Tartalom

Hálózat:

IPv6:

- Neighbor Discovery Protocol
    - Ez a protokoll IPv6-s környezetben építi ki és tartja fenn a kapcsolatot eszközök között
    - Használt ICMPv6 üzenetek
        - Router Solicitation | Router keresés
            - 133 ICMPv6 típus üzenet
            - Host eszköz csatlakozik egy IPv6-s környezetű hálózathoz
                - Legelső dolga lesz egy router-t találni, hogy attól információt kapjon
                - Az üzenetnek forrás címe az adott host eszköz MAC címe, cél címe `FF02::2`
                - Cím előtagot és egyéb konfigurációs információkat kér az indítás utáni automatikus konfiguráláshoz
        - Router Advertisement | Router hirdetés
            - 134 ICMPv6 típus üzenet
            - Router IPv6-s környezetben rendszeresen, 200 mp-ként, vagy RS üzenetre válaszként küld ilyet
            - Az üzenetnek cél címe `FF02::1`
            - Információkat hirdet benne
                - A hálózati előtagot és annak hosszát
                - A default gateway címét
                - DNS címeket és Domain neveket.
            - 3 féle módon lehet használni, erről bővebben a DHCPv6-ban
        - Neighbor Solicitation | Szomszéd keresés
            - 135 ICMPv6 típus üzenet
            - Mivel IPv6-s környezetben nincsen ARP, ezért NS és NA üzenettel fogják a különböző host eszközök megszerezni a szomszéd MAC címét
                - Ellenőrzik
                - Adott szomszéd elérhető-e
                - Van-e duplikált cím.
        - Neighbor Advertisement | Szomszéd hirdetés
            - 136 ICMPv6 típus üzenet
            - Az NS üzenet válasza
                - Megadja a saját MAC címét
                - A fogadó el tárolja a saját Neighbor Cache-ba.
        - Redirect | Átirányítás
            - 137 ICMPv6 típus üzenet

- Lényege az, hogy az adott host-t értesítse egy optimálisabb útvonalról a hálózatban
- Cím típusok
  - Unicast | Egyedi címek
    - Global Unicast Address | Globálisegyedi cím
      - A cím, amivel a saját alhálózatán kívülre tudd kommunikálni az eszköz
      - Felépítése
        - Global Routing Prefix | Globális útválasztási előtag
          - 48 bit
          - Az ügyfélnek azonosítója, amit az ISP-től kapott
        - Subnet ID | Alhálózati azonosító
          - 16 bit
          - Ez a 4. hextet, amivel alhálózatokat lehet létrehozni
          - Az ACAD érték mint Subnet ID oktatási célre van fenntartva
        - Interface ID | Interfész azonosító
          - 64 bit
    - Link-local Address | Helyi cím
      - A cím, amivel csak a saját alhálózatán belül tudd kommunikálni
      - Kötelező, hogy legyen
        - Ha nem adunk meg egyet, akkor az eszköz automatikusan generál magának
      - A Router Link-local Address-e lesz, az többi eszköznek a default-gateway-e
        - `FE80::/10` és `FEBF::/10` között terjed
  - Multicast | Csoportcímek
    - `FF02::2`
      - Csak routerek találhatók ebben a csoportban
    - `FF02::1`
      - „All nodes”
      - A hálózat összes eszköze ebben a csoportban van
    - `FF02::1:2`
      - Ebben a csoportban van az összes DHCPv6 szerver
  - Anycast | Bárki címek
- EUI64
  - Egy cím generálási technika, ahol az eszköz a saját MAC címét ketté vágja, középre egy FFFE értéket illeszt és a 7. bit-et pedig 1-re cseréli
    - Egyaránt van GUA-Interface-ID és Link-local-Address generálásban alkalmazva, bár manapság elavultnak minősül
- IPv6 cím adás
  - Manuális/Statikus
    - Cisco Packet Tracer-ben végeszközöknek
      - A config/desktop fülben tudunk IP címet, subnet mask-t, default gateway-t

és DNS-t adni.

- Cisco vendor switch-nek a native vlan-n
  - `SWv6(config)#sdm prefer dual-ipv4-and-ipv6 default`
    `SWv6(config)#do reload`

    `SWv6(config)#int <VLAN ID>vlan 1`
    `SWv6(config-if)#ipv6 add <IPv6 Address / Prefix>`
    `SWv6(config-if)#ipv6 add <IPv6 Link-Local Addres> link-local`
    `SWv6(config-if)#exit`
    `SWv6(config)#ipv6 route ::/0 <IPv6 Default Gateway Adddress>`
- Cisco vendor router-nek interface
  - `Rv6(config)#ipv6 unicast-routing`
    `Rv6(config)#int <Interface ID>`
    `Rv6(config-if)#ipv6 add <IPv6 Address / Prefix>`
    `Rv6(config-if)#ipv6 add <IPv6 Link-Local Address> link-local`

DHCPv6

- DHCPv6 szerverek UDP 547 portján figyelik a kliensek üzeneteit
- DHCPv6 kliensek UDP 546 portján küldik üzeneteiket
- 3 módszer van rá
  - Hogy melyiket használjuk, jelzőbitek diktálják
    - Jelzőbit
      - M
        - Managed Address Configuration flag
      - O
        - Other Configuration flag
- RA üzenet 3 módszere
  - SLAAC
    - Stateless address autoconfiguration | Állapot nélküli
    - M=0, O=0
    - A GUA címet a host egymaga hozza létre az RA üzenet alapján, nincs külső DHCPv6 server
  - DHCPv6 Stateless | Állapot mentes „vegyes módszer”
    - M=0, O=1
    - A host keres egy router-t RS-el
      - Válaszul kapott RA üzenet alapján elintéz mindent, amit tudd
        - A DNS információkat egy külön szervertől kell megtudnia
  - DHCPv6 Stateful | Állapottartó

- M=0
- Egy host felkeress egy router-t RS-el
  - Csak azt adja meg, hogy ő a default gateway és, hogy minden más információt egy Stateful DHCPv6 szervertől kell megtudnia.
    - Solicit
      - Ezt küldi a host a server-nek, hogy megszerezze a GUA és DNS információkat
      - A cél cím `FF02::1:2`
    - Advertise
      - A host Solicit üzenetére ezzel válaszól, és a kért információkat át adja a server
    - Request
      - Miután a host megkapta a címzése információkat, megerősíti őket egy Request-el
    - Reply
      - A szerver ezzel az üzenettel zárja a címzési folyamatot
        - Tartalmazza a szükséges címzési konfigurációkat és információkat
- DHCPv6 Options
  - Az IP címen túl nyúló extra konfigurációs opciók, amiket szerver szolgál a kliensnek, numerikus referencia értékei

Cisco

- Router
  - Stateless
    - Ha bekapcsoltuk az IPv6-s forgalomirányítást és konfiguráltuk a port-kat, csináljunk DHCP pool-t
      - `Routerv6(config)#ipv6 dhcp pool <Pool Name>`
      - Pool DNS szerver
        - `Routerv6(config-dhcpv6)#dns-server <DNS Server address>`
      - Pool domain név
        - `Routerv6(config-dhcpv6)#domain-name <Domain.Name>`
      - Mind ezután ki kell lépni a DHCP konfigurációjából, és be kell lépni abba a portba, amelyik arra a hálózatra mutat, amin szeretnénk a DHCPv6 szolgáltatás érvényesíteni, és a használt pool-t megadni
        - `Routerv6(config-if)#ipv6 nd other-config-flag`
          `Routerv6(config-if)#ipv6 dhcp server <Pool Name>`
  - Stateful
    - Ha bekapcsoltuk az IPv6-s forgalomirányítást és konfiguráltuk a port-kat, csináljunk DHCP pool-t
      - `Routerv6(config)#ipv6 dhcp pool <Pool Name>`
      - IPv6 cím tartomány
        - `Routerv6(config-dhcpv6)#address prefix <IP address/prefix>`

- Pool DNS server
  - `Routerv6(config-dhcpv6)#dns-server <DNS server address>`
- Pool domain név
  - `Routerv6(config-dhcpv6)#domain-name <Domain.Name>`
- Mind ezután ki kell lépni a DHCP konfigurációjából, és be kell lépni abba a portba, amelyik arra a hálózatra mutat, amin szeretnénk a DHCPv6 szolgáltatás érvényesíteni, és a használt pool-t megadni
  - `Routerv6(config-if)#ipv6 nd managed-config-flag`
    `Routerv6(config-if)#ipv6 dhcp server <Pool name>`

IPv6 címzés + dinamikus címkiosztás (SLAAC + DHCPv6)

- conf t
- ipv6 unicast-routing
- !
- interface g0/0
- description LAN
- ipv6 address 2001:db8:10::1/64
- ipv6 nd other-config-flag
- ipv6 dhcp server LANv6
- !
- ipv6 dhcp pool LANv6
- address prefix 2001:db8:10::/64
- dns-server 2001:4860:4860::8888
- domain-name lab.local
- end

Switch – VLAN-ok, access portok, trunk

- conf t
- !
- vlan 10
- name USERS
- vlan 20
- name SERVERS
- vlan 99
- name MANAGEMENT
- exit
- !
- interface range f0/1 - 10
- switchport mode access

- switchport access vlan 10
- !
- interface range f0/11 - 15
- switchport mode access
- switchport access vlan 20
- !
- interface f0/24
- switchport trunk encapsulation dot1q
- switchport mode trunk
- switchport trunk allowed vlan 10,20,99
- !
- interface vlan 99
- ip address 192.168.99.2 255.255.255.0
- no shutdown
- !
- ip default-gateway 192.168.99.1
- end

DTP

- Dynamic Trunking Protocol
  - Egy automatikus protokoll, ami switch-ek közötti kapcsolat létrehozását segíti
  - OSI Modell 2. réteg
  - Dynamic Auto/Desirable
    - Automata funkciók, amik vagy Access vagy Trunk összeköttetést teremt, ha csak nem találkozik egy nála magasabb üzemmóddal
    - Cisco vendor switch-en konfigurálás
      - `Swdtp(config)#int <Interface ID>`
        `Swdtp(config-if)#switchport mode <dynamic auto vagy dynamic desirable>`
  - Access
    - Nem tartalmaz tag-t az Ethernet frame-ben.
    - Hálózati kapcsolat, ami csak egy VLAN forgalmának továbbítását oldja meg egyetlen fizikai összeköttetésen keresztül
    - Cisco vendor switch-en konfigurálás
      - `Swdtp(config)#int <Interface ID>`
        `Swdtp(config-if)#switchport mode access`
        `Swdtp(config-if)#switchport access <VLAN ID>`
  - Trunk
    - Hálózati kapcsolat, amely lehetővé teszi több VLAN forgalmának továbbítását egyetlen fizikai összeköttetésen keresztül

- Cisco vendor switch-en konfigurálás
  - `Swdtp(config)#int <Interface ID>`
    `Swdtp(config-if)#switchport mode trunk`
  - VLAN-ID szűrés
    - `Swdtp(config-if)#switchport trunk allowed vlan <VLAN ID_1, VLAN ID_2, …>`
  - Native VLAN kijelölése
    - `Swdtp(config-if)#switchport trunk native vlan <Native VLAN ID>`
  - DTP egyeztetés kikapcsolása
    - `Swdtp(config-if)#switchport nonegotiate`

Router-on-a-stick – Inter-VLAN routing

- conf t
- !
- interface g0/0
- no shutdown
- !
- interface g0/0.10
- encapsulation dot1Q 10
- ip address 192.168.10.1 255.255.255.0
- !
- interface g0/0.20
- encapsulation dot1Q 20
- ip address 192.168.20.1 255.255.255.0
- !
- interface g0/0.99
- encapsulation dot1Q 99
- ip address 192.168.99.1 255.255.255.0
- !
- ip routing
- end

Második rétegbeli redundancia (STP, PortFast, BPDU Guard)

- conf t
- !

- spanning-tree mode rapid-pvst
- !
- spanning-tree vlan 1,10,20 priority 4096
- !
- interface range f0/1 - 10
- spanning-tree portfast
- spanning-tree bpduguard enable
- !
- interface range f0/23 - 24
- spanning-tree link-type point-to-point
- end
- - Bridge Protocol Data Unit
  - STA és STP folyamatok során használt frame, amivel a switch-k megosztják egymással az önmagukról és kapcsolataikról szóló információt
  - Minden BPDU tartalmaz egy BID-t
    - Bridge Identifier | Híd azonosító
    - Összesen 64 bit-s
    - 3 érték összegének eredménye
      - Bridge Priority | Híd prioritás
        - 4 bit
        - Az értéke 0 és 61440 közé eshet, 4096-s lépésekben
          - Az alapértelmezett érték az 32768
        - A legalacsonyabb értékű prioritást részesítjük előnyben
        - Cisco vendor switch-en konfigurálás
          - `Switchstp(config)#spanning-tree vlan <VLAN ID> priority <4096*X>`
          - `Switchstp(config)#spanning-tree vlan <VLAIN ID> root <primary vagy secondary>`
      - Extended System ID | Kiterjesztett rendszer-azonosító
        - 12 bit
        - A VLAN azonosítóval egyenlő érték
          - Ennek köszönhető, hogy ahány VLAN van egy hálózatban, annyi STP legyen
      - MAC Address
        - 48 bit
  - BPDUGuard
    - Egy portfast funkció
    - Megvédi az Access összeköttetéseket
      - Ha érzékkel egy BPDU-t, akkor lezárja azt a port-t
        - Fokozza a hálózat védettségét, mert nem kerül host-hoz fontos adat
    - Cisco vendor switch-en bekapcsolás

- `Switchstp(config)#spanning-tree portfast bpduguard default`

Etherchannel – portösszefogás

- PagP
  - Port aggregation Protocol
  - Cisco vendor protokoll
  - Üzemmódok
    - On → “Nonegotation”
    - Desirable → PagP frame küldése
    - Auto → PagP frame fogadása
- LACP
  - Link aggregation protocol
  - Nyílt szabvány, amit a piac a Cisco-tól tanult el
  - Üzemmódok
    - On → -||-
    - Active → -||-
    - Passive → -||-

Konfigurálás cisco vendor switch-en

- Switchport összefűzés
  - `Swec(config)#int range <Interface ID/X-Y>`
    `Swec(config-if-range)#channel-group <EtherChannel Group Number> mode active`
- Az összefűzött portok egészének konfigurációja
  - `Swec(config)#int Port-channel <EtherChannel Group Number>`

Dinamikus címkiosztás IPv4 (DHCP, DHCP Snooping)

- DHCPv4
  - A szerver konfigurálása több fajta módon is megoldható
    - Lehet parancssoros
      - `/ip/pool/add name=<PoolName> ranges=<Start IP address>-<Last IP address>`
      - `/ip/dhcp-server/network add address=<Network Address/prefix> gateway=<Gateway Address> dns-server=<DNS server address>`
      - `/ip/dhcp-server add name=<Name> interface=<Interface ID> address-pool=<PoolName> lease-time=<XY>`

- Lehet egy setup program keretében
  - `/ip dhcp-server/setup`
    `Select interface to run DHCP server on | Melyik interface a DHCPv4 server?`
    `dhcp server interface: <Interface ID>`

    `Select network for DHCP addresses | DHCPv4 cím tartomány?`
    `dhcp address space: <DHCP Address pool/prefix>`

    `Select gateway for given network | Alapértelmezett átjáró címe?`
    `gateway for dhcp network: <Gateway IP Address>`

    `Select pool of ip addresses given out by DHCP server | Kioszthatő címek?`
    `addresses to give out:<Start IP address>-<Last IP address>`

    `Select DNS servers | DNS szerver címe?`
    `dns servers:<DNS server address>`

    `Select lease time | Bérlési idő hossza?`
    `lease time:<X>`
- DHCP szerverek listázása
  - `/ip dhcp-server print`
- DHCP szerver törlése
  - `/ip dhcp-server remove <sorszám/#>`
- Interface DHCPv4 kliensé alakítása
  - `/ip dhcp-client add disabled=no interface=<Interface ID>`
- DHCPv4 kliensként kapott cím megtekintése
  - `/ip dhcp-client print`
- A router DHCP relay agent alakítása
  - `/ip dhcp-relay add interface=<megfelelő interface> dhcp-server=<DHCP szerver IP címe> local-address=<helyi IP cím>`
- DHCP pool-ok megjelenítése
  - `/ip pool print`
- DHCP pool törlése
  - `/ip pool remove <sorszám/#>`
- DHCP relay megjelenítése
  - `/ip dhcp-relay print`

