

DONANIM STAJ RAPORU

○ CISCO CNNA EĞİTİMİ

OSI referans modeli

Physical (Fiziksel Katman)
Data Link (Veri Bağlantı Katmanı)
Network (Ağ Katmanı)
Transport (Taşıma Katmanı)
Session (Oturum Katmanı)
Presentation (Sunu Katmanı)
Application (Uygulama Katmanı)

Cihazlar:

Switch

- **İşlevi:** Ağ içindeki cihazların birbirleriyle iletişim kurmasını sağlar, veri paketlerini hedef MAC adresine göre iletir.
- **Çalıştığı Katman:** OSI modelinin 2. katmanı (Veri Bağlantı Katmanı).
- **Portları:** Ethernet portları (RJ-45), konsol portu.
- **Bağlantı Kabloları:** Cat5, Cat5e, Cat6 kabloları.

Router

- **İşlevi:** Farklı ağlar arasındaki veri paketlerini yönlendirir, ağlar arası trafik yönetimini sağlar.
- **Çalıştığı Katman:** OSI modelinin 3. katmanı (Ağ Katmanı).
- **Portları:** LAN portları, WAN portu, konsol portu.
- **Bağlantı Kabloları:** Cat5, Cat5e, Cat6 kabloları, fiber optik kablolar.

- **Düz Kablo (Straight-Through Cable),** Farklı türdeki cihazları bağlamak için kullanılır.

- **Bağladığı Cihazlar:**

- Bilgisayar ↔ Switch
- Bilgisayar ↔ Hub
- Switch ↔ Router
- Hub ↔ Router

- **Çapraz kablo (crossover cable),** : Aynı türdeki cihazları doğrudan bağlamak için kullanılır.

- **Bağladığı Cihazlar:**

- Bilgisayar ↔ Bilgisayar
- Switch ↔ Switch
- Hub ↔ Hub
- Router ↔ Router

serial DCE-DTE kabloları: İki router'ı seri portları üzerinden bağlamak için kullanılır.



Düz kablo



Çapraz kablo



CDE-DTE kablo

Router Portları

FastEthernet Portları

- Amaç: Farklı ağlara bağlanmak.
- Örnekler: FastEthernet0/0, FastEthernet0/1.
- Kullanım: Ağları birbirinden ayırarak yönlendirme yapar.

Console Portu

- Amaç: Cihaza doğrudan bağlantı yapmak.
- Kullanım: Router'ın yapılandırılması ve yönetimi için kullanılır.

AUX Portu

- Amaç: Uzaktan yönetim ve yedek erişim.
- Kullanım: Genellikle bir modem aracılığıyla uzaktan erişim sağlamak için kullanılır.
- **Seri Interface portları**
- Amaç: WAN (Geniş Alan Ağı) bağlantısı.
- Kullanım: Uzun mesafe bağlantılar için seri iletişim sağlar.

Switch Portları

Ethernet Portları (RJ-45)

- **Amaç:** Ağ cihazlarını bağlar.
- **Bağlantı:** Ethernet kabloları.

Uplink Portları

- **Amaç:** Diğer switch'lere bağlanır.
- **Bağlantı:** RJ-45 veya fiber optik.

Fiber Optik Portları (SFP/SFP+)

- **Amaç:** Yüksek hızlı ve uzun mesafe bağlantılar.
- **Bağlantı:** Fiber optik kablolar.

Management Portu (Konsol Portu)

- **Amaç:** Switch'in yönetimi.
- **Bağlantı:** Seri kablo veya USB.

Router Konfigürasyonu

```
Router> // Başlangıç modunda (setup mode).
Router>enable
Router# // priviledge moduna geçti
Router#configure terminal // Konfigürasyon moduna geçiş.
Router(config-if)# // konfigürasyon moduna geçti
Router(config)#interface fastethernet 0/0 // FastEthernet 0/0 portunu seçme.
Router(config-if)#ip address 192.168.1.1 255.255.255.0 // IP adresi ve subnet maskesi atama
Router(config-if)#no shutdown // Portu etkinleştirme.
```

Consolea bağlanıldığında şifre sorulması

```
Router>enable //user mode
Router#configure terminal
Router(config)#line console 0
Router(config-line)#password 123
Router(config-line)#login
Router(config-line)#exit
```

Enable modundan Priviledge moduna geçişte şifre oluşturma

```
Router(config)#enable password 123
```

Router Konfigürasyon modları

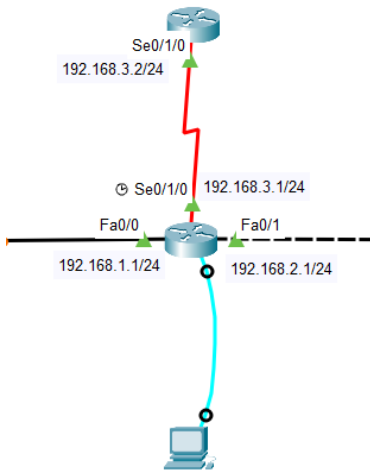
- **User Mode** (Router>)
Temel komutlar, yönetim moduna geçiş için enable komutu.
- **Privileged Mode** (Router#)
Gelişmiş komutlar, konfigürasyon moduna geçiş için configure terminal komutu.
- **Global Configuration Mode** (Router(config)#)
Genel yapılandırma, tüm router ayarları burada yapılır.

Ping, ağ bağlantılarını test etmek ve sorunları gidermek için kullanılan basit bir ağ aracıdır. "Ping" komutu, bir cihazın başka bir cihazla ağ üzerinden iletişim kurup kuramayacağını kontrol eder. ICMP (Internet Control Message Protocol) kullanılarak çalışır.

Telnet: Bir ağ üzerinden uzaktaki bir cihazla iletişim kurmak için kullanılan bir protokoldür.

Örnek telnet bağlantısı uygulaması :

Uygulama amacı: IP adresi olmayan bir pc bulunmakta. PC router1e console portu ile bağlı durumda. PCyi aradaki router1 aracılığıyla telnet bağlantısı ile router2 ye bağlıyoruz. Router2yi PCden konfigüre edebiliyoruz.



PCnin terminalinden router1e bağlanıyoruz.

Daha sonra router1 üzerinden router2nin telnet konfigürasyonunu yapacağız.

Router üzerinden telnet şifresi verilir.

```
Router(config)#  
Router1(config)#line vty 0 15  
Router1(config-line)#password 123  
Router1(config-line)#exit
```

Enable şifresi ayarlanır.

```
Router1(config)#enable secret <sifre>
```

Tekrar PCnin terminalinden aşağıdaki komutlar yazılır.

```
Router1(config)# do 192.168.3.2 // router2nin ip adresi verilir.
```

Istenecek şifreler girildiğinde artık router2yi konfigüre edebilir duruma geliyoruz.

Routerın istediği adrese gitmesi için yapılan konfigürasyon komutları

ip route <kaynak ip adres> <subnet mask> <hedef(komşu) ip adres>

örnek: ip route 192.168.1.0 255.255.255.0 192.168.2.1

default gateway network : Varsayılan rota (default route) tanımlar.

örnek: ip route 0.0.0.0 0.0.0.0 192.168.2.1

traceroute: Ağ üzerinde belirli bir hedefe giden yol üzerindeki yönlendiricileri ve bu yönlendiricilere ulaşma sürelerini belirlemek için kullanılır.

Router# traceroute <hedef_ip_adresi veya hedef_adi>

örnek: Router# traceroute 192.168.2.1

Yapılan konfigürasyonların kaydedilmesi

1.do copy running-config startup-config

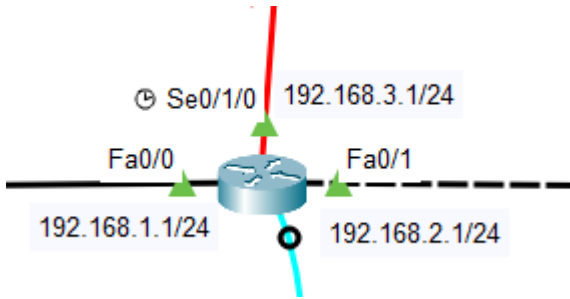
2.do write

startup-config komutu: cihazın yapılandırmasını kalıcı olarak kaydetmek için kullanılır.

running-config komutu : cihazın mevcut yapılandırmasını görüntülemek için kullanılır.

Router# copy running-config startup-config: Bu komut, mevcut çalışan yapılandırmayı (running-config) kalıcı olarak başlangıç yapılandırma dosyasına (startup-config) kopyalar.

Aşağıda bir router için örnek konfigürasyon işlemi bulunmaktadır:



```
Router1(config)#interface fastethernet 0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#interface fastethernet 0/1
Router1(config-if)#ip address 192.168.2.1 255.255.255.0
Router1(config-if)#no shutdown
```

```
Router1(config-if)#interface serial 0/1/0
Router1(config-if)#ip address 192.168.3.1 255.255.255.0
Router1(config-if)#no shutdown
```

Görselde routerın fastethernet 0/0 , fastethernet 0/1 ve serial 0/1/0 portları için ip atama konfigürasyonu yapılmıştır.

Router serial port konfigürasyonu:

```
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
```

Routerla bağlı cihazları gösteren komut: Router(config)#do show users

TCP: güvenilirlik ve hata kontrolü sağlayan, bağlantı tabanlı bir protokoldür. Verilerin doğru sırayla ve eksiksiz olarak iletilmesini sağlar. Kontrol mekanizması vardır. İletilen veri boyutları büyüktür.

UDP: daha hızlı, bağlantısız bir protokoldür ve güvenilirlik sağlamaz.

Verilerin hızlı iletimi gerektiğinde, örneğin canlı video akışı veya online oyunlar için kullanılır. Kontrol mekanizması yoktur. İletilen veri boyutları daha küçüktür.

FTP(File Transfer Protocol):Bir ağ üzerindeki iki bilgisayar arasında dosya transferi yapmak için kullanılan bir protokoldür.

TFTP (Trivial File Transfer Protocol), basit ve hafif bir dosya transfer protokolüdür. TFTP, FTP'nin daha az özellikli ve daha kolay uygulanabilir bir versiyonudur.

Ftp'den daha hızlıdır, daha az güvenlik sağlar.

TFTP ile İşletim sistemi kopyalama konfigürasyonu

Router üzerindeki işletim sistemini servera yedekler.

Router#show flash : işletim sisteminin adını gösterir

Address or name of remote host []? 192.168.1.4 // kopyalamak istediğimiz cihazın ip adresini yazıyoruz.

Router# copy flash tftp : kopyalama işlemi yapar

DNS (Domain Name System): internet üzerindeki cihazların ve hizmetlerin IP adresleriyle ilişkilendirilmesini sağlayan bir sistemdir.

