Bu proje Avrupa Birliği ve Türkiye Cumhuriyeti Tarafından finanse edilmektedir.

AĞ TASARIMI VE İLETİŞİM TEKNOLOJİLERİ

İKG PRO İNSAN KAYNAKLARININ GELİŞTİRİLMESİ PROGRAM OTORİTESİ

İŞKUR

ÇSGB T.C. ÇALIŞMA VE SOSYAL GÜVENLİK BAKANLIĞI

KOCAELİ

2016

İZMİT MESLEKİ VE TEKNİK ANADOLU LİSESİ

KOCAELİ BÜYÜKŞEHİR BELEDİYESİ

KOCAELİ SANAYİ ODASI KOCAELİ CHAMBER OF INDUSTRY

- **Bu yayın Avrupa Birliğinin Mali desteğiyle hazırlanmıştır. Yayının içeriğinden yalnız Kocaeli Büyükşehir Belediyesi sorumlu olup, hiçbir şekilde Avrupa Birliğinin görüşlerini yansıtmamaktadır.**
- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Çalışma ve Sosyal Güvenlik Bakanlığı, Sektörel Yatırım Alanlarında Genç İstihdamın Desteklenmesi Programı kapsamında gerçekleştirilen FİBER KOCAELİ (Kocaeli Ağ ve Fiber Optik Uzmanı Eğitim Merkezi) Projesi kapsamında ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

KOCAELİ

2016

İÇİNDEKİLER

AÇIKLAMALAR

ALAN	Bilişim Teknolojileri
DAL/MESLEK	Ağ İşletmenliği
MODÜLÜN ADI	Ağ Tasarımı ve İletişim Teknolojileri
MODÜLÜN TANIMI	Bu modül; Ağ referans modelleri, taşıma ve uygulama katmanındaki protokolleri kullanma becerilerini, ağ sistemlerinin tasarımı, simülasyonunu ve yönlendiricileri yöneterek yönlendirme işlemlerini yapabilmesi ile ilgili bilgi ve becerilerle ağ üzerinde onarım ve hata giderme işlemlerinin nasıl yapılacağı ile ilgili bilgi ve becerileri kapsar.
SÜRE	40 / 32
ÖN KOŞUL	Bu modül için Ağ Temelleri Modülünü tamamlamış olmak gerekmektedir.
YETERLİK	İhtiyaca uygun ağ yapısını simüle ederek yönlendirme yapmak
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığında, haberleşme sistemlerinde kullanılan yönlendirme teknolojileri, araçları ve kullanım özelliklerini bileceksiniz. **Amaçlar** 1. Taşıma ve Uygulama katmanı protokollerini kullanabileceksiniz. 2. Ağ referans modellerindeki katmanlar arasındaki ilişkiyi açıklayabileceksiniz 3. Simülasyon programını kullanabileceksiniz. 4. LAN ve WAN simülasyonu yapabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam** Bilişim Teknolojileri laboratuvarı, işletme, kütüphane, ev, Bilgi Teknolojileri ortamı, saha vb. **Donanım** Akıllı tahta, projeksiyon, bilgisayar, modem, switch, router, ağ kartı, erişim noktası, sanal ağ yazılımları
ÖLÇME VE DEĞERLENDİRME	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.

GİRİŞ

Sevgili Öğrenciler,

Bilgisayarların günümüzde hayatımıza yaptığı katkıların önemi yadsınamaz. Daha doğmamış bir bebekten – ölünceye kadar doğrudan ya da dolaylı olarak neredeyse bütün insanlar kullanmaktadır.

Günümüzde bilgisayar ve diğer tüm bilişim cihazlarının vazgeçilmez iletişim platformu internet ise bütün dünyayı kapsayan büyük bir ağdır.

Bugün ister kablolu ister kablosuz ister mobil araçlar vasıtasıyla olsun iletişim sağlamak için kullandığımız ağların yapısını anlamak, bu ağları tasarlamak ve yönetmek günümüzün önemli ihtiyaçlarındandır.

Bu modülümüzde Simülasyon programları kullanarak Ağ tasarımı yapmayı, ihtiyaca uygun ağ çözümleri bulmayı, yönlendirme mantığını anlayarak ve sistemimizde kullanmayı öğreneceğiz.

ÖĞRENME FAALİYETİ–1

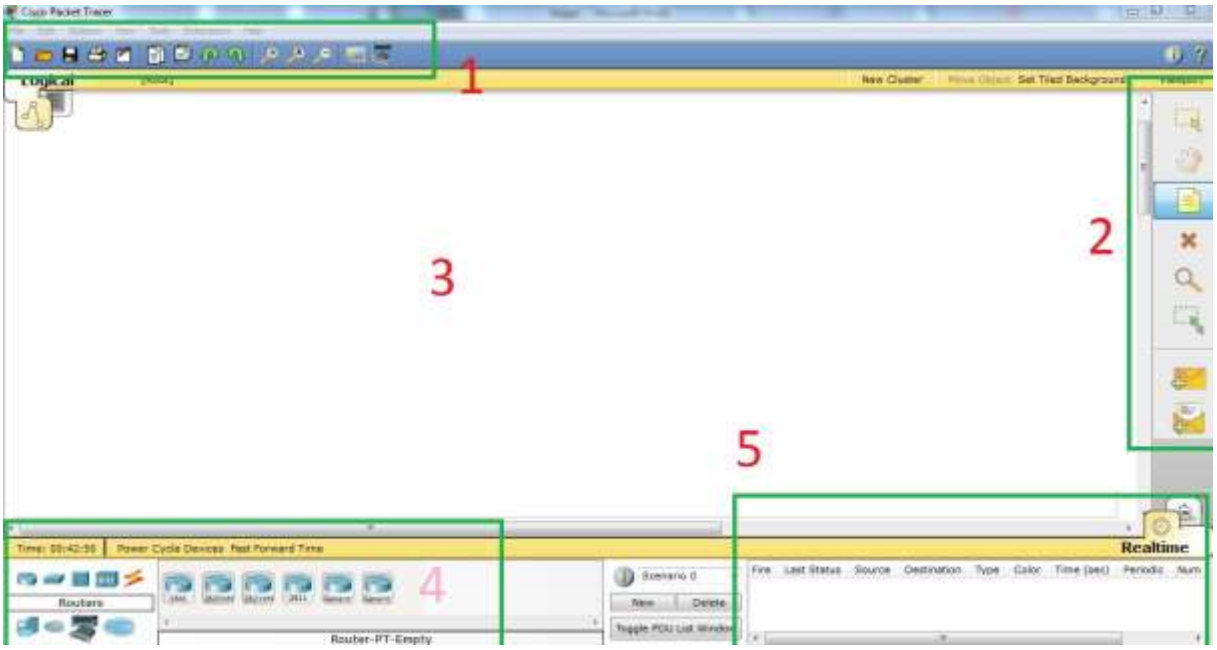
AMAÇ

Bilgisayar laboratuvarında uygun şartlar sağlandığında ağ simülasyon yazılımını kullanabileceksiniz.

ARAŞTIRMA

Ağ simülasyon işlemleri için kullanılan programların isimlerinin neler olduğunu ve ağ tasarım sürecinde dikkat edilmesi gereken hususları araştırınız.

1. PAKET TRACER Genel Bakış



Programı açtığınız zaman basit ara yüzü bulunmaktadır.

İşaretli olan 1. alan da klasik her Windows uygulamasının da olan File,Edit.. vb. sekmeler bulunmaktadır. İçeriklerine bakıldığında basit karmaşık olmayan yardımcı özelliklerdir.

İşaretli olan 2. kısımda ise yukarıdan aşağıya bahsetmek gerekirse, ilk başta olan kısım çalışma alanımıza koymuş olduğumuz network elemanlarını veya simgeleri seçmemizi sağlar. İkincisi (El işareti olan) gene çalışma alanına koyduğumuz network elemanlarını tek tek seçmemizi sağlar. 3. Kısımda ise not eklememizi sağlar. X simgesi seçilen elemanı silmemizi, büyüteç olan yakınlaştırmayı sağlar, büyütecin altında olan da büyüteç ile büyütülmüş çalışma alanının tekrar eski haline dönmesini sağlar. Onun altında bulunan iki tane mektup resmi ise paket gönderilmesini sağlar. Oluşturmuş olduğunuz ağ doğru çalışıyor mu kontrol amaçlı yani ping atma işlemidir. İlerde bahsedeceğiz ama CLI (Command Line Interface) kısmından ping komutunu çalıştırabilirsiniz.

İşaretli 3. Kısım ise bizim çalışma (oyun) alanımızdır.

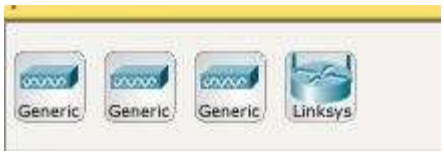
İşaretli 4. Kısım ise,

Routerlar,

Switchler,

Hublar,

Wireless Devices,

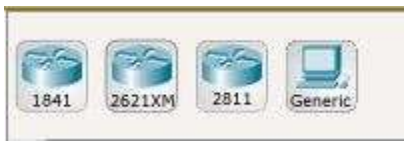


Kablolar,

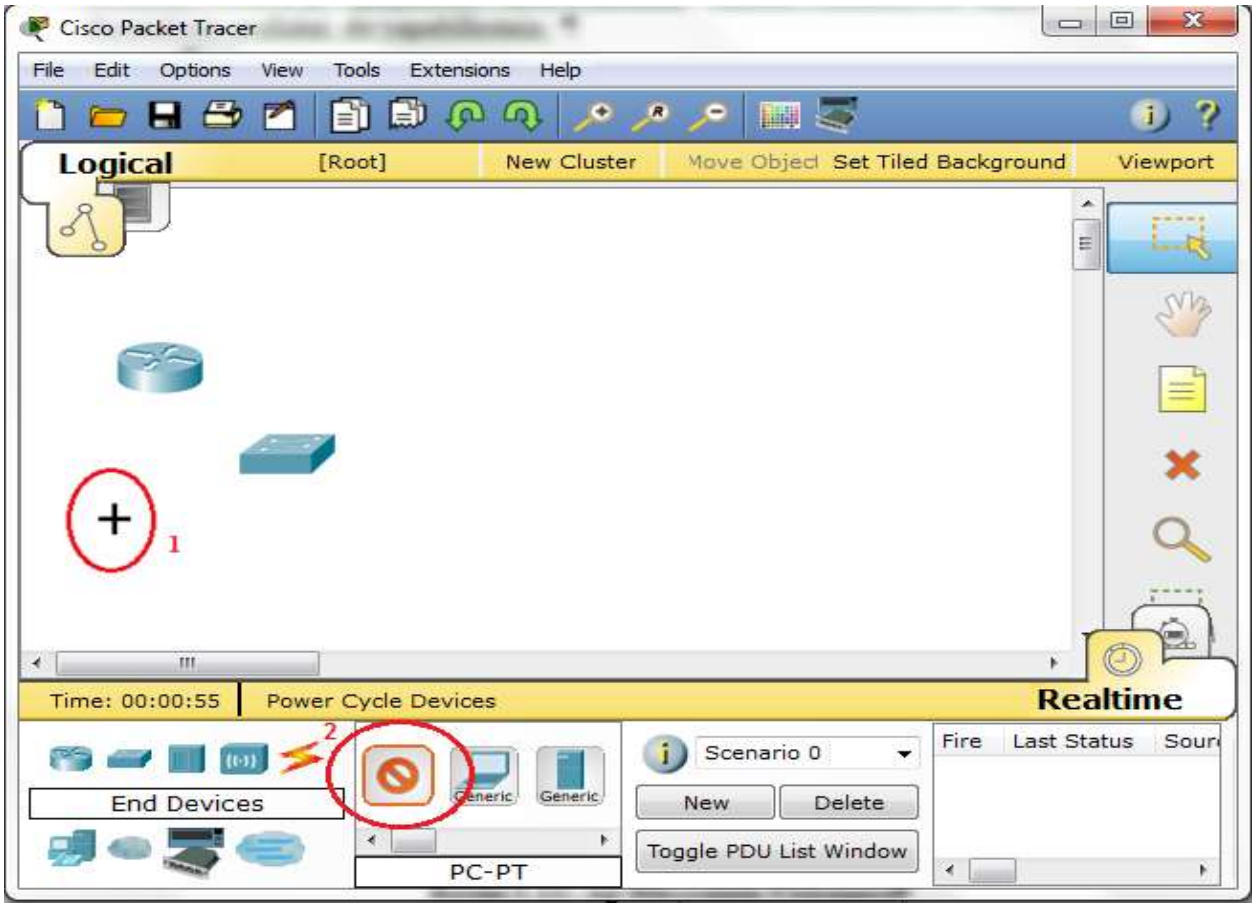
End Devices,

WAN Emulation

Custome Made Devices

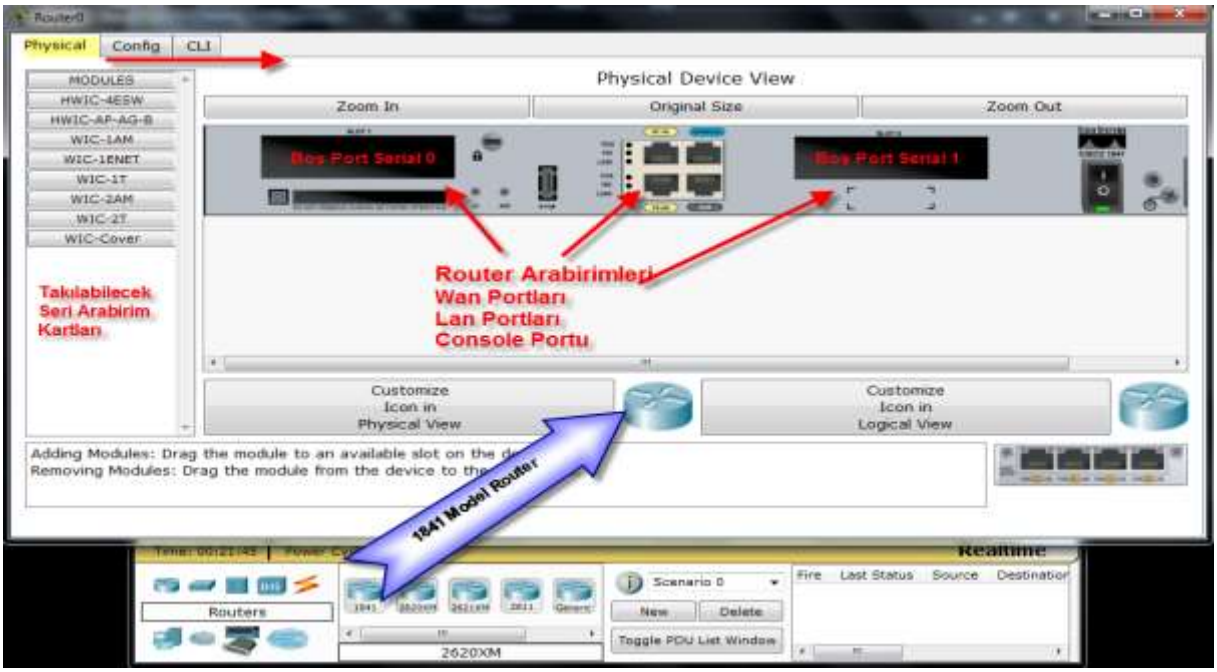


Multiuser Connection

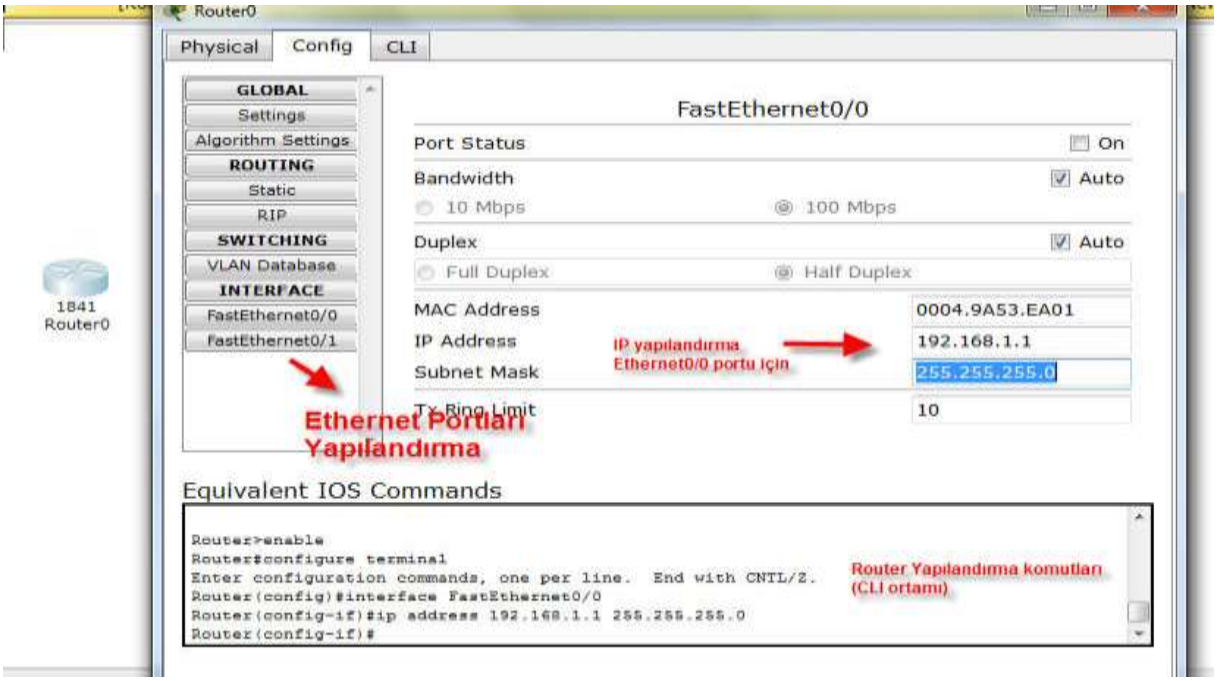


Mantıksal çalışma alanında bir yönlendirici ve bir anahtar eklenmiş bulunan resimde, 1 numaralı daire ile gösterilen bölüm, yeni bir cihaz ekleneceğini gösteren fare imleci şeklidir. İmlecin bu şekilde görünmesinin sebebi, ağ cihazları alanında son kullanıcı cihazları (End Devices) bölümünden bilgisayarın seçilmiş olmasıdır.

1.1. Router Ethernet Portları IP Yapılandırması

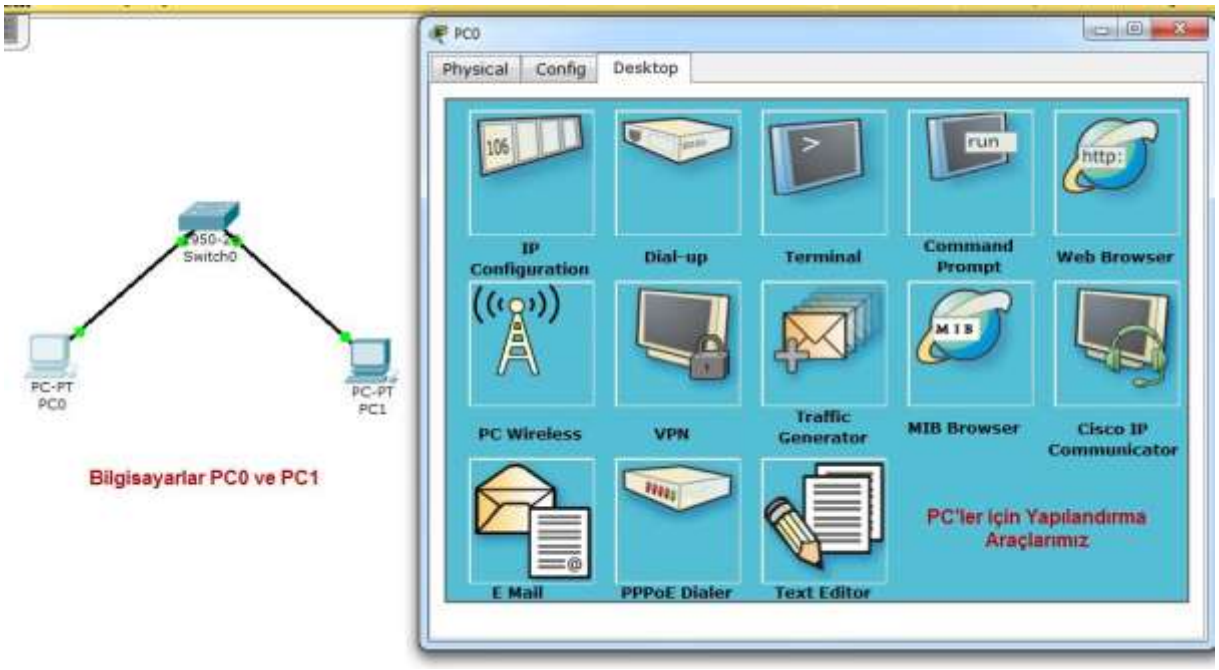


Router arabirimlerinden Ethernet Portları FastEthernet 0/0 ve FastEthernet0/1 isimleri ile tanımlıdır. Bu arabirimlere IP yapılandırması yapılır.

