İSTANBUL
GELİŞİM
ÜNİVERSİTESİ

İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU

BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ

BİLİŞİM GÜVENLİĞİ TEKNOLOJİSİ PROGRAMI

CİSCO PACKET TRACER RAPORU

AĞ TEMELLERİ DERSİ UYGULAMA PROJESİ

Hazırlayan

230175333 – Murat KAZMA

ÖDEV DANIŞMANI

Öğr. Gör. Tuğba Saray ÇETİNKAYA

İSTANBUL – 2023

PROJE TANITIM FORMU

YAZAR ADI SOYADI	:	Murat KAZMA
PROJE ADI	:	Devlet Binası Güvenliği ve Performans Yönetimi
BÖLÜM	:	Bilgisayar Teknolojileri
PROGRAM	:	Bilişim Güvenliği Teknolojileri
PROJENİN TES. TARİHİ	:	18/12/2023
SAYFA NUMARASI	:	31
PROJE DANIŞMANI	:	Öğr. Gör. Tuğba Saray ÇETİNKAYA

ÖZET

Eyalet Binası Güvenlik ve Performans Yönetimi projesi, tek bir ağ odasında on departman için kesintisiz bağlantı ve güvenlik sağlar. Cisco Packet Tracer kullanılarak anahtarlar, yönlendiriciler ve erişim noktaları stratejik olarak yerleştirilmiştir. VLAN'lar güvenliği artırır, OSPF trafiği yönetir ve erişim noktaları güvenli kablosuz bağlantılar sunar. Güvenlik duvarları ve IDS gibi sağlam güvenlik önlemleri alınırken, performans izleme araçları ağın en iyi şekilde çalışmasını sağlar.

Anahtar Kelimeler : Güvenlik, Anahtarlar, Erişim Noktaları, Güvenlik Duvarları, IDS, WLAN, OSPF, Ağ Simülasyonu, Protokol Simülasyonu

İÇİNDEKİLER

1. GİRİŞ

Günümüzde bilgi teknolojilerinin hızla gelişmesi ve ağların hayatımızın her alanına entegre olması, ağ teknolojileri ve ağ yönetimi konularının önemini giderek artırmaktadır. Bu bağlamda, ağ simülasyon araçları, ağ mühendislerinin ve bilgi teknolojileri profesyonellerinin ağları daha iyi anlamalarını ve yönetmelerini sağlayan kritik araçlar haline gelmiştir. Cisco Packet Tracer, bu tür araçlardan biri olup, özellikle eğitim ve pratik amaçlı olarak yaygın bir şekilde kullanılmaktadır.

Cisco Packet Tracer, kullanıcıların ağ yapılarını simüle etmelerine, yapılandırmalar yapmalarına ve çeşitli ağ senaryolarını test etmelerine olanak tanıyan güçlü bir ağ simülasyon aracıdır. Hem öğrenciler hem de profesyoneller için ideal bir öğrenme ve öğretme platformu olan bu yazılım, ağ teknolojileri hakkında derinlemesine bilgi sahibi olmayı ve pratik deneyim kazanmayı mümkün kılar.

Bu doküman, Cisco Packet Tracer'ın tanıtımı, özellikleri, kurulumu ve kullanımı hakkında kapsamlı bilgiler sunmayı amaçlamaktadır. Ayrıca, Cisco tarafından sunulan ve dünya genelinde ağ uzmanları tarafından büyük önem verilen CCNA (Cisco Certified Network Associate) sertifikası hakkında da bilgi verilecektir. CCNA sertifikası, ağ mühendisleri için önemli bir yetkinlik göstergesi olup, bu sertifikayı almak isteyenlerin Cisco Packet Tracer gibi araçları etkin bir şekilde kullanabilmesi gerekmektedir.

Ağ teknolojilerine yeni başlayanlar veya mevcut bilgi birikimlerini derinleştirmek isteyenler için hazırlanmış bu doküman, temel ağ kavramlarından başlayarak, ağ cihazlarının işleyişi ve yönetimine kadar geniş bir yelpazede bilgi sunmaktadır. İlk bölümde Cisco Packet Tracer'ın ne olduğu ve hangi amaçlarla kullanıldığı üzerinde durulacak, ardından yazılımın özellikleri ve nasıl kurulum yapılacağı detaylandırılacaktır. Devam eden bölümlerde ise Cisco Packet Tracer'ın kullanımı ve ağ simülasyonları ile ilgili pratik ipuçları paylaşılacaktır.

2. CİSCO PACKET TRACER TANITIM

2.1 Cisco Packet Tracer Nedir?

Cisco Packet Tracer, Cisco Systems tarafından geliştirilen ve ağ teknolojileri eğitiminde kullanılan güçlü bir simülasyon yazılımıdır. Bu yazılım, kullanıcıların sanal bir ortamda ağ cihazları ve ağ yapıları oluşturmasına, yapılandırmasına ve test etmesine olanak tanır. Cisco Packet Tracer, özellikle ağ mühendisliği, ağ yönetimi ve bilgi teknolojileri alanlarında eğitim gören öğrenciler ve profesyoneller için tasarlanmıştır.

Packet Tracer, çeşitli ağ cihazlarını ve ağ protokollerini simüle edebilen kapsamlı bir araçtır. Yönlendiriciler, anahtarlar, kablosuz erişim noktaları, sunucular ve istemci bilgisayarlar gibi çeşitli ağ cihazları sanal olarak bu yazılım içinde oluşturulabilir ve birbirlerine bağlanabilir. Ayrıca, yazılım ağ topolojileri üzerinde çeşitli ağ protokollerinin nasıl çalıştığını görsel olarak anlamaya yardımcı olur ve kullanıcıların bu protokollerle ilgili yapılandırmaları gerçekleştirmesine imkan tanır.

Cisco Packet Tracer'ın temel özelliklerinden biri, kullanıcıların ağ senaryolarını adım adım oluşturabilmesi ve bu senaryolar üzerinde çeşitli deneyler yapabilmesidir. Örneğin, bir ağda paketlerin nasıl yönlendirildiğini, veri trafiğinin nasıl yönetildiğini ve ağ güvenliği önlemlerinin nasıl uygulandığını simüle edebilirler. Bu, kullanıcılara gerçek dünya ağlarında karşılaşabilecekleri durumları önceden deneyimleme fırsatı sunar.

Ayrıca, Cisco Packet Tracer, Cisco'nun Networking Academy programı ile entegre çalışır ve bu programın müfredatını takip eden öğrenciler için çeşitli laboratuvar çalışmaları ve pratik egzersizler sağlar. Bu sayede, öğrenciler teorik bilgilerini pekiştirirken pratik becerilerini de geliştirebilirler.

2.2 Cisco Packet Tracer Özellikleri

Cisco Packet Tracer, kullanıcılarına geniş bir yelpazede özellikler sunar ve bu özellikler, ağ simülasyonlarının gerçekleştirilmesini kolaylaştırır.

Çoklu Platform Desteği: Cisco Packet Tracer, Windows, macOS ve Linux işletim sistemlerinde çalışabilen bir yazılımdır. Bu, farklı platformlarda çalışan kullanıcıların aynı yazılımı kullanarak öğrenme ve öğretme süreçlerini devam ettirmelerini sağlar.

Zengin Cihaz ve Protokol Desteği: Packet Tracer, yönlendiriciler, anahtarlar, kablosuz erişim noktaları, güvenlik duvarları, sunucular ve istemci cihazlar gibi geniş bir yelpazede ağ cihazlarını

destekler. Ayrıca, TCP/IP, OSPF, EIGRP, RIP, STP, VLAN, EtherChannel ve daha birçok ağ protokolünü simüle edebilir.

Görsel Ağ Tasarımı: Kullanıcılar, sürükle ve bırak yöntemiyle ağ cihazlarını ve bağlantılarını kolayca ekleyebilir ve görsel olarak anlaşılır ağ topolojileri oluşturabilirler. Bu, ağ yapılarının görselleştirilmesi ve anlaşılmasını kolaylaştırır.

Simülasyon ve Gerçek Zaman Modları: Packet Tracer, hem simülasyon hem de gerçek zaman modlarında çalışabilir. Simülasyon modu, kullanıcıların ağdaki olayları adım adım takip etmelerine olanak tanır. Gerçek zaman modu ise ağın gerçek dünyadaki gibi çalışmasını sağlar.

Sürükle ve Bırak Yapılandırma: Cihazların yapılandırılması oldukça kullanıcı dostudur. Cihazların üzerine çift tıklayarak veya sağ tıklayarak hızlıca yapılandırma ekranlarına erişilebilir ve komutlar girilerek ayarlar yapılabilir.

Çok Kullanıcılı Ortam: Packet Tracer, birden fazla kullanıcının aynı ağ senaryosu üzerinde işbirliği yapmasına olanak tanır. Bu, özellikle grup çalışmaları ve sınıf içi etkinlikler için oldukça yararlıdır.

Script ve Olay Temelli Simülasyon: Kullanıcılar, ağ senaryoları için scriptler ve olaylar tanımlayarak belirli durumları test edebilirler. Bu, ağ sorun giderme ve problem çözme becerilerini geliştirmek için idealdir.

