3. YAPILAN VEYA YAPILACAK OLAN İŞ

Bu proje, bir şirketin ofis ağlarının kurulmasını, farklı şehirlerdeki ofislerin ağ tünelleri aracılığıyla birbirleriyle iletişimini ve ağ cihazlarındaki basit güvenlik önlemlerini kapsamaktadır.

3.1. Amaç

Bulunduğum ekip, çalışmalarını Cisco Packet Tracer üzerinden gerçekleştirdiği için öncelikli amacım Cisco Packet Tracer uygulamasını öğrenmek oldu. Diğer bir amacım ise bu uygulamayı öğrendikten sonra gerekli uygulamaları ve bilgileri öğrenip test ederek bir Bilgisayar Ağları projesi geliştirmekti.

3.2. Tanım

Stajımın başlangıcında Cisco Packet Tracer uygulamasını iyice araştırıp öğrenmek için çaba sarfettim. Bu sayede Cisco Packet Tracer uygulamasının bu projede ne kadar önemli olduğunu anlama ve kavrama zamanım oldu. Şirketimin sağladığı dokümanlar sayesinde Cisco Packet Tracer uygulamasını aktif bir şekilde kullandım.

3.3. Süreç ve İşleyiş

Üçüncü sınıfta aldığım Bilgisayar Ağları I ve Bilgisayar Ağları II dersleri sayesinde önceden altyapım zaten vardı. Bunlara ek olarak staj yaptığım şirketimin bana sağladığı dokümanlar ve gerekli lab uygulamaları sayesinde Bilgisayar Ağları I ve Bilgisayar Ağları II dersinde gördüğümüz CCNA konularını hem pekiştirmiş hem de birkaç seviye ileriye götürmüş oldum.

Cisco Packet Tracer uygulumasını öğrenmek için gerekli araştırmaları yapmaya başladım. Bir bilgi çöplüğü olarak gördüğüm internet sitesini en verimli şekilde kullanmaya çalışarak Cisco Packet Tracer uygulamasını kullanmayı ve bunu en verimli hale nasıl getireceğimi öğrendim.

Switch Konfigürasyonu, Router Konfigürasyonu, MLS Konfigürasyonu, Yönlendirme Protokolleri, Ağ, Kapsülleme ve Ağ Yönetimi gibi birçok terimi öğrenip bunları etkin bir biçimde kullanmayı öğrendim. Bunları yaparken konuları olabildiğince kod yazarak yaptım ve özümü kaybetmemeye çalıştım. Bunlara ek olarak sadece yukarıda yazdığım özellikleri öğrenmeyle kalmayarak projede kullanmayacak olsam bile Ağ ve Ağ Güvenliği ile ilgili önemli veya önemsiz farketmeksizin daha birçok başka konuyu öğrenmeye özen göstererek bu alanlarla ilgili teorik ve pratik olmak üzere mesleki ve genel kültür bilgimi üst seviyelere çıkarmaya özen gösterdim.

4. PROJE

Bu proje, yukarıda da belirtildiği gibi iki farklı şehirdeki iki farklı ofisin ağ tünelleri aracılığıyla birbiri ile haberleşmesini ve bu ortamdaki cihazların güvenliğini kapsar. Proje Cisco Packet Tracer üzerinden gerçekleştirilmiş olup çoğu kısmında kodlama tekniği kullanılmıştır.

Projenin temelinde daha sonradan "part" olarak adlandıracağım 8 adet konfigürasyon işlemi vardır. Bunlar:

Part 1: Switch Konfigürasyonu

Part 2: 1. Ofis (Ankara) Router Konfigürasyonu

Part 3: 3560-24PS MLS Konfigürasyonu

Part 4: 2. Ofis (Düzce) Router Konfigürasyonu

Part 5: EIGRP Yönlendirme Protokolü

Part 6: ACL Ağı

Part 7: Jenerik Yönlendirici Kapsülleme - GRE

Part 8: Ağ Yönetimi

4.1. Amaç

Geliştirdiğim projedeki amaç; iki ofisin, şirketin veya iki ağ ortamının birbiri arasında kolayca iletişimini ve siber dünyadaki en önemli durumlardan birisi olan güvenliği sağlamaktır. Bu ortamdaki kişiler istediği çoğu veriyi birbirleri arasında olabilecek en hızlı, en kolay ve en güvenli şekilde birbirlerine gönderip alabilirler ve iletişime geçebilirler.