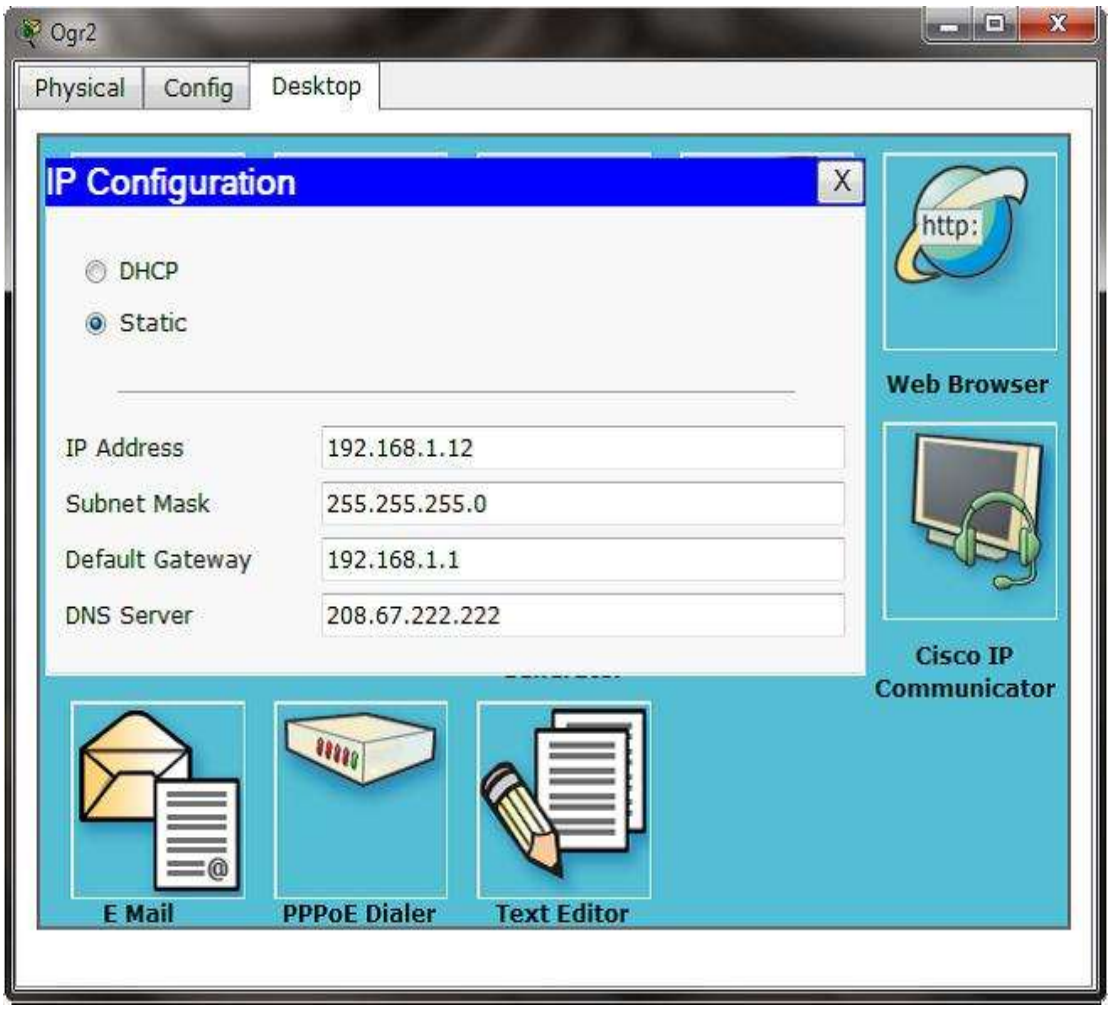


1.2. Bilgisayarlarda IP Yapılandırması

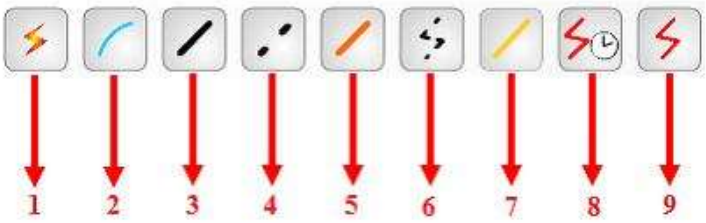
Cisco Packet Tracer programında her hangi bir bilgisayarın yapılandırma işlemlerini gerçekleştirmek için ilgili cihazı çift tıklayın. Gelen ekranda diğer ayarlarla beraber IP Yapılandırması alanını görebilirsiniz.



PC yapılandırması, bilgisayara TCP parametrelerinin (IP adresi, alt ağ maskesi, varsayılan ağ geçidi) atanması işlemidir.



1.3. Kablo Bağlantıları



1- Bağlantı türünü otomatik olarak belirler. Cihazların hangi kabloyla bağlanması gerektiğinden emin olunmadığında bu seçenek kullanılır.

2- Konsol (Console) kablosu, bilgisayarla yönlendirici veya anahtar arasında yapılan bağlantı türüdür. Genellikle yönetilebilir ağ cihazları ilk kez yapılandırılacağı zaman kullanılan bağlantı türüdür.

3- Düz bakır kablo, OSI veya TCP ağ modellerinde farklı katmanlarda çalışan cihazları birbirine bağlamak için kullanılır, yani farklı cihazlar düz kabloyla birbirine bağlanırlar. Örneğin: PC-Switch, Switch- Router vb.

4- Çapraz bakır kablo, OSI veya TCP ağ modellerinde aynı katmanlarda çalışan cihazları birbirine bağlamak için kullanılır. Yani aynı cihazlar çapraz kabloyla birbirine bağlanırlar. Örneğin, PC-PC, PC-Router, Switch- Switch vb.

5- Fiber optik kablo, veri iletiminin ışıkla yapılması gereken durumlarda kullanılan kablo türüdür.

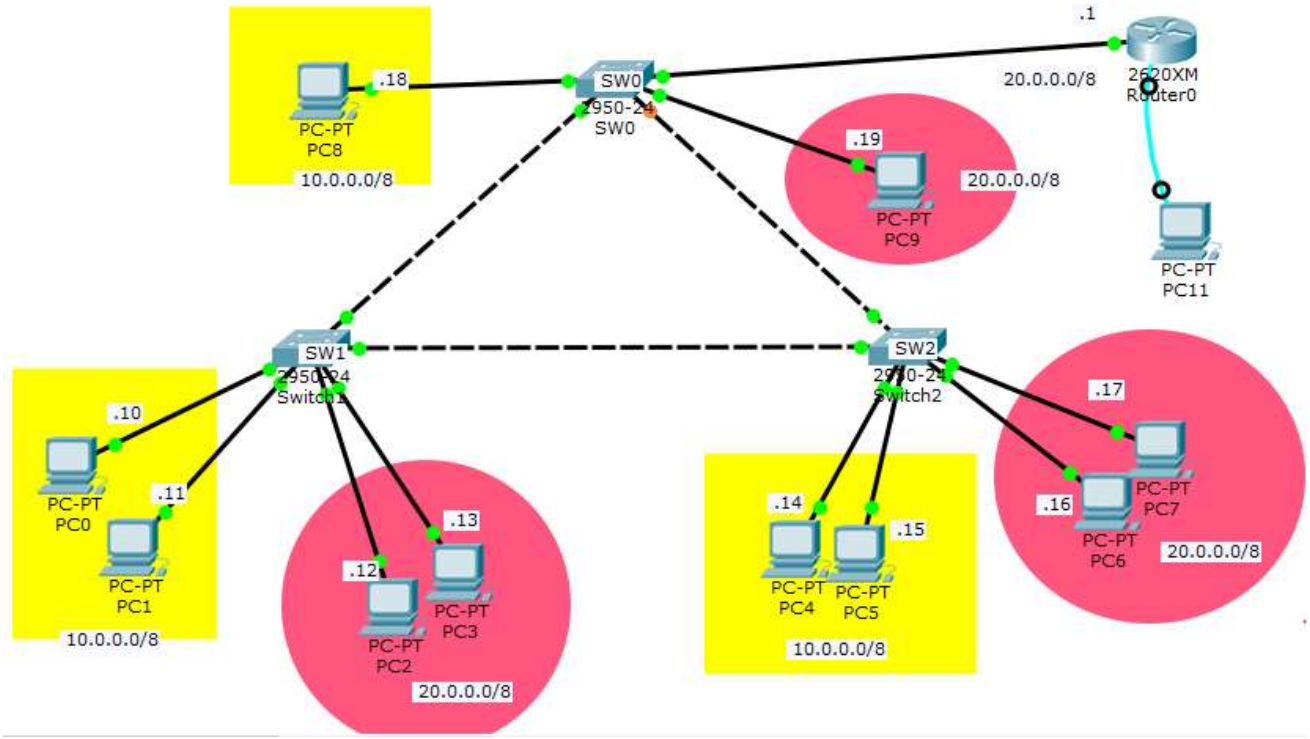
6- Telefon kablosu, modem veya telefonları bağlamak için kullanılır

7- Koaksiyel kablo, kablo TV yayınlarında veya eski ağ topolojilerinde kullanılan kablodur.

8- DCE seri kablo, yönlendirici gibi cihazların birbiriyle bağlantısında kullanılan iletişim hızının belirlenmesi gereken seri kablodur. DCE kablolarda "Clock Rate" değerinin mutlaka verilmesi gerekir.

9- DTE seri kablo, iletişim hızının belirlenmesi gerekmeyen seri kablodur. T1/E1 bağlantılarda standart hızı kullanır.

UYGULAMA FAALİYETİ - 1



İşlem Basamakları	Notlar
Üst resimdeki PC, Switch ve Router'ı çalışma ekranına yerleştirin.	
Doğru bağlantı kablolarını kullanarak ağınızı kurun.	
Her bir PC ve Router için ilgili IP yapılandırmasını tamamlayın	
Her bilgisayardan kendi ağındaki diğer bilgisayarlara PING atarak iletişimin sağlıklı çalıştığını test edin	

ÖĞRENME FAALİYETİ–2

AMAÇ

Bu modül ile gerekli ortam sağlandığında, haberleşme sistemlerinde kullanılan yönlendirme teknolojileri, araçları ve kullanım özelliklerini bileceksiniz.

ARAŞTIRMA

Büyük işletmelerde kullanılan ağ yapılarını inceleyerek, yönlendirme için kullanılan araçları araştırınız.

2. TCP / IP Katmanları

İnternetin temel protokolü olarak yerini almış TCP/IP ‘ nin açılımı Transmission Control Protocol / Internet Protocol’ dür. TCP /IP modeli OSI katmanlarından çok daha önce standartlaştığı için OSI içinde referans olmuş 4 katmanlı bir yapıdır.

• Uygulama Katmanı

• Nakil Katmanı

• Internet Katmanı

• Ağa Giriş Katmanı

Uygulama Katmanı: OSI modelindeki Uygulama, Oturum ve Sunum katmanlarına karşılık gelmekte ve o katmanların işlevlerini yerine getirmektedir. Bu katmanda TFTP, FTP, SMTP, SNMP gibi protokoller çalışmaktadır.

Nakil Katmanı: OSI modelindeki Nakil katmanıyla bire bir eşleştirilebilir. Bu katmanda iki farklı sınıfa ayrılabilecek iki protokol kullanılır. TCP ve UDP.

• Bağlantı Odaklı: TCP

• Bağlantısız: UDP

Internet Katmanı : OSI modelindeki Network katmanına denktir ve adresleme, en iyi yol seçimi gibi işlevleri yerine getirir. Bu katman da IP (Internet Protocol), ICMP (Internet Control Message Protocol), BOOTP (Bootsrap Protocol), DHCP (Dynamic Host Configuration Protocol), ARP (Adres Resolution Protocol) ve RARP (Reverse Address Resolution Protocol) gibi protokoller çalışmaktadır.

Ağa Giriş Katmanı: OSI modelinde ki Data-Link ve Fiziksel Katmana denk gelmektedir.

2.1. OSI REFERANS MODELİ

Kullanıcıların farklı talepleri ve dolayısıyla network üzerinde kullanılmak zorunda kalınan karmaşık uygulamalar, ağ kurulumlarında bir hiyerarşinin doğmasını kaçınılmaz yapmıştır. Bilgisayar ağları büyüdükçe bu ağları yönetmek ve sorun gidermek, standart bir yapı olmadığı da düşünülürse

çok daha zorlaşmaya başladı. Uluslararası Standartlar Organizasyonu (ISO) bir çok ağ yapısını inceleyerek 1984 yılında OSI referans modelini geliştirdi. Artık donanım ve yazılım firmaları bu standarda uygun ürünler üretmeye başladılar. OSI modelinde 7 katmanlı bir yapı kullanılmış ve bu model; karmaşıklığı azaltmış, insanların belli katmanlarda uzmanlaşması için referans olmuş, katmanların işlevlerinin öğrenilmesi ve öğretilmesi kolaylaşmıştır, Farklı donanım ve yazılım ürünlerinin birbirleriyle uyumlu çalışmasını sağlamış ve bir katmanda yapılan değişiklikler diğer katmanları etkilemediği için işbirliği, görev paylaşımı, problem çözümünü gibi konularda kolaylıklar getirmiştir. OSI katmanlarını şu şekilde sıralayabiliriz.

7. Uygulama Katmanı (Application Layer)

6. Sunum Katmanı (Presentation Layer)

5. Oturum Katmanı (Session Layer)

4. Nakil Katmanı (Transport Layer)

3. Ağ Katmanı (Network Layer)

2. Data Link Katmanı (Data Link Layer)

1. Fiziksel Katman (Physical Layer)

Burada Uygulama, Oturum ve Sunum katmanları üst katmanlar olarak adlandırılırlar ve işlevlerini yazılımlar sağlamaktadır. (Bu katmanlar TCP/IP modelinde Uygulama Katmanı adı altında tek bir katman olarak yapıya dahil edilmiştir.) Nakil, Ağ, Data Link ve Fiziksel katmanlar ise alt katmanlar olarak adlandırılırlar ve işlevlerini bilgisayarların ve ağda kullanılan diğer cihazların donanımları ve bu donanımlar üzerindeki yazılımlar sağlar.

Uygulama Katmanı (Application Layer) :Kullanıcıya en yakın olan katmandır ve diğer katmanlara herhangi bir servis sağlamaz. Burada kullanılan bazı uygulamalar FTP TFTP Telnet SMTP SNMP HTTP

Sunum Katmanı (Presentation Layer) : Gönderilecek datanın, datayı alacak bilgisayar tarafından da anlaşılabilecek ortak bir formata dönüştürüldüğü katmandır. Bu katmanda data transferinin güvenli olması için şifreleme de mümkündür. Data formatları MPEG GIF JPEG ASCII

Oturum Katmanı (Session Layer): İletişim kuran bilgisayarlar arasında oturum açar ve sonlandırır. Bu katmanda kullanılan servisler SQL Netbios NFS

Nakil Katmanı (Transport Layer): Bu katman nakil edilecek datanın bozulmadan güvenli bir şekilde hedefe ulaştırılmasını sağlar. Üst katmanlardan gelen her türlü bilgi nakil katmanı tarafından diğer katmanlara ve hedefe ulaştırılır. Gönderilen datanın bozulmadan ve güvenli bir şekilde hedefe ulaşıp ulaşmadığını uygun protokollerle kontrol edebilir. Bu katmanda çalışan protokollere TCP UDP

Bu katmanın en önemli iki fonksiyonun Güvenlilik ve Akış kontroldür. Güvenlilik bilgisayarlar arasında gerçekleştirilen data transferinde datanın sağlıklı bir şekilde hedefe gönderilip gönderilmediğini yöneten, gönderilemediği durumlarda tekrar gönderilmesini sağlayan fonksiyondur. İletişim halindeki bilgisayarlarda datayı gönderen bilgisayar alıcının kapasitesinden üzerinde datalar gönderebilirler. Böyle bir durumda datayı alan bilgisayar alamadığı paketleri yok edecektir ki önlemek için Nakil Katmanı Ara Bellekleme, tıkanıklıktan Kaçınma ve Pencereleme metodlarını kullanarak akış kontrolünü sağlar. Ara bellekleme de datanın akış hızına müdahale etmeden, kapasitenin üzerindeki datanın ara belleğe alınması, tıkanıklıktan kaçınma metodun da ICMP Source Quench

mesajı ile gönderen bilgisayarın gönderimini yavaşlatması, Pencereleme metoduyla paketlerin gruplar halinde gönderilmesi sağlanır.

Ağ Katmanı (Network Layer): Bu katman bir paketin yerel ağ içerisinde ya da diğer ağlar arasında ki hareketini sağlayan katmandır. Bu hareketin sağlanabilmesi için hiyerarşik bir adresleme yapısı gerekmektedir. Gelişen teknolojiyle birlikte mevcut ağlarında büyüme eğiliminde olması adresleme yapısının hiyerarşik olmasını gerektirmektedir. Ayrıca hiyerarşik sistem dataların hedef bilgisayara en etkili ve en kısa yoldan ulaşmasını da sağlar. Bu katmanın bir özelliği olan Adresleme sayesinde bu sağlanabilmiştir. Adresleme Dinamik ya da statik olarak yapılabilir. Sabit adresleme el ile yapılan adreslemedir. Dinamik adresleme de ise otomatik olarak ip dağıtacak örneğin DHCP gibi bir protokole ihtiyaç vardır. Ayrıca bu katmanda harekete geçen bir datanın hedefine ulaşabilmesi için en iyi yol seçimide yapılır. Bu işleme Routing bu işlemi yerine getiren cihaza ise Router diyoruz. Router en basit tarif ile en iyi yol seçimini yapar ve broadcast geçirmediği için ağ performansını olumsuz etkilemez. Bu katmanda kullanılan protokoller IP ARP RARP BOOTP ICMP

Data Link Katmanı (Data Link Layer): Fiziksel adreslemenin ve network ortamında datanın nasıl taşınacağının tanımlandığı katmandır. Burada fiziksel adreslemeden kastedilen MAC (Media Access Control) adresidir. Bu katman Hakemlik, Adresleme, Hata Saptama, Kapsüllenmiş Datayı Tanımlama fonksiyonlarına sahiptir. Ethernet hakemlik için CSMA/CD (Carrier Sense Multiple Access with Collision Detect) adı verilen bir algoritmayı kullanır. Bu algoritma şu adımlardan oluşur;

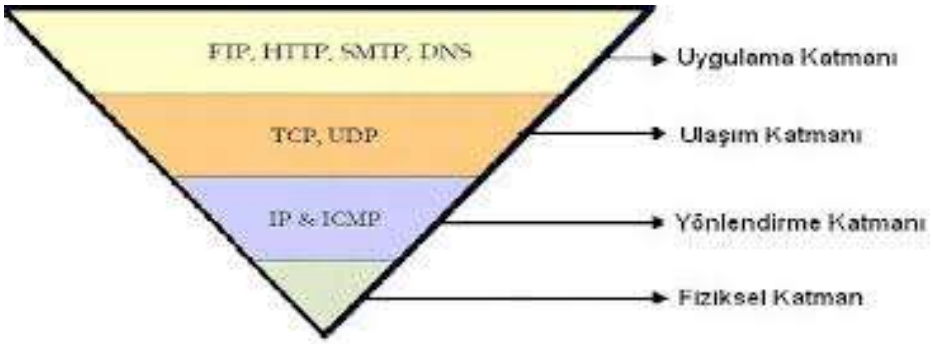
1. Hattın boş olup olmadığını dinler

2. Boşsa data gönderir

3. Doluysa bekler ve dinlemeye devam eder

4. Data transferinde çarpışma olursa durur ve tekrar dinlemeye başlar. Adresleme için, MAC adresi, Unicast adresi, broadcast adresi ve multicast adresi örnek olarak verilebilir. Bu katman kullanılan protokoller HDLC PPP ATM Frame Relay

Fiziksel Katman (Physical Layer) : Bu katman datanın dijital rakamlara dönüştürerek aktarımın yapıldığı katmandır. Kablolar, hub, repeater cihazlar bu katmanda yer alırlar. Bu katman da herhangi bir protokol tanımlanmamıştır.



2.2. Data Encapsulation (Veri Paketleme)

Data Encapsulation 5 adımdan oluşur.

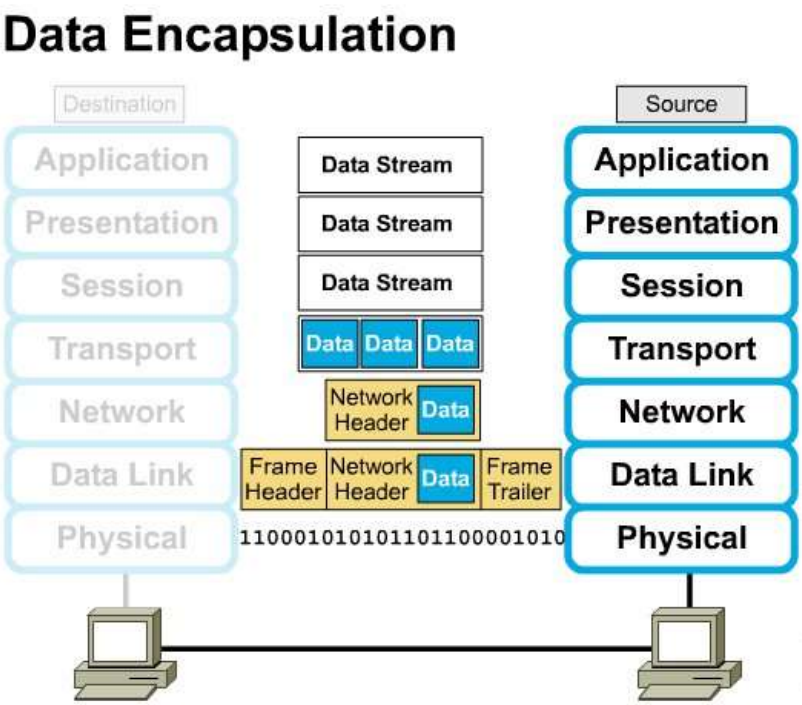
1. Uygulama, Sunum ve Oturum Katmanları kullanıcının girdiği veriyi 4. katman yani Nakil katmanına kadar getirir.

