T.C.

BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

İNTERNET YÖNLENDİRME TEMELLERİ, MPLS VE BGP PROTOKOLÜ İLE ROTA MANİPÜLASYONU

(Yüksek Lisans Tezi)

Tezi Hazırlayan : **Gökhan TATAR**

İstanbul, 2013

TC

BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

İNTERNET YÖNLENDİRME TEMELLERİ, MPLS VE BGP PROTOKOLÜ İLE ROTA MANİPÜLASYONU

(Yüksek Lisans Tezi)

Tezi Hazırlayan :

Gökhan TATAR

Öğrenci No:

110820018

Danışman:

Yrd. Doç. Dr. Ediz ŞAYKOL

İstanbul, 2013

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum “ İnternet Yönlendirme Temelleri, MPLS ve BGP Protokolü İle Rota Manipülasyonu “ başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 27/ 05/ 2013

Gökhan TATAR

İNTERNET YÖNLENDİRME TEMELLERİ, MPLS VE BGP PROTOKOLÜ İLE ROTA MANİPÜLASYONU

Tezi Hazırlayan: Gökhan TATAR

Özet

İnternet yönlendirme temelleri, MPLS ve BGP protokollerini kullanarak rota manipülasyonu sayesinde, ağ alt yapısındaki iletişimin internet üzerinde istenilen veya çizilen rotalar üzerinde değişiklik yapılarak, yapılan bu değişikliklerin ardından etkisinin gösterilmesi amaçlanmıştır.

Anahtar Kelimeler: MPLS, MPLS protokolü, BGP, BGP Protokolü, Internet Yönlendirme, Internet, Rota Manipülasyonu, Yönlendirme Protokolleri

INTERNET ROUTING FUNDAMENTALS, ROUTE MANIPULATION WITH MPLS AND BGP PROTOCOLS

Presented by: Gokhan TATAR

Abstract

Internet routing fundamentals, through the route manipulation using the MPLS and BGP protocols, provides them with a precise guide for evaluating the benefits of MPLS-based applications and solutions. This document through the business case for MPLS and BGP by exploring other technology alternatives, including applications, benefits, and deficiencies.

Key Words: MPLS, MPLS protocol, BGP, BGP Protocol, Internet Routing, Internet, Route Manipulation, Routing Protocols

İÇİNDEKİLER

Sayfa No.

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

Acknowledgement :(Anlaşma), Yönlendirme protokollerinin güncelleme gibi temel iletişimlerinin olumlu gerçekleştirdikten sonra ağ trafiğinin tamamlanmasına verilen paket isimdir.

Administrative Distance:(Yönetimsel Değer), Yönlendirici cihazlar üzerindeki, yönlendirme protokollerinin cihaz üzerindeki önceliklendirilmesini sağlayan değerdir.

ADSL :(Asymetric Digital Subcriber Line), Asimetrik sayısal abone hattı, hizmet hızı 32 Mbit seviyesine kadar çıkabilen internet bağlantı hizmetlerinden biridir.

Area :(Alan), Yönlendirme protokollerinin kapsamını rakamsal olarak ifade eden değerdir.

ARPA :(Address and Routing Parameter Area), Alan adı dizaynı ve yönlendirmelerini yapan kuruluş.

ATM :(Asynchron Transfer Mode) , Asenkron çalışan ve diğer veri iletişim teknolojilerine göre daha yavaş olan iletim teknolojisidir.

Autonomous System:(Otonom Sistem) Ağ Yönlendirici cihazlarının kullandığı yönlendirme protokollerinin rakamlarla ifade edilmesidir.

Backbone :(Omurga) Ağ yapılandırması üzerinde, merkezi olarak çalıştırılan anahtarlama cihazlarına verilen isimdir.

Bandwith :(Bant Genişliği), Yönlendirici veya Anahtarlama cihazlarının ağ üzerindeki bağlantı hızını ifade eder.

BGP :(Border Gateway Protokol), Ağ sınır geçidi dinamik yönlendirme protokolüdür. İnternet tasarımında ve dizaynında kullanılan gelişmiş yönlendirme protokolüdür.

BIT : İletişim dünyasındaki en küçük bilgi parçaçığıdır. En ufak karaktere verilen veya "0" veya "1" ile ifade edilen bilgilerdir.

BYTE :8 bit'lik topluluklar halinde ifade edilen bilgi parçacıklarına verilen isimdir.

Checksum :Veri paketleri içerisindeki paketlerin yapısında bozulma olup olmadığını doğrulamak için kullanılır. Detaylarının paylaşıldığı ve rakamlarla anlamlı kılınan protokllerin genel adıdır.

CIDR :(Classless Inter Domain Routing), Sınıfsız olarak ifade edilen ip adreslerinin alt ağ maskelerine verilen ve kısaltma ile gösterilmiştir halidir.

DARPA :(Defense Advanced Research Projects Agency), ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı ordu tarafından kullanılmak üzere, yeni teknolojiler üretmekle sorumlu ABD Savunma Bakanlığı Ajansıdır.

Delay :(Gecikme), Ağ üzerindeki aktif cihazların, veri iletim hızının iki cihaz arasındaki mesafeye bağlı olarak gecikmesini ifade eder.

Dencapsulation :Tek parça haline getirilmiş veri'nin tek tek ayrılması ve ilgili cihazlara ve protokollere iletilmesini sağlayan standartdır.

DHCP :(Dynamic Host Configuration Protocol), Dinamik olarak cihazlara ip adresi dağıtmak için kullanılan servistir.

Distance Vector :(Uzaklık Bağımlı), Yönlendirme protokollerinin uzaklığa bağlı olarak sınıflandırılmasına verilen tanımdır.

DNS :(Domain Name System), Alan adı sistemi, internet ortamındaki isimlerin, ip adreslerine, ip'lerin isme çevrilmesini sağlayan servistir.

EIGRP :(Enhanced Interior Gateway Routing Protokol), Genişletilmiş iç network'de kullanılan yönlendirme protokolü olarak

kullanılan cisco üreticisinin geliştirmiş olduğu yönlendirme protokolüdür.

Encapsulation :Veri paketlerinin bir araya getirilip, iletim yapılacak olan cihaza tek başlık içerisinde iletilmesini sağlayan iletişim standartıdır.

Fiber Optik :Kızıl ötesi ışınlar ile veri taşıma teknolojisidir.

Firewall :(Güvenlik Duvarı), Ağ içerisindeki güvenliği sağlamak için kullanılan kullanılan yazılım veya donanımlara verilen genel tanımlamadır.

Frame Relay :Ağ üzerindeki, internet ortamında kullanılan bir protokoldür.

FTP :(File Transfer Protocol), Dosya aktarım protokolü, cihazlar arası dosya aktarımı için kullanılan protokoldür.

Gateway :Kaynak ağ bağlantısından, hedef ağ bağlantısına iletişimin gerçekleştirilebilmesi için kullanılan cihazlara verilen ip adresidir.

GHDSL :(Symetric High bit-rate Digital Subscriber Line), Dosya indirme ve karşı tarafa yükleme hızı eşit olan sayısal abone hattıdır.

Hello :(Merhaba), Yönlendirme protokollerinin bilgiyi paylaşabilmesi için, iletişimin başlatıldığı paketdir.

Hertz :1 sn'ye içerisindeki sinüsoidal dalganın tanımlanmasına verilen isimdir.

HTTP :(Hyper Text Transfer Protocol), Dinamik yaz transfer aktarım protokolü, internet sitelerini görüntülemek için kullanılan protokoldür.

HTTPS :(Hyper Text Transfer Protocol Secure), Internet sitelerini görüntülemek için kullanılan protokolün güvenli halidir.

ICMP :(Internet Control Messaging Protocol), Ağ üzerindeki cihazların, olumlu- olumsuz durumlarını mesaj olarak öğrenebilmek ve bilgi almak amaçlı kullanılan protokoldür.

IETF :(Internet Engineering Task Force), Internet üzerindeki birçok iletişim ve elektronik standartlarını açıklayan kuruluştur.

IP :(Internet Protocol), Cihazlara 32 bit olarak verilen ve onlu sayı sistemi ile ifade edilen protokol bilgisidir.

IPV4 :32 bit'den oluşan, Onlu sayı düzeni ile ifade edilen ip protokolüdür.

IPV6 :128 bit'den oluşan, On Altılı sayı düzeni ile ifade edilen ip protokolüdür.

IP TABLE :(IP Tablosu), Yönlendirme cihazı üzerindeki tutulan ip adreslerinin tablosudur.

ISDN :(Integrated Service Digital Network), Entegre hizmet sağlayan dijital network alt yapısı, hem ses, hem veri aktarımı için kullanılır.

ISP :(Internet Service Provider), Internet servis sağlayıcıları.

LAN :(Local Area Network), Yerel alan ağ anlamına gelen kavram, aynı fiziksel yapı içerisinde kurulan ağ bağlantılarını ifade eder.

Loading :(Yükleme), Ağ cihazlarının, ağ üzerindeki iletişimin karşılıklı olarak veri iletişiminin başladığı anlamına gelir.

Load Balance :(Yük Dengeleme), Yönlendirme protokollerinin ağ üzerindeki hattın durumuna göre, ağ trafiğini dengelenmesine verilen isimdir.

MAC TABLE :(Media Access Control), Anahtarlama cihazı üzerine bağlı olan cihazların fiziksel adaptörlerinin adreslerinin tutulduğu tablodur.

Metric :Yönlendirme protokollerinin gideceği ağ üzerindeki değerlerin hesaplanmış halidir.

MPLS :(Multi Protocol Label Swithching), Çoklu protokol etiketleme ve anahtarlama protokolü, geniş alan ağları içerisinde firmaların kendi özel ağlarını internet üzerinden oluşturulmasını sağlayan protokoldür.

MTU :(Maximum Transmit Unit), Ağ üzerindeki verilerin, ağ üzerinde aktarılabileceği maksimum tek parça veri paketi boyutunu belirler.

Multicast :Ağ üzerinden çoklu yayın yapmak anlamına gelir.

Multipoint :(Çoklu İletişim) Aynı anda tek bir cihazın birden fazla cihaz ile iletişimde olmasına verilen isimdir.

NBMA :(Non Broadcast Multi Access), Yönlendirme protokollerinin çalışmasını bağırma (broadcast) yapılmadan gerçekleştirilmesidir.

NIC :(Network Interface Card), Elektronik bir çok cihazın, ağ bağlantısını sağlamak için kullandığı adaptör

Oktet : Internet Protokol (IP), ifadesini 8 parçalık bölümler halinde açıklar.

OSI :(Open System Interconnection), Ağ üzerindeki standart iletişim tiplerinin tamamının anlamlı bir şekilde açıklanması ve incelenmesini ele alan referans 7 katmanlı referans modeline verilen isimdir.

OSPF :(Open Shortest Path First), En kısa yolu seçen protokol ve en yetenekli dinamik yönlendirme protokollerinden biridir.

Ping :Ağ üzerindeki cihazların çift yönlü olarak iletişim durumlarını denetlemek için kullanılan protokoldür.

Point to Point :(Noktadan Noktaya), İki cihaz arasındaki iletişimin birebir olarak gerçekleştirilmesini açıklar.

Proxy :(Vekil), Ağ üzerindeki veri trafiğinin, başka ağ trafikleri üzerine geçişlerine eşlik eden ve yönlendirme yapabilen, cihaz veya donanımlardır.

Query :(Sorgu), Yönlendirme cihazının karşı taraftaki cihaza ulaşıp ulaşmadığını sorgulamak için kullanılan paketin adıdır.

Reliability :(Kararlılık), Ağ üzerindeki aktif cihazların ağ üzerindeki veri paketlerinin yoğunluğunu ifade etmek için kullanılır.

Reply :(Cevap), Yönlendirici cihazın karşı cihazdan olumlu-olumsuz aldığı cevap paketinin adıdır.

RIP :(Routing Information Protocol), Veri yönlendirme protokolüdür, yönlendirici cihazlar üzerinde aktif edilebilirler. Sınırlı yeteneklere sahiptirler.

Router :(Yönlendirici), Farklı İnternet Protokol adreslerine sahip olan ağ'ların yönlendirilmesi ve iletişim kurması için kullanılan fiziksel cihaz.

RFC :(Request for Comment), Ağ üzerindeki tüm standartların detaylarının paylaşıldığı ve rakamlarla anlamlı kılınan protokollerin genel adıdır.

Segment :Veri paketlerinin iki cihaz arasında çift yönlü iletim esnasında, veri işlevselliği bakımından parçalara ayrılması demektir.

SMTP :(Simple Mail Transfer Protocol), Elektronik mail alış verişinde kullanılan protokoldür.

Switch :(Anahtarlayıcı), Yerel Ağ'lar üzerindeki, bilgisayar ve tablet bilgisayar gibi cihazları kablolu ya da kablosuz olarak iletişim kurmalarını sağlar.

Summarization :(Özetleme), Ip adreslerinin varsayılan olarak gelen sınıflarına otomatik olarak dönüştürülmesi demektir.

TCP :(Transmit Control Protocol), İletim Kontrol Protokolü.

Telnet :Uzak cihazlara komut satırı yardımı ile bağlantı kurmayı gerçekleştiren protokoldür.

TFTP :(Text File Transfer Protocol), Fiziksel cihazların üzerindeki küçük boyutlu dosyalar ve işletim sistemlerini uzaktan yüklemek için kullanılan protokoldür.

TTNET :(Türk Telekom Network), Türk Telekom firmasının internet servis sağlayıcı firmasıdır.

TURNET :Türkiye'de ki en eski internet servis sağlayıcıdır.

UDP :(User Datagram Protocol), Kullanıcı veri iletim protokolü.

Update :(Güncelleme), Yönlendirme cihazlarının ağ üzerindeki güncellemeleri paylaştığı paketin ismidir.

VDSL :(Very High Bit Digital Subcriber Line), Yüksek hızlı sayısal abone hattı, 55. 2 Mbit seviyesine kadar çıkabilen internet bağlantı hızıdır.

Vlan :(Sanal Özel Yerel Ağ), Anahtarlama cihazları üzerinde oluşturulan, güvenlik ve performans amaçlı kullanılan anahtarlama protokolüdür.

VLSM :(Variable Lenght Subneting Mask), Alt ağ maskesinin 32 bit kapsamında standart subnet mask ayarlarının dışında kullanılmasını açıklayan kavramdır.

WAN :(Wide Area Network), Geniş alan ağ bağlantısı anlamına gelen kavram, farklı fiziksel lokasyonlarda bulunan internet kullanıcılarını ortak bir payda da iletişim kurmasını açıklamaktadır.

1. GİRİŞ

Bu tez dökümanın amacı, Internet hakkında bilinmeyen pek çok temel bilgileri ve son kullanıcıların her gün internet erişiminde farkında olmadan kullandığı protokollerin ve teknik terimlerin neler olduğunu açıklamak, ardından internet trafiğinin yönünü değiştiren bu kavramları ve protokolleri detaylıca öğrenip, uygulamaktır.

Tez dökümanı kapsamında, İnternet nedir? İnternetin gelişimi ve kullanımı hakkında genel bilgilerin aktarılması, Dinamik ve Statik yönlendirme protokollerinin çalışmasına dair genel algoritmalar ve örnekler verilmektedir.

Ayrıca Dinamik yönlendirme protokolleri kapsamında, RIP, OSPF, EIGRP, BGP ve MPLS protokolleri temelleri, çalışması ve özellikleri ile birlikte uygulamalı olarak paylaşılmaktadır.

Bu bilgiler vasıtası ile Internet yönlendirme temellerinin, dinamik yönlendirme protokollerinin detayları, internetin dünü ve bugünü hakkında bilgilerin aktarılmasının ardından, MPLS ve BGP protokolü kullanılarak, Internet üzerindeki çizilen rotalar üzerinde değişiklikler yapılarak, internet üzerindeki iletişimin yönünü isteğe veya ihtiyaca göre değiştirilip, iletişim performansının artırılması amaçlanmıştır.

Ortaya atılan Tez iddası, temelinde dinamik yönlendirme protokollerini kullanarak rota manipülasyonu yapmaktır.

Kaynak ağ'dan hedef ağ'a gidişte birçok alternatif rota hesaplamak ve bu rotaların elle veya dinamik olarak kullanımı amaçlanmıştır.