- DHCP relay törlése
  - `/ip dhcp-relay  remove <sorszám/#>`

- A Services fül DHCP részében tudjuk a szolgáltatásnak adottságait beállítani
  - Új DHCP pool-t hozzunk létre az „Add” gombbal tudjuk hozzáadni az aktív pool-ok listájához
  - Meglévő pool-t akarunk szerkeszteni, akkor kiválasztjuk és átírjuk, és a „Save” gombbal mentünk
  - Ha törölni akarjuk az adott pool-t, akkor kiválasztjuk és a „Remove” gombot használjuk.
- Adott eszköznél, az IP config-ban statikusról DHCP-re kapcsoljuk
  - Ha minden jó, akkor „DHCP Request Succesful” felirattal együtt megkapja az eszköz az adatokat
- Külsős alhálózatba szóló DHCP címosztás bekapcsolása
  - Azon az interface-n kell megadni, ahol a cél alhálózat van
  - `Router0(config)#int <Inteface ID>`
    `Router0(config-if)#ip helper-address <DHCP Server address>`
- Router
  - Router-n konfigurált DHCP szolgáltatás erősen terheli az eszközt
  - CLI-ben kell megoldani mindent
  - Nem kiosztásra szánt ip cím(ek) megadása
    - `Router5(config)#ip dhcp excluded-address <Start IP address> <Last IP address (Ha többet akarunk egyszerre)>`
  - DHCP Pool létrehozása
    - `Router5(config)#ip dhcp pool <PoolName>`
    - Pool default gateway
      - `Router5(dhcp-config)#default-router <Default Gateway IP>`
    - Pool DNS
      - `Router5(dhcp-config)#dns-server <DNS Server address>`
    - Pool domain név
      - `Router5(dhcp-config)#domain-name <Domain.Name>`
    - Pool hálózat megadása
      - `Router5(dhcp-config)#network <IP Address> <Subnet Mask>`

- conf t
- !
- ip dhcp excluded-address 192.168.10.1 192.168.10.20
- !
- ip dhcp pool VLAN10

- network 192.168.10.0 255.255.255.0
- default-router 192.168.10.1
- dns-server 8.8.8.8
- domain-name lab.local
- !
- ip dhcp pool VLAN20
- network 192.168.20.0 255.255.255.0
- default-router 192.168.20.1
- dns-server 8.8.8.8
- end

Switch – DHCP Snooping

- DHCP Támadás
  - Legfőbb gyengepont
    - DHCP folyamat legelső lépése broadcast-t használ
      - Könnyű lefülelni
      - Legelső válaszra reagál, tehát könnyű átverni
  - Fajták
    - DHCP Starvation
      - A DHCP Pool-t folyamatos IP cím kérésekkel kiéheztetik
        - A támadó eszköze állandóan változtatja a MAC címet
        - Elfogynak az IP címek
    - DHCP Exhaustion
      - A DHCP Servert folyamatos IP cím kéréssel működés képtelenné teszik
        - Általában a Starvation után következik
    - DHCP Poisoning
      - A támadó lefüleli a DHCP kommunikációt és hamis válaszokat ad a DHCP kérésekre
    - Man in the middle
      - A támadó beékeli önmagát a hálózatba, adatot gyűjt, forgalmat eltereli, stb
    - Ha ez egyik össze jön, csak idő kérdése hogy a többi is össze jöjjön a támadónak
  - Megoldás
    - DHCP-Snooping
      - OSI Model 2. réteg
      - DHCP kérésekre csak beállított, megbízhatónak titulált port-ból fogad választ
  - Cisco vendor switch-en konfiguráció
    - Elindítás
      - `Snoopdog(config)#ip dhcp snooping`
    - Specifikus VLAN aktiválása
      - `Snoopdog(config)#ip dhcp snooping VLAN <VLAIN ID>`

- Megbízhatónak beállítani egy port-t
  - `Snoopdog(config)#int <interface ID>`
    `Snoopdog(config-if)#ip dhcp snooping trust`
  - Amikor ezt bekapcsoljuk, mindegyik másik port egyből nem megbízható lesz, muszáj nekünk külön-külön megadni
- Ha olyan switch-t használunk, ami nem egy DHCP-Relay-Agent vagy 3. szintű switch, akkor egy option 82 DHCP funkció miatt hiba keletkezik a topológiában. Eme probléma kikerüléséhez a következő parancs kell
  - `Snoopdog(config)#no ip dhcp snooping information option`

- conf t
- !
- ip dhcp snooping
- ip dhcp snooping vlan 10,20
- !
- interface f0/24
- ip dhcp snooping trust
- !
- interface range f0/1 - 15
- ip dhcp snooping limit rate 10
- end

Harmadik rétegbeli redundancia (HSRP)

- Hot Standby Router Protocol
  - Cisco vendor exclusive protokoll

Állapotok

- Initial
  - HSRP nem futt
  - Startup-kor, vagy konfigurációs változtatások után áll be
- Learn
  - Router próbálja a HSRP adatokat megtanulni egy authenticated hello-packet-ből
- Listen
  - A Router tudja a HSRP adatokat és passzívan további hello-packet-et vár más HSRP Router-ektől
- Speak
  - A Router Hello-packet-et küld, részt vesz a választási folyamatban és Standby vagy Active Router lesz belőle
    - HSRP Hello-Packet
      - Tartalmazz
        - HSRP Group ID

- Router Priority érték
- Virtuális Címek
- Md5-s authentikáció (ha konfiguráltál)
- Multicast address
- Version 1
- `224.0.0.2`
- Version 2
- `224.0.0.102`
- 1db/3mp

- Active
- Választás folyamat
- Legnagyobb HSRP Priority értékű router az Active egy csoporton belül
- Ha döntetlen, akkor a nagyobb IP cím tulajdonosa a győztes
- Ő tulajdonában áll a virtuális IP és MAC cím
- Virtuális IP
- A HSRP rendszer DG-e
- Manuálisan konfigurált
- Virtual MAC Address
- A HSRP rendszer MAC címe
- ARP-hez kell
- Automatikusan generált, de konfigurálható is
- Version 1
- `0000.0C07.AC<HSRP group ID Értékek>`
- Version2
- `000.0C9F.F<HSRP group ID értékek>`
- Ő végzi a forgalomirányítás feladatát
- Standby
- Tartalék router, ami akkor kezd acitve lenni, mikor az eredeti active kiesik
- Amikor tényleg kiesik az active, akkor egy hold-time mennyiségik vár mielőtt active lesz
- Hold Time = Hello Time * 3
- Amikor az Ex-Active router visszatér, az standby-ban fog működni

- Egy router több HSRP csoportnak is tagja lehet
- Adott virtuális HSRP csoport összes tagjában definiálni kell a különböző paramétereket

CLI

- HSRP engedélyezése
- `RHSRP(config-if)#standby <Group ID> ip <Virtuális IPv4 cím>`
- Preempt

- Ezzel tudjuk engedélyezni, hogy active router lehessen az eszköz, tehát a választás folyamatban részt vehessen, vagy hogyha kiesés után vissza kelljen vennie a szerepkört, akkor megtehesse azt
  - Ha nem adjuk ki akkor adott csoportban nem lehet active a router
  - `RHSRP(config-if)#standby <Group ID> preempt`
- Priority
  - A router HSRP priority értékének manuális megadása
  - Választás folyamatban fontos
  - Alapértelmezett érték 100
  - `RHSRP(config-if)#standby <Group ID> priority <Szám>`
- Standby Authentication
  - Ha megadjuk, a HSRP csoport összes router-én meg kell adni
  - Ezzel a max 8 karakteres szöveggel hitelesítik a hello-packet-et
  - Bármilyen router, ami nincs hitelesítve, nem fog tudni beleszólni az adott HSRP csoport működésébe
  - `RHSRP(config-if)#standby authentication md5 key-string <text>`
- Standby timers
  - Hello time és Hold time manuális konfigurációs parancsa
  - `HSRP(config-if)#standby <Group ID> timers <hello-timer értéke> <hold-timer értéke>`
- Version
  - Manapság a 2-s verziót használják gyakrabban, ugyanis annak van IPv6-s támogatása
  - `HSRP(config-if)#standby version <1-2>`
- Tracking
  - Amikor egy Active HSRP Router kiesik hálózati hiba miatt a hálózatból, akkor megtörténhet az, hogy a prioritás értékek mentén még mindig Active-nak van titulálva, hozzá irányul a forgalom, de mivel hibádzik, ezért a kommunikáció elakad
  - A HSRP Tracking-el lehet megoldani hogy dinamikusan alkalmazkodjanak a prioritás értékek egy másik objektumnak státusza/állapota alapján.
  - Interface kiesés esetén dinamikus csökkenés konfigurációja
  (- Az itt lévő példában HSRP az Active router, aminek `e0/0`-s interface a külvilág felé tekint, míg `e0/1`-s interface-n van konfigurálva az összes standby adat. Kiadjuk, hogyha kapcsolat szintű/interface szintű hiba alakul ki `e0/0`-n, akkor csökkentse `e0/1` prioritását `<X>`-el. Ha a HSRP topológia jól van konfigurálva, akkor a másik router, tegyük fel `HSRP2`, át fogja venni az Active státusz, hiszen nagyobb a prioritás értéke és preempt-elt)
  - `HSRP(config)#track <track ID> interface <Interface ID> line-protocol`
    `HSRP(config-tracK)#exit`

`HSRP(config)int <Inteface ID>`
`HSRP(config-if)# standby <Group ID> track <track ID> decrement <X>`

- Standby adatok lekérdezése
  - `HSRP#show standby`
- Stadnby track adatok lekérdezése
  - `HSRP#show track`
- Standby összeköttetés lekérdezése
  - `HSRP(config-if)#standby neighbors`

- conf t
- !
- interface g0/0
- ip address 192.168.10.2 255.255.255.0
- standby 1 ip 192.168.10.1
- standby 1 priority 110
- standby 1 preempt
- standby 1 authentication md5 key-string HSRPKEY
- end

Hálózatbiztonság – kapcsoló biztonságossá tétele

- Port biztonság
  - OSI Modell 2. rétegbeli technika
    - Switch
      - MAC tábla betöltéskor alapból üres, csak a switch port-ján keresztül menő adat alapján tölti ki
        - Korlátozott
          - Túlcsordulás
            - Úgy kezd működni a switch, mint egy hub
              - Küld mindent mindenhova
            - Előidézhető (Példa)
              - Egy támadó gép olyan programot használ, amivel állandóan változtatja a MAC címét
        - Védelem
          - MAC cím szűrés
            - Csak az engedélyezett MAC címeket engedje a hálózatra fel/tanulja meg
  - Konfigurálás cisco vendor switch-en
    - Elindítás
      - Ahhoz, hogy el tudd indítani mindenképpen Access üzemmódban kell lennie az adott port-nak
        - `Xmpl(config)#int <Interface ID>`

`Xmpl(config-if)#Switchport port-security`

- Mennyi MAC címet tanuljon meg az adott Port maximum
  - `Xmpl(config-if)#Switchport port-security maximum <szám>`
- Elfogadható cím megadása
  - Statikus módszer
    - `Xmpl(config-if)#Switchport port-security mac-addres <Eszköz MAC címe>`
  - Ragadós módszer
    - `Xmpl(config-if)#Switchport port-security mac-addres sticky`
- Vészhelyzetre hogyan reagáljon
  - `Xmpl(config-if)#Switchport port-security violation <mode>`
    - mode
      - `Protect`
        - Ez a leggyengébb, ezért rendszergazdáknak a legkényelmesebb
        - Megvédi a port-t, de semmi extrát nem végez
      - `Restrict`
        - Védi a port-t és eszközt
          - Feljegyzést is készít
            - Egyebet nem csinál viszont, de a feljegyzéssel a rendszergazda tudd manuálisan büntetni
      - `Shutdown`
        - Alapértelmezett
        - A legerősebb a három közül
          - Ez véd a legjobban, ezt a legmacerásabb visszafordítani
            - Adminisztratívan kapcsolja le az adott megrágalmazott port-t

- conf t
- !
- enable secret STRONGPASS
- !
- line vty 0 4
- transport input ssh
- login local
- !
- username admin secret STRONGADMINPASS
- !
- ip ssh version 2
- !
- interface range f0/1 - 10
- switchport mode access
- switchport port-security
- switchport port-security maximum 1

- switchport port-security mac-address sticky
- switchport port-security violation shutdown
- !
- no cdp run
- !
- service password-encryption
- end

Dinamikus routing

Open Shortest Path First

- Nyílt szabvány
- Verziók
  - v1
    - Elfeledett, csak papíron létezik valahol
  - v2
    - Ez tarolt a legnagyobbat
  - v3
    - Van benne IPv6

OSPF táblák

- Forgalom Irányító tábla
  - Az adott topológia számára legjobb útvonalat tartalmazza
  - Forwarding Database-ből képződik le
  - Megtekintés
    - Cisco vendor router-en
      - `R1#Show ip route`
- Topológia/Adatbázis tábla
  - Az adott topológiában lévő összes útvonalat tartalmazza
  - Link state database-ből képződik le
  - Megtekintés
    - Cisco vendor router-en
      - `R1#Show ip ospf database`
- Szomszédsági tábla
  - Link-State típusnak adottsága
  - A szomszéd router-el kapcsolatos adatokat tartalmazza
  - Adjacency Database-ből képződik le
  - Megtekintés
    - Mikrotik vendor router-en
      - `/routing/ospf/neighbor/print`

- Cisco vendor router-en
  - `R1#Show ip ospf neighbour`

OSPF Metric

- DIJKSTRA algoritmus
  - Ez az SPF alapú algoritmus cost érték alapján számol
    - Cost
      - Kábel minősége és típusától függő érték
      - Reference bandwidth / interface bandwidth
      - Útvonal választás befolyásolása
        - Reference bandwidth érték módosítása
          - Cisco vendor router-en
            - `R1(config-router)#auto cost reference-bandwidth <érték>`
        - Cost érték módosítása
          - Cisco vendor router-en
            - `R1(config-if)#ip ospf cost <érték>`
        - Interface sebességének módosítása
          - Cisco vendor router-en
            - `R1(config-if)#bandwidth <érték>`

OSPF indítási folyamat

- 1) Hello-zás
  - Hello packet-el felismerik egymást, közvetlen kapcsolatot felveszik a router-ek
    - Hello csomagokkal
      - Hello időzítő – Dead timer
        - 1db/10 sec – 1db/40 sec
          - Mindig 4x-nek kell lennie a Dead-nek a Hello-hoz képest
            - Ha különböznek a hálózat szétesik
        - Konfigurálhatók
          - Cisco vendor router
            - `R1(config-if)#ip ospf hello-interval <X>`
              `R1(config-if)#ip ospf dead-interval <X*4>`
- 2) Szomszédság kialakítása
  - Addig tart, amig mindenki meg nem ismerte a szomszédját
    - Eltanulják a szomszédok a saját szomszédjuk által ismert közvetlen hálózattokat
- 3) Távoli hálózatok megismerése
  - LSA elárasztás
- 4) Konvergencia
  - Addig tart, amig ki nem alakul a konvergens hálózat

- Konvergens hálózat olyan, amiben a routerek megismerik az összes fő és alhálózatot
- Csomagváltási folyamat/működés
  - R1 (DOWN) Hello → R2 (DOWN)
    - Hello tartalmazza az RID érteket és a szomszédokat
  - R1 (DOWN) ← Hello R2 (INIT)
    - Hello tartalmazza az RID értéket és a szomszédokat, amik közzé R1 most már tartozik
  - R1 (TWO-WAY) Hello → R2 (INIT)
    - Hello tartalmazza az RID értéket és a szomszédokat, amik közzé R2 most már tartozik
  - R1 (TWO-WAY) R2 (TWO-WAY)
    - Point-to-Point hálózatokban úgy alakít ki az OPSF szomszédsági viszonyt, hogy DR-t, illetve BDR-t nem választ
    - Multi access hálózatokban viszont itt dől el, hogy ki a DR és BDR
      - Designated Router és Backup Designated Router
        - LSA packet-ek és Broadcast üzenetek állandó kommunikációja terheli és veszélyezteti a hálózatot
          - Ha csak egy router-nek kell figyelni és jelezni a topológiai változásokat, akkor az megoldás
            - Designated Router
              - Választási módok
                - Router-ID
                  - Egy 32 bit-s cím
                    - Hierarchikus beosztottságot lehet megadni
                    - Minél nagyobb, annál közelebb áll a DR státuszhoz
                  - Manuálisan megadható
                    - Cisco vendor router-en
                      - `R1(config-router)#router <ID-érték>`
                - Loopback-Interface
                  - Virtuális interface
                    - Tesztelésre használják
                  - Ha nincsen RID értéke a router-nek, akkor alkalmazza ezt
                  - Forgalomirányító táblában megtekinthető
                    - Cisco vendor router-en
                      - `R1(config)#Interface loopback`
                - Fizikai interface IP címe
                  - A legnagyobb értékű IP címet fogja választani, akkor ha nincsen se megadott RID, se loopback interface
            - A DR versenyben 2. helyezett lesz a Backup Designated Router
  - R1 (EXSTART) R2 (EXSTART)

