# Fejezet 2: Kapcsolás alapjai és beállítása

# Kapcsolás alapjai és beállítása

## Bevezetés

A kapcsolókat az azonos hálózatban lévő eszközök összekötésére használják. Egy megfelelően kialakított hálózatban a LAN-kapcsolók felelősek az adatfolyam hozzáférési rétegből a hálózati erőforrásokig történő továbbításában.

A Cisco kapcsolók kicsomagolásuk és bekapcsolásuk után, manuális konfiguráció nélkül is, azonnal működőképesek. Mivel ezek az eszközök a Cisco IOS operációs rendszeren alapulnak, így a manuális beállítások által a kapcsolók jobban meg tudnak felelni az adott hálózat igényeinek. Ez magában foglalja többek között a portsebesség-, a sávszélesség- és a biztonsági követelmények konfigurálását.

A Cisco kapcsolók helyileg és távolról is egyaránt menedzselhetők. A távoli menedzseléséhez a kapcsolón IP-címet és alapértelmezett átjárót kell beállítani. A fejezetben tárgyalt beállítások közül ez csak két konfigurációs feladat.

A kapcsolók a hozzáférési rétegben működnek, ahol a kliens hálózati eszközök közvetlenül csatlakoznak a hálózatra, és az informatikai gyakorlat szerint a lehető legegyszerűbb módon biztosítják a hozzáférést a felhasználók számára. Ez egyben a hálózat egyik legveszélyeztetett területe is, hiszen itt van a hálózat leginkább kitéve a felhasználói visszaéléseknek. A felhasználói adatok védelme érdekében a kapcsolókat be kell állítani a támadások minden formája ellen, mindeközben a nagysebességű összeköttetést is biztosítani kell. A portbiztonság a menedzselhető Cisco kapcsolók egyik beépített adatbiztonsági szolgáltatása.

Ez a fejezet a kapcsolók néhány alapvető konfigurációs beállításával foglalkozik, melyekkel a stabil és biztonságos LAN-környezet megvalósítható.

# Kapcsolás alapjai és beállítása

## Bevezetés

**Állj mellém!**

**Esetleírás**   
Amikor ma megérkezünk az osztályterembe, egy számot kapunk az oktatótól ehhez a bevezető iskolai feladathoz.

Az óra elején az oktató felkér adott számokkal rendelkező hallgatókat, hogy álljanak fel. Feladatunk minden esetben az álló hallgatók számának feljegyzése.

**1. eset**   
Azok a diákok álljanak fel, **akiknek a számuk elején** **5** van. Jegyezzük fel az álló diákok számát!

**2. eset**   
Azok a diákok álljanak fel, **akiknek a számuk** végén **B** van. Jegyezzük fel az álló diákok számát!

**3. eset**   
Azok a diákok álljanak fel, **akiknek a papírjukon az 504C** van. Jegyezzük fel az álló diákok számát!

A feladatok végén az osztály szerveződjön kisebb csoportokba, és a válaszokat jegyezzük fel a kinyomtatott PDF-dokumentum megfelelő részébe.

Mentsük el munkánkat, hogy azt bármikor meg lehessen osztani más diákokkal vagy az egész osztállyal!

[Csoportos feladat - Stand By Me Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/2.0.1.2%20Stand%20By%20Me%20Instructions.pdf)

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

Egy Cisco kapcsoló elindulásakor a következő rendszerindítási lépéseken megy keresztül:

1. A kapcsoló először betölti a ROM-ból a bekapcsolási öntesztelő programot (Power-On Self Test, POST). A POST ellenőrzi a CPU alrendszert, azaz megvizsgálja a CPU-t, a DRAM-ot, és a flash memóriában található fájlrendszert.

2. Ezután a kapcsoló betölti a rendszerindító szoftvert (boot loader, "csizmahúzó"), mely a ROM-ban tárolt kis program, és a POST sikeres befejeződése után fut le.

3. A boot loader elvégzi a CPU alapszintű inicializálását. Beállítja a CPU-regisztereket, amelyek a fizikai memória használatát, a memória mennyiségét és annak sebességét vezérlik.

4. A boot loader működésre előkészíti az alaplapi flash memória fájlrendszerét.

5. Végül, a boot loader megkeresi és betölti a memóriába az alapértelmezett IOS operációs rendszert, és átadja a kapcsoló vezérlését az IOS-nek.

A boot loader a Cisco IOS-képfájlt a következő sorrendben keresi: a kapcsoló megpróbálja a BOOT környezeti változó szerinti módon végrehajtani a rendszerindítást. Ha ez a változó nincs beállítva, a kapcsoló megkísérli betölteni az első futtatható fájlt, amit a flash memória fájlrendszerében talál a rekurzív mélységi keresés által (recursive Depth-First Search, recursive DFS). Egy könyvtár mélységi keresésében először a könyvtár összes létező alkönyvtára kerül ellenőrzésre, majd a keresés az eredeti könyvtárban folytatódik. A Catalyst 2960 sorozatú kapcsolóknál a képfájl általában a vele megegyező nevű könyvtárban található (kivéve ha .bin a fájl kiterjesztése).

Az IOS operációs rendszer ezután az NVRAM-ban tárolt indító konfigurációs fájl, és az abban található utasítások alapján inicializálja az interfészeket.

Az ábrán a BOOT környezeti változó beállítását látjuk a **boot system** globális konfigurációs paranccsal. A **show bootvar** utasítással (**show boot** régebbi IOS-ek esetén) megnézhetjük az aktuális IOS rendszerindítási beállításait.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

Ha az operációs rendszer hiányzó vagy sérült rendszerfájlok miatt használhatatlanná válik, akkor a boot loader segítségével még hozzáférhetünk a kapcsolóhoz. A rendszertöltő program parancssorán keresztül ugyanis elérhetők a flash memóriában tárolt fájlok.

Egy konzol kapcsolaton keresztül a boot loader parancssora az alábbi lépésekkel érhető el:

**1.** Konzol kábellel csatlakoztassunk egy PC-t a kapcsoló konzol portjához. Konfiguráljunk egy terminál emulációs szoftvert a kapcsolóhoz történő csatlakozásra.

**2.** Húzzuk ki a kapcsoló tápkábelét.

**3.** Csatlakoztassuk újra a kapcsoló tápkábelét, és 15 másodpercen belül nyomjuk meg és tartsuk lenyomva a **Mode** gombot, míg a System LED el nem kezd zölden villogni.

**4.** Tartsuk továbbra is lenyomva a **Mode** gombot, míg a System LED egy rövid ideig sárgán, majd hosszan zölden nem világít. Csak ezután engedjük el a **Mode** gombot.

**5.** Megjelenik a rendszertöltő **switch:** promptja a terminál emulációs szoftver ablakában.

A **boot loader** parancssora segítségével formázni lehet a flash fájlrendszerét, újra lehet telepíteni az operációs rendszert, és vissza lehet állítani egy elveszett vagy elfelejtett jelszót. Például a **dir** paranccsal egy megadott könyvtár fájljai megtekinthetők, amint az ábrán is látható.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

A Cisco Catalyst kapcsolókon számos állapotjelző LED található. Ezek segítségével könnyen áttekinthetjük a kapcsoló aktivitását és teljesítményét. A LED-ek jelentése és előlapi elrendezésük a kapcsoló modellje és felszereltsége szerint változhat.

Az ábrán egy Cisco Catalyst 2960 kapcsoló LED-jeit és Mode gombját láthatjuk. A Mode gombbal válthatunk a portállapot, a port duplexitás, a portsebesség és a PoE-állapotok (ha ezt a kapcsoló támogatja) kijelzése között. Az alábbiakban megismerkedhetünk a LED-ek funkcióival és a használt színek jelentésével:

* **SYST (System, rendszer) LED** Ez jelzi, hogy a rendszer áram alatt van, és rendeltetésszerűen működik. Ha a LED nem világít, akkor a rendszer nincs bekapcsolt állapotban. Ha a LED zölden világít, a rendszer megfelelően működik. Ha a LED sárga, a rendszer áram alatt van, de nem működik megfelelően.
* **RPS (Redundant Power System, redundáns tápellátás) LED** - Az RPS állapotáról tájékoztat. Ha a LED nem világít, az RPS ki van kapcsolva, vagy nincs megfelelően csatlakoztatva. Ha a LED zölden világít, az RPS csatlakoztatva van, és készen áll a tartalék tápfeszültség biztosítására. Ha a LED villogó zöld, akkor az RPS csatlakoztatva van, de nem elérhető, mivel más eszköz számára biztosít tápfeszültséget. Ha a LED sárga, akkor az RPS vagy készenléti állapotban van, vagy meghibásodott. Ha a LED villogó sárga, akkor a kapcsolóban található belső tápegység meghibásodott, és az RPS szolgáltat áramot a készüléknek.
* **STAT (Status, portállapot) LED** - A LED zöld, ha a portállapot üzemmód került kiválasztásra, mely az alapértelmezett mód. Ekkor az egyes port LED-ek színei az üzemmódnak megfelelően világítanak. Ha a port LED nem világít, akkor nincs kapcsolat vagy a port adminisztratívan le van tiltva. Ha a port LED zöld, a kapcsolat működik. Ha a port LED villogó zöld, akkor a port éppen adatokat küld vagy fogad. Ha a port LED felváltva zöld-sárga, akkor hibás a kapcsolat. Ha a port LED sárga, a port a hurokmentesítés miatt le van tiltva, és nem továbbít adatokat (tipikusan a port ebben az állapotban van a bekapcsolása utáni első 30 másodpercben). Ha a port LED sárgán villog, a port le van tiltva, hogy megakadályozza egy esetleges hurok kialakulását az adott hálózati szegmensen.
* **DUPLX (port duplex) LED** - Ha a LED zöld, akkor a port duplex üzemmód került kiválasztásra. Ebben az esetben, ha az egyes port LED-ek nem világítanak, akkor azok félduplex (half-duplex) módban működnek. Ha a port LED zöld, a port teljes duplex (full-duplex) módban üzemel.
* **SPEED (Port Speed, portsebesség) LED** - Ez jelzi, hogy a portsebesség mód került kiválasztásra. Ha aktív, az egyes port LED-ek színei az üzemmódnak megfelelően világítanak. Ha a port LED nem világít, a port 10 Mb/s sebességen működik. Ha a port LED zöld, a port 100 Mb/s sebességen működik. Ha a port LED zölden villog, a port 1000 Mb/s sebességen működik.
* **PoE (Power over Ethernet, Ethernet hálózati tápellátás) LED** - Ha a kapcsolón a PoE támogatott, a PoE-üzemmód LED is megtalálható a kapcsoló előlapján. Ha a LED nem világít, az azt jelzi, hogy a PoE-mód nincs ugyan kiválasztva, de egyik porton sincsen tápellátás hiány vagy meghibásodás. Ha a LED sárgán villog, a PoE-mód ugyan nincs kiválasztva, de legalább az egyik port nem kapott tápellátást, vagy PoE hiba lépett fel. Ha a LED zöld, a PoE-mód került kiválasztásra, és az egyes port LED-ek színei ennek az üzemmódnak megfelelően világítanak. Ha a port LED nem világít, a PoE ki van kapcsolva az adott porton. Ha a port LED zöld, a PoE be van kapcsolva. Ha a port LED felváltva zöld-sárga, a PoE le van tiltva, mert nincs elegendő tápkapacitás a portra csatlakoztatott eszköz ellátására. Ha a LED sárgán villog, akkor a PoE meghibásodás miatt ki van kapcsolva. Ha a LED sárga, a PoE a porton le van tiltva.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