Eğitim ve Sınav Modülleri: Cisco Networking Academy müfredatına uygun olarak hazırlanmış eğitim ve sınav modülleri içerir. Bu, öğrencilere belirli konuları öğrenme ve bilgilerini test etme fırsatı sunar.

2.3 Cisco Packet Tracer Kurulumu

İndirme: İlk adım olarak, Cisco Packet Tracer'ın en son sürümünü Cisco Networking Academy web sitesinden indirin. Bu, Cisco Networking Academy'ye kaydolmuş kullanıcılar için ücretsiz olarak sunulmaktadır.

Kurulum Dosyasını Çalıştırma: İndirme işlemi tamamlandıktan sonra, indirdiğiniz kurulum dosyasına çift tıklayarak kurulum sürecini başlatın. Bu, işletim sisteminize bağlı olarak bir .exe, .dmg veya .bin dosyası olabilir.

Lisans Sözleşmesini Kabul Etme: Kurulum sihirbazı açıldığında, ilk adım olarak lisans sözleşmesini kabul etmeniz istenecektir. Lisans sözleşmesini okuyun ve kabul ettiğinizi belirtmek için ilgili kutucuğu işaretleyin.

Yükleme Yeri Seçimi: Kurulum sihirbazı, yazılımın nereye yükleneceğini seçmenizi isteyecektir. Varsayılan yükleme yeri genellikle uygundur, ancak isterseniz farklı bir yer seçebilirsiniz.

Kurulumu Tamamlama: Yükleme yeri seçildikten sonra, kurulum sürecini başlatmak için "Yükle" veya "Install" düğmesine tıklayın. Kurulum sihirbazı, gerekli dosyaları kopyalayarak ve yapılandırarak yazılımı bilgisayarınıza yükleyecektir.

Kurulumun Tamamlanması ve Başlatma: Kurulum tamamlandığında, sihirbaz size kurulumun başarılı bir şekilde tamamlandığını belirten bir mesaj gösterecektir. "Son" veya "Finish" düğmesine tıklayarak kurulum sihirbazını kapatın. Ardından, masaüstünüzde veya başlangıç menüsünde oluşan Cisco Packet Tracer simgesine tıklayarak yazılımı başlatabilirsiniz.

Giriş Yapma: İlk başlatmada, Cisco Networking Academy kullanıcı adınız ve şifreniz ile giriş yapmanız istenecektir. Bu adımı tamamladıktan sonra, Cisco Packet Tracer'ı tam işlevselliği ile kullanmaya başlayabilirsiniz.

2.4 Cisco Packet Tracer Kullanımı

Cisco Packet Tracer'ın kullanımı, hem eğitim hem de profesyonel amaçlar için oldukça etkilidir. Yazılımın sunduğu çeşitli araçlar ve özellikler sayesinde kullanıcılar, karmaşık ağ yapılarını kolayca simüle edebilir ve yönetebilirler.

Arayüzü Anlamak: Cisco Packet Tracer'ı ilk açtığınızda, ana arayüzde cihaz simgeleri, araç çubukları ve ağ çalışma alanı ile karşılaşırsınız. Araç çubukları, cihazları eklemek, bağlantıları yapmak ve simülasyonu kontrol etmek için kullanılır.

Ağ Topolojisi Oluşturma: Yeni bir ağ topolojisi oluşturmak için, araç çubuğundan gerekli cihazları (örneğin, yönlendiriciler, anahtarlar, bilgisayarlar) seçip çalışma alanına sürükleyip bırakın. Bu cihazları birbirine bağlamak için, bağlantı aracı ile cihazlar arasında bağlantılar oluşturabilirsiniz.

Cihazları Yapılandırma: Cihazları yapılandırmak için, cihaz simgesine çift tıklayarak yapılandırma penceresini açın. Bu pencerede, cihazın IP adresi, ağ maskesi, ağ geçidi ve diğer ağ

ayarlarını yapılandırabilirsiniz. Ayrıca, komut satırı arayüzünü kullanarak daha ileri düzeyde yapılandırmalar yapabilirsiniz.

Simülasyon Modu: Simülasyon modunu kullanarak, ağınızın nasıl çalıştığını adım adım inceleyebilirsiniz. Paketlerin nasıl yönlendirildiğini, veri trafiğinin nasıl hareket ettiğini ve ağ cihazlarının nasıl tepki verdiğini izleyebilirsiniz. Bu mod, ağ sorunlarını teşhis etmek ve ağ performansını değerlendirmek için çok faydalıdır.

Gerçek Zaman Modu: Gerçek zaman modu, ağın gerçek dünyadaki gibi çalışmasını sağlar. Bu modda, cihazlar anında tepki verir ve veri trafiği gerçek zamanlı olarak hareket eder. Gerçek zaman modu, ağın normal çalışma koşullarını simüle etmek için kullanılır.

Senaryolar ve Projeler: Cisco Packet Tracer, kullanıcıların belirli senaryolar ve projeler oluşturmasına olanak tanır. Bu, özellikle ağ eğitiminde ve laboratuvar çalışmalarında kullanışlıdır. Öğrenciler, belirli ağ problemlerini çözmek için senaryolar oluşturabilir ve bu senaryolar üzerinde çalışarak pratik yapabilirler.

Değerlendirme ve Sınav Modülleri: Cisco Packet Tracer, Cisco Networking Academy müfredatına uygun olarak hazırlanmış değerlendirme ve sınav modülleri içerir. Bu modüller, öğrencilerin bilgi seviyelerini değerlendirmelerine ve sınavlara hazırlanmalarına yardımcı olur.

Çok Kullanıcılı Ortam: Cisco Packet Tracer, birden fazla kullanıcının aynı ağ senaryosu üzerinde işbirliği yapmasına olanak tanır. Bu, grup çalışmaları ve sınıf içi etkinlikler için mükemmel bir özelliktir.

2.4 CCNA Sertifikası Nedir?

CCNA (Cisco Certified Network Associate) sertifikası, Cisco Systems tarafından sunulan ve ağ mühendisliği alanında dünya genelinde tanınan bir sertifikadır. Bu sertifika, temel ağ teknolojileri ve ağ yönetimi konularında yetkinlik kazanmış profesyonelleri belgelendirir. CCNA sertifikası, ağ mühendisleri, ağ yöneticileri ve bilgi teknolojileri profesyonelleri için önemli bir kariyer basamağıdır.

CCNA sertifikası, çeşitli ağ teknolojileri ve protokoller hakkında kapsamlı bir bilgi gerektirir. Sertifika sahipleri, ağ cihazlarının kurulumu, yapılandırılması, işletilmesi ve sorun giderilmesi gibi konularda yetkinlik kazanır.

CCNA sertifikası, bireylerin ağ dünyasındaki bilgi ve becerilerini doğrulayarak, bu alandaki güvenilir profesyoneller arasında yer almalarını sağlar.

CCNA Sertifikaları hakkında bilgi almak için:

https://www.cisco.com/c/en/us/training-events/training- certifications/exams.html

Temel Ağ Kavramları: CCNA sertifikası, IP adresleme, alt ağ oluşturma, yönlendirme ve anahtarlama gibi temel ağ kavramlarını kapsamlı bir şekilde ele alır. Bu, adayların ağların nasıl çalıştığını ve ağ bileşenlerinin nasıl etkileşimde bulunduğunu anlamalarını sağlar.

Yönlendirme ve Anahtarlama: CCNA, yönlendirme protokolleri (OSPF, EIGRP, RIP) ve anahtarlama teknolojileri (VLAN, STP, EtherChannel) konularında derinlemesine bilgi sunar. Bu, ağ mühendislerinin karmaşık ağ topolojilerini tasarlamalarına ve yönetmelerine yardımcı olur.

Ağ Güvenliği: CCNA sertifikası, ağ güvenliği konularında da kapsamlı bir eğitim sağlar. Güvenlik duvarları, VPN'ler, erişim kontrol listeleri (ACL'ler) ve diğer güvenlik mekanizmaları hakkında bilgi verir.

Kablosuz Ağlar: CCNA, kablosuz ağ teknolojileri ve kablosuz ağların nasıl yapılandırılacağı ve yönetileceği hakkında da bilgi sunar. Bu, günümüzün mobil ve kablosuz bağlantılara dayalı dünyasında önemli bir yetkinliktir.

Otomasyon ve Programlanabilirlik: Yeni CCNA müfredatı, ağ otomasyonu ve programlanabilirlik konularını da içermektedir. Bu, ağ mühendislerinin Python gibi programlama dilleri ve otomasyon araçları kullanarak ağ işlemlerini otomatikleştirmelerine olanak tanır.

Kariyer Fırsatları: CCNA sertifikası, dünya genelinde tanınan bir sertifika olup, ağ mühendisliği kariyerinde önemli bir adım olarak kabul edilir. CCNA sahipleri, ağ mühendisleri, ağ yöneticileri, sistem mühendisleri ve diğer bilgi teknolojileri pozisyonlarında iş bulma şansını artırır.

Sürekli Eğitim: CCNA sertifikası, adayların bilgi ve becerilerini güncel tutmalarını sağlar. Sertifika sahipleri, sürekli eğitim ve sertifika yenileme yoluyla ağ teknolojilerindeki yenilikleri takip edebilirler.

3. NETWORKİNG 101 ve AĞ CİHAZLARINI TANIMAK

3.1 Switch

Switch, ağda MAC (Media Access Control) adresleri üzerinden iletişimi sağlayan ve OSI modelinin 2. ve 3. katmanlarında konumlanan kritik bir ağ cihazıdır. MAC adres tablosunu kullanarak, switch, ağdaki her bir cihazın MAC adresini öğrenir ve bu bilgiyi bir tabloda saklar. Veri paketleri geldiğinde, switch bu tabloya bakarak, her paketin hedef MAC adresini belirler ve doğrudan ilgili cihaza yönlendirir. Bu sayede, veri trafiği doğrudan hedeflenen cihaza iletilir, bu da ağ trafiğini daha etkili hale getirir.

Switch'in diğer önemli özelliği ise her portun bağımsız bir veri akışı sağlamasıdır. Yani her bir bağlı cihaz için ayrı bir veri yolu oluşturur. Bu, aynı anda farklı cihazlardan gelen veri akışlarının çakışmasını önler ve ağ performansını artırır.

Eğer switch'in MAC adres tablosunda hedef MAC adresi kayıtlı değilse, switch bu durumu broadcast yaparak çözer. Yani, veriyi tüm portlara ileterek, hedef cihazın MAC adresi tanımlandığında veriyi doğrudan ilgili port üzerinden iletebilir.

Switch, Hub'a benzerlik gösterse de, switch daha maliyetlidir çünkü MAC adresleri üzerinden hedef belirlerken, Hub ise genellikle IP adreslerini kullanır. Hub, veri iletiminde daha temel bir yaklaşım benimser ve ağ trafiğini yönetme yeteneği sınırlıdır. Switch'ler ise ağ trafiğini daha verimli ve güvenli bir şekilde yönetirler.

Şekil 3.1 : Switch

3.2 Hub

Ethernet Hub, temelde birden çok Ethernet çıkışı sağlayan ancak daha ilkel bir ağ cihazıdır. Hub, veri iletimini switch'e göre daha basit bir şekilde gerçekleştirir. Veri paketlerini aldığında, Hub bu paketleri tüm bağlı cihazlara eş zamanlı olarak ileterek iletişimi sağlar. Hub, bu işlemi genellikle ağdaki cihazların IP adresleri üzerinden yapar. Bu nedenle, Hub'un iletişimde daha temel bir yaklaşımı vardır ve veriyi hedef cihazların IP adreslerine göre değil, tüm cihazlara broadcast yaparak iletebilir.

Hub'un basit işlevselliği ve yapısı nedeniyle, ağ trafiği yönetimi switch'e göre daha sınırlıdır. Çünkü tüm cihazlara veriyi aynı anda ilettiği için, ağda çakışmalara ve bant genişliği sorunlarına neden olabilir. Ayrıca, Hub'un herhangi bir güvenlik veya veri yönlendirme yeteneği bulunmaz; veri paketlerini doğrudan tüm bağlı cihazlara ileterek, gizlilik ve güvenlik risklerini artırabilir.

Maliyet açısından da, Hub'lar genellikle daha ucuzdur ve basit ağ yapılarında kullanılabilirler. Ancak, switch'lerin yaygınlaşmasıyla Hub'ların kullanımı azalmıştır çünkü switch'ler daha akıllı ve verimli ağ iletişimi sağlarlar. Switch'ler, her bir port için bağımsız veri yolu sağlayarak ağ trafiğini daha iyi yönetir ve veriyi doğrudan hedef cihaza ileterek ağ performansını artırırlar.

Şekil 3.2 : Hub

3.3 Access Point

Access Point (AP), kablosuz iletişim ağlarında kullanılan ve kablolu ağa bağlı cihazların kablosuz ağa erişimini sağlayan bir ağ cihazıdır. Genellikle evlerde, işyerlerinde veya geniş alanlarda (campus, havaalanı gibi) kablosuz ağ kapsama alanını genişletmek ve kullanıcıların mobil cihazlarını internete bağlamak için kullanılır.

Access Point, kablolu ağ üzerinden aldığı veriyi kablosuz sinyallere dönüştürür ve bu sinyalleri kablosuz istemcilere (örneğin, dizüstü bilgisayarlar, akıllı telefonlar, tabletler) ileterek ağa erişimlerini sağlar. Aynı zamanda, Access Point, ağ güvenliğini sağlamak için çeşitli şifreleme protokolleri (WEP, WPA, WPA2 gibi) ve diğer güvenlik önlemlerini destekler.

Access Point'in çalışma prensibi, modem veya router gibi başka ağ cihazlarıyla işbirliği yaparak internet bağlantısını kablosuz cihazlara dağıtmasıdır. Bu sayede, ev veya işyerindeki kullanıcılar kablolu olmayan mobil cihazlarıyla da internete erişebilirler.

Access Point, genellikle yönetim arayüzü üzerinden yapılandırılabilir ve ağ yöneticileri tarafından ağ performansını izlemek ve yönetmek için kullanılır. Aynı zamanda, birden fazla Access Point kullanılarak büyük alanlarda (örneğin, bir kampüs veya otel) geniş kapsama alanı sağlanabilir ve kablosuz ağın güvenilirliği artırılabilir.

Şekil 3.3: Access Point

3.4 Firewall

Firewall (Güvenlik Duvarı), ağ güvenliği için kullanılan bir cihaz veya yazılımdır. Ağ trafiğini izleyerek, belirli protokoller, portlar veya IP adreslerine izin verilen veya yasaklanan trafiği filtreler. Bu sayede, ağı zararlı içeriklere karşı korur ve yetkisiz erişimleri engeller.

Firewall, ağın güvenlik mekanizmasının bir parçası olarak çalışır. Gelen ve giden veri paketlerini inceleyerek, potansiyel tehditler içeren paketleri tespit eder ve engeller. Belirli kurallara göre hareket eder; izin verilen paketlerin ağa iletilmesine izin verirken, kurallara uymayan ve risk oluşturan paketleri engeller.

Bu işlevleri sayesinde, Firewall ağın sınırlarını koruyarak, bilgisayarların ve ağ kaynaklarının güvenliğini sağlar. Örneğin, kötü niyetli yazılımların veya saldırı girişimlerinin ağa sızmalarını önler ve kullanıcıların güvenli bir çevrimiçi deneyim yaşamasını sağlar.

Ayrıca, Firewall'ün gelişmiş versiyonları, Intrusion Prevention System (IPS) gibi ek özelliklerle saldırıları tespit edip önler ve Virtual Private Network (VPN) gibi güvenli bağlantıları yönetme yetenekleri sunabilir.

Şekil 3.4: Firewall

3.5 Server

Server (Sunucu), ağdaki diğer cihazlara (istemcilere) hizmet veren ve genellikle özel görevler için yapılandırılmış olan bilgisayar sistemidir. Örneğin, dosya sunucuları, e-posta sunucuları, web sunucuları gibi farklı işlevlere sahip olabilirler. Sunucular, genellikle yüksek performans, güvenilirlik ve erişim kolaylığı sağlamak için özel olarak yapılandırılır.

Server, kullanıcıların istediği hizmetleri sunan bir dijital hizmet sağlayıcısı olarak düşünülebilir. Kullanıcı cihazlarından gelen isteklere duyarlılıkla cevap verir ve dosya depolama, veritabanı erişimi, web sayfalarını gönderme gibi görevleri başarıyla yerine getirir.

Bu merkezi bilgisayar veya yazılım, kullanıcı istemcilerine istedikleri bilgi ve hizmetleri sağlamak için tasarlanmıştır. Dosyaları saklar, veritabanlarına erişir, web sayfalarını ziyaretçilere sunar ve tüm bu işlemleri, ağın hizmet ihtiyaçlarını karşılamak adına kusursuz bir şekilde yerine getirir.

Server, ağ dünyasında önemli bir rol oynar; istemcilere hizmet sunmanın yanı sıra verileri korur ve ağ trafiğini düzenler. Bu yönüyle, server, ağın güvenliği ve verimliliği için kritik bir bileşen olarak kabul edilir.

Şekil 3.5: Server

3.6 Router

Router (Yönlendirici), farklı ağları birbirine bağlayan ve veri paketlerini bu ağlar arasında ileten bir ağ cihazıdır. Router, IP adresleri ve ağ segmentleri arasında iletim yapar, en uygun yolu seçer ve ağ trafiğini yönetir. Internet'e bağlı ağlarda, router'lar internete erişim sağlamak için kullanılır ve ağ güvenliğini korurlar.

Router, bilgisayar ağı üzerinde veri paketlerini yönlendiren önemli bir cihaz veya yazılımdır. Temel görevi, farklı ağlar arasında veri iletimini organize etmek ve bilgisayarlar arasındaki iletişimi düzenlemektir. Router'lar, ağ trafiğini etkili bir şekilde yönlendirerek, bilgisayarların birbirleriyle iletişim kurmasını, internete erişim sağlamasını ve veri transferini yönetmesini mümkün kılar.

Bu cihazlar, ağ topolojilerini birbirine bağlayarak, veri paketlerini doğru hedeflere yönlendirirler. Ayrıca, IP adresleri ve diğer ağ protokollerini kullanarak, verilerin güvenli ve düzenli bir şekilde iletilmesini sağlarlar. Router'lar, ağ yönetimi ve performans optimizasyonu açısından kritik bir rol oynarlar, çeşitli ağ segmentleri arasında veri transferini optimize ederek ağın verimli çalışmasını sağlarlar.

Şekil 3.6: Router

4. CİSCO PACKET TRACER'DA FARKLI AĞ TOPOLOJİLERİ

4.1 Ring (Halka Topolojisi)

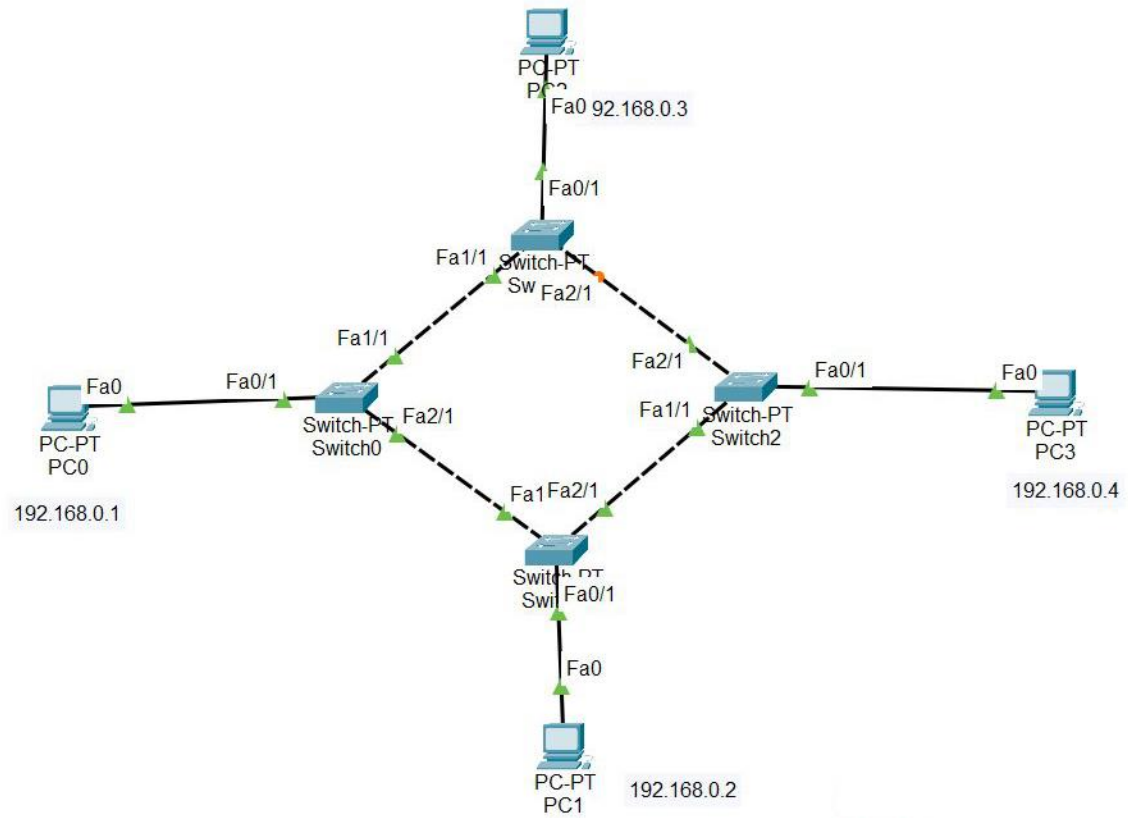
Ring topolojisi, bilgisayar ağlarında kullanılan ve her düğümün (cihazın) sadece iki komşusu olan bir yapıdır. Bu topolojide, her düğüm doğrudan komşularıyla bir bağlantı kurar ve bu bağlantılar halka şeklinde birleşerek bir döngü oluşturur. Veri iletimi için kullanılan iletişim yolu, bu halka üzerinde dolaşan veri paketleridir.

Her bir veri paketi, halka üzerinde sabit bir yönde dolaşır. Veri paketi, gönderildiği düğümün komşularından biri tarafından alınır ve hedefine doğru yönlendirilir. Eğer veri paketi hedef

düğüme ulaşmazsa veya hedefe ulaşana kadar döngü devam eder, bu durumda veri paketi halka üzerinde sürekli dolaşabilir.

Ring topolojisi, ağdaki her düğümün eşit yetkiye sahip olduğu ve iletişimin sürekli döngü halinde olduğu bir yapı sağlar. Bu sayede, her düğüm veri iletimine katılır ve veri paketleri hedefe ulaşana kadar halka üzerinde dolaşır. Ancak, bir düğüm arızalanırsa veya ağdaki döngü bozulursa, iletişimde kesinti olabilir ve ağın performansı etkilenebilir.

Ring topolojisi genellikle Token Ring protokolüyle ilişkilendirilmiştir, bu protokolde veri paketleri token adı verilen bir sıra üzerinde dolaşır ve yalnızca token sahibi düğüm veri iletimi yapabilir. Bu şekilde, çakışma (collision) sorunları önlenir ve ağdaki veri iletimi daha düzenli hale gelir.



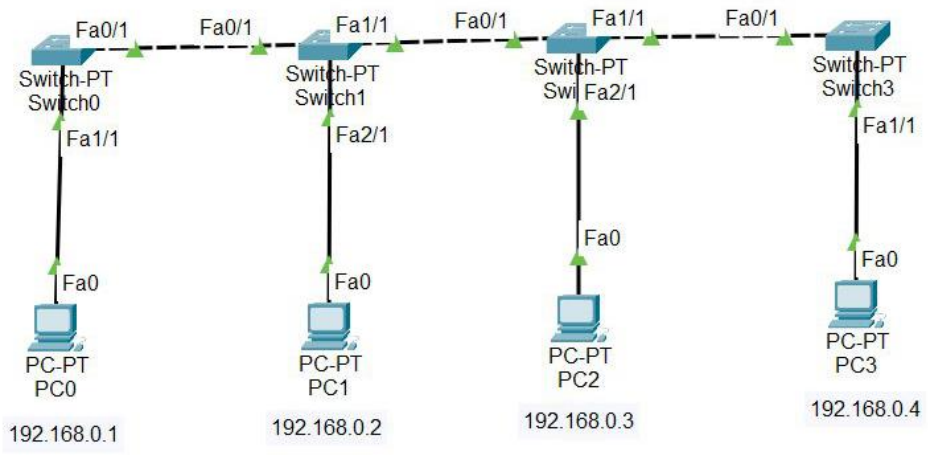
Şekil 4.1: Halka Topolojisi

4.2 Bus (Ortak Yol Topolojisi)

Bus topolojisi, bilgisayar ağlarında en eski ve temel topoloji yapılarından biridir. Bu yapıda, tüm cihazlar tek bir iletişim hattını paylaşırlar ve bu hat üzerinden iletişim kurarlar. Her bir cihaz, bu ortak iletişim hattına birer nokta bağlantısıyla katılır ve veri iletimi için bu hattı kullanır. Veri iletimi, gönderici cihaz tarafından iletişim hattına yerleştirilen veri paketleri aracılığıyla gerçekleşir. Bu paketler, hattın her noktasına yayılır ve hedef cihaz, veriyi alarak işler ve gerektiğinde yanıtını ileterek iletişimi tamamlar.

Bus topolojisinin en önemli avantajlarından biri, kolay kurulum ve düşük maliyetidir. Tek bir iletişim hattının kullanılması, ağın donanım maliyetlerini ve kurulum zamanını azaltır. Ayrıca, yeni cihazların ağa eklenmesi veya mevcut cihazların yer değiştirmesi bu yapıda pratiktir. Bununla birlikte, iletişim hattında herhangi bir arıza durumunda ciddi sorunlar ortaya çıkabilir. Çünkü tüm cihazlar aynı iletişim hattını paylaştığı için, hattın herhangi bir noktasındaki bir arıza, ağın tamamını etkileyebilir ve iletişim kesintisine yol açabilir.

Bu topoloji genellikle küçük ve orta ölçekli ağlar için uygundur. Ancak ağdaki cihaz sayısı arttıkça iletişim performansı ve veri güvenliği gibi konularda zorluklar ortaya çıkabilir. Özellikle büyük ölçekli ağlarda, iletişim hattının bant genişliği paylaşımı ve veri çakışmaları gibi sorunlar daha sık görülebilir. Bu nedenle, büyük ve karmaşık ağ yapıları için daha gelişmiş topoloji çözümleri tercih edilebilir.



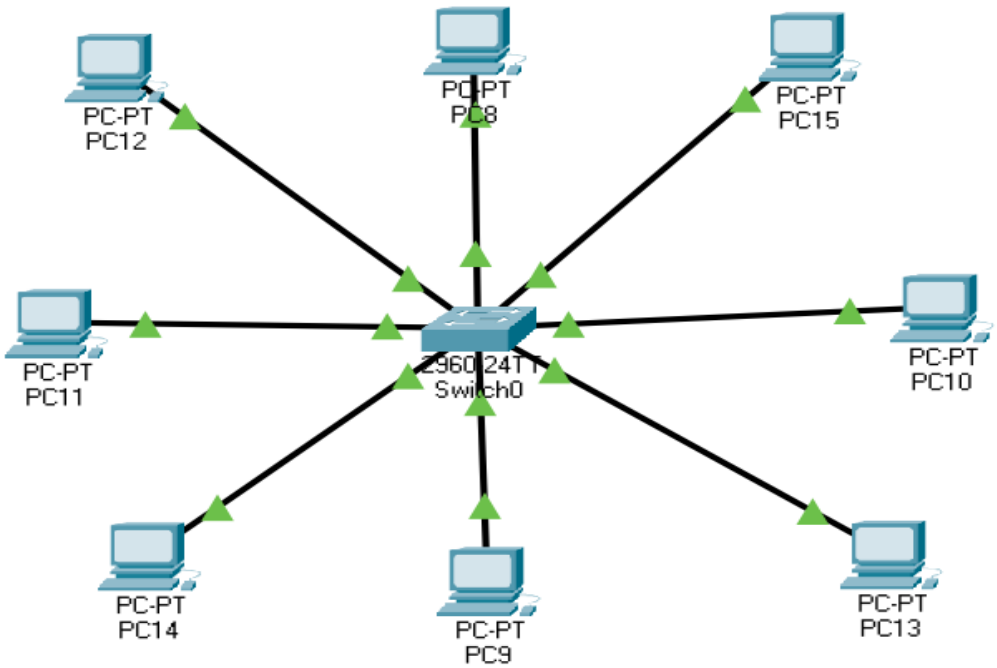
Şekil 4.2: Ortak Yol Topolojisi

4.3 Star (Yıldız Topolojisi)

Star topolojisi, bilgisayar ağlarında yaygın olarak kullanılan ve merkezi bir noktada (çoğunlukla bir switch veya hub) bulunan tüm cihazların bu merkezi noktaya bağlı olduğu bir yapıdır. Her bir cihaz, kendi kendine merkezi noktaya noktadan noktaya bağlantı yapar. Bu bağlantılar genellikle Ethernet kablosu veya kablosuz bağlantılar aracılığıyla sağlanabilir. Her cihaz, merkezi noktaya bağlı olduğu için, veri iletimi doğrudan merkezi noktaya gönderilir ve merkezi nokta, veriyi doğru hedefe yönlendirir.

Star topolojisi, güçlü merkezi yönetim özellikleri sunar. Merkezi switch veya hub, ağ trafiğini yönetir ve veri iletimini düzenler. Bu yapı, ağ yöneticilerine kolaylıkla ağ trafiğini izleme, yönetme ve güvenlik önlemleri uygulama imkanı tanır. Ayrıca, ağa yeni cihazlar eklemek veya mevcut cihazları yeniden yapılandırmak da oldukça basittir, çünkü her cihaz doğrudan merkezi noktaya bağlıdır ve bu nokta üzerinden iletişim kurar.

Star topolojisi, genişletilebilirlik açısından da avantajlıdır. Ağa yeni cihazlar eklendiğinde veya ağdaki yapı değiştirildiğinde, sadece merkezi noktaya yeni bir bağlantı eklenmesi yeterlidir. Bu yapı, özellikle büyük ağlarda ve kurumsal ortamlarda tercih edilir, çünkü ağın büyümesi ve değişiklikleri kolayca yönetilebilir.



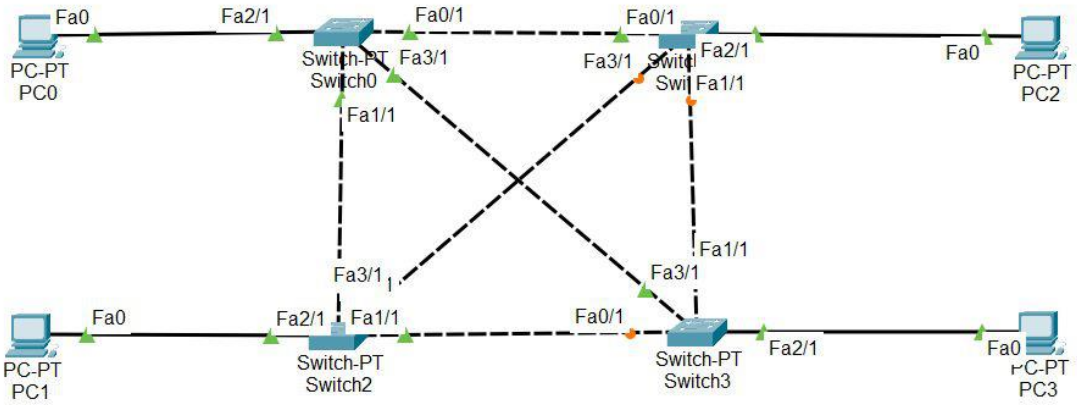
Şekil 4.3: Yıldız Topolojisi

4.4 Mesh (Örgü Topolojisi)

Mesh topolojisi, bilgisayar ağlarında kullanılan bir yapı olup, her cihazın diğer tüm cihazlarla doğrudan bağlantıya sahip olduğu bir yapıdır. Bu durum, her cihazın birden fazla yol seçeneği ile veri iletimi sağlayabileceği anlamına gelir. Herhangi bir cihazdan gönderilen veri, doğrudan hedefe ulaşmak için birden fazla yol üzerinden iletilir. Bu çoklu yol seçenekleri, ağın esnekliğini artırır ve iletişim güvenilirliğini sağlar. Tek bir bağlantı noktasının arızalanması durumunda, diğer bağlantılar devreye girerek iletişimin kesintisiz olarak sürmesini sağlar.

Mesh topolojisi, özellikle yüksek güvenilirlik gerektiren ağ ortamlarında tercih edilir. Her cihazın diğer cihazlarla doğrudan bağlantıya sahip olması, veri iletimi sırasında tek bir noktanın arızalanmasının ağ performansını veya iletişimi olumsuz etkilemesini önler. Bu yapı, kritik ağ uygulamaları için idealdir, çünkü iletişimin kesintisiz ve güvenilir olması büyük önem taşır, örneğin finansal işlemler veya sağlık hizmetleri gibi alanlarda.

Ancak, Mesh topolojisinin bazı dezavantajları da vardır. Öncelikle, bu yapıdaki her cihazın diğer tüm cihazlarla doğrudan bağlantıya sahip olması, kurulum ve yönetim kompleksliğini artırır. Ağdaki her yeni cihazın diğer tüm cihazlarla bağlantı kurması gerektiği için, büyük ölçekli ağlarda yönetim zorlukları ve maliyet artışı yaşanabilir. Ayrıca, her cihaz için gereken bağlantı noktaları ve kablolama miktarı da maliyeti artırabilir.



Şekil 4.4: Örgü Topolojisi

5. CİSCO PACKET TRACER LAN KURULUMU

5.1 Bilgisayarların IPv4 Adreslerinin Girilmesi

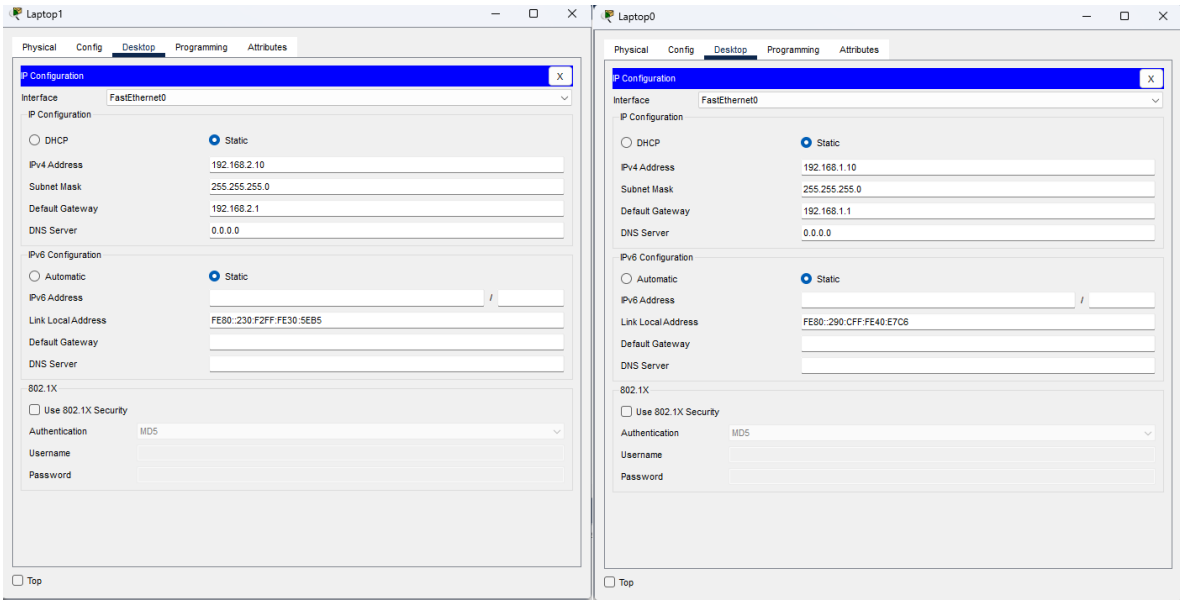
LAN kurulumu sürecinde, bilgisayarların IPv4 adreslerinin doğru ve düzenli bir şekilde atanması, ağın düzgün çalışması için temel gereksinimlerden biridir. IPv4 adresi, bir bilgisayarın ağ üzerinde tanınmasını ve diğer cihazlarla iletişim kurmasını sağlar. Cisco Packet Tracer kullanılarak yapılan bu işlem, birkaç aşamadan oluşur ve her adım dikkatle takip edilmelidir.

Öncelikle, ağın genel adresleme planı oluşturulmalıdır. Bu plan, ağda bulunan her cihaz için benzersiz bir IPv4 adresi sağlar. Adresleme planı, genellikle ağın büyüklüğüne ve yapısına göre belirlenir. Örneğin, küçük bir ağda basit bir adresleme planı kullanılabilirken, büyük ve karmaşık ağlarda daha detaylı bir plan gerekebilir. Adresleme planı oluşturulurken, her cihazın belirli bir IP aralığında yer almasına dikkat edilmelidir. Örneğin, ağda kullanılan bilgisayarlar için 192.168.1.0/24 IP aralığı kullanılabilir.

Bilgisayarların IPv4 adreslerinin girilmesi, Cisco Packet Tracer yazılımı üzerinden gerçekleştirilir. İlk olarak, IP adresi atanacak bilgisayar seçilir. Packet Tracer arayüzünde, bilgisayara tıklanarak "Desktop" sekmesine geçilir ve "IP Configuration" seçeneği seçilir. Bu pencerede, bilgisayar için belirlenen IPv4 adresi ve alt ağ maskesi girilir. Alt ağ maskesi, ağın hangi kısmının ağ adresi ve hangi kısmının cihaz adresi olduğunu belirtir. Genellikle, küçük ağlarda 255.255.255.0 (veya /24) alt ağ maskesi kullanılır.

IPv4 adresinin yanı sıra, varsayılan ağ geçidi (default gateway) ve DNS sunucusu adresleri de girilmelidir. Varsayılan ağ geçidi, bilgisayarın kendi alt ağı dışındaki ağlara nasıl erişeceğini belirler. DNS sunucusu adresi ise, alan adlarını IP adreslerine çeviren sunucunun adresidir. Bu bilgiler de "IP Configuration" penceresinde ilgili alanlara girilir.

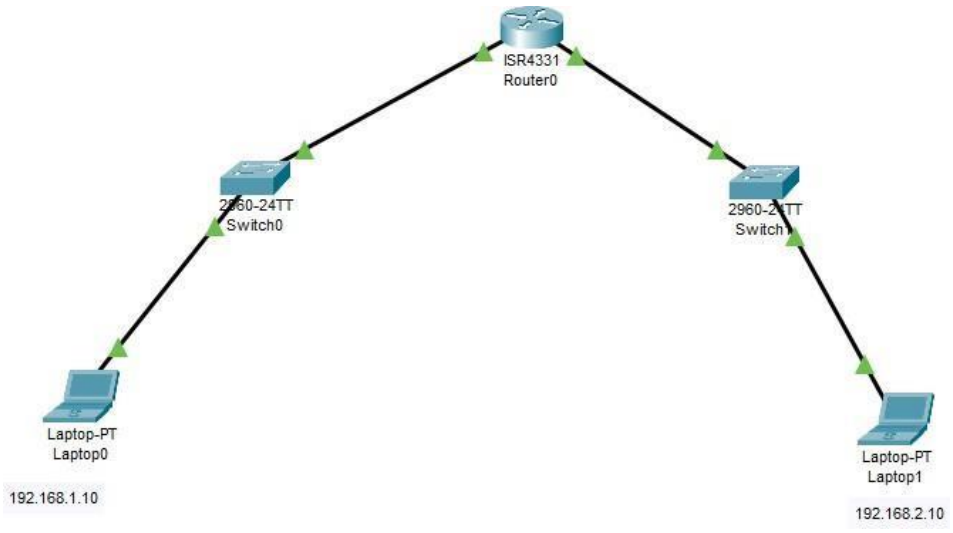
Ayarlamalar tamamlandıktan sonra, yapılan değişiklikler kaydedilir ve pencere kapatılır. Bu işlem, ağdaki her bilgisayar için tekrarlanarak tüm cihazların doğru IPv4 adresleriyle konfigüre edilmesi sağlanır. Bu şekilde, ağ üzerindeki tüm cihazlar arasında sorunsuz bir iletişim kurulmuş olur. Ayrıca, doğru adresleme, ağ trafiğinin yönetimini ve sorun giderme işlemlerini de kolaylaştırır.



Şekil 5.1: IPv4 Adreslerinin Girilmesi

6. ROUTER CİHAZININ YAPILANDIRILMASI

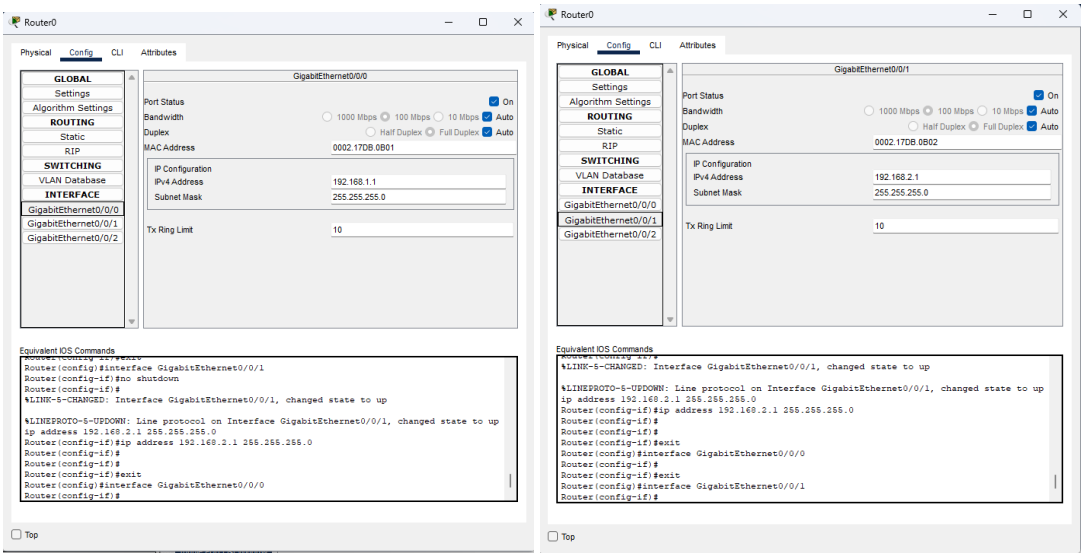
Router cihazının yapılandırılması, bir ağın verimli ve güvenli bir şekilde çalışabilmesi için kritik bir adımdır. Router, farklı ağları birbirine bağlayan ve veri paketlerinin doğru yöne yönlendirilmesini sağlayan bir cihazdır. Cisco Packet Tracer kullanılarak bir router'ın yapılandırılması birkaç temel adımdan oluşur.



Şekil 6.1 Router Yapılandırılması

6.1 Router'ın Temel Yapılandırılması

Router'ın temel yapılandırması, cihazın temel işlevlerini yerine getirebilmesi için gerekli olan ayarların yapılmasını içerir. Bu adımlar genellikle router'ın ilk kurulum aşamasında gerçekleştirilir ve ağın sorunsuz bir şekilde çalışmasını sağlamak için kritik öneme sahiptir.



Şekil 6.2: Router'ın Temel Yapılandırılması

6.1.1 Hostname ve Şifre Ayarları

İlk adım olarak, router'ın hostname ve şifre ayarları yapılır. Hostname, router'ı ağ üzerinde tanımlamak için kullanılan bir isimdir. Şifreler ise, router'a yetkisiz erişimi engellemek için kullanılır. Bu ayarlar, router'ın komut satırı arayüzü (CLI) üzerinden yapılır.

6.1.2 IP Adreslerinin Atanması

Router üzerindeki her arayüz için benzersiz bir IP adresi atanmalıdır. Bu IP adresleri, router'ın diğer ağ cihazlarıyla iletişim kurabilmesi için gereklidir. Her arayüz, bağlı olduğu ağ segmentine uygun bir IP adresi alır. Bu işlem, CLI üzerinden gerçekleştirilir.

6.1.3 Routing Protokollerinin Yapılandırılması

Router'lar, veri paketlerinin doğru yöne yönlendirilmesi için routing protokollerini kullanır. En yaygın kullanılan routing protokollerinden bazıları OSPF, EIGRP ve RIP'tir. Bu protokoller, router'ın ağ topolojisini öğrenmesini ve veri trafiğini en verimli şekilde yönlendirmesini sağlar.

6.2 Router'ın Güvenlik Ayarları

Router'lar, ağın güvenliğini sağlamak için çeşitli güvenlik önlemleriyle yapılandırılmalıdır. Bu güvenlik ayarları, yetkisiz erişimi engellemeye ve ağın bütünlüğünü korumaya yönelik olarak yapılır.

6.2.1 Access Control Lists (ACLs)

Access Control Lists (ACLs), router üzerinden geçen veri trafiğini kontrol etmek için kullanılır. ACL'ler, belirli IP adreslerine veya adres aralıklarına yönelik erişim izinleri ve kısıtlamaları tanımlar. Bu sayede, ağ üzerindeki belirli kaynaklara sadece yetkili cihazların erişimi sağlanır.

6.2.2 Şifreleme ve VPN Ayarları

Router'lar, ağ üzerindeki verilerin güvenli bir şekilde iletilmesini sağlamak için şifreleme yöntemlerini ve VPN (Virtual Private Network) yapılandırmalarını kullanabilir. VPN'ler, uzak ağlar arasında güvenli bir iletişim kanalı oluşturur. Bu ayarlar, router'ın CLI üzerinden yapılır.

6.3 Router'ın İleri Seviye Yapılandırmaları

Router'ın ileri seviye yapılandırmaları, daha karmaşık ağ gereksinimlerini karşılamak için gerçekleştirilir. Bu yapılandırmalar, ağın performansını artırmak ve yönetimini kolaylaştırmak amacıyla yapılır.

6.3.1 QoS (Quality of Service)

QoS, ağ trafiğinin önceliklendirilmesi ve bant genişliğinin etkin bir şekilde yönetilmesi için kullanılan bir teknolojidir. QoS ayarları, belirli veri türlerinin (örneğin, ses veya video trafiği) öncelikli olarak iletilmesini sağlar. Bu ayarlar, ağ performansını ve kullanıcı deneyimini iyileştirebilir.

6.3.2 NAT (Network Address Translation)

NAT, özel IP adreslerini genel IP adreslerine dönüştürerek, ağ üzerindeki cihazların internet erişimini sağlar. Bu özellik, IP adreslerinin etkin kullanımını sağlar ve ağ güvenliğini artırır. NAT ayarları, router'ın CLI üzerinden yapılandırılır.

6.3.3 VLAN (Virtual Local Area Network)

VLAN'lar, fiziksel olarak aynı ağda bulunan cihazları sanal olarak farklı ağ segmentlerine ayırmak için kullanılır. Bu özellik, ağ trafiğini daha etkin yönetmeyi ve güvenliği artırmayı sağlar. VLAN yapılandırmaları, router ve switch cihazlarında yapılabilir.

7. CMD ARACILIĞIYLA PİNG TESTİ

Ağ bağlantılarının doğrulanması ve iletişim sorunlarının tespit edilmesi için en yaygın kullanılan yöntemlerden biri, Command Prompt (CMD) üzerinden yapılan ping testidir. Ping testi, bir cihazın başka bir cihazla iletişim kurup kuramayacağını belirlemek amacıyla, belirli bir IP adresine ICMP (Internet Control Message Protocol) ECHO_REQUEST paketleri gönderir ve bu paketlere gelen yanıtları değerlendirir.

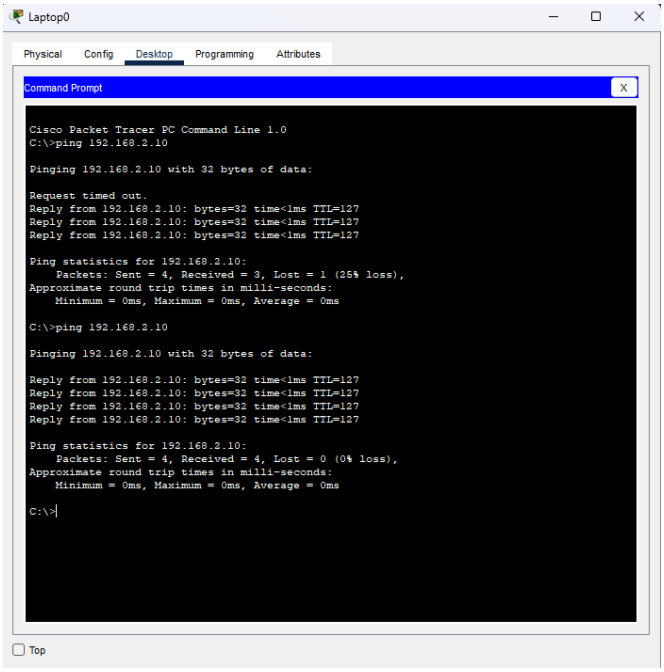
7.1 Ping Testinin Adımları

1 - CMD Penceresinin Açılması:

CMD (Command Prompt) penceresi açılarak ping testine başlanır. Windows işletim sisteminde, başlat menüsünden "cmd" veya "Command Prompt" yazılarak arama yapılır ve uygulama çalıştırılır.

2 - Ping Komutunun Girilmesi:

CMD penceresi açıldığında, test edilecek IP adresine ping komutu gönderilir. Örneğin, "ping 192.168.2.10" komutu girilir. Bu komut, 192.168.2.10 IP adresine 32 baytlık veri paketleri gönderir ve yanıtları bekler.



Şekil 7.1: Ping Testi

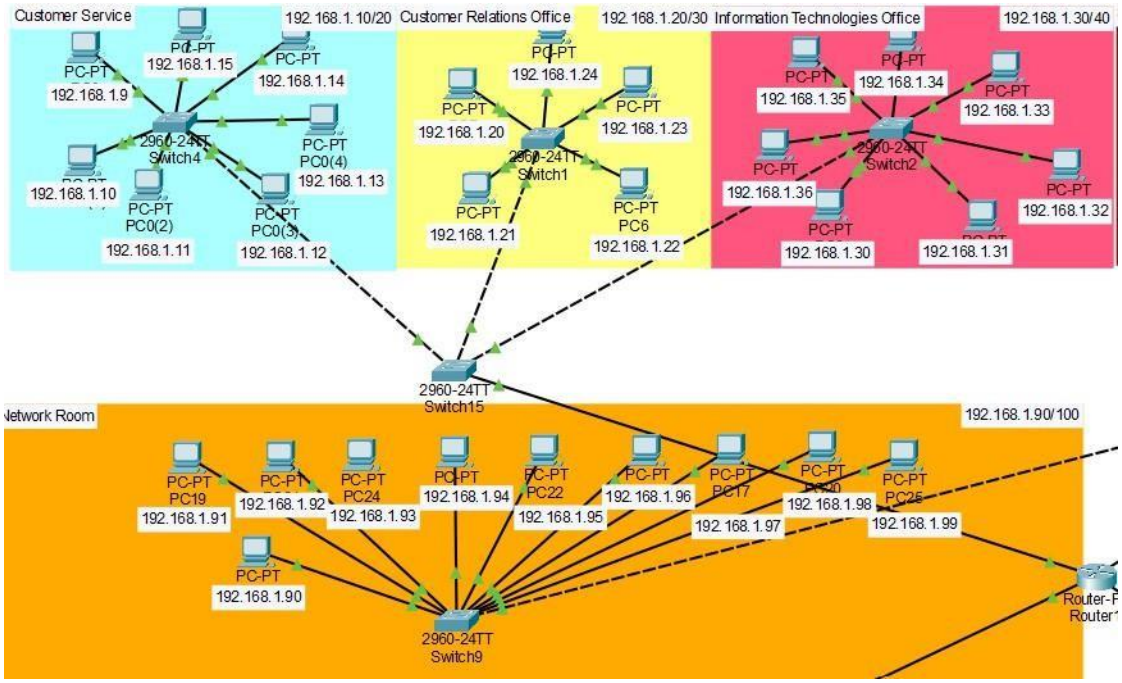
7.2 Ping Testinin Önemi

Ping testi, ağ bağlantılarının durumunu hızlı ve etkili bir şekilde değerlendirmek için kullanışlı bir araçtır. Bir cihazın ağ üzerindeki diğer cihazlarla iletişim kurabilme yeteneğini doğrulamak ve bağlantı sorunlarını tanımlamak için sıkça kullanılır. Bu test, özellikle ağ yapılandırmaları sonrasında veya bağlantı sorunları yaşandığında ilk kontrol adımı olarak tercih edilir.

8. DEVLET BİNASI GÜVENLİK ve PERFORMANS YÖNETİMİ

Devlet binasının network altyapısı son derece kritik ve güvenlik odaklıdır. Bu nedenle, ağ yöneticileri ve sistem uzmanları, ağın güvenliği ve performans yönetimi için bir dizi önlemler almalıdır. Devlet binası içinde kullanılan kablosuz ağlar güçlü şifreleme ve doğrulama yöntemleri ile korunmalıdır. Ayrıca, konuk kullanıcılar için izole edilmiş bir misafir ağı oluşturularak, güvenlik riskleri en aza indirilmelidir.

Personel Eğitimi: Ağ kullanıcıları ve yöneticileri, güvenlik politikaları ve ağ kullanımı konusunda düzenli eğitimlere tabi tutulmalıdır. Bilinçli kullanıcılar, güvenlik risklerini en aza indirmeye yardımcı olabilir.