İhtiyaç halinde hattın ve protokolün durumuna göre gidilecek yolun değiştirilmesi ve en optimum metod ile yönlendirmenin yapılması amaçlanmaktadır.

Bu işlem adımlarını inceledikten sonra BGP protokolü detaylarından faydalanılarak rota manipülasyon işlemi uygulamalı olarak sunulmaktadır.

2.İNTERNET

2.1. İnternet Nedir?

İnternet, birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygın olan ve sürekli büyüyen bir iletişim ağıdır.

Bu iletişim ağında bilgisayarlar birbirlerine fiziksel olarak (kablolar, uydu bağlantıları, telsiz bağlantı vb) bağlıdır ve geliştirilen bazı özel protokollerle (TCP/IP) birbirine bağlı bilgisayarlar arasında bilgi paylaşımına dayalı birçok işler yapılabilir (dosya alma/gönderme, sohbet vb gibi).

Bilgisayarların bilgiyi saklama (harddisk, fiberoptik ortam vb), bilgiyi çok hızlı işleme (veri tabanı programları, bazı analiz programları vb) özellikleriyle bilgisayar ağlarının herhangi iki bilgisayar arasında veri iletişimini olanaklı kılma özellikleri birleştiğinde ortaya muazzam bir bilgi paylaşım ortamı çıkar. İşte, internetin felsefesini oluşturan temel altyapı ana hatlarıyla böyledir.

Şekil.1. İnternet Topolojisi

İnternet, insanların her geçen gün gittikçe artan "üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma" istekleri sonrasında ortaya çıkmış bir teknolojidir.

Bu teknoloji yardımıyla pek çok alandaki bilgilere insanlar kolay, ucuz, hızlı ve güvenli bir şekilde erişebilmektedir. İnternet'i bu haliyle bir bilgi denizine, ya da büyükçe bir kütüphaneye benzetebiliriz. Internet'e, bakış açımıza bağlı olarak farklı tanımlamalar da getirebiliriz:

İnternet, 2000 yılı sonu itibariyle 150,000,000'u aşkın insanın kendi arasında etkileştiği, bilgi değiş-tokuşu yapabildiği ve kendi yazısız kuralları olan büyük bir topluluktur.

Bu, internetin sosyal yönüdür. Pek çok yararlı bilginin bir tuşa basmak kadar yakın olduğu dev bir kütüphanedir.

2000 yılı sonu itibariyle, 30,000,000'u aşkın bilgisayarın bağlı olduğu çok büyük bir bilgisayar ve iletişim ağıdır.

Kişilerin değişik konularda fikirlerini serbestçe söyleyebilecekleri ortamlar barındıran bir demokrasi platformudur.

Evden alış-veriş, bankacılık hizmetleri, radyo-televizyon yayınları, günlük gazete servisleri vb gibi uygulamaları ile aslında internet aynı zamanda bir hayat kolaylaştırıcıdır.

Sonuç olarak, Internet, önümüzdeki yıllarda üretilecek bilgilerin dolaşım sistemidir. Ticari boyutunun da ortaya çıkmasıyla yaşamla daha çok iç içe geçmeye başlamıştır.

2000'li yıllarda hayatın iyice içine giren internet ile, banka hesaplarımıza, borsaya internet üzerinden erişebiliyor ve işlem yapabiliyoruz.

Günlük gazetelere yarım saat içinde ücretsiz göz atıp, elektronik postalarımızı okuyabiliyoruz. Eskiden sadece haberleşme özellikleri ön plana çıkan internet teknolojileri, artık yaşamın içine iyice girmiş durumda. İnternet ve onun geniş kitlelere ulaşımını sağlayan WEB teknolojileri bir insanın yaşamını sürdürmesini sağlayan tüm aşamalarda kullanılıyor.

İnternet, tüm dünyayı kapsayan, 110 Ülkeye dağılmış ve 2.000.000'dan fazla bilgisayarı (host) birbirine bağlayan yaklaşık 5000 bilgisayar ağının toplamıdır.

1994 yılı başında yaklaşık 12 milyon Internet kullancısı bulunmaktadır. Internet genel bilgiye erişimi destekler ve elektronik posta (elektronik mail), konferans, bildiriler gibi konularda iletişim hizmetleri sağlar. Bütün bilgi ve servisler, Internet'i oluşturan çeşitli ağlara dağıtılmıştır ve geçerli bir Internet adresi ve fiziksel baglantısı olan herhangi bir yerden ulaşılabilir durumdadırlar. Kuruluşlar Internet'e iki ana nedenden dolayı bağlanmaktadırlar.

Birincisi, Internet de ki yararlı bilgilere dünya çapında bir bağlanabilirlik ve erişim sağlar.

İkincisi, Internet'e bağlanmak, kuruluşlara özel bir geniş bölge ağı kurmaktan daha ucuza mal olmaktadir.

Internet'in kullanımı bir zamanlar araştırma, eğitim ve devlet kuruluşlarının etkinlikleriyle sınırlandırıldıysa da, son zamanlarda ticari kullanimi buyuk oranda artmistir. Bu gelişmeler, bazi gözlemcileri Internet'in yakin gelecekte tamamıyla özellestirileceği yolunda spekulasyonlara itmektedir. Boyle bir durumda Internet kaynaklarına ulaşım kullanım fiyatlarına göre belirlenebilecektir.

Internet Society, Brief History of the Internet (b.t.) kaynağından alıntıdır.

2.2. İnternetin Tarihçesi

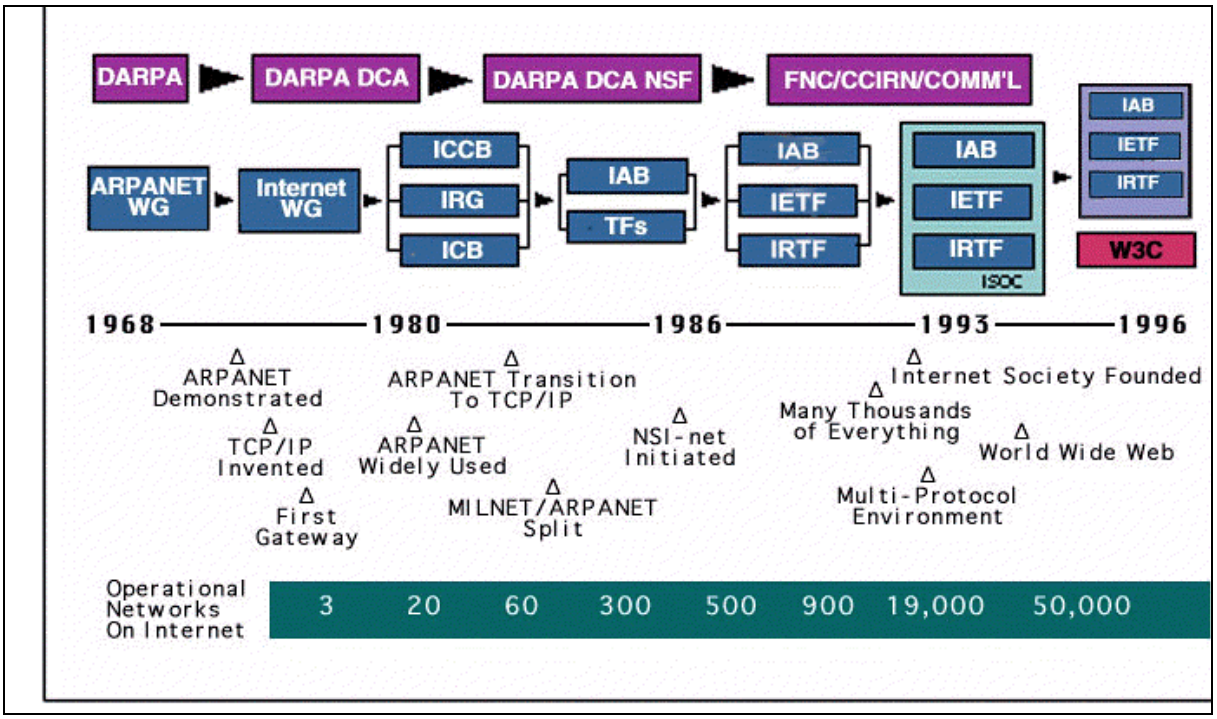
İnternet'in ortaya cıkışı Amerikan Federal Hukumeti Savunma Bakanligi'nin araştırma ve geliştirme kolu olan 'Savunma Ileri Duzey Arastirma Projeleri Kurumu'na (DARPA- Defence Advanced Research Project Agency) dayanir.1969'da cesitli bilgisayar bilimleri ve askeri araştırma projelerini desteklemek icin Savunma Bakanligi ARPANET adında Paket Anahtarlamali Ag'i oluşturmaya basladı.

Bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarları da içererek büyüdü. 1973 yılında, ağ için bir protokol seti geliştirmek

amacıyla Stanford Universitesi'nde - daha sonra BBN'in ve University College, London'in da dahil olduğu bir internetworking projesi başlatıldı.

1978'e kadar 'Iletim Kontrol Protokolu'nun (TCP - Transmission Control Protocol) dört uyarlaması geliştirildi ve denendi.

1980'de bu küme sabitlesti ve ARPANET'e bağlı bilgisayarlar arasındaki iletişimi kolaylaştırdı. 1983'te tum ARPANET kullanıcıları Iletim Kontrol Protokolu/Internet Protokolu (TCP/IP Transmission Control Protocol/Internet Protocol) olarak bilinen yeni protokole geçiş yaptılar. O yil TCP/IP, ARPANET'i de içeren Savunma Bakanlığı Internet'inde kullanılmak üzere standartlaştırıldı. ARPANET 1990 Haziranın'da kullanımdan kaldırıldı. Yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalar (backbone) aldı. ARPANET'in kaldırılmasına rağmen, TCP/IP protokolu kulanılmaya devam etti ve gelişti. Internet Society, History of the Internet (b.t.) kaynağından alıntıdır.



Şekil.2. İnternetin Tarihsel Gelişimi

2.3. Türkiye’de İnternet

Türkiye Internet'e Nisan 1993'ten beri bağlıdır. İlk bağlantı ODTÜ’den gerçekleştirilmiştir. 64kbit/sn hızında olan bu hat, çok uzun bir süre, tüm ülkenin tek çıkışı olmuştur.

Ege Üniversitesi’nden olan bağlantı ise, 1994 başlarında, 64kbit/san. hızı ile gerçekleştirilmiştir. Ardından sırayla, Bilkent Ün. (1995 Eylül), Boğaziçi Üniv. (1995 Kasım) ve İTÜ (1996 Şubat) bağlantıları gerçekleşmiştir. 1996 yılı Ağustos ayında da Turnet çalışmaya başlamıştır. 1997 yılına gelindiğinde, akademik kuruluşların internet bağlantısını sağlayan ULAKNET çalışmaya başlamış ve üniversiteler nispeten hızlı bir omurga yapısıyla birbirlerine bağlanmış ve internet kullanır hale gelmişlerdir. 1999 yılı içerisinde, ticari ağ altyapısında büyük değişiklikler olmuş ve TURNET'in yerini TTNet adında yeni bir oluşum almıştır. 2000'lerin başında; ticari kullanıcılar TTNet omurgası üzerinden; akademik kuruluşlar ve ilgili birimler de Ulaknet omurgası üzerinden internet erişimine sahiptir. Ayrıca bu iki omurga arasında yüksek hızlı bağlantı mevcuttur.

Şu anda Türkiye'nin Internet çıkışını sağlayan merkezler üç ana grupta toplanabilir;

Üniversiteler ve Akademik kuruluşların internet bağlantı çıkışları;

Genellikle ticari kuruluşların ve Internet Servis Sağlayıcılarının (İSS) yararlandığı TTNET çıkışları.

Diğer bazı özel şirketlerin ve servis sağlayıcıların, TTNET ile yaptıkları İnternet Erişim Noktasi (İEN) anlaşması sonrasında kullandıkları firma bazlı doğrudan yurtdışı internet çıkışları.

ALTUN, A. (29.04.2003) ‘dan alıntıdır.

2.4. TCP/IP Nedir?

"Bilgi Ağı" üzerindeki bilgi iletimi ve paylaşımı bazı kurallar dahilinde yapılmaktadır. Bu kurallara kısaca "internet protokolleri", ya da TCP/IP protokoller ailesi denir.

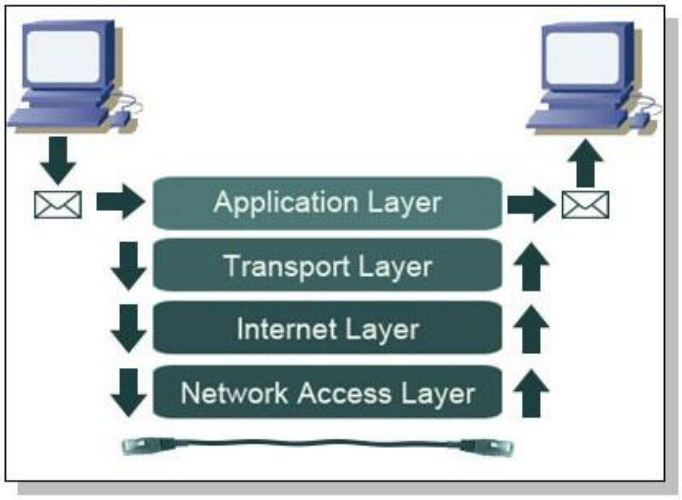
TCP/IP (Transmission Control Protocol/Internet Protocol), bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel ismidir. Bir başka değişle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar.

Bu protokollere örnek olarak, dosya alma/gönderme protokolü (FTP, File Transfer Protocol), Elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol), TELNET protokolü (Internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen *login* protokolü) verilebilir.

Adını sıkça duyduğumuz WWW ortamında birbirine link objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır. TCP/IP protokolü aynı zamanda, diğer iletişim ağlarında da kullanilabilir. Özellikle pek çok farklı tipte bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır.

TCP/IP katmanlardan oluşan bir protokoller kümesidir. Her katman değişik görevlere sahip olup altındaki ve üstündeki katmanlar ile gerekli bilgi alışverişini sağlamakla yükümlüdür.

Aşağıdakı şekilde bu katmanlar bir blok şema halinde gösterilmektedir.



Şekil.3. TCP/IP Katmanları

TCP/IP katmanlarının tam olarak ne olduğu, nasıl çalıştığı konusunda bir fikir sahibi olabilmek için bir örnek üzerinde inceleyelim;

TCP/IP nin kullanıldığı en önemli servislerden birisi elektronik postadır (e-posta). E- posta servisi için bir uygulama protokolü belirlenmiştir (SMTP).

Bu protokol e- posta'nın bir bilgisayardan bir başka bilgisayara nasıl iletileceğini belirler. Yani e- postayı gönderen ve alan kişinin adreslerinin belirlenmesi, mektup içeriğinin hazırlanması vs. gibi.

Ancak e-posta servisi bu mektubun bilgisayarlar arasında nasıl iletileceği ile ilgilenmez, iki bilgisayar arasında bir iletişimin olduğunu varsayarak mektubun yollanması görevini TCP ve IP katmanlarına bırakır. TCP katmanı komutların karşı tarafa ulaştırılmasından sorumludur. Karşı tarafa ne yollandığı ve hatalı yollanan mesajların tekrar yollanmasının kayıtlarını tutarak gerekli kontrolleri yapar.

Eğer gönderilecek mesaj bir kerede gönderilemeyecek kadar büyük ise (Örnegin uzunca bir e-posta gönderiliyorsa) TCP onu uygun boydaki segment'lere (TCP katmanlarının iletişim için kullandıkları birim bilgi miktari) böler ve bu segment'lerin karşı tarafa doğru sırada, hatasız olarak ulaşmalarını sağlar. İnternet üzerindeki tek servis e-posta olmadığı için ve segment'lerin karşı tarafa hatasız ulaştırılmasını sağlayan iletişim yöntemine tüm diğer servisler de ihtiyaç duyduğu için

TCP ayrı bir katman olarak çalışmakta ve tüm diğer servisler onun üzerinde yer almaktadır. Böylece yeni bir takım uygulamalar da daha kolay geliştirilebilmektedir. Üst seviye uygulama protokollerinin TCP katmanını çağırmaları gibi benzer şekilde TCP de IP katmanını çağırmaktadır.

