***2.SZEMESZTER 5. MODUL***

**copy running-config startup-config;** vagy **copy run start**

**vagy**

**write   
wr**

az aktuális konfiguráció az indító konfigurációs fájlba menthető

**>show version**

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

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

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

**0x2120 -** A forgalomirányító ROMmon módban indul

**show startup-config** parancs segítségével nézzük meg, az indítási konfigurációt tartalmazó fájlt

Hostnév> - felhasználói exec

Hostnév> **enable** -> Hostnév# - privilegizált exec

Hostnév# **configure terminal** , vagy **conf t** -> Hostnév(config)# – globális konfigurációs mód

interface [típus] [szám] -> Hostnév(config-if)# - interf. konf. mód

**line console 0** – vonalbemenet

pl.:

Route(config)# line console 0

Router(config)# password <password>

Router(config)# login

Router(config)# end

**line vty** – teminálkapcsolat

pl.:

Route(config)# line vty 0 4

Router(config)# password <password>

Router(config)# login

Router(config)# end

**terminal history size** és a **history size -** A terminálkapcsolat eltárolt parancssorai számának megváltoztatásához

**>show history** – parancselőzmények kilistázása

**show running-config –** aktuális, futó konfig megtekintése

**>show interfaces –** interfészek beállításának megtekintése

**>show arp –** arp tábla megtekintése

**>show ip route –** forgalomirányítási tábla megtekintése

**>show protocols –** beállított protokollok megtekintése, melyik port milyen állapotban van

**>show users** – bejelentkezett felhasználók megtekintése, ki melyik Console porton

**>show flash** – Flash memória tartalmának kiíratása

Router(config)# **hostname** <név> - Eszköznek való névadás

Router(config)# **enable** **password** <password> Jelszó létrehozása

Router(config)# **enable** **secret** <password> Titkos jelszó létrehozása, felülírja az előzőt!

R1(config)#security passwords min-length 10 – a jelszó hosszúság minimum 10 karakternek kell lenni!

Router(config)# login block-for 100 attempts 2 within 100

A bejelentkezési üzenetek beállításához a:

**(config)#banner motd –** A nap üzenete PL.: #banner motd#

**(config)#banner login -**  Bejelentkező üszenet

**(config)#logging synchronous –** egyidejű naplózás kéretlen üzeneteinek elválasztása

pl.: R1(config)#line console 0

R1(config-line)#logging synchronous

**(config)#no ip domain-lookup** – DNS szerver keresésének tiltása

**(config)#service password-encryption**

forgalomirányítón tárolt összes jelszó titkosítására

**(config)#interface fa 0/0**

**(config-if)#description** – leírása az adott kapcsolatról (komment)

**(config-if)#ip address [cím][maszk]–** ip cím megadása

**(config-if)#ipv6 address /előtaghossz – ipv6-os címeknél**

**(config-if)#no shutdown** – adott port felkapcsolása

**Csak serialnal:**

**(config-if)#clock rate [szám]–** órajel megadása DCE eszközön!

Alapéertelmezett útvonal megadása:

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

**Router1(config)#ip route 192.168.16.0 255.255.255.0 192.168.15.1**

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

**Router1(config)#ip route 192.168.16.0 255.255.255.0 S0/0/0**

Sw-Floor-1# **configure terminal**

Sw-Floor-1(config)# **interface vlan 1**

Sw-Floor-1(config-if)# **ip address 192.168.1.20 255.255.255.0**

Sw-Floor-1(config-if)# **no shutdown**

Sw-Floor-1(config-if)# **exit**

Sw-Floor-1(config)# **ip default-gateway 192.168.1.1**

**DHCP konfigurálás:**

1.Címkészlet létrehozás

**>enable**

**#conf t**

**(config)#ip dhcp excluded-address 172.16.1.100 172.16.1.103**

ip címek kizárása!

**(config)# ip dhcp pool LAN-cimek <- a pool neve**

2.Hálózat / Alhálózat létrehozás

**(dhcp-config)# network [IP-cím] [maszk] pl.: network 172.16.0.0 255.255.0.0**

3.Bizonyos IP címek kizárása (itt: 100;101;102;103 nem kerül kiosztásra)

4.tartománynév megadása (ELHAGYHATÓ paraméter!) nem szükséges a dhcp működéséhez!

**(dhcp-config)# domain – name cisco.com**

5. DNS- kiszolgáló IP-címe

**(dhcp-config)# dns-server 172.16.1.103 172.16.2.103 [elsődleges] [másodlagos]**

6. Alapértelmezett átjáró megadása:

**(dhcp-config)# default-router 172.168.1.100**

7. Bérleti időtartam beállítása

**(dhcp-config)# lease {nap[óra ][perc]|infinite} (vagy ez|vagy az)!!!**

DHCP konfig befejezése, visszatérés globális konf. módba

**(dhcp-config)#end**

IPv6 interface konfig:

**(config –if)#** ipv6 address IPV6os cmí/prefix

ha kell link local is:

**(config –if)#** ipv6 address IPV6os cmí/prefix link-local

IPv6 SLAAC

a megfelelő interfacen:

**(config –if)#** ipv6 enable

globális konfigban:

**(config )#** ipv6 unicast-routing

NAT-olás beállítása:

1.Belső interface megadása:

**>endable**

**#conf t**

**(config)# interface fastethernet 0/0**

2.A belső inteface elsődleges IP-címének megadása

**(config –if)# ip address 172.31.232.182 255.255.255.0**

3. Belső interface azonosítása

**(config –if)#ip nat inside**

**(config –if)# no shutdown**

**(config –if)# exit**

4.Külső interface megdása

**(config)# interface serial 0/0**

**5. A külső inteface elsődleges IP-címének megadása**

**(config –if)# ip address 209.165.201.1 255.255.255.252**

6. Külső interface azonosítása

**(config –if)#ip nat outside**

**(config –if)# no shutdown**

**(config –if)# exit**

7. Statikus címfordítása megadása

3. Belső interface azonosítása

**(config)#ip nat inside source static172.31.232.14 209.165.202.130**

A 232.14 kiszolgáló belső címe mindig a …. 202.130 címre fordul!

**show ip nat translations** - A parancs megjelenít minden beállított statikus és a forgalom által generált dinamikus fordítást.