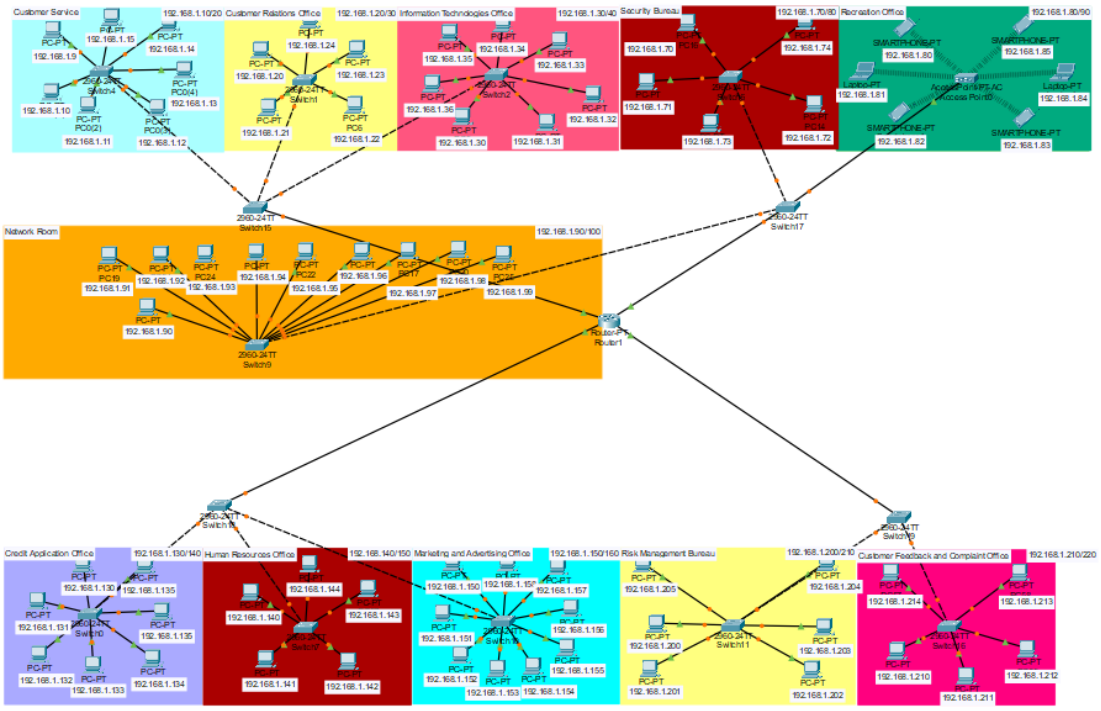


Şekil 8.1: Customer Service

Görselde belirtilen 'Customer Service', 'Customer Relations Office' ve 'Information Technologies Office' ağları, tek bir switch cihazına bağlanmıştır. Topolojilerdeki bilgisayarlara IP adresleri ve Varsayılan Ağ Geçidi (Default Gateway) adresleri atanmış ve bu bilgisayarlar alt ağlara bölünmüştür. Projede yer alan diğer iki veya üç ağda olduğu gibi, bu ağlar da tek bir switch cihazına bağlanmakta ve ardından ortak bir router'a yönlendirilmektedir.

Ağ Geliştiricisi, bilgisayarların altlarında bulunan IPv4 adreslerini tek tek atayarak bir IP havuzu oluşturur. Daha sonra, Devlet Binasının her bölümü için ayrı ayrı Varsayılan Ağ Geçidi (Default Gateway) adresleri atar. Bu atamalar, yukarıda belirtildiği şekilde gerçekleştirilir.

Bu adımlardan sonra, LAN bağlantılarının Varsayılan Ağ Geçidi (Gateway) adresleri, bağlı oldukları portun IPv4 bölümüne yazılır.



Şekil 8.2: Cihaz Ağları

8.1 Ağ Yapılandırması ve IP Subnetting İşlemi

Ağlar, genellikle bir Router üzerinden farklı alt ağlara bölünmüş şekilde yapılandırılarak ağ trafiğinin etkili bir biçimde kontrol edilmesi sağlanmaktadır. Bu tür karmaşık ağ sistemlerinde, IP Subnetting işlemi kullanılarak veri trafiğinin düzenli bir şekilde yönlendirilmesi ve yönetilmesi hedeflenir. IP Subnetting, bir IP adresi bloğunu daha küçük alt ağlara bölerek ağ yönetimini ve performansını iyileştirmeyi amaçlayan bir tekniktir.

Bu ağda, toplamda 46 adet kablolu ağ cihazı ve 6 adet kablosuz ağ cihazı bulunmaktadır. Kablolu ağ cihazları, fiziksel bağlantı üzerinden veri iletimi gerçekleştiren cihazlardır ve genellikle ağ performansının artırılması için tercih edilir. Kablosuz ağ cihazları ise, radyo dalgaları üzerinden veri iletimini sağlar ve ağın esnekliğini artırır. Kablolu ve kablosuz ağ cihazlarının her biri, ağ üzerinde farklı fonksiyonlara hizmet eder ve belirli alt ağ yapılandırmalarına ihtiyaç duyar.

Bu bağlamda, her alt ağa farklı bir varsayılan ağ geçidi (gateway) adresi tanımlamak yerine, Router'dan ilk Switch'lere farklı gateway adresleri atanmış, aynı Switch'e bağlı olan farklı LAN bağlantıları ise aynı Gateway adresini kullanacak şekilde yapılandırılmıştır. Bu yaklaşım, ağın yönetimini daha basit hale getirirken, aynı zamanda ağ trafiğinin verimli bir şekilde yönlendirilmesini sağlar.

Ayrıca, her bilgisayarın 11 farklı alt ağa sahip olduğu bu yapılandırmada, her alt ağ için 255.255.255.192 subnet maskesi kullanılmıştır. Bu subnet maskesi, her bir alt ağda toplam 62 kullanılabilir IP adresi sağlayarak, her alt ağda 62 cihazın birbirleriyle iletişim kurmasını mümkün kılar. IP Subnetting işlemi ile, ağ adresi 192.168.1.0/26 gibi bir biçimde yapılandırılmıştır, burada /26 ifadesi 26 bitlik ağ bölümünü ve kalan 6 biti ise cihaz adresleri için ayırır.

Bu yöntemle, her alt ağ kendi IP adres aralığına sahip olur ve Router üzerinden her alt ağ için ayrı bir gateway tanımlanarak ağ trafiği daha etkin bir şekilde yönetilir. Router, her alt ağ arasındaki veri paketlerini yönlendirerek ağ trafiğinin düzgün bir şekilde bağlanmasını ve yönlendirilmesini sağlar.

8.2 IP Subnetting ve Ağ Yönetimi

IP Subnetting, IP adresi bloğunu daha küçük alt ağlara bölerek ağ kaynaklarının etkin bir şekilde yönetilmesini sağlar. Bu işlem, ağ trafiğinin yönlendirilmesi, güvenliğinin sağlanması ve performansının iyileştirilmesi amacıyla gerçekleştirilir. Ağ yöneticileri, bu yapılandırma sayesinde IP adresi kaynaklarını daha verimli kullanabilir ve ağ üzerinde farklı alt ağlar oluşturabilir.

Subnet maskesi, IP Subnetting işleminin temel bileşenlerinden biridir ve her alt ağ için IP adreslerini tanımlayan bir şemayı belirler. Örneğin, 255.255.255.192 subnet maskesi, 64 IP adresini kapsayan alt ağlar oluşturur ve bu alt ağlar 62 kullanılabilir IP adresi sunar. Bu yapılandırma, özellikle geniş ağlarda IP adresi yönetimini daha etkin hale getirir.

Router ve Switch konfigürasyonları, ağ trafiğinin yönetimi ve güvenliğinin sağlanması açısından kritik bir rol oynar. Router'lar, farklı alt ağlar arasında veri trafiğini yönlendirirken, Switch'ler ağ içinde cihazlar arasındaki veri iletimini gerçekleştirir. Her bir Switch için belirlenen gateway adresleri, ağ üzerindeki veri iletimini kolaylaştırırken, her alt ağ için yapılan yapılandırmalar ağın genel performansını iyileştirir.

Ağ yönetiminde kullanılan bu teknikler, ağ tasarımı ve yapılandırması açısından kapsamlı bir anlayış gerektirir. IP Subnetting, ağ yöneticilerine, ağ altyapısının daha verimli bir şekilde tasarlanması ve yönetilmesi için gerekli araçları sunar, böylece ağ performansı ve güvenliği artırılır.

9. KAYNAKÇA

www.netacad.com

www.cisco.com/c/en/us/support/index.html

https://en.wikipedia.org/wiki/Router_(computing)

https://tr.wikipedia.org/wiki/Sunucu_(bili%C5%9Fim)

https://www.geeksforgeeks.org/what-is-cisco-packet-tracer/

https://www.techtarget.com/searchnetworking/definition/hub

https://www.techtarget.com/searchnetworking/definition/switch

www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780136632375

www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-2-9780136632375

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

https://www.juniper.net/us/en/research-topics/what-is-an-access-point-in-networking.html