DNS, insanların anlayabileceği alan adlarını (örneğin, www.example.com) internet protokolü (IP) adreslerine dönüştürür (örneğin, 192.0.2.1).

Bu sayede, internet üzerindeki kullanıcılar, web sitelerine, e-posta sunucularına, dosya sunucularına vb. erişmek için alan adlarını kullanabilirler.

Routerdan dns kontrol etme komutu

ip name-server 192.168.1.4

ip domain-name test.com

Cihazın hangi cihazlara komşu olduğunu gösteren komut:

Router#show cdp neighbours

Router# show version : cihazın durumu ve bilgilerini gösterir.

telnet server: Kullanıcıların ağ üzerinden Telnet protokolü aracılığıyla bağlanmasına ve uzaktaki bir bilgisayarda komutlar çalıştırmasına izin veren bir sunucu uygulamasıdır.

NVRAM: enerji kaybında içindeki verileri korur. Bu tür bellek, sistem konfigürasyonları ve önemli verilerin saklanması için kullanılır.

Kullanım Alanları: BIOS veya firmware ayarlarının saklanması, router ve diğer ağ cihazlarında konfigürasyon verilerinin saklanması, kritik sistem bilgileri.

Router, NVRAM'deki (Non-Volatile Random Access Memory) startup-config dosyasını kullanarak önyüklemeye yapar.

0x2102 Değeri: Cisco yönlendiricilerinde varsayılan configuration register değeridir.

0x2142 Değeri: Yönlendiricinin NVRAM'deki startup-config dosyasını atlayarak başlatılmasını sağlar.

Örneğin, 0x2142 olarak ayarlamak için:

```
Router(config)#config-register 0x2142
```

Bir cihaz şifresini resetlemek istediğimizde izlememiz gereken adımlar:

```
Cihaz yeniden başlatılır.  
Açılırken ctrl+break tuşuna basılarak rommon moduna geçilir.  
rommon 1> confreg 0x2142  
rommon 2> reset  
cihaz konfigürasyon olmadan tekrar başlatılır.  
Router> enable  
Router# copy startup-config running-config
```

Console şifresini kaldırma:

```
Router(config)#no enable secret  
Router(config)#line console 0  
Router(config-line)#no password  
Router(config-line)#no login
```

telnet şifresi kaldırma:

```
Router(config-line)#line vty 0 807  
Router(config-line)#no password  
Router(config-line)#no login
```

Yönetici (enable) şifresini değiştirmek için:

```
Router(config)#enable secret yeni_sifre
```

Konfigürasyon register değerini değiştirmek için:

Router(config)#config-register 0x2102
Router(config)#do write // konfigürasyon kaydedilir.

ios silme:

Router# delete flash: ?
Router# dosya_adi yazılır

ios kopyalama:

Router#copy tftp flash
Address or name of remote host []? 10.3.29.240
source filename []? <dosya_adi>
dosyayı açmak için config mooda geçilir.
Router(config)# boot system ?
Router(config)# boot system flash ?
Router(config)# boot system flash <dosya_adi>

IP HESAPLAMA

Unicast: Tek bir gönderici ile tek bir alıcı arasında veri iletişimini ifade eder.
Bu tür yayınlarda, veri paketi bir kaynaktan tek bir hedefe gönderilir.
Örneğin, bir web sitesine bağlanmak için yapılan istek unicast iletişim kullanır.

Broadcast: Tek bir göndericiden tüm ağa veya belirli bir ağ segmentindeki tüm cihazlara veri gönderimini ifade eder.
Bu, tüm ağ düğümlerinin aynı anda veri paketini alması anlamına gelir.
Genellikle yerel ağlar (LAN) içinde kullanılır.

Multicast: Bir göndericiden belirli bir grup alıcıya veri gönderimini ifade eder.
Bu tür yayınlarda, veri paketi yalnızca bu gruba katılan cihazlara iletilir.
Örneğin, bir video konferans veya canlı yayın uygulaması multicast kullanabilir.

Public IP adresleri: Dünya genelindeki internet üzerindeki cihazlar tarafından erişilebilir.

İnternet Servis Sağlayıcıları (ISP) tarafından atanır ve global bir ağa erişim sağlamak için kullanılır. Bu adresler, internet üzerindeki benzersiz kimliklerdir ve herhangi bir çakışma olmadan tüm dünya tarafından tanınır.

örnek:172.217.16.142

Private IP adresleri: Yalnızca yerel ağlar içinde kullanılır ve dış dünya tarafından doğrudan erişilemez.
Bu IP adresleri, ev ağları veya iş yerleri gibi yerel ağlarda cihazlar arasında iletişim sağlamak için kullanılır.

Private IP adres aralıkları (IPv4):

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Subnet mask: IP adresinin ağ kısmını ve host kısmını ayırt etmek için kullanılan bir numaradır.

IP adresine uygulandığında, ağın hangi bölümünün ağ adresi olduğunu ve hangi bölümünün cihazlara (host'lara) ait olduğunu belirler.

Örneğin 192.168.1.10/24 ve 192.168.1.12/24 IP adreslerine sahip iki cihaz var.

İki cihazın da subnet mask kısımları eşleştiği için haberleşebilir

İki cihazın da subnet mask kısımları eşleştiği için haberleşebilir

Örneğin 192.168.1.10/24 ve 192.168.1.12/16 IP adreslerinin subnet mask kısımları eşleşmese de bu cihazlar haberleşebilir.

192.168.1.10/24 ve 192.168.1.12/24 IP adreslerine sahip iki cihaz router ile birbirine bağlanırsa haberleşemez. İki cihaz arasına router koyulursa farklı networklerde olmalıdır.

IP ADRES SINIFLANDIRMASI

Class A

- **Adres Aralığı:** 0.0.0.0 - 127.255.255.255
- **Varsayılan Subnet Maskesi:** 255.0.0.0 (veya /8)
- **Ağ Yapısı:** 8 bit ağ kısmı, 24 bit host kısmı.
- **Örnek IP Adresi:** 10.0.0.1

Class B

- **Adres Aralığı:** 128.0.0.0 - 191.255.255.255
- **Varsayılan Subnet Maskesi:** 255.255.0.0 (veya /16)
- **Ağ Yapısı:** 16 bit ağ kısmı, 16 bit host kısmı.
- **Örnek IP Adresi:** 172.16.0.1

Class C

- **Adres Aralığı:** 192.0.0.0 - 223.255.255.255
- **Varsayılan Subnet Maskesi:** 255.255.255.0 (veya /24)
- **Ağ Yapısı:** 24 bit ağ kısmı, 8 bit host kısmı.
- **Örnek IP Adresi:** 192.168.1.1

IP SUBNETTING

Bir networkte kullanılabilecek max ip sayısı: $2^n - 2$ formülü ile hesaplanır.

örnek: 172.16.0.0 ip adresi için kullanılabilecek max ip sayısı: $2^{16} - 2$

192.168.1.0/24 -> 192.168.1.00000000 : network id numarasıdır.

Br networkteki bilgisayara id olarak verilemez.

192.168.1.1/24 -> 192.168.1.11111111 : broeacast ip : en büyük kombinasyon

Br networkteki bilgisayara id olarak verilemez. Pc broadcast yayın göndrirken bu ip adresini kullanır.

Örnek: 172.176.1.10 ve 172.192.2.20 ip adreslerine sahip iki cihazın subnet maskı kaç olursa haberleşebilirler

172.1/0110000

172.1/1000000 subnet mask 9 olursa haberleşebilirler.

Örnek: 200.1.1.0/30 ip adresi için

kullanılabilir ağ(ip) sayısı: $2^2 - 2 = 2$

subnet mask: 255.255.255.252 -> 255.255.255.11111100

network id: 200.1.1.00000000

broadcast ip: 200.1.1.3

verilebilcek ip adresleri: 200.1.1.00000001 , 200.1.1.00000010

Örnek: birbirine switch cihazı ile bağlı iki tane pc grubu olsun.

1.grup IP adresleri: 200.1.1.2/30 , 200.1.1.1/30

2. grup IP adresleri: 200.1.1.5/30 , 200.1.1.6/30

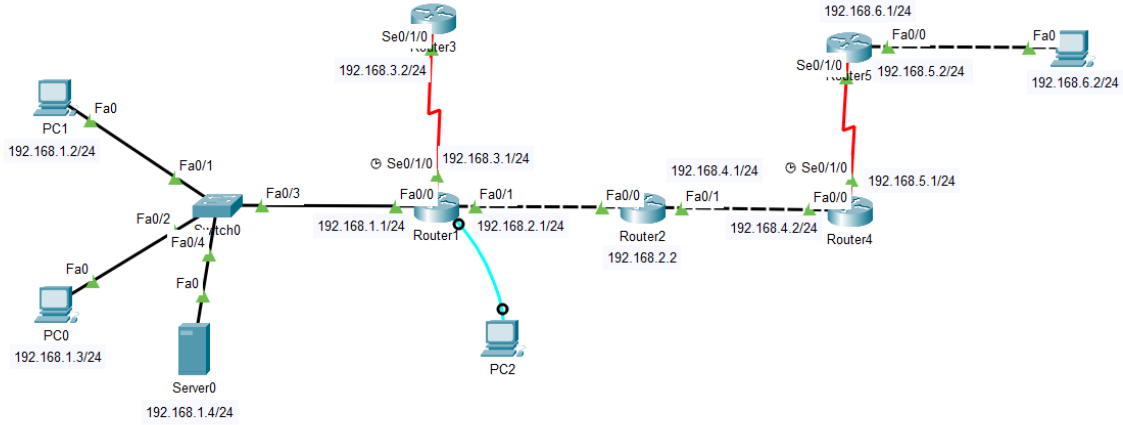
1. grup ve 2. grup, farklı subnetlerde yer alır. 200.1.1.0/30 subneti, 200.1.1.1 ve 200.1.1.2 IP adreslerini kapsar; 200.1.1.4/30 subneti ise 200.1.1.5 ve 200.1.1.6 IP adreslerini kapsar. Dolayısıyla bu iki grup birbirleriyle haberleşemez.

STATIC ROUTING

Static Yönlendirme: Ağdaki veri paketlerinin hedeflerine ulaşmak için izledikleri yolların manuel olarak belirlenmesi ve yönlendiricilere elle yapılandırılmasıdır.

Statik yönlendirme tabloları, yönlendiricilere sabit bir şekilde tanımlanır ve değişiklikler manuel olarak yapılır.

Ip route <hedef_ağ> <subnet_mask> <bir_sonraki_atlama>



Resimdeki topolojiden örnek verecek olursak;

Router4 cihazı 192.168. 6.0 networke ulaşmak istediğinde 192.168.5.2 üzerinden gitmelidir.

Tüm networkü haberleştirmek için bu şekilde tüm routerlara hangi yoldan gitmesi gerektiği belirtilmelidir.