Ayrıca bazı servisler TCP katmanına ihtiyaç duymamakta ve bunlar direk olarak IP katmanı ile görüşmektedirler. Böyle belirli görevler için belirli hazır yordamlar oluşturulması ve protokol seviyeleri inşa edilmesi stratejisine 'katmanlaşma' adı verilir. Yukarıda verilen örnekteki e- posta servisi (SMTP), TCP ve IP ayrı katmanlardır ve her katman altındaki diğer katman ile konuşmakta diğer bir deyişle onu çağırmakta ya da onun sunduğu sevisleri kullanmaktadır. En genel haliyle TCP/IP uygulamaları 4 ayrı katman kullanır.

Bunlar; Bir uygulama protokolü, mesela e-posta, Üst seviye uygulama protokollerinin gereksinim duyduğu TCP gibi bir protokol katmanı IP katmanıdır. Gönderilen bilginin istenilen adrese yollanmasını sağlar. Belirli bir fiziksel ortamı sağlayan protokol katmanı; Örneğin Ethernet, seri hat, X.25 vs.

İnternet birbirine geçis yolları (gateway) ile bağlanmış cok sayıdaki bağımsız bilgisayar ağlarından oluşur ve buna 'catenet model' adı verilir. Kullanıcı bu ağlar üzerinde yer alan herhangi bir bilgisayara ulaşmak isteyebilir.

Bu işlem esnasında kullanıcı farkına varmadan bilgiler, düzinelerce ağ üzerinden geçis yapıp varış yerine ulaşırlar. Bu kadar işlem esnasında kullanıcının bilmesi gereken tek şey ulaşmak istediği noktadaki bilgisayarın 'İnternet Adresi'dir.

Bu adres toplam 32 bit uzunluğunda bir sayıdır. Fakat bu sayı 8 bitlik 4 ayrı ondalık sayı şeklinde kullanılır (144.122.199.20 gibi). Bu 8 bitlik gruplara 'octet' ismi de verilir.

Bu adres yapısı genelde karşıdaki sistem hakkında bilgi de verir. Mesela 144.122 ODTÜ için verilmiş bir numaradır. ODTÜ üçüncü octet'i kampüs içindeki birimlere dağıtmıştır. Örneğin, 144.122.199 bilgisayar merkezinde bulunan bir Ethernet ağda kullanılan bir adrestir. Son oktet ise bu Ethernete 254 tane bilgisayar

bağlanmasına izin verir (0 ve 255 bilgisayar adreslemesinde kullanılmayan özel amaçlı adresler olduğu için 254 bilgisayar adreslenebilir).

IP bağlantısız "connectionless" ağ teknolojisini kullanmaktadır ve bilgi "datagramlar" (TCP/IP temel bilgi birim miktari) dizisi halinde bir noktadan diğerine iletilir.

Büyük bir bilgi grubunun (büyük bir dosya veya e-posta gibi) parçaları olan "datagram" ağ üzerinde tek başına yol alır. Mesela 15000 oktet'lik bir kütük pek çok ağ tarafından bir kere de iletilemeyecek kadar büyük olduğu için protokoller bunu 30 adet 500 oktet'lik datagramlara böler.

Her datagram ağ üzerinden tek tek yollanır ve bunlar karşı tarafta yine 15000 oktet lik bir kütük olarak birleştirilir. Doğal olarak önce yola çıkan bir datagram kendisinden sonra yola çıkan bir datagram'dan sonra karşıya varabilir veya ağ üzerinde oluşan bir hatadan dolayı bazı datagramlar yolda kaybolabilir.

Kaybolan veya yanlış sırada ulaşan datagramların sıralanması veya hatalı gelenlerin yeniden alınması hep üst seviye protokollerce yapılır. Bu arada "paket" ve "datagram" kavramlarına bir açıklama getirmek yararlı olabilir. TCP/IP ile ilgili kavramlarda "datagram" daha doğru bir terminolojidir. Zira datagram TCP/IP'de iletişim için kullanılan birim bilgi miktarıdır.

Paket ise fiziksel ortamdan (Ethernet, X.25 vs.) ortama değişen bir büyüklüktür. Mesela X.25 ortamında datagramlar 128 byte lik paketlere dönüştürülüp fiziksel ortamda böyle taşınırlar ve bu işlemle IP seviyesi hiç ilgilenmez. Dolayısıyla bir IP datagramı X.25 ortamında birden çok paketler halinde taşınmış olur.

2.5. TCP Katmanı

TCP'nin ("Transmission Control Protocol - İletişim Kontrol Protokolü") temel işlevi, üst katmandan (uygulama katmanı) gelen bilginin segment'ler haline donüştürülmesi, iletişim ortamında kaybolan bilginin tekrar yollanması ve ayrı sıralar halinde gelebilen bilginin doğru sırada sıralanmasıdır. IP ("internet protocol") ise tek tek datagramların yönlendirilmesinden sorumludur.

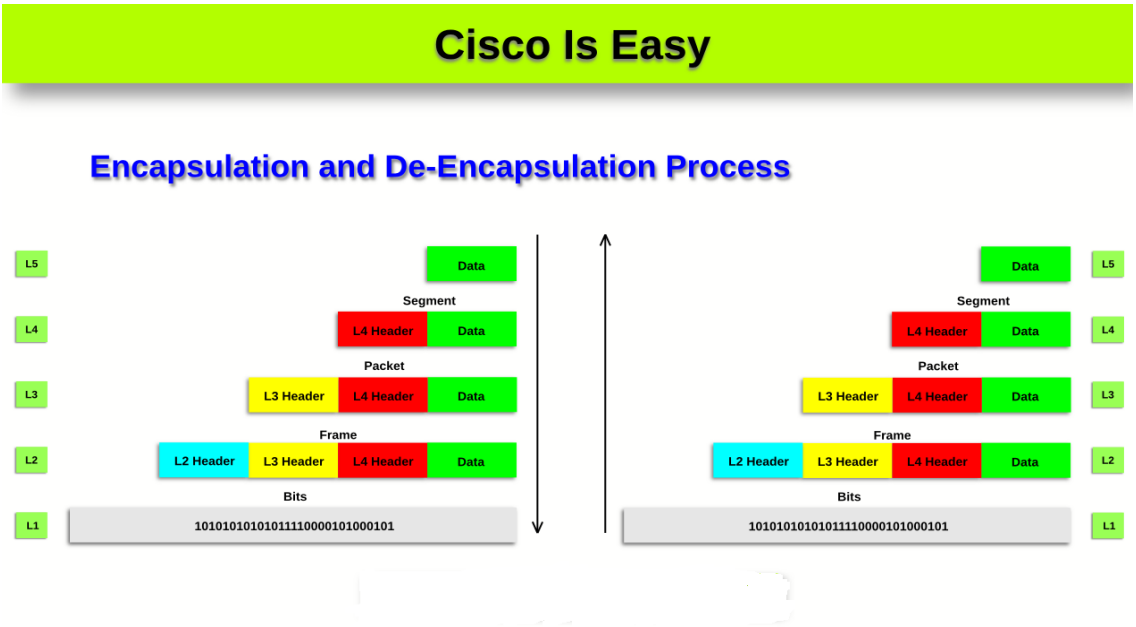
Bu açıdan bakıldığında TCP katmanının hemen hemen tüm işi üstlendiği görülmekle beraber (küçük ağlar için bu doğrudur) büyük ve karmaşık ağlarda IP katmanı en önemli görevi üstlenmektedir. Bu gibi durumlarda değişik fiziksel katmanlardan geçmek, doğru yolu bulmak çok karmaşık bir iş halini almaktadır.

Doğal olarak bir segment'i doğru varış noktasına ulaştırmak tek başına yeterli değildir. TCP bu segment'in kime ait olduğunu da bilmek zorundadır. "Demultiplexing" bu soruna çare bulan yöntemdir. TCP/IP 'de değişik seviyelerde "demultiplexing" yapılır.

Bu işlem için gerekli bilgi bir seri "başlık" (header) içinde bulunmaktadır. Başlık, datagram'a eklenen basit bir kaç octet'den oluşan bir bilgiden ibarettir. Yollanmak istenen mesaji bir mektuba benzetecek olursak başlık o mektubun zarfı ve zarf üzerindeki adres bilgisidir.

Her katman kendi zarfını ve adres bilgisini yazıp bir alt katmana iletmekte ve o alt katmanda onu daha büyük bir zarfın içine koyup üzerine adres yazıp diğer katmana iletmektedir.

Benzer işlem varış noktasında bu sefer ters sırada takip edilmektedir.



Şekil.4. Enkapsulasyon ve Dekapsulasyon işlemi

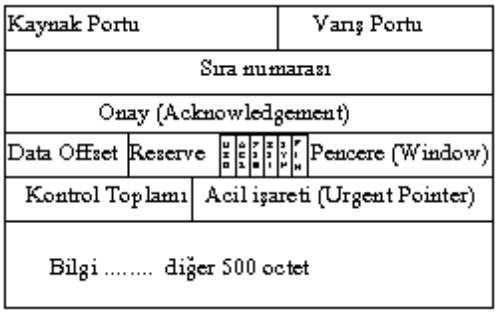
Her segment'in başına TCP bir başlık koyar. Bu başlık bilgisinin en önemlileri 'port numarası' ve 'sıra numarası' dır. Port numarası, örneğin birden fazla kişinin aynı anda dosya yollaması veya karşıdaki bilgisayara bağlanması durumunda TCP'nin herkese verdiği farklı bir numaradır.

Üç kişi aynı anda dosya transferine başlamıssa TCP, 1000, 1001 ve 1002 "kaynak" port numaralarını bu üç kişiye verir böylece herkesin paketi birbirinden ayrılmış olur. Aynı zamanda varış noktasındaki TCP de ayrıca bir "varış" port numarası verir. Kaynak noktasındaki TCP nin varış port numarasını bilmesi gereklidir ve bunu iletişim kurulduğu anda TCP karşı taraftan öğrenir. Bu bilgiler başlıktaki "kaynak" ve "varış" port numaraları olarak belirlenmiş olur.

Ayrıca her segment bir "sıra" numarasına sahiptir. Bu numara ile karşı taraf doğru sayıdaki segmenti eksiksiz alıp almadığını anlayabilir. Aslında TCP segmentleri değil oktet'leri numaralar.

Diyelim ki her datagram içinde 500 octet bilgi varsa ilk datagram numarası 0, ikinci datagram numarası 500, üçüncüsü 1000 şeklinde verilir. Başlık içinde bulunan üçüncü önemli bilgi ise "kontrol toplamı" (Checksum) sayısıdır. Bu sayı segment içindeki tüm octet ler toplanarak hesaplanır ve sonuç başlığın içine konur. Karşı noktadaki TCP kontrol toplamı hesabını tekrar yapar.

Eğer bilgi yolda bozulmamışsa kaynak noktasındaki hesaplanan sayı ile varış noktasındaki hesaplanan sayı aynı çıkar. Aksi takdirde segment yolda bozulmuştur bu durumda bu datagram kaynak noktasından tekrar istenir.

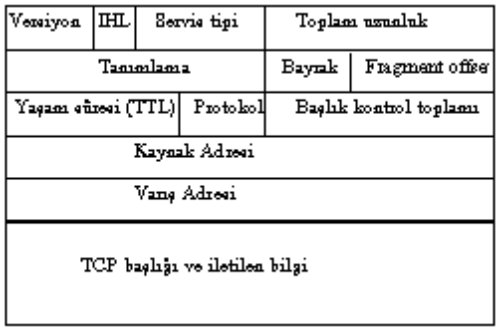


Şekil.5. TCP Segmenti

2.6. IP Katmanı

TCP katmanına gelen bilgi segmentlere ayrıldıktan sonra IP katmanına yollanır. IP katmanı, kendisine gelen TCP segmenti içinde ne olduğu ile ilgilenmez. Sadece kendisine verilen bu bilgiyi ilgili IP adresine yollamak amacındadır.

IP katmanının görevi bu segment için ulaşılmak istenen noktaya gidecek bir "yol" (route) bulmaktır. Arada geçilecek sistemler ve geçiş yollarının bu paketi doğru yere geçirmesi için kendi başlık bilgisini TCP katmanından gelen segment'e ekler. TCP katmanından gelen segmentlere IP başlığının eklenmesi ile oluşturulan IP paket birimlerine datagram adı verilir. IP başlığı eklenmiş bir datagram aşağıdaki çizimde gösterilmektedir;



Şekil.6. IP Datagram

Bu başlıktaki temel bilgi kaynak ve varış İnternet adresi (32-bitlik adres, 144.122.199.20 gibi), protokol numarası ve kontrol toplamıdır. Kaynak İnternet adresi tabiki sizin bilgisayarınızın İnternet adresidir. Bu sayede varış noktasındaki bilgisayar bu paketin nereden geldiğini anlar. Varış İnternet adresi ulaşmak istediğiniz bilgisayarın adresidir.

Bu bilgi sayesinde aradaki yönlendiriciler veya geçiş yolları (gateway) bu datagram'i nereye yollayabileceklerini bilirler. Protokol numarası IP'ye karşı tarafta bu datagram'i TCP'ye vermesi gerektiğini söyler. Her ne kadar IP trafiğinin çoğunu TCP kullansa da TCP dışında bazı protokollerde kullanılmaktadır dolayısıyla protokoller arası bu ayrım protokol numarası ile belirlenir. Son olarak kontrol toplamı IP başlığının yolda bozulup bozulmadığını kontrol etmek için kullanılır. Dikkat edilirse TCP ve IP ayrı ayrı kontrol toplamları kullanmaktalar.

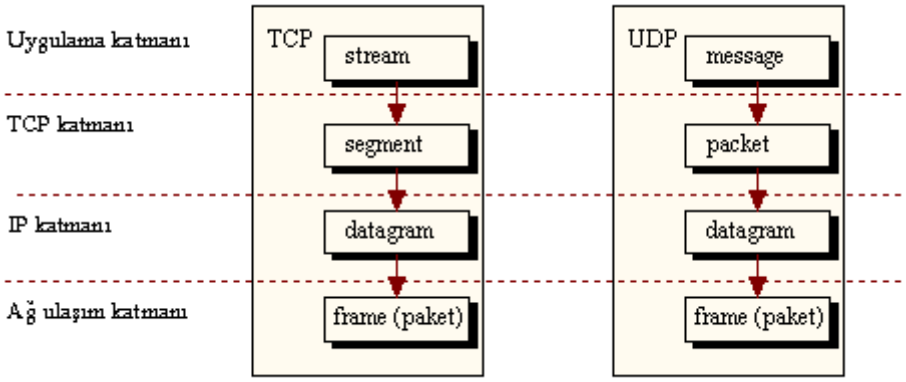
IP kontrol toplamı başlık bilgisinin bozulup bozulmadığı veya mesajın yanlış yere gidip gitmediğinin kontrolü için kullanılır. Bu protokollerin tasarımı sırasında TCP'nin ayrıca bir kontrol toplamı hesaplaması ve kullanmasi daha verimli ve güvenli bulundugu için iki ayrı kontrol toplamı alınması yoluna gidilmiştir.

IP başlığını "I" ile gösterecek olursak IP katmanından çıkan ve TCP verisi taşıyan bir datagram şu hale gelir:

IT...IT...IT...IT...IT...

Başlıktaki "Yaşam süresi" (Time to Live) alanı IP paketinin yolculuğu esnasında geçilen her sistemde bir azaltılır ve sıfır olduğunda bu paket yok edilir. Bu

sayede oluşması muhtemel sonsuz döngüler ortadan kaldırılmış olur. IP katmanında artık başka başlık eklenmez ve iletilecek bilgi fiziksel iletişim ortamı üzerinden yollanmak üzere alt katmana (bu Ethernet, X.25, telefon hattı vs. olabilir) yollanır.