A kapcsolók távoli felügyeletéhez be kell állítani rajtuk egy IP-címet és egy alhálózati maszkot. Ne felejtsük el, hogy a kapcsoló távoli hálózatról történő eléréséhez konfigurálni kell egy alapértelmezett átjárót is! Ez nagyban hasonlít a munkaállomások IP-beállításához. Az ábrán az S1 kapcsoló virtuális interfészéhez (Switch Virtual Interface, SVI) kell IP-címet rendelni. Az SVI egy virtuális interfész és nem a kapcsoló egy fizikai portja.

Az SVI a VLAN-hoz szorosan kötődő fogalom. A VLAN-ok számmal ellátott logikai csoportok, amikhez fizikai portokat lehet hozzárendelni. Egy VLAN konfigurációs beállításai az adott VLAN-hoz rendelt fizikai portokra is érvényesek.

Alapértelmezésben a kapcsoló felügyelete a VLAN 1-en keresztül történik. Csak a VLAN-hoz tartozó virtuális interfész (SVI) kaphat IP-címet, a fizikai portok nem. Szintén alapértelmezés, hogy kezdetben minden port az 1-es VLAN-hoz van hozzárendelve. Biztonsági okokból ajánlatos nem a VLAN 1-et használni felügyeleti célokra!

Ne felejtsük el, hogy ezek az IP-beállítások csak a kapcsoló távoli felügyeletére vonatkoznak, vagyis nem teszik lehetővé a kapcsolón áthaladó hálózati rétegbeli (Layer 3) csomagok forgalomirányítását!

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

**1. A felügyeleti interfész konfigurálása**

A kapcsoló felügyeleti SVI-interfészén IP-címet és alhálózati maszkot kell beállítani (VLAN interfész konfigurációs mód). Amint az 1. ábrán is látható, az **interface vlan 99** utasítással lépünk be az interfész konfigurációs módba. Majd az **ip address** paranccsal IP-címet állítunk be. A **no shutdown** utasítás engedélyezi (felkapcsolja) az interfészt. Ebben a példában, a VLAN 99-en a 172.17.99.11 IP-címet állítottuk be.

A VLAN 99-hez tartozó SVI interfész addig nem kerül "up/up" állapotba, míg a VLAN 99-et nem hozzuk létre, és nem csatlakozik egy eszköz a VLAN 99-hez tartozó valamelyik fizikai porthoz. Használjuk a következő utasításokat a 99-es azonosítójú VLAN létrehozásához és fizikai porttal történő összerendeléséhez:

S1(config)# **vlan** *vlan\_azonosító*

S1(config-vlan)# **name** *vlan\_név*

S1(config-vlan)# **exit**

S1(config)# **interface** *interfész\_azonosító*

S1(config-if)# **switchport access vlan** *vlan\_azonosító*

**2. Alapértelmezett átjáró beállítása**

Alapértelmezett átjárót kell beállítani a kapcsolón, ha nem csak a saját (közvetlenül csatlakoztatott) hálózatáról szeretnénk felügyelni az eszközt. Az alapértelmezett átjáró általában az a forgalomirányító, amelyhez a kapcsoló csatlakozik. A kapcsoló az alapértelmezett átjáró felé fogja továbbítani azokat a csomagokat, melyek célállomása egy külső hálózatban található. Amint a 2. ábrán látható, S1 számára az R1 az alapértelmezett átjáró. Az R1 forgalomirányító S1 kapcsolóhoz csatlakozó interfészének IP-címe 172.17.99.1. Tehát ez a cím az alapértelmezett átjáró S1 számára.

A kapcsoló alapértelmezett átjárójának beállításához használjuk a **ip default-gateway** parancsot, majd adjuk meg az átjáró IP-címét. Az alapértelmezett átjáró a forgalomirányító azon interfészének az IP-címe, amely a kapcsolóhoz csatlakozik. A beállítások elmentéséhez használjuk a **copy running-config startup-config** utasítást.

**3. A konfiguráció ellenőrzése**

Amint a 3. ábrán látható, a **show ip interface brief** utasítást használhatjuk a kapcsoló fizikai és virtuális interfészeinek ellenőrzésére. Megfigyelhetjük, hogy a VLAN 99-en beállítottuk az IP-címet és az alhálózati maszkot, valamint hogy az interfész működőképes is.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló kezdeti beállításai

**Ebben a laborgyakorlatban a következő feladatokat végezzük el:**

* 1. rész: A hálózat kábelezése és a kapcsoló alapértelmezett beállításainak vizsgálata.
* 2. rész: Hálózati eszköz alapvető konfigurálása.
* 3. rész: Beállítások ellenőrzése és a hálózati kapcsolatok tesztelése.
* 4. rész: MAC-címtábla kezelése.

[Laborgyakorlat - Configuring Basic Switch Settings](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/2.1.1.6%20Lab%20-%20Configuring%20Basic%20Switch%20Settings.pdf)

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

Az ábra a teljes- és félduplex (full-duplex és a half-duplex) kommunikációt szemlélteti.

A teljes duplex kommunikáció javítja a kapcsolt LAN-ok teljesítményét. Megnöveli a hasznos sávszélességet azáltal, hogy a kapcsolat mindkét végén egyszerre lehet küldeni és fogadni adatokat. A műveletsort kétirányú kommunikációnak is nevezik. Ez a hálózati teljesítményt optimalizáló módszer feltételezi az úgynevezett mikro-szegmentálást, amely akkor jön létre, ha a LAN-kapcsoló minden portjára csak egy eszköz csatlakozik, és a portok teljes duplex módban üzemelnek. Ennek eredménye egy egyetlen eszközből álló, "minimális" méretű ütközési tartomány. Mivel csak egy eszközt tartalmaz, a mikro-szegmentált LAN ütközésmentes.

Ellentétben a teljes duplex kommunikációval, a félduplex kommunikáció egyirányú, az adatok küldése és fogadása nem egyidejűleg történik. Az ilyen kommunikáció teljesítményromlást okoz, mert az adatok csak egy irányban történő áramlása gyakran ütközésekhez vezet. A félduplex kapcsolatokat főleg a régebbi hardverekben találjuk meg, mint például a koncentrátorokban (hub). A legtöbb eszközben a félduplex kommunikációt már kiváltotta a teljes duplex mód.

A manapság forgalomban kerülő Ethernet és FastEthernet hálózati csatolók (NIC) teljes duplex képességgel rendelkeznek. A Gigabit Ethernet és a 10 Gb-es hálózati kártyák csak teljes duplex kapcsolaton működnek. Teljes duplex módban az ütközést érzékelő áramkör a hálózati kártyán le van tiltva, mivel a két csatlakozott eszköz egymásnak küldött keretei nem tudnak ütközni egymással, ugyanis azok külön-külön áramköröket használnak a hálózati kábelben. A teljes duplex csatlakozáshoz vagy egy kapcsoló szükséges, vagy megvalósíthatjuk azt két gép között egy Ethernet kábellel is.

Míg egy normál, hub-alapú osztott Ethernet hálózat hatékonysága általában 50-60 százalék az alap sávszélességhez képest, addig a teljes duplex kapcsolat 100 százalékos hatékonyságot biztosít mindkét irányban (adó és vevő). Ennek eredménye a megadott sávszélesség 200 százalékos felhasználásának lehetősége.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

**Duplexitás és sebesség**

A kapcsoló portjait manuálisan is be lehet állítani az egyedi duplexitás vagy sebesség követelményeknek megfelelően. Használjuk a **duplex** interfész konfigurációs parancsot egy port duplexitásának beállításához. Használjuk a **speed** interfész konfigurációs parancsot egy port sebességének beállításához. Az 1. ábrán az S1 és S2 kapcsolók F0/1 portja manuálisan lett konfigurálva a **duplex** utasítás **full** opciójával, és a **speed** utasítás **100** opciójával.