4.2. Tanım

Bir kullancı diğer kullanıcıya veri gönderdiği zaman ya da iletişime geçtiği zaman veri, sırasıyla;

- Bilgisayar
- Switch
- MLS

gibi birkaç yoldan geçtikten sonra (bunları aşağılarda açıklayacağım için detay verip bu kısmı boğmak istemiyorum.) hızlı, kayıpsız ve güvenli bir şekilde karşı tarafa ulaşır.

4.3. Gereksinimler ve İhtiyaçlar

Bu projeyi sanal ortamda geliştirdiğim için en önemli ihtiyaç Cisco Packet Tracer oldu. Buna ek olarak projeyi yapmak için gerekli bilgileri içeren bir doküman olması da diğer önemli bir ihtiyaçtır.

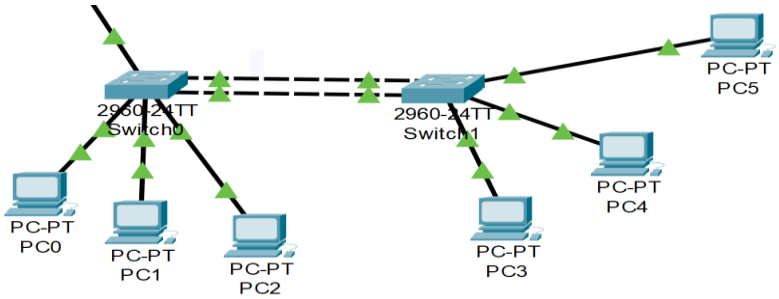
4.4. Analiz

Projeye başlangıç almadan önce proje için gerekli analizler yerine getirildi. Veri iletişim hızının nasıl gerçekleşeceği bunun için hangi protokolün uygun olacağı, nasıl daha hızlı hale getirilebileceği ve veri iletişim güvenliği için nasıl bir yol izleneceği ve hangi yolun daha uygun olduğu ve bunlara ek olarak da veri kaybının nasıl önleneceği veya veri kaybının nasıl en az hale getirileceğinin analizi yapıldı.

4.5. Gelişim Süreci

Switch Konfigürasyonu:

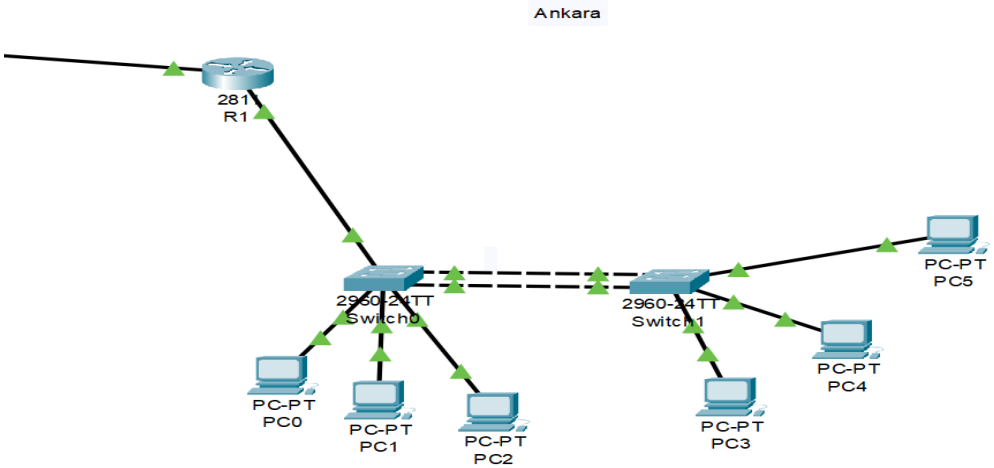
- 4 adet VLAN atama işlemleri yapılır.
- Her bir FastEthernet her bir VLAN'a atanır.
- GigabitEthernet arayüzleri arasında bağlantı oluşturulur.
- Yönetim Arayüzü oluşturulur.
- Switch için kullanıcı adı ve şifre oluşturulur.