Şekil.7. TCP ve UDP Katmanları

2.7. Internet'e Kimler Dahildir?

2.7.1. Kaç Tane Bilgisayar İnternet'e Bağlıdır Ve Kaç Kişi İnternet Kullanıyor?

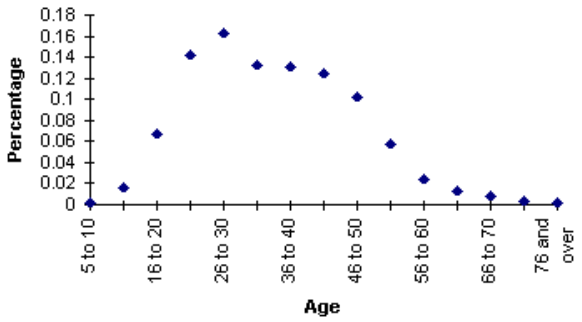
Bütün dünya üzerinde Internet'e; üniversiteler, araştırma enstitüleri, kamu kuruluşları, pek çok ticari kuruluş vb değişik yerler bağlıdır ve İnternet'e bağlı bilgisayar sayısı 25,000,000 civarında tahmin edilmektedir. (1997 sonundaki durum) Bu sayı her gün süratle artmaktadır. Ortalama İnternet kullanıcısı sayısının ise, 100,000,000 'un üzerinde olduğu tahmin edilmektedir (1997 sonlarındaki durum). Internet iletişim ağına bağlı bir bilgisayarın bir tek kullanıcısı olabildiği gibi, birden çok (bazen yüzlerce, binlerce) kullanıcısı da olabilir. Kişisel bilgisayarlar ve evden bağlantılar tek kullanıcılı internet bağlantılarına örnek olarak verilebilirler.

Öte yandan, aynı anda birden çok kullanıcının erişebildiği ve kullandığı daha çok "Unix"işletim sistemi ile çalışan orta ve büyük boy sistemler de çok kullanıcılı internet bağlantı örnekleridir.

Amerikan Uzay ve Havacılık Dairesi NASA, 2008 yılında dünya ile Mars arasında ilk ağ (network) bağlantısının gerçekleştirileceğini öngörmektedir (InterPlaNet!).

Aşağıdaki grafikte, tüm dünyada internete bağlı bilgisayar sayılarının yıllara göre değişimi görülmektedir. Üstel bir şekilde artım hemen göze çarpar.

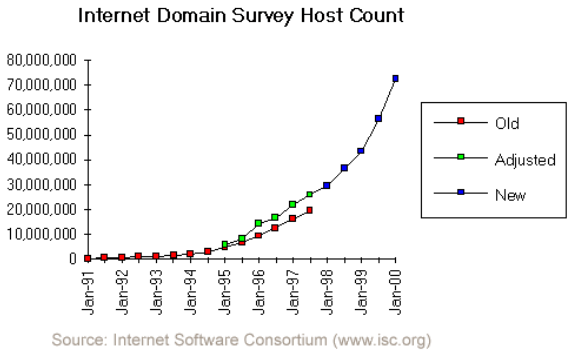
Bir sonraki şekilde ise, internet kullanıcılarının yaşlara göre dağılımı görülmektedir.
Grafikten görüleceği gibi, internet kullanıcılarının büyük bir bölümü 20-35 arası yaşlardadır.



Şekil.8. Dünyadaki İnternet Kullanıcılarının Artış Grafiği

Şekil.8 Internet Systems Consortium,(b.t.) web sitesinden alıntıdır.

İnternet üzerindeki alan adlarının (domain) yıllara göre değişimi de aşağıdaki gibidir. Grafikten görüleceği gibi, 1991'de onbinlerle ölçülen alan adı sayısı, 2000'e gelindiğinde 70 milyona ulaşmıştır.



Şekil.9. İnternet Üzerindeki Domain'lerin Yıllara Göre Değişimi

Şekil.9 Internet Systems Consortium,(b.t.) web sitesinden alıntıdır.

Tablo.1. İnternet Kullanıcılarının Dünya Üzerindeki Bölgelere Göre Dağılımı (Mayıs 1999)

Kanada ve ABD	% 56.6
Asya/Pasifik	% 27
Avrupa	% 23.4
Latin Amerika	% 5.3
Afrika	% 1.1
Orta Doğu	% 0.5

1998 yılı verilerine göre, evden ya da işyerinden internete bağlı insanların toplam nüfusa oranı, ABD, Kanada ve Baltık Ülkelerinde %35 civarındadır. Bu oran,

Almanya için %10, İngiltere için %15, Japonya için %10, Fransa için %8, Türkiye için ise %0.5'ten azdır.

2.8. İnternet Ne Sunar ?

İnternet'i bir "iletişim ağı" olarak tanımladıktan ve bu ağ üzerinde bilgi dolaştığını belirttikten sonra, internet'in bu altyapı üzerinde neler sunduğunu tahmin etmek kolaydır. Bu "iletişim ağı"nın içinde bulunan her hangi iki bilgisayar arasındaki en temel işlem çift yönlü bilgi aktarımıdır. Burada bilgiden kasıt, bilgisayarlardan birinde bulunan bir dosya, bir bilgisayar programı ya da bir mesaj olabilir.

Internet, teknik olarak, TCP/IP protokolü ile desteklenen pek çok servis sunar. Örnek olarak, Internet erişimi olan bir kullanıcı, eğer kendisine yetki verilmişse, Internete bağlı diğer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına alabilir, kendi bilgisayarından da Internet erişimi olan başka bir bilgisayara dosya/bilgi gönderebilir.

Bu özellik, dosya transfer protokolü olarak bilinir. Benzer şekilde, internet üzerindeki kullanıcılar birbirlerine elektronik posta gönderebilirler. Bu da, posta iletim protokolü olarak bilinir.

İnternet, değişik protokoller aracılığı ile, insanlara "bilgiye erişim" olanakları sunar. Yani, internet yardımıyla "her çeşit" bilgiye erişebilirsiniz.

İçerik bakımından, Internetin sundukları bazen insan hayal gücünü zorlayacak boyutlara varmaktadır. Vizyondaki filmlerin kısa tanıtımlarını kolayca evimizdeki ekrana taşıyabilir ya da Amerikan Kongre Kutuphanesi'nde tarama yapabiliriz. Tübitak arşivine bağlanıp Bilim ve Teknik dergilerinin yeni ve eski sayılarını tarayabilir, yazıları okuyabiliriz. Ya da, Hacettepe Üniv.'ne uzanıp o anki Beytepe Kampüsü

sıcaklıklarını grafiksel olarak görebiliriz. Başka bir örnek olarak, katılmak istediğimiz bir bilimsel toplantıya bildirimizi Internet üzerinden gönderebiliriz.

Örnekleri arttırmak mümkün; Nasa servislerine bağlanıp, son uydu fotoğraflarını tarayabiliriz ya da şiir arşivlerine bağlanip şiirler okuyabiliriz. Son yıllarda geliştirilen World Wide Web (WWW, Web) temelli internet araçları ile bilgiye ulaşım daha da kolaylaşmış ve ulaşılabilecek bilgiler ve sunulan servisler miktar ve çeşit olarak artmışlardır. İnternet'in sundukları; onu kullananların istekleri, hayal güçleri ve gelişen İnternet teknolojisi ile hep çoğalmaktadır.

2.9. İnternet Adresi Nedir?

2.9.1. Domain İsmi ve IP numarası ne demektir?

İnternet'e bağlı her bilgisayarın kendine özgü bir adresi vardır. Domain Name System (DNS) olarak adlandırılan hiyerarşik bir isimlendirme sistemi ile (Internet adresi), internete bağlı bilgisayarlara ve bilgisayar sistemlerine isimler verilir. DNS de, bir TCP/IP servis protokoludur. DNS, 'host' olarak adlandırılan internete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırılmasını sağlar. Bu şekilde, bütün adreslerin her yerde tanımlı olmasına gerek kalmaz. Örnek olarak, beykent.edu.tr altında, ehb.beykent.edu.tr, onun altında da, titan.ehb.beykent.edu.tr vb seklinde dallanmış birçok adres olabilir.

Her bir internet adresine 4 haneli bir numara karşılık gelir. a.b.c.d seklindeki bu numaralara IP (Internet Protocol) numaraları denir. Burada, a,b,c ve d 0-255 arasında değişen bir tam sayıdır. (32 bit adresleme sistemi).

Örnek olarak titan.ehb.beykent.edu.tr için bu numara 160.75.27.250 'dir.

Her internet adresinin ilk kısmı bulunduğu domain'in network adresini, son kısmı ise makinanın (host) numarasını verecek şekilde ikiye bölünür.

Bir bilgisayar ağında bulunan makinaların miktarına göre makina numarası için ayrılan kısmın daha büyük veya daha küçük olması gerekebilir. Değişik ihtiyaçlara cevap verebilmesi açısından IP adresleri aşağıdaki şekilde gruplanmıştır.

Class A network adresleri 1.0.0.0 adresinden 127.0.0.0 a kadar olan aralığı kaplarlar. Her networkte kabaca 1.6 Milyon makina bulunabilir

Class B network adresleri 128.0.0.0 adresinden 191.255.0.0 adresine kadar olan aralıktadır: 16065 network adresi ve her networkte kabaca 65500 makina bulunabilir

Class C network adresleri 192.0.0.0 adresinden 223.255.255.0 adresine kadar olan aralıktadır. Herbiri 254 makinadan oluşan yaklasik 2 milyon network adresi barındırır.

Class D 224 ve 254 arasında kalan adresler herhangi bir network tanımlamazlar, ileri kullanımlar için rezerve edilmişlerdir.

Bu domain adreslerinin dağıtımı NIC (Network Information Center) tarafından yapılır, daha sonra her domain sahip olduğu adresi kendi ihtiyaçlarına gore parçalayarak dağıtabilir. (Son zamanlarda, sınırlı sayıdaki internet adres uzayının bitebileceği düşüncesi ile, yeni bir adresleme stratejisine doğru da gidilmektedir. Önümüzdeki yıllarda, yeni tip IP adreslerinin (128 bit) ortaya çıkacağını bekleyebiliriz.)

Bu IP numaralarına (domain adreslerine) karşılık düşen bir makina ismi de bulunur. Bu sayede makinaların isimleri daha kolay akılda kalır. Her domain'de o domaine ait IP numaraları ile bu isimler arasında geçişi sağlayan bir servis (Domain Name Service) bulunur. Bu servis aynı zamanda diğer domain'lere ait isimleri ilgili DNS'lere sorarak öğrenir.

127.0.0.1 adresi ve 127.0.0.0 Network'u test ve geliştirme için kullanılır. 127.0.0.1 adresi her makinanın kendisini tanımlar buraya gonderilen her şey, sanki bir başka network'ten geliyormuş gibi makinanıza geri dönecektir.

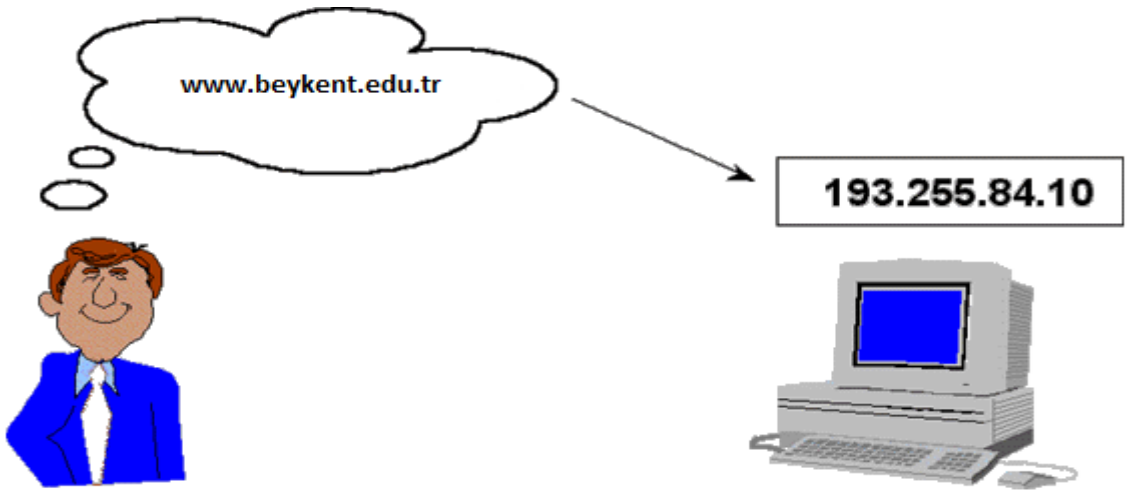
Bu adresleme sisteminde 128 bit uzunluğunda bir sistem kullanılmıştır. IPv6 olarak adlandırılan yeni adresleme sisteminde, teorik olarak, 340 trilyon kere trilyon kere trilyon adet (340'ın yanına 37 sıfır daha koyun !!) bilgisayarı adreslemek mümkündür. Bu sayı IPv4 için (32 bit adresleme sistemi) 4 milyar idi.

Bu IP numaralarına (domain adreslerine) karşılık düşen bir makina ismi de bulunur. Bu sayede makinaların isimleri daha kolay akılda kalır. Her domain'de O domaine ait IP numaraları ile bu isimler arasında geçişi sağlayan bir servis (Domain Name Service) bulunur. Bu servis aynı zamanda diğer domain'lere ait isimleri ilgili DNS'lere sorarak öğrenir.

Örneğimize geri dönecek olursak Beykent Üniversitesi bir kaç tane Class C network numarasına sahiptir. (193.255.84.0, 193.255.85.0) .beykent.edu.tr domaininde bulunan tum IP numaraları 193.255.84. ya da 193.255.85. ile başlar. Bunlar birer network tanımlar. Bu ağdaki tüm bilgisayarların adresleri ".beykent.edu.tr" ile biter. Ayrıca, istenirse, bağımsız alt alanlar da oluşturulabilir. Söz gelimi, Mühendislik Fakültesi için "eng.beykent.edu.tr" tanımlanmıştır. Burada eng, üst ağ altındaki başka bir alt ağı tanımlar. Söz gelimi bu ağda yer alan aurora ismi verilen makinenin IP numarası 193.255.84.10 aurora.eng.beykent.edu.tr şeklindedir.

Dikkat edilirse bir host numarası 1'den 254'e kadar 254 farklı değer alabilir. Zira 0 ve 255 bu numaralandırmada özel anlamlar içerirler. 0, network'u tanımlarken 255 de o network'teki tum hostları tanımlar.

Bilgisayarlar birbirlerini IP numaralarından tanırlar. İnsanların aklında kolay kalsın ve hiyerarşik yapılanma rahat yapılsın diye bunlar alt ağlar, makina adları gibi isimlendirmelere tabi tutulurlar. Yukarda görüldüğü gibi, internete bağlı her bilgisayarın (teorik olarak) bir IP numarası, ve o numaraya karşılık gelen de bir gerçek adı vardır. İki mekanizma arasındaki dönüştürmelerden DNS sorumludur.



Şekil.10. DNS'in Çalışma Mantığı

Şekil.10. Domain Name System protokolünün çalışmasını simgelemek için örneklendirilmiştir.

DNS, ayrıca, İnternet adresini nümerik adrese çevirir. Domain'ler hiyerarşik DNS adresleme sistemi içindeki farklı yapıları temsil ederler. Her domain kendi içinde bağımsız bir topluluktur. Doğal olarak, herkes kafasına göre gelişi güzel internet domain ismi ve IP numarası alamaz. Network Information Center (NIC)'e bunun için başvurmak gerekir. Aksi taktirde karmaşayı siz düşünun!!! Türkiye için bu numaraların dağıtımı ODTÜ, Ulaknet ve TTNet tarafından (ticari kullanımlar için) yapılmaktadır.

How DNS Works (28.03.2003)'dan alıntı yapılmıştır.

Domain Name System protokolünün çalışmasına ilgili linkten ulaşılabilir.

2.10. İnternet adreslerinde görülen kısaltmalar ne anlama gelir?

İnternet'e bağlı kuruluşlar değişik gruplara ayrılabilir ve bir kuruluşun domain adresi, o kuruluş hangi gruba dahilse ilgili kısaltmayı bazı istisnalar dışında mutlaka içerir. Ayrıca ülkelerin 2 harfli tanıtım kodları da (Amerika Birlesik Devletleri ve Kanada çıkışlı adreslerin çoğu ve geniş bir kitleye servis sunan bazı birimler dışında) adresin sonuna eklenir. Internet adresi, eğer özel amaçlı bir servise (ftp, gopher, www gibi) aitse, genellikle bu durum, adresin başında kullanılan bir kısaltmayla verilir. Aşağıdaki liste, adreslerde kullanılan bazı kısaltmaları ve ne anlama geldiklerini göstermektedir.