- Eldöntik ki lesz a Master és Slave router RID értékek alapján (minél nagyobb annál jobb)
- R1 (EXCHANGE) R2 (EXCHANGE)
  - A Master router elindítja a TYPE 2-s ospf csomagok cseréjét
- R1 (LOADING) R2 (LOADING)
  - LSR, LSU és LSAck csomagok cseréjével a szomszédok egyeztetnek egymás között
- R1 (FULL) R2 (FULL)
  - Konvergens hálózatban, készen álló OSPF területben lévő router-ek

OSPF Area

- Single Area
  - Egyterületű OSPF
  - area 0
- Multi-Area
  - Többterületű OSPF
  - Olyan hálózatban érdemes használni, ahol sok a forgalomirányító
  - Előny
    - Kisebb forgalomirányító táblázatok
    - Gyorsabb konvergencia
    - Csökkentett hálózati forgalom
  - Router fajták
    - DR / BDR
    - Internal router
      - Olyan router-ek, amiknek összes aktívan alaklmazott interface-i ugyanazon area-nak részei.
    - Area border router
      - Olyan router-ek, amiknek összes aktívan alkalmazott interface-i legalább kettő különböző area-nak részei
        - Összekötik a topológia internal router-eit
    - Backbone router
      - Minden olyan router, ami az area 0-hoz tartozik
      - Multi-Area OSPF Backbone
        - Ez az area 0
        - A különböző OSPF area-k közötti forgalomirányításért felel, ez a gerinc/központ
          - Minden más területnek valahogyan csatlakoznia kell hozzá
          (- VLAN közötti forgalomirányítás esetében is mindenkinek el kell érnie a natív VLAN-t, hogy működjön a kommunikáció. Ez olyasmi. Az egész többterületű OSPF-nek egy dezignált központi OSPF területe, ami mindenkit számontart és ki-be-köztes kommunikációt biztosít számukra. (Ezért is van az, hogy egy területű OSPF-ben

area 0-t alkalmazunk))
- Autonomous System Border Router
- Olyan router, ami külső forgalomirányítás információt importál be az OSPF topológiába.

OSPF packet
- TYPE 1
  - Hello packet
    - Szerepet kap az OSPF szomszédsági kapcsolatok felépítésében
    - Karbantartáskor is szokták használni
- TYPE 2
  - DBD
    - Database Descriptor Packet | Adatbázis leíró packet
    - Ez a packet biztosítja az adatbázis szinkronizációt az OSPF-ben résztvevő routerek között
- TYPE 3
  - LSR
    - Link State Request Packet | Kapcsolatállapot kérés packet
    - Ezzel tudja egy router lekérdezni a szomszéd egy konkrét kapcsolat állapotát
- TYPE 4
  - LSU
    - Link State Update Packet | Kapcsolatállapot frissítés packet
    - Az előbb említett LSR lekérdezésekre ezekben az LSU packet-ben érkezik a válasz
- TYPE 5
  - LSAck
    - Link State Acknowledgment | Kapcsolatállapot nyugta packet
    - Ezzel nyugtázza egy router a kapott LSU-t

OSPF LSA
- Link State Advertisement packet-ek
  - LSDB táblázatba kerülnek
    - Link State Database
- Fajták
  - TYPE 1
    - Router LSA
    - Egy területen belül az összes router 1-1 ilyennel árasztja el a területet
    - Tartalmazza
      - Milyen interface-i vannak, és azokhoz milyen hálózat csatlakozik
        - Egy interface IP prefix
        - Link type

- Fajták
  - 1
    - Point-to-point kapcsolat
    - Link ID
      - Neighbor router ID
  - 2
    - Transit hálózathoz kapcsolat
    - Link ID
      - DR IP címe
  - 3
    - Stub hálózathoz kapcsolat
    - Link ID
      - IP hálózat
  - 4
    - Virtuális link
    - Link ID
      - Szomszéd router ID
- TYPE 2
  - Network LSA
  - Multi-access hálózatokban jön létre
    - Egy area-ban belül maradnak
  - DR generálja őket
  - Itt fel van tüntetve az összes router, aki a hálózathoz/területhez csatlakozik, a DR hálózati adatai, a prefixek és SM-ek
- TYPE 3
  - Summary LSA
  - Area Border Router hozza létre őket
  - Többi területbe árad el, nem ott ahol létrejött
    - Többterületű OSPF-nél így tudják a különböző területek router-ei a „külső” router-k prefixeit
    - Nagyobb elárasztások esetén érdemes lehet egy címösszevonást konfigurálni, ezzel a terhelést picit leveszük az ABR és Internal Router eszközökről
- TYPE 4
  - Summary ASBR LSA
  - Ez a router a TYPE 1 LSA üzenetében kicserél egy bit-t, hogy így azonosítsa magát az OSPF tagok előtt
  - Az az ABR eszköz generálja, aki egy adott area-n belül van az ASBR router-el
    - Az OSPF-ből kivezető ASBR eszköz elérési adatait hírdeti
- TYPE 5
  - Autonomous system external LSA
  - Az ASBR eszköz által tovább osztott külsős router prefixe

OSPF Hitelesítés

- Fajták
  - NULL
    - Effektíve nincsen, ez az alapértelmezett
  - Plain Text
    - Minimális biztonságot nyújt
      - Egyszer kell csak megfelelően lefülelni
    - Oktatási célra van használva inkább
  - MD5-key
    - Leggyakoribb
    - Biztonságos
  - HMAC-SHA
    - Ritkább módszer
    - Legbiztonságosabb
- Kivitelezés
  - Area Authentication
    - Globális szint
      - Az érintett eszközökön és interface-en is ki kell adni
      - Plain text
        - Cisco vendor router-en
          - `R1(config)router ospf <PID>`
            `R1(config-router)#area <Area ID> authentication`
            `R1(config-router)#exit`
            `R1(config)#int <Interface ID>`
            `R1(config-if)#ip ospf authentication-key <LINE>`
            `R1(config-if)#ip ospf authentication`
      - MD5-key
        - Cisco vendor router-en
          - `R1(config)#router ospf <PID>`
            `R1(config-router)#area <Area ID> authentication message-digest`
            `R1(config-router)#exit`
            `R1(config)#interface <Interface ID>`
            `R1(config-if)#ip ospf message-digest -key <Key Number> md5 <LINE>`
            `R1(config-if)#ip ospf authentication message-digest`
  - Interface szint
    - Két router közötti összeköttetés két végében kell kiadni
    - Plain text
      - Cisco vendor router-en
        - `R1(config)#int <Interface ID>`

```
R1(config-if)#ip ospf authentication
R1(config-if)#ip ospf authentication-key <LINE>
R1(config-if)#ip ospf authentication
```

- MD5-key
  - Cisco vendor router-en
    - `R1(config)#int <Interface ID>`
      `R1(config-if)#ip ospf message-digest-key <Key Number> md5 <LINE>`
      `R1(config-if)#ip ospf authentication message-digest`

OSPF szolgáltatás beállítása

- OSPFv2
  - Cisco vendor
    - Indítás
      - `Ttrl(config)#route ospf <process ID>`
    - Ismert hálózat megadása
      - `Ttrl(config-router)#network <IPv4 cím> <wild-card SM> area <area ID>`
    - Passzívitás kiadása
      - A hálózat kevesebbé van terhelve és veszélyeztetve, ha a host hálózatokban nincsen OSPF
      - `Ttrl(config-router)#passive-interface <Host network port>`
    - OSPF hálózatból ki és be kommunikáció
      - Ha hálózat topológiában az egyik router OSPF terület része, a másik pedig nem
        - `R1(config)#router ospf <PID>`
          `R1(config-router)#default-information originate`
        - `RISP(config)#ip route <OSPF topológia össze vont CIDR címe> <SM> <R1 IPv4 cím>`
    - OSPF Authentikációt hagyjuk legutoljára, hogy könnyebben tudjunk minden mást javítani
  - Mikrotik vendor
    - `/routing/ospf/instance add name=<InstanceName> router-id=<x.x.x.x> version=2`
    - `/routing/ospf/area add name=<AreaName> instance=<InstanceName> area-id=0.0.0.0`
    - `/routing/ospf interface-template/add interface=<valami> area=<AreaName> passive`
    - `/routing/ospf interface-template/add interface=<valami> area=<AreaName>`
    - OSPF folyamathoz rendelt interface-k lekérdezése

- `/routing/ospf/interface print`
- OSPF folyamathoz rendelt területek lekérdezése
- `/routing/ospf/area print`
- OSPF folyamathoz rendelt interface szabványok lekérdezése
- `/routing/ospf/interface-template print`

- OSPFv3
- IPv6 bekapcsolása
- Cisco vendor router-en
- `R1(config)#ipv6 unicast-routing`
- OSPFv3 bekapcsolása
- Cisco vendor router-en
- `R1(config)#ipv6 router ospf <process ID>`
  `R1(config-router)#router-id <RID>`
- OSPFv3 konfigurálása esetén ha csak IPv6-t használunk, és IPv4-t egyáltalán nem, akkor mindenképpen kell router ID-t beállítani
- A default-information originate, passive-interface és hasonlók ugyanúgy megvannak
- Interfész hozzáadása az ospf folyamathoz
- Cisco vendor router-en
- `R1(config)#interface <Interface ID>`
  `R1(config-if)#ipv6 address <ipv6 cím>`
  `R1(config-if)#ipv6 address <ipv6 cím> link-local`
  `R1(config-if)#ipv6 ospf <process ID> area <area ID>`
- Timer beállítása
- Cisco vendor router-en
- `R1(config-if)#ipv6 ospf hello-interval <X>`
  `R1(config-if)#ipv6 ospf dead-interval <X*4>`

- conf t
- router ospf 1
- router-id 1.1.1.1
- network 192.168.10.0 0.0.0.255 area 0
- network 10.0.0.0 0.0.0.3 area 0
- end

Statikus és dinamikus címfordítás (NAT, PAT)

Ez a fajta címfordítás egy adatcsomagnak csak a harmadik rétegbeli részében, a packet-ben lévő adatokat fordítja/módosítja

Static

- Egyértelmű fordítás egy darab Privát és Publikus IPv4 cím között
  - Mivel 1 Privát = 1 Publikus, valójában nem éri el az IP cím fogyasztás csökkentését, pusztán nagyobb hatáskörű kommunikációt engedélyez
- Belső végeszközt és annak erőforrásait külsősen elérhetővé teszi
- A statikus NAT használata azon esetekben előnyös, amikor kívülről egy fix IP-címről egy szerver állandóan elérhető kell, hogy legyen.
- Kétirányú
  - Az adatforgalom át van fordítva, függetlenül attól, hogy kívülről vagy belülről van kezdeményezve
    - Bejövő adatforgalomnak a cél címét fordítja
    - Kimenő adatforgalomnak a forrás címét fordítja

Konfigurálás

Cisco

- ```
  RSNAT(config)#int <Interface ID>
  RSNAT(config-if)#ip nat inside
  RSNAT(config-if)#exit
  RSNAT(config)#int <Interface ID>
  RSNAT(config-if)#ip nat outside
  RSNAT(config-if)#exit
  RSNAT(config)#ip nat inside source static <Privát IPv4 cím> <Publikus IPv4 cím>
  ```

Dynamic

- A rendszergazda megadja a fordítandó Privát címek halmazát, valamint azokat a Publikus címek halmazát, amikre kell fordítani. Azt, hogy melyik Publikus cím kerül melyik Privát címhez (hol a „keresztmetszet”) a NAT-ást végző eszköz dönti el helyzet függően.
  - Mivel 1 Privát = 1 Publikus, valójában nem éri el az IP cím fogyasztás csökkentését, pusztán nagyobb hatáskörű kommunikációt engedélyez plusz könnyebb, mert nem kell egyesével megadni SNAT-t
- Kétirányú, ameddig a kommunikáció aktív
- Ha nagyobb a fordítandó címek halmaza, mint a fordításhoz használt címek halmaza, akkor könnyen futunk kommunikációs elakadásba
  - Tegyük fel van 4 eszköz, ami interneten akar kommunikálni, de a router csak 3 Publikus címet tudd ehhez nyújtani. Ha mind a 4 akar egyszerre csevegni, valamelyiknek várakoznia kell.

Konfigurálás

Cisco

- ```
  RDNAT(config)#int <Interface ID>
  RDNAT(config-if)#ip nat inside
  ```

```
RDNAT(config-if)#exit
RDNAT(config)#int <Inteface ID>
RDNAT(config-if)#ip nat outside
RDNAT(config-if)exit
RDNAT(config)#access-list <ID v. Name> permit <Privát IPv4 cím halmaz> <WSM>
RDNAT(config)#ip nat pool <pool name> <1. Publikus IPv4 cím> <Utolsó Publikus IPv4 cím> netmask <SubnetMask>
RDNAT(config)#ip nat inside source list <ID v. Name> pool <pool name>
```

PAT

- Port Address Translation
- Ez a fajta címfordítás egy adatcsomagnak a negyedik és harmadik rétegbeli részében, tehát a segment-ben és packet-ben lévő adatokat egyaránt fordítja/módosítja

Static

- Egyértelmű fordítás több Privát és egy Publikus IPv4 cím valamint azokhoz csatolt port-ok között
  - Mivel port-kat is fordít, ezért alkalmas IP cím fogyasztás csökkentésére
    - Két Privát című szerver használhatja ugyanazt a Publikus címet, két különböző port számmal
- Belsős végeszköznek adott port-át és ahhoz fűződő erőforrásokat külsősen elérhetővé teszi
- Kétirányú
  - Az adatforgalom át van fordítva, függetlenül attól, hogy kívülről vagy belülről van kezdeményezve
    - Bejövő adatforgalomnak a cél adatait fordítja
    - Kimenő adatforgalomnak a forrás adatait fordítja
- Engedélyezi a nem standard port-ok használatát
  - Lehetséges, hogy adott eszköznek szolgáltatásához nem a szabványos port szám van rakva, hanem valami egyedi
    - A port fordítás segítségével a megfelelő számra, legyen az szabványos vagy sem, át lehet fordítani, és így elérhetővé válik számunkra
      - Például a „weboldal.com” a 8080 port-n van, nem a szabványos 80 számon. A statikus PAT-al ez nem jelent problémát, nem kell a végfelhasználónak külön emlékezni és beírnia az egyedi port számot, a fordítás megoldja ezt számunkra.

Port forwarding

(- Ritkán „Hole Punching”-nak is hívják)

- Mivel a elsősorban a fordításhoz megadott port számot nézi az eszköz, így csak azok lesznek átengedve
  - Tehát az előző példában felhozott „weboldal.com”-t tároló szerver :22 port

számához fűződő erőforrásokat nem fogják elérni, ha mi csak a 8080-t adjuk meg a fordításhoz.

Konfigurálás

Cisco

-
```
RSPAT(config)#int <Interface ID>
RSPAT(config-if)#ip nat inside
RSPAT(config-if)#exit
RSPAT(config)#int <Interface ID>
RSPAT(config-if)#ip nat outside
RSPAT(config-if)#exit
RSPAT(config)# ip nat inside source static <protocol> <Privát IPv4 cím> <port szám> <Publikus IPv4 cím> <port szám>
```

Dynamic

- A rendszergazda megadja a fordítandó Privát címek és ahhoz kapcsolódó port-ok halmazát, valamint azokat a Publikus címek és port-ok halmazát, amikre kell fordítani. Azt, hogy melyik Publikus cím és port kerül melyik Privát címhez és port-hoz (hol a „keresztmetszet”) az DPAT-ást végző eszköz dönti el helyzet függően.
- Egyirányú
  - Külsős információt nem tudd befogadni, csak belsősen kezdeményezhető kapcsolat DPAT-on keresztül
    (- Természetesen ha megfelelően összekombináljuk egy SPAT-al például, akkor ez kiküszöbölhető)
- Több Privát végeszköz osztozkodhat ugyanazon az egy darab Publikus címen
  - A fordítás során, az újonnan kapott címnek mindig egyedi port száma lesz, így az összes megkülönböztethető
    - Ha nem így lenne, és fordítás végeredményében megtartaná az alap port számot, nagyon könnyen előfordulhatna, hogy egyező port számok miatt akadás alakulna ki, mert az adott eszköz nem tudná eldönteni, hogy melyikhez továbbítsa az adatokat.

