

Bevezetés Bevezetés a Cisco IOS-be

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

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

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

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

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

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

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

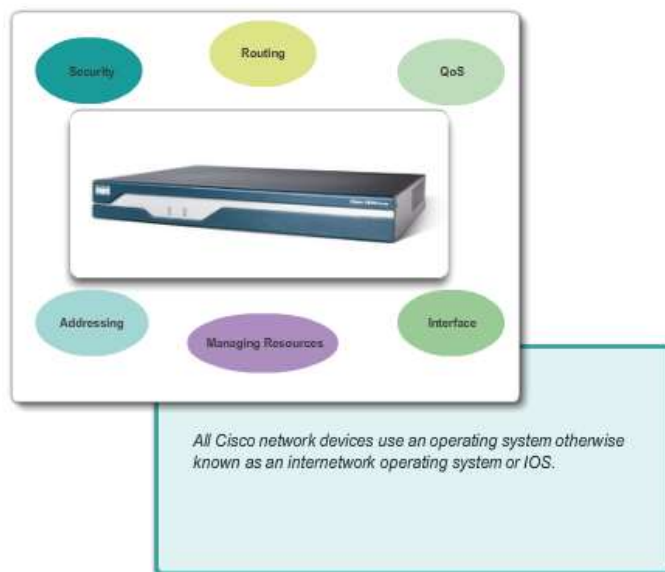
Ebben a fejezetben egy két kapcsolóból és két PC-ből összeállított alap topológia segítségével ismerkedhetünk meg a Cisco IOS működésével.

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

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

- lámpák
- ablaktörlők
- rádió
- mobiltelefon
- klímaberendezés
- gyújtás

Csoportos feladat - 2.0.1.2 Class Activity - It is Just an Operating System Instructions.pdf



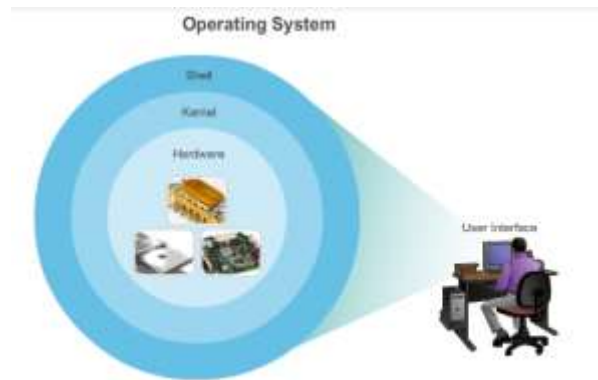
2.1 IOS alapképzés

2.1.1 Cisco IOS

2.1.1.1 Operációs rendszerek

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

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



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

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

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

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

2.1.1.2 Az IOS célja

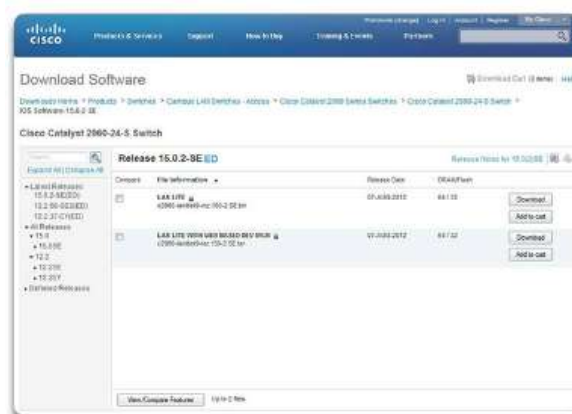
A hálózati operációs rendszerek sok dologban hasonlítanak a PC-s operációs rendszerekhez, melyek olyan funkciók háttérét biztosítják a felhasználó számára, mint:

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

Kapcsolók és forgalomirányítók esetében a funkciók háttérének biztosítása nagyon hasonló. A hálózati szakember számára mindkét eszközön az IOS jelenti a csatlakozási felületet. A szakember parancsok segítségével tudja konfigurálni vagy programozni az eszköz különféle hálózati funkcióit. Az IOS hálózati eszközön való működésének részletei különbözőek, függően a berendezés jellemzőitől és használatának céljától.

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

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



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

2.1.1.3 A Cisco IOS helye

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

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

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



2.1.1.4 Az IOS funkciói

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

- Hálózatbiztonság
- IP-címzés virtuális és fizikai interfészeken
- Interfész specifikus konfigurációs lehetőség az adott közeghez való kapcsolódás optimalizálására

- Forgalomirányítás
- A szolgáltatás minőségének biztosítása (Quality of Service, QoS)
- Hálózatfelügyelet támogatása

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

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



2.1.2 A Cisco IOS elérése

2.1.2.1 Konzol elérési mód

A parancssori környezet többféleképpen is elérhető, a leggyakoribb módok:

- Konzol
- Telnet vagy SSH
- Aux port

Konzol

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



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

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

2.1.2.2 Telnet, SSH és AUX hozzáférési módok

Telnet

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

SSH

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

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

AUX

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

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

Megjegyzés:A Cisco Catalyst kapcsolók nem rendelkeznek AUX porttal.

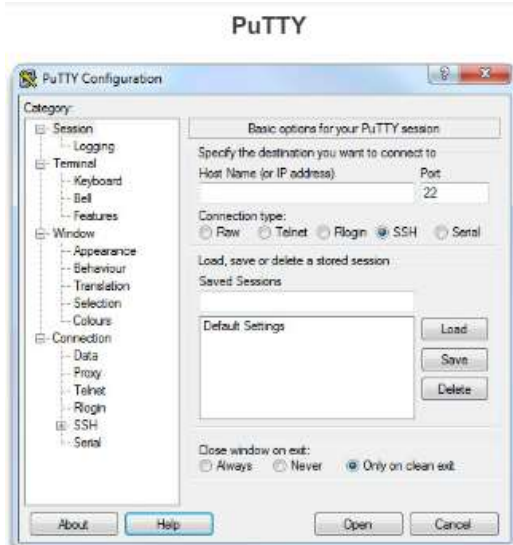
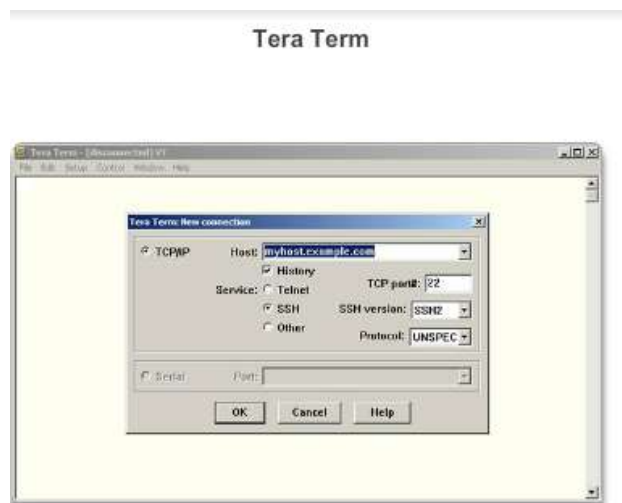