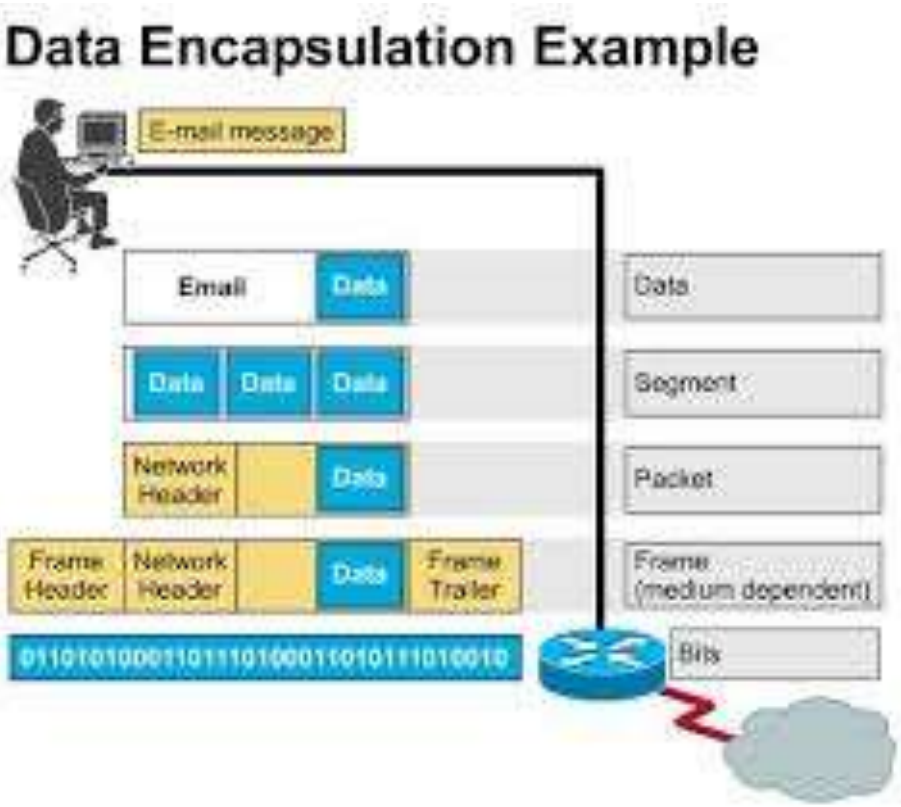
2. Nakil katmanı kendisine gelen bilgiyi segment adı verilen bölümlere ayırır ve datanın hangi protokolle gönderileceği (TCP - UDP) bilgisini de ekleyerek network katmanına gönderir.

3. Bu katmana gelen segment burada packetlere ayrılır ve IP header dene, hedef ve kaynak Ip ler gibi bilgileri bulunduğu başlığı ekleyerek bir alt katman olan data link katmanına gönderir.

4. Burada data artık framelere çevrilir ve mac adresleride eklenmiştir

5. Frame yapı bu katmanda bitlere ayrılır ve iletilir.





2.3. TCP / IP Protokolleri TCP (Transmission Control Protocol)

TCP, IP 'nin bir üst katmanında çalışan iki aktarım katmanı protokolünden birisidir. TCP, güvenilir ve sanal devre üzerinden çalışan bir protokoldür. Aynı ağ üzerinde ya da farklı ağlar üzerinde iki hostun birbirleriyle güvenilir bir şekilde haberleşmesini sağlar.

TCP 'nin başlıca özellikleri şunlardır:

• Bir bağlantının (connection) kurulması ve sonlandırılması

• Güvenilir (Reliable) paket dağıtımının sağlanması

• Akış kontrolü (flow control) olanağı ile hostlarda veri taşmasının (overflow) önlenmesi

• Bozulmuş ya da ikilenmiş verinin düzeltilmesi (error recovery)

• Alıcı host içerisinden birçok uygulama arasında demultiplexing yapılması TCP, internet ortamında şu işlevleri sağlar:

• Temel Veri Aktarımı (Basic Data Transfer) • Güvenilirlik (Reliability)

• Uçtan uca Akış Kontrolü (End to end flow control)

• Çoğullama (Multiplexing) • Bağlantılar (connections)

• Tam çift yönlü işlem (full duplex process)

TCP bağlantısının kurulması üç aşama (Three Way Handshake) sonucunda gerçekleşir:

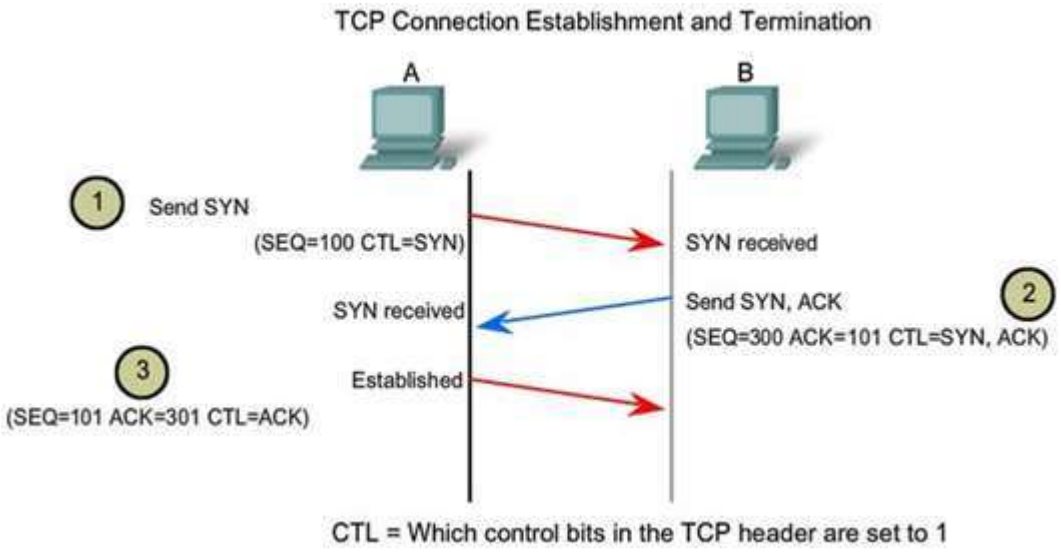
1.Aşamada: Kaynak host bağlanmak istediği hosta bir istek paketi gönderir. Bu paketin TCP başlığında SYN = 1 ve ACK = 0 'dır. Gönderdiği paket içindeki segmente ait sıra numarası X 'tir.

2.Aşamada: Bu paketi alan hedefe TCP başlığında SYN = 1, ACK = 1 bitlerini kurarak kendi paketini sıra numarasına SEQ Numarası=Y ve onay numarası, ACK Numarası = (X + 1) 'i gönderir.

3.Aşamada: İsteğine karşılık bulan istemci son aşamada hedefe onay paketi gönderir ve bağlantı kurulmuş olur. Sonra kaynak, hedefe göndermek istediği veri paketlerini gönderir. TCP ve UDP üst protokollerle bağlantıda portları kullanırlar. 65535 adet port vardır ve IANA (Internet Assigned Numbers Authority) ilk 1024 portu Well-known portlar olarak ilan etmiştir. Bu portlardan bazıları

• FTP: 21 • SMTP: 25

• Telnet: 23 • DNS: 53



2.4. PROCESS/ APPLİCATİON(UYGULAMA) KATMANI PROTOKOLLERİ

2.4.1. TELNET

Telnet bir terminal emülasyon protokolüdür. Bu protokol, kullanıcıların telmet istemci programlarını kullanarak Telnet sunuculara bağlanmalarını sağlar. Böylece telnet sunucuları uzaktan yönetilebilir.

2.4.2. FTP (FİLE TRANSFER PROTOCOL)

TCP tabanlı dosya transfer protokolüdür. FTP bağlantı kurulurken FTP sunucunun 21 numaralı portu kullanılır. TFTP (Trivial File Transfer Protocol) UDP tabanlı Cisco IOS tarafından desteklenen bir protokoldür. Router ve switchlerde dosya transferi için kullanılır, daha az hafıza ve işlemci gücü gerektirir. UDP tabanlı olduğu için hızlı bir iletişim söz konusudur fakat hata telafisi yoktur.

2.4.3. LPD (LİNE PRİNTER DEAMON)

Bu protokol yazıcı paylaşımını gerçekleştirmek için kullanılır.

2.4.4. SNMP (SİMPLE NETWORK MANAĞEMENT PROTOCOL)

SNMP protokolü ağlar üzerindeki birimleri denetlemek amacıyla geliştirilmiştir. Bir network cihazı üzerindeki sıcaklıktan o cihaza bağlı kullanıcılar, internet bağlantı hızından sistem çalışma süresine kadar bir çok bilgi SNMP protokolünde tanımlanmış bir yapı içerisinde tutulur.

TF SNMP protokolü ağlar üzerindeki birimleri denetlemek amacıyla geliştirilmiştir. Bir network cihazı üzerindeki sıcaklıktan o cihaza bağlı kullanıcılar, internet bağlantı hızından sistem çalışma süresine kadar bir çok bilgi SNMP protokolünde tanımlanmış bir yapı içerisinde tutulur. IP (Internet Protocol) Bağlantısız bir protokoldür. Bu protokol datanın hedefe ulaşması için gidebileceği en iyi yolu seçer ve gelen paketleri IP başlıklarını okuyarak networkteki bilgisayarların yerlerini belirler. IP başlıklarında gönderilecek datanın yaşam süresi, datanın gönderilmesini sağlayacak protokol, kaynak ve hedef ip adresleri, kullanılan ip versiyonu gibi bilgiler bulunur.

2.4.5. TP (TRİVİAL FİLE TRANSFER PROTOCOL)

UDP tabanlı Cisco IOS tarafından desteklenen bir protokoldür. Router ve switchlerde dosya transferi için kullanılır, daha az hafıza ve işlemci gücü gerektirir. UDP tabanlı olduğu için hızlı bir iletişim söz konusudur fakat hata telafisi yoktur.

2.4.6. SMTP (SİMPLE MAİL TRANSFER PROTOCOL)

Mail göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Sadece mail yollamak için kullanılan bu protokolde, basitçe, istemci bilgisayar SMTP sunucusuna bağlanarak gerekli kimlik bilgilerini gönderir, sunucunun onay vermesi halinde gerekli maili sunucuya iletir ve bağlantıyı sonlandırır.

2.4.7. NFS (NETWORK FİLE SYSTEM)

Bu protokol farklı tipte iki dosya sisteminin bir arada çalışmasını sağlar.

2.4.8. X WİNDOW

Grafiksel kullanıcı ara yüzü tabanlı istemci sunucu uygulamaları geliştirmek için

tanımlanmış bir protokoldür.

2.4.9. DNS (DOMAIN NAME SERVICE)

Bu protokol internet isimlerinin (örneğin www.geocities.com gibi) IP adreslerine dönüştürülmesini sağlar.

2.4.10. DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

BOOTP protokolünün gelişmiş hali olan bu protokol ile tam dinamik ip konfigürasyon dağıtımı yapılabilir. sunucu – istemci ortamında çalışırlar ve istemcilerde ip adreslerini otomatik olarak alacaklarına dair bir konfigürasyon yapılmalıdır. DHCP ile belirlenen ip adresleri, subnet masklar, DNS server adresleri, varsayılan ağ geçidi gibi adresler dağıtılabilir, ip adresleri MAC adreslerine reserve edilebilir veya bazı ip adresleri tamamen kullanıma kapatılabilir. DHCP' den

alınan ip adresleri DHCP server tarafından istemciye belirli sürelerle kiralanır ve istemci belirli aralıklara ile DHCP serverdan kira süresini yenilemesini ister. Yenilenme kira süresi dolana kadar yapılamazsa DHCP server tarafından istemciye yeni bir ip adresi verilir.

2.5. HOST-TO-HOST (NAKİL) KATMANI PROTOKOLLERİ

2.5.1. TCP (TRANSMISSION CONTROL PROTOCOL)

TCP, IP 'nin bir üst katmanında çalışan iki aktarım katmanı protokolünden birisidir. TCP, güvenilir ve sanal devre üzerinden çalışan bir protokoldür. Aynı ağ üzerinde yada farklı ağlar üzerinde iki hostun birbirleriyle güvenilir bir şekilde haberleşmesini sağlar.

TCP 'nin başlıca özellikleri şunlardır:

1. Bir bağlantının (connection) kurulması ve sonlandırılması
2. Güvenilir (Reliable) paket dağıtımının sağlanması
3. Akış kontrolü (flow control) olanağı ile horstlarda veri tasmasının (overflow) önlenmesi
4. Bozulmuş yada ikilemmiş verinin düzeltilmesi (error recovery)
5. Alıcı host içerisinden birçok uygulama arasında demultiplexing yapılması

TCP, internet ortamında su işlevleri sağlar:

1. Temel Veri Aktarımı (Basic Data Transfer)
2. Güvenilirlik (Reliability)
3. Uçtan uca akış Kontrolü (End to end flow control)
4. Çoğullama (Multiplexing)
5. Bağlantılar (connections)
6. Tam çift yönlü işlem (full duplex process)

TCP bağlantısının kurulması üç asama (Three Way Handshake) sonucunda gerçekleşir:

1.Aşamada: Kaynak host bağlanmak istediği hosta bir istek paketi gönderir. Bu paketin

TCP baslığında SYN = 1 ve ACK = 0 ‘dar. Gönderdiği paket içindeki segmente ait sıra numarası X ‘tir.

2.Aşamada: Bu paketi alan hedefe TCP baslığında SYN = 1, ACK = 1 bitlerini kurarak kendi paketini sıra numarasına SEQ Numarası=Y ve onay numarası, ACK Numarası = (X + 1) ‘i gönderir.

3.Aşamada: İsteğine karşılık bulan istemci son aşamada hedefe onay paketi gönderir ve bağlantı kurulmuş olur. Sonra kaynak, hedefe göndermek istediği veri paketlerini gönderir. TCP ve UDP üst protokollerle bağlantıda portları kullanırlar. 65535 adet port vardır ve IANA (Internet Assigned Numbers Authority) ilk 1024 portu Well-known portlar olarak ilan etmiştir. Bu portlardan bazılar şunlardır: **FTP: 21 Telnet: 23 SMTP: 25 DNS: 53**

Bir bilgisayar bir IP adresi ve bir port belirlediğinde buna soket **(socket)** ismi verilmektedir. Yani “X IP adresindeki bilgisayara, Y port ’undan bilgi gönderildiğinde, bu bilgi su işlem için ele alınacaktır.” seklinde bir önerme ortaya çıkar.

2.5.2. UDP (User Datagram Protocol)

UDP, TCP / IP protokol grubunun iki aktarım katmanı protokolünden birisidir. UDP, onay (acknowledge) gönderip alacak mekanizmalara sahip değildir. Bu yüzden veri iletiminde başarıyı garantileyemez. Uygulamalar güvenli ve sıralı paket dağıtımı gerektiriyorsa UDP yerine TCP protokolü tercih edilmelidir. Bazı UDP port numaraları şunlardır;

- Who Is: 43
- DNS: 53
- NTP: 123
- SNMP: 161

2.6. İnternet Katmanı Protokolleri

2.6.1. IP (INTERNET PROTOCOL)

Bağlantısız bir protokoldür. Bu protokol datanın hedefe ulaşması için gidebileceği en iyi yolu seçer ve gelen paketleri IP baslıklarını okuyarak networkteki bilgisayarların yerlerini belirler. IP baslıklarında gönderilecek datanın yasam süresi, datanın gönderilmesini sağlayacak protokol, kaynak ve hedef ip adresleri, kullanılan ip versiyonu gibi bilgiler bulunur.

2.6.2. ICMP (Internet Control Message Protocol)

Internet protokolünün control ve yönetimine yardımcı olan bir protokoldür. Bu protokol sayesinde network üzerindeki sorunlar kolaylıkla tespit edilebilmektedir. RFC 792 standardı ile belirlenmiştir ve iki bilgisayar arasındaki iletişimde, hedef bilgisayarda, varsayılan ağ geçidinde veya routerlarda oluşan hatalar ICMP mesajı olarak kaynak bilgisayara bildirilir. Farklı durumlara göre farklı hata mesajları vardır. Bunlardan bazıları şunlardır:

Hedefe Ulaşılamıyor: Kaynak bilgisayara datanın gönderilmesiyle ilgili bir problem olduğu bilgisi döner.

Zaman Aşımı: Gönderilen datanın hedefe ulaşması için gereken zamanın dolduğunu ve bu sebeple paketin yok edildiğini belirten mesajdır.

Source Quench: Kaynak bilgisayara yönlendirmeyi yapan cihazdan daha hızlı data gönderdiğini ve yavaşlaması gerektiğini belirtir.

Tekrar Yönlendirme: Bu mesajı gönderen yönlendirici hedef için daha iyi bir yola sahip yönlendiricinin var olduğunu belirtir.

Yankı: Ping komutu tarafından bağlantıyı onaylamak için kullanılır.

Parameter Problem: Parametrenin yanlış olduğunu belirtmek için kullanılır.

Address Mask Request / Reply: Doğru Subnet Maskın öğrenilmesi için kullanılır.

2.6.3. BOOTP (Bootsrap Protocol)

UDP tabanlıdır ve RARP protokolü gibi sunucu - istemci ortamında çalışır. IP adresi isteyen bilgisayarlar bu isteklerini bir broadcast ile bildirirler. BOOTP sunucu ise ip adresini, kendi ip adresini ve varsayılan ağ geçidi adresini bir broadcast ile networke gönderir. İstemciler MAC adreslerine bakarlar ve kendi MAC adreslerini gördüklerinde bu bilgileri alırlar.

2.6.4. HTTP (**HYPERTEXT** TRANSFER PROTOCOL)

HTTP (HyperText Transfer Protocol – HiperMetin Aktarım Protokolü): HTTP, Internet'te bağlandığınız Web sayfalarının kodlarını aktarmak için kullandığımız protokoldür.

Örneğin www.sistem.com.tr yazdığımızda, ilk olarak bu protokol alt seviyedeki

2.6.5. RARP (Reverse Address Resolution Protocol)

Sabit diski olmayan terminaller tarafından otomatik olarak ip adresi almak için kullanılan protokoldür. RARP istemci kendisiyle aynı segmentte bulunan RARP sunucudan ARP paket formatını kullanarak broadcast yapar ve ip adresi ister. RARP sunucu da uygun bir ip adresini istemciye gönderir.

2.6.6. ARP (Address Resolution Protocol)

ARP protokolü ip adresi bilinen bir bilgisayarın MAC adresini öğrenmede kullanılır. İki bilgisayar iletişim kuracağı zaman kaynak bilgisayar hedef bilgisayara MAC adresini sorar ve bu işlem ARP Request denen ve broadcast olan mesajla gerçekleşir. İlgili ip adresine sahip olan bilgisayar içinde MAC adresinin bulunduğu cevap paketini istemciye gönderir. Bu cevap mesajına ARP Reply denir. ARP protokolü Internet Katmanında çalışır. Kaynak bilgisayar ip adresi ve edindiği mac adresini eşleştirerek ön belleğinde saklar. "ARP -a" komut satırı ile ön bellekte bulunan MAC adresleri görüntülenebilir.

ÖĞRENME FAALİYETİ–3

AMAÇ

Alt ağ maskesi hesaplayabileceksiniz..

ARAŞTIRMA

IPv4 adresleri ile en fazla kaç cihaz ağa bağlanabilir? Hangi cihazlar ağa bağlanabilmektedir? Ağdaki sorunlar nasıl tespit edilir?

3. IP HESAPLARI VE SUBNETTING

TCP/IP protokolünde tüm bilgisayarlar 32 bitlik "özgün" bir IP numarasına sahip olacak şekilde adreslenirler. IP adresleri sınıflara ayrılmıştır.

Class A :0.0.0.0 - 127.255.255.255

Class B:128.0.0.0 - 191.255.255.255

Class C:192.0.0.0 - 223. 255.255.255

Class D:224.0.0.0 - 239. 255.255.255

Class E:240.0.0.0 – 255. 255.255.255

Her ip sınıfının subnet maskıda belirlenmiştir.

A sınıfı için subnet mask: 255.0.0.0

B sınıfı için subnet mask: 255.255.0.0,

C, D, E sınıfları için subnet mask: 255.255.255.0 'dır.

Bazı ip aralıkları iç networkte kullanılmak üzere ayrılmıştır ve herhangi bir şekilde dış networkte (internette) kullanılamaz.

Bu ip aralıkları

10.0.0.0 – 10.255.255.255

172.16.0.0 -172.31.255.255

192.168.0.0 – 192.168.255.255

Internet ortamında bu ip adresleri kesinlikle kullanılmaz, iç network kullanıcıları internete çıkarken, ISP tarafından sağlanan static veya dynamic bir ip adresine dönüşürler. İşte bu ip adresi tüm dünya da tek olacaktır.

Yerel networkler de ip adresi manuel olarak static konfigüre edilebileceği gibi örneğin DHCP gibi bir yazılımla dinamik olarak da dağıtılabilir. Ip adreslerinin dağıtılması sırasında subnet maskların standart verilmesi ciddi sorunlara sebep olacaktı. Örneğin bir ISP firması söz gelimi 150 adet ip adresi almak istiyorsunuz. Bu durum standart subnet mask kullanılarak size verilebilecek minimum ip sayısı 255'dir. Daha vahim bir senaryo ise siz söz gelimi 500 tane ip adresi isteseniz ortaya çıkar çünkü o zaman size verilebilecek minimum ip sayısı 255*255 = 65025 ' dir. Bunun önüne geçebilmek için yapılabilecek tek şey ise subnet masklar ile oynamaktan geçer. Bu sayede networkler sub-networklere bölünebilir ve ip israfın biraz olsun azalabilir.

Örnek: Elinizde adresi 192.168.1.0 olan C Class bir network var ve bunu 4 subnetworke bölmek istiyorsunuz; Bu durumda 256/4 = 64 'er tane ip adresiniz olacak. Subnet Maskın son oktetini 256-64 yaparsanız bunu gerçekleştirmiş olursunuz. Bu durumda subnet mask=255.255.255.192 olacaktır ve elimizde subnet maskı 255.255.255.192 ve network adresleri sırasıyla; 192.168.1.0 192.168.1.64 192.168.1.128 192.168.1.192 Olan 4 adet networkümüz, her networkte 64'er tane ip adresimiz olacak.

Bir networkün ilk ip adresi network adresini, son ip adresi broadcast adresini gösterdiği için kullanılamaz dolayısıyla bir networkte "useable" olarak adlandırılan, yani kullanılabilecek ip sayısı toplam ip sayısından 2 eksiktir.

Useable Ip sayısı = toplam ip sayısı – 2 Network adresleri örneğin /24 şeklinde gösterilebilirler. /24 ip adresinin binary yazılımında soldan sağa 24 tane 1 olduğu anlamına gelir. Bu şekilde yazılımına CIDR denir. (Classless)

Örneğin; 255.255.255.0 binary olarak 11111111.11111111.11111111.00000000 'e eşittir ve 24 tane 1 den dolayı /24 olarak gösterilebilir.