Tablo.2. Adres Kısaltmaları ve Açıklamaları

gov	Hükümet kuruluşları
edu	Eğitim kurumları (üniversiteler gibi)
org	Ticari olmayan, kar amacı gütmeyen kuruluşlar
com	Ticari kuruluşlar
mil	Askeri kuruluşlar
net	Servis Sunucuları (Internet Servis Sağlayıcıları gibi)
ac	Akademik kuruluşlar (bazı ülkelerde edu yerine kullanılmaktadır)
int	Uluslararası organizasyonlar, kuruluşlar
ftp	FTP Arşiv Sitesi (ön ek)
www	World Wide Web Sitesi (bazen **web** de kullanılır) -önek-

2.10.1. Bazı Ülke Kısaltmaları

tr: Türkiye, jp: Japonya, uk: İngiltere, it: İtalya, ch: İsviçre, ca: Kanada, ru: Rusya, id: Endonezya, nl: Hollanda, de: Almanya, fr: Fransa, il: İsrail, no: Norveç, se: İsveç, fi: Finlandiya, gr: Yunanistan, hr: Hırvatistan, yu: Yeni Yugoslavya, br: Brezilya, bg: Bulgaristan ...

2.10.2. Örnek Domain Adresleri

hokudai.ac.jp (jp=Japonya), bilkent.edu.tr (tr=Turkiye), oak.oakland.edu, servis.net.tr, www.microsoft.com, ftp.netscape.com, tubitak.gov.tr, garbo.uwasa.fi (fi=Finlandiya, www.nato.int (Nato).

Genel olarak bu sınıflamaya uyulsa da, bazı domain adlarında daha farklı sözcük grupları da olabilir (rl.ac.uk (uk=Ingiltere), www2.beykent.edu.tr gibi).

Özellikle .com domain-lerindeki sıkışmadan dolayı, yeni global domain adları oluşturma çalışmaları 1997 ortalarında tamamlanmıştır.

Yeni kullanıma açılan alan adları şunlardır:

Tablo.3. Yeni Alan Adları

firm	Ticari Firmalar
info	Bilgi servisi sunan siteler
nom	Kişisel domainler için kullanılan adresler
rec	Eğlence siteleri
stor	Alışveriş merkezleri, ticari ürün satılan yerler
web	www ile ilgili servis sunan siteler

2.11. İnternet Ne Kadar Güvenli?

İnternet'in, şu an için, çok fazla güvenli olduğu söylenemez. Nadiren de olsa, kişisel iletiler (e-posta, e-mail) kötü amaçlı, profesyonel kişiler tarafından illegal yollarla ele geçirilebilir. Özellikle ticari kuruluşların Internet'i kullanmaya başlamaları ile birlikte, Internet'te güvenlik probleminin çözümü için ciddi çalışmalar yapıldı. Web üzerinden iletilen her türlü bilginin, yeni şifreleme teknikleri ve çok yüksek hızlı hatlar sayesinde yeterince güvende olduğunu söyleyebiliriz. Ancak, yine de, kullanıcı şifreleri, banka kredi kart numaraları ve benzeri gibi gizlilik içeren bilgileri net üzerinde serbestçe göndermeyin (e-mail ile, güvenlik kilidi olmayan Web listeleyicileri ile vb.)

2.12. İnternette Bilgiler Hangi Hızlarla İletilir?

2.12.1. Band Genişliği Nedir? Doluluk Oranı Nedir?

Band genişliği, bir iletişim ortamının taşıyabileceği bilgi miktarını gösteren bir ölçüdür. Söz gelimi, ses iletimi için band genişliği, iletilebilen en yüksek ve en düşük frekanslar arasındaki farktır (Hertz). Bilgisayarlar arası haberleşme için de benzer şekilde, band genişliği, saniyede iletilen bit sayısı ile verilir.

Internet'teki bilgi iletim hızları çeşitlilik gösterir. Bilgisayarları ve değişik ağları birbirine bağlayan hatlar, kablo (çoğunlukla fiber optik), uydu ya da radyo link (yakın birimler için) bağlantılı olabilir. Internette hat hızı, saniyede iletilen "bit" sayısı ile (bps, bit/san) ölçülür.

Söz gelimi, 64 kilobit/saniye hızındaki bir hat saniyede 64kbit=65556 bit iletebilir. Bu da, ideal şartlarda, yaklaşık 8 kilobyte/saniye hızına denk gelmektedir. Söz gelimi, böyle bir hat ile, tam kapasite kullanımında, 1 Megabyte'lık bir dosya yaklaşık 2 dakikada iletilecektir.

Bir birimin, bağlantılarında kullanabileceği en fazla hıza "Band Genişliği" denir. 64kbit/saniye bant genişliği olan bir hattı aynı anda 10 birime kullandırırsak, buna göre hızımız, en fazla hızın ortalama %10'una kadar düşer.

Günümüzde bağlantı hızları 9.6kbit/saniyelerden (modem bağlantısı) 100Megabit/saniyelere kadar geniş bir aralıkta değişmektedir. Yurt dışındaki bağlantılarda, tipik hızlar, yaklaşık 5-10 Megabit/saniyeler mertebesinde iken, bu oran ülkemiz için, 64Kbit/san-2Mbit/saniyeler mertebesindedir.

Bir hattın bant genişliğinin ne kadarının kullanıldığı, o hattın doluluk oranını verir. Eğer 64kbit/san lik bir hat, 1 saat boyunca, %100 çalışırsa; 3600*64kbit 'lik veri aktarımı yapması gerekir.

Gerçekte ne kadar veri aktardığını bulup bu iki sayıyı birbirine oranlarsak, hattın, o saat için doluluk oranını bulmuş oluruz. Bunu 1 ay boyunca yaparsak, hattın 1 ay boyunca ortalama % kaç doluluk oranı ile çalıştığını tespit edebiliriz. Doluluk oranı ne kadar fazlaysa, o hattı kullananların veri aktarımları da o kadar yavaşlar.

2.13. DSL Çeşitleri

Bu bölüm içinde DSL çeşitlerini incelerken “data hızı” ve “santral–kullanıcı arası maksimum mesafeyi” de söylemek faydalı olacaktır.

Aşağıdaki tablo, herhangi bir ağ üzerindeki bilgisayarların ve internet üzerinde bilgisayarlar ve bilgisayar sistemlerininin birbirleriyle haberleşmesinde kullanılan bazı standart bağlantı hızlarını göstermektedir. Rouse, M.(Kasım 2010). Ülkemizdeki (özellikle internet için) bağlantı hızları aşağıdaki tanımlamalardan biraz uzaktır.

Tablo.4. DSL Çeşitleri

DSL Türü	**Tanımı**	**Data Hızı Download; Upload**	**Santral-Kullanıcı Arasındaki Max. Mesafe**	**Kullanıldığı Yerler**
IDSL	ISDN Digital Subscriber Line	128 Kbps	24 gauge tel üzerinden 5.5 km.	ISDN'e benzer ama ses iletilemez.
CDSL	Rockwell firmasının verdiği bir hizmet. Consumer DSL	1 Mbps download; daha az upload	24 gauge tel üzerinden 5.5 km.	"Splitter"sız. Ev ve küçük ofisler için kullanılıyor.
DSL Lite (G.Lite)	"Splitter" sız DSL	1.544 Mbps - 6 Mbps arası download, abone seçeneklerine göre değişen upload.	24 gauge tel üzerinden 5.5 km.	Standard ADSL, Splitter kullanılmıyor.
HDSL	High bit-rate Digital Subscriber Line	2 ayrı tel kullanılarak 1.544 Mbps download ve upload. 3 ayrı tel kullanılarak 2.048 Mbps upload ve download	24 gauge tel üzerinden 4 km.	Şirket içi LAN veya WAN çözümleri.
SDSL	Symmetric DSL	1.544 Mbps duplex (Amerika); 2.048	24 gauge tel	HDSL ile aynı fakat tek

		Mbps (Avrupa) download ve upload.	üzerinden 4 km.	kablo yettiği için daha ekonomik.
ADSL	Asymmetric Digital Subscriber Line	1.544 - 6.1 Mbps arası download; 16 - 640 Kbps arası upload.	1.544 Mbps - 5.5 km. 2.048 Mbps - 4km. 6.312 Mpbs - 3.5km. 8.448 Mbps - 2.8km.	İnternet ve yüksek hızda data iletişimi gerektiren diğer uygulamalar. Türkiye de uygulanan sistem.
RADSL	Westell firmasının bir hizmeti. Hız ihtiyaca göre değişiyor.	640 Kbps - 2.2 Mbps download; 272 Kbps - 1.088 Mbps upload. İhtiyaca göre anında değişiyor.	ADSL ile aynı	ADSL gibi fakat hıza göre anlık değişen tarifeler seçildiğinde kullanılıyor.
VDSL	Very High Digital Subscriber Line	12.9 - 52.8 Mbps download; 1.5 to 2.3 Mbps upload	1.2km - 12.96 Mbps; 900 m. - 25.82 Mbps; 300m. - 51.84 Mbps	İki fiber hattı birbirine bağlamak veya ISP yi internet omurgasına bağlamak için kullanılıyor. pek yaygın değil ama zaman içinde geliştirilip evlerde

				kullanılması bekleniyor.

Kaynak: TürkTelekom, (2013)

Ayrıca, farklı türde DSL çeşitlerini incelerken, bu türlere ait farklı modem çeşitlerine de değinmemin faydalı olacağını düşündüm. Burada aklımıza şu soru takılabilir (en azından benim takıldı) “Hani veriler dijital geliyordu? Bu modeme ne gerek var?” Sorunun cevabı ise: "yine de 0 ve 1 leri telefon hattına koymamız gerekmektedir. Oysa, bilgisayar frekanstan banttan anlamaz, dijital verileri bakır telin taşıyabileceği bir formata sokmamız gerekmektedir."

2.13.1. ADSL (Asimetric Digital Subscriber Line)

Mevcut telefon kabloları üzerinden asimetrik olarak ses, görüntü ve data iletimine olanak sağlanmaktadır. Asimetriktir, yani kullanıcıya doğru maksimum 8 Mbps iletişim hızı sağlarken, şebekeye doğru maksimum 640 Mbps hızlarını sağlar.

Tablo.5. ADSL Modem Cihazları

ADSL MODEM CİHAZLARI	
Ürün	**Açıklama**
Cisco827	Cisco 827 ADSL Router 1E, ADSL
MTD100U	Multitech ADSL USB Modem
Ürün	**Açıklama**
Prestige 630	Zyxel ADSL USB Modem

Prestige 642R-11	Zyxel Multi Mode ADSL Router
ST Pro (Ethernet)	Alcatel Speedtouch PRO (Ethernet)
ST Pro (HUB)	Alcatel Speedtouch PRO (Ethernet HUB)
ST Pro FW	Alcatel Speedtouch PRO with Firewall (Ethernet)
ST Pro FW (HUB)	Alcatel Speedtouch PRO with Firewall (Ethernet HUB)
ST USB	Alcatel Speedtouch USB (USB)

2.13.2. HDSL (High bit-rate Digital Subscriber Line)

High bit-rate Digital Subscriber Line, yada HDSL, Metal kablo perleri (bakır telefon kabloları olabilir) 2.340Mbps hızlara kadar iki yönlü simetrik data transferine izin veren fiziksel katman veri iletişim standardıdır.

Bu iletişim standardı sayesinde çok daha pahalı olan T1 (1.544Mbps) ve E1 (2.408 Mbps) bağlantılarının sağladığı tüm servisler HDSL tarafından da desteklenmektedir.

Tablo.6. HDSL ve HDSL2 Modem Cihazları

HDSL ve HDSL2 MODEM CİHAZLARI	
Ürün	**Açıklama**
90-0889-98	Newbridge 2703 V.35 DTU 64-128Kbps (PWR ADPTR inc)
90-2904-01	Newbridge 2902 G704+2V.35 DTU 64-2048Kbps (PWR ADPTR inc)

AL-HDSL-G703	Alcatel HDSL 1512LC Modem (G.703) PAKET
AL-HDSL-TTNET	Alcatel HDSL 1512LC Modem (TTNet) Paket
AL-HDSL-V35	Alcatel HDSL 1512LC Modem (V.35) PAKET
AL-RS-02	Alcatel Çekmeceli Sistem (G.703) Max. 16 Kart
CTU-S/G.703	Tellabs CTU-S/G.703 G.703 HDSL Modem
CTU-S/V.35	Tellabs CTU-S/V.35 V.35 HDSL Modem
HTU-2M	Tellabs HTU-2M HDSL Modem "64-2048 CH-E1"
InterDSL 2000	Zyxel HDSL Modem
STU-160	Tellabs STU-160 "64/128 Kbit/s BB Modem, 4 Telli”

Tablo.7. HDSL ve HDSL2 Router Cihazları

HDSL ve HDSL2 ROUTER CİHAZLARI	
Ürün	**Açıklama**
CISCO1601-R	Cisco 1601-R Ethernet/Serial Modular Router
CISCO1605-R	Cisco 1605-R Dual Ethernet/WAN Interface Card slot Router
CISCO1720	10/100BaseT Modular Router w/2 WAN slots, 8M Flash/32M DRAM
CISCO1750	10/100 Modular Router w/1VIC, 2WIC/VIC slots, Cisco IOS IP SW

CISCO1750-2V	10/100 Modular Router w/2 Voice channels, IOS IP/VOICE + SW
CISCO1750-4V	10/100 Modular Router w/4 Voice channels, IOS IP/VOICE + SW
CISCO1751	10/100 Modular Router w/ 3 slots, IOS IP, 16F/32D
CISCO1751-V	10/100 Modular Router w/Voice, IOS IP/VOICE Plus, 32F/64D
CISCO2501	Cisco 2501 Ethernet/Dual Serial Router
CISCO2514	Cisco 2514 Dual Ethernet/Dual Serial Router
CISCO805	Cisco 805 Ethernet/Serial Router
RT1602	Huawei Quidway R1602 Router/2 WAN
RT1603	Huawei QuidwayR1603 Router/1 WAN/1 BRI S/T
RT1760E	Huawei Quidway R1760 Host, 1 MIM Slot, 2 SIC slots with 1 10/100 Ethernet & 1 serial port
RT2501E	Huawei Quidway R2501E Router, 2 WAN/110V/220V
RT2509E	Huawei Quidway R2509E Router, 2 WAN/8 Asynchronous Serial Ports/110V/220V
RT2511E	Huawei Quidway R2509E Router, 2 WAN/16 Asynchronous Serial Ports/110V/220V
RT2620E	Huawei Quidway R2620 Router Chassis, 2 modular Slot, 1 10/100TX FE, 2 Synchronous serial port
RT2621E	Huawei Quidway R2621 Router Chassis, 2 modular Slot, 2 10/100TX FE, 2 Synchronous serial port

2.13.3. IDSL (ISDN Digital Subscriber Line)

IDSL (ISDN Digital Subscriber Line) 2-tel kiralık hat üzerinden 2B1Q hat kodlaması -2 bitli bir kodlanma tekniği - ile 5,5 km'de full-duplex 128Kbps BRI veri oranı sağlayan bir DSL teknolojisidir.

Tablo.8. IDSL Cihazları

IDSL CİHAZLARI	
Ürün	**Açıklama**
Cisco802-IDSL	Cisco 802 IDSL Router with Internet DSL
Cisco804-IDSL	Cisco 804 IDSL Router with Internet DSL
Omni 128 L	Zyxel IDSL Modem
Prestige 100L	Zyxel IDSL Multi Protocol Client-Router
Prestige 128L	Zyxel IDSL Multi Protocol Router

2.13.4. RADSL (Rate Adaptive Digital Subscriber Line)

RADSL, Rate Adaptive Digital Subscriber Line kelimelerinin baş harflerinden oluşan bir DSL teknolojisidir. Kullanıcılar telefon kabloları üzerinden data transfer ederken, hat kalitesi sürekli olarak değişmektedir. RADSL, hattaki bu değişimlere adapte olarak çalışır ve kullanıcılara ADSL mesafe limitini (3.5km) aşarak 5.5km içerisinde geniş bant bağlantı olanağı sağlar.

RADSL teknolojisi şu an Türkiye'de kullanılmamaktadır.

2.13.5. SDSL (Symmetric Digital Subscriber Line)

SDSL, Symmetric Digital Subscriber Line kelimelerinin baş harflerinden oluşan, halihazırdaki bakır telefon kabloları üzerinden daha fazla data transferine izin veren bir modem teknolojisidir. SDSL, sayısal abone hattına (DSL - Digital Subscriber Line) dayanarak ortaya çıkan ve telefonlarının sayısal kapasitesini oldukça arttıran bir seri teknolojinin parçalarından birisidir.