Şekil 4.1: Switch ve Bilgisayar Bağlantıları

1. Ofis (Ankara) Router Konfigürasyonu:

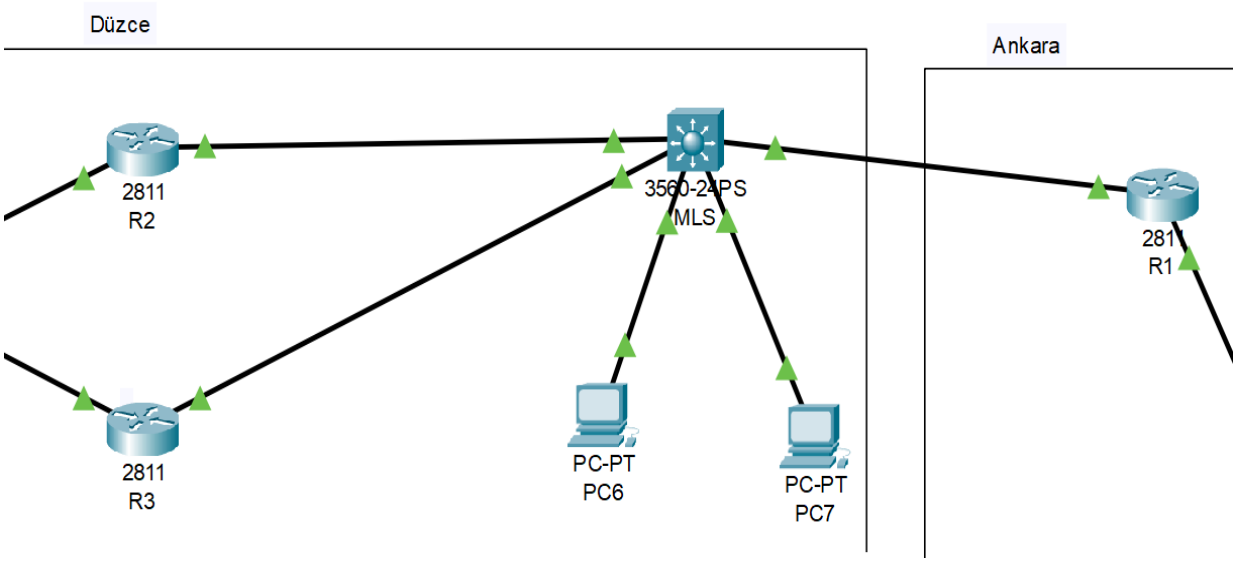
- FastEthernet0/1, 40.40.40/24 IP adresine atanır.
- Swtich0 ve Switch1 için 4 adet VLAN arasında yönlendirme yapılır. Bu yönlendirme için Router yapılandırılır.
- 4 adet VLAN'a bağlı herhangi bir makine için Router DHCP sunucusu olarak yapılandırılır.



Şekil 4.2: Ankara Ofisi Cihaz Bağlantıları

3560-24PS MLS Konfigürasyonu:

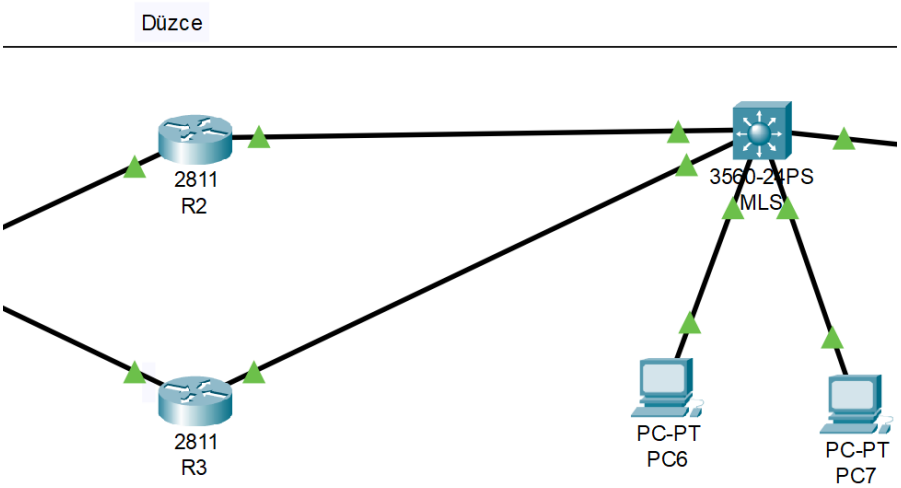
- Yönlendirme özellikleri etkinleştirilir.
- VLAN 100 ve VLAN 200 adıyla 2 adet VLAN oluşturulur.
- FastEthernet0/4 VLAN 100'e ve FastEthernet0/5 VLAN 200'e atanır.
- Switch Virtual Interface kullanılarak VLAN 100 ve VLAN 200 arası yönlendirme etkinleştirilir.



Şekil 4.3: MLS ve Bağlantı Cihazları

2. Ofis (Düzce) Router Konfigürasyonu:

- Router2 FastEthernet0/0 ve FastEthernet0/1 IP adresleri yapılandırılır.
- Router3 FastEthernet0/0 ve FastEthernet0/1 IP adresleri yapılandırılır.
- Cisco Yüksek Kullanılabilirlik Protokolü yapılandırılır.



Şekil 4.4: Router ve Bağlantı Cihazları

EIGRP Yönlendirme Protokolü:

- EIGRP; R1, R2, R3 ve MLS'de 100 numara olarak yapılandırılır.

ACL Ağı:

- Switch 2 sadece Server 10.0.0.100 ve PC 2.0.0.100'den gelecek SSH bağlantılarını kabul edecek şekilde yapılandırılır.
- PC 2.0.0.100'ü VLAN 2'de Web Sunucusuna erişmesine izin verilen tek makine olacak şekilde yapılandırılır.
- Router 2 ve Router 3, herhangi bir makineye ping atabilecek ancak herhangi bir makineden gelen ping isteklerine cevap veremeyecek şekilde yapılandırılır.

Jenerik Yönlendirici Kapsülleme – GRE:

- Router 1'de 192.168.101.1/24 IP adresi ile loopback interface oluşturulur.
- Router 3'de 192.168.101.1/24 IP adresi ile loopback interface oluşturulur.
- Router 1 ve Router 3 arasında bu loopback'leri RIPv2 kullanarak birbirlerine tanıtmasını sağlayın.

- RIPv2 **sadece** Router 1 ve Router 3'de çalışıyor olmalıdır.

- IP adresi, tünel kullanılıyor ise 200.200.200.#/24 olmalıdır. (# yönlendirici kimliği demektir.)

- Router 1 loopback'inin Router 2 loopback'ine ping atabildiğinden emin olmak için extended (genişletilmiş) ping kullandım.

Ağ Yönetimi:

- Router 1, Router 2, Router 3 ve MLS'de 10.0.0.100 numaralı sunucuyu güvenli NTP sunucusu olarak kullanmak için yapılandırın.
- Set ve mesaj almak için "cisco" şifresi ile Router 2 ve Router 3'te SNMP etkinleştirilir.
- İlk kimlik doğrulama yöntemi olarak AAA sunucusunda 10.0.0.100 sunucusunu kullanarak Router 3'te Telnet etkinleştirilir.
- Router 2, 10.0.0.100 sunucusunu kullanıcı adı ve şifre "cisco" olarak kullanarak FTP sunucusu olacak şekilde yapılandırılır.