2.1.2.3 Terminál emulációs programok

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

- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- OS X Terminal

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



	Console	Telnet/SSH	AUX
1. You are in the equipment room with a new switch that needs to be configured.	✓		
2. The device you are configuring cannot be accessed by cable, because you are not in the building. You use a telephone to dial into it.			✓
3. Your manager gives you a special cable and tells you to use it to configure the switch.	✓		
4. You access the IOS by using another intermediary device over a network connection.		✓	
5. You are on vacation and need to check on one of your routers. The only access you have is your hotel analog phone.			✓
6. You do not need remote access services to the networking device to configure it because the device is physically accessible to you.	✓		
7. You call your manager to tell him you cannot access your router in another city over the Internet. He provides you with the information to access the switch through a telephone connection.			✓
8. The password for a device was changed. No one knows what the new password is and you need to reset a new password.	✓		

2.1.3 Az IOS használata

2.1.3.1 Cisco IOS működési módok

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

Hierarchikus sorrendjük az egyszerűbbtől a speciálisabb módok felé a következők:

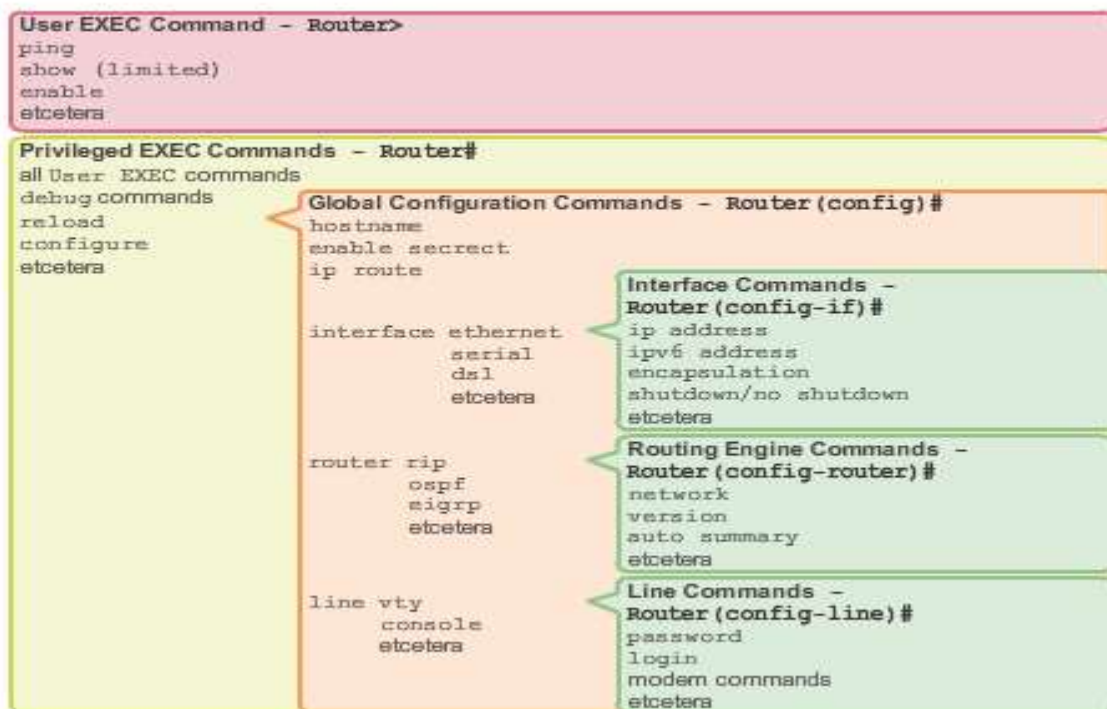
- Felhasználói mód (User EXEC)
- Privilegizált mód (Privileged EXEC)
- Globális konfigurációs mód
- További specifikus konfigurációs módok, például interfész konfigurációs mód

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

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

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

IOS Mode Hierarchical Structure



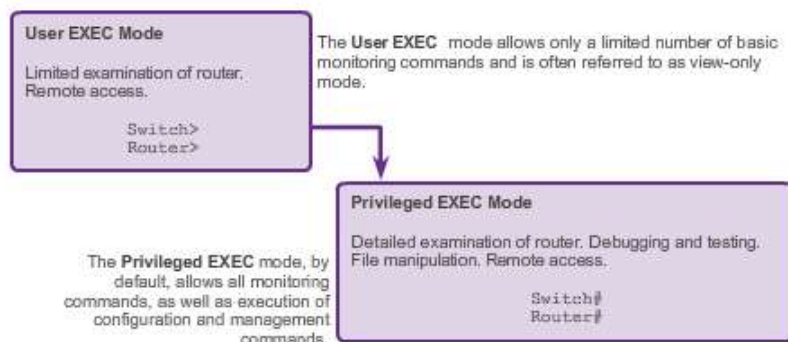
2.1.3.2 Elsődleges módok

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

Felhasználói EXEC mód

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

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



2.1.3.3 Globális konfigurációs mód és almódok

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

Globális konfigurációs mód

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

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

Switch# **configure terminal**

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

Switch(config)#

Specifikus konfigurációs módok

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

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

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

Készenléti jelek (prompt)

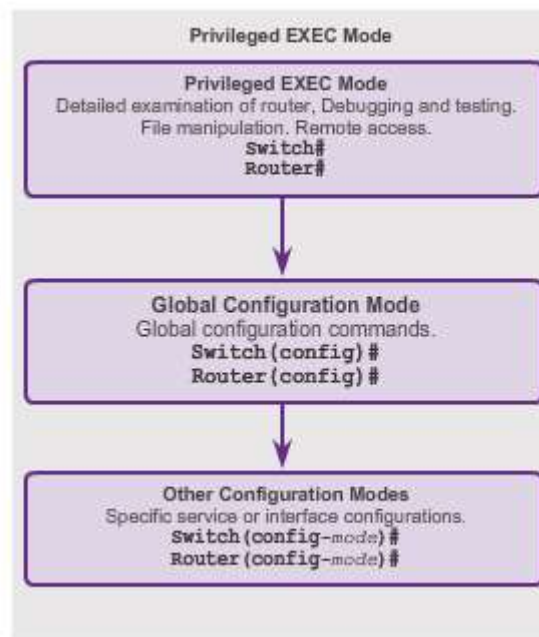
Parancssor használata esetén a készenléti jel egyedi az adott módra nézve. Alapértelmezésben a prompt az eszköz nevével kezdődik és a módra jellemző rövidítéssel folytatódik. Például, egy kapcsoló globális konfigurációs módjának készenléti jele:

Switch(config)#

Amikor az üzemmód megváltozik, a prompt is tükrözi az aktuális környezetet



Within Privileged EXEC mode, network administrators can access the global configuration mode and all other sub-configuration modes.