Yukarıdaki örneğimizdeki subnet mask ise binary olarak; 11111111.11111111.11111111.11000000 'a eşit olacak dolayısıyla /26 olarak gösterilebilecektir.

Örnekler: Subnet Mask Binary Yazılım CIDR İfade

255.255.128.0 11111111.11111111.100000000.00000000 /17

255.255.255.128 11111111.11111111.111111111.01000000 /25

255.255.255.252 11111111.11111111.111111111.11111100 /30

Elimizde bir ip adresi ve onun subnet maskı varsa ikisinin binary yazılışını AND' leyerek network adresini bulabiliriz.

Örneğin elimizde subnet maskı 255.255.255.128 olan 192.168.1.141 gibi bir ip var. 192.168.1.141 = 11000000.10101000.00000001.10001101

255.255.255.128 = 11111111.11111111.11111111.10000000

AND (çarpıyoruz) = 11000000.10101000.00000001.10000000

Network Adresi = 192. 168. 1. 128

3.1. Classfull - Classless IP Adresleri

Classfull adreslerde subnet masklar ip adresinin hangi sınıfa ait olduğu ile direk ilgilidir. İp adreslerinin ilk oktetleri sınıflarını belirlerler ve her sınıf için subnet mask belirlenmiş durumdadır. Örnek vermek gerekirse 10.x.x.x gibi bir ip adresi A sınıfı bir ip adresidir ve Classfull olarak çalışan bir sistem de bu adresin subnet maskı her zaman 255.0.0.0 olacaktır. RIP ve IGRP protokolleri

Classfull protokollerdir ve subnet maskı sınıflarına göre kendileri belirlerler. Classless adreslerde ise subnet mask sınıftan bağımsızdır. Şöyleki 10.x.x.x gibi bir ip adresine istendiğinde 255.255.255.0 gibi bir subnet mask verilebilir ve Classless olan sistemlerde bunu algılarlar. Ospf, Eigrp gibi protokoller classless' dır. Classless adreslemeye VLSM (Variable Length Subnet Mask) veya CIDR (Classless Inter Domain Routing) denir.

3.2. ICMP (Internet Control Message Protocol)

3. katman yani Internet yada Network katmanı olarak adlandırdığımız katman IP bazında yönlendirmenin yapıldığı katmandır. IP data iletimi ve yönlendirme için belki de en iyi çözümdür. Fakat IP ile ilgili datanın iletimi sırasında herhangi bir sebeple fail olma durumu olduğunda bu durumu kontrol edecek hata mesajlarına sahip olmaması gibi bir sorun vardır. Sözgelimi yanlış konfigürasyonlar, donanımsal arizalar yada Routing Table' lar ile ilgili sorunlarda IP bir hata mesajı döndürmez. ICMP IP' nin bu akiğini gidermek üzere geliştirilmiş bir protokoldür. Bu durumlarda ICMP ilgili mesajı dondurur ve problem çözümlerde Network Mühendislerine yardımcı olur. Ancak burada IP bazında iletişimin güvenilir olmadığını, ICMP mesajları ile bu güvenilirliğin sağlandığını söylemek yanlış olur. Datanın güvenilir şekilde iletilmesi bir üst katman olan Transport katmanı ve bu katmanda çalışan protokoller tarafından sağlanmalıdır. Genel olarak ICMP mesajları iki ana baslık altında incelenebilir.

1. Hata Raporlama Mesajları

2. Durum Kontrol Mesajları

ICMP mesajları kendi frame yapısına sahip değildir. Bu mesajlar IP ile encapsule edilmiş frameler içerisine gömülmüşlerdir. Dolayısıyla ICMP mesajları tarafından oluşturulmuş hata mesajları kendi ICMP mesajlarını yaratmazlar. ICMP mesajları Type' lardan ve Code' lardan oluşur.

UYGULAMA FAALİYETİ - 3

İşlem Basamakları	Öneriler
128.129.130.131 /20 IP adresi için • Alt ağ maskesi (Subnet Mask) nedir? • Ağ Adresi nedir? • Broadcast (Yayın) Adresi nedir? • Her bir alt ağa kaç bilgisayar bağlanır? • Toplamda ağa kaç bilgisayar bağlanır?	• IP adresinin sınıfını belirleyiniz. • Varsayılan alt ağ maskesini hatırlayınız. • Şayet IP numarası herhangi bir alt ağa bölündüyse, alt ağ maskesinden kaç bit ödünç alındığını bulunuz. • Yeni alt ağ maskesini yazınız. • Alt ağ maskesini ve IP adresini mantıksal VE işlemine tabi tutarak ağ adresini bulunuz. • Cihaz bitleri için kullanılabilecek bitleri hesaplayınız. • Her bir alt ağa kaç bilgisayar bağlanabileceğini hesaplayınız. • Bölünen alt ağ sayısı ile her bir alt ağa bağlanabilecek cihaz sayısını çarparak toplamda ağa kaç bilgisayar bağlandığını hesaplayınız. • Ağ adresinde bulunan cihaz bitlerini “1” yaparak yayın (broadcast) adresini bulunuz.
30 bilgisayarlı bir subnet kurabilmek için gerekli sub netmask’ı yazınız.	

ÖĞRENME FAALİYETİ–4

AMAÇ

Yönlendirici bağlantılarını yapabileceksiniz.

ARAŞTIRMA

LAN ve WAN hakkında araştırma yapınız. ¬ Yönlendiricilerin içyapısını, fiziksel görünümünü ve arayüzlerini araştırınız. Topladığınız bilgileri rapor haline getiriniz. Hazırladığınız raporu sınıfta öğretmeninize ve arkadaşlarınıza sununuz.

4. ROUTER

Network katmanında bulunan ve temel işlevi farklı networklere erişimde en iyi yol seçimini (Best Path Determination) yapan cihaza Router denir. Router Bileşenleri RAM: Random Access Memory' nin kısaltmasıdır. Router running-configuration adı verilen ve çalıştığı andaki konfigürasyonunu içeren bilgileri bulundurur. Bazı kaynaklarda RAM' a Dinamik RAM anlamında DRAM, running-configuration dosyasına da active-configuration denir. Router kapatıldığında ya da yeniden başlatıldığında RAM' de bulunan bilgiler silinir.

4.1. Router Birleşenleri

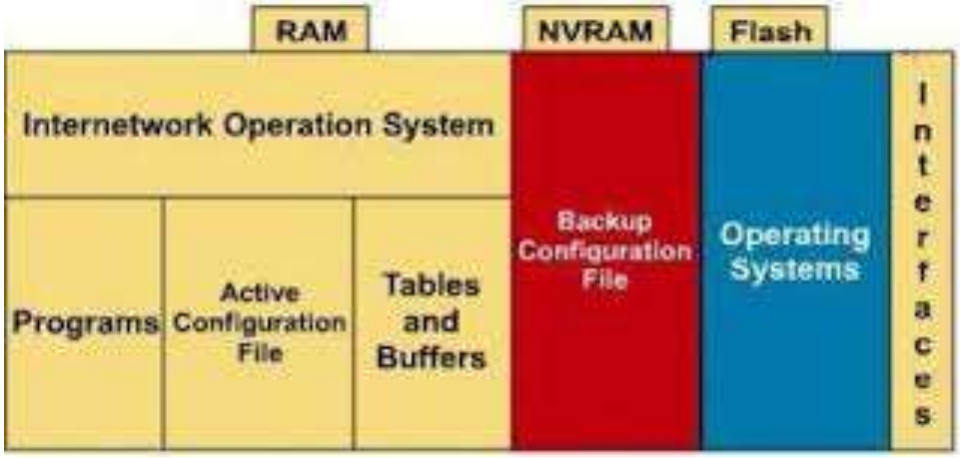
Router'ların başlıca bileşenleri RAM, ROM, FLASH ve NVRAM ve INTERFACE olarak sıralanabilir.

a. ROM (Read Only Memory): Bootstrap yazılımı ,test ve bakım amaçlı kullanılan temel seviyede bir işletim sistemi olan ROM Monitor, POST (Power On Self Test) rutin'leri ve RXBoot olarak adlandırılan mini bir IOS ROM'da tutulur.

b. FLASH: Silinebilir, yeniden programlanabilir (EPROM / Erasable Programmable Read Only Memory) olan bu yongada Cisco'nun IOS işletim sisteminin imajları tutulur. Bir flash'ta birden fazla IOS imajı bulunabilir. Router kapatıldığında flash'daki veri korunur.

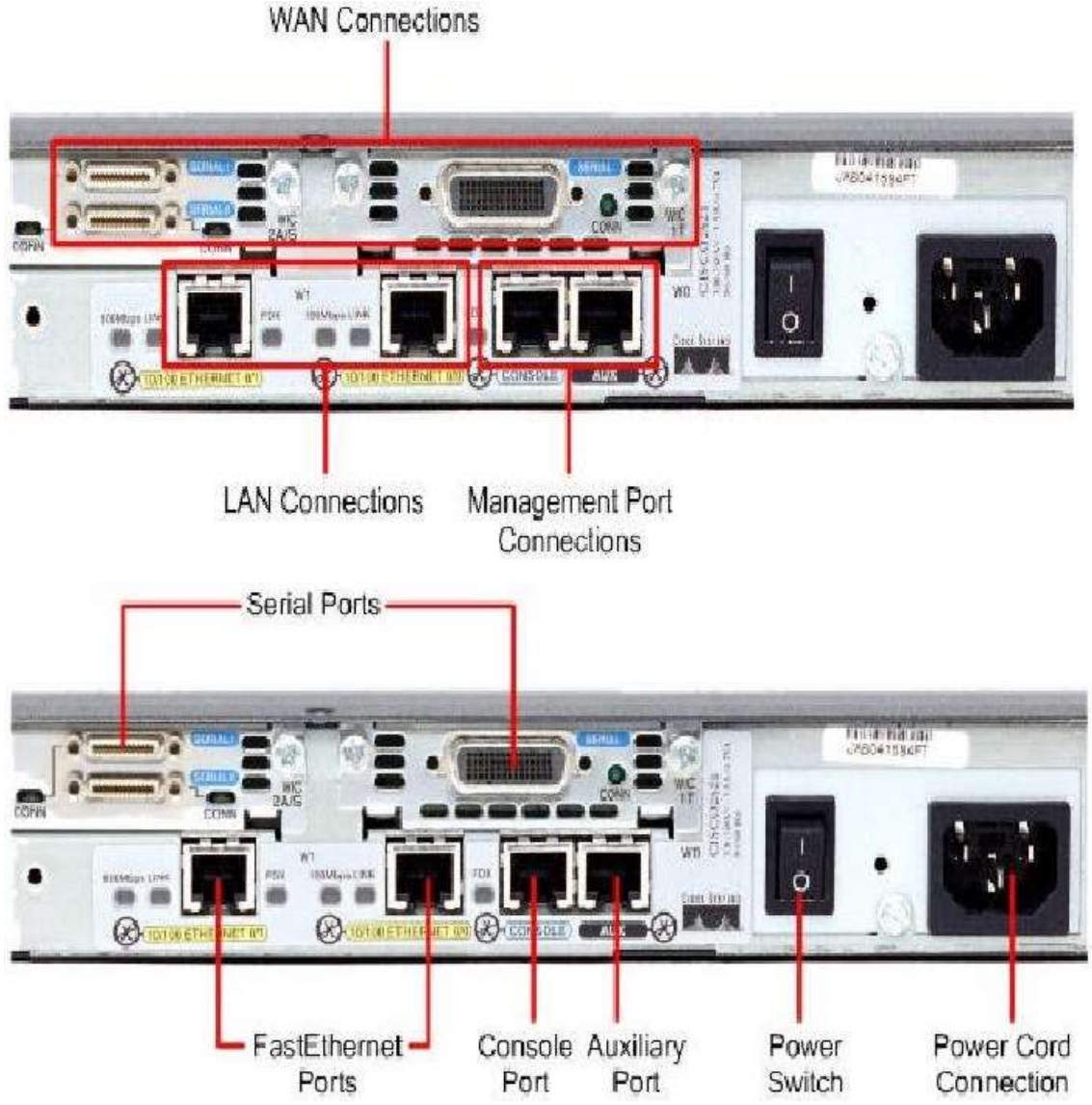
c. NVRAM (Non-volatile random access memory): Router'ın konfigürasyon dosya veya dosyalarının tutulduğu yeniden yazılabilir bir yongadır. Router kapatıldığında NVRAM'daki veri korunur.

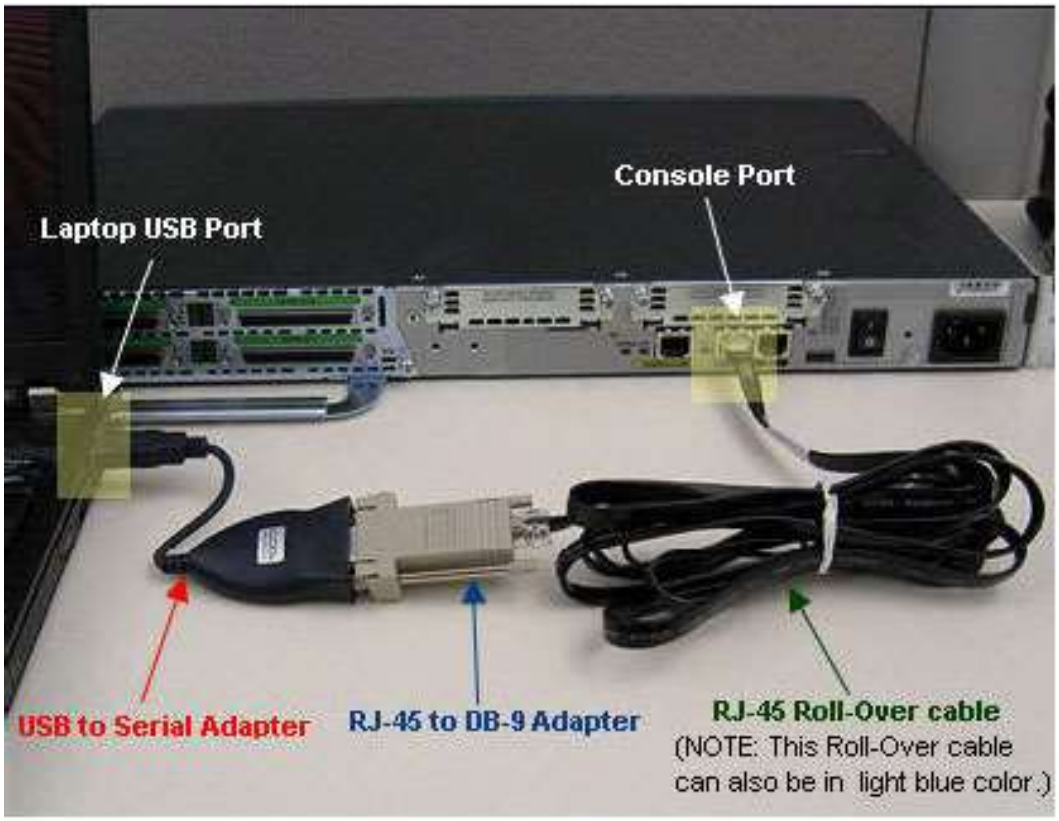
d. RAM / random access memory veya DRAM / Dynamic random access memory; Çalışan IOS konfigürasyonlarını tutar. Ayrıca kaşelere (caching) ve paket depolama sağlar. Router kapatıldığında RAM'deki tüm veri kaybolur.



e.INTERFACE: Router'a erişmek ya da çeşitli fiziksel bağlantıları yapmak için kullanılan fiziksel arabirimlerdir. İnterfaceleri "Serial Interface" ve "Ethernet Interface" ler olarak sınıflandırabiliriz. Bu interfaceler default olarak kapalı durumdadır.

Router'in arayüz bağlantılarında üç tip mevcuttur. Bunlar LAN arayüzü, WAN ara yüzü ve Yönetim Portlarıdır.





4.2. Router Temel Arayüzleri

Simdi de bir Router'da bulunan temel arayüzleri ve nerede kullanıldıklarına bir göz atalım.

- AUI (Attachment Unit Interface): 15 pin'lik bir arayüzdür ve bir harici transceiver ile

Enhernet ağlara bağlanabilir.

- Seri Arayüzler: Senkron WAN bağlantıları için kullanılırlar. 2400 Kbps ile 1.544 Mbps arasında bir veri hızına destek verirler. Serial 0, serial 1 gibi isimlerle isimlendirilirler..

- BRI Portları: Basic Rate ISDN portu, uzak bağlantılarda ISDN network'ünü kullanmamıza imkan verir. Genellikle asıl bağlantının yanında yedek bir bağlantı olarak kullanılır. Ayrıca Dial on Demond (DOR) özelliği ile eğer asıl link'in yükü çok artarsa bu bağlantıya yardımcı olmak için devreye girebilir.

Konsol Portu: Router'a yerel olarak bağlanıp konfigüre etmek için kullanılan porttur. Varsayılan veri iletim hızı 9600 bps'dir. Bu portu kullanmak için **rollover kablo** kullanılır. Bu kablonun her iki ucunda RJ 45 konnektor bağlanmıştır. Daha sonra bu konnektörlerin bir tanesi PC'nin seri portlarına bağlanabilmesi için RJ45 - 9 pin seri veya RJ45-25 pin seri dönüştürücüsüne takılarak PC'nin seri portlarından birisine takılır. Kullanılan rollover kablonun her iki uçtaki konnektörlere bağlantı sekli ise söyle olmalıdır; Bir uçtaki konnektördeki kablo sırası 1-8 ise diğer uçtaki konnektöre bağlantı sırası ise 8-1 olmalıdır.

- AUX Portu: Router'ı konfigüre etmek için her zaman router'ın yanına gitmek zahmetli

bir istir. Router'ı uzaktan konfigüre etmek için bir modem aracılığıyla Router'ın bu portuna bağlantı kurulup gerekli işlemler yapılabilir.

4.2.1.DTE ve DCE

DTE ve DCE kavramları network'teki cihazları işlevsel olarak sınıflandırmamızı sağlar. DTE cihazları genellikle end-user cihazlardır. Örneğin PC'ler, yazıcılar ve router'lar, DTE cihazlardır. DCE cihazları ise DTE'lerin servis sağlayıcıların ağlarına ulaşabilmek için kullandıkları modem, multiplexer gibi cihazlardır. DCE'ler DTE'lere clock işaretini sağlarlar.

Cisco Router'ların seri interface'leri DTE veya DCE olarak konfigüre edilebilir. Bu özellik kullanılarak WAN bağlantıları simüle edilebilir. Bunun için birbirine bağlı Router'ların interface'lerinden bir tanesini DCE diğer Router'ın interface'sini ise DTE olarak kabul edilir. ardından DCE olarak kabul ettiğimiz interface'in DTE olan interface clock sağlaması gerekir. DCE olarak kullanabileceğimiz interface'de "**clock rate**" komutunu kullanarak bir değer atamamız gerekir. Aksi halde bağlantı çalışmayacaktır. Örneğin;

RouterA(conf-if)#clock rate 64000

Ayrıca clock rate parametresinin yanında "**bandwidth**" parametresininde girilmesi gerekiyor. DCE ve DTE olarak konfigüre edilecek interface'lerde tanımlanan "bandwidth" değerinin aynı olması gerekiyor. Eğer bandwidth değerini belirtmezseniz varsayılan değeri olarak 1,544 Mbps alınır. Bandwidth'e atadığınız değer sadece yönlendirme protokolü tarafından yol seçimi için kullanılır. Örneğin;

RouterA(conf-if)#bandwidth 64

4.2.2.HYPERTERMINAL

Router'ı konfigüre etmek için kullanılan bir terminal emülasyon yazılımıdır. Bu yazılım Win 95/98 ve Win NT ile birlikte geldiği için en çok kullanılan terminal emülasyon programıdır.

Bu programı kullanarak Router'a nasıl bağlantı kurulacağını anlatalım. PC'nin herhangi bir seri portuna taktığımız (COM1 veya COM2) DB-9-RJ45 dönüştürücüye rollover kabloyu takıyoruz. Ardından hyperterminal programını (hypertrm.exe) Start-Programlar-Donatılar'dan çalıştırıyoruz. Karsımıza çıkan "Connection Description" başlıklı pencerede kuracağımız bağlantıya bir isim veriyoruz. Ardından karsımıza çıkan "Connect to" penceresinde ise bağlantının kurulacağı seri port seçiliyor. Bağlantıyı kuracağımız seri portu seçtikten sonra bu portun özelliklerinin belirlendiği bir pencere ile karşılaşıyoruz. Uygun değerleri girdikten sonra Hyper terminal penceresindeki "Call" butonuna basıp Router'a bağlantıyı sağlamış oluyoruz.

4.2.3.IOS (Internetworking Operating System)

IOS, Router ve Switch' lerin yönetilmesinde kullanılan işletim sistemidir. IOS bize CLI (Command Line Interface) denen text görünümünde bir arayüz sağlar. Bu arayüze erişmenin üç temel yolu vardır. Consol Port, Auxilary Port ya da Telnet vasıtasıyla erişmek mümkündür. Consol port ile erişmek için, Roll Over denen, her iki ucu RJ45 ile sonlandırılmış ve bilgisayarımızın com portundan girilmesi için bir dönüştürücüye sahip özel kablolar kullanılır. Bunlara Konsol kablosuda denir. Hyper Terminal yardımıyla CLI' e erişilebilir. Auxilary Port veya Yardımcı portta denilen bu port modem aracılığı ile asenkron çevirmeli bağlantı kullanarak erişmemizi sağlar.

Burada "Varsayılanı Yükle" dedikten sonra Tamam' a basıyoruz ve routerımıza erişimimiz tamamlanıyor.

Telnet ile Router'ımıza erişebilmemiz için öncelikle Telnet oturumunun aktif hale getirilmesi gerekir. Bunun için Telnet ve enable şifreleri verilmelidir. Bu şifrelerin nasıl verileceğini daha detaylı inceleyeceğiz.

4.3. ROUTER Yapılandırması

Router'ın açılması sırasında router konfigürasyon dosyasını arar. Eğer herhangi bir konfigürasyon dosyası bulamazsa sistem konfigürasyon işlemi baslar. Bu işlem sırasında aşağıdaki sorulara "Yes" diye cevap verirseniz Router'ı soru temelli konfigüre edebilirsiniz.