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

**clear ip nat translation \*** - dinamikus címfordítások törlése

**copy startup-config tftp** – indító konfig TFTP-re másolása

**copy running-config tftp** – aktuális konfig TFTP-re másolása

**copy tftp running-config** – visszaállítás TFTP-ről; !!utána copy run start!!

Kapcsolóknál:

IP cím megadása:

**(config)# interface vlan 1**

**(config-if)# ip address Ip cím maszk**

Alapértelmezett átjáró

**(config)# ip default-gateway IP-cím**

Portbiztonság:

Statikus:

**(config)# interface Fa0/18**

**(config-if)# switchport mode access**

**(config-if)# switchport port-security mac-address <mac-cím>**

**(config-if)#end**

Dinamikus: alapértelmezetten portonként max: 1 (változtatható)

**(config)# interface Fa0/18**

**(config-if)# switchport mode access**

**(config-if)# switchport port-security**

**(config-if)#end**

Sticky

**(config)# interface Fa0/18**

**(config-if)# switchport mode access**

**(config-if)# switchport port-security**

**(config-if)# switchport port-security maximum SZÁM**

**(config-if)# switchport port-security mac-address sticky**

**(config-if)# switchport port-security violation** {*protect | restrict |shutdown*}

**(config-if)#end**

**show port-security interface SZÁM** - Egy bizonyos interfész portbiztonsági beállításainak ellenőrzéséhez használjuk

**show port security address –** Biztonságos MAC címek ellenőrzése

**clear port-security sticky interface <port száma> access** - segítségével töröljük ki a megtanult címeket

**no switchport port-security –** portbiztonság letiltása

**show cdp neighbors** és a **show** **cdp neighbors detail** parancsok kimenete megjeleníti az adott Cisco eszköz által a közvetlenül csatlakozó szomszédjairól szerzett információkat.

CDP globális letiltása / engedélyezése:

**(config)# no** **cdp** **run** – letiltás

**(config)# cdp run** – engedélyezés

CDP adott porton való letiltása / engedélyeése:

**(config-if)# cdp enable -** engedélyezés

**(config-if)# no cdp enable –** letiltás

rommon**> boot flash:** IOSnév

LABGYAK:

**reload** – újraindítás

**Router#erase startup-config –** indító konfig file törlése!

VLAN adatbázis információs fájlt eltávolítása:

**Switch#delete flash:vlan.dat**

Delete filename [vlan.dat]?[Enter]

Delete flash:vlan.dat? [confirm][Enter]

**show mac-address-table -**  a kapcsoló által megtanult fizikai címek megjelenítése!

**CustomerSwitch(config)#mac-fastethernet 0/18 vlan 1 -**  statikus MAC cím beállítás!

Törölje a sticky address bejegyzést az Fa0/18 porton, a *clear port-security* parancs

alkalmazásával!

**S1#clear port-security sticky interface fa0/18 access**

Az intefészt az error disable állapotból, administratively up állapotba kell hozni. Ezért adja ki a no shutdown parancsot a shutdown parancs után.

**S1(config)#interface fa0/18**

**S1(config-if)#shutdown**

**S1(config-if)#no shutdown**

**ping 192.168.1.5 –n 100** - 4 helyett 100 ping!

kapcsolat sebességének és duplexitásának beállítása:

**CustomerSwitch(config-if)#interface fastEthernet 0/10**

**CustomerSwitch(config-if)#speed 10**

**CustomerSwitch(config-if)#duplex half**

**CustomerSwitch(config-if)#end**

**show cdp interface** - A kimenet megmutatja a forgalomirányítón lévő összes interfész időzítési információit

***2.SZEMESZTER 6. MODUL***

A RIPv2 konfiguráció három megjegyzendő utasítása:

**Router(config)#router rip**

**Router(config-router)#version 2**

**Router(config-router)#network [hálózatazonosító]** <-közvetlenül csatlakozó hálózatok!!!

**show ip protocols -** ellenőrizhető, hogy a RIP konfigurálva van, a megfelelő interfészek küldenek és fogadnak frissítéseket, és a forgalomirányító a megfelelő hálózatokat hirdeti

**show ip route -**  megjeleníti az irányítótáblát, és így ellenőrizhető, hogy a RIP szomszédoktól kapott útvonalak bekerültek a forgalomirányító táblába.

**debug ip rip** utasítás használható a küldött és fogadott frissítésekben hirdetett hálózatok megfigyelésére. A debug parancsok mindig valós időben jelenítik meg a forgalomirányító működését

A BGP engedélyezése:

**(config)# router bgp [AS\_szám]**

**(config-router)# neighbor [IP-cím] remote\_as [AS\_szám]**

**(config-router)# network [hálózati\_cím]**

**(config-router)# end**

**GYAKORLAT**

ISP1(config)#interface loopback0 – visszacsatolási cím beállítása!

ISP1#**show ip bgp –** BGP információk megjelenítése!

***2.SZEMESZTER 8. MODUL***

A Cisco IOS kód biztonsági mentése

**copy flash tftp**

A ROMmon környezeti változóinak beállításához be kell gépelni a változó nevét, majd az egyenlőség (=) jelet, és végül a változó értékét.

**RomMon:**

**IP\_ADDRESS** - a LAN interfész IP-címe

**IP\_SUBNET\_MA**SK - a LAN interfész alhálózati maszkja

**DEFAULT\_GATEWAY** - a LAN interfész alapértelmezett átjárója

**TFTP\_SERVER - a TFTP** kiszolgáló IP-címe

**TFTP\_FILE** - a Cisco IOS állományneve a kiszolgálón

**set -** használatával a ROMmon környezeti változói megnézhetők és ellenőrizhetők.

A változók beállítása után a **tftpdnld** parancsot kell használni

A ROMmon parancssorának (rommon1>) megjelenésekor a forgalomirányító a **reset** parancs, vagy az **i** begépelésével újraindítható

Gyakorlat:

8.3.3.2

R1>**telnet 10**.10.10.2 .- telnet kapcsolat kezdeményezése!

debug ip rip Leállítása:

**no debug ip rip** vagy **undebug all** parancsokat

R2#**terminal monitor -** Az R1 éa R2 forgalomirányító közötti Telnet kapcsolat során érkező konzolüzenetek megjelenítéséhez

**Leállítása:**  **terminal no monitor**

A Telnetkapcsolat megszakításához írja be az**exit** parancsot

**A** felfüggesztett Telnetkapcsolat megszakítható a **disconnect** paranccsal, valamint a kapcsolat számának megadásával. pl.: R1>**disconnect 1**

**show sessions -** aktív Telnetkapcsolatok megtekintése

???

**1. lépés: Telnetkapcsolat létesítése az R3 forgalomirányítóval.**

a. Az R1 forgalomirányítóról jelentkezzen be Telnettel az R3 forgalomirányítóra!

b. Konfigurációs parancssorban adja ki a **no hostname** parancsot!

???

**A korábban felfüggesztett Telnetkapcsolat folytatása.**

A **resume** parancsot követően írja be a folytatni kívánt kapcsolat számát

**8.3.3.4**

***RSA-Key generálása SDM-el!!!!***

Nem SDM-el:

Router(config)#**username <username> privilege 15 password <password>**

Konfigurálja a távoli bejövő vty terminálvonalat Telnet és SSH fogadására!

