Karamanoğlu Mehmetbey Üniversitesi

Mühendislik Fakültesi

Bilgisayar Mühendisliği Bölümü

FİNAL BİTİRME PROJESİ
(2024-25)

Cisco Pocket Tracer Kullanarak Kampüs Ağı Ve Bina Ağ Tasarımı

Öğrenci Bilgileri	
Öğrenci No	201312039
Öğrenci Ad Soyadı	EBUBEKİR ÖZ

Ders Sorumlusu Unvan, Ad, Soyadı

Doç. Dr. Metin Toz

İÇERİKLER

1.	ÖZET	2
2.	GİRİS	3
3.	Temel Kavramlar	4
4.	Kullanılan Cihazlar ve Sunucular	9
5.	Yazılım ve Donanım Gereksinimi	12
6.	Tasarım ve Çalışmalar	13
7.	Sonuç & Tartışma	40
8.	Sonuçlar ve Gelecekteki Çalışmalar	45
9.	Kaynaklar	46

1.ÖZET

Bilgisayar ağları bir organizasyonun işleyişi üzerinde önemli bir etkiye sahiptir. Üniversiteler eğitim, yönetim, iletişim, e-kütüphane, otomasyon vb. için ağlarının düzgün işleyişine ve analizine bağlıdır. Verimli bir ağ, bir organizasyonda mesajlar, dosyalar ve kaynaklar biçiminde bilgilerin sistematik ve maliyet açısından verimli bir şekilde aktarılmasını kolaylaştırmak için olmazsa olmazdır. Bu proje, bir üniversite kampüsündeki belirli bir binanın ağ altyapısının ayrıntılı bir şekilde tasarlanmasını ve simülasyonunu amaçlamaktadır. Proje kapsamında, topoloji tasarımı, IP adresi yapılandırması, VLAN yapılandırmaları ve kablosuz ağlar aracılığıyla bilgi aktarımı gibi çeşitli ağ bileşenleri ele alınmıştır.

Bu projenin amacı, bir üniversite kampüsünde bir binada kullanılan ağ sistemlerinin Cisco Packet Tracer yazılımını kullanarak üniversite ağının topolojisini tasarlamaktır. Bu üniversite ağı aşağıdaki cihazlardan oluşmaktadır:

1) Router
2) Switches
3) Firewall
4) Email server
5) DNS server
6) Web server (HTTP)
7) DHCP server
8) SYSLOG SERVER
9) Wireless Device (Access Point)
10) PCs
11) Laptops

2.GİRİŞ

Bilgisayar ağları, modern organizasyonların işleyişi için kritik bir rol oynamaktadır. Özellikle eğitim kurumlarında, ağ altyapıları eğitim, iletişim, araştırma ve idari işlemler gibi bir dizi temel faaliyetin düzgün bir şekilde gerçekleştirilebilmesi için büyük öneme sahiptir. Üniversiteler, öğrencilere ve akademik personele kesintisiz ve güvenli bir ağ hizmeti sunabilmek amacıyla güçlü ağ altyapıları tasarlamak zorundadır. Bu altyapıların tasarımı, doğru ağ topolojisinin seçilmesi, IP adresleme, ağ güvenliği ve kablosuz bağlantı gibi unsurları içerir. Bu proje üniversite kampüsünde bulunan bir binanın ağ altyapısını tasarlamak ve ağ yönetiminde kullanılan terimler hakkında bilgi sunmayı amaçlamaktadır.

- **Proje Beyanı**

Bu proje, bir üniversite kampüsündeki belirli bir binanın ağ altyapısının analizi ve yapılandırılmasına odaklanmaktadır. Amacımız, üniversite kampüsündeki ağ altyapısını verimli ve güvenli bir şekilde planlamak, kullanılan ağ cihazları ve terimlerinin işlevselliğini incelemektir. Proje kapsamında yönlendiriciler, anahtarlar ve erişim noktaları gibi temel ağ cihazlarıyla birlikte, merkezi hizmetlerin sağlanabilmesi için sunucular da dahil edilmiştir. IP adresleme, VLAN yapılandırması, kablosuz ağların entegrasyonu ve ağ güvenliği gibi temel konular ele alınacaktır.

Sunucular, ağ üzerinde veri yönetimi, kullanıcı erişimi ve güvenlik sağlamak amacıyla eklenmiştir. Örneğin, dosya sunucuları veri paylaşımını kolaylaştırırken, web sunucuları eğitim materyallerine erişimi sağlar.

Sonuç olarak, bu proje üniversite kampüslerinde ağ altyapısı konusunda bilgi sağlamaktadır.

3.TEMEL KAVRAMLAR

- **Packet Tracer Nedir?**

Packet Tracer, Cisco Systems tarafından tasarlanan ve kullanıcıların ağ topolojileri oluşturmasına ve modern bilgisayar ağlarını taklit etmesine olanak tanıyan çapraz platformlu bir görsel simülasyon aracıdır. Yazılım, kullanıcıların simüle edilmiş bir komut satırı arayüzü kullanarak Cisco yönlendiricilerinin ve anahtarlarının yapılandırmasını simüle etmelerine olanak tanır. Packet Tracer, kullanıcıların uygun gördükleri şekilde simüle edilmiş ağ cihazlarını eklemelerine ve kaldırmalarına olanak tanıyan sürükle ve bırak kullanıcı arayüzünü kullanır. Yazılım, temel CCNA kavramlarını öğrenmelerine yardımcı olmak için bir eğitim aracı olarak esas olarak Certified Cisco Network Associate Academy öğrencilerine odaklanmıştır. Daha önce CCNA Academy programına kayıtlı öğrenciler, aracı eğitim amaçlı olarak ücretsiz olarak indirip kullanabilirlerdi [1].

- **İnternet Nedir?**

  İnternet bütün dünyada kullanılan, bilgisayar ve diğer akıllı cihazlar aracılığıyla veri ve bilgi iletmeyi/almayı sağlayan iletişim ağıdır. İnternet aracılığıyla istenilen web sitesine ve bilgiye erişim sağlanabilir.

- **Network Packet**

  Ağ paketi, paket anahtarlamalı bir ağ tarafından taşınan biçimlendirilmiş bir veri birimidir. Bir paket, kontrol bilgileri ve kullanıcı verilerinden oluşur; bu kullanıcı verileri aynı zamanda yük olarak da bilinir [7].

- **Wireless Network**

Bir kablosuz ağ, iş istasyonlarına veya bilgisayarlara erişim sinyali yayar. Bu, dizüstü bilgisayarlar, tabletler ve bilgisayarlar arasında odadan odaya geçiş yaparken sürekli ve sağlam bir ağ bağlantısının korunmasını sağlar. Kablosuz ağ ayrıca ek güvenlik gereksinimlerini de beraberinde getirir [7].

- **Ağ (Network) Nedir?**

Ağ, iki veya daha fazla cihazın veri alışveriş amacıyla birbirine bağlandığı yapıdır. **Ağ**, internet tarayıcılığı, dosya paylaşımı, kurumsal altyapılar ve iletişim ağları gibi birçok alanda modern iletişimin temelini oluşturur. Bağlantılar, kablolu ya da kablosuz olabilir.

Veri aktarımı ise belirli protokoller aracılığıyla gerçekleştirir. Buna en iyi örnek İnternet verilebilir.

- **Network Türleri**

Local Area Network (LAN):

Local Area Network (LAN), küçük bir alanı kapsayan ağ türüdür. Ev, okul veya ofis gibi küçük bir bölge ile sınırlıdır. LAN, cihazların dosya paylaşımını ve yazıcı gibi kaynakları kullanmalarını sağlar. Kablolu LAN'lar Ethernet kablolarıyla çalışırken, kablosuz LAN'lar (Wi-Fi) radyo sinyallerini kullanır[11].

Wide Area Network (WAN):

Wide Area Network (WAN), geniş bir coğrafi alanı kapsar. İnternet, dünya çapında milyonlarca cihazı birbirine bağlayan en büyük WAN örneğidir. WAN, yüksek hızlı bağlantılarla büyük veri transferi sağlar[11].

Metropolitan Area Network (MAN):

Metropolitan Area Network (MAN), bir şehir veya büyük bir kampüsü kapsayan bir network türüdür. Örneğin, üniversite kampüsündeki binalar arasındaki veri aktarımını sağlayan MAN, bu tür bir ağdır[11].

Personal Area Network (PAN):

Personal Area Network (PAN), kişisel cihazlar arasında kısa mesafede bağlantı sağlayan bir network türüdür. Örneğin, telefon ile kablosuz kulaklık arasındaki Bluetooth bağlantısı bir PAN örneğidir[11].

- **IP Adresleme ve Sınıflandırma**

  IP Adresi Nedir?

  IP adresi, internet protokolü kullanılarak cihazları birbirine bağlayan, her cihazın ağ üzerindeki kimliğini belirleyen sayısal bir etikettir.

  IP adresi, iki ana versiyonla bulunur:

  IPv4: 32 bit uzunluğunda olup, dört 8 bitlik sayıdan oluşur (örneğin: 192.168.1.1). IPv4, halen en yaygın kullanılan IP adresleme sistemidir.

  IPv6: 128 bit uzunluğunda olup, daha geniş bir adresleme kapasitesine sahip olarak gelecekteki ağ ihtiyaçlarına yanıt vermek için tasarlanmıştır.

  IP Adresi Sınıflandırma (IPv4):

  Sinif A, **Sinif B**, **Sinif C**, **Sinif D** ve **Sinif E** olmak üzere beş farklı IP sınıfı vardır. Her sınıfın belirli bir adres aralığı ve kullanımı vardır.

  - **Sinif A** (1.0.0.0 - 127.255.255.255): Çok büyük ağlar için ayrılmıştır. 1.0.0.0 ile 127.255.255.255 arasındaki adresler bu sınıfı oluşturur. Büyük kurumsal ağlar için kullanılır.
  - **Sinif B** (128.0.0.0 - 191.255.255.255): Orta büyüklükteki ağlar için ayrılmıştır. Bu sınıf genellikle orta ölçekli işletmeler tarafından tercih edilir.
  - **Sinif C** (192.0.0.0 - 223.255.255.255): Küçük ağlar için ayrılmıştır. Çoğu yerel ağ (LAN) ve ev ağları bu sınıfa girer.

- **Sinif D** (224.0.0.0 - 239.255.255.255): Multicast adresleri için ayrılmıştır, yani birden fazla cihazla veri paylaşımı yapabilmek için kullanılır.
- **Sinif E** (240.0.0.0 - 255.255.255.255): Gelecekteki kullanımlar ve deneysel adresler için ayrılmıştır.

Özel IP Adres Araliklari (Private IP Adresleri)

Private IP adresleri yerel ağlarda kullanılır ve internet üzerinde doğrudan erişilebilir değildir. IPv4 adresleri için özel aralıklar:

- **10.0.0.0 - 10.255.255.255** (Sınıf A)
- **172.16.0.0 - 172.31.255.255** (Sınıf B)
- **192.168.0.0 - 192.168.255.255** (Sınıf C)

Bu özel adresler, şirket içi ağlar, yerel ağlar (LAN) ve ev ağlarında sıkça kullanılır[9].

- **Ağ Yapılandırma ve Yönetim**

Ağ Yapılandırma (Network Configuration)

Ağ yapılandırması, ağın düzgün çalışabilmesi için cihazların doğru şekilde ayarlanması ve ağın kurulumunun yapılması anlamına gelir. Ağ yapılandırması şu alanları kapsar:

IP Adresleme ve Subnetting (Alt Ağlara Bölme)

- IP adresleme, ağdaki her cihazın benzersiz bir şekilde tanımlanması için gereklidir. IP adres planlaması yapılırken, özel IP adres aralıkları kullanılarak alt ağlar oluşturulabilir.
- Subnetting, büyük bir ağın küçük alt ağlara bölünmesidir. Alt ağlar, ağın daha verimli kullanılmasını sağlar ve yönetimi kolaylaştırır.
- Subnet Mask (Alt Ağ Maskesi) kullanılarak, ağın hangi kısmının ağ adresi, hangi kısmının ise cihaz adresi olduğu belirlenir[9].

VLAN Yapılandırması (Virtual Local Area Network)

VLAN, aynı fiziksel ağ altyapısı üzerinde, farklı sanal ağlar oluşturulmasına olanak tanır. VLAN'lar, ağın bölünmesine ve yönetilmesine yardımcı olur.

VLAN yapılandırması sayesinde, farklı departmanlar veya bölümler için ayrılmış sanal ağlar oluşturulabilir. Bu, ağ trafiğini düzenlemeye ve güvenliği artırmaya yardımcı olur[10].

Ağ Yönetimi (Network Management)

Ağ yönetimi, ağın düzgün çalışmasını sağlamak için sürekli izleme, bakım ve yönetim işlemlerini içerir. Ağın yönetilmesi, çeşitli yönetim protokollerini ve araçlarını kullanmayı gerektirir. Ağ cihazlarından bir sonraki maddede bahsedeceğim.

Burada bahsedeceğim iki maddeden bahsedeceğim.

Ağ İzleme ve Performans Yönetimi

SNMP (Simple Network Management Protocol): Ağ cihazlarının izlenmesi ve yönetilmesi için kullanılan bir protokoldür. SNMP, ağdaki cihazların sağlık durumunu ve performansını izlemeye olanak tanır.

Ağ İzleme Araçlari: Ağın verimli çalışmasını sağlamak için ağ performansı izlenir. Örneğin, Wireshark gibi araçlarla ağ trafiği analiz edilebilir ve ağda tıkanıklık veya diğer sorunlar tespit edilebilir.