- Continue with configuration dialog? [yes/no]

- Would you like to see the current interface summary? [yes/no]

Bu konfigürasyon türünde router size bir takım sorular sorar ve sizden bu soruların cevaplarını ister. Sorulan soruların varsayılan cevapları soru sonundaki köseli parantezlerin ([]) içinde verilmiştir. Varsayılan cevapları kabul ediyorsanız yapmanız gereken tek şey Enter'a basmaktır. Eğer soru cevap tabanlı konfigürasyondan herhangi bir zamanda çıkmak istiyorsanız o zaman **Ctrl+C** tuşlarına basmanız yeterlidir.

Eğer yukarıda sorulan sorulara "No" diye cevap verirseniz Router'ı konfigüre edeceksiniz demektir. Bu durumda komut satırı aşağıdaki şekildedir.

Router>

Yani ilk düştüğünüz mod "user exec" moddur. Varsayılan olarak konfigüre edilmemiş tüm Router'ların adı Router'dır ve "privileged exec" moda geçmek için herhangi bir şifre tanımlanmamıştır. Router üzerinde herhangi bir konfigürasyon değişikliği yapmak istiyorsak privileged moda geçmemiz gerekiyor. Bunun için komut satırına aşağıdaki komutu yazalım.

Router>enable

Komutu yazdıktan sonra Enter'a basarsanız privileged moda geçersiniz. Bu sırada komut satırının seklinin değiştiğine dikkat edin. Komut satırı su sekli almıştır;

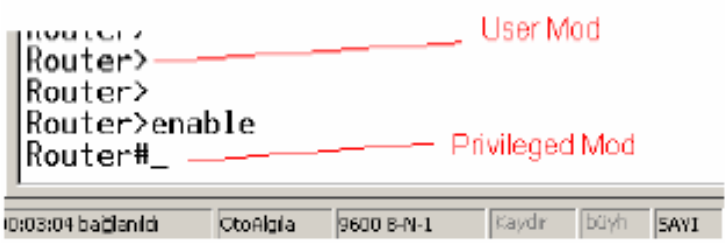
Router#

Privileged exec modan, user exec moda geri dönmek için ise “disable” komutunu kullanabilirsiniz. Router’da tamamen bağlantıyı koparmak için ise “logo ut”, “exit” veya “quit” komutlarını kullanabilirsiniz**.**

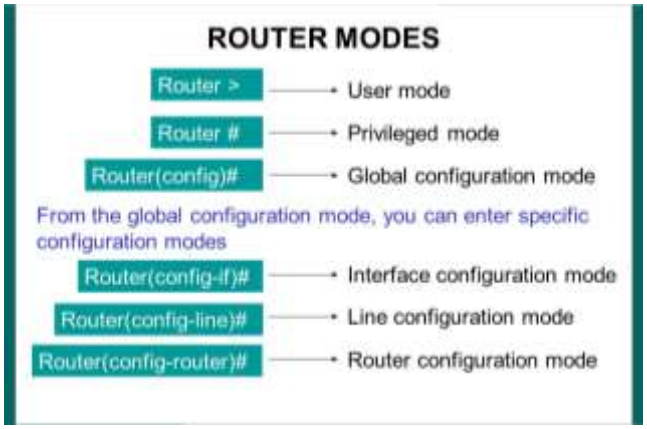
4.3.1.Router Çalışma Modları

User Mod: Router’ ı açıp arayüze eriştiğimiz anda karşımıza çıkan moddur. Burada yönetimsel işlemler yapılamaz. Bir sonraki modlara geçiş için kullanılır.

Privileged Mod: User modda iken “enable” yazıp entera bastığımızda bu moda geçeriz. Bu moda enable moda denir ve önerilen davranış bu moda geçerken şifre konulmasıdır. Zira bir kullanıcı bu moda geçtikten sonra Router’a tamamen hakim olur.



Global Configuration Mod: Config Mod diye de anılan bu moda geçmek için enable moda iken “configure terminal” yazılır ve entera basılır. Bu modda yapılan değişiklikler bürün Router’ı etkiler. Örneğin bu modda iken bir router’a isim verilebilir.



4.3.2.Router Komut Satırı İslemleri

IOS’lar kullanıcılara birçok bakımdan kolaylıklar sunarlar. Örneğin IOS’lar komut kullanımı sırasında kullanıcılara geniş bir yardım seçeneği sunar. Mesela komut satırındayken **?** karakterine basarsanız bulunduğunuz modda kullanabileceğiniz tüm komutlar bir liste halinde karsınıza çıkacaktır. Eğer sıralanan komutlar ekrana sığmıyorsa ekranın alt kısmında **–More-** diye bir ifade belirecektir. Burada space tuşuna basarsanız sonraki komutları bir ekrana sığacak şekilde görebilirsiniz. Yok eğer var olan komutları teker teker görmek istiyorsanız Enter tuşuna basmanız gerekir.

Bunun haricinde IOS’lar komut bazında da yardım sağlıyor. Söyle ki; farzedelimki siz sh harfleriyle baslayan komutları listelemek istiyorsunuz. Bunun için komut satırına sh? yazarsanız sh ile

baslayan tüm komutlar listelenecektir. Ayrıca kullandığınız komutun parametreleri hakkında bilgi almak içinde komutu yazdıktan sonra bir boşluk bırakıp ? karakterine basın. Örneğin show komutuyla birlikte kullanılabilecek parametreleri görmek için show ? ifadesini yazmalısınız.

IOS'un kullanıcılara sağladığı diğer önemli bir kolaylık ise komutların syntax'ını tam yazmaya gerek kalmadan komutu anlayarak zaman kazandırmasıdır. Örneğin Show komutunu kısaltılmış hali sh'dir. Yani siz komut satırından sh girerseniz IOS bunun Show komutu olduğunu anlayacaktır. Komutların kısaltılmış halini belirleyen kural ise o komutun komut listesinde tek (unique) olarak tanımlayabilecek karakter dizisini belirlemektir. Ayrıca komutun kısaltılmıs halini yazdıktan sonra Tab tuşuna basarsanız IOS bu komutu, kısaltılmamış haline tamamlayacaktır. Örneğin show komutunu yazmak için sh yazıp Tab tuşuna basarsanız

IOS bu komutu show seklinde tamamlayacaktır. Ayrıca IOS varsayılan olarak yazdığınız son 10 komutu hafızasında tutar. Bu sayıyı "history size" komutunu kullanarak 256'ya kadar arttırabilirsiniz. Komut yazımı sırasında karşılaşabileceğiniz hata mesajları ve açıklamaları aşağıdaki tabloda verilmiştir.

HATA MESAJI	AÇIKLAMA
%Incomplete command	Yazdığımız komutun tamamlanmadığını, eksik parametre girildiğini belirtir.
%Invalid input	Bu hata mesajıyla birlikte ^ karakteri kullanılır ve bu karekter yanlış girilen omutun neresinde yanlış yapıldığını gösterir.
%Ambiguous command	Girilen komut için gerekli karakterlerin tamamının girilmediğini belirtir. Kullanmak istediğiniz komutu ? karakterini kullanarak tekrar inceleyin.

Asağıgaki tabloda ise komut satırında kullanılabilecek kısayol tusları ve fonksiyonlarını bulabilirsiniz.

Kısayol	İşlevi
Ctrl+A	İmleç'i komut satırının başına taşır.
Ctrl+E	İmleç'i komut satırının sonuna taşır.
Ctrl+N veya (↓)	Router'a son girdiğiniz komutlar arasında gezinmemizi sağlar.
Ctrl+F veya (→)	İmleç'i komut satırında bir karakter sağa götürür.
Ctrl+B veya (←)	İmleç'i komut satırında bir karakter sola götürür.
Ctrl+Z	Konfigürasyon modundan çıkartıp exec moda geri döndürür.
Ctrl+P veya (↑)	Router'a girdiğiniz son komutu gösterir.

4.3.3.Router Configurasyon Komutları

Router üzerinde yapmış olduğunuz değişikliklerin kalıcı olması için bu değişikliklerin konfigürasyon dosyasına yazılması gerekir. Aşağıdaki tabloda Router üzerindeki konfigürasyon ayarlarını görmek, kaydetmek veya silmek için kullanılabilecek komutları bulabilirsiniz.

OS 10.3 ve oncesi	IOS 11.3 ve oncesi	IOS 12.0	Açıklama
Write terminal	Show running-config	More system: startup-config	Router üzerinde çalışan konfigürasyonu gösterir
Show configuration	Show startup-config	More NVRAM: startup-config	NVRAM'de bulunan ve Router boot ederken kullanılan konfigürasyonu gösterir
Write erase	Erase startup-config	Erase NVRAM	NVRAM'de bulunan ve Router boot ederken kullanılan konfigürasyon dosyasını siler
Write memory	Copy runnig-config startup-config	Copy system: running–config	Router üzerinde yapmış olduğumuz konfigürasyon ayarlarının kalıcı olması için NVRAM'daki konfigürasyon dosyasını yazar
Write network	Copy running-config TFTP	Copy system: running-config FTP; TFTP	Çalışan konfigürasyonunu FTP veya TFTP server'a kaydetmek için kullanılır

4.3.4.Ios'un Yedeklenmesi Ve Geri Yüklenmesi

Cisco IOS'ların yedeklenmesi ve yedekten geri yüklenmesi için kullanılan komutlar aşağıdaki tabloda listelenmiştir

Komut	Açıklama
Copy flash tftp	Router'ın flash'ındaki IOS'un yedeğini TFTP server'a kopyalar.
Copy tftp flash	TFTP server'da bulunan bir IOS imajını flash'a kopyalamak için kullanılır.
Copy running-config tftp	Router üzerinde çalışan konfigürasyonu TFTP sunucuna kopyalar.
Copy tftp running-config	TFTP sunucunda bulunan bir konfigürasyon dosyasını router'a yükler.

4.3.5. Router Configurasyonu -I

Router'ı konfigüre etmek yönlendirme yapabilecek duruma getirmek için ilk önce Router'a login oluyoruz. Ardından privileged exec mode geçmeniz gerekiyor. "enable" yazıp bu mode giriyoruz. Ardından router'a onu konfigüre edeceğimizi belirten "configure terminal" komutunu veriyoruz. (Bu komutun kısa yazılısı ise "config t"dir.) Simdi Router'ı konfigüre etmeye başlayabiliriz. İlk önce Router'ımıza bir isim vererek başlayalım. Bunun için "**hostname**" komutunu aşağı şekilde giriyoruz.

Router(config)#hostname RouterA

Bu komutu girdikten sonra komut satırı aşağıdaki gibi olacaktır.

RouterA(config)#

Router'ımıza bağlanan kullanıcılara bir banner mesajı göstermek isteyebiliriz. Bunu gerçekleştirmek için "**banner motd**" komutunu aşağıdaki şekilde kullanmalıyız.

RouterA(config)#banner motd#turkmcse.com Router'ına hosgeldiniz#

Burada komuttan sonra kullandığımız # karakterlerinin arasına mesajımızı yazıyoruz **.**Şifre belirleme önemli bir işlemdir. Router'larda beş farklı şifre bulunur.

Bunlardan ikisi privileged mod'a erişim için **t**anımlanırken, bir tanesi konsol portu, bir tanesi AUX portu ve diğeri de Telnet bağlantıları için tanımlanır. Bu şifrelerden "**enable secret**" ve "**enable**

password", privileged mod'a geçmek için kullanılırlar ve aralarındaki fark "enable secret"'in şifrelenmiş bir şekilde saklanmasıdır.

Yani konfigürasyon dosyasına baktığınızda "enable secret" şifresinin yerinde şifrelenmiş halini görürsünüz. Ama aynı dosyada "enable password"'u ise açık bir şekilde şifreleme yapılmadan saklandığını görürsünüz. Bu da sizin konfigürasyon dosyanızı ele geçiren birisinin "enable password" şifresini kolayca okuyabileceğini ama "enable secret" şifresinden bir şey anlamayacağı anlamına gelir. "Enable password" sifresi ise "enable secret" şifresi tanımlanmamışsa veya kullanılan IOS eski ise kullanılır. "Enable secret" şifresinin konfigürasyon dosyasına yazılırken kullanılan şifrelemenin derecesini ise "**service passwordencryption**" komutu ile belirleyebilirsiniz.

"Enable secret" ve "enable password" şifreleri aşağıdaki şekilde tanımlanır.

RouterA(config)#enable password cisco

RouterA(config)#enable secret cisco

Burada cisco bizim koyduğumuz şifrelerdir. Eğer Router'ın konsol portuna şifre koymak istiyorsanız

RouterA(config)#line console 0

RouterA(config-line)#login

RouterA(config-line)#password cisco

Router'ın AUX portuna şifre koymak için:

RouterA(config)#line aux 0

RouterA(config-line)#login

RouterA(config-line)#password cisco

Router'ın Telnet bağlantılarında soracağı sifreyi ise söyle belirleyebilirsiniz:

RouterA(config)#line vty 0 4

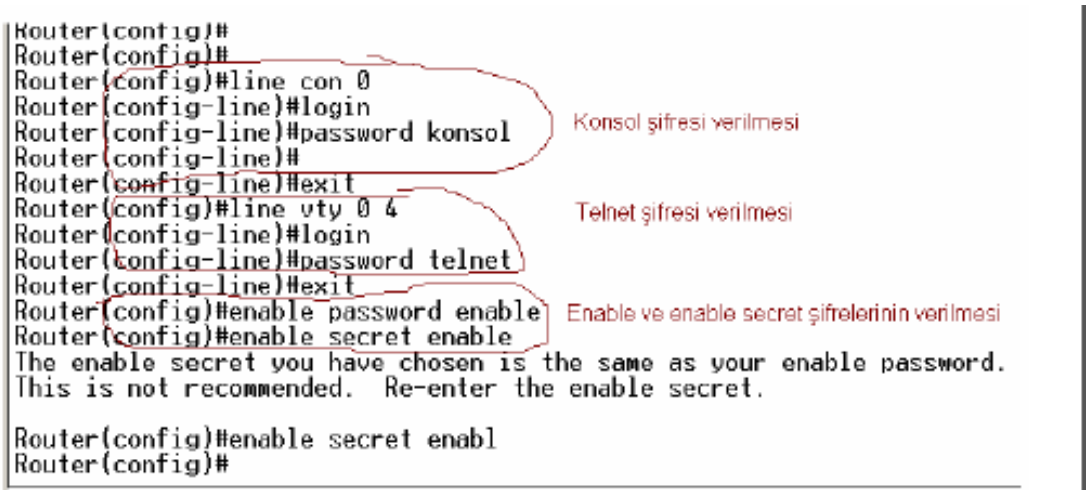
RouterA(config-line)#login 17

RouterA(config-line)#password turkiye

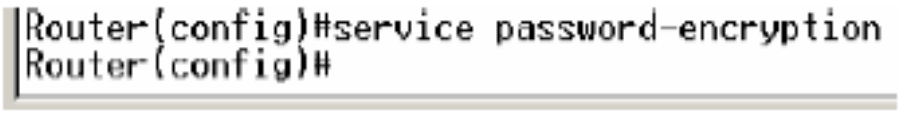
Burada telnet portlarının tamamına aynı şifre verilmiştir. Bu portların her birisine farklı şifreler atanabilir. Fakat router'a yapılan her telnet isteğine router, o zaman kullanımda olmayan bir port'u atadığı için bağlantıyı kuran kişinin tüm bu telnet portlarına atanmış şifreleri bilmesi gerekir. Bu yüzden telnet portlarına ayrı ayrı şifre atamak iyi bir yaklaşım değildir. Bunun haricinde Router'a yapılan konsol bağlantılarının, kullanıcı herhangi bir işlem yapmadan ne kadar süre aktif kalacağını da **"exec-timecut**" komutuyla belirleyebiliriz.

4.3.6. Enable, Telnet Ve Konsol Şifreleri Verme

Enable şifresi Global Configuration modda verilirken konsol ve telnet şifreleri line Configuration mod denilebilecek alt modlarda verilebilir. Enable şifre "**enable secret**" komutu kullanılarak 5. leveldan şifrelenebilirken telnet ve konsol şifrelerinde bu mümkün değildir. Fakat 7. leveldan şifrelenebilirler ve bunun için gerekli komutumuz "**service-password encryption**"dır. Bir Router' a "enable secret" ve "enable" şifreleri, aynı olmamak şartıyla birlikte verilebilir. Bu durumda "enable secret" şifresi geçerli olacaktır.



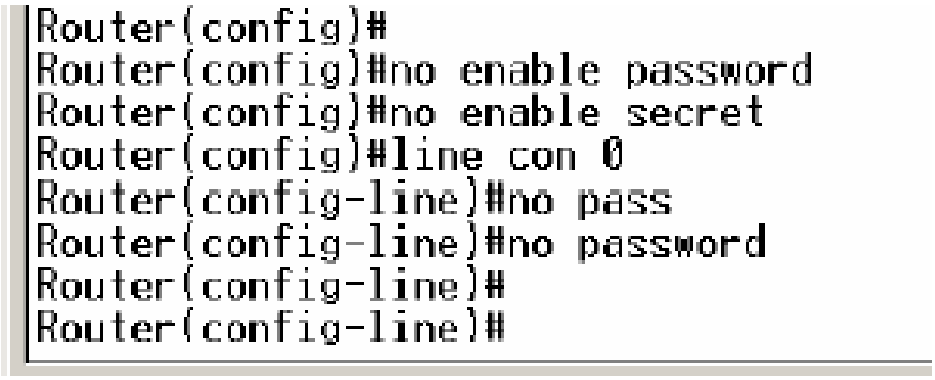
(Dikkat edilirse enable ve enable secret şifrelerinin aynı olmasına izin verilmiyor)



(Sifrelerin 7. leveldan encrypted edilmesi)

Sifre verirken kullandığımız “login” komutu dikkatinizi çekmiştir. Default olarak şifresiz kabul edilen Router’ a bu komut ile artık kendisine şifre vasıtasıyla erişileceği bilgisini vermiş

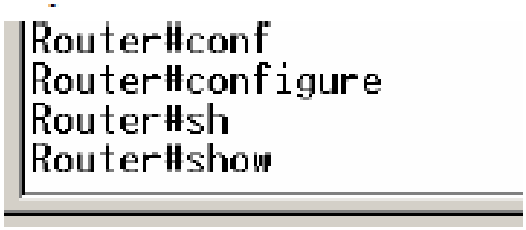
“ no enable secret” gibi bir komut ile enable secret şifresini kaldırabiliriz.



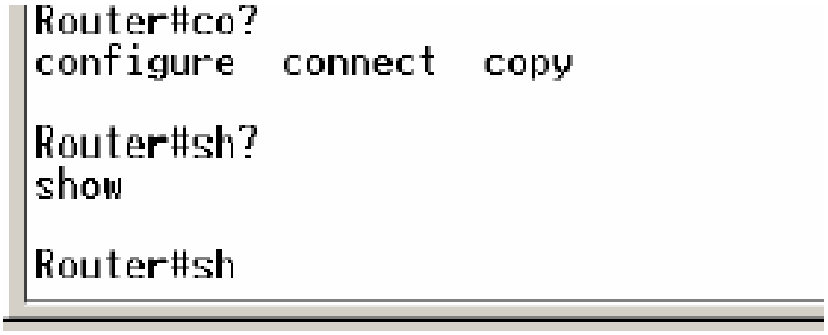
oluyoruz. Bütün komutlar basına ”no” yazılarak geçersiz hale getirilebilir. “ no enable secret” gibi bir komut ile enable secret şifresini kaldırabiliriz.

4.3.7. Yardım Alma

Router konfigürasyonu sırasında kullanacağınız komutun ilk harflerini yazıp tab tuşuna bastığınızda, yazdığınız komut bulunduğunuz mod için geçerliyse ve o harflerle başlayan başka bir komut yoksa Router sizin için komutu tamamlayacaktır.



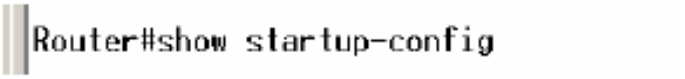
Ve yine devamını hatırlamadığınız komutlar için sonuna "?" koymak suretiyle yardım alabilirsiniz.



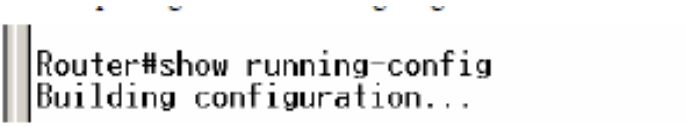
4.3.8. Konfigürasyon Dosyaları

Routerın açılış konfigürasyonunun tutulduğu **startup-config** ve çalışan konfigürasyonunun tutulduğu **running-config** adı altında iki dosyası vardır. Bir router' ın running-config ve startup-config dosyalarını **"show**" komutu ile görebilir, "**copy**" komutu ile birbirleri üzerine kopyalayabilir, "**erase**" komutu ile silebiliriz.

Startup-Config: NVRAM'da bulunur, yeni alınmıs bir Router için üzerinde hiçbir bilgi bulunmaz. Ve böyle bir Router açılışta startup ve running konfigürasyonunun bir sihirbaz yardımıyla yapıp yapmayacağımız sorusunu sorar. Bu sihirbaz gereksiz ve boşa zaman harcatan bir çok soru ile doludur ki önerilen konfigürasyonu manuel yapmaktır.



Running-Config: RAM'da bulunur ve Router'ın çalıştığı andaki konfigürasyonunu tutar. Router kapatıldığında buradaki bilgiler gider.



Bir Router yeniden başlatıldığı zaman startup-config dosyası dolu ise, IOS tarafından bu dosya alınıp RAM'a aktarılır ve dolayısıyla o artık Running-config olmuştur. Bir router' ın running-config ve startup-config dosyalarını "show" komutu ile görebilir, "copy" komutu ile birbirleri üzerine kopyalayabiliriz.

```
Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

```
Router#erase nvram:
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
Router#
```

Write Komutu

Kopyalama ve silme işlemlerinde "Write" komutu da kullanılabilir. Write komutu ile birlikte kullanılabilecek komutlar aşağıdadır.