0.0.0.0 0.0.0.0 192.168.4.1: bu komut ile bilmediği bütün networkleri 192.168.4.1 adresine yönlendirmek için kullanılır.

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.6.0 255.255.255.0 192.168.5.2
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.1
Router(config)#
```

Router2 cihazı için bakacak olursak routing komutları şu şekildedir;

```
Router(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.1
Router(config)#ip route 192.168.5.0 255.255.255.0 192.168.4.2
Router(config)#ip route 192.168.6.0 255.255.255.0 192.168.4.2
```

Aşağıdaki görselde ise routing tablosu görüntülenmektedir.

no auto-summary komutu: Otomatik özetlemeyi devre dışı bırakır. Bu komut, özellikle sınıfsız yönlendirme (classless routing) yapmak ve daha doğru ve ayrıntılı yönlendirme bilgileri iletmek için kullanılır.

komut önceliği şu şekilde olmalıdır:

```
router rip
version 2
no auto-summary
network 192.168.1.0
network 192.168.2.0
```

do show ip route komutu mevcut yönlendirme tablosunu görüntülemek için kullanılır. Bu komut, cihazın öğrendiği tüm ağları ve bu ağlara ulaşmak için hangi yolları kullanacağını gösterir.

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 3 subnets
C    10.1.1.0 is directly connected, Serial0/1/0
O    10.1.2.0 [110/130] via 10.1.1.2, 00:11:26, Serial0/1/0
O    10.1.5.0 [110/192] via 10.1.1.2, 00:13:11, Serial0/1/0
172.16.0.0/24 is subnetted, 2 subnets
C    172.16.1.0 is directly connected, FastEthernet0/0
O    172.16.2.0 [110/129] via 10.1.1.2, 00:11:47, Serial0/1/0
O    192.168.1.0/24 [110/2] via 172.16.1.1, 00:25:10, FastEthernet0/0
O    192.168.2.0/24 [110/128] via 10.1.1.2, 00:17:30, Serial0/1/0
C    192.168.10.0/24 is directly connected, Serial0/1/1
```

Administrative Distance (AD): Bir yönlendiricinin birden fazla yönlendirme protokolünden gelen yönlendirme bilgileri arasında en güvenilir olanını seçmesine yardımcı olan bir değerdir.

RIP : AD değeri 120'dir.

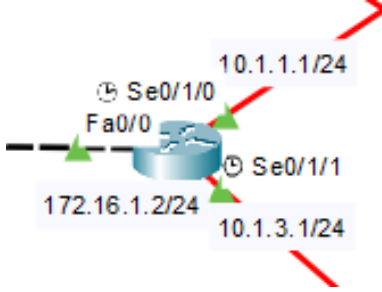
OSPF : AD değeri 110'dur.

Örneğin, bir yönlendirici aynı hedefe hem RIP hem de OSPF tarafından gelen yönlendirme bilgileri alıyorsa, OSPF'in AD değeri daha düşüktür (110), dolayısıyla yönlendirici OSPF tarafından gelen yönlendirme bilgilerini tercih eder.

RIP (Routing Information Protocol): Dinamik yönlendirme protokollerinden biridir. Ağlardaki yönlendirme tablolarını otomatik olarak günceller ve yönlendirme bilgilerini komşu router'lara yayar.

RIP, bağlantı hızını dikkate almaz. Geçiş yolundaki router sayısına bakarak yönlendirme yapar. Maksimum 15 router ile çalışabilir; daha fazlası erişilemez olarak kabul edilir.

RIP KONFIGÜRASYONU



```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#no auto-summary
Router(config-router)#network 172.16.1.0
Router(config-router)#network 10.1.1.0
Router(config-router)#network 10.1.3.0
```

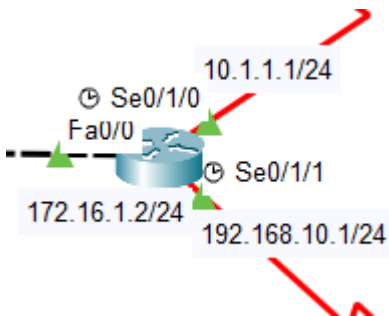
OSPF (Open Shortest Path First) : Geniş çaplı kullanımıyla bilinen, dinamik yönlendirme protokollerinden biridir.

OSPF, karmaşık ve büyük ölçekli ağlarda etkili bir şekilde yönlendirme yapmak için tasarlanmıştır.

Link-State Yönlendirme Protokolü: OSPF, link durumu bilgilerini (link-state information) kullanarak ağ topolojisini belirler ve yönlendirme tablolarını oluşturur.

Bu sayede ağın genel durumu hakkında daha ayrıntılı ve doğru bilgi elde edilir.

OSPF KONFIGÜRASYONU



```
Router(config-if)#
Router(config-if)#router ospf 1
Router(config-router)#network 172.16.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#network 10.1.1.0 0.0.0.255 area 0
Router(config-router)#
```

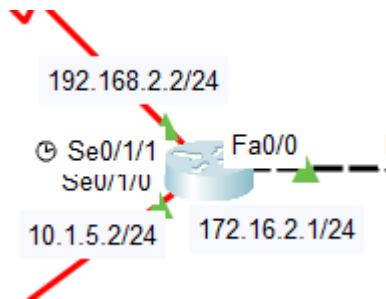
EIGRP (Enhanced Interior Gateway Routing Protocol): Cisco tarafından geliştirilmiş bir yönlendirme protokolüdür. Hybrid protocol olarak bilinir.

AD değeri : 90

Ağın performansını artırmak, hızlı yakınsama sağlamak ve yönetimi kolaylaştırmak için kullanılır.

Summarization açık olarak gelir.

EIGRP KONFIGÜRASYONU



```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 1
Router(config-router)#no auto-summary
Router(config-router)#network 192.168.2.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.2.1 (Serial0/1/1) is up: new adjacency

Router(config-router)#
Router(config-router)#network 172.16.2.0
Router(config-router)#network 10.1.5.0
Router(config-router)#
```

Redistribution: Bir yönlendirme protokolü (örneğin, EIGRP) tarafından öğrenilen yönlendirme bilgilerini başka bir yönlendirme protokolüne (örneğin, OSPF)yeniden dağıtma işlemidir.Bu işlem, farklı yönlendirme protokollerinin bir arada çalıştığı ağlarda kritik öneme sahiptir.Farklı routing protokolleri kullanan routerları,areaları birbirine öğretmek için kullanılır.

```
redistribute ospf 1 metric <bandwidth> <delay> <reliable> <Load> <MTU>
```

EIGRP'den OSPF'ye Redistribution

```
router ospf 1  
redistribute eigrp 10 subnets
```

OSPF'den EIGRP'ye Redistribution

```
router eigrp 10  
redistribute ospf 1 metric 10000 100 255 1 1500
```

Örnek (OSPF to EIGRP):

```
router eigrp 1  
Router(config-router)#redistribute ospf 1 metric 100000 10 255 1 10
```

örnek (EIGRP to OSPF):

```
router ospf 1  
redistribute eigrp 1 subnets
```

no router eigrp 1: eigrp konfigürasyonunu geri almak için kullanılır.

ACCESS LIST (ACL)

Ağlarda "Access List" (Erişim Listesi), ağ trafiğini kontrol etmek ve yönetmek için kullanılan bir dizi kuraldır.

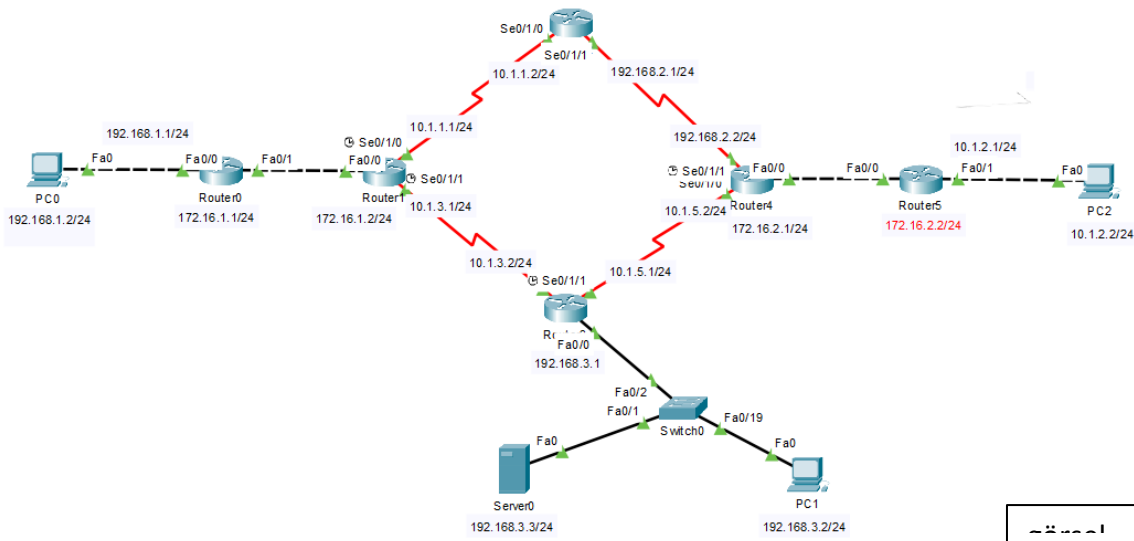
Access List'ler, belirli trafiğin izin verilmesine veya engellenmesine karar verir ve genellikle router'lar, switch'ler veya firewall'lar üzerinde uygulanır. Belirli IP adresleri, protokoller, port numaraları ve diğer kriterler baz alınarak trafik filtrelemeyi sağlar.

Inbound Access List: Gelen trafiği kontrol eder ve filtreler.

Outbound Access List: Giden trafiği kontrol eder ve filtreler.

Standart Access List: (hedefe yakın) Sadece kaynak IP adresine dayalı olarak trafiği kontrol eden erişim listeleridir. Sadece kaynak IP adresine göre filtreleme yaparlar. Hedefe yakın tarafta bağlanır.

Extended Access List: (kaynağa yakın) Kaynak ve hedef IP adresleri, protokoller (TCP, UDP, ICMP gibi), port numaraları gibi daha spesifik kriterlere dayalı olarak trafiği kontrol eden erişim listeleridir. Kaynağa yakın tarafta bağlanır.



Standart ACL konfigürasyonu

Görseldeki 192.168.1.2/24 adresli PCden gelen verinin 10.1.2.2/24 adresli PCye ulaşmasını engellemek için 10.1.2.2/24 adresli PCye en yakın Router konfigüre edilir.

```
Router(config)#access-list ?
<1-99>      IP standard access list
<100-199>   IP extended access list
Router(config)#access-list 1 ?
deny        Specify packets to reject
permit      Specify packets to forward
remark      Access list entry comment
Router(config)#access-list 1 remark bu liste 1.2 adresli PCyi deny eder.
Router(config)#
Router(config)#access-list 1 deny ?
A.B.C.D     Address to match
any         Any source host
host        A single host address
Router(config)#access-list 1 deny host 192.168.1.2
Router(config)#
```

outbound acl konfigürasyon

```
Router(config)#int fa 0/1
Router(config-if)#ip access-group 1 out
Router(config-if)#
```

1 numaralı listeyi 0/1 interfacei'ne outbound olarak bağlar.