- FTP Protokolü kullanılarak Router 2'nin çalışan konfigürasyonunun kopyası 10.0.0.100 sunucusuna gönderilir.
- TFTP Protokolü kullanılarak Router 3'ün çalışan konfigürasyonunun kopyası 10.0.0.100 sunucusuna gönderilir.
- Router 3'de herhangi bir sistem önyükleme komutu kullanılmaz.
- Router 2'nin "standby" kullanarak Router 3'e ping veya telnet yapabilmesi sağlanır.

4.7. Proje Sonucu

Projemi geliştirirken okulda gördüğüm Bilgisayar Ağları I ve Bilgisayar Ağları II dersinde gördüğümüz konuları tekrar edip pekiştirme şansım oldu. Cisco Packet Tracer uygulamasını öğrendim ve olabilecek en aktif bir biçimde kullandım. Bunlara ek olarak da CCNA eğitimlerini tamamlayarak Router, Switch kullanım mantığını ve bunların ne işe yaradığını öğrenme fırsatı yakaladım. Server, Ağ Yönetimi, İnternet Protokolleri ve Güvenliği gibi daha birçok konuyu öğrenip bu konular hakkında bilgi sahibi olma şansı yakaladım.

6.EKLER

Aşağıda yer alan komutlar proje üzerinde gerçekleştirilen işlemleri ifade etmektedir. Anlamları daha önceden belirtilen komutlar alt satırlarda anlamları tekrarlanmamıştır.

6.1. Part I – Switch Konfigürasyonu

6.1.1. Switch 1

ena **/*** Asıl adı "enable" komutudur. "priviledge exec" moduna geçilir. Burada temel konfigürasyonlar baz alınarak ayarlar yapılır. */

config t **/*** Asıl adı "configure terminal" komutudur. Bu modda temel ayarlar, arayüz ayarları, şifre ve güvenlik ayarları gibi birçok network ayarı yapılır. */

hostname sw1 **/*** "hostname" komutu ile switch'e isim verilir. Burada Switch 1'in adı sw1 olarak belirlenmiştir. */

ip domain-name ank **/*** Ankara ofisinin **domain name**'ini tanımlıyoruz. Bunu tanımlamazsak **ssh** veya **key** gerektiren uygulamaları yapamayız. */

vlan 2 // vlan ID atama komutu

vlan 3 // vlan ID atama komutu

vlan 4 // vlan ID atama komutu

int range g0/1 – 2 **/*** Asıl adı "interface range" komutudır. Bu komut ile belirtilen port aralığı seçilir. ***/**

channel-group 1 mode active **/*** Bu komut sayesinde herhangi bir protokol kullanmadan statik bir şekilde portları kümelere ayırabiliriz. ***/**

int port-channel 1

sw mo tr

int vlan 1 // VLAN'a ait sanal interface devreye alınır.

ip add 1.0.0.50 255.0.0.0 // Interface için IP adresi ve SubnetMask tanımlanır.

no sh // "no shutdown" anlamına gelir. Sistemi açık tutar.

exit

ip default-gateway 1.0.0.1 // Switchin uzaktan yönetilebilmesini sağlar.

username ank sec cisco

ena cisco

crypto key generate rsa // Bu komut SSH erişimi için kullanılır.

1024 // Modüldeki bit sayısını ifade eder. (Defaul değer 512, en fazla 2048 olur.)

line vty 0 4 // Telnet ile bağlanacak kişi sayısını belirtir.

login local **/*** Bu ve altındaki komutların anlamı sanal terminal için SSH transport desteğini etkinleştirmektir. */

trans input ssh

exit

ip ssh version 2 **/*** Bu komut SSH versiyon 2 yi etkinleştirmeyi sağlar ancak versiyon 1 devre dışı kalır. ***/**

int f0/24 // "Interface" seçmemizi sağlayan komut

sw mo tr

int f0/2

sw acc vlan 2 // Seçilen portun hangi VLAN'da hizmet vereceği belirlenir.