Bant Genişliği Yönetimi: Ağ trafiği ve bant genişliği kullanımı izlenir, gerekirse trafiği yönetmek için QoS (Quality of Service) protokolleri kullanılır.

Ağ Trafiği Yönetimi ve Optimizasyonu

QoS (Quality of Service): Ağ trafiğini yönetmek için kullanılan bir tekniktir. QoS, yüksek öncelikli veri akışlarının daha iyi performans göstermesini sağlar. Özellikle video konferans veya VoIP gibi zaman duyarlı uygulamalarda QoS kullanımı önemlidir.

Tikaniklik Yönetimi: Ağda tıkanıklık veya düşük hızlar gibi sorunlar oluştuğunda, ağ trafiği izlenir ve iyileştirme adımları atılır.

4.Kullanılan Cihazlar ve Sunucular

- **ROUTER**

  Yönlendiriciler, farklı ağlar arasında veri iletimi yapar. Yönlendiricilerin doğru yapılandırılması, ağlar arasındaki bağlantıların düzgün çalışmasını sağlar[2].

- **SWİTCHES**

  Switch'ler, cihazlar arasında veri iletimini sağlamak için kullanılır. Anahtarların yapılandırılması, ağın hızını ve verimliliğini etkiler. OSI modelinin veri bağlantı katmanında (katman 2) verileri iletmek için MAC adreslerini kullanan çok portlu bir ağ köprüsüdür. Bazı anahtarlar, yönlendirme işlevselliğini ek olarak dahil ederek ağ katmanında (katman 3) da veri iletebilir. Bu tür anahtarlar genellikle katman-3 anahtarları veya çok katmanlı anahtarlar olarak bilinir[3].

- **FİREWALL**

  Firewall, bir kuruluşun daha önce oluşturulmuş güvenlik politikalarına göre gelen ve giden ağ trafiğini izleyen ve filtreleyen bir ağ güvenlik aygıtıdır . En temel haliyle, bir güvenlik duvarı esasen özel bir dahili ağ ile genel İnternet arasında bulunan bariyerdir[4].

- **DNS Server**

  DNS (Domain Name System) sunucusu, internetin ya da özel ağların üzerinde bulunan alan adlarını (domain) IP adreslerine dönüştüren bir sistemdir.

  Kullanıcılar genellikle alan adlarını (örneğin, www.ornek.com) hatırlarken, bilgisayarlar ve diğer ağ cihazları IP adreslerini (örneğin, 192.168.1.1) kullanır. DNS sunucuları, bu iki sistem arasındaki köprü işlevini görerek, kullanıcıların alan adlarını yazdıklarında ilgili IP adresine ulaşmalarını sağlar[7].

- **EMAİL Server**

  E-posta sunucusu, standart e-posta protokollerini kullanarak bir ağ üzerinden e-postayı işleyen ve ileten bir sunucudur. Örneğin, SMTP protokolü iletileri gönderir ve giden posta isteklerini işler. POP3 protokolü iletileri alır ve gelen postayı işlemek için kullanılır. Bir web postası arayüzü veya e-posta istemcisi kullanarak bir posta sunucusunda oturum açtığınızda, bu protokoller sahne arkasındaki tüm bağlantıları işler[7].

- **WEB Server**

  Günümüz pazarında yaygın olarak kullanılan sunuculardan biri web sunucusudur. Web sunucusu, kullanıcılar tarafından İnternet veya intranet üzerinden talep edilen programları ve verileri barındıran özel bir uygulama sunucusu türüdür. Web sunucuları, istemci bilgisayarlarda çalışan tarayıcılardan gelen web sayfaları veya diğer web tabanlı hizmetlere yönelik taleplere yanıt verir[7].

- **DHCP Server**

  DHCP Sunucusu, ağdaki cihazlara IP adreslerini ve diğer ağ konfigürasyon bilgilerini otomatik olarak dağıtarak, ağ yönetimini daha verimli hale getirir. Özellikle büyük ağlarda, her cihaza manuel olarak IP ataması yapmak yerine DHCP kullanmak, yönetimi kolaylaştırır ve ağ bağlantılarının daha hızlı kurulmasını sağlar. Bu protokol, ağdaki cihazların doğru yapılandırılmasını sağlarken, ağ yöneticilerine IP adres yönetiminde büyük bir kolaylık sunar[8].

- **FTP Server**

  FTP sunucusu, dosyaların ağ üzerinden güvenli bir şekilde aktarılması ve paylaşılması için kritik bir araçtır. Kullanıcıların dosya yükleme ve indirme işlemlerini gerçekleştirebileceği merkezi bir platform sağlar. FTP sunucusunun doğru yapılandırılması, ağdaki dosya transferlerini daha güvenli ve verimli hale getirir. Güvenlik önlemleri, şifreli bağlantılar ve kullanıcı erişim izinleri, sunucunun güvenli çalışmasını sağlamak için önemlidir.

- **Wireless Device (Access Point)**

  Kablosuz ağların yapılandırılması, öğrenciler ve öğretmenler için internete kablosuz erişim sağlar. Erişim noktalarının doğru konfigürasyonu, kapsama alanı ve sinyal gücü açısından önemlidir.

- **INTERNET PROTOCOL**

  İnternet Protokolü (IP), internetin çalışmasını sağlayan temel protokollerden biridir. IP adresleri, her ağdaki benzersiz bir sayı kümesidir ve makinelerin bir ağ üzerinden birbirlerine adres vermesini sağlar. IP/TCP modelinde internet katmanında uygulanır[5].

- **SSH PROTOCOL**

  Secure Shell, bir kullanıcının uzak bir cihaza erişmesini ve onu uzaktan yönetmesini sağlar. Ancak SSH ile bir ağ üzerinden iletilen tüm veriler (kullanıcı adları ve parolalar dahil) şifrelenir ve gizlice dinlenmeye karşı güvenlidir.

  SSH, bir SSH istemcisi ve bir SSH sunucusu olan bir istemci-sunucu protokolüdür. İstemci makinesi (örneğin bir PC) uzak bir cihazda (örneğin bir yönlendirici) çalışan bir SSH sunucusuna bağlantı kurar. Bağlantı kurulduktan sonra, bir ağ yöneticisi uzak cihazda komutları yürütebilir[6].

- **Simülasyon Ortamı**

  Ağ topolojimizin simülasyonları cisco packet tracer kullanılarak kolayca gerçekleştirilebilir. Bir simülasyon modu kullanarak, paketlerin bir düğümden diğerine aktığını görebilir ve ayrıca ağın OSI katmanları hakkında ayrıntılı bilgi görmek için bir pakete tıklayabilirsiniz. Packet Tracer, gerçekçi simülasyonu birleştirmek ve bunları aynı anda görselleştirmek için büyük bir platform sunar. Cisco Packet Tracer, çok kullanıcılı işbirliğini destekleyerek ve projelerle denemeler yapmak için gerçekçi bir simülasyon ortamı sağlayarak öğrenmeyi ve öğretmeyi önemli ölçüde kolaylaştırır.

5.Yazılım Ve Donanım Gereksinimleri

1. **Donanim Gereksinimleri**

   - **İşlemci (CPU):** Intel Core i5 veya üstü
   - **RAM:** En az 8 GB RAM (daha iyi performans için 16 GB önerilir)
   - **Depolama Alani:** 256 GB SSD veya HDD (Proje dosyalarının ve simülasyon yazılımlarının saklanması için)
   - **Ekran Çözünürlüğü:** 1366 x 768 veya üzeri
   - **Ağ Karti:** Ethernet veya kablosuz bağlantı destekli ağ kartı

2. **Yazilim Gereksinimleri**

   - **Cisco Packet Tracer:** Ağ tasarımı ve simülasyonları için kullanılan temel yazılım. Packet Tracer, ağ bileşenlerinin simülasyonunu yaparak, farklı ağ topolojilerinin ve ayarlarının test edilmesine olanak sağlar.
   - **İşletim Sistemi:** Windows 10 veya üstü, macOS veya Linux (Packet Tracer ve diğer ağ araçlarının uyumlu çalıştığı bir işletim sistemi

6.TASARIM VE ÇALIŞMALAR

Network Bilgisi

Ağ 1 alandan olusmaktadır:

1. Kampüs Alanı
Kampüs alanı ayrıca Fakülteler, BT ve sunucuların bulunduğu merkez gibi çeşitli erişim noktalarına ayrılmıştır.

Ağda Kullanılan Cihazlar

Devices	Quantity
ROUTER (ISR4321)	2
FIREWALL	1
MULTİ-SWİTCH (3650-24PS)	6
L2 SWITCHS	8
WIRELESS DEVİCE (Access Point)	4
WLC	1
SERVERS	9
PCs	10
IP Phone, Printer	3
Laptops	3
Tablets	3
Smartphone	3

Figure: Ağda kullanılan cihazlar

UYGULAMA

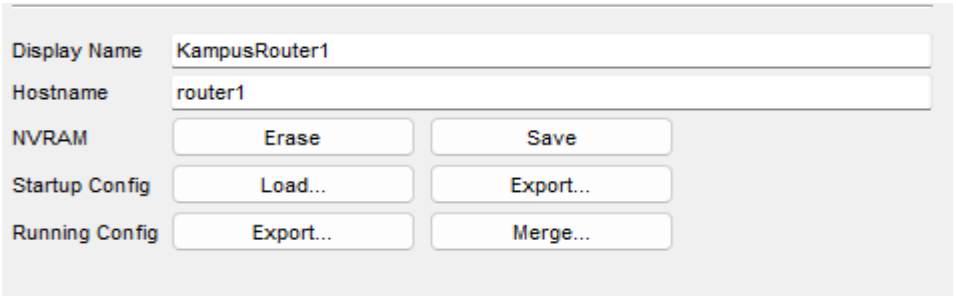
Üniversitenin kablosuz ağını tasarlamak için başlangıçta, düzende belirtildiği gibi çekirdek cihazları çerçeveye yerleştirerek başladık.

- Öncelikle, ana yönlendiriciyi üniversite taslağının merkezine yerleştirdik. Bu Gigabit ethernet portu kullanılarak firewall(güvenlik duvarı) cihazına bağladık ve serial DCE kablosuyla seri portu kullanarak dış ağa çıkan yönlendirici cihazlarına bağlantı kurarak dış ağa bağlandık.
- Yönlendiriciye bağladığımız Firewall cihazındaki gigabit ethernet portlarını kullanarak bir tanesini DEMILIRITIZED ZONE adında bir alana bağlantı kuruldu ve diğer portlar ise ağımızın dağıtım katmanı olarak belirlediğimiz Multi-Switch cihazlara bağlantı kuruldu.
- DEMILIRITIZED ZONE alanında 2 DHCP , 2 DNS , EMAIL , WEB sunucuları kuruldu.
- Multi-Switch ’e L2 Switch bağlanarak sunucular kuruldu.
- Bu sunucularda sırasıyla SYSLOG , DHCP, DNS, WEB , FTP sunucuları kuruldu.
- Multi-Switch e LAP-PT kuruldu.
- Dağıtım katmanına yerleştirdiğimiz 4 Multi-Switch ‘den birine WLC kuruldu.
- 2 adet Multi-Switch ’e fiber kablo bağlanarak Kampüste bulunan Fakültelerden ilkine bağlantı kuruldu. Mühendislik fakültesine 2 adet Multi-Switch bağlayarak fiber kablo ile bağlantı kuruldu.
- Fakülteyi 3 kata ayıralım.
- Her katta 2 adet L2 Switch koyduk.
- Her L2 Switch ’i Multi-Switch ’e bağladık.
- L2 Switch ‘e IP Phone, PC, Printer , LAP-PT(Access Point) bağladık.
- Kablosuz erişim noktaları daha sonra bilgi işlem cihazlarına bağlandı
- (PC'ler, dizüstü bilgisayarlar ve akıllı telefonlar), her alanın yalnızca bir parola yardımıyla bağlanabilen özel bir erişim noktası var.
- Tüm bu bağlantılar bakır düz kablolar kullanılarak ethernet portları (gigabit ethernet ve hızlı ethernet) aracılığıyla yapılır.