A Cisco Catalyst 2960 és 3560 kapcsolóknál a duplexitás és a sebesség automatikus felismerése az alapértelmezett beállítás. A 10/100/1000 portok működhetnek fél- vagy teljes duplex módban is, ha 10 vagy 100 Mb/s-ra vannak állítva, de amikor értékük 1000 Mb/s, akkor csak teljes duplex módban üzemelhetnek. A Cisco javasolja, hogy használjuk a **auto** opciót a duplexitás és a **sebesség** beállításához, hogy elkerüljük az eszközök közötti kapcsolódási problémákat. Egy kapcsoló portjának hibajavításakor a duplexitás és a sebesség beállításokat ellenőrizni kell!

**MEGJEGYZÉS**: A duplexitás és sebesség eltérő beállításai kapcsolódási problémákat okozhatnak. Az automatikus egyeztetés (auto negotiation) hibája eltérő beállításokat eredményezhet.

A száloptikai kapcsolatok, mint például 100BASE-FX portok, csak az előre beállított sebességgel és mindig teljes duplex módban működnek.

Használjuk a 2. ábrán lévő parancsszimulátort az S1 kapcsoló F0/1 portjának beállítására!

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

Egészen a közelmúltig a készülékek egymáshoz csatlakoztatásához különböző típusú (egyenes vagy kereszt) kábelek voltak szükségesek. Kapcsoló és kapcsoló, vagy kapcsoló és forgalomirányító között másfajta Ethernet kábelt kellett alkalmaznunk. Az auto-MDIX (automatic medium-dependent interface crossover, automatikus közegfüggő interfész fordítás) funkció kiküszöbölte ezt a problémát. Amikor az auto-MDIX engedélyezett, az interfész automatikusan felismeri a megfelelő kábel típusát (egyenes vagy kereszt), és ennek megfelelően konfigurálja a kapcsolatot. Ha egy kapcsolót az auto-MDIX funkció nélkül kívánunk más eszközökkel összekötni, akkor egyenes kábelt kell használnunk szerverek, munkaállomások és forgalomirányítók csatlakoztatására, míg fordított kábelt kapcsolók és hub-ok esetén.

Az auto-MDIX engedélyezésével, bármelyen típusú kábelt használhatunk két eszköz összekötésénél, az interfész automatikusan be fogja állítani a megfelelő értékeket. Az újabb Cisco forgalomirányítóknál és kapcsolóknál az **mdix auto** paranccsal engedélyezhetjük ezt a képességet interfész konfigurációs módban. Az auto-MDIX használatakor az interfész sebességét és duplexitását is **auto** értékre kell állítani, hogy ez a funkció is megfelelően működjön.

Az auto-MDIX beállításához szükséges parancsok az 1. ábrán láthatók.

**MEGJEGYZÉS**: Az automatikus MDIX funkció alapértelmezés szerint engedélyezve van a Catalyst 2960 és a Catalyst 3560 kapcsolóknál, de nem támogatott a régebbi Catalyst 2950 és a Catalyst 3550 kapcsolók esetén.

Egy interész auto-MDIX beállításának ellenőrzésére használjuk a **show controllers ethernet-controller** utasítást a **phy** opcióval. Hogy leszűkítsük a megjelenő kimenetet az auto-MDIX-el kapcsolatos sorokra, alkalmazzuk a **include Auto-MDIX** szűrőt. A 2. ábrán látható módon ellenőrizhetjük, hogy a funkció engedélyezett-e.

A 3. ábrán lévő parancsszimulátorral gyakorolhatjuk az S2 kapcsoló F0/1 portjának auto-MDIX beállítását.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

Az 1. ábra a **show** utasítás néhány opcióját tartalmazza, amelyek segíthetnek a kapcsolón beállított funkciók áttekintésében.

A 2. ábrán a **show running-config** utasítás rövidített kimenete látható. Ezt a parancsot is használhatjuk a kapcsoló konfigurációjának ellenőrzésére. Amint a parancskimenetből látható, az S1 az alábbi beállításokkal rendelkezik:

* A Fast Ethernet 0/18 interfész a menedzsment VLAN-hoz (VLAN 99) van rendelve
* A VLAN 99 IP-címe és alhálózati maszkja 172.17.99.11 255.255.0.0
* Az alapértelmezett átjáró címe 172.17.99.1

A **show interfaces** egy másik közkedvelt parancs, amely megmutatja a kapcsoló interfészeinek állapotát és különböző statisztikai információit. A **show interfaces** utasítást gyakran használjuk, ha beállítunk vagy felügyelünk hálózati eszközöket.

A 3. ábrán a **show interfaces fastEthernet 0/18** utasítás kimenetét láthatjuk. Az első sor azt mutatja, hogy a FastEthernet 0/18 interfész "up/up" állapotban van, vagyis mind a fizikai-, mind az adatkapcsolati réteg működőképes. Lejjebb az látszódik, hogy a port teljes duplex üzemmódban és 100 Mb/s sebességgel működik.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

A **show interface** parancs segít felismerni az átviteli közeg gyakori problémáit. A parancskimenet egyik legfontosabb eleme a vonali és adatkapcsolati protokollok állapotának megjelenítése. Az 1. ábrán egy interfészre vonatkozó összegző sor látható.

Az első paraméter (FastEthernet0/1 is up) a fizikai rétegre utal és lényegében azt tükrözi, hogy a fogadó interfész megkapja-e a vonal túloldaláról a vivőérzékelő jelet. A második paraméter (line protocol is up) az adatkapcsolati rétegre utal, és azt mutatja, hogy az adatkapcsolati réteg protokollja "ébrenléti" (keepalive) jeleket fogad.

A **show interface** utasítás kimenete alapján a következő lehetséges problémákra következtethetünk:

* Ha az interfész működik, de a vonali protokoll nem (up/down), akkor második rétegbeli hiba áll fenn. Lehetséges, hogy eltérő a beágyazás (encapsulation) típusa, a túloldal interfésze hiba miatt lekapcsolt (error-disabled) állapotban van, vagy hardver jellegű probléma lépett fel.
* Ha a vonali protokoll és az interfész egyaránt nem működő (down) állapotban van, akkor vagy a kábel nincs csatlakoztatva, vagy valamilyen más interfész probléma áll fenn. Például, egy közvetlen (úgynevezett back-to-back) kapcsolat esetén a túloldali interfész felügyeletileg lekapcsolt (administratively down) állapotban van.
* Ha az interfész felügyeletileg lekapcsolt állapotban van, akkor azt manuálisan (a **shutdown** utasítás kiadásával) tiltották le a konfigurációban.

A 2. ábrán egy példa látható a **show interface** utasítás kimenetére, mely számlálókat és statisztikai adatokat mutat a FastEthernet0/1 interfészről.

Néha az átviteli közeg hibái nem vezetnek az áramkör leállásához, de hálózati teljesítménycsökkenést okoznak. A 3. ábrán azokat a gyakori hibákat láthatjuk, amelyeket a **show interface** parancs használatával vehetünk észre.

A bejövő hibák (input errors) számláló az összes, a vizsgált interfészre érkező hibás adatcsomag darabszámát adja meg. Ez magában foglalja a következő számlálókat: töredékek (runts), óriások (giants), CRC, nincs puffer (no buffer), keret (frame), túllépett (overrun), és mellőzött (ignored). A **show interface** utasítás által vizsgált bemeneti számlálók jelentése a következő:

* **Töredék (runt) keretek** - Azokat az Ethernet kereteket hívják töredéknek, amelyek kisebbek, mint a 64 bájtos megengedett minimális keretméret. Számuk túlzott növekedését általában egy hibásan működő hálózati kártya okozza, de keletkezhetnek a gyakori ütközések eredményeképpen is.
* **Óriás (giant) keretek** - Azokat az Ethernet kereteket nevezzük óriásoknak (giants), amelyek nagyobbak, mint a maximálisan megengedett keretméret. A kiváltó okok általában megegyeznek a töredék kereteket létrehozó okokkal.
* **CRC-hibák** - Az Ethernet és a soros interfészeken a CRC-hiba általában azt jelzi, hogy átviteli közeg vagy kábel probléma lépett fel. Jellemző hibák: elektromos interferencia, meglazult vagy sérült csatlakozók, nem megfelelő kábeltípus alkalmazása. Ha túl sok a CRC-hiba, akkor "zajos" a vonal, és meg kell vizsgálni a kábel épségét és hosszát. Egyben a zajforrást is érdemes megkeresni és megszüntetni.

A kimenő hibák (output errors) számláló az interfészen fellépő hiba miatt el nem küldött adatcsomagok számát mutatja meg. A **show interface** utasítás által vizsgált kimeneti számlálók jelentése a következő:

* **Ütközések (collisions)** - Az ütközések a félduplex üzemmód teljesen normális jelenségei, és nem kell aggódni miattuk, amíg a kapcsolat a kívánalmaknak megfelelően működik. Teljes duplex üzemmódban, egy helyesen megtervezett és kialakított hálózatban, soha nem fordulhat elő ütközés. Ezért mindenhol ajánlott a teljes duplex üzemmód használata, hacsak nem olyan régebbi berendezéseket használunk, amelyek csak a félduplex működést támogatják.
* **Késői ütközések (late collosions)** Ha az ütközés az első 64 bájtnyi adat (az un. preamble mező) elküldése után történik, akkor késői vagy időrés utáni ütközésről beszélünk. A késői ütközés egyik leggyakoribb előidézője a túl hosszú kábel, egy másik pedig a duplexitás helytelen beállítása. Például, akkor lehet ilyen probléma, ha a kapcsolat egyik végén teljes duplex, míg a másikon félduplex beállítás található. Azon az interfészen láthatók a kései ütközések, amelyiken félduplex továbbítás van konfigurálva. A hiba kijavítása érdekében mindkét oldalon ugyanazt a duplexitást kell beállítani. Egy helyesen megtervezett és kialakított hálózatban soha nem fordulhat elő késői ütközés.

