Projekt segédlet cisco

Tartalom

1.Alap beállítások

Hostname megadása:

(config)#hostname NAME

Konzol és telnet kapcsolatok jelszavainak megadása:

(config)#line console 0

(config-line)#password cisco

(config-line)#login

(config-line)#exit

(config)#line vty 0 5

(config-line)#password cisco

(config-line)#login

(config-line)#exit

Felhasználói névvel való belépés:

(config)#username admin privilege 15 secret cisco

(config)#line vty 0 15

(config-line)#privilege level 15

(config-line)#login local

Privilegizált (EXEC) üzemmód jelszavának (class) megadása:

(config)#enable secret 0 class

SSH engedélyezése:

(config)#hostname router1

(config)#ip domain-name teszt.hu

(config)#crypto key generate rsa

vagy:

(config)#crypto key generate rsa general-keys modulus 1024

(config)#ip ssh version 1 | 2

esetleg még:

(config)#ip ssh time-out 60 (mp-ben megadva)

(config)#ip ssh authentication-retries 2

(config)#username admin privilege 15 password 0 cisco

(config)#line vty 0 15

(config-line)#login local

(config-line)#transport input ssh

(config-line)#privilege level 15

Kulcs törlése:

(config)#crypto key zeroize rsa

IP útválasztás engedélyezése:

(config)#ip routing

Interfész konfiguráció (Ethernet, soros DCE és DTE interfész):

(config)#interface Ethernet 0

(config-if)#ip address 192.220.123.1 255.255.255.0

(config-if)#description LAN-kapcsolat

(config-if)#no shutdown

(config-if)#exit

(config)#interface Serial 0

(config-if)#ip address 193.155.145.2 255.255.255.0

(config-if)#encapsulation hdlc

(config-if)#clocl rate 64000

(config-if)#no shutdown

(config-if)#exit

(config)#interface Serial 1

(config-if)#ip address 188.15.70.1 255.255.255.0

(config-if)#encapsulation hdlc

(config-if)#no shutdown

(config-if)#exit

Mentés és törlés:

Konfiguráció mentése az NVRAM-ba:

#copy running-config startup-config

Konfiguráció mentése TFTP szerverre:

#copy running-config tftp

Konfiguráció visszatöltése TFTP szerverről:

#copy tftp running-config

Konfiguráció törlése az NVRAM-ból:

#erase startup-config

Újraindítás:

#reload

Enable jelszó beállítása:

Switch(config)#enable password jelszo

Enable titkos jelszó:

Switch(config)#service password-encryption

Virtuális terminálok jelszavainak beállítása:

Switch(config)#line vty 0 15

Switch(config-line)#password jelszo

Switch(config-line)#login

Napi üzenet beállítása (elválasztó karakter pl.:@):

Switch(config)#banner motd @Belepes csak engedellyel!@

Switch portok beállítása:

switch(config)#interface FastEthernet 0/2

switch(config-if)#duplex auto | half | full

switch(config-if)#speed auto | 10 | 100

MAC-cím statikus megadása adott porthoz:

switch(config)#mac-address.table static xxxx.xxxx.xxxx vlan 1 int f0/1

MAC-címtábla törlése:

switch#clear mac-address-table dynamic

Portbiztonság:

switch(config)#int fa0/1

switch(config-if)#switchport mode access

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

vagy általunk megadott címmel:

switch(config-if)#switchport port-security mac-address xxxx.xxxx.xxxx

switch(config-if)#switchport port-security violation shutdown

ha nem szeretnénk, hogy letiltson:

switch(config-if)#switchport port-security violation [protect | restrict]

Portbiztonság miatt letiltott port újraengedélyezése:

switch(config)#int fa0/1

switch(config-if)#shutdown

switch(config-if)#no shutdown

Porthoz leírás, megjegyzés fűzése:

switch(config)#int fa0/24

switch(config)#description Porthoz leiras

Felügyeleti IP-cím adása a kapcsolóknak:

switch(config)#int vlan 1

switch(config-if)#ip address 10.0.0.1 255.0.0.0

switch(config-if)#no shutdown

Alapértelmezett átjáró megadása:

switch(config)#ip default-gateway 10.0.0.254

Sikertelen bejelentkezések naplózása:

router(config)#login on-success log

router(config)#login on-failure log

Tartománynév beállítása:

router(config)#ip domain-name nev

2.Show parancsok

Aktív konfiguráció ellenőrzése:

router#show running-config

Verzió ellenőrzése:

router#show version

Forgalomirányítótábla ellenőrzése:

#show route

SSH ellenőrzése:

switch#show ip ssh

switch#show ssh

Időbélyeg ellenőrzése router-en:

router#show clock

NTP kliens működésének ellenőrzése:

router#show ntp associations

router#show ntp status

DHCP által kiosztott IP címek ellenőrzése:

router#show ip dhcp binding

DHCPv4 üzenetek küldése és fogadása:

router#show ip dhcp server statictics

Címkiosztás során IP cím ütközés ellenőrzése:

router#show ip dhcp conflict

Login parancs kimenetének ellenőrzése:

router#show login

Bejelentkezett felhasználók ellenőrzése:

router#show users

Hálózati címfordítás ellenőrzése:

router#show nat

Módosítási lista ellenőrzése:

router#show access-list autosec_firewall_acl

Hozzáférési lista és CBAC működésének ellenőrzése:

router#show access-list autosec_firewall_acl

router#show ip inspet all

router#show ip inspect sessions detail

EIGRP ellenőrzése:

router#show ip route

router#show ip protocols

router#show ip eigrp neighbors

router#show ip eigrp topology

router#show ip eigrp traffic

Beállított szabályok ellenőrzése:

router#show crypto isakmp policy

Titkosítási átvitel beállításának ellenőrzése:

router#show crypto ipsec transform-set

Beállított titkosítási térkép ellenőrzése:

router#show crypto map

Módosított hozzáférési lista ellenőrzése:

router#show access-lists autosec_firewall_acl

NAT ellenőrzése:

router# show ip nat translations

router#show ip nat statistics

RIP ellenőrzése:

router#show ip route

OSPF ellenőrzése:

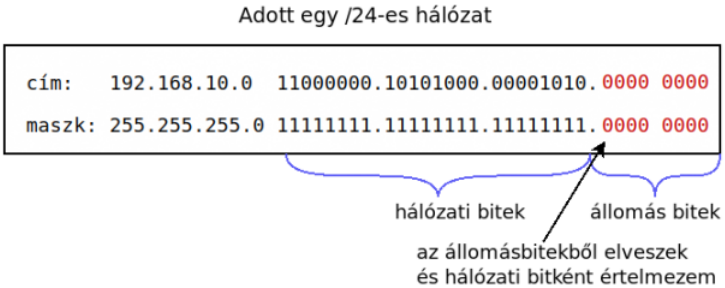
router#show ip ospf interface

router#show ip ospf neighboor detail

3.IP cím számítás

I. IP cím számolás egyenlő alhálózati maszkokkal

Alhálózatok képzése:



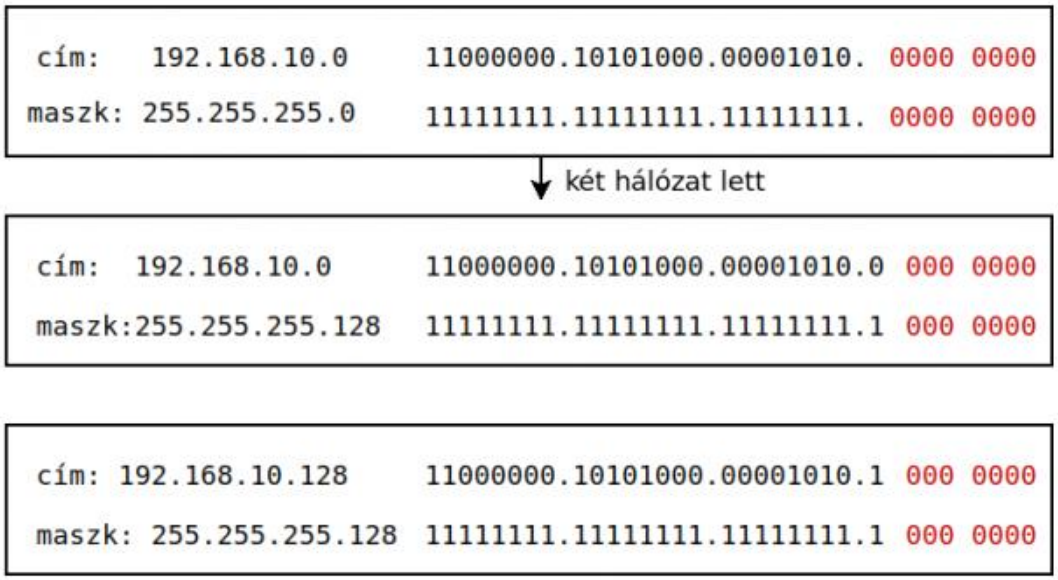
Első lépésként felírjuk a címet kettes számrendszerben.