2.1.3.4 Átjárás az IOS-módok között

Váltás a felhasználói és a privilegizált EXEC módok között

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

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

Az **enable** parancs szintaxisa a következő:

```
Switch> enable
```

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

```
Switch#
```

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

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

Például:

```
Switch> enable
```

Password:

```
Switch#
```

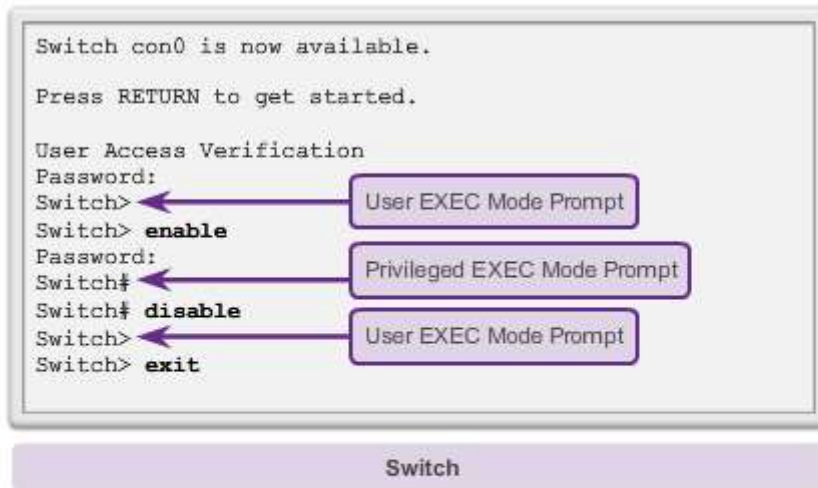
A **disable** utasítás szolgál a felhasználói EXEC módba való visszatérésre.

Például:

```
Switch# disable
```

```
Switch>
```

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



Mozgás a globális konfigurációs mód és alüzemmódjai között

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

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

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

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

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

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```

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

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

2.1.4 A parancsok felépítése

2.1.4.1 Az IOS-parancsok felépítése

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

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

A kulcsszavakon keresztül jutnak el meghatározott paraméterek a parancsértelmezőhöz. Például nézzük meg a **show** parancsot, ami formációkat jelenít meg az eszközről. Ennek a

parancsnak számos kulcsszava van, melyek használatával különféle eredmények jeleníthetők meg. Például:

Switch# **show running-config**

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

IOS-parancs konvenciók

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

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

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

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

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

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

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

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

A **ping** parancs:

Szintaxis:

Switch> **ping** *IP-cím*

Például:

Switch> **ping** **10.10.10.5**

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

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

Szintaxis:

Switch> **traceroute** *IP-cím*

Például:

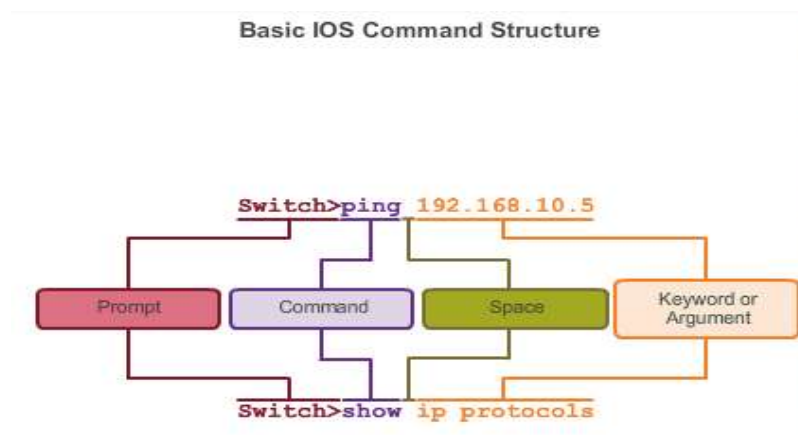
Switch> **traceroute** 192.168.254.254

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

Gyakorlat: 1.8.1 Packet Tracer - Navigating the IOS Instructions.pdf

PKA: 1.8.1 Packet Tracer - Navigating the IOS.pka

Konzolos gyakorlat: 1.8.1 Lab - Establishing a Console Session with Tera Term.pdf



IOS Command Conventions

When describing the use of commands, we generally use these conventions.	
Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets indicate an optional element (keyword or argument).
{x}	Braces indicate a required element (keyword or argument).
[x {y z}]	Braces and vertical lines within square brackets indicate a required choice within an optional element.

2.1.4.2 A Cisco IOS Command Reference

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

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

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

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

1. Keressük fel: www.cisco.com.
2. Kattintsunk: **Support**.
3. Kattintsunk: **Networking Software** (IOS & NX-OS).
4. Kattintsunk: **15.2M&T** (például).
5. Kattintsunk: **Reference Guides**.
6. Kattintsunk: **CommandReferences**.
7. Kattintsunk a kívánt kategóriára, amelybe a keresett parancs tartozik.
8. A bal oldali listában kattintsunk a parancs kezdőbetűjének megfelelő hivatkozásra.
9. Kattintsunk a parancsra.

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

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

2.1.4.3 Környezet érzékeny súgó

Az IOS többféle segítséget is biztosít:

- Környezetérzékeny súgó
- Parancs szintaxis ellenőrzés
- Gyorsbillentyűk és billentyűkombinációk

Környezetérzékeny súgó

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

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

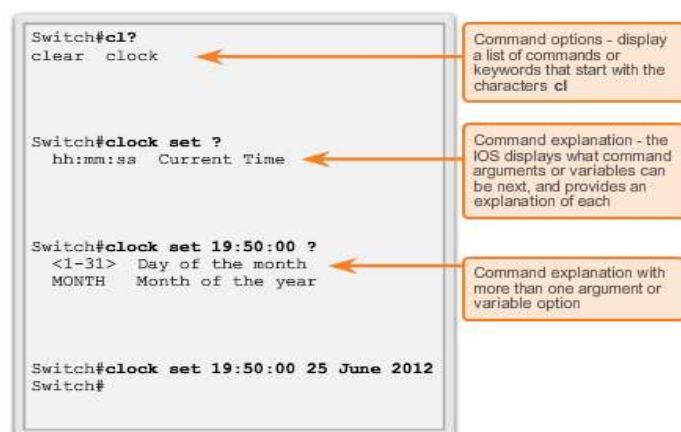
Például a felhasználói EXEC mód parancsainak kilistázásához gépeljük be a kérdőjelet (?) a Switch> prompt után.

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

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

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

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



2.1.4.4 Parancs szintaxis ellenőrzés

Egy parancs Enter billentyűvel történő érvényesítése után a parancsértelmező balról jobbra haladva értelmezi az utasítást, hogy meghatározza a végrehajtandó műveletet. Az IOS rendszerint csak a negatív eredményről küld visszajelzést (lásd 1. ábra). Ha a parancsértelmező

felismeri az utasítást, a kért művelet végrehajtódik és a CLI visszatér az aktuális prompthoz. Ha a parancsértelmező nem ismeri fel az utasítást, visszajelzést küld a hiba okáról.

A 2. ábrán három különféle hibaüzenet látható:

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

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

Command Syntax Check Help		
<pre>Switch#>clock set % Incomplete command. Switch#clock set 19:50:00 % Incomplete command.</pre> <p>The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.</p>	<pre>Switch#c % Ambiguous command: 'c'</pre> <p>The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.</p>	
<pre>Switch#clock set 19:50:00 25 6 % Invalid input detected at '^' marker.</pre> <p>The IOS returns a '^' to indicate where the command interpreter can not decipher the command.</p>		
Error Message	Meaning	Examples
% Ambiguous command: 'command'	Not enough characters were entered for the IOS to recognize the command.	Switch# % Ambiguous comma
% Incomplete command.	Not all of the required keywords or arguments were entered.	Switch#clock set % Incomplete comman
% Invalid input detected at '^' marker	The command was entered incorrectly. The error occurred where the caret mark (^) appears.	Switch#clock set 19:50 % Invalid input detect marker.