Do show access-list: Bu komut, cihazda tanımlanmış tüm erişim listelerini ve bunların içeriklerini görüntüler.

```
Router(config-if)#do show access-list
Standard IP access list test
 10 deny host 192.168.3.2
 20 deny host 192.168.1.2
 30 permit any
```

192.168.1.2/24 adresli PCden 10.1.2.2/24 adresli PCye ping atmaya denediğimizde artık failed olarak hata alıyoruz.



Failed

PC0

PC2

ICMP



0.000

N

17

(edit)

(delete)

Extended ACL konfigürasyonu

access-list [ACL_NUMARASI] [izin_veya_reddet] [protokol] [kaynak_ip] [hedef_ip]

Örnek: 192.168.1.2/24 adresli PCden 10.1.2.2/24 adresli PCye ping atmayı engellemek istiyoruz. Ping protokolü: icmp

172.16.1.1 ip adresli router üzerinde yapılan konfigürasyon işlemi:

```
Router(config)#access-list ?
  <1-99>      IP standard access list
  <100-199>   IP extended access list
Router(config)#access-list 100?
<100-199>
Router(config)#access-list 100 deny ?
  ahp      Authentication Header Protocol
  eigrp    Cisco's EIGRP routing protocol
  esp      Encapsulation Security Payload
  gre      Cisco's GRE tunneling
  icmp     Internet Control Message Protocol
  ip       Any Internet Protocol
  ospf     OSPF routing protocol
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
Router(config)#access-list 100 deny icmp ?
  A.B.C.D   Source address
  any       Any source host
  host      A single source host
Router(config)#access-list 100 deny icmp host 192.168.1.2 ?
  A.B.C.D   Destination address
  any       Any destination host
  host      A single destination host
Router(config)#access-list 100 deny icmp host 192.168.1.2 host 10.1.1.2
Router(config)#
```

Access-list 100 permit ip any any : komutu ile diğer işlemlere izin verilmiş olur.

```
Router(config)#do show access-list
Extended IP access list 100
  10 deny icmp host 192.168.1.2 host 10.1.1.2 (2 match(es))
  20 permit ip any any
```

Inbound acl konfigürasyon

```
Router(config)#int fa 0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

Server ACL konfigürasyon işlemi

Görsel 8'de bulunan server için bazı kısıtlamalar yapmak istiyoruz. 192.168.3.1 ip adresli router üzerinde bazı konfigürasyon işlemleri yapacağız. Bu ACL konfigürasyonu, belirli bir sunucuya (192.168.3.3) giden HTTP trafiğini kontrol ederken diğer tüm IP trafiğini engeller. HTTP trafiği için özel

izin verilmişken, diğer trafiğe izin verilmemiştir. Bu yapılandırma, sunucunun yalnızca belirli türdeki trafiği almasını sağlamak için kullanılır.

```
Router(config)#access-list 100 permit tcp any host 192.168.3.3 eq 80
Router(config)#access-list 100 deny ip any host 192.168.3.3
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#interface fastethernet 0/0
Router(config-if)#ip access-group 100 out
Router(config-if)#
```

1. Komut, herhangi bir kaynaktan 192.168.3.3 IP adresindeki sunucuya HTTP (port 80) trafiğine izin verir.
2. Komut herhangi bir kaynaktan 192.168.3.3 IP adresindeki sunucuya giden tüm IP trafiğini engeller.
3. Komut önceki kurallardan etkilenmeyen tüm IP trafiğine izin verir. Bu, ACL'nin sonunda "default" olarak tüm diğer trafiği geçişine izin verir.

Named Access List (Adlandırılmış Erişim Listesi), Cisco IOS cihazlarında kullanılan bir erişim listesi türüdür. Adlandırılmış ACL'ler, erişim listelerini daha anlamlı isimlerle tanımlamanıza olanak tanır, bu da yönetimi ve konfigürasyonu daha kolay hale getirir.

Örnek: İlk Konfigürasyon:

192.168.3.2 IP adresinden gelen trafiği engeller. Diğer tüm trafiğe izin verir.

```
Router(config)#ip access-list standard test
Router(config-std-nacl)#deny 192.168.3.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#do show access-list
Standard IP access list test
  10 deny host 192.168.3.2
  20 permit any
```

Güncellenmiş Konfigürasyon:

192.168.3.2 IP adresinden gelen trafiği engeller. Diğer tüm trafiğe izin verir.

```
Router(config-std-nacl)#no permit any
Router(config-std-nacl)#deny 192.168.1.2
Router(config-std-nacl)#permit any
Router(config-std-nacl)#do show access-list
Standard IP access list test
  10 deny host 192.168.3.2
  20 deny host 192.168.1.2
  30 permit any
```

SWITCH CİHAZIYLA İLGİLİ KONFIGÜRASYON İŞLEMLERİ

switch ismini değiştirme

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#hostname merkez-sw
merkez-sw(config)#
```

mesaj yazdırma

```
merkez-sw(config)#banner motd *
Enter TEXT message. End with the character '*'.
giris mesaji
*
```

Console şifresi verme

```
merkez-sw(config)#
merkez-sw(config)#line console 0
merkez-sw(config-line)#password sifrel23
merkez-sw(config-line)#login
merkez-sw(config-line)#
```

enable şifresi verme

```
merkez-sw(config-line)#
merkez-sw(config-line)#enable secret sifrel23
merkez-sw(config)#
```

telnet şifresi verme

```
merkez-sw(config)#line vty 0 15
merkez-sw(config-line)#password sifrel23
merkez-sw(config-line)#
```

Ip adresi atama

```
merkez-sw(config-line)#
merkez-sw(config-line)#interface vlan 10
merkez-sw(config-if)#ip address 192.168.1.100 255.255.255.0
merkez-sw(config-if)#no shutdown
merkez-sw(config-if)#
```

VLAN (Virtual Local Area Network)

VLAN (Virtual Local Area Network), fiziksel ağ cihazlarını kullanarak mantıksal ağ segmentleri oluşturma yöntemidir. VLAN'lar, aynı fiziksel ağ altyapısı üzerinde birden fazla, izole edilmiş ağ oluşturmaları sağlar. Bu, ağ trafiğini izole etmek, güvenliği artırmak ve ağ yönetimini kolaylaştırmak için kullanılır. Her VLAN, kendi ayrı broadcast domain'ine sahiptir. Bu, bir VLAN'daki broadcast trafiğinin diğer VLAN'lara yayılmasını engeller. Ağları izole ederek güvenliği artırır.

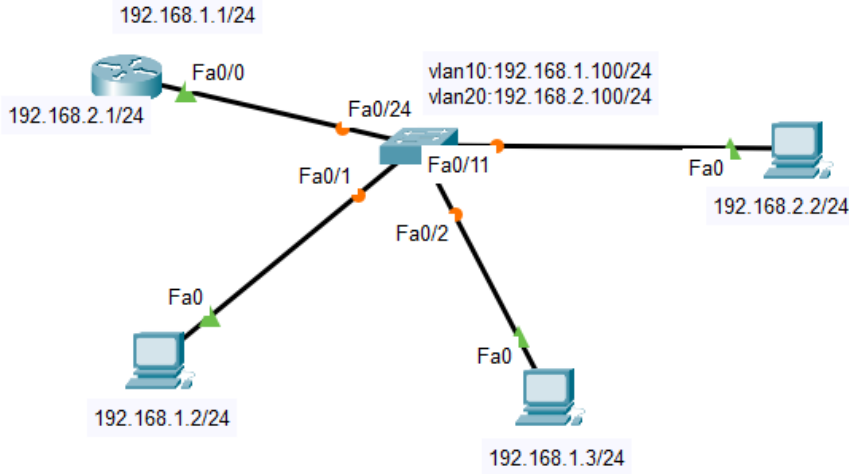
VLAN kullanmadan her bir grup farklı bir IP ağı ve farklı bir switch üzerindedir. VLAN kullanıldığında switch, portlarıyla uygun VLAN'lar üzerinde konfigüre edilir. Hala her bir grup farklı bir IP ağı üzerindedir, fakat gruplar aynı switch üzerindedirler.

port based vlan: Fiziksel portlar üzerinden yapılan VLAN yapılandırmasını ifade eder.

mac based vlan: Cihazların MAC adreslerine göre VLAN'lara atanmasını sağlar.

VLAN oluşturma

```
Switch(config)#vlan 2
Switch(config-vlan)#name muhasebe
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
```



görsel:9

Görsel 9'daki topolojide bulunan switch cihazının konfigürasyon işlemlerini yapalım:

```
Switch(config)#
Switch(config)#interface range fastethernet 0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#
```

- **interface range fastethernet 0/1-10:** FastEthernet0/1 ile FastEthernet0/10 arasındaki portları aynı anda yapılandırmak için bu komut kullanılır.

- **switchport mode access:** Portları erişim moduna (access mode) ayarlar. Bu, portların yalnızca bir VLAN'a ait olacak şekilde yapılandırıldığı anlamına gelir.
- **switchport access vlan 10:** Seçilen portları VLAN 10'a atar. Bu, FastEthernet0/1 ile FastEthernet0/10 arasındaki portların VLAN 10'a ait olmasını sağlar.

```
Switch(config)#
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.1.100 255.255.255.0
Switch(config-if)#
```

- **interface vlan 10:** VLAN 20 için sanal bir arayüz (SVI - Switched Virtual Interface) oluşturur. Bu sanal arayüz, VLAN 20'ye IP adresi atamak ve bu VLAN'a IP tabanlı yönetim erişimi sağlamak için kullanılır.
- **Ip address 192.168.1.100 255.255.255.0:** VLAN 20 arayüzüne IP adresi ve alt ağ maskesi atar. Bu, VLAN 20 içindeki cihazların bu IP adresi ile ağ üzerinde iletişim kurmasını sağlar.

