Harkály Krisztián, Számadó Milán, Horváth Márió

Záróvizsga 5. csoport

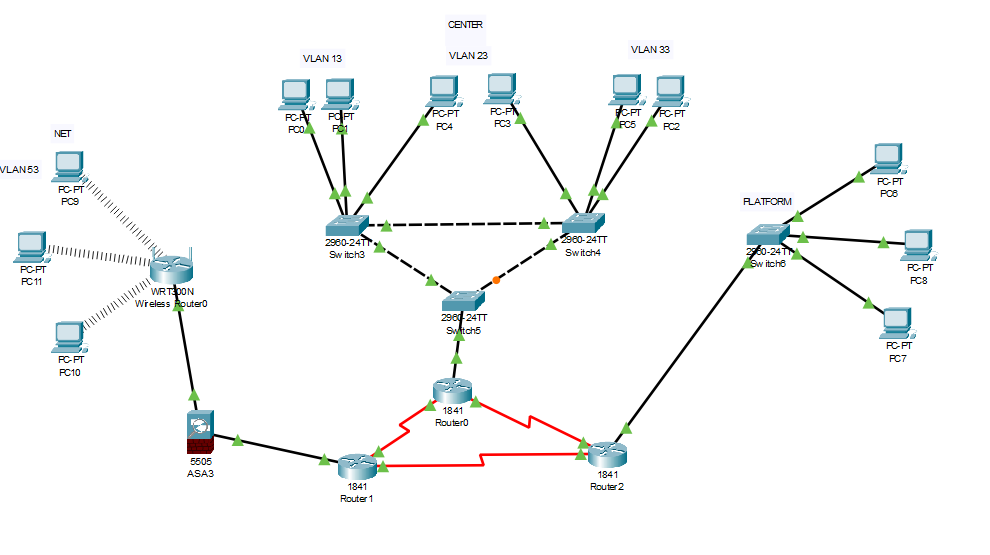
**13.B**

**Bevezetés a projekthez**

**A projekt:**

Egy közepes méretű vállalatnak három telephelyét megterveztük. A rendszer támogatja a vállalat összes technikai igényét

**A hálózati topológia:**

****

Három telephelyet tartalmaz a vállalkozás hálózatja:

Az első telephely a Center telephely – ez lenne a fő adatközpont. Itt található a menedzsment.

Több szintű VLAN került kialakításra. Három VLAN lett létrehozva a telephelynél: VLAN 13, az adminisztrációs VLAN, VLAN 23: az IT VLAN. VLAN 33: Ez nem más, mint a vendéghálózat.

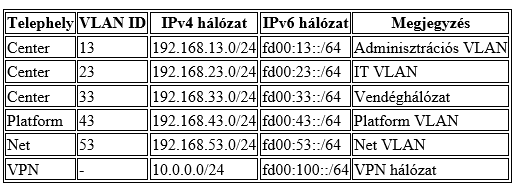
Ennél a telephelynél használtunk redundans forgalomirányítókat és kapcsolókat (a használt redundancia technológiája: HSRP és VRRP). Szükség volt a telephelynél a WLAN hozzáférési pontok használata (802.1x alapú hitelesítéssel). Az eszközökön elvégeztünk statikus és dinamikus IPv4, illetve IPv6 címzést is.

A második telephely a Platform telephely – ez a gyártás és a logisztikai telephely. Szintén található ennél a telephelynél egy VLAN: VLAN 43. Ez a gyártási folyamatok VLAN. A központi irodához (vagyis a Center telephelyhez) VPN kapcsolódás áll rendelkezésre. A VPN IPsec alapú. A telephelyen rendelkezésre áll egy helyi DHCP és DNS szolgáltatás redundanciával.

A harmadik telephely a Net telephely – az ügyfélszolgálat és az értékesítés telephelye. Itt található meg az értékesítési VLAN. Ennél a telephelynél rendelkezésre áll egy WLAN hozzáférési pont: egy Cisco WRT300N Wireless Router, ami a vezetéknélküli kapcsolatot biztosítja. Három eszköz van csatlakozva a hálózathoz a wireless routeren keresztül. Dinamikus címfordítást végeztünk (NAT és PAT).

Az összes telephelyek között rendelkezésre áll egy MPLS (Multiprotocol Label Switching) kapcsolat. Tartalékkapcsolatként IPsec VPN-t építettünk be. Az internetelérés a központi irodán keresztül történik.

**Hálózat címzési terv:**



Az összes telephelynél alkalmaztunk statikus és dinamikus IPv4/IPv6 címzést. Több VLAN ID kiosztásra került: három VLAN a Center telephely, és egy a Platform és a Net telephelyen.

**Feladatleírás:**

* Létrehoztuk a hálózat topológiáját a Cisco Packet Tracer szimulációs környezetben. Megterveztük az alhálózatokat, és a címzési struktúrát.
* Konfiguráltuk az összes hálózati eszközöket, mint például a forgalomirányítókat, és a kapcsolókat.
* Implementáltuk forgalomirányítást a VLAN-ok között. A redundáns protokolokat (HSRP, VRRP) használjuk a hálózat kiépítésében. A WLAN hozzáférés WPA3 titkosítással történt meg, 802.1x hitelesítéssel egyaránt.
* Alkalmaztuk az IPv4 és IPv6 címzést, konfiguráltuk a statikus és dinamikus routing protokolokat (mint például az OSPFv2, az OSPFv3, és az EIGRP.) Beépítettük a NAT és a PAT megoldásokat.
* A hálózaton két kiszolgáló található: egy Linux kiszolgáló, és egy Windows Server alapú kiszolgáló.
* A Linux kiszolgálón egy Debian 12.10 rendszer fut, és bizonyos szolgáltatásokat futtatunk ezen a szervergépen.
* Ezek között találhatóak a DHCP szerver, a DNS szerver, A HTTP/HTTPS webszerver (Apache2 webszerver-t használunk.) Egy Samba fájlszervert is futtatunk a szerveren, főleg biztonsági mentésekre.
* A Windows kiszolgálón egy 64-bites Windows Server 2019 fut.
* Ez a kiszolgáló főleg egy Active Directory tartományvezérlő számára áll rendelkezésre, de fut rajta sok más szolgálatás, mint például egy fájlszerver, és nyomtatómegosztás.
* Csoportházirendekkel be van állítva az automatizált szoftvertelepítés az összes számítógépre a domainen.
* A hálózat biztonságára figyeltünk, beállítottuk az ACL-eket a fontos, érzékeny adatok védelmére.
* Hardveres tűzfalat használunk a védelemért, egy Cisco ASA 5505 eszközt.
* Ez alkalmas nekünk a hálózat hardveres tűzfal védelmére, és illetve még egy IPsec alapú VPN-t is biztosít.
* Teszteltük a telephelyek közötti kommunikáció, minden lezajlott sikeresen és bizonságosan, semmiféle hiba nélkül.
* Ping és traceroute alapú tesztelés sikeres volt. Ellenőriztük az ACL-eket, a VLAN-okat, és a VPN működését, ami szintén sikeresen lezajzlott.

**VPN:** A VPN a Virtual Private Network rövidítése. Általában a nyílt hálózaton egy privát alagút használatáról van szó, amelyen titkosított forgalom zajlik. A távoli elérése egy IPsec alapú VPN-en keresztül jön létre.

**DHCP:** A DHCP a Dynamic Host Configuration Protocol rövidítése. Ezzel dinamikusan ki tudjuk osztani az IP címeket.

**ACL:** Az ACL tulajdonképpen engedélyező és tiltó utasítások szekvenciális sorozata, amelyeket címekre, portokra, szolgáltatásokra vagy felsőbb rétegbeli protokollokra alkalmazhatunk. Ezek a listák határozzák meg a forgalomirányító számára, hogy mely csomagokat fogadja el és melyeket utasítsa vissza. Ezzel az ACL, lehetővé teszi a forgalom felügyeletét, s a meghatározott csomagok ellenőrzését is.

**VLAN:** A számítógép-hálózatok körében a virtuális helyi hálózat vagy látszólagos helyi hálózat (rövidebben virtuális LAN, virtual LAN, azaz VLAN) hálózati eszközök egy olyan csoportja, aminek tagjai úgy kommunikálnak, mintha ugyanabba a szórási tartományba tartoznának, fizikai elhelyezkedésüktől függetlenül.

**NAT:** A NAT a Network Address Translation rövidítése, magyarul címfordítás.

Háromféle NAT létezik:

1. statikus NAT
2. dinamikus NAT
3. kiterjesztett NAT (PAT)

**MPLS:** Az MPLS (Multiprotocol Label Switching) egy sokoldalú megoldás, amely a mai hálózatok által tapasztalt problémákra - sebesség, skálázhatóság, szolgáltatásminőség (QoS) menedzsment és forgalomirányítás - kínál megoldást. Az MPLS az adatokat egyik hálózati csomópontból a másikba rövid útvonalcímkék alapján irányítja, ahelyett hogy hosszú hálózati címeket használna.

**HTTP:** A HTTP (HyperText Transfer Protocol) egy információátviteli protokoll elosztott, kollaboratív, hipermédiás, információs rendszerekhez. A http egy kérés-válasz alapú protokoll kliens és szerver között. A webszerverek ezt a protokollt használják, a HTML fájlokat kiszolgálja a kliensekhez.

**IPsec:** Az Internet Protocol Security (IPsec) egy biztonságos hálózati protokollcsomag, amely hitelesíti és titkosítja az adatcsomagokat, hogy biztonságos, titkosított kommunikációt biztosítson két számítógép között.

**Eszközök**

**2960-24 Switch**

A Cisco Catalyst 2960-24 egy 24 portos, Layer 2-es switchekhez tartozó eszköz. A Cisco 2960-24 a Catalyst 2960 sorozat tagja.

**Főbb jellemzők:**

**1.Portok és teljesítmény**: A 2960-24 switch 24 darab 10/100 Mbps Ethernet porttal rendelkezik, amelyek biztosítják a gyors adatátvitelt és alacsony késleltetést a csatlakoztatott eszközök között, amely lehetővé teszi az intenzívebb adatforgalom kezelését, miközben a kisebb igényű alkalmazások számára is optimális sebességet biztosít. 2 uplink port 10/100/1000 Mbps sebeséggel rendelkezik. 16Gbps kapacitása van a switchnek, 16 MB DRAM-al rendelkezik.

**2.Kezelhetőség:** A Cisco Catalyst 2960-24 switch teljes mértékben menedzselhető, a soros konzol segítségével kezelhető a switch. A felületben beállítható bizonyos technológiák, mint például az SPAN, RSPAN, CiscoView, Cisco Discover Protocol (CDP), VTP (Virtual Trunking Protocol), BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clusterezés, és a Web alapú kezelhetőség.

**3.Hálózati biztonság**: A Cisco 2960-24 beépített biztonsági funkciókkal rendelkezik, mint például az 802.1X port alapú hitelesítés, amely lehetővé teszi, hogy a hálózathoz csak megfelelően hitelesített eszközök csatlakozhassanak. Ezen kívül támogatja a VLAN-ok (Virtuális Lokális Hálózatok) használatát, amellyel a hálózaton belül különböző szegmensek hozhatók létre.

**Cisco ASA 5505**

**A Cisco ASA 5505** egy új generációs, teljes funkcionalitású biztonsági készülék kisvállalkozások, fiókirodák és vállalati távmunkás környezetek.

**Főbb jellemzők:**

**1. Típus:** Integrált tűzfal és VPN eszköz.

**2.Ethernet portok:** 8 db 10/100 Mbps Ethernet port, amelyek közül 8 portot használhatsz (6 alapértelmezett adatport és 2 "secure" port).