Második lépésként felírjuk alá az alhálózati maszkot kettes számrendszerben.

Ahol csak nulla van mindkét részben azok az állomás bitek. A többi bitet hálózati biteknek nevezzük.

Ha az állomás bitekből elveszek egyet, és hozzáadom a hálózati bitekhez, akkor új alhálózati maszkot kapunk /25

Lett két /25-ös hálózat



Az újonnan kapott hálózat adatai:

- a hálózati maszk: 255.255.255.128
- CIDR jelzés: /25
- helyettesítő maszk: 0.0.0.127
- a két hálózatban az állomások száma összesen: 252
- 1. hálózat adatai:
  - hálózati cím: 192.168.10.0/25
  - első állomás címe: 192.168.10.1
  - utolsó állomás címe: 192.168.10.126 (nem szabály, de érdemes ezt a címet adni a router-nek)
  - szóráscím: 192.168.10.127
  - állomás: 126
- 2. hálózat adatai:
  - hálózati cím: 192.168.10.128/25
  - első állomás címe: 192.168.10.129
  - utolsó állomás címe: 192.168.10.254

- szóráscím: 192.168.10.255
- állomás: 126

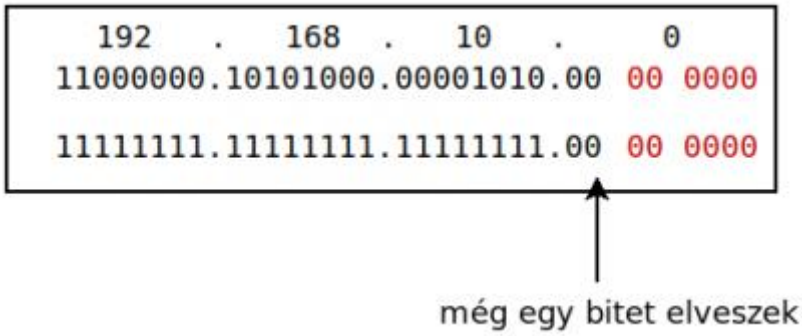
A hálózati címhez 1 bitet vettünk el 2^1 hatvány szóval 2, vagyis 2 alhálózatunk van. Az állomások számára 7 bit maradt ami 2^7=128, ebből elveszünk kettőt (hálózati címet és a szóráscímet így 126, azaz 126 gép lehet egy alhálózatban.

alhalozatokSzama=2^1=2

gepekSzama= 2^7-2=128

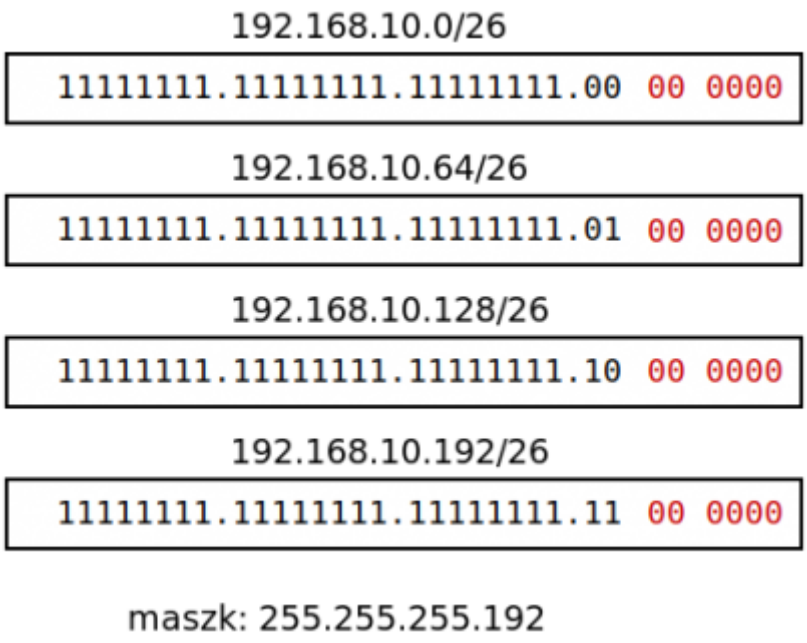
Ha több alhálózatra van szükségünk akkor több bitet kell elvennünk.

pl.:



alhalozatokSzama=2^2 = 4

gepekSzama=2^6-2=62



maszk: 255.255.255.192

1. hálózat:
    - hálózat: 192.168.10.0/26
    - első kioszthető: 192.168.10.1
    - utolsó kioszthető:192.168.10.62
    - szóráscím:192.168.10.63

2. hálózat:
    - hálózat: 192.168.10.64/26
    - első kioszthető: 192.168.10.65
    - utolsó kioszthető:192.168.10.126
    - szóráscím:192.168.10.127

3. hálózat:
    - hálózat: 192.168.10.128/26
    - első kioszthető: 192.168.10.129
    - utolsó kioszthető:192.168.10.190
    - szóráscím:192.168.10.191

4. hálózat:
    - hálózat: 192.168.10.192/26
    - első kioszthető: 192.168.10.193
    - utolsó kioszthető:192.168.10.254
    - szóráscím:192.168.10.255

Alhálózatszámítás általánosan:

alhalozatokSzama=$2^{elvettBitek}$

gepekSzama=$2^{megmaradtBitek}$-2

II. VLSM

Változó Hosszúságú Alhálózati Maszk

A VLSM a hálózati címzés egy módszere, amely lehetővé teszi, hogy a hálózatokat különböző méretű alhálózatokra osszuk fel.

Maszkok és az IP címek száma:

/30:

255.255.255.252
1 HC
1 BC
2 kiosztható IP cím

/29:

255.255.255.248
1 HC
1 BC
6 kiosztható IP cím

/28:

255.255.255.240
1 HC
1 BC
14 kiosztható IP cím

/27:

255.255.255.224
1 HC
1 BC
2 kiosztható IP cím

/26:

255.255.255.196
1 HC
1 BC
30 kiosztható IP cím

/25:

255.255.255.128
1 HC
1 BC
126 kiosztható IP cím

/24:

255.255.255.0
1 HC
1 BC
254 kiosztható IP cím

4.VLAN

A VLAN-ok szegmentációt és szervezeti rugalmasságot biztosítanak egy kapcsolt hálózaton belül. Az eszközök egy VLAN-on belül úgy kommunikálnak egymással, mintha ugyanarra a vezetékre csatlakoznának.

Az egyedi címzéses (unicast), a szórásos (broadcast) és a csoportcímzéses (multicast) csomagok is kizárólag azon végberendezésekhez lesznek továbbítva, amelyek a csomagok forrásához tartozó VLAN-on belül vannak. Más VLAN-ba tartozó állomásoknak címzett csomagokat olyan eszközön keresztül kell továbbítaniuk, amely a forgalomirányítást (routing) is támogatja.

VLAN-ok kialakítása során a hierarchikus hálózatcímzési terv megalkotását is figyelembe kell venni. A hierarchikus hálózatcímzés annyit jelent, hogy a hálózati szegmensekhez vagy VLAN-okhoz a hálózat egészét szem előtt tartva, rendezett módon, IP-alhálózatokat rendelünk.

Adat VLAN: Az adat VLAN-ok a felhasználó által generált forgalom elkülönítésére konfigurált VLAN-ok. Az adat VLAN-okat a hálózat felhasználói vagy eszközcsoportok alapján történő szétválasztására használjuk. A hang- és hálózatkezelési forgalom nem engedélyezhető az adat VLAN-okon.

Natív VLAN: A VLAN-ról érkező felhasználói forgalmat meg kell jelölni a VLAN-azonosítóval, amikor egy másik kapcsolóra kerül tovább küldésre. Egy 802.1Q trönkport egy 4 bájtos címkét helyez el az Ethernet keret fejlécébe, hogy azonosítsa azt a VLAN-t, amelyhez a keret tartozik. A címkézetlen forgalmat egy switch generálja, és származhat elavult eszközökből is. A Cisco switch-ek natív VLAN-ja a VLAN 1.

