IP címek kiosztása

Az IP címek megfelelő kezelése és kiosztása elengedhetetlen egy hálózatnál manapság, legyen szó akár kis vagy nagy cégről. Azért hogy a legjobban tudjuk beosztani a címeket VLSM-et használtunk, aminek segítségével jobban belehet osztani a címeket, mert lehetőséget ad az alhálózatokra bontásra, így többet lehet kiosztani. Az alhálózatokat úgy hoztuk létre, hogy ha a jövőben még szükség lenne plusz címekre, akkor beleférjen a már meglévő hálózatokba, de figyelembe vettük, hogy melyik részeken várható esetleges bővítés.

VLAN

VLAN-t használtunk annak érdekében, hogy a hálozatok jobban elkülöníthetőek legyenek, illetve könnyebben kezelhetőek legyenek egymástól, bizonyos lanok más prioritásokat igényelnek, így VLAN-ok segítségével megfelelően lehet ezeketet kezelni egymástól függetlenül.

A következő VLAN-ok vannak:

VLAN10 – RECEPCIÓ

* 192.168.0.192/28 -as IP cím tartomány
* Itt a következő eszközök találhatók:
  + 2 db számítógép
  + 1 db Laptop
  + 1 db nyomtató
  + 1 db TV
  + 1 db IP telefon
  + 1 db SOHO Router, hogy a vendégek számára is legyen vezeték nélküli internet elérés

A hálózat mérete miatt még bővíthető és még van hely okostelefonoknak, illetve egyéb eszközöknek is elegendő ip cím.

VLAN20 – IRODA

* 192.168.0.0/26 -os IP cím tartomány
* A földszinten található
* Itt számítógépek és nyomtatók találhatók
* A hálózatban 62 kiosztható cím van

A 62 cím elegendő, ha esetleg új alkalmazottak kerülnének felvételre.

VLAN30 – SZOFTVERFEJLESZTŐK

* 192.168.0.64/26 -os IP cím tartomány
* Az első emeleten található
* Itt számítógépek, nyomtatók és egy pár laptop található
* A hálózatban 62 kiosztható cím van

VLAN50 – VEZETŐSÉG ÉS TÁRGYALÓ TEREM

* 192.168.0.160/27 -es IP cím tartomány
* A második emeleten található
* A hálózatban 30 kiosztható IP cím van
* Itt a recepcióhoz hasonlóan ugyanazok az eszközök találhatóak

A 30 IP cím elegendő ahhoz, hogy egyszerre két konferencia is megtartásra kerüljön és még egyéb eszközöknek is marad elegendő cím, általános munkavégzéssel kapcsolatos feladatok ellátására.

Ezen az emeleten a videókonferenciához kialakított helyiségek találhatók és az eszközök ennek megfelelően lettek elhelyezve, kiválasztva. Fontos a magas sávszélesség és a stabil kapcsolat, a VoIP használatához, ezért ennek megfelelően választottunk eszközöket.

VTP

A VTP protokoll segítségével könyebben, kevesebb idő alatt fellehet konfigurálni a Kapcsolókat, hogy ugyanaz a VLAN legyen az összesen beállítva. Mindössze annyit kell tennünk, hogy beállítjuk a domaint, a jelszót és a mode-ját a Kapcsolónak. Elég csak a VTP szerveren létrehozni a VLAN-okat és ha a megfelelő Kapcsolókat beállítjuk kliensre, akkor létrehozza a VLAN-okat az adott Kapcsolón, ha transparent mode-ba rakjuk, akkor átengedi a forgalmat, de nem kapja meg a VTP beállításokat.

A hálózatban VTP version 1 van használatban, mivel nem használunk több VTP domain-t, ezért nincs szükségünk arra, hogy amielőtt megnézi a VTP által küldött advertisement-et, lecsekkolja hogy a domain name eltér-e az eszközön beállított domaintól.

Ha kiadjuk a show vtp status parancsot a következőket mutatja meg nekünk:

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírásA parancs megjelenít minden fontos információt arról hogyan van bekonfigurálva a VTP.

EtherChannel

Az EtherChannel fontos szerepet játszik az olyan hálózatokban, ahol sok, illetve nagy mennyiségű adat mozog. Az EtherChannel lehetővé teszi, hogy több portot egy virtuális portba vonja össze őket. Egyszerre nyolc portot tudunk összevonni a jelenlegi szabványokkal. Mi is használtunk EtherChannelt, hogy zavarmentesen lehessen nagy mennyiségű adatot átvinni a hálózaton. Ennek megvalósítását LACP-vel oldottuk meg, hogy acitve-ba raktuk a porokat, ezért folyamatosan üzemel az EtherChannel. Két csoportot használtunk, mivel két külön helyen van szükség a hálózatban nagyobb mennyiségű adat átvitelére. Az egyik csatorna az SW1 és VTP\_SZERVER Switchek között található az 1-es csoportban. A másik csatorna az SW2 és a VTP\_SZERVER között található a 2-es csoportban. Nem építettünk ki mindenhol EtherChannelt, mivel nagyobb az erősforrás igénye is és nemcakartuk A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírásA képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírásfölöslegesen terhelni a hálózatot, viszont a két EtherChannelre szükség volt a redundancia miatt.