2.1.4.5 Gyorsbillentyűk és billentyűkombinációk

Gyorsbillentyűk és billentyűkombinációk

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

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

- **Lefelé nyíl** - Visszagörgeti a korábbi parancsokat
- **Felfelé nyíl** - Előregörgeti a korábbi parancsokat
- **Tab** - Kiegészíti a részlegesen begépelt parancsokat
- **Ctrl+A** - Ugrás a parancssor elejére
- **Ctrl+E** - Ugrás a parancssor végére
- **Ctrl+R** - Újra megjelenít egy sort
- **Ctrl+Z** - Kilép a konfigurációs módból és visszatér felhasználói EXEC módba
- **Ctrl+C** - Kilép a konfigurációs módból vagy elveti az aktuális parancsot
- **Ctrl+Shift+6** - Megszakít egy IOS-folyamatot, mint például egy ping vagy traceroute futását

Néhány ezek közül részletesebben:

Tab

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

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

Ctrl+R

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

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

Switch# **show mac-**

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

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

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

Switch# **show mac**

Ctrl+Z

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

Felfelé és lefelé nyilak

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

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

Ctrl+Shift+6

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

Ctrl+C

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

Rövidített parancsok és kulcsszavak

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

A kulcsszavak is rövidíthetők.

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

Switch# **show interfaces**

Switch# **show int**

Rövidíthetjük egyszerre a parancsot és a kulcsszót is, például:

Switch# **sh int**

2.1.4.6 Az IOS állapotvizsgáló parancsai

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

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

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

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

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

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

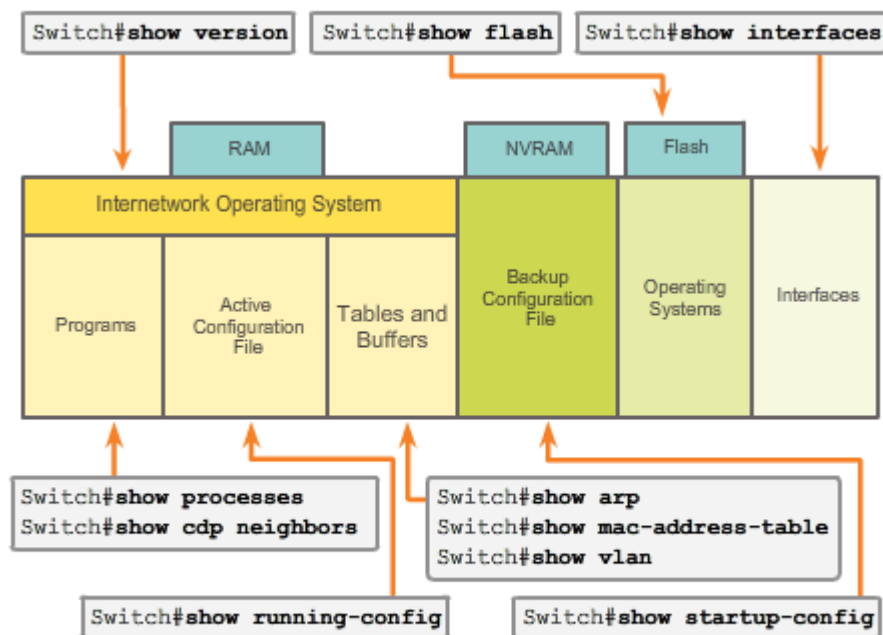
További **show** parancsok, amelyeket a hálózati szakemberek gyakran használnak :

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

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

A More prompt

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



IOS **show** commands can provide information about the configuration, operation, and status of parts of a Cisco switch or router

2.1.4.7 A show version parancs

A kapcsolókon és forgalomirányítókön használt egyik leggyakoribb parancs:

Switch# **show version**

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

- **Szoftver verzió** - Az IOS verziója (a flash memóriában tárolt)
- **Bootstrap verzió** - A rendszerbetöltő program verziója (a ROM-ban tárolt)
- **Rendszer felkapcsolási idő** - Az utolsó újraindítás óta eltelt idő
- **Rendszer újraindulási információ** - Az újraindulás módja (pl.: áramkimaradás, összeomlás)
- **A rendszer kép fájl neve** - A flash memóriában tárolt IOS-fájl neve
- **Az eszköz és a processzor típusa** - Modell szám és processzor típus
- **Memória típus és foglalás (fő/osztott)** - A fő és az I/O puffer memória mérete
- **Szoftver tulajdonságok** - A támogatott protokollok és jellemzők

- **Hardver interfészek** - Az eszköz rendelkezésre álló interfészei
- **Konfigurációs regiszter** - Indítási előírások, konzolsebesség és kapcsolati paraméterek összessége

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

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

cisco1941 uptime is 41 minutes
System returned to ROM by power-on
System image file is ""flash0:c1900-universalk9-mz.SPA.152-
4.M1.bin""
Last reload type: Normal Reload
Last reload reason: power-on

This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

Router# show version

```
Switch# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3,
RELEASE SOFTWARE (fc1)

Switch uptime is 44 minutes
System returned to ROM by power-on
System image file is ""flash:/c2960-lanbasek9-mz.150-2.SE.bin""

This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product
```

Switch# show version

2.1.4.8 Packet Tracer - Az IOS használata

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

Packet Tracer – 2.1.4.8 Packet Tracer - Navigating the IOS Instructions.pdf

Packet Tracer - 2.1.4.8 Packet Tracer - Navigating the IOS.PKA

2.1.4.9 Laborgyakorlat - Konzol kapcsolat létesítése Tera Term használatával

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

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

Gyakorlat: 2.1.4.9 Lab - Establishing a Console Session with Tera Term.pdf

2.2 Alapok

2.2.1 Állomásnevek

2.2.1.1 Miért a kapcsoló?

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

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

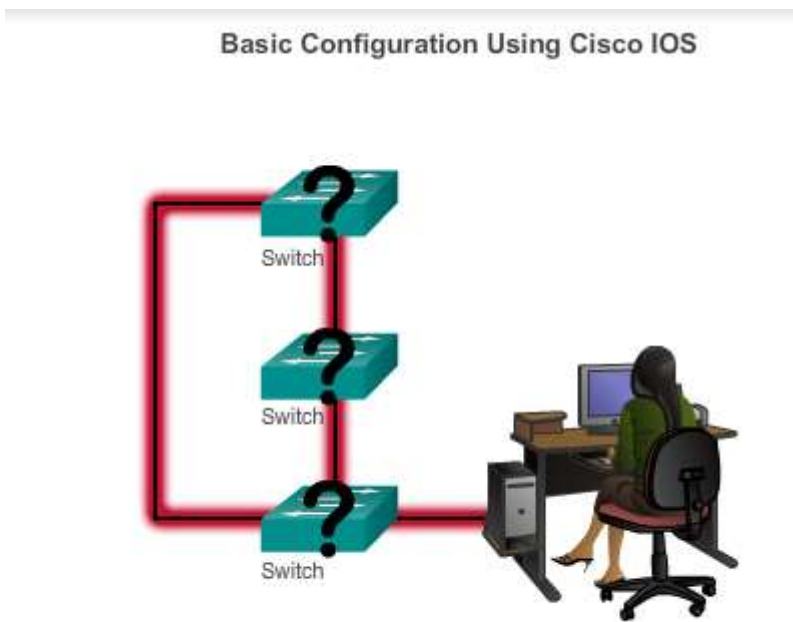
Cisco IOS 2960 Switch



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

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

2.2.1.2 Eszköznevek



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

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

Without names, network devices are difficult to identify for configuration purposes.