Felügyeleti VLAN: A felügyeleti VLAN egy olyan adat VLAN, amely kifejezetten hálózatkezelési forgalomra van konfigurálva, beleértve az SSH, telnet, HTTPS, http és SNMP protokollokat. Alapértelmezés szerint egy 2. rétegbeli switch-en a VLAN 1 felügyeleti VLAN-ként van konfigurálva.

Hangátviteli VLAN: A Voice over IP (VoIP) támogatásához külön VLAN-ra van szükség. A VoIP forgalom a következőket igényli: biztos sávszélesség a hangminőség biztosításához; az átviteli prioritás a többi hálózati forgalomhoz képest; lehetőség a hálózat zsúfolt területei körül történő továbbításra 150 ms-nál kisebb késleltetés a hálózaton.

A VLAN-ok nem lennének jól használhatóak VLAN trönkök nélkül. A VLAN trönkök biztosítják az összes VLAN forgalom terjedését a switch-ek között. A trönk egy pont-pont kapcsolat két olyan hálózati eszköz között, amelyek egynél több VLAN forgalmát is továbbítják.

VLAN létrehozása:

```
switch(config)#vlan 20

switch(config-vlan)#name student
```

```
switch(config-vlan)#end
```

Portok VLAN-hoz rendelése:

```
switch(config)#interface fa0/1
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 20
switch(config-if)#end
```

Trönkkonfiguráció:

```
switch(config)#interface fa0/1
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk native vlan 99
switch(config-if)#switchport trunk allowed vlan 10,20,30,99
switch(config-if)#end
```

Trönk visszaállítása alapértelmezett állapotra:

```
switch(config)#interface fa0/1
switch(config-if)#no switchport trunk allowed vlan
switch(config-if)#no switchport trunk native vlan
switch(config-if)#end
```

VLAN konfigurálása:

```
router(config)#interface g0/0/1.10
router(config)#description Default Gateway for VLAN 10
router(config-subif)#encapsulation dot1Q 10
router(config-subif)#ip address 192.168.10.1 255.255.255.0
router(config-subif)#exit
router(config)#interface g0/0/1.20
router(config-subif)#description Default Gateway for VLAN 20
router(config-subif)#encapsulation dot1Q 20
router(config-subif)#ip address 192.168.20.1 255.255.255.0
router(config-subif)#exit
```

router(config)#interface g0/0/1.99

router(config-subif)#description Default Gateway for VLAN 99

router(config-subif)#encapsulation dot1Q 99

router(config-subif)#ip address 192.168.99.1 255.255.255.0

router(config-subif)#exit

router(config)#interface g0/0/1

router(config-if)#description Trunk link to switch

router(config-if)#no shutdown

router(config-if)#end

5. SSH

A Secure Shell (SSH) egy biztonságos protokoll, amely a 22-es TCP-portot használja. Biztonságos (titkosított) felügyeleti kapcsolatot biztosít egy távoli eszközhöz. Az SSH-nak át kell vennie a Telnet szerepét a felügyeleti kapcsolatokat valósít meg.

SSH beállítása:

1. Ellenőrizni kell az SSH-támogatást. A show ip ssh paranccsal. Ha a kapcsoló által futtatott IOS nem támogatja a titkosítási funkciókat, akkor az eszköz ezt a parancsot nem fogja felismerni.
   switch#show ip ssh
2. Be kell állítani az IP domaint.
   switch(config)#ip domain-name cisco.com
3. RSA-kulcspárok létrehozása
   switch(config)#crypto key rsa 1024
4. Be kell állítani a felhasználói azonosítókat.
   switch(config)#username admin secret ccna
5. vty vonal konfigurálása
   switch(config)#line vty 0 15
   switch(config-line)#transport input ssh
   switch(config-line)#login local
   switch(config-line)#exit
6. SSH 2 engedélyezése

6.DHCP

A DHCPv4 (Dynamic Host Configuration Protocol v4) az IP-címek és egyéb hálózati beállítások dinamikus kiosztására szolgál. Mivel egy hálózatban a csomópontok túlnyomó részét asztali

számítógépek képezik, a DHCPv4 rendkívül fontos eszköz a hálózati rendszergazdák számára, amellyel rengeteg időt takaríthatnak meg.

A DHCPv4-szerver dinamikusan hozzárendel (bérbe ad) a klienshez egy címet a rendelkezésre álló készletből a szerver által meghatározott időre, vagy ameddig a kliensnek szüksége van rá.

A DHCPv4 ügyfél-kiszolgáló módban működik. Ha egy kliens kommunikációt folytat egy DHCPv4-szerverrel, a szerver egy IPv4-címet oszt ki vagy ad bérbe a kliensnek. A kliens ezzel a bérelt IP-címmel kapcsolódik a hálózatra, amíg a bérleti idő le nem jár. A bérleti idő meghosszabbításához a kliensnek rendszeres időközönként fel kell keresnie a DHCP-szervert. Ez a bérleti mechanizmus garantálja, hogy az áthelyezett vagy kikapcsolt kliensek ne tartsák meg azokat a címeket, amelyekre már nincs szükségük a továbbiakban. A bérleti idő lejárta után a DHCP-szerver gondoskodik arról, hogy a cím visszakerüljön az ismételten kiosztható címek készletébe.

DHCPv4 kiszolgáló konfigurálásának lépései:

1. Címek kizárása
   router(config)#ip dhcp excluded-address x.x.x.x x.x.x.x
2. A DHCPv4-készlet nevének megadása
   router(config)#ip dhcp pool pool-name
3. A készlet konfigurálása
   router(dhcp-config)#network x.x.x.x mask/prefix
   router(dhcp-config)#default-router x.x.x.x
   router(dhcp-config)#dns-server address x.x.x.x
   router(dhcp-config)# domain-name domain
   router(dhcp-config)#lease {days [hours[minutes]] | infinite}
   router(dhcp-config)#netbios-name-server address x.x.x.x

DHCP tiltása:

#no dhcpd auto_config outside

Ha automatikus IPv6-címzés van kiválasztva, az állomás megpróbálja automatikusan megszerezni és beállítani az IPv6-címadatokat az interfészen. Az állomás az interfészen kapott ICMPv6 (Internet Control Message Protocol version 6) protokoll router hirdetés (Router Advertisement, RA) üzenetben meghatározott három módszer egyikét fogja használni. Az állomással közös hálózaton található IPv6-router olyan RA üzeneteket küld, amelyek azt közlik az állomásokkal hogyan szerezhetik be IPv6-címzési információikat. Az állomás automatikusan létrehozza az IPv6 link-local címet az elindulásakor, amikor az Ethernet interfész aktívvá válik.

DHCPv6:

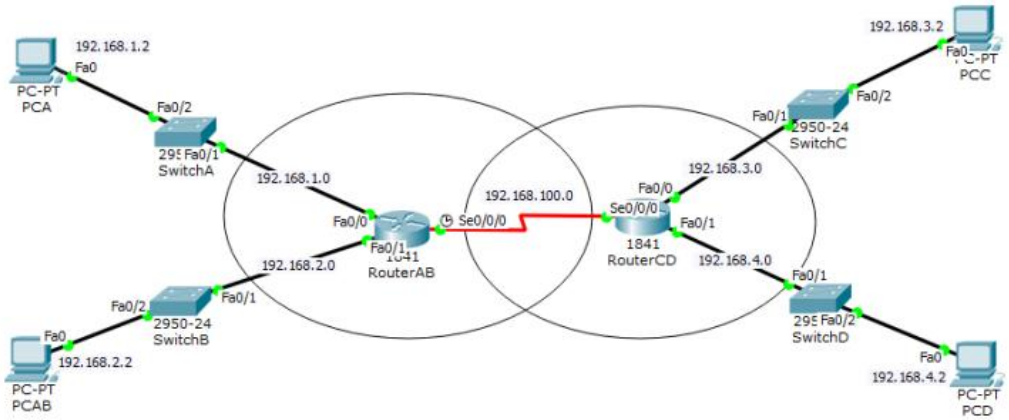
1. Engedélyezzük az IPv6 forgalomirányítást
   router(config)#ipv6 unicast routing

2. Adjuk meg a DHCPv6 készlet nevét
   router(config)#ipv6 dhcp pool IPV6
3. Állítsuk be a DHCPv6 készletet
   router(config-dhcpv6)#dns-server 2001.db8:acad:1::254
   router(config-dhcpv6)#domain-name example.com
   router(config-dhcpv6)#exit
4. Csatoljuk a DHCPv6 készletet egy interfészhez
   router(config)#int g0/0/1
   router(config-if)#ipv6 address fe80::1 link-local
   router(config-if)#ipv6 address 2001:db8:acad:1::1/64
   router(config-if)#ipv6 and other config-flag
   router(config-if)#ipv6 dhcp server IPV6-STATELESS
   router(config-if)#no shutdown
   router(config-if)#exit

7.RIP

Forgalomirányítási protokoll.