# Kapcsoló alapszintű konfigurálása

## Kapcsoló portjainak beállítása

A kapcsolt hálózat teljesítményét befolyásoló legtöbb probléma már a telepítés során felmerülhet. Elméletileg, a telepítés után egy hálózat gond nélkül működik tovább. Azonban sérülhet a kábelezés, változhat a konfiguráció, és olyan új eszköz is csatlakozhat a kapcsolóhoz, amelyik konfigurációs változtatásokat igényel. Ezért szükséges a hálózat folyamatos karbantartása és hibaelhárítása!

Ha nincs vagy rossz a csatlakozás a kapcsoló és egy másik eszköz között, akkor a hiba elhárításához kövessük ezt az általános eljárást:

Használjuk a **show interface** parancsot az interfész állapotának ellenőrzésére!

Az interfész nem működik (down állapot):

* Győződjünk meg arról, hogy megfelelő kábeleket használunk, és ellenőrizzük a kábel és a csatlakozók épségét. Ha rossz vagy nem megfelelő a kábel, akkor cseréljük ki!
* Amennyiben az interfész még mindig nem működik, akkor a probléma oka az eltérő sebességbeállítás lehet. Az interfész sebessége általában automatikusan kerül konfigurálásra. Ha az egyik interfész mégis manuálisan lenne beállítva, akkor ettől függetlenül a másik oldal használhatja az automatikus beállításokat. Ha a sebességeltérés téves beállítások vagy hardver-szoftver probléma miatt lép fel, akkor ez az interfész leállásához is vezethet. Amennyiben ilyen jellegű probléma valószínűsíthető, akkor állítsuk be kézzel ugyanazt a sebességet mindkét oldalon!

Az interfész működik, de a kapcsolat problémái továbbra is fennállnak:

* A **show interface** utasítással ellenőrizzük, hogy van-e túlzott zajra utaló jelzés. Ilyen lehet a töredék-, óriás- és a CRC-hibák számlálóinak növekedése. Ha túl nagy a zaj, először találjuk meg és távolítsuk el a zaj forrását, amennyiben ez lehetséges. Vizsgáljuk meg, hogy a kábelhossz nem haladja-e meg a maximálisan engedélyezett értéket és ellenőrizzük a használt kábel típusát is. Rézkábel esetén ajánlott a minimum 5-ös kategóriájú (Cat5) vezeték használata.
* Ha nem a zaj a probléma, akkor ellenőrizzük az ütközések mértékét. Ha vannak ütközések, vagy késői ütközések, akkor nézzük meg a kapcsolat mindkét végén a duplex beállításokat. Hasonlóan a sebességértékekhez, a duplex beállítások is általában automatikusan történnek. Ha az eltérő duplexitás használata lehet a probléma, akkor manuálisan állítsuk be azt a kapcsolat mindkét oldalán. Javasolt a teljes duplex mód alkalmazása, ha mindkét fél támogatja azt.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonságos távoli hozzáférés

A Secure Shell (SSH) protokoll biztonságos (titkosított) felügyeleti kapcsolatot biztosít egy távoli eszközhöz, ezért Telnet helyett ennek használata javasolt. A Telnet egy régi protokoll, amely nem biztonságos módon, nyílt szövegként továbbítja mind a bejelentkezési hitelesítő adatokat (felhasználónév és jelszó), mind az eszközök közötti egyéb adatkommunikációt. Az SSH biztonságos távoli kapcsolatokat valósít meg, mert erős titkosítást használ a hitelesítéshez (felhasználónév és jelszó kezelése), valamint az eszközök között kommunikációhoz. Az SSH-hoz a 22-es TCP-portot rendelték, míg a Telnet a 23-as TCP-portot használja.

Az 1. ábrán egy támadó Wireshark használatával követi nyomon a csomagokat. A Telnet kommunikáció ki van téve a felhasználónév és jelszó lehallgatásának.

A 2. ábrán a támadó elfogja a rendszergazda felhasználónevét és a jelszavát a nyílt szöveget használó Telnet kapcsolatból.

A 3. ábrán egy SSH-kapcsolatot láthatunk a Wireshark programmal. A támadó képes követni a kapcsolatot a rendszergazda számítógép IP-címe által.

Azonban, ahogy a 4. ábrán látható, a felhasználónév és a jelszó titkosított.

Ahhoz, hogy engedélyezzük az SSH-t a Catalyst 2960 kapcsolón, az eszköznek kriptográfiai (titkosítási) funkciókkal és képességekkel rendelkező IOS-t kell futtatnia. Az 5. ábrán, a **show version** utasítást használjuk az IOS típusának megállapítására. Az IOS nevében szereplő "k9" a kriptográfiai (titkosítási) funkciókat és képességeket jelenti.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonságos távoli hozzáférés

Az SSH konfigurálása előtt a kapcsolónak rendelkeznie kell egyedi eszköznévvel és megfelelő hálózati beállításokkal.

**1. Az SSH támogatás ellenőrzése.**

A **show ip ssh** paranccsal lehet ellenőrizni a kapcsoló SSH-támogatását. Ha a kapcsoló nem kriptográfiai IOS-t futtat, akkor ezt a parancsot az eszköz nem fogja felismerni.

**2. Az IP-tartománynév beállítása.**

A hálózat IP-tartománynevének beállítására használjuk az **ip domain-name** *tartománynév* globális konfigurációs parancsot. Az 1. ábrán a *tartománynév* értéke **cisco.com.**.

**3. RSA-kulcspár generálása.**

Az RSA-kulcspár generálása automatikusan engedélyezi az SSH-t. A **crypto key generate rsa** globális konfigurációs paranccsal engedélyezhetjük a kapcsolón az SSH-t, és egyben RSA-kulcspárt is generálhatunk. Az RSA-kulcsok létrehozásakor a rendszergazdának meg kell adni a használni kívánt modulus hosszúságot. A Cisco javaslata szerint legalább 1024 bit hosszúságúnak kell lennie a modulusnak (lásd az 1. ábrán látható mintát). Hosszabb modulus használata sokkal biztonságosabb, de egyben hosszabb ideig is tart a kulcs előállítása és használata.

**MEGJEGYZÉS**: az RSA-kulcspár törléséhez használjuk a **crypto key zeroize rsa** globális konfigurációs parancsot. Miután az RSA-kulcspár törlésre kerül, az SSH-szerver automatikusan kikapcsol.

**4. Felhasználói hitelesítés beállítása.**

Az SSH-szerver hitelesítheti a felhasználókat helyi adatbázis vagy hitelesítési szerver segítségével. A helyi adatbázisból történő hitelesítéshez meg kell adnunk egy felhasználónevet és jelszót a **username** *felhasználónév* **secret** *jelszó* globális konfigurációs paranccsal. A példában a felhasználó **admin** és a hozzárendelt jelszó a **ccna.**.

**5. A VTY-vonalak beállítása.**

Az SSH-protokoll VTY-vonalon történő engedélyezéséhez használjuk a **transport input ssh** vonali konfigurációs parancsot. A Catalyst 2960 VTY-vonalai a 0-15 értéktartományba esnek . Ez a beállítás megakadályozza a nem SSH (például Telnet) kapcsolatokat, és egyedüli felügyeleti protokollnak az SSH-t engedélyezi. Használjuk a **line vty** globális konfigurációs parancsot, majd a **login local** vonali konfigurációs utasítást a helyi hitelesítési adatbázis használatához.

A 2. ábrán található parancsszimulátorban gyakorolhatjuk az S1 kapcsoló SSH-támogatásának beállítását.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonságos távoli hozzáférés

A PC-n egy SSH-kliens, mint például a PuTTY, szükséges az SSH-szerverhez való csatlakozásra. Az 1-3. ábrákon szereplő példában az alábbiak lettek beállítva:

* Az SSH engedélyezett az S1 kapcsolón
* Az S1 kapcsoló VLAN 99 (SVI) interfészének IP-címe 172.17.99.11
* A PC1 IP-címe 172.17.99.21

Az 1. ábrán látható, hogy a számítógép kezdeményezi az SSH-kapcsolatot az S1 kapcsoló SVI VLAN-interfészének IP-címére.

A 2. ábrán az látható, hogy a felhasználónak meg kell adnia a felhasználónevet és a jelszót. Az előző példában látható beállítások alapján a felhasználónév **admin** és a jelszó **ccna** . A helyes belépési adatok megadása után a felhasználó SSH-n keresztül csatlakozik a Catalyst 2960 kapcsoló CLI-felületére.

Az SSH-verzió és a beállítások megjelenítésére használjuk a **show ip ssh** parancsot. A példában az SSH 2-es verziója van engedélyezve. Az eszköz SSH-kapcsolatainak ellenőrzésére használjuk a **show ssh** parancsot (lásd 3. ábra).

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonságos távoli hozzáférés

A felügyeleti kapcsolatok biztosítására a Telnet helyett az SSH ajánlott. A Telnet nem biztonságos, nyílt szöveg alapú kommunikációt folytat. Az SSH biztonságos távoli kapcsolatokat valósít meg, mert erős titkosítást használ minden adat továbbításához. Ebben a feladatban egy távoli kapcsoló számára kell beállítani a titkosított jelszavak és az SSH használatát.