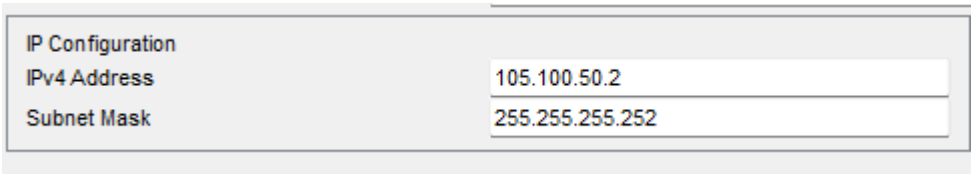
Configuring IP Addresses

Tüm IP yapılandırmasının ekran görüntülerini aşağıya ekledik:

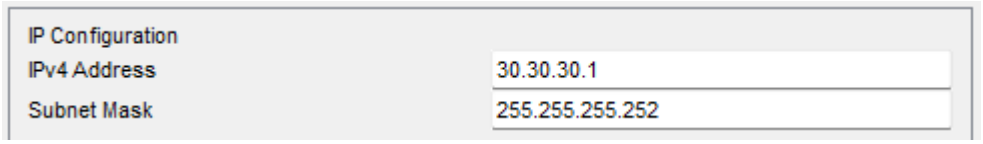
Router 1 configuration



GigabitEthernet0/0/0



Serial0/1/0

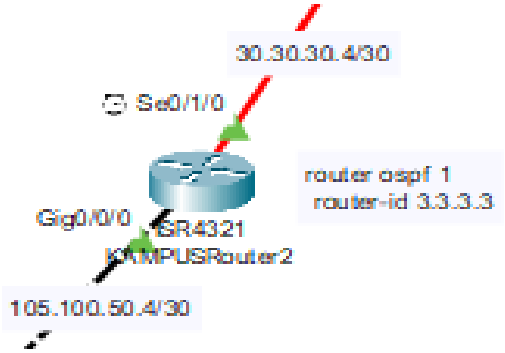


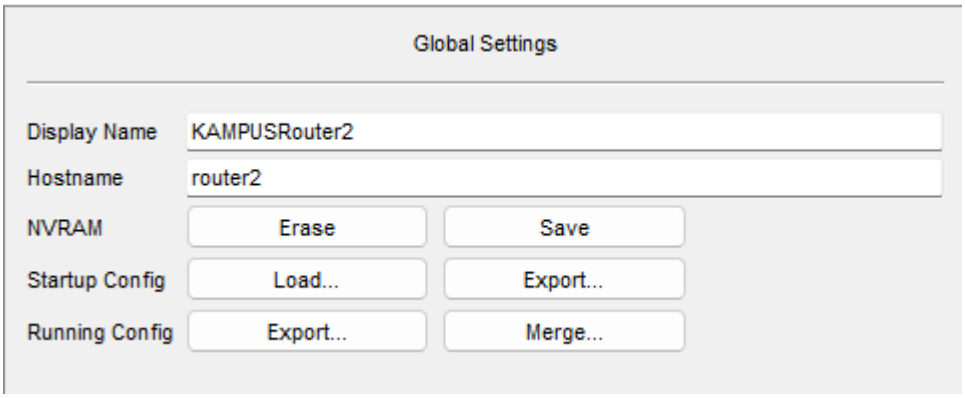
OSPF Nedir?

OSPF, bir TCP/IP ağındaki router'ların birbirini otomatik olarak tanımasında kullanılan bir protokoldür. OSPF yönlendirme internette intra-AS yönlendirme için RIP gibi yaygınca kullanılan bir yöntemdir. OSPF temelde internet servis sağlayıcılarının (ISP) üst-tabakalarında kullanılır. OSPF kelimesindeki ilk O harfi yönlendirme protokolü şartlarının açık olduğunu gösterir (örnek olarak, Cisco'nun EIGRP protokolünün karşıtı gibi). OSPF'nin en güncel versiyonu ikincisidir.

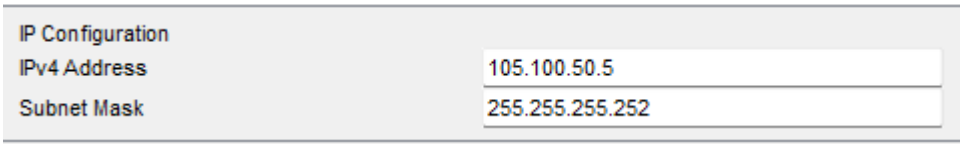
```
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 105.100.50.0 0.0.0.3 area 0
 network 30.30.30.0 0.0.0.3 area 0
 network 105.100.50.4 0.0.0.3 area 0
```

Router 2 configuration

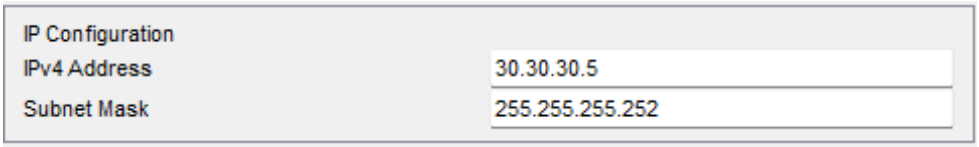




GigabitEthernet0/0/0



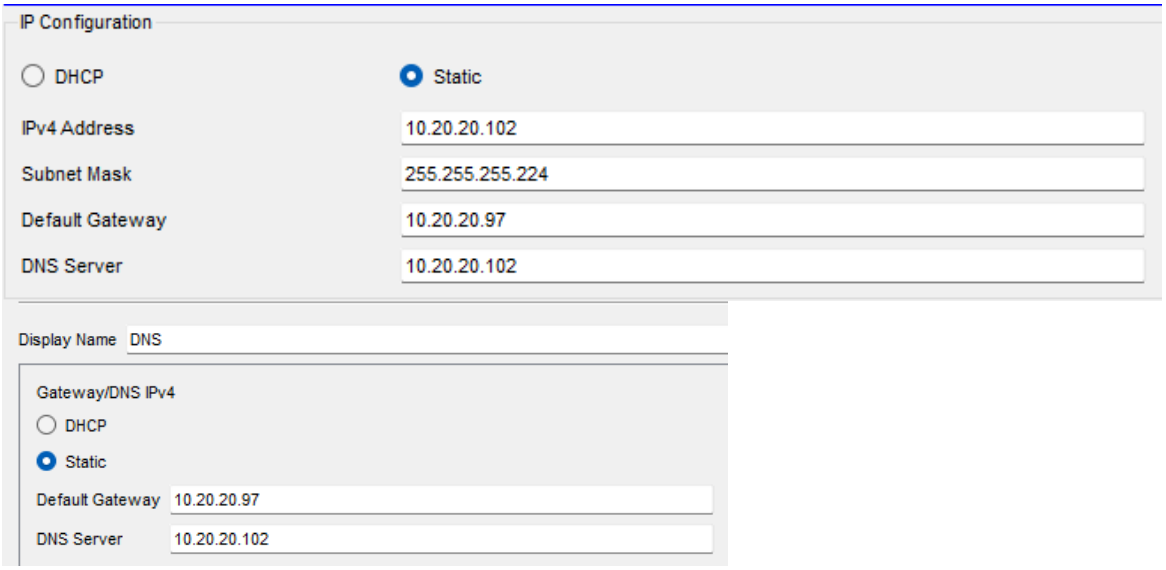
Serial0/1/0



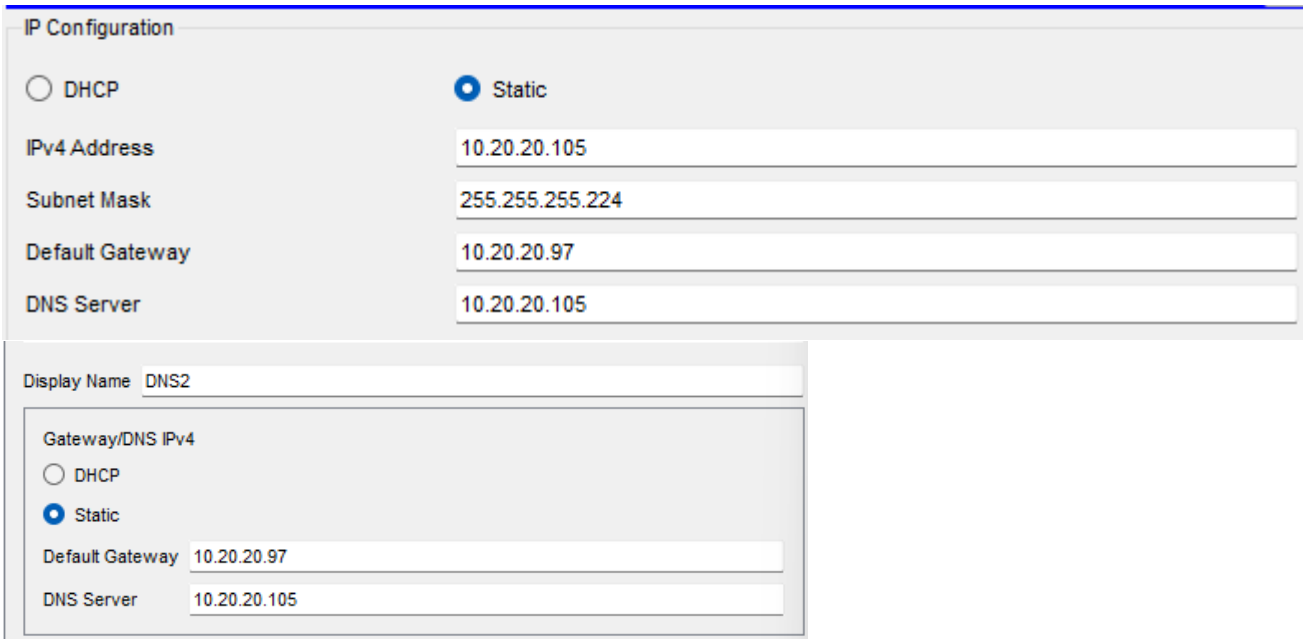
OSPF

```
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 105.100.50.4 0.0.0.3 area 0
 network 30.30.30.4 0.0.0.3 area 0
 network 105.100.50.0 0.0.0.3 area 0
!
```