Példa:



Konfigurálás:

RouterAB(config)#router rip

RouterAB(config-router)#version 2

RouterAB(config-router)#network 192.168.1.0

RouterAB(config-router)#network 192.168.2.0

RouterAB(config-router)#network 192.168.100.0

RouterCD(config)#router rip

RouterCD(config-router)#version 2

RouterCD(config-router)#network 192.168.3.0

RouterCD(config-router)#network 192.168.4.0

RouterCD(config-router)#network 192.168.100.0

Valós idejű RIP kommunikáció megtekintése:

RouterAB#debug ip rip

RouterAB#undebug all

8.RIP VLAN

Forgalomirányítási protokoll.

Konfiguráció:

VLAN létrehozása

switch>enable

switch#configure terminal

S1(config)#vlan 10

S1(config-vlan)#exit

S1(config)#vlan 20

S1(config-vlan)#exit

S1(config)#vlan 30

S1(config-vlan)#exit

Portok VLAN-hoz rendelése

S1(config)#int f0/1

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 10

S1(config-if)#exit

S1(config)#int f0/2

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 20

S1(config-if)#exit

S1(config)#intf0/3

S1(config-if)#switchport mode access

S1(config-if)#switchport access vlan 30

S1(config-if)#exit

S1(config)#int f0/24

S1(config-if)#switchport trunk allowed vlan none

S1(config-if)#switchport trunk allowed vlan add 10

S1(config-if)#switchport trunk allowed vlan add 20

S1(config-if)#switchport trunk allowed vlan add 30

S1(config-if)#exit

Router konfiguráció:

R1(config)# int f0/0

R1(config-if)# no sh

R1(config-if)#exit

R1(config)# int f0/0.10

R1(config-if)# encapsulation dot1Q 10

R1(config-if)# ip address x.x.x.x x.x.x.x

R1(config-if)#exit

R1(config)#int f0/0.20

R1(config-if)#encapsulation dot1Q 20

R1(config-if)#ip address x.x.x.x x.x.x.x

R1(config-if)#exit

R1(config)#int f0/0.30

R1(config-if)#encapsulation dot1Q30

R1(config-if)#ip address x.x.x.x x.x.x.x

R1(config-if)#exit

R1(config)#exit

9.Forgalomirányítás

Statikus forgalomirányításnak négy típusa van:

- hagyományos statikus útvonal
- alapértelmezett statikus útvonal
- lebegő statikus útvonal

- összevont statikus útvonal

Hagyományos statikus útvonal beállítása:

router(config)#ip route network-address subnet-mask {ip-address | exit-interface} [distance]

router(config)#ipv6 route ipv6-prefix/prefix-length {ipv6-address | exit-interface} [distance]

Alapértelmezett statikus útvonal:

Akkor használunk alapértelmezett útvonalat, ha a hálózatunk szélső (edge, perem-) routerét konfiguráljuk, amely a szolgáltató hálózatához csatlakozik, vagy ha a routernek csak egyetlen felfelé irányú szomszédja van (stub router)

router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-interface)

router(config)#ipv6 route ::/0 {ipv6-address | exit-interface)

Lebegő statikus útvonalak:

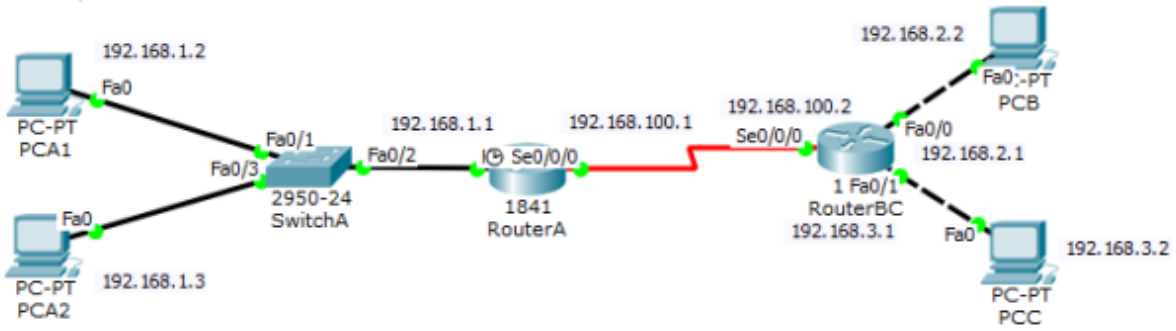
Ezek olyan statikus útvonalak, amelyek egy elsődleges statikus vagy dinamikus útvonal kapcsolatának kiesése esetén tartalék útvonalakat biztosítanak

10. Access Lists

A zárt lakóközösség őréhez hasonlóan a hálózati forgalom, amely egy hozzáférési listával (ACL) konfigurált interfészen halad át, engedélyezett és tiltott forgalomból áll. A router szekvenciális sorrendben összehasonlítja a csomagban lévő információkat a hozzáférési lista egyes bejegyzéseivel (ACE), hogy megállapítsa, a csomag illeszkedik-e valamelyikre. Ezt a folyamatot csomagszűrésnek nevezzük. A routerek a csomag fejlécében található információk alapján hozzák meg az útválasztási döntéseket. A router interfészeire érkező adatforgalom kizárólag az irányítótáblában szereplő információk alapján kerül továbbításra. A router összehasonlítja a cél IP-címét az irányítótáblában szereplő útvonalakkal, hogy megtalálja a legjobb egyezést, majd a csomagot a legjobb egyezés alapján továbbítja. Ugyanez a folyamat használható a forgalom szűrésére egy hozzáférési lista (ACL) segítségével.

Az ACL olyan IOS-parancsok sorozata, amelyek a csomagok szűrésére szolgálnak a csomag fejlécében található információk alapján. Alapértelmezés szerint a router nem rendelkezik semmilyen ACL beállítással. Azonban, ha egy ACL-t beállítunk egy interfészre, a router végrehajt az összes áthaladó csomagon egy további kiértékelő feladatot is, annak eldöntésére, hogy továbbítható-e az adott csomag.

Példa konfiguráció:



RouterBC csak PCA1 számára engedélyezi, a többi számára tiltja a hozzáférést, illetve engedélyezi RouterA útvonalfrissítéseit serial 0/0/0 irányból:

RouterBC(config)#access-list 1 permit 192.168.1.2

RouterBC(config)#access-list 1 permit 192.168.1.1

RouterBC(config)#access-lis 1 deny any

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

RouterBC(config-if)#ip access-group 1 in

PCC elérheti PCA1-t, de a többi eszközt nem:

RouterBC(config)#access-list 101 permit ip host 192.168.3.2 host 192.168.1.2

RouterBC(config)#access-list 101 deny ip any any

RouterBC(config)#interface fa0/0

RouterBC(config-if)#ip access-group 101 in

Csak PCB érheti el RouterA-t:

RouterA(config)#access-list 101 permit ip host 192.168.2.2 host 192.168.100.1

RouterA(config)#access-list 101 permit ip host 192.168.2.2 host 192.168.1.1

RouterA(config)#access-list 101 deny ip any host 192.168.100.1

RouterA(config)#access-list 101 deny ip any host 192.168.1.1

RouterA(config)#access-list 101 deny ip any any

RouterA(config)#interface fa0/0

RouterA(config-if)#ip access-group 101 in

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

RouterA(config-if)#ip access-group 101 in

PCA1 elérését tiltja RouterBC felé de megengedi neki PCA2 és RouterA elérését, nevesített kiterjesztett ACL-lel (kiterjesztett: extended, normál: standard)

RouterA(config)#ip access-list extended H1_limit_access

RouterA(config-ext-nacl)#deny ip host 192.168.1.2 host 192.168.100.2

RouterA(config-ext-nacl)#permit ip any any

RouterA(config)#interface s0/0/0

RouterA(config-if)#ip access-group H1_limit_access out

'A' hálózatnak tiltja a Telnet elérést RouterBC-re

RouterBC(config)#access-list 2 deny 192.168.1.0 0.0.0.255

RouterBC(config)#access-list 2 permit ip any any

RouterBC(config)#line vty 0 4

RouterBC(config-line)#access-class 2 in

RouterA tiltja az összes http kérést, ami RouterBC felöl jön:

RouterA(config)#access-list 101 deny tcp 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 80

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

RouterA(config-if)#ip access-group 101 in

11. NAT

A 209.165.201.11 IPv4-cím nyilvános és irányítható az interneten. Viszont, bármely olyan cím, amelynek első oktettjében a 10 szerepel, magán IPv4-címnek minősül és nem továbbítható az interneten. Ezért a router egy hálózati címfordításnak (Network Address Translation, NAT) nevezett folyamatot használ, hogy a privát IPv4-címeket interneten is továbbítható IPv4-címekké alakítsa. A NAT használatával egy privát (helyi) forrás IPv4-cím átfordítható egy publikus (nyilvános) címre. Bejövő csomagoknál a folyamat fordított irányban zajlik le. A router a NAT segítségével több belső IPv4-címet is képes nyilvános IP-címekre fordítani.