int f0/3

sw acc vlan 3

int f0/4

sw acc vlan 4

6.1.2. Switch 2

ena

config t

hostname sw2

ip domain-name ank

vlan 2

vlan 3

vlan 4

int range g0/1 - 2

channel-group 1 mode passive

int port-channel 1

sw mo tr

int vlan 2

ip add 2.0.0.50 255.0.0.0

no sh

exit

ip default-gateway 2.0.0.1

username ank sec cisco

ena cisco

crypto key generate rsa

1024

line vty 0 4

login local

trans input ssh

exit

ip ssh version 2

int f0/2

sw acc vlan 2

int f0/3

sw acc vlan 3

int f0/4

sw acc vlan 4

6.1.3. Switch 1

ena

config t

banner motd # This is SW1 # **/*** Bu komut, cihaz açılırken açıklama amaçlı mesaj belirtilmesi için kullanılır. */

6.1.4. Switch 2

ena

config t

banner motd # This is SW2 #

6.1.5. Switch 1 ve Switch 2

int range f0/2 - 4

span portfast **/*** Bu komut, switch ilk açıldığında loop oluşmaması için oluşan 30 saniyelik zaman kaybını ortadan kaldırır. */

span bpduguard enable // Bu komut, BPDU Guard koruma modunu aktifleştirir.

no cdp enable // CDP protokolünü kapatır.

sw mo acc // Arayüz, access moduna ayarlandı.

sw po

sw po max 1 // Hafızada en az 1 adet MAC Adresi tutulur.

sw po mac-address sticky **/*** Bu komut, ilgili porta bağlanan MAC Adresler'inin direkt hafızaya kaydedilmesini sağlar. */

sw po vio sh **/*** Bu komut, hafızaya alınan MAC Adres sayısı aşıldığı anda sistemi kapatır. ***/**

exit

line con 0 // Konsolun 0. Portunu seçer.

motd-banner

login local

exec-timeout 0 // Bu komut, hareket zamanlayıcısını belirtir.

logging synchronous // Eş zamanlı log tutmamızı sağlayan komut.

history size 256 // Bu komut, geçmişte saklanan komutların sayısını ayarlar.

line vty 0 4

motd-banner

exec-timeout 0

logging synchronous

history size 256

6.2. Part II – Ankara Ofisi Router Konfigürasyonu

6.2.1. Router 1

ena

config t

ip dhcp excluded-address 1.0.0.1 1.0.0.99 // Dağıtılmayacak olan adres aralığı

ip dhcp excluded-address 1.0.0.201 1.255.255.255

ip dhcp excluded-address 2.0.0.1 2.0.0.99

ip dhcp excluded-address 2.0.0.201 2.255.255.255

ip dhcp excluded-address 3.0.0.1 3.0.0.99

ip dhcp excluded-address 3.0.0.201 3.255.255.255

ip dhcp excluded-address 4.0.0.1 4.0.0.99

ip dhcp excluded-address 4.0.0.201 4.255.255.255

ip dhcp pool vlan1 // Verilen isim ile DHCP Pool oluşturulur.

network 1.0.0.0 255.0.0.0 // Ağ adresi tanımlama

default-router 1.0.0.1 // Varsayılan Ağ Geçidi tanımlaması (Defaul Gateway)

ip dhcp pool vlan2

network 2.0.0.0 255.0.0.0

default-router 2.0.0.1

ip dhcp pool vlan3

network 3.0.0.0 255.0.0.0

default-router 3.0.0.1

ip dhcp pool vlan4

network 4.0.0.0 255.0.0.0

default-router 4.0.0.1

int f0/0

no ip add

no sh

int f0/0.1

encap dot 1 **/*** Bu komut, bir switche giden bir ana bağlantı noktası olarak bir router interfacesi kullanılmasına izin verir. ***/**