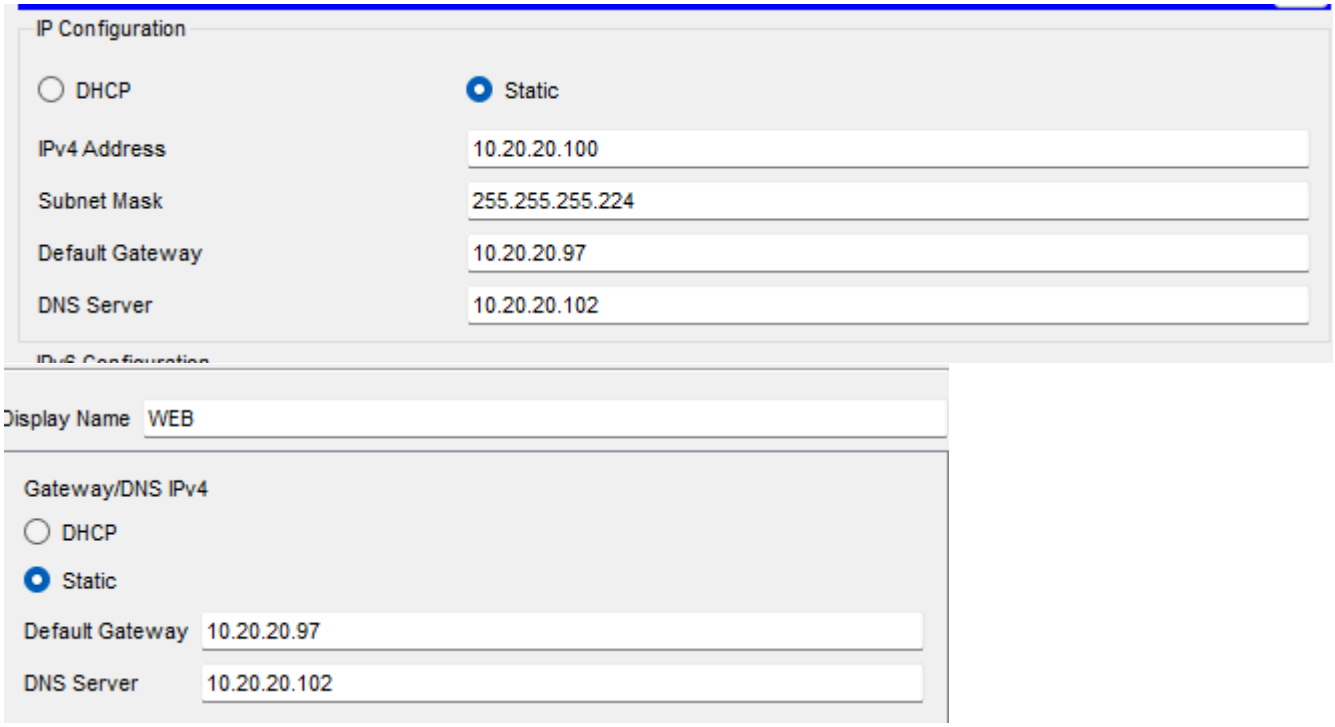
DMZ DNS SERVER 1



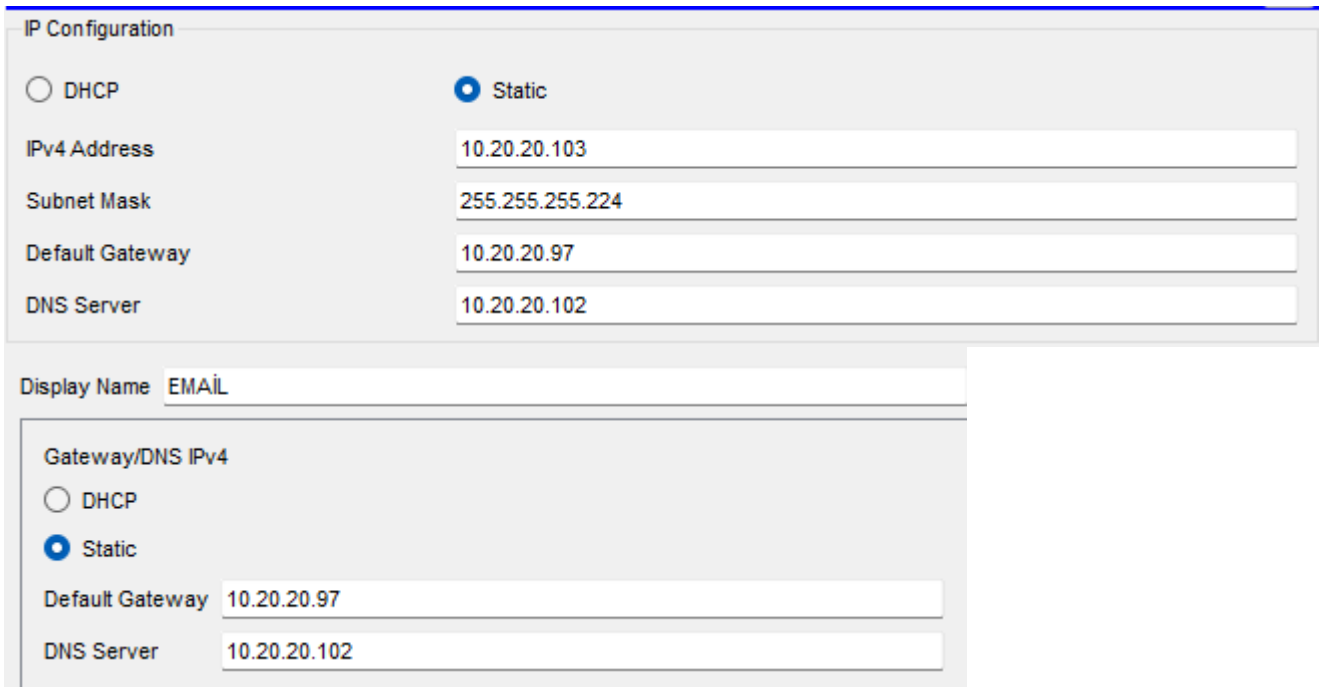
DMZ DNS SERVER 2



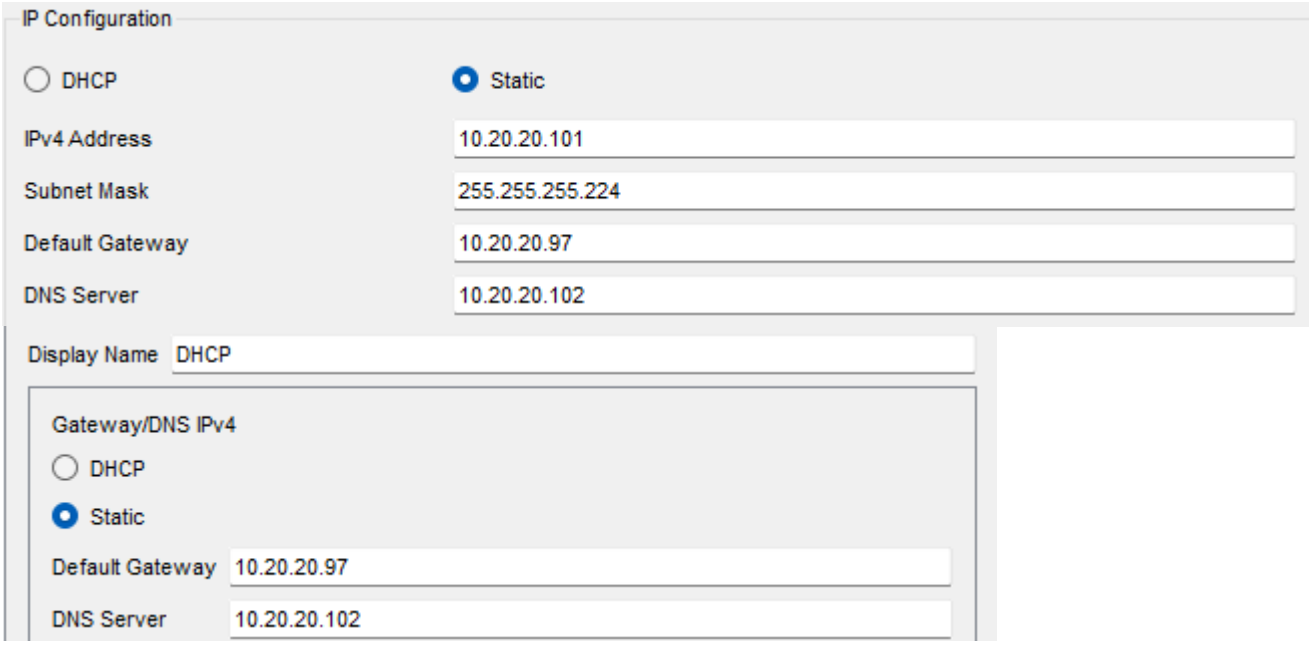
DMZ WEB SERVER



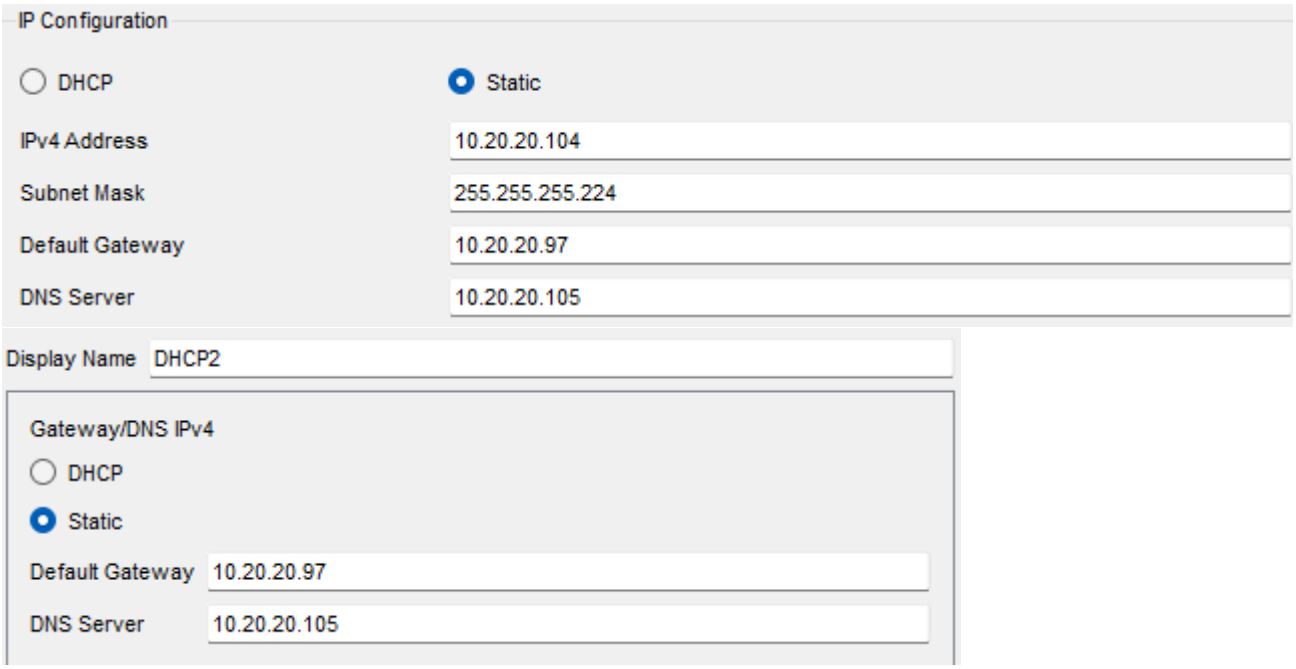
EMAIL SERVER



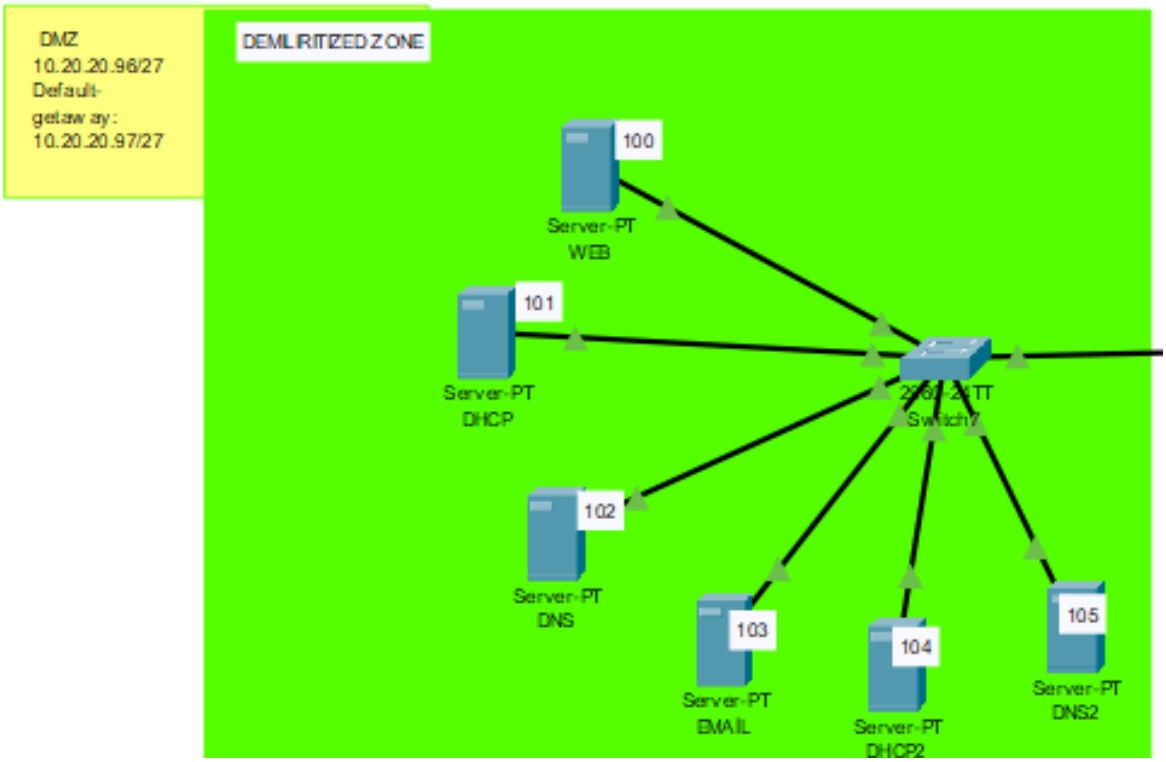
DMZ DHCP SERVER 1



DMZ DHCP SERVER 2



DEMILIRITIZED ZONE



En basit tanımı ile fiziksel ya da mantıksal olarak sadece dış dünya ile irtibatta olan sunucuların iç ağlarınızdan ayrılıp farklı bir ağda konumlandırılmasıdır. Ayrılma noktası güvenlik duvarları (Firewall 'lar) olduğu gibi router 'lar olabilir.

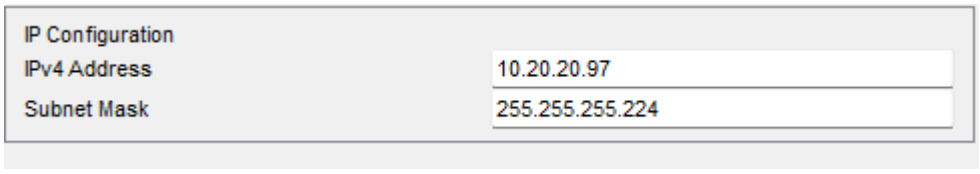
DMZ ağlarında amaç nedir?

DMZ ağlarında konumlandırılan ve sadece dış dünya ile iletişimi olan temelde web, mail, DNS ve (eğer hala kaldıysa) FTP sunucuların dış ağ kaynaklı saldırganlar tarafından ele geçirilmesi durumunda kritik verilerin olduğu ağ segmentlerine geçmesini engellemektir.

DMZ ağları için en temel ve neredeyse tek prensip DMZ 'de bulunan sunucuların asla hiç bir ağ ile mantıksal iletişiminin **olmamasıdır.**

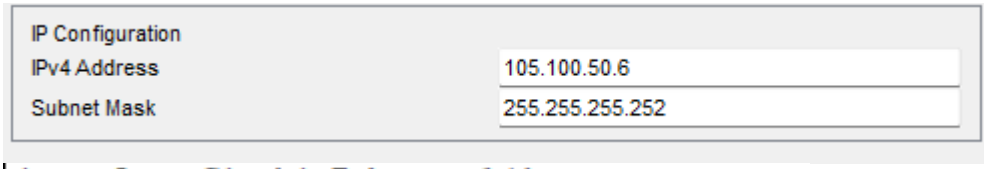
FIREWALL Configuration

DMZ GigabitEthernet1/5



```
interface GigabitEthernet1/5
 nameif DMZ
 security-level 70
 ip address 10.20.20.97 255.255.255.224
!
```

Router 2 GigabitEthernet1/4

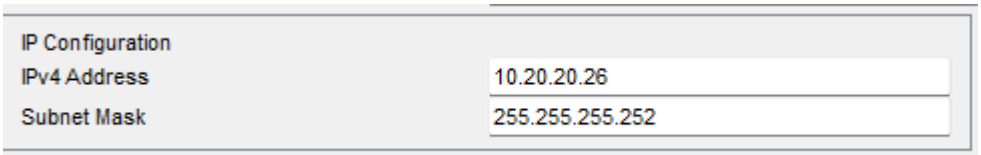



```
interface GigabitEthernet1/4
 nameif outside2
 security-level 0
 ip address 105.100.50.6 255.255.255.252
!
```

Router 1 GigabitEthernet1/3

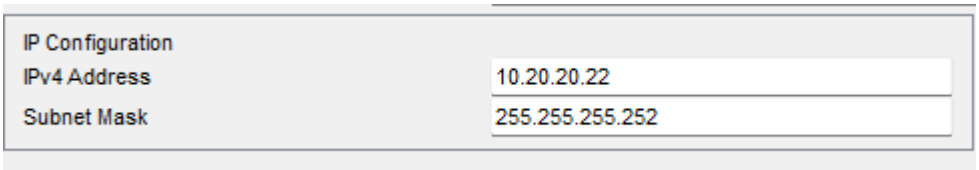

```
interface GigabitEthernet1/3
 nameif outside1
 security-level 0
 ip address 105.100.50.1 255.255.255.252
!
```

Multi-Switch 1 GigabitEthernet1/2




```
!
interface GigabitEthernet1/2
 nameif inside2
 security-level 100
 ip address 10.20.20.26 255.255.255.252
!
```

Multi-Switch 2 GigabitEthernet1/1



```
interface GigabitEthernet1/1
 nameif inside1
 security-level 100
 ip address 10.20.20.22 255.255.255.252
!
```

OSPF

```
!
router ospf 15
 router-id 3.2.4.1
 log-adjacency-changes
 network 105.100.50.0 255.255.255.252 area 0
 network 10.20.20.20 255.255.255.252 area 0
 network 10.20.20.24 255.255.255.252 area 0
 network 105.100.50.4 255.255.255.252 area 0
 network 10.20.20.96 255.255.255.224 area 0
!
```

ROUTER 1 VE 2 de HSRP Configuration

HSRP Nedir?