Statikus címfordítás: egy az egyhez típusú hozzárendelés a helyi és a globális címek között.
Dinamikus címfordítás: több a többhöz típusú hozzárendelés a helyi és a globális címek között.
Port címfordítás (Port Address Translation, PAT): több az egyhez típusú megfeleltetés a helyi és a globális címek között. Ezt a módszert túlterhelésként (NAT overloading) is ismerjük.

Statikus NAT konfigurálása:

1.lépés: Létrehozzunk egy leképezést a belső helyi cím és a belső globális cím között

interface type number
ip nat inside
interface type number
ip nat outside

2.lépés: A fordításban részt vevő interfészeket konfiguráljuk mint belső vagy külső interfészt, a NAT-hoz viszonyítva

interface type number
ip nat inside
interface type number
ip nat outside

3. lépés: A NAT beállításának ellenőrzése:

show ip nat translations

Dinamikus NAT konfigurálása:

1.lépés: Határozzuk meg a fordításhoz használandó címkészletet az ip nat pool paranccsal. Ez a címkészlet jellemzően nyilvános címek egy csoportja. A címek meghatározása a készlet kezdő IP-címe és az utolsó IP-cím megadásával történik. A netmask vagy prefix-length kulcsszó jelzi, hogy a címe és az utolsó IP-cím megadásával történik. A netmask vagy prefix-length kulcsszó jelzi, hogy mely címbitek tartoznak a hálózathoz és mely bitek tartoznak az állomáshoz a címtartományban.

ip nat pool name start-ip end-ip

2.lépés: Állítsuk be egy normál ACL-t kizárólag a lefordítandó címek azonosítására (engedélyezésére). Egy túl engedékeny ACL kiszámíthatatlan eredményekhez vezethet.

access-list access-list-number permit source [sourve-wildcard]

3.lépés: Rendeljük hozzá az ACL-t a címkészlettel. Az ip nat inside source list hozzáférési lista száma pool pool-neve paranccsal rendeljük hozzá az ACL-t a címkészlethez. Ezt a konfigurációt használja a forgalomirányító annak megállapítására, hogy melyik eszköz (list) melyik címet (pool) kapja meg

ip nat inside source list access-list-number pool name

4.lépés: Határozzuk meg, melyek a belső interfészek a NAT viszonylatban, azaz minden olyan interfészt, amely a belső hálózathoz kapcsolódik

interface type number

ip nat inside

5.lépés: Határozzuk meg, melyek a külső interfészek a NAT viszonylatban, azaz minden olyan interfészt, amely összeköt a külső hálózattal

interface type number

ip nat outside

Példa:

router(config)#ip access-list standard NAT-list

router(config-std-nacl)#permit host 192.168.20.1

router(config-std-nacl)#permit 192.168.20.128 0.0.0.127

router(config)#ip nat inside source list NAT-list interface Serial 0/0/0 overload

router(config)#interface s0/0/0

router(config-if)#ip nat outside

router(config)interface fa0/0.20

router(config-subif)#ip nat inside

12. Feszítőfa-protokoll (Spanning tree protocol)

A Spenning Tree Protocol (STP) egy hurok létrejöttét megelőző hálózati protokoll, amely redundanciát tesz lehetővé egy hurokmentes 2. rétegbeli topológia létrehozásakor. Az IEEE 802.1D az eredeti IEEE-féle MAC Bridging szabvány STP-hez.

Switch-en feszítő-fa protokoll beállítása úgy, hogy a switch legyen a fa gyökere.

switch(config)#spanning-tree vlan 1 priority 0

switch#show spanning-tree

13. Syslog

Amikor a hálózaton bizonyos események bekövetkeznek, a hálózati eszközökön megbízható mechanizmusok működnek, hogy a rendszergazdát részletes információkkal lássák el. Ezek az üzenetek lehetnek jelentéktelenek vagy kritikus fontosságúak is. A rendszergazdáknak számos lehetőségük van ezen üzenetek tárolására, értelmezésére és megjelenítésére. Figyelmeztetést kaphatnak azokról az üzenetekről is, amelyeknek nagy hatása van a hálózat infrastruktúrájára.

A leggyakoribb módszer a hálózati eszközök által biztosított rendszerüzenetekbe való betekintésre a syslog nevezetű protokoll.

A syslog protokollt UNIX-rendszerekhez fejlesztették ki az 1980-as években, de először az IETF által kiadott RFC 3164-ben dokumentálták 2001-ben. A syslog az 514-es UDP portot használja az eseményekről értesítő üzenetek IP-hálózatokon keresztül történő küldésére az üzenetgyűjtők felé.

A syslog protokollt számos hálózati eszköz támogatja, többek között routerek, switch-ek, alkalmazásszerverek, tűzfalak és más hálózati eszközök. A syslog protokoll lehetővé teszi a hálózati eszközök számára, hogy elküldjék a rendszerüzeneteket a hálózaton keresztül a syslog szerverhez.

A syslog naplózási szolgáltatásnak három fő funkciója van:

- Összegyűjti a naplóadatokat ellenőrzési és hibaelhárítási céllal.
- Kiválasztja a rögzítésre kerülő naplózási információk típusát.
- Megadja a célállomásokat a syslog üzenetek továbbításához.

Warning Level 4 - Emergency Level 0: Ezek az üzenetek szoftver- vagy hardver-meghibásodásból eredő hibaüzenetek; az ilyen típusú üzenetek azt jelentik, hogy a készülék működőképessége veszélyben van. Az esemény súlyossága határozza meg az aktuálisan alkalmazott syslog szintet.

Notification Level 5: Ez az értesítési szint normál, de jelentős eseményekre vonatkozik. Például interfészek elindulási vagy leállási üzenetei, valamint a rendszer-újraindítási üzenetek jelennek meg ezen a szinten.

Informational Level 6: Ez egy normál információs üzenet, amely nem befolyásolja az eszköz működését. Például, amikor egy Cisco eszköz elindul, a következő tájékoztató üzenet jelenhet meg: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.

Debugging Level 7: Ez a szint azt jelzi, hogy az üzenetek különböző debug parancsok eredményeképp jöttek létre.

Router beállítása mint syslog kliens:

```
router(config)#logging host 192.168.0.253

router(config)#logging trap debugging
```

Switch beállítása mint syslog kliens:

```
switch(config)#logging 192.168.0.253

switch(config)#logging trap debugging

switch(config)#service timestamps log datetime msec
```

14. NTP

Network Time Protocolt (NTP)

Idő és naptár szolgáltatások

Az NTP a 123-as UDP-portot használja és az RFC 1305-ben van dokumentálva.

Az NTP-hálózatok az időforrások hierarchikus rendszerét használják. Ebben a hierarchikus rendszerben a szinteket rétegnek vagy stratumnak nevezzük. A stratum szint (stratum level) a mérvadó forrástól levő ugrások száma. A szinkronizált időt NTP használatával terjesztjük el a hálózaton.

Az NTP-hálózat mérvadó időforrásokból szerzi be az időt. A 0-s stratumú eszközök, például az atom- vagy GPS-órák a legpontosabb mérvadó időforrások. Egészen pontosan a 0-s stratumú eszközök olyan időmérő eszközök, amelyeket pontosnak feltételezünk és kicsi vagy nulla késleltetéssel rendelkeznek.