[Packet Tracer - Configuring SSH Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/2.2.1.4%20Packet%20Tracer%20-%20Configuring%20SSH%20Instruction.pdf)

[Packet Tracer - Configuring SSH - PKA](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/2.2.1.4%20Packet%20Tracer%20-%20Configuring%20SSH.pka)

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonsági problémák LAN-környezetben

A kapcsoló alapbeállításai nem védenek a rosszindulatú támadások ellen. A biztonság egy rétegekbe rendezett folyamat, amely lényegében soha nem teljes. Cél, hogy egy szervezet hálózati szakemberei minél inkább tisztában legyenek a biztonsági támadásokkal és a velük járó veszélyekkel. Néhány biztonsági támadás leírása megtalálható a következő fejezetekben, de a támadások kivitelezésének pontos részletei már túlmutatnak a kurzus keretein. További részletes információ található a CCNA WAN-protokollok és a CCNA Security tananyagokban.

**MAC-cím elárasztás**

Egy kapcsoló MAC-címtáblája a portokhoz csatlakozott eszközök MAC-címeit és a porthoz tartozó VLAN adatait tartalmazza. Amikor egy 2. rétegbeli kapcsoló egy továbbítandó keretet kap, akkor a kapcsoló megkeresi a cél MAC-címet a MAC-címtáblázatában. Minden Catalyst kapcsoló a MAC-címtáblát használja a 2. rétegbeli kerettovábbításra. Amint a keret megérkezik a kapcsoló egy portjára, a keret forrás MAC-címe rögzítésre kerül a MAC-címtáblázatban. Ezután a kapcsoló megvizsgálja a cél MAC-címet, és ha létezik már bejegyzés hozzá a táblában, akkor továbbítja a keretet a megfelelő portra. Ha a cél MAC-cím még nem létezik a MAC-címtáblázatban, akkor a kapcsoló elárasztással kiküldi a keretet az összes aktív porton, kivéve azon, ahonnan a keret érkezett.

A táblában nem létező címek miatt alkalmazott keret elárasztás lehetőséget ad a kapcsoló megtámadására, melyet úgynevezett MAC-címtábla túlcsordulásos támadásnak hívnak. További gyakori elnevezései a MAC-elárasztásos támadás vagy CAM-tábla túlcsordulásos támadás. Az ábrákon megtekinthető, hogyan működik egy ilyen típusú támadás.

Az 1. ábrán az "A" állomás adatokat küld a "B"-nek. A kapcsoló fogadja a kereteket, és megkeresi a cél MAC-címet a MAC-címtáblában. Ha nem találja a célcímet a táblázatban, akkor elárasztással kiküldi a keretet az összes porton, kivéve azon, ahonnan a keret érkezett.

A 2. ábrán a "B" állomás megkapja a keretet, és elküldi válaszát az "A"-nak. A kapcsoló ekkor tanulja meg, hogy a "B" MAC-címe a 2-es porton található, és ezt az információt rögzíti a MAC-címtáblában.

A "C" állomás szintén megkapja az "A"-ból a "B"-nek címzett keretet, de mivel a cél MAC-cím a "B", ezért a "C" eldobja a keretet.

A 3. ábrán látható, hogy ezután az "A" állomás (vagy bármely másik) által a "B"-nek küldött keret a 2-es portra kerül továbbításra és a kapcsoló már nem árasztja el a kerettel az összes portot.

Mivel a MAC-címtábla korlátozott méretű, a MAC elárasztásos támadások kihasználják ezt, és addig küldenek a kapcsolónak hamis forrás MAC-című kereteket, míg ezekkel a táblázat megtelítődik.

A 4. ábrán látható, hogy a támadó "C" állomás küldhet olyan kereteket, amelyek hamis, véletlenszerűen generált forrás és cél MAC-címeket tartalmaznak. A kapcsoló folyamatosan frissíti a MAC-címtáblázatát a hamis keretekben található információkkal. Ha a MAC-címtábla telítődött a hamis MAC-címekkel, akkor a kapcsoló úgynevezett meghibásodott-nyitott (fail-open) módba vált. Ebben az üzemmódban a kapcsoló minden beérkező keretet elárasztásos módon küld tovább a hálózaton, ennek eredményeként, a támadó láthatja a hálózati forgalom összes keretét.

Egyes hálózati támadó segédprogramok képesek akár percenként 155 000 MAC-bejegyzést generálni a kapcsolón, melynek MAC-címtáblája a modelltől függően változó méretű.

Amint az 5. ábrán látható, ameddig a kapcsoló MAC-címtáblája tele van, addig minden fogadott keretet elárasztásos módon továbbít minden portra. A példában az "A"-ból a "B"-nek küldött kereteket a kapcsoló a 3-as portra is továbbítja, és így azt a "C"-n lévő támadó is láthatja.

A MAC-címtábla túlcsordulásos támadás kivédésének egyik módja, ha beállítjuk a portbiztonság funkciót.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonsági problémák LAN-környezetben

A DHCP-protokoll a munkaállomásokhoz automatikusan hozzárendel egy érvényes IP-címet egy adott tartományból. A DHCP-t majdnem olyan régóta használják, mint amióta a TCP/IP vált az iparág domináns protokollcsaládjává. Kétféle DHCP-támadás hajtható végre egy kapcsolt hálózaton: a DHCP-kiéheztetés és a DHCP-hamisítás.

A DHCP-kiéheztetés esetén a támadó elárasztja a DHCP-szervert DHCP-kérésekkel, hogy felhasználja az összes rendelkezésére álló IP-címet a tartományából. Miután az IP-címek elfogytak, a szerver nem képes több címet kiadni, így ez a módszer szolgáltatásmegtagadási (DoS) támadásnak minősíthető, ugyanis új kliensek nem tudnak csatlakozni a hálózathoz. Minden olyan támadást DoS-támadásnak nevezünk, amelyben hamis forgalommal terhelnek túl egy adott eszközt vagy szolgáltatást, hogy megakadályozzák a valódi kliensek kiszolgálását.

A DHCP-hamisítás esetén a támadó egy hamis DHCP-szervert állít fel a hálózaton, hogy az osszon IP-címeket az ügyfelek számára. Ennek a támadásnak az az általános célja, hogy hamis DNS- vagy WINS-szerver beállításokat kényszerítsen rá a kliensekre, tovább, hogy hamis alapértelmezett átjáróként használják a támadó, vagy az irányítása alatt lévő egyik eszközt.

A DHCP-kiéheztetést gyakran használják a DHCP-hamisítás támadás előtt, hogy blokkolják a valódi DHCP-szervert, ami azután megkönnyíti a hamis DHCP-szerver beillesztését a hálózatba.

Cisco Catalyst kapcsolókon a DHCP-támadások kivédésére használjuk a DHCP-ellenőrzés (DHCP-snooping) és a portbiztonság funkciókat! Ezekkel egy későbbi témakör foglalkozik részletesebben.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Biztonsági problémák LAN-környezetben

A Cisco Discovery Protocol (CDP) egy Cisco által fejlesztett saját protokoll, amelyet az összes Cisco eszközön be lehet állítani. A CDP felderíti a közvetlenül kapcsolódó Cisco eszközöket, így lehetővé válik a kapcsolatnak megfelelő automatikus eszközbeállítás. Egyes esetekben ez leegyszerűsíti a konfigurációt és a csatlakozást.

Alapértelmezés szerint a legtöbb Cisco forgalomirányító és kapcsoló összes portján engedélyezett a CDP. A CDP rendszeres időközönként szórással továbbít az eszközökről titkosítatlan információkat, melyek frissítik a lokális CDP-adatbázist. Mivel a CDP egy 2. rétegben működő protokoll, ezért a CDP-üzeneteket a forgalomirányítók nem továbbítják.

A CDP-üzenetek információkat tartalmaznak a készülékekről, ilyenek például az IP-címek, szoftververzió, platform, képességek, és a natív VLAN beállítás. Ezen információk ismeretében a támadó megtalálhatja a támadás megfelelő módját, amely rendszerint valamilyen szolgáltatásmegtagadási (DoS) támadás.

Az ábra egy Wireshark által elfogott CDP-csomag részletét mutatja be. A Cisco IOS szoftververzióját láthatjuk a CDP-csomagban, ami különösen veszélyes, mert így megállapítható, hogy van-e a szoftverváltozatnak valamilyen támadható sérülékenysége. Továbbá, mivel a CDP nem hitelesíti a másik felet, ezért a támadó hamis CDP-csomagokat is küldhet a közvetlenül csatlakozó Cisco eszköznek.

Javasolt, hogy tiltsuk le a CDP-t azokon az eszközökön vagy portokon, ahol használata nem szükséges. Ezt a **no cdp run** globális konfigurációs paranccsal tehetjük meg. A CDP-t tilthatjuk portonként is.

**Telnet támadások**

A Telnet protokoll nem biztonságos, és ezt egy támadó felhasználhatja egy távoli Cisco hálózati eszközhöz való hozzáféréshez. Rendelkezésre állnak olyan segédeszközök, amelyek lehetővé teszik, hogy a támadó nyers erő (Brute force) jelszófeltörést indítson a kapcsolók vty-vonalaihoz való hozzáférésért.

**Nyers erő (Brute force) jelszótámadás**

A nyers erő jelszótámadás első fázisa az, hogy a támadó egy alkalmazás segítségével megpróbál Telnet kapcsolatokat kiépíteni, eközben végigpróbálja a gyakran használt jelszavakat és egy szótárállomány összes tételét. Ha a jelszót nem sikerült kitalálni az első fázisban, akkor a nyers erő támadás második szakaszában a támadó egy program segítségével szekvenciális karakter kombinációkat hoz létre, és ezekkel próbálja kitalálni a jelszót. Ha elegendő idő áll rendelkezésre, a nyers erő támadás szinte az összes jelszót fel tudja törni.