Cisco tarafından geliştirilen ve Cisco'ya özel olan HSRP (Hot Standby Router Protocol) protokolü, router yedeklilik için geliştirilmiş olan bir protokoldür . Birden fazla routerın tek bir router gibi davranmasını sağlar. Bunun için de sanal IP adresi oluşturulur ve bu sanal IP gateway olarak işlev görür. Routerlardan bir tanesi active(ana) router seçilir ve diğeri standby(yedek) olarak seçilir. Trafik active router üzerinden geçer ve active routera bir şey olması durumunda standby router devreye girer. Böylece trafik akışı minimal düzeyde kesintiye uğrayarak devam eder.

Routerlar arasında 3 saniyede bir 'hello' mesajları gönderilir. 10 saniye boyunca active router'dan cevap gelmemesi durumunda standby router görevi üstlenir ve active router olarak işlev yapmaya başlar. HSRP active router seçimi priority (öncelik) değerine göre belirlenir. Priority değeri yüksek olan router, active router seçilir. Priority değerinin aynı olması durumunda ise, yüksek IP adresine sahip olan router, active router olarak seçilir.

1) Router 1 de firewall'a bağlı olan portu seçiyoruz.

```
interface GigabitEthernet0/0/0
 description Connection to Firewall (Outside1)
 ip address 105.100.50.2 255.255.255.252
 duplex auto
 speed auto
 standby 1 ip 105.100.50.3
 standby 1 priority 110
 standby 1 preempt
 standby 1 track GigabitEthernet0/0/0
!
```

2) Router 2 de firewall'a bağlı portu seçiyoruz.

```
interface GigabitEthernet0/0/0
 description Connection to Firewall (Outside2)
 ip address 105.100.50.5 255.255.255.252
 duplex auto
 speed auto
 standby 1 ip 105.100.50.3
 standby 1 priority 50
 standby 1 preempt
 standby 1 track GigabitEthernet0/0/0
!
```

105.100.50.3 bizim virtual ip adresimiz eğer HSRP'miz çalışmasını istiyorsak firewallda rota oluşturmalıyız.

```
!
route outside1 0.0.0.0 0.0.0.0 105.100.50.3 1
route outside2 0.0.0.0 0.0.0.0 105.100.50.3 2
!
```

Static rotaların sonundaki sayılar (1,2) öncelik değerini temsil ediyor.

Firewall da Gig1/1 , Gig1/2 portları inside1 ve inside2 olarak isimlendiriyoruz. Çünkü bu portlar iç ağımıza bağlanıyor. Gig1/4 ve Gig1/3 portlarımızda outside1 ve outside2 olarak isimlendiriyoruz. Bu portlarda dış ağımıza bağlanıyor. Peki neden böyle isimlendirdik?

Bu isimlendirme, ağ güvenliği, yönetim kolaylığı ve trafik akışının daha iyi anlaşılması açısından oldukça önemlidir. Inside ve Outside portlar arasında net bir ayrım yaparak, güvenlik politikalarını uygulamak ve trafik akışını kontrol etmek daha verimli hale gelir.

Multi-Switch Configuration

1) ITMSW

Bu bizim ana switchimiz. Bu switchde VTP yapılandırması yaparak bu switch'i vtp modunu server olarak seçtik. Bunun sayesinde tek bir switchden vlan oluştururken diğer switchlerde de oluşmus olacak.

VTP Yapılandırması

VTP Nedir?

VTP (VLAN Trunking Protocol), Cisco cihazlarında VLAN yapılandırmalarının merkezi bir şekilde yönetilmesini sağlayan bir protokoldür. VTP, bir ağda birden fazla switch kullanıldığında, VLAN bilgilerini bu switch'ler arasında otomatik olarak yaymak ve senkronize etmek için kullanılır. Bu sayede, her switch'in elle VLAN oluşturmasına gerek kalmadan, tüm ağ boyunca VLAN bilgileri merkezi bir noktadan yönetilebilir.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
Switch(config)#vtp domain kmu
Changing VTP domain name from NULL to kmu
Switch(config)#vtp ver
Switch(config)#vtp version 2
Switch(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#do sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : kmu
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.432D.1900
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:55
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 1
MD5 digest                        : 0xF3 0xB6 0x81 0x72 0x90 0x1D 0x81 0x76
                                    0x50 0xCE 0x89 0xFC 0xBA 0xEE 0x8F 0xDE
Switch(config)#
```

VTP'nin Temel Özellikleri:

VTP Domain:

VTP, tüm switch'lerin bir "VTP domain" içinde çalışmasını gerektirir. Bu domain, tüm switch'lerin aynı VLAN bilgilerini paylaşacağı ve birbirleriyle senkronize olacakları bir alandır. Aynı VTP domain'inde olan switch'ler, birbirlerine VLAN bilgilerini iletebilirler.
VTP Modları: VTP, üç farklı modda çalışabilir:

Server Modu:

Bu modda switch, VLAN'ları yaratabilir, silebilir ve güncelleyebilir. Ayrıca, diğer switch'lere bu bilgileri gönderebilir. Server modundaki switch, VTP domain'inde merkezi kontrol sağlar.

Client Modu:

Client modundaki switch'ler VLAN bilgilerini sadece alabilir, fakat yeni VLAN oluşturamaz, silemez veya güncelleyemezler. Client switch'ler sadece VTP server'dan aldıkları VLAN bilgilerini kullanabilirler.

Transparent Modu:

Bu modda switch, VLAN bilgilerini yalnızca kendisi için tutar. VTP bilgilerini diğer switch'lere iletebilir, fakat VLAN bilgilerini değiştirmez.
Transparent moddaki switch, diğer switch'ler için sadece bir "geçiş" cihazıdır, VLAN bilgilerini iletmek için kullanılır ama VLAN bilgilerini depolamaz veya güncellemez.

VTP Versiyonları:

VTP v1: İlk versiyonudur, sadece VLAN bilgilerini yönetir ve VLAN ID'leri 1-1005 arasındaki aralıkla sınırlıdır.

VTP v2: VTP v1'e benzer, ancak bazı iyileştirmeler içerir, örneğin Token Ring VLAN'larını destekler.

VTP v3: VTP v2'ye göre daha gelişmiştir ve gelişmiş güvenlik özellikleri, VLAN bilgilerini şifreleme gibi özellikler ekler. Ayrıca, private VLAN'lar ve VLAN filtering desteği sunar.

Packet Tracer ‘da version 2 desteklediğinden biz 2. Versiyonu kullanıyoruz.

VTP'nin Avantajları:

Merkezi Yönetim: Bir VLAN yapısı merkezi bir switch üzerinden yönetilir, bu da yapılandırma hatalarını en aza indirir.

Verimlilik: Bir VLAN oluşturduğunuzda veya sildiğinizde, tüm ağdaki switch'ler otomatik olarak bu değişiklikten haberdar olur.

Zaman Tasarrufu: Birçok switch üzerinde VLAN yapılandırması yapmanız gerekmez. VTP, bu işlemi otomatikleştirir.

VTP'nin Dezavantajları:

Yanlış Yapılandırma Riskleri: Eğer yanlış yapılandırılmışsa (örneğin, yanlış bir server modunda bir switch), VLAN bilgileri istenmeyen şekilde değiştirilebilir veya silinebilir.
VTP Versiyon Uyumsuzluğu: Farklı VTP versiyonlarının kullanılması, uyumsuzluklara yol açabilir.

Yukarıda VTP ‘nin açıklamasında modlarında client (istemci) modu bulunuyor ve bu modu da diğer bütün switchlere uyguladık.

IP ADDRESS

IP ADDRESS	Default getaway	Subnetmask	VLAN	Name
192.168.1.0-128	192.168.1.1	/25	10	1.kat student
192.168.1.128-256	192.168.1.129	/25	11	1kat akademik personel
192.168.2.0-128	192.168.2.1	/25	12	lab bilgisayarlar
192.168.2.128-256	192.168.2.129	/25	13	ip telefonlar
192.168.3.0-128	192.168.3.1	/25	14	yazıcılar
192.168.4.0-128	192.168.4.1	/25	15	2.kat
192.168.4.128-256	192.168.4.129	/25	16	2.kat akedemik personel
192.168.5.0-128	192.168.5.1	/25	17	3.kat
192.168.5.128-256	192.168.5.129	/25	18	3.kat akedemik personel
10.20.20.96	10.20.20.97	/27		DMZ
192.168.0.0-128	192.168.0.1	/25	100	IT
10.10.0.0	10.10.0.1	/16	50	WLAN

```
!
interface Vlan18
 mac-address 00d0.ba90.8909
 ip address 192.168.5.129 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan50
 mac-address 00d0.ba90.890a
 ip address 10.10.0.1 255.255.0.0
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan100
 mac-address 00d0.ba90.890b
 ip address 192.168.0.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 192.168.0.10
!
interface Vlan999
 description 'Kullanlmayan portlar buraya gnder!!'
 mac-address 00d0.ba90.890c
 no ip address
!
```

