**Router, switch alapkonfigurációja**

**Vonali interfészek védése (konzol port, Telneten, SSH-n keresztül bejelentkezés védése)**

**Konzol port védése jelszóval:**

line con 0

password [*jelszó*]

login

logging synchronous

exit

**Telneten keresztüli elérés csak jelszóval:**

line vty 0 15

password [*jelszó*]

login

exit

**Helyi felhasználó létrehozása:**

username [*felhasználói név*] secret [*jelszó*]

username [*felhasználói név*] password [*jelszó*]

**Konzol port védése a helyi felhasználóval:**

line con 0

login local

logging synchronous

exit

**Telneten keresztüli elérés a helyi felhasználóval:**

line vty 0 15

login local

exit

**SSH-n keresztüli elérés beállítása a helyi felhasználóval:**

hostname [*az eszköz neve*]

ip domain-name [*tartománynév*]

crypto key generate rsa

1024

line vty 0 15

login local

transport input ssh

exit

**Telneten keresztüli elérés kliens parancssorából:**

telnet [*IP cím*]

**SSH-n keresztüli elérés kliens parancssorából:**

ssh –l [*felhasználói név*] [*IP cím*]

**Privilégizált üzemmód elérésének levédése jelszóval**

enable secret [*jelszó*]

**A konfigurációs állományokban titkosítva jelenjenek meg a jelszavak:**

service password-encryption

**Figyelmeztető üzenet beállítása:**

banner motd # [*Üzenet – ékezet nélkül*] #

**DNS szerver címének beállítása:**

ip name-server [*IP cím*]

**Router konfigurálása**

**Interface-k beállítása:**

int [*interface azonosítója*]

ip add [*IP cím*] [*maszk*] vagy dhcp

no shut

exit

**Interface beállítása több vlan-nál:**

int [*főinterface azonosítója*]

no ip add

no shut

exit

**Alinterface létrehozása:**

int [*főinterface*].[*alinterface száma, ami célszerű, ha a vlan azonosítója*]

encapsulation dot1q [*vlan azonosító*]

ip add [*IP cím*] [*maszk*]

exit

**Hurok interface beállítása:**

int loopback [*hurok interface azonosító száma*]

ip add [*IP cím*] [*maszk*]

exit

**DHCP szerver konfigurálása – ez lehetséges Catalyst 2960-as switchen is.**

ip dhcp excluded-address [*kezdő IP*] [*záró IP*] – mettől meddig NE OSSZON ki címeket

ip dhcp pool [*szórási tartomány azonosítója*]

network [*hálózat cím*] [*maszk*]

default-router [*IP cím*]

dns-server [*IP cím*]

exit

**DHCP manual binding** *–* mindig ugyanazt az IP címet ossza ki a szerver a kliensnek

host *[IP cím] [maszk vagy /prefix hossz]*

hardware-address *[MAC cím]*

client-name *[eszköz neve]*

**Routing konfigurálása**

**RIP:**

router rip

version 2

no auto-summary

network [*közvetlenül csatlakozó* *hálózat címe*]

passive-interface [*interface azonosítója*]

redistribute ospf [*az* *ospf folyamatazonosító száma*] metric 5

redistribute eigrp [*az* *eigrp AS azonosító száma*] metric 5

exit

**EIGRP:**

router eigrp [*az* *AS azonosító száma*]

no auto-summary

network [*közvetlenül csatlakozó* *hálózat címe*]

vagy

network [*közvetlenül csatlakozó* *hálózat címe*] [*maszk*]

vagy

network [*közvetlenül csatlakozó* *hálózat címe*] [*wildcard* *maszk*]

passive-interface [*interface azonosítója*]

redistribute rip metric 10000 100 255 1 1500

redistribute ospf [*az* *ospf folyamatazonosító száma*] metric 10000 100 255 1 1500

exit

**OSPF**

router ospf [*az* *ospf folyamatazonosító száma*]

network [*közvetlenül csatlakozó* *hálózat címe*] [*wildcard* *maszk*] area [*az ospf területazonosító száma*]

passive-interface [*interface azonosítója*]

redistribute rip subnets

redistrubute eigrp [*az EIGRPS-s az AS azonosító száma*] subnets

exit

**Statikus routing konfigurálása**: ip route [*távoli hálózat címe*] [*maszk*] [*next hop*]

vagy ip route [*távoli hálózat címe*] [*maszk*] [*kimenő interface azonosítója*]

**Pont-pont Frame-Relay**

**konfigurálása – közvetlenül vannak összekapcsolva a routerek, felhő nem kell – DTE kábelt kell alkalmazni.**

int [*fő interface azonosítója*]

no ip add

encapsulation frame-relay

no keep alive

no shut

exit

Alinterface létrehozása

int [*főinterface*].[*alinterface száma*] point-to-point

ip add [*IP cím*] [*maszk*]

frame-relay interface-dlci [*útvonal azonosító száma*]

exit

**Pont-multipont Frame-Relay konfigurálása**

**Felhőn keresztül vannak összekapcsolva a routerek. DCE kábelt kell alkalmazni.**

int [*fő interface azonosítója*]

no ip add

encapsulation frame-relay

no keep alive

no shut

exit

Alinterface létrehozása

int [*főinterface*].[*alinterface száma*] multipoint

ip add [*IP cím*] [*maszk*]

frame-relay interface-dlci [*útvonal azonosító száma*] – több útvonal azonosító is lehet, így többször is be kell írni ezt a sort, csak más-más dlci-vel

exit

A felhő konfigurálása pont-multipont Frame-Relay-nél.