A nyers erő támadások kivédésére használjunk erős jelszavakat és változtassuk azokat rendszeresen! Az erős jelszavaknak tartalmazniuk kell kis- és nagybetűket, valamint számokat és szimbólumokat (speciális karaktereket). Továbbá, a VTY-vonalakra történő belépés is korlátozható a hozzáférési listák (ACL) használatával.

**Telnet DoS-támadás**

A Telnet-et fel lehet használni DoS-támadás indítására is, melyben a támadó kihasználja a Telnet szerver sérülékenységeit, ezáltal ellehetetleníti, hogy mások is hozzáférhessenek az eszközhöz Telnet protokollon keresztül. Ez a fajta támadás megakadályozza, hogy a rendszergazda távolról is elérje a kapcsolót. Ráadásul más támadásokkal is összehangolható, így tovább nehezíti a rendszergazda távoli hozzáférését az eszközökhöz.

A DoS-támadásokat lehetővé tevő Telnet sérülékenységeket ki lehet védeni újabb IOS-ek használatával, amelyek már tartalmazzák az említett hibák javításait.

**MEGJEGYZÉS**: Távoli felügyelet biztosítására ajánlott Telnet helyett SSH-t használni.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Bevált biztonsági módszerek

A hálózati támadások elleni védekezés éberséget és képzettséget igényel. A hálózat biztonságossá tételében a következő bevált módszerek alkalmazhatók:

* Dolgozzunk ki egy írásos biztonságpolitikát a szervezet számára!
* Tiltsuk le a nem használt szolgáltatásokat és portokat!
* Használjunk erős jelszavakat és cseréljük azokat gyakran!
* Szabályozzuk az eszközökhöz történő fizikai hozzáférést!
* Kerüljük a nem biztonságos HTTP-oldalakat, különösen bejelentkezési adatok megadásánál, helyette használjuk a biztonságos HTTPS-t!
* Rendszeresen készítsünk mentéseket, és teszteljük is azokat!
* Világosítsuk fel a dolgozókat a megtévesztési technikákról (social engineering), valamint dolgozzunk ki olyan szabályokat, amelyekkel a felek ellenőrizhetik a másik személyazonosságát telefonon, e-mailen és személyes érintkezés közben!
* Kódoljuk és védjük jelszóval a fontos információkat!
* Használjunk biztonsági hardvereket és szoftvereket, mint például a tűzfalak!
* Frissítsük a szoftvereket állandóan, heti vagy akár napi rendszerességgel a javítócsomagok telepítésével!

Ezek a módszerek csak kiindulópontok a biztonsági felügyelethez. A szervezeteknek állandóan ébernek kell maradniuk a folyamatosan változó fenyegetésekkel szemben. Fontos az olyan hálózati biztonsági segédeszközök használata, amelyekkel mérhető a hálózat jelenlegi sérülékenysége.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Bevált biztonsági módszerek

A hálózati biztonsági eszközök segítik a rendszergazdát a hálózat gyenge pontjainak tesztelésében. Egyes segédeszközök lehetővé teszik, hogy a rendszergazda a támadó szerepét tölthesse be. Egy ilyen eszköz használatával a rendszergazda támadást indíthat a saját hálózata ellen, és ellenőrizheti annak eredményét, hogy meghatározza a támadások kivédésére szükséges biztonsági szabályokat. A biztonsági audit és a behatolási tesztelés az a két alapvető funkció, amelyeket ezeknek az eszközöknek biztosítaniuk kell.

A biztonsági tesztelési eljárásokat a rendszergazda manuálisan is kezdeményezheti, míg más tesztek nagy mértékben automatizáltak. A teszt típusától függetlenül az ellenőrzés lefolytatását és kiértékelését végző személyzetnek kiterjedt biztonsági és hálózati ismeretekkel kell rendelkezni. Ez magában foglalja a következő területeken való jártasságot:

* Hálózati biztonság
* Tűzfalak
* Behatolás-megelőző rendszerek (Intrusion Prevention Systems, IPS)
* Operációs rendszerek
* Programozás
* Hálózati protokollok (pl.: TCP/IP)

# Kapcsolók védelme - Felügyelet és megvalósítás

## Bevált biztonsági módszerek

A hálózatbiztonsági segédeszközök lehetővé teszik a rendszergazdák számára, hogy biztonsági ellenőrzést (audit) végezzenek el a hálózaton. A biztonsági ellenőrzés feltárja, hogy milyen típusú információkhoz képes hozzáférni egy támadó a hálózat forgalmának lehallgatásával.

Például, egy biztonsági ellenőrző eszköz lehetővé teszi az adminisztrátor számára, hogy eláraszthassa fiktív MAC-címekkel a kapcsoló MAC-címtábláját. Ezt egy biztonsági audit követi majd, mert a kapcsoló az összes portján elkezdi elárasztással továbbítani a forgalmat. A vizsgálat során kiderül, hogy a kapcsoló szabályos MAC-cím bejegyzései eltűntek, és helyettük csak fiktív MAC-cím bejegyzések találhatók a táblázatban. Az audit megmutatja, melyik porton történt a támadás, és arra is rávilágít, hogy nem volt megfelelő védekezés beállítva a porton.

Az időzítés fontos tényező az ellenőrzés sikeres végrehajtásában. A különböző kapcsolók eltérő számú MAC-cím tárolását teszik lehetővé a MAC-címtáblájukban. Így nehéz meghatározni, hogy milyen mennyiségű hamis MAC-címmel történjen a támadás. A hálózati rendszergazdáknak ráadásul figyelembe kell venniük a MAC-címtábla bejegyzések automatikus elévülését is. Ha a hamis MAC-cím bejegyzések elkezdenek elévülni az audit ideje alatt, és érvényes MAC-címekkel kezd feltöltődni a MAC-címtábla, akkor korlátozódnak az audit által kinyerhető támadási információk.

A hálózatbiztonsági segédeszközök behatolási tesztelésre is használhatók. A behatolási tesztelés egy szimulált támadás, amely során meghatározható, hogy mennyire sérülékeny a hálózat egy valódi támadás esetén. Ez lehetővé teszi a rendszergazda számára a hálózati eszközök konfigurációjában lévő hiányosságok beazonosítását és a szükséges változtatásokat is, amelyekkel az eszköz ellenállóbbá válik a támadásokkal szemben. A rendszergazda számos támadást indíthat el, amiben az is a segítségére van, hogy a legtöbb ilyen eszköz részletes dokumentációval rendelkezik, és pontosan megadott szintaktika található bármelyik kívánt támadás elindításához.

Mivel a behatolási vizsgálatok káros hatással is lehetnek a hálózatra, ezért ezeket fokozottan ellenőrzött körülmények között és a hálózati biztonsági irányelvekben részletezett eljárások alapján kell végrehajtani. Egy olyan, elszigetelten működő teszthálózat, amely utánozza a valódi termelési közegben működő hálózat sajátosságait, ideális a hálózati osztály mérnökei számára a behatolási tesztek elvégzésére.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

**A nem használt portok letiltása**

A legegyszerűbb módszer, melyet sok rendszergazda alkalmaz az illetéktelen hozzáférés megakadályozására, a nem használt portok letiltása. Például, ha a Catalyst 2960 kapcsoló 24 portja közül csak háromhoz van eszköz csatlakoztatva, akkor ajánlott a 21 nem használt portot letiltani. Keressük meg az összes használaton kívüli portot, és mindegyiknél adjuk ki a **shutdown** parancsot! Ha egy portot később újra engedélyezni szeretnénk, akkor ezt a **no shutdown** utasítás kiadásával tehetjük meg, (lásd ábra).

Egy egyszerű módszerrel egyszerre több porton is lehet beállításokat végezni. Ha a portok egy tartományát kell konfigurálnunk, akkor használjuk az **interface range** parancsot.

Switch(config)# **interface range** *típus modul/első portszám - utolsó portszám*

A folyamat, amellyel elvégezhető a portok engedélyezése és letiltása, időigényes lehet, de növeli a biztonságot a hálózaton, vagyis mindenképp megéri ezt a minimális erőfeszítést.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

A DHCP-snooping egy Cisco Catalyst funkció, amely megszabja, hogy a kapcsoló melyik portja válaszolhat a DHCP-kérésekre. A portok lehetnek megbízhatók (trusted) és nem megbízhatók (untrusted). A megbízható portok mindenféle DHCP-üzenetet továbbíthatnak, míg a nem megbízható portok csak a DHCP-kéréseket fogadhatják. A megbízható porthoz csatlakozik, vagy azon keresztül érhető el a DHCP-szerver. Ha a támadó eszköz egy nem megbízható porton keresztül próbál DHCP-válaszcsomagot küldeni a hálózatra, akkor a port letiltásra kerül (shut down). Egy másik funkció a DHCP-opciók küldése, amelyekben a kapcsoló adatai is továbbításra kerülnek a DHCP-kérésben, például a továbbító port azonosítója.

Amint az 1. és 2. ábra mutatja, minden port, amelyeket nem állítottak be közvetlenül megbízhatónak, nem megbízhatónak minősül. A DHCP-hozzárendelés táblában látható, hogy melyik portok nem megbízhatók. A bejegyzések tartalmazzák a kliens MAC-címét, IP-címét, a bérlet időtartamát, a hozzárendelés típusát, a VLAN és port azonosítót. Ezek az adatok a kliens által küldött DHCP-kérés alapján kerülnek rögzítésre. A táblázat alkalmas az elkövetkező DHCP-forgalom szűrésére, mivel a nem megbízhatónak beállított port nem továbbíthat DHCP-szerver típusú válaszokat.

A DHCP-snooping funkciót beállításához, egy Catalyst 2960 kapcsolón, kövessük az alábbi lépéseket::

**1.** Engedélyezzük a DHCP-snooping funkciót a **ip dhcp snooping** globális konfigurációs paranccsal.

**2.** Engedélyezzük a DHCP-snooping funkciót egy adott VLAN-on a **ip dhcp snooping vlan** *VLAN\_azonosító* parancs használatával.