OSPF Hitelesítés

Az OSPF(Open Shortest Path First) hitelesítésének az a lényege, hogy az OSPF üzeneteket csak azok az eszközök fogadják el, amelyek rendelkeznek az engedélyezett hitelesítési kulcsokkal. Ez megakadályozza a hamis OSPF üzenetek befogadását vagy a hálózatba történő illetéktelen beavatkozást. Természetesen mi is használtunk ilyes fajta titkosítást, hálózatunk biztonsága érdekében. Mi az MD5(Message Digest Method 5) titkosítását használtuk mivel az MD5 kódolás bármilyen adatból méretétől vagy típusától függetlenül egy 16 bájt hosszú bináris hasht eredményez. A kódolás egyirányú, így nem lehet visszafejteni. Éppen emiatt alkalmas az eredetiség ellenőrzésére. Ez a módszer sokkal biztonságosabb mint a Plain Text titkosítás.

Soros kapcsolat védelme

Ahhoz hogy az adat biztonságban eljusson a másik félhez megfelelő módszerekkel kell megvédeni. Egy WAN kapcsolatnál ez kiemelten fontos, hiszen olyan információk haladnak át általában egy WAN kapcsolaton, amik kifejezetten privát információt tartalmaznak. A PPP(Point-to-Point) alapú hálózatoknál, csakmint egy WAN kapcsolat esetében lehetőségünk van kihasználni a külön erre a célra kifejlesztett CHAP(Challange-Handske Autchentication Protocol)-t. A CHAP működése a következő: A hitelesítő küld egy kihívást, ami tartalmazza a viszony azonosítóját, valamint egy tetszőleges értéket. A felhasználó válaszában elküldi a felhasználó nevét és egy egyirányú hash algoritmussal (pl. MD5) a szervertől kapott kihívást, a viszony azonosítóját és a jelszavát.

Forgalom Irányítás

A forgalom irányítás azaz IP Routing lehetővé teszi, hogy csomagokat küldjünk másik hálózatokba. Két fajta forgalom irányítást különböztetünk meg: Statikus és Dinamikus forgalom irányítás.

A statikus forgalom irányítás típúsai:

* hagyományos
* alapértelmezett
* lebegő
* összevont

Előnyei:

* router nem hirdeti a hálózaton
* kevesebb sávszélességet foglalnak
* továbbítási útvonal előre ismert

Hátrányok:

* időigényes a rendszergazda számára
* hibaérzékeny (nagy hálózaton különösen)
* nagy hálózat esetén nem egyszerű a karbantartás

Hol használjuk

* kisméretű hálózatok
* véghálózat beállítása
* alapértelmezett útvonal beállítása

Dinamikus forgalom irányítási protokollok:

* RIP
* OSPF
* IS-IS
* IGRP
* EIGRP
* BGP

Dinamikus protokollok előnyei:

* automatikus topológia felderítés és frissítés
* a hálózat méretétől kevésbé függ

Dinamikus protokollok hátrányai:

* több erőforrást igényel
* támadási felület az automatizmus
* összetettebb megvalósítás

Dinamikus protokollok működése:

* ha a szomszéd ugyanazt a protokollt használja, akkor információt cserélek vele
* rögtön frissíti a topológiát, ha változik

Vannak osztály alapú és osztály nélüli irányító protokollok.

Osztály alapú

* nem küld maszkot
* a hálózat címe meghatározható a címből
* VLSM és CIDR kizárva (változó hosszúságú maszk; körzetek közötti forgalomi.)

Osztály nélküli

* küld maszkot is

Az IPv6-os irányító protokollok mind osztály nélküli (classless) protokoll.

A hálózatunkban használtunk egyaránt dinamikus, illetve statikus forgalom irányítást is. Használtunk EIGRP-t, illetve OSPF protokollt MD5 és CHAP hitelesítésekkel.

OSPF

Az OSPF az Open Shortest Path First rövidítése, amelyet általában belső hálózati útválasztásban használnak. Az OSPF egy kapcsolatállapot alapú forgalomirányító protokoll, amelyet az Internet Engineering Task Force (IETF) által szabványosított. A távolságalapú RIP leváltására alkották meg. A RIP kis ugrásszám korlátja, és az útvonalak különböző sebessége nem teszi ideális útválasztó protokollá. A RIP-el szemben a OSPF gyorsabb konvergenciát is lehetővé tesz.

Jellemzők:

* gyors konvergencia
* osztály nélküli
* skálázható
* terület alapú
* SPF(Shortest Path First) algoritmust használ
* támogatja a VLSM-et és a CIDR-et
* frissítés csak változáskor
* nincs periodikus frissítés
* hitelesítés
* Link State Routing Protocol-t használ
* költséget számít
* Hierarchikus struktúrát használ
* Hello üzeneteket és kapcsolat-állapot alapú hirdetéseket küld
* Az OSPf körkeresési mechanizmusokat alkalmaz a hurkok elkerülése érdekében

SPF algoritmus

* Edsger Wybe Dijkstra
  + holland matematikus, programozó és elméleti fizikus
  + munkáit számos nyelven használják
* az algoritmus:
  + célok elérésének teljes költségét számolja
  + SPF fát épít