Az 1-es stratumú eszközök olyan hálózati eszközök, amelyek közvetlenül kapcsolódnak a mérvadó időforrásokhoz. Elsődleges hálózati időforrásként működnek az NTP-t használó 2-es stratumú eszközök számára.

A 2-es stratumú szerverek hálózati kapcsolatokon keresztül csatlakoznak az 1-es stratumú eszközökhöz. A 2-es stratumú eszközök, például az NTP-kliensek, az 1-es stratumú szerverekhez szinkronizálják idejüket NTP-csomagokkal. Ezek működhetnek 3-as stratumú eszközök szervereiként is.

Konfigurálja a kiszolgálón futó NTP szolgáltatás használatára az R1 forgalomirányítót:

```
router(config)#ntp server 192.168.0.253

router(config)#ntp update-calendar
```

switch esetén:

```
switch(config)#ntp server 192.168.0.253
```

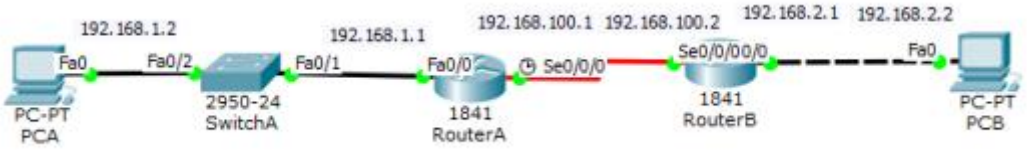
15. OSPF

OSPF (Open Shortest Path First)

Az OSPFv2 az IPv4-hálózatokhoz használatos. Az OSPFv3 pedig IPv6-hálózatokhoz való. egy kapcsolatállapot alapú irányító protokoll, amelyet a távolságvektor alapú RIP-protokoll leváltására fejlesztettek ki. A RIP a hálózatok és az internet korai időszakában elfogadható útválasztó protokollnak számított . Ugyanakkor az, hogy a RIP legjobb út meghatározásában egyedül az ugrásszámra támaszkodik, viszonylag korán problémássá vált. Az ugrásszám használata a különböző sebességű utakat is tartalmazó, kiterjedt hálózatok esetében nehezen skálázható. A RIP-pel szemben az OSPF lényeges előnye, hogy a nagyobb hálózatok esetében gyorsabb konvergenciát és méretezhetőséget biztosít.

Az OSPF olyan kapcsolatállapot alapú irányító protokoll, amely bevezeti a terület (area) fogalmát is. A hálózati rendszergazda feloszthatja az irányítási tartományt különálló területekre, ez elősegíti a frissítési forgalom kontrollálását. Kapcsolatnak nevezzük a router valamelyik interfészét. Kapcsolatnak számít a két routert összekötő hálózati szegmens, vagy a routerhez kapcsolódó felhasználói Ethernet LAN is. A kapcsolatok állapotának információja a kapcsolatállapot (link-state). Minden kapcsolatállapot információ tartalmazza a hálózati előtagot, az előtag hosszát és a költséget.

Példa konfiguráció:



Konfigurálás:

RouterA(config)#router ospf 1

RouterA(config-router)#network 192.168.1.0 0.0.0.255 area 0

RouterA(config-router)#network 192.168.100.0 0.0.0.255 area 0

RouterA(config-router)#log-adjacency-changes

RouterB(config)#router ospf 1

RouterB(config-router)#network 192.168.2.0 0.0.0.255 area 0

RouterB(config-router)#network 192.168.100.0 0.0.0.255 area 0

RouterB(config-router)#log-adjacency-changes

MD5 hitelesítés beállítása:

RouterA(config)#router ospf 1

RouterA(config-router)#area 0 authentication message-digest

RouterA(config)#interface s0/0/0

RouterA(config-if)#ip ospf message-digest-key 10 md5 secretpassword

RouterB(config)#router odpf 1

RouterB(config-router)#area 0 authentication message-digest

RouterB(config)#interface s0/0/0

RouterB(config-if)#ip ospf message-digest-key 10 md5 secretpassword

DR(nagyobb prioritás) és BDP (kisebb prioritás) választás:

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

RouterA(config-if)#ip ospf priority 25

RouterA#clear ip ospf process

RouterA#reload

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

RouterB(config-if)#ip ospf priority 50

RouterB#clear ip ospf process

RouterB#reload

Paraméterek beállítása:

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

Router(config-if)#bandwidth 64

Router(config)#ip ospf cost 2000

Statikus útvonal hirdetése:

Router(config-router)#default-information originate

16. DNS

A DNS (Domain Name System) egy olyan szolgáltatás, amely a domainnevek IP-címekké alakításáért felelős, lehetővé téve a webhelyek és online szolgáltatások elérését. Ezért, ha a DNS rosszul van konfigurálva vagy nem hatékony, az közvetlenül befolyásolhatja az internetkapcsolat sebességét és stabilitását.

Kiadható utasítások:

ip domain lookup

ip name-server

ip domain-list

ip domain name

ip ospf name-lookup

17. AAA

Az AAA a hitelesítés (Authentication), jogosultságkezelés (Authorization) és a naplózás (Accounting) rövidítése. Hozzáférés-szabályozás alapját biztosítják a hálózati eszközökön. Az AAA szabályozza, hogy ki férhet hozzá a hálózathoz (hitelesítés), mit csinálhat belépés után (jogosultságkezelés), és nyomon követi a használat során végrehajtott műveleteket (naplózás).

Az AAA-hitelesítés megvalósításának két gyakori módja a helyi- és a szerver alapú.

A lokális AAA helyben tárolja a felhasználóneveket és jelszavakat a hálózati eszközökön, például egy Cisco routeren. A lokális AAA ideális a kis hálózatok számára.

A szerver alapú módszer esetében a router egy központi AAA-szervert használ. A router a RADIUS (Remote Authentication Dial-In User Service) vagy a TACACS+ (Terminal Access Controller Access Control System) protokollt használja az AAA-szerverrel való kommunikációhoz. Több router és switch esetén a szerver alapú AAA a megfelelőbb.

Az AAA naplózás összegyűjti és regisztrálja a használati adatokat. Ezek az adatok aztán olyan célokra használhatók fel, mint az auditálás vagy a számlázás. Az összegyűjtött adatok közé tartozhatnak a kapcsolat megkezdésének és befejezésének időpontjai, a végrehajtott parancsok, a csomagok és a bájtok száma.

A naplózás elsődleges felhasználási módja az AAA-hitelesítéssel való kombinálás. Az részletes naplót vezet arról, hogy egy hitelesített felhasználó pontosan mit csinál az eszközön. Ez magában foglalja a felhasználó által kiadott összes EXEC módú és konfigurációs parancsot. A napló számos adatmezőt tartalmaz, többek között a felhasználónevet, a dátumot és az időt, valamint a felhasználó által beírt tényleges parancsot. Ezek az információk hasznosak az eszközök hibaelhárításakor. Emellett bizonyítékot szolgáltat arra az esetre is, ha valaki rosszindulatú cselekményeket hajt végre.

AAA engedélyezése:

```
router(config)#aaa new-model

router(config)#aaa authentication login default local none

router(config)#aaa authentication login SSH-lines local

router(config)#line vty 0 4

router(config-line)#login authentication SSH-lines
```

AAA nyomkövetés engedélyezése:

```
router#debug aaa authentication
```

AAA nyomkövetés tiltása:

```
router#no debug aaa authentication
```

18. RADIUS

A hitelesítő adatokat a RADIUS-kiszolgáló ellenőrzi. Így szükség esetén nyomon követhető és naplózható az egyéni felhasználói hozzáférés, és a fiókok központi helyről adhatók hozzá vagy módosíthatók. A WPA2 Enterprise hitelesítést használó WLAN-ok esetében RADIUS-kiszolgáló szükséges.