```
erase     Erase NV memory
memory    Write to NV memory
network   Write to network TFTP server
terminal  Write to terminal
<cr>
```

Kısaca "wr" yazmak Running Konfigürasyonumuz NVRAM'a kayıt edecektir.

4.3.9. Şifre Kırma

Routerın şifrelerini unuttuğunuzu yada ikinci el bir Router aldığınızı ve bu router' ın konfigürasyon dosyalarının hala üzerinde olduğunu dolayısıyla şifrelerini bilmediğinizi varsayalım. Böyle bir durumda şifreyi değiştirmek istersek ve eski konfigürasyonun bozulmamasını da sağlayarak bunu yapmak mümkündür. Bu ilk bakışta bir güvenlik açığı gibi görünse de, bu işlemin yapılabilmesi için konsoldan router' a bağlanmamız, dolayısıyla fiziksel olarak router'ın yanında olmamız gerekeceği için açık denilemez. Zira fiziksel olarak erişilebilen bir router' ın şifreleriyle oynayabilmenin bir sakıncası yoktur. Adım adım şifre kırma işlemini inceleyecek olursak;

1. Router açılırken Ctrl+Break tuşlarına basılarak Rom Monitöre girilir. Burada "Router>" yerine "rommon>" ifadesiyle karşılaşacağız.

```
monitor: command "boot" aborted due to user interrupt
rommon 1 >
rommon 1 >
rommon 1 >
rommon 1 >
```

2. "confreg" komutu ile başlangıç register' ı değiştirilir ve NVRAM yerine direk RAM' dan çalışmaya başlaması sağlanır. Bu sayede mevcut konfigürasyon NVRAM' da bulunmaya devam ederken Router RAM'dan sıfır konfigürasyon ile açılacaktır. 0x2102 olan register 0x2142 olarak değiştirilmelidir.

```
rommon 1 >
rommon 1 > confreg 0x2142

You must reset or power cycle for new config to take effect
rommon 2 > _
```

3. Router yeniden başlatılır. Açıldığında Router' ın herhangi bir şifre sormadığını göreceksiniz.

4. Enable moda geçilir. Bu moda geçtikten sonra artık istediğimiz her şeyi yapabileceğimize göre, eski konfigürasyonu kaybetmek istemiyorsak, "copy startupconfig running-config" komutu ile o dosyayı alır ve şifreleri değiştirip yeniden NVRAM' a kaydederiz.

```
Router#copy startup-config running-config
Destination filename [running-config]?
499 bytes copied in 0.889 secs
Router#
```

Bundan sonra istediğimiz değişiklikleri yapıp running-config dosyasını tekrar Startupconfig üzerine yeni haliyle kopyalayabiliriz.

5. Son olarak Rom Monitör' e girip değiştirdiğimiz register' ı eski haline getirip (0x2102) getirip Router' ımızı yeniden başlatabilir ve eski konfigürasyon ve yeni şifreyle router'ın açıldığını görebiliriz.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#conf
Router(config)#config-register 0x2102
Router(config)#_
```

4.3.10. Temel Router Konfigürasyonu

Bir router' ın çalışması için şifre vermekten çok daha fazlası gerekir. En temel gereklilik ise Router' ın interface' lerine ip adresi atamaktır. Router' ın interfaceleri default olarak shutdown durumdadır ve bunun kaldırılması gerekir ki bu da ip adresinin atadıktan sonra ilgili interface' e "no shutdwon" komutu vermek ile mümkündür. Bir router' ın interfacelerinden herhangi birine ip adresi atamanın diğerinden farkı yoktur. Yapılacak işlemler sırasıyla interface konfigürasyon moduna geçmek, ip adresini subnet maskı ile birlikte yazmak ve "no shutdown" ile interface' i aktif hale getirmektir. Eğer bu interface için bir açıklama eklemek istiyorsanız bunu aşağıdaki gibi "description" komutunu kullanarak yapabilirsiniz.

RouterA(config-if)#description Pazarlama Grubunun LAN bağlantısı

Konfigüre ettiğiniz interface'in işlevselliğini yerine getirebilmesi için aktif (up) olması gerekiyor. Varsayılan olarak bütün interface'ler pasif (administratively disabled)'dir. Bunun için ise aşağıdaki komutu kullanmalısınız.

RouterA(config-if)#no shutdown

Ayrıca aşağıdaki formatta bir komut kullanarak interface tanımlamalısınız; Interface tip slot/port adaptör/port numarası

Örneğin; RouterA(config)#interface ethernet 2/0/0

1.1.1. Debug İşlemi

Router üzerinde hata ayıklamak için kullanılabilecek komutlar mevcuttur. Bu komutların başında “debug” komutu gelir.

RouterA#debug all

Unutulmaması gereken bir nokta da debug işleminin Router’ın kaynaklarını bir hayli fazla kullandığıdır. Bu yüzden debug işlemi bitirildikten sonra “undebug all” veya “no debug all” komutlarından bir tanesi kullanılarak Router’a debug yapmaması gerektiği bildirilmelidir.

4.3.11. CDP (Cisco Discovery Protocol)

Data Link katmanında çalışan bu protokol Cisco tarafından geliştirilmiştir ve fiziksel olarak birbirine bağlı tüm Cisco cihazlarının birbirleri hakkında bilgi sahibi olmalarını sağlar. IOS 10.3 veya daha yukarı versiyon çalıştıran Router’larda CDP default olarak aktifdir ve otomatik olarak komşu Router ve switch’ler hakkında bilgi toplar. Bu bilgiler arasında cihaz ID’si ve cihaz tipi gibi bilgilerde bulunur.

CDP kullanılarak öğrenilen bilgileri privileged mod’da “show cdp neighbors” komutunu kullanarak görebilirsiniz. Bu komutu kullandığınızda fiziksel olarak bağlı olduğunuz cihazların isimlerini, portlarını, cihaz tiplerini(router,switch vs.) ,sizin router’ınıza hangi interface’inin bağlı olduğunu,bu cihazların hangi platforma ait olduğunu, holdtime değerini interface isimlerini görebilirsiniz.

CDP ile toplanmış bilgileri daha ayrıntılı bir şekilde görmek istiyorsanız “show cvp neighbor detail” komutunu kullanmalısınız.

Bu komutun çıktısında ise show cdp neighbors komutunun çıktısında bulunan bilgilere ek olarak cihazda kullanılan IOS versiyonu, IP adresleri gibi bilgileri bulabilirsiniz.

Eğer CDP protokolünün Router üzerinde çalışmasını istiyorsanız o zaman global konfigürasyon modunda iken “no CDP run” komutunu girmelisiniz.

Ayrıca CDP’yi interface bazında da pasif yapabilirsiniz. Bunun için interface konfigürasyon modunda iken “no CDP enable” komutunu girmelisiniz.

Örnek bir çalışma olarak Router’ımıza şu ip adreslerini atayalım.

Ethernet Interface Ip adresi : 192.168.1.1 / 24 Serial (0/0)

Interface Ip Adresi: 192.168.2.1 /24 Serial (0/1)

Interface Ip Adresi : 192.168.3.1 /24

```
Router(config)#interface et
Router(config)#interface ethernet 0/0
Router(config-if)#ip addr
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
```

(Ethernet 0/0 interface'ine ip adresi verildi)

```
Router(config)#interface serial 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

(Serial 0/0 interface' ine ip adresi verildi)

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

(Serial 0/1 interface' ine ip adresi verildi)

Buradaki 0/0, 0/1 gibi ifadeler standart olmamakla birlikte Router' ımızın üzerinde yazıyor olmalı. Eğer yazmıyorsa, Router'ımıza "show running-config" komutunu verip hangi interface' in hangi numaraya sahip olduğunu öğrenebiliriz. Router' ımıza gerekli şifreleri verip interfacelerine de gerekli ipleri atadıktan sonra "Show running-config" ile göreceğimiz text ifade şu şekilde olacaktır.

```
Router#sh running-config
Building configuration...
Current configuration : 526 bytes
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Router
memory-size iomem 10
ip subnet-zero
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
half-duplex interface Serial0/0
ip address 192.168.2.1 255.255.255.0
no fair-queue
interface Serial0/1
ip address 192.168.3.1 255.255.255.0
!
ip classless ip
http server
dial-peer cor custom
!gatekeeper
Shutdown
line con 0
```

```
line aux 0
line vty 0 4
!
End
```

4.3.12. Router'a Telnet İle Bağlanma

Router üzerinde bir konfigürasyon yapılacak olması mutlaka Router'a fiziksel olarak erişmeyi yani Konsol' dan bağlanmayı gerektirmez. Router'a Telnet ile de bağlanılabilir. Tüm Router ve switch'ler Telnet isteklerine cevap verecek şekilde, üzerlerinde Telnet server servisi çalışır vaziyette gelirler. Bunun yanında tüm Router'ları ve bazı switch'ler Telnet istemci programı ile birlikte gelir ve ağ yöneticilerinin Router'ları uzaktan yönetmesini sağlar. Privileged modda iken herhangi bir Router'a bağlanmak için "telnet" veya "connect" komutlarını kullanabilirsiniz. Bu komutlar parametre olarak bağlantının kurulacağı Router'ın IP adresini veya host ismini alır. Eğer parametre olarak host ismi kullanılmışsa Router'da DNS ayarlarının yapılması gerekir. Ya da Router'daki host tablosuna "ip host" komutunu kullanarak bu host'a ait kayıt girilmelidir. Fakat bunun için bazı şartların yerine gelmesi gerekir. Öncelikle Router' ın Ethernet interface' i up olmalıdır ve Telnet, Enable şifreleri verilmiş olmalıdır. Telnet şifresi verilmediğinde "Password Required, but none set" şeklinde bir hata mesajı alınacak ve bağlan gerçekleştirilemeden kaybolacaktır.

```
Router(config)#
Router(config)#enable pass
Router(config)#enable password academytech
Router(config)#line vty 0
Router(config-line)#pass
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

(Telnet ve Enable Şifrelerinin Verilmesi)

```
Telnet 192.168.1.175

User Access Verification

Password:
Password:
Router>enable
Password:
Password:
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname AcademyTech
AcademyTech(config)#exit
AcademyTech#copy run
AcademyTech#copy running-config star
AcademyTech#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
AcademyTech#
```

Görüldüğü gibi şifreler verildikten sonra bağlantı gerçekleştirilebilir ve her türlü konfigürasyon yapılabilir.

Örneğin aşağıdaki komutla adı RouterB ve IP adresi 10.3.10.1 olan router'ın kaydı host tablosuna girilmektedir.

RouterA(config)#ip host RouterB 10.3.10.1

Eğer router'ın isim çözümleme işini host tablosuyla değilde DNS sunucu ile halletmek istiyorsanız o zaman Router'a DNS sunucunun adresini "ip name-server" komutunu kullanarak belirtmelisiniz.

RouterA(config)#ip name-server 10.3.9.2

Router'ın komut satırında herhangi bir şeyi örneğin bir komutu yanlış veya eksik yazarsanız router bunun bir isim olduğunu farzedip DNS sunucuyu arayacak ve bu ismi çözmeye çalışacaktır. Bu işlemde bir hayli zaman alacaktır. Böyle bir durumda beklememek için Ctrl+Shift+6 tuş kombinasyonuna bastıktan sonra X tuşuna basıp bu işlemi sonlandırabilirsiniz.

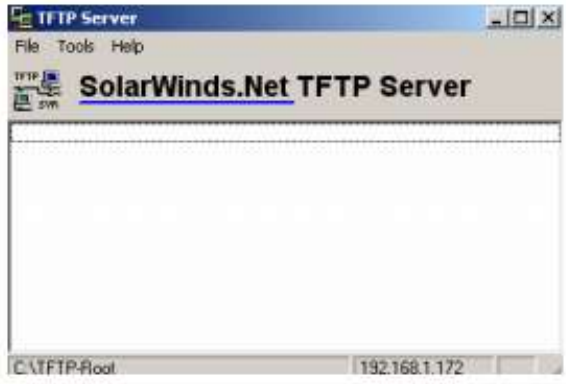
Bunun haricinde bu tuş kombinasyonu uzak sistemlere yapılan telnet bağlantısını askıya alıp kendi router'ınıza geri dönmek içinde kullanılır.

Bir telnet otrumunu kapatmak için "disconnect", "exit", "quit" veya "logo ut" komutlarını kullanabilirsiniz. Eğer birden fazla Router'a Telnet ile bağlanmışsanız bu bağlantıları "show session" komutunu kullanarak görebilirsiniz.

Şekilde ki gibi bir tabloyla karşılaşıldığında anlaşılması gereken gerekli şifrelerin verilmemiş olduğudur. Önceki bölümlerde öğrendiğimiz gibi şifreleri verdikten sonra bağlantımızı gerçekleştirebiliriz.

4.3.13. TFTP SERVER'A YEDEK ALMA

Konfigürasyonu yapılmış bir Router'ın startup ve running-config dosyalarının yedeklerini almak akıllıca bir harekettir. Bu TFTP Server sayesinde mümkün. Ve yine TFTP sayesinde Flash' ın yedeği alınabilir, güncellemesi yapılabilir. TFTP Server normal bir PC'ye yükleyeceğimiz UDP protokolünü kullanan ufak bir programdır. Bu program network üzerinden TFTP isteklerini karşılamak için devamlı networkü dinler. TFTP Server' a yedek alınabilmesi için kurulu olduğu bilgisayarın ip adresini, flas' ın yedeği alınacaksa onun tam adını bilmek gerekir. Flash' ın tam adını "Show version" komutu ile öğrenebiliriz. "copy" komutu bundan sonrasını kendisi halledecektir.



Copy startup-config tftp:

Copy running-config tftp:

Copy flash tftp

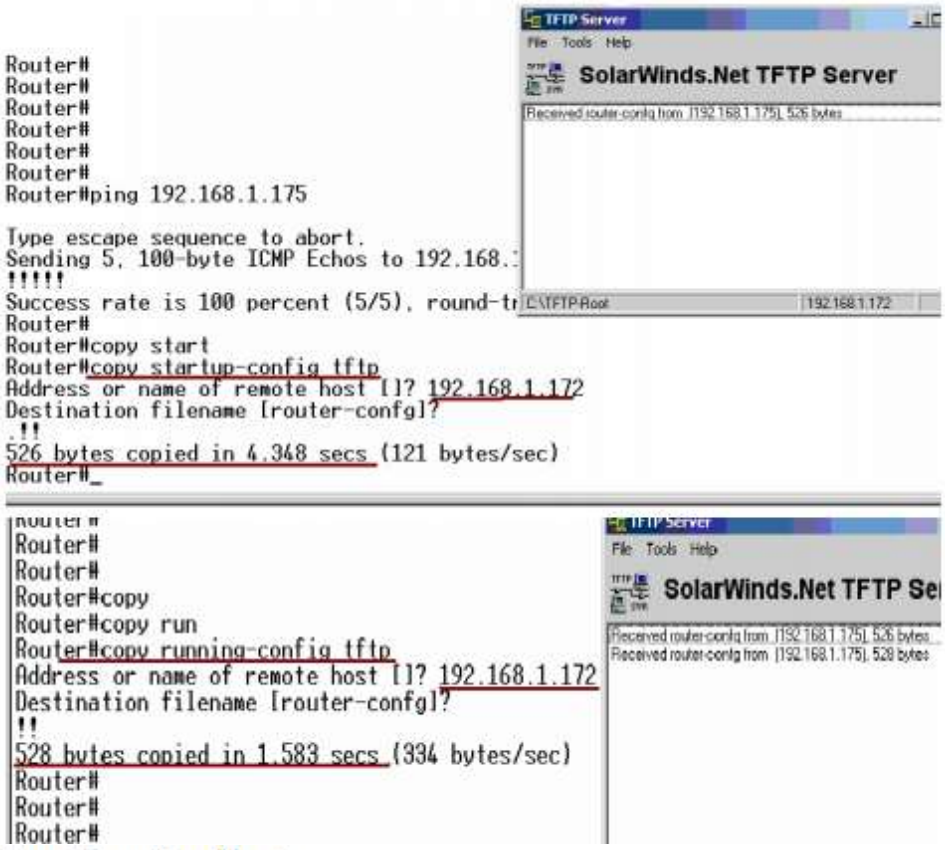
Gibi bir komut yazdığımız da bize ilk olarak TFTP Server'ın ip adresi ve şayet Flas' ın yedeğinin alacaksak onun tam adını soracaktır. Ve bütün bunlar yapılırken TFTP Server çalışıyor durumda olmalı.

TFTP Serverdan geri yüklemelerde ise komut tam tersi yazılarak çalıştırılacaktır.

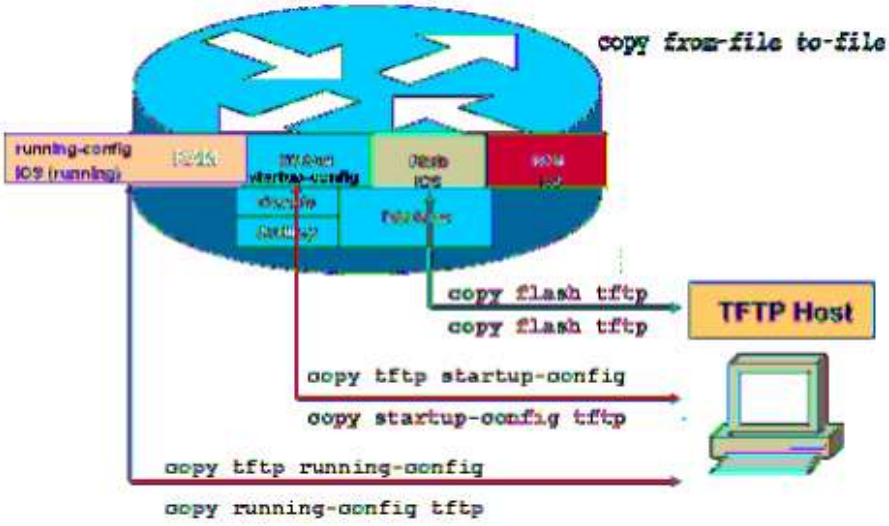
Copy tftp startup-config

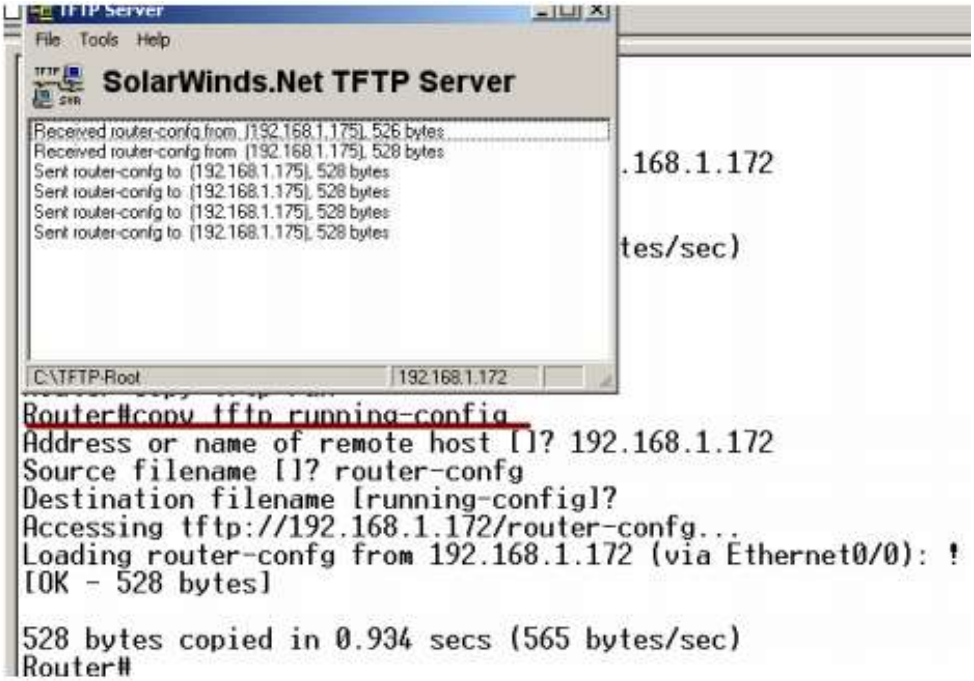
Copy tftp running-config

Copy tftp flash



Copy Komutları Özet





4.3.14. IOS YEDEK ALMA VE YÜKLEME

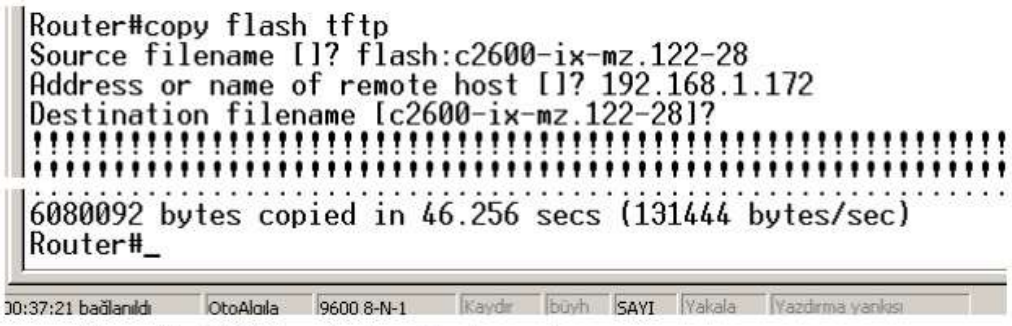
TFTP Server kullanarak IOS' in yedeği alınabilir veya IOS yüklenebilir. Bunun için Sistem Imağe File' ın tam dosya adı bilinmelidir ve bu "show version" komutu ile öğrenilebilir. Alınan bütün yedekler gibi IOS' in yedeği de TFTP Server tarafından TFTP-Root klasörünün altına atılır.

```
ROM: System Bootstrap, Version 11.3(2)XA3, PLATFORM SPECIFIC RELEASE SOFTWARE (f
c1)
ROM: C2600 Software (C2600-IX-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Router uptime is 34 minutes
System returned to ROM by power-on
System image file is "flash:c2600-ix-mz.122-28"

cisco 2610 (MPC860) processor (revision 0x202) with 36864K/4096K bytes of memory
.
Processor board ID JAB024903E2 (2074409390)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
 --More--
```

Yedek alırken startup-config ve running-config' den farklı olarak dikkat edilecek tek konu hedef dosya adıdır ve şekilde belirtildiği gibi tam adı olmalıdır.



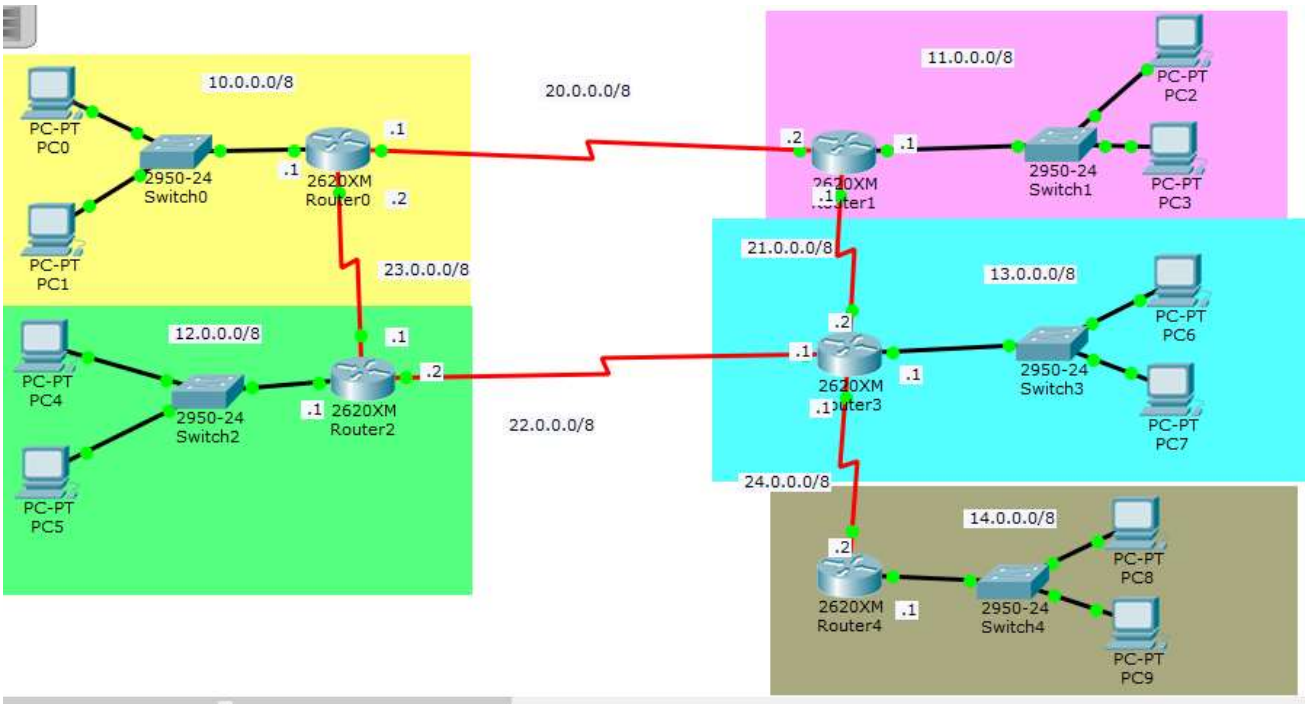
("copy flash tftp" komutuyla yedek alınması)

(Yedekleri alınan dosyalar TFTP-Root klasörünün altında)

IOS olmadığında router ethernet interface' ine ip adresi veremeyeceğimizde IOS' in konsoldan yüklenmesi gerekmektedir. Bunun için kullanılacak iletişim kuralı "xmodem"' dir ve konsol hızı 115200 bps' a çıkarılmalıdır. Tabii ki bu işlemlerin tamamı Rom Monitör (Rommon) kullanılarak yapılabilir.

Bunun için Router açılırken Ctrl+Break tuşlarını basılara Rommon' a girilir ve konsol hızı 115200 bps' a çıkartılır. (Flash tamamen boş ise, IOS yoksa CTRL+Break tuşlarına basmaya da gerek yoktur. Zira IOS olmadığı zaman Router direk Rommon' dan açılır.) Bu durumda ilk bağlantımız 9600 bps ile yapıldığı için kopacaktır. Hyper Terminal' de bağlantı hızı 115200' e çıkarılarak yeniden bağlanılır. Rommon açılıp komut satırında "confreg" yazıldığında router bize değiştirmek istediğimiz bölümleri sıralayacak ve burada sadece konsol hızı için evet deyip uygun hızı seçeceğiz. Ve router' ı yeniden başlatmamız istenecek.

UYGULAMA FAALİYETİ - 4



İşlem Basamakları	Öneriler
Yukarıdaki PC, switch ve Router ları yerleştirip, gerekli bağlantıları tamamlayın.	
Her Router için gerekli yapılandırmayı tamamlayın	Router(config)#hostname R0 R0(config)#enable secret disco R0(config)#int fa0/0 R0(config-if)#ip address 10.0.0.1 255.255.255.0 R0(config-if)#no shutdown R0(config-if)#exit R0(config)#line console 0 R0(config-line)#login R0(config-line)#password disco R0(config-line)#exit
Ağların birbiri ile haberleşmesi için gerekli RIP yönlendirmesini yapın	

ÖĞRENME FAALİYETİ–5

AMAÇ

Yönlendirme iletişim kuralını kavrayarak yönlendirme tablosunu görüntüleyip yönlendiricileri tespit edebileceksiniz.

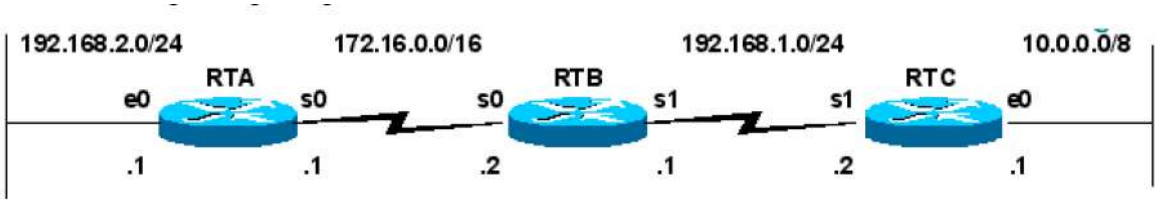
ARAŞTIRMA

IP adresi ve alt ağ maskesi (subnet mask) hangi ölçütlere göre verilmektedir. Bu konuyla alakalı topladığınız bilgileri sınıfta tartışınız. RIP, IGRP yönlendirme protokollerini araştırınız.

5. YÖNLENDİRME (ROUTING)

Routing en basit ifadeyle bir uzak networke gitmek için gereken yol bilgisinin Router' lar tarafından sağlanmasıdır. Routerlar kendilerine gelen paketlerde, hedef ip adresi olarak, nerede olduğunu ve nasıl gidileceğini bildikleri bir networkten adres bulunduğunda, hedefe yönlendirme yaparlar. Aksi takdirde paketi yok ederler. Routerler uzak Networklerin adreslerini oluşturdukları bir "Routing" tablosunda tutarlar. Bu bilgiler manuel olarak yada otomatik olarak tutulur. Manuel olarak tutulmasına Static Routing , Otomatik olarak tutulmasına Dynamic Routing denir.

Routerlar için Directly Connected networklerine herhangi bir yönlendirme yazmaya gerek yoktur. İki Routeri birbirine bağladığınızda ve interfacelerini uygun şekilde konfigure edip up durumuna getirdiğinizde Routing Tabla' larda o networkler ile ilgili bilgileri görürüz.

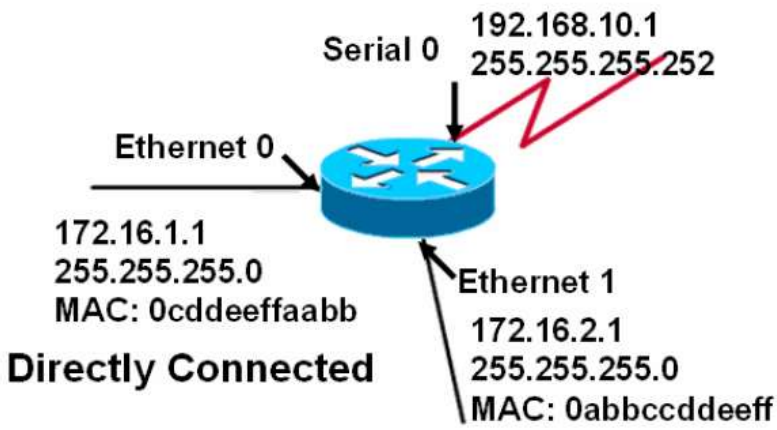


Böyle bir networkte interfaceleri up duruma getirdiğimizde Routing Tabla' lar aşağıdaki gibi olacaktır.

```
RTA#show ip route
Codes: C - connected,.....................................
C    172.16.0.0/16 is directly connected, Serial0
C    192.168.2.0/24 is directly connected, Ethernet0

RTB#show ip route
Codes: C - connected,.....................................
C    172.16.0.0/16 is directly connected, Serial0
C    192.168.1.0/24 is directly connected, Serial1

RTC#show ip route
Codes: C - connected,.....................................
C    10.0.0.0/8 is directly connected, Ethernet0
C    192.168.1.0/24 is directly connected, Serial1
```



5.1. Static Routing

Static Routing "ip route" komutu ile Global Configuration modda yapılır ve küçük ölçekli networklerde ideal çözümdür.Statik route networklerde Routing tablosuna hedef network'e ulaşılacak olan yolun manuel olarak(elle) girilmesi işlemidir. Küçük yapılarda kullanılır,karmaşık yapılarda farklı protokoller uygulanır.

Static Routing yapılırken hedef network adresi, subnet maskı ve bizi o hedefe götürecek

bir sonraki routerın ip adresi bilinmelidir. Burada bir sonraki router ile ilgili bir kavram ortaya

çıkıyor; "next hop". Bunlar bilindiğinde komut su şekilde kullanılacaktır.

Router(config)#ip route [hedef adres][subnet mask][Next Hop] [distance]

Bu komut yönlendirme tablosundan silinmek istendiğinde ise basına "no" ifadesini yazmak yeterli olacaktır. Distance ifadesi seçimlik olup gerektiği durumlarda Routingler arasında önceliği belirlemeye yarayan Administrative Distance değerini değiştirmek için kullanılır. Static Routing için Administratice Distance default olarak "1" dir.

Router'da tanımlanmış statik kayıtları görmek için privileged modda iken "**show IP route**" komutunu kullanmalıyız.

Karsımıza çıkan listedeki kayıtların basında bulunan C harfi fiziksel olarak birbirine bağlı ağlara olan yönlendirmeyi, S harfi yönlendirmenin statik olduğunu S* isareti ise kaydın default yönlendirme olduğunu gösterir.. C ile baslayan satırlar "**Directly Connected"** networklerdir, Routerlar kendi Directly Connected networklerini bilirler ve bu networkler ulasmak için yönlendirme yapılmasına gerek yoktur.

Default yönlendirmenin router'larda çalısabilmesi için "ip classless" komutunun girilmesi gerekir. Ayrıca statik bir kaydı yönlendirme tablosunda silmek için "no ip route" komutunu parametreleriyle birlikte kullanmanız gerekir.

NOT: Cisco Router'ların seri interface'leri DTE veya DCE olarak konfigure edilebilir. Bu özellik kullanılarak WAN bağlantıları simüle edilebilir. Bunun için birbirine bağlı Router'ların interface'lerinden bir tanesini DCE diğer Router'ın interface'sini ise DTE olarak kabul ediyoruz. Ardından DCE olarak kabul ettigimiz interface'in DTE olan interface clock sağlaması gerekiyor. DCE olarak kullanabileceğimiz interface'de "clock rate" komutunu kullanarak bir değer atamamız gerekiyor. Aksi halde bağlantı çalışmayacaktır. Örneğin;

RouterA(conf-if)#clock rate 64000

Eğer bir interface sebebi ne olursa olsun "down" ise o interface bağlı network Routing Table, da görünmez.

5.2. Default Routing

Burada ISP Routeri ile bağlanılan networke (Internet) R1 üzerinde default route yazılarak ulasılabiliecektir.Default hedefi bilinmeyen paketleri yönlendirmek için yazilabilecek Route satırıdır seklinde tanımlanabilir.

R1(config)#ip route 0.0.0.0 0.0.0.0 Serial3/0 yada

R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2

5.3. Dynamic Routing

Dynamic Routing' te Static Routing' de olduğu gibi sabit bir tanımlama yapmak yerine her Router' a kendi Directly Connected networklerini, çeşitli Routing Protokoller ile tanımlıyoruz. Ve ilgili Routing protokolün çalışma mantığına göre en iyi yol seçimi (Best Path Determination) Router tarafında gerçekleştiriliyor.

Burada bahsettiğimiz Routing Protokolleri üç başlık altında incelememiz mümkün.

1. Distance Vector Protokoller (RIP, IGRP)

2. Link State Protokoller (OSPF)

3. Hybrid Protokoller (EIGRP)

Distance Vector protokoller routing table update mantığıyla çalışırlar. Yani belirli zaman aralıklarında sahip oldukları network bilgilerini komşu routerlarına gönderirler ve komşu

routerlarından da aynı bilgileri alırlar. Bu döngünün sonunda her router sistemde ki bütün networkleri öğrenmiş olur ve uygun yol seçimini yapar.

Link State Protokoller ise sürekli bir update yapmak yerine, komşu routerlarının up olup olmadıklarını anlamak için küçük "Hello" paketleri gönderirler. Sadece gerektiği zamanlarda, yeni bir router ortama eklendiğinde veya bir router down olduğunda, sadece o bilgi ile ilgili update gerçekleştirirler.

Hybrid Protokoller hem Distance Vector hem de Link State protokollerin bazı özelliklerini taşır. Bu gruba üye olan EIGRP Cisco tarafından ortaya çıkarılmıştır ve sadece Cisco routerlarda çalışır.

5.4. Distance Vector Protokoller

5.4.1. **RIP** (RIPv1)

Rip (Routing Information Protocol) en iyi yol seçimi yaparken tek kriter olarak hop sayısına bakar. Rip tanımlanarak oluşturulmuş bir networkte maksimum hop sayısı 15' dir. 16. hop' tan sonra Destination Unreachable hatası verecektir. Rip ile tanımlanan routerlar her 30 saniyede bir kendisinde tanımlı olan networkleri komşu routerlarına iletirler. Burada dikkat edilmesi gereken bir konu, RIP ile tanımlanan bir networkün bağlı bulunduğu interface' i, aynı zaman da routing update gönderilecek bir interface olarak seçiyor olmamızdır. Rip classfull bir routing protokoldür. Yani konfigürasyon sırasında subnet mask girilemez ve subnet masklar update sırasında ip adresinin sınıfına ait subnet mask seçilerek gönderilir. Rip konfigürasyonu diğer bütün routing protokoller de olduğu gibi oldukça basittir. (Bütün subnet maslar 255.255.255.0)

Rip Load Balancing

Load Balancing tam olarak yükü birden fazla yol arasında dağıtmak demektir. (Routerlar metricler eşit olduğu için load balancing yapar) Mantıksal olarak düşündüğümüz de Rip' in load balancing yapma ihtimali her zaman vardır. Çünkü referans olarak bir tek hop sayısına bakar. Oysa diğer protokoller de load balancing ihtimali en iyi yol seçimi sırasında bir çok kriter göz önüne alındığı için mucize derecesinde zayıf bir ihtimaldir.

5.4.2. Split Horizon

Bir Router kendi directly connected networkünü başka bir router'dan da öğrenirse öğrendiği bilgiyi çöpe atar. Ayrıca router'ın ağ üzerinde herhangi bir değişiklik olduğunu anladığında bu değişikliği, öğrendiği interface haricindeki interface'lerden yayınlamasını sağlar. Böylece router'lar değişikliği sadece bir yönde yayınlarlar.

5.4.3. IGRP (Interior Gateway Routing Protocol)

IGRP Cisco tarafından geliştirilmiş bir uzaklık-vektör algoritmasıdır. Bu yüzden

network'te IGRP çalıstırmak için tüm router'ların Cisco olması gerekir. IGRP'de maksimum

hop count değeri 255 dir ve RIP'te tanımlanabilecek maksimum hop count olan 15'den çok daha büyük bir değerdir. Bunun haricinde IGRP, RIP'ten farklı olarak en iyi yolu seçerken kullanılan metric değeri için varsayılan olarak, hattın gecikmesi **(delay)** ve band genisliğini **(bandwidth)** kullanır. Bunun haricinde güvenilirlik **(reliability),** yük **(load)** ve MTU**(Maximum Transmission Unit**) değerleri de metric hesabında kullanılabilir.

IGRP Load Balancing

Her Routing protocol esit metrikli yollara Yük dağıtımı yapar ancak IGRP konusan Routerlardan esit olmayan yollar için load balancing yaptirilabilir. (Bu durum EIGRP tarafından da desteklenmektedir.)

Bunun için **"variance"** komutu kullanılır.

Örnek;

```
Router(config)#router igrp 102
Router(config-router)#network 10.1.1.0
Router(config-router)#network 192.168.1.0
Router(config-router)#network 172.16.1.0
Router(config-router)#variance 2
```

Burada Router variance ile belirtilmiş sayısı alıp en küçük metrik değeri ile çarpar ve o değerin altında metriğe sahip yollar arasında load balancing yapar.

IGRP Konfigurasyonu

IGRP' de tıpkı Rip gibi classfull bir routing protokoldür. IGRP konfigürasyonu Rip' in ki ile büyük ölçüde aynıdır. Burada tek fark aynı sistemde çalıştığımızı belirtmek için kullanacağımız **Autonomus System** numarasıdır. Kısaca **AS** denebilir. **Bütün Routerlarda aynı AS kullanılmaz ise routerlar arasında iletişim olmaz.** Router üzerinde IGRP'yi çalıştırmak için aşağıdaki komutu girmeniz gerekiyor.

```
RouterA(config)#router igrp 10
RouterA(config-router)#network 172.16.0.0
```

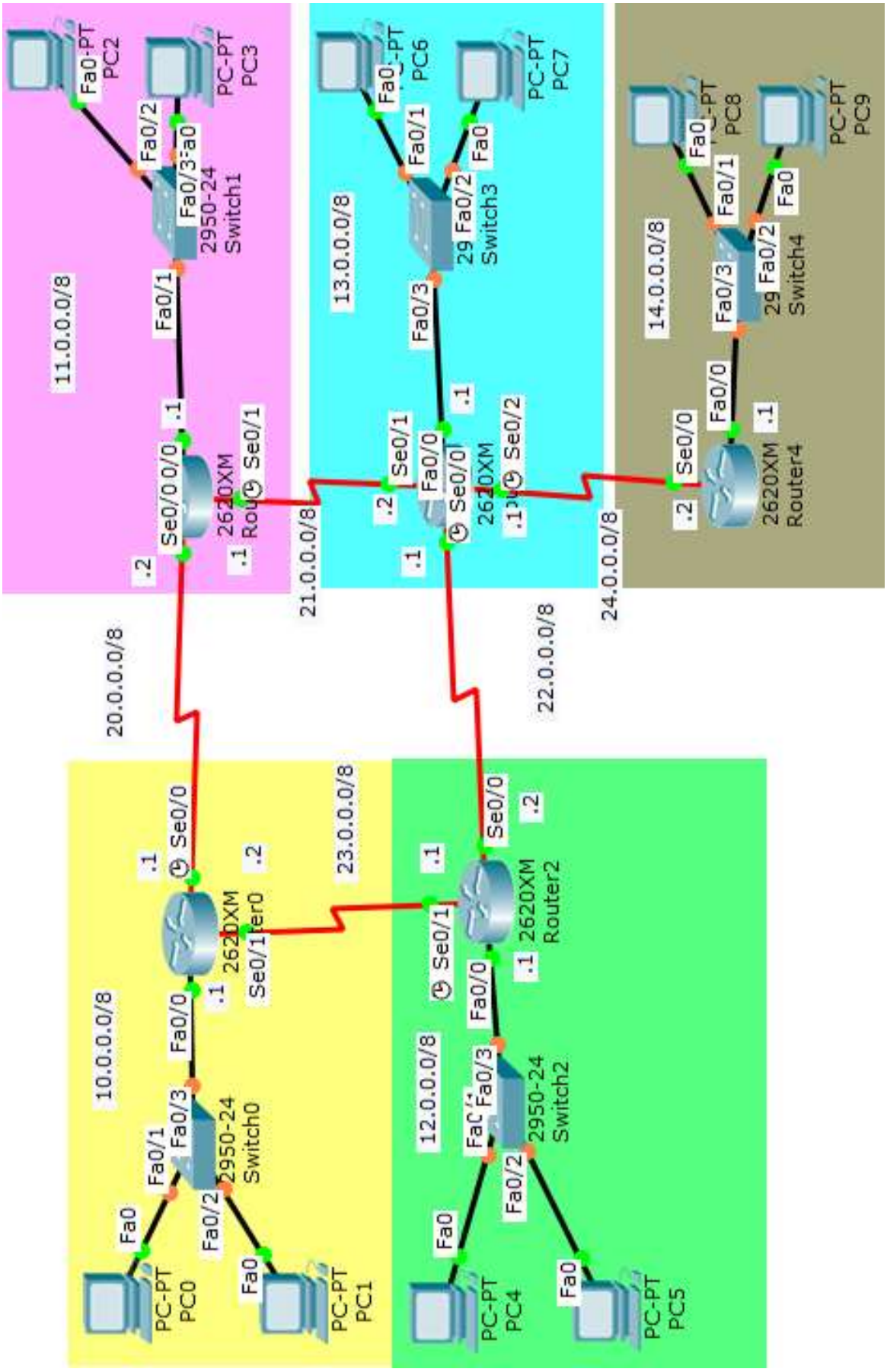
Yukarıdaki komutta router'a autonomous system (AS) numarasının 10 olduğunu ve bağlı bulunduğu ağın IP numarası bildiriliyor.