Konfigurálás

Cisco

-
```
RDPAT(config)#int <Interface ID>
RDPAT(config-if)#ip nat inside
RDPAT(config-if)#exit
RDPAT(config)#int <Interface ID>
RDPAT(config-if)#ip nat outside
RDPAT(config-if)#exit
RDPAT(config)#access-list <ID v. Name> permit <Privát IPv4 cím halmaz> <WSM>
```

```
RDPAT(config)#ip nat inside source list <ID v. Name> interface <Interface ID>  overload
```

Policy NAT

- A fordítási folyamatot nem csak a forrás, hanem a cél adatok is befolyásolják
  - Előbb összeméri az eszköz, hogy melyik célhoz passzol a fordítási opciók közül, majd pedig SNAT, DNAT, SPAT vagy DPAT-t alkalmaz
    (- Ezen opciók mindegyike csak a forrás adatot módosítja)

Twice NAT

- Egyaránt fordítja át a forrás és cél adatokat
  - Például, van 10 kliens, akik alapértelmezetten a 8.8.8.8-as DNS cím felé néznek, de a mi céges szerverünk címe 32.8.3.1. Mind a 10-t egyesével átkonfigurálni is egy opció. Viszont az is egy kézre eső opció, hogy Twice NAT-al megadjuk az eszköznek, hogy külön-külön NAT fordítási technikával érintse a forrás adatokat és cél adatokat, az alapján, hogy mikkel érkezett az eszközhöz az adatcsomag.
    (- Így képes egyszerre átfordítani a Privát forrás címet, a publikus cél címet, és esetleges port-kat is akár)

NAT adatok lekérése

Cisco

- `R1#show ip nat translation`

Kivitelezési példák

Cisco

Static 1:1 hozzárendelés

-
```
RNAT(config)#ip nat inside source static 192.168.1.100 200.200.200.10
RNAT(config)#int gig0/0
RNAT(config-if)#ip nat inside
RNAT(config-if)#exit
RNAT(config)#int gig0/1
RNAT(config-if)#ip nat outside
```

Dynamic 1:N hozzárendelés

-
```
RNAT(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RNATconfig)#ip nat pool Ceg 200.200.200.20 200.200.200.30 netmask 255.255.255.0
RNAT(config)#ip nat inside translation source list 1 pool Ceg
RNAT(config)#int gig0/0
```

```
RNAT(config-if)#ip nat inside
RNAT(config-if)#exit
RNAT(config)#int gig0/1
RNAT(config-if)#ip nat outside
```

PAT hozzárendelés

```
-RPAT(config)#access-list 1 permit 192.168.1.0 0.0.255
 RPAT(config)#ip nat inside source list 1 interface gig0/1 overload
 RPAT(config)#int gig0/0
 RPAT(config-if)#ip nat inside
 RPAT(config-if)#exit
 RPAT(config)#int gig0/1
 RPAT(config-if)#ip nat outside
```

Statikus

- conf t
- interface g0/0
- ip address 192.168.10.1 255.255.255.0
- ip nat inside
- !
- interface g0/1
- ip address 203.0.113.1 255.255.255.248
- ip nat outside
- !
- ip nat inside source static 192.168.10.10 203.0.113.10
- end

Dinamikus NAT + PAT (overload)

- conf t
- access-list 1 permit 192.168.10.0 0.0.0.255
- !
- interface g0/0
- ip nat inside
- !
- interface g0/1
- ip nat outside
- !
- ip nat inside source list 1 interface g0/1 overload
- end

WAN technológiák – PPP alap (soros link)

Point-to-Point Protocol

- OSI Model 2. réteg
- Két soros/serial kábellel összekötött kábel router között valósul meg
- Kapcsolatminőségi-kezelési szolgáltatásokat nyújt
- Encapsulation HDLC
  - High Level Data Link Control
    - Cisco eszközökön alapértelmezett ősrégi PPP szabvány
      - 0 hitelesítés, és PPP-hez mérve kevesebb funkció
      - Bár lehet más cégtől származó eszközökön is HDLC-t állítani, a cisco saját fabrikálása miatt nem lesz kompatibilis
        - Valamint bár lehet HDLC-t is alkalamzni, nem nagyon éri meg, mert több szempontból hiányos és elmaradott
          - Interface encapsulation csere cisco vendor router eszközön
            - `R1(config-if)#encapsulation ppp`

            (- Ahhoz, hogy a két router közötti konfigurációnak megfelelőnek és megegyezőnek kell lenni, különben az interface protocol down, tehát nem működő képes állapotban lesz és a kapcsolat megakad)

- Főbb részei
  - LCP
    - Link Control Protocol
    - Kapcsolat felépítése
  - NCP
    - Network Control Protocol
    - IPv4 és v6 címkezelés
- Képes nyilvános IPv4 címet hozzárendelni az előfizetőhöz
  - Feltéttel, hogy sikeres hitelesítéssel igazolnia kell magát a fizető

PAP

- Password Authentication Protocol
- A kapcsolat kiépítés legelején folyik le a hitelesítés
  - Felhasználó név és jelszó páros átküldésre kerül
    - Az információ csere nincsen titkosítva
      - Egyszerű konfigurálni de egyáltalán nem megbízható
- Konfiguráció cisco vendor router-en
  - Logikája az, hogy adott eszközön létrehozod a túloldali router adatai szerint a felhasználót, és ugyanazon router saját adatait pedig a pap parancson keresztül átküldöd a túloldalinak
    - `R1(config)#username <R2 Device Name> password <Password>`

      `R1(config)#int <Interface ID>`

```
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authenticaiton pap sent-username
<R1 Device Name> password <Password>
```

- `R2(config)#username <R1 Device Name> password <password>`

```
R2(config)#int <Interface ID>
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap sent-username
<R2 Device Name> password <Password>
```

CHAP

- Challenge Handshake Authentication Protocol
- Kapcsolat kiépítés legelején folyik le a hitelesítés, valamint onnantól kezdve időszakosan újra-újra lefolyik
- Szerver küld egy Challenge-t
- A kliens erre válaszul küld egy hash kódot
- A felhasználónév és jelszó párosával lehet a kód helyességét ellenőrizni
- Nehezebb konfigurálni (a PAP-hez mérve), de mivel nem kerül küldésre a felhasználó név és jelszó, azok így titkosítottak, és ezért biztonságosabb
- Konfiguráció cisco vendor router-en
- Logikája, hogy a túloldali eszköz adatait és a közös jelszót konfiguráljuk, aztán pedig tudatjuk az interface-el, hogy chap hitelesítést alkalmazzon
(- Ugyebár azért a túloldalit, mert a hitelesítéskor a saját user adatok alapján generálja a hash-t, amiket a túloldali eszköz szintén azon saját adatai által kapott hash-el egyeztett össze)

- `R1(config)#username <R2 Device Name> password <Password>`

```
R1(config)#int <Interface ID>
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
```

- `R2(config)#username <R1 Device Name> password <Password>`

```
R2(config)#int <Interface ID>
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

PPoE

- PPP over Ethernet
- Ebben az esetben már Ethernet/UTP kábelen keresztül, tehát párhuzamos adattovábbításon keresztül valósul meg
- Ethernet frame-be csomagol PPP funkcionalitást
- Fejlettebb/Korszerűbb mint a PPP

- Állapotok
  - Discovery
    - PADI
      - PPoE Active Discovery Initation
      - A kliens ezt kiküldi, hogy megtalálja a PPPoE szervert
    - PADO
      - PPPoE Active Discovery Offer
      - A szerver válaszol az adataival a PADI üzenetre
    - PADR
      - PPPoE Active Discovery Request
      - A kliens kér egy PPPoE session-t a szervertől
    - PADS
      - PPPoE Active Discovery Session-Confirmation
      - Szerver igazolja a session, kiszab rá egy ID értéket
  - Session
    - LCP
      - Kapcsolat kiépítés
    - NCP
      - 3. rétegbeli funkciókat és protokollokat szabályozz
    - Authentication
      - Hitelesítés
  - PADT
    - PPPoE Active Discovery Termination
    - Vagy a kliens vagy a szerver kiküldi, hogy a PPPoE session-t lezárják
- Konfiguráció cisco vendor router-en
  - Kliens (R1)
    - Hitelesítési adatok létrehozása
      - `username <R2 Device Name> password <Password>`
    - Dialer interface létrehozása
      - Ez a logikai PPP interface a kliensen, amivel fel tud „tárcsázni” a szerver logikai PPP interface-re
      - `R1(config)#interface Dialer<DID>`
        `R1(config-if)#ip address <IP address> <Subnet Mask>`
        `R1(config-if)#encapsulation ppp`
        `R1(config-if)#dialer pool <DID>`
        `R1(config-if)#ppp authentication chap`
        `R1(config-if)#no sh`
    - PPPoE engedélyezése az interface-n
      - `R1(config)#interface <Interface ID>`
        `R1(config-if)#no ip address`