Forgalomirányítón RADIUS hitelesítés beállítása a console felhasználóinak:

router(config)#aaa new model

router(config)#aaa authentication login default group radius local none

router(config)#radius-server host 192.168.0.253 key 12345

Forgalomirányítón RADIUS hitelesítés beállítása a távoli felhasználóknak:

router(config)#aaa authentication login SSH-lines group radius

router(config)#line vty 0 4

router(config-line)#login authentication SSH-lines

19. Forgalomszűrés

Forgalomszűrésre használt ACL módosítása. Engedélyező szabályok felvétele az EIGRP unicast és multicast forgalom engedélyezésére:

router(config)#ip access-list extended autosec_firewall_acl

router(config-ext-nacl)#1 permit eigrp host 10.0.0.2 host 10.0.01

router(config-ext-nacl)#2 permit eigrp host 10.0.0.2 host 224.0.0.10

router(config)#ip access-list extended 101

router(config-list-nacl)#permit icmp host 192.168.0.1 host 192.168.20.1

router(config-list-nacl)#permit tcp host 192.168.0.1 eq 22 host 192.168.20.1 gt 1024

router(config-list-nacl)#permit udp host 192.168.0.1 eq 123 host 192.168.10.1 eq 123

router(config-list-nacl)#permit udp host 192.168.0.1 eq 514 host 192.168.10.1 eq 514

Forgalomszűrés beállítása úgy, hogy a külső hálózatba ne kerüljön ki csomag belső hálózati címmel.

router(config)#ip access-list extended 100

router(config-ext-nacl)#permit ip host 10.0.0.1 any

router(config)#interface serial0/0/0

router(config-if)#ip access-group 100 out

Belső hálózat forgalomszűrése:

router(config)#ip access-list extended 121

router(config-ext-nacl)#permit udp host 192.168.20.1 gt 1024 host 20.0.0.1 eq 53

router(config-ext-nacl)#permit udp 192.168.20.128 0.0.0.127 gt 1024 host 20.0.0.1 eq 53

router(config-ext-nacl)#permit tcp host 192.168.20.1 gt 1024 any eq www

router(config-ext-nacl)#permit tcp 192.168.20.128 0.0.0.127 gt 1024 any eq www

router(config-ext-nacl)#permit tcp host 192.168.20.1 gt 1024 host 192.168.20.254 eq 22

router(config)#interface fa0/0.20

router(config-subif)#ip access-group 121 in

router(config-ext-nacl)#permit udp host 20.0.0.1 eq 53 host 192.168.20.1 gt 1024

router(config-ext-nacl)#permit udp host 20.0.0.1 eq 53 192.168.20.128 0.0.0.127 gt 1024

router(config-ext-nacl)#permit tcp any eq www host 192.168.20.1 gt 1024

router(config-ext-nacl)#permit tcp any eq www 192.168.20.128 0.0.0.127 gt 1024

router(config-ext-nacl)#permit tcp host 192.168.20.254 eq 22 host 192.168.20.1 gt 1024

router(config)#interface fa0/0.20

router(config-subif)#ip access-group 122 out

Belső hálózaton csak NTP, Syslog és RADIUS protokollok legyenek engedélyezve:

router(config)#ip access-list extended 111

router(config-ext-nacl)#permit udp host 192.168.10.1 eq 1645 host 192.168.10.254 eq 1645

router(config-ext-nacl)#permit udp host 192.168.10.1 eq 123 host 192.168.10.254 eq 123

router(config)#interface fa0/0.10

router(config-subif)#ip access-group 111 in

router(config)#ip access-list extended 112

router(config-ext-nacl)#permit udp host 192.168.10.254 eq 1645 host 192.168.10.1 eq 1645

router(config-ext-nacl)#permit udp host 192.168.10.254 eq 514 host 192.168.10.1 eq 514

router(config-ext-nacl)#permit udp host 192.168.10.254 eq 123 host 192.168.10.1 eq 123

router(config)#interface fa0/0.10

router(config-subif)#ip access-group 112 out

Belső forgalomszűrés úgy, hogy csak az admin gépről lehessen pingelni:

router(config)#ip access-list extended 121

router(config-ext-nacl)#permit icmp host 192.168.20.1 host 192.168.20.254 echo

router(config-ext-nacl)#permit icmp host 192.168.20.1 host 192.168.10.1 echo

router(config)#ip access-list extended 122

router(config-ext-nacl)#permit icmp host 192.168.20.254 host 192.168.20.1 echo-reply

router(config-ext-nacl)#permit icmp host 192.168.10.1 host 192.168.20.1 echo-reply

router(config)#ip access-list extended 111

router(config-ext-nacl)#permit icmp host 192.168.10.1 host 192.168.20.1 echo-reply

router(config)#ip access-list extended 112

router(config-ext-nacl)#permit icmp host 192.168.20.1 host 192.168.10.1 echo

20. Switch Port Analyzer

A SPAN (Switch Port Analyzer) vagy a porttükrözés a Cisco Catalyst kapcsoló funkciója, amely lehetővé teszi a forrásportról vagy VLAN-ból érkező összes forgalom másolását a célfelületre.

Switch Port Analyzer aktiválása:

switch(config)#monitor session 1 source interface fa0/5 both

switch(config)#monitor session 1 destination interface fa0/6

21. Óra és időbélyegzés beállítása

Óra és időbélyegzés beállítása router-en:

router#clock set hh:mm:nn:YYYY

router(config)#service timestamps debug datetime msec

router(config)#enable secret cisco12345

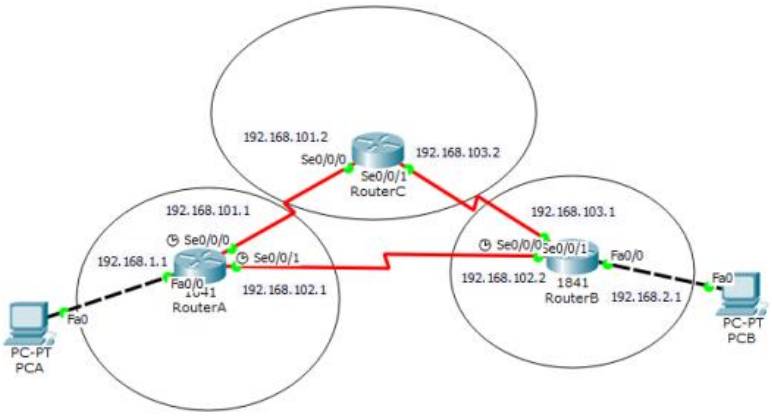
22. EIGRP

Enhanced Interior Gateway Routing Protocol rövidítése. Távolság alapú dinamikus útválasztó protokoll. IGRP helyett fejlesztették ki. VLSM és CIDR támogatása, hurokmentes és gyors konvergenciát alkalmaz.

EIGRP beállítása forgalomirányítón:

router(config)#router eigrp 101
router(config-router)#network 192.168.1.0 0.0.0.255
router(config-router)#network 10.1.1.0 0.0.0.3
router(config-router)#no auto-summary

Példa:



Konfigurálás:

RouterA(config)#router eigrp 100

RouterA(config-router)#no auto-summary

RouterA(config-router)#network 192.168.101.0

RouterA(config-router)#network 192.168.102.0

RouterA(config-router)#network 192.168.1.0

RouterB(config)#router eigrp 100

RouterB(config-router)#no auto-summary

RouterB(config-router)#network 192.168.102.0

RouterB(config-router)#network 192.168.103.0

RouterB(config-router)#network 192.168.2.0

RouterC(config)#router eigrp 100

RouterC(config-router)#no auto-summary

RouterC(config-router)#network 192.168.101.0

RouterC(config-router)#network 192.168.103.0

MD5 hitelesítés beállítása:

RouterA(config)#key chain discchain

RouterA(config-keychain)#key 1

RouterA(config-keychain-key)#key-string kul-cs

RouterA(config-keychain-key)#exit

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

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

RouterA(config-if)#ip aithentication key-chain eigrp 100 discchain

RouterA(config)#interface serial 0/0/1

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

RouterA(config)#ip authentication key-chain eigrp 100 discchain

Manuális útvonal összefogás:

Router(config)#interface s0/0/0

Router(config-router)#redistribute static

23. CBAC

AutoSecure funkció használata forgalomirányítón:

router#auto secure

Engedélyezett szolgáltatásokhoz ICMP és Telnet hozzáadása:

router(config)#ip inspect name autosec_inspect icmp timeout 5

router(config)#ip access-list extended autosec_firewall_acl

router(config-ext-nacl)#18 permit tcp any any eq 23

24. IPS-CBAC:

Védett hálózatot biztosít. Mindkét irányba figyeli a forgalmat. Csak az előre definiált forgalmat engedélyezi. A legtöbb tűzfal állapotteljes vizsgálat alapján működik (SPI). Kéretlen WAN csomagok bejutásának megakadályozása. Nyomon követi a cél géppel folytatott forgalmat. Alapja a biztonsági házirend, ami meghatározza a tűzfal viselkedését.