A serial-os interfészeknél LMI kiválasztása (Cisco, ANSI, Q933a), DLCI-k felvétele.

Frame-Relay-es kapcsolatoknál (Connection – > Frame-Relay) az interfészek, DLCI-k összepárosítása.

**NAT, PAT - Network Address Translate, Port Address Translate**

**Statikus NAT:** router mögé rejtünk egy szervert, azaz az Internet felől, a router nyilvános címe alapján lehet elérni a belső hálózaton lévő, magán című szervert. Egy nyilvános címhez egy belső szolgáltatás tartozik.

int [*router külső lába*]

ip nat outside

exit

int [*router belső, szerver felöli lába*]

ip nat inside

exit

ip nat inside source static [*belső* *szerver magán címe*] [*router külső lábának nyilvános címe*]

**Port-forwarding**: egy nyilvános címhez több belső cím is tartozik, és a router azok között a portszámok alapján tud különbséget tenni.

int [*router külső lába*]

ip nat outside

exit

int [*router belső, szerver felöli lába*]

ip nat inside

exit

ip nat inside source static [*protokoll*] [*belső* *szerver magán címe*] [*portszám*] [*router külső lábának nyilvános címe*] [*portszám*]

**Dinamikus NAT:** belső hálózaton lévő magán IP című gépek **több**, a router külső lábához rendelt nyilvános IP címen keresztül érik el a külső hálózatot. Egyszerre annyian tudnak kimenni belülről, ahány nyilvános cím van.

int [*router külső lába*]

ip nat outside

exit

int [*router belső lába*]

ip nat inside

exit

ip nat pool [*nat pool név*] [*kezdő nyilvános IP cím*] [*záró nyilvános IP cí*m] netmask [*hálózati maszk*]

access-list [*normál ACL azonosító száma*] permit [*belső hálózat címe*] [*wild card maszk*]

ip nat inside source list [*normál ACL azonosító száma*] pool [*nat pool név*]

**PAT:** belső hálózaton lévő, magán IP című gépek (kliensek, szerverek, switchek stb.) a router külső lábának **EGYETLEN** nyilvános címével érik el az internetet. Ez van beállítva alapértelmezetten a SOHO routereknél.

int [*router külső lába*]

ip nat outside

exit

int [*router belső lába*]

ip nat inside

exit

access-list [*normál ACL azonosító száma*] permit [*belső hálózat címe*] [*wild card maszk*]

ip nat inside source list [*normál ACL azonosító száma*] interface [r*outer külső lábának azonosítója*] overload

**NAT eredményének megnézése:**

show ip nat translations

**ACL-k**

Címek megadásánál: **host [*IP cím*] = [*IP cím*] 0.0.0.0,**

több címnél: **[*IP cím*] [*wild card maszk*]**,

összes cím: **any**

**Normál (standard) ACL: azonosító szám: 1-99, 1300-1999**

Csak a forrás IP címe alapján tud szűrni, emiatt célszerű a **célhoz legközelebbi interfészhez** kell felvenni!

access-list [*ACL azonosító száma*] permit/deny host [*IP cím*] / [*IP cím*] [*wildcard maszk*] / *any*

ACL hozzárendelése interfészhez:

int [*interfész azonosítója*]

ip access-group [*ACL azonosító száma*] in / out

**Kiterjesztett (extended) ACL: azonosító szám: 100-199, 2000-2699**

Tud szűrni a forrás IP címe mellett a cél IP cím, cél port, forrás port illetve protokoll alapján is. A **forráshoz legközelebbi interfészhez** célszerű felvenni!

Operátorok portok megadásánál: eq – egyenlő; neq – nem egyenlő; gt – greater than, nagyobb mint; lt – less than, kisebb, mint.

access-list [*ACL azonosító száma*] permit/deny [*protokoll*] [*forrás* *IP cím*] … [*cél IP cím*] … [*operátor*] [*portszám*]

ACL hozzárendelése interfészhez ugyanúgy történik, mint a normál ACL-nél.

**Nevesített ACL:** nem rendelkezik sorszámmal, normál illetve kiterjesztett is lehet.

szöveg alapján könnyebb azonosítani az ACL-eket, mint szám alapján

ip access-list standard [*ACL neve*] vagy ip access-list extended [*ACL neve*]

ACL hozzárendelése interfészhez:

int [*interfész azonosítója*]

ip access-group [*ACL neve*] in / out

**Routerek redundanciája – FHRP – First Hop Routing Protocol**

**HSRP: Hot Standby Routing Protocol**

**Csak redundancia** – terheléselosztás nincs. Csak egy csoport van, ami lehet az alapértelmezett, 0-s számú, és amelyet nem kell külön kiírni. Egy aktív router van, és egy vagy több meleg tartalék.

int [*interfész azonosítója*]

**…**

standby ip [*virtuális átjáró IP címe*]

standby preempt – ha a parancs nincs kiadva, akkor az adott router nem lehet aktív

standby priority [*érték*] – alapértelmezett 100. A nagyobb értékű router lesz az aktív. 0 – 255

standby track [*interface azonosítója*] – ha ezen az interfészen nincs kapcsolat, akkor az aktív router a szerepét átruházza a sorban utána következőnek.

**Redundancia és terheléseloszlás.** Több csoport is van. Az egyik csoportban az A router aktív, a B meleg tartalék, a másik csoportban pont fordítva. A csoportok száma 0 és 255 közötti lehet.

int [*interfész azonosítója*]

**…**

standby ip [*csoport azonosító száma*] [*virtuális átjáró IP címe*]

standby [*csoport azonosító száma*] preempt

standby priority [*csoport azonosító száma*] [*érték*]

standby [*csoport azonosító száma*] track [*interface azonosítója*]

show standby

show standby brief

**Switch konfigurálása**

**Felügyeleti IP cím beállítása:**

int vlan *[vlan azonosító száma*]

ip add *[IP cím*] [*maszk*]

no shut

exit

ip default-gateway [*átjáró címe*]

ip name-server [*DNS szerver címe*]

**Vlan-ok létrehozása:**

vlan [*a vlan azonosító száma*]

name [*a vlan neve*]

exit

**VTP szerver konfigurálása – minden switch alapértelmezetten szerver:**

vtp mode server

vtp domain [*tartománynév*]

**VTP kliens konfigurálása:**

vtp mode client

vtp domain [*tartománynév*]

**Vlan-ok hozzárendelése porthoz – trunk:**

int [*interface azonosító*]

switchport mode trunk

switchport trunk allowed vlan [*vlan azonosító számok*]

exit

**Vlan hozzárendelése porthoz – access:**

int [*interface azonosító*]

switchport mode access

switchport access vlan [*vlan azonosító szám*]

exit

**Port-security – védekezés DHCP kiéheztetés (starvation) ellen:**

int [*interface azonosítója*]

vagy

int range [*interface-ek azonosítója*]

switchport mode access – csak access típusú portoknál lehet beállítani

switchport port-security – a port-security engedélyezése

switchport port-security max [*szám: 1-3072*] – hány db MAC címnek legyen engedélyezve a hozzáférés

switchport port-security violation [*protect | restrict | shutdown*]

*protect –* eldobja a más MAC című eszközről érkező keretet. Nem történik naplózás.

*restrict –* eldobja a más MAC című eszközről érkező keretet. Történik naplózás.

*shutdown –* lekapcsolódik a port, ha más MAC című eszközről érkezik keret. A támadás elhárítása után a rendszergazdának a portot először le kell állítania, majd el kell indítania.

switchport port-security mac-address *[sticky | MAC cím]*

sticky – a switch automatikusan megjegyzi az adott portra csatlakozó eszköz MAC címét

a második esetben a rendszergazdának kézzel kell felvinnie a MAC címet.

**DHCP snooping – csaló DHCP szerver kiszűrése:**

ip dhcp snooping – *engedélyezés*

ip dhcp snooping vlan *[vlan azonosító száma] –* vlan-hoz történő hozzárendelés

azoknak a portoknak a felsorolása, amelyeken keresztül történhet DHCP forgalom – akár szerver, akár kliens csatlakozik rá*.*

int [*interface azonosítója*]

vagy

int range [*interface-ek azonosítója*]

ip dhcp snooping trust

exit

**Etherchannel – portok, kapcsolatok aggregálása, összevonása**

Az LACP szabványügyi szervezetes, a PAgP Cisco-s

int range [*interfészek azonosítója*]

channel-group [*csoport azonosító száma*] mode active – LACP

vagy

channel-group [*csoport azonosító száma*] mode desirable – PAgP

exit

int port-channel [*csoport azonosító száma*]

switchport mode access

switchport access vlan [*azonosító száma*]

exit

**Konfigurációk megnézése, mentése, betöltése**

**Futó konfiguráció megnézése:**

show run

**Indító konfiguráció megnézése:**

show startup

**Futó (aktív - running) konfiguráció mentése az indító (startup) konfigurációba:**

write vagy copy run startup

**Indító konfiguráció betöltése a futó konfigurációba:**

copy startup run

**Indító konfiguráció mentése TFTP szerverre:**

copy startup tftp

**Indító konfiguráció betöltése TFTP szerverről:**

copy tftp startup

**MAC cím tábla megnézése:**

show mac-address-table

**Routing tábla megnézése:**

show ip route

**Fizikai illetve virtuális interface-ekhez rendelt IP címek megnézése:**

show ip int brief

**Flash tartalmának megnézése:**

show flash

**Másolás Flash-ről a TFTP szerverre:**

copy flash tftp

**HSRP beállításainak megnézése:**

show standby

**NAT, PAT fordítások megnézése:**

show ip nat translations