```
R1(config-if)#pppoe enable
R1(config-if)#pppoe-client dial-pool-number <DID>
R1(config-if)#No shutdown
```

- Szerver (R2)
  - Hitelesítési adatok létrehozása
    - `username <R1 Device Name> password <Password>`
  - Virtual Template létrehozása
    - Ez a logikai PPP interface a szerveren, kliensek számára, amibe fel tudnak „tárcsázni”
    - `R2(config)#interface Virtual-Template<VTID>`
      `R2(config-if)#ip address <IP address> <Subnet Mask>`
      `R2(config-if)#ppp authentication chap`
  - PPPoE csoport létrehozása
    - `R2(config)#bba-group pppoe <ISP_GROUP Name>`
      `virtual-template<VTID>`
  - PPPoE engedélyezése az interface-n
    - `R2(config)#interface <Interface ID>`
      `R2(config-if)#no ip address`
      `R2(config-if)#pppoe enable group <ISP_GROUP Name>`
      `R2(config-if)#no sh`
- Kábel
  - Nagy sebességű állandóan aktív csatlakozási módszer
  - DOCSIS
    - Data Over Cable Service Interface Specification
    - Nagy sávszélességű adatok meglévő kábelrendszerhez való hozzáadásának nemzetközi szabványa
  - Kábelhálózat a rádió frekvenciás jelek továbbítására koaxiális vezetéket használ
- Optikai
  - Optikai szálas technológiák WAN-ban
    - SDH
      - Synchronous Digital Hierarchy
      - Globális szabvány a száloptikai kábelen keresztüli adatátvitelhez
    - SONET
      - Synchronous Optical Network
      - Észak-USA szabvány, amely ugyanazokat a szolgáltatásokat nyújta, mint az SDH
    - DWDM
      - Dense Wavelength Division Multiplexing
        - Multiplexing
          - Multiplexálás

- Egyetlen optikai szálon rengeteg párhuzamos adatcsatornát képes egyidejűleg küldeni
- Az SDH és SONET egyaránt optikai szálas technológiák, amik gyors, egyszerre több formátumból/forrásból származó adattovábbításra fókuszálnak nagy távolságokon át, a DWDM pedig az átviteli kapacitás szabályozására van kialakítva
- Fajták
  - FTTH
    - Fiber To The Home
  - FTTB
    - Fiber To The Building
  - FTTN
    - Fiber tot he Node/Neighborhood
- Vezeték nélküli
  - Szolgáltatói Wi-FI
  - Mobilhálózat
  - Műholdas internet
  - WiMAX

- conf t
- interface s0/0/0
- encapsulation ppp
- ip address 10.0.0.1 255.255.255.252
- no shutdown
- !
- interface s0/0/1
- encapsulation ppp
- ip address 10.0.1.1 255.255.255.252
- no shutdown
- end

szit.hu alapján:

PAP beállítás 2 routeren

- R1(config)#username R2 password titok
- R1(config)#int s0/0/0
- R1(config-if)#encapsulation ppp
- R1(config-if)#ppp authentication pap
- R1(config-if)#ppp pap sent-username R1 password titok
- R1(config-if)#

- R2(config)#username R1 password titok
- R2(config)#int s0/0/0
- R2(config-if)#encapsulation ppp
- R2(config-if)#ppp authentication pap
- R2(config-if)#ppp pap sent-username R2 password titok

Hálózattervezés, hibaelhárítás – alap „show” arzenál

- ✓ show ip interface brief
- ✓ show vlan brief
- ✓ show interfaces trunk
- ✓ show spanning-tree
- ✓ show ip route
- ✓ show ip ospf neighbor
- ✓ show ip eigrp neighbors
- ✓ show access-lists
- ✓ show ip nat translations
- ✓ show crypto isakmp sa
- ✓ show crypto ipsec sa
- ✓ show logging

ACL-ek:

- Access Contol List
- OSI Modell 4. és 3. réteg egyaránt
- Csomag szűrés/ellenőrzés a célja
  - Egy forgalomirányítón kifelé, valamint befelé menő forgalmat szűrjük át, a csomag fejléceiben található adatok alapján
  - Több kontextusban fontos tudd ez lenni, legyen az Interface vagy NAT vagy VPN vagy etc.
- Működés
  - Amikor egy csomag érkezik a forgalomirányítóhoz, sorban végig nézi az összes ACE-t, amig nem talál egy illeszkedőt. Az illeszkedő ACE utasításait végig követi, ez vagy engedés, vagy tiltás lesz.
    - Fontos a sorrend
    - Ha nincsen semmi ACE, amit kövesen, akkor egyből tiltja a csomagot. Minden ACL végén ott van egy „implicit deny”, ami mindent tilt.
    - ACE
      - Access Control Entry
      - Ezen szabályok szerint szűri a forgalmat
        - Engedés
        - Tiltás

Szakma jegyzet

- Fajták
  - Numbered | Számozott
    - Standard
      - Csak a forrás IP cím alapján dolgozik
      - Cisco vendor router-en konfigurálás
        - `RACL(config)#access-list <ID> <action> <source>`
          - `ID`
            - ACL száma
            - 1-99 v. 1300-1999
          - `Action`
            - `Permit`
              - Forgalom beengedése
            - `Deny`
              - Forgalom tiltása
            - `Remark`
              - Megjegyzés hagyása az adott ACL-l kapcsolatban
              - Nem folyásolja be a működést
          - `Source`
            - A megfigyelendő forgalom forrás IP címe
              - Ha egy alhálózatot akarunk megfigyelni
                - `<NetID> <Wildcard Mask>`
              - Egyedi végeszközt akarunk megfigyelni
                - `host <Adott host IP címe>`
              - Ha mindenkit akarunk megfigyelni
                - `any`
    - Extended
      - Forrás IP cím, Cél IP cím, Forrás Port, Cél Port és Protocol alapján dolgozik
      - Cisco vendor router-en konfigurálás
        - `RACL(config)#access-list <ID> <action> <protocol> <source> <destination>`
          - `ID`
            - ACL száma
            - 100-199 v. 2000-2699
          - `Action`
            - `Permit`
              - Forgalom beengedése
            - `Deny`
              - Forgalom tiltása
            - `Remark`
              - Megjegyzés hagyása az adott ACL-l kapcsolatban
              - Nem folyásolja be a működést

- `Protocol`
  - `IP`
    - Internet Protocol forgalmat ellenőriz
    - A standard csak ezt ismeri
  - `TCP`
    - Transmission Control Protocol forgalmat ellenőriz
  - `UDP`
    - User Datagram Protocol forgalmat ellenőriz
  - `ICMP`
  - Etc.
- `Source`
  - A megfigyelendő forgalom forrás IP címe
    - Ha egy alhálózatot akarunk megfigyelni
      - `<NetID> <Wildcard Mask>`
    - Egyedi végeszközt akarunk megfigyelni
      - `host <Adott host IP címe>`
    - Ha mindenkit akarunk megfigyelni
      - `any`
  - `Port`
    - Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
    - Standard nem képes Port-kat szűrni
    - `Operator`
      - `eq`
        - Egy specifikus port megadása
      - `range`
        - Egy halmaznyi port megadása
        (- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)
      - `gt`
        - Egy adott port számnál összes nagyobb szám megadása
      - `lt`
        - Egy adott port számnál összes kisebb szám megadása
      - `neq`
        - Egy adott port számmal nem egyenlő számok megadása
- `Destination`
  - A megfigyelendő forgalom cél IP címe
    - Ha egy alhálózatot akarunk megfigyelni
      - `<NetID> <Wildcard Mask>`
    - Egyedi végeszközt akarunk megfigyelni
      - `host <Adott host IPv4 címe>`
    - Ha mindenkit akarunk megfigyelni

- `any`
- `Port`
- Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
- Standard nem képes Port-kat szűrni
- `Operator`
- `eq`
- Egy specifikus port megadása
- `range`
- Egy halmaznyi port megadása
(- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)
- `gt`
- Egy adott port számnál összes nagyobb szám megadása
- `lt`
- Egy adott port számnál összes kisebb szám megadása
- `neq`
- Egy adott port számmal nem egyenlő számok megadása
- Törléskor az adott ID alatt lévő összes bejegyzést töröljük, tehát macerás utólagosan szerkeszteni, ha valamilyen hiba merül fel

- Named | Nevesített
- Standard
- Konfigurálás cisco vendor router-en
- `RACL(config)#ip access-list standard <ID v. Name>`
`RACL(config-ext-nacl)#<sequence> <action> <source>`
- `ID v. Name`
- Az ACL neve
(- Itt számoktól független, nem úgy mint Numbered-ben)
- `Sequence`
- Nem szükséges a hozzáadása, de jól jöhet
- Az itt megadott számmal sorrendbe lehet őket már alapból rendezni
- Alapértelmezetten minden egyes ACE a lista legvégére kerül máskülönben
- Törléskor a Sequence szám alkalmazásával elkerülhető az a probléma, hogy az egész ACL-t kitöröljük, itt lehet ACE-ként
- `Action`
- `Permit`
- Forgalom beengedése
- `Deny`
- Forgalom tiltása
- `Remark`
- Megjegyzés hagyása az adott ACL-l kapcsolatban
- Nem folyásolja be a működést

- `Source`
  - A megfigyelendő forgalom forrás IP címe
    - Ha egy alhálózatot akarunk megfigyelni
      - `<NetID> <Wildcard Mask>`
    - Egyedi végeszközt akarunk megfigyelni
      - `host <Adott host IP címe>`
    - Ha mindenkit akarunk megfigyelni
      - `any`
- Extended
  - Konfigurálás cisco vendor router-en
    - `RACL(config)#ip access-list extended <ID v. Name>`
      `RACL(config-ext-nacl)#<sequence> <action> <protocol> <source> <destination>`
      - `ID v. Name`
        - Az ACL neve
        (- Itt számoktól független, nem úgy mint Numbered-ben)
      - `Sequence`
        - Nem szükséges a hozzáadása, de jól jöhet
        - Az itt megadott számmal sorrendbe lehet őket már alapból rendezni
          - Alapértelmezetten minden egyes ACE a lista legvégére kerül máskülönben
        - Törléskor a Sequence szám alkalmazásával elkerülhető az a probléma, hogy az egész ACL-t kitöröljük, itt lehet ACE-ként
      - `Action`
        - `Permit`
          - Forgalom beengedése
        - `Deny`
          - Forgalom tiltása
        - `Remark`
          - Megjegyzés hagyása az adott ACL-l kapcsolatban
          - Nem folyásolja be a működést
      - `Protocol`
        - `IP`
          - Internet Protocol forgalmat ellenőriz
          - A standard csak ezt ismeri
        - `TCP`
          - Transmission Control Protocol forgalmat ellenőriz
        - `UDP`
          - User Datagram Protocol forgalmat ellenőriz
        - `ICMP`
        - Etc.
      - `Source`

- A megfigyelendő forgalom forrás IP címe
  - Ha egy alhálózatot akarunk megfigyelni
    - `<NetID> <Wildcard Mask>`
  - Egyedi végeszközt akarunk megfigyelni
    - `host <Adott host IP címe>`
  - Ha mindenkit akarunk megfigyelni
    - `any`
- `Port`
  - Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
  - Standard nem képes Port-kat szűrni
  - `Operator`
    - `eq`
      - Egy specifikus port megadása
    - `range`
      - Egy halmaznyi port megadása
      (- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)
    - `gt`
      - Egy adott port számnál összes nagyobb szám megadása
    - `lt`
      - Egy adott port számnál összes kisebb szám megadása
    - `neq`
      - Egy adott port számmal nem egyenlő számok megadása
- `Destination`
  - A megfigyelendő forgalom cél IP címe
  - Ha egy alhálózatot akarunk megfigyelni
    - `<NetID> <Wildcard Mask>`
  - Egyedi végeszközt akarunk megfigyelni
    - `host <Adott host IPv4 címe>`
  - Ha mindenkit akarunk megfigyelni
    - `any`
- `Port`
  - Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
  - Standard nem képes Port-kat szűrni
  - `Operator`
    - `eq`
      - Egy specifikus port megadása
    - `range`
      - Egy halmaznyi port megadása
      (- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)

- `gt`
  - Egy adott port számnál összes nagyobb szám megadása
- `lt`
  - Egy adott port számnál összes kisebb szám megadása
- `neq`
  - Egy adott port számmal nem egyenlő számok megadása

- Újra osztás
  - Ha valamilyen oknál fogva szűkíteni vagy nagyobbítani kell a már meglévő bejegyzések között, vagy csak egy számsorrendbe akarod őket rendezni, mert sok utó munkát végeztél
  - Cisco vendor router-en újra osztás
    - `RACL(config)#ip access-list resequence <ID v. Name> <számsor legelső száma> <increment>`
- IPv6
  - Csak a nevesített ACL alkalmas IPv6-s címek szűrésére, azt is mindig extended módon fogja tenni
  - Cisco vendor router-en konfigurálás
    - `RACL(config)#ipv6 access-list <ID v. Name>`
      `RACL(config-ipv6-acl)#<sequence> <action> <protocol> <source> <destination>`
      - `ID v. Name`
        - Az ACL neve
      - `Sequence`
        - Nem szükséges a hozzáadása, de jól jöhet
        - Az itt megadott számmal sorrendbe lehet őket már alapból rendezni
          - Alapértelmezetten minden egyes ACE a lista legvégére kerül máskülönben
        - Törléskor a Sequence szám alkalmazásával elkerülhető az a probléma, hogy az egész ACL-t kitöröljük, itt lehet ACE-ként
        - Itt IPv6-ban az alábbi módon kell beírni
          - `sequence <szám>`
      - `Action`
        - `Permit`
          - Forgalom beengedése
        - `Deny`
          - Forgalom tiltása
        - `Remark`
          - Megjegyzés hagyása az adott ACL-l kapcsolatban
          - Nem folyásolja be a működést
      - `Protocol`
        - `IP`
          - Internet Protocol forgalmat ellenőriz

- `TCP`
  - Transmission Control Protocol forgalmat ellenőriz
- `UDP`
  - User Datagram Protocol forgalmat ellenőriz
- `ICMP`
- Etc.

- `Source`
  - A megfigyelendő forgalom forrás IP címe
    - Ha egy alhálózatot akarunk megfigyelni
      - `<GUA>/<Prefix>`
    - Egyedi végeszközt akarunk megfigyelni
      - `host <Adott host IP címe>`
    - Ha mindenkit akarunk megfigyelni
      - `any`
  - `Port`
    - Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
    - `Operator`
      - `eq`
        - Egy specifikus port megadása
      - `range`
        - Egy halmaznyi port megadása
        (- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)
      - `gt`
        - Egy adott port számnál összes nagyobb szám megadása
      - `lt`
        - Egy adott port számnál összes kisebb szám megadása
      - `neq`
        - Egy adott port számmal nem egyenlő számok megadása

- `Destination`
  - A megfigyelendő forgalom cél IP címe
    - Ha egy alhálózatot akarunk megfigyelni
      - `<GUA>/<Prefix>`
    - Egyedi végeszközt akarunk megfigyelni
      - `host <Adott host IP címe>`
    - Ha mindenkit akarunk megfigyelni
      - `any`
  - `Port`
    - Bizonyos esetekben (pl. TCP v. UDP) érdemes de nem szükséges, hogy Port számot is megadjunk, a pontosabb szűréshez
    - `Operator`

- `eq`
  - Egy specifikus port megadása
- `range`
  - Egy halmaznyi port megadása
  (- ne felejtsd, ha 20 25-t adsz meg, akkor összesen 6db port-t adsz meg)
- `gt`
  - Egy adott port számnál összes nagyobb szám megadása
- `lt`
  - Egy adott port számnál összes kisebb szám megadása
- `neq`
  - Egy adott port számmal nem egyenlő számok megadása

- Ahhoz hogy bármilyen ACL érvénybe lépjen, hozzákell rendelni valamihez
  - Irányelvek
    - Minden protokollhoz külön ACL kell
    - Külön bejövő és külön kimenő ACL kell forgalomirányítóként
    - Egy ACL interfészenként
  - Cisco vendor router-en
    - `RACL(config)#interface <Interface ID>`
      `RACL(config-if)#ip access-group <ID v. Name> <in v. out>`
    - `RACL(config-if)#interface <Interface ID>`
      `RACL(config-if#ipv6 traffic-filter <ID. Name> <in v. out>`
  - Fontos mindig logikusan végig gondolni, hogy hova rakjuk az ACL-t, sokszor helyzet függő
    - Átlagos tanács
      - Standard ACL-t érdemesebb a célhoz közel konfigurálni
        - Mivel nem tudd finomhangoltan szűrni, mint az extended, ezért minél közelebb van a célhoz, annál nagyobb eséllyel nem fogunk fölöslegesen sok forgalmat szűrni
        (- Érdemes úgy nagy általánoságban elkerülni a Standard ACL-t)
      - Extended ACL-t érdemesebb a forráshoz közel konfigurálni
        - Minél hamarabb annál jobb, az eszköz erőforrásait is kíméli
- Olvasás
  - Cisco vendor router-en
    - `RACL#show access list`

standard

- conf t
- access-list 10 permit 192.168.10.0 0.0.0.255
- access-list 10 deny any
- !
- interface g0/0
- ip access-group 10 in

- end

extended

- conf t
- access-list 100 deny tcp any any eq 23
- access-list 100 permit ip any any
- !
- interface g0/0
- ip access-group 100 in
- end

named:

- conf t
- ip access-list extended BLOCK_SOCIAL
- deny tcp any any eq 443
- permit ip any any
- !
- interface g0/1
- ip access-group BLOCK_SOCIAL out
- end

Windows szerverek:

Mikrotik jegyzet:

jelszó megváltoztatás –

/user set admin password="Titok!2026"

Ip címzés –

- /ip dhcp-client add interface=ether1 disabled=no
- /ip address add address=172.25.100.1/24 interface=ether2
- /ip address add address=172.25.56.99/24 interface=ether3

Nat – internetmegozstás – A belső hálózat (ether2) forgalmát az ether1-en keresztül NAT-oljuk.

- /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

Portovábbítások:

- /ip firewall nat add chain=dstnat in-interface=ether3 protocol=tcp dst-port=30000 \ action=dst-nat to-addresses=172.25.100.254 to-ports=3389

- /ip firewall nat add chain=dstnat in-interface=ether3 protocol=tcp dst-port=2222 \action=dst-nat to-addresses=172.25.100.253 to-ports=22

RDP kapcsolat kialakítása CLI:

Win + R

mstsc

- 172.25.56.99:30000

és hitelesítés végül

Powershell dhcp telepítés:

- Install-WindowsFeature -Name DHCP -IncludeManagementTools

engedélyezem a szolgáltatást:

- netsh dhcp add securitygroups
- Restart-Service dhcpserver

scope létrehozása:

- Add-DhcpServerv4Scope -Name "fesztival_scope" -StartRange 172.25.100.100 -EndRange 172.25.100.150 -SubnetMask 255.255.255.0

dns beállítása:

- Set-DhcpServerv4OptionValue -DnsServer 172.25.100.254 -DnsDomain fesztival.lan

átjáró beállítása:

- Set-DhcpServerv4OptionValue -Router 172.25.100.1

lease time beállítása:

- Set-DhcpServerv4Scope -ScopeId 192.168.1.0 -LeaseDuration 0.00:45:00

DHCP Opciók (GW, DNS):

- Set-DhcpServerv4OptionValue -OptionId 3 -Value 192.168.13.1;
- Set-DhcpServerv4OptionValue -OptionId 6 -Value 192.168.13.10

Active directory telepítése

1. Server Manager → Add Roles and Features
2. Active Directory Domain Services
3. Telepítés után: „Promote this server to a domain controller”

4. Új domain létrehozása vagy meglévőhöz csatlakozás -> new tree

Felhasználók és csoportok kezelése (Active Directory Users and Computers)

Új felhasználó létrehozása:

Server Manager → Tools → Active Directory Users and Computers (ADUC)

Válaszd ki az OU-t (pl. „Users” vagy saját OU)

Jobb klikk → **New → User**

Add meg:

- First name
- Last name
- User logon name (pl. jkovacs)

Jelszó beállítása:

- User must change password at next logon (ajánlott)
- Password never expires (nem ajánlott)

Új csoport létrehozása:

OU → jobb klikk → **New → Group**

Group name: pl. „HR-ReadOnly”

Group scope:

- **Global** (legtöbbször ezt használjuk)

Group type:

- **Security** (engedélyekhez)
- Distribution (levelezéshez)

Jelszóházirend config

1. Eszköz: Group Policy Management
2. Útvonal:
   Computer Configuration
   → Policies
   → Windows Settings
   → Security Settings

→ Account Policies
→ Password Policy

Felhasználó hozzáadása csoporthoz

1. Csoport → jobb klikk → Properties
2. Members → Add
3. Írd be a felhasználó nevét → OK

Ökölszabály: 👉 *Jogosultságot mindig csoportnak adj, nem felhasználónak.*

Jogosultságok – hitelesítés utáni engedélyek

1. *User Right Assingment*
2. Computer Configuration
3. → Windows Settings
4. → Security Settings
5. → Local Policies
6. → User Rights Assignment

Csoportalapú jogosultságkezelés (Ajánlott módszer)

- Lépések:
  1. AD Users and Computers → New → Group
  2. Security type: Security
  3. Scope: Global (általában ez ajánlott)
  4. Felhasználók hozzáadása a csoporthoz
  5. Jogosultság hozzárendelése a csoporthoz

NTFS jogosultságok (Security fül) NTFS az alapértelmezett fájlrendszer Windows Serveren.

Mappa → jobb klikk → **Properties → Security**

- Beállítása:
  - Edit
  - Add (csoport hozzáadása)
  - Engedély kiválasztása

Alapértelmezetten:

- A mappa engedélyei öröklődnek az al-mappákra.
- Beállítás:
  - Security → Advanced → Disable inheritance

Megosztási engedélyek (Sharing)

Mappa → jobb klikk → **Properties → Sharing → Advanced Sharing**

NTFS × Share = végső jogosultság

Három szint:

- **Read**
- **Change**
- **Full Control**

Effective Access (Végső jogosultság)

Security → Advanced → Effective Access

Ez kiszámolja:

- Share + NTFS kombinációját
- Öröklődést
- Csoporttagságokat

GPO-k

GPO létrehozása

1. Tools → Group Policy Management
2. Domain → Right Click → Create GPO
3. Linkeld OU-hoz
4. Szerkesztés

Létrehozás CLI-ből:

New-GPO -Name "Fesztival_Helyszinek_Policy"

Linkelés az OU-hoz CLI-ből:

New-GPLink -Name "Fesztival_Helyszinek_Policy" -Target "OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"

Fájlrendszerek, fájlműveletek, partíciók, szoftveres RAID

Windows Server GUI-ban a fájlműveletek főként a
“File Explorer” vagy “Server Manager” → File and Storage Services → Shares részeken történnek

Alapvető műveletek

- Másolás / Áthelyezés / Törlés: Jobb-klikk → Copy / Move / Delete
- Új mappa létrehozása: Jobb-klikk → New → Folder

- Jogosultságkezelés:
    - Jobb-klikk → Properties → Security → Edit
    - Hozzáadás / eltávolítás felhasználók, csoportok
    - Jogosultságok: Full Control, Modify, Read, Write

Partíció létrehozása:

1. Nyisd meg a Server Manager → File and Storage Services → Volumes → Disks.
2. Válaszd ki a nem inicializált lemezt → Initialize Disk.
3. Hozz létre új partíciót a New Volume Wizard segítségével:
    - Válaszd ki a partíció méretét.
    - Fájlrendszer: NTFS vagy ReFS.
    - Hozz létre meghajtóbetűjelet.
    - Készíts formázást (quick format ajánlott új lemezeknél).

RAID

RAID konfiguráció:

1. Nyisd meg: Server Manager → File and Storage Services → Volumes → Disks.
2. Válaszd a több lemezt, jobb-klikk → New Mirrored Volume / New Striped Volume / New RAID-5 Volume.
3. Kövesd a Volume Wizard lépéseit:
    - Válaszd ki a lemezeket.
    - Add meg a volume nevét, betűjelét.
    - Formázás NTFS-sel.

RAID karbantartás:

    - Hibás lemezt Remove → Replace Disk → Resync.
- Rendszeresen készíts backupot, mert szoftveres RAID nem helyettesíti a backupot.

DHCP

DHCP telepítése (GUI – Server Manager)

1. Nyisd meg: Server Manager → Manage → Add Roles and Features
2. Role-based installation
3. Válaszd ki a szervert
4. Pipáld ki: DHCP Server
5. Install
6. Telepítés után: Complete DHCP Configuration

Ha a szerver tartomány tag, akkor Authorize-olni kell Active Directoryban

- Ha nincs Authorize, a DHCP szolgáltatás elindul, de:

- Event Viewerben hiba jelenik meg
- Nem fog IP-t kiosztani
- A konzolban piros lefelé mutató nyíl látható

Miután telepítetted a DHCP Server role-t:

- Server Manage
- Felső sárga figyelmeztetés → Complete DHCP configuration
- Kattints → Authorize

DNS

DNS konfiguráció

1. Forward Lookup Zone létrehozása
   Server Manager → Tools → DNS
   1. Forward Lookup Zones
   2. New Zone
   3. Primary Zone
   4. AD Integrated (ha DC)
   5. Zone name: <domain_name>
2. "A Record" létrehozása
   Zone → jobb klikk → New Host (A)
   - Name: server
   - IP: <ip_address>
3. Reverse Lookup Zone
   Reverse Lookup Zones → New Zone
   - Network ID: <halozati_azonosito_ipcim> -> prefixtől függ, hogy milyen IP-t adunk meg
   - PTR rekord automatikusan generálható.

MMC

Snap-inek létrehozása:

1. Nyisd meg: Win + R → mmc → Enter
2. Menj a File → Add/Remove Snap-in... menüpontra
3. Válaszd ki a kívánt snap-ineket, majd Add → OK
4. Beállíthatod, hogy a snap-inek vagy helyi, vagy távoli szerverekhez kapcsolódjanak

Konzol mentése:

- Állítsd be a megfelelő snap-ineket
  → File → Save As... → nevezd el → mentsd .msc-ként
- Később közvetlenül megnyitható dupla kattintással

Jogosultságok:

- Az MMC konzol fájlokra (pl. saját .msc) biztonsági jogosultságokat adhatsz, így korlátozhatod, ki nyithatja vagy szerkesztheti a konzolt

Active Directory tartományvezérlő telepítés, konfigurálás

Az AD DS egy központi címtárszolgáltatás, amely:

- Felhasználókat kezel (bejelentkezés, jelszavak)
- Számítógépeket kezel (tartományba léptetés)
- Jogosultságokat szabályoz
- Erőforrásokhoz való hozzáférést irányít (megosztások, nyomtatók, alkalmazások)
- Központi házirendeket alkalmaz (Group Policy)

Előkészületek (telepítés előtt)

1. Fix IP cím beállítása (Az AD-nak mindig fix IP címmel kell rendelkeznie!)
    1. Start → Settings → Network & Internet
    2. Adapter settings
    3. Jobb klikk az aktív hálózati kártyára → Properties
    4. Internet Protocol Version 4 (TCP/IPv4)
    5. Manual IP beállítás
2. Gépnév beállítása
    1. Server Manager → Local Server
    2. Computer name → Change
    3. Adj meg egy hostnamet:
    4. Újraindítás szükséges.

Active Directory Domain Services szerepkör telepítése

1. Role telepítés GUI-val
2. Nyisd meg a Server Manager
3. "Manage" → Add Roles and Features
4. Role-based or feature-based installation
5. Válaszd ki a helyi szervert
6. Pipáld be: Active Directory Domain Services
   (A rendszer ezekután automatikusan felajánlja a szükséges feature-öket → Add Features)
7. Next → Install

Az AD DS tartományvezérlővé promótálása

1. *AD DS szerepkör telepítés után:*
    1. Server Manager → Notification flag
    2. Promote this server to a domain controller
2. *Deployment Configuration*
   Három lehetőség van:
    - Add a new forest (Új forest létrehozása)
    - Add a new domain to an existing forest (Új domain meglévő forestben)

- Add a domain controller to an existing domain (További DC meglévő domainhez)

1. Új rendszer esetén: **Add a new forest / Új forest létrehozása**
2. Ezután meg kell adni egy “domain name”-t
   a. Lehet lokális pl. ceg.local
   b. Lehet publikus pl. ceg.hu

3. *Domain Controller Options*
   Beállítások:
   - DNS Servert engedélyezzük
   - Global Catalog-ot engedélyezzük
   - Nem engedélyezzük a Read Only DC-t (ha nem RODC!)

   DSRM jelszó: Directory Services Restore Mode jelszó (nagyon fontos!)

DNS Options

- Ha új forest, figyelmeztetés lesz (delegation nem található) → normális.

PATH

Alapértelmezett mappák:

- Database: C:\Windows\NTDS
- Logs: C:\Windows\NTDS
- SYSVOL: C:\Windows\SYSVOL

A telepítés után:

1. Automatikus újraindítás
2. A gép tartományvezérlővé válik

Organizational Units (OU) létrehozása

1. Tools → Active Directory Users and Computers
2. Domain név → jobb klikk → New → Organizational Unit

Felhasználók létrehozása

OU → jobb klikk → New → User

Fontos mezők:

- First name
- Last name
- User logon name

Jelszó beállítás:

- User must change password at next logon, vagy
- Password never expires

Csoportok létrehozása

New → Group

Group scope:

- Global
- Domain Local
- Universal

Group type:

- Security (jogosultsághoz)
- Distribution (email)

DHCP (ha ugyanazon a szerveren van)

Ha DHCP is telepítve van:

1. DHCP role telepítése
2. Authorize DHCP in AD
3. DHCP Scope DNS beállítása:
   - DNS server: <DC IP>
   - DNS suffix: <domain-name>

Group Policy konfiguráció

Tools → Group Policy Management

Új GPO létrehozása:

1. OU → Create a GPO in this domain
2. Edit
   - Példák:
     - USB tiltás
     - Desktop háttér
     - Szoftver telepítés
     - Tűzfal szabályok

Tartományba léptetés (kliens oldalon)

1. Client gépen: System → Rename this PC → Join domain
2. Írd be a “domain-name”-t (pl. ceg.local)
3. Domain admin hitelesítés → jogosult user és password megadása (admin)
4. Újraindítás

CLI-ből tartományba léptetés:

- Add-Computer -DomainName "fesztival.lan" -Restart

Kliens gépnév módosítása:

- Rename-Computer -NewName "C10-1" -Restart

Organizational Unit (OU) kezelése

1. *OU létrehozása*