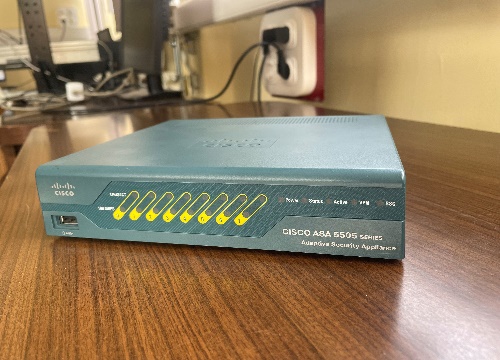
Console, USB port: 1 db konzolport (RJ-45), 1 db USB port (például szoftverfrissítéshez vagy mentésekhez).

**3.VPN teljesítmény:** Akár 25 IPsec VPN kapcsolatot támogat egyszerre.

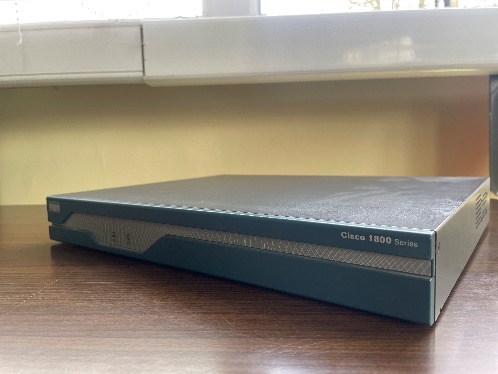
**4.Maximális párhuzamos kapcsolat**: 10 000 kapcsolatra képes. Ez a kis eszköz alapvető tűzfal, VPN és biztonsági feladatokat lát el, de nem igazán skálázható nagyobb vállalati környezetekhez.

**5.Biztonság**: Tűzfal, VPN, IDS/IPS alapú védelem.

**6. Támogatott licenszek**: A modellek lehetnek "Base" vagy "Security Plus" licensszel, ami extra funkciókat ad (pl. VPN bővítés).



**1841 Router**

**Főbb jellemzők:**

**1.Teljesítmény:** Ötszörös útválasztási teljesítménynövekedés a Cisco 1700 sorozathoz képest.

Az új generációs nagysebességű WAN-interfészkártyák (HWIC) támogatása. Több modulhely és nagyobb teljesítmény az interfészkártyákhoz

**2.Portok:** Opcionális beépített 10/100 megabites kapcsoló és két beépített 10/100 megabites LAN-port. USB-port jöv őbeli alkalmazásokhoz, például a VPN-hitelesítési adatok készüléken kívüli tárolásához.

**3.Alkalmazások:** Megnövekedett rugalmasság a gyorsabb VPN-kapcsolat és a jövőbeli alkalmazások számára készült belső AIM-modulhely révén.

**4.QoS (Quality of Service):** A minőségszolgáltatás támogatása, amely lehetővé teszi az adatok forgalmának priorizálását (pl. VoIP hívások vagy videókonferenciák).

**5.NAT (Network Address Translation):** A NAT támogatása lehetővé teszi több eszköz használatát egyetlen publikus IP címmel.

**Cisco 867VAE-W-E-K9**

1. Jellemzők és előnyök
2.  A Cisco 860VAE sorozatú ISR-ek belépő szintű, fix konfigurációjú útválasztók
3. Költséghatékony alap- vagy biztonságos kapcsolat minőségi szolgáltatással (QoS) a távmunkások számára és felügyelt CPE-eszközök a szolgáltatók számára
4. Három 10/100 Fast Ethernet switch port és két Gigabit Ethernet switch port a 2,4 GHz-es 802.11n FCC- vagy ETSI-kompatibilis vezeték nélküli LAN-nal rendelkező vezeték nélküli modellekben
5. Egy USB 2.0 port az USB-ről történő rendszerindításhoz vagy a konfiguráció betöltéséhez
6. IPv6 támogatás minden modellen
7. A Cisco 860VAE útválasztók támogatják a Gigabit Ethernet (GE) vagy a nagyon nagy sebességű DSL 2/aszimmetrikus DSL2+ (VDSL2/ADSL2+) szabványt egyetlen rögzített ISR-en.