ip add 1.0.0.1 255.0.0.0

int f0/0.2

encap dot 2

ip add 2.0.0.1 255.0.0.0

int f0/0.3

encap dot 3

ip add 3.0.0.1 255.0.0.0

int f0/1

ip add 40.40.40.1 255.255.255.0

no sh

6.3. Part III - 3560-24PS MLS Konfigürasyonu

```
ena
config t
vlan 100
name Satis_dep  // VLAN için isim atama komutu
vlan 200
name BT_dep
ip routing
hostname MLS  // MLS'e isim verilir.
```

```
int f0/1
no sw
ip add 11.0.0.50 255.0.0.0
no sh
int f0/2
no sw
ip add 12.0.0.50 255.0.0.0
no sh
int f0/3
no sw
ip add 40.40.40.50 255.255.255.0
no sh
int vlan 100
ip add 100.0.0.50 255.0.0.0
no sh
int vlan 200
ip add 200.0.0.50 255.255.255.0
```

no sh

int f0/4

sw acc vlan 100

int f0/5

sw acc vlan 200

6.4. Part IV – Düzce Ofisi Router Konfigürasyonu

6.4.1. Router 2

ena

config t

int f0/1

ip add 11.0.0.2 255.0.0.0

no sh

// HSRP Yapılandırması

int f0/0

ip add 10.0.0.2 255.0.0.0

no sh

standby 1 ip 10.0.0.1 **/*** Bekleme grubu ve bekleme IP adresi atar.

standby 1 priority 120 **/*** Belirli bir grup numarası (1) için yönlendirici arayüzüne (f0/0) bir öncelik (120) atanır**. */**

standby 1 preempt **/*** Öncelik, etkin bekleme grubundaki diğer tüm HSRP ile yapılandırılmış yönlendiricilerden daha yüksek olduğunda yönlendiricinin etkin yönlendirici olmasına izin verir. **/**

standby 1 track fastEthernet 0/1 **//** HSRP'nin fastEthernet0/1 arabirimini izlediğini gösterir. **/**

6.4.2. Router 3

ena

config t

int f0/1

ip add 12.0.0.3 255.0.0.0

no sh

int f0/0

ip add 10.0.0.3 255.0.0.0

no sh

standby 1 ip 10.0.0.1

6.5. Part V – EIGRP Yönlendirme Protokolü

6.5.1. Router 1

// EIGRP Konigürasyonu

ena

config t

router eigrp 100

no auto

network 1.0.0.0 0.255.255.255

network 2.0.0.0 0.255.255.255

network 3.0.0.0 0.255.255.255

network 4.0.0.0 0.255.255.255

network 40.40.40.0 0.0.0.255

6.5.2. MLS

// EIGRP Konfigürasyonu

ena

config t

router eigrp 100

no auto

network 11.0.0.0 0.255.255.255

network 12.0.0.0 0.255.255.255

network 100.0.0.0 0.255.255.255

network 40.40.40.0 0.0.0.255

network 200.0.0.0 0.0.0.255

6.5.3. Router 2

// **EIGRP Konfigürasyonu**

ena

config t

router eigrp 100

no auto

network 11.0.0.0 0.255.255.255

network 10.0.0.0 0.255.255.255

6.5.4. Router 3

// **EIGRP Konfigürasyonu**

ena

config t

router eigrp 100

no auto

network 12.0.0.0 0.255.255.255

network 10.0.0.0 0.255.255.255

6.6. Part VI - ACL Ağı

6.6.1. Switch 2

ena

config t

access-list 1 permit host 10.0.0.100 **/*** Bu komut, oluşturulacak listenin numarasını ve o listede izinli olan IP adresini belirler. ***/**

access-list 1 permit host 2.0.0.100

line vty 0 4

access-class 1 in

6.6.2. Router 1

ena

config t

access-list 100 permit tcp host 2.0.0.100 host 10.0.0.100 eq 80 **/*** 100 numara verilir, TCP Protokolü seçilir, kaynak ve hedef Ipler belirtilir ve kullanılmak istenilen servisin port numarası belirtilir. ***/**