```
interface Vlan10
 mac-address 00d0.ba90.8901
 ip address 192.168.1.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan11
 mac-address 00d0.ba90.8902
 ip address 192.168.1.129 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan12
 mac-address 00d0.ba90.8903
 ip address 192.168.2.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan13
 mac-address 00d0.ba90.8904
 ip address 192.168.2.129 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan14
 mac-address 00d0.ba90.8905
 ip address 192.168.3.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan15
 mac-address 00d0.ba90.8906
 ip address 192.168.4.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan16
 mac-address 00d0.ba90.8907
 ip address 192.168.4.129 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
interface Vlan17
 mac-address 00d0.ba90.8908
 ip address 192.168.5.1 255.255.255.128
 ip helper-address 10.20.20.101
 ip helper-address 10.20.20.104
 ip helper-address 192.168.0.10
!
```

VLAN arayüzleri oluşturduk ve default-gateway atamalarını yaptık.

ip helper-address : Bir Cisco yönlendiricisinin veya L3 switch'in DHCP (Dynamic Host Configuration Protocol) gibi UDP tabanlı protokolleri başka bir ağa (veya başka bir DHCP sunucusuna) iletmesini sağlayan bir komuttur. Sırasıyla yazılmalıdır. Çünkü sıraya göre DHCP sunucularına istek gönderir ve cevap alınamaz ise diğer DHCP sunucusuna istek gönderir.
Bu projede Kampüste bulunan bir fakülte üstünde çalışma yaptım. Tabi bu yaptığım çalışma kolay bir şekilde genişletilebir. Fakulte içinde Vlanlara ayırma işlemi yaptık.
Neden?

1) **Güvenlik:** Farklı departmanların veya kullanıcı gruplarının ağ trafiği birbirinden izole edilir.

Örneğin, öğrenciler, personel, öğretim üyeleri ve idari birimler için ayrı VLAN'lar oluşturulabilir.

2) **Trafik Yönetimi:** Broadcast trafiği VLAN'lar arasında izole edilir, bu da ağ

performansını artırır.

3) **Esneklik:** Mantıksal gruplandırmalar yapılabilir. Örneğin, bir VLAN'da sadece öğretim üyeleri, başka bir VLAN'da sadece laboratuvar cihazları bulunabilir.
4) **Kolay Yönetim**: Ağ yöneticileri, belirli VLAN'ları kolayca izleyebilir ve yönetebilir.

Ayrıca 3 adet DHCP sunucusu kullandık. Ip helper-address de gördüğümüz gibi. Bunun nedeni;

1) Kesinti Durumunda Devamlılık: DMZ'de bir DHCP sunucusunda problem yaşanırsa, diğer sunucu yükü devralabilir. Bu, ağın sürekliliğini sağlar.

DMZ DHCP1

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Fakult1_3KStaff	192.168.5.129	10.20.20.102	192.168.5.130	255.255.255.128	126	0.0.0.0	0.0.0.0
IT	192.168.0.1	10.20.20.102	192.168.0.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_1KStudent	192.168.1.1	10.20.20.102	192.168.1.1	255.255.255.128	126	0.0.0.0	0.0.0.0
WLAN	10.10.0.1	10.20.20.102	10.10.0.11	255.255.0.0	60000	0.0.0.0	10.10.0.8
Fakult1_1KStaff	192.168.1.129	10.20.20.102	192.168.1.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStudent	192.168.4.1	10.20.20.102	192.168.4.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStaff	192.168.4.129	10.20.20.102	192.168.4.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_3KStudent	192.168.5.1	10.20.20.102	192.168.5.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_Lab	192.168.2.1	10.20.20.102	192.168.2.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_VOIP	192.168.2.129	10.20.20.102	192.168.2.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_Printer	192.168.3.1	10.20.20.102	192.168.3.11	255.255.255.128	117	0.0.0.0	0.0.0.0

DMZ DHCP2

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Fakult1_3KStaff	192.168.5.129	10.20.20.105	192.168.5.130	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_Printer	192.168.3.1	10.20.20.105	192.168.3.11	255.255.255.128	117	0.0.0.0	0.0.0.0
Fakult1_VOIP	192.168.2.129	10.20.20.105	192.168.2.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_Lab	192.168.2.1	10.20.20.105	192.168.2.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_3KStudent	192.168.5.1	10.20.20.105	192.168.5.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStaff	192.168.4.129	10.20.20.105	192.168.4.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStudent	192.168.4.1	10.20.20.105	192.168.4.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_1KStaff	192.168.1.129	10.20.20.105	192.168.1.129	255.255.255.128	126	0.0.0.0	0.0.0.0
WLAN	10.10.0.1	10.20.20.105	10.10.0.11	255.255.0.0	60000	0.0.0.0	10.10.0.8
Fakult1_1KStudent	192.168.1.1	10.20.20.105	192.168.1.1	255.255.255.128	126	0.0.0.0	0.0.0.0
IT	192.168.0.1	10.20.20.105	192.168.0.1	255.255.255.128	126	0.0.0.0	0.0.0.0

DHCP3

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Fakult1_Printer	192.168.3.1	192.168.0.100	192.168.3.11	255.255.255.128	117	0.0.0.0	0.0.0.0
WLAN	10.10.0.1	192.168.0.100	10.10.0.11	255.255.0.0	60000	0.0.0.0	10.10.0.8
Fakult1_VOIP	192.168.2.129	192.168.0.100	192.168.2.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_Lab	192.168.2.1	192.168.0.100	192.168.2.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_3KStudent	192.168.5.1	192.168.0.100	192.168.5.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStaff	192.168.4.129	192.168.0.100	192.168.4.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_2KStudent	192.168.4.1	192.168.0.100	192.168.4.1	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_1KStaff	192.168.1.129	192.168.0.100	192.168.1.129	255.255.255.128	126	0.0.0.0	0.0.0.0
Fakult1_1KStudent	192.168.1.1	192.168.0.100	192.168.1.1	255.255.255.128	126	0.0.0.0	0.0.0.0
IT	192.168.0.1	192.168.0.100	192.168.0.1	255.255.255.128	126	0.0.0.0	0.0.0.0

Bu yapılandırmalardan sonra, iç ağda haberleşme için OSPF protokolünü kullanıyoruz.

Her switch'te OSPF yapılandırmak için önce router ospf 15 komutuyla OSPF'yi başlatır, ardından network <ip-address> <wildcard-mask> area 0 komutuyla ağları OSPF'ye dahil edersiniz. Ancak, her switch'te farklı process ID kullanmak da mümkündür ve bazı durumlarda daha esnek yapılandırma imkanı tanıyabilir. Yani, avantajlar yönetim kolaylığı ve tutarlılıkla ilgilidir.T abi ama avantajları vardır.

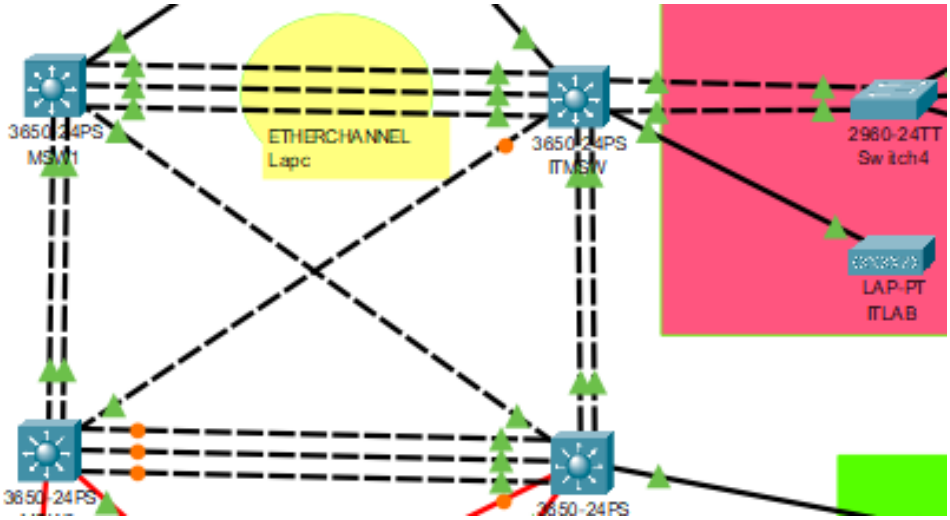
1) **Yönetim Kolaylığı:** Aynı process ID kullanmak, ağın tamamında OSPF yapılandırmalarını daha tutarlı hale getirir ve yönetimini kolaylaştırır. Özellikle büyük ağlarda, tek bir process ID ile tüm yönlendiriciler arasında daha düzenli bir yapı oluşturulabilir.

2) **Komşuluk İlişkileri:** Aynı process ID'yi kullanan yönlendiriciler, birbirleriyle OSPF komşuluğu kurabilir. Bu, OSPF'nin doğru şekilde çalışmasını sağlamak için önemlidir.

ITMSW

```
router ospf 15
 router-id 3.1.3.1
 log-adjacency-changes
 network 10.20.20.24 0.0.0.3 area 0
 network 192.168.0.0 0.0.0.127 area 0
 network 192.168.1.0 0.0.0.127 area 0
 network 192.168.1.128 0.0.0.127 area 0
 network 192.168.2.0 0.0.0.127 area 0
 network 192.168.2.128 0.0.0.127 area 0
 network 192.168.3.0 0.0.0.127 area 0
 network 192.168.4.0 0.0.0.127 area 0
 network 192.168.4.128 0.0.0.127 area 0
 network 192.168.5.0 0.0.0.127 area 0
 network 192.168.5.128 0.0.0.127 area 0
 network 10.10.0.0 0.0.255.255 area 0
 network 10.20.20.96 0.0.0.31 area 0
!
```

ETHERCHANNEL YAPILANDIRMASI



```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-3
Switch(config-if-range)#channe
Switch(config-if-range)#channel
Switch(config-if-range)#channel-gro
Switch(config-if-range)#channel-group 1 mode pas
Switch(config-if-range)#channel-group 1 mode passive
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if-range)#
%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch(config-if-range)#channel-pro
Switch(config-if-range)#channel-protocol lacp
```

```
Switch(config)#int range gi1/0/1-3
Switch(config-if-range)#channel?
channel-group  channel-protocol
Switch(config-if-range)#channel
Switch(config-if-range)#channel-g
Switch(config-if-range)#channel-group ?
  <1-48>  Channel group number
Switch(config-if-range)#channel-group 1 ?
  mode  Etherchannel Mode of the interface
Switch(config-if-range)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
Switch(config-if-range)#channel-group 1 mode active ?
  <cr>
Switch(config-if-range)#channel-group 1 mode active
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

Switch(config-if-range)#channel-pro
Switch(config-if-range)#channel-protocol ?
  lacp  Prepare interface for LACP protocol
  pagp  Prepare interface for PAgP protocol
Switch(config-if-range)#channel-protocol lacp
```

```
interface Port-channel1
 switchport mode trunk
!
interface Port-channel2
 switchport mode trunk
!
interface Port-channel3
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active
!
interface GigabitEthernet1/0/2
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
 no switchport
 ip address 10.20.20.25 255.255.255.252
 tx-ring-limit 20
 duplex auto
 speed auto
!
interface GigabitEthernet1/0/5
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/0/6
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/0/7
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface GigabitEthernet1/0/8
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active
!
interface GigabitEthernet1/0/9
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active
!
```

EtherChannel, birden fazla fiziksel bağlantıyı tek bir mantıksal bağlantı olarak gruplandırarak ağ performansını artıran ve yük dengeleme sağlayan bir teknolojidir. Bu sayede, ağdaki veri iletimi daha hızlı hale gelir ve daha güvenilir bir bağlantı sağlanır. EtherChannel, genellikle switch'ler ve yönlendiriciler arasında yüksek bant genişliği ve yedeklilik sağlamak için kullanılır.
Active/Passive Durumu: EtherChannel'da bağlantıların "active" (aktif) ve "passive" (pasif) durumları, bağlantıların nasıl yönetileceğini belirler.

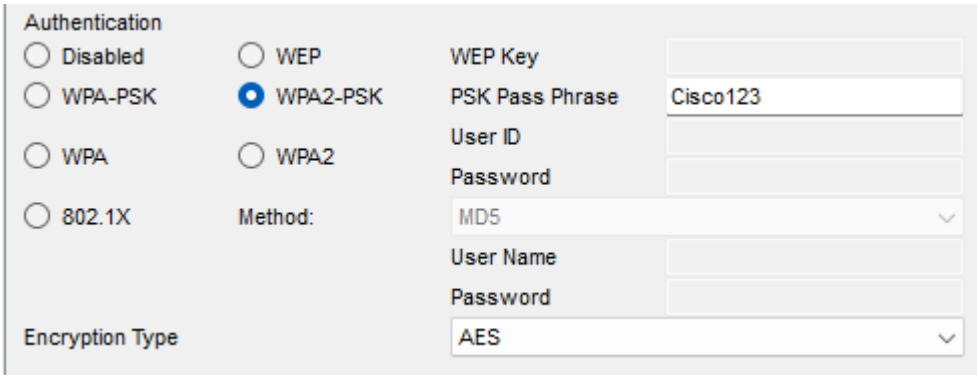
Active (Aktif): Bu bağlantı, EtherChannel yapılandırmasında aktif olarak veri iletimi yapar. Bu bağlantı veri trafiği için kullanılır.

Passive (Pasif): Bu bağlantı, sadece diğer bağlantı aktif olduğunda devreye girer. Eğer aktif bağlantı başarısız olursa, pasif bağlantı otomatik olarak devreye girer ve yük dengeleme sağlanır.

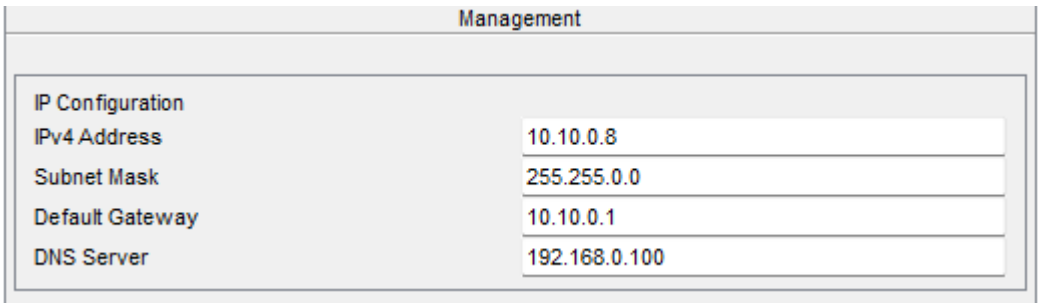
LACP Active/Passive: Bir bağlantı LACP Active modunda ise, sürekli olarak bağlantı kurmaya çalışır. Passive moddaki bağlantı ise, yalnızca Active moddaki bağlantı tarafından başlatılan bir bağlantıya yanıt verir. Bu sayede, sadece bir bağlantı grubu aktif olur ve diğer bağlantılar yedek olarak bekler.

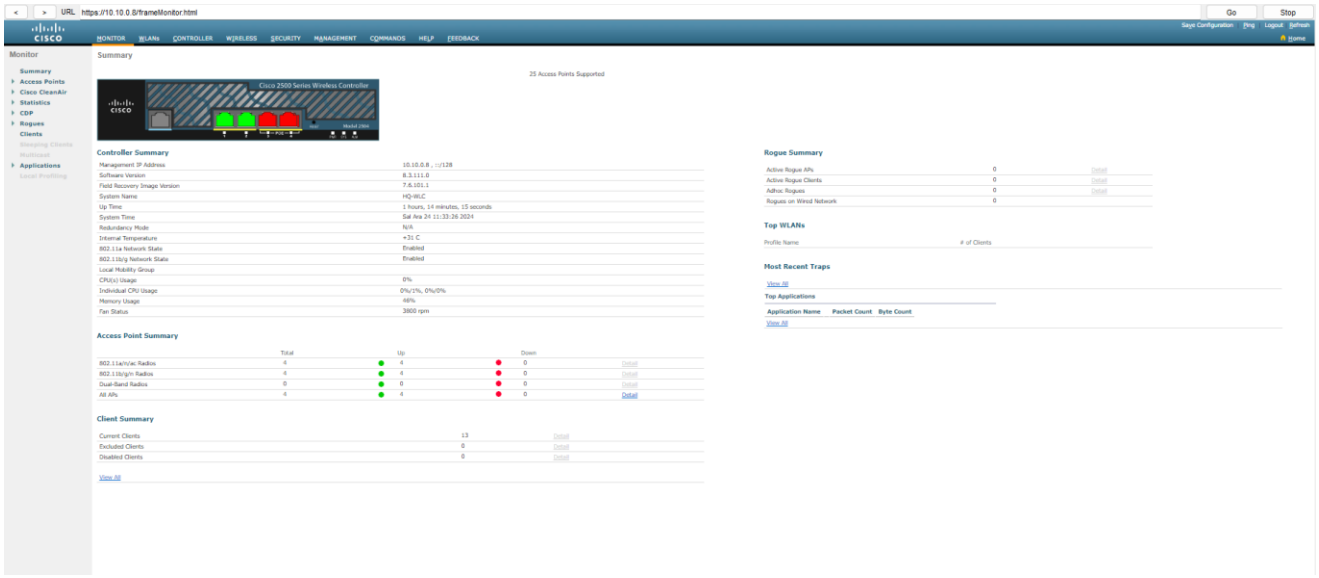
WIRELESS ACCESS POINT

SSID	PASSWORD
1) EMPLOYEE WIFI	Cisco123
2) CORP WIFI	Cisco123
3) AUDIT WIFI	Cisco123
4) GUEST WIFI	Cisco123



WLC Management





WLANs

Current Filter: [Change Filter] [Clear Filter]

Create New Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies	
1	WLAN	EMPLOYEES	EMPLOYEE WIFI	Enabled	[WPA2][Auth(PSK)]	Remove
2	WLAN	CORPORATE USERS	CORP WIFI	Enabled	[WPA2][Auth(PSK)]	Remove
3	WLAN	EXTERNAL AUDITORS	AUDIT WIFI	Enabled	[WPA2][Auth(PSK)]	Remove
4	WLAN	GUEST USERS	GUEST WIFI	Enabled	[WPA2][Auth(PSK)]	Remove

Number of APs 4

AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Statu
CAMLAP3	10.10.0.12	PT-AIR-CAP1000I-A-K9	00:E0:F9:46:C7:AA	0 d, 1 h 15 m 8 s	Enabled
CAMLAP2	10.10.0.13	PT-AIR-CAP1000I-A-K9	00:01:97:9D:21:01	0 d, 1 h 15 m 8 s	Enabled
ITLAB	10.10.0.31	PT-AIR-CAP1000I-A-K9	00:60:2F:E6:1B:01	0 d, 1 h 15 m 8 s	Enabled
CAMLAP	10.10.0.11	PT-AIR-CAP1000I-A-K9	00:02:17:9C:B0:01	0 d, 1 h 15 m 8 s	Enabled

Network Güvenliği

Parolalar, yönlendiriciye ve tüm kablosuz ağlara (5. adımda belirtilen kablosuz erişim noktası) erişimde kullanılır ve erişimi yalnızca Üniversite tarafından yetkilendirilmiş kullanıcılarla sınırlandırır.
Yönlendiriciler ayrıca ssh (Güvenli Kabuk) ile güvence altına alınır.

Switch Name	Passwords
1)CEMSW1	Console password: cisco ssh password: cisco
2)CEMSW2	Console password: cisco ssh password: cisco
3)1KSW	Console password: cisco ssh password: cisco
4)1.1KSW	Console password: cisco ssh password: cisco
5)2KSW	Console password: cisco ssh password: cisco
6)2.1KSW	Console password: cisco ssh password: cisco
7)3KSW	Console password: cisco ssh password: cisco
8)3.1KSW	Console password: cisco ssh password: cisco
9) ITSwitch	Console password: cisco ssh password: cisco
10) DMZSW	Console password: cisco ssh password: cisco