Çevirmeli ağ bağlantılarından çok daha hızlı, yaklaşık olarak 3Mbps, veri transferine izin verir. SDSL'in simetrik olarak adlandırılmasının sebebi data gönderme ve alma trafiğinin aynı hızlarda olmasıdır.

2.13.6. SHDSL (Symetric High-Data-Rate Digital Subscriber Line)

SHDSL, Symmetric High-data-rate Digital Subscriber Line'ın kısaltmasıdır. TC-PAM (Trellis Ceded Pulse Amplitude Modulation) üzerine kurulmuş ve 2 tel bakır telefon kablosu üzerinden 144Kbps veri hızından 2320Kbps veri hızına kadar simetrik olarak çoklu-oranlı (multi-rate) veri transferine olanak sağlamaktadır.

Tablo.9. SHDSL Cihazları

SHDSL CİHAZLARI	
Ürün	**Açıklama**
CISCO828	Cisco 828 G.SHDSL Router 1E, 1G.SHDSL
LPS510	SHDSL Application Pack
Prestige782	ZyXel Prestige 782

2.13.7. VDSL(Very-High-Bit-Rate Digital Subscriber Line)

VDSL telekom operatörlerinin, mevcut telefon hatları üzerinden kullanıcılarına multi-megabit servisler sunmasını sağlayan bir modem teknolojisidir.

VDSL, diğer xDSL teknolojilerine bakır telefon hatları üzerinden geniş bant veri ve ses transferini arttırmak yönünden benzerdir, fakat en hızlı teknoloji olan ADSL'den bile daha hızlı olmasıyla bunlardan ayrılır. Bunun yanında kapsama çevresi 1.5km ile diğer DSL teknolojilerinden daha düşüktür.

Tablo.10. CISCO ve PLANET VDSL Çözümleri

CISCO VDSL ÇÖZÜMÜ	
Ürün	**Açıklama**
CISCO575-LRE	Long Reach Ethernet CPE
PS-1M-LRE-48	POTS Splitter, 1MHz, 48 Port
WS-C2912-LRE-XL	12-port Catalyst Long Reach Ethernet switch

PLANET VDSL ÇÖZÜMÜ	
Ürün	**Açıklama**
VC-101M	1-port 10/100Base-TX/1-port VDSL Converter (Master)
VC-101S	1-port 10/100Base-TX/1-port VDSL Converter (Slave)

2.14. Ülkemizde DSL

2.14.1. Ülkemizde DSL - ADSL

Ülkemizde ve genelde dünyanın çoğu yerinde, ev ve ofis kullanıcılar için uygun olan ADSL kullanılmaktadır. Buna göre download hızı upload hızından daha yüksektir, çünkü normal bir kullanıcı eğer bir server çalıştırmıyorsa upload'dan ziyade

download yapıyor. Aşağıdaki tabloda da görüleceği gibi ADSL in normal DSL den farkı sadece asenkron olması yani download ile upload hızlarının farklı olması onun dışında kullanılan teknoloji veya ekipman açısından diğer DSL lerden farkı yoktur. Bu arada yukarıda gördüğümüz transfer hızları, biz kullanıcılara çekici gelmekle beraber; bu hız değerleri, mevcut teknolojiler kullanılarak dünya üzerinde sağlanan limit hızlardır ve Türkiye' de Türk Telekom un DSL tarifeleri oldukça maliyetlidir.

Standart ve en ucuz tarifemiz 128/32, yani 128 kbit = 16kilobyte download, 32kilobit = 4kilobyte upload. Diğer tarifeler ve ücretlerini de aşağıda belirttim:

Tablo.11. DSL Tarifeleri

HIZI (Kbps)	**BAĞLANTI ÜCRETİ**	**AYLIK ÜCRET(TL)**
128/32	11.000.000	**33.000.000**
256/64	11.000.000	**112.000.000**
512/128	11.000.000	**342.000.000**
1024/256	11.000.000	**918.000.000**
2048/512	11.000.000	**1.555.000.000**

Buna ek olarak bir DSL modem almamız gerekmektedir. Bu modem de aşağı yukarı 200 - 300 dolar tutmaktadır. Elkotek,(b.t.) Modem fiyatları.

2.15. Elektronik Para (e-para, e-cash, sanal para) Nedir?

E-para, tam olarak, kullandığınız bilgisayarın sabit diskinde sizin adınıza bulunan ve internet üzerinde yaptığınız alışverişlerde harcayabileceğiniz paradır. Siz harcama yaptıkça, harcadığınız miktar toplamdan düşülür. e-para kullanımı pek yaygın değildir. Ancak, gelecekte sık kullanacağımız bir araç olabilir.

Temel olarak, gidip, e-para servisi veren bir bankadan, kredi kartımızla ya da peşin ödemeyle, bir miktar e-para alıyoruz.

Daha sonra, banka bu miktarı bizim bilgisayarımıza transfer ediyor. Internet üzerinde bir alışveriş yaptığımızda da, eğer burada e-para geçiyorsa, sipariş formunda e-para ile ödeme yapılacağını belirtiyoruz. Miktar otomatik olarak bilgisayarımızdaki miktardan düşülüyor. Bütün bu işlemler, e-para servisi veren bankamızdan da kontrol ediliyor. Bazı uygulamalarda, e-para ödemesi doğrudan bankadan yapılıyor.

Bu durumda, size bir e-posta mesajı ile ilgili siparişi alıp almayacağınız soruluyor. Böylece, alışverişlerde, fiziksel olarak alışageldiğimiz "para dolaşımı" ortadan kalkıyor.

1997 itibarıyla, 3 tane e-para sistemi var : Digital Cash (http://www.digicash.com), Cyber Cash (http:www.cybercash.com) ve First Virtual (http://www.fv.com). Tüm dünyada, e-para kabul eden banka sayısı ise şu anda 4. (3 ABD'de, 1 Almanya'da)

2.16. Firewall (Güvenlik Sistemleri) Nedir?

Firewall (Internet Güvenlik Sistemi), internet üzerinden bağlanan kişilerin, bir sisteme girişini kısıtlayan/yasaklayan ve genellikle bir internet gateway servisi (ana internet bağlantısını sağlayan servis) olarak çalışan bir bilgisayar ve üzerindeki yazılıma verilen genel addır.

Firewall sistemleri, bu engelleme işini, sadece daha önceden kendisinde tanımlanmış bazı domainlere erişim yetkisi (telnet,ftp, http vb) vererek yaparlar. Günümüzde, Internet Servisi veren makinalar oldukça sofistike Firewall sistemleri ile donanmıştırlar.

2.17. Proxy Servisleri Nedir?

Proxy servisi, internet üzerindeki yerel bir ağ (ya da internete bağlı bir bilgisayar) ile dış dünya arasındaki ilişkiyi sağlayan bir yardımcı geçiş (gateway) sistemidir. İki amaç için kullanılabilirler.

Bir proxy servisi (sunucusu), sizin adınıza (proxy'nin kelime anlamı VEKİL'dir) sizden aldığı "internet'ten bilgi alma" isteklerini yürütür ve sonucu yine size iletir. Ancak, aynı anda, bu bilgilerin bir kopyası da (cache),bu proxy sunucusu üzerinde tutulur ve bir dahaki erişimde kullanıcının istediği bilgiler doğrudan ilgili siteden değil de, proxy servisinden gelir; dolayısıyla, iletişim daha hızlı olur. Internet'e erişim için mutlaka bir proxy servisine ihtiyaç yoktur, ancak, size en yakın bir servis noktasındaki proxy servisini kullanmanız, internet erişiminizi birhayli hızlandıracaktır.

Özellikle evinizden modemle internete erişiyorsanız, proxy servislerini kullanmanız performansınızı arttırır. Çünkü istediğiniz bilgileri, dış bağlantı hızı daha fazla olan proxy bilgisayarı sizin adınıza alır, siz de kişisel bağlantınızla bu bilgilere daha hızlı erişmiş olursunuz.

Firewall-güvenlik sistemlerinin kullanıldığı yerlerde, kullanıcıları çıkışları tek bir makine üzerinden olabilir.

Bu durumda proxy servis makinesi sadece bir aracı olarak çalışır.

Proxy servisi kullanmanın avantajı çoktur. Herhangi bir siteden istediğiniz bir bilgi (web sayfası, ftp dökumanı vb) eğer kullandığınız proxy servisinde henüz depolanmamışsa, bu bilginin olduğu siteden alınır ve size iletilir. Ancak, daha sonra başka bir kullanıcı (ya da siz) aynı dökümanı/bilgiyi istediğinizde, ilgili döküman/bilgi proxy servisinde depolandığı (cache) için, doğrudan oradan size iletilir ve erişiminiz de çok daha hızlı olur.

Proxy servisleri, uluslararası internet bağlantılarındaki yoğunluğu azaltmak, erişimleri hızlandırmak ve ağı daha etkin kullanmak için çok yararlı araçlardır.

En popüler proxy servisleri, Web (http), FTP, Gopher ve Wais internet araçları için tanımlıdır.

2.18. İnternet Society (Internet Grubu) Nedir?

İnternet Society (IS), 1992'de kurulan ve amacı internet ile ilgili gelişimler, yeni çalışmalar için bir nevi yol göstericilik olan, kar amacı gütmeyen (non-profit) Biri kuruluştur. IS, Internet ile ilgili teknik çalışmaları yönlendiren ve denetleyen Internet Architecture Board (IAB)'un çalışmalarını destekler. IAB'nin aktivitelerinden bir diğeri de, TCP/IP konusunda çalışmalar yapan Internet Engineering Task Force (IETF) tır. IAB'nin diğer aktiviteleri arasında, Ağ Teknolojileri ile ilgili çalışmalar yapan Internet Research Task Force; IP adreslerinin verilmesi ile ilgili çalışmalar yapan Internet Assigned Numbers Authority; ve DNS ile ilgili konularda çalışan Internet Registary grubu gösterilebilir.

Internet Society ‘den alıntıdır.

2.19. İnternet Kullanım Etiği

Ağ üzerindeki her kullanicının, servisleri, sistemleri kullanmaları konusundaki sorumluluklarını farketmeleri önemlidir. Kullanıcı, ağdaki her servise ulaştığında yaptığı hareketlerden sorumlu olmak zorundadır.

"Internet" ya da kısaca "Net" , tek bir ağ değildir, hatta bir birinde ayrı protokollere, yapılara sahip binlerce irili ufaklı ağların toplamıdır. Internet'teki bilgi akışı, birçok

değisik ağ'dan gelip geçmekte, ulasacağı yere öylece varmaktadır. Bu yüzden, her kullanıcının, kendi bölgesindeki ağ yukünü dengede tutması gerekmektedir.

Bir ağ kullacısı olarak, başka bilgisayar ağlarına ulasmanıza izin verilmiş olabilir. Her ağın kendine ait sorumlulukları, kuralları ve yasakları vardır, Ağ üzerindeki izin verilmiş işlemler, bu ağdaki sorumlular tarafından her zaman izlenebilecek sekilde tasarlanmıştır. Fakat bir yerde izin verilen bir hareket başka bir ağda yasaklanmış olabilir. Bu kuralları bilmek ve bunlara uymak, kullanıcının sorumluluğundadır. Sunu unutmayın ki, izin verilen hareketleri kötü yönde de "YAPABİLİRSİNİZ" , ama yapmanız gerekmez.

Ağ'ın, özellikle Internet'in kullanımı, bir ayrıcalıktır, bir "hak" değildir. Bu ayrıcalık, istenildiği zaman, kötüye kullanım ya da başka sebeplerle, elinizden alınabilir. Bu kötüye kullanım, bir sistemdeki gizli bilgileri hileli yollarla almak, kötü, anlaşılmaz mesajlarla diğerlerini rahatsız etmek, sistemin kaynaklarını kullanıp sistemi yavaşlatmak, ardarda mesajlar postalayarak başkalarının e-posta kutularını doldurmak, ağ üzerinde yasalarla belirlenmiş kuralların dışına çıkmak vs vs olarak sayılabilir.

Bulunduğunuz ağ'ın durumuna gore, disiplin cezasından işten çıkarılmaya; hesabınızın silinmesinden hapse kadar cezalara çarptırılabilirsiniz.

2.20.İnternetin Sosyal, Ticari ve Hukuki Boyutu

2.20.1. İnternet'in Sosyal Boyutu

Yaygın bir görüşe göre internet, kişilerin sosyal yaşamlarında olumsuz etkilere sahiptir. Gerçek dünyadan farklı bir ortamda, "sanal dünyada, insanlar arası ilişkiler değişmektedir. Bu bir bakıma doğru, Çoğu durumda birbirleri ile etkileşen insanlar bir internet adresi, bir e-mail adresi vb gibi. Öte yandan internet, kişiler arasındakji

mesafe, yaş, cinsiyet, ırk, kültür vb gibi gerçek dünyada önemli olabilecek pek çok özelliği de ortadan kaldırmaktadır.

Yerinden alışveriş, yerinden bankacılık, hatta işe gitmeden evden çalışma vb gibi kullanımlar insanın sosyal yaşamını etkileyebilecek unsurlardır. Bir açıdan bunlar insana başka işler yapmak için zaman kazandırmakta; öte yandan başka bir açıdan da tembelliğe itmektedir. Ancak, internet kullanımının hayatın akışını yönlendiren servislere kaydığını düşünürsek, artık iş tanımları, yaşam biçimleri vb değişmeye başlamıştır. Bu yüzden internetin sosyal boyutunu düşünürken; yaşam kurallarını klasik anlamda değil de "değiştiği" anlamlarda düşünmekte fayda var.

2.20.2. İnternet'in Ticari Boyutu

Internet'in 1990'ların başlarından itibaren bu kadar yaygınlaşmasının en temel nedenlerinden birisi ve belki de en önemlisi "para kazandırabilecek potansiyele sahip" bir imkan olmasıdır. Bu iletişim ağına bağlı bilgisayarlar yolu ile alışverişler yapılabilmekte, borsa/bankacılık işlemleri yerine getirilebilmektedir. Bu haliyle internet'in "ağ teknolojisi" kimliğinin yanında bir de "medya" özelliğinden söz edebiliriz. Internet artık ciddi reklam paralarının dönmeye başladığı ve şirketlerin ürünlerini pazarladığı bir ortam haline gelmeye başlamıştır.

2.20.3. İnternet'in Hukuki Boyutu

Siber kültür ve siber toplum, büyümeyle beraber kendi kurallarını da "yazılı" hale getirmeye başlamıştır. Halen "kontrol edilememe" noktasındaki serbesti ve kişilik hakları, telif hakları gibi önemli konular, ticari uygulamalardaki boşluklar, vergilendirme sistemi gibi birçok "geleneksel hukuk" konuları, bu "yeni" toplumsal ortama adapte edilmeye çalışılmaktadır.

Kaynak: İnternetin sosyal,ticari ve hukuki boyutu, (b.t.)

3. ROUTING TEMELLERİ (YÖNLENDİRME TEMELLERİ)

Bu tez dökümanı içerisinde yer alan bilgiler, network dünyasının temellerini oluşturan LAN ve WAN switching ve routing kavramlarından özellikle "routing" (yönlendirme) temelleri üzerine network dünyası ele alınmıştır.