25. Internet Key Exchange (IKE)

Az Internet Key Exchange (IKE) egy kulcsfontosságú protokoll, amely a biztonságos kommunikáció alapját képezi a számítógépes hálózatokban. Elsődleges feladata, hogy biztonságos csatornát hozzon létre két fél között, lehetővé téve a titkosított adatok cseréjét. Ez a folyamat magában foglalja a kölcsönös hitelesítést és a titkosítási kulcsok generálását, amelyek elengedhetetlenek a bizalmas adatok védelméhez a nyilvános hálózaton, például az interneten.

Internet Key Exchange engedélyezése:

```
router(config)#crypto isakmp enable
```

Kulcsok élettartamának beállítása (példában egy óra):

```
router(config)#crypto isakmp policy 1
router(config-isakmp)#authentication pre-share
router(config-isakmp)#encryption aes 156
router(config-isakmp)#hash sha
router(config-isakmp)#group 5
router(config-isakmp)#lifetime 3600
```

26. AES algoritmus

Advanced Encryption System

A 802.1X az alapértelmezett kulcskezelési protokoll a RADIUS-kiszolgálóval történő kommunikációhoz.

Az AES a jelenlegi legerősebb titkosítási protokoll.

CCMP-t (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) használ, hogy a célállomás érzékelni tudja a titkosított és titkosítatlan adatokban menet közben történt változásokat.

Biztonsági beágyazási protokoll (ESP) AES 256 titkosítás használata SHA hitelesítéssel:

router(config)#crypto ipsec transform-set 1 esp-aes 256 esp-sha-hmac

router(config)#crypto ipsec security-association lifetime seconds 1800

27. ASA Tűzfal

Védett hálózatot biztosít. Mindkét irányba figyeli a forgalmat. Csak az előre definiált forgalmat engedélyezi. A legtöbb tűzfal állapotteljes vizsgálat alapján működik (SPI). Kéretlen WAN csomagok bejutásának megakadályozása. Nyomon követi a cél géppel folytatott forgalmat. Alapja a biztonsági házirend, ami meghatározza a tűzfal viselkedését.

Tűzfal beállítása, hogy figyeljen a kimenő csomagjainkra és engedje vissza a válaszokat

#class-map INSPECTION-DEFAULT

#match default-inspection-traffic

#exit

#policy-map GLOBAL-POLICY

#class INSPECTION-DEFAULT

#inspect icmp

#exit

#service-policy GLOBAL-POLICY global

28. DTP

DTP = Dynamic Trunking Protocol

A DTP felgyorsítja a hálózati konfigurációs folyamatot.

29. WAN

Wide Area Network

A LAN határain túli csatlakozáshoz szükséges. A WAN egy viszonylag nagy földrajzi területen átívelő távközlési hálózat.

Konfiguráció:

1. Alap router konfiguráció

    enable

    conf t

    hostname R1

    no ip domain-lookup

2. IP-cím beállítása
    int s0/0/0
    ip add x.x.x.x x.x.x.x
    clock rate 64000 (Csak a DCE oldalon)
    no sh
3. IP-cím beállítása ethernet interfészen
    int g0/0
    ip add x.x.x.x x.x.x.x
    no sh
4. Alapértelmezett statikus forgalomirányítás
    ip route 0.0.0.0 0.0.0.0 x.x.x.x
5. OSPF
    router ospf 1
    network HC(hálózati cím) 0.0.0.3 area 0
    network HC(hálózati cím) 0.0.0.255 area 0
6. EIGRP
    router eigrp 1
    network HC(hálózati cím) 0.0.0.3
    network HC(hálózati cím) 0.0.0.255
    no auto-summary
7. PPP konfiguráció (soros WAN, PPP bekapcsolása)
    int s0/0/0
    encapsulation ppp
8. Hitelesítés (CHAP)
    username R2 password cisco
    int s0/0/0
    encapsulation ppp
    ppp authentication chap
9. DHCP (Ha WAN végponton szükséges)
    ip dhcp pool SITE1
    network x.x.x.x x.x.x.x
    default-router x.x.x.x
    dns-server 8.8.8.8
10. NAT
    access-list 1 permit x.x.x.x x.x.x.x
    int g0/0 (WAN interfész)
    ip nat outside
    int g0/1 (LAN interfész)
    ip nat inside

ip nat inside source list 1 interface g0/0 overload

30. VPN

Virtuális magánhálózatok

VPN típusok: Site-to-Site, Remote access

VPN felhasználók többsége tűzfal mögött van

Site-to-Site:

1.Alapértelmezett útvonal beállítása:

R1(config)#ip route 0.0.0.0 0.0.0.0 x.x.x.x

2.IKE protokoll engedélyezése:

R1(config)#crypto isakmp enable

3.Ellenőrzéshez előre megosztott kulcsukat használ, ami SHA algoritmust használ, 1536 bites, AES algoritmus 256 bites kulcsokat használ, kulcsok élettartama 1 óra

R1(config)#crypto isakmp policy 1

R1(config-isakmp)#authentication pre-share

R1(config-isakmp)#encryption aes 256

R1(config-isakmp)#hash sha

R1(config-isakmp)#group 5

R1(config-isakmp)#lifetime 3600

4.Előmegosztott kulcsok beállítása:

R1(configI#crypto isakmp key cisco12345 address x.x.x.x

5.AES 256 titkosítás SHA hitelesítéssel

R1(config)#crypto ipsec transform-set 1 esp-aes 256 esp-sha-hmac

R1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

6.Titkosítási térkép létrehozása

R1(config)#crypto map CMAP 1 ipsec-isakmp

R1(config-crypto-map)#match address 100

R1(config-crypto-map)#set peer x.x.x.x

R1(config-crypto-map)#set pfs group5

R1(config-crypto-map)#set transform-set 1

R1(config-crypto-map)#set security-association lifetime seconds 900

R1(config-crypto-map)#exit

R1(config)#int s0/0/0

R1(config-if)#crypto map CMAP

Remote Access

1.Hitelesítési lista létrehozása

R1(config)#aaa new-model

R1(config)#aaa authentication login VPN-user group radius

R1(config)#aaa authorization network VPN-group group radius

2. RADIUS kiszolgáló elérhetőségének beállítása

R1(config)#radius server x.x.x.x

R1(config-radius-server)#address ipv4 x.x.x.x auth-port 1645

R1(config-radius-server)#key cisco

R1(config-radius-server)#exit

3.DHCP

R1(config)#ip local pool VPN-pool 192.168.1.129 192.168.1.253

4.Hitelesítés beállítása, SHA algoritmus, Diffie-Hellman algoritmus 1024 bites kulcsokkal, AES algoritmus, kulcsok élettartama 1 óra

R1(config)#crypto isakmp policy 1

R1(config-isakmp)#authentication pre-share

R1(config-isakmp)#encryption aes

R1(config-isakmp)#hash sha

R1(config-isakmp)#group 2

R1(config-isakmp)#lifetime 3600

5.VPN kliensek beállítása

R1(config)#crypto isakmp client configuration group VPN-group
R1(config-isakmp-group)#key ciscogroupvpn
R1(config-isakmp-group)#pool VPN-pool
R1(config-isakmp-group)#netmask 255.255.255.0

6.IPsec átviteeli paraméterek megadása

R1(config)#crypto ipsec transform-set 1 esp-des esp-sha-hmac

7.Titkosítási térképek létrehozása

R1(config)#crypto dynamic-map DMAP 1

R1(config-crypto-map)#set transform-set 1

R1(config-crypto-map)#reverse-route

R1(config)#crypto map SMAP client configuration address respond

R1(config)#crypto map SMAP client authentication list VPN-user

R1(config)#crypto map SMAP isakmp authorization list VPN-group

R1(config)#crypto map SMAP 1 ipsec-isakmp dynamic DMAP

R1(config)#int f0/1

R1(config-if)#crypto map SMAP

8.Forgalomszűrés

R1(config)#ip access-list extended bejovo

R1(config-ext-nacl)#permit udp any eq isakmp host x.x.x.x eq isakmp

R1(config-ext-nacl)#permit udp any eq non500-isakmp host x.x.x.x eq non500-isakmp

R1(config-ext-nacl)#permit tcp x.x.x.x 0.0.0.255 gt 1024 host x.x.x.x eq www

R1(configl)#ip access-list extended kimeno

R1(config-ext-nacl)#permit tcp host x.x.x.x eq www x.x.x.x 0.0.0.255 gt 1024

R1(config-ext-nacl)#exit

R1(config)#int f0/1

R1(config-if)#ip access-group bejovo in

R1(config-if)#ip access-group kimeno out

R1(config-if)#exit