```
(config)#line console 0
(config-line)#password cisco
(config-line)#login
(config-line)#exec-timeout 3 0
(config-line)#exit
(config)#
(config)#enable password cisco
(config)#
(config)#no ip domain-lookup
(config)#
(config)#service password-encryption
(config)#
(config)#username cisco password cisco
(config)#ip domain-name cisco.com
(config)#crypto key generate rsa general-keys modulus 1024
ame for the keys will be: keser.cisco.com

 key modulus size is 1024 bits
erating 1024 bit RSA keys, keys will be non-exportable...[OK]
1 1:18:30.705: %SSH-5-ENABLED: SSH 2 has been enabled
(config)#
(config)#ip ssh version 2
(config)#
(config)#access-list 2 permit 192.168.0.0 0.0.0.127
(config)#access-list 2 deny any
(config)#
(config)#line vty 0 15
(config-line)#login local
(config-line)#transport input ssh
(config-line)#access-class 2 in
(config-line)#exit
(config)#
(config)#do wr
```

```
CEMSW2(config)#line console 0
CEMSW2(config-line)#password cisco
CEMSW2(config-line)#login
CEMSW2(config-line)#exec-timeout 3 0
CEMSW2(config-line)#exit
CEMSW2(config)#
CEMSW2(config)#enable password cisco
CEMSW2(config)#
CEMSW2(config)#no ip domain-lookup
CEMSW2(config)#
CEMSW2(config)#service password-encryption
CEMSW2(config)#
CEMSW2(config)#username cisco password cisco
CEMSW2(config)#ip domain-name cisco.com
CEMSW2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: CEMSW2.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:31:35.369: %SSH-5-ENABLED: SSH 1.99 has been enabled
CEMSW2(config)#
CEMSW2(config)#ip ssh version 2
CEMSW2(config)#
CEMSW2(config)#access-list 2 permit 192.168.0.0 0.0.0.127
CEMSW2(config)#access-list 2 deny any
CEMSW2(config)#
CEMSW2(config)#line vty 0 15
CEMSW2(config-line)#login local
CEMSW2(config-line)#transport input ssh
CEMSW2(config-line)#access-class 2 in
CEMSW2(config-line)#exit
CEMSW2(config)#
CEMSW2(config)#do wr
Building configuration...
[OK]
```

FIREWALL NAT YAPILANDIRMASI

```
object network inside1-outside1
 subnet 192.168.0.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside1-outside2
 subnet 192.168.0.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside10-outside1
 subnet 192.168.5.128 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside10-outside2
 subnet 192.168.5.128 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside10a-outside1
 subnet 192.168.5.128 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside10a-outside2
 subnet 192.168.5.128 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside11-outside1
 subnet 10.10.0.0 255.255.0.0
 nat (inside1,outside1) dynamic interface
object network inside11a-outside1
 subnet 10.10.0.0 255.255.0.0
 nat (inside2,outside1) dynamic interface
object network inside1a-outside1
 subnet 192.168.0.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside1a-outside2
 subnet 192.168.0.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside2-outside1
 subnet 192.168.1.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside2-outside2
 subnet 192.168.1.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside2a-outside1
 subnet 192.168.1.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside2a-outside2
 subnet 192.168.1.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside3-outside1
 subnet 192.168.1.128 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside3-outside2
 subnet 192.168.1.128 255.255.255.128
 nat (inside1,outside2) dynamic interface
```

```
object network inside3a-outside1
 subnet 192.168.1.128 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside3a-outside2
 subnet 192.168.1.128 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside4-outside1
 subnet 192.168.2.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside4-outside2
 subnet 192.168.2.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside4a-outside1
 subnet 192.168.2.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside4a-outside2
 subnet 192.168.2.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside5-outside1
 subnet 192.168.2.128 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside5-outside2
 subnet 192.168.2.128 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside5a-outside1
 subnet 192.168.2.128 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside5a-outside2
 subnet 192.168.2.128 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside6-outside1
 subnet 192.168.3.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside6-outside2
 subnet 192.168.3.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside6a-outside1
 subnet 192.168.3.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside6a-outside2
 subnet 192.168.3.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside7-outside1
 subnet 192.168.4.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside7-outside2
 subnet 192.168.4.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside7a-outside1
 subnet 192.168.4.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside7a-outside2
 subnet 192.168.4.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside8-outside1
 subnet 192.168.4.128 255.255.255.128
 nat (inside1,outside1) dynamic interface
```

```
object network inside8-outside2
 subnet 192.168.4.128 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside8a-outside1
 subnet 192.168.4.128 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside8a-outside2
 subnet 192.168.4.128 255.255.255.128
 nat (inside2,outside2) dynamic interface
object network inside9-outside1
 subnet 192.168.5.0 255.255.255.128
 nat (inside1,outside1) dynamic interface
object network inside9-outside2
 subnet 192.168.5.0 255.255.255.128
 nat (inside1,outside2) dynamic interface
object network inside9a-outside1
 subnet 192.168.5.0 255.255.255.128
 nat (inside2,outside1) dynamic interface
object network inside9a-outside2
 subnet 192.168.5.0 255.255.255.128
 nat (inside2,outside2) dynamic interface
!
```

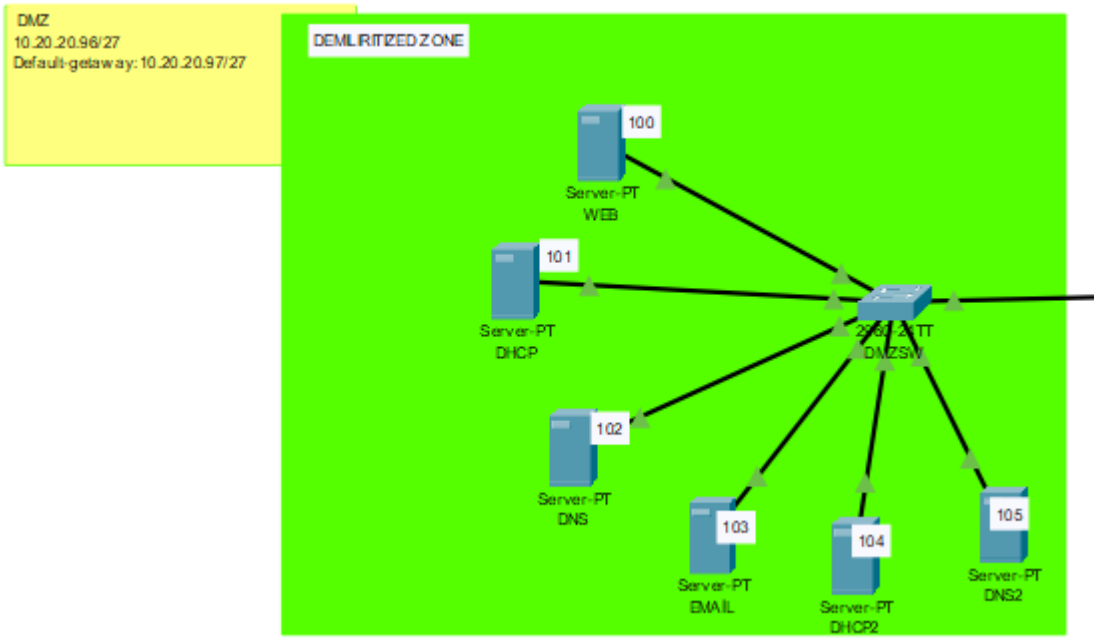
ACCESS-LİST Oluşturma Ve Atama