CustomerRouter(config)#**line vty 0 4**

CustomerRouter(config-line)#**privilege level 15**

CustomerRouter(config-line)#**login local**

CustomerRouter(config-line)#**transport input telnet / ssh** CustomerRouter(config-line)#**exit**

Generáljon egy RSA titkosítási kulcspárt a forgalomirányítónak az átküldendő adatok titkosítása és hitelesítése céljából! A tényező bitek száma **768** legyen! Alapértelmezett értéke 512.

(hostnév nem lehet alapértelmezett és kell domain név)  
Router(config)#ip domain-name <név>

Router(config**)#crypto key generate rsa**

**How many bits in the modulus [512] 768 1024 …**

CustomerRouter(config)#**exit**

CustomerRouter(config)#ip ssh version 2

**show ip ssh**

2. A forgalomirányítón a HTTP/HTTPS kiszolgáló indítása.

Router(config)#**ip http server**

Router(config)#**ip http secure-server**

Router(config)#**ip http authentication local**

3) Felhasználói fiók létrehozása 15-ös szintű privilegizált módban (enable privileges). A *felhasználónevet* és a *jelszót* helyettesítse a konfigurálni kívántakkal!

Router(config)#**username <username> privilege 15 password 0 <password>**

4) SSH és Telnet konfigurálása helyi és 15-ös szintű privilegizált belépéshez.

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

Router(config-line)#**privilege level 15**

Router(config-line)#**login local**

Router(config-line)#**transport input telnet**

Router(config-line)#**transport input telnet ssh**

Router(config-line)#**exit**

**Konfigurációs regiszter megváltoztatása:**

Router(config)#**config-register 0x2100**

**vagy:**

rommon 5 **> confreg 0x2102 vagy > o/r 0x2102**

**rommon>? – parancsok kilistázása**

**rommon> dir flash: - flash tartalom megjeleanítése**

rommon 4 >**boot flash:c1841-advipservicesk9-mz.124-10b.bin –** érvényes IOS betöltése!

ROMMON KÖRNYEZETI VÁLTOZÓK BEÁLLÍTÁSA:

rommon 7 > **IP\_ADDRESS=172.17.0.1**

rommon 8 > **IP\_SUBNET\_MASK=255.255.0.0**

rommon 9 > **DEFAULT\_GATEWAY=172.17.0.1**

rommon 10 > **TFTP\_SERVER=172.17.0.2**

rommon 11 > **TFTP\_FILE=c1841-advipservicesk9-mz.124-10b.bin**

A ROMmon környezeti változóinak megtekintéséhez és ellenőrzéséhez a **set** parancsot használja!

rommon 12 > **set**

PS1=rommon ! >

BSI=0

RANDOM\_NUM=1770598170

WARM\_REBOOT=

RET\_2\_RTS=18:04:12 UTC Mon Feb 25 2008

RET\_2\_RCALTS=1203962657

?=0

IP\_ADDRESS=172.17.0.1

IP\_SUBNET\_MASK=255.255.0.0

TFTP\_SERVER=172.17.0.2

TFTP\_FILE=c1841-advipservicesk9-mz.124-10b.bin

A Cisco IOS képfájl TFTP-ről történő letöltésének a megkezdéséhez írja be a **tftpdnld** parancsot!

rommon 14 > **reset – újraondítás**

***2.SZEMESZTER 9. MODUL***

**show ip interface brief** és a **show interfaces** parancsok alkalmazhatók az átviteli közeg és a kábelezési problémák azonosításában. milyen állapotban van a kapcsolat!

A **show interface portazonosító counter errors** paranccsal egy adott interfész hibastatisztikái gyorsan megjeleníthetők.

A **show interface portazonosító status** parancs segítségével megjeleníthető, hogy milyen duplex- és sebességbeállítások

A soros interfészek és vonali problémák többségének felismeréséhez és megoldásához elegendő a **show interfaces serial**

**show ip dhcp conflict** paranccsal kilistáztatható az összes olyan címütközés, melyet a DHCP kiszolgáló regisztrált.

A forgalomirányítók az **ip helper-address** parancs segítségével konfigurálhatók a szórásos üzenetek,

**Router(config-if)# ip helper-address x.x.x.x**

**show running-config interface -** A belső és külső interfészek hibás kijelölése

**show ip nat translations verbose - ?**

Customer(config)#username admin privilege 15 secret cisco123 - ???

?

Customer(config)#ip http server

Customer(config)#ip http authentication local

Customer(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226

?

**Customer#show ip dhcp binding –** DHCP kötések megtekintése!

**show ip dhcp conflict** paranccsal kilistáztatható az összes olyan címütközés, melyet a DHCP kiszolgáló regisztrált.

Gyakorlat:

A **show clock** parancs kiadásával ellenőrizze, hogy az óra most már a pontos időt mutatja-e

**clock set [hh:mm:ss]+dátum– óra beállítása!**

pl.: S1#clock set 18:56:00 22 november 2012

Állítsa vissza a duplex módot a Fast Ethernet 0/3 porton önműködő egyeztetésre!

S1(config)#**interface FastEthernet 0/3**

S1(config-if)#**duplex auto (vagy full; v. half)**

S1(config-if)#**end**

Állítsa a sebességet a FastEthernet 0/3 interfészen 100 Mb/s értékre!

S1(config)#**interface FastEthernet 0/3**

S1(config-if)#**speed 100 (vagy auto)**

S1(config-if)#**end**

A soros 0/0/0 órajelének eltávolítására!

R1(config)#**interface serial 0/0/0**

R1(config-if)#**no clock rate**

R1(config-if)#**end**

Számlálók törlése:

**clear counters serial** - az interfész statisztika alaphelyzetbe állítására!

R1#**clear counters serial 0/0/0**

**Beágyazás beállítása:**

R1(config-if)#**encapsulation ppp**

R1(config-if)#**encapsulation hdlc**

R1(config-if)#**encapsulation frame-relay**

**show running-config interface Serial 0/0/0 ????kipróbálni!!!!9.2.5.4**

**no auto-summary** - Az útvonal összevonás kikapcsolásához a forgalomirányító rip-konfigurációs módjában

***3.Szemeszter***

2.modul

**show sessions** - Megjeleníti a távoli állomásokkal létesített telnetkapcsolatokat (VTY). Megjeleníti a kapcsolatazonosítót, az állomásnevet és a címet.