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

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

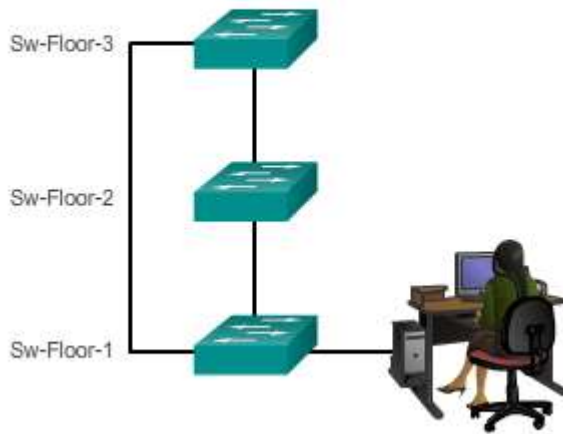
A névadásra vonatkozó szabályok alapján egy név:

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

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

2.2.1.3 Állomásnevek

Configuring Device Names



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

Példák nevek alkalmazására

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

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

Például az ábrán a három kapcsoló

neve rendre Sw-Floor-1, Sw-Floor-2, és Sw-Floor-3.

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

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

2.2.1.4 Állomásnevek konfigurálása

IOS állomásnév beállítása

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

Switch# **configure terminal**

Ezután a prompt megváltozik:

Switch(config)#

Ezt követően állítsuk be az állomásnevet:

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

Ezután az új prompt:

Configure a Hostname

```
Configure the switch hostname to be 'Sw-Floor-1'.
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
You successfully configured the switch hostname.
```

Sw-Floor-1 (config)#

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

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

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

Például egy eszköz nevének eltávolítása:

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

Switch(config)#

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

2.2.2 Az eszközkonfigurációhoz való hozzáférés korlátozása

2.2.2.1 A hozzáférés biztonságossá tétele

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

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

A következő jelszavak kerülnek bemutatásra:

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

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

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

Jelszó választásakor ügyeljünk a következőkre:

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

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

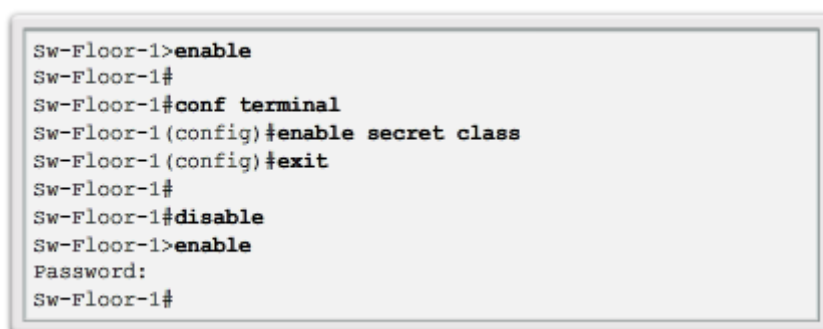
2.2.2.2 A privilegizált EXEC mód védelme

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

Példa a jelszó beállítására:

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

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



```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

2.2.2.3 A felhasználói EXEC mód védelme

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

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

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

```
Switch(config-line)# password cisco
```

```
Switch(config-line)# login
```

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

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

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

VTY-jelszó

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

Használjuk a következő parancsokat a vty-vonalak jelszavának beállításához:

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

```
Switch(config-line)# password cisco
```

```
Switch(config-line)# login
```

Alapértelmezésben az IOS tartalmazza a **login** parancsot a VTY-vonalakon. Ez

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

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```


2.2.2.4 Jelszó titkosítás

Létezik egy hasznos utasítás, amely megakadályozza a jelszavak egyszerű szöveggént való megjelenítését a konfigurációban. Használatához gépeljük be a **service password-encryption** parancsot.

Hatására a konfigurált jelszavak titkosítva lesznek. A **service password-encryption** parancs gyenge titkosítással kódolja a jelszavakat. Ez a titkosítás csak a konfigurációs állományban lévő jelszavakra vonatkozik, a hálózaton keresztül küldöttekre nem. Az utasítás célja a konfigurációs fájl jelszavainak védelme a jogosulatlan személyek általi megtekintéstől.

Ha lefuttatjuk a **show running-config** vagy a **show startup-config** parancsot a **service password-encryption** parancs futtatása nélkül, a titkosítatlan jelszavak láthatók lesznek a kimenetben. A **service password-encryption** parancs kiadásával azonban a jelszavak titkosíthatók. Ezt követően a titkosítási szolgáltatás leállítása már nem befolyásolja a titkosított jelszavak meglétét, azok nem kerülnek visszaállításra.



2.2.2.5 Banner üzenetek

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

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

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

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

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

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

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

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

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

A MOTD szintaxisa globális konfigurációs módban a következő:

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

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

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



2.2.3 Konfiguráció mentése

2.2.3.1 Konfigurációs fájlok

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

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

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

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

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

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

Switch# **copy running-config startup-config**

Végrehajtás után az aktív konfiguráció frissíti az indító konfigurációt.

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

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

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

Például:

Switch# **reload**

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

Proceed with reload? [confirm]

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

Reload Command.

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

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

Copyright (c) 2004 by cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 processor with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled

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

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

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

Switch# **erase startup-config**

Az utasítás kiadása után a kapcsoló megerősítést kér:

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

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

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

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

Switch# **delete vlan.dat**

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# **erase startup-config**

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

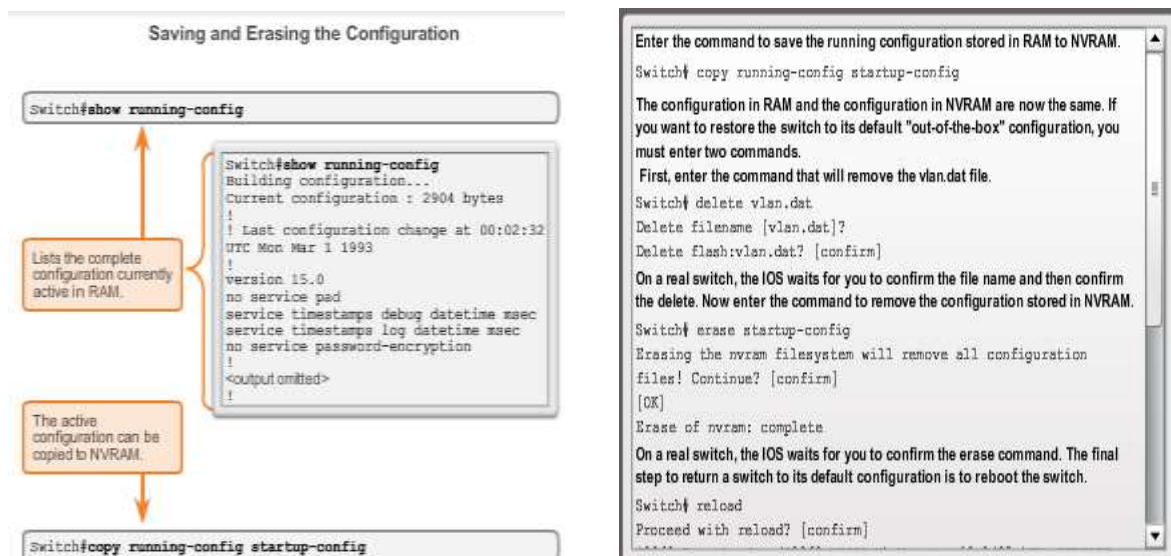
[OK]

Erase of nvram: complete

Switch#

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

Az ábrán látható az aktív konfiguráció mentését a RAM-ból az NVRAM-ba.



2.2.3.2 Szövegek rögzítése

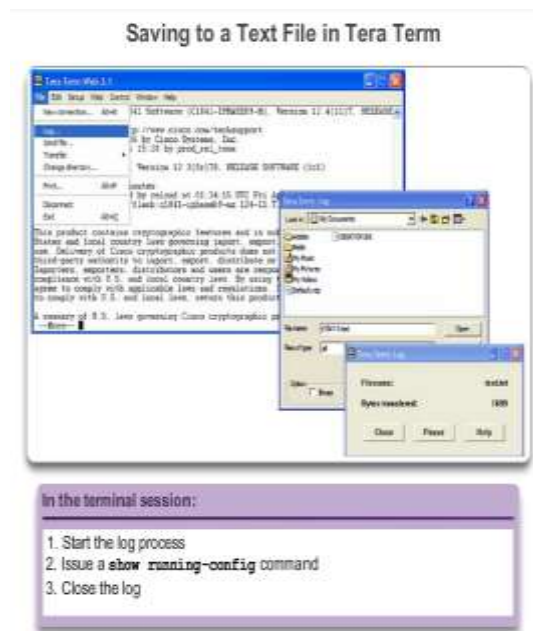
Biztonsági másolat készítése szöveg rögzítésével

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

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

A lépések a következők:

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



A szöveges konfiguráció vissztöltése

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

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

Tera Term esetén a lépések:

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

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

2.2.4 Packet Tracer - Kapcsoló kezdeti konfigurálása

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

Packet Tracer - 2.2.3.3 Packet Tracer - Configuring Initial Switch Settings Instructions.pdf

Packet Tracer - 2.2.3.3 Packet Tracer - Configuring Initial Switch Settings.PKA

2.3 Címzési sémák

2.3.1 Portok és címek

2.3.1.1 Eszközök IP-címzése

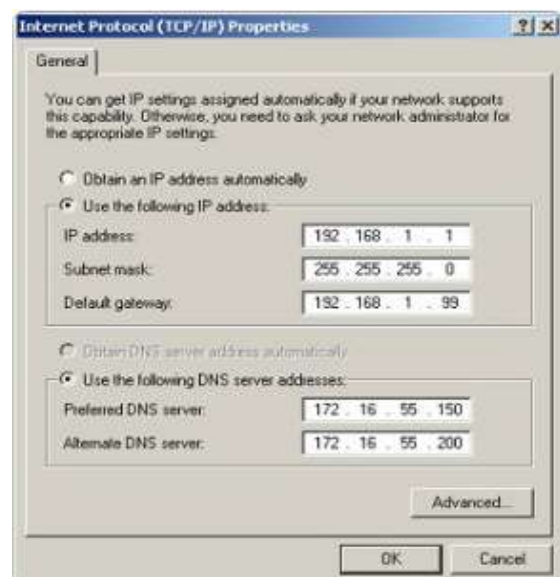
Az IP-címzés, legyen az IPv4 vagy IPv6, elsődleges jelentőségű az interneten lévő eszközök számára egymás azonosításához és a végponttól végpontig terjedő kommunikáció biztosításához. Tény tehát, hogy bármely hálózatról is van szó, az IP-címek nélkülözhetetlenek a berendezések számára a forrástól a célig és vissza irányuló kommunikációhoz.

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

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

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

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

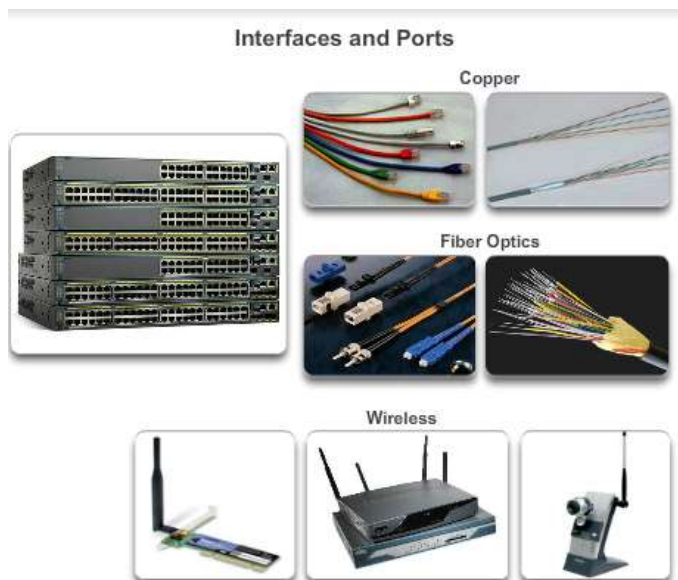


IP-cím rendelhető a készülékek fizikai portjaihoz és virtuális interfészeihez is. A virtuális interfész azt jelenti, hogy nincs fizikai hardver elem hozzárendelve az eszközben.

2.3.1.2 Interfészek és portok

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

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



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

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

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

2.3.2 Eszközök címezése

2.3.2.1 Kapcsoló virtuális interfészének (SVI) konfigurálása

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

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

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

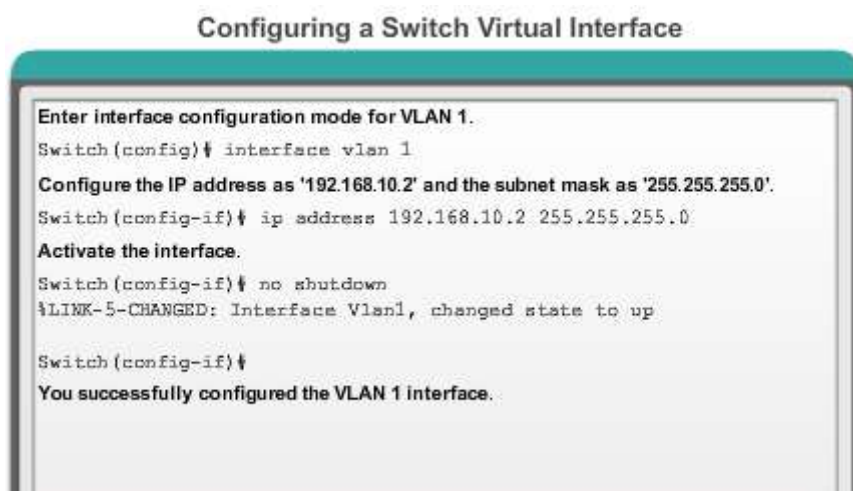
Rövidesen megtanuljuk az IP-címezés részleteit is, de most a legfontosabb a kapcsoló távoli elérésének gyors konfigurálása. Az ábrán az S1 kapcsoló IP-címének (192.168.10.2) beállítása és engedélyezése látható:

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

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

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

Az ábrán lévő parancs szimulátorban gyakorolhatjuk az SVI konfigurálását.



```
Configuring a Switch Virtual Interface

Enter interface configuration mode for VLAN 1.
Switch(config)# interface vlan 1
Configure the IP address as '192.168.10.2' and the subnet mask as '255.255.255.0'.
Switch(config-if)# ip address 192.168.10.2 255.255.255.0
Activate the interface.
Switch(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Switch(config-if)#
You successfully configured the VLAN 1 interface.
```

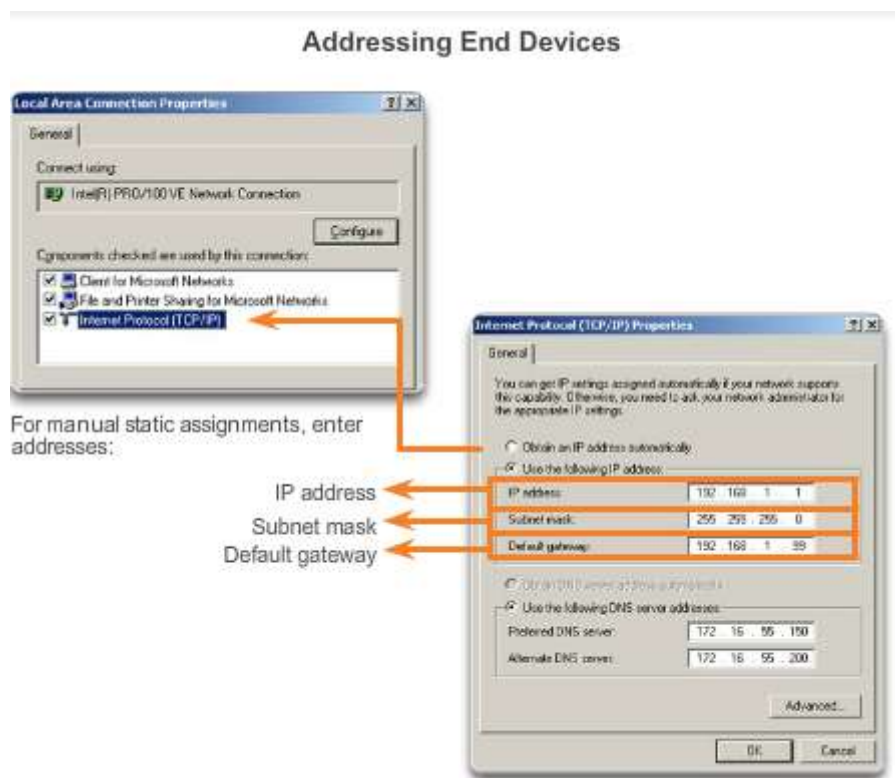
2.3.2.2 Manuális IP-cím konfiguráció végberendezéseken

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

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

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

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



2.3.2.3 Automatikus IP-cím konfiguráció végberendezéseken

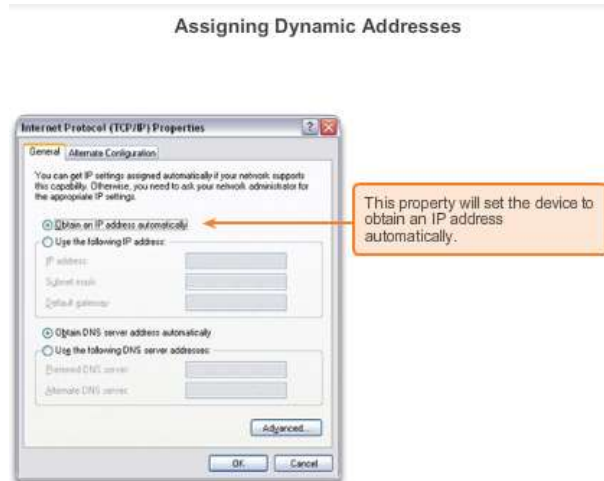
Egy állomás IP-cím információi megadhatók kézzel, vagy DHCP (Dynamic Host Configuration Protocol) használatával, mely automatikusan biztosítja azokat.

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

A DHCP automatikus IP-cím hozzárendelést biztosít minden hálózati végberendezés számára, melyen a DHCP engedélyezve van. Gondoljuk végig, hogy mennyi időt emésztene fel, ha minden hálózatra való csatlakozás alkalmával manuálisan kellene megadni az IP-címet, a maszkot, az alapértelmezett átjárót és a DNS-szervert. Szorozzuk meg ezt az összes felhasználó és az általuk használt hálózati eszközök számával, így láthatjuk a probléma méretét.

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

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



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

Az ábrán lévő parancs szimulátorban gyakorolhatjuk a Windows PC IP-cím beállításának megjelenítését.



2.3.2.4 IP-cím ütközések

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

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

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

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

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



2.3.2.5 Packet Tracer - Alapkonfiguráció megvalósítása

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

Packet Tracer - 2.3.2.5 Packet Tracer - Implementing Basic Connectivity Instructions.pdf

Packet Tracer - 2.3.2.5 Packet Tracer - Implementing Basic Connectivity.pka

2.3.3 Kapcsolatok ellenőrzése

2.3.3.1 A visszacsatolási cím tesztelése végberendezéseken

A visszacsatolás (loopback) tesztelése

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

Az állomás parancssorába begépelésre kerülő ping parancs szintaxisa:

C:\> ping 127.0.0.1

Az utasítás válasza egy ehhez hasonló üzenet:

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

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

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

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

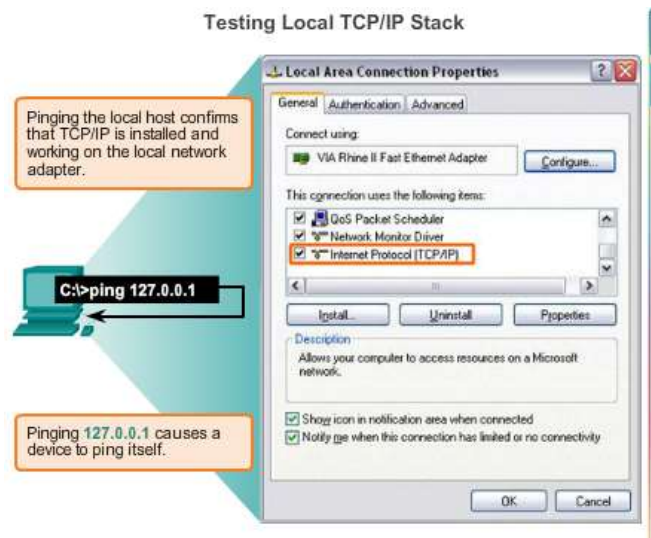
Ping statistics for 127.0.0.1:

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

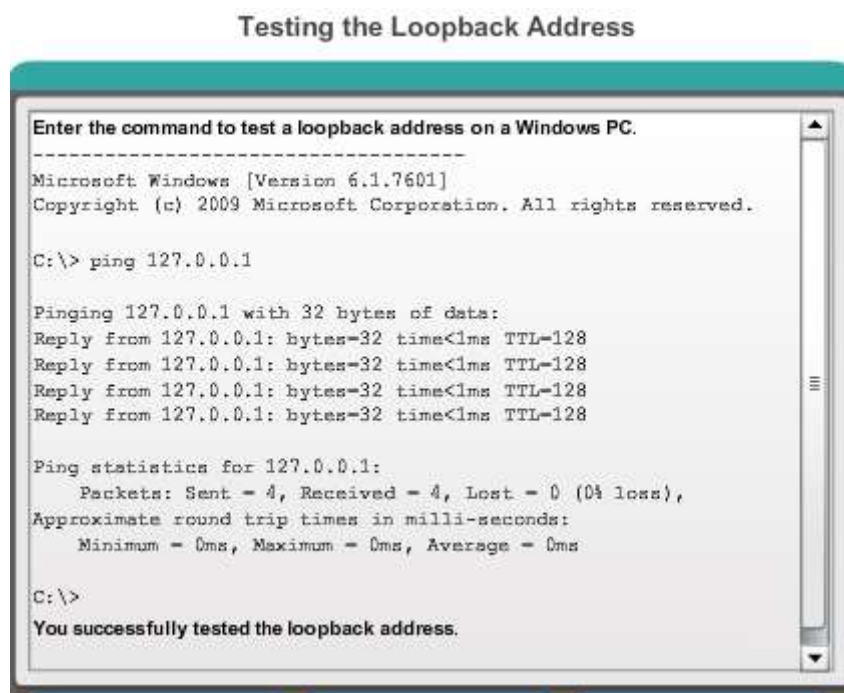
Approximate round trip times in milli-seconds:

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

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



A *cmd* ablak gyakorolhatjuk a loopback cím tesztelését.

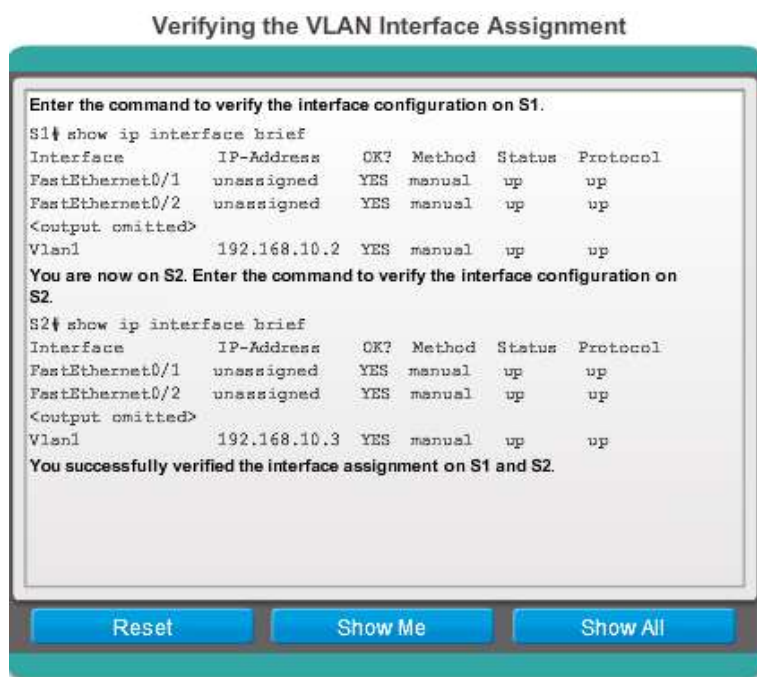


2.3.3.2 Az interfész tesztelése

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

A kapcsoló interfészeinek ellenőrzése

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



2.3.3.3 A végponttól végpontig tartó kapcsolat tesztelése

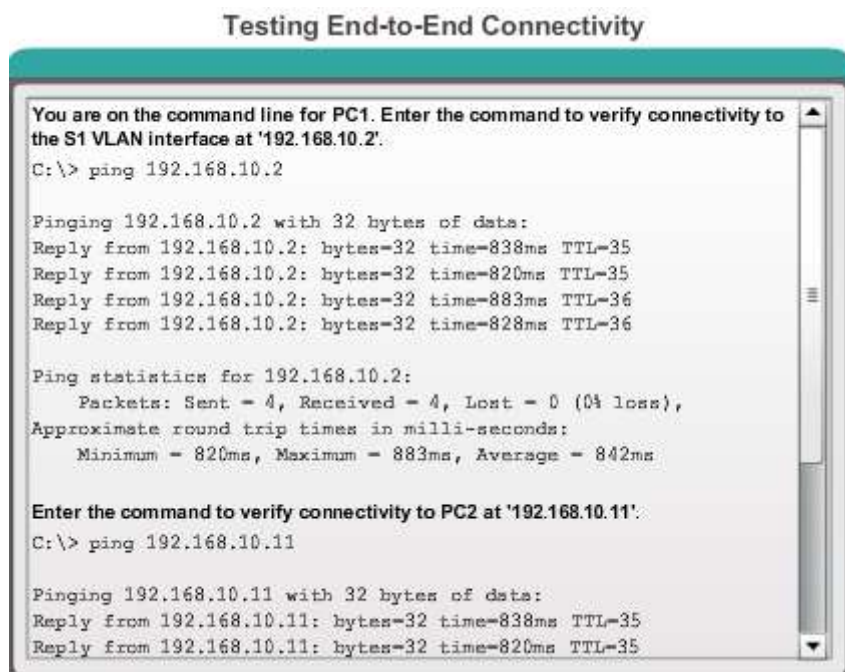
A **ping** parancs egyaránt használható PC-n és Cisco IOS eszközökön. Az ábrán ellenőrizhető, hogy az S1 kapcsoló VLAN 1 interfészének 192.168.10.2 IP-címe sikeresen pingelhető a PC1-ről.

A végponttól végpontig tartó kapcsolat tesztelése

A PC1 IP-címe 192.168.10.10, alhálózati maszkja 255.255.255.0 és alapértelmezett átjárója 192.168.10.1.

A PC2 IP-címe 192.168.10.11, alhálózati maszkja 255.255.255.0 és alapértelmezett átjárója 192.168.10.1.

A PC2 sikeres pingelése a PC1-ről ellenőrzi a két eszköz közötti végponttól végpontig tartó kapcsolatot.



```
Testing End-to-End Connectivity

You are on the command line for PC1. Enter the command to verify connectivity to
the S1 VLAN interface at '192.168.10.2'.
C:\> ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 820ms, Maximum = 883ms, Average = 842ms

Enter the command to verify connectivity to PC2 at '192.168.10.11'.
C:\> ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
```

2.3.3.4 Laborgyakorlat - Egyszerű hálózat építése

Ebben a laborgyakorlatban a következő feladatokat végezzük el:

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

Laborgyakorlat - 2.3.3.4 Lab - Building a Simple Network

2.3.3.5 Ebben a laborgyakorlatban a következő feladatokat végezzük el:

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

Laborgyakorlat - 2.3.3.5 Lab - Configuring a Switch Management Address

2.4 Összefoglalás

2.4.1 Csoportos feladat - Taníts meg!

Taníts meg!

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

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

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

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

Összpontosítsunk a következőkre:

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

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

Csoportos feladat - 2.4.1.1 Class Activity - Tutor me! Instructions.pdf

2.4.1.1 Packet Tracer - Skills Integration Challenge

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

Packet Tracer - 2.4.1.1 Class Activity - Tutor me! Instructions.pdf

Packet Tracer - 2.4.1.2 Packet Tracer - Skills Integration Challenge.PKA