Aynı işlemi vlan20 için de yapıyoruz:

```
Switch(config)#
Switch(config)#int range fastethernet 0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#
Switch(config-if-range)#exit
Switch(config)#
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.2.100 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

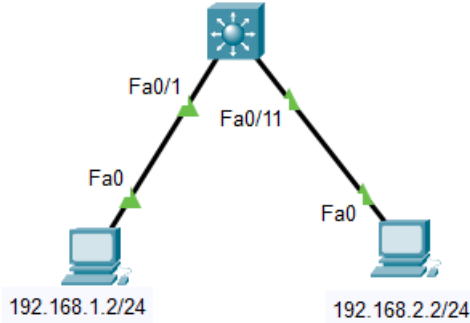
Router Interface VLANlara bölme

Görsel 9'daki router üzerinde VLAN'lara göre arayüzleri yapılandırma ve her VLAN için IP adresi atama işlemlerini yapalım:

```
Router(config)#
Router(config)#interface fastethernet 0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#interface fastethernet 0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
```

Multilayer switch: hem Layer 2 (Veri Bağlantı Katmanı) hem de Layer 3 (Ağ Katmanı) fonksiyonlarını yerine getirebilen ağ cihazlarıdır. Bu switch'ler, hem geleneksel switch özelliklerine sahip olup aynı zamanda yönlendirme (routing) yapabilme yeteneğine sahiptirler.

Şekilde **192.168.1.2** ve **192.168.2.2** IP adresli iki PC, farklı ağlarda bulundukları için doğrudan haberleşemezler. İletişim sağlanabilmesi için ağlar arasında yönlendirme yapılması gerekir. Bu, bir yönlendirici veya multilayer switch kullanılarak sağlanır.



Trunk Port

Trunk port, bir switch portunun birden fazla VLAN'ı taşımasını sağlayan bir yapılandırma modudur. Trunk portları, genellikle switch'ler arasında veya switch ile router arasında bağlantı kurmak için kullanılır ve birden fazla VLAN'a ait trafiği tek bir fiziksel bağlantı üzerinden taşır.

Bu portlarda encapsulation vardır:

ISL

802.1Q



Yukarıdaki şekilde üç switch arasındaki bağlantıyı trunk modunda yapılandırmak ve birbirleriyle iletişim kurmalarını sağlamak için aşağıdaki adımlar takip edilmelidir:

Switch 1 Konfigürasyonu

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Switch 2 Konfigürasyonu

```
Switch(config)#  
Switch(config)#interface fastethernet 0/24  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#  
Switch(config-if)#exit  
Switch(config)#  
Switch(config)# interface fastethernet 0/23  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#end
```

Switch 3 Konfigürasyonu

```
Switch>en  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#interface fastethernet 0/23  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#end  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console
```

VTP: VLAN bilgilerinin ağdaki diğer cihazlar ile paylaşılması amacı ile oluşturulan bir protokoldür. Böylece geniş bir ağ içerisindeki tüm cihazlar için aynı VLAN konfigürasyonunun yapılmasına gerek kalmaz. VTP, switch'lerin VLAN bilgilerini birbirlerine iletmelerini sağlayarak, VLAN yapılandırmasını daha kolay ve tutarlı hale getirir.

Switch cihazlarının birbiriyle VLAN alışverişi yapabilmesi için Trunk mode, aynı VTP domain ve aynı VTP password olması gerekir. Şifre belirlenmezse konfigürasyonlar switchlerin hepsine yapılır.

VTP Modları

Server Mode: Bu modda çalışan switch üzerinde VLAN oluşturulur, değiştirilir ve silinebilir.

Transparent Mode: Bu modda çalışan switch VTP'den VLAN bilgilerini alabildiği gibi, kendi üzerinde de VLAN oluşturulabilir. Ancak, kendi üzerinde üretilen VLAN bilgilerini diğer switchler ile paylaşmaz.

Client Mode: Bu modda çalışan switch trunk portları üzerinden VLAN bilgisini alırlar ve VLAN bilgilerini diğer trunk portlara taşırlar. Ancak kendi üzerlerinde VLAN oluşturamaz ya da silemezsiniz.

VTP durumunu gösteren komut: `do show vtp status`

VTP şifre belirleme komutu: `vtp password 123`

VLAN trafiği esnekliği sağlamak amacıyla portları taşımaz.

relay agent: genellikle DHCP (Dynamic Host Configuration Protocol) bağlamında kullanılan bir terimdir. Bir relay agent, bir DHCP istemcisinden gelen DHCP mesajlarını, istemciyle aynı ağda bulunmayan bir DHCP sunucusuna ileten bir ağ cihazıdır. Relay agent'lar, DHCP istemcileri ve sunucuları farklı alt ağlarda olduğunda kullanılır.

DHCP istemcilerinden gelen mesajları alır.Bu mesajları uygun DHCP sunucusuna iletir.DHCP sunucusundan gelen yanıtları alır ve istemciye geri iletir.

NAT

(Network Address Translation), ağ adresi çevrimi anlamına gelir ve ağdaki IP adreslerinin, özellikle özel (private) IP adreslerinin, başka bir ağdaki IP adreslerine çevrilmesi işlemini ifade eder.

NAT, internet üzerinde sınırlı sayıda IP adresi kullanarak birden fazla cihazın internete erişmesine olanak tanır ve güvenlik sağlar.

- **İki Taraf Private:** İç ağdaki cihazlar, özel IP adresleri kullanarak sadece iç ağ içinde iletişim kurar.
- **İki Taraf Public:** Her iki taraf da genel IP adreslerine sahiptir ve doğrudan iletişim kurar.
- **Public-Private:** İç ağdaki cihazlar, NAT kullanılarak genel IP adresi ile internete erişir ve genel IP adresleri, özel IP adreslerine dönüştürülür.

*Özel IP adres aralıkları (IPv4):

10.0.0.0 - 10.255.255.255

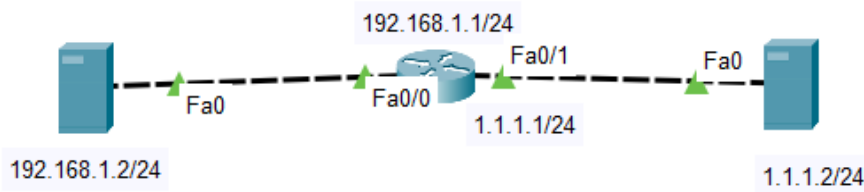
172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

PAT (Port Address Translation), NAT türlerinden biridir ve birden fazla özel IP adresinin tek bir genel IP adresini paylaşmasına olanak tanır.

PAT, her özel IP adresini ve port numarasını benzersiz bir genel IP adresi ve port numarası kombinasyonuna çevirir. Bu sayede, sınırlı sayıda genel IP adresi kullanarak birçok cihazın internete erişimini sağlar.

Örnek topoloji



NAT İŞLEM ADIMLARI

Adım 1: 192.168.1.2 IP adresine sahip Server1, internet üzerindeki Server2 cihazına erişim talebinde bulunur.

Adım 2: Yönlendirici, bu isteği alır ve NAT işlemi uygular.

Adım 3: Yönlendirici, özel IP adresini (192.168.1.2) genel bir IP adresine (1.1.1.2) çevirir ve paketi Server2ye gönderir.

Adım 4: Artık Server2nin ip adresi 1.1.1.2 yani nat işlemi uygulanan ip ile aynı networkte bulunmakta yani server1 ve server2 haberleşebilir durumdadır. Server2 yanıtı Genel IP adresine (1.1.1.2) gönderilir.

Adım 5: Yönlendirici, bu yanıtı alır, NAT tablosunu kullanarak özel IP adresine (192.168.1.2) çevirir ve paketi server1e iletir.

NAT Konfigürasyonu

```
Router>
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#interface fast
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface fastEthernet 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat inside source list 1 int fa 0/1
Router(config)#ip nat inside source list 1 int fa 0/1 overload
Router(config)#
```

- **access-list 1 permit 192.168.1.0 0.0.0.255:** Belirli IP adresleri için NAT uygulanmasını sağlar.
- **interface fastEthernet 0/0:** İç ağ arayüzünü yapılandırır.
- **ip nat inside:** İç ağ arayüzü olarak işaretler.
- **interface fastEthernet 0/1:** Genel ağ arayüzünü yapılandırır.
- **ip nat outside:** Genel ağ arayüzü olarak işaretler.
- **ip nat inside source list 1 interface fastEthernet 0/1:** İç IP adreslerini genel IP adresine dönüştürür, tek bağlantıyı destekler.
- **ip nat inside source list 1 int fa 0/1 overload:** PAT uygular, çoklu bağlantıları destekler.
- **do debug ip nat:** NAT işlemlerinin ayrıntılı hata ayıklamasını sağlar. adresiyle (NAT ile) değiştirir ve aynı anda birden fazla bağlantıyı desteklemek için "overload" (PAT - Port Address Translation) kullanır.

Belirli bir iç IP adresi ve port numarasını belirli bir dış IP adresi ve port numarası ile statik olarak eşlemek için konfigürasyon:

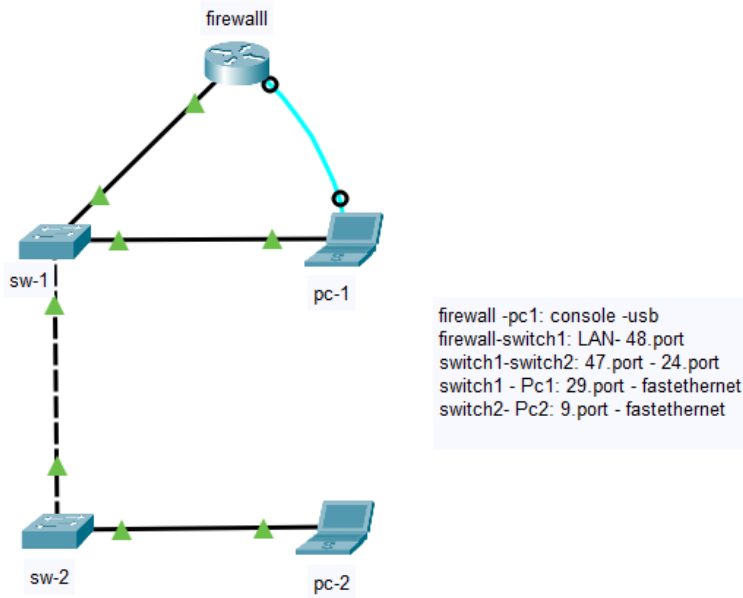
```
Router(config)#ip nat inside source static
Router(config)#ip nat inside source static tcp 10.1.1.1 80 192.168.1.2 80
Router(config)#ip nat inside source static tcp 192.168.1.2 80 1.1.1.1 80
```

Router(config)#do show ip nat translations: mevcut nat dönüşümlerini gösterir.

PROJE -1

Switch ve firewall cihazlarını kullanarak yaptığımız proje ve detayları:

Aşağıdaki görsel projeye ait topoloji örneğidir.



Öncelikle mevcut switch ve firewall cihazlarının konfigürasyon bilgileri sıfırlanır.

Switch1 ve switch2 cihazları içindeki konfigürasyonları sıfırlamak için kullanılan komut:

`erase startup-config`

Fortinet firewall cihazının arayüzüne giriş yapmak için kullanılan default ip :192.168.1.99

Firewall içindeki konfigürasyonları sıfırlamak için kullanılan komut: `execute factoryreset`

Öncelikle merkez-sw1 PC1e usb ile bağlanır ve konfigüre edilir.

IP ataması yapılır. Vlanlar oluşturulur.

Telnet bağlantısı ile merkez-sw2 ye bağlanılır ve aynı şekilde bu switch de konfigüre edilir.

Switch1'de 47-48 portlar trunk mode olarak ayarlanır. Bu portlardan biri firewalla diğeri switch2'ye bağlanır.

Switch2'de 24. port trunk mode olarak ayarlanır. Bu port switch1'e bağlanır.

Firewall'ı konfigüre etmek için switch1'e bağlanılır ve firewall arayüzüne girilir.

Daha sonra Firewall arayüzünde interfaceler oluşturularak vlanlar tanımlanır.

birimler ve mgmt adında iki tane zone oluşturulur.

birimler zone: bilgiislem,muhasebe,destek vlanları bulunur.

mgmt zone: management vlanları bulunur.

Bu vlanlara uygun policy yazılır.

Pc1 bilgiislem vlanına dahil etmek için switch1'de 1-5 arası bir porta bağlanır.

Pc2 muhasebe vlanına dahil etmek için switch2'de 20-30 arası bir porta bağlanır.

PC1'i bilgiislem vlanına dahil etmek için yazılan policy

incoming interface: birimler

outgoing interface:management

source : bilgiislem

destination: management

service: all

Aynı işlem PC2'yi switch2'deki muhasebe vlanına dahil etmek için yapılır.

BAĞLANTI PORTLARI

firewall -pc1: console - usb

firewall-switch1: LAN - 48.port

switch1-switch2: 47.port - 24.port

switch1 - Pc1: 29.port - fastethernet

switch2- Pc2: 9.port - fastethernet

Switch1