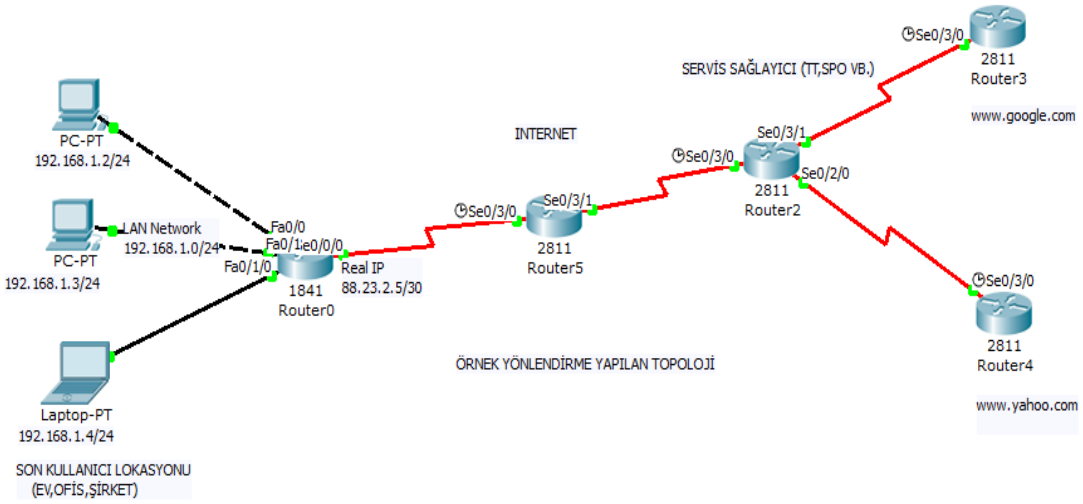
Routing kavramı genel bir kavram olmakla beraber en popüler olan network üreticisi Cisco ile özdeşleşmiş durumda görünmektedir.

3.1. Routing

LAN (Yerel Ağ Bağlantısı) bağlı olan ve iç network'de yer alan dosyaların, videoların bulunduğu sunuculara erişirken mutlaka bir yönlendirmeye ihtiyaç duyulur. Örneğin; 192.168.1.2 Ip adresine ve 255.255.255.0 Alt ağ maskesine sahip olan bir kullanıcının, internet erişimi üzerinden bir web sayfasına (www.google.com, Ip add= [173.194.39.81] erişmesi adına yönlendirmeye ihtiyaç duyulur. Sebebi farklı IP subnetlerinde, yani farklı network'lerde olmalarıdır.

Yönlendirme işlemi yapılabilebilmesi için "Router" yönlendiriciye ihtiyaç duyulmaktadır. En basit örneği ile evlerde router amacı ile kullanılan ADSL (Asimetrik Sayısal Abone Hatları) destekleyen, "ADSL" modemler mevcuttur. Yani internet erişimi olan herkes doğrudan Router ile routing işleminden faydalanmaktadır.

Tüm bilgisayar kullanıcılarının, tabi tutulduğu bu işlem nasıl oluyorda karşı taraftaki network'e gideceğini biliyor? Routing Tabloları IP adreslerinin, hangi kaynaktan gelip hangi kaynağa gittiğinin bilgisini tutmaktadır. Bu tutulan tabloda Kaynak (Source) ve Hedef (Destination) adresler yer almaktadır. Router'ların routing tablosu tutabilmesini sağlayan Routing Protokoller mevcuttur.



Şekil.11. Yönlendirme Topolojisi

Routing Protokoller kendi içlerinde genel kapsam çerçevesinde ikiye ayrılırlar.

- Statik Yönlendirme
- Dinamik Yönlendirme

3.1.1. Statik Yönlendirme

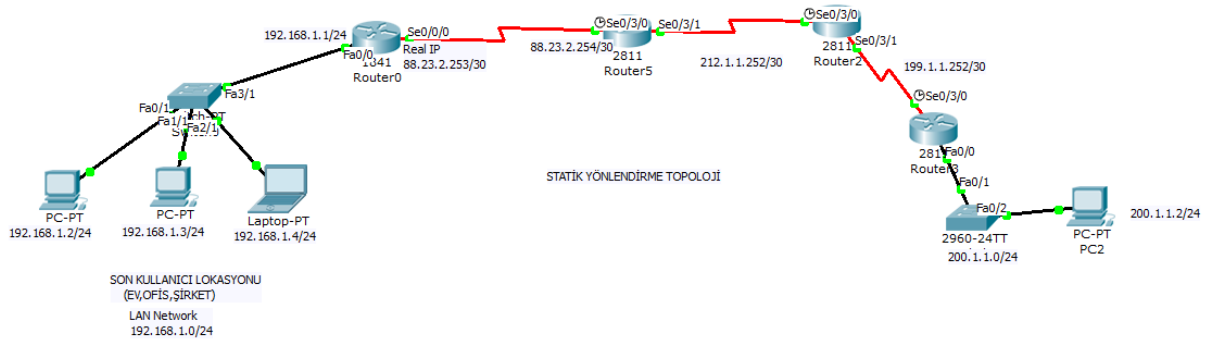
IP tabanlı olarak çalışan ve IP (Layer3) katmanına müdahele edebilen cihazlarının tamamında olan bir yetenektir. Kişisel bilgisayarlarda komut satırından istenilen yönlendirme rotaları yazılabilmektedir. Bilgisayarların özellikle ve öncelikli olarak erişmesini istedilen herhangi bir "IP" için rota yazılabilir.

Statik yönlendirme desteği ADSL modem'ler dahil olmak üzere bir çok Layer 3 cihazda mevcuttur. Örneğin Başlangıç serisi Cisco 8xx serisi veya HP 9xx serisi router'lar mevcuttur. Statik yönlendirme işlemi "16 Adet " IP networküne yönlendirme gibi limitlere takılmaktadır.

Duruma göre kullanılır, 1 veya 2 Adet network için tanımlama yapmak gerekiyorsa Yönlendirme sayısının az olduğu durumlarda rahatlıkla kullanılabilir. Fakat mevcut'da gerçekleşecek IP değişiklikleri gibi olası müdahele gerektiren durumları göz önünde tutmak gerekmektedir. IP değişiklikleri söz konusu olduğunda yapılmış olan yönlendirme tanımlamalarınıda, yeni IP lere göre güncellemek gerekmektedir.

İşte bu gibi durumlarda protokolün yetersizliğinden ve yaratacağı ek işlem yükünden dolayı dinamik routing protokollere ihtiyaç vardır.

Aşağıdaki Örnek topoloji referans alınarak statik yönlendirme tablosu oluşturulacaktır.



Şekil.12. Statik Yönlendirme Topolojisi

Statik Yönlendirme yapılabilmesi için aşağıdaki kavramların bilinmesi gerekmektedir.

Örnek statik route komutu; İp route 212.1.1.252 255.255.255.252 88.23.2.252

İp route : Statik IP yönlendirme işlemine başlanıldığını ifade eder.

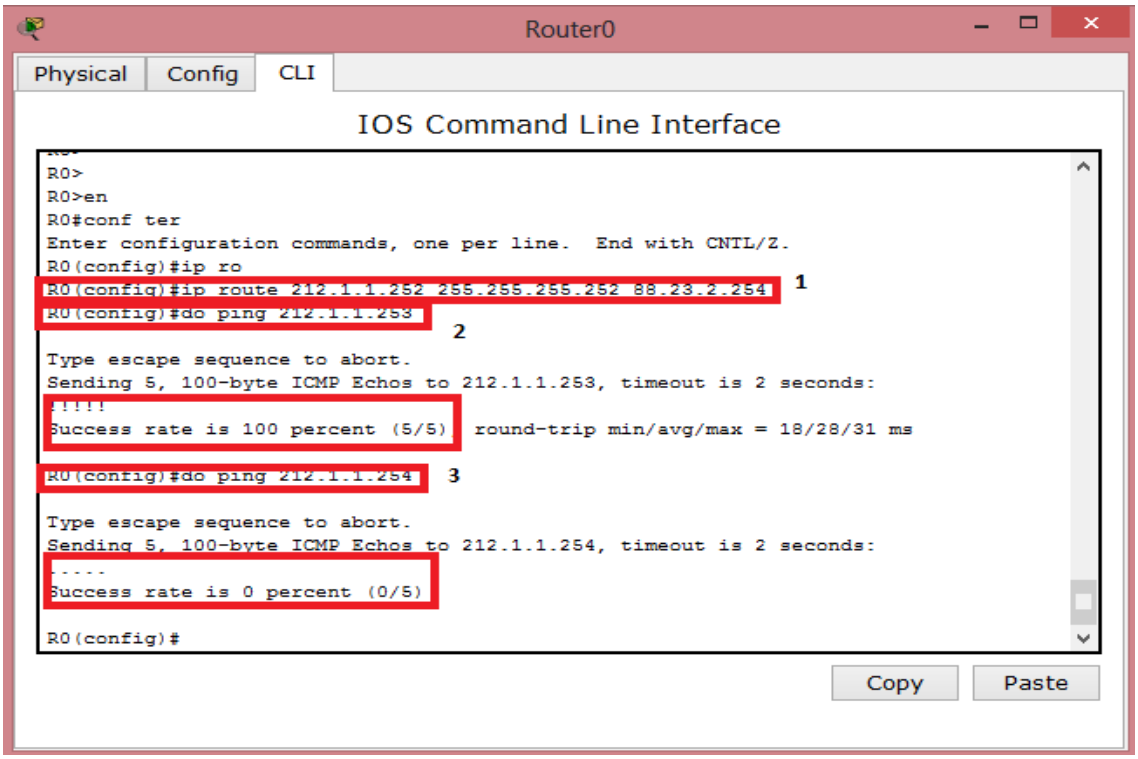
Destination Network: Yönlendirilmesi istenen IP networkü (ulaşılamayan). (212.1.1.252)

Destination Mask: Yönlendirilmesini istediğimiz IP networküne ait olan Subnet Mask. (255.255.255.252)

Forwarding IP Address: Hedef network'e ulaşabilmek için bir önceki interface'de yazılı olan IP adresi. (88.23.2.252)

Yukarıdaki örnekteki açıklamalar göz önünde bulundurularak tek yönlü sadece gidiş yönünde statik yönlendirme kuralı girilmiştir. Statik yönlendirmelerde yönlendirme konusu tek yönlü çalışmamaktadır. Mutlaka her iki yönlendirici cihaz için çift taraflı olarak yönlendirme bilgisi yukarıdaki gibi girilmelidir. "R0 " Routerından - "R5" Router'a yönüne Rota bilgisi yazıldıktan sonra, "R5" routerından – "R0" routerı yönündede trafiğin tam tersi düşünülerek bir rota tanımlanması gerekmektedir. Aksi halde paket iletimi tamamlanır fakat geri dönüş yolu bilinmediği için iletişim çift yönlü gerçekleşmeyecektir.

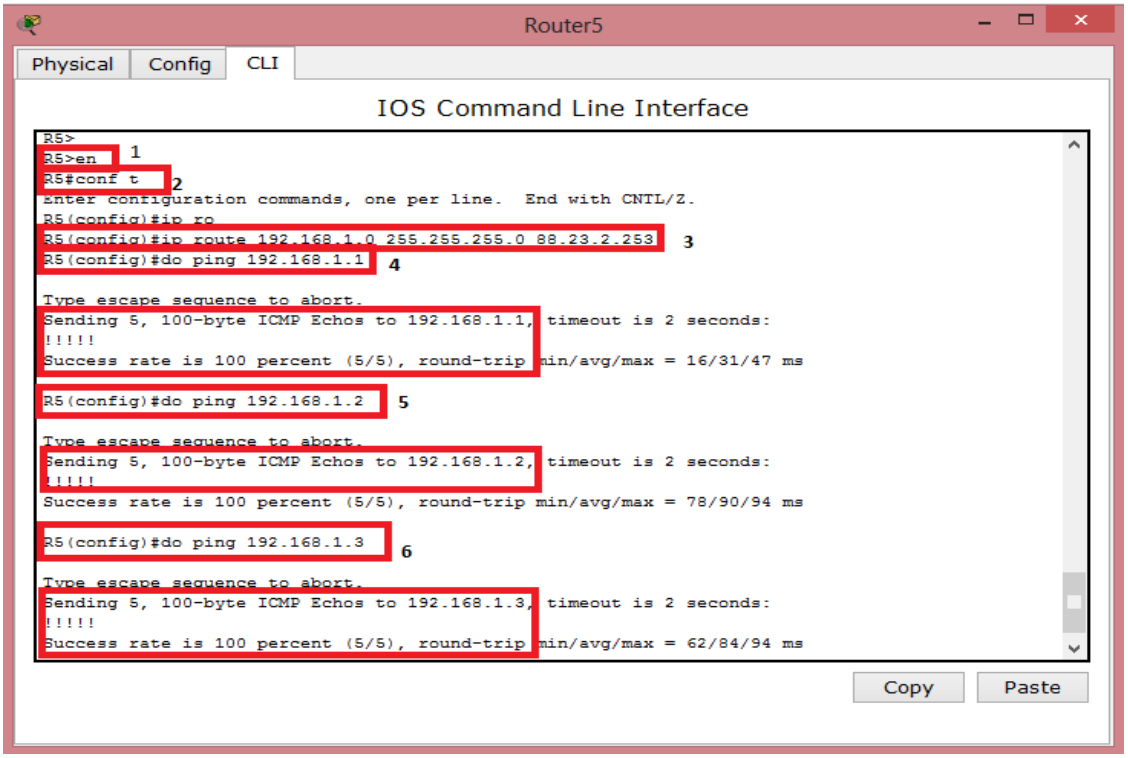
Bahsedilen temel komut yazımı her iki router içinde aşağıda yer almaktadır.



Şekil.13. Statik Yönlendirme(Tek Yönlü)

Yukarıdaki ekran çıktısında “Router 0” dan - “Router 5 “arkasındaki network’e statik yönlendirme kaydı girilmiştir. Yönlendirme şablonu ve test komutları kırmızı çerçeve içerisine alınmıştır.

Bu ekran çıktısı tek yönlü yapıldığı için karşı network’e “ping” atılamamıştır. Tam tersi yönünde erişimin çift yönlü olabilmesi için “Router 5” ekran çıktısından faydalanılması gerekmektedir.

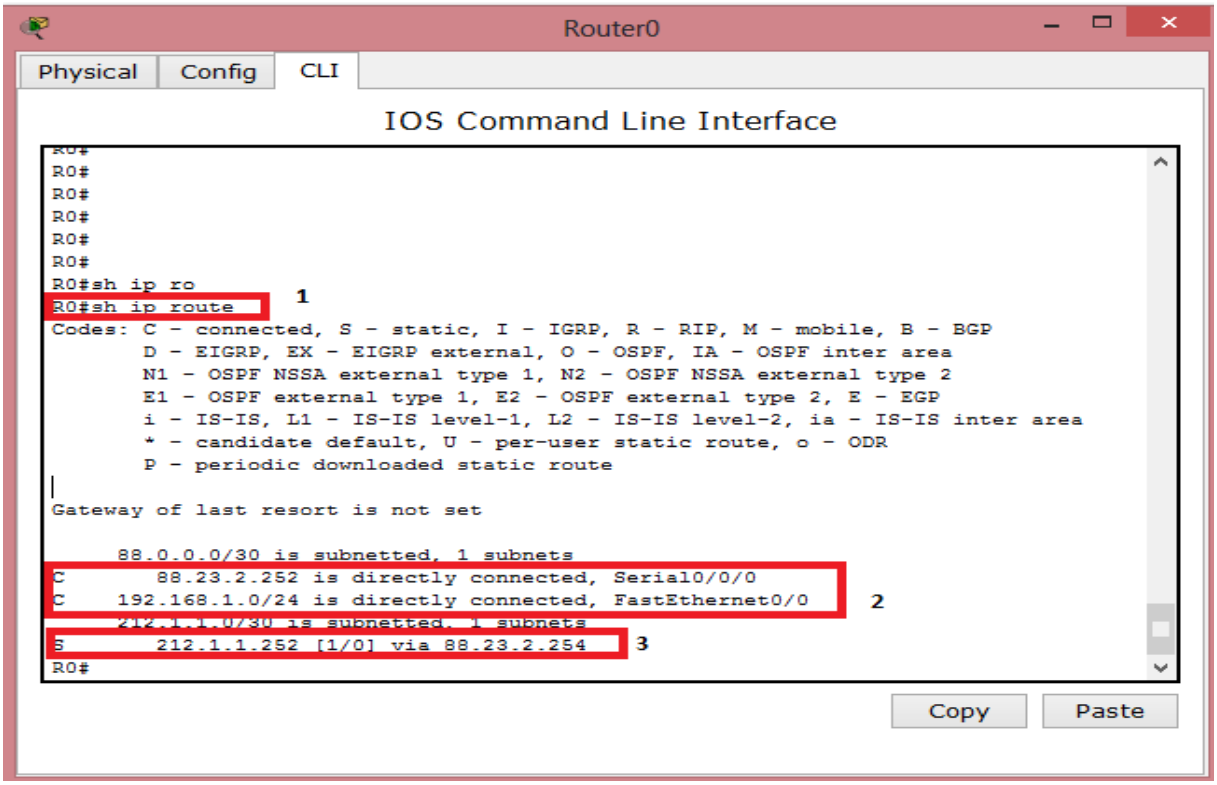


Şekil.14. Statik Yönlendirme(Çift Yönlü)

Yukarıdaki çıktıda çift yönlü tanımlama gerçekleştirilmiştir. Ardından test amaçlı çift yönde erişim testi son kullanıcı bilgisayarlarına ve onların bağlı olduğu default gateway’e (Router) ping atılarak test işlemi ve 2 Router arasındaki yönlendirme işlemi tamamlanmıştır.