   ADUC → Domain → jobb klikk → New → Organizational Unit

   Fontos beállítás (**pipáld be**): Protect container from accidental deletion

2. *OU konfiguráció*
   Jobb klikk OU → Properties

   Lehetőségek:
   - Description
   - Managed By (delegálás miatt fontos)
   - Group Policy linkelés (GPMC-ben)

3. *Delegation (Jogosultság delegálás)*
   OU → jobb klikk → Delegate Control

   Használható:
   - pl. ha a HR csak user jelszót resetelhet
   - pl. ha az IT csak számítógépet hozhat létre

User objektum kezelése

1. *Felhasználó létrehozása*
   OU → New → User

   Beállítások:
   - First name
   - Last name
   - User logon name (UPN)
     - username@domain
   - Pre-Windows 2000 logon name
     - csak username
     - bejelentkezésnél: DOMAIN\username

2. *User konfiguráció (Properties)*
   General: Alapadatok

   Account
   Fontos opciók:
   - User must change password at next logon
   - User cannot change password
   - Password never expires
   - Account is disabled

   Logon Hours: Időkorlátozás beállítása

   Logon To: Meghatározható, mely gépekre jelentkezhet be

Profile

- Roaming profile path
- Home folder
- Logon script

3. *Fiók zárolás és feloldás*
   Account → Unlock account

4. *Speciális attribútumok (Advanced Features)*
   View → Advanced Features

   Ekkor elérhető:

   - Attribute Editor
   - Object tab
   - Security tab

Computer objektum kezelése

1. *Gépfiók létrehozása*
   OU → New → Computer

   Általában tartományba léptetéskor jön létre.

2. *Computer objektum konfiguráció*
   Properties:
   - Description
   - Managed by
   - Delegation
   - Location

3. *Computer reset*
   Ha trust hiba van: Jobb klikk → Reset Account

Group objektum kezelése

1. *Csoport létrehozása*
   OU → New → Group

   Group scope:
   - Global
   - Domain Local
   - Universal

   Group type:
   - Security
   - Distribution

2. *Csoport konfiguráció*
   Properties → Members

   Tagok hozzáadása

3. *AGDLP modell*
   Accounts → Global → Domain Local → Permission

   Gyakorlat:
   - User → Global Group
   - Global → Domain Local
   - Domain Local → NTFS jog

Objektum jogosultságok kezelése

View → Advanced Features
Object → Properties → Security

Beállítható:
- Read
- Write
- Delete
- Reset password
- Full control

Objektum törlés

Törléshez:
1. ADUC → View → ✓ Advanced Features
2. Objektum → Properties
3. Object fül
4. Vedd ki a pipát: Protect object from accidental deletion
5. Ok (mostmár törölhető az objektum)
6. Törlés

Gyakori admin műveletek

User disable / enable

ADUC → User → jobb klikk
- Disable Account
- Enable Account

Password reset

User → jobb klikk → Reset Password
Itt:
- Új jelszó
- User must change password

Computer account reset

Computer → jobb klikk → Reset Account

Ez:

- Trust kapcsolatot nulláz

Group membership módosítás

User → jobb klikk → Properties → Member Of

Itt:

- Add
- Remove

Bulk műveletek (multi-select)

Több objektum kijelölése:

- CTRL + kattintás
- SHIFT + kijelölés

Jobb klikk után:

- Disable
- Move
- Delete

Megjegyzés: Nem minden művelet érhető el tömegesen

Csoportházirend szolgáltatások konfigurálása

GPMC megnyitása (GUI)

Lépések:

1. Server Manager megnyitása
2. Tools → Group Policy Management
3. Megnyílik a GPMC konzol

Itt látható:

- Forest
- Domains
- Group Policy Objects
- Sites
- WMI Filters

Új GPO létrehozása

Lépések:

1. Domain → jobb klikk → Create a GPO in this domain
2. Név megadása
3. OK
4. Ezután: Jobb klikk a GPO-n → Edit

Megnyílik a Group Policy Management Editor

GPO felépítése

A GPO két fő részből áll:

- User Configuration (felhasználóra vonatkozó beállítások):
  - Desktop korlátozások
  - Start menü
  - Script-ek
  - Registry
  - Folder redirection
  - Computer Configuration
- Számítógépre vonatkozó beállítások:
  - Biztonság
  - Szolgáltatások
  - Windows Update
  - Tűzfal
  - Software deployment

Security in Group Policy

Útvonal:

Computer Configuration → Policies → Windows Settings → Security Settings

Gyakori beállítások:

Jelszóházirend:

Account Policies → Password Policy

Konfiguráció:

- Minimum jelszóhossz
- Komplexitás
- Maximum életkor
- Jelszóelőzmények

Account lockout

Account Policies → Account Lockout Policy

Beállítható:

- Hibás próbálkozások száma
- Zárolási idő
- Reset idő

Vezérlőpult elérés és programfuttatás tiltása:

User Configuration

└ Administrative Templates

└ Control Panel

Prohibit access to Control Panel and PC settings → Enabled

User Configuration

└ Administrative Templates

└ System

Don't run specified Windows applications → Enabled

regedit.exe

msconfig.exe

gpupdate /force

Tűzfal konfig

Útvonal:

Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender Firewall

Konfiguráció:

- Domain / Private / Public profil
- Bejövő és kimenő szabályok
- Port megnyitás
- ICMP engedélyezés

Scriptek konfig

Startup / Shutdown

Útvonal: Computer Configuration → Windows Settings → Scripts

Logon / Logoff

Útvonal: User Configuration → Windows Settings → Scripts

Használat:

- meghajtó csatolás
- automatizálás
- környezet konfiguráció

GPO linkelése

Linkelés:

- Site
- Domain
- OU

Jobb klikk → Link an Existing GPO

Házirend frissítése

Kliensen: *gpupdate /force*

Ellenőrzés: *gpresult /r*

PowerShell szkript

Gépnév megváltoztatása:
Rename-Computer -NewName "win-srv-core” -Restart

Ellenőrzés:
Get-ComputerInfo | Select-Object CsName

Az elérhető afdapterek megjelenitése (ifindex):
Get-NetAdapter

IP és Gateway beállítása:

New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress <ipaddress> -PrefixLength <prefix> -DefaultGateway <ipaddress>

DNS server beállítása:

Set-DnsClientServerAddress -InterfaceAlias "Ethernet"
-ServerAddresses ("<ipaddress>","<ipaddress>")

Reverse Lookup zóna:

Add-DnsServerPrimaryZone -NetworkId "172.25.100.0/24" -ReplicationScope "Domain"

PTR rekord hozzáadása:

Add-DnsServerResourceRecordPtr -Name "254" -ZoneName "100.25.172.in-addr.arpa"
-PtrDomainName "windows.fesztival.lan"

Forward Lookup zóna:

Add-DnsServerResourceRecordA -Name "www" -ZoneName "fesztival.lan" -
IPv4Address "172.25.100.254"

IP beállítások törlése:
Remove-NetIPAddress -InterfaceIndex <interfaceindex> -Confirm:$false

Alapértelmezett átjáró törlése:
Remove-NetRoute -intefaceindex <interfaceindex>

DNS kliensek lekérdezése:
Get-DnsClientServerAddress

DNS beállitások törlése:
Set-DnsClientServerAddress -InterfaceIndex <interfaceindex> -ResetServerAddresses

Időzóna beállitások:

Az elérhető időzonák listája:

Get-TimeZone -ListAvailable

Időzóna beállitása (CET esetén):

Set-TimeZone -Id "Central Europe Standard Time"

Ellenőrzés:

Get-timezone

AD DS, DNS, DHCP, IIS szerepkörök telepítése:

- Install-WindowsFeature AD-Domain-Services, DNS, DHCP, Web-Server -IncludeManagementTools

Tartomány létrehozása: pl. **skyguard.lan**

- Install-ADDSForest -DomainName "skyguard.lan" -DomainNetbiosName "SKYGUARD" -InstallDNS -Force

DHCP inicializálása:

- Add-DhcpServerInDC -DnsName "win-srv-core.skyguard.lan" -IPAddress 192.168.23.10
- scope: Add-DhcpServerv4Scope -Name "LAN" -StartRange 192.168.23.50 -EndRange 192.168.23.200 -SubnetMask 255.255.255.0

ADDS scriptel

AD DS szolgáltatás telepítése:
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Erdő létrehozása:
Install-ADDSForest -DomainName "example.com" -DomainMode "Win2016" -ForestMode "Win2016" -DomainNetbiosName "EXAMPLE" -InstallDns -Force

OU létrehozása PowerShellből:

- New-ADOrganizationalUnit -Name "Gyakornokok" -Path "DC=skyguard,DC=lan"

Csoport létrehozása:

- New-ADGroup -Name "GyakornokokCsoport" -GroupScope Global -GroupCategory Security -Path "OU=Gyakornokok,DC=skyguard,DC=lan"

ellenőrzés:

- Get-ADOrganizationalUnit -Filter * | Select Name, DistinguishedName

felhasználó létrehozása:

- New-ADUser "Marco" -AccountPassword (ConvertTo-SecureString "Jelszo123" -AsPlainText -Force) -Enabled $true

Fő OU és al OU-k létrehozása scriptben:

- New-ADOrganizationalUnit -Name "Fesztival_Helyszinek"
- New-ADOrganizationalUnit -Name "Nagy_Szinpad" -Path "OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"
- New-ADOrganizationalUnit -Name "VIP_Sator" -Path "OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"
- New-ADOrganizationalUnit -Name "Kemping" -Path "OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"

bejelentkezési idő állítása:

- Set-ADAccountLogonHours -Identity "marco" -LogonHours (
  Get-ADAccountLogonHours -Days Monday,Tuesday,Wednesday,Thursday,Friday `
  -StartTime 07:00 -EndTime 18:00
- felhasználó ellenőrzése: Get-ADUser marco -Properties *

Felhasználó létrehozása:
New-ADUser -Name "Nagy_Szinpad_User" -AccountPassword (ConvertTo-SecureString "Titok!2026" -AsPlainText -Force) -Enabled $true -Path "OU=Nagy_Szinpad,OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"

Csoport létrehozása:
New-ADGroup -Name "Nagy_Szinpad" -GroupScope Global -Path "OU=Nagy_Szinpad,OU=Fesztival_Helyszinek,DC=fesztival,DC=lan"

Felhasználó hozzáadása csoportba:

- Add-ADGroupMember -Identity "CsoportNeve" -Members "FelhasznaloNeve"
- Felhasználó eltávolítása csoportból:
- Remove-ADGroupMember -Identity "CsoportNeve" -Members "FelhasznaloNeve"
- Csoport törlése:
- Remove-ADGroup -Identity "CsoportNeve"
- Csoport tagjainak lekérdezése:
- Get-ADGroupMember -Identity "CsoportNeve"
- Szervezeti egységek (OU) lekérdezése:
- Get-ADOrganizationalUnit -Filter *

Új szervezeti egység (OU) létrehozása:

- New-ADOrganizationalUnit -Name "ÚjOU" -Path "OU=ParentOU,DC=domain,DC=com"

Objektum hozzáadása szervezeti egységhez:

- Add-ADGroupMember -Identity "CN=Group,CN=Users,DC=domain,DC=com" -Members "CN=User,CN=Users,DC=domain,DC=com"

DHCP szerepkör beállítása:

DHCP szolgáltatás engedélyezése:

- Add-DhcpServerInDC -DnsName "win-srv-core.skyguard.lan" -IPAddress 192.168.23.10

DHCP scope létrehozása:

- Add-DhcpServerv4Scope -Name "LAN" -StartRange 192.168.23.50 -EndRange 192.168.23.200 -SubnetMask 255.255.255.0

DNS opciók:

- Set-DhcpServerv4OptionValue -DnsServer 192.168.23.10 -DnsDomain "skyguard.lan"

Csatlakozás létező domainhoz

Install-ADDSDomainController -DomainName "MeglévőDomainNeve" -SiteName "AzonosítottTelephelyNeve" -Credential (Get-Credential)

Ebben a parancsban a következő paramétereket kell megadni:

- *DomainName:* A meglévő tartomány neve, ahova a szerver csatlakozni fog.
- *SiteName:* A telephely neve, amelyhez a szerver csatlakozni fog.
- *Credential:* Az adminisztrátori jogosultsággal rendelkező felhasználói fiókhoz tartozó hitelesítési objektum, amelynek joga van Domain Controller telepítésére.

ADDS erdő törlése

- Uninstall-ADDSDomainController -DemoteOperationMasterRole -RemoveApplicationPartitions -Force

Windows 10 kliens beállítása:

fix IP, DNS:

- New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 192.168.23.100 -PrefixLength 24 -DefaultGateway 192.168.23.1
- Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 192.168.23.10

Tartományba léptetés:

- Add-Computer -DomainName "skyguard.lan" -Credential skyguard\Administrator s-Restart

RSAT telepítés és beállítás Powershellben:

Elérhető RSAT komponensek listázása

- Get-WindowsCapability -Name RSAT* -Online

Minden RSAT komponens telepítése:

- Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online

Csak bizonyos RSAT modulok telepítése:

- Active Directory module → Add-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
- DNS Server Tools → Add-WindowsCapability -Online -Name Rsat.Dns.Tools~~~~0.0.1.0
- DHCP Tools → Add-WindowsCapability -Online -Name Rsat.Dhcp.Tools~~~~0.0.1.0
- Group Policy Management → Add-WindowsCapability -Online -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0

RSAT konfigurálása PowerShellből

modulok betöltése:

- Import-Module ActiveDirectory
- Import-Module DnsServer
- Import-Module GroupPolicy

Telepített RSAT modulok listázása:

- Get-WindowsCapability -Name RSAT* -Online | Where-Object State -eq Installed

RSAT telepítése GUI-ból:

- **Útvonal:** Beállítások → Apps → Optional features → Add a feature → RSAT modulok

Gyakori hibák és megoldások

„Add-WindowsCapability : 0x800f0954” hiba

- Megoldás:
  - reg add HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU /v UseWUServer /t REG_DWORD /d 0 /f

    - net stop wuauserv
    - net start wuauserv
-

Windows Server Backup

Windows Server Backup telepítése

Alapból nem mindig telepített.

Telepítés lépései (GUI):

1. Nyisd meg a Server Manager
2. Manage → Add Roles and Features
3. Features résznél jelöld be:
    - Windows Server Backup
4. Next → Install
5. Telepítés után nem szükséges újraindítás

Windows Server Backup megnyitása

1. Server Manager
2. Tools → Windows Server Backup

Megnyílik a WSB konzol.

Mentési konfigurációk

Egyszeri mentés (One-time backup)

Lépések:

1. Jobb oldalon Local Backup
2. Action → Backup Once
3. Válaszd:
    - Scheduled Backup options (ha már van ütemezés)
    - Different options (legtöbbször ez)

Mentés típusa

- Full server
- Custom
    - Custom esetén kiválasztható:
        - Kötetek
        - Fájlok
        - System State

Cél kiválasztása

- Local drives
- Remote shared folder

Ütemezett mentés (Scheduled backup)

Ez a legfontosabb vizsgán és gyakorlatban.
Lépések:

1. Local Backup → Backup Schedule
2. Backup Configuration Wizard indul

Mentési mód

- Full Server (gyors visszaállítás)
- Custom (erőforrás kímélő)

Ütemezés

- Naponta egyszer
- Naponta többször (pl. 4 óránként)

Visszaállítás (Recovery)

Lépések:

1. Windows Server Backup
2. Recover
3. Backup hely kiválasztása
4. Recovery típus:
    - Files and folders
    - Volumes
    - Applications
    - System State
    - Bare metal

Távmenedzsment (pl. RSAT)

OpenSSH szerver és RDP szolgáltatás engedélyezése:

OpenSSH Server telepítése

Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

Szolgáltatás indítása és automatikusra állítása

Start-Service sshd

Set-Service -Name sshd -StartupType Automatic

Tűzfal engedélyezése SSH-hoz

New-NetFirewallRule -Name "OpenSSH-In" -DisplayName "OpenSSH Server" -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

RDP engedélyezése

Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections" -Value 0

Tűzfal engedélyezése RDP-hez

Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

#felhasználó hozzáadása az RDP-hez

Add-LocalGroupMember -Group "Remote Desktop Users" -Member "Administrator"

#NLA kikapcsolása

Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -Name "UserAuthentication" -Value 0

GUI-ban RDP:

Start → Server Manager

Local Server

Remote Desktop: Disabled

Allow remote connections to this computer

Apply

RDP port: 3389

User jogosultság: Select Users…

utána: másik gépről –
mstsc

Távoli asztali kapcsolat

192.168.1.10 és hostname és jelszó

extra:

- Ha NLA be van kapcsolva → csak domain-tag gépek vagy modern Windowsok tudnak belépni
- Ha kikapcsolod → *bárki* tud csatlakozni, aki ismeri a felhasználónevet és jelszót

Szerveren:

A kiindulás az, hogy:

- Már fut és működik a Windows szerveren az AD DS, DNS szolgáltatás.
- A szerver domain tag

- A WinRM engedélyezve van
- A jogosultságok be vannak állítva a távmendezsmenthez

1. *Remote Management Check*
   Server Manager → Local Server

   Keresd: Remote Management (Enabled kell legyen, ha nem katt → Enable)

2. *WinRM check*
   PowerShell: winrm quickconfig

   Ha fut → kész

3. *Firewall check*
   Server Manager → Tools → Windows Defender Firewall

   Ellenőrizd inbound

   - Windows Remote Management
   - Remote Event Log
   - WMI
   - RPC

4. *Remote Desktop (nem kötelező de ajánlott)*
   Server Manager → Local Server → Remote Desktop → Enable

Kliensen:

A kiindulás az, hogy a Windows 10/11 gép:

- admin gép (tehát itt ugye fontos a jogosultság!!!)
- domain tag
- DNS működik

Helyi admin létrehozása CLI

New-LocalUser -Name "ujadmin" -Password (Read-Host -AsSecureString "Add meg a jelszót")

admin csoporthoz adása:

Add-LocalGroupMember -Group "Administrators" -Member "ujadmin"

GUI:

Gépház → Fiókok → Egyéb felhasználók → Felhasználó hozzáadása

Vezérlőpult → Felügyeleti eszközök → Számítógép-kezelés → Helyi felhasználók és csoportok

1. *RSAT telepítés*

   GUI:

   Settings → Apps → Optional Features → Add feature

   Telepítsd:

   - AD DS Tools
   - DNS Tools
   - Group Policy
   - DHCP (ha van)

   VAGY

   PowerShell:

   Az online elérhető RSAT modulok klistázása:
   Get-WindowsCapability -Name RSAT* -Online

   A parancs kimenete nem könnyen átekinthető, ezért érdemes a megjelenitendő paraméteerek számát csökkenteni:
   Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property DisplayName, State

   Az összes elérhető RSAT modul telepítése:
   Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online

VPN

1. Nyisd meg a Server Manager → Add Roles and Features
2. Válaszd a Role-based or feature-based installation lehetőséget → Next
3. Válaszd ki a szervert → Next
4. A Roles listából pipáld ki:
   - Remote Access
   - Ezután jelöld a DirectAccess and VPN (RAS) szerepkört
5. A Features résznél hagyd az alapértelmezettet → Next
6. Telepítsd a szerepkört → várd meg a telepítést → Close
7. Nyisd meg a Server Manager → Tools → Routing and Remote Access
8. Jobbklikk a szerver nevére → Configure and Enable Routing and Remote Access
9. Válaszd a Custom Configuration → Next
10. Pipáld ki a VPN Access → Next
11. Indítsd újra a szolgáltatást, ha kéri
12. Ekkor a szerver készen áll VPN kapcsolatok fogadására

VPN taromány és címek beállítása

1. RRAS → jobbklikk a szerver → Properties
2. Menj a IPv4 fülre → Static address pool → add hozzá a VPN klienseknek szánt IP-cím tartományt (pl. 192.168.100.50–192.168.100.100)
3. Alternatív: DHCP szervert is használhatsz
4. Győződj meg róla, hogy a szerver útvonalat ad a VPN IP-knek az intranethez

Hitelesítés beállítás

1. RRAS → jobbklikk a szerver → Properties → Security fül
2. Válaszd az “Authentication provider”-t:
    - Windows Authentication (Active Directory felhasználók)
    - RADIUS (külső AAA szerver)
3. PPTP esetén: MS-CHAP v2
4. L2TP/IKEv2 esetén: előre megosztott kulcs (PSK) vagy tanúsítvány szükséges

VPN kliens

1. Settings → Network & Internet → VPN → Add a VPN connection
2. Töltsd ki:
    - VPN provider: Windows (built-in)
    - Connection name: pl. Cég VPN
    - Server name or address: szerver publikus IP-je vagy DNS neve
    - VPN type: L2TP/IPsec with pre-shared key
    - Pre-shared key: amit a szerveren beállítottál
    - Sign-in info: felhasználónév/jelszó (AD felhasználó)
3. Mentés → Connect

IIS

1. IIS telepítése GUI használatával
    1. *Server Manager megnyitása*
        - Kattints a Start menüre → Server Manager.
        - Vagy keresd a Server Manager-t a keresőben.
    2. *Role & Feature hozzáadása*
        - Server Manager → Manage → Add Roles and Features.
        - Válaszd a Role-based or feature-based installation lehetőséget.
        - Válaszd ki a szervert, amin telepíteni szeretnéd.
    3. *IIS szerepkör kiválasztása*
        - A Server Roles listában pipáld ki az Web Server (IIS) lehetőséget.

- Megjelenik egy ablak a szükséges funkciókkal → Add Features gomb.

4. *Feature-ek kiválasztása (opcionális)*
   - Alapértelmezett feature-ek elegendőek a legtöbb webkiszolgálóhoz.
   - Ha szükséges, pipálhatod a .NET Extensibility, ASP.NET, WebDAV Publishing, FTP Server funkciókat.
5. *Telepítés*
   - Kattints a Install gombra.
   - A telepítés után ellenőrizheted az IIS működését: nyisd meg a böngészőt → http://localhost → a "Welcome to IIS" oldalnak kell megjelennie.

2. IIS GUI alapú kezelése
   - Nyisd meg az Internet Information Services (IIS) Manager-t:
     - Start → IIS Manager
     - Vagy inetmgr parancs a Futtatás ablakból (Win+R)

Fő ablak felépítése:

- Connections panel: a szerver, site-ok és alkalmazások hierarchiája.
- Features View: kiválasztott webhelyhez tartozó beállítások.
- Actions panel: gyors műveletek (pl. Start, Stop, Restart, Add Website).

3. Webhely létrehozása GUI-ban
   1. *Jobb klikk a Sites → Add Website...*
      - Site name: A webhely neve.
      - Physical path: Mappa az alkalmazásfájloknak.
      - Binding:
        - IP Address: Minden IP vagy konkrét IP.
        - Port: 80 (HTTP), 443 (HTTPS).
        - Host name: pl. www.example.com (ha több domain ugyanazon IP-n).
   2. *Alkalmazás pool hozzárendelése*
      - Alapértelmezett: DefaultAppPool.
      - Külön alkalmazás pool létrehozása:
        - Application Pools → Add Application Pool → név, .NET verzió, pipeline mode.
      - Alkalmazás pool beállításai:
        - Managed pipeline mode: Integrated (általában).
        - .NET CLR version: pl. v4.0.
        - Start application pool immediately: pipáld be.

4. Alapvető konfigurációk IIS-ben
   1. *Authentication (Hitelesítés)*

- IIS Manager → kiválasztott webhely → Authentication
    - Anonymous Authentication: alapértelmezett engedélyezett.
    - Windows Authentication: csak intranetes oldalakhoz.
    - Basic / Digest Authentication: opcionális, HTTPS mellett.

2. *Authorization Rules (Engedélyezési szabályok)*
    - Kiválasztott webhely → Authorization Rules
        - Alapértelmezett: mindenki hozzáfér.
        - Lehet szabályozni felhasználó, csoport, IP alapján.

3. *MIME Types*
    - Meghatározza, hogy a szerver milyen fájlformátumokat szolgálhat ki.
    - Példa: .json → application/json.

4. *SSL / HTTPS konfiguráció*
    - Webhely → Bindings → Edit → HTTPS
    - Szükséges SSL Certificate telepítése a szerverre.
    - Port: 443
    - SSL/TLS beállítások az SSL Settings panelen:
        - Require SSL: pipáld be, ha kötelező a titkosított kapcsolat.
        - Client certificates: Optional vagy Required.

5. Alkalmazás pool konfiguráció
    1. *Alkalmazás pool beállításai*
        - Start / Stop / Recycle.
        - Advanced Settings:
            - Identity: alkalmazás futtatása rendszer- vagy felhasználói fiókkal.
            - Idle Time-out: alapértelmezett 20 perc.
            - Recycling: naponta, heti vagy CPU használat alapján újraindítás.

    2. *Teljesítmény optimalizálás*
        - Maximum worker processes (web garden): több processz párhuzamos futtatása.
        - Rapid-fail protection: automatikusan leállítja a problémás alkalmazást.

6. Logging és monitoring
    - IIS Manager → kiválasztott webhely → Logging
        - Alapértelmezett: **<SystemDrive>\inetpub\logs\LogFiles**
        - Log format: W3C, UTF-8, daily rollover.

    - Monitoring:
        - Worker Processes: futó folyamatok.
        - Requests: per-site statisztika.

Linux szerverek

Hostname megváltoztatása:

- sudo hostnamectl set-hostname linux-srv

linux szerver tartományba léptetése:

ehhez csomagok telepítése –

- sudo apt update
- sudo apt install realmd sssd adcli samba-common-bin -y

tartomány keresése –

- realm discover fesztival.lan

beléptetés:

- sudo realm join -U Administrator fesztival.lan

SeDiskOperatorPrivilege kiosztása a Domain Admins csoportnak: Ez a samba jogosultság kiosztása

- sudo net rpc rights grant "FESZTIVAL\Domain Admins" SeDiskOperatorPrivilege -U "Administrator"

OpenSSH és Apache2 telepítése:

sudo apt update

sudo apt install openssh-server -y

systemctl status ssh

sudo apt install apache2 -y

sudo ufw allow OpenSSH

sudo ufw allow 'Apache Full'

sudo ufw enable

UFW tűzfal beállítása:

alapértelmezett tiltás:

- sudo ufw default deny incoming
- sudo ufw default allow outgoing

Engedélyezett szolgáltatások:

- sudo ufw allow 'Apache Full'
- sudo ufw allow OpenSSH
- sudo ufw allow Samba

sudo ufw enable

VIM használata:

sudo apt-get install vim -y

cím, dns és gateway beállítása:

sudo vim /etc/network/interfaces

iface enp0s8 inetc static

address 192.168.13.50

netmask 255.255.255.0

gateway 192.168.13.1

dns-nameservers 192.168.13.10

dns-search fesztival.lan

mentés:

ESC

:wq

Enter

Hálózat újraindítása:

sudo systemctl restart networking

Ellenőrzés:

ip a

ip route

cat /etc/resolv.conf

Megosztási könyvtár létrehozása

Könyvtár létrehozása:

sudo mkdir -p /mnt/sdb1/shares

Csoport beállítása:

sudo chown root:"Domain Admins" /mnt/sdb1/shares

Jogosultságok:

sudo chmod 770 /mnt/sdb1/shares

Samba megosztás létrehozása

Nyisd meg a Samba configot:

sudo nano /etc/samba/smb.conf

Add hozzá a végére:

[shares]

path = /mnt/sdb1/shares

browseable = yes

writable = yes

valid users = @"FESZTIVAL\Domain Admins"

force group = "Domain Admins"

create mask = 0770

directory mask = 0770

Samba újraindítása:

sudo systemctl restart smbd

Roaming profil beállítása Windows 10 kliensen

1) Nyisd meg a Server Manager → File and Storage Services → Shares

2) Keresd meg a Linux Samba megosztást

3) Jogosultságok módosítása Domain Admins számára

4) Felhasználó profiljának beállítása:

Active Directory Users and Computers → Felhasználó → Properties → Profile fül:

Profile path: \\linux-szerver\shares\%username%

interface felkapcsolasa:

- sudo ip link set eth0 up

cimzes :

Address

- Netmask
- Gateway
- Nameserver

Particionálás (fdisk)

sudo fdisk /dev/sdb

n → új partíció

p -> elsődleges

d -> ha törölni akarom

méret megadása:

utolsó szektor: +7,5G

w → mentés

Fájlrendszer létrehozása

mkfs.ext4 /dev/sdb1

mkfs.xfs /dev/sdb2

Csatolási pont létrehozása

mkdir -p /mnt/disk1

mkdir -p /mnt/disk2

Csatolás

mount /dev/sdb1 /mnt/disk1

mount /dev/sdb2 /mnt/disk2

lecsatolás utána:

umount /mnt/disk1

umount /mnt/disk2

fstab

UUID lekérése: blkid /dev/sdb1

UUID=xxxx /mnt/disk1 ext4 defaults 0 2

teszt: sudo mount -a

Fájlhozzáférések, ACL-ek

Jogosultságok megtekintése – ls -l

Jogosultságok módosítása – chmod

chmod u+rwx file

chmod g-w file

chmod o-rwx file

chmod u=rw,g=r,o= file

Oktális mód (gyors, profi)

Jog	Érték
r	4
w	2
x	1

chmod 755 script.sh → rwx r-x r-x (tipikus könyvtárakra, binárisokra)

chmod 644 index.html → rw- r-- r-- (tipikus fájlokra)

chmod 700 secret.txt → rwx --- --- (csak tulajdonos fér hozzá)

chmod 770 shared_folder → rwx rwx --- (csoportmunka)

Tulajdonos és csoport módosítása – chown, chgrp

Tulajdonos módosítása: sudo chown marco file.txt

Tulajdonos + csoport módosítása: sudo chown marco:admins file.txt

Csak csoport módosítása: sudo chgrp admins file.txt

Rekurzív mód (könyvtárakra): sudo chown -R www-data:www-data /var/www

ACL – finomhangolt jogosultságok

setfacl -m u:marco:rwx /mnt/disk1

setfacl -m g:developers:rx /mnt/disk1

ACL törlése: setfacl -x u:marco /mnt/disk1

ACL megtekintése: getfacl /mnt/disk1

Fájlrendszer parancsok

- ls -l
- cp file1 file2
- mv file1 file2
- rm file
- mkdir dir
- rmdir dir
- touch file

Keresés + számlálás

grep "error" logfile | wc -l

Hozzáfűzés: echo "new line" >> file.txt

DHCP szerver

DHCP szerver telepítése: sudo apt install isc-dhcp-server

Konfigurációs fájl: /etc/dhcp/dhcpd.conf

Interfész beállítása: /etc/default/isc-dhcp-server

DHCP konfiguráció - Példa egy 10.50.10.0/24 hálózatra:

```
subnet 10.50.10.0 netmask 255.255.255.0 {
  range 10.50.10.100 10.50.10.200;
  option routers 10.50.10.254;
  option domain-name-servers 10.50.10.10;
  option domain-name "cloudforge.local";
  default-lease-time 600;
  max-lease-time 7200;
}
```

DHCP szolgáltatás újraindítása:

- sudo systemctl restart isc-dhcp-server
- sudo systemctl status isc-dhcp-server

DNS szerver

DNS szerver telepítése: sudo apt install bind9

/etc/resolv.conf

- `nameserver 10.50.10.10`
- `nameserver 8.8.8.8`

curl http://10.50.10.10

DNS teszt: nslookup cloudforge.local, dig cloudforge.local

Forward zóna létrehozása

/etc/bind/named.conf.local:

zone "cloudforge.local" {

type master;

file "/etc/bind/db.cloudforge.local";

};

Zónafájl:

$TTL 86400

@ IN SOA ns1.cloudforge.local. admin.cloudforge.local. (

1 ; Serial

3600 ; Refresh

1800 ; Retry

604800 ; Expire

86400 ; Minimum TTL

)

@ IN NS ns1.cloudforge.local.

ns1 IN A 10.50.10.10

www IN A 10.50.10.10

Reverse zóna

zone "10.50.10.in-addr.arpa" {

type master;

file "/etc/bind/db.10.50.10";

};

Reverse rekord:

10 IN PTR www.cloudforge.local.

DNS újraindítása: sudo systemctl restart bind9

Tesztelés:

- nslookup www.cloudforge.local
- dig www.cloudforge.local

Routing + NAT

Új route hozzáadása: sudo ip route add 10.0.0.0/24 via 192.168.1.1

Default route: sudo ip route add default via 10.50.10.254

NAT (masquerade): sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

IP forwarding engedélyezése:

- sudo nano /etc/sysctl.conf
- net.ipv4.ip_forward=1

Apache2

Webroot: /var/www/html

VirtualHost: /etc/apache2/sites-available/000-default.conf

Példa saját weboldalra:

- sudo nano /etc/apache2/sites-available/cloudforge.conf

tartalom:

- <VirtualHost *:80>
- ServerName cloudforge.local
- DocumentRoot /var/www/cloudforge
-
- <Directory /var/www/cloudforge>
- AllowOverride All
- Require all granted
- </Directory>
-
- ErrorLog ${APACHE_LOG_DIR}/cloudforge_error.log
- CustomLog ${APACHE_LOG_DIR}/cloudforge_access.log combined
- </VirtualHost>

Aktiválás:

- sudo a2ensite cloudforge.conf
- sudo systemctl reload apache2

Webroot létrehozása és jogosultságok:

- sudo mkdir /var/www/cloudforge
- sudo chown -R www-data:www-data /var/www/cloudforge
- sudo chmod -R 755 /var/www/cloudforge

Tesztoldal:

- echo "Hello CloudForge" | sudo tee /var/www/cloudforge/index.html

Modulok listázása:

- apache2ctl -M

Modul engedélyezése:

- sudo a2enmod rewrite
- sudo systemctl restart apache2

Logok

/var/log/apache2/access.log

/var/log/apache2/error.log

élő nézet: tail -f /var/log/apache2/error.log

UFW alapok

- ufw default deny incoming
- ufw default allow outgoing
- ufw allow 80/tcp
- ufw enable

Statikus címzés

- auto enp0s8
- iface enp0s8 inet static
    - address 10.50.10.10
    - netmask 255.255.255.0
    - gateway 10.50.10.254
    - dns-nameservers 10.50.10.10

Újraindítás:

- sudo systemctl restart networking

Felhőszolgáltatások

RDS (ADATBÁZIS)

Lépések:

- Create database
- Engine: MySQL
- Name:

web-server-database-<monogram>

⚠️ **FONTOS:**

- Username: default
- Password: jegyezd meg!!!
- Connectivity:
    - EC2-hez kapcsolni

Kulcs betöltése:

- bal oldalon:

Connection → SSH → Auth → Credentials

- Private key file → .ppk fájl

⚠️ **HIBA:**

- “Connection timed out” → Security Group rossz
- “Access denied” → rossz user

APACHE TELEPÍTÉS

🎯 Cél:

Webszerver működjön

```
sudo apt install apache2 -y
```

▶️ Ellenőrzés:

```
systemctl status apache2
```

WEBOLDAL MAPPA

🎯 **Cél:**

Ide kerül a WordPress

---

cd /var/www/
ls

👉 itt van:

html

Új mappa:

sudo mkdir wordpress

FELHASZNÁLÓ LÉTREHOZÁSA (FTP)

🎯 **Cél:**

WinSCP-vel tudj feltölteni

---

sudo adduser webuser

👉 jelszó megadása!

Jogosultság:

sudo chown -R webuser:webuser /var/www/wordpress

🔒 **Chroot (vizsgán fontos lehet!):**

sudo usermod -d /var/www/wordpress webuser

PHP TELEPÍTÉS

🎯 **Cél:**

WordPress működés

---

sudo apt install php php-mysql libapache2-mod-php -y

php -v

APACHE KONFIGURÁLÁS

🎯 **Cél:**

A wordpress mappát szolgálja ki

---

1. Konfig fájl létrehozás:

sudo nano /etc/apache2/sites-available/wordpress.conf

Bele:

```
<VirtualHost *:80>
   ServerName example-<monogram>.ddns.net
   DocumentRoot /var/www/wordpress

   <Directory /var/www/wordpress>
      AllowOverride All
      Require all granted
   </Directory>
</VirtualHost>
```

Aktiválás:

sudo a2ensite wordpress.conf
sudo a2enmod rewrite
sudo systemctl reload apache2

ADATBÁZIS KAPCSOLAT TESZT

🎯 **Cél:**

EC2 látja-e az RDS-t

Telepíts MySQL klienst:

sudo apt install mysql-client -y

Kapcsolódás:

mysql -h <RDS endpoint> -u admin -p

WordPress DB létrehozás:

CREATE DATABASE wordpress;

SSL (HTTPS) – TELJES FOLYAMAT

🚀 6.1. CERTBOT TELEPÍTÉS

sudo apt install certbot python3-certbot-apache -y

6.2. TANÚSÍTVÁNY KÉRÉS

sudo certbot --apache

Kérdések:

- Email → add meg
- Terms → YES
- Domain →

example-<monogram>.ddns.net

Redirect:

👉 válaszd:

2: Redirect

WORDPRESS TELEPÍTÉS – FULL

🚀 7.1. LETÖLTÉS

cd /tmp
wget https://wordpress.org/latest.zip

KICSOMAGOLÁS

unzip latest.zip

ÁTMÁSOLÁS

sudo cp -r wordpress/* /var/www/wordpress/

JOGOSULTSÁGOK

sudo chown -R www-data:www-data /var/www/wordpress
sudo chmod -R 755 /var/www/wordpress

TELEPÍTÉS BÖNGÉSZŐBEN

Megnyitod:

https://domain

KÉSZ

Belépés:

https://domain/wp-admin

UTOLSÓ BIZTONSÁG

sudo chmod -R 750 /var/www/wordpress

Mi az RDS endpoint?

👉 Az **RDS endpoint** = az adatbázis “címe”, amin keresztül a szerver (EC2) csatlakozik hozzá.

Olyan, mint egy domain/IP, pl:

web-server-database-xyz.abcd1234.eu-central-1.rds.amazonaws.com

1. Menj ide:

AWS → **RDS**

---

2. Bal oldalon:

👉 **Databases**

---

3. Kattints az adatbázisodra:

(pl.)

web-server-database-<monogram>

---

4. Keresd meg ezt a részt:

👉 **Connectivity & security**

---

5. Itt lesz:

Szakma jegyzet

Endpoint

👉 mellette egy hosszú cím

AWS közös jegyzet alapjan

sorrend:

1. EC2 létrehozás
2. Apache/PHP telepítés
3. RDS létrehozás
4. DB user + DB
5. WordPress összekötés
6. jogosultságok
7. browser setup

https://drive.google.com/file/d/1vDjwI4S1zuTizs_hJRyT1KZ2jktnWv39/view?usp=sharing

jelszó hozzá: G1mcI@ZXJZds!eRs5?e3

sudo apt update && sudo apt upgrade -y

sudo apt install -y apache2

sudo mkdir /var/www/example

sudo chmod 777 /var/www/example

parancsok textben

sudo apt update && sudo apt upgrade -y

sudo apt install -y apache2

sudo mkdir /var/www/example

sudo chmod 777 /var/www/example

sudo addgroup sftponly

sudo adduser sftpawsweb

sudo usermod -d /var/www sftpawsweb

```
sudo usermod -aG sftponly sftpawsweb
sudo usermod -aG www-data sftpawsweb
sudo chown -R sftpawsweb:www-data /var/www/example

sudo nano /etc/ssh/sshd_config
# Subsystem sftp internal-sftp
# Match Group sftponly
# ChrootDirectory /var/www/
# ForceCommand internal-sftp
# PasswordAuthentication yes
# AllowTcpForwarding no
# X11Forwarding no

sudo systemctl restart ssh

sudo ufw app list
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow in 'Apache Full'
sudo ufw allow in 'OpenSSH'
sudo ufw allow 20,21,990/tcp
sudo ufw enable
sudo ufw status verbose

sudo nano /etc/apache2/apache2.conf
# ServerName localhost

sudo nano /etc/apache2/sites-available/example.conf
```

```
# <VirtualHost *:80>
#    ServerName example-bp.ddnsfree.com
#    ServerAlias www.example-bp.ddnsfree.com
#    DocumentRoot /var/www/example
#    ErrorLog ${APACHE_LOG_DIR}/baseline-error.log
#    CustomLog ${APACHE_LOG_DIR}/baseline-access.log combined
# </VirtualHost>

sudo a2ensite example.conf
sudo a2dissite 000-default.conf
sudo apache2ctl configtest
sudo systemctl restart apache2

sudo su
apt install -y lsb-release ca-certificates apt-transport-https wget
mkdir -p /etc/apt/keyrings
wget -O /etc/apt/keyrings/deb.sury.org-php.gpg
https://packages.sury.org/php/apt.gpg
echo "deb [signed-by=/etc/apt/keyrings/deb.sury.org-php.gpg]
https://packages.sury.org/php/ \
$(lsb_release -sc) main" | sudo tee /etc/apt/sources.list.d/php.list
apt update
apt install -y php8.4 libapache2-mod-php8.4 php8.4-cli php8.4-fpm php8.4-mysql
php8.4-opcache \
php8.4-mbstring php8.4-intl php8.4-xml php8.4-gd php8.4-zip php8.4-curl php8.4-
xmlrpc php8.4-cgi

a2enmod proxy_fcgi setenvif
a2enconf php8.4-fpm
```

systemctl restart apache2

php -v

sudo nano /etc/apache2/mods-enabled/dir.conf

DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm

sudo systemctl restart apache2

sudo systemctl status apache2

SSL tanusitvany kikapcsolasa:

mysql -h fesztival-cms-databasee.czvytxikun9o.us-east-1.rds.amazonaws.com -P 3306 -u admin -p --skip-ssl

------- SSL tanusitvany hiba eseten

sudo apt install -y mariadb-client

mysql -h web-server-database.cfeeww6usdtm.us-east-1.rds.amazonaws.com -P 3306 -u admin -p

CREATE DATABASE wordpress;

SHOW DATABASES;

quit

FONTOS, hogy pontosvessző kell a végükre

sudo apt install -y certbot python3-certbot-apache

sudo certbot –apache