```
access-list RES-ACCESS extended permit icmp any any
access-list RES-ACCESS extended permit udp any any eq bootps
access-list RES-ACCESS extended permit udp any any eq bootpc
access-list RES-ACCESS extended permit udp any any eq domain
access-list RES-ACCESS extended permit tcp any any eq domain
access-list RES-ACCESS extended permit tcp any any eq www
access-list RES-ACCESS extended permit tcp any any eq smtp
access-list RES-ACCESS extended permit tcp any any eq 20
access-list RES-ACCESS extended permit tcp any any eq ftp
access-list RES-ACCESS extended permit udp any any eq 5246
access-list RES-ACCESS extended permit udp any any eq 5247
access-list RES-ACCESS extended permit udp any any eq 12222
access-list RES-ACCESS extended permit udp any any eq 12223
!
!
access-group RES-ACCESS in interface outside1
access-group RES-ACCESS in interface DMZ
access-group RES-ACCESS in interface outside2
!
```

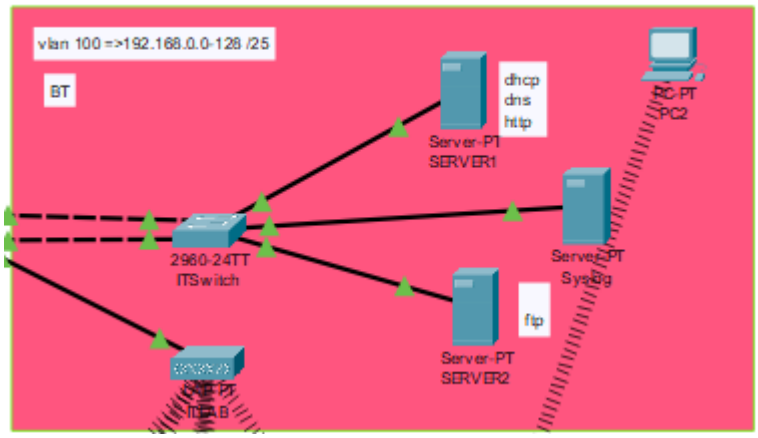
7.SONUÇ & TARTIŞMA

Son olarak, gerçekleştirdiğimiz işlemleri birleştirerek, üniversite ve bünyesindeki fakülteler için hem kablosuz hem de kablolu bağlantıya sahip kapsamlı bir ağ altyapısı oluşturduk.

DMZ

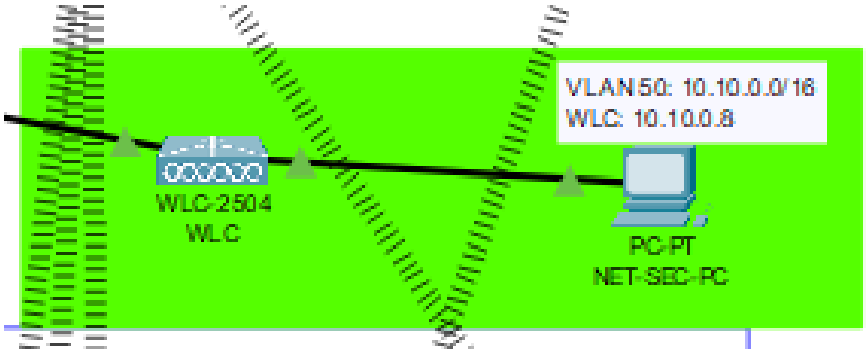


BT

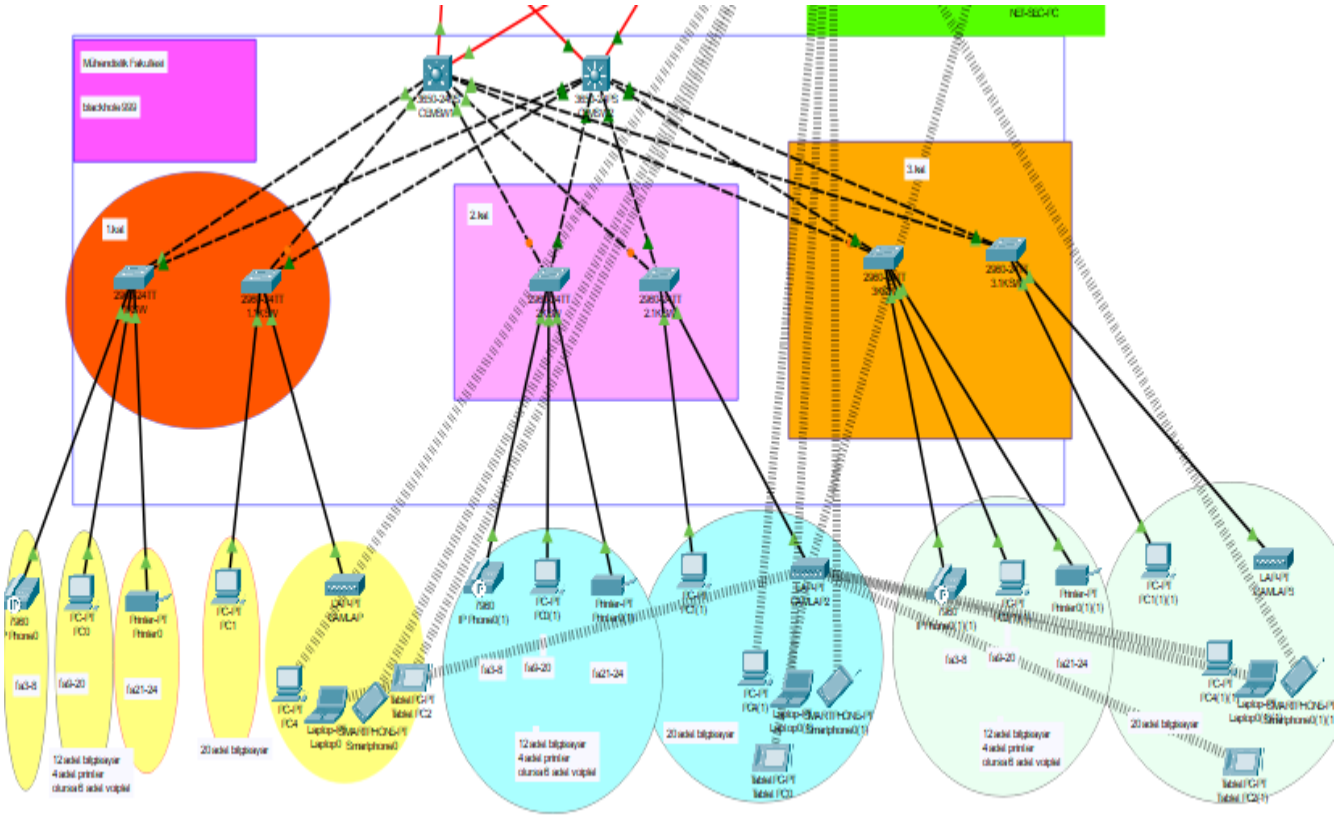


Default-gateway:192.168.0.1/25
SERVER1:192.168.0.10/25
SERVER2:192.168.0.12/25
SYSLOG: 192.168.0.13

WLC

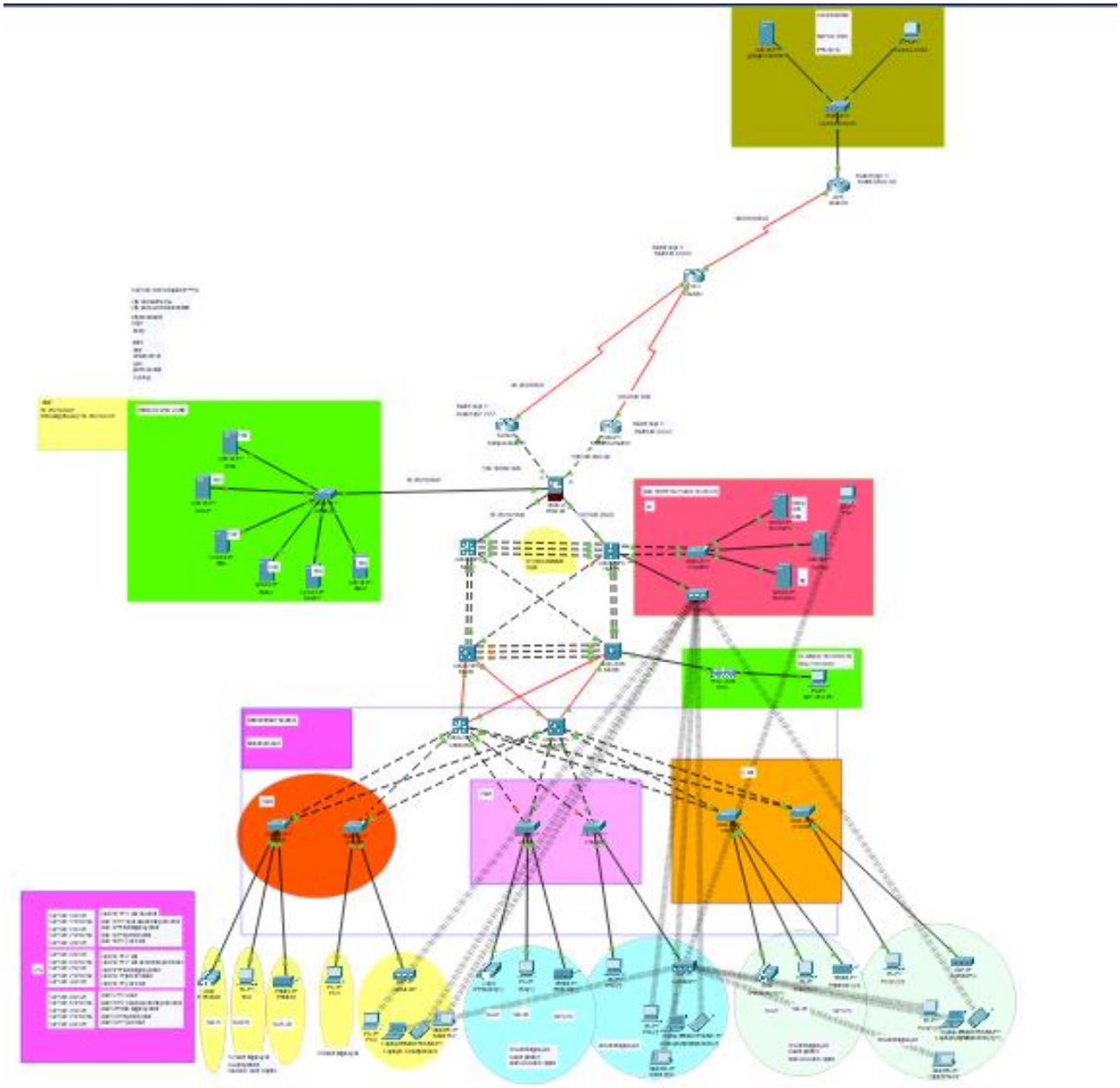


FAKÜLTE 1



Fakülte bünyesindeki cihazlar ve bağlantılar

Son Tasarım



Üniversite ve bünyesindeki fakülte için Packet Tracer ’da oluşturulmuş bir ağ modeli

TESTLER

Ping Testi: Ağ bağlantısı ve iletişimi, ping komutu kullanılarak, ardından bağlantısını doğrulamak istediğiniz cihazın (ekipmanın) etki alanı adı veya IP adresi eklenerek test edilebilir.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.11: bytes=32 time<1ms TTL=127
Reply from 192.168.3.11: bytes=32 time=26ms TTL=127
Reply from 192.168.3.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 26ms, Average = 8ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time<1ms TTL=127
Reply from 192.168.2.3: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>
```

Router SSH Bağlantı

```
C:\>ssh -l admin 105.100.50.2

Password:

Yaplan Deiikliklerden nce yedek aliniz!

router1>
router1>
router1>
router1>
router1>
router1>
router1>ping 105.100.50.5
```

```
C:\>ssh -l admin 105.100.50.5

Password:

Degisik yapmadan once yedek aliniz!

router2>end
```

8.SONUÇ VE GELECEKTEKİ ÇALIŞMALAR

- **SONUÇ**

Bu proje kapsamında, üniversite kampüsündeki belirli bir binanın ağ altyapısı Packet Tracer kullanılarak başarıyla tasarlanmış ve simüle edilmiştir. Ağın güvenilir, verimli ve yönetilebilir bir yapı sağladığı görülmüştür. Proje sonuçlarına göre aşağıdaki bulgular elde edilmiştir:

Ağ Performansı: Ağın topoloji ve IP adresleme planlaması, veri akışında düşük gecikme süresi ve yüksek hız sağlanmasına yardımcı olmuştur. VLAN yapılandırması, ağ trafiğinin düzenlenmesine ve kampüs içindeki farklı birimler arasında veri akışının iyileştirilmesine katkı sağlamıştır.

Güvenlik ve Erişim Yönetimi: Firewall ve SSH protokolü gibi güvenlik önlemleri sayesinde ağ güvenliğinde yüksek bir seviye sağlanmıştır. Bu önlemler, yetkisiz erişimlerin önlenmesine ve verilerin koruma altına alınmasına olanak tanımıştır. Özellikle FTP, DNS ve e-posta sunucuları gibi kritik sunucuların güvenliği artırılmıştır.

Otomatik IP Dağıtımı: DHCP sunucusu, cihazlara IP adreslerinin otomatik olarak atanmasını sağlamış ve manuel adresleme sürecini ortadan kaldırarak yönetim işini kolaylaştırmıştır. Bu, özellikle cihaz sayısının fazla olduğu kampüs ağı gibi ortamlarda büyük bir verimlilik sağlamıştır.

Kablosuz Erişim: Kablosuz erişim noktaları aracılığıyla öğrencilere ve personele kesintisiz internet hizmeti sağlanmıştır. Bu, kampüs içinde mobil cihazların özgürce hareket edebilmesi ve internet erişimine rahatça ulaşması açısından önemli bir fayda sunmuştur.

Sunucuların İşlevselliği: DNS, e-posta, web ve FTP sunucularının sağladığı hizmetler, ağ üzerinde sorunsuz bir şekilde çalışmış, verimli veri paylaşımı ve erişim imkânı sağlamıştır. Bu sunucuların yapılandırılması ve işlevselliği, ağın yönetilebilirliğini ve kullanım kolaylığını artırmıştır.

Bu proje, üniversite kampüsünde örnek bir ağ altyapısının nasıl oluşturulabileceğini göstermiş ve elde edilen bulgular, gelecekteki kampüs ağ yapılarının geliştirilmesine yönelik önemli çıkarımlar sunmuştur.

- **Gelecekteki çalışmalar**

Yapılandırma ve özellikler ilk prototip içindir ve daha sonra geliştirilebilir ve mevcut ağımızın desteğini ve kapsamını artırmak için ek işlevler eklenebilir. DHCP sadece kesinti durumu için fazla kullanmaktan ziyade misafir kullanıcı ve akademik personeller için kullanılacak. IPv6 adres ataması gelecek.

9.KAYNAKÇA

- [1] https://tr.wikipedia.org/wiki/Packet_Tracer
- https://tr.wikipedia.org/wiki/Kamp%C3%BCs_a%C4%9F%C4%B1
- [2]https://en.wikipedia.org/wiki/Router_(computing)
- [3]https://en.wikipedia.org/wiki/Network_switch
- [4]https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.
- https://acikders.ankara.edu.tr/pluginfile.php/155274/mod_resource/content/0/2.%20A%C4%9F%20Topolojileri.pdf
- https://tr.wikipedia.org/wiki/A%C4%9Fa%C3%A7_topolojisi
- [5]https://www.cloudflare.com/learning/network-layer/internet-protocol/
- [6]https://www.ssh.com/academy/ssh/protocol
- https://www.irjet.net/archives/V8/i4/IRJET-V8I4679.pdf
- https://github.com/Jose-Ch1/Cisco-CampusUniversity
- https://github.com/katejay/College-Network
- https://github.com/Jahid-Hasan-96/Campus_Network_Design_and_Implementation
- https://github.com/pradeepchegur/Hospital_Network_Design_Mesh_Topology
- https://tr.wikipedia.org/wiki/RADIUS
- https://en.wikipedia.org/wiki/TACACS
- [7]https://milestoneresearch.in/JOURNALS/index.php/IJCLI/article/view/141
- [8]https://tr.wikipedia.org/wiki/DHCP
- [9]https://learn.microsoft.com/tr-tr/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting
- [10]https://www.firatboyan.com/vlan-nedir-vlan-konfigurasyonu-nasil-yapilandirilir.aspx
- [11]https://acikders.ankara.edu.tr/pluginfile.php/155273/mod_resource/content/0/1.1.%20A%C4%9F%20T%C3%BCrleri.pdf
- https://www.cisco.com/c/en/us/td/docs/wireless/mwam/user/guide/mwam1/CLI.pdf
- https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm