot ki kell küszöbölnie.
- A Cisco.com weboldal értékes információkat szolgáltat a tervezőnek, többek között a telepített eszközök dokumentációját, a hálózat kiértékelését segítő eszközöket, új szoftverek és alkalmazások letölthető verzióit, és egy fórumot a szakmabeliekkel történő együttműködéshez.
- A show version parancs kimenetéből létrehozható a hálózatban telepített eszközök nyilvántartási listája, mely tartalmazza az eszköz modellt és típusát, a telepített memóriát, az interfészek számát és típusát, valamint a telepített Cisco IOS szoftvert.
- Az IOS fájlok elnevezése megmutatja az IOS szolgáltatáskészletét és verziószámát.

- Egy Cisco.com eszköz, a szolgáltatásnavigátor (Feature Navigator) segít a hálózattervezőnek a hálózat meghatározott szolgáltatásait támogató IOS verzió kiválasztásában.
- Egy új IOS verzióra való áttérés előtt fontos meggyőződni arról, hogy az eszköz elegendő memóriával rendelkezik-e a szoftver futtatásához. A frissítés tesztkörnyezetben történő tesztelése kritikus, hiszen a különböző IOS verziók eltérő konfigurációs lehetőségekkel rendelkeznek.
- A Cisco IOS frissítése után fontos az eszközön a rendszerindítási folyamat megtekintése a szoftver helyes és megfelelő működésének ellenőrzéséhez.
- Az eszköz rendszerbetöltési folyamata három lépésből áll:
  1. A POST tesztelése és a kezdeti rendszerbetöltő program betöltődik
  2. A Cisco IOS megkeresése és betöltése.
  3. A konfigurációs fájl megkeresése és betöltése
- A meglévő eszközök új tervbe illesztésénél a tervezőnek figyelembe kell vennie az eszközök opcionálisan telepíthető hardverelemeit. A Cisco.com weboldalon ezek az információk megtalálhatók.
- A vezetéknélküli hálózat tervezése előtt általában szükség van a vezetéknélküli hálózat helyszíni felmérésére.
- A vezetéknélküli hálózat helyszíni felmérésénél a lefedettségi területek és a vezetéknélküli jelet befolyásoló interferencia alapjául szolgáló források meghatározására kerül sor.
- A helyszíni felmérés megtervezésénél a tervezőnek és a szakembereknek a lefedettségi területeket, a hozzáférési pontok előzetes helyeit kell meghatározniuk és egy vezetéknélküli műszerrel a hozzáférési ponttól különböző távolságokra a jel erősségét kell mérniük.
- A PPDIOO modell tervezési fázisának befejezésénél részletes tervezési követelmények dokumentációt kell készíteni. Ebben a dokumentációban leírt követelmények alapján történik a hálózat végső megtervezése.

4. Az alkalmazások hatása a hálózat-tervezésre

4.1 A hálózati alkalmazások azonosítása

4.1.1 Az alkalmazások teljesítményének jelentősége

A hálózati szolgáltatások felhasználói általában nagyon keveset tudnak a szolgáltatások mögötti hálózatról és hálózattervezésről. Felhasználói tapasztalatuk a hálózati alkalmazásokkal folytatott kommunikáción alapul.

A sportstadion esetében a hálózati alkalmazások alapvető szolgáltatásokat nyújtanak a rajongóknak, a csapatoknak és a vezetőségnek. Ezek a szolgáltatások és a hátteret biztosító hálózat üzleti szempontból kulcsfontosságúak, és lehetővé teszik a felhasználók és ügyfelek igényeinek kielégítését.

Forgalomirányítók, kiszolgálók és más hálózati eszközök statisztikai adataiból meghatározható, hogy egy adott rendszer a gyártó által meghatározott jellemzőknek megfelelően működik-e. A technikai szempontok érvényesítése azonban önmagában nem feltétlenül jelent sikert a piacon.

A siker azon múlik, hogyan látják a hálózati teljesítményt az ügyfelek, a beszállítók és a forgalmazók.

A végfelhasználók számára az alkalmazások teljesítménye az alábbiakon múlik:

- Elérhetőség- Az alkalmazás mindig elérhető, amikor szükség van rá?
- Válaszidő - Az elvárt időn belül válaszol az alkalmazás?

A stadionban például a jegyértékesítésből, az étel- és italárusításból, valamint az emléktárgyak eladásából származó bevétel csökken, ha a tranzakciós folyamatok nem hajthatók végre vagy túl hosszú ideig tartanak.

A stadion ügyfelei az alkalmazások használhatóságát aszerint értékelik, hogy a tranzakcióik végrehajtásához mennyi idő szükséges. Az ügyfelek azt is elvárják, hogy az alkalmazások szükség esetén bármikor elérhetőek legyenek.

A gyors válaszidőt igénylő alkalmazások közé tartoznak a következők:

- interaktív önkiszolgáló szolgáltatások
- jegyárusító automaták
- étel- és italárusítás nyilvántartása

A stadion személyzete számára alapvető fontosságú alkalmazások közé tartoznak az alábbiak:

- sürgősségi szolgáltatások
- hang- és videojelfolyam átvitele, illetve felügyelete

Az alkalmazások teljesítményét a felhasználók elégedettségi mutatói és a szokásos technikai adatok együttes figyelembe vételével érdemes értékelni. A hálózat áteresztő-képessége és a sikeres tranzakciók száma például két ilyen együttes mutató.

4.1.2 A különböző alkalmazáskategóriák jellemzői

Egy meglévő hálózatban az alkalmazásjellemzők meghatározása segít a hálózattervezőnek abban, hogy az üzleti célokat és a műszaki követelményeket együttesen tudja érvényesíteni a készülő tervben.

Az alkalmazásjellemzők meghatározása során a hálózati alkalmazásokat az alábbi szempontok szerint vizsgálják:

- az adott alkalmazás miként működik a hálózaton
- az alkalmazás műszaki követelményei
- az egyes alkalmazások miként hatnak egymásra a hálózaton

A tervezés korai fázisában összegyűjtött információból a tervező meghatározza, melyek az üzleti szempontból döntő fontosságú alkalmazások. Megbecsüli, hogyan fognak működni ezek az alkalmazások a tervezett hálózatban.

A jellemzési folyamat információt ad a vizsgált alkalmazások sávszélesség használatáról és válaszidejéről. Ezek a paraméterek a következő tervezési döntéseket befolyásolják:

- az átviteli közeg megválasztása
- a szükséges sávszélesség megállapítása

A különféle típusú alkalmazások forgalma más és más követelményeket támaszt a hálózattal szemben. A tervező az alkalmazások közötti kommunikáció négy különböző típusát különíti el:

- ügyfél - ügyfél
- ügyfél - elosztott kiszolgáló
- ügyfél - kiszolgálófarm
- ügyfél - vállalati határ

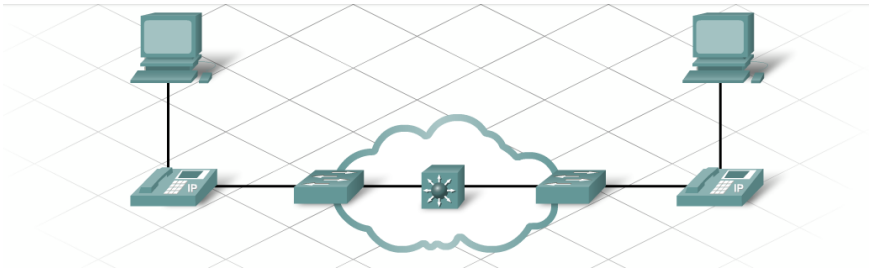
Ügyfél - ügyfél

Tipikus ügyfél - ügyfél alkalmazások közé tartoznak az alábbiak:

IP-telefónia - A kommunikálni akaró felek telefonhálózat közvetitésével létesitenek kapcsolatot, de a kapcsolat létrejötte után a kommunikáció a két fél között zajlik.

Fájlmegosztás - Néhány operációs rendszer (vagy alkalmazás) egy másik munkaállomáson tárolt adat közvetlen elérését igényli.

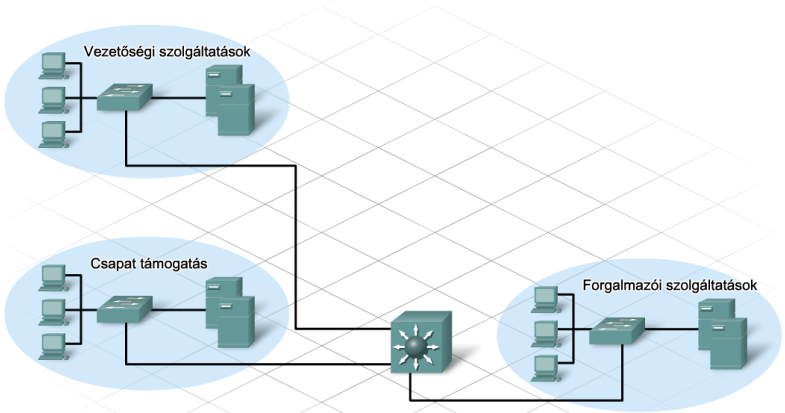
Videokonferencia-rendszerek - Ez az alkalmazás hasonló az IP-telefóniához, de hálózati követelménye magasabb, különös tekintettel a sávszélesség-használatra és a QoS követelményekre.



Ügyfél – elosztott kiszolgáló

Tipikus ügyfél – elosztott kiszolgáló alkalmazások közé tartoznak az alábbiak:

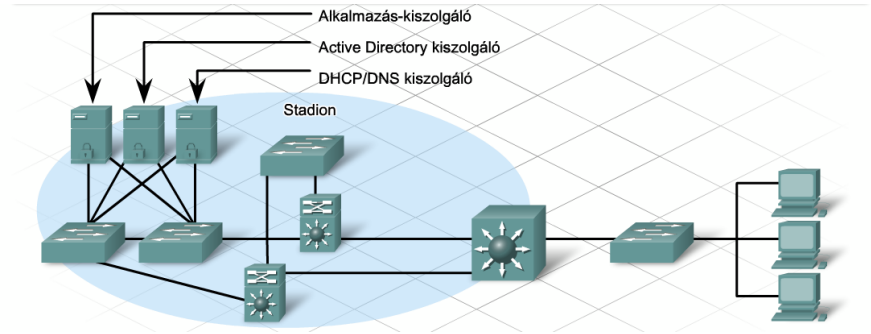
A kiszolgálók és a felhasználók ugyanabban a VLAN-ban vannak. A részleghez tartozó rendszergazda kezeli és ellenőrzi a kiszolgálókat. Az egyes részlegek forgalmának jelentős szegmensen belül zajlik. csak kis része meg más szegmensek felé.



Ügyfél – kiszolgálófarm

Tipikus ügyfél-kiszolgálófarm alkalmazások közé tartoznak a:

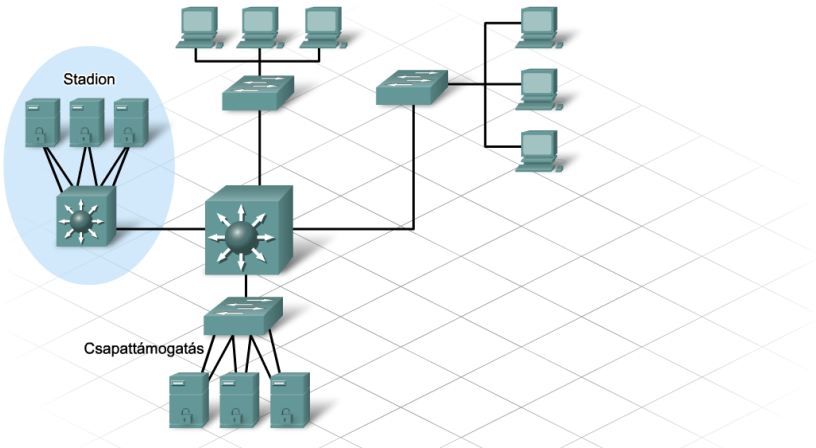
- szervezeti levelező-kiszolgálók (Lotus Notes és Microsoft Exchange)
- általános fájlkiszolgálók (Novell, Microsoft és Sun)
- szervezeti alkalmazások általános adatbázis-kiszolgálója (Sybase, Oracle és IBM)



Ügyfél – vállalati határ

Tipikus ügyfél-vállalati határ alkalmazások közé tartoznak a:

A vállalat határán telepített alkalmazások kritikusak lehetnek a szervezeti folyamatok adatfolyamai szempontjából, így minden kiesés megnövelheti a költségeket. A tipikus ügyfél-vállalati határalkalmazások webes technológián alapulnak. Ilyen típusú alkalmazásokra példa a külső levelező-kiszolgáló és a publikus webkiszolgáló. Az elektronikus kereskedelmet támogató szervezetek szintén a vállalat határára telepítik az e-kereskedelmi kiszolgálókat. Az internet felé irányuló ügyfélforgalom - mely a vállalat határán megy ki - kevesebb sávszélességet foglal, mint a helyi kiszolgálók felé irányuló forgalom.



Egy meglévő hálózatban az alkalmazásjellemzők meghatározási folyamatának első lépése a hálózattal kapcsolatos összes lehetséges információ begyűjtése. Az alábbi adatok tartoznak ide:

- szervezeti adatok
- a hálózat felülvizsgálatának dokumentumai
- forgalomanalízis

Szervezeti adatok

A szervezeti adatok a hálózat meglévő dokumentációiból és a személyzettel folytatott beszélgetések révén szerzett információból állnak össze. A tervezés korai fázisában könnyű adatokat gyűjteni, az ilyenkor megszerzett információ azonban nem mindig megbízható. Előfordulhat például, hogy olyan alkalmazásváltozásokat, mint a fejlesztések vagy a felhasználók által telepített szoftverek, egyszerűen nem dokumentálnak, vagy nem is észlelnek.

A hálózat felülvizsgálata

A hálózat felülvizsgálata lehetővé teszi a hálózati eszközökre vonatkozó információ begyűjtését, a forgalom folyamatos figyelését, és a meglévő hálózat konfigurációs részleteinek a megismerését.

Forgalomanalízis

A forgalomanalízis az alkalmazások és protokollok hálózathasználatáról nyújt információt. Segítségével felfedhetők a hálózat hiányosságai. Például számos, azonos hálózati közeget használó nagy sávszélesség-igényű alkalmazás nagymennyiségű forgalmat hozhat létre, ami a készülő terv gyenge pontja lehet.

A Cisco IOS beágyazott vizsgálóeszközei

A hálózat-alapú alkalmazás felismerés (Network-Based Application Recognition, NBAR) egy forgalomvizsgálatra és forgalomanalízisre használható olyan Cisco eszköz, amely számos különféle alkalmazás felismerésére képes. Az NBAR felismeri a web alapú és más, nehezen osztályozható, dinamikus TCP és UDP port hozzárendelést alkalmazó protokollokat.

A Cisco IOS NetFlow olyan további eszköz, amely IP alkalmazások számára nyújt hatékony, az alábbiakban felsorolt szolgáltatásokat:

- Hálózati forgalom könyvelése
- Használat szerinti hálózati számlázás
- Hálózattervezés
- Biztonsági funkciók
- Szolgáltatásmegtagadás nyomon követése
- Hálózatfelügyelet

A NetFlow értékes információt nyújt a hálózat felhasználóiról, az alkalmazásokról, a csúcskihasználtsági időkről és a forgalomirányításról is.

Minta NBAR kimenet

```
Router# show ip nbar protocol-discovery interface FastEthernet 6/0
 FastEthernet6/0
                            Input                     Output
   Protocol                 Packet Count              Packet Count
                            Byte Count                Byte Count
                            5 minute bit rate (bps)   5 minute bit rate (bps)
   ------------------------ ------------------------  ------------------------
   igrp                     316773                    0
                            26340105                  0
                            3000                      0
```

```
   streamwork              4437                    7367
                           2301891                 339213
                           3000                    0
   rsvp                    279538                  14644
                           319106191               673624
                           0                       0
   ntp                     8979                    7714
                           906550                  694260
                           0                       0
.
.

Total                  17203819                151684936
                          19161397327             50967034611
                          4179000                 6620000
```

Minta NetFlow kimenet

```
Router# show ip cache flow
IP packet size distribution (2381 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .092 .000 .003 .000 .141 .048 .000 .000 .000 .093 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .048 .189 .381 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  22 active, 4074 inactive, 45 added
  2270 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 100 seconds
IP Sub Flow Cache, 25736 bytes
  23 active, 1001 inactive, 47 added, 45 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never

Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP              4      0.0        67   840      2.6      59.4       0.7
TCP-SMTP             1      0.0        67   168      0.6      59.4       0.5
TCP-BGP              1      0.0        68  1140      0.6      60.3       0.4
TCP-NNTP             1      0.0        68  1340      0.6      60.2       0.2
TCP-other            7      0.0        68   913      4.7      60.3       0.4
UDP-TFTP             1      0.0        68   156      0.6      60.2       0.1
UDP-other            4      0.0        36   151      1.4      45.6      14.7
ICMP                 4      0.0        67   529      2.7      60.0       0.2
Total:              23      0.2        62   710     14.3      57.5       2.9
```

4.1.3 Hogyan befolyásolja a forgalom a hálózattervezést?

Az alkalmazásjellemzők meghatározásához hozzá tartozik a hálózat belső és külső adatfolyamainak meghatározása is.

Belső forgalom

A belső forgalom a telephely területén belüli állomások közötti adatforgalom. A belső adatforgalom ábrázolásával azonosíthatók a nagy sávszélesség igényű kapcsolatok és a torlódások

kialakulására hajlamos hálózati helyek. Ezen ábrák segítségével választja ki a tervező a forgalom kezelésére legmegfelelőbb berendezéseket és alakítja ki a legjobb infrastruktúrát.

Külső forgalom

A külső forgalom a helyi hálózaton kívüli felhasználók által kezdeményezett, valamint a távoli hálózatok felé irányuló forgalomként definiálható. A külső forgalom egyes típusai (pl. a sürgősségi vagy pénzügyi szolgáltatások), redundanciát igényelnek, és a szokásosnál komolyabb biztonsági problémákat vetnek fel. A tervező a külső forgalom ábrázolásával határozza meg a tűzfalak és a DMZ hálózatok helyét, valamint az internetkapcsolatra vonatkozó elvárásokat.

A tervező az NBAR és a Netflow segítségével vizsgálja meg a belső és a külső adatforgalmat. A hálózati sávszélesség hatékony kihasználásának biztosításához a forgalom összetevői NBAR segítségével azonosíthatók és osztályozhatók, majd ezáltal a megfelelő QoS mechanizmusok alkalmazhatók.

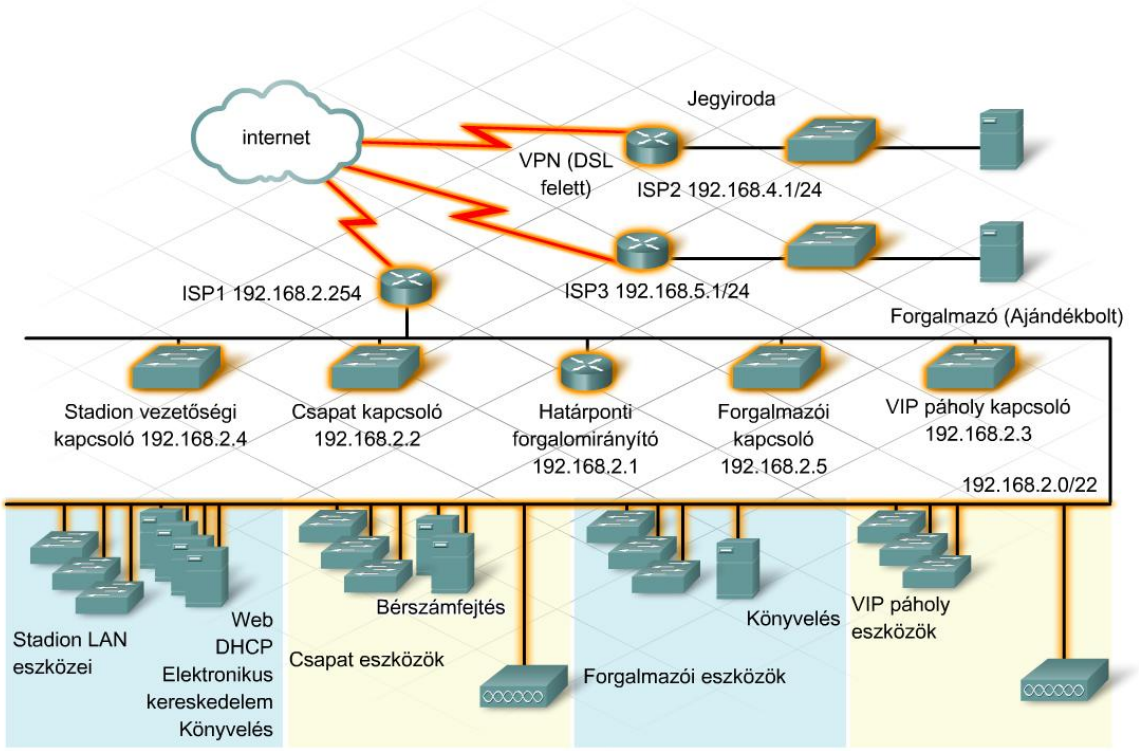
4.1.4 Hogyan befolyásolják az alkalmazásjellemzők a hálózattervezést

A hálózaton telepített különböző típusú hardvereszközök befolyásolják az alkalmazások teljesítményét. Egy olyan összetett hálózat, mint amilyen a sportstadioné is, több különböző típusú hardvert is tartalmazhat. Minden egyes eszköztípus megnövelheti a felhasználói kérések válaszidejét. A késleltetés kihat az alkalmazások teljesítményére, s ebből adódóan az ügyfelek elégedettségére is. A hang- és videó alkalmazásokat például jelentősen befolyásolhatja a hardvereszközök késleltetése, ami a teljesítmény romlásához vezethet. A késleltetések a következők miatt is létrejöhetnek:

- A forgalom továbbításához szükséges idő egy forgalomirányítón.
- Régebbi kapcsolók, melyek nem képesek kezelni a modern alkalmazások okozta forgalomlöketeket.

A kimagasló teljesítmény biztosításának egyik módja a felülről-lefelé haladó tervezési megközelítés használata. Ez a megközelítés a fizikai infrastruktúrának a hálózati alkalmazások igényeihez igazodó megtervezését jelenti. A hálózati eszközöket csak a műszaki követelmények gondos elemzése után választják ki.

Egy modern hálózaton a hálózati alkalmazások csomagok sorozatát állítják elő. Ezek a csomagok különböző méretűek, eltérő protokollkészletet használnak, eltérő módon viszonyulnak a késleltetéshez és az egyéb hálózatjellemzőkhöz. Ha ezeknek az alkalmazásoknak a szolgáltatási követelményei egymással ellentmondók, akkor teljesítményproblémák jelentkezhetnek. Egy új alkalmazás telepítésekor a hálózattervező mérnöknek végig kell gondolnia az új alkalmazásnak a meglévők teljesítményére kifejtett hatását, valamint meg kell becsülnie az alkalmazás várható teljesítményét különböző konfigurációk és hálózati körülmények esetén.



WAN-összeköttetés

A WAN-összeköttetéseknek támogatniuk kell az alkalmazások forgalmának sávszélesség-igényét. Másképp a hálózat áteresztőképessége jelentős mértékben romlana.

Forgalomirányító

A forgalomirányítók forgalomszűrési és -továbbítási folyamata időt vesz igénybe. Ez a feldolgozási idő késleltetést okozhat, mely akadályt jelenthet az időzítésre érzékeny alkalmazások (videofolyam) kézbesítésénél.

Kapcsoló

A kapcsolók a céleszköz fizikai címe alapján továbbítják a forgalmat. A feldolgozási idő ugyan kicsi, de a késleltetést számításba kell venni.

Kábelezés

A kábelezésnek támogatnia kell az alkalmazások forgalmának sávszélesség-igényét. Másképp a hálózat áteresztőképessége jelentős mértékben romlana.

4.2 A gyakori hálózati alkalmazások magyarázata

4.2.1 Tranzakció-kezelés

Manapság a hálózati alkalmazások képezik az üzleti tevékenység gerincét. Az ügyfél üzleti céljainak elérése érdekében a hálózattervezőnek biztosítania kell az alkalmazások megfelelő teljesítményét. Teljesítményproblémákat okozhat azonban az egyes alkalmazások, alkalmazáscsoportok és forgalmi típusok eltérő követelményrendszere.

A leggyakrabban előforduló alkalmazástípusok közé tartoznak az alábbiak:

- Tranzakció-kezelő alkalmazások
- Valósidejű adatfolyamokat továbbító alkalmazások
- Fájlátviteli és levelező alkalmazások

4. Az alkalmazások hatása a hálózat-tervezésre

- HTTP és webes alkalmazások
- Microsoft tartományi szolgáltatások.

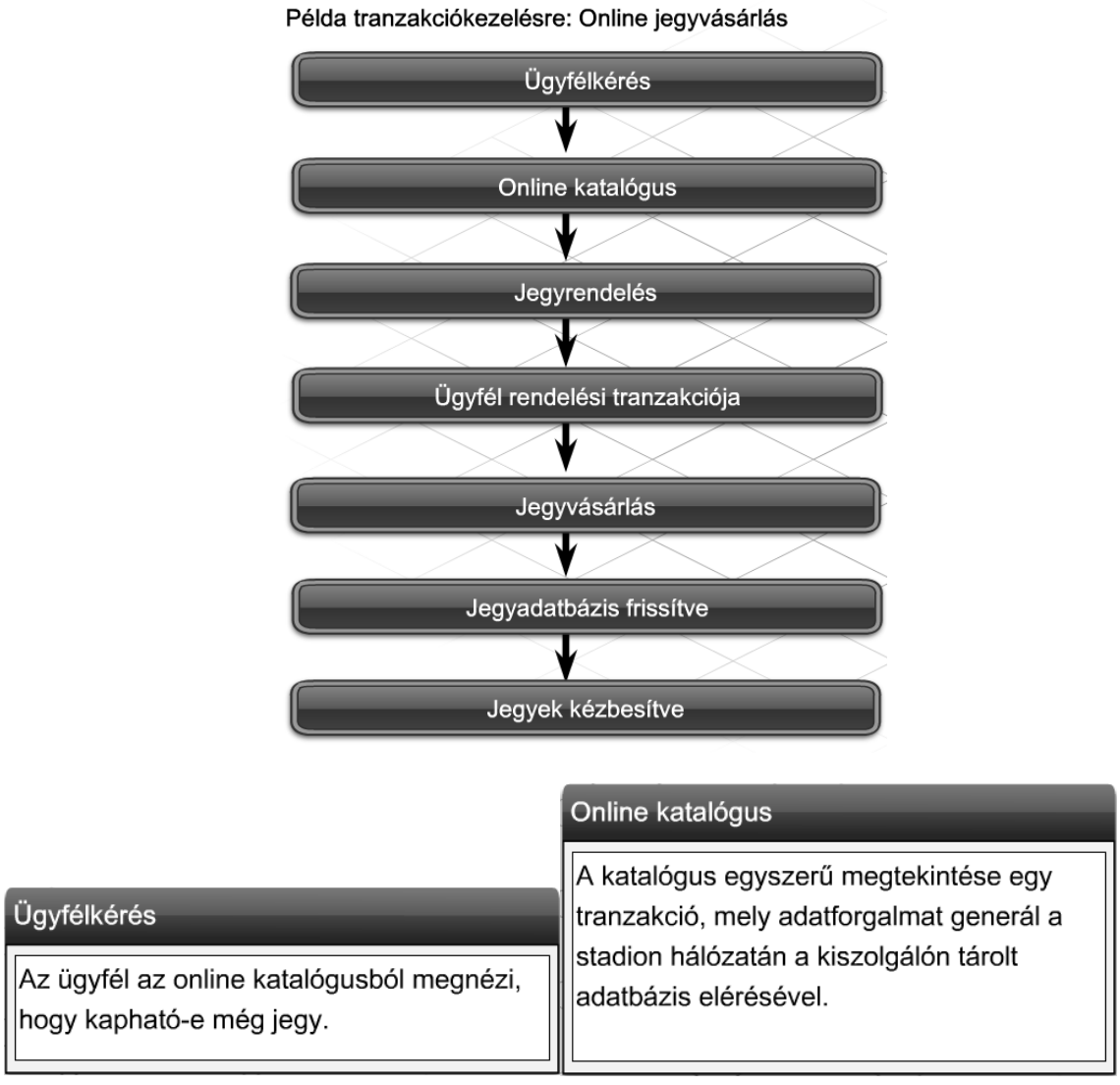
Tranzakció-kezelő alkalmazások

A tranzakció-kezelés a feldolgozási folyamatok azon típusa, amikor a számítógép azonnal válaszol a felhasználói kérésre. A felhasználó által kezdeményezett minden kérés egy tranzakció. Ezek a tranzakciók további műveleteket igényelhetnek az eredeti kérésre adott válaszként, ezért a hálózattervezés során a tranzakciókkal érdemes külön foglalkozni.

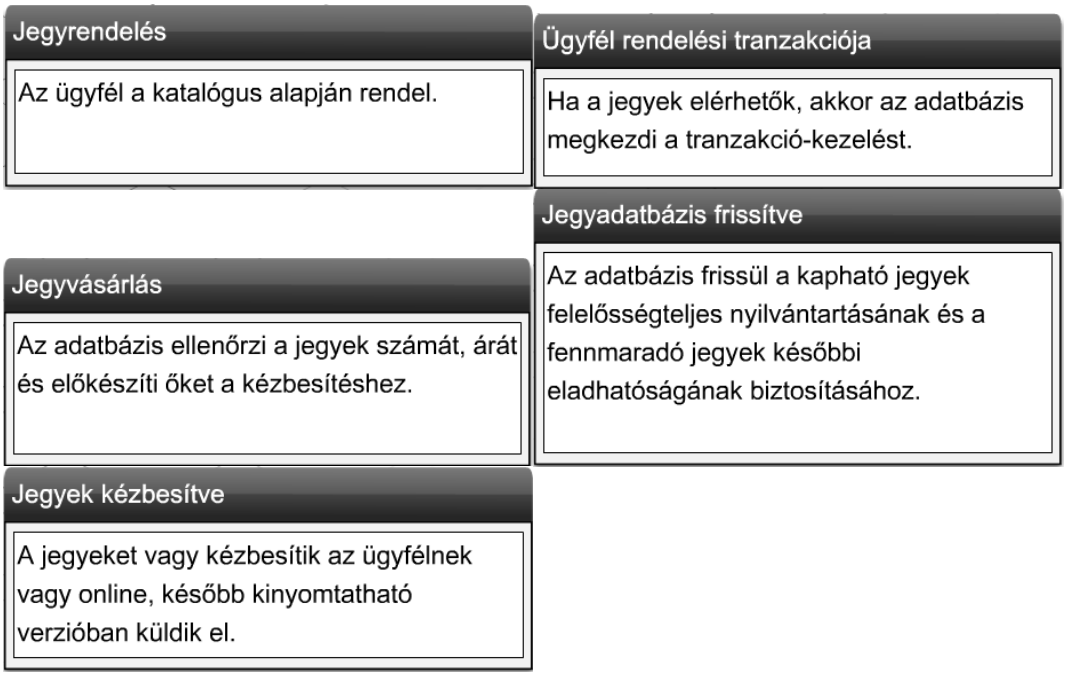
Tranzakció-kezelésként említhető például az online jegyvásárlás a stadion egy eseményére.

Ez az egyetlen tranzakció a következő műveleteket idézi elő a hálózaton:

- Webes forgalom az ügyféltől a hálózat felé
- Adatbázis tranzakció
- Az ügyfél rendelési tranzakciója
- Rendelés feldolgozó tranzakció
- Szállítási/kézbesítési tranzakció



4. Az alkalmazások hatása a hálózat-tervezésre



Nem minden hálózatból kimenő vagy hálózatba érkező forgalom tekinthető tranzakció-kezelésnek. Egy érvényes tranzakciónak a következő kritériumoknak kell eleget tennie:

- Atomi
- Következetes
- Elkülönített
- Tartós

Atomi tranzakció

Az atomi tranzakció vagy teljes egészében végrehajtódik, vagy semmi sem hajtódik végre belőle. Ha egy tranzakció nem teljesen hajtódik végre, akkor a teljes tranzakció érvénytelen.

Következetes tranzakció

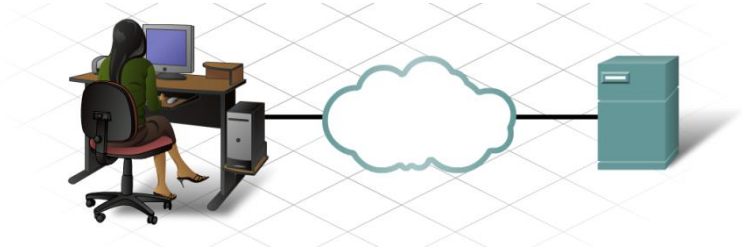
A tranzakciók következetessége biztosítja, hogy ne lehessen be nem fejezett tranzakció. Ha egy tranzakció nem fejeződik be teljesen, akkor a rendszer visszatér a tranzakció megkezdése előtti állapotba.

Elkülönített tranzakció

Az elkülönített tranzakciót más hálózati tranzakcióktól külön, biztonságosan kezelik. A biztonság a hálózati tervezés egyik legfőbb szempontja. A biztonsági megoldások közé tartoznak a hozzáférési listák (ACL), a titkosítás, valamint a tűzfalak alkalmazása.

Tartós tranzakció

A tranzakció tartóssága garantálja, hogy egy befejezett tranzakció még rendszerhiba esetén sem semmisül meg. A gondos tervezés során a tranzakció-kezeléshez többszintű redundanciát kell biztosítani. Ezen szintek közé tartoznak a fizikai réteg csatlakozásai, a kiszolgálók, a kapcsolók és a forgalomirányítók.



Atomi	Következetes
Az online jegyvásárlást intéző ügyfél az árak átutalását és a jegyek postázását, vagy nyomtatásra kész állapotát várja. Az adatbázis frissül, így ezeket a jegyeket már nem lehet megvenni.	Ha az ügyfél törli a tranzakciót a befejezés előtt, akkor a számlája nincs megterhelve és az adatbázis továbbra is azt mutatja, hogy a jegyek megvásárolhatók.
Elkülönített	**Tartós**
Az ügyfél biztos akar lenni benne, hogy az általa indított tranzakció titkos. Például az ügyfél anyagi helyzetének részletei nem láthatók más felhasználó számára.	A tranzakcióról készült bejegyzésnek rendszerhiba esetén is meg kell maradnia. Így a jegyek továbbra is elérhetők az ügyfél számára, és a számlát a megfelelő összeggel terhelték meg.

A hálózattervező kiértékeli a tranzakció-kezelő alkalmazásokat támogató redundancia és biztonsági eszközöket.

Redundancia

Tranzakció-kezelő alkalmazások használata esetén a tervező mérnöknek minden egyes tranzakció hálózatra gyakorolt hatását végig kell gondolnia. Ez egy lényeges feladat, hiszen további kábelekre és hálózati eszközökre lehet szükség a tranzakciók által igényelt redundancia vagy a szükséges sávszélesség biztosításához. A hálózati redundancia biztosítása a következő előnyökkel jár:

- A hálózat leállási idejének csökkentése vagy megszűnése.
- Az alkalmazások megnövelt rendelkezésre állása.

A redundáns hálózatok kiküszöbölik azokat a kritikus hibaforrásokat (single point of failure), melyek a teljes hálózat leállását eredményezhetik. Ha egy útvonal vagy egy eszköz meghibásodik, akkor a tartalék útvonal vagy eszköz befejezheti a folyamatot vagy a tranzakciót. A tranzakciós folyamatokat kezelő kiszolgálók tartalék útvonallal rendelkeznek a forgalom fogadására és kézbesítésére. Ez biztosítja az alkalmazásoknak a felhasználói igényekhez igazodó elérhetőségét.

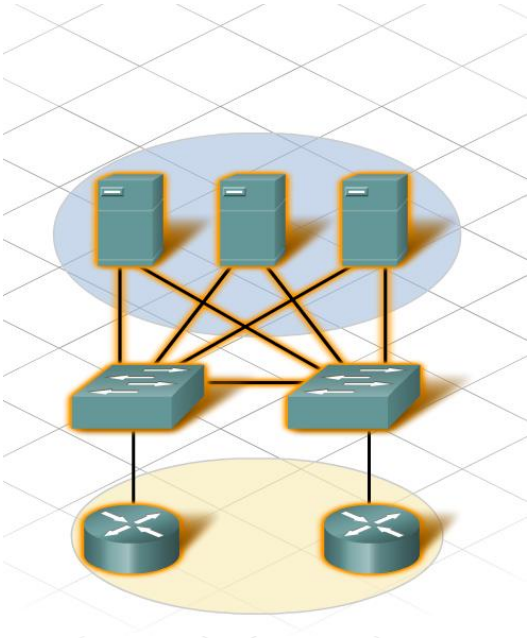
A hálózati eszközöket is lehet redundanciára konfigurálni. A két leggyakoribb protokoll:

- Gyors feszítőfa protokoll (RSTP)
- Melegtartalékolt forgalomirányító protokoll (HSRP)

Redundáns kapcsolók esetén az RSTP a 2. rétegbeli kapcsolási hurkok kialakulását akadályozza meg.

A HRSP 3. rétegű redundanciát képes biztosítani a hálózatban azáltal, hogy azonnali hibakezelést és helyreállítási mechanizmust biztosít.

A stadion tervezett hálózatában redundáns összeköttetések és eszközök az elosztási és a központi rétegben is alkalmazhatók.



Kiszolgálók
Az egyik kiszolgáló kiesése esetén a másik kezeli a felhasználói kéréseket.
Kapcsolók
Tartalék kapcsolókkal elkerülhetők a kapcsolási hibák.
Hivatkozások
Ha az egyik kapcsolóhoz vezető összeköttetés meghibásodik, akkor a másik kapcsoló elérhető.

Biztonság

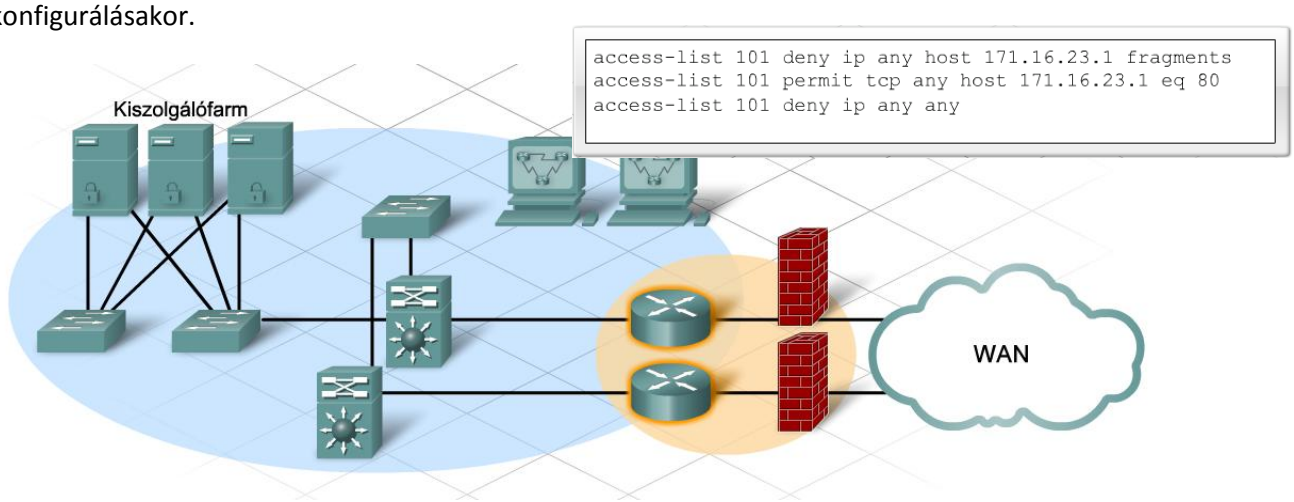
A biztonság mindig az egyik legfontosabb szempont. Nem csak a tranzakciós folyamatokra, hanem a külső és belső hálózat összes alkalmazására és teljes forgalmára kihatással van. A tranzakciós adatok sértetlenségét és titkosságának megőrzését, illetve a tranzakciós adatbázisok védelmét a biztonsági megfontolások központi problémájaként kell kezelni. A tervezőnek meg kell vizsgálnia a tranzakciós adatok engedély nélküli hozzáférhetőségének és megváltoztatásának lehetőségeit.

A VPN-ek alagúttechnikát használnak, melyet gyakran „port továbbításnak” neveznek. Ez a privát hálózat felé irányuló adatforgalom nyilvános hálózaton keresztül történő továbbítását jelenti. Az alagúttechnika a privát hálózati adatoknak és protokoll információknak a nyilvános hálózat átviteli egységébe történő beágyazása révén valósul meg.

A gyanús tevékenységek kiszűrése érdekében behatolás érzékelő rendszereket (Intrusion Detection System – IDS) alkalmaznak a hálózati forgalom megfigyelésére. Gyanús tevékenység észlelésekor az IDS riasztja a rendszert vagy a rendszergazdát. Az IDS-t lehet úgy konfigurálni, hogy egy felhasználót a forrás IP-címe alapján akadályozzon meg a hálózat elérésében.

A tűzfalak számos kritérium alapján szűrik a forgalmat. Összetettségük késleltetést okozhat. A késleltetések lehetséges hatásait figyelembe kell venni a hálózat tervezésekor.

A hálózatba való belépést megkísérlő, potenciálisan veszélyt jelentő adatforgalom szűrése, illetve a hálózatból kifelé irányuló, meghatározott tulajdonságú adatforgalom blokkolása a hozzáférési listák (ACL) segítségével történik, amelyek azonban lelassíthatják a tranzakciós folyamatokat. Bizonyos tranzakciók időérzékeny természetét számításba kell venni hozzáférési listák konfigurálásakor.



4.2.2 Valósidejű video- és hangfolyam továbbítás

Valósidejű alkalmazások

Valósidejű alkalmazásokat is támogató hálózat tervezésekor a hálózattervezőnek figyelembe kell vennie, hogy a hálózat felépítése hogyan befolyásolja az alkalmazások teljesítményét.

A befolyásoló tényezők közé tartoznak az infrastruktúra fizikai elemei:

- Hardver eszközök és csatlakozók
- Hálózati topológia
- Fizikai redundancia

Fontos tényezők, hogy a QoS konfigurációja, valamint a biztonsági megoldások milyen hatást gyakorolnak a forgalomra. Mindezek a megfontolások befolyásolják az olyan hálózati szolgáltatások, mint pl. az IP telefónia, tervezését.

Valósidejű folyamokat továbbító alkalmazások egyedi követelményeket támasztanak a hálózat tervezésével szemben. A sportstadion jelenleg használatban lévő, egyetlen valósidejű alkalmazása a videó felügyelet. Az IP-telefónia a tervezett korszerűsítés része. Az ilyen típusú alkalmazások forgalmát a lehető legkisebb késleltetéssel és késleltetés ingadozással kell továbbítani.

Az üzleti célok és a technikai követelmények meghatározása során minden hálózati vonatkozást alaposan meg kell vizsgálni annak érdekében, hogy a megvalósítás és a valósidejű alkalmazások támogatása megfelelő szintű legyen.

Infrastruktúra

A meglévő és a tervezett valósidejű alkalmazások támogatása érdekében a hálózati infrastruktúrának a különböző jellemzőkkel bíró forgalmak mindegyikéhez igazodnia kell.

A hálózattervező mérnöknek el kell döntenie, hogy a meglévő kábelezés és kapcsolók támogatják-e a hálózat tervezett új forgalmát. A gigabites sebességű kábelezésnek az infrastruktúra megváltoztatása nélkül is képesnek kell lennie a tervezett forgalom átvitelére. Elképzelhető, hogy a régebbi kapcsolók nem támogatják az Ethernet rendszerrel megvalósított áramellátást (Power over Ethernet, PoE), az elavult kábelezés pedig nem képes a sávszélesség-igény kielégítésére. Ebben az esetben a kapcsolókat és a kábelezést is korszerűsíteni kell az alkalmazások kiszolgálása érdekében.

VoIP

Egy hagyományos telefonokat használó hálózaton a VoIP bevezetéséhez hangátvitelre képes forgalomirányítók szükségesek. Ezek a forgalomirányítók alakítják át a hagyományos telefonokról érkező analóg hangot IP-csomagokká.

Az így kialakított IP-csomagokat a forgalomirányító a megfelelő állomások között irányítja. A hangátvitelre képes forgalomirányítókat szintén be kell illeszteni a tervbe.

IP Telefónia

Az IP-telefóniában maga az IP-telefon hajtja végre a hang IP-csomagokká történő átalakítását. Hangátvitelre képes forgalomirányítóra nincs szükség a vállalat hálózatán belül. Az IP-telefonok a Cisco Egyesített Kommunikációs Menedzser (Cisco Unified Communications Manager) használhatják hívásvezérlési és jelzési feladatok ellátására. A stadion hálózati követelményei az IP-telefóniát is tartalmazzák.

500-as sorozatú Cisco egyesített kommunikációs menedzser (Cisco Unified Communications 500 Series)

Valós idejű videó protokoll

A videó folyam hatékony átviteléhez a hálózatnak a késleltetés érzékeny kézbesítést igénylő alkalmazásokat is támogatnia kell. A valós idejű szállítási protokoll (RTP) és a valós idejű szállítás-vezérlési protokoll (RTCP) két olyan protokoll, melyek támogatják ezeket a feltételeket.

Az RTP és RTCP QoS mechanizmusok használatával lehetővé teszi a hálózati erőforrások szabályozását és méretezhetőségét. Ezek a QoS mechanizmusok értékes eszközöket biztosítanak a valósidejű adatfolyamokat továbbító alkalmazások késleltetési problémáinak csökkentésére. Ilyen eszköz például a prioritásos-, a testreszabott-, a kis késleltetésű és az osztály alapú súlyozott egyenlő esélyű sorban állási algoritmus.

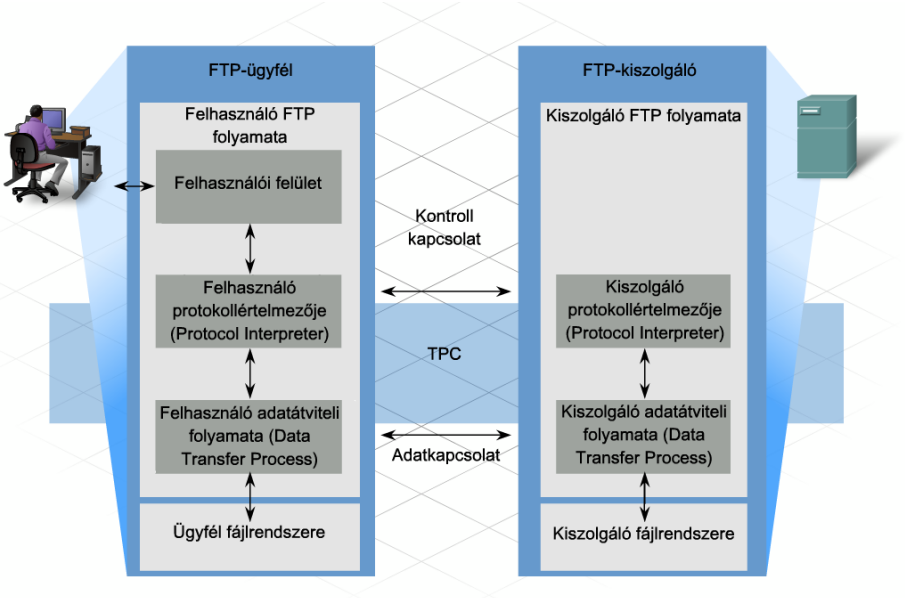
A stadion hálózatának egyik műszaki követelménye, hogy a sportlétesítményben megtartott események videofelvétele a stadion bármely pontján valós időben megtekinthető legyen.

4.2.3 Fájlátvitel és elektronikus levelezés

A fájlátvitel nagy mennyiségű adatforgalmat hoz létre a hálózaton, amely nagyobb hatással lehet az átbocsátóképességre, mint az interaktív végpontok közötti kapcsolatok. Noha a fájlátvitel sávszélesség-igényes alkalmazás, jellemzően rövid válaszidőt nem igényel.

A fájlátvitel forgalmának néhány jellemzője:

- **Nehezen megbecsülhető sávszélesség használat** – Az ilyen típusú forgalom általában felhasználó által kezdeményezett, így nem becsülhető meg pontosan.
- **Óriási csomagméret** – az FTP és más fájlátvitel forgalom nagyon nagy csomagméreteket használ a hatékony átvitel érdekében. Ezek a hatalmas csomagok hálózati torlódás kialakulása esetén késleltetést okozhatnak a más típusú forgalom számára.



A hálózat kezdeti jellemzésének fontos részfeladata a rendszeres fájlátvitelt kezdeményező felhasználók számának meghatározása. A LAN-okon nem az FTP az egyedüli fájlátviteli forgalom. Megosztott hálózati meghajtókról történő fájlmásolás, valamint nagyméretű fájlok http-vel történő letöltése az FTP-hez hasonló jellemzőkkel rendelkezik.

A tervező ezekből az információkból becsüli meg a sávszélességre vonatkozó elvárásokat. Ha ezek az elvárások meghaladják a hálózat kapacitását, akkor QoS jellemzők bevezetésére van szükség a késleltetésre érzékeny alkalmazások korrekt működésének biztosításához.

Elektronikus levelezés

Az elektronikus levelezés az egyik legnépszerűbb hálózati szolgáltatás. Egyszerűségével és gyorsaságával forradalmasította az emberek közti kommunikációt. Egy számítógépen vagy más végberendezésen történő használathoz azonban számos alkalmazást és szolgáltatást igényel. A két legelterjedtebb alkalmazásrétegbeli protokoll a POP (Post Office Protocol – postahivatal protokoll) és az SMTP (Simple Mail Transfer Protocol – egyszerű levéltovábbító protokoll).

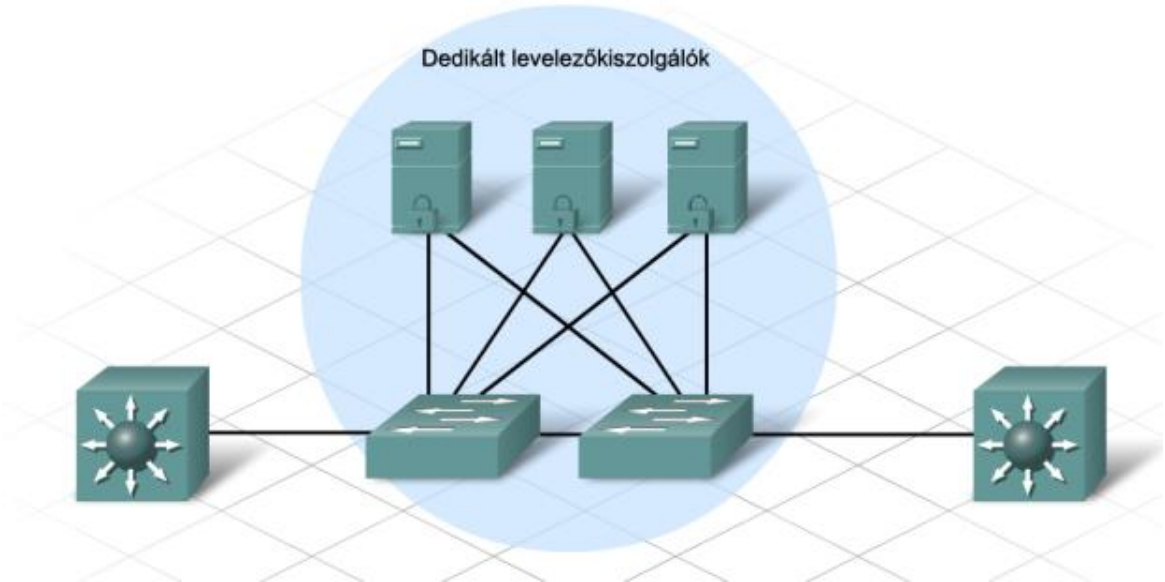
Levelezőügyfél folyamatok

Az e-mail felhasználók általában egy levelező ügyfélalkalmazáson keresztül érik el levelezési szolgáltatásukat. A levelező ügyfélalkalmazás lehetővé teszi a felhasználók számára üzenetek megszerkesztését és elküldését, a beérkező üzeneteket pedig a felhasználó postaládájába helyezi.

Levelező kiszolgáló folyamatok

A levelezőkiszolgáló szállítja és kézbesíti a levelező ügyfelek számára az e-maileket.

Bár egyetlen e-mail nem generál jelentős mennyiségű forgalmat, mégis lehetséges, hogy a tömegesen elküldött levelek elárasztják a kiszolgálót vagy a hálózatot.

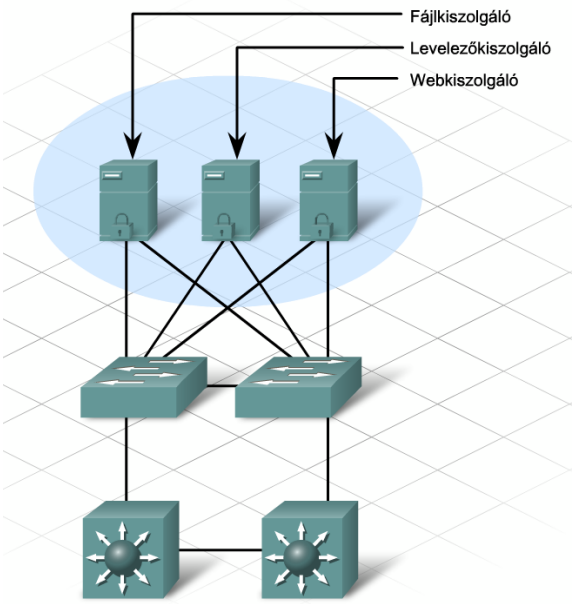


Levelezést és fájlátvitelt megvalósító alkalmazások támogatása

Az ügyfelek az e-mailek és a megosztott vagy frissíteni kívánt fájlok azonnali elérését várják el.

Az elérhetőség biztosításához a hálózattervező a következő lépéseket hajtja végre:

- Egy központi helyen, például egy kiszolgálófarmon helyezi biztonságba a fájl- és levelező-kiszolgálókat.
- Fizikai és logikai védelmet biztosít a jogosulatlan hozzáféréssel szemben.
- Redundancia biztosításával teszi lehetővé, hogy egy eszköz kiesése esetén is megmaradjanak a fájlok.
- Tartalék útvonalat konfigurál a kiszolgálókhoz.



4.2.4 http és webes forgalom

HTTP és webes adatforgalom

A hiperszöveg átviteli protokoll (HTTP) a TCP/IP protokollkészlet egyik eleme, melyet eredetileg a weboldalak közzétételére és letöltésére fejlesztettek ki, de ma már az együttműködésen alapuló, elosztott információs rendszerekben is használják. A http a WWW (World Wide Web) rendszeren belül az adatok átvitelére szolgál. Ez az egyik legszélesebb körben elterjedt alkalmazás protokoll.

A http egy kérés/válasz típusú protokollt specifikál egy ügyfél (általában webböngésző) és egy kiszolgáló között.

Amikor az ügyfél egy kérés üzenetet küld a kiszolgálónak, a http protokoll határozza meg az ügyfél által használt üzenet típusát, valamint a kiszolgáló által küldött válasz típusát is.

Ez a folyamat látszólag nem igényel túlzott figyelmet a tervezési folyamat során. Ennek ellenére, ha egy kiszolgálót elektronikus kereskedelemre vagy ügyféladatok tárolására is használnak, akkor a biztonsági és redundancia problémák fontosakká válnak.

Hálózati eszközök

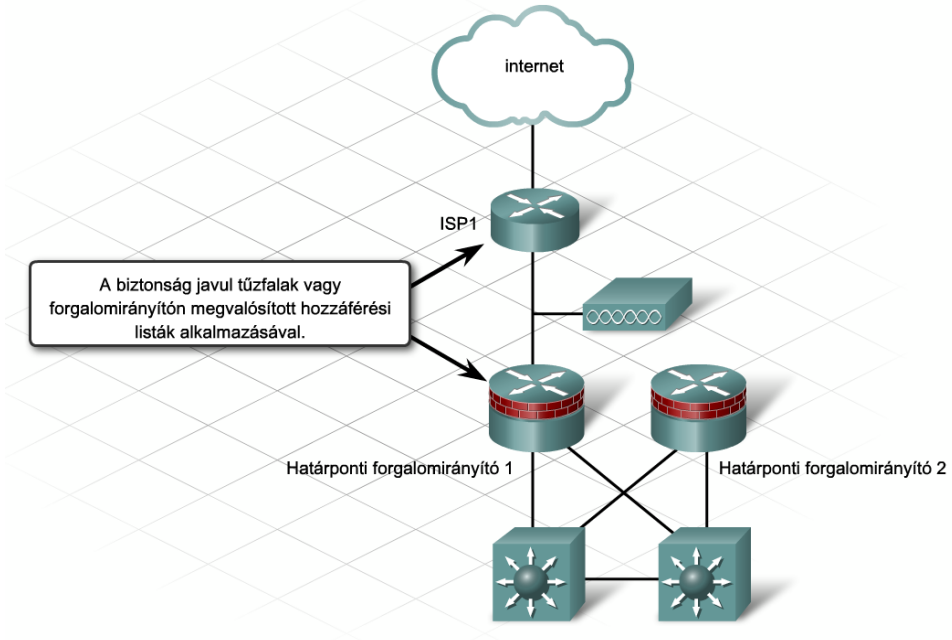
A http és webes forgalom támogatásához szükség van 3. rétegbeli eszközökre, melyek képesek a belső- és külső adatfolyamok szabályozására. Egy hálózat átvizsgálása során a befelé irányuló forgalmat a hálózati referencia vizsgálat részeként kell kezelni.

Redundancia

A kiszolgálók gyakran rendelkeznek tartalék összetevőkkel és áramforrással. Legalább kettő hálózati kártyával kell rendelkezniük, amelyek külön kapcsolókhoz csatlakoznak.

Biztonság

Egy védett hálózatba vagy a hálózatból kifelé irányuló jogosulatlan forgalom letiltására olyan biztonsági eszközöket is használnak, mint a hozzáférési listák, a tűzfalak vagy a behatolás érzékelő rendszerek. Más alkalmazás kiszolgálókhoz hasonlóan a http kiszolgálót is az internetszolgáltatónál vagy egy központosított kiszolgálófarmon kell elhelyezni a fizikai biztonság és redundancia biztosításához.



4.2.5 Microsoft tartományi szolgátatások

A stadion a Microsoft Active Directory szolgáltatásait használja, így a hálózattervezőnek mind a kiszolgálók közti, mind a kiszolgáló és ügyfél közötti kommunikációt számításba kell vennie. A Microsoft kiszolgálók több különböző típusú, kiszolgálók közötti, nagysebességű kommunikáción alapuló szolgáltatást támogatnak. Az ilyen szolgáltatásokra (pl. az Active Directory replikációra) komolyan oda kell figyelni a hálózat újratervezése során a kiszolgálók áthelyezésekor.

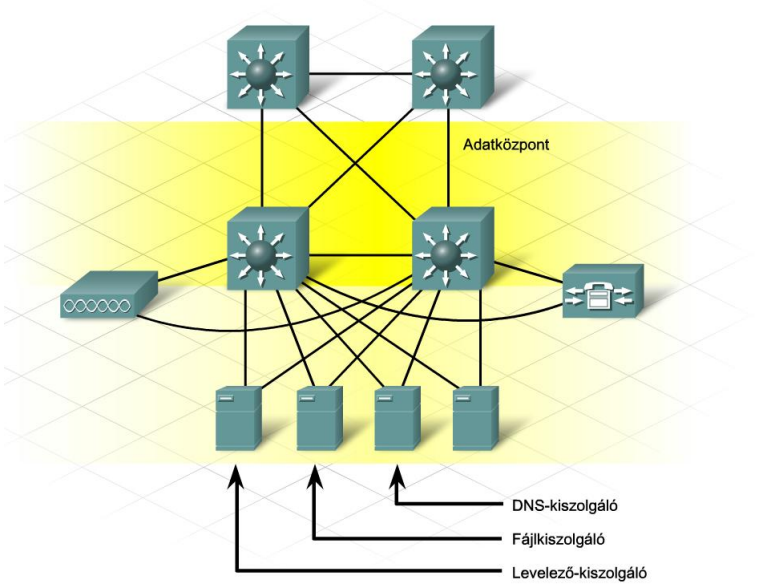
A Microsoft tartományi szolgáltatások által használt portok

A Microsoft kiszolgálók és ügyfelek TCP és UDP portok használatával kommunikálnak egymással. Ezeket a portokat különféle Microsoft szolgáltatások használják, például hitelesítés és jogosultság kezelés céljára. Több Microsoft-alapú szolgáltatás hoz létre helyi üzenetszórásos, valamint egyedi címzésű kérés csomagokat ezeken a portokon. A leggyakrabban használt TCP és UDP portok, melyeknek nyitva kell lenniük a Microsoft tartományi szolgáltatások helyes működéséhez, az alábbiak:

- UDP 53 – DNS szolgáltatások
- UDP 67 – DHCP
- UDP 123 – Windows idő (Windows Time Service)
- TCP 135 – Távoli eljárás hívás (Remote Procedure Call, RPC)
- UDP 137 – NetBIOS névfeloldás
- UDP 138 – NetBIOS datagramszolgáltatás (NetBIOS Datagram Service)
- TCP 139 – NetBIOS Kapcsolat szolgáltatás (NetBIOS Session Service)
- TCP 389 és UDP 389 – LDAP szolgáltatás
- TCP 445 – Kiszolgálói üzenetblokkok (Server Message Blocks, SMB)
- TCP 1433 – Microsoft SQL TCP felett

Active Directory és DNS

Ha Microsoft Windows 2003 kiszolgálót telepítünk egy hálózaton, akkor nagyon szoros együttműködés jön létre az Active Directory és a DNS szolgáltatások között. Az Active Directory szolgáltatásnak szüksége van a DNS-re a hitelesítést és jogosultságkezelést biztosító tartományvezérlők helyének meghatározásához. A Windows 2003 tartományvezérlőknek egyben DNS kiszolgálóknak is kell lenniük. Ez a DNS szolgáltatás biztosíthatja egy szervezet elsődleges DNS-ét, de nem Windows kiszolgálón működő internet DNS szolgáltatás esetén lehet másodlagos kiszolgáló is. A Microsoft tervezési útmutatók a DHCP és a DNS együttes használatát ajánlják. Ez biztosítja a DNS fájlokban létrejövő azonnali bejegyzéseket, ha egy PC vagy egy eszköz DHCP segítségével kap IP-címet.



4.3 A minőségbiztosítás (Quality of Service, (QoS)) bevezetése

4.3.1 Mi a szolgáltatásminőség (QoS) és miért van rá szükség?

A szolgáltatásminőség (QoS) a hálózatnak arra a képességére utal, hogy kiválasztott hálózati forgalom számára elsőbbségi szolgáltatást tud nyújtani. A QoS elsődleges célja a prioritás biztosítása, beleértve a dedikált sávszélességet, a szabályozott késleltetés ingadozást és késleltetést, valamint az alacsony értékű csomagvesztést.

Egy szervezet QoS irányelveinek létrehozásakor érdemes az előnyben részesített forgalom igényeit szem előtt tartani. A hálózat tervezőinek végig kell gondolniuk, hogy a QoS bevezetése hogyan befolyásolja a hálózati eszközök, valamint a hálózatot használó alkalmazások teljesítményét.

A felhasználók a szolgáltatás minőségét két kritérium alapján értékelik:

- A hálózatnak a felhasználók kéréseire adott válaszadási sebessége.
- Az általuk használni kívánt alkalmazások elérhetősége.

QoS segítségével kezelhetők a hálózati infrastruktúrán belüli adatfolyamok, és a hálózatot használó alkalmazások fent említett problémái.

Néhány Cisco eszköz, például a forgalomirányítók, beépített QoS mechanizmusokkal rendelkeznek.

Egyes alkalmazások rendkívül érzékenyen reagálnak a sávszélességi követelményekre, a csomagkésleltetésre, a hálózati késleltetés ingadozásra és az esetleges csomagvesztésre. Ilyen például a valósidejű IP-telefónia és a videó folyamok továbbítása.

Az IP-telefónia követelményei

Az IP-telefónia követelményrendszere egy konvergált hálózat valósidejű alkalmazásainak több problémáját is magában foglalja. A hangforgalom egy egyszerű, felhasználók közötti kapcsolatnál többet igényel. Az átvitel minősége ebben az esetben különösen fontos. Késleltetés esetén ugyanis a hang szétesik, és a szavak eltorzulnak.

A kifogásolható átviteli minőség elkerülése érdekében az IP-telefóniának QoS mechanizmusokra van szüksége. A hangcsomagoknak egy irányban nem lehet nagyobb a késleltetése, mint 150 ms. IP-telefónia alkalmazása esetén kritikus követelmény, hogy egy útvonal szomszédos ugrásai között a hangcsomagok késleltetése és késleltetés ingadozása ne legyen nagy.

Videó folyamok követelményrendszere

A videó folyam olyan videó adás, ami általában egy előre rögzített fájl küldésével valósul meg. A videót tömörített digitális jellé alakítva, és a továbbításra egy speciális webkiszolgálót alkalmazva élő műsorszórást is létrehozhatunk. Ez a videó folyam csoportcímzéssel küldve több felhasználó által is megtekinthető egy időben.

Egy QoS nélküli hálózatban minden csomag egyforma elbánásban részesül, ezért a valósidejű alkalmazások hátrányt szenvedhetnek.

A QoS nem hoz létre nagyobb sávszélességet, csak prioritáshoz köti a sávszélesség használatát. Ezzel képes támogatni az olyan alkalmazásokat (pl. IP-telefónia), melyek kivételes kezelést igényelnek. A konvergált hálózaton a prioritások kezeléséhez a QoS várakozási sorokat használ.

4.3.2 Várokozási sorok

Hang és adatforgalom

Konvergált hálózatokban állandó, kisméretű csomagokat használó hangforgalom verseng a hatalmas és rendszertelen adatfolyamot generáló kiszolgáló frissítésekkel és fájlátvitellel. Bár a hangforgalom kisméretű csomagokban utazik a hálózaton, az áthaladáskor fellépő késleltetés gyenge hangminőséget eredményez.

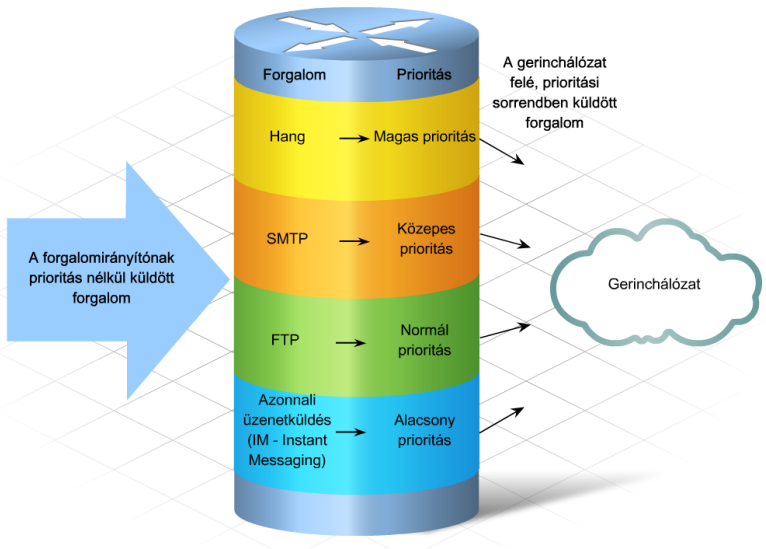
Az IP-telefóniához hasonló, valósidejű alkalmazások adatait a küldési sebességgel megegyező iramban kell feldolgozni, és nincs idő a hibás csomagok újraküldésére. A fentiek miatt a VoIP az UDP-t, mint „legjobb szándékú” szállítási protokollt használja.

Ezzel ellentétben, a fájlátvitelben résztvevő adatcsomagok óriási méretűek. Ezek a csomagok a TCP hibaellenőrző és újraküldő mechanizmusát használják a késleltetés és a csomagvesztés kezelésére.

Amíg egy adatfájl elvesztett részét újra el lehet küldeni, addig ugyanezt egy beszélgetés részeivel nem célszerű megtenni. Az előzőekből következik, hogy a kritikus, időzítésre érzékeny hang és videó forgalomnak prioritást kell élveznie az adatforgalommal szemben.

QoS mechanizmusok

A QoS prioritás biztosításához speciális mechanizmusokra van szükség. Egy forgalom prioritása lehet nagy, közepes, normális és alacsony. A várakozási sorok használata csak egyike a hálózati forgalom prioritás kezeléséhez rendelkezésre álló QoS módszereknek. A várakozási sorok segítenek a biztonságos, előre tervezhető és garantált szolgáltatás elérésében. Egy konvergált hálózaton még egy rövid idejű hálózatkiesés is komoly fennakadást eredményezhet az üzleti folyamatokban.



A prioritásos sorba rendezés négy különböző sort definiál: a magas prioritású sort ürítik mindig először.

Hardveres és szoftveres várakozási sorok

A várakozási sorokat az adatfolyamok QoS-el történő kezelésére használják. A hardveres sorok általában beérkezési sorrendben (first-come-first-served) tárolják és küldik ki a forgalmat. A hardveres sorra, mint továbbítási sorra (transmit queue – TxQ) is szoktak hivatkozni. Ez egy olyan fizikai sor, ahol a sorban álló csomagok a prioritásukhoz igazodó sorrendben várakoznak a továbbításra.

A szoftveres sorok lehetővé teszik, hogy a csomagokat a hálózat tervezője vagy a rendszergazda által beállított prioritás alapján továbbítsák. A sorok a QoS követelményeken alapulnak. Szoftveres sorokra példa a prioritásos (PQ) és a testreszabott sorban állás (CQ).

QoS megvalósítása várakozási sorokkal

Egy hálózaton a QoS megvalósítására a tervező három alaplépést hajt végre a megfelelő prioritáskezelés érdekében:

1. lépés: Forgalmi követelmények meghatározása

A QoS követelmények meghatározására feltétlenül szükség van a hang- és más kritikus alkalmazásokhoz tartozó forgalmak esetén, míg az alacsony prioritású forgalmakat „legjobb szándékú” továbbításra lehet megjelölni.

2. lépés: Forgalmi osztályok meghatározása

Egy adott típusú forgalom, azonosítása után, a megfelelő osztályba sorolható, így például a hangforgalom kapja a legnagyobb prioritást, majd ezt követi a kritikus alkalmazások forgalma. Minden más típusú forgalom az adat céljától függően normális vagy alacsony prioritású. A csomagokat megjelölik, melyik forgalmi osztályba tartoznak.

3. lépés: QoS irányelvek definiálása

Az utolsó lépés az egyes osztályok esetében használandó QoS irányelvek meghatározása. Ilyen például a várakozási sorok ütemezése és a torlódás-kezelési szabályok.

4.3.3 Prioritás és forgalomkezelés

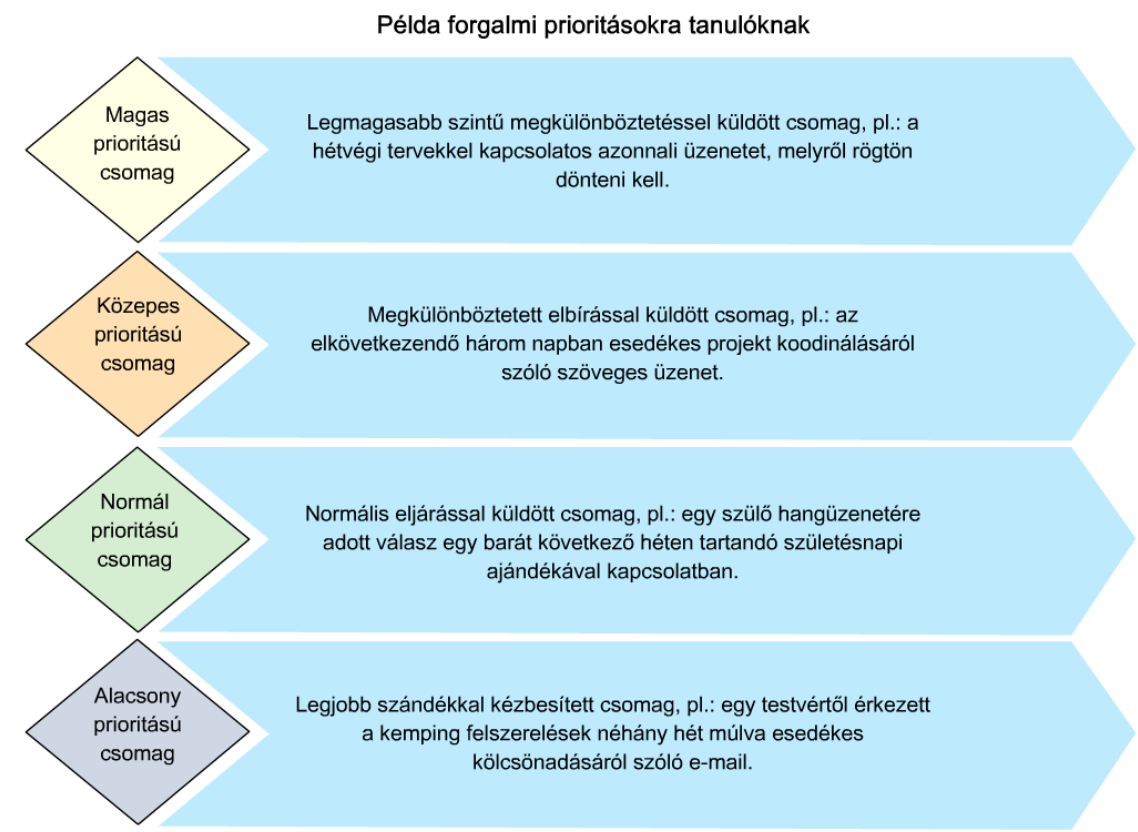
Több módszer is létezik a hálózati forgalom kezelésére. Az egyik ilyen módszer a prioritásos sorban állás (priority queuing – PQ). A QoS megvalósításának részeként a prioritásos sorban állás a forgalmat magas, közepes, normál vagy alacsony prioritású osztályokba sorolja. A prioritásos sorban állás azután ezekre a QoS osztályokra alkalmazható.