```
Running configuration:

; J9019B Configuration Editor; Created on release #Q.11.17

hostname "merkez-sw2"
ip default-gateway 10.1.100.1
snmp-server community "public" Unrestricted
vlan 1
    name "DEFAULT VLAN"
    untagged 16-26
    ip address dhcp-bootp
    no untagged 1-15
    exit
vlan 5
    name "bilgiislem"
    untagged 1-5
    exit
vlan 10
    name "muhasebe"
    untagged 6-10
    exit
vlan 15
    name "destek"
    untagged 11-15
    exit
vlan 100
    name "management"
    ip address 10.1.100.101 255.255.255.0
    tagged 23-24
    exit
password manager
password operator
```

switch2

```
Running configuration:

; j9020a Configuration Editor; Created on release #U.11.04

hostname "merkez_sw1"
ip default-gateway 10.1.100.100
snmp-server community "public" Unrestricted
vlan 1
    name "DEFAULT VLAN"
    untagged 31-52
    ip address dhcp-bootp
    no untagged 1-30
    exit
vlan 10
    name "muhasebe"
    untagged 1-10
    exit
vlan 20
    name "destek"
    untagged 11-20
    exit
vlan 30
    name "BilgiIslem"
    untagged 21-30
    exit
vlan 100
    name "Management"
    ip address 10.1.100.1 255.255.255.0
    tagged 47-48
    exit
password manager
password operator

merkez_sw1(config)#
```

Firewall arayüzü

Firewall arayüzüne bağlanmak için management vlan ip ile giriş yapılır.
Ip address: 10.1.100.1

Login page

Mevcut Interfaces

FortiGate 30E FortiGate-30E								
Dashboard								
Security Fabric								
FortiView								
Network								
Interfaces								
DNS								
Packet Capture								
SD-WAN								
SD-WAN Rules								
Performance SLA								
Static Routes								
FortiExtender								
System								
Policy & Objects								
Security Profiles								
VPN								
User & Device								
WiFi & Switch Controller								
Log & Report								
Monitor								

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
Hardware Switch							
fortilink	Hardware Switch		Dedicated to FortiSwitch	PING Security Fabric Connection		169.254.1.2-169.254.1.254	2
lan	Hardware Switch	lan1 lan2 lan3 lan4	192.168.1.99/255.255.255.0	PING HTTPS SSH HTTP	2	192.168.1.110-192.168.1.210	7
Physical Interface							
wan	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			1
Zone							
birimler	Zone	bilgislem destek muhasabe	0.0.0.0/0.0.0.0				1
mgmt	Zone	management	0.0.0.0/0.0.0.0				1

Mevcut Policies

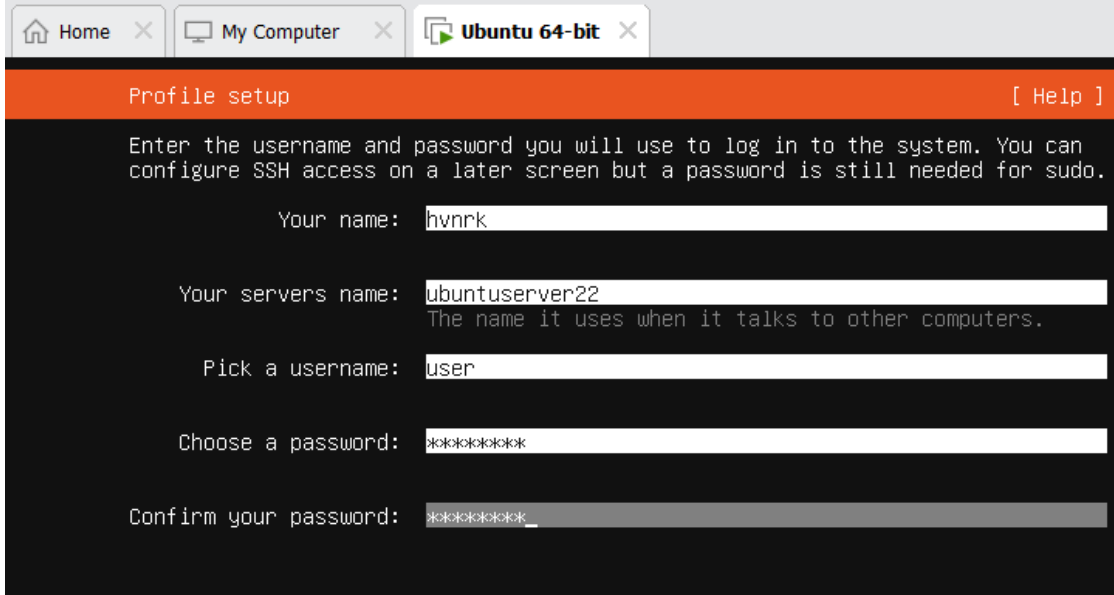
FortiGate 30E FortiGate-30E											
Dashboard											
Security Fabric											
FortiView											
Network											
System											
Policy & Objects											
IPv4 Policy											
Authentication Rules											
Addresses											
Internet Service Database											
Services											
Schedules											
Virtual IPs											
IP Pools											

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Interface Pair View By Sequence										
2	1	bilgislem address	management address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	all	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
Implicit										
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	50.22 kB

UBUNTU SERVER KURULUMU

Ubuntu server kurmak için öncelikle VmWare Workstation indiriyoruz. Daha sonra yeni bir sanal makine oluştur seçeneğine tıklayarak aşağıdaki adımları izliyoruz:

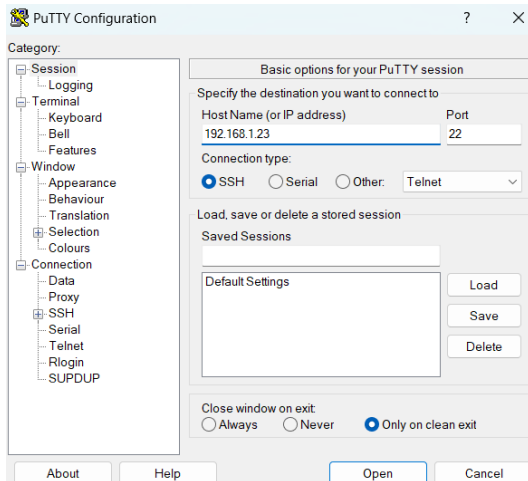
- "Installer disc image file (iso)" seçeneğini seçin.
 - "Browse" (Gözet) düğmesine tıklayın ve Ubuntu Server ISO dosyanızı seçin.
 - "Linux" ve "Ubuntu" seçeneklerini seçin. Uygun Ubuntu sürümünü seçin (örneğin, Ubuntu 20.04).
 - Sanal makinenize bir ad verin (örneğin, "Ubuntu Server") ve sanal makineyi kaydedeceğiniz bir konum seçin.
 - <https://ubuntu.com/download/server> adresinden iso dosyasını indiriyoruz.
 - Sanal makinenizi başlatın ve ISO dosyasından önyükleme yapmasını bekleyin.
- Kurulum tamamlandığında görseldeki login sayfasına istenen bilgileri yazın.



Putty ile bağlanma

Putty uygulamasını <https://www.putty.org/> adresinden indiriyoruz.

Puttyye bağlanmak için server'ın IP adresini yazarak giriş yapıyoruz:



Username ve password ile giriş yapıyoruz:

```
user@ubuntuserver: ~  
login as: user  
user@192.168.1.23's password:  
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-116-generic x86_64)
```

Kullanıcıdan root yetkisine geçmek için sudo su komutu kullanılabilir:

```
user@ubuntuserver:~$  
user@ubuntuserver:~$ sudo su  
[sudo] password for user:  
root@ubuntuserver:/home/user#
```

LAMP Stack Kurulumu

Sistem Güncellemesi

```
sudo apt update  
sudo apt upgrade
```

Apache Web Sunucusunun Kurulumu

```
sudo apt update  
sudo apt install apache2  
sudo ufw allow in "Apache"
```

ufw app list :Bu komut, ufw'de tanımlı olan uygulama profillerinin bir listesini verir.

```
root@ubuntuserver:/home/user# ufw app list  
Available applications:  
  Apache  
  Apache Full  
  Apache Secure  
  OpenSSH
```

ufw status komutu, ufw'nin mevcut durumunu gösterir. Bu komutu çalıştırdığınızda, güvenlik duvarının etkin olup olmadığını ve mevcut kuralları listeleyebilirsiniz.

```
josh@ubs24:~$ sudo ufw status  
Status: active  
  
To Action From  
--  
OpenSSH ALLOW Anywhere  
OpenSSH (v6) ALLOW Anywhere (v6)
```


ufw allow apache komutu, ufw (Uncomplicated Firewall) kullanarak Apache web sunucusunun gerekli olan portlarını açar. Bu komut, Apache'nin HTTP (80) ve HTTPS (443) portlarının trafiğine izin verir.