**3.** Állítsuk be interfész konfigurációs módban a **ip dhcp snooping trust** paranccsal, hogy az adott port megbízható legyen.

**4.** Korlátozzuk a nem megbízható portokon a támadó által küldhető hamis DHCP-kérések számát az **ip dhcp snooping limit rate** *kérések\_száma* paranccsal (opcionális).

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

**Portbiztonság**

Minden portot (interfészt) védeni kell, mielőtt a kapcsolót a végleges környezetébe telepítenénk. Az egyik biztonsági módszer a portok védelmére az úgynevezett portbiztonság funkció, mely fizikai interfészenként korlátozza az engedélyezett MAC-címek számát. A szabályosan üzemelő eszközök MAC-címeiről engedélyezi a hozzáférést, míg a többi MAC-címről letiltja azt.

A portbiztonságot egy vagy több MAC-cím számára is be lehet állítani. Ha a porton egyetlen engedélyezett MAC-cím van, akkor kizárólag csak csak a meghatározott MAC-című eszköz kapcsolódhat a portra.

Ha a portbiztonság be van állítva és az engedélyezett MAC-című gépek már kapcsolódtak erra a portra, akkor bármilyen más, idegen MAC-címről érkező csatlakozási kísérlet a biztonsági szabályok megsértését vonja maga után. Az 1. ábrán a legfontosabb megvalósítási elveket láthatjuk.

**MAC-cím védelem típusai**

A portbiztonságot többféle módon is be lehet állítani, melyek a következők:

* **Statikus MAC-cím védelem** - A MAC-címeket manuálisan állítjuk be a portokon a **switchport port-security mac-address** *MAC-cím* interfész konfigurációs paranccsal. A statikusan beállított MAC-címeket a címtábla és az aktív konfiguráció is tárolja.
* **Dinamikus MAC-cím védelem** - A MAC-címek megtanulása ebben az esetben dinamikusan történik, ezeket címeket csak a címtábla tárolja. A táblában levő MAC-címek a kapcsoló újraindulásakor törlődnek.
* **Sticky MAC-cím védelem** - Azokat a címeket soroljuk ide, amelyeket dinamikusan tanult meg a kapcsoló, de nem csak a címtáblában tárolja el, hanem hozzáadja az aktív konfigurációhoz is.

**Sticky MAC-cím védelem**

Annak érdekében, hogy az interfész a dinamikusan tanult címeket átalakítsa "sticky" címekké és elhelyezze az aktív konfigurációban, portonként engedélyeznünk kell ezt a funkciót a **switchport port-security mac-address sticky** interfész konfigurációs paranccsal.

A parancs kiadásával a kapcsoló átalakítja az összes dinamikusan megtanult MAC-címet "sticky" MAC-címmé. Minden ilyen MAC-cím bekerül a címtáblába és az aktív konfigurációba is (a konfigurációhoz ragasztja ezeket a címeket).

"Ragadós" MAC-címeket manuálisan is beállíthatunk a **switchport port-security mac-address sticky** *MAC-cím* interfész konfigurációs paranccsal. Ekkor az összes megadott cím eltárolásra kerül a címtáblában és az aktív konfigurációban.

Ha a "sticky" MAC-címeket elmentjük az indító konfigurációs állományba, akkor újrainduláskor vagy az interfész letiltásakor a kapcsolónak nem kell ismételten megtanulnia ezeket a címeket. Amennyiben a biztonságos címeket nem mentjük el, azok ilyenkor elvesznek.

Ha a funkciót letiltjuk a **no switchport port-security mac-address sticky** interfész konfigurációs paranccsal, a már megtanult címek megmaradnak a címtáblában, de az aktív konfigurációból kitörlődnek.

A 2. ábrán a "sticky" MAC-címek sajátosságai láthatók.

Ne felejtsük, hogy a fenti portbiztonsági utasítások addig nem érvényesek, amíg a **switchport port-security** paranccsal magát a portbiztonságot nem engedélyezzük!

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

Ha az alábbi esetek bármelyike bekövetkezik, akkor az a biztonság megsértésének minősül:

* Az adott interfészen a maximális számú MAC-címet már eltárolta a kapcsoló, de egy újabb munkaállomás próbál meg csatlakozni a portra.
* A VLAN egyik biztonságos interfészén megtanult vagy beállított cím ugyanazon VLAN egy másik biztonságos interfészén is megjelenik.

Az interfész három különböző módon képes fellépni a portbiztonság megsértése ellen. Az ábra bemutatja, hogy milyen módon viselkedik a kapcsolón a három, úgynevezett megsértési mód beállítása esetén:

* **Védelem (Protect)** - Ha a biztonságos MAC-címek elérik a porthoz beállított maximális értéket, a kapcsoló eldobja a más MAC-címekről érkező forgalmat mindaddig, amíg elegendő MAC-cím eltávolításra nem kerül, vagy meg nem növelik az engedélyezett címek számát. Ebben a módban a kapcsoló nem küld értesítést és nem növeli a "szabályszegési" számláló értékét, ha a portbiztonságot megsértik.
* **Korlátozás (Restrict)** - Ha a biztonságos MAC-címek elérik a porthoz beállított maximális értéket, a kapcsoló eldobja a más MAC-címekről érkező forgalmat mindaddig, amíg elegendő MAC-cím eltávolításra nem kerül, vagy meg nem növelik az engedélyezett címek számát. Ebben a módban a kapcsoló értesítést küld és növeli a "szabályszegési" számláló értékét, ha a portbiztonságot megsértik.
* **Letiltás (Shutdown)** - Ebben a módban (alapértelmezett), a portbiztonság megsértése esetén az interfész azonnal "hiba miatt letiltott" (error-disabled) állapotba kerül és kialszik a port LED-jelzőfénye is. A kapcsoló értesítést küld és növeli a "szabályszegési" számláló értékét. Ha egy biztonságos port "hiba miatt letiltott" állapotban van, akkor azt újraengedélyezni a **shutdown** és a **no shutdown** interfész konfigurációs parancsok egymás utáni kiadásával lehet.

A biztonság megsértési módjának beállításához használjuk a **switchport port-security violation** {*protect | restrict |shutdown*} interfész konfigurációs parancsot.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

Az 1. ábra összefoglalja egy Cisco Catalyst kapcsoló alapértelmezett portbiztonsági beállításait.

A 2. ábrán láthatók azok a Cisco IOS CLI-parancsok, amelyek a portbiztonság beállításához szükségesek az S1 kapcsoló Fast Ethernet F0/18 portján. Figyeljük meg, hogy a példa nem határozza meg a megsértési üzemmódot, tehát alapértelmezés szerint az letiltott lesz.

A 3. ábrán látható, hogyan kell a "sticky" MAC-cím védelmet beállítani az S1 kapcsoló Fast Ethernet 0/19 portján. Amint korábban szó volt róla, a védett MAC-címek maximális számát manuálisan is konfigurálhatjuk, ebben a példában a MAC-címek számát 10-re állítjuk a 0/19-es porton. A megsértési mód marad az alapértelmezett, letiltott mód.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

**Portbiztonság ellenőrzése**

A kapcsoló portbiztonsági beállítása után ellenőrizzük, hogy megfelelően lettek-e konfigurálva az egyes opciók és a statikusan beírt MAC-címek is helyesek-e!

**Portbiztonsági beállítások ellenőrzése**

A kapcsoló vagy egy adott interfész portbiztonsági beállításainak megjelenítésére használjuk a **show port-security [interfész** *interfész-azonosító***]** parancsot. Az 1. ábrán egy dinamikus módú portbiztonsági beállítás látható. Alapértelmezés szerint csak egy MAC-cím engedélyezett ezen a porton.

A 2. ábrán egy "sticky" módú portbiztonsági beállítás látható. A maximálisan engedélyezett címek száma 10, ahogy azt az előző példában konfiguráltuk.

**MEGJEGYZÉS**: A MAC-cím "sticky"-ként került beazonosításra.

A "sticky" MAC-címek bekerülnek a címtáblába és az aktív konfigurációba is. Amint a 3. ábrán látható, a PC2 MAC-címe bekerült az S1 aktív konfigurációjába.

**Biztonságos MAC-címek ellenőrzése**

A kapcsoló összes vagy portonként beállított biztonságos MAC-címeinek megjelenítésére használjuk a **show port-security address** parancsot. Amint a 4. ábrán látható, a MAC-címek mellett a típusaik is szerepelnek.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

A portbiztonság megsértése esetén a port "hiba miatt letiltott" (error disabled) állapotba kerülhet. Ilyenkor az interfész ténylegesen lekapcsolódik, vagyis nem küldhet és nem fogadhat adatokat, a konzolon pedig néhány biztonsággal kapcsolatos üzenet jelenik meg (lásd 1. ábra).

**MEGJEGYZÉS**: Ebben az esetben mind a vonali protokoll, mind a fizikai port lekapcsolt (down) állapotba kerül.

A port LED átvált narancssárga színre. A **show interface** parancskimenete alapján a port státusza **"hiba miatt letiltott"** (err-disabled, lásd 2. ábra). A **show port-security interface** parancskimenete szerint pedig a port biztonsági állapota **"biztonsági-letiltott"** (secure-shutdown). Mivel a portbiztonság megsértési módja letiltás, ennak megszegése esetén a port a "hiba miatt letiltott" állapotba kerül.