A prioritásos sorban állás az időzítésre érzékeny és a kritikus protokollok számára hasznos. A PQ négy – magas, közepes, normál és alacsony - várakozási sort hoz létre a kimenő interfészen , amelyek mind egy-egy prioritási szintnek felelnek meg. Ezek a sorok a következő jellemzőkkel konfigurálhatók:

- Sor típusa
- Forgalom hozzárendelés
- Méret

A beérkező forgalmat először osztályozzák, megjelölik az osztály jelével, majd továbbítják.

A forgalom a prioritási listában meghatározott QoS irányelvek alapján kerül a különböző sorokba. Ezek a szabályok épülhetnek a protokollra, portszámra, vagy egyéb, a megjelölt forgalomra vonatkozó kritériumra. A szabályok olyan szűrőkként viselkednek, melyek a különböző forgalomtípusokat a négy osztály-alapú várakozási sorba különítik el.

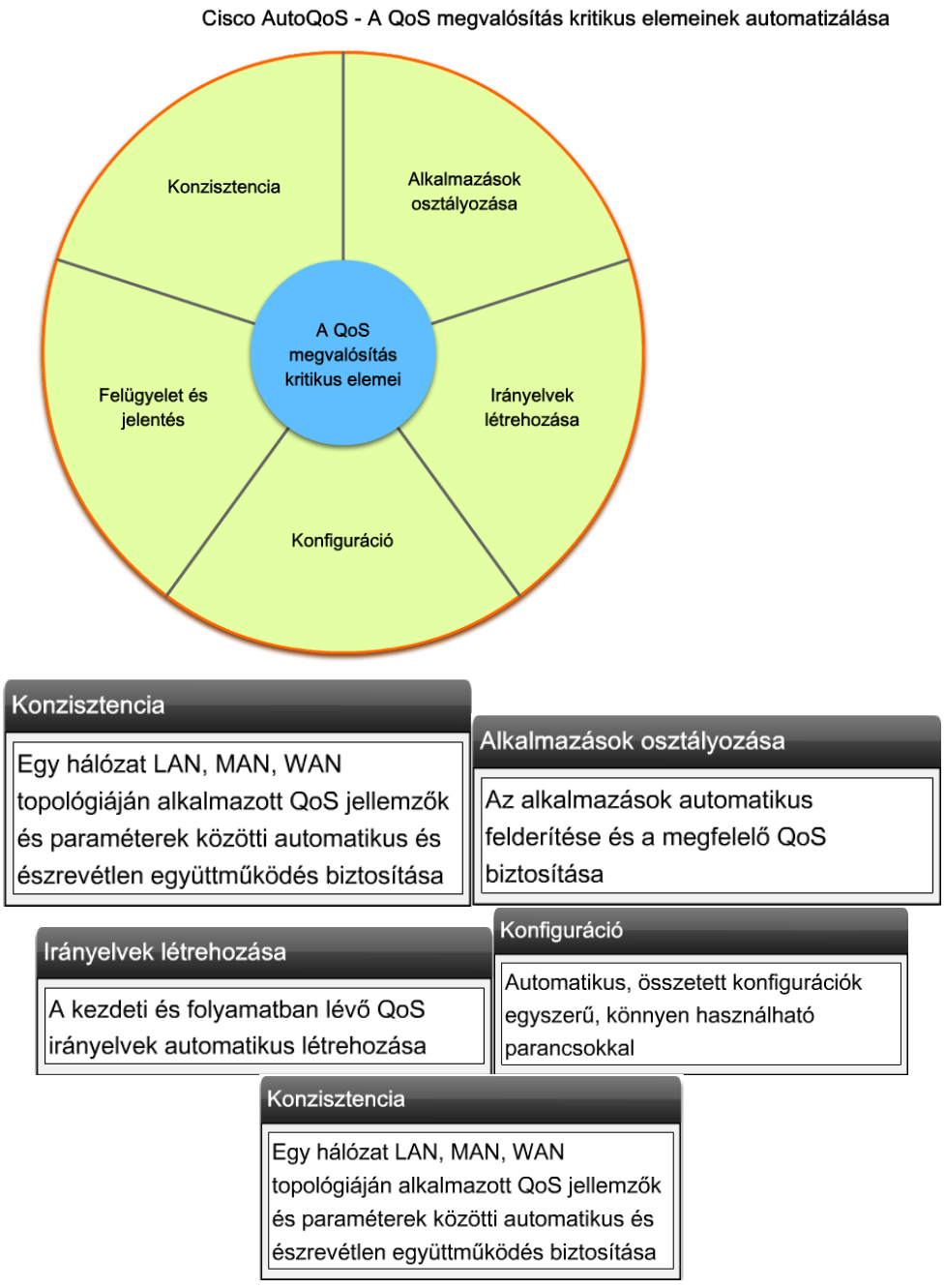


A Cisco beépített eszközöket nyújt a QoS konfigurálásának megkönnyítésére. Egyik ilyen eszköz az AutoQoS, mely a Cisco IOS szoftver részeként érhető el.

A Cisco AutoQoS egy egyszerű, intelligens parancssoros interfészt (CLI) nyújt. Ez az interfész lehetővé teszi Cisco forgalomirányítókon és kapcsolókon a LAN és a WAN QoS beállítását a VoIP támogatására.

Az AutoQoS a Cisco-tól már megszokott kiváló minőségű szolgáltatás gyakorlatát folytatja, és az ügyfelek számára megkönnyíti a hálózatok konfigurálását olyan esetekben, amikor a hang- és videó átvitelhez hasonló magas prioritású forgalom támogatását kell biztosítani.

A manuális beállítással összehasonlítva, a Cisco AutoQoS segítségével két-harmadára csökkenthető a konfigurációs idő és költség.



4.3.4 Hol alkalmazható a QoS?

QoS tulajdonságok konfigurálásakor a rendszergazda először kiválaszt egy meghatározott típusú hálózati forgalmat, és fontosságának megfelelő prioritást rendel hozzá, majd torlódáskezelő technikák használatával elsőbbségi bánásmódot biztosít számára. A QoS megvalósítható az elérési, az elosztási és a központi rétegben is.

2. rétegbeli eszközök

A elérési rétegben működő 2. rétegbeli kapcsolók az IEEE 802.1p szolgáltatási osztályok (Class of Service, CoS) alkalmazásával támogatják a QoS-t. A 2. rétegbeli kapcsolókon alkalmazott QoS osztályozással és ütemezéssel biztosítja a keretek prioritásos küldését a kapcsolóról a hálózat irányába.

3. rétegbeli eszközök

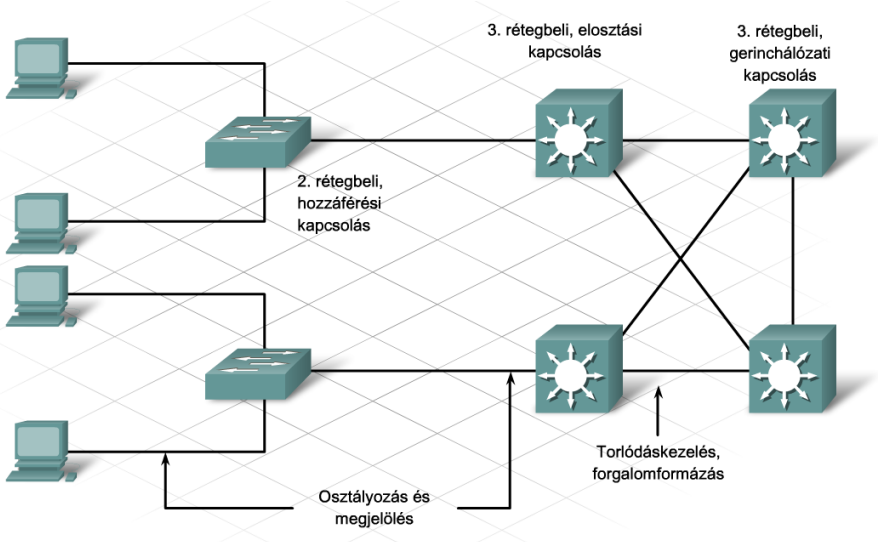
3. rétegbeli eszközök a QoS-t a fizikai interfész, az IP-cím, a logikai portszám és az IP-csomagok QoS bitjei alapján is képesek megvalósítani. Az elosztási és a központi réteg eszközein a forgalom mindkét irányában alkalmazható QoS.

Osztályozás és megjelölés

Az osztályozás az a folyamat, ahol a forgalmat csoportokba sorolják. Az osztályozás történhet protokoll vagy a forgalom jelölése alapján is. A forgalmat 2. rétegbeli szolgáltatási osztályokkal, IP sorrendiséggel (IP precedence) vagy ún. DSCP (Differentiated Services Code Point – megkülönböztetett szolgáltatások kód pont) értékkel lehet megjelölni.

- A szolgáltatási osztály (CoS) a 802.1q VLAN címke első 3 bitje.
- Az IP sorrendiség az IP fejrész ToS (Type of Service) bájtjának első 3 bitje.
- A DSCP a fejrész ToS bájtjának első 6 bitje, értékét a forgalomirányító és a kapcsoló is beállíthatja.

Az osztályozás és a megjelölés a forgalom több prioritási szintre vagy szolgáltatási osztályba történő besorolását teszi lehetővé.



4.4 A hang- és video-opciók vizsgálata

4.4.1 Konvergált hálózatok tervezési megfontolásai

A modern hálózatok az olyan konvergált szolgáltatásokat is képesek támogatni, amelyekben az adat-, hang- és videó forgalom keveredik egymással. Ennek tipikus példája a stadion hálózata.

Konvergált hálózatok kezelése

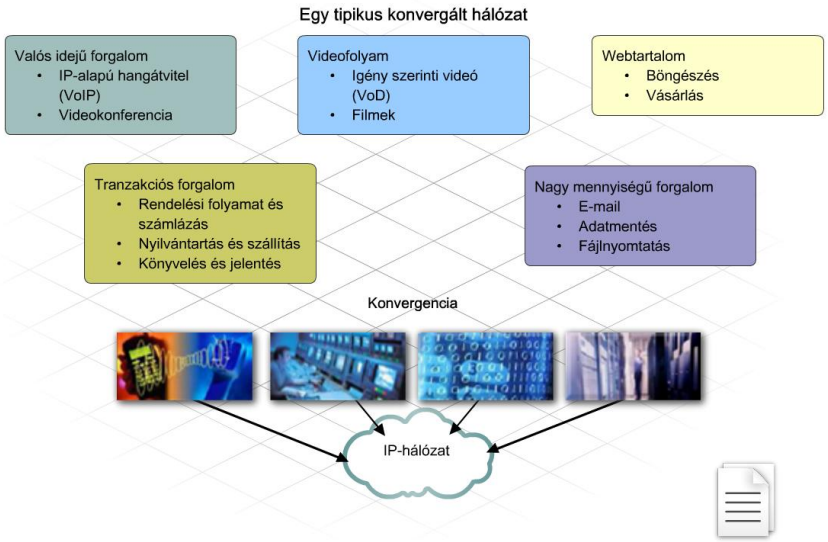
Egy konvergált hálózat hang- és videó forgalmának vezérlési módszere eltér a többi, például a webes forgalom (HTTP) szabályzásától.

Szolgáltatásminőség (QoS) konvergált hálózatokon

Minden hálózat jobban működik, ha QoS szabályozza a következőket:

- Késleltetés és késleltetés ingadozás
- Sávszélesség használat
- Csomagvesztési paraméterek

Konvergált hálózatokon erős teljesítmény - és biztonsági követelmények szükségesek az egymásnak ellentmondó igényeket támasztó forgalmak kezeléséhez. Az ilyen hálózatokon a QoS módszerek bevezetése elengedhetetlen.



Konvergált hálózatok kevert forgalomtípusaira példa:

- Hang- és videoforgalom, pl.: IP-telefónia video-műsorszórással és konferencia
- Gyakran csoportos címzésű IP-forgalomként szállított videoforgalom
- Hangalkalmazások forgalma, melyet hanggal kapcsolatos alkalmazások, mint pl.: ügyfélszolgálatok generálnak
- Kritikus forgalom, melyet például tőzsdei alkalmazások generálnak
- Elektronikus kereskedelem által generált tranzakció alapú forgalom
- Irányítóprotokollok frissítései (forgalomirányító információs protokoll - RIP, legrövidebb út protokoll - OSPF, továbbfejlesztett belső átjáróirányító protokoll - EIGRP)
- Hálózatfelügyeleti forgalom
- Legjobb szándékú forgalomként kezelt nagy mennyiségű adatátvitel, mint a fájlátvitel vagy a HTTP
- Legjobb szándékú kézbesítésnél rosszabb besorolású Scavenger forgalom (hétköznapi szórakoztató vagy illetéktelen forgalom)

4.4.2 Az IP-telefónia megvalósításának következményei

Az stadion hálózat korszerűsítésének egyik műszaki követelménye az IP-telefónia megvalósítása.

Az IP-telefónia tervezési megfontolásai

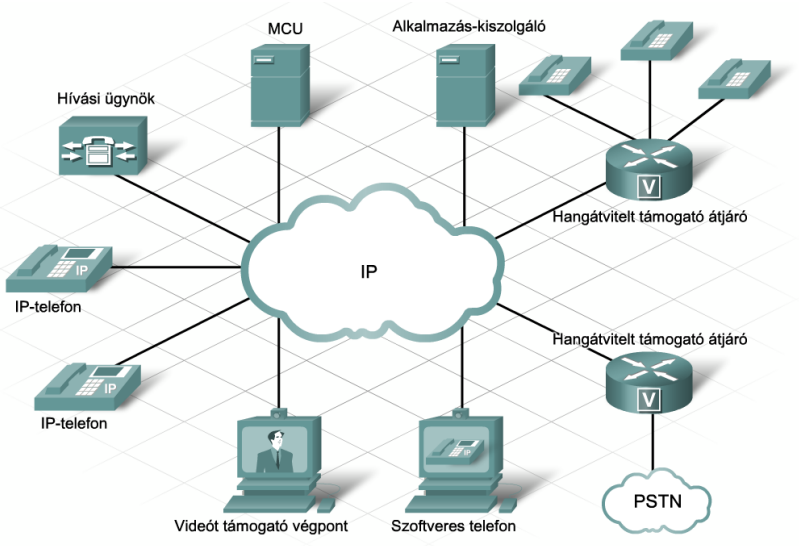
A hálózati tervnek a következőket kell tartalmaznia:

- Áramellátási és kapacitási terv
- A versengő adatfolyamok meghatározása
- Az IP-telefónia megvalósításához szükséges összetevők kiválasztása

Egy IP-telefónia megvalósítás a következő összetevőket tartalmazhatja:

- IP telefonok
- Átjáró
- Többpontos vezérlő egység (MCU)
- Hívási ügynök
- Alkalmazás kiszolgálók
- Videót támogató végpontok
- Szoftver alapú telefon

Más komponensek, mint például a szoftveres hangalkalmazások vagy az interaktív hangválasz rendszerek (interactive voice response – IVR)) további szolgáltatásokat nyújthatnak a vállalatok szükségleteinek kielégítésére.



Többpontos vezérlő egység (Multipoint Control Units, MCU)	Alkalmazás-kiszolgáló
Video- és audio-konferenciahívásokat tesz lehetővé. Erre példa a Cisco egyesített videokonferenciát támogató 3515 típusú MCU (Cisco Unified Videoconferencing 3515 MCU).	Az IP-telefon felhasználói számára biztosítja a hangeszközök, pl.: vállalati könyvtárak elérését.

Hangátvitelt támogató átjáró

Olyan eszköz (pl.: hangátvitelre képes forgalomirányító), mely a hagyományos PSTN hálózatot vagy egy analóg telefont IP-hálózathoz kapcsol. Az analóg hangcsomagok és az IP-csomagok közötti átalakítást végzi.

Szoftveres telefon

Egy PC-n vagy laptopon telepített szoftveralkalmazás, mely hanghívásokat támogat. Erre példa a Cisco IP Communicator.

Videót támogató végpont

A felhasználóknak videoalkalmazásokat nyújtó eszköz.

IP-telefon

Olyan telefon, mely IP-hálózat feletti hanghívásokat támogat. Erre példa a Cisco 7940G típusú egyesített IP-telefonja (Cisco Unified IP Phone 7940G).

Hívási ügynök

A hívásokat kezelő eszközöket és az átjárót vezérli. A hívási ügynök a PBX hagyományos telefonrendszerben betöltött feladatát látja el. Két példája a Cisco egyesített kommunikációs menedzser (Cisco Unified Communications Manager) és ennek egyszerűsített változata (Cisco Unified Communications Manager Express).

A forgalom elkülönítése

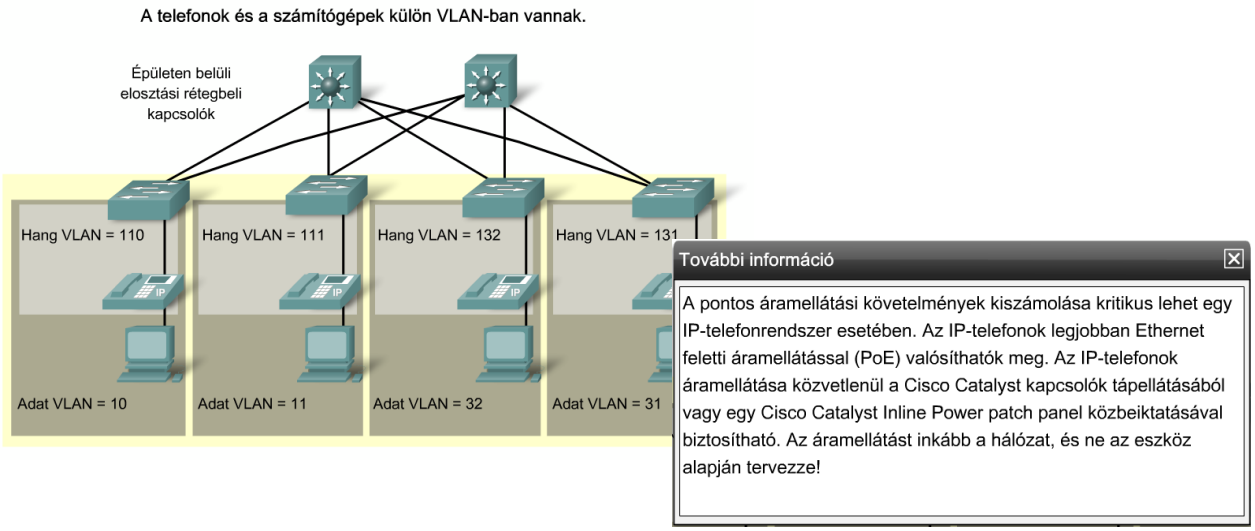
Ha az ügyfél PC és az IP-telefon is egy VLAN-ba tartozik, akkor mindkettő az elérhető sávszélesség kihasználására törekszik tekintet nélkül a másik eszközre. Az ütközések elkerülésének legegyszerűbb módszere az adatforgalom és a telefonos forgalom külön VLAN-ba helyezése.

A forgalomtípusonként külön VLAN használatának előnyei

Az eltérő típusú forgalmak külön VLAN-okba csoportosítása a következő előnyöket nyújtja:

- A hálózaton történő áthaladáskor prioritás adható az IP-telefon forgalomnak QoS segítségével.
- A hálózati problémákat könnyebben tudja azonosítani és megoldani a rendszergazda, ha a telefonos forgalom külön alhálózathoz és VLAN-hoz tartozik.

A stadion hálózatának tervezett korszerűsítése – az IP-telefónia bevezetését is beleértve – egy hatékonyabb IP-címzési rendszer és VLAN struktúra kifejlesztését igényli. A tervezőnek ezeket az információkat is bele kell foglalnia a tervezési követelmények dokumentációjába.



4. Az alkalmazások hatása a hálózat-tervezésre

A stadion vezetősége a digitális telefonrendszerét IP-telefóniára szeretné cserélni.

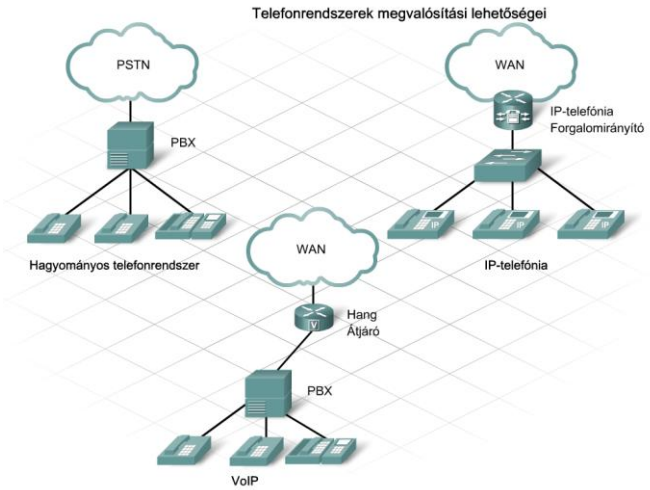
Hagyományos telefonrendszer

A hagyományos üzleti telefonrendszert tipikusan egy központi vezérlő egység, más néven magán alközpont (private branch exchange, PBX) köré építik. A PBX az eszköz típusától függően a hívásokat analóg vagy digitális vonalakra irányítja. Egy analóg faxgép vagy egy analóg telefon például analóg vonalat használ, míg egy digitális asztali telefon digitálisat. A hagyományos telefonrendszerben a telefon fizikai címe a kábelcsatlakoztatás függvénye, ezért a telefonok cseréje vagy helyváltoztatása, illeteve új telefonok üzembe helyezése jelentős mennyiségű manuális konfigurációt igényel. A legtöbb vállalat az adathálózatot támogató infrastruktúra mellett külön kábelezési infrastruktúrával is rendelkezik a telefonhálózat támogatására.

A stadion vállalatnak egy külön infrastruktúrán működő digitális PBX rendszere van.

VoIP

A Cisco a VoIP kifejezést a hangátvitelre képes forgalomirányítóknak arra a képességére használja, amivel a hagyományos telefon analóg hangcsomagjait IP csomagokká alakítja és a végállomások között irányítja. Az informatikában ezt a kifejezést az IP-telefóniával felváltva használják. A VoIP esetén a PBX egy hangátvitelre képes forgalomirányítóhoz csatlakozik, és nem a hagyományos kapcsolt telefonhálózathoz (PSTN) vagy más PBX-hez. A vállalatok a VoIP-t azért választják, hogy a távolsági hívásdíjak és a szükséges kiszolgáló személyzet számának csökkentésével, valamint állandó WAN összeköttetések létrehozásával a költségeket a lehető legalacsonyabb szintre szorítsák.



IP-telefónia

Az IP-telefónia a hagyományos telefonokat IP-telefonkészülékekkel cseréli fel, és Egyesített kommunikációs menedzsert (Cisco Unified Communications Manager) használ, mely a hívások vezérlésére és jelzésére alkalmas kiszolgáló. Az IP-telefónia a következő jellemzőkkel rendelkezik:

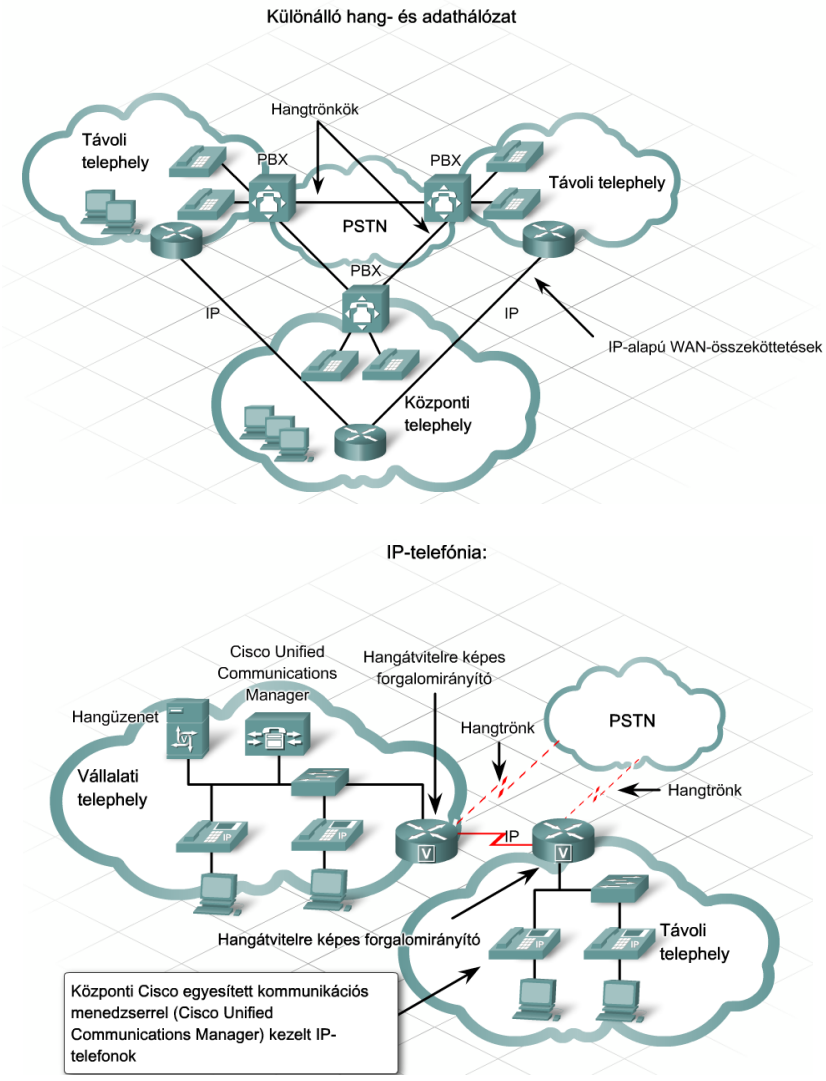
- Analóg vagy digitális rendszerek helyett IP hálózaton kommunikáló hang és hangüzenet alkalmazásokat egyesít.
- IP-telefonkészülék segítségével alakítja át a hangcsomagokat IP-csomagokká

- A hívások PBX-re jellemző központi irányítása helyett egyenrangú kapcsolatokat létesít a kommunikáló telefonok között.

A hálózattervező és az ügyfél beépítheti a VoIP-t vagy az IP-telefóniát a meglévő adathálózatba, és így egy konvergált hálózatot hozhat létre.

A Stadion Kht. az IP-telefónia bevezetésétől a következő előnyöket várja:

- A szervezeten belüli irodákat érintő változások (költözés, átszervezés vagy új iroda létesítése) egyszerűbb adminisztrációja.
- Új alkalmazások bevezetésének lehetősége a telefonrendszerben (pl. címtárak és weboldalak).
- Az elkülönített infrastruktúrák kisebb kezelési költsége.



4.4.3 Élő- és igény szerinti video adás

A nagyobb sávszélesség lehetővé teszi, hogy a felhasználók számítógépeiken audió és videó alkalmazásokat is futtathassanak, valamint a videót élőben és VoD-ként (Video on Demand – igény szerinti videó adás) is megtekinthessék.

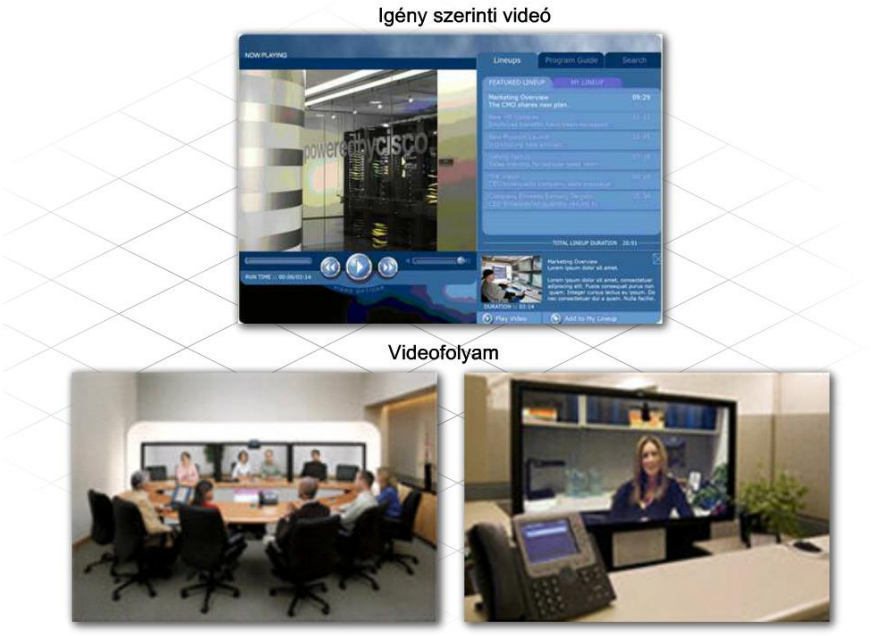
Élő videó

Az élő videó (videófolyam) lehetővé teszi, hogy a felhasználók még azelőtt láthassák annak tartalmát, hogy az összes médiacsomag megérkezne a számítógépükre. A videó folyam fájljai megszakítás nélküli adatfolyamként rögtön hozzáférhetőek, nem kell várni a megtekintés előtt. A videó folyamoknál nincs szükség a nagyméretű médiafájlok tárolására vagy a tárolási hely lefoglalására lejátszás előtt. Élő videó adást gyakran küldenek multicast csomagokban egyszerre több felhasználónak is.

VoD

VoD-vel a felhasználók elindíthatnak egy videó folyamot, vagy letölthetik a teljes tartalmat a számítógépükre. Egy teljes videó fájl lejátszás előtti számítógépre mentését tárol-és-továbbít eljárásnak is nevezik. Ez a módszer csökkenti a rendszer erőforrásainak terhelését. Egy erre a célra telepített kiszolgáló segítségével arra is lehetősége van a felhasználóknak, hogy a médiafolyamot a számítógép gyorsítótárába irányítsák, s így a fájlok eltárolhatók, és későbbi időpontban megtekinthetők. A VoD egyedi címzésű csomagokkal küldi el az adatokat a videó kérést indító felhasználónak.

A stadion vezetősége az élő és igény szerinti videó letöltést is szeretné megvalósítani. Ez további forgalmat eredményez a hálózaton A videó tárolását megvalósító kiszolgálók egy közös kiszolgálófarmon történő elhelyezése megkönnyíti a hibakeresést, valamint a biztonsági és redundancia problémák kezelését.



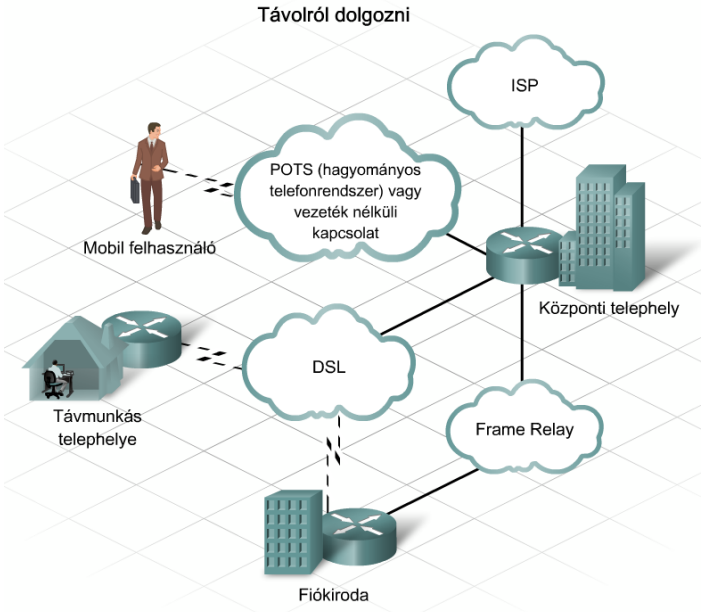
4.4.4 Hang- és videó alkalmazások biztosítása távmunkások számára

A technológia fejlődése nagyobb rugalmasságot nyújt az alkalmazottaknak a munka módjának és helyszínének megválasztásában. A stadion esetében például a dolgozók számos távoli helyszínről csatlakozhatnak a központi telephelyhez.

A központi erőforrások és a kommunikációs lehetőségek kihasználásához a távmunkás vagy ingázó alkalmazottaknak és a fiókirodáknak legalább egy WAN összeköttetéssel kell rendelkezniük a központi telephelyhez. A WAN összeköttetés sávszélesség igénye a felhasználó munkájához szükséges hálózati erőforrás típusától függ. Ha a távmunkás az IP-telefonhálózatba is bekapcsolódik, akkor szükség lehet egy híváskezelő rendszer elhelyezésére a távoli helyszínen. A tervezőnek azt is figyelembe kell vennie, hogy a távdolgozóknak szükségük van-e a videó erőforrások egyidejű elérésére. Ez a körülmény befolyásolja a sávszélesség követelményt. A videó folyamok használhatók például szervezeti értekezletek tartásához is. Ezekhez a tervezési megfontolásokhoz fel kell mérni a központi telephely WAN csatlakozásának sávszélességét is.

Állandó vagy igény szerinti összeköttetés?

A hálózattervező eldönti, hogy a központi telephellyel állandó vagy igény szerint felépülő összeköttetésre van-e szükség. A tervező az ügyféllel együtt gondolja végig a költségvetési, a biztonsági és elérhetőségi követelmények.



További információ

Az ábrán látható hálózatnak elsődleges kapcsolatként Frame Relay, tartalék kapcsolatként DSL összeköttetése van. A távmunkásoknak is szükségük lehet a fiókiroda elérésére különböző kapcsolattípusokon keresztül. Ezért a fiókirodában található forgalomirányítóknak képeseknek kell lenniük a különböző WAN-kapcsolatok támogatására.

A nagysebességű internetkapcsolat megfelelő megoldás a távolról dolgozók számára. Távoli irodákban könnyen telepíthető és a legtöbb szállodában is elérhető. A stadion vezetősége vezetéknélküli hozzáférési pontok segítségével szeretne internet elérést biztosítani a luxus páholyokban és a stadion éttermében.

Az utazók számára néha az aszinkron betárcsázós kapcsolat az egyetlen megoldás a távoli elérés biztosítására. Modemmel felszerelt laptop és a meglévő telefonhálózat segítségével kapcsolódhatnak a vállalat hálózatához.

A távmunkások számára elérhető WAN kapcsolatok a következő jellemzőkkel rendelkeznek:

- Aszinkron betárcsázós
- ISDN BRI
- Kábelmodem
- DSL
- Vezetéknélküli és műholdas
- VPN

4.5 Az alkalmazások és a forgalom áramlásának dokumentálása

4.5.1 Mi az adatfolyam?

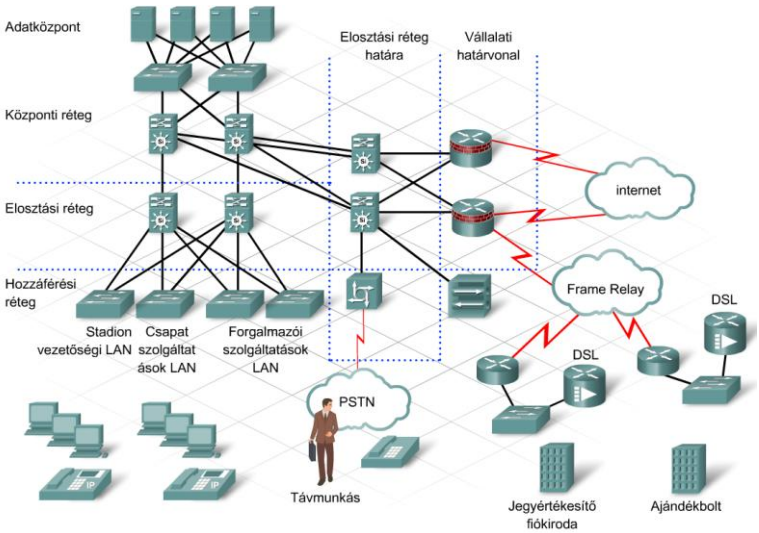
Adatfolyam

A hálózati forgalom hasonló a város utcáinak forgalmához. Ahogy az autók mozognak városszerte egyik helyről a másikra, ugyanúgy áramlik az alkalmazások által generált adatfolyam is a hálózaton egyik helyről a másikra.

Egy autó egy kiindulópontból egy célállomás felé közlekedik az utcán. Ugyanígy, egy alkalmazás által generált adatfolyam, mint egy egyirányú csomagáradat mozog a forrás és a cél között. Az útvonalat általában a hálózati réteg IP-címei határozzák meg. A hálózaton konfigurált QoS-től és egyéb felügyeleti paraméterektől függően más információ, például a szállítási rétegbeli forrás- és célport címek is befolyásolhatják az útvonalat. Egy állomás például egy adatfolyam formájában elküld egy fájlra vonatkozó kérést egy kiszolgálónak. A kiszolgáló feldolgozza a kérést, és egy másik adatfolyammal elküldi a fájlt az állomásnak.

Forgalomszabályozás

Valamiféle forgalomszabályozás nélkül (útjelző táblák, vagy elterelő utak) az utcákon torlódás alakulna ki. A hálózatokon szintén szükség van az adatforgalom szabályozására. A QoS mechanizmusok az alkalmazások forgalma számára biztosítják az akadálymentes adatáramlást a hálózaton.



Alkalmazások adatfolyamai

Az alkalmazásoknak a hálózatba befelé, illetve onnan kifelé irányuló adatforgalma lehet néha minimális, míg máskor igen jelentős mértékű. A sportstadion esetében például a kora reggeli forgalom általában e-mailezést, internetelérést és a kiszolgálókra történő fájlfeltöltéseket jelent. A délutáni forgalomban ezzel szemben VoIP, e-mail, fájlátviteli és jegyárusításból származó tranzakciós folyamatok is lehetnek.

Ha a hálózattervező mérnök a stadion tervezésének kezdeti fázisában nem helyesen becsüli meg az alkalmazások adatforgalmának mennyiségét, akkor mindegyik alkalmazás torlódást és teljesítmény visszaesést érzékelhet. A jegyárusító vagy az étel- és italárusító pavilonokban dolgozó ügyfelek jelentős mértékű késleltetést észlelhetnek, sőt az is előfordulhat, hogy nem érik el az igényelt alkalmazást. Az ügyfelek elégedettsége az ilyen helyzetek miatt csökkenhet.

A jelenlegi és a tervezett forgalom könnyebb áttekintéséhez a tervező adatáramlási grafikont készít. Az első lépés a tervezett hálózati alkalmazások meghatározása. A szükséges információ a következő forrásokból gyűjthető össze:

- Felhasználói visszajelzések
- Hálózat felülvizsgálata
- Forgalomanalízis

A tervező bejelöli az alkalmazásokat és a hozzájuk kapcsolódó hardverelemeket a hálózati diagramon.

Alkalmazás típusa	Alkalmazási	Prioritás	Megjegyzések
Belső e-mail	Outlook	Magas	
Külső e-mail	Outlook	Normális	
Hangátvitel a hálózaton	IP Telephony	Magas	A vállalat a hagyományos telefonokat IP telefonokra cseréli.
Webböngésző	Internet Explorer, Netscape Navigator, Opera	Alacsony	
igény szerinti videó szolgáltatás (Video on Demand)	IP/TV	Magas	Vezetéknélküli videoszolgáltatások elérhetők lesznek a stadion egész területén.
Adatbázis		Magas	Kiszolgálókat a hálózat egész területére fognak telepíteni.
Ügyfélszolgálati alkalmazás	A stadion alkalmazásainak listája	Magas	

Különösen fontos az állomások közötti adatfolyamok meghatározása. A tervező a logikai vagy fizikai diagram alapján tervezi meg a meglévő és az új alkalmazások együttműködését.

A tervező általában egy tervező program, például az MS Visio segítségével készíti el a hálózat alkalmazásokat és logikai topológiát is tartalmazó diagramját.

Miután elkészült az alkalmazásokat, eszközöket és adatáramlást is felvázoló diagram, a tervező megvizsgálja a tervezetet és meghatározza azokat a helyeket, ahol a hálózat még fejleszthető.

A logikai diagramból a lehetséges torlódási pontok is meghatározhatók. A tervező ezután kiválasztja az állomások közötti, illetve az állomások és a kiszolgáló közötti adatforgalom kezelésére alkalmas berendezést.

A stadion esetében a logikai topológiai diagram megmutatja mind az állomások közötti, mind pedig az állomások és kiszolgáló közötti adatáramlást. Az eszközök közötti kapcsolat az ott használni kívánt alkalmazásokat is jelöli. Az állomások közötti adatforgalom viszonylag elenyésző az állomás és kiszolgáló közötti adatforgalomhoz képest.

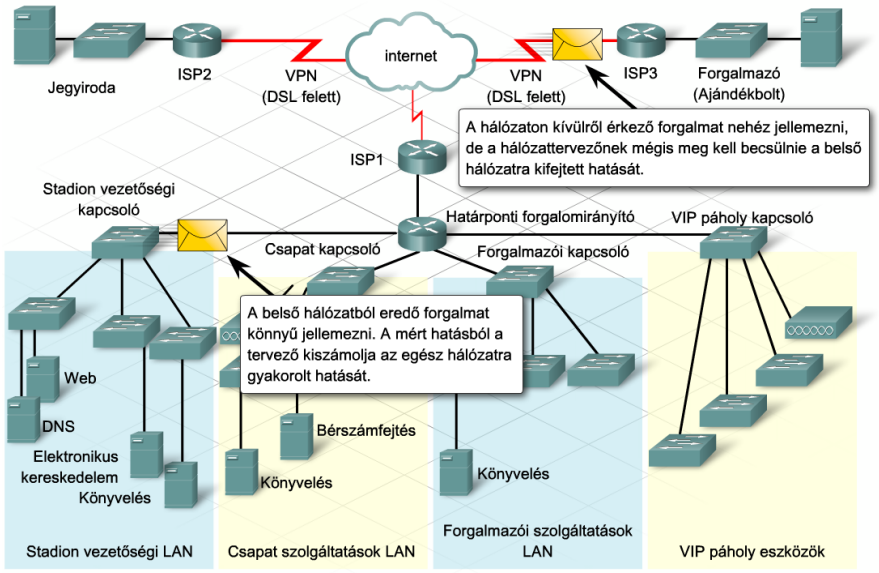
4.5.2 Belső (intranet) adatfolyamok ábrázolása

A stadion hálózata egy több működési területtel rendelkező, összetett szervezetet szolgál ki. A vezetőségi irodák, kiszolgálók, forgalmazók és jegyárusító irodák mind egy nagyobb hálózat részeit alkotják.

A stadion minden LAN-ja állomások közötti, valamint állomás és kiszolgáló közötti forgalmat kezel. Az állomások közötti általános fájlátvitel és az e-mail forgalom nem használ nagy sávszélességet. A kiszolgálóra történő napi mentések azonban nagy sávszélességet igényelnek, melyet a tervezési fázisban alaposan mérlegelni kell.

Egy új hálózat tervezésekor vagy egy meglévő hálózat korszerűsítésekor mind a külső, mind a belső adatforgalmat gondosan fel kell mérni. Ez a felmérés különleges kihívást jelent a hálózattervező számára:

- A belső hálózat forgalmát könnyű meghatározni. A felbecsült forgalom alapján a hálózat kihasználtsága számítható.
- A külső forrásoktól érkező forgalmat nehéz jellemezni, a tervezőnek azonban meg kell becsülnie a külső forgalom sávszélesség követelményét is.



4.5.3 A távoli telephelyekre illetve onnan kifelé áramló adatfolyamok ábrázolása

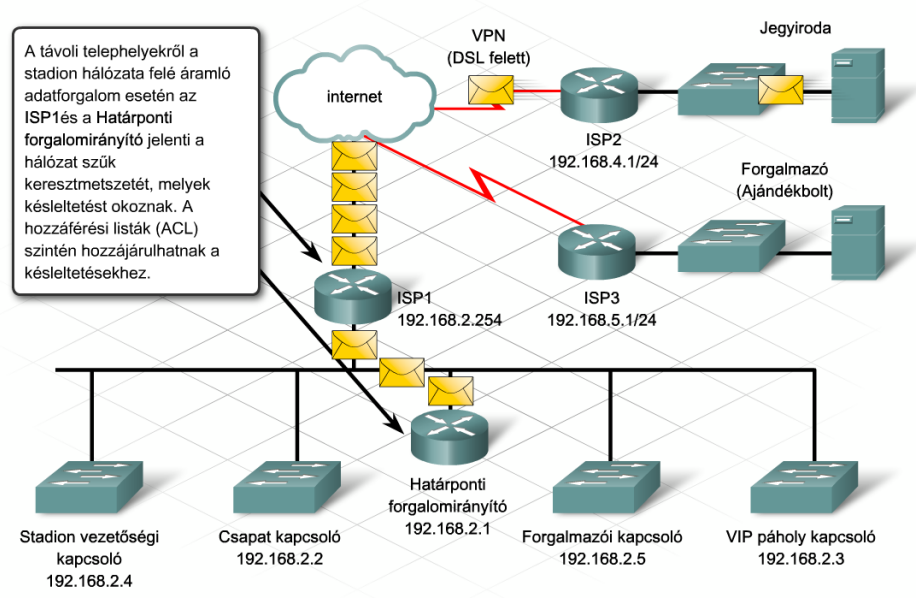
A belső LAN összes részének jellemzése és ábrázolása után a tervező a távoli telephelyekre, valamint a VPN-re összpontosít.

Egy távoli telephelyre érkező vagy onnan induló adatforgalom kicsi is lehet. A stadion hálózatában ez a forgalom ugyan szerény, de a jegyirodáktól a stadionban elhelyezett kiszolgálókig mozgó

elsődlegesen tranzakciós folyamatokat is tartalmaz. Mivel ezek kritikus alkalmazások, ezért fontos az adatfolyamok beazonosítása a QoS, a redundancia és a biztonsági szempontok érvényesítéséhez.

A LAN diagramhoz hasonlóan a forgalmat generáló távoli eszközök meghatározására is szükség van. A távoli telephelyeket a stadionnal összekötő forgalomirányítók és kapcsolók az alkalmazások adatforgalma által megtett útvonal részét képezik.

A tervező mérnöknek a távoli telephelyekről áramló forgalom mennyiségét a stadion hálózatába érkező külső forgalom részeként kell felbecsülnie. Azt is meg kell határoznia, hogy ACL vagy tűzfal használata mennyire befolyásolja a forgalom áramlását.



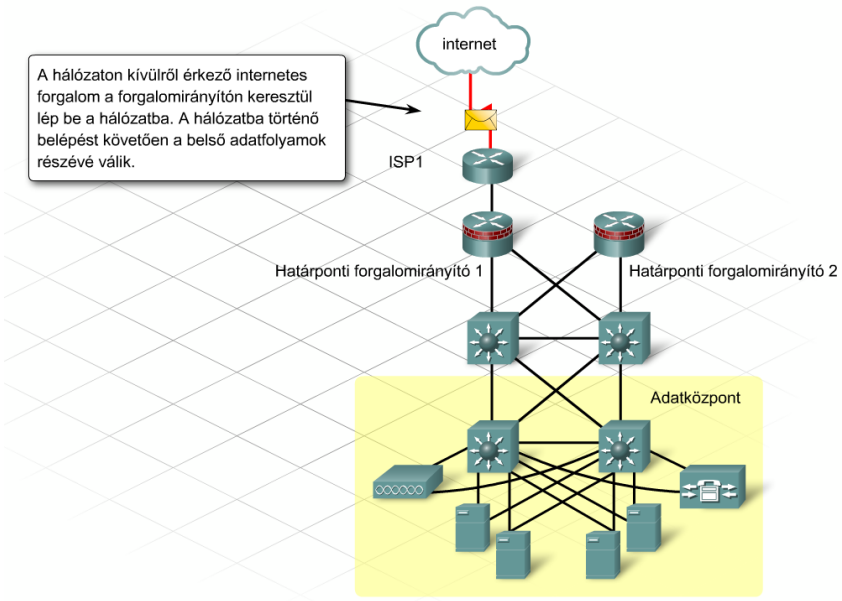
4.5.4 A külső forgalom ábrázolása

Bár a stadion meglévő hálózatában a forgalom túlnyomóan hálózaton belüli, a tervezőnek számításba kell vennie az internet felé irányuló külső forgalmat is.

Az internet ábrázolása lehetetlen, tekintettel a kapcsolódó eszközök hatalmas számára. Ennek ellenére meghatározhatók az alábbiak:

- Az internet felé irányuló kimenő forgalom. Az ilyen forgalomra példa a stadion felhasználói által, külső erőforrások (pl. online sportesemények) elérését célzó forgalom.
- Az internet felől érkező, helyi szolgáltatások elérésére irányuló forgalom. Erre példa a vásárlások feldolgozását végző belső kiszolgálók elérésével történő online jegyvásárlás.

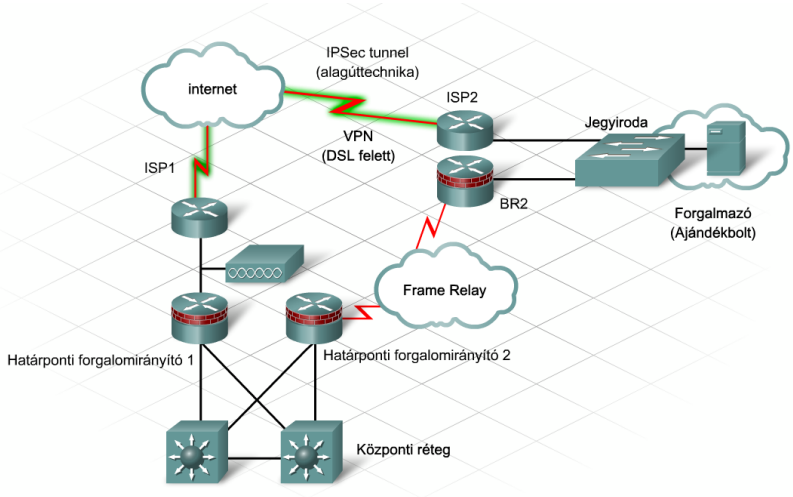
Az internettel kapcsolatos belső vagy külső adatfolyamok meghatározásakor a tervező felméri a forgalom megfelelő kezeléséhez szükséges redundanciára és biztonságra vonatkozó igényeket.



4.5.5 Extranet forgalom ábrázolása

A stadionnak egy távoli telephelye és egy külső forgalmazója van, s ezeknek jogosultságuk van a belső hálózat VPN-en keresztüli elérésére. Ezek a VPN-ek a stadion belső hálózatának elérését engedélyezik biztonságos, titkosított kapcsolaton keresztül. A stadionnak van egy web-alapú, elektronikus kereskedelmet támogató kiszolgálója, mellyel az ügyfelek jegyet vásárolhatnak. Ez a kiszolgáló SSL használatával védett.

A megbízhatónak minősített forgalmazók és ügyfelek IPSec-et használnak a stadion hálózata felé áramló adatfolyamok védelméhez.



4.6 A fejezet összefoglalása

- A végfelhasználók a hálózat teljesítményét az alkalmazások rendelkezésre állása és válaszideje alapján mérik.
- Az alkalmazások teljesítményének mértékét a felhasználó elégedettsége és a normális technikai adatok kombinációjaként kellene megadni, mint pl.: a hálózat áteresztőképessége vagy a sikeres tranzakciók száma.

4. Az alkalmazások hatása a hálózat-tervezésre

- Az alkalmazások közötti kommunikációnak négy különböző típusa létezik:
  - Ügyfél-ügyfél
  - Ügyfél-elosztott kiszolgáló
  - Ügyfél-kiszolgálófarm
  - Ügyfél-vállalati határ
- Egy meglévő hálózat alkalmazásjellemzési folyamatának első lépése az információk több eljárás szerinti begyűjtése, melyek származhatnak a szervezeti adatokból, a hálózat átvizsgálásából és forgalom elemzéséből.
- A telepített hardverek befolyásolhatják a hálózati alkalmazások teljesítményét.
- Hardverkésleltetést okozhat egy eszköz csomagszűrési és -továbbítási ideje.
- Késleltetést azok az eszközök is okozhatnak, melyek nem rendelkeznek megfelelő processzorral és elég memóriával a modern alkalmazások által létrehozott forgalomlöketek kezeléséhez.
- A felülről-lefelé megközelítés a fizikai infrastruktúrának a hálózati alkalmazások igényeihez igazodó megtervezése.
- Egy új alkalmazás telepítésekor a hálózattervező mérnöknek végig kell gondolnia az új alkalmazásnak a meglévők teljesítményére kifejtett hatását.
- Az alkalmazások forgalmának típusa és a különböző alkalmazáscsoportok határozzák meg a hálózattervezés során a sávszélesség és áteresztőképesség követelményeit.
- A leggyakrabban előforduló alkalmazástípusok közé tartoznak:
  - Tranzakciókezelő alkalmazások
  - Valós idejű adatfolyamokat továbbító alkalmazások
  - Fájlátviteli és levelező alkalmazások
  - HTTP és webes alkalmazások
  - Microsoft tartományi szolgáltatások
- A tranzakciókezelés rendelkezésre állást, gyors válaszidőt és biztonságos átviteli módszerek biztosítását várja a hálózattól.
- Az adatfolyam letöltése és az IP-telefónia is csak alacsony késleltetés mellett képes magas színvonalú eredmény létrehozására. Ezek az alkalmazások egyedi követelményeket támasztanak a hálózat tervezésével szemben.
- A valós idejű szállítási protokoll (Real-Time Transport Protocol, RTP) és a valós idejű átvitelvezérlésű protokoll (Real-Time Transport Control Protocol, RTCP) két olyan protokoll, mely a késleltetésérzékeny alkalmazások követelményeit támogatja.
- A fájlátviteli és a levelező alkalmazások hatalmas csomagméretet használnak és megbecsülhetetlen időintervallumokban nagy mennyiségű forgalmat hoznak létre a hálózaton. Ez a forgalom megakadályozhatja a késleltetésre érzékeny (hang- és video-) alkalmazások csomagjainak kézbesítését.
- A fájlátviteli és levelező alkalmazások számára a megbízhatóság és rendelkezésre fontosabb mint a késleltetés.
- Nagy mennyiségű webes forgalmat támogató hálózat elsődleges megfontolásai közé tartozik a biztonság és megbízhatóság. Az üzleti webkiszolgálók számára szükséges megbízhatóság redundáns eszközökkel és útvonalakkal biztosítható.
- A tervezésnél külön megfontolást igényel a Microsoft tartományi szolgáltatások támogatása. Az Active Directory-hoz a Microsoft tartományvezérlőkön aktív DNS-

szolgáltatásra van szükség, valamint a kiszolgálók és az ügyfelek közötti meghatározott UDP és TCP portok nyitott állapotára.

- A QoS elsődleges célja a prioritás, beleértve a dedikált sávszélesség, a szabályozott késleltetésingadozás és késleltetés, valamint kevesebb csomagvesztés biztosítása.
- A QoS nem hoz létre nagyobb sávszélességet. Várakozási sorokkal kezeli a sávszélesség-használatot, így támogatva az olyan alkalmazásokat (IP-telefónia), melyek a leginkább késleltetésérzékenyek.
- A megfelelő prioritáskezelés érdekében a következő három alaplépés végrehajtása szükséges:
    - 1. lépés: Forgalmi követelmények meghatározása
    - 2. lépés: Forgalmi osztályok meghatározása
    - 3. lépés: QoS szabályok definiálása
- IP-telefóniát is támogató hálózat tervezésénél számos új eszköz hozzáadását kell megfontolni. Ezek közé tartoznak a telefonok, IP-átjáró és a hívásvezérlő egységek.
- VoIP szolgáltatásokat hangátvitelre képes forgalomirányítókon is lehet alkalmazni, melyek az analóg hangcsomagokat IP-csomagokká alakítják a WAN-kapcsolaton történő továbbításhoz. Így kiküszöbölhetők a fiókirodák közötti távolsági hívásdíjak.
- Az IP telefónia a hagyományos telefonok helyett IP telefonokat használ, mely azonnal IP csomagokká alakítja a hangforgalmat. Ilyen rendszereknél hívásvezérlő egységek, pl.: a Cisco egyesített kommunikációs menedzser (Cisco Unified Communications Manager) segítségével történik a hívásfelépítés és -irányítás.
- Az élő videofolyam letöltése és az igény szerinti videó eltérő forgalmi követelményekkel rendelkezik. Az élő műsorszórás csoportos címzésű, míg az igény szerinti videó a kérést indító felhasználónak küldött egyedi címzésű csomagokkal történik.

5. A hálózati terv létrehozása

5.1 A követelmények elemzése

5.1.1 Az üzleti célok és a műszaki követelmények elemzése

A stadion hálózat korszerűsítésének tervezését csak a követelmények ismeretében és a meglévő hálózat elemzését követően lehet elkezdeni.

A hálózat tervezője először fontossági sorrendben mérlegeli az üzleti célokat. Korábban a PPDIOO folyamat részeként már elkészítette a Tervezési Követelmények című dokumentumot, mely az üzleti célokat és az azokat támogató műszaki követelményeket tartalmazza. A projekt sikerének alapvető feltétele, hogy az új terv megvalósítson minden üzleti célt.

Az üzleti céloknak megfelelő hálózati terv létrehozása többlépéses folyamat. A tervező általában a következő lépéseket követi:

1. lépés: Felsorolja azokat az üzleti célokat, melyeket az új tervnek teljesítenie kell.

2. lépés: Meghatározza a célok eléréséhez szükséges változtatásokat és fejlesztéseket.

3. lépés: Megállapítja az egyes változtatások végrehajtásához szükséges műszaki követelményeket.

4. lépés: Meghatározza, hogy a terv milyen módon képes az egyes műszaki követelményeket teljesíteni.

5. lépés: Meghatározza a végső terv összetevőit.

Minden üzleti cél esetében ezeket a lépéseket követve határozhatók meg a hálózati terv szükséges elemei.

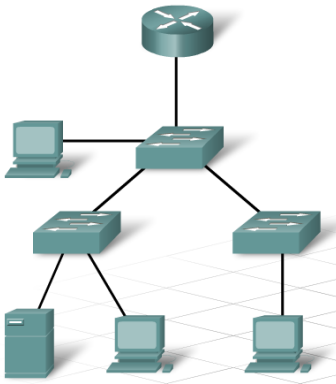
2. lépés: A célok eléréséhez szükséges változtatások és kiegészítések meghatározása.

1. 24 órás hozzáférés biztosítása a kamerákhoz és a tárolt videókhoz a helyi hálózaton és az interneten keresztül.
2. Automatikus jegykezelés bevezetése a látogatók stadionba jutásának meggyorsítására.
3. A vezetéknélküli lefedettség növelése az ügyfél-elvárásokhoz igazodva.
4. A stadionban lévő forgalmazók számának növelése és a szolgáltatások javítása.

3. lépés: A változtatásokhoz szükséges technikai követelmények meghatározása.

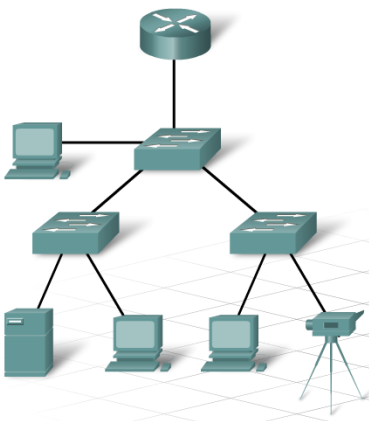
1. 24 órás hozzáférés biztosítása a kamerákhoz és A tárolt videókhoz a helyi hálózaton és az interneten keresztül.
   - A biztonsági megfigyelő hálózat csatlakoztatása a LAN-hoz.
   - Korlátozott hozzáférés biztosítása a kamerákhoz és a videókat tároló kiszolgálókhoz.
   - Webes hozzáférés biztosítása a kamerákhoz és a tárolt videókhoz.
   - A biztonsági megfigyelő hálózat rendelkezésre állásának biztosítása.

4. lépés: A technikai követelmények tervezésre gyakorolt hatásainak meghatározása:



A biztonsági megfigyelő hálózat csatlakoztatása a LAN-hoz.
- A LAN-on belül hova kell a biztonsági megfigyelő hálózatot csatlakoztatni (Hozzáférési réteg? Elosztási réteg? Központi réteg?)
- A szükséges eszközök képességeinek felmérése - Sávszélességigény? Hány összeköttetésre van szükség? Ezek irányított vagy kapcsolt összeköttetések?

5. lépés: A végső terv összetevőinek meghatározása:



- A központi réteghez vezető irányított összeköttetések hozzáférést biztosítanak a videókhoz mind a helyi LAN, mind az internet felől.
- A forgalomirányító tűzfal jellemzői lehetővé teszik a hozzáférések korlátozásának konfigurálását, hogy csak az arra jogosult állomások láthassák a videokat.

A korlátok kezelése

A Tervezési Követelmények dokumentuma a korlátok listáját is tartalmazza. Amikor a tervező korlátokba ütközik, rendszerint kompromisszumot kell kötnie, melynek során megvizsgálja az összes lehetséges megoldást, majd kiválasztja a legjobbakat.

A kompromisszumok kezelése

A kompromisszum itt azt jelenti, hogy a tervező egy előnyös megoldást egy másik, hasznosabbnak ítélt megoldásra cserél. A tervezési korlátok miatt gyakran előfordul, hogy kompromisszumra kell jutni az ideális és a reálisan megvalósítható tervek, vagyis az ideális megoldás valamint a költség- és időkorlátok realitása között. A tervező feladata, hogy ezeknek a kompromisszumoknak a bővíthetőségre, rendelkezésre állásra, biztonságra és felügyelhetőségre gyakorolt hatását minimálisra csökkentse.

A stadion hálózat tervezésekor például kompromisszumra kell jutni az internet csatlakozásokkal kapcsolatban, mivel anyagi okokból nem lehetséges egy tartalékvonal megrendelése egy másik szolgáltatótól (ISP). Ennek következtében az e-kereskedelmi kiszolgálók rendelkezésre állási követelményeinek teljesítéséhez egy alternatív megoldásra van szükség. A tervező tartalék kiszolgálók kihelyezését javasolja az internetszolgáltatóhoz, hogy a kapcsolat hibája esetén is biztosítható legyen az elvárt elérhetőség.

Minden egyes ilyen tervezési fázisban a tervezőnek tájékoztatni kell az ügyfelet és a beleegyezését kell kérnie.

A stadion hálózati tervének korlátai

Korlátozás	Összegyűjtött adatok	A tervező megjegyzései
Költségvetés	• A hozzáférési rétegben a redundancia megvalósítása nincs tervbe véve. Használni kell a meglévő 26 db 2960-48TT kapcsolót. • Új kábelszakasz létrehozásához nincs anyagi keret, kivéve az új vezetéknélküli hozzáférési pontok csatlakoztatását. szükséges optikai kábeleket.	Mivel a 2960-as kapcsolók csak 2. rétegbeli szolgáltatásokat támogatnak, így 3. rétegbeli huzalozási központok létrehozása nem lehetséges. A huzalozási központokhoz vezető két optikai kábelpár egy elosztási rétegbeli kapcsolópár csatlakoztatását teszi lehetővé.
Irányelvek	• A vezetőségi irányelvek szerint az alacsony költségű távoli kapcsolatok biztosítására interneten keresztüli, ISP által felügyelt VPN-eket kellett használni. (Felülvizsgálat alatt)	Mivel az üzleti alkalmazásokhoz szükséges QOS és SLA támogatás a helyi internetszolgáltatón keresztül nem lehetséges, így egy alternatív WAN technológiára van szükség.
Ütemterv	• Az alapvető változtatásokra kb. 4 hónap áll rendelkezésre, amíg a sportszezon el nem kezdődik.	Figyelembe kell venni az új áramkörök és berendezések telepítéséhez és beüzemeléséhez szükséges időt.
Személyzet	• További alkalmazottak felvétele nincs tervbe véve.	A jelenleg dolgozó egy rendszergazda, a három technikus, és az egy vezető nem elegendő a tervezett hálózati növekedés kezeléséhez. Az alkalmazottaknak azonnali oktatásra van szükségük vezetéknélküli hálózatok és IP-telefónia témakörben.

5.1.2 Bővíthetőségi követelmények

A stadion vezetősége a hálózat egyes részein jelentős növekedésre számít, ugyanakkor nem tartja valószínűnek a vezetékes kapcsolatok számának gyors növekedését. A vezetőség legalább két új távoli irodai telephely létrehozását tervezi. Ez a bővítés 50%-kal, mintegy 750 főre fogja növelni a felhasználók számát.

A stadion vezetőségétől kapott bővíthetőségi követelmények jelentősek:

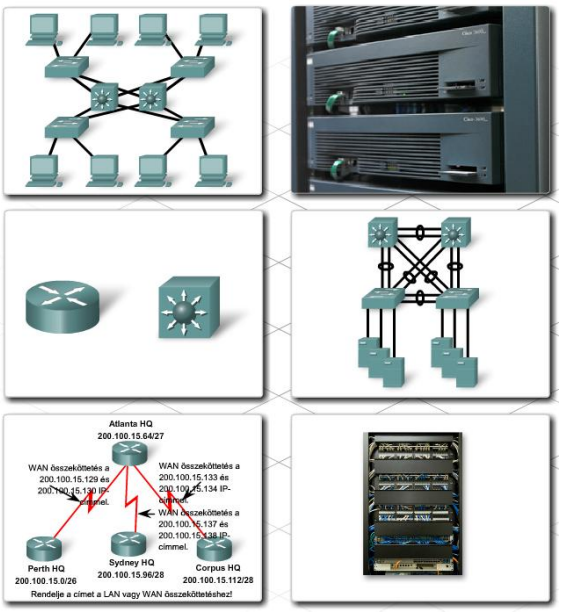
- 50%-os növekedés a felhasználók összlétszámában (LAN és WAN)
- 75%-os növekedés a vezetéknélküli felhasználók számában
- 75%-os növekedés a stadion e-kereskedelmi kiszolgálója által biztosított online tranzakciók számában
- 100%-os növekedés a távoli telephelyek számában
- IP-telefonok hozzáadása, a videó hálózat integrálása, 350 végponti eszköz telepítése

A hálózattervező szerint a stadion vezetősége jelentősen alábecsülte a vezetéknélküli igényeket azzal, hogy a jelenleg kapcsolódó 40 vezetéknélküli eszközhöz képest mindössze 75%-os növekedésre számítanak. Szerinte a szükséges területek lefedéséhez már a kezdeti tervekben lényegesen több eszközt kell szerepeltetni, ráadásul a fentieken túl erre még egy 20%-os növekedést is érdemes rászámítani. A tervező ebben a kérdésben azonnali megbeszélést kezdeményez a stadion vezetőségével.

5. A hálózati terv létrehozása

A gyors növekedés támogatása érdekében a tervező a hálózat hatékony és könnyű bővíthetőségét elősegítő stratégiát dolgoz ki. A stratégia javaslatai a következők:

- A hozzáférési réteg moduláris kialakítása amely szükség esetén az elosztási és a központi réteg tervének módosítása nélkül újabb modulok üzembehelyezésével bővíthető.
- Bővíthető, moduláris vagy fürtbe szervezett eszközök használata, melyek képességei könnyen bővíthetők.
- Az üzenetszórások korlátozása és a hálózat nem kívánatos forgalmának szűrése érdekében forgalomirányítók vagy többrétegű kapcsolók alkalmazása.
- Az eszközök között tartalék útvonalak létrehozása EtherChannel, vagy egyenlő költségű terheléselosztás alkalmazásával a sávszélesség növelése érdekében.
- Útvonal összevonást támogató, hierarchikus IP-címzés kialakítása.
- A huzalozási központokban lehetőség szerint lokális VLAN-ok használata.



Hozzon létre és teszteljen egy minta hozzáférési réteg modult, hogy lássa egy eszköz hálózathoz adásának hatásait! Használja ezt a letesztelt tervet mintaként, a hálózat könnyebb méretezhetősége érdekében.	Új szolgáltatások és eszközök támogatása érdekében a meglévő hálózathoz az alapvető eszközök bővítése nélkül adhatók modulok. Néhány eszközt fürtbe szervezve és egy eszközként kezelve egyszerűsödik a hálózat felügyelete és konfigurációja.	A forgalom szűréséhez és a hálózat központi rétegébe tartó forgalom csökkentése érdekében az elosztási rétegben használjon 3. rétegbeli eszközöket! Moduláris elosztási réteg terv esetén egy új hozzáférési rétegbeli modul alapvető konfigurációs változtatások nélkül csatlakoztatható.

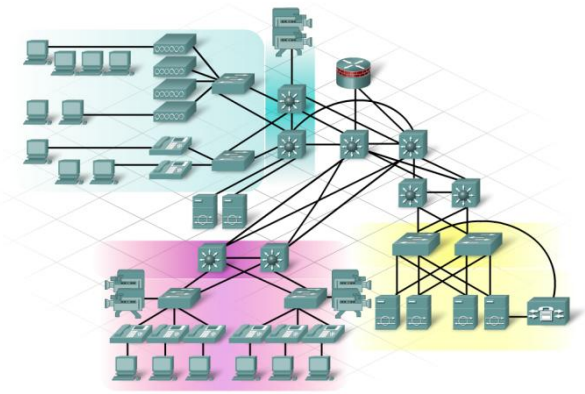
Több Ethernet kapcsolat összefogása egyetlen terheléselosztást végző EtherChannel-be növeli a rendelkezésre álló sávszélességet. Az EtherChannel-ek létrehozását akkor használják, ha anyagi okokból nincs mód nagysebességű interfészek és optikai kábelek beszerzésére.	Gondos IP-címzési terv esetén további felhasználók és szolgáltatások hálózathoz adásakor nincs szükség újracímzésre. Az útvonalösszegzés csökkenti az irányítótáblák méretét, és így javítja a hálózat konvergencia idejét.	A huzalozási központokban lokális VLAN-ok használata minimalizálja a szükséges feszítőfa konfigurációkat. Ez a terv elősegíti a gyorsabb hálózati konvergenciát, és növeli a skálázhatóságot és a stabilitást.

5.1.3 A rendelkezésre állásra vonatkozó követelmények

A stadion hálózatában a tervezett e-kereskedelmi és biztonsági rendszerek, valamint az IP-telefonrendszer az alap hálózat napi 24 órás és heti 7 napos rendelkezésre állását igényli.

A befejezetlen web alapú tranzakciók anyagi károkat okozhatnak a stadionnak. A biztonsági megfigyelő rendszer hibája a stadion ügyfeleinek biztonságát, a telefonrendszer zavarai pedig az alapvető kommunikációt veszélyeztetik.

A hálózattervezőnek az elérhetőség biztosítására olyan nem túl költséges megoldást kell alkalmaznia, amely maximális hibavédelmet nyújt. A hálózati alkalmazások által megkívánt közel 100%-os rendelkezésre állási igény teljesítéséhez az új hálózatnak nagyfokú redundanciával kell rendelkeznie.

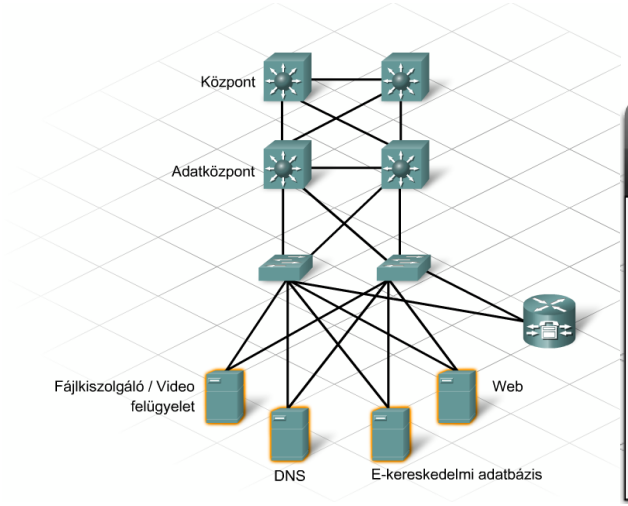


Az e-kereskedelem elérhetősége

Egy megbízhatatlan webhely rövid időn belül problémákat okozhat, sőt az ügyfeleket is elriaszthatja a tranzakciók végrehajtásától. A e-kereskedelem megbízhatóságának eléréséhez a következő bevált módszerek alkalmazása ajánlott:

- Csatlakoztassuk a kiszolgálókat két külön hozzáférési rétegbeli kapcsolóhoz!
- Biztosítsunk tartalék összeköttetéseket az elosztási rétegben!
- Helyezzünk ki másodlagos DNS-kiszolgálókat az internetszolgáltatóhoz!
- A kritikus útvonalak esetében, helyben vagy interneten keresztül végzett megfigyeléssel fokozottabban kövessük nyomon az eszközök állapotát!

- A kulcsfontosságú berendezésekben alkalmazzunk tartalék modulokat és tartalék tápegységeket, ha erre lehetőség van!
- Használjunk szünetmentes tápegységet és tartalék áramgenerátort!
- Válasszunk gyors konvergenciát és megbízható működést biztosító forgalomirányító protokoll stratégiát!
- Vizsgáljuk meg egy második internetszolgáltató (ISP) vagy az adott internetszolgáltatóval létesített tartalék összeköttetés biztosításának lehetőségeit!



A kiszolgálók rendelkezésre állási stratégiái:

- Több hálózati interfész kártya
- Tartalék szünetmentes tápegység
- RAID lemezvezérlők
- Több tápegység
- Megfigyelés felügyeleti programcsomaggal, és hibák esetén riasztások.

A biztonsági megfigyelő rendszer

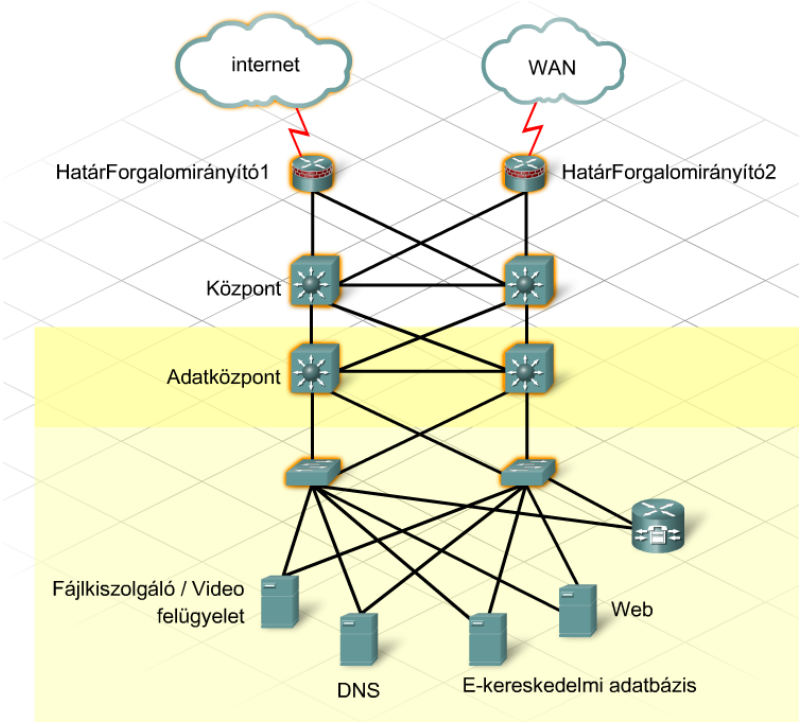
A videó fájlokat és a biztonsági megfigyelő programokat kezelő kiszolgálókkal szemben az e-kereskedelmi szerverekkel megegyező elvárásokat kell támasztani. A kamerákkal és a biztonsági eszközökkel kapcsolatban további intézkedések szükségesek, melyek a következők:

- A kritikus területeken külön kapcsolókhoz csatlakoztatott tartalék kamerák használata a hibák következményeinek csökkentése érdekében.
- A kamerák számára az Ethernet kapcsolatukon keresztüli áramellátás biztosítása szünetmentes tápegységgel és/vagy tartalék generátorral.

Az IP-telefonrendszer

Bár az új IP-telefonrendszer telepítése nem ennek a hálózati tervnek a feladata, a tervezőnek mégis figyelembe kell vennie a rendelkezésre állással kapcsolatos követelményeit. A hozzáférési rétegbeli kapcsolókon a redundancia és a nagyfokú rendelkezésre állás biztosítása érdekében a következőket kell elvégezni:

- A hozzáférési és az elosztási réteg között lehetőség szerint hozzunk létre 3. rétegbeli összeköttetést.
- Biztosítsunk tartalék áramellátást és szünetmentes tápegységet.
- Alakítsunk ki tartalék útvonalakat a hozzáférési réteg és a központi réteg között.
- Csökkentsük a hibatartományok méretét.
- Lehetőség szerint válasszunk redundáns összetevőket támogató eszközöket.
- Használjunk olyan gyorsan konvergáló irányító protokollt, mint például az EIGRP.



Az internet/vállalati határpont rendelkezésre állási stratégiái:

- Kapcsolat két internetszolgáltatóval, vagy kettős kapcsolat egy szolgáltatóval.
- Kihelyezett kiszolgálók
- Másodlagos DNS kiszolgálók

A forgalomirányítók rendelkezésre állási stratégiái:

- Tartalék tápegységek, szünetmentes tápegység és áramgenerátor
- Tartalék eszközök
- Redundáns összeköttetések
- Sávon-kívüli felügyelet
- Gyors konvergenciát biztosító protokollok

A 3. rétegbeli kapcsolók rendelkezésre állási stratégiái:

- Tartalék tápegységek, modulok és eszközök
- Szünetmentes tápegység és áramgenerátor
- Üzem közben cserélhető kártyák és vezérlők
- Redundáns összeköttetések
- Sávon-kívüli felügyelet
- Gyors konvergenciát biztosító protokollok

A 2. rétegbeli kapcsolók rendelkezésre állási stratégiái:

- Tartalék tápegységek, modulok és eszközök
- Üzem közben cserélhető kártyák és vezérlők
- Redundáns összeköttetések
- Szünetmentes tápegység és áramgenerátor

További információ

Számos hivatalos kiadvány és megoldási útmutató található a Cisco.com oldalon (http://www.cisco.com/en/US/netsol/index.html), amelyek referenciaként használhatók egy IP-telefon rendszer megvalósítási terve során.

5.1.4 A hálózat teljesítményére vonatkozó követelmények

A konvergált hálózatok, mint amilyen a stadion tervezett hálózata is, adat-, hang- és videó forgalom átvitelére képesek. Minden forgalomtípusnak megvannak a saját egyedi követelményei.

Egy konvergált hálózat alkalmazásainak legfőbb tulajdonságai:

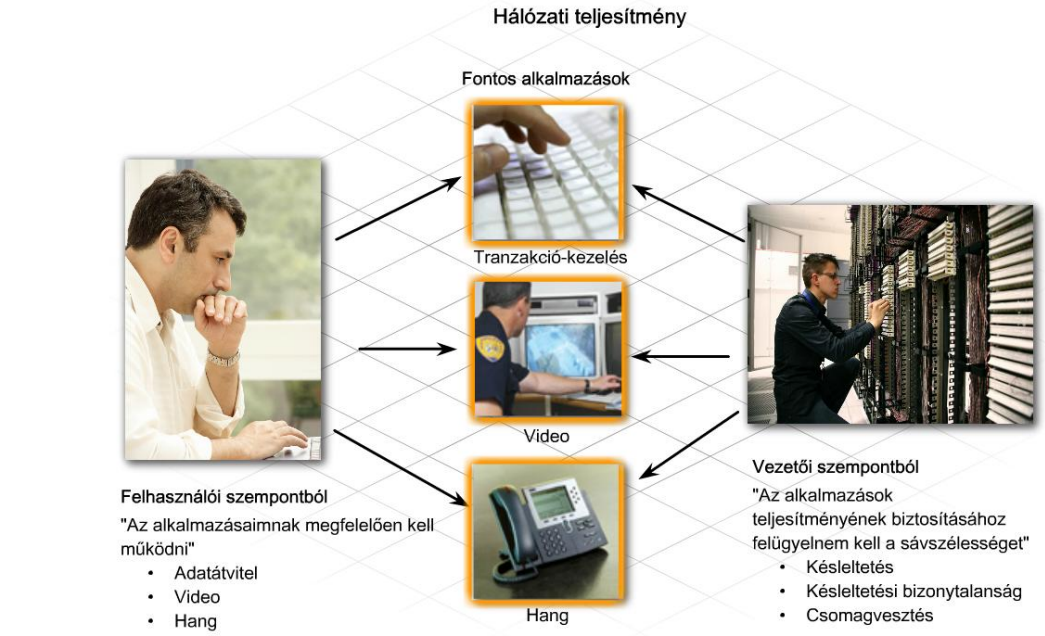
- Különféle méretű csomagok
- Különféle protokollok
- Eltérő érzékenység a késleltetésre és a időzítési bizonytalanságra

Bizonyos esetekben az alkalmazások egymásnak ellentmondó követelményei teljesítményproblémákhoz vezethetnek, és ilyenkor az érintett felhasználók alkalmazásaik lassúságára panaszkodhatnak.

Képzett és tapasztalt IT szakembereknek is sokszor nehézséget okoz a megfelelő alkalmazásteljesítmény fenntartása. Az új alkalmazások és szolgáltatások bevezetése a meglévők megzavarása nélkül nem könnyű feladat.

A stadion új hálózatában három alkalmazásnak sajátosak a követelményei:

- Tranzakció-kezelés
- Videó elosztás és felügyelet
- IP-telefon hangminőség biztosítás



Tranzakció-kezelés	Video elosztás és felügyelet	IP-telefon hangminősége
A stadion vezetőségének célja az adatbázis kiszolgálókat használó alkalmazások válaszidejének 3 másodperc alá szorítása.	A stadion vezetőségének jövőbeni terve kiváló minőségű élő videoszolgáltatás biztosítása a stadionban. A vezetőség szeretne jó minőségű megfigyelő kamerákat is.	A felhasználók hangminőséggel szemben támasztott elvárásai nagyok. Azt gondolják, hogy a jelenlegi digitális telefonjuk és az új IP-telefon hangminősége között nem lesz különbség.

A tervező listát készít azokról a célokról és megfontolásokról, amelyek befolyásolhatják ezeknek a magas prioritású alkalmazásoknak a teljesítményét.

Cél: a tranzakciók végrehajtási idejének 3 másodperc alá szorítása.

- Törekedni kell a hálózati átmérő (a hálózat kiterjedtsége) csökkentésére.
- Korlátozni kell a nem kívánatos forgalmat és üzenetszórást.
- A kulcsfontosságú kiszolgálókhoz nagy sávszélességű útvonalakat kell biztosítani.
- További nagysebességű tárolókat vagy tartalom kiszolgálókat kell alkalmazni.

Cél: Jó minőségű hang- és videó folyam biztosítása

- VLAN-okat és forgalomosztályozási stratégiákat kell alkalmazni.
- A kiszolgálók és a végpontok között a lehető legrövidebb útvonalakat kell biztosítani.
- Csökkenteni kell a forgalomszűrés és a forgalomelemzés gyakoriságát.
- A WAN összeköttetések sávszélességét növelni, a minőségét javítani kell.
- QoS stratégiát és forgalmi prioritásokat kell alkalmazni.
- Meg kell határozni az üvegnyak-effektusra érzékeny területeket és ott QoS stratégiát kell alkalmazni.

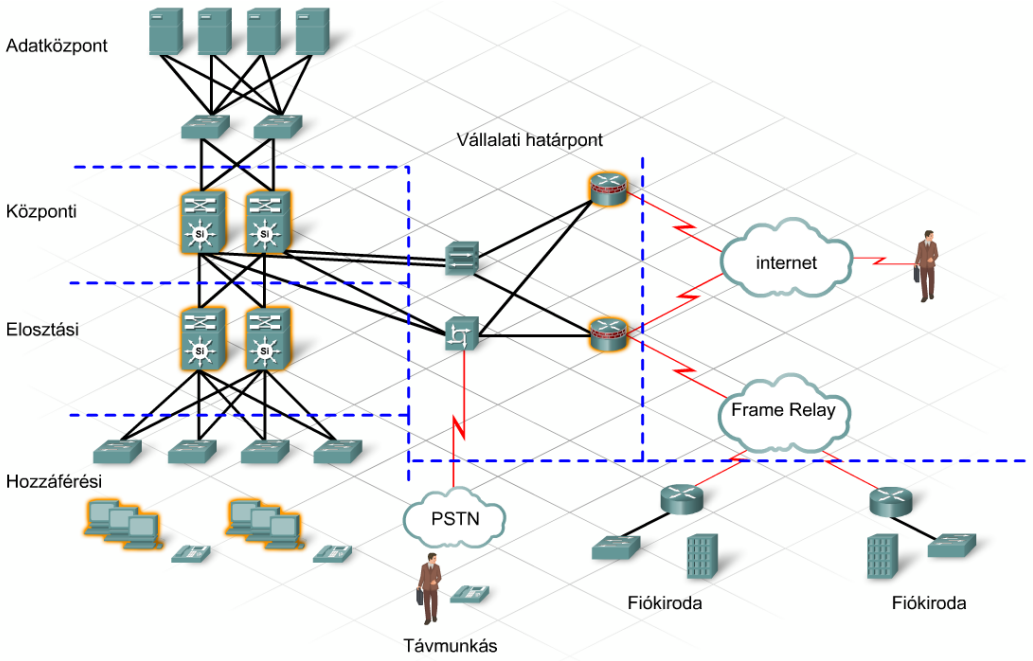
5.1.5 Biztonsági követelmények

A biztonság a hálózati terv egyik olyan területe, ahol nem lehet kompromisszumokat kötni. Az előfordulhat, hogy egy biztonságos hálózat létrehozásakor szükségessé válhat alacsonyabb költségű vagy kevésbé racionális megoldások alkalmazása, de a hálózati szolgáltatások fejlesztése soha nem mehet a biztonság rovására.

A hálózati kockázatfelmérés megmutatja a hálózat leginkább sebezhető pontjait. Nagyon bizalmas és kényes információkat tartalmazó hálózat gyakran igényel egyedi biztonsági megfontolásokat. A szervezetek a kockázatfelmérést az általános üzletfolytonossági és katasztrófavédelmi terv részeként végzik.

A legtöbb hálózat esetében a biztonság kialakításához a következő általános lépések javasolhatók:

- Tűzfalak alkalmazásával különítsük el a biztonságos központi hálózat egyes szintjeit minden egyéb nem biztonságos hálózattól, például az internettől. A forgalom megfigyelésére és ellenőrzésére konfiguráljunk tűzfalakat a leírt biztonsági irányelveknek megfelelően.
- A biztonságos kommunikáció eléréséhez VPN-ek alkalmazásával titkosítsuk az információt, mielőtt harmadik félnek továbbítanánk, vagy nem biztonságos hálózatot használnánk.
- behatolás-védelmi rendszerek (Intrusion prevention system) alkalmazásával kerüljük el a hálózati betöréseket és támadásokat. Ezek a rendszerek az ártalmas vagy rosszindulatú eseményeket figyelik a hálózatban, és szükség esetén riasztják a hálózat kezelőit.
- Védelmi rendszer telepítésével óvjuk meg a felhasználókat és az adatokat az internetes fenyegetésekkel (vírusok, kémprogramok, levélszemét) szemben.
- Kezeljük a végpontok biztonságát, hogy megvédjük a hálózatot az egyes felhasználói azonosítások ellenőrzése előtt, mielőtt megkapják a hozzáférést a hálózathoz.
- Bizonyosodjunk meg arról, hogy a fizikai biztonsági intézkedések rendben vannak és megelőzhetőek az azonosítatlan hozzáférések a hálózati eszközökhöz és helyiségekhez!
- Védjük a vezetéknélküli hozzáférési pontokat és helyezzünk el vezetéknélküli kezelési megoldásokat a hálózaton!



5.1.6 A hálózati terv kompromisszumai

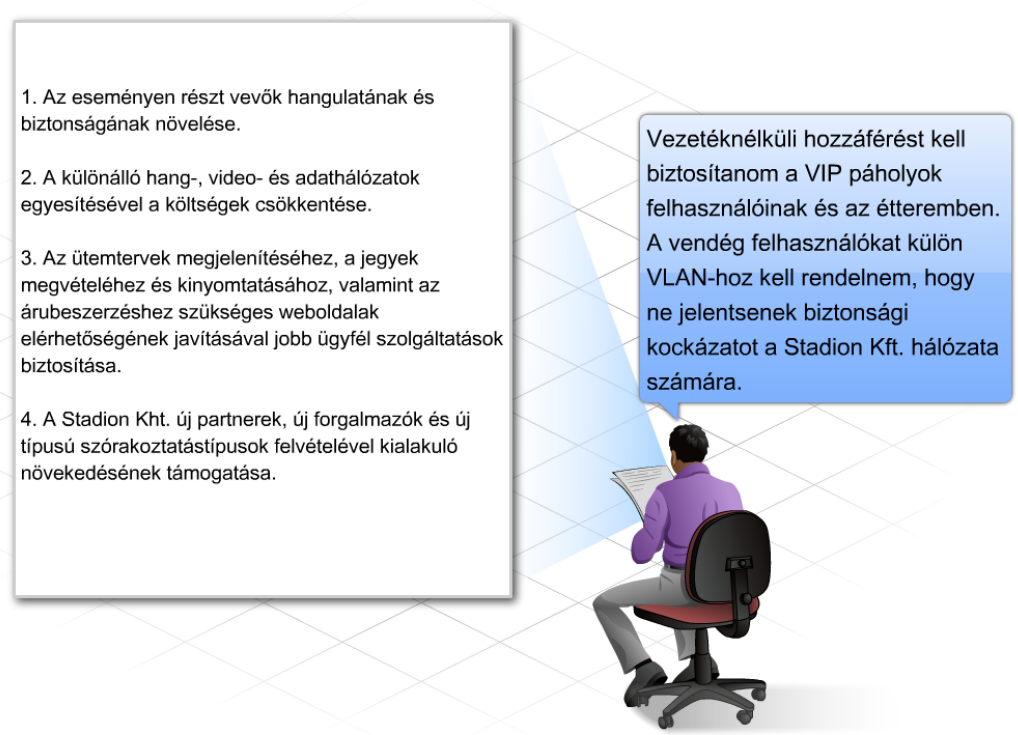
Miután a hálózattervező felsorolja a stadion korszerűsítési tervének minden szükséges elemét, néhány nehéz döntést kell meghoznia. Sajnos kevés hálózat tervezhető meg az alábbiak figyelembevétele nélkül:

- A hálózat megvalósításának költsége
- A megvalósítás nehézségei
- A jövőbeni fenntartásra vonatkozó elvárások

A Hálózat Kft. a hálózat korszerűsítésére vonatkozóan néhány megszorítást tett, emiatt a tervezőnek mérlegelnie kell a különböző megoldási lehetőségeket. Előfordulhat, hogy a megszorítások bizonyos területeken kompromisszumokhoz vezetnek.

A Stadion Kht. elsődleges üzleti célja a stadion eseményein résztvevő több ezer ember biztonságának növelése, és minél kellemesebb légkör kialakítása számukra. Az ezeket a célokat közvetlenül érintő hálózati fejlesztéseket kell a tervezőnek elsősorban szem előtt tartania, amikor tervezési kompromisszumokra kényszerül.

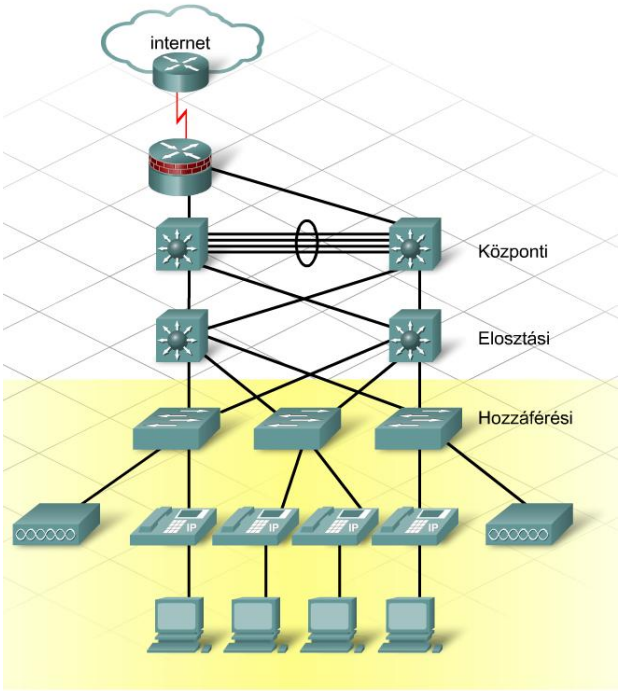
Az üzleti célok megvalósítása olyan döntéseket eredményezhet, melyek lehetetlenné tesznek vagy megnehezítenek más szükséges fejlesztéseket. Például a VIP páholyokban és az étteremben telepített vezetéknélküli internet hozzáférés növeli a látogatók elégedettségét, azonban ha a vendég hozzáférés nincs a központi hálózattól elkülönítve, veszélyeztetheti a kiszolgálók biztonságát.



5.2 A megfelelő LAN topológia kiválasztása

5.2.1 A hozzáférési réteg topológiájának megtervezése

A tervező készen áll a stadion LAN korszerűsítési tervének elkészítésére. A meglévő lokális hálózat topológiája egyszintű, nem tartalmaz tartalék összeköttetéseket, és csak minimális védelmet biztosít. Mindez nem teljesíti a stadion vezetőségének igényeit.



A hozzáférési rétegre vonatkozó követelmények

A tervező a következő listát állítja össze az új hálózat hozzáférési rétegének követelményeiről:

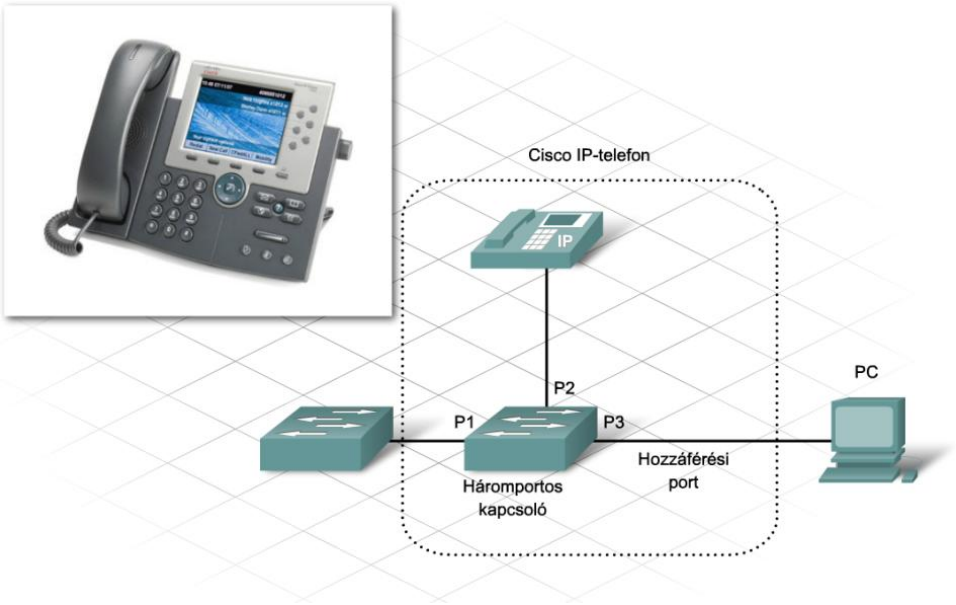
- A meglévő hálózati eszközök kapcsolatainak biztosítása, a hálózat bővítése vezetéknélküli hozzáféréssel és IP-telefonokkal.
- VLAN-ok létrehozása a hang, a biztonsági megfigyelő rendszer, a vezetéknélküli hozzáférés és a hagyományos adatok elkülönítésére.
- VLAN-ok működésének korlátozása a huzalozási központokra. Kivételt képez a jövőbeni barangolási igényeket támogató vezetéknélküli VLAN.
- Az elosztási réteg hálózatához vezető tartalék összeköttetések biztosítása.

- Lehetőség szerint mind a 16 meglévő 2960-as kapcsoló alkalmazása.
- Ethernet feletti áramellátás (PoE) biztosítása az IP-telefonok és a vezetéknélküli hozzáférési pontok számára.
- QoS osztályozási és jelölési lehetőségek biztosítása.

A felhasználók számának növekedése nem mindig teszi szükségessé az eszközök és portok azonos mértékű növelését. Az IP-telefonok és más eszközök például beépített kapcsolóval rendelkeznek, ami lehetővé teszi egy számítógép közvetlen csatlakoztatását. Ez a kapcsoló csökkenti a huzalozási központban a további eszközök csatlakoztatásához szükséges portok számát. Feltéve, hogy az IP-telefonok több mint 50%-ához csatlakozik egy számítógép, további adatkapcsolat létrehozása nem feltétlenül igényel új kapcsolót a huzalozási központban.

Az IP-telefonok három porttal rendelkeznek:

- Az 1. port egy külső port a kapcsoló vagy más VoIP eszköz csatlakoztatásához.
- A 2. port egy belső 10/100-as interfész az IP-telefon forgalmának továbbításához.
- A 3. port egy külső hozzáférési port egy számítógép vagy más eszköz csatlakoztatásához.



A 16 meglévő 2960-as kapcsoló a hozzáférési rétegben a végpontok közötti kapcsolatokat biztosítja. A tervező feladata, hogy a 2960-as kapcsolók alkalmazhatók legyenek az új hálózatban.

A 2960-as kapcsoló jellemzői

A 2960-as kapcsoló fix konfigurációjú 10/100-as Ethernet kapcsoló két 10/100/1000-es felmenő (uplink) porttal. Ezek a kapcsolók teljesítik az hozzáférési réteg hálózatának legtöbb követelményét, melyek a következőek:

- **Bővíthetőség** – Mivel a 2960-as kapcsolók támogatják a Cisco kapcsoló fürttechnológiát (Cisco switch clustering), így további végpontkapcsolatok létrehozásakor könnyen bővíthető a hálózat új kapcsolókkal.

- **Rendelkezésre állás** – A 2960-as kapcsolók tartalék tápegységekről is működtethetőek. Fürtbe rendezett kapcsolók esetén redundáns kapcsolófelügyelet valósítható meg. Az irányító funkcióra két kapcsoló is konfigurálható, így az egyik kiesése esetén a fürt többi része még működőképes marad. QoS osztályozási és jelölési lehetőségek is elérhetőek ebben a modellben.
- **Biztonság** – Portbiztonság és más kapcsoló alapú biztonsági lehetőségek alkalmazhatók.
- **Felügyelhetőség** – A kapcsolók támogatják az egyszerű hálózatfelügyelő protokollt (SNMP) A felügyelet sávon belül és sávon kívül is megvalósítható. A 2960-as kapcsolók tartalmazzák a szabványos Cisco IOS parancskészletet, valamint támogatják a Cisco Network Assistant grafikus felületű konfigurációs és felügyeleti eszközöket.

A meglévő eszközök korlátai

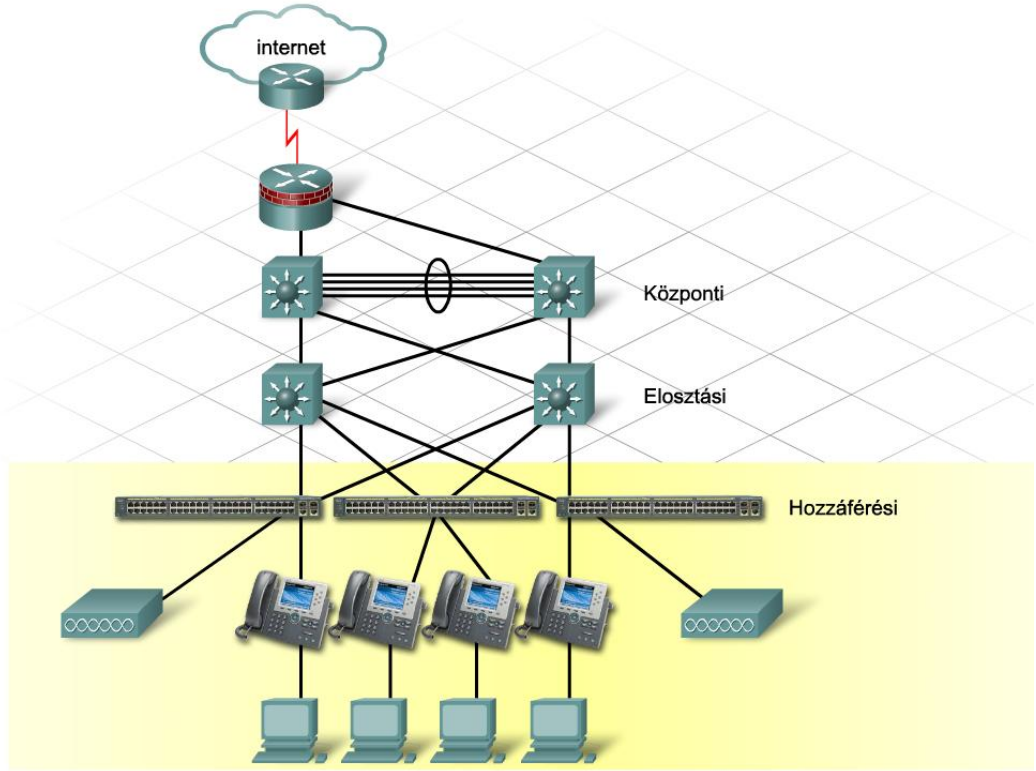
A 2960-as kapcsolók használata korlátokat is eredményez az új hálózati tervben. A stadion hálózatának jelenlegi 2960-as kapcsolói ugyanis optikai összeköttetéseket csak kiegészítő átalakítókkal képesek kezelni. Mivel minden huzalozási központhoz csak két optikai kapcsolat vezet, több kapcsoló fürtbe rendezésével kell a felmenő (uplink) kapcsolatokat megosztani. A 2960-as kapcsoló 2. rétegbeli eszköz, így a hozzáférési rétegben csak 2. rétegbeli funkciók valósíthatók meg.

Áramellátási követelmények

Bár a 2960-as kapcsolók nem képesek Ethernet feletti áramellátásra (PoE), a hang VLAN-ok létrehozását támogatják. Amíg a kapcsolókat le nem cserélik, az IP-telefonokhoz tápellátás biztosítására is képes kábelrendezőkre van szükség.

A szünetmentes tápegységek tartalék tápellátást biztosítanak a kapcsolóknak és az IP telefonok tápellátását is ellátó kábelrendezőknek. A tervező egy generátor beszerzését javasolja a hozzáférési réteg kritikus területeinek ellátásához.

A tervező nem határozza meg a vezetéknélküli hálózat hozzáférési rétegbeli megvalósításának módját. Vannak egyéb tényezők, mint például a vezetéknélküli barangolás (roaming) lehetősége, amelyek befolyásolják a vezetéknélküli hálózat tervét. A tervező tisztában van vele, hogy a vezetéknélküli terv még nem teljes.



5.2.2 Az elosztási rétegbeli topológia megtervezése

A stadion hálózatának elosztási rétege felel a VLAN-ok közötti forgalomirányításért és a nem kívánatos forgalom szűréséért.

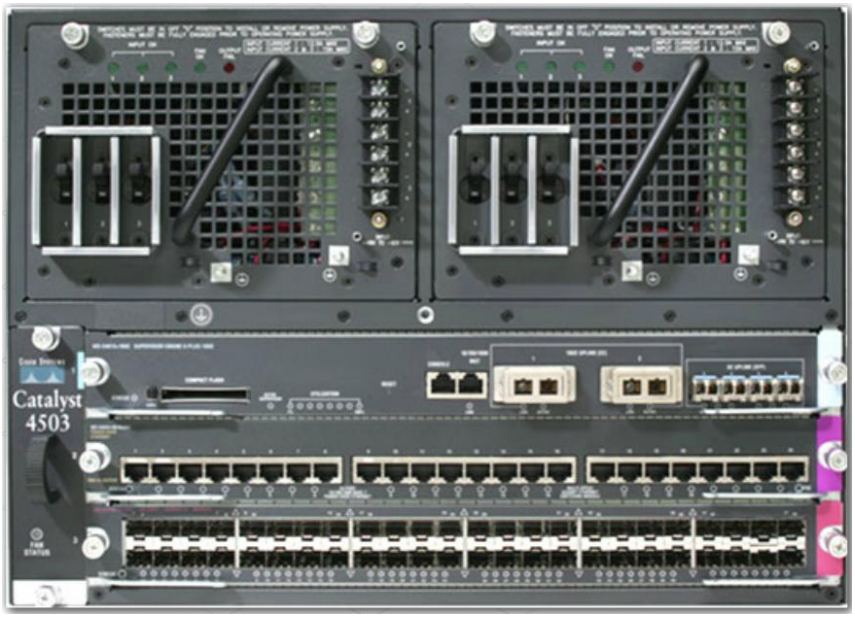
Az elosztási rétegre vonatkozó követelmények

A hálózattervező a következő listát készíti az új hálózat elosztási rétegének követelményeiről:

- A hibák következményeinek csökkentése érdekében tartalék összetevők és összeköttetések biztosítása.
- Nagyszámú kapcsolatot kezelő forgalomirányítás támogatása. A stadion mind a 16 huzalozási központjának legalább két összeköttetéssel kell rendelkeznie az elosztási réteg kapcsolóihoz.
- Forgalomszűrési lehetőség biztosítása.
- QoS megvalósítása.
- Nagy sávszélességű kapcsolatok létrehozása.
- Gyorsan konvergáló irányító protokoll alkalmazása.
- A forgalom összefogása és útvonal-összevonás.

A többrétegű kapcsolók alkalmasak ezeknek a követelményeknek a teljesítésére. Nagyszámú portot biztosítanak, és támogatják a szükséges forgalomirányítási jellemzőket. Az elosztási réteg

terve tartalmazza a helyi hálózat felhasználóihoz és a kiszolgálófarmhoz tartozó kapcsolatokat, valamint a vállalat határán megvalósuló forgalomelosztást. A követelmények teljesítéséhez hat darab többrétegű kapcsoló beszerzése szükséges.



A terv korlátai

A huzalozási központokhoz vezető optikai kapcsolatok korlátozott száma az egyetlen elosztási rétegbeli megszorítás. A huzalozási központok két optikai összeköttetéssel rendelkeznek, és ez korlátozza azoknak a kapcsolóknak a számát, amelyek tartalék útvonalakat képezve kapcsolódhatnak az elosztási réteg eszközeihez. Mivel minden optikai kapcsolat vége a központi helyszínen van, az elosztási réteg eszközeit az új adatközpontba kell telepíteni.

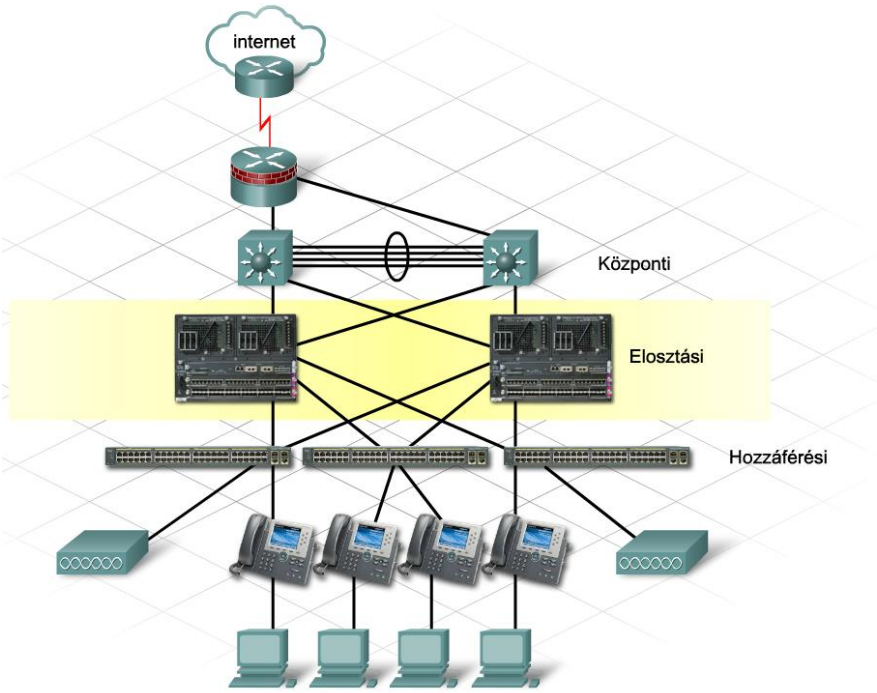
A többrétegű kapcsolók képességei

Az elosztási rétegben többrétegű kapcsolók alkalmazásával teljesíthetők a stadion terv alább felsorolt műszaki követelményei:

- **Bővíthetőség** – A moduláris többrétegű kapcsolók lehetővé teszik további optikai és réz alapú portok használatát is. Az elosztási rétegben történő forgalomirányítással sok esetben elkerülhetők a 2. rétegbeli feszítőfa protokoll (STP) újrakonfigurálásánál jelentkező problémák. Új kapcsoló blokkok telepíthetők anélkül, hogy az hatással lenne a meglévő topológiára.
- **Rendelkezésre állás** – A középkategóriás, többrétegű kapcsolók támogatják a tartalék tápegységeket és ventilátorokat, de ami még fontosabb, a redundáns felügyeleti modulokat és a gyors helyreállítási technológiát is. Egy felügyeleti modul kiesésekor a másodlagos modul érzékelhető kapcsolatvesztés nélkül veszi át a kiesett szerepét. A 3. rétegű kapcsolt hálózati terv az irányított forgalom hatékony terheléselosztásával a hálózati összeköttetések lehető legjobb kihasználását teszi lehetővé. A forgalomirányító protokollok beállíthatók úgy, hogy az STP-vel megegyező sebességgel vagy még gyorsabban konvergáljanak. Az útvonal-összevonás elvégezhető az elosztási rétegben, ami

csökkenti egy hozzáférési rétegbeli eszköz vagy összeköttetés hibájának a központi rétegre gyakorolt hatását.

- **Biztonság** – A többrétegű kapcsolókon hozzáférési listákkal megvalósított szűrés, portbiztonság és tűzfalszolgáltatások is alkalmazhatók. Ezekkel a biztonsági funkciókkal megakadályozható a jogosulatlan, illetve a nem kívánatos hálózati forgalom.
- **Felügyelhetőség** – A kapcsolók támogatják az SNMP-t, és felügyelhetők sávon belül és kívül is.



5.2.3 A központi réteg topológiájának megtervezése

A stadion LAN központi rétegének nagysebességű kapcsolatokat és nagymértékű rendelkezésre állást kell biztosítania. A stadion helyi és távoli hálózatának kapcsolatai is a központi réteg kapcsolóitól függnek.

A központi rétegre vonatkozó követelmények

A központi réteg hálózatának tervezési követelményei:

- Nagysebességű kapcsolatok az elosztási réteg kapcsolóihoz
- 24 * 7-es rendelkezésre állás
- Forgalomirányítóval megvalósított kapcsolatok a központi réteg eszközei között
- Nagysebességű, redundáns összeköttetések a központi kapcsolók, valamint a központi és elosztási réteg eszközei között.

A központi rétegben nagysebességű, többrétegű kapcsolásra van szükség. Az új tervben a stadion hálózatának központi rétege két nagyteljesítményű, többrétegű kapcsolóval megvalósítható.

A központi réteg feladata a nagysebességű kapcsolás, így itt nem történik csomagszűrés, vagy csak kis mértékben.

Kisvállalati környezetben az elosztási és központi réteg gyakran közös, emiatt a zsugorított központi réteg vagy zsugorított gerinchálózat elnevezést szokták használni.

Magas szintű rendelkezésre állás

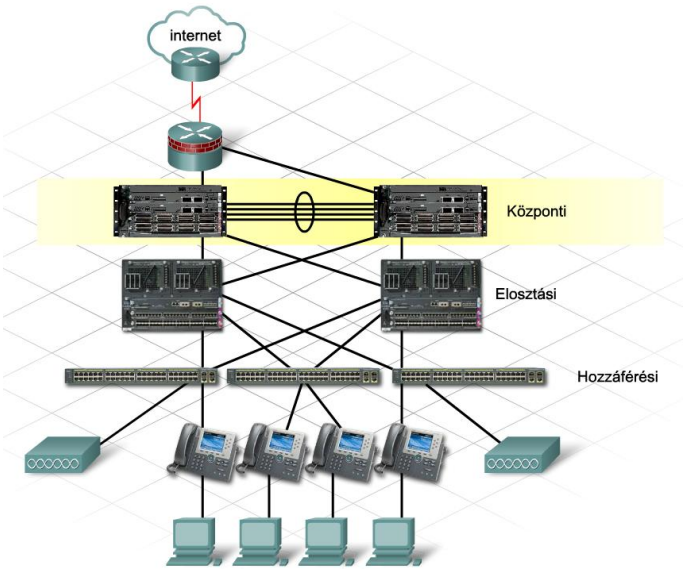
A hálózat központi rétege esetében a legfontosabb a magas szintű rendelkezésre állás. A tervezőnek át kell gondolnia azokat az intézkedéseket, amelyekkel növelhető a hálózat megbízhatósága és üzemideje.

A központi és az elosztási réteg között tartalék összeköttetésekre van szükség. A központi réteg tartalék elemeinek telepítését, valamint a tartalék rendszerek (légkondicionálás, áramellátás és egyéb szolgáltatások) lehetőség szerint mindenhol biztosítani kell.

Az olyan 3. rétegbeli irányító protokollok, mint pl. az EIGRP vagy az OSPF alkalmazása a központi rétegben csökkenti az összeköttetési hibák helyreállítási idejét. A központi réteg kapcsolói közötti irányított összeköttetéseken lehetőség van egyenlő költségű terheléselosztásra és a gyors helyreállításra.

Sebesség

A központi réteg másik fontos tulajdonsága a sebesség. A stadion hálózatának szinte a teljes forgalma áthalad a központi réteg eszközein. Nagysebességű interfészekkel, optikai kapcsolatokkal és megfelelő technológiákkal (pl. EtherChannel), elegendő sávszélesség biztosítható a jelenlegi forgalomszint és a jövőbeni növekedés támogatásához.



5.2.4 A helyi hálózat logikai tervének elkészítése

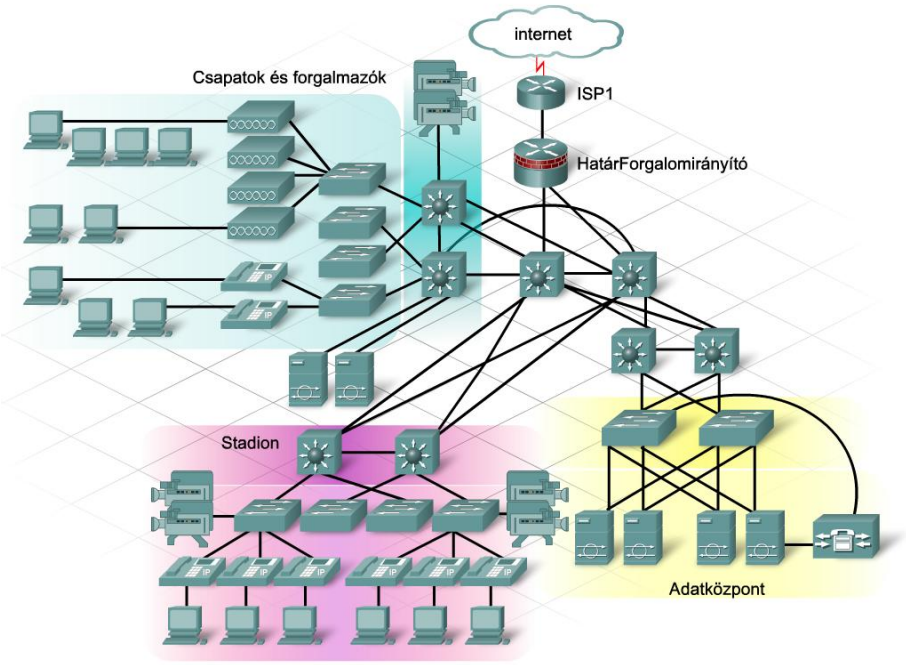
Logikai LAN diagram létrehozása

A helyi hálózat előzetes hálózati tervének utolsó lépése az új stadion hálózat logikai diagramjának létrehozása, mely a különböző rétegek és eszközök kapcsolatait ábrázolja.

A stadion új helyi hálózatában mind a 16 huzalozási központban található legalább egy 2960-as kapcsoló. Mivel a stadion hálózata három különálló egységből áll, így hat elosztási rétegben működő többrétegű kapcsoló végzi az útvonal-összevonást és a forgalomirányítást a hozzáférési és a központi réteg között.

A központi réteg két csúcsteljesítményű, többrétegű, redundáns kapcsolóból áll. Ezek az elosztási réteghez és egymáshoz gigabites összeköttetésen keresztül csatlakoznak.

A hálózattervező a hálózati diagramon tünteti fel a kiszolgálók és az IP-szolgáltatások helyét. A vezetékes helyi hálózat tervét követően készül el a hálózat azon részének terve, amelyik támogatja a stadionhoz vezető távoli összeköttetéseket.



5.3 A WAN és a távolról dolgozók támogatásának megtervezése

5.3.1 A távoli telephelyekkel való kapcsolat meghatározása

A stadion hálózata a vállalati határon, egy helyi internetszolgáltató DSL kapcsolatán keresztül csatlakozik az internethez. Az internetszolgáltató által felügyelt forgalomirányítók a stadionban találhatók, és a Stadion Kht. határ-forgalomirányítójához csatlakoznak.

A szolgáltatások kiterjesztése a távoli helyszínekre

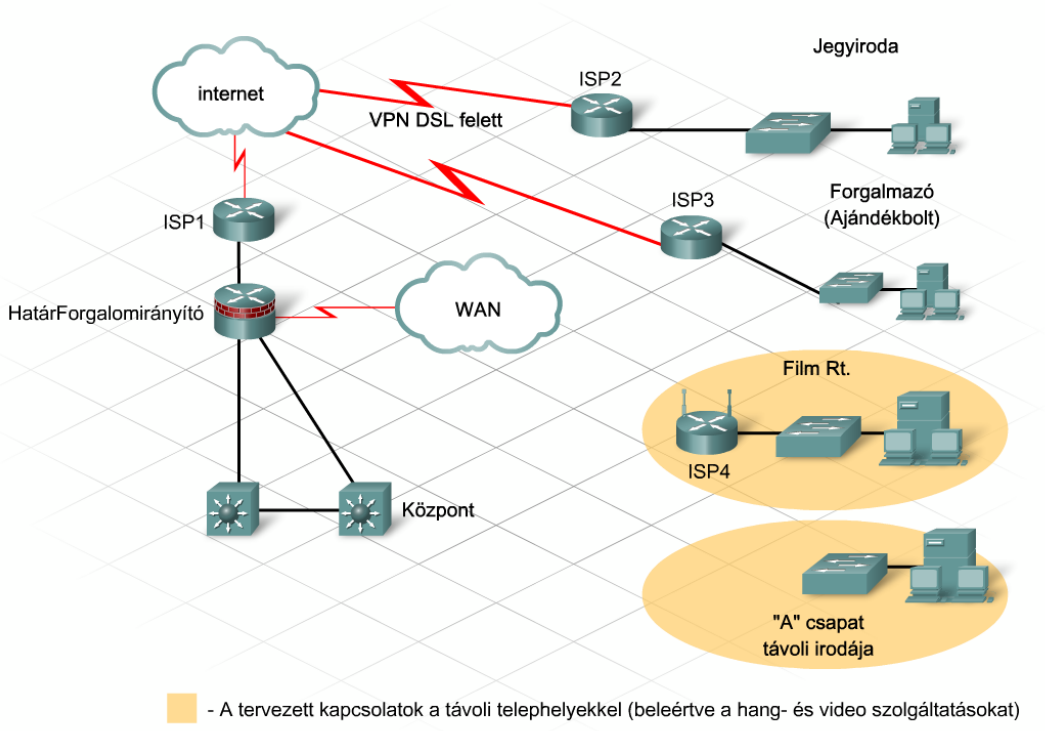
A két meglévő távoli helyszín, a belvárosban lévő jegyiroda és a helyi bevásárlóközpontban található ajándék üzlet, ugyanazzal az internetszolgáltatóval áll kapcsolatban, mint a központi

stadion. Az internetszolgáltató felügyelt VPN szolgáltatást is biztosít számukra. A távoli helyszínek ezeken az összeköttetéseken keresztül férnek hozzá a stadion irodáiban lévő kiszolgálók adatbázisaihoz.

A stadion új hálózatának egyik legfontosabb célja a hang és videó hálózat kiterjesztése a távoli helyszínekre. Két további távoli kapcsolat létrehozását tervezik:

- Az Stadion Kht. az események alatti és utáni videó felvételek elkészítésére egy filmes céggel áll szerződésben.
- Ennek a cégnek fájlokat kell le-és feltöltenie, ezért biztosítani kell számukra a hozzáférést a stadion hálózatához. A stadionban jelenleg helyet bérlő sportcsapat egy távoli irodával bővül. A csapat szeretne ott is ugyanazokhoz a hálózati erőforrásokhoz hozzáférni, mint a stadion hálózatában.

Az internetszolgáltató nem támogatja a QoS-t, és szolgáltatói szerződés (SLA) formájában sem nyújt a szolgáltatására garanciát. A tervező a stadionban egy különálló WAN-kapcsolat telepítését javasolja a vállalati alkalmazásokhoz szükséges QoS biztosításához.



Az új WAN-kapcsolat telepítése

Az új célok eléréséhez dedikált WAN-kapcsolatokra van szükség. A költségekre és a WAN szolgáltatások elérhetőségére vonatkozó ajánlatkérést (RFQ) kiküldték a területi telekommunikációs szolgáltatónak (TSP).

Mivel a stadion a városhatáron kívül fekszik, így mindösszesen két WAN-kapcsolattípus választható: pont-pont alapú T1 vagy Frame Relay. Ezek a szolgáltatások egy helyi telekommunikációs szolgáltatón keresztül mind a stadionban, mind a távoli helyszíneken hozzáférhetők.

Bár a pont-pont alapú T1 összeköttetés biztosítja a legszigorúbb ellenőrzést a WAN összeköttetések QoS szolgáltatásai felett, a Frame Relay lényegesen olcsóbb. A hálózattervező a stadion számára a távoli telephelyek csatlakoztatásához Frame Relay használatát javasolja mindaddig, amíg a térségben elérhető nem lesz a Metro Ethernet vagy más nagysebességű szolgáltatás.

Beállítások	Leírás	Előnyök	Hátrányok	Sávszélesség tartomány	Használt protokoll példák
Vonalkapcsolás	Dedikált áramkör alakul ki a végpontok között. A legjobb példa a betárcsázós kapcsolat.	Legolcsóbb	Hívásfelépítés	28 Kbps - 144 Kbps	PPP, ISDN
Csomagkapcsolás	Az eszközök a csomagokat osztott pont-pont vagy pont-többpont összeköttetésen keresztül küldik át a vivő hálózaton. Különböző hosszúságú csomagokat küldenek állandó vagy kapcsolt virtuális áramkörökön keresztül.	Rugalmas sávszélesség, kevésbé költséges	Összeköttetésen keresztüli osztott átviteli közeg	56 Kbps - 45 Mbps	Frame Relay
Bérelt vonal	Pont-pont kapcsolat két számítógép vagy helyi hálózat között.	Legbiztonságosabb	Drága	56 Kbps - 45 Mbps	PPP, HDLC, SDLC
Cellatovábbítás	A csomagkapcsoláshoz hasonló, de a különböző hosszúságú csomagok helyett egyenlő hosszúságú cellákat használ. Az adatokat egyforma hosszúságú cellákra osztják, és így viszik át őket a virtuális áramkörökön.	A legalkalmasabb az egyidejű hang- és adatátvitelre	Jelentős többletterhelés	1.54 Mbps - 622 Mbps	ATM

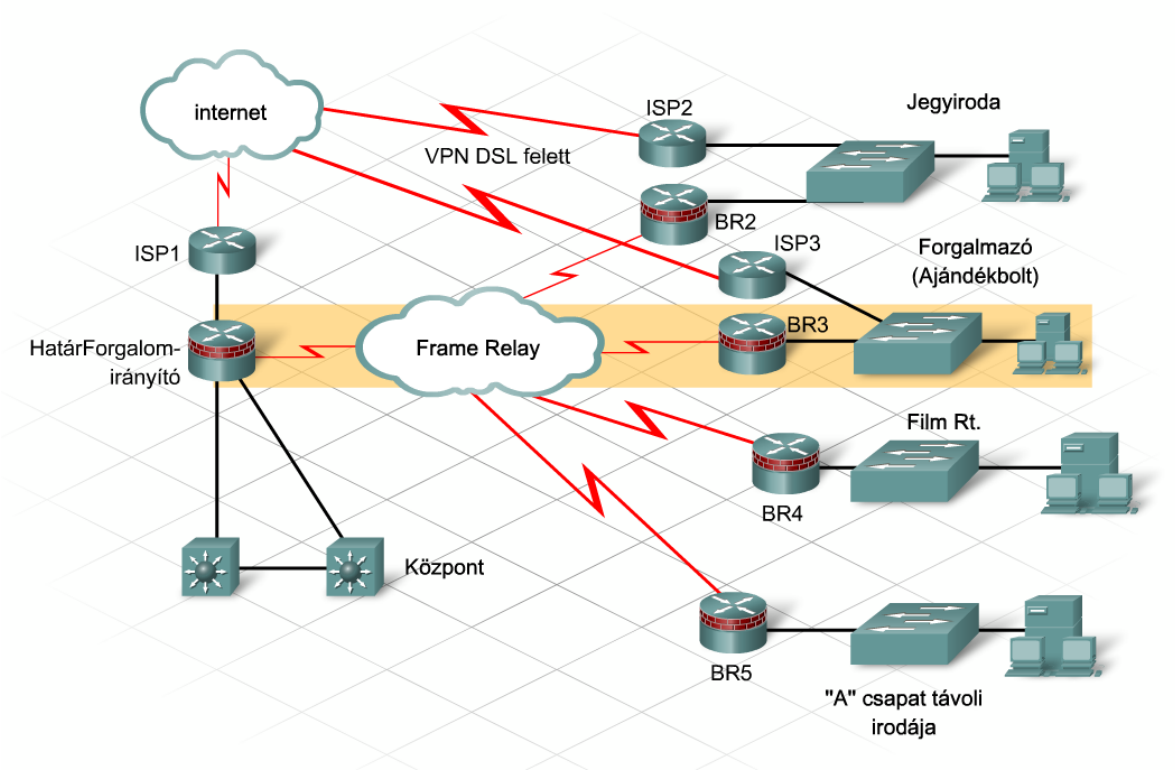
A pont-pont alapú T1 kapcsolattal szemben a Frame Relay előnye, hogy egyetlen fizikai kapcsolat a TSP-hez lehetővé teszi a stadion és az összes távoli helyszín közötti összeköttetést.

A Frame Relay összeköttetések típusai

A Frame Relay hálózatok az adatátvitelhez a következő két összeköttetés típus valamelyikét használják:

- A **kapcsolt virtuális áramkörök** (switched virtual circuit – SVC) minden adatátvitelhez átmenetileg létrejövő kapcsolatok, melyek az adatküldés befejeztével megszűnnek.
- Az **állandó virtuális áramkörök** (permanent virtual circuit – PVC) állandó kapcsolatok. A stadion és a távoli helyszínek között ilyen típusú összeköttetésre van szükség.

A stadion vezetőségével történt megbeszélést követően a Hálózat Kft. dolgozói a dedikált WAN-kapcsolat tesztelése érdekében a stadion és az ajándék üzlet között Frame Relay próba kapcsolat telepítése mellett döntött. A próba telepítés egy új hálózati technológia megvalósítása annak tesztelésére, hogy a technológia képes-e a tervezési célok teljesítésére.



5.3.2 A forgalmi minták és az alkalmazás támogatás meghatározása

A távoli helyszínek hálózati szolgáltatásai

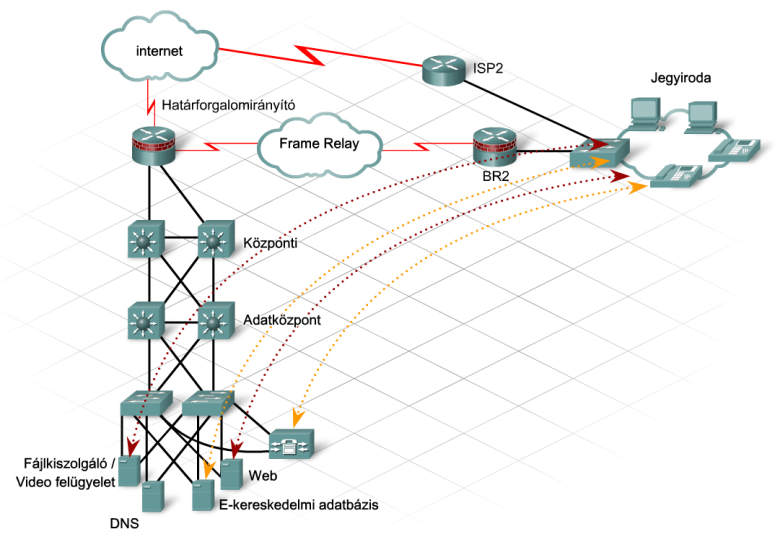
A távoli helyszínek és a stadion hálózata közötti kapcsolat fizikai megvalósításának tervezése során meg kell vizsgálni, hogy a távoli helyszíneken dolgozók várhatóan miként fogják a hálózati szolgáltatásokat igénybe venni. A távoli helyszíneken léteznek egymáshoz hasonló és egyedi követelményeket támasztó alkalmazások is. A távoli helyszíneken szükséges szolgáltatások:

- E-kereskedelmi és adatbázis szolgáltatások
- IP telefon
- Videó felügyelet és megfigyelés

Ezeken felül a távoli csoportiroda hozzáférést igényel a stadionban lévő bérszámfejtési és ügyviteli kiszolgálókhoz.

A Film Rt. alkalmazottainak képesnek kell lenni arra, hogy távolról megfigyeljék a stadion videó képernyőit, és video fájlokat küldjenek a stadion web kiszolgálóihoz.

A tervező diagramot készít az összes forgalomról, ami a WAN-kapcsolatokon keresztül valamelyik szolgáltatási helyszín felé áramlik. A diagramon található információk birtokában hozhatók létre a tűzfal szabályok és az ACL szűrés. Ezeknek a szabályoknak biztosítania kell, hogy az összes távoli helyszín dolgozója képes legyen a szükséges szolgáltatások elérésére.



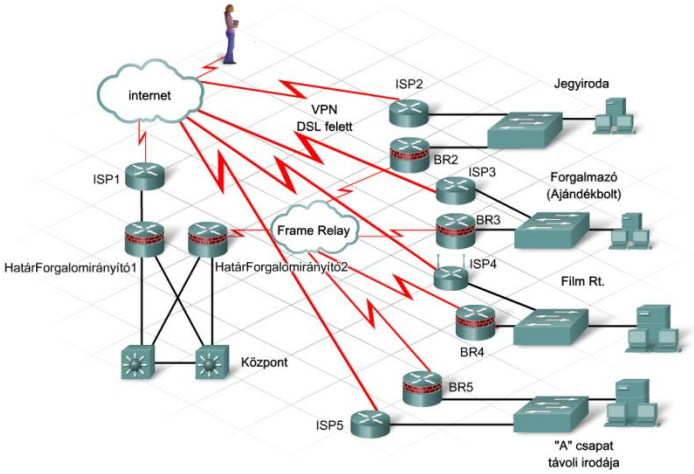
5.3.3 A VPN és a végpontok közötti kapcsolatok tervezése

A Frame Relay összeköttetés tartalék útvonalai

A jegyárusító iroda és az ajándék üzlet az interneten keresztül, telephelyközi (site-to-site) VPN-ek segítségével csatlakozik a stadion hálózatához. A stadionban és a távoli helyszíneken a VPN végpontokként szolgáló saját forgalomirányítóit az internetszolgáltató felügyeli. A tervező ezeket a VPN kapcsolatokat a dedikált Frame Relay kapcsolat hibája esetén tartalék útvonalakként szeretné használni. A tervező mindkét új helyszín esetében ezeknek a tartalék összeköttetéseknek a létrehozását, valamint a redundancia érdekében, a központi helyszínen egy második határ-forgalomirányító használatát javasolja.

A távmunkások támogatása

A stadion vezetősége szeretné az alkalmanként otthonról vagy távoli helyszínekről dolgozók számára is a hálózat elérését biztosítani. A sportcsapat alkalmazottainak például utazásaik során szükségük van a csoport kiszolgálóhoz való biztonságos hozzáférésre. Mivel az ügyfél VPN hozzáférés az ISP által eddig nyújtott szolgáltatással biztosítható, a tervező ennek a lehetőségnek a megfontolását, és az internetszolgáltatóval történő megbeszélését javasolja a stadion vezetőségének.



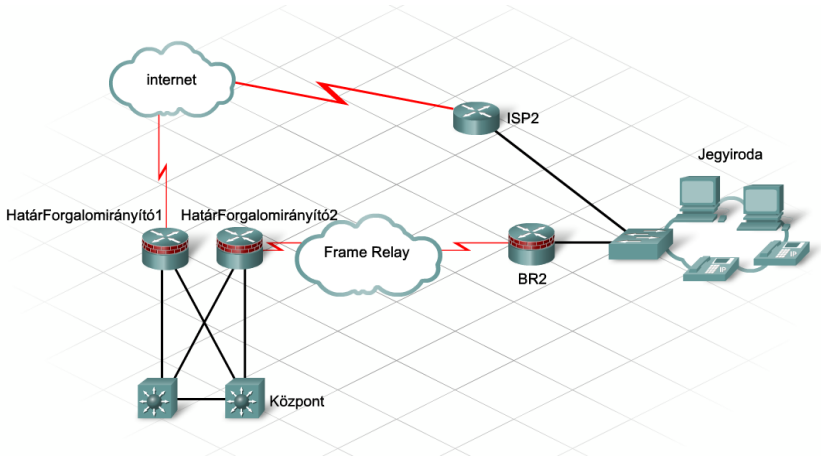
5.3.4 A WAN logikai hálózati tervének létrehozása

Forgalomirányítás és IP-címzés

A meglévő hálózatban a távoli telephelyek csak VPN-en keresztül csatlakoznak a stadionhoz. Egyszerű statikus forgalomirányítással biztosíthatók ezek a kapcsolatok, és az internetszolgáltató által felügyelt forgalomirányító DHCP-vel biztosítja a távoli helyszínek helyi hálózatainak címzését.

Mivel a távoli telephelyek elérését VPN és dedikált WAN-kapcsolat is biztosítja, ezért nagy odafigyeléssel kell az egyes helyszínek IP-címtartományát kiválasztani. Esetenként szükség lehet a távoli telephelyek címtartományainak megváltoztatására is.

A telephelyeken telepitett új WAN-kapcsolatok egyről kettőre növelik a stadion hálózatához vezető lehetséges útvonalak számát. Ennek következtében a stadion LAN-szolgáltatásainak eléréséhez már nem feltétlenül megfelelő a statikus forgalomirányítás. A Frame Relay kapcsolatok hibája esetén a távoli LAN-ok hálózatelérésének biztosításához szükség lehet dinamikus forgalomirányításra. A hálózattervező mindezt feljegyzi, hogy később, a stadion forgalomirányításának megvalósításakor ezt figyelembe vehesse.



5.4 A vezetéknélküli hálózat terve

5.4.1 Lefedettség és mobilitás

A vezetéknélküli lefedettség bővítése

Az új terv legfontosabb célja a vezetéknélküli lefedettség bővítése.

A helyi média kérésére a stadion vezetősége a sajtópáholyban a vezetéknélküli internet hozzáférés érdekében egy kis költségű, vezetéknélküli hozzáférési ponttal bővítette a hálózatot. Néhány alkalmazott vezetéknélküli forgalomirányítókat szerzett be, amelyek csak alacsony szintű lefedettséget biztosítottak a csoportirodákban. Ezek az eszközök nem rendelkeznek megfelelő teljesítménnyel és megbízhatósággal a vállalati szintű vezetéknélküli hálózat megvalósításához.

Vezetéknélküli lefedettség

A stadion hálózati tervében megfogalmazott követelmények teljesítéséhez a következő négy területen van szükség vezetéknélküli lefedettségre:

- Sajtópáholy
- Csapat társalgók
- A stadion étterme
- A stadion területén található VIP helyiségek

A két meglévő vezetéknélküli hozzáférési pont helyett több és jobban felügyelhető eszközökre van szükség. Néhány helyszínen a vendégek részére kell vezetéknélküli hozzáférést biztosítani, a munkaterületeken pedig biztonságos hozzáférésre van szükség a bérszámfejtési és ügyviteli kiszolgálók eléréséhez.

A stadion vezetősége a vezetéknélküli hozzáférés iránti igény gyors növekedésére számít. Véleményük szerint két éven belül szükségessé válik az IP-telefon támogatás, ami vezetéknélküli barangolási lehetőséget és QoS eljárásokat igényel a hálózatban.

Egyesített vezetékes és vezetéknélküli megoldások

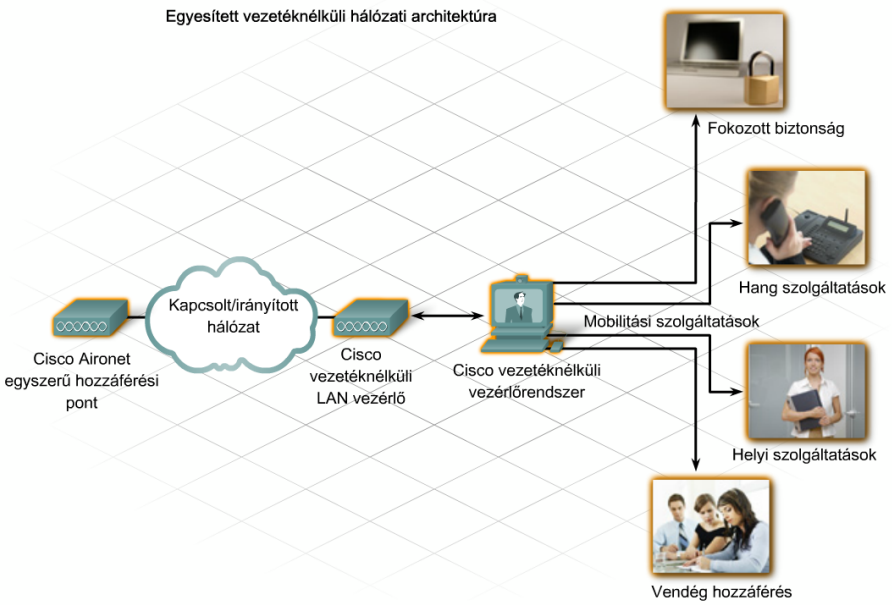
Az új vezetéknélküli hálózat integrálása a stadion vezetékes helyi hálózatába egyszerűsíti a felügyeletet, és lehetővé teszi az Ethernet infrastruktúra biztonságának és redundanciájának a használatát.

A huzalozási központban az Ethernet kapcsolókhoz csatlakozó független hozzáférési pontok megfelelő lefedettséget biztosítanak a stadion korábban kijelölt négy területén. Korlátozott vezetéknélküli barangolás biztosítható olyan vezetéknélküli VLAN-ok létrehozásával, amelyek a hálózaton keresztül az egymást átfedő vezetéknélküli lefedettségi területekre terjednek ki.

Bár ezzel a megoldással teljesíthetők a stadion hálózatának pillanatnyi céljai, a hálózattervező a vezetéknélküli követelmények kielégítéséhez egyszerű (vezérlő alapú) hozzáférési pontok (LAP – Lightweight Access Point) és az ezekhez tartozó vezetéknélküli LAN vezérlők beszerzését javasolja. Az egyszerű hozzáférési pontok nem független eszközök, működésük a vezetéknélküli vezérlő konfigurációs és biztonsági információin alapul.

A vezetéknélküli vezérlőrendszer szoftvert alkalmazó egységes vezetéknélküli megoldások olyan speciális lehetőségeket biztosítanak, mint például a központosított felügyelet, vagy a többszintű szolgáltatási rendszer a különböző felhasználók és ügyfelek számára. Ezek a rendszerek a különböző vezetéknélküli felhasználásokhoz különböző QoS és biztonsági szinteket biztosítanak.

A vezetéknélküli vezérlők és a felügyeleti programok alkalmazása a hálózatban egyszerűsíti a vezetéknélküli barangolás megvalósítását, és az IP-telefonok telepítését. Ezekkel a beállításokkal nincs szükség a vezetéknélküli barangoláshoz külön végpontok közötti VLAN létrehozására.



Biztonsági szolgáltatások

A vezetéknélküli veszélyek felügyelete és elhárítása, a biztonsági irányelvek érvényesítése és az adatok védelme érdekében egyesíti a vezetékes és a vezetéknélküli biztonságot.

Hang szolgáltatások

A valósidejű mobil hangkommunikáció megvalósítása érdekében kiterjeszti az egységes vezetéknélküli hálózat mobilitását.

Helyfüggő szolgáltatások

Lehetővé teszi az eszközök nyomon követését RF-ID segítségével, a hálózati felügyeletet, a biztonságot, és a környezetfüggő alkalmazások használatát.

Vendég hozzáférés

A vendégeknek, a forgalmazóknak és a partnereknek biztosított valós idejű, vezetéknélküli internet hozzáférés a vállalatokat versenyképesebbé teszi napjaink üzleti világában.

A hálózattervező által javasolt vezetéknélküli megoldás teljesíti a stadion hálózat korszerűsítésének alábbi követelményeit:

- **Bővíthetőség** – Az új hozzáférési pontok könnyen hozzáadhatók a hálózathoz, és központilag felügyelhetők.
- **Rendelkezésre állás** – A hozzáférési pontok egy másik hozzáférési pont kiesése esetén automatikusan képesek a jelerősségük növelésére.
- **Biztonság** – Az egész vállalatot érintő biztonsági irányelvek a vezetéknélküli hálózat minden rétegében (a rádiós rétegtől a MAC rétegen át a hálózati rétegig) érvényesek. Ez a megoldás megkönnyíti az egységesen érvényes biztonság, a QoS és a felhasználói irányelvek biztosítását. Ezek az irányelvek figyelembe veszik az eszközök különböző osztályainak (PDA-k, hordozható lapolvasók, számítógépek stb.) specifikus tulajdonságait. A biztonsági irányelvek a DoS támadások felderítését és hatásainak mérséklését, valamint az illetéktelen hozzáférési pontok (rogue AP) megtalálását és kizárását is elősegítik. Ezek a funkciók a teljes felügyelt WLAN-ban működnek.
- **Felügyelhetőség** – A megoldás dinamikus, az egész rendszerre kiterjedő RF felügyeletet biztosít, beleértve az olyan zavartalan vezetéknélküli működést elősegítő szolgáltatásokat is, mint amilyen a dinamikus csatornakiosztás, az átviteli teljesítményszabályozás és a terheléselosztás. Az egységes grafikus interfész vállalati szintű irányelveket kezelő része lehetővé teszi a VLAN-ok, a biztonsági rendszerek és a QoS felügyeletét.

Egyszerű hozzáférési pontok

Vezetéknélküli vezérlők

5.4.2 A vezetéknélküli hozzáférési pontok elhelyezése

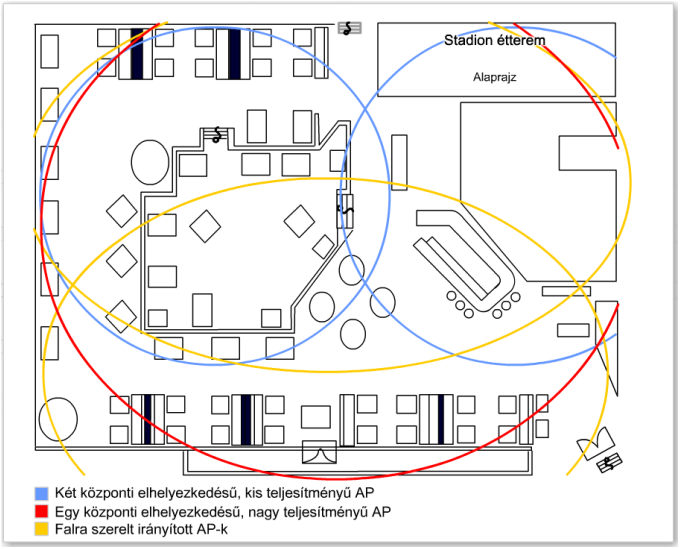
A stadion vezetéknélküli hálózatának helyszíni felmérése alapján az étteremben a jó minőségű vezetéknélküli lefedettség érdekében legalább két hozzáférési pontra van szükség.

Az étteremben a vezetéknélküli jel biztosításához a legjobb megoldás irányított antennájú hozzáférési pontok felszerelése a két külső falon.

A helyszíni szemle során a tervező az étkezőkben nem talált semmit, ami vezetéknélküli interferenciát okozhatna, a konyhában elhelyezett mikrohullámú sütő viszont interferenciát okozhat a bár környékén. Ha a kiválasztott hozzáférési pontok esetében ez indokolt, a megfelelő lefedettség biztosítása érdekében még egy helyszíni szemlére is szükség lehet.

A stadion területén található 20 VIP helyiség közepén egy mennyezetre szerelt, kis teljesítményű hozzáférési pontot érdemes használni.

A sajtópáholyban jelenleg egy független hozzáférési pont található. Mivel ez nem biztosít megfelelő lefedettséget, két új, egyszerű hozzáférési pont használata javasolt.



5.4.3 A vezetéknélküli hálózat redundanciája és rugalmassága

Rendelkezésre állással kapcsolatos megfontolások

A vezetéknélküli kapcsolat rendelkezésre állása a következő tényezőktől függ:

- A hozzáférési pont helye
- A hozzáférési pont jelerőssége
- A hozzáférési pont felhasználóinak száma

Független hozzáférési pontokat tartalmazó vezetéknélküli hálózatokban a tervező által meghatározott csatorna- és teljesítmény paramétereket statikusan állítják be a hozzáférési pontokon. Ezt követően a vezetéknélküli jelek változásai a beállításokat már nem befolyásolják. A helyszíni felmérés egy meghatározott hely lefedettségét egy adott időben mutatja. A tervezőnek nehéz előre kiszámítania az irodák konfigurációs változásait és az új interferencia források megjelenését.

Dinamikus újra konfigurálás

Az autonóm hozzáférési pontokkal szemben a vezetéknélküli vezérlők automatikusan meghatározzák egy hálózaton belül az egyszerű hozzáférési pontok közötti jelerősséget, majd ezeknek az információknak a segítségével létrehozzák a hálózat dinamikus, optimális RF topológiáját.

Induláskor egy egyszerű hozzáférési pont (Cisco LAP) azonnal vezetéknélküli LAN vezérlőt keres a hálózatban. Amikor talál egyet, a szomszédos hozzáférési pontok jelerősségét és MAC-címét tartalmazó, titkosított üzeneteket küld. Egyetlen vezetéknélküli LAN vezérlőt tartalmazó hálózatban a vezérlő minden hozzáférési pont csatornáját az optimális jelerősségre, lefedettségre és kapacitásra hangolja.

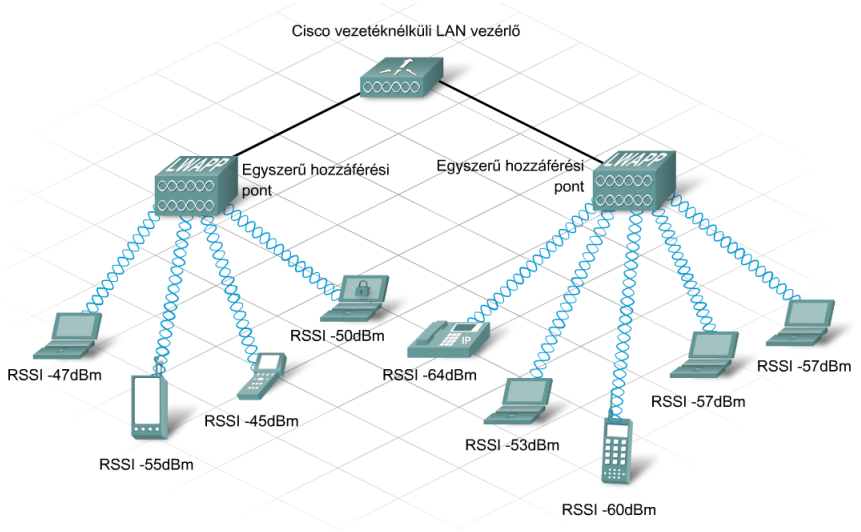
Központosított felhasználói terheléselosztás

A titkosított, vezetéknélküli üzenetek segítségével a Cisco vezetéknélküli vezérlők az egész hálózatot és a hozzáférési pontok közötti jelerősséget is felderítik. Amikor egy felhasználó egy hozzáférési ponthoz szeretne csatlakozni, a felhasználó kérését vevő minden egyszerű hozzáférési

pont egy próbakérést küld a vezérlőnek. A vezérlő a felhasználói jelerősség és a jel-zaj viszony alapján dönti el, hogy melyik hozzáférési pont válaszoljon a felhasználói kérésre.

Ha egy szomszéd hozzáférési pont például ugyanazt a szolgáltatást alacsonyabb jelerősséggel biztosítja, a vezérlő a jelerősség vagy az RSSI (Receiver Signal Strength Indicator – vevő jelerősség mutató) alapján határozza meg az ügyfél próbakérésére válaszoló hozzáférési pontot.

Ezek az intézkedések növelik a WLAN-on belüli vezetéknélküli szolgáltatások rendelkezésre állását. Az adatközpontban található vezetéknélküli vezérlők kihasználják a vezetékes LAN nagymértékű rendelkezésre állásának és redundáns kapcsolatainak előnyeit.



5.4.4 A WLAN logikai hálózati tervének elkészítése

A WLAN IP-címzése

Egy vezetéknélküli LAN barangolási lehetőségeinek kialakításakor a hálózattervezőnek az IP-címzést is figyelembe kell vennie. Független hozzáférési pontok esetében egy VLAN-t kell létrehozni és kiterjeszteni minden huzalozási központra azért, hogy az azonos 3. rétegbeli IP-hálózatban lévő hozzáférési pontok csatlakoztatását biztosítani lehessen. Ha azonban sok vezetéknélküli felhasználó csatlakozik a hálózathoz, nehézzé válik az üzenetszórás. Ilyen esetben a hálózat bővíthetőségéről már nem beszélhetünk.

3. rétegbeli helyváltoztatás

Vezetéknélküli vezérlők és egyszerű hozzáférési pontok segítségével 3. rétegbeli vezetéknélküli barangolás valósítható meg. Egyszintű vezetéknélküli alhálózat létrehozásához nincs szükség a VLAN-ok kiterjesztésére a hálózat minden hozzáférési pontjára.

Vezetéknélküli vezérlő használatával az egyszerű hozzáférési pontok illeszkednek az alhálózati infrastruktúrába, és olyan IP-címet kapnak, amely az őket tartalmazó alhálózatból való. A vezetéknélküli kliensektől érkező minden forgalom egy speciális csomagba kerül, melyet az alaphálózaton keresztül, alagúttechnikával visznek át a vezetéknélküli LAN vezérlőhöz.

A kliens eszközök a vezérlőtől kapják az IP-címet, nem pedig annak az épületnek a területén lévő alhálózatból, ahol tartózkodnak. Az alhálózat IP infrastruktúrája a felhasználók elől rejtve marad. A

vezérlő felügyel minden barangolást és alagúthasználatot, így a felhasználó a barangolás során mindvégig ugyanazzal az IP-címmel rendelkezik.

5.5 A biztonság kialakítása

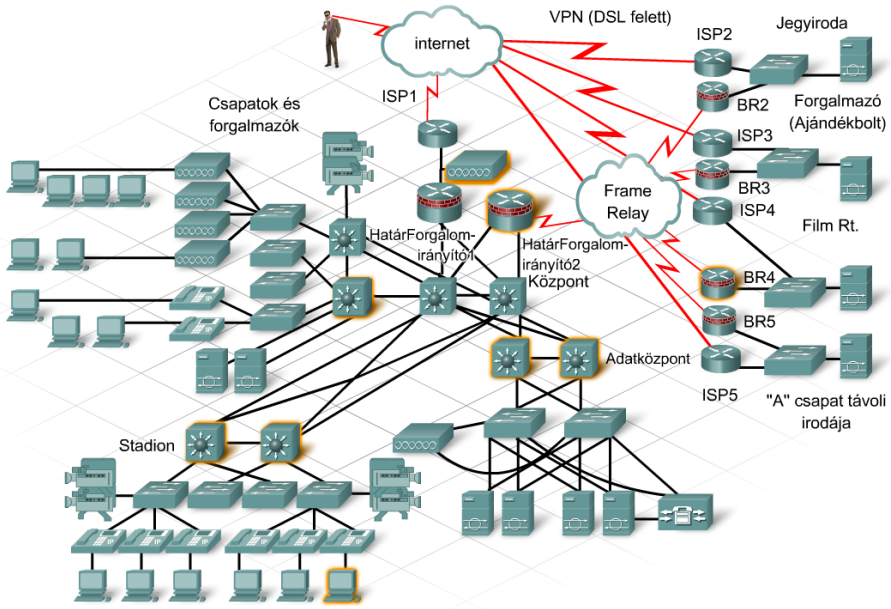
5.5.1 A biztonsági funkciók és alkalmazások elhelyezése

A hálózatok elleni támadás különböző formákat ölthet, és származhat mind belső mind külső forrástól. A hálózat határán elhelyezett tűzfal nem biztosítja a teljes hálózati biztonságot. A hálózattervezőnek kell meghatároznia, hogy melyek a veszélyeztetett adatok és kommunikációs folyamatok, és várhatóan honnan érkeznek a támadások. A biztonsági szolgáltatásokat az esetleges támadások megakadályozása érdekében a hálózat megfelelő pontjain kell elhelyezni.

Az elektronikus kereskedelem kiszolgálói a stadion hálózatán olyan ügyfél információkat tárolnak, melyek hitelkártya és banki adatokat is tartalmazhatnak. A felhasználók ezekhez a kiszolgálókhoz a stadion hálózatából és az interneten keresztül férnek hozzá.

A stadion adminisztrációs és ügyviteli feladatait kiszolgáló szerverek személyzeti vonatkozású és bérszámfejtési információkat tartalmaznak. Ezeket a kiszolgálókat, és a bennük tárolt adatokat továbbító infrastruktúrát megfelelően kell védeni a jogosulatlan használattól.

A stadion vezetéknélküli hálózatát érintő biztonsági intézkedéseket is át kell gondolni.



A biztonsági szolgáltatások segítenek megvédeni az eszközöket és a hálózatot a betörésektől, a hamisításoktól, az adatmódosításoktól és a szolgáltatásmegtagadás (Denial of Service - DoS) támadás következtében fellépő szolgáltatás kimaradásoktól. A biztonsági szolgáltatások az alábbi módon csoportosíthatók:

- Az infrastruktúra védelme
- A kapcsolatok védelme
- A biztonsági kockázatok felismerése és mérséklése

Az infrastruktúra védelme

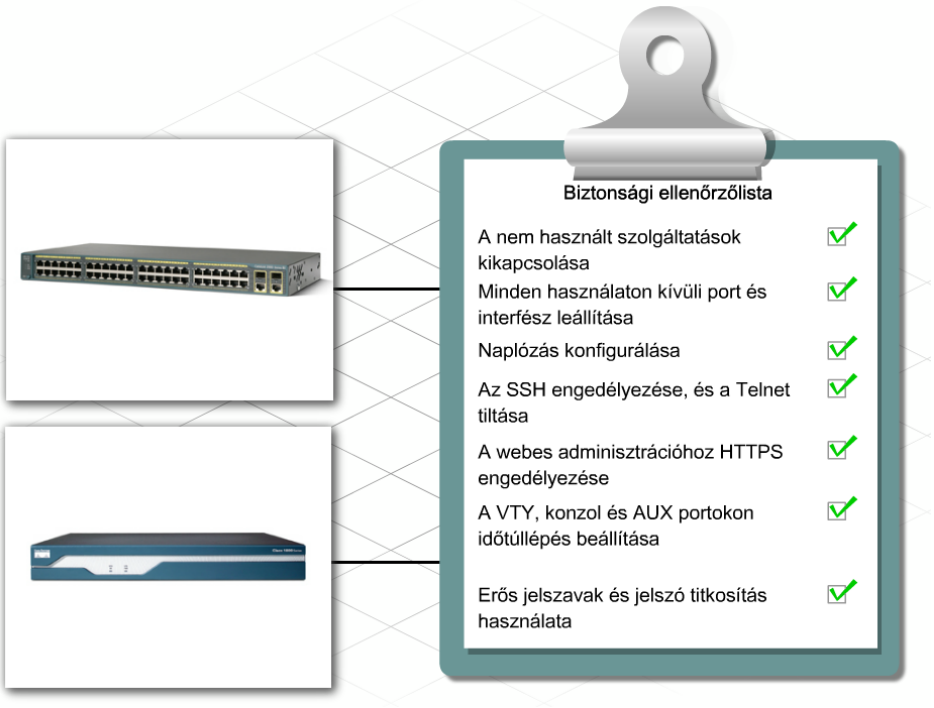
A hálózati biztonság a hálózati eszközök védelmével kezdődik. Mindez tartalmazza a Cisco IOS alapú forgalomirányítók, kapcsolók és berendezések védelmét a közvetlen és közvetett támadásoktól. Ez a védelem lehetővé teszi a hálózaton történő megbízható adatátvitelt.

A kapcsolatok védelme

Az illetéktelen felhasználók hálózathoz való hozzáférésének megakadályozása alapvető fontosságú. Mindez egy biztonságos fizikai hálózattal, és a vezetéknélküli szolgáltatások hozzáférésének hitelesítésével megvalósítható. A stadion alkalmazottainak és vendégeinek külön SSID-t és WLAN-t kell biztosítani. Az adatok védelme a hálózaton való áthaladás közben VPN-ek vagy adattitkosítás segítségével biztosítható.

A biztonsági kockázatok felismerése és mérséklése

A tűzfalak, a behatolás érzékelő (IDS) és behatolás megelőző (IPS) rendszerek, valamint a hozzáférési listák védelmet biztosítanak a fenyegetésekkel és a támadókkal szemben. A hozzáférési listák és a tűzfalszabályok a forgalom szűrésével csak a hasznos forgalmat engedik át a hálózaton.



A biztonsági szolgáltatások megvalósítása

A biztonsági szolgáltatások csak akkor hatékonyak, ha a hálózat megfelelő helyén valósítjuk meg őket. A vállalat határán lévő tűzfalak és szűrők nem védik a kiszolgálókat a lokális hálózaton belüli támadásoktól. A hálózattervező elemzi a korábban létrehozott forgalmi diagramokat, melyek a következőket tartalmazzák:

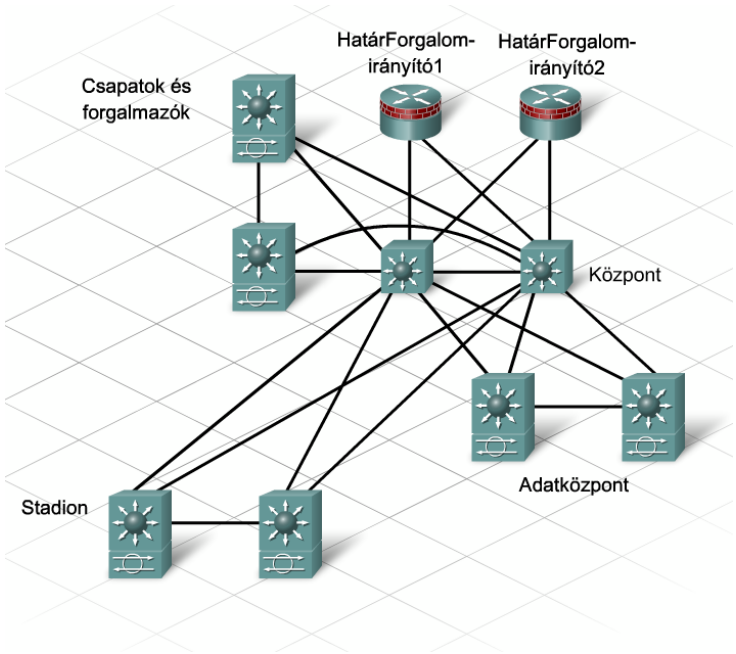
- A belső felhasználók által használt erőforrások

- A külső felhasználók által használt erőforrások
- A felhasználói hozzáférésekhez használt hálózati útvonalak

Ezek az információk segítik a hálózattervezőt abban, hogy a stadion biztonsági irányelvei alapján a biztonsági szolgáltatásokat a megfelelő helyen valósítsa meg.

Integrált szolgáltatások alkalmazása

A hálózattervező, ahol lehetséges, integrált szolgáltatásokat (pl. IOS alapú tűzfalakat és IDS modulokat) alkalmaz, így szükségtelenné válhat különálló biztonsági célberendezések telepítése. Nagyobb hálózatban az ilyen berendezések használata már elkerülhetetlen, mivel a többletterhelés a forgalomirányítók és a kapcsolók túlterheléséhez vezethet.



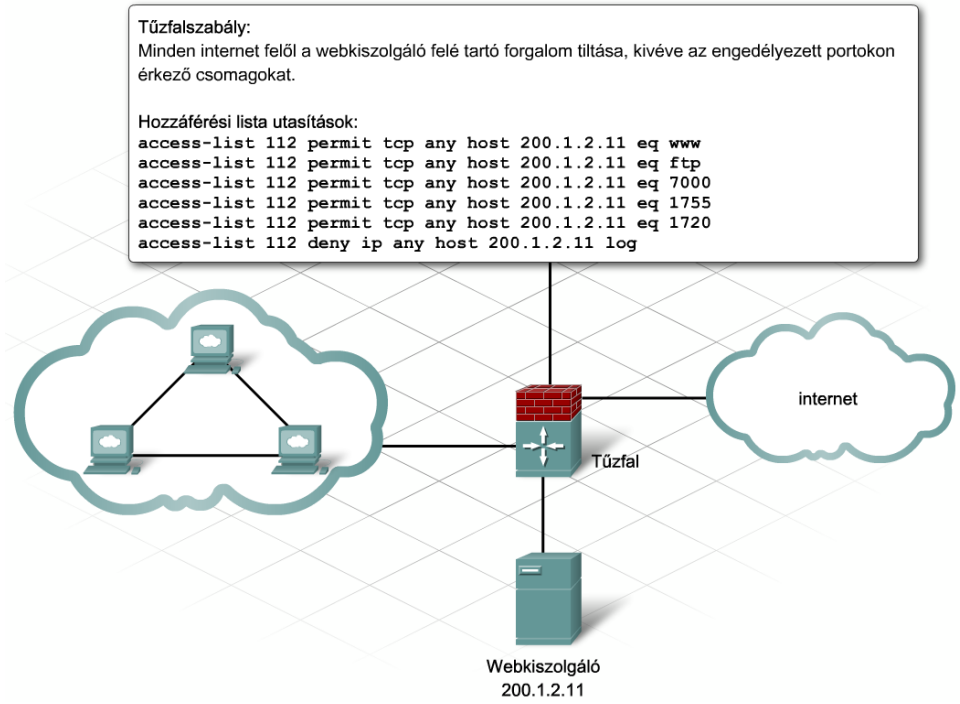
5.5.2 Hozzáférési listák létrehozása és szűrés

A hálózattervező a stadion informatikai munkatársaival együttműködve határozza meg a bővítés során megvalósítandó tűzfalszabályokat.

Egy tűzfalszabály-gyűjtemény például a következő utasításokat tartalmazhatja:

- **A regisztrált belső IP-címekkel megegyező hálózati címekről érkező, befelé irányuló forgalom tiltása** – A hálózatba érkező forgalom nem származhat belső címekkel megegyező hálózati címektől.
- **Külső címekkel rendelkező kiszolgálóhoz érkező, befelé irányuló forgalom tiltása** - A szabály az engedélyezett portok kivételével letiltja a kiszolgáló címfordításos IP-címére érkező forgalmat.
- **Minden bejövő ICMP visszhangkérés tiltása** – A szabály megvédi a belső hálózat felhasználóit a külső, nem megbízható hálózatból érkező ping kérésektől.
- **A Microsoft tartománybeli üzenetszórás, illetve az Active Directory és az SQL kiszolgáló portjaira érkező, befelé irányuló forgalom tiltása** – A Microsoft tartomány forgalmának VPN kapcsolaton keresztül kell haladnia.

- **DNS engedélyezése a DNS kiszolgálóhoz** – Külső DNS lekérdezések engedélyezése.
- **Külső címről a web kiszolgáló címtartományába érkező webes forgalom (TCP 80/443) engedélyezése.**
- **Az FTP kiszolgáló címtartományába érkező forgalom (TCP 21) engedélyezése** – Külső felhasználók számára biztosított FTP szolgáltatás esetén engedélyezi az FTP kiszolgálóhoz való hozzáférést. Emlékeztetőül: FTP szolgáltatás használatakor a felhasználónév és jelszó információk nyílt szövegként kerülnek továbbításra. A passzív FTP (PASV) a 20-as TCP port helyett egy véletlen adatportot használ.
- **Az SMTP kiszolgáló felé irányuló forgalom (TCP 25) engedélyezése** – Engedélyezi a külső SMTP felhasználók és kiszolgálók hozzáférését a belső SMTP levelező kiszolgálóhoz.
- **A belső IMAP kiszolgáló felé irányuló forgalom engedélyezése** – Engedélyezi a külső IMAP kliensek hozzáférését a belső IMAP kiszolgálóhoz.

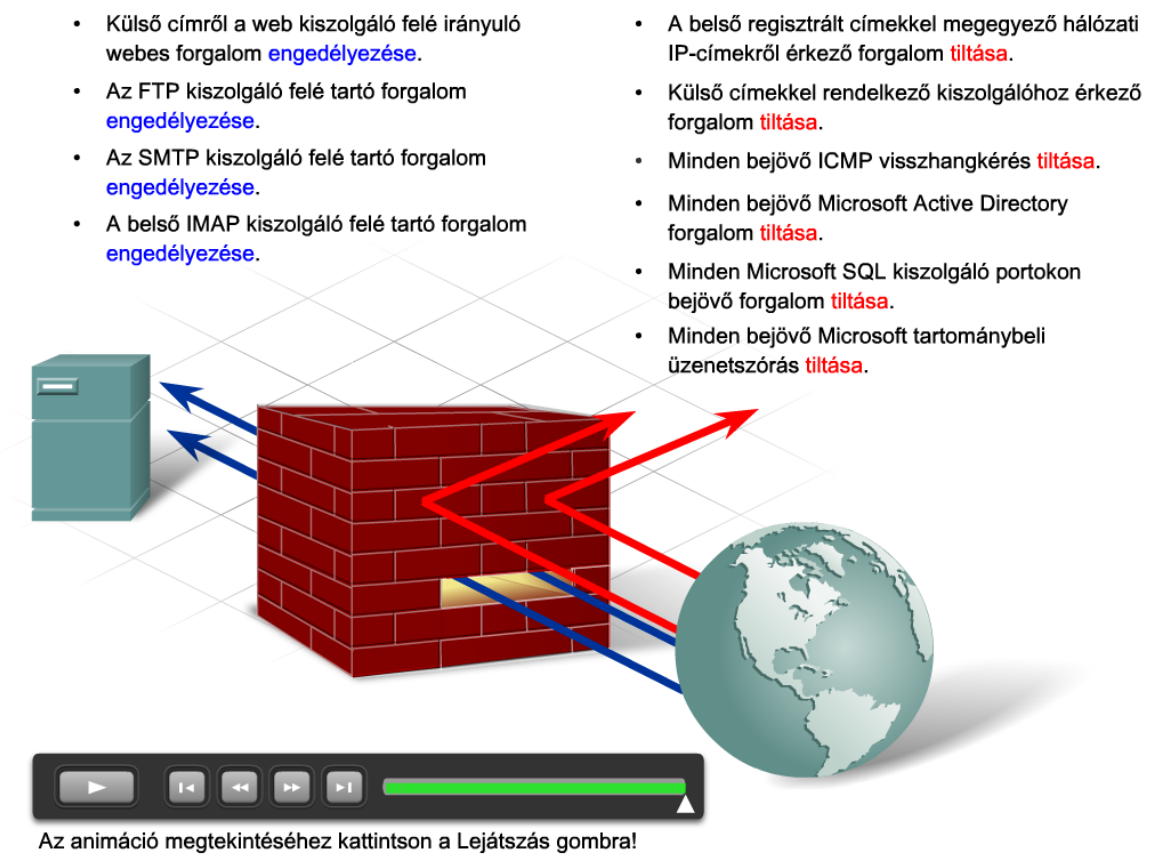


A stadion vezetősége által megfogalmazott biztonsági irányelvek határozzák meg az erőforrásokhoz való felhasználói- és csoporthozzáférési jogosultságokat. A hálózattervező a kiszolgáló operációs rendszerének forgalmazója által meghatározott ajánlásokat is figyelembe veszi, melyek segítenek a rosszindulatú forgalom azonosításában és szűrésében.

A tűzfalszabály-gyűjtemények és hozzáférési listák tervezésekor alapvető fontosságú minden olyan forgalomnak a letiltása, amelyik vagy nem külön engedélyezett, vagy nem egy engedélyezett kérésre adott válasz.

Szabálygyűjtemények és hozzáférési listák

A tűzfal szabálygyűjtemények alapján hozhatók létre a forgalomirányítókon és a tűzfal eszközökön a hozzáférési listák utasításai. Mindegyik szabálygyűjtemény több ACL parancssor létrehozását igényelheti, kimenő és bejövő irányban egyaránt.



5.5.3 A logikai hálózati tervdokumentáció frissítése

A tervdokumentáció tartalmaz minden tűzfalszabály-gyűjteményt, hozzáférési listát, és megadja ezek alkalmazási helyét. A szabálygyűjtemény megállapításai bekerülnek a stadion biztonsági intézkedéseket tartalmazó dokumentációjába.

A tűzfalszabályok és a hozzáférési listák alkalmazási helyének dokumentálása a következő előnyökkel jár:

- Tanúsítja, hogy a hálózaton biztonsági szabályok vannak érvényben.
- Szükséges változások esetén biztosítja, hogy az összes engedélyező és tiltó feltétel megismerhető és megvizsgálható legyen.
- A hálózati alkalmazásokhoz vagy szegmensekhez való hozzáférés szabályaival segíti a hibaelhárítást.

5.6 A fejezet összefoglalása

- Az üzleti céloknak megfelelő hálózati terv létrehozása többlépéses folyamat.
- Minden üzleti cél esetében a tervezőnek meg kell határoznia a cél eléréséhez szükséges hálózati változtatásokat. Minden változtatásnak technikai követelményei vannak, amit a hálózati terv egyes összetevői elégítenek ki.
- Ha a terv összetevőit meghatározta, a tervező az ügyfél által megadott korlátozásokat vizsgálja meg, és szükség esetén kompromisszumokat hoz.

- Minden tervezési döntést az alapján kell meghozni, hogy mennyire teljesíti a négy alapvető technikai követelményt, a skálázhatóságot, a rendelkezésre állást, a biztonságot és a felügyelhetőséget.
- A konvergált hálózatok, mint amilyen a stadion tervezett hálózata is, adat-, hang- és videó forgalom átvitelére képesek. Minden forgalomtípusnak megvannak a saját egyéni teljesítmény követelményei, amihez a tervben QOS megvalósításra van szükség.
- A biztonság a hálózati terv egyetlen olyan része, ahol nem lehet kompromisszumokat kötni. Az előfordulhat, hogy egy biztonságos hálózat létrehozásakor szükséges egy alacsonyabb költségű vagy kevésbé racionális megoldás alkalmazása, de a hálózati szolgáltatások fejlesztése soha nem mehet a biztonság rovására.
- A korlátozások hálózati tervben való figyelembe vételekor szükség van az ügyfél által megadott, fontossági sorrendbe állított üzleti célok megfontolására. Ha kompromisszumot kell hozni, a magas prioritású céloknak megfelelő szolgáltatásokat kell megvalósítani az alacsonyabb célokat biztosító szolgáltatásokkal szemben.
- A hozzáférési réteg tervezési elemei: portsűrűség, VLAN stratégiák, fizikai biztonság, áramellátás, QOS osztályozási és jelölési lehetőségek, és az elosztási réteghez vezető összeköttetések redundanciájának támogatása.
- Az elosztási réteg tervezési elemei: redundáns összetevők és összeköttetések, magas sűrűségű forgalomirányítás, forgalomszűrés, QOS mechanizmusok, gyors konvergálás és forgalomösszegzés.
- A központi réteg tervezési elemei: redundáns összetevők és összeköttetések, magas fokú rendelkezésre állás, és gyorsan konvergáló protokollok.
- A WAN kapcsolatok megtervezéséhez az ügyfél földrajzi helyén elérhető telekommunikációs szolgáltatások ismerete szükséges.
- A távoli telephelyek és a stadion központi hálózata közötti fizikai kapcsolatok meghatározásához a hálózattervezőnek meg kell vizsgálnia, hogy a távoli telephelyek dolgozói várhatóan miként használják a hálózati szolgáltatásokat. A kiszolgáló felé tartó és onnan érkező forgalmi minták a központi helyszínen meghatározzák a sávszélesség igényt és a biztonsági eljárásokat.
- Mivel a WAN kapcsolatok a LAN kapcsolatoknál kisebb megbízhatóságúak is lehetnek, ezért fontos meggondolni egy esetleges tartalék vagy alternatív hozzáférés megvalósítását a WAN tervben.
- A VPN-ek a távmunkások és a kisebb távoli irodák számára biztonságos távoli hozzáférést biztosítanak az interneten keresztül. Az ilyen típusú VPN kapcsolat is hatékony tartalék összeköttetési lehetőség.
- A vezetéknélküli vezérlőrendszer szoftvert alkalmazó egyesített vezetéknélküli megoldások olyan speciális lehetőségeket biztosítanak, mint például a központosított felügyelet, vagy a többszintű szolgáltatási rendszer a különböző felhasználók és ügyfelek számára.
- Az egyszerű vezetéknélküli hozzáférési pontok és a vezetéknélküli LAN vezérlő használata a hálózati tervben központosított felügyeletet, a hozzáférési pontok dinamikus újrakonfigurálását és 3. rétegbeli barangolást biztosít.

- Az LWAPP engedélyezett hozzáférési pontok és a vezetéknélküli vezérlők támogatják a harmadik rétegbeli barangolást. A vezetéknélküli hálózat felhasználói a hozzáférési pontot tartalmazó fizikai hálózattól független IP-címet kapnak.
- A hálózattervezőnek kell meghatároznia, hogy melyek a veszélyeztetett adatok és kommunikációs folyamatok, és várhatóan honnan érkeznek a támadások. Mindez segíti abban, hogy a biztonsági szolgáltatásokat az esetleges támadások megakadályozása érdekében a hálózat megfelelő pontjain helyezze el.
- A biztonsági szolgáltatásoknak három alapvető típusa van: infrastruktúra védelem, kapcsolatok védelme, és a veszélyek felismerése. A veszélyek felismerése magában foglalja az elkerülést és a mérséklést.
- Ahol lehetséges a tervnek integrált szolgáltatásokat (pl. IOS alapú tűzfalakat és IDS modulokat) kell alkalmaznia, így szükségtelenné válhat különálló biztonsági célberendezések telepítése.
- A tűzfalszabály-gyűjtemények és hozzáférési listák tervezésekor alapvető fontosságú minden olyan forgalomnak a letiltása, amelyik nem engedélyezett, vagy nem egy engedélyezett kérdésre adott válasz.

6. Az IP-címzés használata a hálózati tervezésben

6.1 A megfelelő IP-címzési terv kialakítása

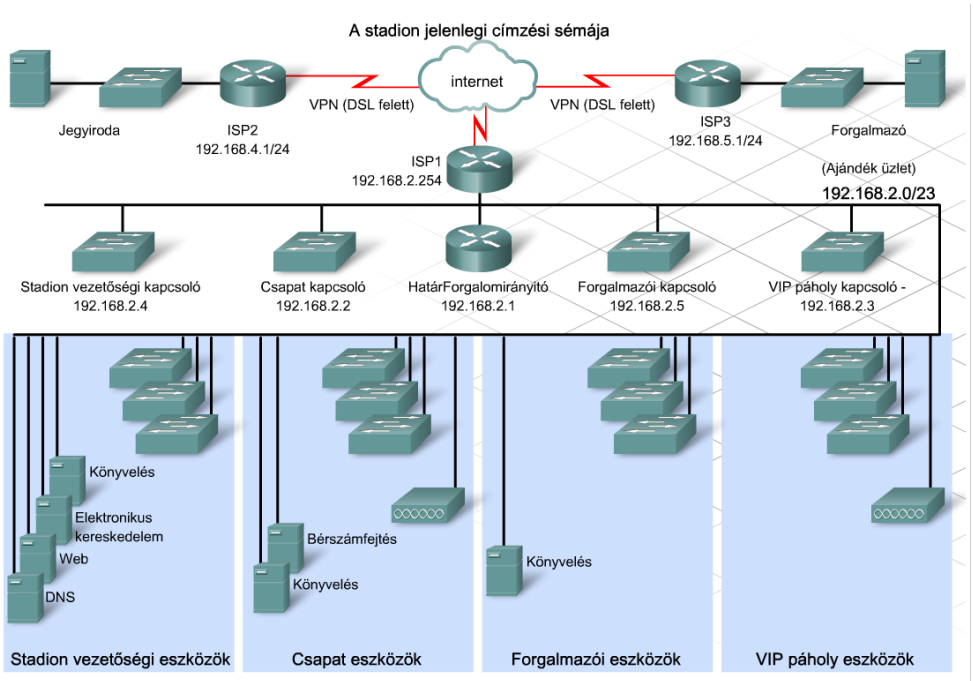
6.1.1 Hierarchikus forgalomirányítási és címzési séma alkalmazása

Az IP-címzési séma

A stadion hálózatának meglévő IP-címzési sémájában a rendszergazda a 192.168.2.0/23 privát IP hálózati címet alkalmazta. További két alhálózat, a 192.168.4.0/24 és a 192.168.5.0/24 szolgált a távoli helyszínek címzésére. A különböző hálózati eszközökhöz a rendszergazda DHCP-t és statikus beállítást használva rendelt egyedi felhasználói IP-címet.

A meglévő címzési séma nem megfelelő, mert nem alkalmas a hálózat tervezett bővítésének kielégítésére, továbbá a két vezetéknélküli hozzáférési pont által kiosztott IP-címek is átfedik a Stadion Kht. jelenlegi címeit.

Az új tervekhez olyan IP-címzésre van szükség, amely minden hálózati eszköz számára egyedi IP-címet biztosít.

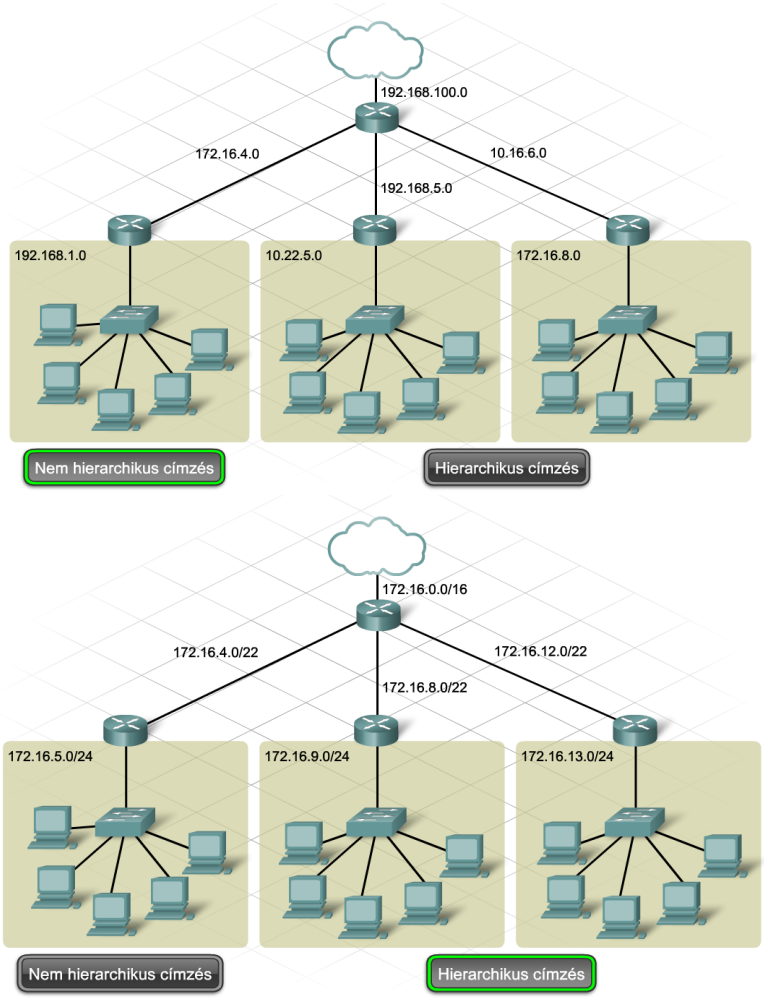


Amikor egy hálózaton ugyanazt az IP-címet több eszköz is használja, IP-cím ütközés történik. Ilyenkor az azonos IP-című eszközökhöz történő csomagtovábbítás nem megbízható.

Megfelelő tervezéssel az új IP-címzési séma elősegítheti a hierarchikus forgalomirányítást, és hatékony 3. rétegbeli felépítést biztosíthat. Az IP címkiosztás megtervezése és dokumentálása az alábbiak miatt szükséges:

- Címismétlések elkerülése
- Hozzáférés biztosítása és felügyelete
- Biztonság és teljesítmény ellenőrzése
- Moduláris tervezés támogatása
- Útvonalösszegzést alkalmazó, bővíthető megoldás támogatása

Hierarchikus IP-címzéssel a stadion hálózata könnyebben kezelhető.



Hierarchikus IP-címzési séma alkalmazása

Az egyszintű IP-címzés nem teljesíti a stadion hálózatának méretezhetőségi követelményeit.

Az IP-címblokkok megfelelő kiosztásával rendelkező hálózat a következő tulajdonságokkal rendelkezik:

- Forgalomirányítási stabilitás
- Hozzáférhető szolgáltatás
- Skálázható hálózatkezelés
- Hálózati modularitás

A stadion hálózatában a hierarchikus IP-címzési séma alkalmazása megkönnyíti a hálózat későbbi bővítését. Egy nagyobb hálózat több felhasználó, jegyiroda, távoli iroda és ajándék üzlet kiszolgálására alkalmas.

A megfelelően tervezett hierarchikus IP-címzési séma egyszerűsíti az útvonalösszegzést.

Példák IP-címet igénylő eszközökre

6.1.2 Osztály alapú alhálózatok és útvonalösszegzés

Útvonalösszegzés alkalmazásához a hálózatnak folytonos, egymással határos alhálózatokat kell tartalmaznia. Ilyen hálózat esetén minden alhálózat szomszédos az ugyanabban a hálózatban lévő többi alhálózattal.

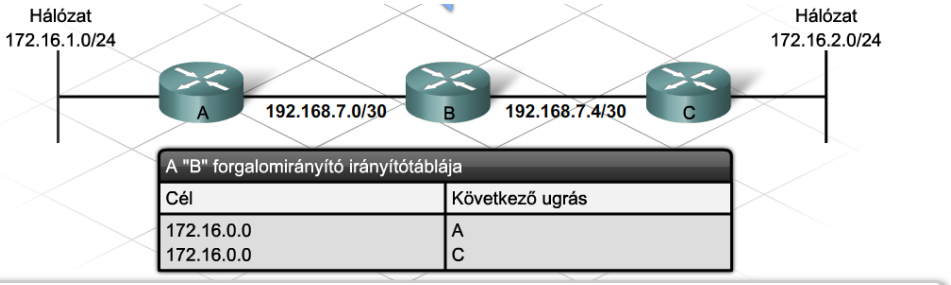
A nem folytonos hálózatokban találhatók alhálózatok, melyek nem szomszédosak, illetve melyeket más hálózatok választanak el egymástól.

Hibásan megtervezett IP-címzés nem folytonos hálózatokat eredményezhet. Ezek a hálózatok forgalomirányítási problémákat okozhatnak, mivel az irányítótáblák több összegzett útvonalat tartalmaznak a hálózat alhálózatainak eléréséhez. Ebben az esetben, – hacsak manuális konfigurálással nem avatkozunk be – előfordulhat, hogy az irányító protokollok nem megfelelően irányítják a forgalmat, mivel némelyikük alapértelmezetten automatikus útvonalösszegzést végez.

Az automatikus útvonalösszegzés letiltása

Az automatikus útvonalösszegzés rendszerint kívánatos. Nem folytonos alhálózatok esetén azonban a következő paranccsal mindenképpen le kell tiltani mind RIPv2, mind EIGRP esetén:

```
Router(config-router)# no auto-summary
```



6.1.3 VLSM alkalmazása az IP-címzésben

A stadion vezetősége és a hálózattervező egyaránt úgy gondolja, hogy a stadion hálózata az elkövetkező két évben jelentős mértékben fog bővülni. A méretezhetőségi követelmények teljesítéséhez hierarchikus IP-címzésre és osztály nélküli irányító protokollra van szükség.

Változó hosszúságú alhálózati maszk (VLSM)

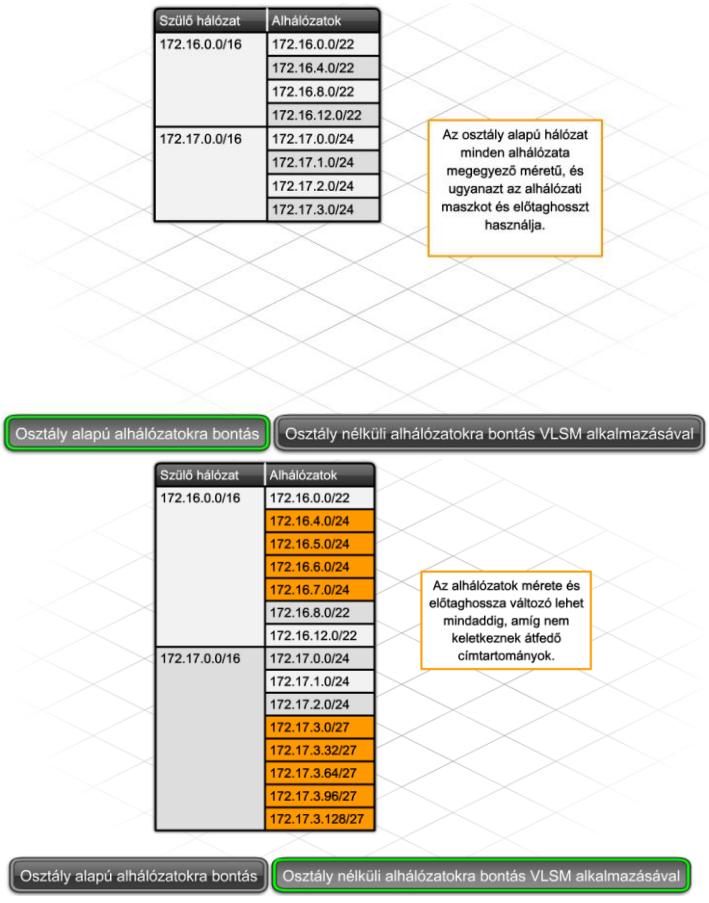
A hálózat tervezője az új hálózat alhálózati sémájának létrehozásához VLSM-et használ. Ezzel megoldható, hogy ne kelljen egy szülő hálózat minden alhálózatának ugyanannyi állomáscímmel és előtaghosszal rendelkeznie. A VLSM az IP-címtér hatékonyabb használatát teszi lehetővé, valamint engedélyezi a forgalomirányítókon a nem osztály határokon történő útvonalösszegzést.

Osztály nélküli forgalomirányítás (CIDR – Classless InterDomain Routing)

VLSM használatakor olyan irányító protokollra van szükség, amelyik támogatja az osztály nélküli forgalomirányítást.

Az osztály alapú irányító protokollok útvonalfrissítései nem tartalmazzák sem az alhálózati maszkot, sem az ezzel egyenértékű előtaghosszt. Ezek a protokollok az alapértelmezett alhálózati maszkok alapján határozzák meg az IP-címek hálózati részét.

Az osztály nélküli protokollok útvonalfrissítéseikben az irányítási információk mellett elküldik az előtag hosszát is. Ezzel lehetővé teszik, hogy a forgalomirányítók az alapértelmezett maszkok mellőzésével határozzák meg a cím hálózati részét.



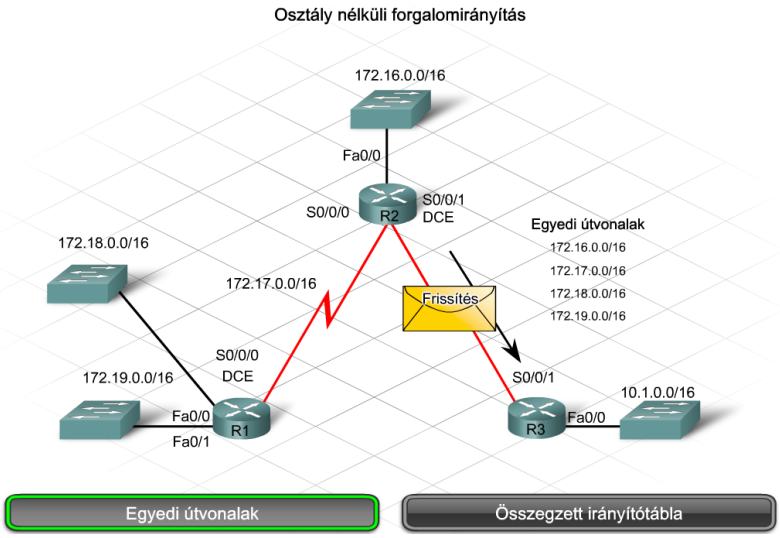
6.1.4 CIDR forgalomirányítás és útvonalösszegzés

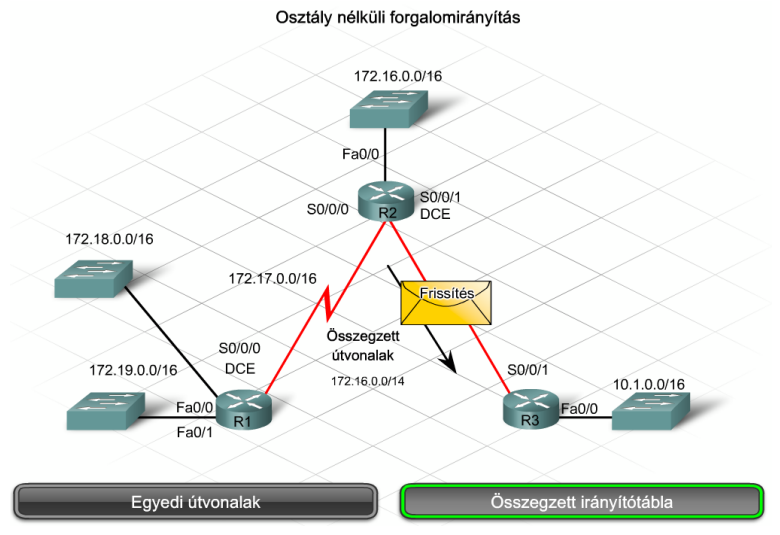
CIDR és útvonalösszegzés

A stadion hierarchikus hálózati tervének célja az útvonalösszegzés megkönnyítése és a forgalomirányítási folyamatok protokoll feldolgozási tevékenységeinek a csökkentése. Az útvonalösszegzés útvonalösszevonásként is ismert. Az útvonalösszegzés eredményeként a forgalomirányítók a folytonos címek egy halmazát rövidebb, kevésbé specifikus alhálózati maszkkal ill. előtaggal, egyetlen útvonalként hirdetik.

A CIDR az osztály alapú határok okozta korlátok megszüntetésével lehetővé teszi az útvonalösszegzést az alapértelmezett maszknál rövidebb, változó hosszúságú alhálózati maszkok (VLSM – Variable Length Subnet Mask) segítségével. Az alapértelmezett osztály alapúnál rövidebb előtaghosszú hálózati címet szuperhálózatnak nevezik. Ilyen szuperhálózati cím például a 172.16.0.0/14. A B osztályú 172.16.0.0 cím alapértelmezett előtagja 16 bit. A /14-es előtag használatával négy folytonos B osztályú hálózatcímet lehet egyetlen irányítótábla bejegyzéssé összevonni.

Az útvonalösszegzés csökkenti az útvonalfrissítések és a helyi irányítótábla bejegyzések számát. Mindez gyorsabb keresést eredményez az irányítótáblában.





Előtagcímek és útvonalösszegzés

Az osztály nélküli irányító protokollok útvonalfrissítéseikben a 32 bites cím mellett tartalmazzák az előtag hosszát ill. az alhálózati maszkot is.

A változó méretű hálózatok és alhálózatok összetett hierarchiáját egy előtagcím segítségével különböző pontokon lehet összevonni. Egy összevont útvonal például tartalmazhat egy 14 bites előtagot, amely egy forgalomirányítón keresztül elérhető minden cím esetén azonos.

Például a 172.16.0.0./14, (bináris formában

10101100.00010000.00000000.00000000

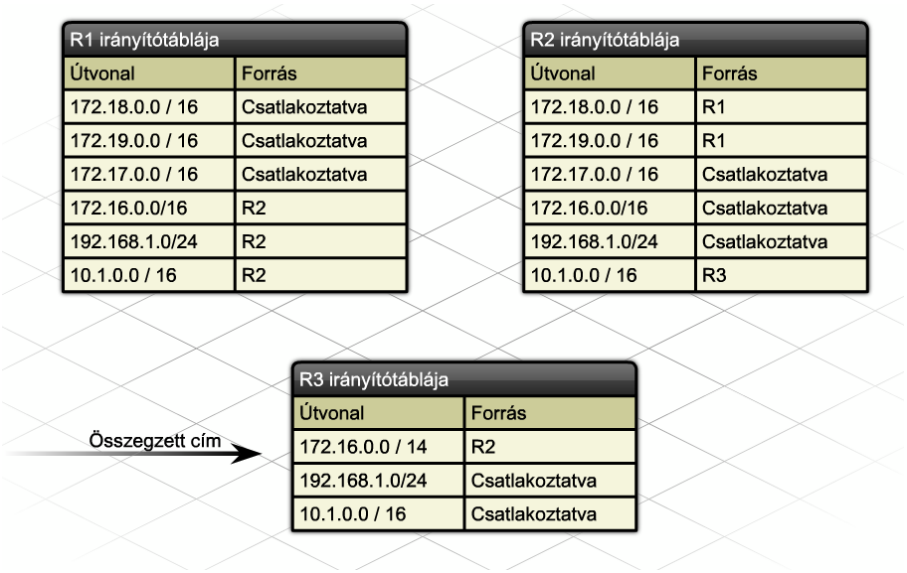
cím és

11111111.11111100.00000000.00000000 alhálózat maszk)

a 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 és 172.19.0.0/16 alhálózatokat összevonja egy hálózatcímmé.

Az útvonalösszegzés csökkenti a felsőbb szintű forgalomirányítók terhelését.

Ahhoz, hogy az útvonalösszegzés megfelelő működjön, a hierarchikus címkiosztást nagy körültekintéssel kell elvégezni. Az összevont hálózati címet úgy kell meghatározni, hogy az összegzésben szereplő hálózati címek ugyanazokkal a magas helyiértékű bitekkel rendelkezzenek.



6.2 A megfelelő IP-címzési és elnevezési séma kialakítása

6.2.1 A logikai LAN IP-címzési sémájának megtervezése

A hálózattervező számára a stadion hálózatának IP-címzésével kapcsolatban vannak olyan egyértelműen meghozható döntések, mint például a nyilvános címtartomány helyett privát címek használata. Más döntések meghozatala viszont gondos tervezést igényel.

6. Az IP-címzés használata a hálózati tervezésben

Az IP-címzési séma kialakításakor a tervező a következő lépéseket követi:

1. lépés: A címek kiosztása előtt megtervezi a teljes címzési sémát.

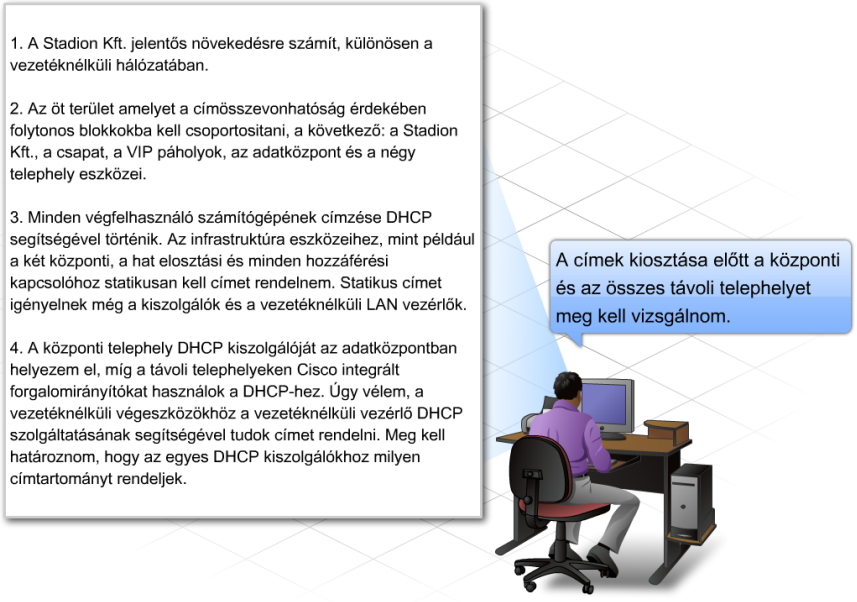
2. lépés: Figyelembe veszi a hálózat jövőbeni jelentős növekedését.

3. lépés: A címzésnél a központi hálózat összevont címeivel kezdve halad kifelé a hálózat határa felé.

4. lépés: Meghatározza a statikus címet igénylő gépeket és eszközöket.

5. lépés: Megállapítja, hol és hogyan kell dinamikus címeket alkalmazni.

Ezeket a szempontokat mind nyilvános, mind privát címek használata esetén figyelembe kell venni.



A hálózat címzését számos feltétel határozza meg:

- A hálózatban jelenleg meglévő állomások és hálózati eszközök száma
- A hálózat várható növekedésének mértéke
- Azon állomások száma, melyeket a helyi hálózathoz vagy intranethez nem tartozó hálózatokból is elérhetővé kell tenni
- A hálózat fizikai elrendezése
- Az alkalmazott forgalomirányítási és biztonsági irányelvek

A stadion hálózatában jelenleg nincs túl sok állomás. Megközelítőleg 500 állomás csatlakozik a vezetékes, és néhány a vezetéknélküli hálózathoz. A Stadion Kht. várható növekedésének megfelelően a tervező az elkövetkező két évre legalább 2000 végfelhasználóval számol. Mindez tartalmazza mindazokat a nyomtatókat, szkennereket, hozzáférési pontokat, vezetéknélküli eszközöket, IP alapú telefonokat és kamerákat, amelyek egyedi IP-címet igényelnek. A növekedés biztosításához a tervező B osztályú privát címek használata mellett dönt.

Az állomások elérhetősége

Néhány állomásnak elérhetőnek kell lennie a helyi hálózathoz vagy intranethez nem tartozó hálózatokból is. Az internet felőli elérhetőség biztosítása érdekében a szerverekhez és szolgáltatásokhoz nyilvánosan regisztrált IP-címet kell rendelni. A feltételek hatékony teljesítése érdekében hálózati címfordításra (NAT) van szükség. A stadionban a két csoportkiszolgáló, valamint a web- és e-kereskedelemi kiszolgálók olyan szolgáltatásokat biztosítanak, melyeknek az interneten keresztül is elérhetőnek kell lennie. A tervező arra a következtetésre jut, hogy az internetszolgáltatótól kapott 30 darab /27-es nyilvános cím elegendő lesz.

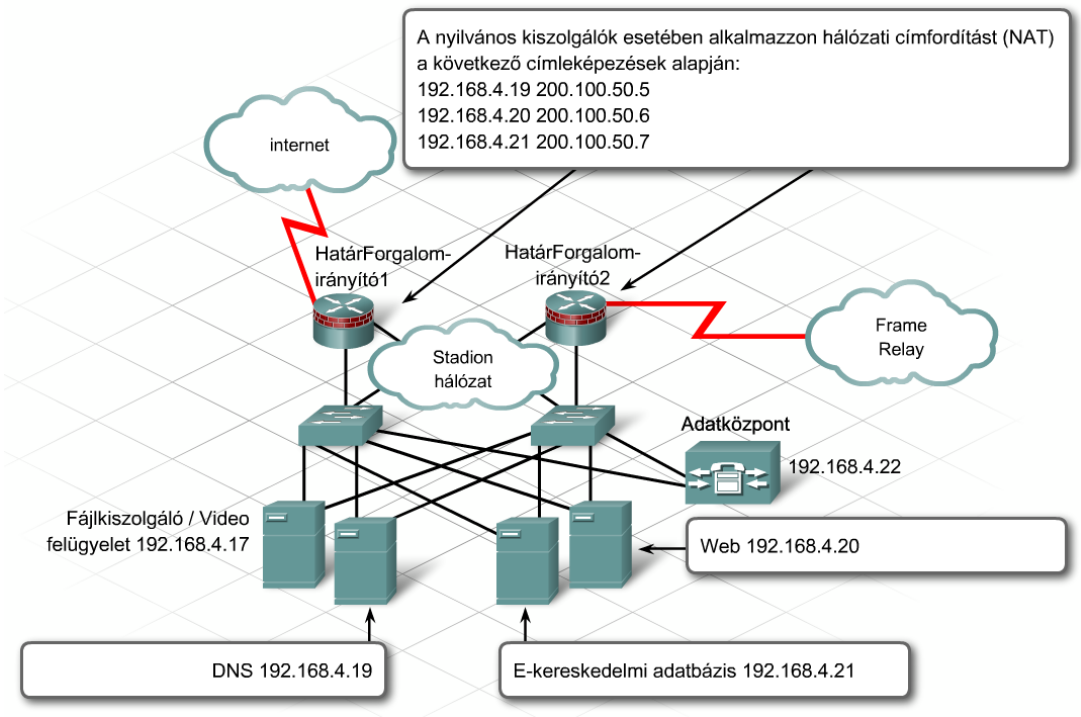
A hálózat fizikai elrendezése

A stadionban 16 elkülönített huzalozási központ van, melyek a földrajzilag más-más területen elhelyezkedő végfelhasználók csatlakozását támogatják. Biztonsági megfontolásból jó megoldás minden IP-alhálózatot egy-egy huzalozási központ által ellátott területre korlátozni. Külön hálózati címet igényel a forgalomirányítók, a 3. rétegbeli kapcsolók és a WAN közötti minden redundáns összeköttetés.

Biztonsági és forgalomirányítási irányelvek

Bizonyos esetekben, a forgalom biztonsági vagy szűrési célból történő szétválasztásához további IP-hálózatokra lehet szükség. Ilyenkor külön alhálózatok létrehozása ajánlott. A vezetéknélküli eszközök és az IP-telefonok például külön hálózatot igényelnek.

Az irányító protokoll megválasztása befolyásolja a hálózat címzését. Egyes irányító protokollok például nem támogatják az osztály nélküli címzést. A protokollok alapértelmezett útvonalösszegzése szintén meghatározó lehet. A tervezőnek figyelembe kell vennie, hogy a B osztályú címzési séma osztály nélküli irányító protokollt igényel.



6.2.2 A címzési blokk meghatározása

A hálózat tervezője a stadion IP-címzési terve alapján meghatározza a szükséges IP hálózatok és alhálózatok számát.

Megszámolja az alhálózatokat, és minden hálózat esetében feljegyzi a felhasználók vagy eszközök jelenlegi és tervezett számát.

Minden huzalozási központhoz legalább négy alhálózat tartozik:

- Adatok
- IP Hang
- Video felügyelet és mérkőzés felvétel
- Hálózatfelügyeleti szolgáltatások

Bizonyos területeken a forgalom szétválasztásához négynél több alhálózatra van szükség. Ilyen esetekben a kapcsolókon VLAN-ok alkalmazásával biztosíthatók az egyes alhálózatok.

A tervező a hálózat minden egyes helyszínéről a következő információkat jegyzi fel:

- A helyszín elhelyezkedése és leírása
- A VLAN vagy a hálózat típusa
- A hálózatok és az állomások száma

Elhelyezkedés és leírás

A tervező úgy azonosítja az egyes helyszíneket, hogy feljegyzi a huzalozási vagy adatközpont helyiségszámát, valamint leírást készít arról a területről, amely az adott központhoz tartozik.

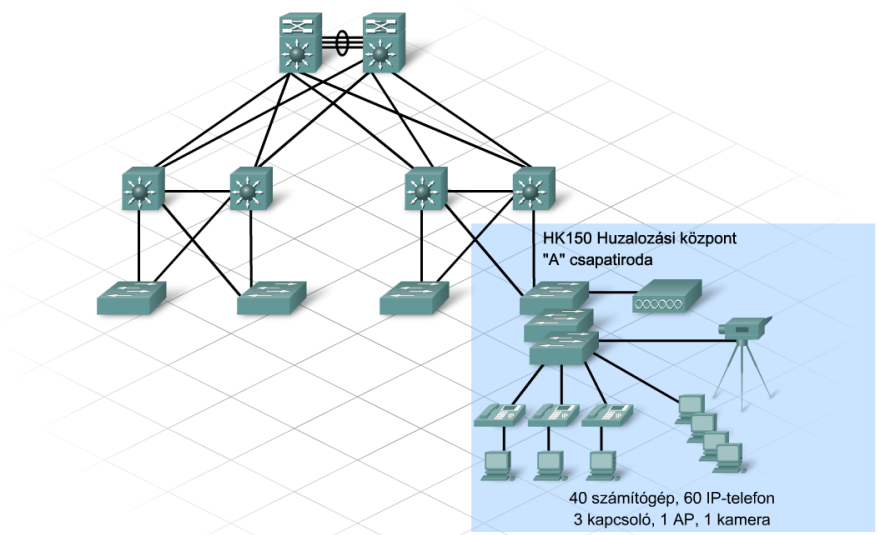
A VLAN vagy a hálózat típusa

A VLAN vagy a hálózat típusának dokumentálása lehetővé teszi a tervező számára, hogy megalapozott becslést végezzen az állomásszám várható növekedésére. Egy adat-VLAN például nagyobb mértékben növekedhet, mint egy IP-telefonokat támogató VLAN. Egy 3. rétegbeli pont-pont hálózat viszont általában az eredeti két állomáscímnél később sem igényel többet.

A hálózatok és állomások száma hálózatonként

Mindezeket követően a tervező számba veszi és felsorolja az új tervben szereplő hálózatok, és hálózatonként az állomások számát. Ez adja meg a pillanatnyilag szükséges címek számát. Ennek tudatában becsülhető meg az egyes területeken a növekedés, és így az IP hálózat vagy alhálózat mérete is.

A vezetéknélküli hálózat követelményeinek meghatározása külön történik. A vezetéknélkül csatlakozó eszközök hozzáadása a szükséges IP-címek számát növeli, viszont ezek az eszközök nem igényelnek új kapcsolókat vagy portokat.



IP hálózati követelmények táblázat

Hozzáférési réteg	Terület leírása	VLAN vagy hálózat típusa	Hálózatok száma	Állomások száma	Növekedés
Hozzáférési réteg					
HK150	"A" csapatiroda	Adat VLAN	1	40	50%
HK150	"A" csapatiroda	Hang VLAN	1	60	20%
HK150	"A" csapatiroda	Felügyeleti VLAN	1	4	25%
HK150	"A" csapatiroda	Videofelügyelet	1	1	Nincs
W172	"B" csapatiroda	Adat VLAN	1	22	50%
HK172	"B" csapatiroda	Hang VLAN	1	38	20%
HK172	"B" csapatiroda	Felügyeleti VLAN	1	4	25%
AK172	"B" csapatiroda	Videofelügyelet	1	1	Nincs
Elosztási réteg					
AK220	Csapatiroda és étterem elosztó	3. rétegbeli összeköttetés a központi réteghez	5	2	Nincs
AK220	Vezetőségi iroda és étterem elosztó	3. rétegbeli összeköttetés a központi réteghez	5	2	Nincs

6.2.3 A forgalomirányítási elvek meghatározása

A tervezőnek ki kell választania azt az irányító protokollt, amely megfelel a stadionra vonatkozó alábbi követelményeknek:

- VLSM-et támogató, osztály nélküli forgalomirányítás
- A forgalom csökkentése érdekében kisméretű és ritkán küldött irányítótábla frissítések
- Hiba esetén gyors konvergencia

Elvárás, hogy a stadion jelenlegi hálózati szakemberei képesek legyenek az újonnan kialakított hálózat támogatására is. Ennek érdekében olyan irányító protokollra van szükség, amelynél a hibakeresés és az átkonfigurálás egyszerűen elvégezhető.

A hálózati alkalmazottak közül ketten rendelkeznek tapasztalattal

az EIGRP használatában. Mivel az EIGRP teljesíti a stadion minden elvárását, így a tervező OSPF és RIPv2 helyett ennek használata mellett dönt.

Az EIGRP egy Cisco specifikus irányító protokoll, így a stadion minden dinamikus forgalomirányításban résztvevő eszközének Cisco eszköznek kell lennie.

EIGRP terheléselosztás

A stadion hálózatában a rendelkezésre állásra vonatkozó követelmények teljesítéséhez redundáns és tartalék összeköttetések használata szükséges. Az EIGRP azért jó választás, mert a tartalék összeköttetéseken terheléselosztásra alkalmas. Az EIGRP alapértelmezetten ugyanahhoz a célhálózathoz maximum négy azonos költségű útvonalat képes rendelni az irányítótáblában. Az útvonalak számának meghatározására a maximum-paths parancs szolgál. A maximum-paths parancs lehetséges értéke 1 és 6 között van. Az 1 érték a terheléselosztás letiltását jelenti, hiszen egy adott célhoz mindössze egyetlen útvonal szerepel az irányítótáblában.

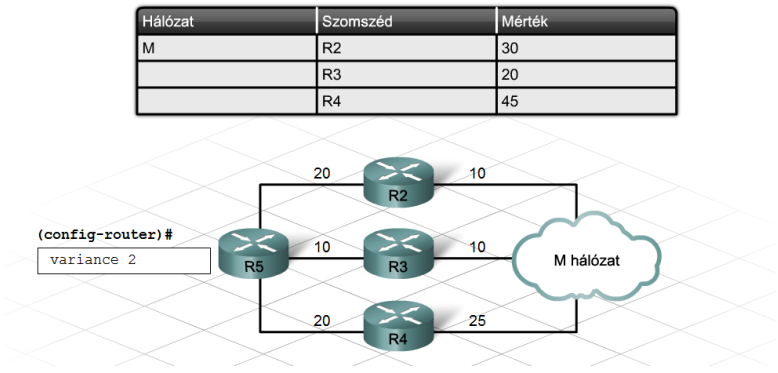
Eltérő költségű terheléselosztás

Bizonyos esetekben, mint például népszerű események jegyárusításakor, szükség lehet a megnövekedett forgalom elosztására a tartalék összeköttetéseken. Mivel a tartalék és az elsődleges összeköttetések költsége nem mindig egyezik meg, a forgalom elosztása a tartalék útvonalakon alapértelmezetten nem működik. Egy EIGRP hálózatban a forgalomirányítón a variance paranccsal konfigurálható az eltérő költségű terheléselosztás.

EIGRP esetén a variance értéke határozza meg azt, hogy egy adott útvonal megjelenhet-e az irányítótáblában terheléselosztási céllal. A még elfogadható maximális mérték megadására az EIGRP a variance és a legkisebb mérték szorzatát használja. A variance parancs után egy 1 és 128 közötti érték adható meg. A parancs használatára egy példa:

```
Router(config-router)# variance 2
```

A forgalom ily módon történő elosztása nagy forgalom esetén megakadályozza egy útvonal túlterhelését, amennyiben rendelkezésre áll alternatív útvonal.



Az R5 forgalomirányító az M hálózat eléréséhez az R3 forgalomirányítón keresztüli útvonalat használja, mivel annak mértéke a legkisebb. (20=10+10)

Az M hálózat felé tartó forgalom esetén a terheléselosztáshoz használható útvonalak meghatározásához az R5 forgalomirányítón az EIGRP a legjobb mértéket a konfigurált variance értékével szorozza meg. Ebben az esetben az R3

forgalomirányítón keresztüli útvonal mértéke a legjobb (20). Minden 40-nél (20x2) kisebb mértékű útvonal bekerül az irányítótáblába, és részt vesz a terheléselosztásban.

Az R5 forgalomirányító használhatja az R2 forgalomirányítón keresztüli útvonalat terheléselosztásra, mivel annak mértéke (30) kisebb 40-nél. Az R4 forgalomirányítón keresztüli útvonal nem kerül az irányítótáblába, mert annak mértéke (45) nagyobb az elfogadhatónál (40).

Hitelesítés

A stadion hálózatának forgalomirányításában kereskedelmi partnerek és távoli telephelyek is részt vesznek. Fontos annak ellenőrzése, hogy az útvonalfrissítések megbízható forgalomirányítótól származnak-e. Az irányító protokollok konfigurálhatók úgy, hogy csak hitelesített szomszédok megbízható frissítéseit fogadják el. Ilyenkor a forgalomirányító minden fogadott útvonalfrissítés forrását azonosítja.

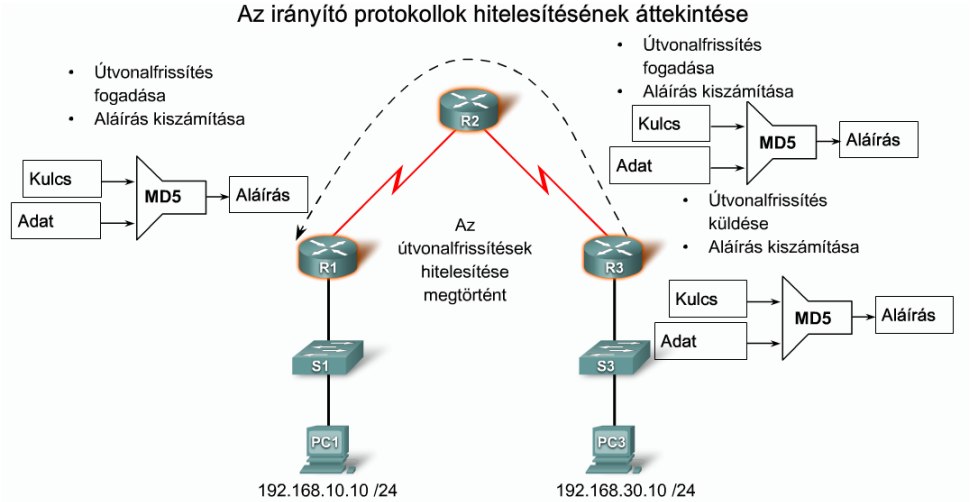
A szomszédok hitelesítésének két típusa létezik: A nyílt szövegű és az MD5 (Message Digest Algorithm Version 5) hitelesítés. Biztonsági okokból ajánlott az MD5 hitelesítés alkalmazása, mert ilyenkor a kulcsot vagy jelszót továbbítás közben nem lehet elkapni és kiolvasni.

A kulcs kezelése

MD5 esetén a hitelesítésben résztvevő szomszédok egy hitelesítési kulcsot osztanak meg egymással, vagyis azonos hitelesítési kulcsot használnak. A RIPv2 és az EIGRP irányító protokollok kulcsláncokkal további lehetőségeket biztosítanak a kulcsok kezelésére. Ezzel kulcsok egy sorozata adható meg, és a Cisco IOS szoftver ezek váltogatásával csökkenti a kulcsok sebezhetőségét.

A kulcsok definiálásakor minden esetben meg kell adni a kulcs érvényességi idejét (“élettartamát”). Egy adott kulcs élettartama alatt az útvonalfrissítések elküldése az aktív kulccsal történik. Ajánlott, hogy a kulcsok egy részének aktív intervalluma átfedje egymást annak érdekében, hogy ne legyenek aktív kulcs nélküli időintervallumok. Ilyen időszakban ugyanis a szomszédok hitelesítése nem lehetséges, és így útvonalfrissítések sem lehetségesek.

Egy hitelesítési kulcs vagy kulcslánc aktív időintervallumának beállításához a send-lifetime parancs használható. Az accept-lifetime parancs segítségével megadható, hogy egy forgalomirányító mennyi ideig fogadjon el útvonalfrissítéseket az adott kulccsal. Mindkét parancs alapértelmezett értéke a végtelen.

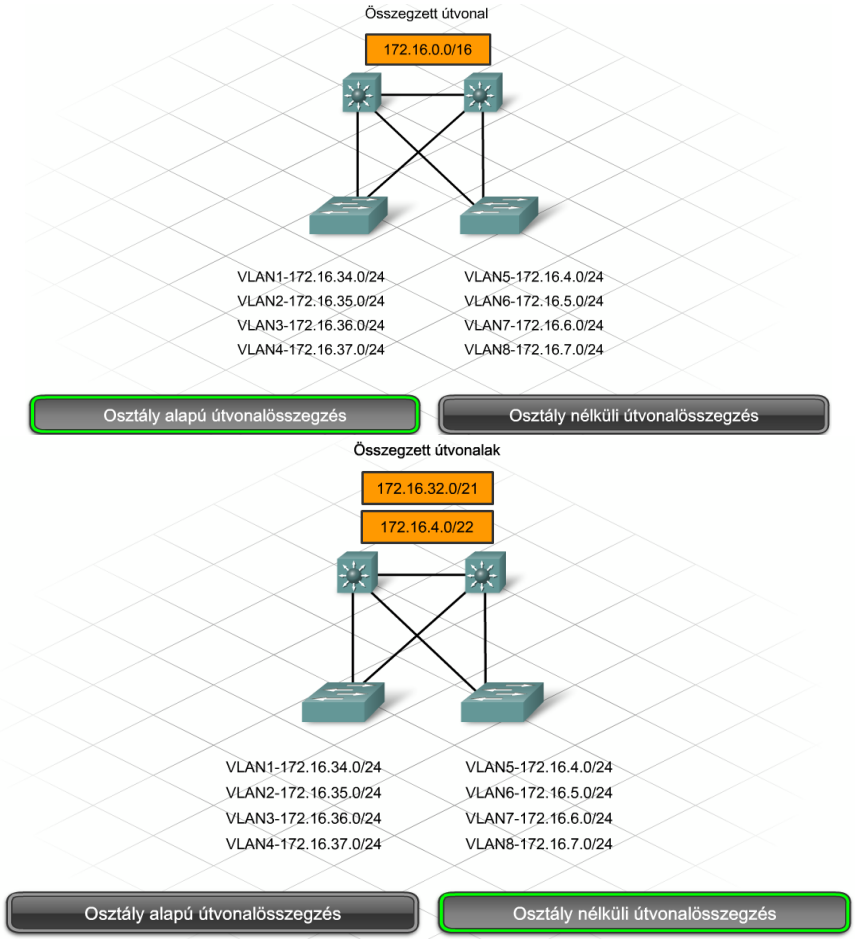


6.2.4 A útvonalösszegzés és –elosztás megtervezése

Hierarchikus hálózatban az útvonalösszegzés a folytonos IP hálózatok átjárójaként szolgáló 3. rétegbeli eszközökön történik. Ezt követően a forgalomirányítók az összevont útvonalakat a központi réteg felé hirdetik. A stadion lokális hálózatában az útvonalösszegzés az elosztási réteg forgalomirányítóin és a 3. rétegbeli kapcsolókon valósul meg.

Az EIGRP lehetővé teszi az osztály nélküli útvonalösszegzést az alapértelmezettől eltérő maszkok segítségével. Ezzel csökkenthető az útvonalfrissítések és a helyi irányítótáblák bejegyzéseinek száma. Az útvonalösszegzés csökkenti az útvonalfrissítésekhez szükséges sávszélességet, és így az irányítótáblában gyorsabb keresést eredményez.

Az EIGRP automatikus útvonalösszegzést használ az alapértelmezett osztály alapú határokon, ami a stadion hálózata esetében nem megfelelő. A tervezett B osztályú címzés alhálózatainak összevonásához az automatikus útvonalösszegzést le kell tiltani.



Az automatikus összegzés letiltása esetén az összevonásokat manuálisan kell konfigurálni.

A hálózat tervezője a következő lépésekkel határoz meg egy összevont útvonalat:

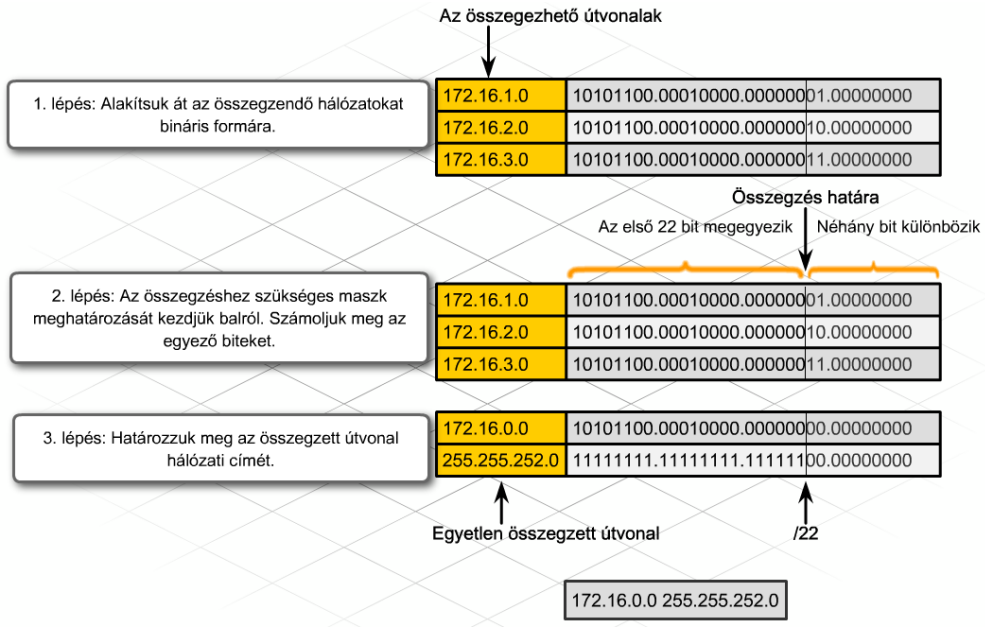
1. lépés: Átalakítja a hálózatok címeit bináris formára.

2. lépés: Megállapítja az összegzett útvonalhoz szükséges alhálózati maszkot.

3. lépés: Meghatározza az összevont útvonal hálózati címét.

Összevont útvonalak alkalmazása esetén a tervezőnek meg kell győződnie arról, hogy az útvonalak nem fednek-e át más összevont vagy egyedi útvonalat.

Az útvonalak meghatározását követően a tervező manuálisan konfigurálja azokat a forgalomirányítókon.



6.2.5 A címzés megtervezése

IP címblokkok

Az IP hálózati követelmények adatait tartalmazó táblázat alapján a tervező meghatározza az egyes hálózati területekhez szükséges IP címblokkok méretét. A szükséges alhálózati maszkok számának csökkentése érdekében az azonos igényekkel rendelkező területeket csoportosítja.

Amennyiben minden eszköz regisztrált nyilvános címet igényel, a csoportosítás nem hatékony. Privát címek használatakor viszont az egyes területek csoportosítása jó megoldás lehet. Az egyesített alhálózatok számának csökkentésével egyszerűbbé válik a konfiguráció, a hálózat kezelése és a hibajavítás is. A tervező 4 alhálózati maszk használata mellett dönt: /19, /22, /24 és /30.

A címblokkok kiosztása

A tervező lépésről lépésre osztja ki az alhálózatok címeit, a legnagyobbtól a legkisebb felé haladva.

A 0-s és a csupa 1-s alhálózatot a tervező speciális célokra tartja fenn. Bonyolultabb hálózatok esetében ezek az alhálózatok egyedi konfigurációt igényelhetnek. Noha a stadion hálózatában jelenleg semmi nem utal arra, hogy ezek a hálózatok megbízhatatlanok lennének, a tervezőnek minden lehetséges helyzetre fel kell készülnie. Mivel az alkalmazott IP hálózati séma messze elegendő címet biztosít, így ezeknek az alhálózatoknak a használata nem szükséges.

A 0-s és a csupa 1-s alhálózat használata

A Cisco IOS 12.0 verzió óta a 0-s és csupa 1-s alhálózat használata engedélyezett, bár nem ajánlott. A korábbi verziókban a 0-s alhálózat alkalmazásához az ip subnet-zero globális konfigurációs parancsot kellett kiadni.

Az RFC 1878 szerint a 0-s és 1-s alhálózatok kizárása már elavult gyakorlatnak tekinthető. A modern programok már alkalmasak minden lehetséges hálózat kezelésére.

Napjainkban a 0-s és a csupa 1-s alhálózat használata elfogadott, és a legtöbb gyártó által támogatott is. Ennek ellenére elsősorban régebbi szoftvereket használó hálózatokban ezeknek az alhálózatoknak az alkalmazása problémákat okozhat.

Alhálózati maszk	Használható alhálózatok	Maximális állomásszám	Alhálózati maszk bitek
255.255.128.0	2	32766	/17
255.255.192.0	4	16382	/18
255.255.224.0	8	8190	/19
255.255.240.0	16	4094	/20
255.255.248.0	32	2046	/21
255.255.252.0	64	1022	/22
255.255.254.0	128	510	/23
255.255.255.0	256	254	24
255.255.255.128	512	126	/25
255.255.255.192	1024	62	/26
255.255.255.224	2048	30	/27
255.255.255.240	4096	14	/28
255.255.255.248	8192	6	/29
255.255.255.252	16384	2	/30

A stadion hálózati tervében használt alhálózatok megtekintéséhez kattintson a táblázatra!

6.2.6 A névadási rendszer megtervezése

A hálózati eszközök neveinek megválasztása sokszor önkényes, kevés figyelmet szentelnek az eszközök struktúrájának vagy az általuk tartalmazott információnak. Egy jó hálózati névadási rendszer megkönnyíti a hálózat irányítását és a felhasználók eligazodását.

A hálózati nevek hozzárendelésének két alapvető típusa létezik:

- **Belső eszköznevek** – Ezeket a neveket csak az adminisztrátor látja. Ilyenek például a forgalomirányítók és a kapcsolók nevei.
- **Külső eszköznevek** – Ezeket a neveket a hálózat felhasználói is láthatják. Ilyenek például a Windows eszköznevek és a DNS nevek.

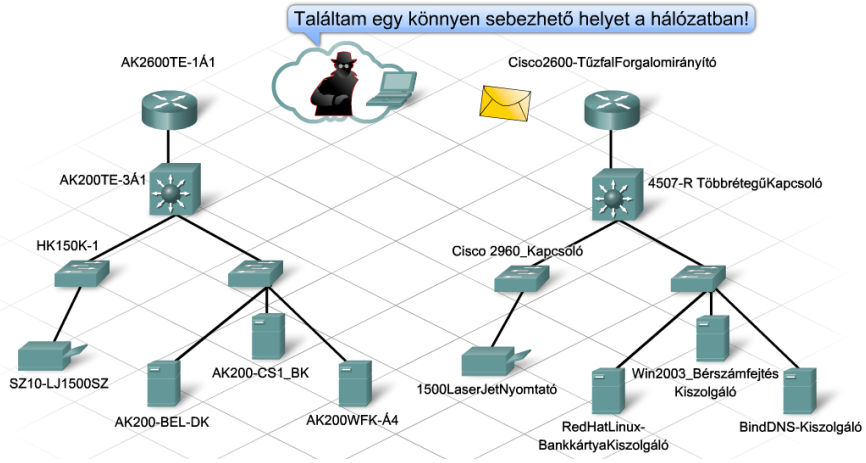
Névadási alapelvek

Gyakran a józan ész határozza meg a névadási elgondolást. Egy jól használható névadási rendszer kialakításához kövessük a következő alapelveket:

- Használjunk minél rövidebb, lehetőleg 12 karakternél nem hosszabb neveket.
- Szavak vagy rövidítések helyett kódokkal utaljunk az eszköz típusára, rendeltetésére és elhelyezkedésére.

- Hozzunk létre következetes névadási rendszert, melynek köszönhetően könnyebbé válik az eszközök nyilvántartása és dokumentálása, valamint a felügyeleti rendszerek kialakítása.
- Dokumentáljuk a neveket az informatikai osztály fájljaiban és a hálózati térképeken.
- Kerüljük a védett erőforrások könnyű felderítését lehetővé tevő nevek használatát.

Bizonyos esetekben a hekkerek már a hálózati nevek alapján is elegendő információhoz jutnak ahhoz, hogy megtalálják célpontjukat, és kihasználják a sebezhető pontokat. Lehetséges kompromisszumos megoldást jelent könnyen megjegyezhető és használható külső DNS nevek használata.



Belső eszköznevek:

HK150K-1 *A huzalozási központ első kapcsolója a 150-es szobában*

AK200TE-3SZ1 *Többrétegű elosztási kapcsoló az adatközpont 200-as szobájában az 1-es állványon*

AK200WFK-Á4 *Windows fájlkiszolgáló az adatközpont 200-as szobájában a 4-es állványon*

Külső eszköznevek:

SZ10-LJ1500Sz *Színes lézernyomtató a 10-es szobában*

AK200-CS1-BK Az 1. *csapat bérszámfejtési kiszolgálója az Adatközpont 200-as szobájában*

AK200-BEL-DK *A belső DNS kiszolgáló*

Rossz belső nevek:

Cisco2600-TűzfalForgalomirányító

NATForgalomirányító

Rossz külső nevek

Win2003_BérszámfejtésKiszolgáló

RedHatLinux-BankkártyaKiszolgáló

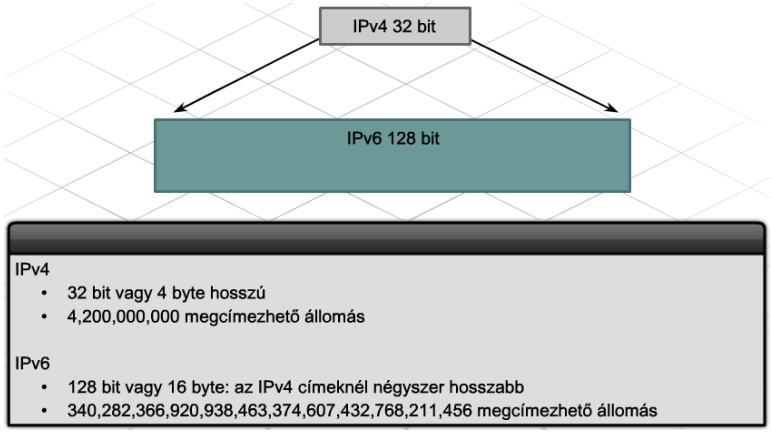
BindDNS-kiszolgáló

6.3 Az IPv4 és az IPv6 leírása

6.3.1 Az IPv4 és az IPv6 címzés összehasonlítása

Az IPv4 címtér megközelítőleg 4,3 milliárd címet biztosít, melyek közül kb. 3,7 milliárd használható, a többi olyan speciális célokra fenntartott, mint például a csoportos címzés, a privát címtér, a loopback tesztelés és a kutatás. A még kiosztható IPv4 címtartományok száma kevés, így néhány internetszolgáltató már megkezdte az IPv6 címek kiosztását.

Az IPv6 cím egy 128 bites bináris érték, amely 32 hexadecimális számmal ábrázolható, és összesen $3,4x10^{38}$ db IP-címet biztosít.



Az IPv6 az IPv4 továbbfejlesztett változata. A fejlesztések közé tartoznak:

- Mobilitás és biztonság
- Egyszerűbb fejrész
- Címformátum

Mobilitás és biztonság

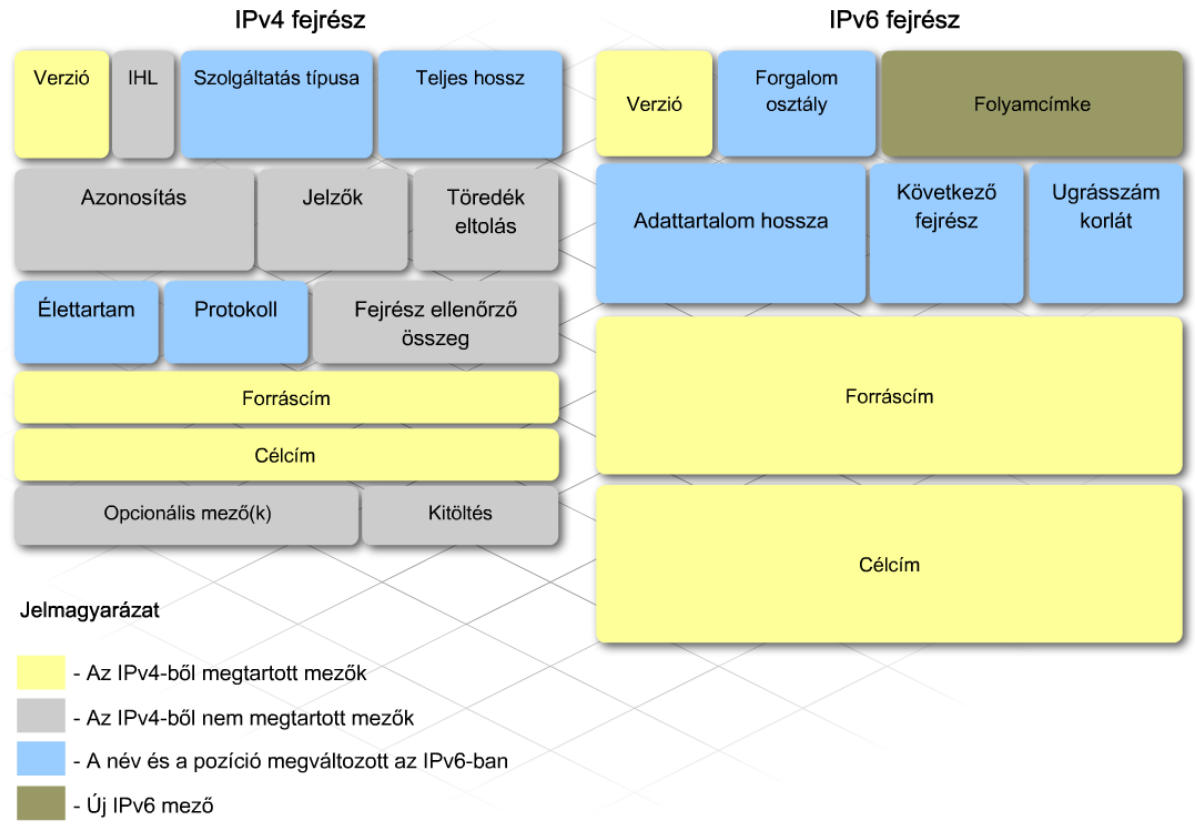
A mobilitás lehetővé teszi a hálózati eszközök hálózaton belüli mozgását. A mobil IP egy IETF szabvány mind az IPv4, mind az IPv6 számára. A szabvány lehetővé teszi a hálózati eszközök mozgását a létrejött kapcsolat megszakítása nélkül. Az IPv4 nem támogatja ezt a fajta mobilitást, ez csak az IPv6 jellemzője.

Az IPSec az IP hálózatok biztonsági szabványa, mely elérhető mind IPv4, mind IPv6 esetén. Az IP hálózati biztonság lehetőségei lényegében megegyeznek mindkét esetben, bár az IPSec mélyebben integrálódott az IPv6 szabványba, és engedélyezhető minden IPv6 állomáson.

Egyszerűbb fejrész

Az IPv6 által használt fejrész az irányítótábla bejegyzések számának csökkentésével növeli a forgalomirányítás hatékonyságát.

Az IPv6 nem használ üzenetszórást. IPv4 esetén az üzenetszórások jelentős forgalmat generálnak a hálózatban, ami úgynevezett üzenetszórási viharokhoz vezethet, és a teljes hálózatot működésképtelenné teheti. Az IPv6 szórásos (broadcast) címek helyett csoportos (multicast) és többszörös felhasználású (anycast) címeket használ.



Címformátum

Az IPv6 címeket nyolc darab, kettőspontokkal elválasztott, 16 bites hexadecimális számmal ábrázoljuk. A címek A, B, C, D, E és F hexadecimális karakterei nem érzékenyek a nagy- és kisbetűkre.

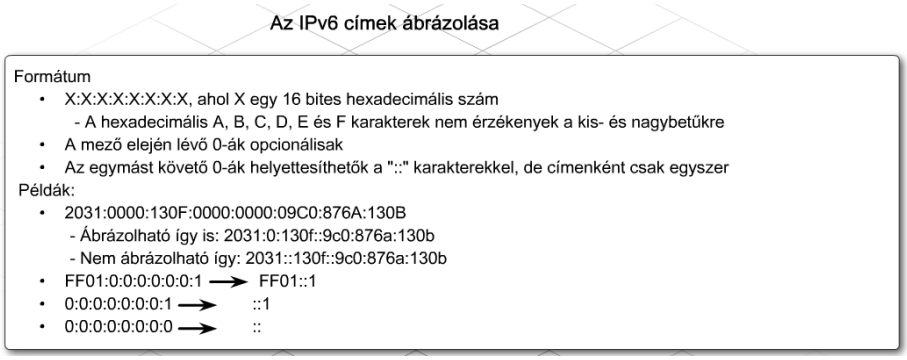
Az IPv4 címekkel ellentétben az IPv6 címek formátuma nem rögzített. Az IPv6 címek jelölésére a következő alapelvek érvényesek:

- A mezők elején található 0-k opcionálisak: A 09C0 ugyanaz, mint a 9C0, és a 0000 megegyezik a 0-val.
- A 0-k egy vagy több csoportja elhagyható, és helyettesíthető a „::” karakterekkel. Egy címben egyetlen „::” karakterkombináció használható.
- Egy nem meghatározott címet a „::” karakterek jelölik, mivel az ilyen cím csak 0-kat tartalmaz.

A „::” jelölés használata jelentősen csökkenti a legtöbb cím méretét. Például az FF01:0:0:0:0:0:0:1 címből FF01::1 lesz. Ez az átalakítás eltér az IPv4 esetén használt 32 bites pontozott decimális jelöléstől. Az IPv6 címek legfontosabb típusát egyedi címnek (unicast) nevezik.

Egyedi címzéskor a csomagok küldése egy konkrét címmel rendelkező konkrét eszközhöz történik. Csoportos (multicast) címzés esetén a csoport minden tagja megkapja a csomagokat, míg többszörös használatú (anycast) cím használatával a csomag az azonos címet használó csoport egyetlen tagjához kerül csak továbbításra. Hatékonysági szempontok miatt egy többszörös

használatú címre küldött csomag a legközelebbi interfészre kerül csak továbbításra, így az ilyen címre, mint “azonosak közül a legközelebbi” típusú címre gondolhatunk.



Az egyedi IPv6 címek alapvető típusai:

- Globális
- Fenntartott (privát, loopback, nem meghatározott)

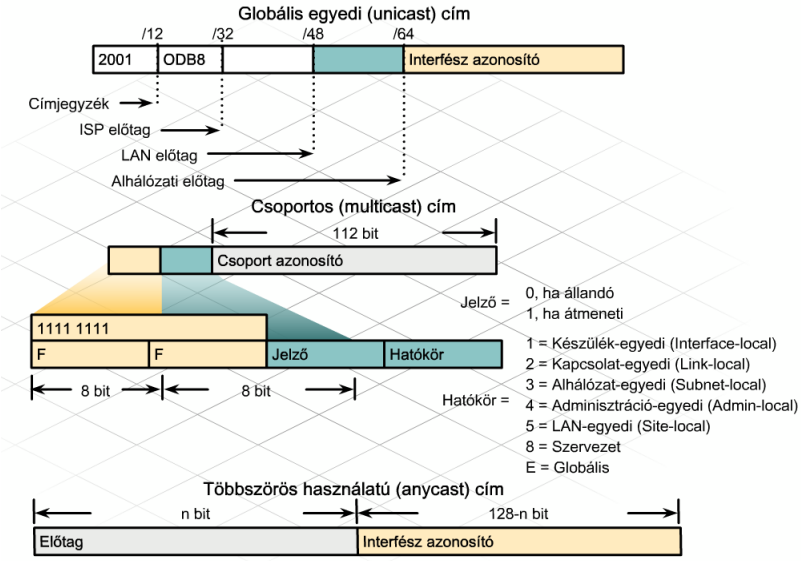
Globális egyedi címek

Az IPv6 állomáscímek egyenértékűek a regisztrált IPv4 állomáscímekkel, és globális egyedi címeknek nevezik őket. A globális egyedi címblokkok felépítése lehetővé teszi a forgalomirányítási előtagok összegzését, mellyel csökkenthető az irányítótábla bejegyzések száma. A globális egyedi címeket a szervezeteken keresztül az internetszolgáltató felé haladva összegzik.

Foglalt címek

Az IETF az IPv6 címek egy részét különböző felhasználási célokra tartja fenn. Az IPv4-hez képest az IPv6 jelentősen több foglalt címet használ, a címek 1/256-oda foglalt cím. Néhány más típusú IPv6 cím, mint például a privát és loopback cím is ezekből a címekből való.

Az IPv4 címekhez hasonlóan az IPv6 címek egy csoportja is privát címzésre van fenntartva. A privát címek első oktettjének értéke a hexadecimális FE, a következő hexadecimális szám pedig 8 és F között van.



6.3.2 Áttérés IPv4-ről IPv6 címekre

Áttérési módszerek

Egy IPv6 rendszer meglévő IPv4 hálózatba történő integrálására különböző módszerek léteznek. Az IPv4-ről IPv6-ra történő teljes áttérést nem szükséges egyszerre elvégezni. A három leggyakoribb módszer:

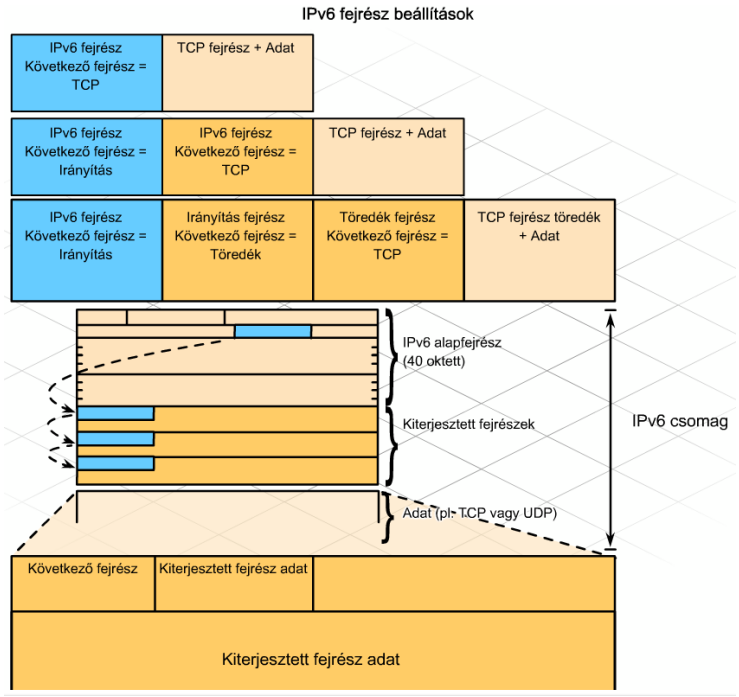
- Kettős protokollkészlet
- Alagúttechnika (tunneling)
- Proxy használata és címfordítás

Kettős verem esetén mind az IPv4, mind az IPv6 konfigurációt létre kell hozni a hálózati eszközön. Mindkét protokoll egyidejűleg fut ugyanazon az eszközön, és lehetővé válik az IPv4 és IPv6 együttes működése.

Az alagúttechnika az IPv6 terjedésével egyre jelentősebb szerephez jut. Az alagúttechnika egy protokoll csomagjának beágyazása egy másik protokollba. Például egy IPv6 csomag beágyazható egy IPv4 protokollba. Többféle IPv6 és IPv4 beágyazási technika létezik, melyek manuális vagy automatikus konfigurációt igényelnek.

A 12.3(2)T és újabb Cisco IOS verziók tartalmazzák a hálózati cím- és protokollfordítást (NAT-PT - Network Address Translation-Protocol Translation) az IPv6 és IPv4 címek között. Ez a fordítás lehetővé teszi a közvetlen kommunikációt olyan állomások között, amelyek különböző IP-protokoll verziót használnak.

Az IPv4-ről IPv6-ra történő teljes áttérés a közeljövőben még nem várható, bár a világ olyan részein már alkalmazzák, ahol a rendelkezésre álló IPv4 címtartományt már majdnem teljesen kimerítették.



6.3.3 Az IPv6 alkalmazása Cisco eszközökön

Az IPv6 forgalom továbbítása egy Cisco forgalomirányítón alapértelmezetten le van tiltva. Az IPv6 engedélyezéséhez kövessük a következő két alaplépést:

1. lépés: Engedélyezzük az IPv6 forgalom továbbítását az `ipv6 unicast-routing` globális konfigurációs paranccsal.

2. lépés: Konfiguráljuk az érintett interfészeket az IPv6 támogatására.

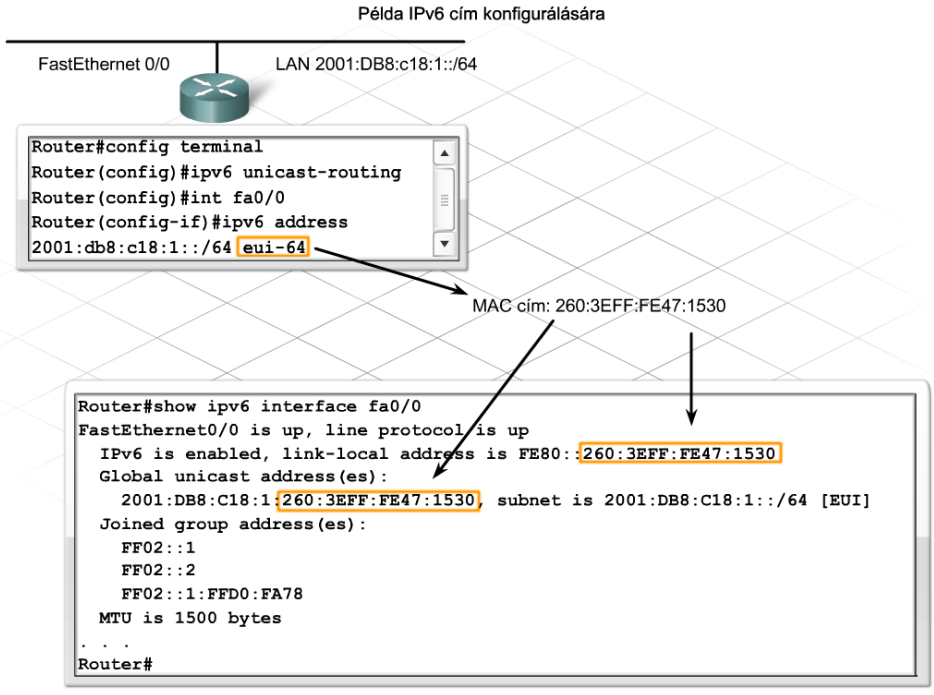
Az IPv6 címek interfészazonosítói az adott kapcsolaton belül azonosítják az interfészeket és az IPv6 cím állomás részeként értelmezhetők. Ezek az azonosítók mindig egyediek, 64 bitesek és dinamikusan levezethetők a 2. rétegben használt beágyazásból és protokollból.

Az IPv6 address parancs egy globális IPv6 cím konfigurálására alkalmas. A teljes 128 bites IPv6 cím megadásához `az ipv6 address ipv6-address/prefix-length` parancs használható:

```
RouterX(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
```

Másik módszerként megadható a cím hálózati részének EUI-64 azonosítója. Ethernet hálózaton az állomás azonosítója az eszköz MAC-címének EUI-64 formátumú változata. Ez a módszer az `ipv6 address ipv6-address/prefix-length eui-64` paranccsal konfigurálható:

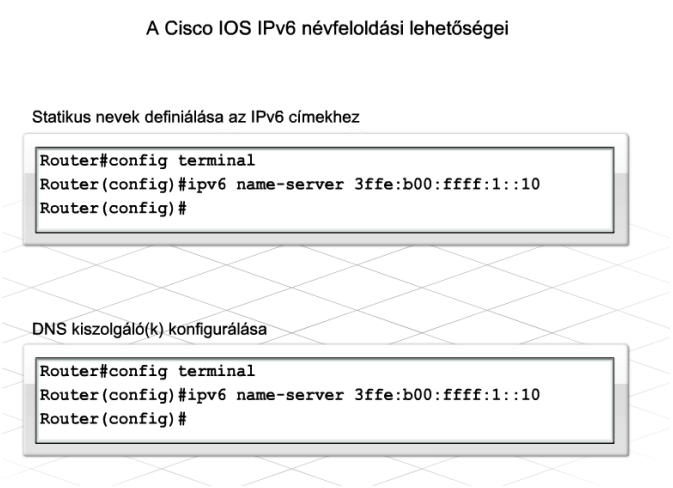
```
RouterX(config-if)# ipv6 address 2001:DB8:c18:1::/64 eui-64
```



Amennyiben egy forgalomirányítót úgy kell konfigurálni, hogy képes legyen az állomásnevek IPv6 címekre történő fordítására, használjuk az `ipv6 host name ipv6addr` parancsot.

IPv6 címek fordítására alkalmas külső DNS kiszolgáló megadására az `ip name-server address` parancs szolgál.

A forgalomirányítón a névfeloldás a szakemberek kényelmét szolgálja, mivel így a forgalomirányítóról nevek segítségével érhetők el más hálózati eszközök. Mindez semmilyen hatással nincs a forgalomirányító működésére, és a DNS kiszolgáló címe sem kerül be a DHCP ügyfeleknek küldött hirdetésekbe.

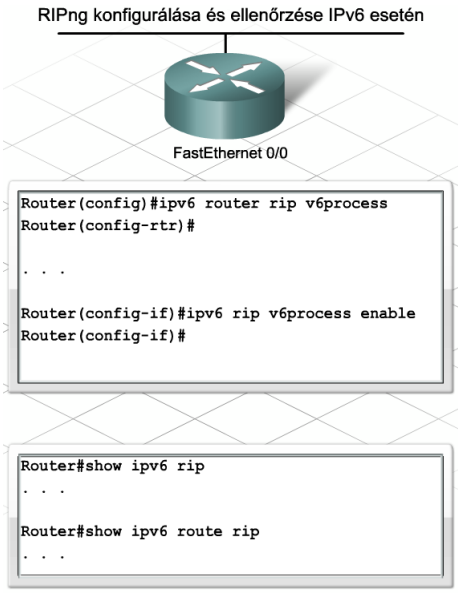


RIPng konfigurálása és ellenőrzése IPv6 esetén

A RIPng konfigurálása IPv6 és IPv4 esetében hasonló, de azért jelentős különbségeket is tartalmaz. Az IPv4 a `network` paranccsal határozza meg az útvonalfrissítésekben szereplő interfészeket, míg az IPv6 esetében az interfész konfigurációs módbeli `ipv6 rip tag enable` parancs engedélyezi a RIPng-t egy interfészen.

Az `ipv6 rip enable` parancsnál használt `tag`-nak és az `ipv6 router rip` parancs tag paraméterének meg kell egyeznie.

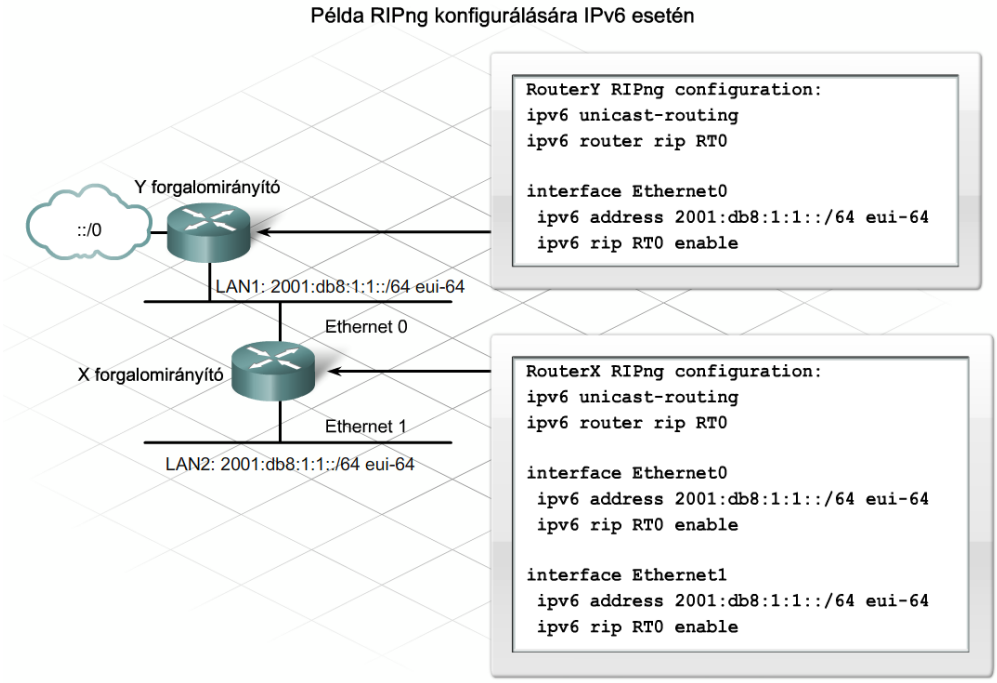
A RIP konfiguráció ellenőrzésére használjuk a `show ipv6 rip` vagy `show ipv6 route rip` parancsot. A RIP-nek egy interfészen történő engedélyezésével automatikusan létrejön egy rip forgalomirányítási folyamat.



RIPng konfiguráció IPv6 esetén

Közvetlenül kapcsolódó hálózatok konfigurálásakor az `ipv6 rip name enable` parancs használható.

Ha egy hálózaton két forgalomirányító kapcsolódik egymáshoz, mindkettő ugyanazt a nevet, például az `RT0`-t, fogja használni a RIPng folyamat azonosítására. A forgalomirányítók Ethernet interfészén a RIPng engedélyezésére ebben az esetben az `ipv6 rip RT0 enable` parancs szolgál.



6.4 A fejezet összefoglalása

- Az IP-címkiosztás megtervezése és dokumentálása az alábbiak miatt szükséges:
  - Címismétlések elkerülése
  - Hozzáférés biztosítása és felügyelete
  - Biztonság és teljesítmény ellenőrzése
  - Moduláris tervezés támogatása
  - Útvonalösszegzést alkalmazó, méretezhető megoldás támogatása
- A megfelelően tervezett hierarchikus IP-címzési séma egyszerűbbé teszi az útvonalösszegzések létrehozását is.
- Útvonalösszegzések alkalmazásához a hálózatnak folytonos alhálózatokat kell tartalmaznia. Folytonos hálózat esetén minden alhálózat szomszédos az ugyanabban a hálózatban lévő többi alhálózattal.
- VLSM használatakor nem szükséges, hogy egy szülőhálózat minden alhálózata ugyanannyi állomáscímmel és azonos előtaghosszal rendelkezzen.
- Az osztály nélküli protokollok útvonalfrissítéseikben az irányítási információk között elküldik az előtag hosszát is, ezzel lehetővé teszik, hogy a forgalomirányítók az alapértelmezett maszkok nélkül határozzák meg a cím hálózati részét.

- A CIDR az osztály alapú határok okozta korlátok megszüntetésével lehetővé teszi az útvonalösszegzést az alapértelmezett maszknál rövidebb, változó hosszúságú alhálózati maszkok (VLSM – Varable Length Subnet Mask) segítségével.
- A változó méretű hálózatok és alhálózatok összetett hierarchiáját egy előtagcím segítségével különböző pontokon lehet összegezni.
- Rugalmas, méretezhető IP-címzési séma tervezéséhez egy tervező a következő ötlépéses folyamatot követi:
    - 1. lépés: A címek kiosztása előtt a teljes címzési sémát megtervezi.
    - 2. lépés: Figyelembe veszi a hálózat jelentős növekedését.
    - 3. lépés: A címzést a központi hálózat összegzett címeivel kezdve halad kifelé a hálózat határa felé.
    - 4. lépés: Meghatározza a statikus címet igénylő gépeket és eszközöket.
    - 5. lépés: Megállapítja, hol és hogyan kell dinamikus címzést megvalósítani.
- A kiválasztott irányító protokollnak támogatnia kell a VLSM címzést és az útvonalösszegzést.
- Az EIGRP lehetővé teszi az osztály nélküli útvonalösszegzést az alapértelmezettől eltérő maszkok segítségével. Ezzel csökkenthető az útvonalfrissítések és a helyi irányítótáblák bejegyzéseinek száma.
- A tervező lépésről lépésre osztja ki a címeket az alhálózatoknak, a legnagyobbtól a legkisebb felé haladva.
- Egy jó hálózati névrendszer megkönnyíti a hálózat irányítását és a felhasználók eligazodását.
- Az RFC 1878 szerint a 0-s és 1-s alhálózatok kizárása már elavult gyakorlatnak tekinthető. A modern programok már alkalmasak minden lehetséges hálózat kezelésére.
- A hatalmas 128 bites címtérnek köszönhetően az IPv6 gyakorlatilag végtelen sok címet biztosít.
- Az IPv6 címeket nyolc darab, kettőspontokkal elválasztott, 16 bites hexadecimális számmal ábrázoljuk.
- Az IPv6 állomáscímek egyenértékűek a regisztrált IPv4 állomáscímekkel, és globális egyedi címeknek nevezik őket.
- Az IPv4-ről IPv6-ra történő teljes áttérést nem szükséges egyszerre elvégezni. A három leggyakoribb módszer az áttérésre:
    - Kettős verem
    - Alagúttechnika
    - Proxy használata és címfordítás

7. Egy telephelyi hálózat prototípusa

7.1 A terv ellenőrzése teszthálózat segítségével

7.1.1 A teszthálózat célja

Tesztek és próbák

Egy új tervet mindig ajánlott tesztelni, még mielőtt a véglegesítésre és a megvalósítása sor kerülne. A tesztelés bizonyíthatja, hogy a tervben szereplő elképzelések helyesek. Ez a tesztelési szakasz lehetőséget teremt a terv nem megfelelően működő részeinek felderítésére és újratervezésére.

Mivel a stadion hálózatában számos változtatást terveznek, ezért a Hálózat Kft. tervezője a végleges ajánlat előtt ellenőrzi a terv kritikus részeinek működését.

Hálózati terv tesztelésére két ismert módszer alkalmazható:

- **Teszthálózat (protoype network) készítése** – A teszthálózat független a meglévő hálózattól, és a teljes hálózatnak csak azokat a részeit valósítja meg, melyek a vizsgált funkciók és képességek teszteléséhez feltétlenül szükségesek.
- **Próbahálózat (pilot network) telepítése** – A próbahálózat az új funkciók és képességek tesztelését teszi lehetővé a meglévő hálózat egy részének felhasználásával.

Mindkét módszer a terv azon funkcióit teszteli, melyek az elsődleges üzleti célokat szolgáló hálózati képességekre vannak hatással.

Teszthálózat vagy próba közötti választás mérlegelése

teszthálózat	próba
+ A működő hálózattól független + Több, akármilyen valószínűségű meghibásodás hatásának vizsgálata + Bármikor megváltoztatható, mert működése nem érinti a felhasználókat + Jól szabályzott, szimulált körülmények + Nincs kockázat	+ Valós hálózati forgalom + Olyan esetekben jó, amikor fizikai környezet vagy valódi forgalom szükséges a működés meghatározásához + Nem tervezett és előre nem látható helyzetekben tesztelhető a hálózat viselkedése
- Nincsenek valóságos körülmények - Nincs annyi lehetőség	- Nehézkesen irányítható - A felhasználókkal egyeztetve kell megvalósítani - Nem rugalmas - Nagyon érzékelhető és kockázatos

A tesztelési módszer megválasztása

Annak eldöntéséhez, hogy teszthálózatot vagy próbahálózatot alkalmazzunk-e, az alábbi tényezőket kell figyelembe venni:

- A szükséges tesztelés típusa
- A próbahálózat megvalósítása miatt milyen üzemzavar következhet be a meglévő hálózaton.

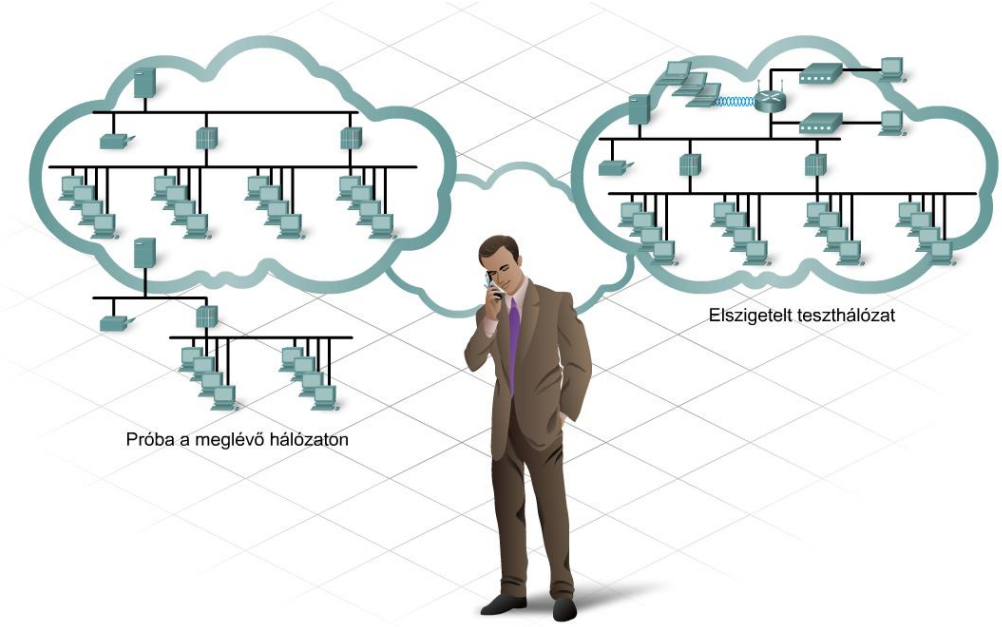
Egy teszthálózatot általában könnyű összeállítani és ellenőrizni, mivel ez aktív hálózati felhasználókat nem érint. Ebben az esetben könnyen eltávolíthatók az eszközök, megváltoztatható a hardver vagy a konfiguráció, és különböző feltételek mellett újra meg újra elvégezhetők a tesztek. Próbahálózat alkalmazása esetén ezek a tevékenységek komoly problémákat idézhetnek elő a hálózatban.

Mikor alkalmazható próbahálózat?

A tervezett hálózat számos funkciója ellenőrizhető teszthálózat alkalmazásával. Mindemellett a próbahálózat is jó megoldást jelent az alábbi körülmények mellett:

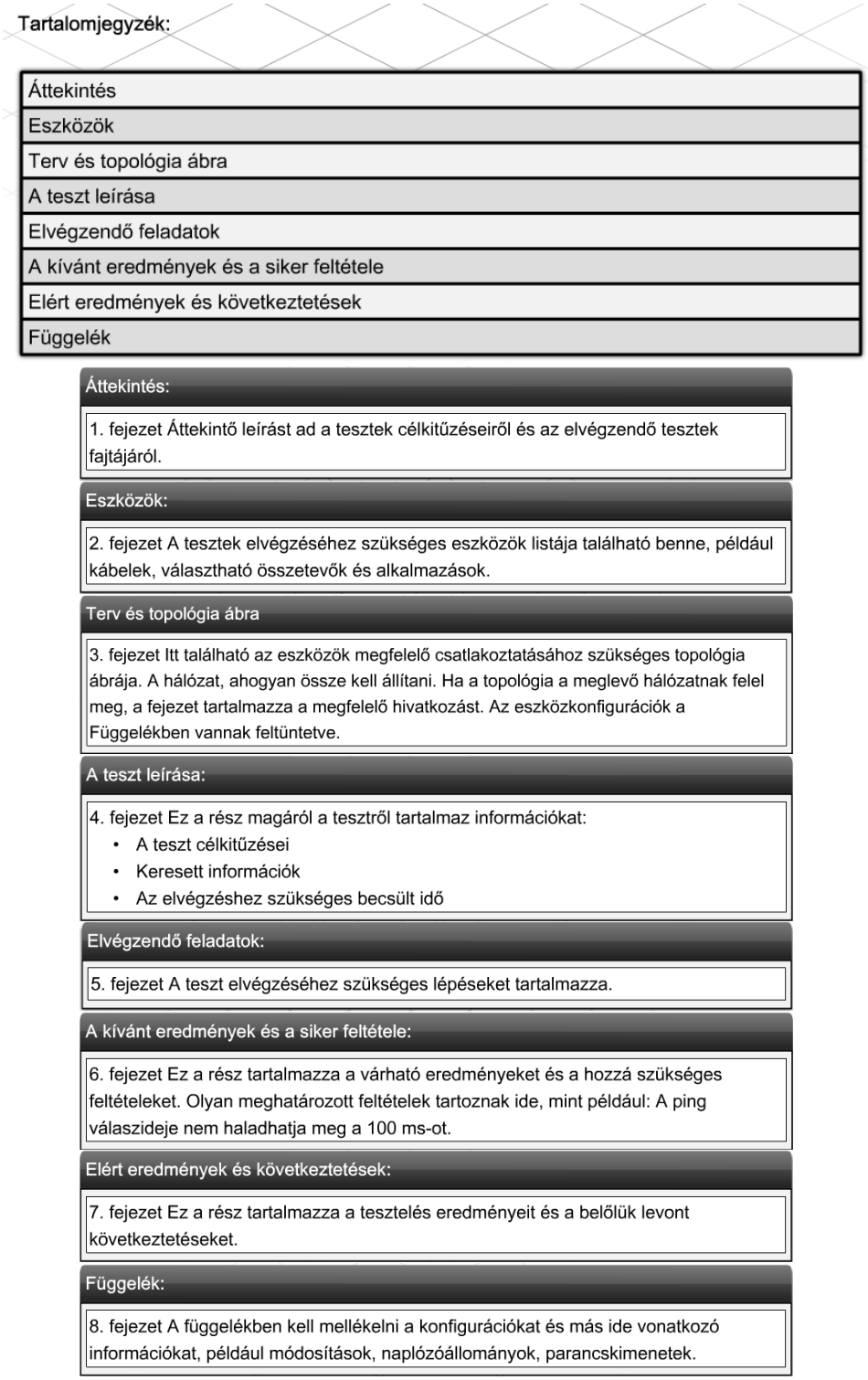
- **A teszthálózat nem elég nagy a működés ellenőrzéséhez** – száz forgalomirányítót tartalmazó hálózat irányítóprotokolljának tesztelése nem valósítható meg teszthálózat alkalmazásával.
- **A hálózat teljesítménye egy adott eszköz működésétől vagy harmadik féltől származó technológiától függ** – Egy nagy értékű videó eredményjelző tábla vagy harmadik féltől származó WAN összeköttetés alkalmazása például ilyen helyzetet teremt.

A távoli telephelyekkel kialakított Frame Relay összeköttetés az egyetlen olyan fontos változtatás a tervben, mely próbahálózat alkalmazását igényli. A próbahálózattal könnyen tesztelhető az aktuális kapcsolat minősége, illetve az eszköz beállítása és működőképessége.



7.1.2 Tesztelési terv készítése

Egy hálózat ellenőrzésére megépítendő teszthálózat komoly tervezést igényel. A hálózattervező szakember az egyértelmű és mérhető teszteredmények érdekében a folyamat megkezdése előtt tesztelési tervet készít. A tesztelési terv több részből álló dokumentum.



7.1.3 A célok és követelmények teljesülésének ellenőrzése

A teszthálózat elkészítésének előnyei

A hálózati terv teszthálózattal történő ellenőrzésének fontos szerepe van, mivel szemlélteti az üzleti célok és technikai követelmények teljesülését mind a megrendelő, mind pedig a tervező számára. Lehetőséget nyújt továbbá több tervezési megoldás összehasonlítására, és a legmegfelelőbb kiválasztására.

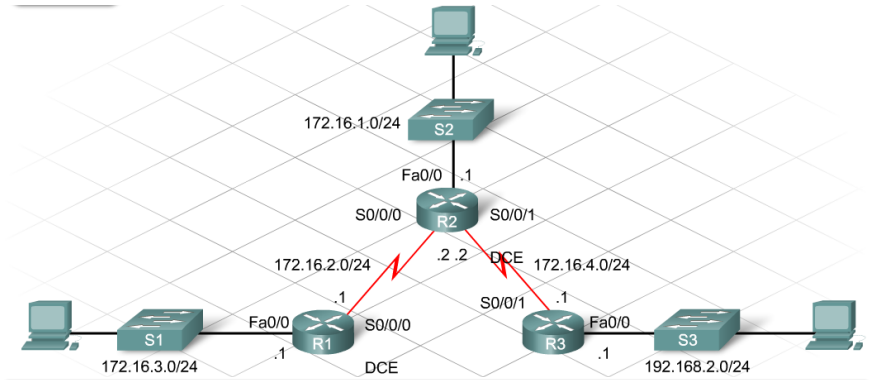
Az egyes hálózati funkciók tesztelésének megkezdése előtt a Hálózat Kft. szakemberei összeállítják és ellenőrzik a teszthálózatot. Ezután a tervező a Hálózat Kft. szakembereivel együttműködve elkészíti a tesztelési tervet. Megvitatják, hogy különböző körülmények mellett milyen módszerek alkalmazhatók a teszthálózat működésének vizsgálatára.

Alapszintű kapcsolatok

Az összes eszköz csatlakoztatása után a szakemberek ellenőrzik, hogy a teszthálózat alapszintű összeköttetései megfelelően működnek-e. Ez abban az esetben tekinthető megfelelőnek, ha a hálózat működik, és az eszközök képesek adatok küldésére és fogadására. Bár a kapcsolatok ellenőrzése általában nem része a szűkebb értelemben vett tesztelési tervnek, de ez teszi lehetővé a további tesztelések elvégzését.

Az alapszintű kapcsolatok ellenőrzésére használt módszerek a következők:

- A hálózati kártya és a hálózati eszközök LED jelzőfényeinek szemrevételezése.
- Konzolkapcsolatok létrehozása az interfészek állapotának ellenőrzésére.
- Információ gyűjtése a közvetlenül csatlakozó eszközökről `show` parancsok segítségével. A forgalomirányító `show` parancsait (pl. `show cdp neighbors`, `show ip arp`) gyakran alkalmazzák a közvetlenül csatlakozó eszközök vizsgálatára.




```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Fas 0/0            140          S I      WS-C2960-2Gig 0/1
R2               Ser 0/0/1          173        R S I      Cisco 1841Ser 0/0/1
R3#
```

```
R3#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.2.2             3   0007.951e.6679  ARPA   FastEthernet0/0
Internet  192.168.2.1             -   001b.53d0.fa78  ARPA   FastEthernet0/0
R3#
```

A működés ellenőrzése

A teszthálózat konfigurálását követően megkezdődhet a működés ellenőrzése. A üzleti célok határozzák meg azt, hogy milyen típusú hálózati tesztekre van szükség. A hálózattervező

összehangolja az egyes üzleti célokat a technikai követelményekkel. Ez a munka megfelelő alapot biztosít a hálózat teljesítményének szemléltetésére leginkább alkalmas módszer kiválasztásához.

A tesztelési módszer kiválasztása

A stadion vezetőségének elsődleges célja, hogy a stadion rendezvényeinek látogatói biztonságban legyenek és pozitív élményekkel távozzanak.

Az e célokat támogató technikai követelmények egyike például a biztonsági kamerákból álló megfigyelő hálózat beillesztése a stadion helyi hálózatába.

Annak bizonyításához, hogy az elvárások valóban teljesülnek, lehetővé kell tenni a biztonsági videofelvételek megtekintését a hálózat egy más részén elhelyezett asztali számítógépen. A teszthálózatnak bizonyítania kell, hogy a felvételek csak az erre jogosult állomásokról tekinthetők meg. A tervező felsorolja, hogy milyen teendőkre van szükség ennek a megvalósításához:

- Elérési rétegbeli VLAN-ok létrehozása a felügyeleti videó forgalomnak a többi hálózati forgalomtól való elszigetelésére.
- Olyan IP-címzési séma kialakítása, mely támogatja a videó hálózati VLAN-okat.
- Trönkvonal megvalósítása a VLAN-ok és az elosztási réteg eszközei között.
- A videó folyamok feltöltése a videó felügyeleti kiszolgálóra.
- Hozzáférési listák konfigurálása annak érdekében, hogy a biztonsági felvételek a stadion egyes területeiről az engedélyezett felhasználók számára megtekinthetők legyenek, de a vendég felhasználók ne férhessenek hozzá.
- Hitelesítési rendszer megvalósítása a videó felügyeleti kiszolgálón annak érdekében, hogy a biztonsági felvételekhez csak az engedéllyel rendelkező személyek férhessenek hozzá.

A helyes hálózati beállítások és konfigurációk biztosításához a tervező ellenőrző listát is készít. A végponttól végpontig terjedő kommunikációhoz minden egyes összetevőnek megfelelően kell működnie.

Hálózati működés	Tesztelési módszerek
A forgalom elszigetelése VLAN-okkal az IP kamerák támogatása érdekében.	VLAN létrehozása és kamera telepítése (vagy kamerát szimuláló számítógép). VLAN konfiguráció ellenőrzése a kapcsolón. Wireshark alkalmazással a csomagok vizsgálata.
VLAN trönkölése az elosztási réteg felé.	Trönkkapcsolat létrehozása az elosztási réteg eszközéhez. A trönk működésének ellenőrzése.
A kamerák IP-címének beállítása és elérése.	A hálózati terv alapján az eszközök IP-címének beállítása. Ping segítségével a konfiguráció ellenőrzése.
EIGRP használatával a forgalomirányítás megvalósítása.	EIGRP konfigurálása a VLAN-ok forgalmának irányítására. A show parancsok, a ping és a trace route segítségével a forgalomirányítás ellenőrzése.
Hozzáférési listák alkalmazása a jogosult megfigyelő állomások engedélyezésére.	Hozzáférési listák konfigurálása és alkalmazása annak érdekében, hogy csak a kiválasztott megfigyelő állomások érhessék el a kamerákat. Tesztelés ping segítségével és a hozzáférési listák naplózása.
A végponttól végpontig terjedő alkalmazások teljesítményének ellenőrzése.	A hálózat területén elhelyezett számítógépen a video kivetítése. A sávszélesség használatával és a videoforgalom minőségével kapcsolatos információk összegyűjtése. Forgalomszimulációs program segítségével fogalom generálása a hálózaton és a videofogalom vizsgálata.

7.1.4 A LAN technológiák és eszközök ellenőrzése

A teszthálózatok teljesítményének elemzésére általánosan elfogadott eszközök állnak rendelkezésre.

Cisco IOS parancsok

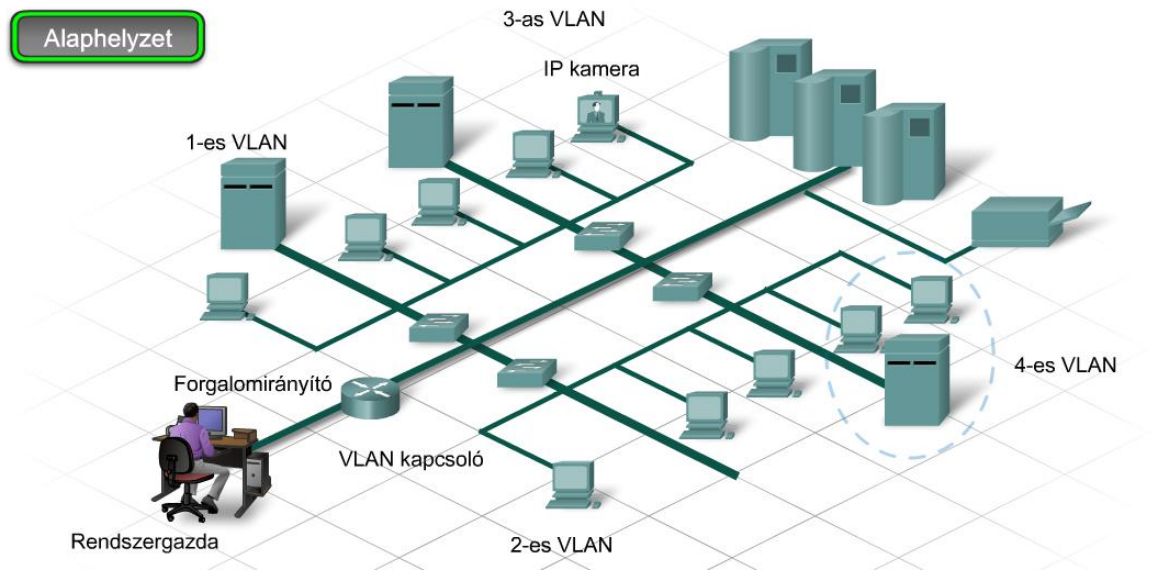
Egy hálózat működésének és teljesítményének különböző szempontok szerinti vizsgálata a Cisco IOS `show` és `debug` parancsainak alkalmazásával végezhető el. A show parancsok megjelenítik az interfészek állapotát, a protokollokat, az irányítótáblákat, a CPU- és memóriahasználatot, valamint számos más jellemzőt. A debug parancsok lehetővé teszik a hálózattervező és a Hálózat Kft. dolgozói számára az információáramlás folyamatának valós idejű vizsgálatát. Az alkalmazások naplózási funkcióival (software logging) az értékes adatok későbbi elemzés céljából elmenthetők és megjeleníthetők.

IP segédprogramok és eszközök

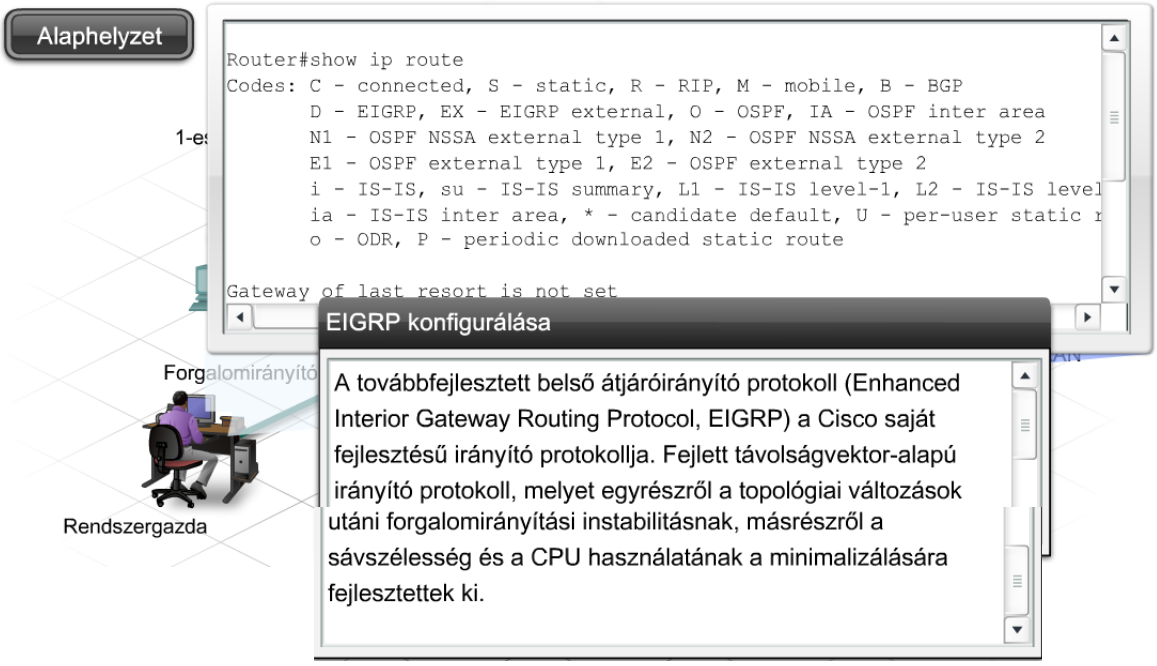
A két legismertebb hálózati kapcsolatokat és elérhetőséget ellenőrző parancs a `ping` és a `traceroute`. Számos további segédprogram és eszköz alkalmazható még egy hálózat működésének vizsgálata során. Egy Windows-alapú számítógépen például a `netstat`, az `nslookup`, az `arp` és a telnet segítségével ellenőrizhetők az összeköttetések, és megjeleníthetők az adatok.

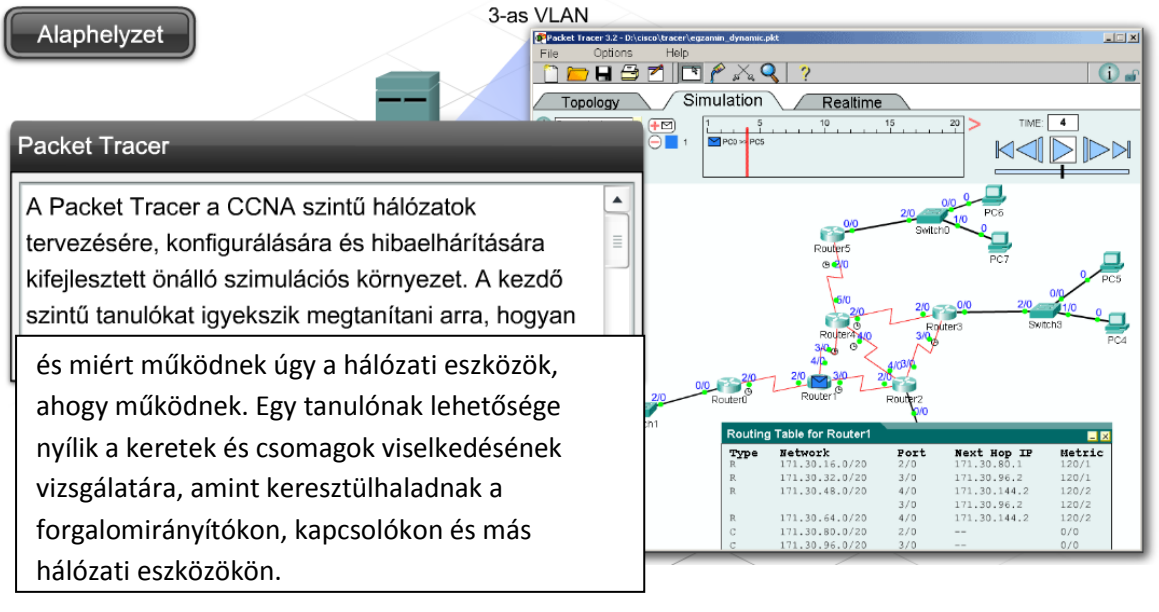
Protokollelemző programok

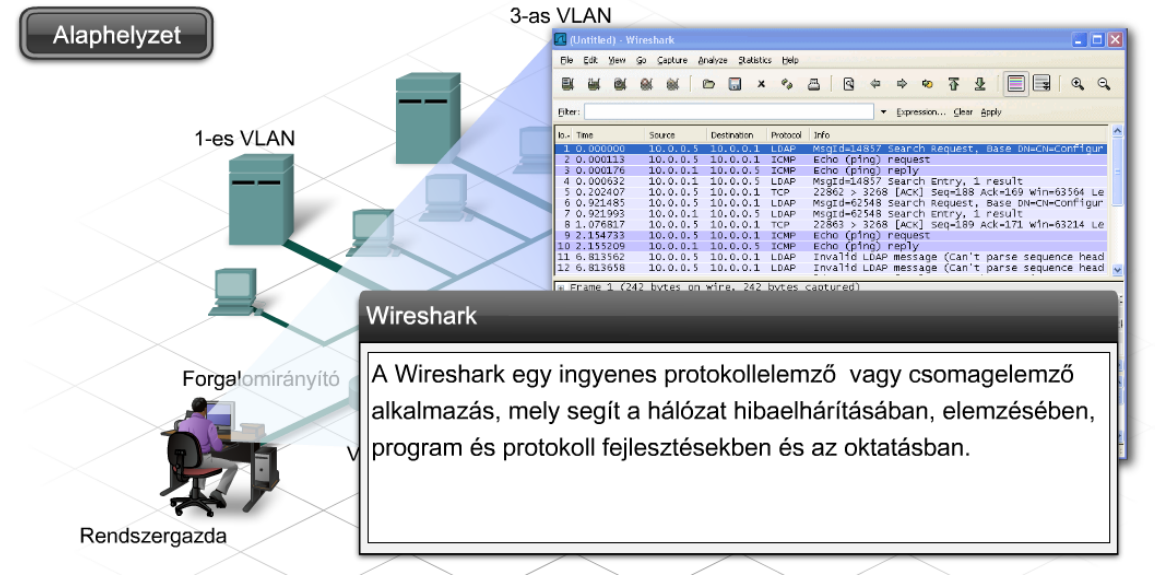
Teszthálózatokban protokollelemző programokkal ellenőrizhető, hogy a csomagok és keretek megfelelő tartalommal rendelkeznek-e. A protokollelemzők segítenek felderíteni az olyan típusú forgalom (pl. üzenetszórás, ARP) jelenlétét, amelyet a csomag és keret szintű adatok vizsgálata nélkül nehéz lenne azonosítani.

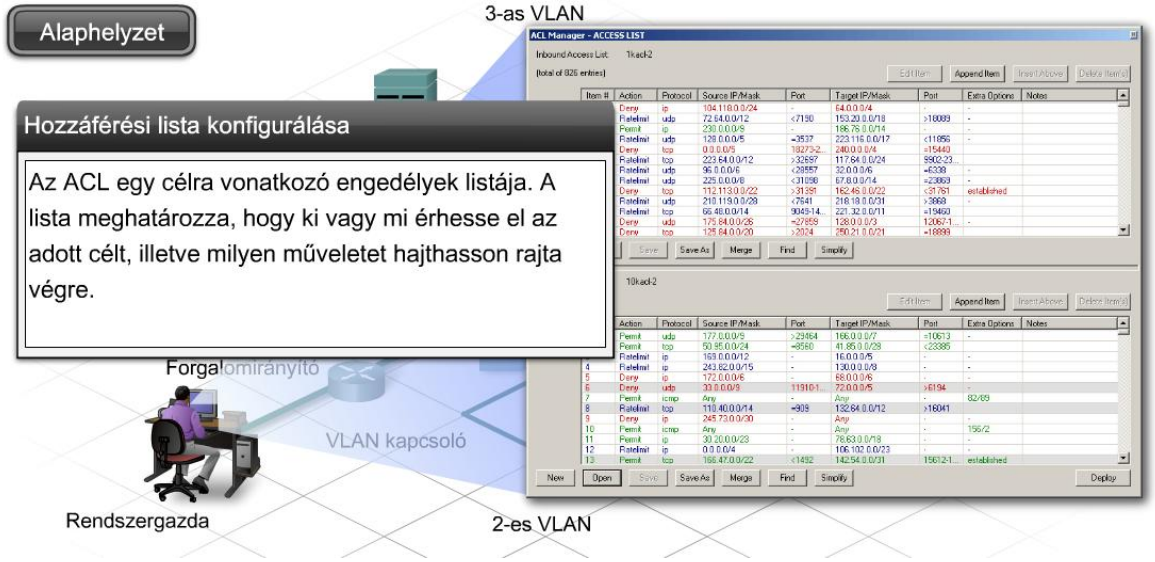



Alaphelyzet
3-as VLAN
1-es VLAN
Camera View
Video megjelenítése
A hálózat területén elhelyezett számítógépen videó kivetítése. A sávszélesség használatával és a videoforgalom minőségével kapcsolatos információk összegyűjtése. Forgalomszimulációs program segítségével fogalom generálása a hálózaton és a videoforgalom vizsgálata.
Rendszergazda

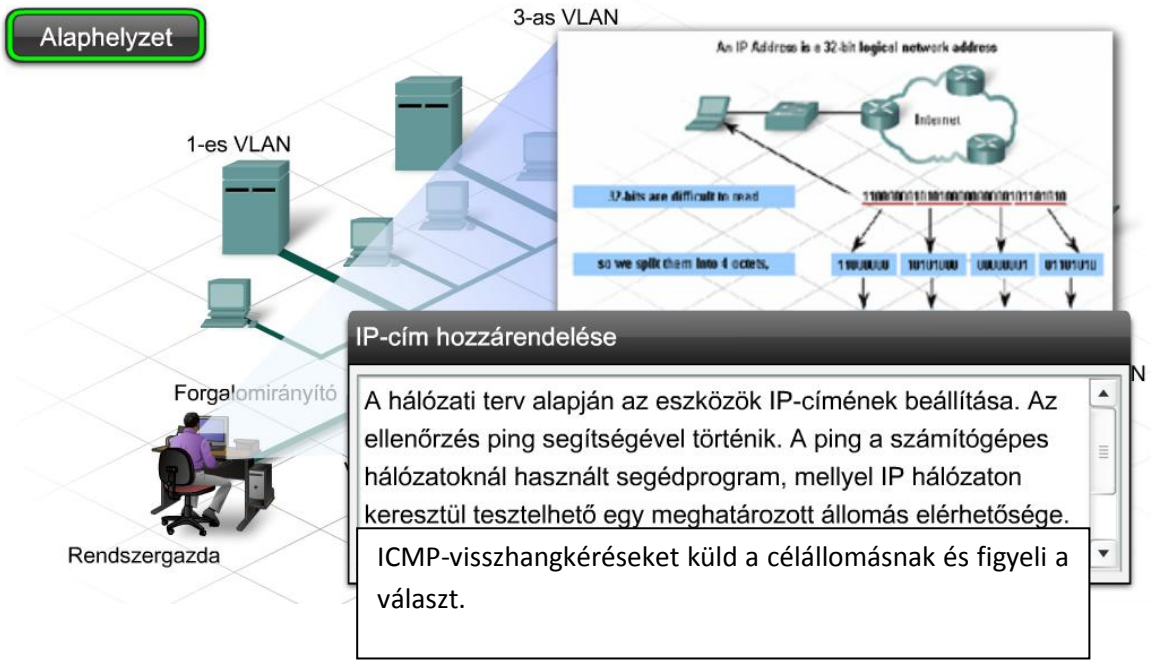

Alaphelyzet
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level
ia - IS-IS inter area, * - candidate default, U - per-user static r
o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
EIGRP konfigurálása
A továbbfejlesztett belső átjáróirányító protokoll (Enhanced Interior Gateway Routing Protocol, EIGRP) a Cisco saját fejlesztésű irányító protokollja. Fejlett távolságvektor-alapú irányító protokoll, melyet egyrészről a topológiai változások utáni forgalomirányítási instabilitásnak, másrészről a sávszélesség és a CPU használatának a minimalizálására fejlesztettek ki.
Rendszergazda


Alaphelyzet
3-as VLAN
Packet Tracer
A Packet Tracer a CCNA szintű hálózatok tervezésére, konfigurálására és hibaelhárítására kifejlesztett önálló szimulációs környezet. A kezdő szintű tanulókat igyekszik megtanítani arra, hogyan és miért működnek úgy a hálózati eszközök, ahogy működnek. Egy tanulónak lehetősége nyílik a keretek és csomagok viselkedésének vizsgálatára, amint keresztülhaladnak a forgalomirányítókon, kapcsolókon és más hálózati eszközökön.
Topology
Simulation
Realtime
Routing Table for Router1


Alaphelyzet
3-as VLAN
1-es VLAN
Forgalomirányító
Rendszergazda
Wireshark
A Wireshark egy ingyenes protokollelemző vagy csomagelemző alkalmazás, mely segít a hálózat hibaelhárításában, elemzésében, program és protokoll fejlesztésekben és az oktatásban.


Alaphelyzet
3-as VLAN
Hozzáférési lista konfigurálása
Az ACL egy célra vonatkozó engedélyek listája. A lista meghatározza, hogy ki vagy mi érhesse el az adott célt, illetve milyen műveletet hajthasson rajta végre.
Forgalomirányító
VLAN kapcsoló
Rendszergazda
2-es VLAN


Alaphelyzet
3-as VLAN
IP kamera
1-es VLAN
Trönkkapcsolat létrehozása
A trönk két pont közötti kommunikációs csatorna. Rendszerint kapcsolóközpontok között nyújt nagy sávszélességű csatornát, melyek egyidejűleg nagy mennyiségű hang és adatjelet kézbesítenek.
Forgalomirányító
VLAN kapcsoló
Rendszergazda
2-es VLAN



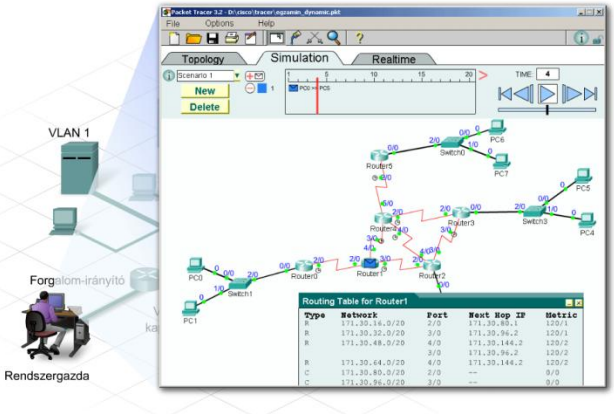
Bizonyos esetekben teszthálózattal nem megvalósítható környezetben kell a hálózat működését ellenőrizni. Ilyenkor a tervező hálózati szimulációs programokat alkalmazhat.

Hálózati szimulációs eszközök

Szoftveres eszközök alkalmazásával az elképzelések szimulált környezetben is ellenőrizhetők. Ezek az eszközök hasonlóak a Networking Academy Packet Tracer programhoz, melynek használata a tanfolyam során engedélyezett. Az ilyen környezetben a vizsgálni kívánt hálózati topológiák és konfigurációk gyorsan létrehozhatók és módosíthatók. A szimulációk segítségével ellenőrizhetők olyan hálózatok is, melyek teszthálózatként megépítve túl költségesek lennének.

A teszthálózatban használt IOS és IP eszközök, illetve segédprogramok a szimulált hálózat tesztelésekor is alkalmazhatók.

A tervező és a Hálózat Kft. szakemberei meghatározzák az egyes hálózati funkciók helyes működésének szemléltetésére szolgáló eszközöket. A `traceroute` például jól alkalmazható eszköz a csomagok hálózatban megtett útvonalának nyomon követésére, de az összevont útvonalak konfigurációjának bemutatására nem alkalmas.



7.1.5 A hálózati redundancia és rugalmasság ellenőrzése

Az eszköz- és kapcsolathibák kiküszöbölése

Amikor egy vállalat folyamatos elérhetőséget igénylő alkalmazásokat használ, a hálózattervező redundáns elemeket ad a hálózathoz. Néhány esetben ezt annak mérlegelése nélkül teszi, hogy mi történik egy valódi meghibásodás, egy adott hálózati hiba esetén. A fentiek miatt fontos ellenőrizni, hogy miként viselkednek a redundáns összeköttetések meghibásodás esetén. Az ellenőrzés során mérni kell, mennyi idő szükséges a hálózat stabilizálódásához a tartalékkapcsolat működésbe lépése után.

Redundáns összeköttetések

A teszthálózatok a redundáns összeköttetések számos típusát alkalmazzák a hálózat rendelkezésre állásának teszteléséhez. A tartalékkapcsolatok nem csak meghibásodás esetén használhatók, hanem megfelelő működés melletti terheléselosztásra is alkalmazhatók.

Terheléselosztás

A redundáns összeköttetések nem minden fajtája támogatja a terheléselosztást, így például az STP működési módjából következően, a 2. rétegbeli kapcsolók közötti redundáns kapcsolatok sem használhatók erre a célra. Normál működés melletti terheléselosztásra azonos költségű, irányított összeköttetések és EtherChannel tagjaként konfigurált 2. és 3. rétegbeli kapcsolatok használhatók. Ezek meghibásodás esetén is képesek a forgalom továbbítására.

A stadion hálózata az eszközök között kétfajta redundáns összeköttetéssel rendelkezik: 2. rétegbeli, felfelé irányuló összeköttetésekkel (uplink), és azonos költségű, 3. rétegbeli összeköttetésekkel.

Ennek a kétfajta összeköttetésnek a teszteléséhez a tervező és a Hálózat Kft. szakemberei kapcsolati hibát idéznek elő a topológiában. A hálózati szolgáltatás kiesési idejének mérésével meg tudják határozni, mennyi idő szükséges a hálózat működésének helyreállásához.

7.1.6 A terv kockázatainak és gyenge pontjainak meghatározása

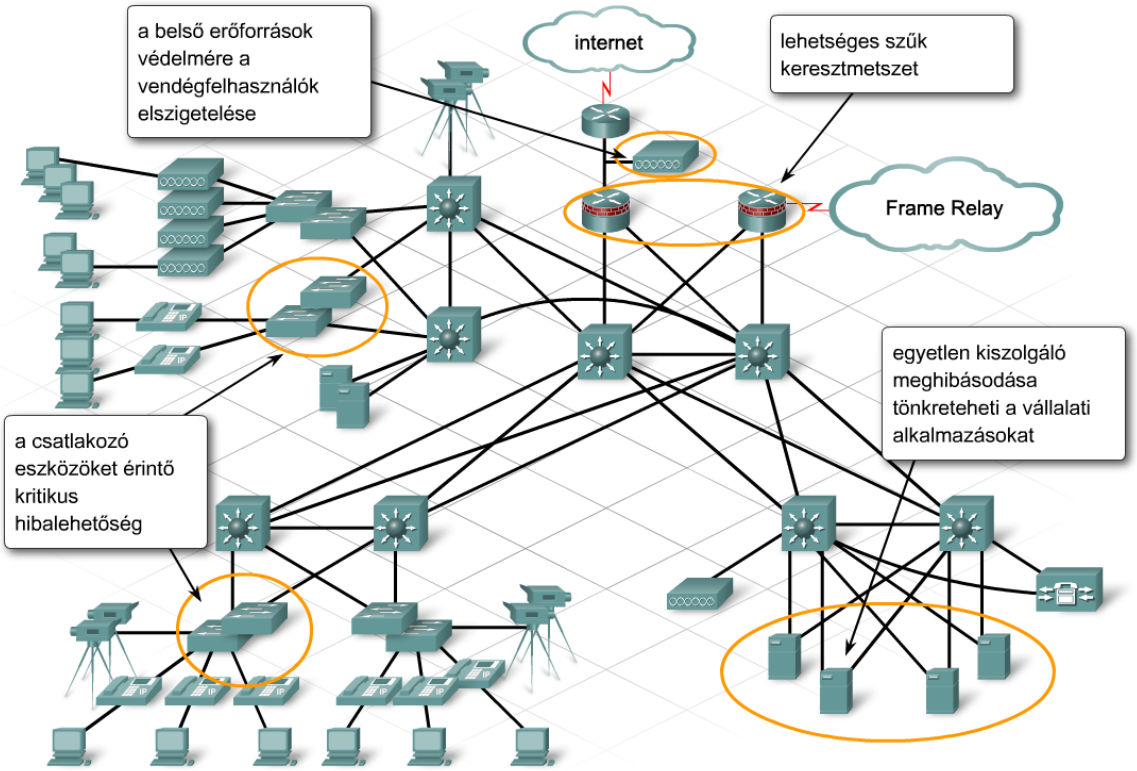
A teszthálózatok és a szimulációk a hálózati tervben rejlő kockázatok és gyenge pontok felderítésére is alkalmasak. Gyenge pontnak számítanak a terv korlátai és hiányosságai, a kockázatok pedig a gyengeségekből fakadó kedvezőtlen következmények. A kockázat nő, ha a hálózat nem optimálisan tervezett területeket is tartalmaz. A korlátozások az eszközök adottságaiból és a korábban felderített megszorításokból származhatnak.

Az alábbiakban felsoroljuk a terv néhány lehetséges gyenge pontját a velejáró kockázattal együtt:

- **Kritikus hibaforrás (Single points of failure)** – Az olyan hálózatrészek esetén, melyek kapcsolataikban korlátozottak vagy amelyek nem tartalmaznak redundáns elemeket, nagy a kockázata annak, hogy egyetlen összeköttetés vagy eszköz meghibásodása az egész hálózatrészre hatással van.

- **Nagy meghibásodási tartomány** – Ha egy kritikus hibaforrás, mint például egy nem redundáns internet kapcsolat, a hálózat egy nagyobb részére van hatással, akkor az ilyen hibából adódó kockázat komoly hatással lehet az üzlet növekedésére.
- **Lehetséges szűk keresztmetszet (bottleneck)** – Bizonyos területeken a forgalom növekedésével torlódások alakulnak ki, aminek következtében emelkedik a válaszidő jelentős növekedésének kockázata.
- **Korlátozott méretezhetőség** – Egyes területek vagy eszközök bővíthetőségi problémákat vethetnek fel, ha a hálózat a vártnál gyorsabban növekszik. Ha egy hálózat nélkülözi a megfelelő rugalmasságot, akkor szükségessé válhat a hálózat újratervezése vagy költséges továbbfejlesztése.
- **A jelenlegi szakembergárda képességei** – Alkalmanként a teszthálózat jelzi, hogy a hálózat konfigurációja túl összetett ahhoz, hogy a jelenlegi alkalmazottak karbantartsák, vagy hibaelhárítást végezzenek rajta. Ilyen esetben a kockázat addig áll fenn, amíg a munkatársak megfelelő képzésben nem részesülnek vagy új karbantartási stratégia nem lép életbe.

A hálózattervező és a Hálózat Kft. szakemberei által a teszthálózat ellenőrzési szakaszában felderített gyenge pontokat az ügyféllel is meg kell beszélni. Fontos rávilágítani a felismert gyenge pontokban rejlő kockázatokra is. A kockázatok feltárása biztosítja az ügyfélnek, hogy lássa mi fog történni a jövőben, ha a hiba ténylegesen is bekövetkezik. Mindez lehetőséget teremt az ilyen helyzetek kezelésére alkalmas rendkívüli intézkedési terv kidolgozására is.



7.2 A helyi hálózat teszthálózata

7.2.1 A helyi hálózati terv követelményeinek és céljainak meghatározása

Az új terv tesztelése

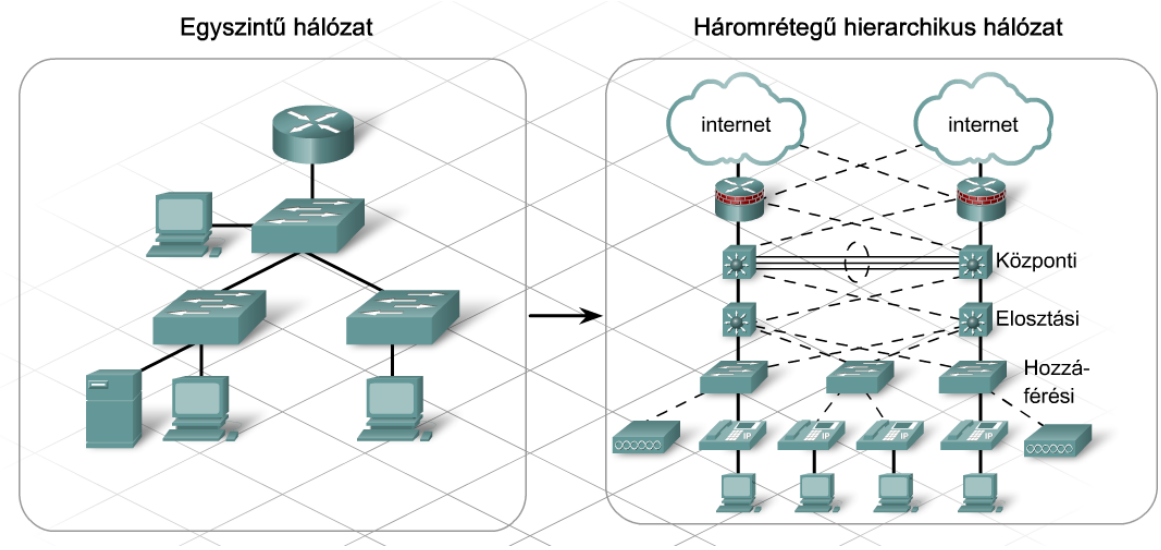
A stadion vezetőségének elsődleges üzleti célja a költségek csökkentése egy konvergens hálózat megvalósításával, mely támogatja az adat-, a videó- és az IP-telefon forgalom átvitelét. Ennek következtében az új terv jelentős változtatásokat tartalmaz a stadion hálózatára vonatkozóan. A hálózat tervezőjének el kell döntenie, hogyan tesztelje a terv különböző elemeit. A kiválasztott teszteknek bizonyítania kell, hogy a fejlesztésben kitűzött célok ténylegesen meg fognak valósulni. A tervező úgy dönt, hogy az ellenőrzést teszthálózat alkalmazásával végzi el.

Mit kell tesztelni?

A tervezőnek először is el kell döntenie, mely hálózati funkciók ellenőrzése szükséges a tesztelés során. Mivel a cél egy olyan hálózat létrehozása, mely támogatja az IP-telefont, az adat- valamint a videó átvitelt, így a hálózati terv azon részeinek az ellenőrzése szükséges, melyek közvetlenül ezt a célt szolgálják.

A stadion hálózata esetében a terv alábbi részeit kell vizsgálni:

- Áttérés az egyszintű hálózatról a moduláris háromrétegű hierarchikus modellre.
- Elkülönített VLAN-ok és IP-alhálózatok kialakítása a különböző típusú forgalmak és a különböző felhasználói csoportok számára.
- Redundáns topológia megvalósítása.
- Hozzáférési listák konfigurálása abból a célból, hogy a stadion erőforrásaihoz csak az arra illetékes felhasználók férjenek hozzá.



7.2.2 A tesztelési terv elkészítése

Miután eldöntötte, milyen üzleti célokat és technikai követelményeket lehet ellenőrizni a teszthálózat segítségével, a tervező elkészíti a tesztelési tervet.

A tesztelési terv

A tervezőnek meg kell mutatnia, hogy az IP-telefon és a videó felügyelet forgalmát egyidejűleg szállító konvergens hálózat megfelelően működik. Ennek érdekében az alábbiakról kell döntenie:

- Milyen típusú tesztet alkalmaz
- A hálózat mekkora részét kell megépíteni a teszt érdekében
- A teszt sikeréből vagy sikertelenségéből mire lehet következtetni

A tervező listát készít azokról a teszteredményekről, melyet a célokban megfogalmazott konvergens hálózatnak teljesítenie kell. A teszt elsődleges szerepe annak bemutatása, hogy az új hálózat mennyiben felel meg a legfontosabb üzleti céloknak. A Hálózat Kft. szakemberei ellenőrzik az egyes technikai követelményeket, hogy lássák, vajon a terv mindenben elérte-e a célját. Ezt a folyamatot megismétlik minden nagy prioritású cél esetén.

Üzleti célkitűzés:	Az általános siker feltétele
A jelenlegi adat- és videófelügyeleti hálózat összekapcsolása, és IP telefon támogatása a stadionban.	A végponttól végpontig terjedő IP kapcsolat, és a szimulált adat, hang és videófelügyeleti forgalom elfogadható minőségű átvitelének a bemutatása.

Technikai követelmények	Az eredményesség feltétele
Méretezhetőség	
Az egyszintű hálózat átalakítása hierarchikus, három rétegű hálózattá	Sikeres ping, telnet és adatátvitel
Különálló VLAN-ok és IP alhálózatok létrehozása a különböző típusú forgalom támogatására	A VLAN-ok elszigetelik a forgalmat, ami a sikertelen ping és IOS **show** parancsok kimeneteiből látszik.
Rendelkezésre állás	
2. rétegbeli kapcsolatok helyett 3. rétegbeliek alkalmazása	Kapcsolati hiba utáni gyors helyreállás
Redundáns topológia megvalósítása	Meghibásodott kapcsolatok ne állítsák le a hálózatot
Biztonság	
Szűrők beállítása annak biztosítására, hogy csak az arra jogosult alkalmazottak férhessenek a videófelügyelethez	Jogosulatlan állomások ne férjenek a videóhálózathoz
A kapcsolón portbiztonság beállítása	Ismeretlen MAC címmel ne lehessen csatlakozni
Felügyelhetőség	
Felügyeleti VLAN létrehozása és SSH konfigurálása	Minden eszközzel lehessen kialakítani SSH kapcsolatot

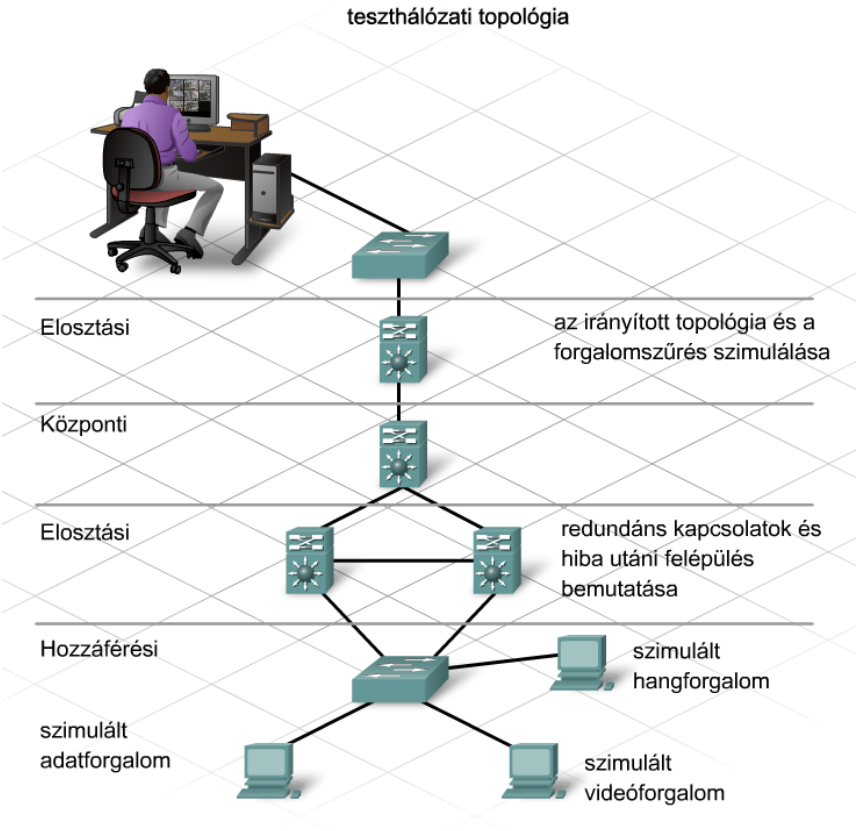
Tesztelés egyszerű minta topológia alkalmazásával

A hálózattervező elkészíti a stadion hálózati topológiájának megfelelő teszthálózatot, mely elég nagy a tervezett hálózat működésének bemutatásához.

A háromrétegű hierarchia szimulálása

A teszthálózatban a háromrétegű hierarchia szimulálásához két 2. rétegbeli és négy 3. rétegbeli eszközt kell használni. A tervező 2. rétegbeli kapcsolókat választ az elérési réteg, illetve 3. rétegbeli kapcsolókat vagy forgalomirányítókat az elosztási és a központi réteg szimulálásához. A tesztelési tervben felsorolja a felhasznált eszközöket, és azt is, hogy szükség esetén mivel helyettesíthetők.

Annak érdekében, hogy a Hálózat Kft. szakemberei is nyomon követhessék, hogy a teszthálózat megfelelően van megépítve, a tervező ellenőrzőlistát készít számukra. Az ellenőrzőlista tartalmazza az összes olyan funkciót, melyek működése szükséges a teszt megkezdéséhez, továbbá minden olyan tervezett változtatást a konfigurációra vonatkozóan, melyre a tesztelés folyamán sort kell keríteni.



7.2.3 A topológia és az eszközök kiválasztásának jóváhagyása

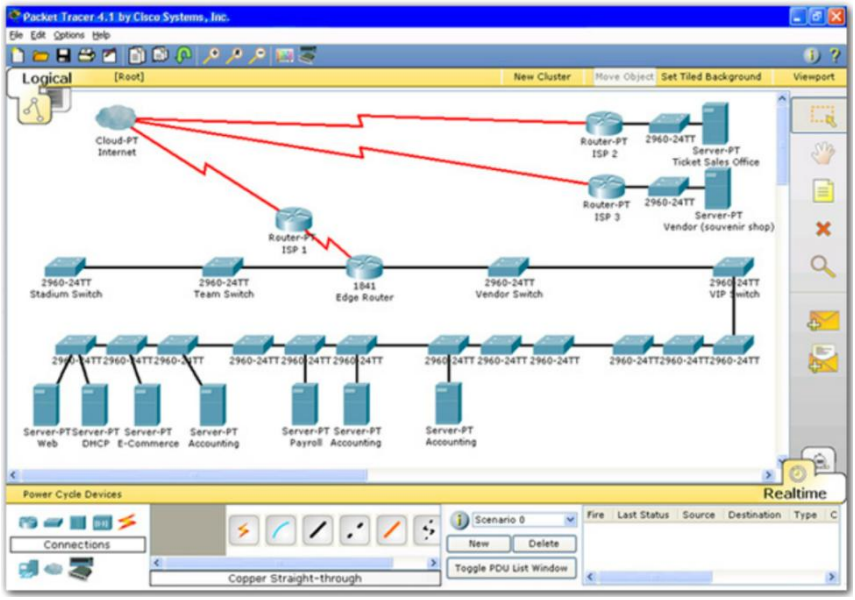
A stadionnak jelenleg egyszintű, kapcsolt, forgalomirányítás és forgalomszűrés nélkül működő hálózata van. A hálózattervező a 2. rétegbeli kapcsolt hálózat kibővítését javasolja hierarchikus, 3. rétegbeli szolgáltatások hozzáadásával. Az új hálózat tartalmazza az elosztási és központi réteget is. Ezekkel a változtatásokkal a tervező a bővíthetőséggel és a rendelkezésre állással kapcsolatos követelmények teljesülését segíti elő.

Az irányított és az egyszintű topológia összehasonlítása

A tervező be akarja mutatni az egyszintű és a hierarchikus topológia közti különbséget egy összeköttetés meghibásodása esetén. A bemutató segít annak megértésében, miért jobb választás az irányított, hierarchikus topológia.

Az új hálózat moduláris, hierarchikus terve lehetővé teszi az elérési réteg kialakítását anélkül, hogy ez a meglévő felhasználókra hatással lenne. A megfelelő működést csak egy nagy teszthálózat felépítése tudná igazolni. Mivel ez nem célszerű, a tervező teszthálózat felépítése helyett szimulációs eszközökkel mutatja be a lehetséges előnyöket. A szimulációs eszközök az irányított, hierarchikus topológia kiválasztásának jóváhagyásában segítenek.

A tervező elkészíti a szimuláció tesztelési tervét, mely megegyezik a teszthálózat tesztelési tervével.



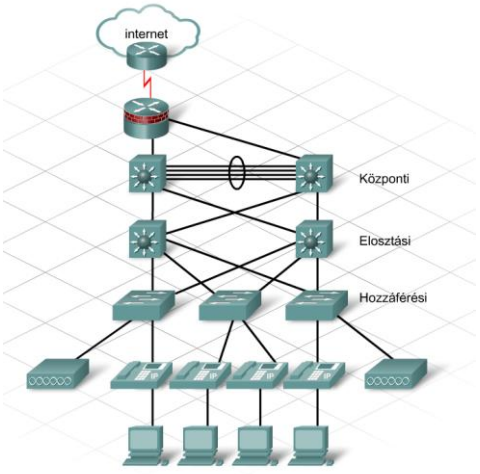
7.2.4 Az irányítóprotokoll kiválasztásának ellenőrzése

Az irányítóprotokoll tesztelése

A stadion hálózatának előzetes hierarchikus tervében dinamikus irányítóprotokollként az EIGRP protokoll szerepel. A hálózattervező azért ezt ajánlja, mert használata egyszerű és jól bővíthető. Az EIGRP a Cisco saját fejlesztésű protokollja; nem Cisco eszközökön nem használható.

A vonalszakadások esetén előálló forgalomirányító-protokoll konvergenciát nagyon kockázatos egy tényleges hálózaton vizsgálni, de még kísérleti hálózatokon is problémás feladat. A próbák során az irányítóprotokoll kisebb félrekonfigurálása is tönkreteheti a teljes hálózatot. A kockázat miatt a tervező úgy dönt, hogy a forgalomirányítás ellenőrzését szimulátor segítségével végzi.

A tervező szeretné összehasonlítani a redundáns összeköttetéseken a statikus forgalomirányítás és az EIGRP irányítóprotokoll használatát. A tesztelési terv szerint először a statikus útvonalakat, majd az EIGRP konfigurációját kell ellenőrizni az összehasonlításhoz.



7.2.5 Az IP-címzési rendszer ellenőrzése

A stadion hálózatának IP-címzési rendszere az előzetes javaslat szerint teszthálózat segítségével lett volna ellenőrizve. A tervező ehelyett egy szimulációs eszközt ajánl az IP-címzési séma ellenőrzésére, melynek segítségével meghatározhatja, vajon a címzési rendszer lehetővé teszi-e az útvonal-összevonást és támogatja-e a szükséges bővíthetőséget.

A tervező először konfigurálja a szimulált hálózatot, amely ugyanannyi hálózati eszközt tartalmaz, mint a tervezett hálózat. Ezután ellenőrzi a különböző alhálózatok elhelyezését és az útvonal-összevonások konfigurációját.

Stadionhálózat	Elosztási blokkok	Huzalozási központ blokkok	Egyedi VLAN-ok	Pont-pont összeköttetések
172.18.0.0/16	172.18.0.0/19	172.18.0.0/22	172.18.0.0/24	172.18.0.0/30
				172.18.0.4/30
				172.18.0.8/30
				-tól
				172.18.0.252/30
			172.18.1.0/24	
			172.18.2.0/24	
			172.18.3.0/24	
		172.18.4.0/22	172.18.4.0/24	
			172.18.5.0/24	
			172.18.6.0/24	
			172.18.7.0/24	
		172.18.8.0/22		
		172.18.12.0/22		
		172.18.16.0/22		
		172.18.20.0/22		
		172.18.24.0/22		
		172.18.28.0/22		
	172.18.32.0/19			
	172.18.64.0/19			
	172.18.96.0/19			
	172.18.128.0/19			
	172.18.160.0/19			
	172.18.192.0/19			
	172.18.224.0/19			

7.2.6 A kockázatok és gyenge pontos felderítése

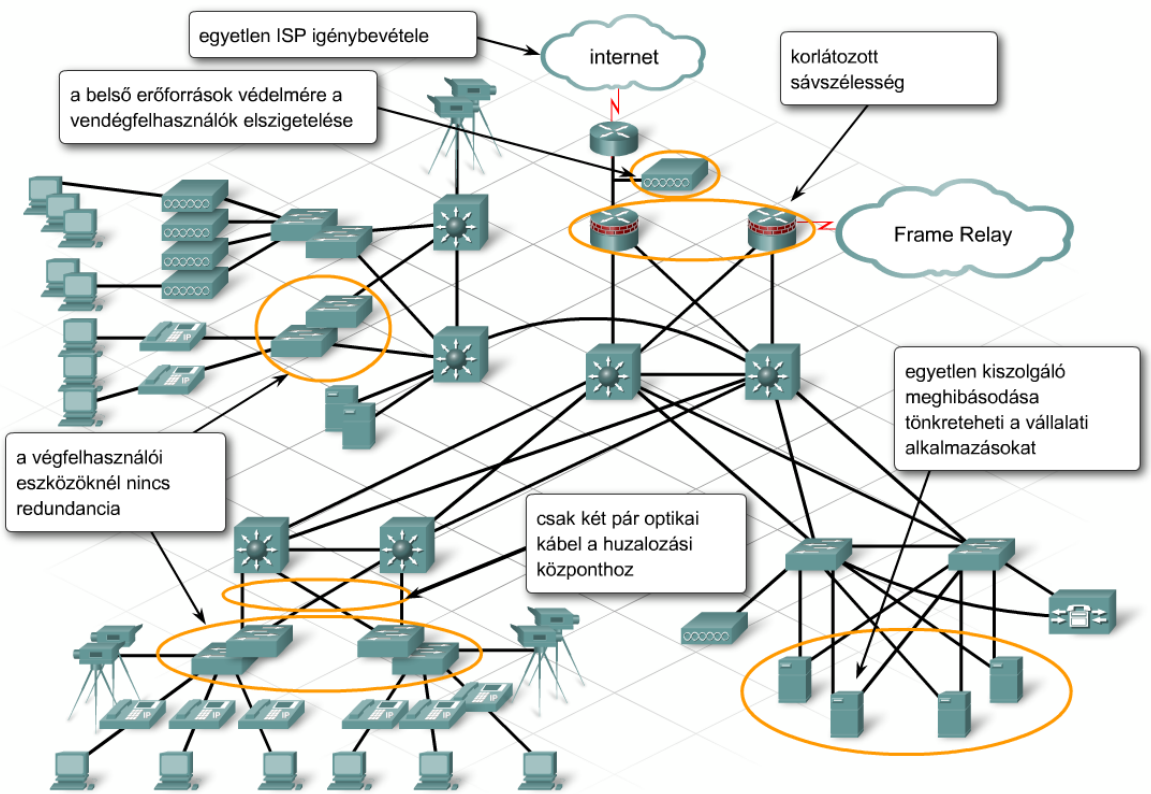
A kockázati tényezők és a gyenge pontok rögzítése

A hálózattervező és a Hálózat Kft. szakemberei a tesztelési terv „Következtetések” című fejezetében rögzítik az ellenőrzési folyamat eredményeivel kapcsolatos észrevételeiket és véleményüket. E fejezet lényeges részét képezi a terv gyenge pontjainak és kockázati tényezőinek elemzése. A stadion hálózatának tervében található néhány említésre méltó kockázati tényező.

Ezek rögzítése segíti a stadion vezetőségét abban, hogy megalapozott döntést hozhasson a terv megvalósításával kapcsolatban.

A kockázatok és gyenge pontok a következők:

- **A hálózat elérési rétegében nincs redundancia** - A legtöbb végfelhasználói eszköz egyetlen elérési szintű kapcsolóhoz csatlakozik. Ez kritikus hibapontot jelent a végfelhasználói eszközök számára. Mivel az adatközpontban található kiszolgálók kiesése magasabb kockázatot jelent, ezért a szerverek két hálózati kártya használatával független hozzáférési kapcsolókhoz csatlakoznak.
- **Az internetkapcsolatot egyetlen ISP szolgáltatja** – Ha az ISP-kapcsolat meghibásodik, vagy a szolgáltatónál probléma merül fel, a stadion hálózatának minden internetkapcsolata megszűnik.
- **Korlátozott sávszélesség a WAN és az internet felé** – Ha a WAN- és internetkapcsolat iránti igény megnő, a korlátozott sávszélesség szűk keresztmetszetté válhat, és csökkentheti az alkalmazások teljesítményét.
- **A huzalozási központtól korlátozott számú üvegszálas kapcsolat vezet ki** – E megszorítás következtében az elérési réteg eszközeitől vezető redundáns kapcsolatok száma mindössze kettő, ezért a huzalozási központ több kapcsolójának osztoznia kell a felfelé irányuló összeköttetéseken.



7.3 A kiszolgálófarm teszthálózata

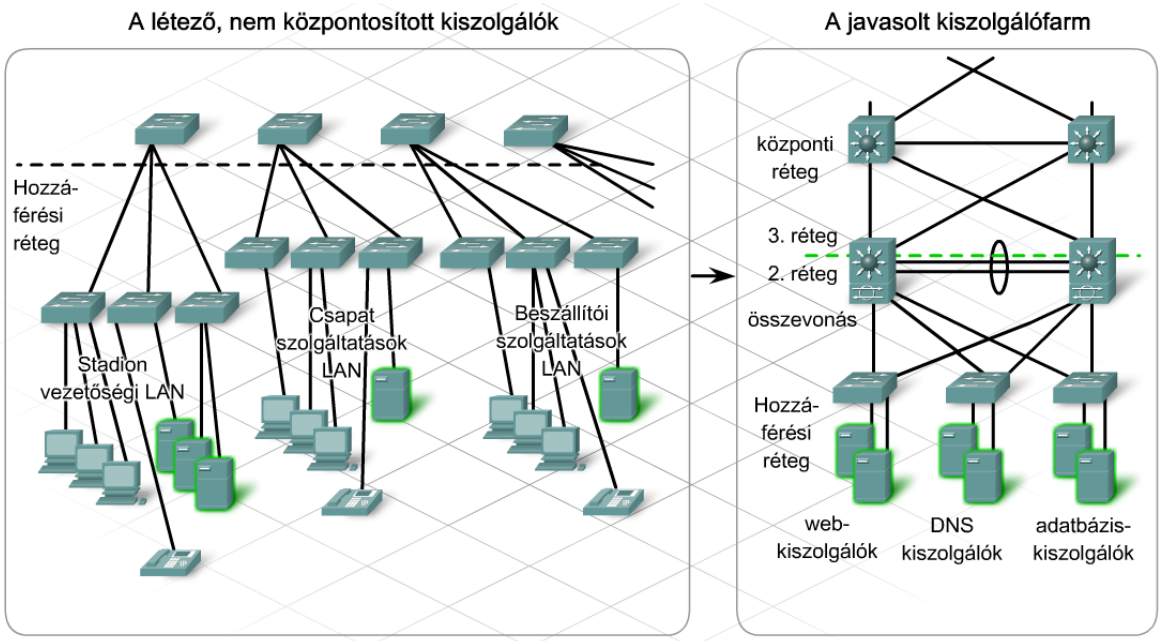
7.3.1 A kiszolgálófarm céljainak és követelményeinek meghatározása

A stadion hálózatának egyik célja az, hogy jobb felhasználói szolgáltatásokat nyújtson. Ez a cél a webhely elérhetőségének javításával érhető el, mivel az események időpontjának közzététele, a jegyvásárlás és -nyomtatás, illetve az ajándéktárgyak árusítása is ezen keresztül zajlik.

A javasolt terv szerint a webkiszolgálót, a DNS- és az adatbázis-kiszolgálót is áthelyezik az új adatközpontban lévő kiszolgálófarmba.

A stadion hálózati kiszolgálóinak áthelyezése

Az adatáramlás szempontjából a legnagyobb változtatás és a javasolt terv kritikus eleme a kiszolgálók áthelyezése a stadion vezetői irodáiból az új adatközpontba. A közel 100 százalékos üzemidő és rendelkezésre állás követelménye könnyebben kivitelezhető, ha a kiszolgálók egy központi adatközpontban helyezkednek el. Az adatközpont egy olyan hálózatrész, mely teszthálózat segítségével könnyen tesztelhető.



7.3.2 A tesztelési terv elkészítése

Mit kell tesztelni?

A stadion hálózati terve szerint, az alábbi elemek közvetlenül érintik a kiszolgálófarmot:

- Moduláris kiszolgálófarm topológia létrehozása.
- Redundáns összeköttetések kialakítása a kiszolgálók kapcsolódásához.
- 2. rétegbeli redundáns kapcsolók telepítése a kiszolgálók kapcsolódásához.
- VLAN-alapú gyors feszítőfa protokoll alkalmazása annak érdekében, hogy meghibásodás után a redundáns kapcsolt összeköttetések minél gyorsabban aktív állapotba kerüljenek.
- Rugalmas IP-címzési rendszer konfigurálása.
- Az adatközpont központi és elosztási rétegében EIGRP protokoll konfigurálása.

- Szigorú forgalomszűrés konfigurálása az illetéktelen hozzáférések megakadályozására.

A hálózattervező teszthálózat megépítése mellett dönt. Mivel nem állnak rendelkezésére többrétegű kapcsolók, ezért a 3. rétegbeli feladatok ellátását forgalomirányítók végzik. A teszthálózat topológiája öt 2. rétegbeli kapcsolóból, öt 3. rétegbeli eszközből, és számos asztali számítógépből áll, melyek a különböző alkalmazásokat futtató kiszolgálókat helyettesítik. Ezzel a topológiával a Hálózat Kft. dolgozói bemutathatják, hogy az üzleti célok és követelmények kielégítésére megfelelő a javasolt terv.

Üzleti célkitűzés	Az általános siker feltétele
Az ütemtervek megjelenítéséhez, a jegyek megvételéhez és kinyomtatásához, valamint az árubeszerzéshez szükséges weboldalak elérhetőségének javításával jobb ügyfél szolgáltatások biztosítása.	A webes szolgáltatások rendelkezésre állása belső és külső telephelyekről egyaránt, amit a kapcsolatok vagy eszközök meghibásodása egyáltalán nem, vagy csak kis mértékben zavar meg.
Technikai követelmények	Az eredményesség feltétele
Méretezhetőség	
Rugalmas IP-címzési rendszer konfigurálása.	További alhálózatok és kiszolgálók hozzáadása ne igényelje a forgalomirányítás vagy a címzés újrakonfigurálását.
Moduláris kiszolgálófarm-terv elkészítése, mely több kiszolgálóhoz tud alkalmazkodni anélkül, hogy a tervre hatással lenne.	További kiszolgáló hozzáadásakor ne legyen szükséges új konfiguráció.
Elérhetőség	
A kiszolgálóktól redundáns kapcsolatok alkalmazása a Hozzáférési réteghez.	Egyetlen Hozzáférési rétegbeli kapcsoló meghibásodása ne zavarja a kiszolgálókapcsolatot.
A Hozzáférési rétegben redundáns, 2. rétegbeli kapcsoló összeköttetések létrehozása, és egy meghibásodás után ezeknek a gyors helyreállása érdekében RSTP alkalmazása.	Egy kapcsolat vagy eszköz meghibásodása után az RSTP gyorsan konvergáljon.
Az Elosztási és a Központi rétegben gyorsan konvergáló irányító protokoll (EIGRP) konfigurálása.	Hiba esetén az EIGRP konvergáljon gyorsan, és a kapcsolatok egyáltalán ne, vagy csak kis időre szakadjanak meg.
Biztonság	
Szűrők alkalmazása, melyek a kiszolgálónak csak a szükséges portjain engedélyezik a forgalmat.	A nemkívánt forgalom tiltása, mielőtt még a kiszolgálót elérné.
Az elosztási rétegben tűzfal és IDS alkalmazása.	Az ismert veszélyek és támadásleíró fájlok a kiszolgálók elérése előtt blokkolva legyenek.
Felügyelhetőség	
Felügyeleti VLAN létrehozása és hozzáférés biztosítása az adatközponthoz SSH alkalmazásával.	A felügyeleti állomás érje el a belső adatközpont eszközeit SSH-n keresztül.

Az Hálózat Kft. dolgozói a tervező által elkészített ellenőrző lista szerint haladnak a teszthálózat megépítésénél.

A teszthálózat ellenőrzése

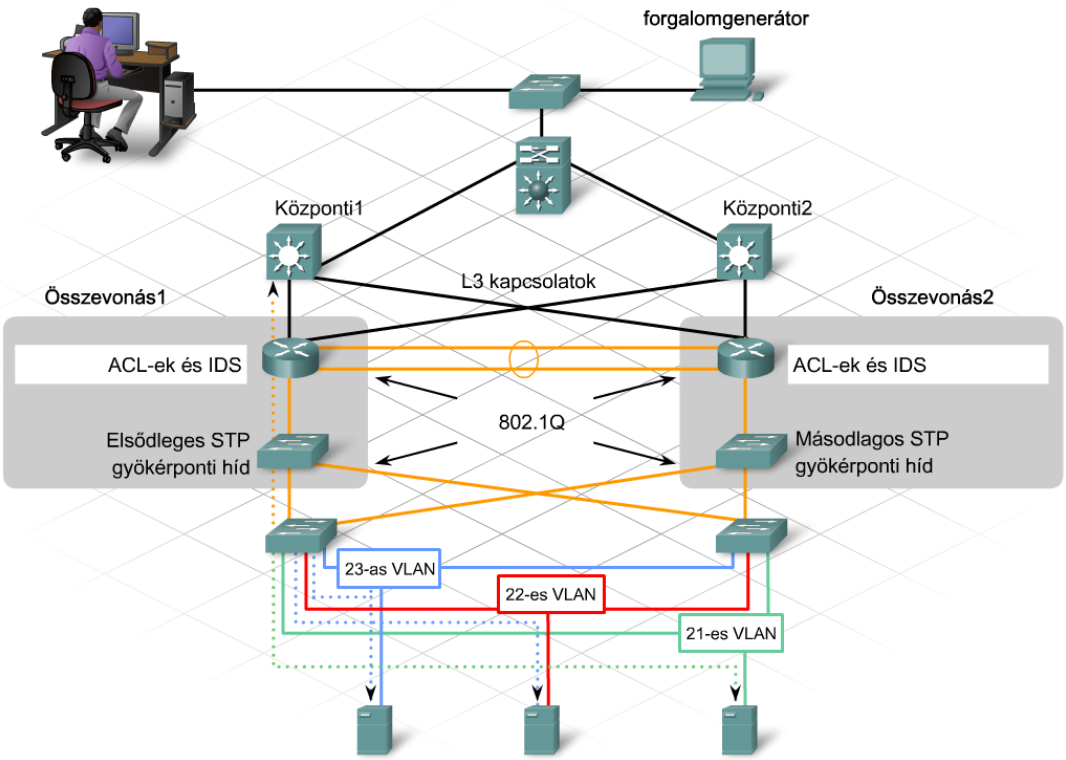
A teszthálózat elkészítése után, a munkatársak elvégzik az alapvető kapcsolatok tesztelését a hálózat helyes működésének biztosításához. Ezt követően elkészítik a hálózat alapkonfigurációját.

A viszonyítási értékek meghatározása

A teszthálózat viszonyítási értékeinek meghatározása fontos feladat. A különböző tesztek során nyert eredményeket végül összehasonlítják a kezdeti értékekkel. Ezzel a módszerrel a

munkatársak felderíthetik és lejegyezhetik azokat a folyamatokat és feladatokat, melyek növelik a processzorhasználatot vagy csökkentik az elérhető sávszélességet.

A hálózati forgalom szimulálására, a tervező egy számítógéphez csatlakoztatott forgalomgenerátor alkalmazását javasolja. A forgalomgenerátor egy olyan teszteszköz, mely a hálózat különböző használati szintjeit tudja szimulálni. A kiszolgálófarm teszthálózatának esetében a tervező az eszközt a webkiszolgáló forgalmának szimulálására fogja használni.



7.3.3 Az eszköz- és topológiaválasztás jóváhagyása

A stadion hálózatánál javasolt adatközpont redundáns hierarchikus topológiát használ a kiszolgálófarmhoz.

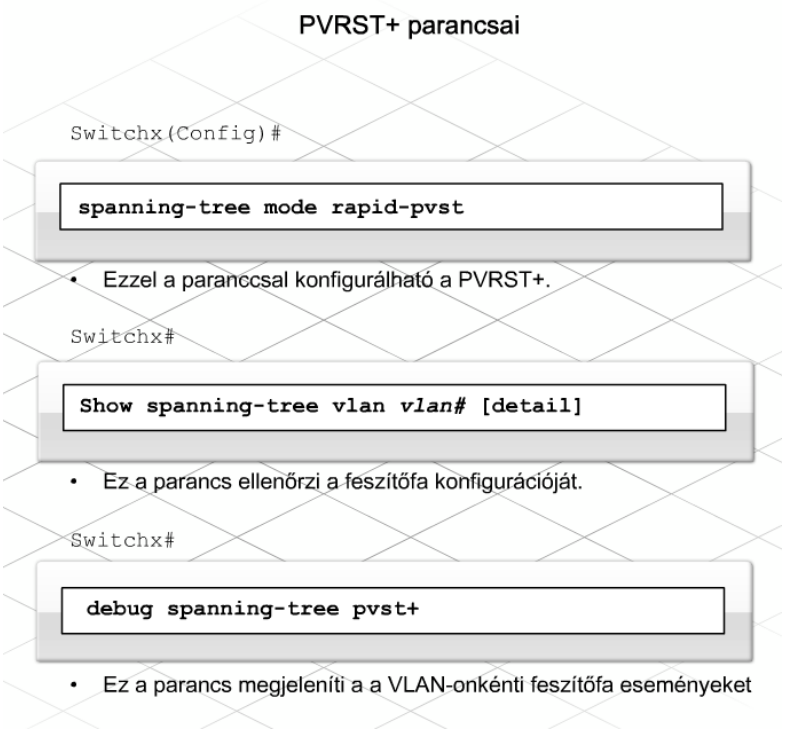
LAN szimuláció

A LAN szimuláció során, a forgalomirányítással beállított összeköttetések gyorsabban konvergáltak egy meghibásodás után, mint az STP protokollal működők. A hálózattervező ezért úgy dönt, hogy a gyors feszítőfa protokollt (RSTP - Rapid Spanning Tree Protocol) alkalmazó kapcsolt hálózatban teszthálózat segítségével ellenőrzi, milyen gyorsan áll helyre a kiszolgálófarm egy meghibásodás után. A teszt beállítása előtt a tervező a hálózati szakemberekkel együtt ellenőrzi az RSTP működését.

Az RSTP protokoll gyors csatlakozásokat biztosít egy kapcsoló, egy port vagy egy LAN meghibásodása után. Az RSTP lehetővé teszi a kapcsolóportok beállítását úgy, hogy azok közvetlenül továbbító állapotba kerüljenek a kapcsoló újraindulását követően.

VLAN-onkénti gyors feszítőfa protokoll

AZ RSTP (802.1w) szabvány egyetlen feszítőfát feltételez az egész kapcsolt hálózatban, függetlenül a VLAN-ok számától. A Cisco saját fejlesztésű RSTP protokollja a (PVRST+ – Per VLAN Rapid Spanning Tree Plus), minden VLAN-on külön definiálja az RSTP egy példányát. A Cisco saját fejlesztésű RSTP protokollja a (PVRST+ – Per VLAN Rapid Spanning Tree Plus), minden VLAN-on külön definiálja az RSTP egy példányát. A Cisco dokumentációk gyakran RSTP-ként hivatkoznak erre a protokollra.

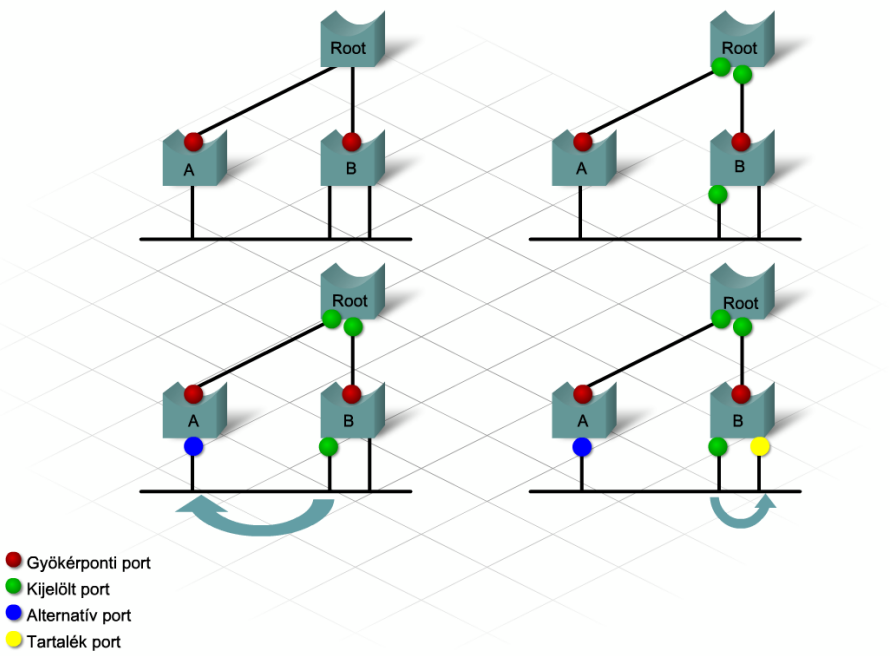


A portok fajtái

Az RSTP az alábbi portfunkciókat definiálja:

- **Gyökérponti** – A nem gyökérponti kapcsolók mindegyikén az RSTP protokoll által kiválasztott továbbító port, amelyen át a legkisebb költségű útvonal vezet a gyökérponti kapcsoló felé.
- **Kijelölt** - A kapcsolt LAN-szegmensek számára az RSTP protokoll által, a legjobb BPDU (bridge protocol data unit) alapján kiválasztott továbbító port. Ez a port a legkisebb költségű útvonalat jelöli ki a LAN szegmenstől a gyökérponti kapcsoló felé.
- **Alternatív** – Nem gyökérponti kapcsolókon a protokoll által kijelölt olyan port, mely a gyökérponti port által meghatározott útvonaltól eltérő, alternatív (második legjobb) útvonalat jelöl ki a gyökérponti kapcsoló felé. A port nem továbbít forgalmat.
- **Tartalék** - Egy olyan tartalék útvonalat kijelölő port, amely redundáns, de kevésbé jó összeköttetést határoz meg egy olyan szegmens felé, melyhez a nem gyökérponti kapcsoló már egy másik portjával csatlakozik. Ez a port nem továbbít forgalmat. (Tartalék port csak akkor létezik, amikor két port hurkot alkotva csatlakozik egymáshoz pont-pont kapcsolattal, vagy amikor egy híd kettő vagy több porttal csatlakozik egy megosztott LAN szegmenshez.)
- **Letiltott** - A feszítőfa működésében nem szereplő port.

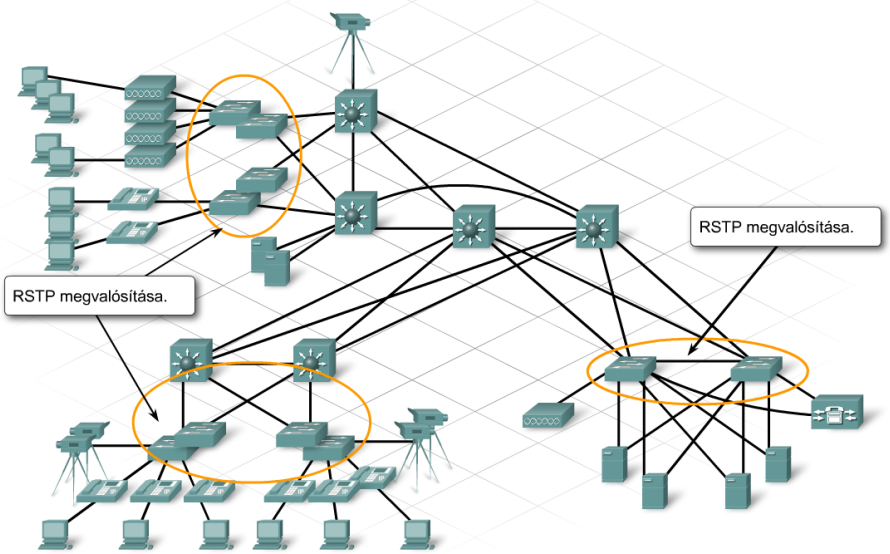
Az aktív topológiában a gyökérponti és a kijelölt portok vesznek részt, az alternatív és a tartalék portok nem.



A Stadion hálózata

A hálózattervező a Hálózat Kft. szakembereivel ellenőrzi az RSTP működését. A tervező elkészíti a telepítési ellenőrzőlistát és a tesztelési tervet annak ellenőrzésére, hogy a kapcsolt hálózat tudja-e biztosítani a szükséges rugalmasságot.

Az ellenőrzőlistában vázolt részletek alapján a Hálózat Kft. szakemberei beállítják a VLAN-onkénti gyors feszítőfa protokollt a hozzáférési rétegbeli kapcsolókon. Kiválasztják az elsődleges és másodlagos gyökérponti hidat, hogy biztosítsák a hálózat stabilitását arra az esetre, amikor új kapcsoló csatlakozik a topológiához. Ezután a kapcsolt topológiában hibák előidézésével vizsgálják az eredményeket.



7.3.4 A biztonsági terv ellenőrzése

A stadionhálózat kiszolgálófarmjával szemben támasztott két legfontosabb követelmény a rendelkezésre állás és a biztonság.

A rendelkezésre állással kapcsolatos követelmények

A hálózattervező redundáns összeköttetések és összetevők használatával igyekszik megvalósítani a rendelkezésre állásra vonatkozó követelményeket, ahol ez lehetséges. A 2. rétegben RSTP, a 3.-ban pedig EIGRP protokoll alkalmazásával biztosítja a hálózati meghibásodást követő gyors konvergenciát.

Többrétegű biztonság

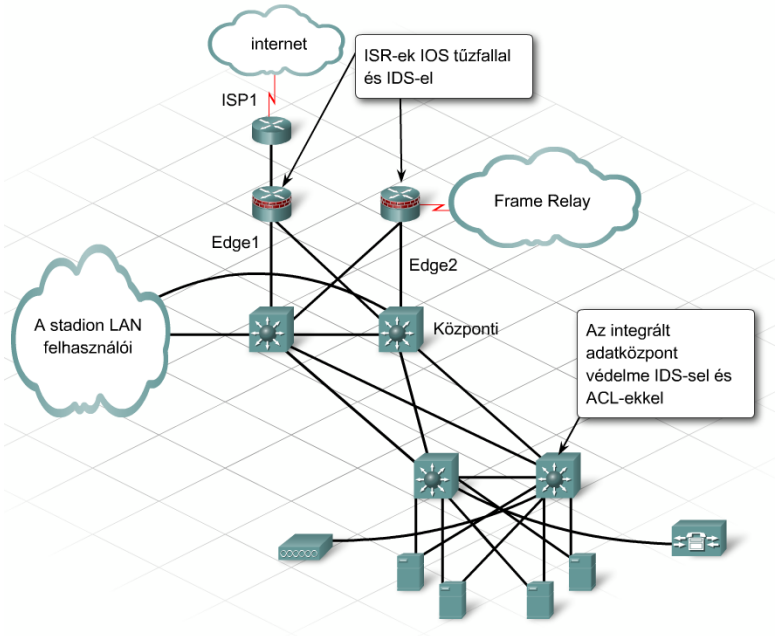
A kiszolgálófarm előzetes tervében többrétegű biztonsági megoldás szerepel. Alkalmazások és segédprogramok védik a kiszolgálókat a vírusok és férgek támadásaitól, és egyúttal állomás alapú behatolás elleni védelmet is biztosítanak. A hitelesítő rendszer kizárólag csak az arra jogosult felhasználók hozzáférését engedélyezi.

A hozzáférési rétegben portbiztonság alkalmazása és a nem használt portok letiltása segít az illetéktelen behatolás megelőzésében.

A hozzáférési listák szűrik és megakadályozzák a kiszolgálók felé irányuló hamis vagy nem kívánatos forgalmat. Az ACL-ek a kiszolgálófarm és a stadionhálózat kapcsolódási pontján helyezkednek el.

Tűzfalak

A tűzfalak és a Cisco IOS-ben beállított tűzfal-jellemzők állapotalapú tűzfal lehetőségeket szolgáltatnak. Az IPS rendszerek védik a hálózatot az ismert férgekkel és a normálistól eltérő forgalmi mintákkal szemben.



Az ACL terv ellenőrzése

Mivel a hozzáférési listák tervezése és elhelyezése biztosítja a legváltozatosabb lehetőségeket, ezért a hálózattervező ezek tesztelését határozza el. Tesztelési tervet készít, melyben felsorolja az összes szűrési feltételt és az ellenőrző módszereket. Teszthálózat alkalmazása helyett egy hálózat szimulátor használatát javasolja. A szimulátorban az ajánlat szerinti összes eszközt és összeköttetést tartalmazó konfiguráció gyorsan elkészíthető.

7.3.5 Megfelel-e a terv a vállalat céljainak?

Laborgyakorlat

7.3.6 A kockázatok és a gyenge pontok megállapítása

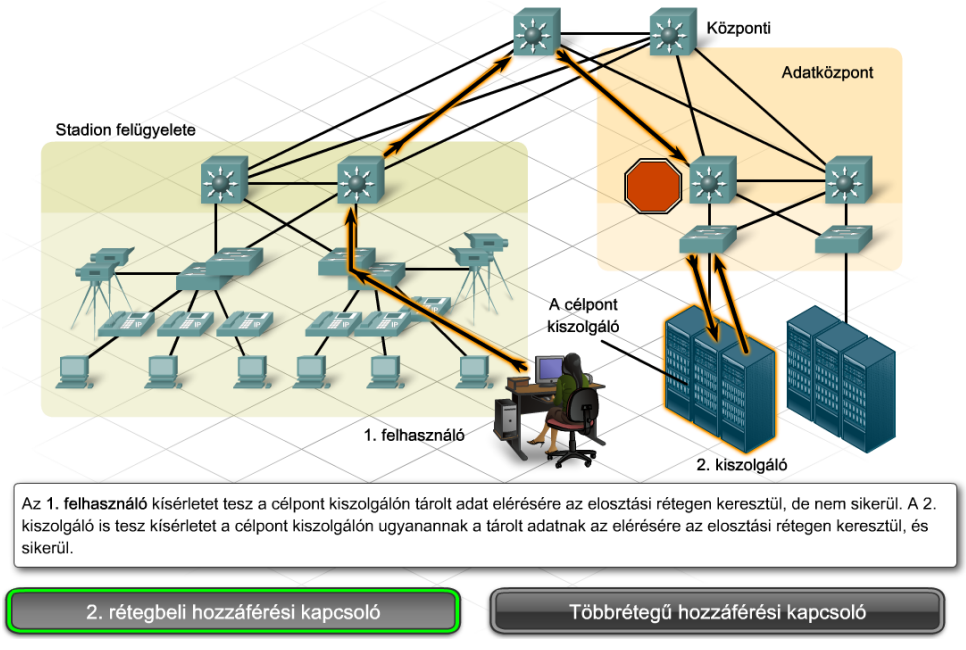
A kiszolgálófarm teszthálózatának és szimulációjának tapasztalataként kirajzolódik néhány, a tervjavaslattal kapcsolatos észrevétel. A hálózattervező megelégedéssel tapasztalja a hálózat várakozásnak megfelelő teljesítményét, azonban megállapítja azt is, hogy a hálózat növekedésével és fejlődésével összefüggésben változtatásokra is szükség lesz.

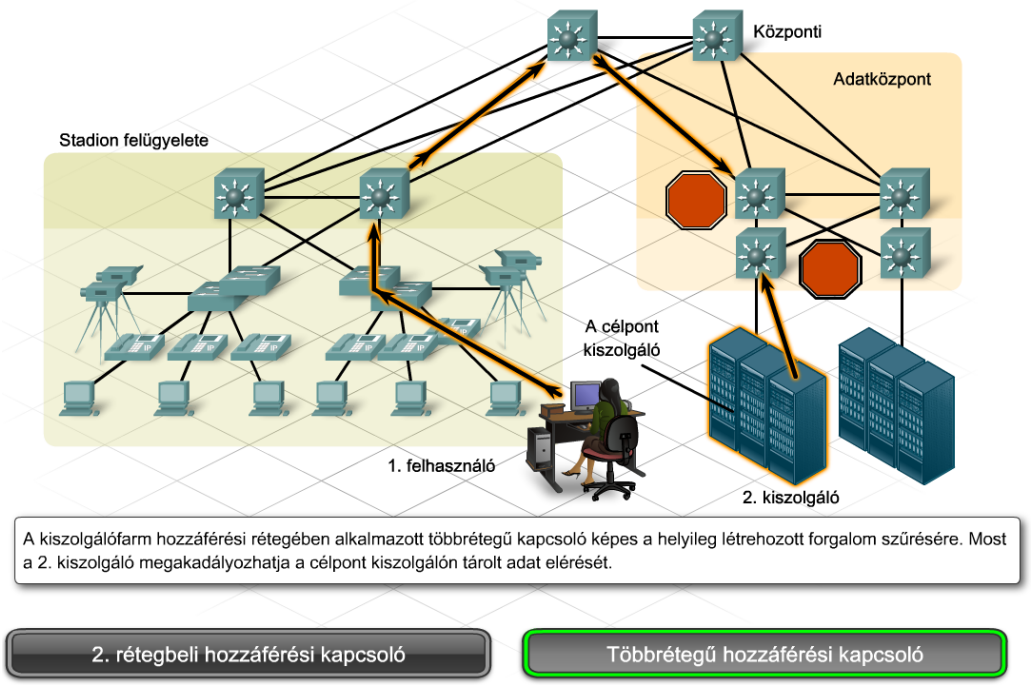
A gyenge pontok felderítése

A tesztek szerint az elosztási réteg hozzáférési listái megakadályozzák az illetéktelen forgalom belépését a kiszolgálófarmra, de a VLAN-okon belüli forgalomszűrésük nem hatékony. Ugyanahhoz a VLAN-hoz tartozó kiszolgálók között a tesztforgalom nem korlátozott.

Javaslatok

A hálózat terve támogatja a kiszolgálófarm és az adatközpont növekedését. A tervező azt javasolja, hogy a stadion vezetése mérlegelje többrétegű kapcsolók használatát a hozzáférési rétegben. A többrétegű kapcsolók a 2. rétegbelieknél rugalmasabbak a felhasználók és az adatközpont forgalmának elkülönítésében és szűrésében, valamint az adatközponton belül elhelyezkedő eszközök forgalmának elkülönítésében és szűrésében.





7.4 A fejezet összefoglalása

- Minden új terv végleges elfogadása és megvalósítása előtt a tervet tesztelni kell. A tesztelés a terv-elképzelések helyességének a bizonyítására szolgál.
- Az elképzelések bizonyítására végzett tesztelésnek (proof-of-concept test) két elfogadott módszere van: teszthálózat felépítése vagy egy létező hálózaton próbák végrehajtása.
- A teszthálózat vagy a próbák közötti választás az alábbi tényezőktől függ:
  - A szükséges teszt típusától
  - A próbák következtében, a létező hálózat működésében keletkező lehetséges zavaroktól
- Az elképzelések bizonyítására végzett teszt megkezdése előtt, érdemes egy részletes tesztelési tervet elkészíteni, mely tartalmazza a módszereket és a várható eredményeket.
- Az elképzelések bizonyítására végzett teszt bemutatja a hálózat új vagy továbbfejlesztett elemeinek feladatait, valamint ellenőrzi az elvárásoknak megfelelő működést.
- Ha a teszteléshez nem valósítható meg a fizikai hálózati környezet pontos mása, szimulációs programok alkalmazására lehet szükség.
- Teszthálózatok és szimulációk használhatók a tervben rejlő gyenge pontok és kockázatok meghatározásához.
- Néhány általános kockázat és gyengeség:
  - kritikus hibapont
  - nagy hibatartomány
  - lehetséges szűk keresztmetszet
  - korlátozott méretezhetőség
  - túl bonyolult terv
- A tesztelési terv elkészítésénél a hálózattervezőnek először az alábbi kérdésekben kell döntenie:
  - Milyen tesztek szükségesek?
  - A hálózatból mekkora részt kell megépíteni a tesztek elvégzéséhez?

    - Hogyan határozható meg a teszt eredményessége vagy eredménytelensége?
- Az RSTP a kapcsolat gyors helyreállását teszi lehetővé a kapcsoló, a kapcsolóport vagy a LAN meghibásodását követően. Engedélyezi a portok konfigurálását, így a kapcsoló újraindításánál a portok közvetlenül továbbító állapotba kerülhetnek.
- Az RSTP az alábbi portszerepeket definiálja:
    - **Gyökér** - A feszítőfa topológia kiválasztott továbbító portja.
    - **Kijelölt** - A kapcsolt LAN-szegmensek számára kiválasztott továbbító port.
    - **Alternatív** - A gyökérport által kijelölt útvonaltól eltérő útvonalat határoz meg a gyökérponti hídhoz.
    - **Tartalék** - Tartalék útvonalat határoz meg egy redundáns, de kevésbé előnyös kapcsolaton egy olyan szegmenssel, amelyhez egy másik kapcsolóport már csatlakozik. Tartalék port csak abban az esetben létezhet, ha két portot visszahurkolással köt össze egy pont-pont összeköttetés vagy híd, és legalább két kapcsolattal rendelkezik egy megosztott LAN-szegmens irányában.
    - **Letiltott** - Olyan port, amelynek nincs szerepe a feszítőfa működésében.

8. A WAN teszthálózatának elkészítése

8.1 Távoli kapcsolatok teszthálózata

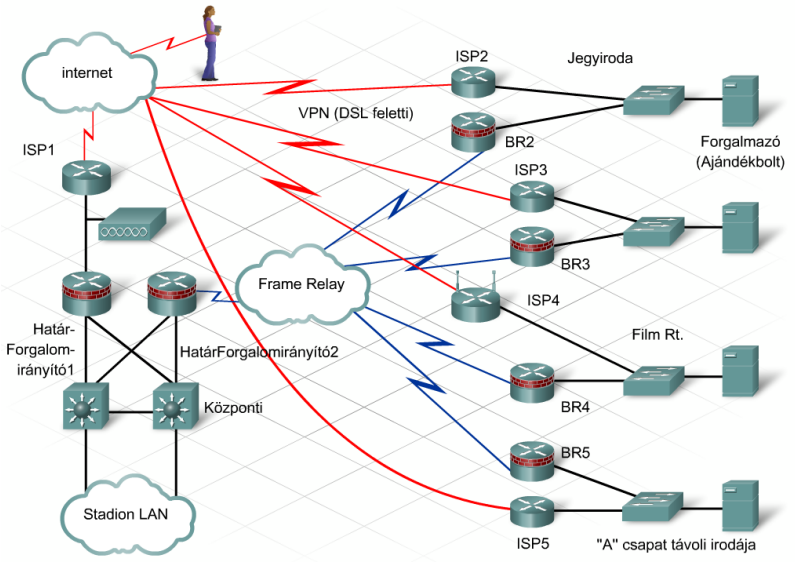
8.1.1 Távoli kapcsolatok tesztelési módszerei

A LAN teszthálózata által szolgáltatott eredmények igazolják a Hálózat Kft. tervezőjének korábbi elképzeléseit. A terv új elemeit, melyek a távoli helyek és dolgozók eléréséhez biztosítanak WAN kapcsolatot, szintén tesztelni kell. A LAN tervéhez képest ezek az összeköttetések nehezebben tesztelhetők.

A távoli kapcsolatokhoz rendszerint olyan átviteli berendezések szükségesek, melyek nincsenek az előfizető tulajdonában. Ezeket a berendezéseket, melyeket például a Frame Relay, a T1 vagy a DSL kapcsolatok használnak, a tervező általában nem tudja tesztelni. A tervezőnek ezért olyan módszereket kell alkalmaznia a javasolt terv ellenőrzéséhez, melyekhez nem szükségesek ilyen átviteli berendezések.

A távoli összeköttetések tervének tesztelésére a tervezőnek három lehetősége van:

- Szimulációs alkalmazások
- Szimulált kapcsolatokat alkalmazó teszthálózat
- Valós környezetben végzett próbák



8.1.2 A WAN kapcsolat tesztelése szimulációs alkalmazással

Az eszközök konfigurációjának és működésének tesztelését szimulált környezetben is el lehet végezni. Ha ez megfelelő eredménnyel zárult, a távoli kapcsolatok tesztelése valós környezetben végzett próbákkal is kiegészíthető.

Hálózati szimulációs alkalmazás

A számítógépes alkalmazások lehetőséget nyújtanak a tervezőnek arra, hogy még a megvalósítás előtt tesztelje az eszközök beállításait. A szimulációs eszközök alkalmazásának előnyei a következők:

- **Kisebb költség** – A teszthálózatok felépítése és fenntartása költséges. A hálózati eszközök képességbeli és beállítási lehetőségei gyakran változnak, ezért a naprakész laborkörnyezet fenntartása nem könnyű feladat.
- **Rugalmasság** – A szimulációs alkalmazások számos különböző eszköztípus és összeköttetési lehetőség használatát biztosítják. A topológia és a konfigurációk módosítása gyorsabban és könnyebben végrehajtható szimulációval, mint tényleges berendezésekkel.
- **Méretehetőség** – Nagy vagy összetett hálózat laborkörnyezetben történő megépítése időigényes, és több hibalehetőséget is magában rejtő feladat. A szimulációs alkalmazásokkal a nagy hálózatok rövidebb idő alatt tesztelhetők.
- **Vezérelhetőség** - Szimulációs alkalmazásokkal a tervező egyszerre vezérelheti az egész hálózat működését. Meghatározhatja a hálózaton keresztül küldött forgalom típusát, a küldés sebességét és gyakoriságát, továbbá megállíthatja a szimulációt a hálózat különböző pontjain áthaladó csomagok mintavételezése és vizsgálata érdekében.

Az alkalmazások korlátai

A hálózati terv helyességét igazoló szimulációs programok alkalmazásának hátrányai is vannak:

- **Korlátozott funkcionalitás** – A programok viszonylag gyorsan elavulnak, mivel már jóval a piaci megjelenésük előtt elkezdődik a tervezésük és a fejlesztésük. Előfordulhat az is, hogy a programok egy adott eszköz képességeinek csak egy részét támogatják.
- **Nem valós teljesítmény** - Egy valódi hálózatban előforduló összes feltétellel számolni és azokat szimulálni nagyon nehéz, sőt szinte lehetetlen feladat a programozó számára. Ennek következtében kockázatos a szimulációs alkalmazás időzítési és teljesítmény értékeire alapozni.

A hátrányok ellenére, a konfigurációk tesztelésére használt szimulációs eszközökkel a terv hiányosságainak nagy része kiválóan felderíthető.

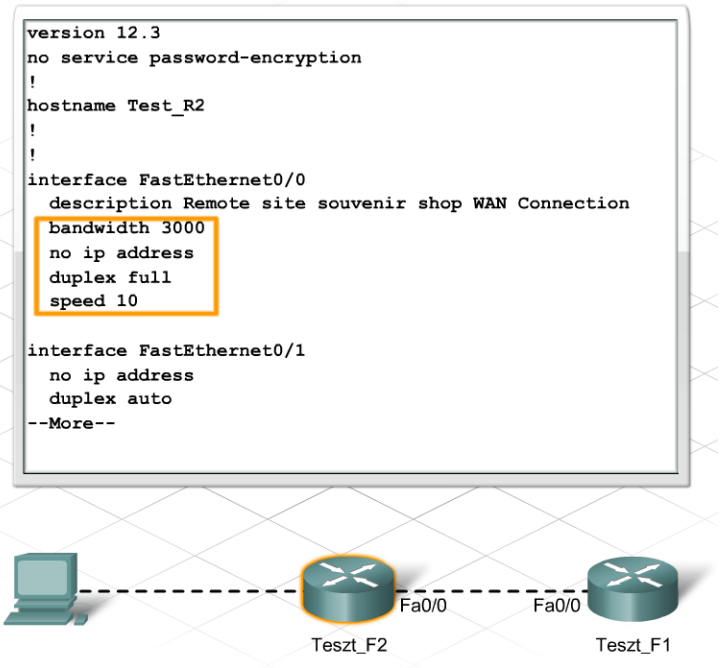
8.1.3 WAN kapcsolat szimulálása laborkörnyezetben

A szimulációs alkalmazásokon kívül, más módszerek is rendelkezésre állnak a távoli kapcsolatok tesztkörnyezetben történő szimulálására.

Szinte minden WAN technológiának szüksége van egy közbülső eszközre, mely az előfizetői oldalon átalakítja a WAN jeleket soros vagy Ethernet jelekre. Ilyen eszközök a különböző típusú modemek és a CSU/DSU eszközök. Kivételt képez a Metro Ethernet, mely nem igényel közbülső eszközt.

DSL- és kábelkapcsolatok szimulációja

Egy DSL vagy kábeles WAN kapcsolat megfelelően szimulálható egy Ethernet kapcsolat segítségével. A legtöbb Ethernet interfész beállítható 10 Mbit/s sebességű adattovábbításra, ami hasonló a DSL- és kábelkapcsolatokhoz. A forgalomirányítókat keresztkötésű Ethernet kábellel kell összekötni. Az interfészeken alkalmazott bandwidth parancs alkalmazásával az irányítóprotokollban használt metrika beállítható úgy, hogy egy kisebb sebességű kapcsolat metrikáját szimulálja. Az statikus útvonalak prioritási sorrendje az útvonalhoz rendelt adminisztratív távolság segítségével állítható be.



Soros kapcsolatok szimulációja

Két, általánosan alkalmazott módszer létezik a soros kapcsolat szimulálására:

- CSU/DSU vagy soros modemek alkalmazása
- V.35 kábelek használata

CSU/DSU vagy soros modemek alkalmazása

CSU/DSU vagy soros modemek alkalmazásánál, az eszköz használati utasításában általában megtalálható a keresztkötésű kábel elkészítéséhez szükséges vezetékbekötési térkép. Ha mégsem,

az interneten rendszerint megtalálható a helyes színsorrend. Ez a keresztkötésű kábel használható két hasonló típusú eszköz csatlakoztatására, mely a távközlési szolgáltató (telecommunications service provider, TSP) által nyújtott kapcsolatot szimulálja.

Az egyik CSU/DSU-t vagy modemet a DCE feladat ellátására kell konfigurálni, a másik eszközt pedig DTE-nek kell beállítani. Ezután a forgalomirányítókat úgy kell csatlakoztatni és konfigurálni, mintha valóságos WAN környezetben lennének. A CSU/DSU vagy a modem fogja az órajelet biztosítani a kapcsolat számára.

11 intelli-Mux FF T1/E1 Modul

Egy TELCO csatlakozónak rendszerint fordított a működése, például az RX és TX fel van cserélve, ezért egy egyeneskötésű kábellel csatlakoztatható a CSU/DSU/TSU csatlakozó a TELCO csatlakozóhoz.

Szélessávú oszcilloszkóp vagy DVM segítségével a TX és RX párokon végzett méréssel meghatározhatja, melyik kapcsolattal rendelkezik. A TX pároknál mérhető feszültség van, az RX pároknál nincs. Megjegyzés: A telefontársaságok számos T1 csatlakozót kínálnak "smart jack" végződéssel. Ezekbe egy automatikus visszacsatolási hurok van beépítve, így ha nincs bedugva csatlakozó, a TX pár az RX-hez kapcsolódik. Ezt a lehetőséget a telefontársaságok annak a vonalnak a tesztelésére használják, amelyik a helyi központ és az ön csatlakozási pontja között van. A telepítés során gyakori hiba, hogy felcserélik a TX és RX párokat, ezért a legjobb a tesztelés előtt bedugni a kábelt a csatlakozóba.