KOMUT	AÇIKLAMA
Show protocol	Her bir interface'in Network katmanı adresini ve interface'lerin aktif (up) mi yoksa pasif(down) mi olduğunu gösterir.
Show ip protocol	Router'da çalışan yönlendirme protokolleri hakkında özet bilgi verir.
Debup ip rip	Router tarafından gönderilen ve alınan yönlendirme güncellemelerinin konsol portuna da yollanmasını sağlar. Böylece yönlendirme işlemlerini izleyebilirsiniz. Eğer telnet ile router'a bağlıysanız bu güncellemeleri izleyebilmek için "**terminal monitor**" komutunu kullanmalısınız.
Debug ip igrp (events/transactions)	Eğer events parametresi ile kullanılırsa ağ üzerindeki IGRP yönlendirme bilgileri hakkında özet bilgi sunar. Transactions parametresi ile birlikte kullanılırsa komşu router'lara yapılan güncelleme istekleri ile broadcast mesajları hakkında bilgi verir.

5.4.4. RIPv2

Rip protokolünün classfull olması ve uygulamada sorunlar çıkarması sebebiyle geliştirilmiş ve Classless olan versiyonu çıkarılmıştır: Ripv2. Classless olmasının yanında bir önemli fark da Ripv2 nin updatelerini broadcast adresinden değil 224.0.0.9 multicast adresinden göndermesidir.

UYGULAMA FAALİYETİ - 5



STATIC YÖNLENDİRME UYGULAMASI	
İşlem Basamakları	**Öneriler**
Router 0, Router1, Router2, Router3 ve Router4 için Statik yönlendirme yapın	R1(config)#ip route 20.0.0.0 255.0.0.0 se0/0 R1(config)#ip route 11.0.0.0 255.0.0.0 fa0/0 R1(config)#ip route 21.0.0.0 255.0.0.0 se0/1
Show ip route komutunu kullanarak her router'ın static yönlendirme tablosuna kaydettiğinizi görün.	R1#sh ip route Gateway of last resort is not set S 10.0.0.0/8 is directly connected, Serial0/1 C 11.0.0.0/8 is directly connected, FastEthernet0/0 S 12.0.0.0/8 is directly connected, Serial0/1 S 13.0.0.0/8 is directly connected, Serial0/0 S 14.0.0.0/8 is directly connected, Serial0/1 C 20.0.0.0/8 is directly connected, Serial0/0 C 21.0.0.0/8 is directly connected, Serial0/1
RIP UYGULAMASI	
İşlem Basamakları	**Öneriler**
Router 0, Router1, Router2, Router3 ve Router4 için RIP Protokolünü kullanarak yönlendirme komutlarını girin.	R1>en R1#conf t R1(config)#router rip R1(config-router)#version 2 R1(config-router)#network 20.0.0.0 R1(config-router)#network 11.0.0.0 R1(config-router)#network 21.0.0.0
Show ip route komutunu kullanarak her router'ın RIP Protokolünü kullanarak diğer networkleri yönlendirme tablosuna kaydettiğinizi görün.	R1(config-router)#do sh ip rou Gateway of last resort is not set R 10.0.0.0/8 [120/1] via 20.0.0.1, 00:00:24, Serial0/0 C 11.0.0.0/8 is directly connected, FastEthernet0/0 R 12.0.0.0/8 [120/2] via 21.0.0.2, 00:00:13, Serial0/1 [120/2] via 20.0.0.1, 00:00:24, Serial0/0 R 13.0.0.0/8 [120/1] via 21.0.0.2, 00:00:13, Serial0/1 R 14.0.0.0/8 [120/2] via 21.0.0.2, 00:00:13, Serial0/1 C 20.0.0.0/8 is directly connected, Serial0/0 C 21.0.0.0/8 is directly connected, Serial0/1 R 22.0.0.0/8 [120/1] via 21.0.0.2, 00:00:13, Serial0/1 R 23.0.0.0/8 [120/1] via 20.0.0.1, 00:00:24, Serial0/0 R 24.0.0.0/8 [120/1] via 21.0.0.2, 00:00:13, Serial0/1

ÖĞRENME FAALİYETİ–6

AMAÇ

Yönlendirme iletişim kuralını kavrayarak yönlendirme tablosunu görüntüleyip yönlendiricileri tespit edebileceksiniz.

ARAŞTIRMA

IP adresi ve alt ağ maskesi (subnet mask) hangi ölçütlere göre verilmektedir. Bu konuyla alakalı topladığınız bilgileri sınıfta tartışınız. EIGRP, OSPF yönlendirme protokollerini araştırınız.

6. ACCESS LISTS (Erisim Listeleri)

Access list'ler sistem yöneticilerine, ağdaki trafik üzerinde geniş bir kontrol imkanı

sunar. Ayrıca access list'ler router üzerinden geçen paketlere izin vermek veya reddetmek içinde kullanılır. Bunun haricinde telnet erişimleri de access list'ler kullanılarak düzenlenebilir.Olusturulan access list'ler router'daki interface'lerin herhangi birisine giren veya çıkan trafiği kontrol edecek şekilde uygulanabilir. Eğer herhangi bir interface'e bir access list atanmışsa router bu interface'den gelen her paketi alıp inceleyecek ve access list'te belirtilen islevi yerine getirecektir. Yani ya o paketi uygun yöne iletecek yada paketi yönlendirmeden yok edecektir.

1. Access List' lerde kriterler satır satır belirtilmiştir. Gelen isteklerin kriterlere uyup uymadıkları sırayla belirlenir.

2. İlk eslesen kriterin bulunduğu satıra gelindiğinde o satırda ki aksiyon (deny ya da permit) gerçekleştirilir.

3. paketleri yoket" (implicit deny all) kuralı uygulanır.

Access List' ler 3 Baslık altında incelenirler:

1. Standart ACL

2. Extended ACL

3. Named Acl

Named Accces Listler hem standart hem de Extended olarak kullanılabilirler. Access Listler arasındaki bu ayırım Acces List Numaraları ile yapılır. Access Listler su numaraları alabilirler;

Access List Numarası	Açıklama
1-99 arası	IP standart access list
100-199 arası	IP extended access list
1000-1099 arası	IPX SAP access list
1100-1199 arası	Extended 48-bit MAC address access list
1200-1299 arası	IPX summary address access list
200-299 arası	Protocol type-code access list
300-399 arası	DECnet access list
400-499 arası	XNS standart access list
500-599 arası	XNS extended access list
600-699 arası	Appletalk access list
700-799 arası	48-bit MAC address access list
800-899 arası	IPX standart access list
900-999 arası	IPX extended acess list

Access List' ler oluşturulurken dikkat edilmesi gerekenler şunlardır;

1. Oluşturulduktan sonra mutlaka bir interface ile ilişkilendirilmelidir aksi takdir de aktif olmayacaktır.

2. Kriterler satır satır uygulanacağı için listeler oluşturulurken en belirgin kriterden en genel kritere doğru Yukarıdan başlayarak organize edilmelidir.

3. Listeden satır silmek ve satır eklemek sadece Named ACL' lerde mümkündür. Diğer listelerde silme işleminde satır değil listenin tamamı silinir. Bu durumda araya satır eklenmek isteniyorsa liste bir yazı editörüne aktarılıp değişiklik orada yapılmalıdır.

4. Standart Access Listler mümkün olduğu kadar hedefe, Extended Access Listler mümkün olduğu kadar kaynağa yakın olmalıdır.

5. Access Listlerin en sonundan görünmeyen bir satır oluştuğunu ve bu satırında diğer satırlardaki herhangi bir kritere uymayan istekleri yok ettiğini söylemiştik.

6. Dolayısıyla mutlaka ve mutlaka bir Access List grubunda "permit" aksiyonu olmalıdır.

7. Access Listler sadece Router üzerinden giden veya gelen trafiği düzenlemek için kullanılabilirler. Router' ın sebep olduğu trafik için kullanılamazlar.

8. Access Listler' den satır çıkaramasanız ve satır eklediğinizde de o satır en son satır olarak yerini alır. Dolayısıyla kriterlerinizi yeniden düzenlemek bu şekilde imkansızdır.

(Named Access List' ler hariç) Bu durumda yapılması gereken Access List' i bir text editörüne kopyalayıp gerekli değişiklikleri yaptıktan sonra ger kopyalamaktır.

Access Listler oluşturulurken subnet Mask yerine Wild Card Mask denilen ve subnet

Maskın 255' e tamamlanmasıyla elde edilen bir maske kullanılır. Örneğin 255.255.128.0 subnet maskının wild-card maskı 0.0.127.255 olacaktır.

Tek bir host belirtmek için kullanılacak;

Ip adresi: 192.168.1.2

Wild-Card Mask: 0.0.0.0

6.1. STANDART ACCESS LİSTLER

Bu tür access list'te IP paketlerinin sadece kaynak (source) adreslerine bakılarak

filtreleme yapılır. Izin verme yada yasaklama bütün protokol kümesi için geçerlidir. Router(config)#acces-list {Access list numarası} {permit / deny} {kaynak} {mask}

Seklinde kullanılır. Burada ki "permit" izin vermek için, "deny" yasaklamak için kullanılır. Daha sonra uygulanacak olan interface' gidilerek "ip Access-group {numarası} in/out" komutuyla interface ile ilişkilendirilir. Burada ki in ve out komutlara isteğe göre içeriden dışarıya (in) ve dışarıdan içeriye (out) olan trafiği kısıtlamak için kullanılır.

Örneğin networkümüz de bulunan 192.168.1.100 ip adresine sahip bilgisayarın dışarıya çıkısını önlemek istersek komut satırında;

Router(config)#access-list 1 deny 192.168.1.100 0.0.0.0

Router(config)#access-list 1 permit any

Router(config)#interface Ethernet 0/0

Router(config-if)#ip Access-group 1 in

Yazmalıyız. Burada 1. satırda ilgili hosta "deny" uygulandı, 2.satırda diğer hostların "implicit deny all" kuralı ile yok edilmemeleri için kalan hostlara "permit uygulandı, 3 ve 4.satırlarda ise oluşturulan Access list Ethernet interface' ile ilişkilendirildi. " Access listlerde "{ip adresi wild-card mask}" yerine "host {ip adresi}" kullanılabilir. Fakat networklere bir aksiyon uygulanacaksa Wild-Card Mask kullanılmalıdır.

6.2. EXTENDED ACCESS LİSTLER

Bu tür Access listler de kaynak ile birlikte kullanılan protokol, hedef ip adresi ve hedef

port numarası da kısıtlanabilir.

Örneğin 192.168.1.100 bilgisayarının 212.1.1.8 bilgisayarına 80. porttan erişememesini,

aynı bilgisayara 25. porttan erişebilmesini, diğer bilgisayarlar için herhangi bir kısıtlama olmamasını istiyoruz. (Söz konusu portlar TCP çalısır) Bu durumda komut satırına;

Router(config)#access-list 101 deny tcp host 192.168.1.100 host 212.1.1.8 eq 80

Router(config)#access-list 101 permit tcp host 192.168.1.100 host 212.1.1.8 eq 25

Router(config)#access-list 101 permit ip any any

Yazmak ve gerekli interface'e uygulamak yeterli olacaktır.

6.2.1. NAMED ACCESS LİSTLER

Diğer Access Listlerden sadece konfigürasyon sırasında farklılık gösterir. Named Acces listler acces-list numarası vermek yerine akılda kalması da kolay olacak, isimler kullanılır. Named Access List' lerde satırlar tek tek silinebilir veya yeni satır eklenebilir. Çünkü listenin Standart ve Extended olmasına göre uygun modlar olusturulur ve konfigürasyon bu modlar altında yapılır.

6.3. EIGRP (Enhanced Interrior Gateway Routing Protocol)

Cisco daha önce gelistirdiği IGRP' nin yetersiz kalması ve RIP'in RIPv2'ye

yükseltilmesiyle bos durmamıs, EIGRP' yi gelistirmis ve bu protokolü sınıflandırmada da, hem Distance Vektör hem de Link State protokollerin özelliklerini tasıdığı için Hybrid baslığı altına yerleştirmiştir.

Bütün Routing protokolleri gibi EIGRP' de Routing update mantığı ile çalısır fakat Rip ve IGRP' den farklı olarak belirli zaman aralıklarında tüm networklerin bilgisini göndermektense küçük hello paketleri yollayarak komsu routerlarının up olup olmadıklarını kontrol eder. Komsu routerlardan gelen Acknowledgement paketleriyle o routerın hala up olduğu kabul eder.

Hello ve Acknowledgement mesajları dikkate alındığında burada TCP gibi bir protokolün kullanılması gerekliliği ortaya çıkar. Fakat bu işlemler sırasında EIGRP yine Cisco'nun geliştirdiği ve RTP (Reliable Transport Protocol) protokolünü kullanır. Çalışma mantığı TCP ile aynıdır. Gerektiği zamanlarda, sözgelimi yeni bir router eklendiğinde veya bir router down olduğunda, "ADD" yada "DELETE" bilgilerini yollar. Bir router ortama dâhil olduğunda öncelikle bir Query paketi yollar ve bu paketlerden gelen Reply' lar ile komsu routerları hakkında bilgi edinir ve topoloji tablosunu oluşturur. Buraya kadar anlattıklarımızla EIGRP' nin 5 farklı paket ile çalıştığını söyleyebiliriz.

EIGRP Paketleri

Hello Acknowledgement

Update Query

Reply

6.4. OSPF (Open Shortest Path First)

OSPF Link State Protocol olup, ulaşılmak istenen networke giden en kısa yolu Dijkstra algoritması kullanarak tespit etmektedir.

"Hello" protokolü ile OSPF çalışan routerlar komsularını keşfederler. Hello paketleri her 10 saniye de bir gönderilir ve bu paketlerden alınan sonuçlara göre OSPF database oluşturulur.

OSPF metrik için Cost adı verilen değeri kullanırlar. Standart bir tanımı yapılamamakla birlikte Cisco Routerlar da ön görülen OSPF metriği bant genişliği ile ters orantılıdır.

(cost= 10.000.000 / bantgenisliği)

Bu protokolde, networkteki yönlendirme bilgilerini kendisinde toplayıp, diğerlerine

dağıtacak bir router vardır. Bu routera Designated Router denir ve DR olarak kısaltılır.

DR aktif olmadığı durumlarda Backup Designated Router devreye direr. (BDR)

OSPF Link State bir protokoldür.

Hızlı yayılma özelliğine sahiptir. VLSM (Variable Length subnet Mask) ve CIDR (Classless Inter Domain Routing) desteği vardır.

Metric hesabi tamamen bant genişliği üzerine kuruludur. Distance Vector protokollerin aksine periyodik updateler yapmaz, gerektiğinde yani networkte değişiklik olduğu zaman update yapar.

Area 0 Backbone area olarak adlandırılır ve diğer bütün arealar ancak area 0 üzerinde birbirleriyle konuşabilirler. Komsu Routerlarına 10 saniye aralıklar ile gönderdiği Hello paketleri ile komşuluk ilişkilerini başlatır ve devam ettirir. Non-Broadcast Multi Access (NBMA) networklerde 30 saniyedir.

6.5. Cisco Router' In Dhcp Server Olarak Konfigüre Edilmesi

Cisco Router' larda DHCP server default olarak çalısır durumdadır. Herhangi bir nedenle daha önceden DHCP Server devre dısı bırakıldıysa;

Router(config)# service dhcp

komutu ile DHCP Server aktif hale getirilebilir. Yine istendiği zaman basına "no"

konularak devre dışı bırakılabilir.

Router(config)# no service dhcp

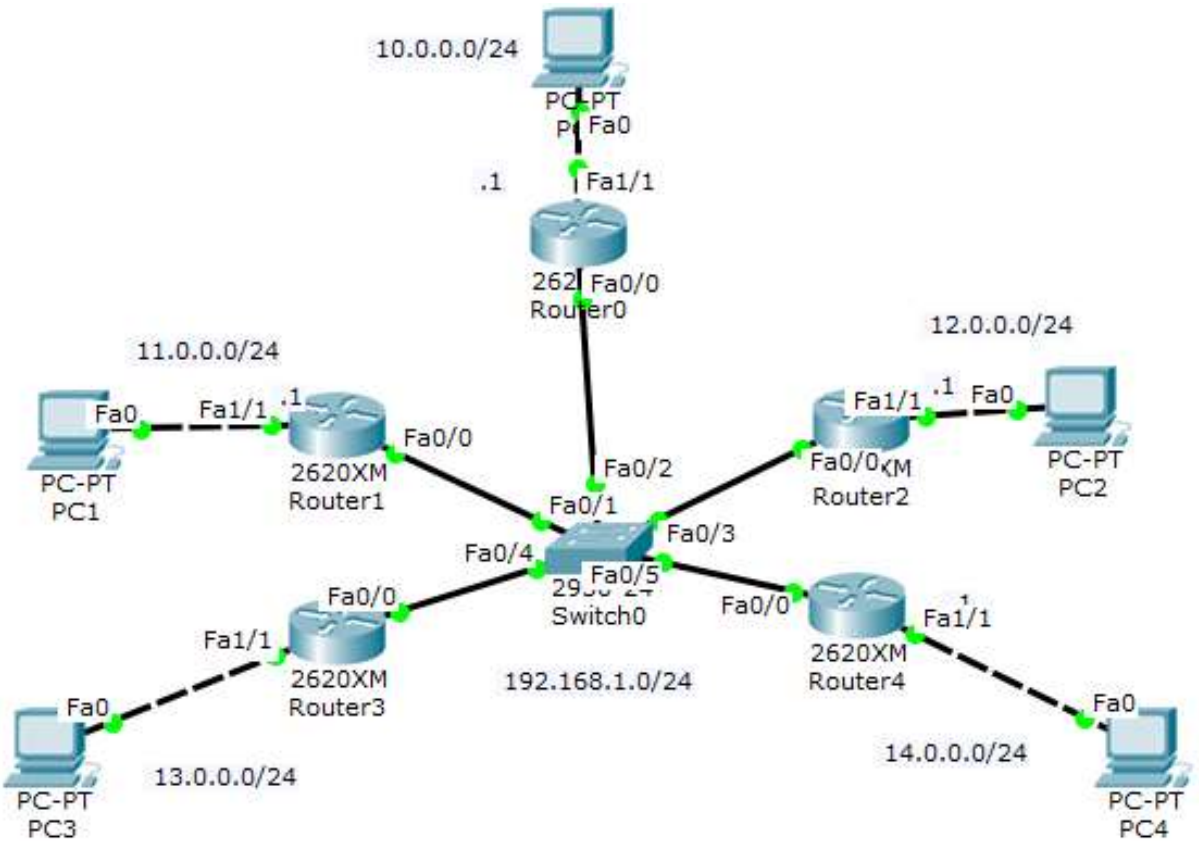
Router' ın DHCP hizmeti verebilmesi için, hangi aralıklarda hangi networke ait ip adreslerinin dağıtılacağı bilgisinin Router' a bildirilmesi gerekir.

Bunun için su komutlar yazılmalıdır.

Router(config)#ip dhcp pool poolismi

Router(Config-dhcp)# network ip_aralığı mask subnet_maski

UYGULAMA FAALİYETİ - 6



OSPF UYGULAMASI	
İşlem Basamakları	**Öneriler**
LOOPBACK interface ayarlarını yapın	R0(config)#interface loopback 0 R0(config-if)#ip address 192.168.100.254 255.255.255.0 R1(config)#int loopback 0 R1(config-if)#ip address 192.168.100.253 255.255.255.0 R2(config)#interface loopback 0 R2(config-if)#ip address 192.168.100.252 255.255.255.0 R3(config)#interface loopback 0 R3(config-if)#ip address 192.168.100.251 255.255.255.0 R4(config)#interface loopback 0 R4(config-if)#ip address 192.168.100.250 255.255.255.0

OSPF yapılandırmasını tamamlayın	R0(config)#router ospf 100 R0(config-router)#network 192.168.1.0 0.0.0.255 area 0 R0(config-router)#network 10.0.0.0 0.255.255.255 area 0 R1(config-router)#router ospf 100 R1(config-router)#network 192.168.1.0 0.0.0.255 area 0 R1(config-router)#network 11.0.0.0 0.255.255.255 area 0 R2(config)#router ospf 100 R2(config-router)#network 192.168.1.0 0.0.0.255 area 0 R2(config-router)#network 12.0.0.0 0.255.255.255 area 0 R3(config)#router ospf 100 R3(config-router)#network 192.168.1.0 0.0.0.255 area 0 R3(config-router)#network 13.0.0.0 0.255.255.255 area 0 R4(config)#router ospf 100 R4(config-router)#network 14.0.0.0 0.255.255.255 area 0 R4(config-router)#network 192.168.1.0 0.0.0.255 area 0
AUTHENTICATION işlemini tamamlayın	R0#conf t R0(config)#interface fa0/0 R0(config-if)#ip ospf authentication R0(config-if)#ip ospf authentication-key cisco R1#conf t R1(config)#interface fa0/0 R1(config-if)#ip ospf authentication R1(config-if)#ip ospf authentication-key cisco R2#conf t R2(config)#interface fa0/0 R2(config-if)#ip ospf authentication R2(config-if)#ip ospf authentication-key cisco R3#conf t R3(config)#interface fa0/0 R3(config-if)#ip ospf authentication R3(config-if)#ip ospf authentication-key cisco R4#conf t R4(config)#interface fa0/0 R4(config-if)#ip ospf authentication R4(config-if)#ip ospf authentication-key cisco

KAYNAKÇA

www.megep.gov.tr

www.ciscorouting.com/

www.studynotes.net/

www.conniq.com/

www.bilgisayarnedir.com/

www.teknik-bilgi.com/

www.ozengen.com/

windows.microsoft.com/

www.bilgisayarkavramlari.com

www.magicfinger.net

www.webhatti.com/

www.veribaz.com/

web.itu.edu.tr

www.guashan.com

www.yeniforumuz.biz

http://www.pcegitim.net/

http://www.practicallynetworked.com

http://tr.wikipedia.org

Mustafa SAYAR, Afyon Kocatepe Üniversitesi

Ağ Simülasyon Yazılımı Yardım Menüsü

MEGEP Bilişim Sistemleri Ağ Simülasyonu Ankara,2012

Açık Kaynak Kodlu Network Simülasyonları, Yrd.Doç.Dr. Enis Karaarslan