**show ssh** - Megjeleníti a távoli állomásokkal létesített ssh kiszolgálói kapcsolatokat.

**erase startup-config –** indító konfig file törlése

3.modul

**S3(config)#spanning-tree vlan 1 priority 4096** – feszítőfa prioritásának beállítása

**S3(config)#no spanning-tree vlan 1 priority** – alapértelmezett prioritás visszaállítása

**Show spanning-tree** – A gyökérponti híd azonosítóját, a hídazonosítót és a portok állapotát jeleníti meg

**Show spanning-tree summary** – A portok állapotáról ad összefoglaló információt

**Show spanning-tree root** – A gyökérponti híd állapotát és konfigurációját jeleníti meg

**Show spannig-tree detail** – Részletes információt nyújt a portokról

**Show spanning-tree interface** - Az STP interfészek állapotát és konfigurációját jeleníti meg

**Show spanning-tree blockedports** - Megmutatja a lezárt portokat

VLAN-ok létrehozására globális konfigurációs módban az alábbi parancsok használhatók:

Switch(config)#vlan vlan\_szám

Switch(config-vlan)#name vlan\_név

Switch(config-vlan)#exit

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

Switch(config)#interface fa0/port\_szám

Switch(config-if)#switchport access vlan vlan\_szám

Switch(config-if)#exit

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

Switch(config)#interface range fa0/tartomány\_kezdete - tartomány\_vége

Switch(config-if)#switchport access vlan vlan\_szám

Switch(config-if)#exit

show vlan - észletes listát jelenít meg a kapcsoló jelenleg aktív VLAN-jairól, feltüntetve azok nevét, számát és a hozzárendelt portokat.

STP statisztikát jelenít meg, ha a kapcsoló VLAN-alapú STP-re van beállítva.

show vlan brief - Összesített listát jelenít meg kizárólag az aktív VLAN-okról és az azokhoz rendelt portokról

show vlan id azonosító\_szám - Az azonosítószámával (ID) megadott VLAN-ra vonatkozóan jelenít meg információkat.

show vlan name vlan\_szám - A nevével megadott VLAN-ra vonatkozóan jelenít meg információkat.

VLAN törlése:

Switch(config)#no vlan vlan\_szám

Port kivétele egy meghatározott VLAN-ból:

Switch(config)#interface fa0/port\_szám

Switch(config-if)#no switchport access vlan vlan\_szám

Alapértelmezés szerint a kapcsolók portjai hozzáférési portok. Trönkport konfigurálására az alábbi parancsok használhatók:

Switch(config)#interface fa0/port\_szám

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}

Az újabb kapcsolók képesek az összeköttetések másik végpontjának beállításait felismerni, így a csatlakozó eszköz szerint konfigurálják a kapcsolatot trönk, illetve hozzáférési portnak.

Switch(config-if)#switchport mode dynamic {desirable | auto}

Ha egy trönkportot ismét hozzáférési portra szeretnénk konfigurálni, az alábbi parancsok használhatók:

Switch(config)#interface fa0/port\_szám

Switch(config-if)#no switchport mode trunk

vagy

Switch(config-if)#switchport mode access

Egy 802.1Q összeköttetéshez tartozó fizikai interfészen a natív VLAN beállítására az alábbi parancs alkalmazható:

Switch(config-if)#dot1q native vlan vlan-azonosító

**VLAN-ok közötti forgalomirányítás konfigurálásához az alábbi lépések szükségesek:**

1. Trönkport konfigurálása a kapcsolón.

Router(config)#interface fa2/0

Switch(config-if)#switchport mode trunk

2. IP-cím és alhálózati maszk nélküli interfész konfigurálása a forgalomirányítón.

Router(config)#interface fa1/0

Router(config-if)#no ip address

Router(config-if)#no shutdown

3. Minden VLAN-hoz alinterfész konfigurálása a forgalomirányítón. Az alinterfészeken 802.1Q beágyazás szükséges.

Router(config)#interface fa0/0.10

Router(config-subif)#encapsulation dot1q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.0

4. A VLAN-ok közötti forgalomirányítás beállításainak és működésének ellenőrzéséhez az alábbi parancsok használhatók:

Switch#show trunk

Router#show ip interfaces

Router#show ip interfaces brief

Router#show ip route

Gyakorlatok:

**mac-address-table static <Mac-Cím> vlan 1 interface fastethernet 0/4 -** statikus MAC-címet a Fa0/4-es interfészen 1-es VLAN-ban

A MAC-címtábla statikus bejegyzésének eltávolítása:

Switch1(config)#**no mac-address-table static 00e0.2917.1884 vlan 1 interface fastethernet 0/4**

Switch1(config-if)#**switchport port-security violation shutdown -** A biztonság megsértése esetén az interfészt le kell állítani.

Switch1(config)#**interface range Fa0/5 – 24 –** röbb port egyszerrre való kezelése

SwitchA#**show hardware**

**show spanning-tree detail**

**show spanning-tree bridge**

**show spanning-tree summary**

Switch1(config)#**vtp domain Csoport1 -** Switch1 kapcsolót, hogy a Csoport1 tartományhoz tartozzon

Switch1(config)#**vtp mode server -** Switch1 kapcsolót VTP kiszolgálónak

Switch2(config)#**vtp mode client**

**show vtp status** parancs alkalmazásával ellenőrizze, hogy az összes VLAN elterjedt-e a tartományban

4.modul

PAT használata: ip nat inside source list 1 interface serial 0/0/0 overload

A NAT és PAT működésének ellenőrzésére szolgáló parancsok:

show ip nat translations

show ip nat statistics - A parancs a fordítások statisztikáját mutatja,

<https://www.manageengine.com/network-configuration-manager/configlets/configuring-pat-cisco.html>

22-es oldal Dinamikus NAT

<https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html>

Ha a dinamukus NAT-nál a kezdő és a végcím ugyan az akkor úgy is működhet a PAT!!!  
overload kell a végére!!!

5.modul

A lebegő statikus útvonal létrehozásához az ip route parancs végére adjunk meg egy adminisztratív távolság értéket:

Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.9.1 200

RIP2 milyen frissítéseket köldjön és fogadjon:

ip rip send version <1 | 2 | 1 2>

ip rip receive version <1 | 2 | 1 2>

Automatikus összegzés kikapcsolása: - Router(config-router)#no auto-summary

A parancsban megadott interfészen letiltja az irányítási frissítések kiküldését - Router(config-router)#passive-interface interfész\_típus interfész\_szám

show ip rip database: Minden RIP által megismert útvonalat listáz

debug ip rip vagy a debug ip rip {events}: A RIP által küldött és fogadott irányítási frissítéseket mutatja valós időben

Az EIGRP hitelesítéséhez előre megosztott kulcsokra van szükség.

A kulcs létrehozásához a következő parancsokra van szükség:

**key chain lánc\_neve**

Globális konfigurációs parancs.

A kulcslánc nevét határozza meg és belép kulcslánc konfigurációs módba.

**key kulcs\_azonosító**

Azonosítja a kulcs számát és belép a megadott kulcsazonosító konfigurációs módba.

**key-string szöveg**

Azonosítja a kulcs karakterláncot vagy más néven jelszót. Ennek minden EIGRP forgalomirányítón egyeznie kell.

Hitelesítés engedélyezése

Az EIGRP MD5 hitelesítését a kulcs segítségével a következő interfész konfigurációs parancsokkal lehet engedélyezni:

**ip authentication mode eigrp md5**

Meghatározza, hogy MD5 hitelesítés szükséges a csomagok küldéséhez, fogadásához.

**ip authentication key-chain eigrp AS lánc\_neve**

Az AS határozza meg az EIGRP konfiguráció AS azonosítóját.

A lánc\_neve paraméter határozza meg az előzőleg konfigurált kulcsláncot.

show ip eigrp neighbors detail - Segítségével leellenőrizhetők az EIGRP szomszédsági viszonyai. Megmutatja a szomszédos forgalomirányítók interfészeit és IP-címeit.

show ip eigrp topology - Megmutatja a legjobb és az összes második legjobb útvonalat, valamint a legkisebb és a jelentett távolságot.

show ip eigrp interfaces detail - Segítségével leellenőrizhetők az EIGRP-t használó interfészek.

show ip eigrp traffic - Megmutatja az EIGRP által küldött és fogadott csomagok típusát és számát.

debug eigrp packet - megmutatja az összes EIGRP csomag küldését és fogadását

debug eigrp fsm - megjeleníti az EIGRP-nek a második legjobb útvonalakkal kapcsolatos tevékenységeit, aminek alapján megállapítható, hogy az útvonalakat törölték, felfedezték vagy bejegyezték-e.

6.modul

**show ip ospf**

**show ip ospf interface**

prioritás beállításával az alábbi parancs segítségével: **ip ospf priority number**

Az OSPF engedélyezése - **router(config)#router ospf <folyamat-azonosító>**

Hálózatok hirdetése **- Router(config-router)#network <hálózati-cím> <helyettesítő-maszk> area <területazonosító>**

**clear ip ospf process** - parancs alkalmazásával biztosítható az új értékek érvénybelépése

**bandwidth** parancs megváltoztatja az OSPF költségmértékének meghatározásához használt sávszélesség értékét.

A költség közvetlen megváltoztatására az **ip ospf cost** parancs használható

**show ip ospf neighbor** parancs, mellyel a szomszédsági viszonyok kialakítása ellenőrizhető

show ip protocols - Megjeleníti a forgalomirányító azonosítóját, a meghirdetett hálózatokat és a szomszédsági viszonyban lévő forgalomirányítók IP-címét.

show ip ospf - Megjeleníti a forgalomirányító azonosítóját és az OSPF folyamatának, időzítőinek és területi információjának részleteit.

show ip ospf interface - Megjeleníti a forgalomirányító azonosítóját, a hálózat típusának költségét és az időzítők beállításait.

show ip route - Információt ad arra vonatkozóan, hogy a forgalomirányító kap-e és küld-e OSPF útvonal információt.

R1(config)#router ospf 1

R1(config-router)#default-information originate

A fenti parancsok eredményeként az OSPF tartomány forgalomirányítóinak irányítótáblájában megjelenik egy végső (last resort) átjáró és a 0.0.0.0/0 hálózat.

7.modul

encapsulation ppp - Ez aktiválja a PPP beágyazást a soros interfészen.

compress [predictor | stac] - Engedélyezi a tömörítést az interfészen, predictor (előjósló) vagy stacker (verem-tárolásos) módszer használatával.

ppp multilink Segítségével terheléselosztás konfigurálható több összeköttetés között.

show interfaces serial - Megjeleníti a beágyazás típusát és a kapcsolatvezérlő protokoll (LCP) állapotait.

show controllers - Kijelzi az interfész-csatornák állapotát és azt, hogy csatlakozik-e kábel az interfészhez.

debug serial interface - Segítségével ellenőrizhető az ébrenléti (keepalive) üzenetek számának folyamatos növekedése. Ha ezeknek a csomagoknak a száma nem növekszik, akkor valószínűleg időzítési probléma lépett fel az interfészkártyában vagy a hálózatban.

debug ppp - Információt biztosít a PPP protokoll működési folyamatának különböző szakaszairól, beleértve az egyeztetést és a hitelesítést.

PPP kapcsolatok hitelesítésének beállításához a következő globális konfigurációs parancsok használhatóak:

username név password jelszó

ppp authentication {chap | chap pap | pap chap | pap}

ppp pap sent-username név password jelszó

debug ppp {authentication | packet | error | negotiation | chap }

8.modul

Normál ACL

Router(config)#access-list 1 permit host 172.16.2.88 - Egy bizonyos IP-címet engedélyez.

Kiterjesztett ACL

Router(config)#access-list 100 deny tcp 172.16.2.0 0.0.0.255 any eq telnet - Tiltja a 172.16.2.0/24 alhálózat számára bármely más állomás elérését, amennyiben telnetkapcsolatot próbálnak létesíten

Nevesített ACL

Router(config)#ip access-list standard permit-ip

Router(config-ext-nacl)#permit host 192.168.5.47 - Létrehoz egy permit-ip nevű normál hozzáférési listát. Engedélyezi a hozzáférést a 192.168.5.47 IP-címről. Az első parancs a forgalomirányítót NACL konfigurációs almódba helyezi.

Az ACL alkalmazása

R2(config-if)#ip access-group hozzáférési lista száma [in | out]

pl.: R2(config)#interface fastethernet 0/0

R2(config-if)#ip access-group 5 in

**show access-lists [hozzáférési lista száma]** - A fenti parancs nem csupán a forgalomirányító összes ACL-jének tartalmát jeleníti meg, hanem az egyes engedélyező és tiltó utasításokhoz tartozó – az ACL alkalmazása óta talált – egyezések számát is. Egy adott lista megtekintéséhez adjuk meg az ACL nevét vagy számát a parancs paramétereként!

Nevesített ACL az alábbi paranccsal hozható létre:

ip access-list {standard | extended} név

Az **ip access-group parancs** helyettaz **access-class** parancsotkell használnunk**.**

A VTY vonalakhoz hozzárendelt hozzáférési listák beállításához kövessük az alábbi irányelveket:

A VTY vonalakhoz ne nevesített, hanem számozott ACL-t használjunk!

A korlátozásokat minden VTY vonalhoz hozzá kell rendelni, mivel nem szabályozható, hogy a felhasználó melyik vonalon kapcsolódjon!

eq - egyenlő (equals)

gt – nagyobb, mint (greater than)

lt – kisebb, mint (less than)

példa: R1(config)#access-list 122 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.89 eq 80

**access-list 101 permit tcp any any established**

A fenti utasítás használatával az összes kívülről érkező tcp csomag engedélyezve lesz, feltéve, ha a válasz egy belülről érkező kérésre jött.

Az ACL utasításban megadott **echo-reply** és az **unreachable** kulcsszó a ping válaszok és a cél elérhetetlenségét jelző üzenetek fogadásának engedélyezésére.

A tcp kulcsszó az FTP, a HTTP, a Telnet és hasonló protokollokat engedélyezi vagy tiltja.

A permit ip kulcskifejezés a teljes IP-forgalmat – beleértve a TCP, az UDP és az ICMP protokollt – engedélyezi.

A **show access-list** parancs használatával ACL soronként megjelenített egyezési számértékek utasításonként megmutatják, hány csomag-egyezés történt. A kimenet a csomag forrását vagy célját, sem pedig a használt protokollt nem jelzi.

A naplózás az egyes ACL utasításokra külön-külön aktiválható, a vizsgálni kívánt utasítások végére illesztett **log** opcióval.

Ha távoli forgalomirányítóval dolgozunk, és az ACL működését ellenőrizzük, használjuk a **reload in 30** parancsot! Ha ugyanis egy esetleges hiba az ACL-ben letiltja a hozzáférést a forgalomirányítóhoz, a távoli kapcsolat is megszűnhet. A fenti parancs használatával a forgalomirányító 30 perc elteltével újraindul az ACL nélküli indítási konfiguráció beállításaival

9.modul

tábla dinamikus bejegyzéseinek törléséhez adja ki az alábbi parancsot:

clear mac-address-table dynamic

Információt ad az STP konfigurációjáról:

show spanning-tree

Információt ad egy adott interfész STP állapotáról:

show spanning-tree interface interface\_azonosító

Ha információra van szükségünk egy bizonyos VLAN-ról, használjuk a **show vlan id vlan\_szám** parancsot, amivel megtekinthetőek az egyes VLAN-okhoz rendelt portok!

vtp password jelszó

show vtp password

A show ip route paranccsal történő tesztelés előtt érdemes törölni az irányítótábla tartalmát a clear ip route \* paranccsal.

show ip ospf interface – Router ID, hlózat típusa, összeköttetés típusa, állapota; DR azonosító stb. …

debug ip ospf events – routerek egymással váltott valós idejű OSPF üzeneteit mutatja meg

debug ip ospf packet – Valós id. inf. minden fogadott OSPF csomagról

A következő utasítás a PPP csomagok áramlásának valós idejű megtekintéséhez használható:

debug ppp packet - a PPP csomagok áramlásának valós idejű megtekintéséhez

A kábel típusának megjelenítéséhez, valamint a DTE, DCE állapot és az órajel felismeréséhez használjuk a következő parancsot:

show controllers <soros\_port>

Ha PAP hitelesítést szeretnénk használni egy aktuális verziójú IOS rendszeren, aktiváljuk azt az alábbi paranccsal:

ppp pap sent-username felhasználói\_név password jelszó

hitelesítési folyamattal kapcsolatban álló csomagok megjelenítéséhez:

debug ppp authentication

Az egyes ACL utasításokhoz tartozó illeszkedési számlálók törléséhez a következő parancs használható:

clear access-list counters

A **debug ip packet** parancs azokat a csomagokat mutatja meg, melyeknek forrás-, illetve célcíme egy forgalomirányító interfésze. Azok a csomagok is megjelennek a parancs hatására, amelyeket letiltott egy ACL az interfészen. Néhány forgalomtípus, melyek debug üzeneteket hoznak létre:

RIP frissítések egy forgalomirányító interfésze irányából vagy irányába

Bármilyen külső forrásból származó, külső célállomás felé tartó telnet forgalom, melyet blokkolt egy ACL az interfészen.

**3 szemeszter**

3. Modul

Az STP prioritás beállítása:

**S3(config)#spanning-tree vlan 1 priority 4096**

A prioritás alapértelmezett értékének visszaállítása:

**S3(config)#no spanning-tree vlan 1 priority**

**Show spanning-tree** – A gyökérponti híd azonosítóját, a hídazonosítót és a portok állapotát jeleníti meg

**Show spanning-tree summary** – A portok állapotáról ad összefoglaló információt

**Show spanning-tree root** – A gyökérponti híd állapotát és konfigurációját jeleníti meg

**Show spannig-tree detail** – Részletes információt nyújt a portokról

**Show spanning-tree interface** - Az STP interfészek állapotát és konfigurációját jeleníti meg

**Show spanning-tree blockedports** - Megmutatja a lezárt portokat

VLAN-ok létrehozására globális konfigurációs módban az alábbi parancsok használhatók:

**Switch(config)#vlan vlan\_szám**

**Switch(config-vlan)#name vlan\_név**

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

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

**Switch(config)#interface fa0/port\_szám**

**Switch(config-if)#switchport access vlan vlan\_szám**

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

Több port egyidejű VLAN-hoz rendelésére az alábbi parancsok használhatók:

**Switch(config)#interface range fa0/tartomány\_kezdete - tartomány\_vége**

**Switch(config-if)#switchport access vlan vlan\_szám**

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

**show vlan** - Részletes listát jelenít meg a kapcsoló jelenleg aktív VLAN-jairól, feltüntetve azok nevét, számát és a hozzárendelt portokat.

STP statisztikát jelenít meg, ha a kapcsoló VLAN-alapú STP-re van beállítva.

**show vlan brief -** Összesített listát jelenít meg kizárólag az aktív VLAN-okról és az azokhoz rendelt portokról

**show vlan id** azonosító\_szám

Az azonosítószámával (ID) megadott VLAN-ra vonatkozóan jelenít meg információkat.

**show vlan name vlan\_szám**

A nevével megadott VLAN-ra vonatkozóan jelenít meg információkat.

VLAN törlése:

**Switch(config)#no vlan vlan\_szám**

Port kivétele egy meghatározott VLAN-ból:

**Switch(config)#interface fa0/port\_szám**

**Switch(config-if)#no switchport access vlan vlan\_szám**

baállítás pl.:

S1(config)#**interface vlan 1**

S1(config-if)#**ip address 172.16.1.2 255.255.255.0**

S1(config-if)#**no shutdown**

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

*S1(config)#****ip default-gateway 172.16.1.1***

S1(config)#**end**

**+**

S1(config)#**interface fastethernet 0/2**

S1(config-if)#**switchport mode access**

S1(config-if)#**switchport access vlan 20**

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

S1(config)#**interface range fastethernet 0/3 - 8**

S1(config-if-range)#**switchport mode access**

S1(config-if-range)#**switchport access vlan 30**

S1(config-if-range)#**end**

S1#**show running-config**

Alapértelmezés szerint a kapcsolók portjai hozzáférési portok. Trönkport konfigurálására az alábbi parancsok használhatók:

**Switch(config)#interface fa0/port\_szám**

**Switch(config-if)#switchport mode trunk**

**Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}**

Ha egy trönkportot ismét hozzáférési portra szeretnénk konfigurálni, az alábbi parancsok használhatók:

**Switch(config)#interface fa0/port\_szám**

**Switch(config-if)#no switchport mode trunk**

vagy

**Switch(config-if)#switchport mode access**

Natív vlan megváltoztatása

**Switch(config-if)#dot1q native vlan vlan-azonosító**

VLAN-ok közötti forgalomirányítás konfigurálásához az alábbi lépések szükségesek:

1. Trönkport konfigurálása a kapcsolón.

**Router(config)#interface fa2/0**

**Switch(config-if)#switchport mode trunk**

2. IP-cím és alhálózati maszk nélküli interfész konfigurálása a forgalomirányítón.

**Router(config)#interface fa0/0**

**Router(config-if)#no ip address**

**Router(config-if)#no shutdown**

3. Minden VLAN-hoz alinterfész konfigurálása a forgalomirányítón. Az alinterfészeken 802.1Q beágyazás szükséges.

**Router(config)#interface interface fa0/0.10**

**Router(config-subif)#encapsulation dot1q 10**

**Router(config-subif)#ip address 192.168.10.1 255.255.255.0**

4. A VLAN-ok közötti forgalomirányítás beállításainak és működésének ellenőrzéséhez az alábbi parancsok használhatók:

**Switch#show trunk**

**Router#show ip interfaces**

**Router#show ip interfaces brief**

**Router#show ip route**

VTP-konfig

**Switch(config)# vtp domain tartomány név**

**Switch(config)# vtp mode (server|client|transparent)**

**Switch(config)# vtp password jelszó**

**Switch(config)# end**

**show vtp status**

**show vtp password**

**show vtp counters**

4. modul

DinamikusNAT

A nyilvános címkészlet megadásához használja az **ip nat pool** parancsot! Gateway(config)#**ip nat pool public\_access 209.165.200.242 209.165.200.253 netmask 255.255.255.224**

A statikus IP NAT-hozzárendelés konfigurálásához privilegizált EXEC módban adja ki az **ip nat inside source static** parancsot!

Gateway(config)#**ip nat inside source static 10.10.10.2 209.165.200.225**

**https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html**

A NAT címfordítás megadásához használja az **ip nat inside source** parancsot!

Gateway(config)#**ip nat inside source list 1 pool public\_access overload**

5. modul

Lebegő statikus útvonal:

**Router(config)#ip route 192.168.4.0 255.255.255.0 192.168.9.1 200**

A RIPv2 egy alapértelmezett útvonalat is képes elküldeni a frissítéseiben: **redistribute static** paranccsal

Az R3 hirdetni fogja ezt az útvonalat a többi forgalomirányítónak, ha a következő paranccsal kiegészítjük a RIP konfigurációját:

R3(config)#**router rip**

R3(config-router)#**default-information originate**

Az interfész konfigurációs módban kiadott passive-interface parancs a parancsban megadott interfészen letiltja az irányítási frissítések kiküldését.

**Router(config-router)#passive-interface interfész\_típus interfész\_szám**

**show ip rip database:** Minden RIP által megismert útvonalat listáz

**debug ip rip vagy a debug ip rip {events**}: A RIP által küldött és fogadott irányítási frissítéseket mutatja valós időben

**EIGRP implementálása:**

A Gateway forgalomirányítón konfiguráljon EIGRP irányító protokollt, melynek autonóm rendszer azonosítója 100 és hirdesse a megfelelő hálózatokat!

**Router** (config)#router eigrp 100

**Router** (config-router)#network 10.0.0.0

**Router** (config-router)#network 10.0.0.4

sávszélességet az érintett portoknál kell állítani!!! (a kapcsolat mindkét oldalán be kell állítani!)

a megadott szám kbit/s-ben értendő!

pl.:

**Router1** (config)#**interface serial 0/0/0**

**Router1** (config-if)#**bandwidth 256**

**Router2** (config)#**interface serial 0/0/0**

**Router2** (config-if)#**bandwidth 256**

Engedélyezze a Branch1 forgalomirányítónak az EIGRP MD5 hitelesítés használatát, az összes EIGRP szomszéddal, a **discchain** kulcslánc alkalmazásával!

Branch1(config)#**key chain discchain**

Branch1(config-keychain)#**key 1**

Branch1(config-keychain-key)#**key-string san-fran**

Branch1(config-keychain-key)#**end**

Branch1#**configure terminal**

Branch1(config)#**interface serial 0/0/0**

Branch1(config-if)#**ip authentication mode eigrp 100 md5**

Branch1(config-if)#**ip authentication key-chain eigrp 100 discchain** Branch1(config-if)#**exit**

Branch1(config)#**interface serial 0/0/1**

Branch1(config-if)#**ip authentication mode eigrp 100 md5**

Branch1(config-if)#**ip authentication key-chain eigrp 100 discchain**

6. modul

**ip ospf cost** parancs alkalmazásával az interfész költsége kézzel beállítható.

Ha az aktív konfiguráció nem változott, írja be az alábbi parancsokat: 6.2.1.4 gyak.:

R1(config)#**router ospf 1**

R1(config-router)#**log-adjacency-changes**

R1(config-router)#**end**

Az OSPF hitelesítés beállítása két lépéses folyamat. Először engedélyezni kell a forgalomirányítón egy területre, majd az interfészeken kell konfigurálni a megfelelő területen.

a. Engedélyezzen MD5 hitelesítést a 0-ás területen mindkét forgalomirányítón!

R1(config)#**router ospf 1**

R1(config-router)#**area 0 authentication message-digest**

R2(config)#**router ospf 1**

R2(config-router)#**area 0 authentication message-digest**

b. Engedélyezze az OSPF hitelesítést az R1 forgalomirányító S0/0/0 interfészén!

R1(config)#**interface s0/0/0** R1(config-if)#**ip ospf message-digest-key 10 md5 secretpassword**

c. A **show ip ospf neighbor** parancs alkalmazásával nézze meg az R1 forgalomirányító ismert szomszédait!

R1#**show ip ospf neighbor**

Minden forgalomirányítón a **clear ip ospf 1 process** parancs alkalmazásával állítsa alaphelyzetbe az OSPF folyamatot!

Pontosabb költségszámítások érdekében szükséges lehet a referencia-sávszélesség értékének módosítása, mely az **auto-cost reference-bandwidth** paranccal hajtható végre.

alapértelmezett útvonal hordetése:

**R1(config)#router ospf 1**

**R1(config-router)#default-information originate**

Az OSPF ASBR eszköz forgalomirányító konfigurációs üzemmódjában az alábbi parancs segítségével konfigurálható összevont útvonal:

**area** terület-azonosító **range** IP-cím maszk

7. modul

A Cisco forgalomirányítók soros interfészein a HDLC az alapértelemezett beágyazási típus. A beágyazás típusának megváltoztatásához, **encapsulation ppp e**z aktiválja a PPP beágyazást a soros interfészen.

Miután a PPP engedélyezésre került, beállíthatóvá válnak az opcionális paraméterek, például a tömörítés és a terheléselosztás.

**compress [predictor | stac]** Engedélyezi a tömörítést az interfészen, predictor (előjósló) vagy stacker (verem-tárolásos) módszer használatával.

**ppp multilink** Segítségével terheléselosztás konfigurálható több összeköttetés között.

PPP kapcsolatok hitelesítésének beállításához a következő globális konfigurációs parancsok használhatóak:

**username név password jelszó**

**ppp authentication {chap | chap pap | pap chap | pap}**

ellenőrzés:

**debug ppp {authentication | packet | error | negotiation | chap }**

A Cisco IOS 11.1-es és újabb változataiban a PAP-ot külön engedélyezni kell az interfészen,

alapállapot szerint ugyanis le van tiltva. Engedélyezze a PAP hitelesítést a Serial 0/0/0 interfész

interfészkonfigurációs módjában!

R1(config-if)#**ppp pap sent-username R1 password cisco**

**A PAP hitelesítés eltávolítása az R1 és R2 forgalomirányítókon**

Távolítsa el a PAP hitelesítést az R1 és R2 forgalomirányítókon, a PAP konfigurálásához használt parancsokelé írt **no** parancs segítségével!

R1(config)#**interface serial 0/0/0**

R1(config-if)#**no ppp authentication pap**

R1(config-if)#**no ppp pap sent-username R1 password cisco**

R1(config-if)#**exit**

R1(config)#**no username R2 password cisco**

R2(config)#**username R1 password cisco**

R2(config)#**interface serial 0/0/0**

R2(config-if)#**ppp authentication chap**

8. modul

A normál ACL utasítás-szintaktikája az alábbi:

**access-list [hozzáférési\_lista\_száma] [deny|permit] [forráscím] [forrás\_helyettesítő\_maszk][log]**

Dokumentáljuk az ACL minden részének vagy utasításának a funkcióját a remark parancs segítségével:

**access-list [a lista száma] remark [szöveg]**

Egy ACL törléséhez használjuk az alábbi parancsot:

**no access-list [a lista száma]**

Az ACL alkalmazása

**R2(config-if)#ip access-group hozzáférési lista száma [in | out]**

**R2(config)#interface fastethernet 0/0**

**R2(config-if)#ip access-group 5 in**

Az ACL eltávolítása az interfészről az ACL érintetlenül hagyásával, a **no ip access-group interface** paranccsal lehetséges.

**show access-lists [hozzáférési lista száma]**

Hozza létre a fenti feladatokat végrehajtó ***kiterjesztett ACL-t***, majd alkalmazza az R2-n!

R2(config)#**access-list 101 permit *ip* host 192.168.1.10 host 192.168.5.10**

R2(config)#**access-list 101 deny *ip* 192.168.1.0 0.0.0.255 host 192.168.5.10**

R2(config)#**access-list 101 permit *ip* any any**

R2(config)#**access-list 101 deny *ip* any any**

**Nevesített ACL az alábbi paranccsal hozható létre:**

**ip access-list {standard | extended} név**

**show access-lists**

Egy már létező sor szerkesztéséhez az alábbiakat kell tenni:

**A no line number parancs használatával távolítsuk el a sort!**

A sorhoz tartozó szám használatával adjuk ismét hozzá ugyanazt a sort az ACL-hez!

Ha terminál kapcsolatra VTY –ra akarunk ACL-t

Az ip access-group parancs helyett az **access-class** parancsot kell használnunk.

Az utasítás kiértékelése előtt a portszámokon kívül egy feltétel megadása is szükséges. Erre az alábbi gyakori rövidítések használatosak:

eq - egyenlő (equals)

gt – nagyobb, mint (greater than)

lt – kisebb, mint (less than)

Vegyük az alábbi példát:

R1(config)#access-list 122 permit **tcp** 192.168.1.0 0.0.0.255 host 192.168.2.89 **eq 80**

R1(config)#access-list 181 deny **tcp** any 192.168.77.0 0.0.0.255 **range 20 21**

**access-list 101 permit tcp any any established**

A fenti utasítás használatával az összes kívülről érkező tcp csomag engedélyezve lesz, feltéve, ha a válasz egy belülről érkező kérésre jött.

Ugyanakkor nem kívánatos, hogy külső felhasználók megpingelhessék a belső hálózat eszközeit vagy követhessék az azokhoz vezető útvonalat. Ilyen esetekben használható az ACL utasításban megadott **echo-reply** és az **unreachable** kulcsszó a ping válaszok és a cél elérhetetlenségét jelző üzenetek fogadásának engedélyezésére. Ugyanakkor a külső forrásokból származó ping mindaddig el lesz utasítva, amíg azt egy másik utasítás külön nem engedélyezi.

*1. Ha egy bejövő csomag érkezik a címfordítást végző külső interfészre, akkor a forgalomirányító:*

*Alkalmazza a bejövő ACL-t.*

*A célcímet külsőről belsőre (globálisról lokálisra) fordítja.*

*Továbbítja a csomagot.*

*2. Ha egy csomag kifelé távozik a címfordítást végző külső interfészről, akkor a forgalomirányító:*

*A forráscímet belsőről külsőre (lokálisról globálisra) fordítja. Alkalmazza a kimenő ACL-t.*

*Alkalmazza a kimenő ACL-t.*

A **show access-list** parancs használatával ACL soronként megjelenített egyezési számértékek utasításonként megmutatják, hány csomag-egyezés történt.

A naplózás az egyes ACL utasításokra külön-külön aktiválható, a vizsgálni kívánt utasítások végére illesztett **log** opcióval.

A naplózás kikapcsolásához használjuk az alábbi parancsot:

**no logging console**

A hibakeresés teljes kikapcsolásához használjuk az alábbi parancsot:

**undebug all**

Egy konkrét (pl. IP-csomagokhoz kapcsolódó) hibakeresés kikapcsolásához használjuk az alábbi parancsot:

**no debug ip packet**