Két megegyező érintkezőkimenettel rendelkező T1 csatlakozó összekötéséhez egy T1 keresztkötésű kábel szükséges, aminek a következő csatlakozói vannak:

T1 keresztkötésű kábel

A kábel "A" végének RJ45 érintkezői	A kábel "B" végének RJ45 érintkezői
1	4
2	5
4	1
5	2

T1 loop-back konnektornak a következő csatlakozói vannak, mind ugyanazon a csatlakozón vagy aljzaton:

T1 Loop-back konnektor

RJ45 érpárok
1-4
2-5

V.35 kábelek használata

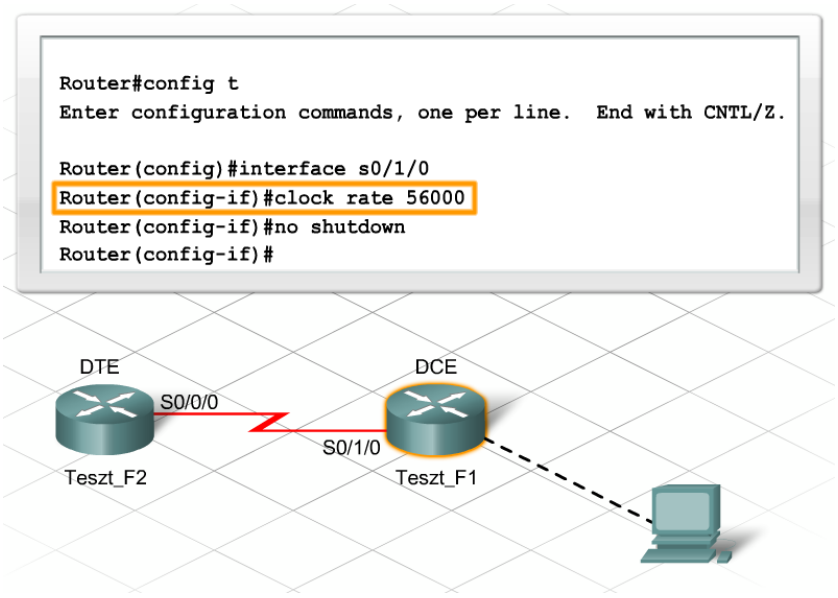
A Hálózat Kft. teszthálózatában a pont-pont WAN kapcsolat szimulálása két V.35-ös kábel segítségével megoldható. Az egyik kábel DCE kábel, a másik pedig DTE. A két kábel V.35-ös csatlakozóinak összekötésével egy keresztkötésű kábel jön létre. Ha a forgalomirányítókat ilyen kábellel kötjük össze, létrejön a pont-pont kapcsolat áramköre. Normál körülmények között a CSU/DSU vagy a modem biztosítja az órajelet. Amennyiben nem használunk ilyen eszközöket, úgy az órajel előállítás funkciója hiányozni fog, következésképpen az egyik forgalomirányítót DCE eszközként kell konfigurálni az interfészen alkalmazott clock rate parancs segítségével. A

tényleges hálózatokban a forgalomirányítók és a CPE eszközök csak ritkán, vagy egyáltalán nem nyújtanak DCE szolgáltatást az áramkör számára.

Különböző órajel értékek beállításával a tesztelést végző hálózattervezőnek és a Hálózat Kft. szakembereinek lehetősége nyílik a különböző sebességű kapcsolatok szimulálására.

A szimulált-, soros WAN összeköttetések használatának előnye, hogy a soros interfész konfigurációja tesztelhető és ellenőrizhető. A szimulációs tesztelés e típusának hátránya pedig abban rejlik, hogy a távközlési szolgáltató valós hálózatának tényezői nem vizsgálhatók.

Miután a szimulációk segítségével megtörtént, akonfigurációk tesztelése, ajánlott további teszteléseket végezni próbatelepítés végrehajtásával.



8.2 A WAN céljainak és követelményeinek meghatározása

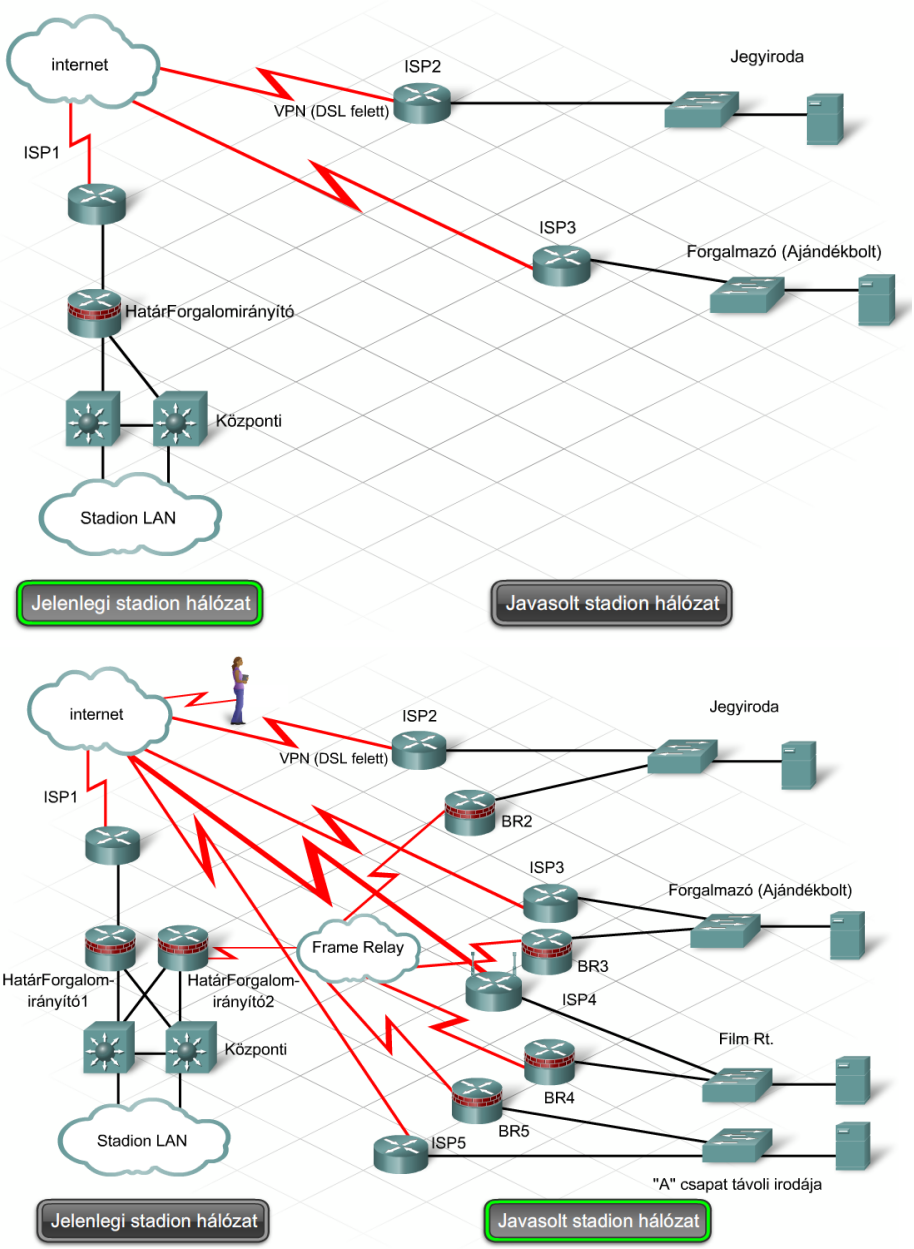
8.2.1 A WAN céljainak és követelményeinek meghatározása

A távoli telephelyekkel kialakított kapcsolatok jelentik az egyik legnagyobb problémát a jelenlegi hálózatban. A stadion vezetőségének elsődleges célja, hogy az új IP-telefonos rendszert és a videó felügyeleti hálózatot kiterjessze a már meglévő távoli telephelyekre is. Ezen szolgáltatásokat a jelenlegi WAN hálózat nem képes támogatni.

A stadion hálózatában a jelenlegi két távoli telephely az interneten keresztül fér hozzá a központi hálózathoz virtuális magánhálózat (virtual private network, VPN) révén. Ezek a VPN kapcsolatok DSL vonalakat használnak. Az ISP sávszélesség garanciát vagy QoS szolgáltatást nem nyújt. Az előzetes terv dedikált Frame Relay WAN kapcsolat kialakítását javasolja fejlesztésként. A hálózattervező Frame Relay alkalmazását ajánlja az “A” csoport és a Film Rt. számára helyet biztosító új, távoli iroda elérésére.

A meglévő, interneten keresztüli VPN kapcsolatok az új tervben az új WAN tartalék összeköttetései lennének.

A tervező úgy dönt, hogy a WAN kapcsolat szimulálására teszthálózatot alkalmaz, mellyel kipróbálhatja a konfigurációkat és a hálózat helyreállását egy kapcsolat meghibásodása esetén. A távközlési szolgáltató teljes csomagkapcsolt hálózatának szimulálása nem valósítható meg sem teszthálózattal, sem szimulációs programmal. A TSP hálózatán áthaladó jelenlegi Frame Relay kapcsolat tesztelése kizárólag gyakorlati próbákkal valósítható meg. A teszthálózat felépítése és a terv elfogadása után próbatelepítés végrehajtását tervezik az ajándékbolt számára.



8.2.2 Tesztelési terv készítése

A TSP hálózat teljesítményét nem lehet teszthálózattal tesztelni. Ezzel szemben a terv más fontos elemei ellenőrizhetők a WAN teszthálózatának segítségével:

- A Frame Relay helyi hurok konfigurációja
- A VPN tartalék kapcsolat életbe lépési mechanizmusa a Frame Relay meghibásodása esetén

- A statikus útvonalak konfigurációja
- A WAN ki- és bemenő forgalmát szűrő hozzáférési listák
- A távoli felügyeletet biztosító SSH konfiguráció

A WAN kapcsolatok teszthálózatának megépítése érdekében a tervező úgy dönt, hogy Cisco forgalomirányító segítségével szimulálja a Frame Relay kapcsolót. Ezzel a módszerrel lehetővé válik a helyi hurok tesztelése anélkül, hogy fizikailag kellene csatlakozni a TSP hálózatához. A teszthálózatban négy forgalomirányító szükséges az összes funkció teszteléséhez.

A Frame Relay kapcsolatok bemutatása céljából a tervező elkészít egy tesztelési topológiai ábrát, egy telepítési ellenőrzőlistát és a tesztelési tervet.

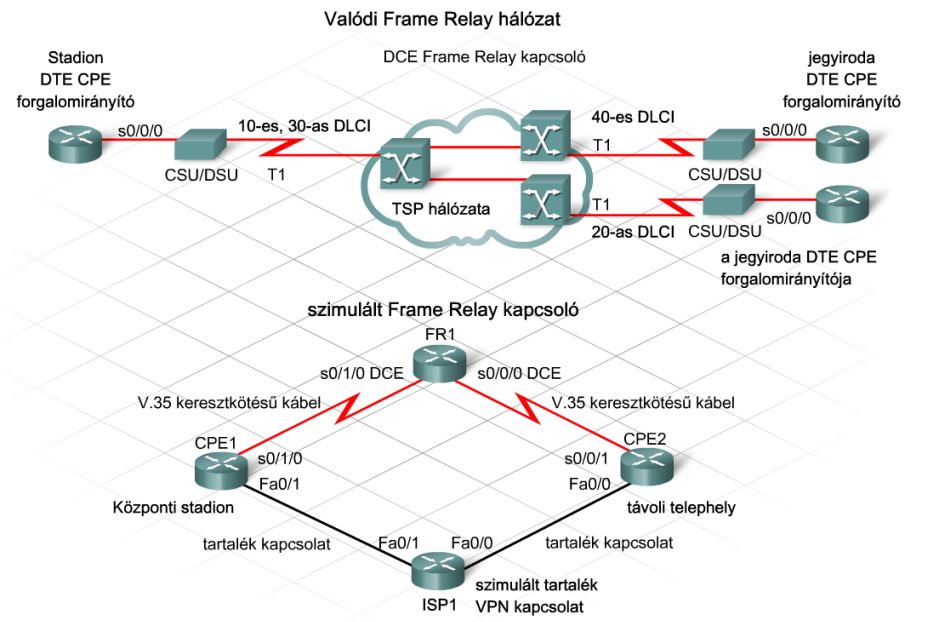
Üzleti célkitűzés	Az általános siker feltétele
A távoli telephelyeken újabb szolgáltatások biztosítása (hang, videó).	Frame Relay kapcsolatok, melyek garantált sávszélességet nyújtanak a késleltetés-érzékeny forgalom számára és tartalék kapcsolatokat biztosítanak az elvárásokat kielégítő működéshez.
Technikai követelmények	Az eredményesség feltétele
Méretezhetőség	
A távoli telephelyek csatlakoztatásához Frame Relay alkalmazása.	További telephelyekkel történő bővítés nem igényel újabb helyi hurok kapcsolatokat.
Sávszélesség követelmények konfigurálása minden egyes virtuális áramkörhöz.	A CIR biztosítsa a sávszélességet a konfigurált virtuális áramköröknek.
Elérhetőség	
Az interneten keresztülhaladó, tartalék VPN kapcsolatotok konfigurálása.	A Frame Relay meghibásodása esetén a kapcsolat ne szakadjon meg a nagyobb alkalmazásokkal.
Biztonság	
Forgalomszűrés alkalmazása annak érdekében, hogy kizárólag az arra jogosult forgalom legyen engedélyezve A WAN felől és felé.	A nemkívánt forgalom blokkolása.
Felügyelhetőség	
Felügyeleti hálózat és az SSH-n keresztüli eszközhozzáférések óvintézkedéseinek létrehozása.	A felügyeleti állomás érje el a WAN hálózati eszközeit SSH-n keresztül.

A Frame Relay WAN tesztelésénél használt topológiában a korábbi teszthálózatokban alkalmazottól eltérő kapcsolatok szükségesek. A jelenlegi megvalósításban a helyi hurok az előfizetői oldalon egy CSU/DSU eszközhöz csatlakozik, melytől soros kapcsolat vezet tovább az előfizetői végberendezésként (customer premise equipment, CPE) működő forgalomirányítóhoz.

A helyi huroknál a DCE feladatot a TSP és a CSU/DSU is elláthatja. A CSU/DSU és a CPE forgalomirányító közötti soros kapcsolat órajelét a CSU/DSU szolgáltatja. A forgalomirányító felöli oldalon minden kapcsolat DTE, ennek megfelelően itt DTE kábel szükséges.

A teszthálózatban a Frame Relay kapcsolóhoz vezető igazi T1 vagy E1 kapcsolat nem létezik. Mindezt egy Cisco forgalomirányítóval kell helyettesíteni, mely Frame Relay kapcsolóként fog működni. Ez az FR1 azonosítóval jelzett eszköz keresztkötésű kapcsolattal csatlakozik a topológia többi forgalomirányítójához. A Hálózat Kft-nél ezeket a keresztkötésű kapcsolatokat V.35 DTE és V.35 DCE kábel közvetlen összekapcsolásával hozzák létre. Mivel a tesztelési topológiában nincs

CSU/DSU, az FR1 forgalomirányító interfészeit a DCE funkció biztosításához órajel szolgáltatásra kell konfigurálni.



8.2.3A topológia és az eszközök jóváhagyása

A javasolt WAN tervben a Frame Relay topológia radikálisan eltér az ISP által felügyelt, meglévő VPN kapcsolattól. A Frame Relay használatával kapcsolatban számos lehetőség létezik. A tapasztalat azt mutatja, hogy, a teszthálózat beállítása előtt a tervezőnek a Hálózat Kft. szakembereivel együtt ajánlott áttekinteni a WAN tervét és működését.

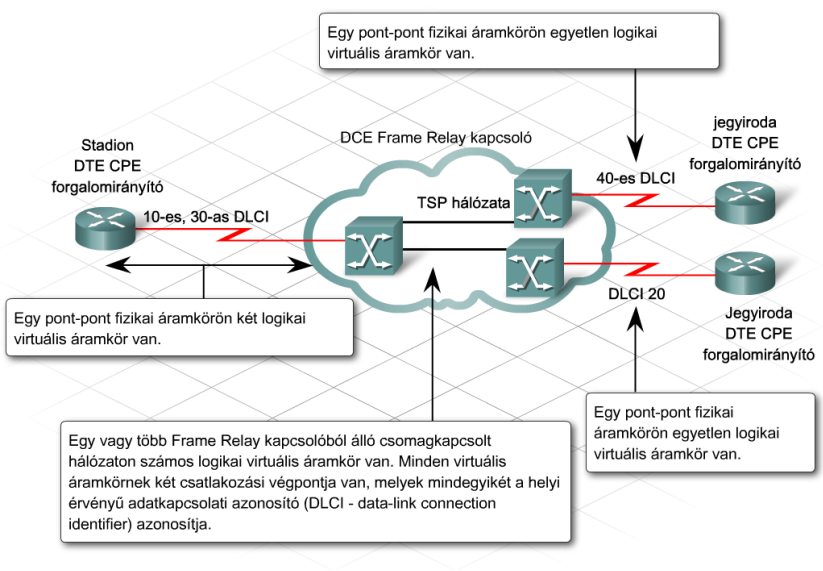
Frame Relay

A Frame Relay, a Nemzetközi Telekommunikációs Szövetség Telekommunikációs Szabványosítási Csoportja (International Telecommunication Union Telecommunications Standardization Sector, ITU-T) által szabványosított nagy teljesítményű WAN protokoll. Az Egyesült Államokban széles körben alkalmazzák. Sokan úgy gondolnak a Frame Relay-re, mint két hely közötti fizikai kapcsolatra. Valójában ez egy virtuális áramkör, mely kapcsolatok sorozatán ível át.

Minden Frame Relay kapcsolat legalább három összetevőből áll:

- Egy helyi pont-pont kapcsolat a CPE forgalomirányító és a TSP Frame Relay kapcsolója között
- A TSP csomagkapcsolt hálózata
- Egy távoli pont-pont kapcsolat a TSP hálózata és a távoli telephely között

A Frame Relay konfigurálása a CPE forgalomirányítón csupán egy pont-pont kapcsolat beállításából áll a TSP Frame Relay kapcsolója felé. Ez a pont-pont kapcsolat rendszerint T1/E1 vagy részleges T1/E1 áramkör. A virtuális áramkört a TSP konfigurálja a csomagkapcsolt hálózatán keresztül. A Frame Relay terminológiája és konfigurációja könnyen összezavarhatja a felhasználót.



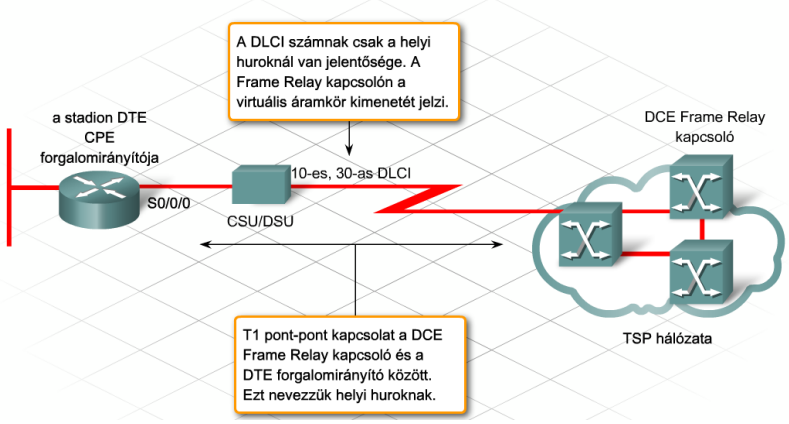
Az alkalmazható konfigurációs lehetőségek megértéséhez elsőként az új terv CPE forgalomirányítója és a távközlési szolgáltató Frame Relay kapcsolója közötti összeköttetést vázolja fel a tervező a Hálózat Kft. szakembereinek.

A helyi hurok

A javasolt kapcsolat a stadion CPE forgalomirányítója és a TSP Frame Relay kapcsolója között, egy T1 áramkör. Ezt a kapcsolatot nevezzük helyi huroknak. A helyi hurok a szolgáltató Frame Relay kapcsolójától indul, csatlakozik az előfizető CSU/DSU készülékébe, majd a CPE forgalomirányítójának soros interfészénél végződik. A helyi hurok és a Frame Relay felhő közötti összeköttetés órajele (portsebessége) a helyi hozzáférési sebesség (local access rate). Ez határozza meg, más beállításoktól függetlenül a szolgáltató csomagkapcsolt hálózatában a ki- és bemenő forgalom sebességét.

Adatkapcsolati azonosító

A helyi hurok egyetlen fizikai áramkörén több virtuális áramkör is kialakítható. Minden egyes virtuális áramköri végpontot adatkapcsolati azonosító (data-link connection identifier, DLCI) azonosít. A DLCI-nek általában csak a helyi huroknál van jelentősége, azaz a DLCI számok csak egyetlen Frame Relay kapcsolón a egyediek. Ugyanakkor, mivel több Frame Relay kapcsoló is lehet a hálózatban, a DLCI számok más kapcsolókon megismétlődhetnek.



A Frame Relay kapcsoló néhány szolgáltatása hatással van a távközlési szolgáltató hálózatán keresztülhaladó adatátvitel minőségére.

Garantált átviteli sebesség

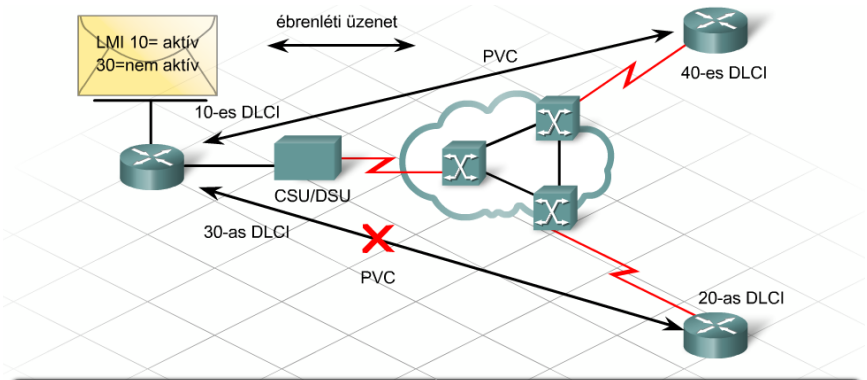
A Frame Relay szolgáltatók garantált, átlagos átviteli sebességű szolgáltatást nyújtanak a csomagkapcsolt hálózatukon keresztül. Ez a vállalt adatsebesség (committed information rate, CIR) határozza meg a maximális, átlagos átviteli sebességet normális feltételek között. A CIR a helyi átviteli sebességnél kisebb, vagy vele egyenlő. A helyi hurkon működő minden egyes DLCI-hez tartozik egy CIR érték. Ha a stadion a CIR értékénél nagyobb sebességgel próbál adatokat küldeni, a szolgáltató megjelöli a kereteket egy figyelmen kívül hagyható (discard eligible, DE) bittel, mely a keret fejrészében található. A hálózat megpróbál továbbítani minden keretet, de ha torlódás lép fel, eldobja a DE bittel megjelölteket.

0-ás CIR

Számos olcsó Frame Relay szolgáltatás 0-ás CIR értéken alapszik. A 0-ás CIR azt jelenti, hogy minden keret DE jelzést kap, így ezeket a hálózat torlódás esetén eldobhatja. A CIR érték 0-ára állítása esetén nincs garantált szolgáltatás, ezért ezek a szolgáltatások létfontosságú adatok továbbítására nem javasoltak.

Helyi kezelőfelület

A helyi kezelőfelület (Local Management Interface, LMI) egy jelzési rendszerre vonatkozó szabvány, amit a forgalomirányító (DTE eszköz) és a helyi Frame Relay kapcsoló (DCE eszköz) használ egymás között. Az LMI a kapcsolat kezeléséért és állapotának fenntartásáért felelős. A hálózati kapcsolatok állapotának figyelemmel követését például ébrenléti üzenetek segítségével valósítja meg. Az LMI-t használó Frame Relay számos továbbfejlesztett lehetőséggel (más néven kiterjesztéssel) rendelkezik az alap Frame Relay technológiához képest. Az egyik fontos kiterjesztés lehetővé teszi a virtuális áramkörökről, de akár még a fizikai kapcsolatok állapotáról szóló jelentést is. Az egyes hálózatok LMI szabványai különbözhetnek egymástól. A Cisco forgalomirányítók három LMI típust támogatnak: Cisco, ANSI Annex D és ITU-T Q.933 Annex A.



Cisco IOS Kulcsszó	Leírás
ansi	Annex D az Amerikai Nemzeti Szabványügyi Intézet (ANSI - American National Standards Institute) által meghatározott szabvány, T1.617.
cisco	A Cisco és még másik három cég által közösen meghatározott LMI típus.
q933a	ITU-T Q.933 Annex A.

Torlódáskezelés

A hálózat forgalmának könnyebb kezelése céljából a Frame Relay két szolgáltatást alkalmaz:

- Előremutató explicit torlódásjelzés (Forward-explicit congestion notification, FECN)
- Visszirányú explicit torlódásjelzés (Backward-explicit congestion notification, BECN)

A FECN és BECN jelzés egyetlen biten történik a Frame Relay keret fejrészében.

FECN

A FECN bit a célállomást tájékoztatja az útvonalon fellépő torlódásról. A Frame Relay keret fejrészének címmezőjében található. Az alábbi lépéseknek megfelelően működik:

1. A DTE eszköz Frame Relay keretet küld a hálózatba.
2. Ha a hálózaton torlódás van, a Frame Relay eszközök (kapcsolók) a FECN bit értékét 1-re állítják.
3. A keretek megérkeznek a távoli cél DTE eszközhöz.
4. A DTE eszköz észleli a cím mezőben szereplő FECN bit 1-re beállított értékét.
5. Ez az érték jelzi, hogy a keret torlódáson haladt keresztül a forrástól a cél felé vezető útvonalon.

BECN

A BECN bit a forrást tájékoztatja az útvonalon fellépő torlódásról. Szintén a Frame Relay keret fejrészének címmezőjében található. Az alábbi módon működik:

1. A Frame Relay kapcsoló torlódást észlel a hálózatban.
2. A FECN bittel megjelölt kerettel ellenkező irányú keretek fejrészében a BECN bit értékét 1-re állítja.
3. Ez a beállítás értesíti a forrás DTE eszközt az adott útvonalon fennálló torlódásról.

8.2.4 A WAN teszthálózatának elkészítése

A Frame Relay teszthálózat konfigurálásához a Hálózat Kft. szakemberei először az FR1 forgalomirányítót állítják be Frame Relay kapcsolónak. A konfigurálást a `frame-relay switching` paranccsal kezdik. Ennek alkalmazásával a forgalomirányító Frame Relay kapcsolóként működik, és DCE eszközként viselkedik. Ezt követően a `frame-relay route` parancsok segítségével engedélyezik a DLCI-k kapcsolását az egyes interfészekről.

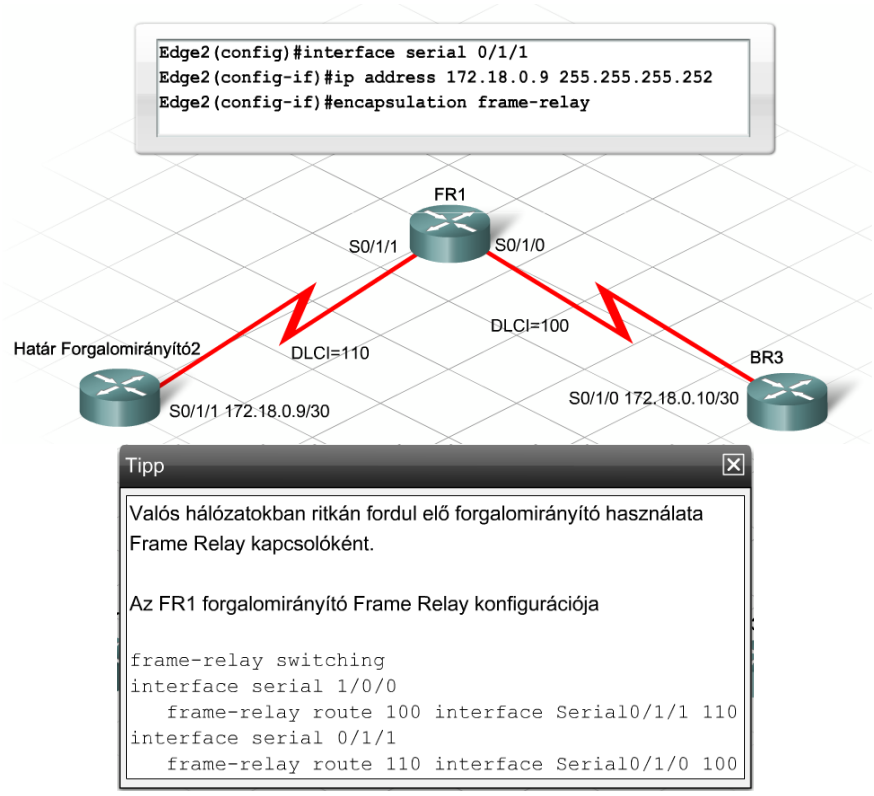
Most már az FR1 forgalomirányító két soros interfésze is Frame Relay DCE eszközként működik. Mindkettőn be kell állítani a beágyazást. A két lehetséges választás az **ietf** és a **cisco**. Az alapértelmezett beágyazás a **cisco**. Ez Cisco fejlesztésű, ezért nem alkalmazható, ha a Frame Relay hálózatban nem csak **Cisco** forgalomirányítók vannak.

A hálózattervező a Frame Relay konfigurálását az interfészek 3. rétegbeli IP-címeinek beállításával végzi, majd a beágyazás típusát adja meg. A beágyazás konfigurálása az alábbi paranccsal történik:

```
Router(config-if)#encapsulation frame-relay {cisco | ietf}
```

A CPE forgalomirányítókat nem szükséges Frame Relay kapcsolónak konfigurálni. Ennek ellenére a soros interfészeiken be kell állítani a beágyazás típusát és az IP-címet. A tervező a tesztelés során a tervben a végleges elrendezéshez javasolt eszközneveket és címeket használja.

A teszthálózatban nincs CSU/DSU eszköz, mely az órajelet szolgáltatná, ezért az FR1 forgalomirányító soros interfészein konfigurálni kell az órajelet.



Tipp

Valós hálózatokban ritkán fordul elő forgalomirányító használata Frame Relay kapcsolóként.

Az FR1 forgalomirányító Frame Relay konfigurációja

```
frame-relay switching
interface serial 1/0/0
   frame-relay route 100 interface Serial0/1/1 110
interface serial 0/1/1
   frame-relay route 110 interface Serial0/1/0 100
```

A teszthálózatban az FR1 forgalomirányító a szolgáltató Frame Relay kapcsolójaként működik. Ez szimulálja a Frame Relay felhőn keresztülvezető kapcsolatot, mely létrehoz egy virtuális áramkört a BR3 és az HatárForgalomirányító2forgalomirányító között. Ez a virtuális áramkör úgy viselkedik, mintha közvetlen kapcsolat lenne.

Inverz ARP és Frame Relay térképek

Az inverz ARP az Ethernet hálózatokban használt ARP protokollhoz hasonlóan működik. ARP esetén a küldő fél a 3. rétegbeli IP-címet ismeri, és üzenetszórás útján megtanulja az adatkapcsolati MAC-címet. Inverz ARP esetén a forgalomirányító a 2. rétegbeli címet ismeri (ez a DLCI), és a távoli eszköz 3. rétegbeli IP-címének megszerzésére irányuló kérést küld. Inverz ARP esetén a forgalomirányító a 2. rétegbeli címet ismeri, mely ez esetben a DLCI, és kérést küld a távoli eszköz 3. rétegbeli IP-címéért.

Amikor egy Cisco forgalomirányítón Frame Relay beágyazást konfigurálnak, az inverz ARP alapértelmezés szerint be van kapcsolva. A DLCI-k és a 3. rétegbeli címek statikus összerendelése manuálisan beállítható. Ez akkor szükséges, ha a távoli forgalomirányító nem támogatja az inverz ARP-t.

A Frame Relay kapcsolat egyik előnye, hogy egyetlen fizikai interfészen több virtuális áramkör lehet. A Frame Relay a szolgáltató csomagkapcsolt hálózatához vezető egyetlen kapcsolaton keresztül teszi lehetővé több távoli féllel kialakított kapcsolat használatát. A WAN-oknak ez a többszörös hozzáférésű típusa kevesebb költséggel jár, mint egy dedikált pont-pont összeköttetés a telephelyek között.

A távolságvektor alapú irányítóprotokollok útvonalfrissítéseinél problémát okozhat, ha egyetlen interfészen több kapcsolat is osztozik. A Frame Relay nem-szórásos, többszörös hozzáférésű (nonbroadcast multi-access, NBMA) protokoll. Ez azt jelenti, hogy egy adott interfészen található összes virtuális áramkört, különálló helyi hálózatként kell kezelni. A látóhatár-megosztás megakadályozza, hogy a forgalomirányító egy interfészén beérkező útvonalfrissítéseket ugyanazon az interfészen küldje ki, amelyen beérkeztek. A fentiek miatt a távoli telephelyről érkező útvonalfrissítés nem kerül továbbításra a többi, ugyanezen a fizikai interfészen osztozó virtuális áramkörökön.

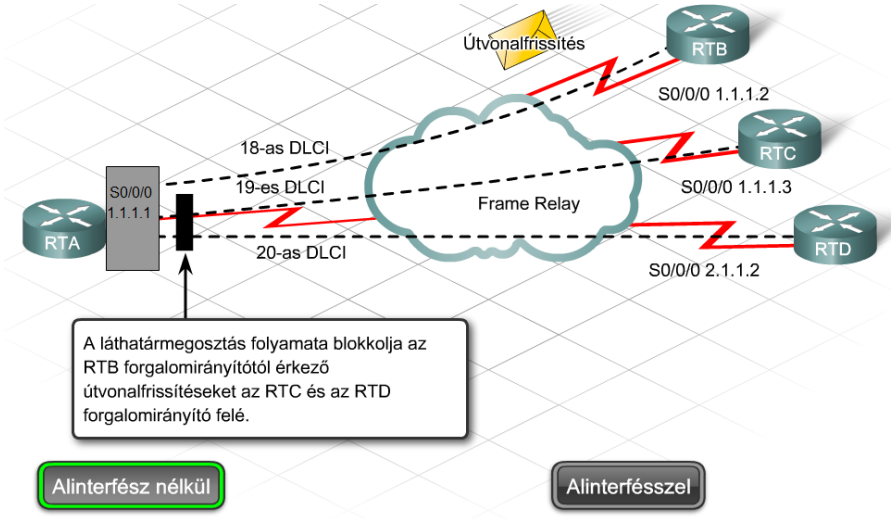
A látóhatár-megosztás problémájának elkerülése érdekében, a fizikai interfészen logikai alinterfészeket kell létrehozni. A Frame Relay alinterfészek két típusa a pont-pont és a többpontos alinterfész.

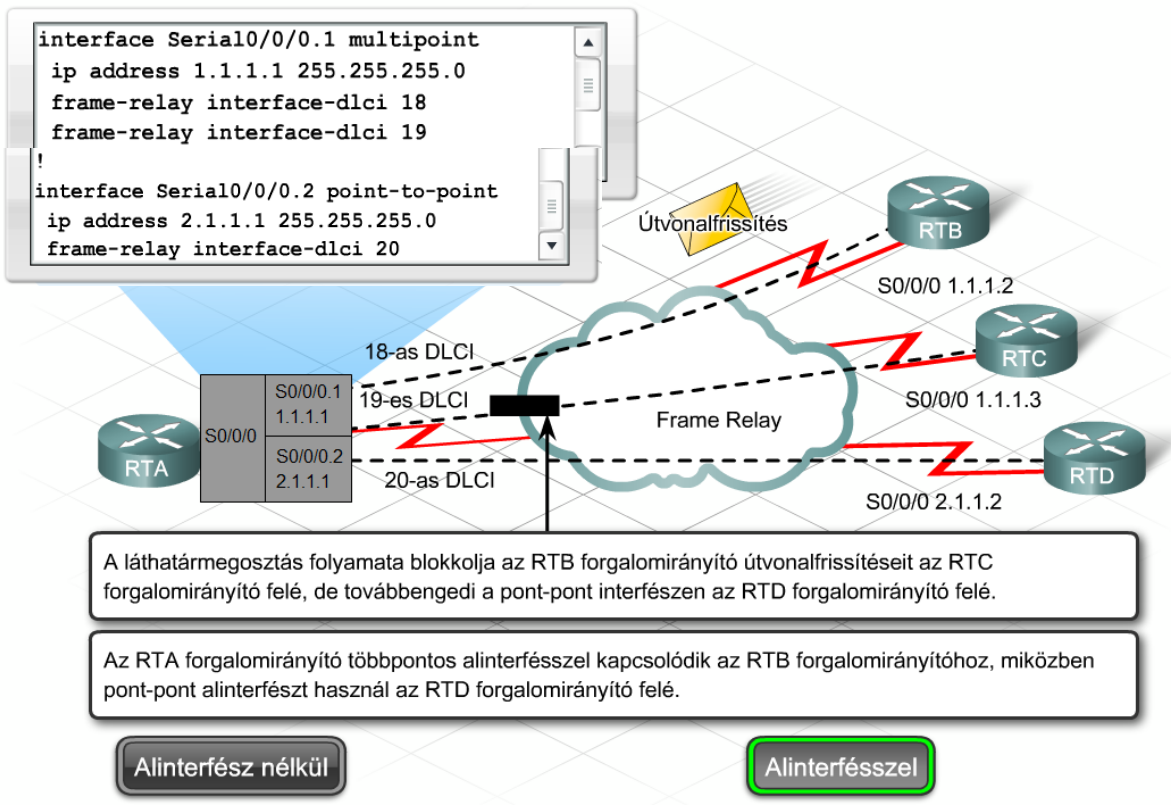
Pont-pont alinterfész

Pont-pont alinterfészek alkalmazásával, egyetlen, állandó virtuális áramkör (permanent virtual circuit, PVC) alakítható ki a távoli forgalomirányító egy másik fizikai interfészével vagy alinterfészével. Minden interfészpár külön alhálózat, és minden interfészen egyetlen DLCI van. Ebben a környezetben az üzenetszórás nem jelent problémát, hiszen a forgalomirányítók – hasonlóan a bérelt vonali kapcsolathoz – pont-pont kapcsolaton keresztül érintkeznek.

Többpontos alinterfész

A többpontos alinterfész lehetőséget nyújt egyetlen alinterfészen több PVC kiépítésére a távoli forgalomirányítók több fizikai interfészével vagy alinterfészével. Ez a beállítás nem oldja meg a látóhatár-megosztás problémáját. Többpontos alinterfészek és távolságvektor alapú irányítóprotokollok együttes alkalmazása esetén, a látóhatár-megosztást ki kell kapcsolni.





A Frame Relay konfigurálása után mindig ellenőrizni kell, hogy a rendszer az elvárásoknak megfelelően működik-e. A CPE forgalomirányítón számos show parancs áll rendelkezésre, melyek megjelenítik a Frame Relay helyi hurok és a PVC áramkörök állapotát.

A `show interfaces serial` parancs megjeleníti az interfészek állapotát, valamint a beágyazás, a DLCI, az LMI típusok és az LMI statisztikák részleteit. A show interface serial parancs által kiírt üzenet az interfész és a vonali protokoll felkapcsolt (up) állapotát jelzi, amennyiben a Frame Relay normálisan működik.

A Frame Relay kapcsoló és a CPE forgalomirányító közötti LMI üzenetcsere ellenőrzéséhez a `show frame-relay lmi` parancs használható.

A `show frame-relay pvc [interface interface] [dlci]` parancs alkalmazásával a konfigurált PVC-ket, valamint a forgalmi statisztikát jeleníthetjük meg. Szintén ez a parancs használható a forgalomirányító által fogadott FECN és BECN jelzéssel ellátott csomagok számának megtekintéséhez.

A `show frame-relay map` parancs lehetővé teszi az inverz ARP segítségével tanult aktuális adatok, a statikusan beállított hozzárendelések és a kapcsolatokról szóló információinak kijelzését.

Az inverz ARP útján tanult, dinamikusan létrehozott Frame Relay hozzárendelések törlésére a `clear frame-relay-inarp` parancs használható.

8.2.5 A Frame Relay működésének hibaelhárítása

Az alapvető Frame Relay kapcsolatok ellenőrzése után, a hálózattervező és a Hálózat Kft. szakemberei a tartalék lehetőségek tesztelését határozzák el. Beállítják a forgalomirányítók

közötti Ethernet kapcsolatokat, melyek a stadion fő hálózata és távoli telephelyei közötti, meglévő VPN kapcsolatokat szimulálják. Az ISP kapcsolat szimulálásához, egy új, ISPX elnevezésű forgalomirányítóval is kiegészítik a topológiát.

A tartalékkapcsolat konfigurálása

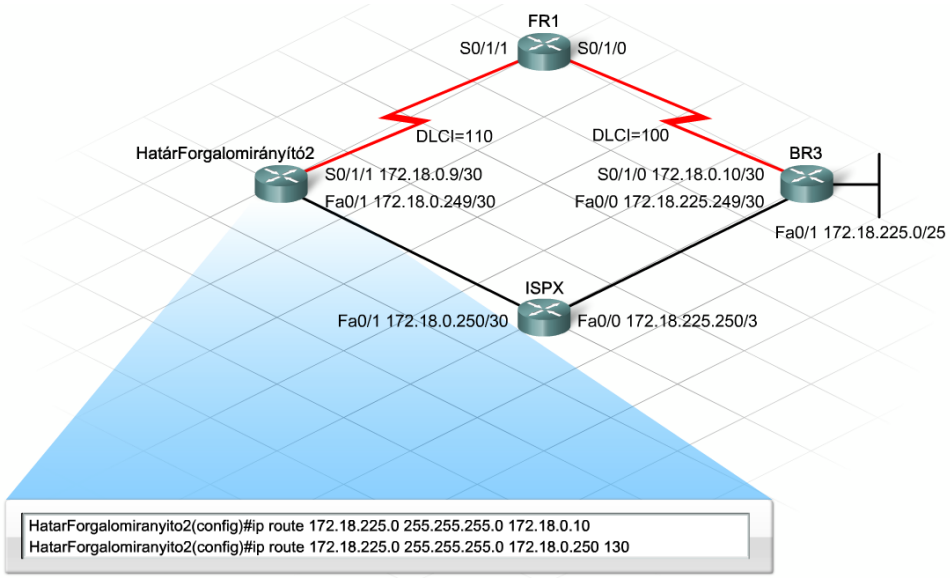
A két CPE forgalomirányító közötti forgalomirányítás konfigurációját úgy kell elvégezni, hogy a Frame Relay meghibásodása esetén a tartalék kapcsolat lépjen működésbe. Ennek egyik módja lebegő statikus útvonalak konfigurálása.

A lebegő statikus útvonal olyan útvonal, melynek adminisztratív távolsága nagyobb, mint a neki megfelelő dinamikusé. A szakemberek a Fast Ethernet interfészeket használják a statikus útvonalak konfigurálásához. A következő parancs alkalmazásával a Frame Relay útvonalénál nagyobb adminisztratív távolságot lehet definiálni:

```
Hatarforgalomiranyíto2(config)#ip route 172.18.225.0 255.255.255.0
172.18.0.250 130
```

Ennek az útvonalnak az adminisztratív távolsága 130, s ez csak akkor kerül az irányítótáblába, ha a kapcsolat meghibásodása vagy egyéb ok következtében a másik útvonal kiesik. Ily módon, amíg a Frame Relay kapcsolat elérhető, a Fast Ethernet interfész nincs használatban.

A tervező tesztelési tervet készít a tartalék kapcsolatok meghibásodás utáni működésének ellenőrzéséhez.



Elsődleges kapcsolati hibák elhárítása

A hálózattervezőnek a WAN hálózati tervében biztosítania kell a tartalék kapcsolatokat, és azok megfelelő működését egy elsődleges kapcsolati hiba esetén. A Frame Relay és a többi WAN technológia általában nagyon megbízható szolgáltatást nyújt, mégis előfordulhat, hogy teljesítményük az elvártnál kisebb lesz, vagy az áramkör megszakad. Ezekben az esetekben, valamint a hibaelhárítás és az elsődleges kapcsolat helyreállítási ideje alatt a tartalék kapcsolatok tudják szállítani a forgalmat.

A Frame Relay áramkörök hibaelhárítása több lépéses folyamat, mely magába foglalja az 1. 2. és 3. rétegbeli működést is.

A Frame Relay interfészek állapotának ellenőrzése

A Frame Relay konfigurációs hibáinak felderítését és elhárítását a `show interface serial` parancs alkalmazásával kell kezdeni. Ha a `show interface serial` parancs kimenete egyidejűleg az interfész és a vonali protokoll lekapcsolt (down) állapotát jelzi, akkor rendszerint 1. rétegbeli problémáról van szó. A javítandó hiba ebben az esetben valószínűleg a kábelezéssel vagy a CSU/DSU eszközzel kapcsolatos.

Az interfész akkor is lekapcsolt állapotba kerülhet, ha a DLCI statikus konfigurációja helytelen. Ennek ellenőrzését a show `frame-relay pvc` parancs segítségével lehet elvégezni. A PVC `DELETED` (törölt) állapota azt is jelezheti, hogy a CPE eszközön konfigurált DLCI nem egyezik meg az áramkörhöz rendelt DLCI-vel.

Az LMI működésének ellenőrzése

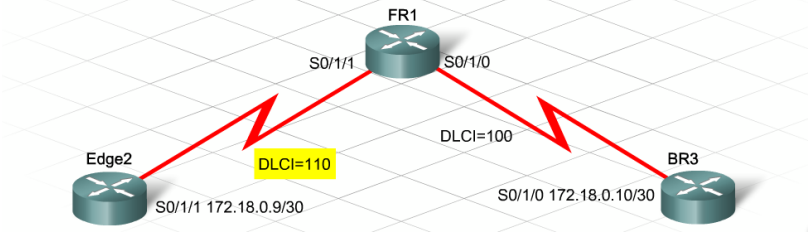
Ha a `show interface serial` parancs kimenete szerint az interfész felkapcsolt állapotban van, de a vonali protokoll leállt, 2. rétegbeli problémáról lehet szó. Ebben az esetben valószínűleg a soros interfész nem kap ébrenléti üzeneteket a Frame Relay kapcsolótól. A hibaelhárítás következő lépéseként a Frame Relay áramkörön kell ellenőrizni az LMI üzenetek küldését és fogadását. A `show frame-relay lmi` parancs kimenetében bármely érvénytelen értéket jelző sor (Invalid counter) nullától eltérő értéke mutatja a problémát. Érdemes ellenőrizni azt is, hogy az LMI típusa megfelelő-e az adott áramkör esetében.

```
Edge2#sh frame-relay pvc

PVC Statistics for interface Serial0/1/1 (Frame Relay DTE)

                Active      Inactive      Deleted       Static
  Local            0             0            1            0
  Switched         0             0            0            0
  Unused           0             0            0            0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = DELETED, INTERFACE = Serial0/1/1
```



Hibakeresés az LMI üzenetváltásban

Ha az LMI típusa megfelel az áramkörnek, de az üzenetek mégis érvénytelenek, a `debug frame-relay lmi` parancs további részletekkel szolgálhat. A `debug` parancs kimenetében látható az LMI üzenetek valós idejű küldése és fogadása a Frame Relay kapcsoló és a CPE forgalomirányító között.

A forgalomirányító által küldött LMI állapotüzeneteket a kimenet (`out`) felirattal jelzi. Az (`in`) a Frame Relay kapcsolótól kapott üzeneteket jelöli.

A `0-ás` típusú üzenet az LMI teljes körű állapotüzenete. Az állapotüzenetnél, a `dlci 110` és a `status 0x2` megjegyzés azt jelzi, hogy a `110-es DLCI` aktív. Az állapotmező tipikus értékei a következők:

0x0: hozzáadva és nem aktív – létezik a kapcsolón ez a DLCI, de nincs használatban.

0x2: hozzáadva és aktív - létezik a kapcsolón ez a DLCI, és használatban van.

0x4: törölve - a Frame Relay kapcsolón nincs ilyen DLCI beállítva a forgalomirányító felé. Ez az állapot akkor alakul ki, ha a DLCI-t törölték a forgalomirányítón, vagy ha a PVC-t törölték a Frame Relay felhőben.

Az 1-es típusú üzenetek az LMI üzenetváltásának ébrenléti üzeneteit jelzik.

A 3. rétegbeli működés ellenőrzése

Előfordulhat, hogy az 1. és 2. rétegbeli funkciók megfelelően működnek, de a PVC-n még sincs IP kommunikáció. A forgalomirányítónak, egy távoli forgalomirányító Frame Relay hálózaton keresztül történő eléréséhez szüksége van a helyes helyi DLCI és a távoli IP-cím egymáshoz rendelésére. Ha a távoli forgalomirányító IP-címe nem jelenik meg a Frame Relay címleképezési táblában, valószínűleg nem működik az inverz ARP. Ebben az esetben az IP-cím hozzárendelését kézileg kell konfigurálni a `frame-relay map ip {ip-cím}{dlci} [broadcast]` parancs segítségével.

A továbbiakban érdemes még ellenőrizni a hozzáférési listákat és az IP forgalomirányítást is. Bár az ezekkel kapcsolatos hibák nem kapcsolódnak szorosan a WAN működéséhez, mégis az áramkörök helytelen működésére utalhatnak.

A Frame Relay működésével kapcsolatos hibák elhárítása

```
Határforgalomirányító2# debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Határforgalomirányító2#
1w2d: Serial0/1/1(out): StEnq, myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/1/1(in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseq 140, myseq 140
1w2d: Serial0/1/1(out): StEnq, myseq 141, yourseen 140, DTE up
1w2d: datagramstart = 0xE008EC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 01 03 02 8D 8C
1w2d:
1w2d: Serial0/1/1(in): Status, myseq 142
1w2d: RT IE 1, length 1, type 0
1w2d: KA IE 3, length 2, yourseq 142, myseq 142
1w2d: PVC IE 0x7 , length 0x6 , dlci 110, status 0x2 , bw 0
```

8.2.6 A kockázatok és gyenge pontok felderítése

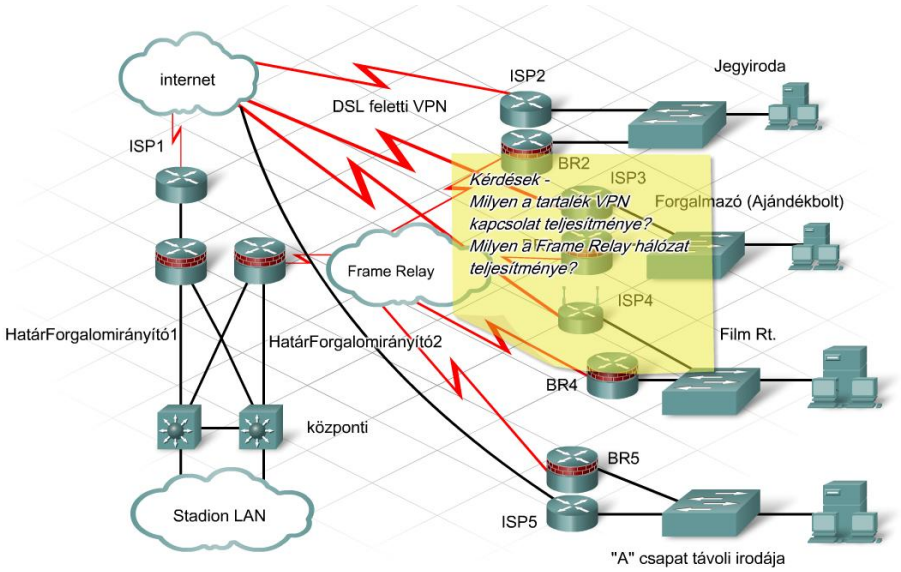
A teszthálózat ellenőrzésének befejezését követően, a hálózattervező és a Hálózat Kft. szakemberei megbeszélik a teszt eredményeit. A Frame Relay konfigurációja az elvárásoknak megfelelően működött, és a tartalék összeköttetések megvédték a WAN kapcsolatokat a Frame Relay kapcsolati hibája esetén.

Mindezek ellenére, a Frame Relay konfigurációval kapcsolatban felmerül némi kockázati tényező, amit a stadion vezetőségével meg kell beszélni.

Kockázati tényezők

A legnagyobb kockázatot a VPN kapcsolatok teljesítménye jelenti, amikor tartalék kapcsolatként működésbe lépnek. Amikor a hang, illetve videó elemeket is tartalmazó WAN forgalomnak a VPN kapcsolaton kell áthaladnia, a szolgáltatás minőségével kapcsolatban problémák merülhetnek fel. Az ISP-n keresztül vezető jelenlegi VPN kapcsolaton nincs garantált szolgáltatási szint, és nem érhetők el azok a mechanizmusok sem, melyek a QoS-t biztosítanák. Hiba esetén ezért a tartalék összeköttetés csak korlátozott szintű kapcsolatot biztosít.

A teljesítmény tesztelése lehetetlen a jelenlegi TSP Frame Relay hálózatán keresztül; ezért marad néhány kockázati tényező a tervben. A terv végleges elfogadása nem történhet meg a valódi hálózaton végzett próbák eredményeinek ismerete nélkül.



8.3 Távmunkás támogatás prototípus

8.3.1 A VPN céljának és követelményeinek meghatározása

A stadion hálózati tervének elsődleges üzleti célja, hogy további szolgáltatásokat nyújtson a forgalmazóknak és látogatóknak, ezzel is növelve a stadionnal kapcsolatos kedvező tapasztalatokat, növelve a stadion vonzerejét.

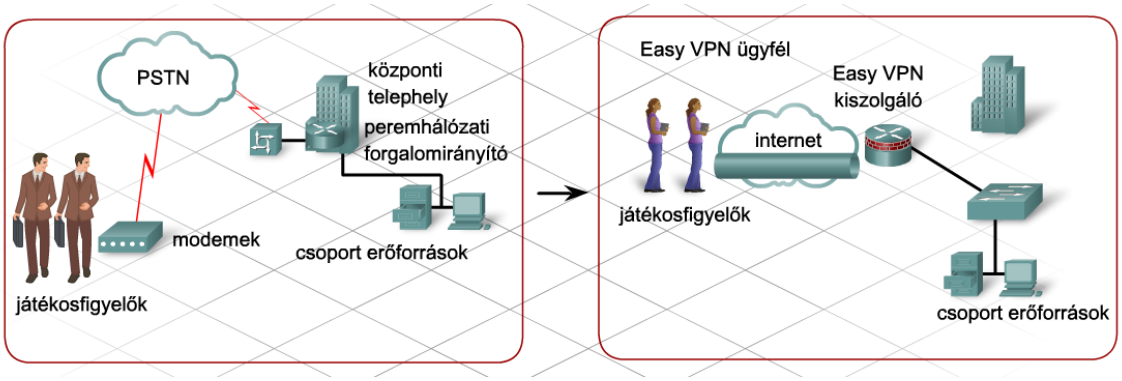
Csapatok irodáival szemben támasztott követelmények

A csapatok irodái biztonságos módszereket igényelnek ahhoz, hogy a játékosaik csatlakozni tudjanak a csapat kiszolgálóihoz. Előfordulhat, hogy amikor a játékosok a stadionon kívül tartózkodnak, a jövőbeni kilátásokkal kapcsolatos információt kell küldeniük a csapat kiszolgálóira. Mivel ezek az adatok különösen bizalmasak, a csapat azt szeretné, ha a játékosok VPN kapcsolaton keresztül tudnának távolról csatlakozni. A VPN a belső magánhálózat egyfajta kiterjesztése. VPN hálózatokkal az adatok biztonságosan küldhetők olyan osztott hozzáférésű vagy nyilvános hálózatokon keresztül, mint amilyen például az internet. A hálózattervezőnek figyelembe kell vennie, milyen hatása van ezeknek a szolgáltatásoknak a hálózatra.

A VPN működése

A VPN pont-pont kapcsolatot emulál. A VPN, a forgalomirányítási információkat tartalmazó fejrészt az adatokkal együtt beágyazza, ezzel lehetővé válik az adatok nyilvános hálózaton történő továbbítása a cél felé. Azért, hogy az adatokat bizalmasan lehessen kezelni, a privát kapcsolat emulálása során a beágyazott adatokat titkosítják. A titkosító algoritmus biztosítja, hogy a nyilvános hálózaton elfogott adatokat ne lehessen elolvasni a titkosító kulcsok nélkül.

A csapat játékosai, valamint azok az alkalmazottak, akik otthonról vagy út közben dolgoznak, VPN kapcsolaton keresztül, távolról érhetik el a stadionban elhelyezett kiszolgálót. A felhasználók szemszögéből, a VPN egy pont-pont kapcsolat a számítógépük (VPN ügyfél) és a stadionban található VPN végpont (VPN kiszolgáló vagy VPN koncentrátor) között.



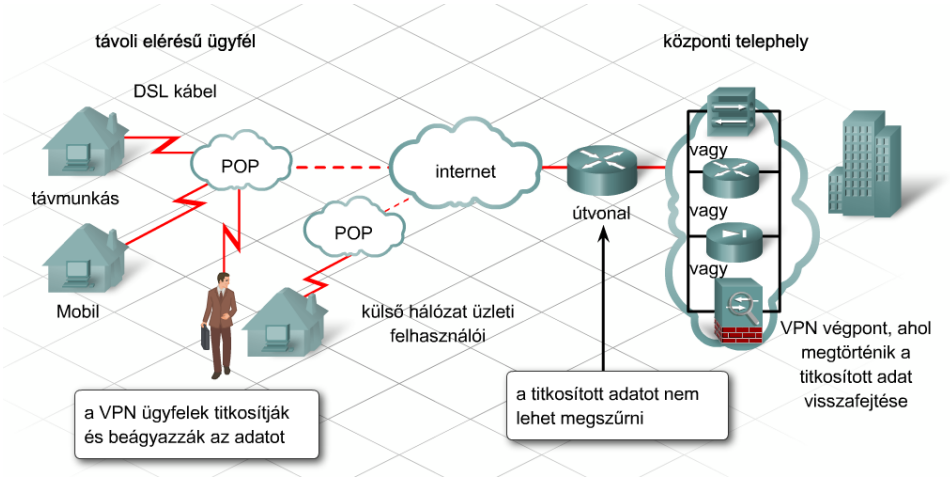
A magánhálózat távoli felhasználókra történő kiterjesztésének kockázta is van.

VPN biztonság

Sok vállalatnál, azokat a dolgozókat, akik távolról, VPN kapcsolaton keresztül érik el a központban lévő erőforrásokat, épp úgy „megbízhatóként” kezelik, mint akik a helyszínen dolgoznak. A belső dolgozókkal ellentétben, a VPN felhasználók sokszor nem biztonságos eszközről vagy nem biztonságos, nyilvános helyről csatlakoznak a hálózathoz. Épp ezért nagy odafigyelést igényel annak biztosítása, hogy a távmunkások ne érjék el a hálózat olyan területeit vagy azokat az erőforrásokat, melyek a munkájukhoz nem szükségesek.

A VPN kiszolgáló elhelyezése

A hálózattervező tisztában van vele, hogy a titkosított adatok szűrése lehetetlen mindaddig, míg azok nincsenek a titkosítatlan formára visszaalakítva a VPN kiszolgálói végpontnál. A fentiek miatt különösen fontos kérdés, hogy a VPN kiszolgáló hol helyezkedik el. Olyan helyen kell lennie, ahol a beérkező csomagok megvizsgálhatók és szűrhetők, mielőtt tovább haladnának a belső hálózat erőforrásaihoz.



8.3.2 A tesztelési terv elkészítése

Mit kell tesztelni?

A stadion VPN hálózatokat használ az ajándékbolt és a jegyiroda eléréséhez. Ezeket a telephelyközi (site-to-site) VPN hálózatokat az ISP felügyeli, és nincs szükség a tesztelésükre.

A csapatjákékosok támogatása

Két lehetőség van a játékosok távoli ügyfeleikkel történő kapcsolattartásához szükséges VPN biztosítására:

- **1. lehetőség:** A stadion vezetősége további VPN szolgáltatásokat vesz igénybe a jelenlegi internetszolgáltatótól
- **2. lehetőség:** A VPN kiszolgálót a stadion hálózatában helyezik el

A VPN kiszolgáló felügyelete

A tervező osztott alagút-technika használatát javasolja, ami lehetővé teszi a felhasználók számára, hogy a vállalati hálózatba tartó csomagokat a VPN alagúton keresztül küldjék tovább, miközben az összes többi forgalom a VPN ügyfél helyi hálózatán keresztül éri el az internetet. A tervezőnek fel kell mérnie, hogy a stadion jelenlegi személyzete képesek-e a VPN kiszolgáló konfigurálására és felügyeletére. Ennek érdekében úgy határoz, hogy VPN kiszolgáló és ügyfél programot telepít, és teszteli mennyire egyszerű ezek konfigurálása és felügyelete. A VPN beállítása után ellenőrzi a VPN kiszolgáló elhelyezését a hálózatban, illetve azt is, hogy a hozzáférési listák megfelelően szűrik-e a VPN kapcsolaton bejövő forgalmat.

Cisco EasyVPN

A tervező úgy határoz, hogy a távoli felhasználók VPN kapcsolatának beállítására és felügyeletére a legjobb megoldás a Cisco EasyVPN használata. Az EasyVPN egy Cisco IOS szoftveres eszköz, amely megkönnyíti a Cisco biztonsági berendezéseinek beállítását, illetve a forgalomirányító VPN kiszolgálóként vagy végpontként történő konfigurálását.

A tervező a teszthálózat felépítéséhez IP Advanced Security támogatással rendelkező 1841-es forgalomirányítót választ. Az 1841-es forgalomirányítón a Cisco SDM kezelőfelület használható az EasyVPN kiszolgáló távoli ügyfeleinek konfigurálásához.

Üzleti célkitűzés	Az általános siker feltétele
A felhasználói elégedettség növelése további szolgáltatások bevezetésével a felhasználóknak és forgalmazóknak.	A sportcsapat alkalmazottai VPN ügyfél segítségével képesek csatlakozni a stadion hálózatában elhelyezett csoport-erőforrásokhoz.

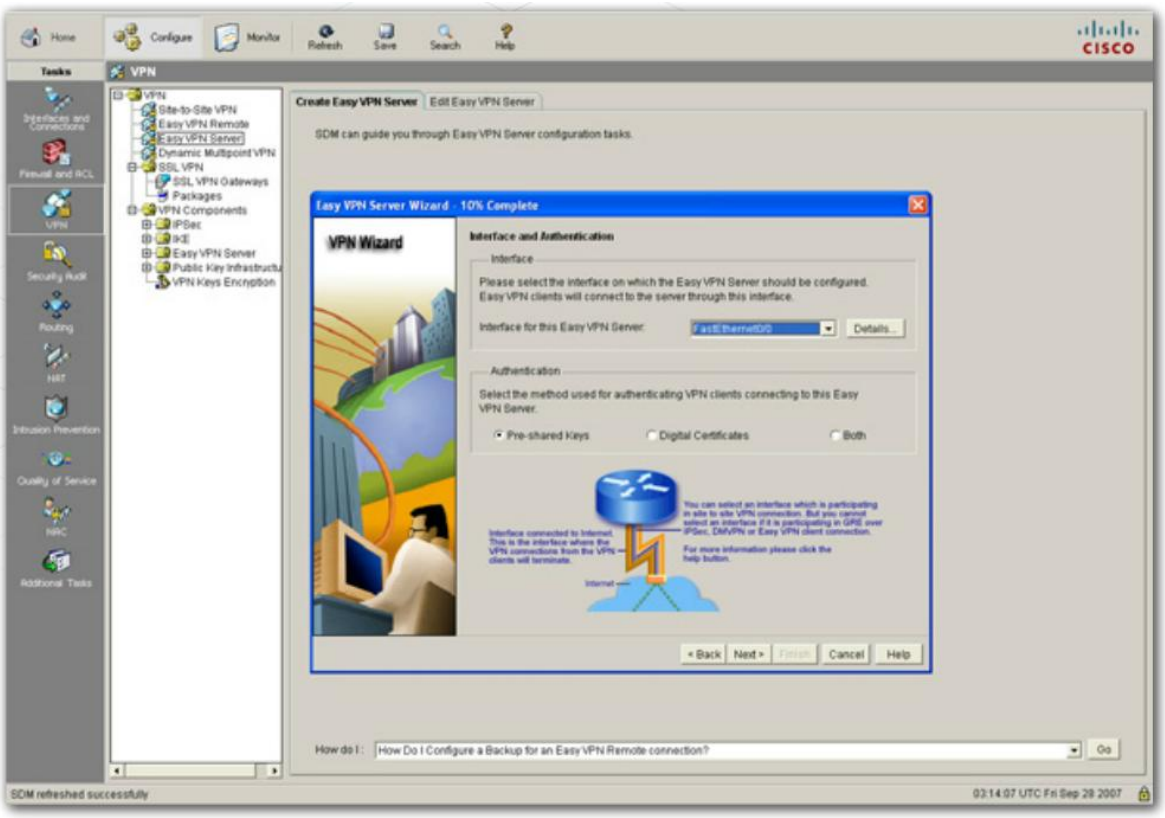
Technikai követelmények	Az eredményesség feltétele
Méretezhetőség	
Osztott alagúttechnika konfigurálása, hogy kizárólag a stadion erőforrásaihoz címzett forgalom legyen engedélyezve a VPN kapcsolaton keresztül.	A LAN teljesítményére ne legyen hatással, ha VPN ügyfelekkel bővül a hálózat.
Elérhetőség	
A hibakezelés érdekében redundáns VPN kiszolgálók konfigurálása.	Az egyik VPN kiszolgáló meghibásodása következtében a kapcsolat ne szakadjon meg.
Biztonság	
IPSec-et használó VPN-ek konfigurálása.	Az EasyVPN ügyfél konfigurációja magas szintű hálózati biztonságot támogat.
Felügyelhetőség	
Cisco EasyVPN használata a VPN beállítások konfigurálására.	Könnyű elvégezni és felügyelni a konfigurációkat.
SDM használata a VPN kiszolgáló konfigurálására és felügyelésére.	Könnyű elvégezni és felügyelni a konfigurációkat.

A Cisco EasyVPN megoldás

A könnyű telepíthetőségnek fontos szerepe van abban, hogy a VPN ki tudja szolgálni a máshol dolgozó játékosokat. A Cisco EasyVPN két elemből áll:

- **Cisco EasyVPN kiszolgáló** – A kiszolgáló lehet forgalomirányító vagy dedikált VPN átjáró, mint például egy PIX tűzfal vagy egy VPN koncentrátor. A VPN átjáró Cisco EasyVPN program segítségével egyaránt képes távoli hozzáférésű VPN (remote access VPN) és a telephelyközi VPN (site-to-site VPN) végpontjaként is működni.
- **Cisco EasyVPN távoli komponens** (Cisco EasyVPN Remote) – Lehetővé teszi távoli eszközök számára egy Cisco EasyVPN kiszolgáló biztonsági intézkedéseinek fogadását. Ez minimalizálja a konfigurációs igényeket a távoli VPN oldalon. A távoli Cisco EasyVPN segítségével a VPN paraméterek átküldhetők a kiszolgálóról a távoli eszközökre. A VPN paraméterek tartalmazzák a belső IP-címeket, a belső alhálózati maszkokat és a DHCP kiszolgálók címeit.

A hálózattervező tesztelési tervet készít, mellyel ellenőrizhető a VPN kiszolgáló Cisco EasyVPN-nel történő konfigurálása és az ügyfélprogram beállítása.



8.3.3 A topológia, az eszközök és a VPN topológia választásának ellenőrzése

Mielőtt a tervező a VPN teszthálózatának konfigurációját tesztelné, számos különböző protokollt, algoritmust és lehetőséget kell figyelembe vennie.

A VPN összetevői

A VPN hálózatoknak két fontos alkotóeleme van:

- Alagút-technika a virtuális hálózat kialakításához
- Titkosítás az információk bizalmas kezeléséhez és a biztonság megvalósításához

A virtuális hálózat

A virtuális hálózat kialakításához egy alagutat kell létrehozni a két végpont között. Telephelyközi VPN esetén, az állomások normál TCP/IP alapú forgalmat küldenek és fogadnak a VPN átjárón keresztül. Az átjáró lehet forgalomirányító, tűzfal, VPN koncentrátor vagy biztonsági berendezés. Az átjáró feladata az egyik oldalon a kimenő forgalmat beágyazni, majd átküldeni az alagúton a távoli oldal egyenrangú átjárója felé. Az alagút önmagában nem garantálja a biztonságot, egyszerűen a helyi hálózat kiterjesztését végzi nyilvános hálózaton vagy WAN-on keresztül. Az alagút titkosított és titkosítatlan forgalmat egyaránt tud továbbítani. A távoli átjáró kibontja a beérkező csomag fejrészét, visszafejti a titkosított csomagot, majd továbbküldi a privát

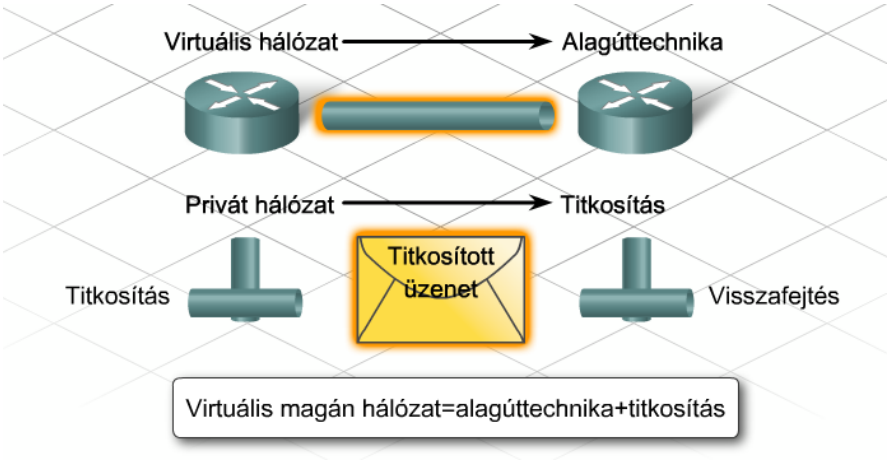
hálózatában található célállomás felé. Távoli hozzáférésű VPN esetén, a felhasználó számítógépén futó VPN ügyfélprogramnak kell kapcsolatba lépnie az átjáróval az alagút felépítéséhez.

VPN alagút-technikai protokollok

A VPN alagutak kialakításához számos különböző beágyazási protokoll használható, melyek a következők:

- általános forgalomirányítási beágyazás (Generic Routing Encapsulation, GRE)
- IP biztonság (IP Security, IPSec)
- 2. rétegbeli továbbító protokoll (Layer 2 Forwarding Protocol, L2F)
- pont-pont alagút protokoll (Point-to-Point Tunneling Protocol, PPTP)
- 2. rétegbeli alagút protokoll (Layer 2 Tunneling Protocol, L2TP)

Nem minden protokoll nyújtja ugyanazt a biztonsági szintet.



Az általános forgalomirányítási beágyazás (GRE - Generic Routing Encapsulation) meghatározott útvonalat biztosít a megosztott WAN hálózaton keresztül. A beágyazás során új fejrészt ad a csomaghoz, így biztosítja a kézbesítését az adott célhoz. Mivel a forgalom csak az egyik végponton tud belépni az alagútba és csak a másik végén tudja elhagyni azt, így a hálózat magán jellegű. Az alagút nem tudja biztosítani az adatok titkos továbbítását (ahogy a titkosítás), de képes a titkosított adatok átvitelére.

Az IP biztonság (IPSec - IP Security) a 3. rétegben, az IP csomagok védelmét és hitelesítését biztosítja a résztvevő IPSec eszközök között. Nem kötődik egyik meghatározott titkosítási, hitelesítési, biztonsági vagy kulcscserélési algoritmushoz sem. Nyílt szabványok keretrendszere.

A 2. rétegbeli továbbító protokoll (L2F - Layer 2 Forwarding Protocol) a Cisco által kifejlesztett protokoll, mely 2. rétegbeli alagúttechnikával támogatja az internet feletti, biztonságos virtuális magán telefonhálózatok megvalósítását.

A pont-pont alagút protokollt (PPTP - Point-to-Point Tunneling Protocol) a Microsoft fejlesztette ki, és az RFC2637 definiálja. Széles körben alkalmazzák Windows ügyfélprogramokban VPN-ek TCP/IP hálózatokon keresztül történő létrehozására.

A 2. rétegbeli alagút protokoll (L2TP - Layer 2 Tunneling Protocol) egy IETF szabvány, mely egyesíti a PPTP és az LF2 szabványok legjobb jellemzőit. Nyilvános hálózaton keresztül, mint az internet is, IP használatával alagúttechnikai pont-pont protokollt alkalmaz. Mivel az alagút a 2. rétegben működik, a felsőbb rétegek

nem tudnak róla. A GRE és L2TP protokollhoz hasonlóan bármilyen 3. rétegbeli protokoll beágyazására képes.