access-list 100 deny tcp 2.0.0.0 0.255.255.255 host 10.0.0.100 eq 80 **/*** Bu yapılandırma ile 2.0.0.0 ağından hiçbir hostun 10.0.0.100 adresindeki 80 port numaralı servise (HTTP) bağlanmamasını sağlamış olduk. ***/**

access-list 100 permit ip any any **/*** Bu komut ile ICMP(Internet Control Message Protocol)'ye tüm kaynaklar ve hedefler için izin veririz. ***/**

interface FastEthernet0/0.2

ip access-group 100 in **/*** ACL 100'ün giriş yönünde uygulanmasını seçtik. Eğer böyle yapmamış olsaydık hostlardan gelen paketler routerda işlenecekti ve sonra erişim/engelleme yapılacaktı. ***/**

6.6.3. Router 2 ve Router 3

ena

config t

access-list 100 permit icmp host 10.0.0.100 any echo

access-list 100 deny icmp host 10.0.0.100 any echo-reply

access-list 100 permit ip any any

int f0/0

ip access-group 100 in

6.7. Part VII – GRE

6.7.1. Router 1

ena

config t

int loop 1

ip add 192.168.101.1 255.255.255.0

int tunnel 1

ip add 200.200.200.1 255.255.255.0

network

tunnel destination 12.0.0.3 // Tünel arayüzünün hedef adresi belirtilir.

// **Router Rip Konfigürasyonu**

router rip

ver 2

no auto

network 192.168.101.0

network 200.200.200.0

6.7.2. Router 3

ena

config t

int loop 3

ip add 192.168.103.3 255.255.255.0

int tunnel 1

ip add 200.200.200.3 255.255.255.0

tunnel source f0/1 //

tunnel destination 40.40.40.1

// **Router Rip Konfigürasyonu**

router rip

ver 2

no auto

network 192.168.103.0

network 200.200.200.0

6.7.3. Extended Ping

Protocol [ip]:

Target IP address: 192.168.103.3 // Ping atmayı planladığımız IP adresini gireriz.

Extended commands [n]: y // Bir dizi ek komutun görünüp görünmeyeceği bilgisi

Source address or interface: 192.168.101.1 /* Problar için kaynak adresi olarak kullanılacak routerın arabirimi veya IP adresinin belirlenir. */

6.8. Part VIII – Ağ Yönetimi

6.8.1. Router 1, Router 2, Router3 ve MLS

// **NTP Server'ı Router'a Tanımlama**

ena

config t

ntp authentication-key 1 md5 cisco **/*** Bu komut, kaç anahtarlı kimlik doğrulama olduğunu gösterir. ***/**

ntp authenticate **//** NTP kimlik doğrulamasını kullanmamızı sağlar.

ntp trusted-key 1 **//** Güvenilir zaman kaynakları için anahtar

ntp server 10.0.0.100 key 1 **//** NTP server konfigürasyonu

// LOGGİNG

logging on

logging host 10.0.0.100 **//** Log kayıtlarının gönderileceği sunucu belirlenir.

service timestamps log datetime msec **/*** Milisaniyeli bir şekilde tarih ve saat ile zaman damgası ***/**

service timestamps debug datetime msec **/*** Hata ayıklama iletilerine milisaniyeli bir şekilde tarih ve saat ile zaman damgası ***/**

6.8.2. Router 2 ve Router 3

ena

config t

snmp-server community cisco rw **//** Yöneticinin read-write özelliklerini belirtir.

6.8.3. Router 3

ena

config t

username ank sec cisco

ena cisco

line vty 0 4

login authentication default

exit

aaa new-model

aaa authentication log default group radius local **/*** Radius ve local ile bağlantıya izin verilir. ***/**

radius-server host 10.0.0.100 // Radius serve IP adresi

6.8.4. Router 2

ip ftp username cisco

ip ftp password cisco

ip host standby 10.0.0.3

7. KAYNAKÇA

[1] https://www.mainty.com.tr/kurumsal/

Şirketin Sağlamış Olduğu CCNA Dokümanları