A rendszergazdának meg kell határozni, hogy mi okozta a biztonság megsértését, mielőtt újra engedélyezetté tenné a portot. A portot addig nem szabad újra engedélyezni, amíg a biztonsági fenyegetés (pl. egy jogosulatlan eszköz csatlakozása) meg nem szűnik. A port újraengedélyezéséhez használjuk a **shutdown** interfész konfigurációs parancsot (lásd 3. ábra). Ennek hatására a port "normál" lekapcsolt (down) állapotba kerül. Ezután alkalmazzuk a **no shutdown** interfész konfigurációs parancsot, hogy a port újra működőképes legyen.

# Kapcsolók védelme - Felügyelet és megvalósítás

## Kapcsoló portbiztonsága

A hálózaton belüli eszközök óráinak egymással és a pontos idővel is szinkronban kell lenniük. Ez lényeges, mivel a hálózati események nyomkövetése, ilyen például a biztonsági beállítások megsértése is, időbélyegzők használatával történik. Továbbá kritikus fontosságú a syslog adatfájlok elemzésében és a digitális tanúsítványok ellenőrzésében.

Az NTP (Network Time Protocol, hálózati idő protokoll) egy olyan szabvány, amely a számítógépes rendszerek óráit a csomagkapcsolt, változó késleltetésű hálózatokon keresztül szinkronizálja. Az NTP lehetővé teszi a hálózati eszközök számára, hogy egy időszerverhez szinkronizálják beállításaikat, így az NTP-kliensek egyetlen megbízható forrásból kapják a szükséges dátum- és időadatokat.

A hálózaton belüli pontos időbeállítás egyik biztonságos módszere, amikor rendszergazda saját időszervert (NTP master) telepít, melyet valamilyen megbízható módon (műhold, rádió stb.) szinkronizál a UTC-időzónához. Ha a rendszergazda nem akar saját NTP-órát (master clock) létrehozni a költségek vagy egyéb okok miatt, akkor további időbeállítási források is rendelkezésére állnak az interneten. Az NTP képes meghatározni a pontos időt belső vagy külső időforrásból is, amelyek lehetnek:

* Helyi központi óra
* Vezéróra az interneten
* GPS vagy atomóra

Egy hálózati eszköz lehet NTP-szerver, NTP-kliens vagy mindkettő. A berendezés szoftveres órájának valamely NTP-szerverhez szinkronizálásához, használjuk az **ntp server** *IP-cím* globális konfigurációs parancsot. Az 1. ábrán látható konfigurációban az R2 NTP-kliensként, míg az R1 forgalomirányító hiteles NTP-szerverként üzemel.

Ha egy eszközt NTP-mesterként állítunk be, akkor lehetővé tesszük más eszközök számára, hogy időbeállításaikat innen szinkronizálják. Ehhez használjuk az **ntp master [***réteg***]** parancsot globális konfigurációs módban. A réteg (stratum) értéke 1 és 15 közötti szám, és azt jelzi, hogy hányadik rétegbeli szinkronizálást igényelhet a rendszer. Ha a rendszer NTP-mesternek van beállítva, és nincs rétegszám megadva, akkor az alapértelmezett érték a 8. Ha az NTP-mester nem ér el kisebb rétegszámú időforrást, akkor azonos értékű NTP-mesterrel is szinkronizálhat, és ezután más eszközök is képesek lesznek tőle időadatokat kérni..

A 2. ábra az NTP-beállítások ellenőrzését mutatja. A kapcsolódások állapotát a **show ntp associations** utasítással lehet megnézni privilegizált EXEC módban. A parancs megmutatja az eszközzel kapcsolatba lépett többi berendezés IP-címét, a statikusan beállított kapcsolatokat és a rétegértéket (stratum number). A **show ntp status** globális paranccsal megjeleníthető az NTP-szinkronizálás állapota, a szinkronforrás, valamint az NTP-rétegérték.

# Összefoglalás

## Összefoglalás

**Kapcsoló trió**

**Esetleírás**

Egy közepes méretű vállalkozásnál érvényben levő központi szabályozás szerint az irodákban található összes kapcsolónak biztonsági beállításokkal kell rendelkeznie. A vállalat hálózati rendszergazdájaként, egy ma reggel kapott feljegyzés alapján, feladatunk a következő:

*Hétfőre, 20xx. április 18-ra az összes konfigurálható kapcsoló első három portját MAC-cím védelemmel kell ellátni. Az alábbi MAC-címek hozzáférését kell biztosítani a portokon: az irodai PC, a laptop és a szerver.*

*A biztonsági beállítások megsértése esetén a port kerüljön letiltásra mindaddig, míg az illetéktelen hozzáférést nem vizsgálják felül!*

*Kérjük, hajtsa végre ezeket a beállításokat legkésőbb a feljegyzésben megadott időpontig! Kérdés esetén hívható szám: 1-800-555-1212. Köszönjük! Hálózatfelügyeleti csoport"*

Dolgozzunk együtt társunkkal és készítsünk egy Packet Tracer topológiát a biztonsági feladat tesztelésére! Miután a hálózat elkészült, teszteljük azt legalább egy eszközzel annak érdekében, hogy a beállítás működőképes és megfelelő.

Mentsük el a feladatot, hogy azt bármikor meg lehessen osztani az osztállyal!

[Csoportos feladat - Switch Trio Instructions](https://contenthub.netacad.com/legacy/RSE/5.02/hu/course/files/2.3.1.1%20Switch%20Trio%20Instructions.pdf)

# Összefoglalás

## Összefoglalás

Egy Cisco kapcsoló elindulásakor a következő rendszerindítási lépéseken megy keresztül:

1. A kapcsoló először betölti a ROM-ból a bekapcsolási önteszt programot (POST, Power-On Self Test). A POST ellenőrzi a CPU alrendszert, azaz megvizsgálja a CPU-t, a DRAM-ot, és a flash memóriában található fájlrendszert.

2. Ezután a kapcsoló betölti a rendszerindító szoftvert (boot loader), mely a ROM-ban tárolt kis program, és a POST sikeres befejeződése után fut le.

3. A boot loader elvégzi a CPU alapszintű inicializálását. Beállítja a CPU-regisztereket, amelyek a fizikai memória használatát, a memória mennyiségét és annak sebességét vezérlik.

4. A boot loader működésre előkészíti az alaplapi flash memória fájlrendszerét.

5. Végül, a boot loader megkeresi és betölti a memóriába az alapértelmezett IOS operációs rendszert, és átadja a kapcsoló vezérlését az IOS-nek.

A BOOT környezeti változóban be lehet állítani, hogy melyik IOS-fájl kerüljön betöltésre. Az operációs rendszer betöltése után a indító konfigurációs állományban található utasítások kerülnek végrehajtásra, melyek inicializálják és beállítják az interfészeket . Ha a Cisco IOS-fájl hiányzik vagy sérült, a boot loader program segítségével lehet másik fájlt betölteni, vagy helyreállítani a problémát.

A kapcsoló aktuális működési állapotát az előlapon található LED-sor mutatja, mely a portok állapotára, duplexitására, és sebességére vonatkozó információkat jelenít meg.

A kapcsoló távoli eléréséhez IP-címet kell beállítani a felügyeleti VLAN-hoz tartozó SVI interfészen. A hozzá tartozó tartozó alapértelmezett átjáró pedig az **ip default-gateway** utasítással konfigurálható. Ha az alapértelmezett átjáró nincs megfelelően beállítva, a távoli felügyelet nem lehetséges. Telnet helyett javasolt a Secure Shell (SSH) alkalmazása, mivel ez biztonságos (titkosított) felügyeleti kapcsolatot biztosít a távoli eszközhöz. Az SSH használatával elkerülhető a jelszavak és felhasználónevek lehallgatása, amelyek Telnet esetén nem titkosított módon továbbítódnak a hálózaton.

A kapcsolók egyik előnye, hogy lehetővé teszik a teljes duplex kommunikációt az eszközök között, gyakorlatilag megduplázva az összeköttetés sebességét. Bár lehetséges az interfészek sebességének és a duplexitásának manuális megadása is, de a hibák elkerülése miatt ezen paraméterek kiválasztását érdemes az automatikus beállításra bízni.

A kapcsoló portbiztonság beállításával megakadályozhatók olyan támadások, mint a MAC-cím elárasztás vagy a DHCP-hamisítás. A kapcsoló portjai konfigurálhatók úgy, hogy csak bizonyos forrás MAC-című kereteket fogadjon. Az ismeretlen címekről érkező keretek, a támadások megakadályozására, letilthatók az interfész blokkolásával.

Nem a portbiztonság az egyetlen lehetőség a hálózat védelmére. Lássuk a 10 leggyakrabban használt módszert:

* Dolgozzunk ki egy írásos biztonságpolitikát a szervezet számára!
* Tiltsuk le a nem használt szolgáltatásokat és portokat!
* Használjunk erős jelszavakat és cseréljük azokat gyakran!
* Szabályozzuk az eszközökhöz történő fizikai hozzáférést!
* Kerüljük a nem biztonságos HTTP-oldalakat, különösen bejelentkezési adatok megadásánál, helyette használjuk a biztonságos HTTPS-t!
* Rendszeresen készítsünk mentéseket, és teszteljük is azokat!
* Világosítsuk fel a dolgozókat a megtévesztési technikákról (social engineering), valamint dolgozzunk ki olyan szabályokat, amelyekkel a felek ellenőrizhetik a másik személyazonosságát telefonon, e-mailen és személyes érintkezés közben!
* Kódoljuk és védjük jelszóval a fontos információkat!
* Használjunk biztonsági hardvereket és szoftvereket, mint például a tűzfalak!
* Frissítsük a szoftvereket állandóan, heti vagy akár napi rendszerességgel a javítócsomagok telepítésével!

Ezek a módszerek csak kiindulópontok a biztonsági felügyelethez. A szervezeteknek állandóan ébernek kell maradniuk a folyamatosan változó fenyegetésekkel szemben.