Titkosítási algoritmusok:

- ***Adattitkosítási szabvány** (Data Encryption Standard) - Az IBM fejlesztette ki. 56-bites kulccsal biztosítja az adatok biztonságos titkosítását. Szimmetrikus kulcsú titkosítási rendszer.*
- ***Háromszoros DES (3DES) algoritmus** - Az 56-bites DES változata. A DES-hez hasonlóan működik. Az adatot 64-bites blokkokra vágja, majd minden blokkot háromszor, egymástól független 56 bites kulccsal titkosít. Lényegesen jobb titkosítást eredményez az 56-bites DES-nél. Szimmetrikus kulcsú titkosítási rendszer.*
- ***Fejlett titkosítási szabvány** (Advanced Encryption Standard, AES) - A Nemzeti Szabványügyi és Technológiai Intézet (NIST - The National Institute of Standards and Technology) mostanában a titkosítási eszközökben lévő DES helyettesítésére alkalmazza. Az AES nagyobb biztonságot nyújt a DES-nél és kiszámíthatóan hatékonyabb, mint a 3DES. Az AES algoritmus esetén három különböző kulcshosszra van lehetőség: 128, 192 és 256 bit*
- ***Rivest - Shamir - Adleman** (RSA) - Aszimmetrikus kulcsú titkosítási rendszer. 512, 768, 1024 bites vagy még hosszabb kulcsot alkalmaz. Az IPSec nem használja adattitkosításra. Az IKE csak RSA titkosítást használ a másik fél hitelesítése közben.*

A VPN technológiák titkosítási algoritmusokat használnak annak érdekében, hogy az esetlegesen elfogott adatok elolvasását megakadályozzák. A titkosítási algoritmusok olyan matematikai függvények, melyek az üzenetet egy karakterlánccal, az úgynevezett kulccsal kombinálják. Az eredmény egy olyan olvashatatlan kód, melynek megfejtése a megfelelő kulcs nélkül mérhetetlenül nehéz, vagy teljesen lehetetlen. A VPN hálózatok leggyakrabban a következő titkosítási eljárásokat használják: adattitkosítási szabvány (Data Encryption Standard, DES), háromszoros DES (Triple DES, 3DES), fejlett titkosítási szabvány (Advanced Encryption Standard, AES), és a Rivest - Shamir - Adleman (RSA).

Titkosítási algoritmusok

Az olyan titkosítási algoritmusoknak, mint például a DES vagy a 3DES, szimmetrikus, osztott használatú kulcsra van szükségük a titkosításhoz és a visszafejtéshez. A kulcsokat a rendszergazda kézileg tudja beállítani.

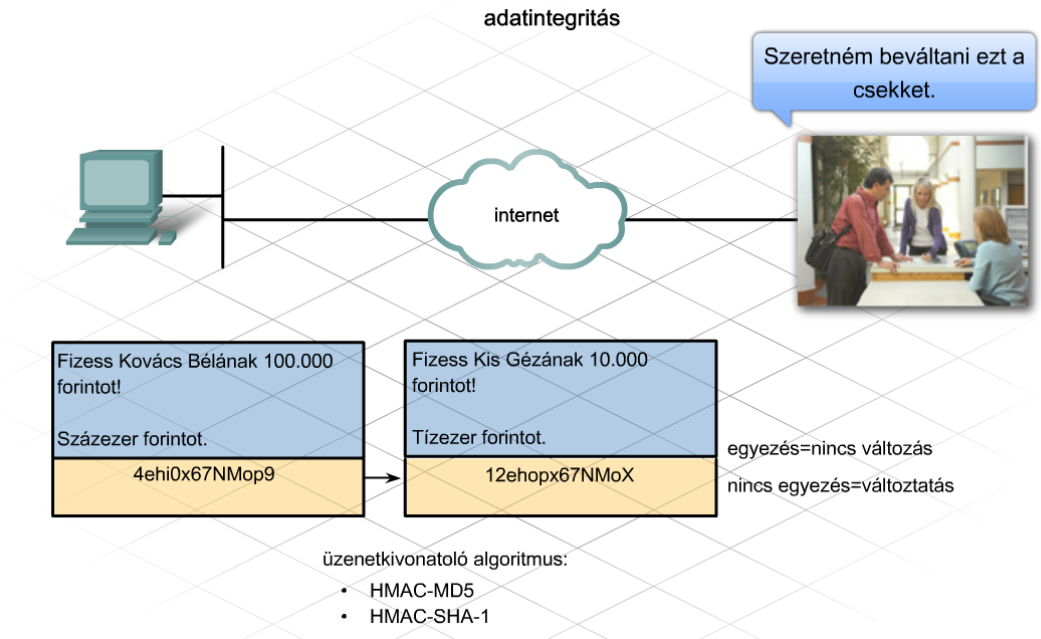
Más megoldásban a kulcs beállítását egy kulcscserélési módszer végzi. A Diffie-Hellman (DH) kulcsegyeztetés egy nyilvános kulcscserélési módszer. Ez lehetővé teszi két fél között egy osztott, titkos kulcs bevezetését, melyet a nem biztonságos csatornán folyó kommunikáció ideje alatt kizárólag ők ismernek. A Diffie-Hellman csoportok a használható titkosítások különböző típusait határozzák meg:

- **1-es DH csoport** – 768 bites titkosítást határoz meg.
- **2-es DH csoport** – Kizárólag Cisco IOS, PIX tűzfal és Cisco Adaptive Security Appliances (ASA) eszközök esetén használható. 1024 bites titkosítást határoz meg.
- **5-ös DH csoport** – Abban az esetben használható, ha az adott szoftver támogatja. 1536 bites titkosítást határoz meg.

Az VPN adatok elfogásának és megváltoztatásának megakadályozására egy adatintegritási algoritmus használható, mely egy hash értéket ad az üzenethez. Ha a küldött és a fogadott hash

érték megegyezik egymással, a kapott üzenet az elküldöttnek pontos másolataként fogadható. A kulcsos kivonatolt üzenethitelesítő kód (Keyed Hashed Message Authentication Code, HMAC) egy adatintegritási algoritmus, mely biztosítja az üzenet sértetlenségét. Két ismert HMAC algoritmus létezik:

- HMAC- 5-ös típusú üzenetkivonatolás (Message Digest 5, MD5) – Ez az algoritmus 128 bites osztott titkos kulcsot használ. A változó hosszúságú üzenetet és a 128 bites osztott titkos kulcsot összekapcsolja, majd lefuttatja a HMAC-MD5 kivonatoló algoritmuson. Az eredmény egy 128 bites kivonat, mely az eredeti üzenethez csatolva jut el a távoli végponthoz.
- HMAC-1-es biztonságos kivonatoló algoritmus (HMAC-Secure Hash Algorithm 1, HMAC-SHA-1) – Ez az algoritmus 160 bites titkos kulcsot használ. A változó hosszúságú üzenetet és a 160 bites osztott titkos kulcsot összekapcsolja, majd lefuttatja a HMAC-SHA-1 kivonatoló algoritmuson. Az eredmény egy 160 bites kivonat, mely az eredeti üzenethez csatolva jut el a távoli végponthoz.



8.3.4 A távmunkások VPN kapcsolatának teszthálózata

A stadion javasolt hálózatában a hálózattervező IPSec technológiát választ a távoli elérésű VPN hálózatokhoz.

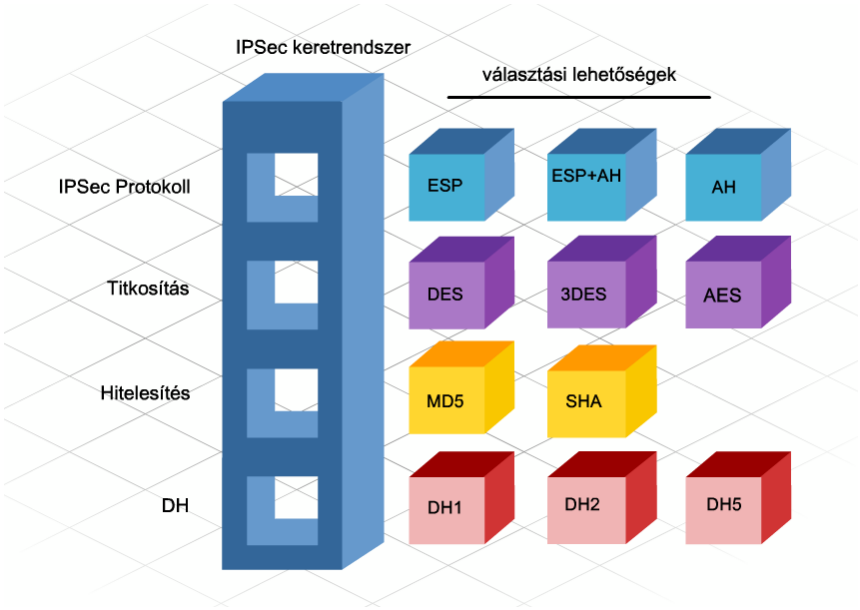
IPSec

Az IPSec nyílt szabványok keretrendszere. Biztosítja az adatok védelmét, integritását és hitelesítését a kommunikációban résztvevő csomópontok között. Az IPSec a 3. rétegben nyújtja a szolgáltatásait.

Az IPSec a létező titkosító, hitelesítő és kulcscserélő algoritmusokra támaszkodik. A VPN kiszolgáló konfigurálása esetén az alábbi beállításokat igényli:

- **IPSec protokoll** – Választható a beágyazott biztonsági adat (Encapsulating Security Payload, ESP) és a hitelesítési fejrész (Authentication Header, AH) protokoll, vagy a kettő együtt.
- **A kívánt biztonsági szintnek megfelelő titkosító algoritmus** – Választási lehetőség a DES, 3DES vagy az AES.
- **Hitelesítő algoritmus az adatok sértetlensége érdekében** – Választható az MD5 vagy az SHA.
- **Diffie-Hellman csoport** – Választási lehetőség a DH1, a DH2 és a DH5 (amennyiben támogatott).

A IPSec képes az Internetes kulcscsere (Internet Key Exchange, IKE) használatára a protokollok és algoritmusok egyeztetése érdekében. Az IKE a szükséges titkosító és hitelesítő kulcsot is elő tudja állítani.



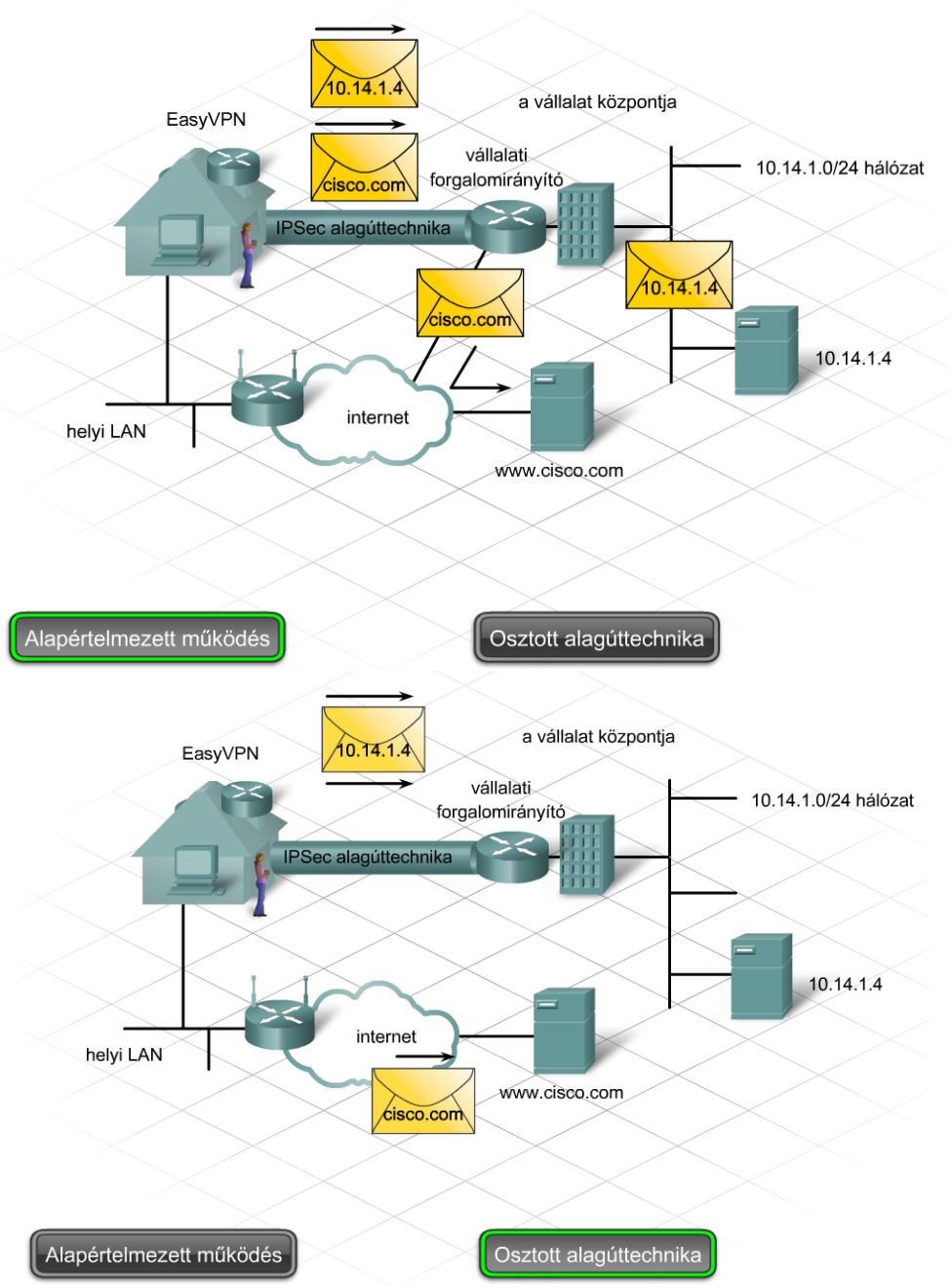
A VPN ügyfelek IPv4 címmel ellátott logikai hálózati interfészt kapnak. Ez az IPv4 cím rendszerint egy privát IP-cím, mely a központi telephely belső hálózatához tartozik. A fentiek miatt előfordulhat, hogy a VPN felhasználók nem tudják elérni a helyi hálózati erőforrásaikat (pl. a nyomtatókat vagy a kiszolgálókat).

Osztott alagúttechnika

Alapszintű VPN környezetben a logikai hálózati interfész alkalmazásával az ügyféltől származó összes forgalom titkosításra kerül. A csomag ezután - a célállomás helyétől függetlenül - a VPN kiszolgálóhoz jut.

Az osztott alagúttechnika lehetőséget nyújt a felhasználónak, hogy csak a központi hálózatba címzett forgalmat küldje az alagúton keresztül. A többi forgalmat a VPN ügyfél a saját helyi hálózatán keresztül küldheti az internet felé. Ilyen jellegű forgalmat generál például az azonnali üzenetváltás, az elektronikus levelezés és a web böngészés. Ha az osztott alagúttechnikát a VPN

kiszolgálón konfigurálták, akkor a Cisco VPN ügyfélen az Allow Local LAN Access lehetőség beállításával engedélyezhető ez a szolgáltatás. Az osztott alagúttechnika használata növeli a biztonsági kockázatot, mivel az ügyfél internet felöli oldaláról támadás érheti a védett hálózatot.



8.3.5 A VPN kiszolgáló elhelyezésének jóváhagyása

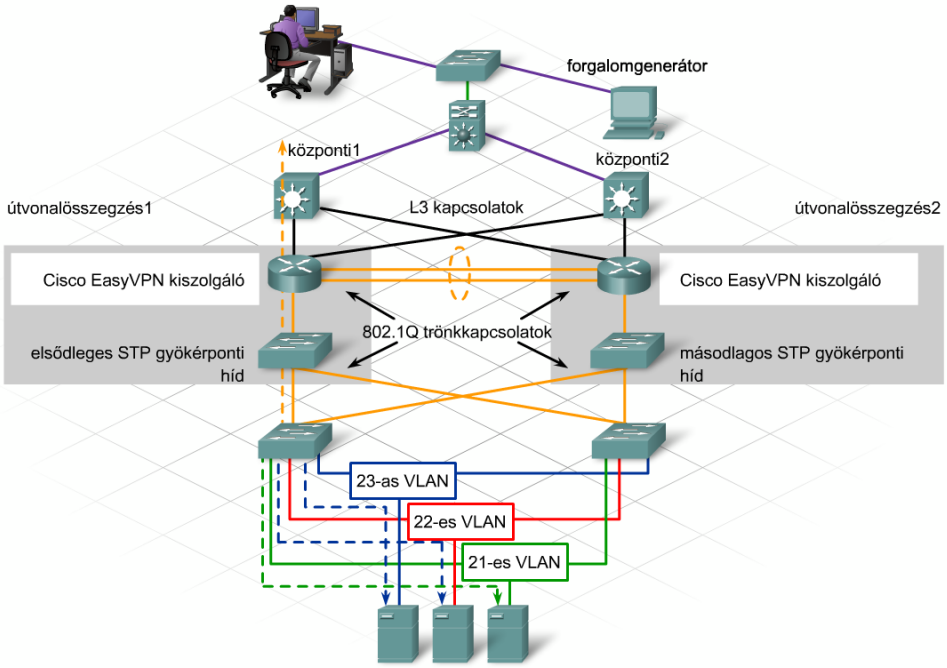
A hálózattervezőnek döntenie kell a VPN kiszolgáló helyéről, mielőtt még meghatározná a forgalomirányítás és szűrés módját és helyét.

A VPN kiszolgáló elhelyezése

A VPN kiszolgálókat gyakran a hálózat WAN felőli határán helyezik el. Ilyen esetekben tűzfalak vagy hozzáférési listák használhatók annak érdekében, hogy a VPN felhasználók csak a megfelelő hálózati erőforrásokat érjék el.

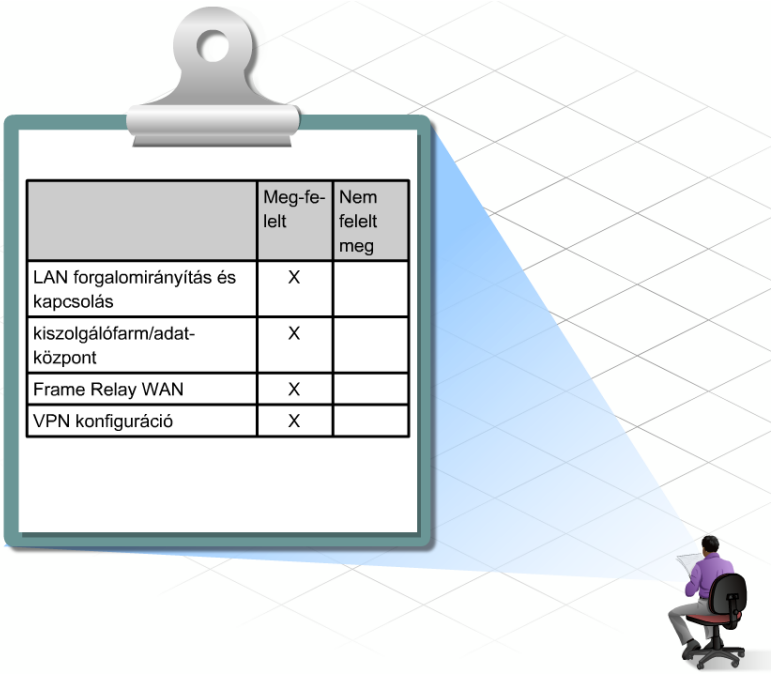
Arra az esetre, ha a stadion vezetősége úgy határozna, hogy helyi VPN kiszolgálót telepít, a tervező azt javasolja, hogy ez ugyanazon az eszközön legyen, amelyik a kiszolgálóknak nyújt tűzfalszűrést. A távoli felhasználók üzenetei így visszafejthetők és szűrhetők, mielőtt elérnék a kiszolgálót.

A tervező elkészíti a kiszolgálófarm próbahálózatának topológiájához hasonlító tesztelési topológiát. Ezt követően, a VPN és a hozzáférési listák működésének ellenőrzéséhez, üzembe helyezési ellenőrzőlistát és tesztelési tervet állít össze.



8.3.6 A kockázatok és gyengepontok felderítése

Amint a hálózattervező végzett a teszteléssel, a terv kockázati szintjének meghatározása érdekében kielemzi az eredményeket.



	Meg-fe-lelt	Nem felelt meg
LAN forgalomirányítás és kapcsolás	X	
kiszolgálófarm/adat-központ	X	
Frame Relay WAN	X	
VPN konfiguráció	X	

A VPN tervében rejlő kockázatok

A távoli alkalmazottak kiszolgálását megcélzó VPN terv legnagyobb kockázata azzal kapcsolatos, hogy a jelenleg alkalmazott informatikai szakemberek képesek-e a VPN kiszolgáló konfigurálására és karbantartására. Az ügyfeleknek a felmerülő igények szerinti azonnali konfigurálása szintén kockázati tényezőt jelent.

A stadion hálózatában a Cisco

EasyVPN és az SDM használata megfelelő választásnak bizonyult a távoli hozzáférésű VPN konfigurálására és karbantartására. Ezzel az összeállítással viszonylag könnyű biztonságos kapcsolatot kiépíteni a távmunkások számára.

A teljes teszthálózat ellenőrzésének befejezése után, a tervező és a Hálózat Kft. szakemberei együtt elkészítik a stadion hálózatának fejlesztéséről szóló végleges tervet.

8.4 A fejezet összefoglalása

- A távoli kapcsolatok tesztelése nehezebb a LAN terv tesztelésénél.
- A hálózattervezőnek a teszteléshez három különböző módszer áll rendelkezésére:
    - szimulációs program, mint a Packet Tracer
    - szimulált kapcsolatokat alkalmazó teszthálózat
    - valódi környezetben végzett próba
- A számítógépes programok, mint a Packet Tracer is, lehetővé teszik, hogy a hálózattervező tesztelje a konfigurációkat mielőtt valódi eszközökön alkalmazná. A szimulációs programok előnyei:
    - kis költség
    - rugalmasság
    - méretezhetőség
    - kezelhetőség
- A szimuláció hátránya lehet, hogy esetleg korlátozott lehetőség áll rendelkezésre vagy nem valóságos teljesítményt mutat.
- A WAN kapcsolatok keresztkötésű kábellel és meghatározott eszközkonfigurációval szimulálhatók teszthálózati környezetben.
- Amikor két soros interfész összeköttetésére keresztkötésű kábelt alkalmazunk, az áramkörben az egyik eszköznek órajelet kell szolgáltatnia. Cisco forgalomirányítón ez a clock rate paranccsal hajtható végre.
- A Frame Relay egy nagy teljesítményű WAN protokoll, melyet a Nemzetközi Telekommunikációs Szövetség Telekommunikációs Szabványosítási Csoportja (International Telecommunication Union Telecommunication Standardization Sector, ITU-T) szabványosított.
- Minden kapcsolata legalább három összetevőből áll:
    - A helyi pont-pont kapcsolat, mely a helyi CPE forgalomirányító és a TSP Frame Relay kapcsolója között van.
    - A TSP csomagkapcsolt hálózata
    - A távoli pont-pont kapcsolat, mellyel a távoli telephely csatlakozik a szolgáltatóhoz.
- Egyetlen, fizikai helyi hurok áramkörén egynél több virtuális áramkör is működhet. A virtuális áramkörök végpontjaihoz egy-egy adatkapcsolati azonosító (DLCI - data-link connection identifier) van hozzárendelve.
- A vállalt adatsebesség (CIR - committed information rate) a legnagyobb átlagos átviteli sebességet határozza meg, mellyel a hálózat normál körülmények között továbbítja az adatokat.
- A hálózati forgalomszabályozás támogatására a Frame Relay két lehetőséget biztosít:
- Előremutató explicit torlódásjelzés (FECN - Forward Explicit Congestion Notification)

    - Visszirányú explicit torlódásjelzés (BECN - Backward Explicit Congestion Notification)
    - Az Inverz címmeghatározó protokoll (Inverse ARP - Inverse Address Resolution Protocol) a 3. rétegbeli címek és DLCI értékek megfeleltetését teszi lehetővé.
- A Frame Relay egy nem szórásos, többszörös hozzáférésű (NBMA - nonbroadcast multi-access) protokoll. Ez azt jelenti, hogy egy interfész összes virtuális áramköre külön helyi hálózatként kezelendő.
- Az elsődleges kapcsolat meghibásodása esetén, a tartalékkapcsolat használatának a konfigurálására az egyik módszer az, ha a forgalomirányítón lebegő statikus útvonalakat állítunk be. A lebegő statikus útvonal egy olyan statikus útvonal, melynek adminisztratív távolsága nagyobb, mint a neki megfelelő dinamikusé.
- A VPN a belső magánhálózatok egy kiterjesztése. Biztonságos adatátvitelt tesz lehetővé egy megosztott, nyilvános hálózaton, mint például az internet.
- A VPN hálózatoknak két fontos eleme van:
    - alagúttechnika a magánhálózat megvalósításához
    - titkosítás a titoktartás és a biztonság megvalósításához
- Alagúttechnikai módszerek:
    - általános forgalomirányítási beágyazás (generic routing encapsulation)
    - IP biztonság (IPSec)
    - 2. rétegbeli továbbítási protokoll (L2F - Layer 2 Forwarding Protocol)
    - Pont-pont alagút protokollt (PPTP - Point-to-Point Tunneling Protocol)
    - 2. rétegbeli alagút protokoll (L2TP - Layer 2 Tunneling Protocol)
- Titkosítási algoritmusok:
    - Adat titkosítási szabvány (DES - Data Encryption Standard) algoritmus
    - Háromszoros DES (3DES) algoritmus
    - Fejlett titkosítási szabvány (AES - Advanced Encryption Standard) algoritmus
    - Rivest - Shamir - Adleman (RSA)
- A titkosítási algoritmusok, mint a DES és 3DES, szimmetrikus, osztott titkos kulcsot használnak a a titkosításhoz és a visszafejtéshez.
- A kulcsok kulcscserélési módszer alkalmazásával konfigurálhatók. A Diffie-Hellman (DH) kulcscsere egyeztetés egy nyilvános kulcscserélési módszer.
- A VPN adatok módisításának és lehallgatásának védelmére adatintegritási algoritmusok használhatók, melyek egy hash értéket adnak az üzenethez.
- Az IPSec nyílt szabványok keretrendszere. Az adatok titkosságát, sértetlenségét és hitelesítését biztosítja a résztvevő felek között. Ezeket a szolgáltatásokat nyújtja a 3. rétegben.

9. Ajánlatkérés

9.1 Az ajánlathoz szükséges információk összegyűjtése

9.1.1 A meglévő információk rendszerezése

A javasolt hálózati terv tesztelése után a tervező az ajánlatkérés (Request for Proposal, RFP) és az előző PPDIOO lépésekből gyűjtött információk alapján ajánlatot állít össze. Az ajánlat jellemzően az alábbi részekből áll össze:

- Vezetői összefoglaló
- Hálózati követelmények
- A meglevő hálózati környezet
- Javasolt fizikai felépítési terv
- Javasolt logikai felépítési terv
- Kivitelezési terv
- Költségbecslés

Ha az ajánlat egy konkrét ajánlatkérésre született, az egyes elemeknek és a tartalomjegyzéknek szigorúan követniük kell az ajánlatkérésben megadott formai követelményeket.

Ha nincs írott ajánlatkérés, vagy az írott ajánlatkérés nem határozza meg a szerkezetet vagy a formátumot, a tervező saját maga választhatja meg ezeket. Ebben az esetben az ajánlatnak jól áttekinthetőnek kell lennie, és segítenie kell az olvasót abban, hogy megtalálja az őt érdeklő információt. Az ábrák növelik a javaslat olvashatóságát, és további információt is közvetítenek. A szöveg legyen könnyen olvasható, jellemzően ‘serif’ típusú (pl. Times Roman), 10-12-es betűméretű karakterekből álljon. A margó legalább 1,2 cm-es legyen, és minden oldal tetején vagy alján legyenek oldalszámok.

Hálózat fejlesztése

Tartalomjegyzék

Vezetői összefoglaló

A projekt célját, kiterjedését írja le a legmagasabb szinten. Szemlélteti, hogy a hálózattervező megértette a projekt nagyságrendjét, és a hálózat szerepét az üzleti célok elérésében. Az összefoglaló célja: világossá tenni a döntéshozóknak a terv üzleti előnyeit. Ez a rész jellemzően egy-két oldal terjedelmű.

Hálózati követelmények

Áttekinti az üzleti célokat és hálózati követelményeket, beleértve a szükséges felhasználók és alkalmazások támogatását is. Fontossági sorrendben sorolja fel az üzleti célokat, megjelölve a legfontosabbakat. Tartalmazza az üzleti célokhoz szükséges topológiát, protokollokat, hardvert, szoftvert és képzést.

9.1.2 A meglévő információk összerendezése

Ebben a tervezési fázisban a Hálózat Kft. pénzügyi vezetője és hálózattervező szakembere a Stadion Kht. ajánlatkérésére válaszul elkészíti az ajánlatot. Az ehhez szükséges anyagok nagy része már rendelkezésre áll, kivéve a kivitelezési tervet és a költségbecslést.

A tervező szerkeszti és összerendezi a meglevő információkat, mielőtt hozzálátna a kivitelezési terv és a költségbecslés elkészítéséhez.

"Vezetői összefoglaló"

A "Vezetői összefoglalót" rendszerint a pénzügyi vezető írja. Ez a dokumentum az ügyfél szemszögéből közelíti meg a projektet, és a hangsúlyt arra fekteti, hogy a javasolt hálózat milyen előnyöket nyújt majd az ügyfél cége számára. A projekt előzőleg végiggondolt és fontosság szerint csoportosított céljai, valamint a projekt által érintett területek képezik a "Vezetői összefoglaló" alapját.

„Hálózati követelmények” és ”A meglévő hálózati környezet”

Ezek a részek a PPDIOO-folyamat során korábban létrehozott „Hálózati követelmények” dokumentumból származó, már jóváhagyott információt tartalmazzák abból a célból, hogy a megrendelő ügyfél ellenőrizhesse, hogy a javasolt hálózat megfelel–e az előzőleg egyeztetett elvárásoknak.

Fizikai és logikai terv

A tervező a javasolt tervezési diagramokból,valamint a teszt- és próbahálózatok tapasztalatai alapján alakítja ki a javasolt fizikai és logikai hálózati tervekről szóló részeket. Fontos, hogy minden lehetséges kockázati tényező fel legyen tüntetve, a kiküszöbölésükre alkalmas stratégiákkal együtt. Ezek az információk segítik a megrendelőt abban, hogy a felkínált tervezési lehetőségek közül választani tudjon.

Az ajánlat összeállítása közben a hálózat tervezője és az pénzügyi vezető minden anyagot átnéz, hogy semmi ne hiányozzon. Fontos, hogy a Stadion Kht. vezetése és technikai munkatársai számára könnyen megtalálhatók és megérthetők legyenek az ajánlat egyes részei. A rendezetlen

vagy hiányos anyag könnyen oda vezethet, hogy a megrendelő másik céggel köt szerződést a projekt kivitelezésére.

A tervező és a pénzügyi vezető közösen készíti el a kivitelezési tervet és a költségbecslést.

9.2 A kivitelezési terv elkészítése

9.2.1 A kivitelezési terv

A PPDIOO folyamat során a hálózati tervezési munka befejezését követően a kivitelezési és a migrációs terv készül el. Mindennél fontosabb, hogy a lehető legtöbb részletet osszuk meg a hálózattervező mérnökökkel és a technikusokkal.

A hálózati terv kivitelezése

A gyakorlati kivitelezés alatt a hardvereszközök telepítését, a rendszerek beállítását, a hálózat tesztelését és a hálózat üzembe helyezését értjük. Ezek a feladatok további részfeladatokra bonthatók. Ezek a feladatok további lépésekből állnak, és az alábbi dokumentációt igénylik:

- Az adott feladat leírása
- Hivatkozás a tervdokumentációkra
- Részletes kivitelezési irányelvek
- Részletes hibakeresési irányelvek esetére
- A megvalósításhoz szükséges idő becslése

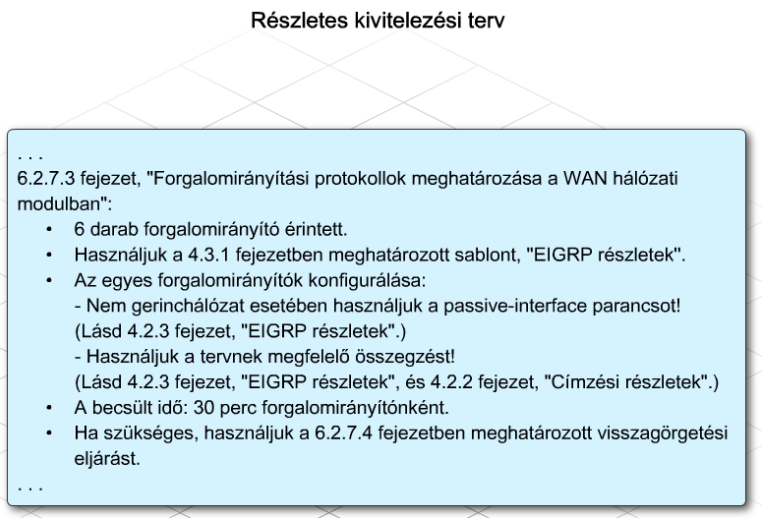
A stadion projekt tervezése

A hálózattervező megállapította a hibás és a helyes működés kritériumait a terv minden vonatkozásával kapcsolatban, és ezek az információk mind bekerültek a dokumentációba.

Egy terv gyakorlati megvalósításakor a hálózattervezőnek számolnia kell a hiba lehetőségével, még sikeres próba-és teszthálózati eredmények esetén is. A kivitelezés minden egyes lépésénél további tesztelés válhat szükségessé, csak ezzel válhat biztossá, hogy a hálózat valóban a terv szerint fog működni.

A kivitelezési terv összegzése

	Dátum, Idő	Leírás	Kivitelezési részletek	Megvalósítás
. . .				
3. feladat	04/02/2008	A telephely hardverének telepítése	6.2.3 fejezet	Igen
1. lépés		A kapcsolók összekötése	6.2.3.1 fejezet	Igen
2. lépés:		A forgalomirányítók beállítása	6.2.3.2 fejezet	Igen
3. lépés:		Kábelezés	6.2.3.3 fejezet	Igen
4. lépés:		Adatkapcsolatok ellenőrzése	6.2.3.4 fejezet	Igen
4. feladat	04/03/2008	A telephely hardverének telepítése	6.2.4 fejezet	Nem
1. lépés		VLAN-ok konfigurálása	6.2.4.1 fejezet	Nem
2. lépés:		IP-címzés létrehozása	6.2.4.2 fejezet	Nem
3. lépés:		Forgalomirányítás beállítása	6.2.4.3 fejezet	Nem
4. lépés:		A kapcsolatok ellenőrzése	6.2.4.4 fejezet	Nem
5. feladat	04/05/2008	A telephely frissítések megkezdése	6.2.5 fejezet	Nem
1. lépés		A meglévő hálózathoz való kapcsolódás.	6.2.5.1 fejezet	Nem
. . .				



Megrendelői jóváhagyás

A stadion projekt kivitelezési terve részletesen leírja, milyen munkát kell a projekt célkitűzéseinek eléréséhez elvégezni. A terv magába foglalja a megrendelő elvárásait és a sikeres megvalósítás kritériumait, amelyek jóváhagyása esetén lezárulhat a projekt.

Amint a megrendelő jóváhagyta a kiviteli tervet, máris kezdődhet a hálózat telepítése. A megrendelő részletes listát kap minden szükséges eszközről és elvégzendő munkafázisról. Ez a lista a kiviteli terv része. Ennek egy aláírt példányát (munkapéldányként) a hálózattervező és a pénzügyi vezető is megkapja.

A megrendelő minden részfeladat elvégzésekor igazolja az adott munka befejezését és azt is, hogy az eredmény megfelel-e az elvárásoknak.

A kivitelezés folyamán háromféle telepítési módszer használható:

- **Új telepítés** - gyakran zöldmezős beruházásnak is hívják
- **Fokozatos telepítés** – új alkotóelemek beépítése a meglevő, működő hálózatba
- **Teljes csere** – gyakran „targoncás fejlesztés”-nek is hívják

Új telepítés

Új telepítés esetén nincsenek felhasználók vagy jelenleg is működő alkalmazások. Ez a tény sokféle előnnyel jár:

- Az összes berendezés és szolgáltatás egyszerre telepíthető és tesztelhető.
- Az új hálózat kivitelezési terve nem olyan bonyolult, mint a másik két módszer szerinti telepítésnél.
- A határidők rugalmasabbak annál, mint amikor már van egy működő hálózat a helyszínen.
- A telepítés a cég működését csak minimális mértékben akadályozza.

A meglevő hálózat fokozatos átalakítása, kiegészítése

Fokozatos telepítés esetén a hálózat fejlesztése a meglevő, jelenleg is működő részektől leválasztva történik meg.

Amikor új hálózati eszközöket vagy technológiákat építünk be egy meglevő hálózatba, nagyon oda kell figyelnünk, hogy feleslegesen ne kapcsoljunk le működő részeket, ne akadályozzuk a szolgáltatásokat. A fokozatos telepítés sokkal részletesebb tervezést és a megrendelő fokozottabb bevonását igényli. A hálózat felújítása apró részekre van bontva, amelyek gyorsan üzembe helyezhetők és tesztelhetők. A kis fázisokban történő fejlesztés jár a legkevesebb leállási idővel.

A módszer hátránya, hogy több pénzre van hozzá szükség és hosszabb ideig is tarthat.

A teljes hálózat cseréje

Bizonyos esetekben a teljes hálózat cseréje válhat szükségessé. A teljes hálózatot akkor szokás lecserélni, ha elavult és már nem fejleszthető tovább. Ebben az esetben az új hálózat gyakran a még működő régi mellett épül ki. Amint működőképessé válik az új, a régivel egyidejűleg tesztelik. Egyeztetett időpontban az adatforgalmat átkapcsolják az új hálózatra, a régi hálózatot pedig lebontják.

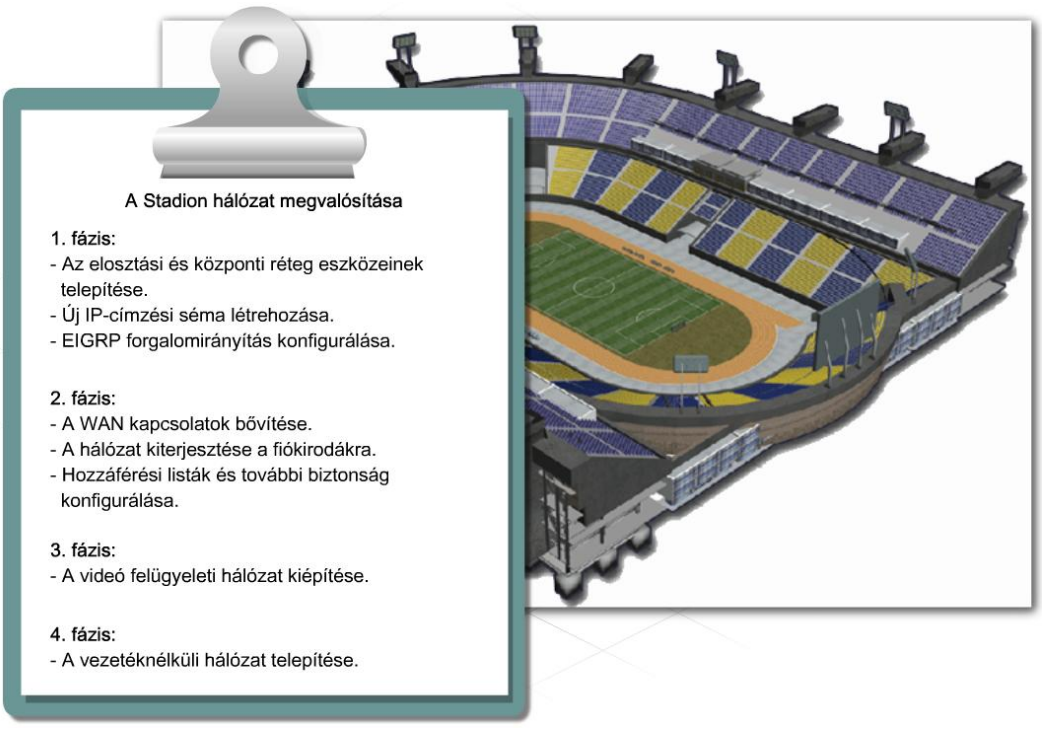
A stadion projekt telepítési módja

A legmegfelelőbb telepítési mód kiválasztása a teljes hálózattervezési munka korai szakaszában történik. A hálózattervező összegyűjti és értékeli a megrendelő üzleti céljait, a technikai követelményeket, és a tervezés korlátait érintő információkat.

A Stadion Kht. két olyan alapvető követelményt támaszt, amelyek lényegesen befolyásolják a telepítési mód kiválasztását:

- A stadion hálózat szolgáltatásainak a fejlesztés ideje alatt is elérhetőknek kell lenniük.
- A meglévő eszközöket használni kell az új hálózati tervben is.

A fentieket mérlegelve, a Hálózat Kft. tervezője a fokozatos telepítést javasolja.



9.2.3 Ütemezés és az erőforrások becsélése

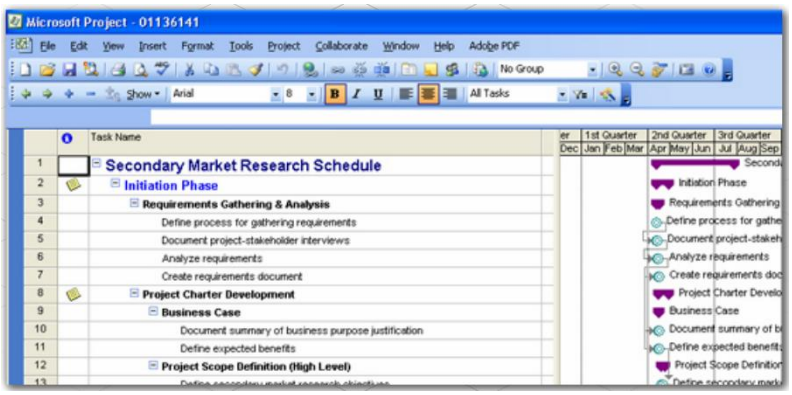
A projekt időtartama a szerződéses megállapodás része. Ahhoz, hogy teljesíteni lehessen az ügyfél által szabott határidőket, a hálózattervező elkészíti a projekt ütemezését. Az anyagok elérhetősége, a kivitelező és az ügyfél ütemterve egyaránt hatással van a kezdési és a befejezési dátumra.

Egy projekt ütemezésének elkészítésénél a hálózattervezőnek számolnia kell azzal a lehetőséggel, hogy a projekt nem a javasolt időpontban indul.

A stadion ajánlatkérési dokumentuma előírja, hogy a projektnek szezonon kívüli időszakban kell elkészülnie. Ez az elvárás 4 hónapos megvalósítási időszakot tesz lehetővé.

A Hálózat Kft. erőforrásai

Az előírt feladatok figyelembevételével a tervező megbecsüli, hogy milyen erőforrások szükségesek a hálózatfejlesztés megvalósításához. Elképzelhető, hogy a 4 hónapos határidő betartásához a Hálózat Kft.nek meg kell növelnie a projektben résztvevő technikusok számát. Előfordulhat, hogy az egyes feladatok sorrendjét bizonyos berendezések leszállításához, vagy a TSP szolgáltatások rendelkezésre állásához kell igazítani.



Becsült ütemezés

A hálózattervezőnek számos tényezőt kell figyelembe vennie a projekt ütemezése során:

- A berendezések megrendelése és leszállítása.
- A szolgáltatások (pl. WAN-kapcsolat) telepítése.
- Az ügyfél ütemterve, beleértve a lehetséges karbantartási és leállási időszakokat is.
- A megfelelő műszaki személyzet rendelkezésre állása.

Az ügyfél által okozott késések

Az ügyfelek gyakran változtatnak a követelményeken egy projekt lebonyolítása során. Ilyenkor a kivitelező az ütemezés alapján módosítja a személyi feltételeket és a szükséges erőforrásokat.

A hálózattervező is az ütemezési dokumentáció segítségével bizonyítja az ügyfélnek, hogyan hat a késedelem a projekt befejezésének dátumára.

Projektkezelő szoftver

Az ütemezés projektkezelő eszközök segítségével készíthető el.

Az ilyen szoftver használata értékes segítség lehet:

- A projekt folyamatának nyomon követésében
- Az ütemtervhez való igazodásban
- A projekt legfőbb tevékanységi mérföldköveinek meghatározásában
- A munkaerő hozzárendelések és a költségek nyomonkövetésében
- A tervező figyelmeztetése esetén, ha a projekt eltér az ütemtervtől

9.2.4 Karbantartási és leállási időszakok tervezése

Karbantartási és leállási időszakok

A telepítési ütemtervnek tartalmaznia kell a tervezett karbantartási és leállási időszakokat is. Ha naponta csak néhány órán keresztül van mód a hálózat módosítására, a projekt ütemezésének tükröznie kell ezt a kényszert. Ennek hiányában az időtartamra vonatkozó becslés nem lesz reális, és a projekt késést szenvedhet. A hálózat leállási időszakait gondosan meg kell tervezni, így elkerülhető, hogy az ügyfelek munkamenetében jelentős kiesés jelentkezzen.

Néha nem lehetséges az összes elvárt feladatot befejezni a már jóváhagyott karbantartási időszakban. Minden olyan esetben engedélyt kell kérni az ügyféltől, ha a fejlesztési feladat megköveteli a teljes hálózat, vagy annak egy részének leállítását a normál üzleti órák alatt. Az összes érintetett személyt azonnal értesíteni kell, amint a leállási időszakot kijelölték és jóváhagyták.

9.3 A kivitelezés tervezése

9.3.1 Az anyaglista elkészítése

A stadion vezetőségének tett javaslat egyik legfontosabb része a költségek becslése.

A költségbecslés előkészítéseként a hálózattervező elkészít egy anyagszükségleti listát (Bill Of Material, BOM). Ez a dokumentum részletezi a javasolt fejlesztés teljesítéséhez szükséges összes előírt hardvert és összetevőt. A lista azokból a hardver- és szoftver elemekből és egyéb tételekből áll, amelyeket meg kell rendelni, és beszerzés után telepíteni kell. A tervező ezt a listát használja, hogy ajánlatokat kérjen be, és elkészítse a berendezésekre vonatkozó megrendeléseket.

Rendelési lista

A tervező a BOM segítségével rendeli meg az új berendezéseket és a pótalkatrészeket a már meglévő berendezésekhez ezért minden szükséges tételnek rajta kell lennie a listán. Bizonyos forgalomirányítókat és kapcsolókat például beépítéshez szükséges tartóelemek (konzolok) nélkül szállítanak. Ezeket a konzolokat külön kell beszerezni. Ha ezt az információt nem tartalmazta a BOM, a felszerelő konzolok hiányozni fognak rendelési listáról is, ami késleltetheti az eszköz telepítését.

A BOM elkészítéséhez a hálózattervező a hálózat minden részét megvizsgálja, és így határozza meg, hogy milyen hálózati berendezések szükségesek, és az egyes eszközöknek milyen képességekkel kell rendelkezniük. A stadionon belül 21 elkülönített helyszín van, ahol új hálózati berendezést kell elhelyezni, vagy a meglévő eszközöket kell továbbfejleszteni:

- 16 huzalozási helyiség
- 4 WAN végpont
- 1 új adatközpont

A fentieken túl a vezeték nélküli hálózat terve 33 helyszínt jelöl ki a hozzáférési pontok (AP) telepítéséhez.

További eszközök meghatározása

A hálózat egyes területeit külön-külön megvizsgálva, a tervező könnyedén azonosítani tudja a további szükséges berendezéseket. A beszerzendő eszközökről készített lista a következőket tartalmazza:

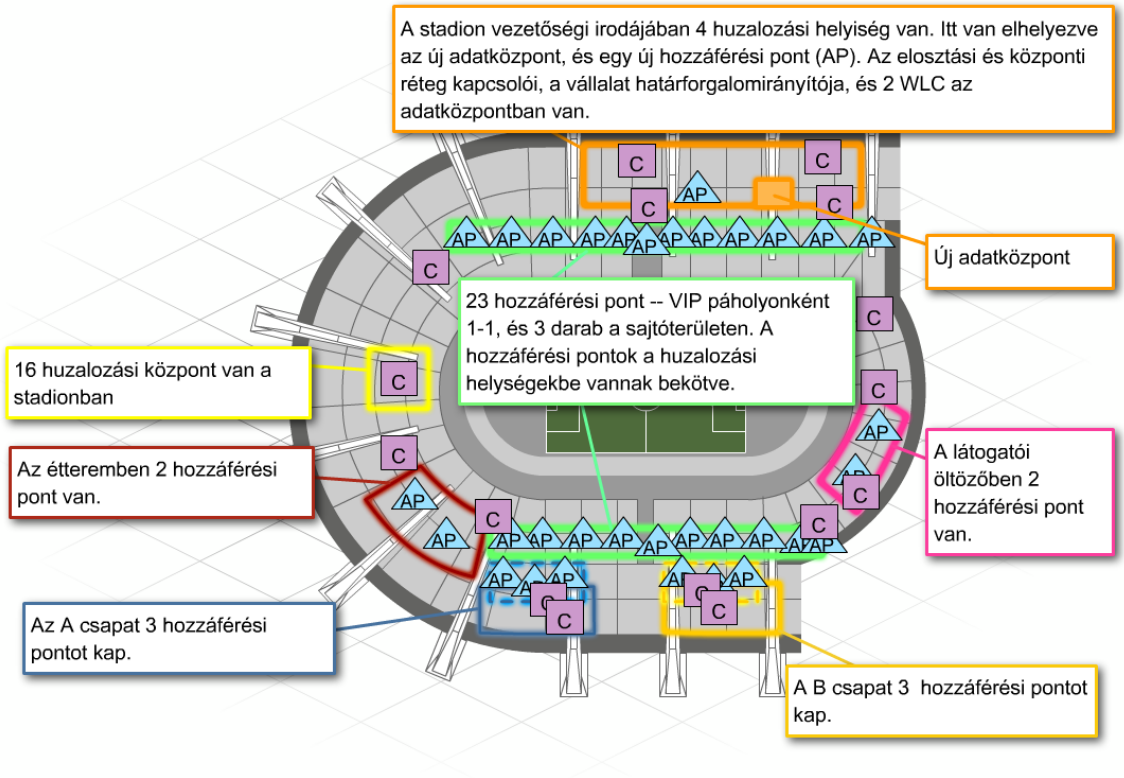
- 6 db elosztási rétegbeli kapcsoló
- 2 db központi rétegbeli kapcsoló
- 1 db WAN kapcsolatért felelős forgalomirányító
- 4 db, a WAN kiszolgálók kapcsolatáért felelős forgalomirányító
- 2 db vezeték nélküli LAN vezérlő
- 33 db centralizált vezérlésű hozzáférési pont (lightweight AP)

Az új berendezés beszerzésének mérlegelésekor a tervezőnek mindig figyelemmel kell lennie a költségvetésre. A tervező a stadion projekt költségvetésével foglalkozó pénzügyi vezetővel együtt áttekinti a lehetséges eszközök választékát . Ez az együttműködés biztosítja, hogy a kiválasztott

eszközökkel ne lépjék át a költségvetés kereteit, és egyidejűleg az aktuális és jövőbeli üzleti célok is megvalósuljanak.

A meglévő eszközök fejlesztése

A javasolt terv számol a meglévő Cisco Catalyst 2960-as kapcsolókkal. A 16 darab huzalozási helyiség mindegyike tartalmaz egyet ezekből a kapcsolókból. Minden 2960-as kapcsolónak rendelkeznie kell tartalék optikai csatlakozási lehetőséggel az elosztási réteg eszközeihez. A tartalék kapcsolatokhoz egy-egy kiegészítő optikai adó-vevőt kell beépíteni minden kapcsolóba. Ezt a 16 adó-vevőt fel kell venni a BOM listára, és csatolni kell a javaslathoz.



Szoftver szükségletek

A stadion projekt korai szakaszában az ügyfél átadta a jelenlegi alkalmazásokról készített listát a hálózati tervezőnek. Ebből, és a hálózati felülvizsgálatból származó információk alapján a tervező az összes meglévő alkalmazást azonosítani tudja.

Meglévő alkalmazások

A jelenlegi alkalmazások listája:

- **Hálózati alkalmazások** – Microsoft fájlmegosztás, nyomtatás, DNS, web kiszolgáló, beolvasó és szövegfelismerő szoftverek
- **Speciális alkalmazások** – Jegy beolvasó és jegyfelismerő szoftver
- **Üzleti alkalmazások** – Könyvelési, kifizetés-kezelő, eseménykezelő, kölcsönzést és bérlést kezelő, piacszervezést (marketing) és ügyfélkezelést (customer relationship management, CRM) végző szoftver

Új alkalmazások

Új alkalmazások az alábbiak:

- **Hálózati alkalmazások** – Hálózatfelügyelő szoftver (Network management software)
- **Speciális alkalmazások** – Jegyek nyomtatása, biztonsági IP kamerák és térfigyelés, e-kereskedelmi helyek

Az új alkalmazások, a telepítési költségek és a szükséges képzések ezek hardverigényével együtt felkerültek a BOM listájára. A tervező megvizsgálja, hogy a hálózatfejlesztés miatt, a meglévő szoftver alkalmazásokhoz szükség van-e új licencek beszerzésére.

Az alkalmazások típusa	Meglévő	Új
Hálózati	DNS, Webkiszolgáló, adatbázis, e-kereskedelem, nyomtatás, fájlmegosztás, beolvasó és szövegfelismerő szoftverek	Hálózatfelügyeleti szoftver
Speciális	Könyvelési, kifizetés-kezelő, eseménykezelő, kölcsönzést és bérlést kezelő, piacszervezést (marketing) és ügyfélkezelést (customer relationship management, CRM) végző szoftver	Jegyek nyomtatása, biztonsági IP kamerák és térfigyelés, e-kereskedelmi helyek a jegyeladáshoz és az ajándéktárgyak értékesítéséhez

9.3.2 SMARTnet szolgáltatás bevezetésére vonatkozó javaslat

Garancia

Az összes új eszköz automatikusan garanciával érkezik. Az általános garancia a következő előnyöket nyújtja:

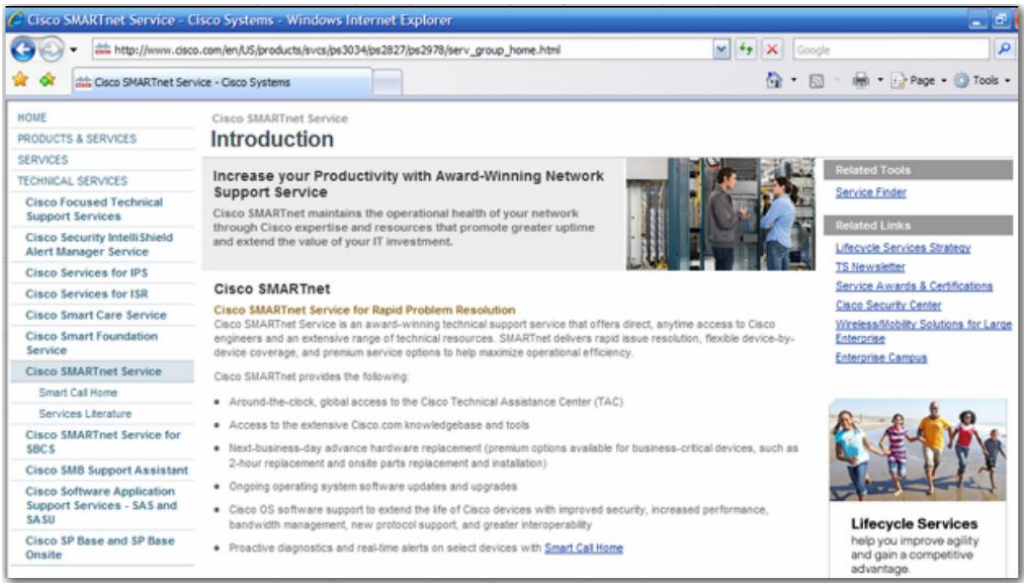
- **Hardvergarancia** — Garantálja, hogy a hardver normál használata mellett nem jelentkezik anyag- vagy megmunkálási hibából eredő probléma.
- **Szoftvergarancia** — Garantálja, hogy a fizikai adathordozó hibamentes, és a szoftver teljesíti az ígért funkciókat.

A garancia azonban időben és a nyújtott szolgáltatások tekintetében is korlátozott. A szoftvergarancia például általában azt garantálja, hogy a szoftver a termék leírásában meghatározott képességekkel rendelkezik. Az eladott termék az aktuális állapotot tartalmazza, és nem jár hozzá semmilyen új szoftver verzió. A legtöbb garancia a hibás termék cseréjére korlátozódik, és nem tartalmaz technikai vagy helyszíni támogatást.

További szolgáltatási szerződések

A javasolt stadion hálózat régi és új hálózati berendezéseket egyaránt tartalmaz. Előfordulhat, hogy néhány régi eszköz garanciája már lejárt. Annak érdekében, hogy a Stadion Kht. beruházása hosszú távon is megtartsa értékét, és hogy a meglévő eszközök élettartama minél hosszabb

legyen, a Hálózat Kft. pénzügyi vezetője azt javasolja a stadion vezetőségének, hogy kössenek további karbantartásra és támogatásra vonatkozó szerződéseket.



SMARTnet megállapodások

A SMARTnet program része annak a szolgáltatási csomagnak, amelyet a Cisco technikai támogatási szolgáltatások (TSS - Technical Support Services) csoport nyújt. A SMARTnet program szolgáltatásbővítést és különböző formában nyújtott karbantartási támogatást kínál a szerződésben meghatározott időszakra.

A SMARTnet megállapodás magában foglalja az alábbiakat:

- Szoftvertámogatás a licencelt operációs rendszerekhez.
- A Cisco Technikai Támogatási Központ (Cisco Technical Assistance Center - TAC) elérése heti hét napon át, napi 24 órában.
- A Cisco.com regisztrált elérése, ami az online technikai jellegű információ könnyű elérhetőségét és a szolgáltatásigénylési kezelőrendszer használatát biztosítja.
- Kedvező feltételekkel történő hardvercsere szolgáltatás.

Hardvercserére vállalt idő

A SMARTnet szerződésben a meghibásodott eszköz helyetti cserehardver biztosításának határideje függ attól, hogy az ügyfél milyen gyors szolgáltatást vár el, valamint attól, hogy milyen konstrukciót választott. Egy 24x7x2-es szerződés esetén például, amennyiben cserére van szükség, a cserealkatrésznek a hiba megállapításától számított két órán belül a helyszínen kell lennie. Ebben az esetben a szolgáltatás maximális kiesése 2 óra lehet, függetlenül attól, hogy a hiba a hét melyik napján, vagy milyen napszakban következett be.

Előnyök

A Hálózat Kft. pénzügyi vezetője elkészít egy táblázatot, ami az alapgaranciánál magasabb szolgáltatási szintet nyújtó SMARTnet szerződéseket hasonlítja össze. Ez az előkészítő anyag

részeként megjelenő összehasonlítás megmutatja megrendelőnek, hogy milyen előnyökkel járnak az egyes lehetőségek.

	SMARTnet	Évi 90 napra korlátozott hardver	Korlátozott élettartamú hardver
Hardvergaranciai időtartama	Nincs	évi 90 nap	Nincs
Technikai támogatás a TAC-tól	Van	Nincs	Nincs
Az operációs rendszer (OS) verziójának karbantartása	Van	90 nap	90 nap
A legrégebbi és a legfrisebb OS verzió	Van	Nincs	Nincs
a szoftver alkalmazások karbantartási és a legkisebb verziói	Nincs	Nincs	Nincs
A legfrissebb verziójú alkalmazások biztosítása	Nincs	Nincs	Nincs
adatállomány módosítások igazolása	Nincs	Nincs	Nincs
A Cisco.com regisztrált elérése az ismeretek és az online eszközök használatához.	Van	Nincs	Nincs
A kicserélt elemek	Szabvány: Következő - munkanap teljesítési opció: 2-óra, 4-óra alatt a helyszínen	RTF (10 nap)	RTF (10 nap)
Garanciális eszközök	összes	összes	összes

9.3.3 Cisco Technikai Szolgáltatások és Támogatás

Elvárás a projekttel szemben, hogy ne legyen szükség nagyobb létszámú IT támogatási csapatra a stadion hálózatának bővítése után sem. A Hálózat Kft. pénzügyi vezetője és a hálózat tervezője egyetért abban, hogy a külső támogatás lehetőségét fel kell vetni a stadion vezetősége számára.

Cisco Koncentrált Technikai Támogatási Szolgáltatások

A Cisco Koncentrált Technikai Támogatási Szolgáltatás (Cisco Focused Technical Support Services) egy háromszintű szolgáltatáscsomag, amely változatos lehetőségeket nyújt az ügyfelek számára.

A Hálózat Kft. pénzügyi vezetője az előterjesztésben a második szintű csomagot, azaz a Cisco Kiemelt Technikai Támogatási Szolgáltatást (Cisco High-Touch Technical Support Service) javasolja, kiegészítve SMARTnet megállapodásokkal. Ezen a második szintű szerződéses csomagon belül a cég elsőbbséget élvezve jut hozzá egy kijelölt mérnökcsapat szakértelméhez. A csapat tagjai minden részletre kiterjedő képzés keretében szereznek ismeretet a stadion üzleti folyamatairól.

A mérnökök a Cisco életciklus (Cisco Lifecycle) megközelítésnek megfelelően az új hálózat működésbe lépésétől annak teljes életciklusán át nyújtják a szolgáltatásukat.

Cisco Koncentrált Technikai Támogatási Szolgáltatások
Cisco Kiemelt Működés vezetési szolgáltatás (Cisco High-Touch Operations Management Service) 1. szint: Az ügyfél személyzetének növelése egy heti öt napon át nyolc órában dolgozó megbízott működési igazgatóval a problémák megoldásának elősegítésére, a visszatérő problémákat megelőző intézkedések meghatározására és a zárásra vonatkozó szolgáltatási kérések kezelésére.
Cisco Kiemelt Technikai Támogatási Szolgáltatás (Cisco High-Touch Technical Support Service) 2. szint: Különleges Cisco mérnökökből álló csapat kijelölése az ügyfél igényeinek heti 7 napon át napi 24 órában történő gyors problémamegoldására és a hálózat működésének javítására vonatkozó ajánlatok kidolgozásában.
Cisco Kiemelt Mérnöki szolgáltatások (Cisco High-Touch Engineering Service) 3. szint: Rendszeres hálózati elemzés készítése egy megbízott Cisco hálózati mérnök által, kinek szakmai tudása az ügyfél igényeihez igazodik és heti öt napon át napi nyolc órában elérhető. Az ügyfél alapos hálózati elemzést kap a probléma forrásának elszigeteléséhez, a hálózati eseményekre válaszolva összefoglalót a szoftver verziókról, javító és megelőző műveletekre vonatkozó ajánlatokat és helyszíni látogatásokat.

9.3.4 Szoftver IOS szolgáltatások és támogatás

A stadiont üzemeltető cég egyik üzleti célja a hálózat napi felügyeletének egyszerűsítése. A Hálózat Kft. stábja hálózati felügyelő program telepítését javasolja erre a célra.

Szoftveralkalmazásokat Támogató Szolgáltatások

A CiscoWorks hálózatkezelő alkalmazás vagy a Cisco IP-telefónia megoldás használatához Cisco szoftver termékeket kell telepíteni a hálózati hardvereken. A Cisco a Szoftveralkalmazásokat Támogató Szolgáltatások (Software Application Support Services - SAS) megoldását kínálja az alkalmazási szoftverek támogatásához.

A SAS szolgáltatás magába foglalja a folyamatos technikai támogatást, az alkalmazási szoftverek frissítését, és bőséges technikai információt a Cisco.com helyen. A SAS-t speciálisan a Cisco szoftver-alkalmazásokhoz tervezték, és az operációs rendszerek szoftvertámogatásán túl további szolgáltatásokat nyújt.

A szoftvertámogatási opciók költsége ugyanúgy részét képezi a javaslatnak, mint a szoftver licencek költsége.

9.4 Az ajánlat elkészítése és bemutatása

9.4.1 Az ajánlat véglegesítése

A Hálózat Kft. pénzügyi vezetője az elkészült kivitelezési és költség rész információi alapján frissíti a „Vezetői összefoglalót”. A javaslati dokumentum részeit egy iratrendezőbe fűzi le, abban a sorrendben, ahogy a tartalomjegyzékben szerepelnek.

A javaslati dokumentum elejére borítólap kerül, amely fontos információt tartalmaz a javaslatról, beleértve a ajánlatkérés azonosító számát és dátumát, az ajánlatkérő elérhetőségi adatait, valamint az ajánlattevő nevét és elérhetőségét.

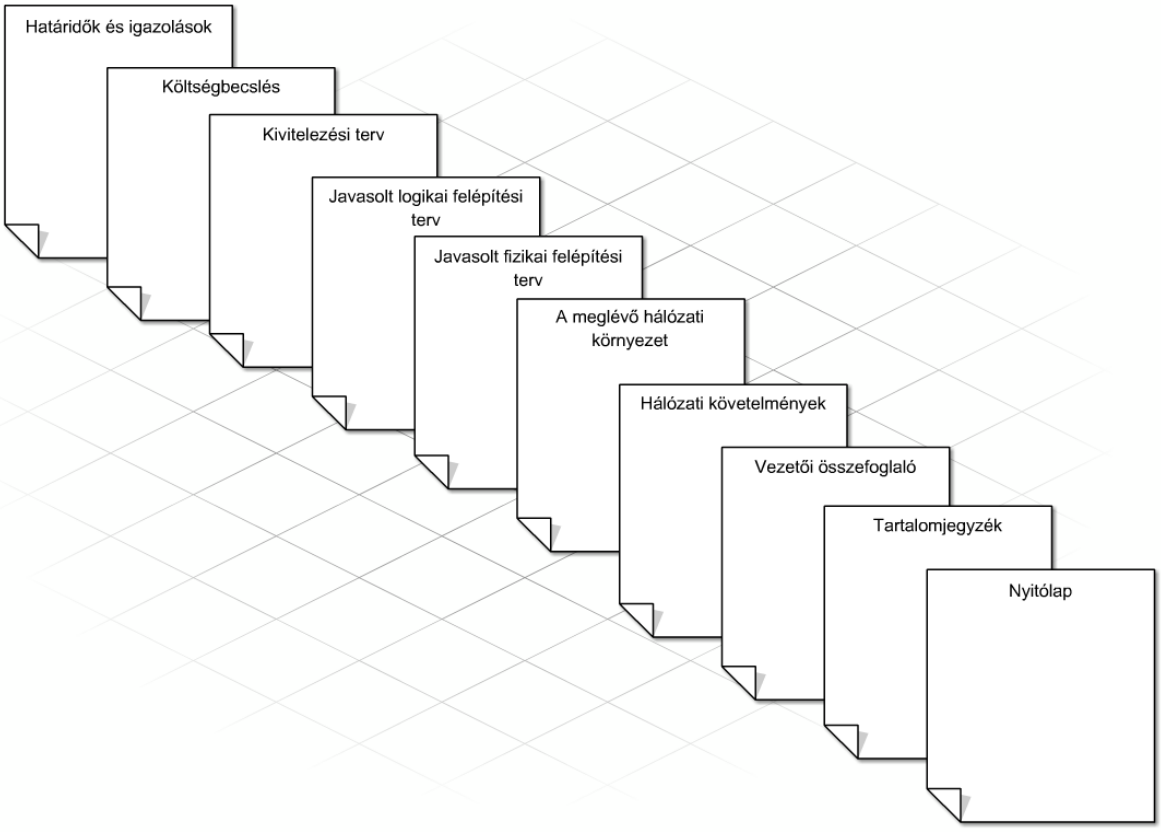
A javaslati dokumentum végén kapnak helyet a megállapodási feltételek, valamint egy külön lapon a megrendelő aláírásának is helyet adó jóváhagyó dokumentum. A megállapodási feltételek rész felsorolja az összes idevonatkozó jogi szabályozást és szerződést. Ezek a szabályozások és feltételek segítséget nyújtanak a hálózatfejlesztéssel és telepítéssel kapcsolatos eszközök és szolgáltatások megrendeléséhez.

A megállapodási feltételek rész a következő fontos elemeket tartalmazza:

- A javaslat érvényességi ideje.
- A megrendelő kötelezettségei, hogy szervezetén belül megszerezze a szükséges engedélyeket és egyetértést.
- A szállító kötelezettségei, hogy a tőle származó berendezésekkel és szolgáltatásokkal kapcsolatban gondosan és megfelelő szakmaisággal járjon el.
- A teljesített részfeladatokhoz kötődő fizetési ütemezés.
- A büntető kamat mértéke késedelmes fizetés esetére.
- A berendezések és a szolgáltatások visszamondása esetén fizetendő díj.
- A szállítói garancia részletei (ha van garanciavállalás).

- A vitás kérdések kezelésének módja.

Ha a megrendelő elfogadja az ajánlatot, akkor képviselője aláírja a megállapodási feltételeket és az elfogadó nyilatkozatot tartalmazó oldalakat.



9.4.2 Az ajánlat bemutatása

Az ajánlat véglegesítése után a hálózat tervezője a Hálózat Kft. vezetésével együtt áttekinti a teljes javaslatot . A tervezésnek ebben a fázisában a tervezőnek el kell fogadtatnia a koncepciót a Hálózat Kft. vezetésével, és ezt követően a megrendelővel is.

Szokásos eljárás, hogy a tervező egy előadást készít az ajánlatról. Az előadás diákat vagy más vizuális elemeket tartalmaz a javaslat képi, grafikus bemutatásához. Az ajánlati dokumentumot bemutató előadás elősegíti a megbeszélés sikerességét, és növeli annak a valószínűségét, hogy a megrendelő elfogadja az ajánlatot.

Az előadás (prezentáció)

A tartalom és az előadás formája meglehetősen fontos az üzleti világban.

Tippek az előadáshoz:

- Minden diának legyen a tartalmához illeszkedő, azt összefoglaló címe.
- A számítógépes prezentációk nem tartalmazhatnak hosszú összefüggő szövegrészeket. Használjon pontozott listát vagy vázlatformátumot, és részletezze az egyes pontokat az előadás közben!

- A szöveg legyen jól olvasható. Használjon nagyméretű betűket, mert a kicsiket nehéz elolvasni!
- Használjon ellentétes színeket: vagy sötét hátteret világos szöveggel vagy világos hátteret sötét szöveggel!
- Kerülje az olyan hátteret, amelynél a szöveg nehezen olvasható! Legyen a háttér egyszerű!
- Ne használjon csupa nagybetűt! A rossz olvashatóság mellett az ilyen szöveg megjelenése nem professzionális.
- Használja a szöveg, kép és grafika kombinációját! A változatosság érdekessé teszi az előadást.

Az előadás után a felhasználó teljes egészében elfogadhatja az ajánlatot, változtatásokat kérhet, vagy elutasíthatja azt.

Fontos emlékeztetni rá, hogy az előadás előtti felkészülés szintje dönthet arról, hogy a megrendelő elfogadja-e vagy elveti-e az ajánlatot.

9.5 A fejezet összefoglalása

- A hálózati ajánlat egy ajánlatkérésre (RFP) adott válasz, ami jellemzően a következő részekből áll:
  - Vezetői összefoglaló
  - Hálózati követelmények
  - A meglevő hálózati környezet
  - Javasolt fizikai felépítési terv
  - Javasolt logikai felépítési terv
  - Kivitelezési terv
  - Költségbecslés
- A nem megfelelően szerkesztett vagy befejezetlen ajánlat könnyen oda vezethet, hogy a megrendelő másik céggel köt szerződést a projekt kivitelezésére.
- A hálózat kivitelezése alatt a hardvereszközök telepítését, a rendszerek beállítását, a hálózat tesztelését és a hálózat üzembe helyezését értjük.
- A kivitelezés során háromféle telepítési módszer használható:
  - Új telepítés - gyakran zöldmezős beruházásnak is hívják
  - Fokozatos telepítés – új alkotóelemek beépítése a meglevő, működő hálózatba
  - Teljes csere – gyakran „targoncás fejlesztés”-nek is hívják
- A hálózattervezőnek számos tényezőt kell figyelembe vennie, amikor egy projekt ütemezését tervezi:
  - A berendezések megrendelése és leszállítása.
  - A szolgáltatások (pl. WAN-kapcsolat) telepítése.
  - Az ügyfél ütemterve, beleértve a lehetséges karbantartási és leállási időszakokat is.
  - A megfelelő személyzet biztosítása.
- A telepítési ütemtervnek tartalmaznia kell a tervezett karbantartási és leállási időszakokat is. Ha naponta csak pár óra áll rendelkezésre a változtatások elvégzésére, akkor a projekt ütemtervében is szerepelnie kell ennek a korlátozásnak.

- A BOM egy dokumentum, ami részletezi az összes előírt hardvert és összetevőt, amelyek szükségesek a javasolt korszerűsítés elvégzéséhez. A lista azokból a hardver- és szoftver elemekből áll, amelyeket meg kell rendelni, majd beszerzés után telepíteni kell.
- Az összes új eszköz automatikusan garanciával érkezik.
- Az általános garancia a következő előnyöket nyújtja:
    - Hardvergarancia— Garantálja, hogy a hardver normál használata mellett nem jelentkezik anyag- vagy megmunkálási hibából eredő probléma.
    - Szoftvergarancia — Garantálja, hogy a fizikai adathordozó hibamentes, és a szoftver teljesíti az ígért funkciókat.
- A SMARTnet program szolgáltatásbővítést és különböző formában nyújtott karbantartási támogatást kínál a szerződésben meghatározott időszakra.
- Az ajánlat bemutatója diákat és más vizuális elemeket tartalmaz a javaslat képi, grafikus bemutatásához.
- A bemutató és az ajánlat dokumentuma elősegíti a megbeszélés sikerességét, és növeli annak a valószínűségét, hogy a megrendelő elfogadja az ajánlatot.
- Ne feledjük, hogy az előadás előtti felkészülés dönthet arról, hogy a megrendelő elfogadja vagy elveti az ajánlatot.

Tartalom