```
josh@ubuntu24:~$ sudo ufw allow Apache
Rule added
Rule added (v6)
josh@ubuntu24:~$ sudo ufw status
Status: active

To Action From
--
OpenSSH ALLOW Anywhere
Apache ALLOW Anywhere
OpenSSH (v6) ALLOW Anywhere (v6)
Apache (v6) ALLOW Anywhere (v6)
```

Apache'nin çalışıp çalışmadığını kontrol etmek için:
sudo systemctl status apache2

http://server_ip adresine gittiğimizde ubuntu default sayfası açılır.



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in** [/usr/share/doc/apache2/README.Debian.gz](#). Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `system` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file outside of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in

MySQL Veritabanı Sunucusunun Kurulumu:

```
sudo apt install mysql-server
systemctl start mysql
systemctl enable mysql
```

MySQL güvenlik ayarlarını yapılandırmak için:

```
sudo mysql_secure_installation
```

MySQL veritabanı sunucusuna root kullanıcısı olarak giriş yapmak için **mysql -u root -p** komutu kullanılır. Daha önceden belirlediğimiz sql şifresi ile giriş yapılır.

```
root@ubuntuserver:/home/user#  
root@ubuntuserver:/home/user# mysql -u root -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 150  
Server version: 8.0.37-0ubuntu0.22.04.3 (Ubuntu)  
  
Copyright (c) 2000, 2024, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql>
```

Kullanıcı adını ve şifreyi güncellemek için:

```
mysql> ALTER USER 'programmer'@'localhost' IDENTIFIED WITH mysql_native_password BY  
'password1';
```

mysql -u programmer -p komutu, MySQL veritabanına "programmer" adlı kullanıcı olarak giriş yapmanızı sağlar. -u seçeneği kullanıcı adını belirtir, -p ise parola girmenizi sağlar.

```
root@ubuntuserver:/home/user# mysql -u programmer -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 151  
Server version: 8.0.37-0ubuntu0.22.04.3 (Ubuntu)  
  
Copyright (c) 2000, 2024, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql>
```

Yeni bir database oluşturmak için: **create database <db_name>** komutu kullanılır.

Görselde demo adında yeni bir db oluşturduk. Daha sonra için **show databases** komutunu kullanarak mevcut databaseleri listelediğimizde demo db eklendiğini görebiliriz.

```
mysql>
mysql> create database demo;
Query OK, 1 row affected (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| demo     |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+
5 rows in set (0.00 sec)

mysql>
```

PHP'yi kurmak için:

```
sudo apt install php libapache2-mod-php php-mysql
php -v
```

Sisteme restart yapmak için: sudo systemctl restart apache2

PHP'nin Apache ile düzgün çalıştığını test etmek için:

- Yeni bir PHP dosyası oluşturun:

```
sudo nano /var/www/html/info.php
```

- Dosyaya şu kodu ekleyin:

```
<?php
phpinfo();
?>
```


- Dosyayı kaydedin ve çıkın (Ctrl + X, ardından Y ve Enter tuşlarına basarak kaydedin).
- Tarayıcınızda <http://<sunucu-ip-adresi>/info.php> adresine gidin. PHP bilgilerini gösteren bir sayfa görmelisiniz.

← → Güvenli değil 192.168.1.6/info.php

Uygulamalar

Tüm Yer İşareti


PHP Version 8.1.2-1ubuntu2.18



System	Linux ubuntu:server 5.15.0-115-generic #126-Ubuntu SMP Mon Jul 1 10:14:24 UTC 2024 x86_64
Build Date	Jun 14 2024 15:52:55
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.1/apache2
Loaded Configuration File	/etc/php/8.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.1/apache2/conf.d
Additional .ini files parsed	/etc/php/8.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.1/apache2/conf.d/10-opcache.ini, /etc/php/8.1/apache2/conf.d/10-pdo.ini, /etc/php/8.1/apache2/conf.d/15-xsl.ini, /etc/php/8.1/apache2/conf.d/20-bz2.ini, /etc/php/8.1/apache2/conf.d/20-calendar.ini, /etc/php/8.1/apache2/conf.d/20-curl.ini, /etc/php/8.1/apache2/conf.d/20-dom.ini, /etc/php/8.1/apache2/conf.d/20-exif.ini, /etc/php/8.1/apache2/conf.d/20-ffi.ini, /etc/php/8.1/apache2/conf.d/20-fileinfo.ini, /etc/php/8.1/apache2/conf.d/20-ftp.ini, /etc/php/8.1/apache2/conf.d/20-gd.ini, /etc/php/8.1/apache2/conf.d/20-gettext.ini, /etc/php/8.1/apache2/conf.d/20-iconv.ini, /etc/php/8.1/apache2/conf.d/20-imagick.ini, /etc/php/8.1/apache2/conf.d/20-ldap.ini, /etc/php/8.1/apache2/conf.d/20-ldap_sasl.ini, /etc/php/8.1/apache2/conf.d/20-mbstring.ini, /etc/php/8.1/apache2/conf.d/20-mysql.ini, /etc/php/8.1/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.1/apache2/conf.d/20-posix.ini, /etc/php/8.1/apache2/conf.d/20-readline.ini, /etc/php/8.1/apache2/conf.d/20-shmop.ini, /etc/php/8.1/apache2/conf.d/20-simplexml.ini, /etc/php/8.1/apache2/conf.d/20-sockets.ini, /etc/php/8.1/apache2/conf.d/20-sysmsg.ini, /etc/php/8.1/apache2/conf.d/20-syssem.ini, /etc/php/8.1/apache2/conf.d/20-sysshm.ini, /etc/php/8.1/apache2/conf.d/20-tokenizer.ini, /etc/php/8.1/apache2/conf.d/20-xmlreader.ini, /etc/php/8.1/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.1/apache2/conf.d/20-xsl.ini, /etc/php/8.1/apache2/conf.d/20-zip.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API20210902.NTS
PHP Extension Build	API20210902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

Bu işlemleri yaptıktan sonra phpmyadmin sayfasına giriş yapabiliriz.

Güvenli değil 192.168.1.6/phpmyadmin/


phpMyAdmin'e Hoş Geldiniz

Dil - Language

Türkçe - Turkish

Oturum aç

Kullanıcı Adı: programmer

Parola:

Git

PhpMyAdmin arayüzü:

Güvenli değil 192.168.1.6/phpmyadmin/index.php?route=/&route=%2F

Sunucu: localhost:3306

Veritabanları SQL Durum Dışa aktar İçe aktar Ayarlar Değişkenler Karakter Grupları Motorlar Eklentiler

Son Sık kullanılanlar

Yeni BookStore exampleDB information_schema performance_schema

Genel ayarlar

Parola değiştir

Sunucu bağlantısı karşılaştırması: utf8mb4_unicode_ci

Daha fazla ayar

Görünüm ayarları

Dil - Language Türkçe - Turkish

Tema: pmahomme

Veritabanı sunucusu

- Sunucu: Localhost via UNIX socket
- Sunucu türü: MySQL
- Sunucu bağlantısı: SSL kullanılmamakta
- Sunucu sürümü: 8.0.37-0ubuntu0.22.04.3 - (Ubuntu)
- Protokol sürümü: 10
- Kullanıcı: programmer@localhost
- Sunucu karakter grubu: UTF-8 Unicode (utf8mb4)

Web sunucusu

- Apache/2.4.52 (Ubuntu)
- Veritabanı istemcisi sürümü: libmysqld - mysqld 8.1.2-1ubuntu2.18
- PHP uzantısı: mysql curl mbstring
- PHP sürümü: 8.1.2-1ubuntu2.18

phpMyAdmin

- Sürüm bilgisi: 5.1.1deb5ubuntu1
- Belgeler
- Resmî phpMyAdmin Anasayfası
- Katkıda bulun
- Destek al
- Değişikliklerin listesi

Konsol

Kaynaklar:

<https://www.howtoforge.com/>

How To Install Linux, Apache, MySQL, PHP (LAMP) Stack on Ubuntu | DigitalOcean,

FILEZILLA KULLANIMI

FileZilla, kullanıcıların FTP (File Transfer Protocol), SFTP (SSH File Transfer Protocol), ve FTPS (FTP Secure) protokollerini kullanarak dosyaları sunucularla paylaşmasını sağlayan açık kaynaklı ve ücretsiz bir dosya aktarım programıdır. Özellikle web geliştirme ve sunucu yönetimi süreçlerinde kullanışlıdır. FileZilla ile dosyaları sunuculara yükleyebilir, sunucudan dosyaları indirebilir ve dosyaların yönetimini yapabilirsiniz.

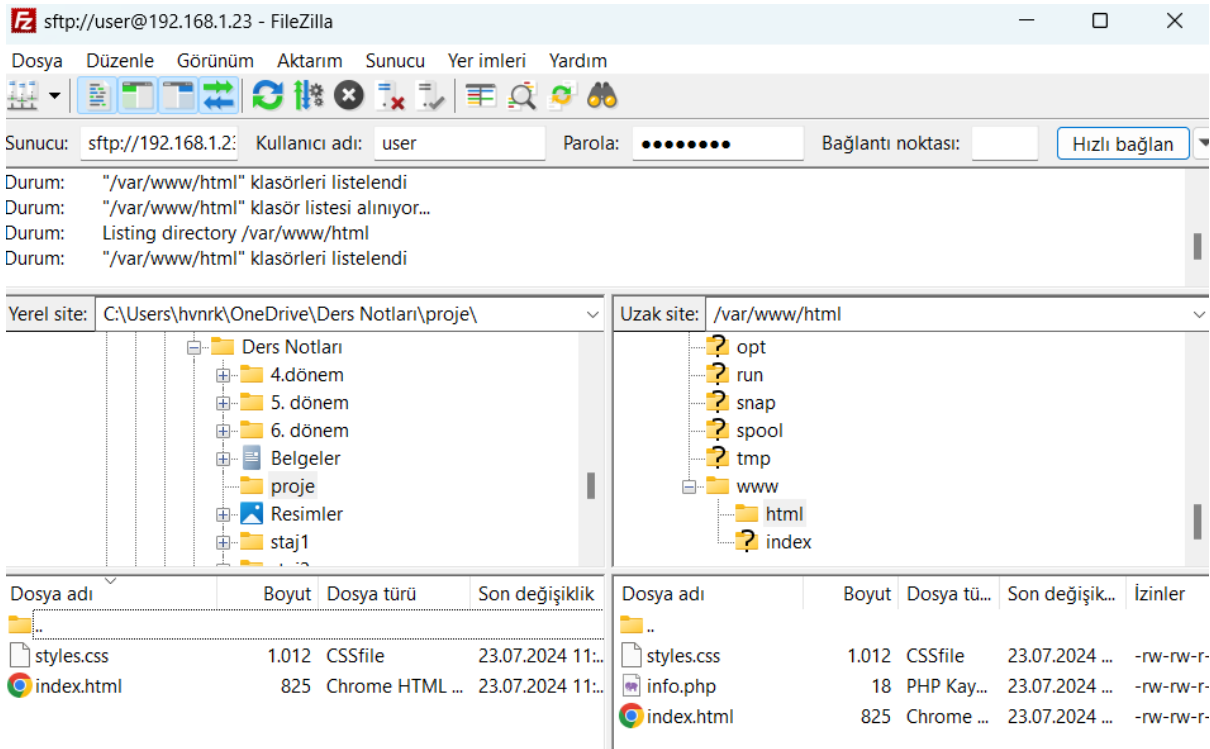
Filezilla kullanmak için öncelikle [Download FileZilla Client for Windows \(64bit x86\) \(filezilla-project.org\)](https://filezilla-project.org) sitesinden Filezilla client indirip kuruyoruz. Daha sonra Filezilla arayüzünden kendi sunucumuza bağlanmak için login bilgilerini giriyoruz.

Sunucu: ip adresi

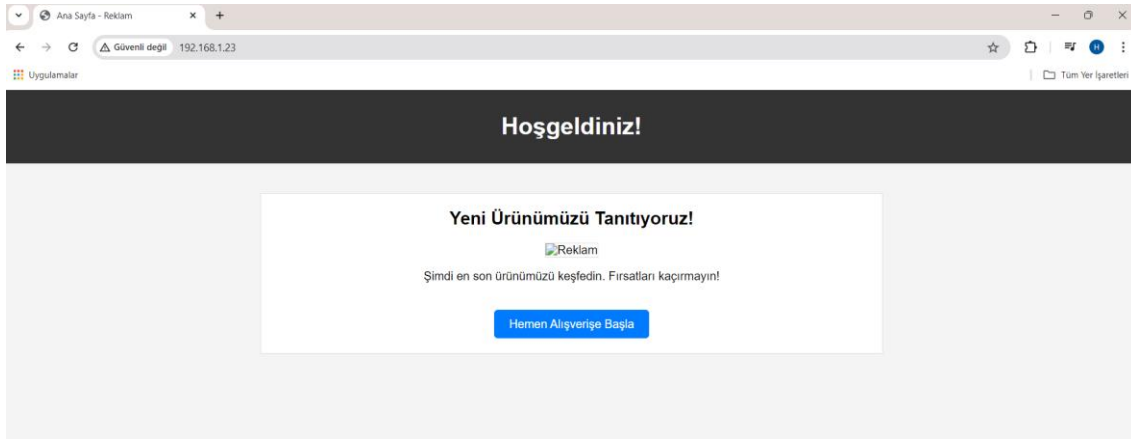
Kullanıcı adı: server username

Parola: server parolası

Bağlantı noktası: 21 veya 22 olarak girebiliriz

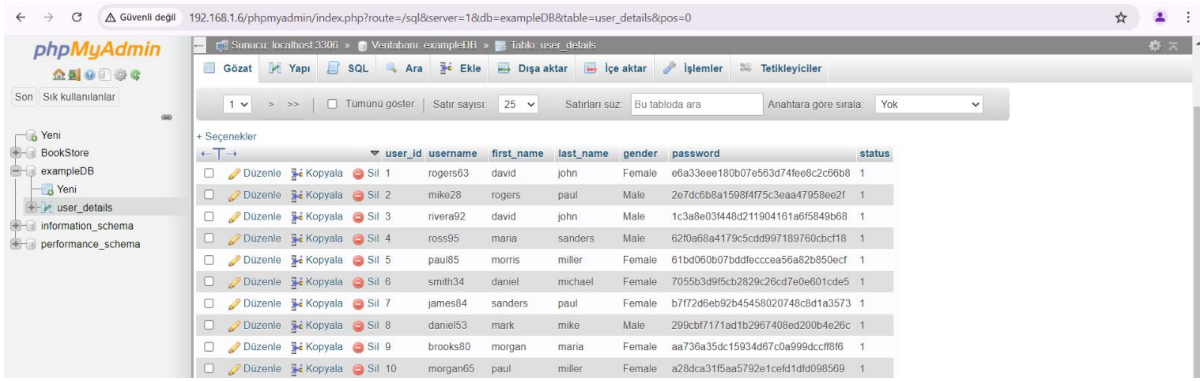


Örneğin /var/www/html dizinine html ve css dosyası aktarmak istiyoruz. Önceden bilgisayarımızda oluşturduğumuz index.html ve styles.css dosyasını sürükleyip bırak veya upload yöntemi ile /var/www/html dizinine yüklüyoruz. Serverda update yaptıktan sonra <https://192.168.1.23> adresine gittiğimizde index.html sayfasını görüntüleyebiliriz.



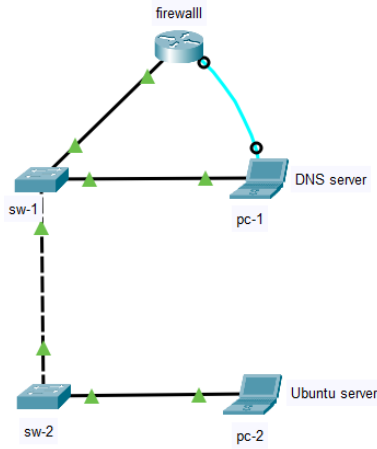
PhpMyAdmin database import etme

Database import etmek için öncelikle bir tane database oluşturuyoruz. Daha sonra sql dosyasını import ediyoruz. Import işlemini yaptıktan sonra verilerin sunucuya yüklendiğini görebiliriz:



İstersek bu databasei serverda bir php ve html sayfasına da bağlayarak web sayfasında görüntüleyebiliriz.

PROJE -2



BAĞLANTI PORTLARI

firewall -pc1: console - usb

firewall-switch1: LAN - 48.port

switch1-switch2: 47.port - 24.port

switch1 - Pc1: 29.port - fastethernet

switch2- Pc2: 9.port - fastethernet

switch1- Pc2: 45.port

1.projedeki kurulu sistemi kullanarak dns ve dhcp kuracağımız ve internete dns aracılığıyla bağlanacağımız bir proje gerçekleştirdik.

PC1, muhasebe VLAN'ına bağlıdır.

DHCP Sunucusu: Muhasebe VLAN'ında IP adresleri dinamik olarak dağıtmak için bir DHCP sunucusu yapılandırılmıştır. DHCP sunucusunun IP adresi 10.1.200.3 olarak belirlenmiştir.

Sunucu VLAN IP Adresi: Sunucu VLAN'ının gateway'i olarak kullanılan IP adresi 10.1.200.1 olarak belirlenmiştir.

PC1de windows server üzerinde dns yapılandırması yapılır.

DNS Ayarları: destek.orcun.com DNS adresi kullanılarak internete çıkış sağlanmaktadır.

Bu cihaz, DNS olarak destek.orcun.com adresini kullanıyor. Bu DNS sunucusu, internete erişim için kullanılan DNS sunucusudur.

Switch1de 45.port sunucu vlanı için ayarlanır ve Pc2ye ethernet kartı aracılığıyla bağlanır.

PC2, bilgi işlem departmanına ait bir bilgisayardır ve bilgi işlem VLAN'ına bağlıdır.

PC2 IP adresi 10.0.10.1/24, bilgi işlem VLAN'ın IP adresine bağlıdır.

Pc2de Ubuntu server, 10.0.10.3 IP adresi ile ağa bağlıdır.

Pc2de fileZilla aracılığıyla Ubuntu servera yüklediğimiz index.html sayfası destek.orcun.com DNS sunucu adresini kullanılarak internete çıkış yapar.

Firewall Interfaces:

Sunucu VLANı için interface oluşturulur.

The image shows the FortiGate 30E configuration interface for editing a new interface named 'sunucu'. The interface is configured as a VLAN with ID 101 and role LAN. The addressing mode is set to Manual with IP/Netmask 10.1.200.1/255.255.255.0. A secondary IP address is not configured. Administrative access is disabled for all protocols. The DHCP Server section is also visible, showing the address range 10.1.200.2-10.1.200.254 and netmask 255.255.255.0.

FortiGate 30E FortiGate-30E

Dashboard > Edit Interface

Security Fabric >

FortiView >

Network >

Interfaces >

DNS

Packet Capture

SD-WAN

SD-WAN Rules

Performance SLA

Static Routes

FortiExtender

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

Name: sunucu

Alias:

Type: VLAN

Interface: lan

VLAN ID: 101

Role: LAN

Address

Addressing mode: Manual DHCP PPPoE

IP/Netmask: 10.1.200.1/255.255.255.0

Create address object matching subnet: ☒

Name: sunucu address

Destination: 10.1.200.1/255.255.255.0

Secondary IP address: ☐

Administrative access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection

OK Cancel

FortiGate 30E FortiGate-30E

Dashboard > Edit Interface

Security Fabric >

FortiView >

Network >

Interfaces >

DNS

Packet Capture

SD-WAN

SD-WAN Rules

DHCP Server

Address range: 10.1.200.2-10.1.200.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP Specify

DNS server: Same as System DNS Same as Interface IP Specify

Lease time: 604800 second(s)

Advanced

Muhasebe VLANında DHCP sunucu ip adresi verilir.

The image shows the FortiGate 30E configuration interface for the DHCP Server. The Mode is set to Relay and the Type is set to Regular. The DHCP Server IP is 10.1.200.3.

FortiGate 30E FortiGate-30E

DHCP Server

Advanced

Mode: Server Relay

Type: Regular IPsec

DHCP Server IP: 10.1.200.3

Bilgiislem vlanı için oluşturulan interfacede dns server açılır. DHCP için belirlenen ip adresi verilir:

DHCP Server

Address range

10.0.10.2-10.0.10.254

Netmask

255.255.255.0

Default gateway

Same as Interface IP

Specify

DNS server

Same as System DNS

Same as Interface IP

Specify

Lease time

604800

second(s)

Advanced

Firewall Policies

Muhasebe VLAN'ından sunucu VLAN'ındaki DHCP servisine erişim izni, muhasebe bölümündeki cihazların IP adreslerini dinamik olarak alabilmesini sağlar.

Muhasebe VLAN'ındaki cihazların Sunucu VLAN'ındaki DHCP sunucusuna erişimini sağlar.

Sunucu VLAN'ındaki DNS servisine erişim izni, bilgiislem VLAN'ındaki cihazların sunucuya bağlanmasını sağlar.

Sunucu_vlan policy: Bu policy, bilgiislem address ve sunucu address arasında geçiş yapan tüm trafiğe izin vermeyi amaçlar. Bu, belirli bir VLAN (sunucu_vlan) üzerinde geçerlidir.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
5	55	all	sunucu address	always	DHCP Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
6		sunucu address	all	always	DHCP Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
4	sunucu_vlan	bilgiislem address	sunucu address	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B