Not : Tüm Router’lar da trafik çift yönlü düşünülerek arada geçilmesi gereken IP tabanlı tüm tanımlamalara her router için ayrı ayrı statik yol yazılması unutulmamalıdır.

Son Olarak Routing Tablosu aşağıdaki gibi görünmektedir.



Şekil.15. Statik Yönlendirme(Routing Tablosu)

3.1.2. Dinamik Yönlendirme

Dinamik yönlendirme protokolleri routing operasyonu yapabilen ADSL modem ve Diğer Router üreticilerinde donanım ve işletim sistemi yeteneğine göre detayları ile kullanmak mümkündür.

Dinamik routing protokoller, isminden de anlaşıldığı üzere statik routing'in tam tersi şeklinde çalışmaktadır. Yani IP tabanlı olarak yapılan tüm cihazlardaki değişiklikler sadece ilgili cihazı bağlayan bir faktördür. Tüm cihazlarda IP tabanlı rotaları değiştirmeye gerek kalmamaktadır. Yalnızca IP değişikliğinin yapıldığı cihazda dinamik rotayı değiştirmek yeterlidir.

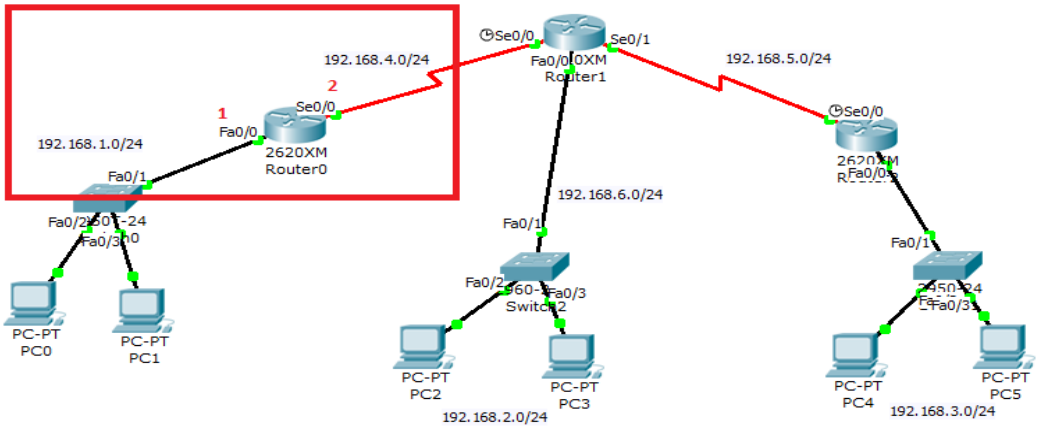
Dinamik yönlendirme protokolleri yeteneklerine ve ihtiyaçlara göre çeşitlilik göstermektedir.

RIP, EIGRP (Cisco) , OSPF, BGP, IS-IS olmak üzere çeşitli routing protokoller mevcuttur. Bu protokollerin tamamı detayları ile dinamik yönlendirme protokolleri başlığı altında detaylıca incelenmektedir.

3.2. Dinamik Yönlendirme Protokolleri

Dinamik Yönlendirme Protokolleri başlığı altında dinamik yönlendirmenin çalışması hakkında genel bilgi verilmektedir.

Dinamik Yönlendirme protokolleri, her router kendi üzerine direkt olarak bağlı olan networklerden sorumludur diye bir klasik kavram mevcuttur.



Şekil.16. Dinamik Yönlendirme

Şekil.16.'ya bakıldığında Router "0" üzerindeki direkt bağlı olan Fa0/0 ve Se0/0 interfacelerini Router"0" bilir ve diğer networklerin bilgisini bu interface IP'leri üzerinden alabilir.

Dinamik yönlendirme konfigürasyonu yapıldığı zaman sadece Router'larda üzerlerine direkt bağlı olan interfacelerin IP network adresleri girilir ve diğer router'larda aynı şekilde networkler anons edilir.

Bu işlem doğrultusunda bütün networkler, her router'da yapılan network IP tanımlamaları sonucunda, Router'ların IP Tablolarında, kullanılan Yönlendirme protokololünün yeteneğine ve özelliklerine göre tabloda yer alır ve kaynak network ile hedef network arasında iletişim gerçekleştirilmiş olur.

Yönlendirme protokolü tipleri;

Yönlendirme protokolleri çalışma şekillerine göre 3 farklı başlıkta incelenir.

1. Distance Vector Routing Protokol
2. Link-State Routing Protokol
3. Hybrid Routing Protokol

Distance Vector çalışan protokol RIP (Routing Internet Protokol) dir.

Link State Routing çalışan protokol IS-IS ve OSPF 'dir

Hybrid çalışan EIGRP ve BGP protokolleridir.

3.2.1. Distance Vector Protokol

Uzaklık vektör protokolünün çalışma mantığı ortamdaki birbirlerine direkt bağlı olan tüm router'ların IP bilgilerini öğrenip, aynı zamanda birbirlerine bağlı olan tüm routerlar için uzaklık bilgisi, geçilen router sayısı ve IP tablosu bilgisini "broadcast" bağırma yolu ile öğrenip bahsi geçen bilgilerin tamamını topoloji üzerindeki tüm routerlar ile paylaşırlar.

Paylaşılan bu bilgiler doğrultusunda gidilebilecek maksimum mesafe uzunluğu geçilecek router ve network sayısı göz önünde bulundurularak network analizi broadcast yolu ile yapılıp network haritası çıkartılmış ve tüm routerlar ile paylaşılmış olur.

Bu protokol çalışma mantığında temelde bir sorun yokmuş gibi görünsede, yetenekleri bakımından küçük ölçekli networklerde kullanılması tavsiye edilir.

Güncellemelerin routerlar arasında yapılması bu protokoller vasıtası ile çok yavaştır. Güncellemelerin yavaş paylaşılması ve paylaşılan bilgilerin karşılaştırılmasının yapılması gibi bir algoritma söz konusu olmadığı için, Count İnfinity ve Split Horizon gibi olumsuz durumlar ile karşı karşıya kalınır. Bu problem keşfedildikten sonra bu protokole yetenek olarak kazandırılmıştır. Fakat sonuca yavaş ulaşılmasından dolayı pek sıcak bakılan ve rağbet gören bir protokol olma görüntüsünden uzaklaşmıştır.

4. RIP PROTOKOLÜ ÖZELLİKLERİ

Routing Information Protocol yeteneği maksimum 15 Hop(Router) geçebilir. 16. Router arkasındaki network'e ulaşamaz.

RIP protokolü her 30 sn'de bir routing tablosunu güncellerler.

RIP v1 ve v2 olmak üzere iki tip RIP versiyonu vardır.

4.1. RIP V1 Özellikleri

Classful çalışır

VLSM desteği yok

Broadcast çalışırlar

Summarization desteği yok

Authentication desteği yok

RFC 1058'e göre çalışması açıklanmıştır

4.2. RIP V2 Özellikleri

Classless çalışır

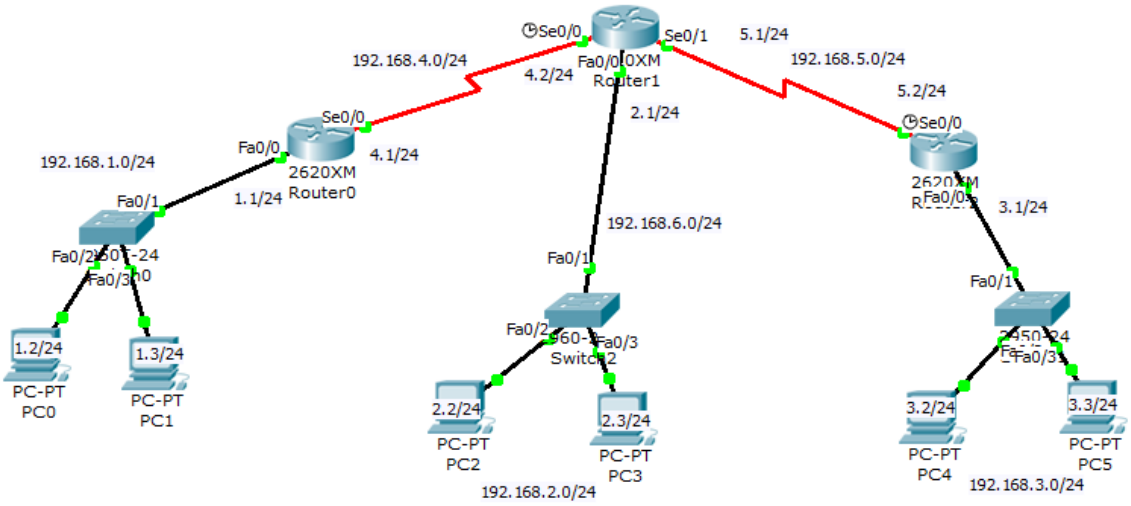
VLSM desteği var

Multicast çalışır

Summarization desteği var

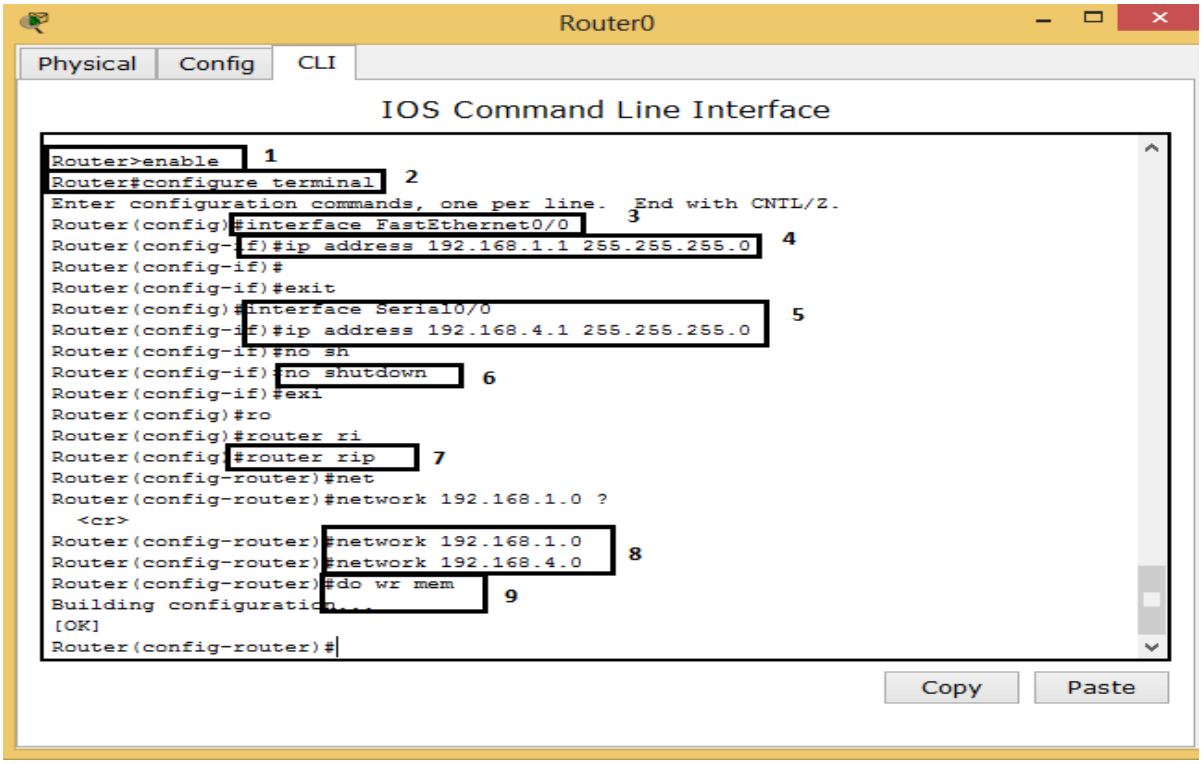
Authentication desteği var

RFC 1721,1722 ve 2453'e göre çalışması açıklanmıştır.



Şekil.17. RIP Konfigürasyonu

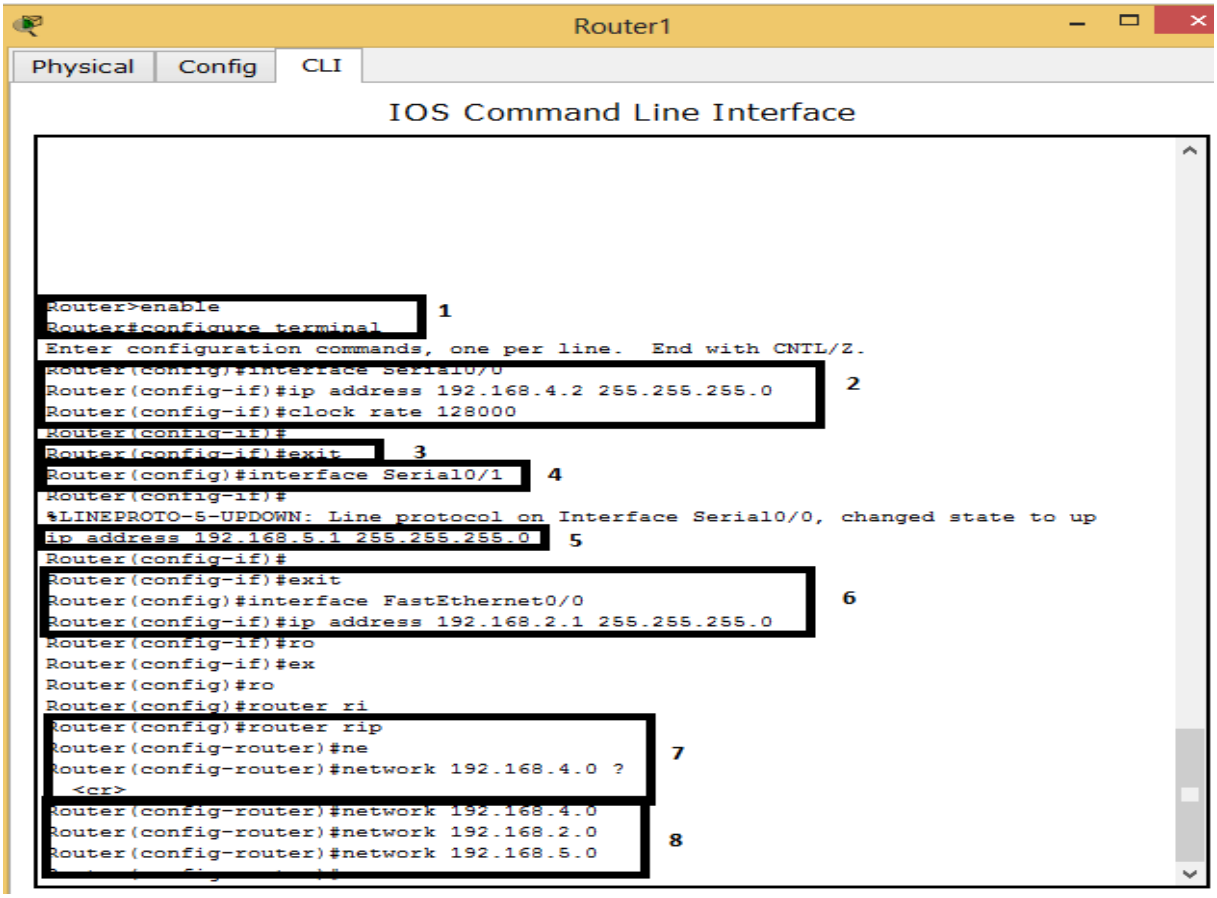
Router "0" üzerindeki sıfırdan yapılması gereken konfigürasyon adımları aşağıdaki gibidir.



Şekil.18. RIP Konfigürasyonu-Router 0

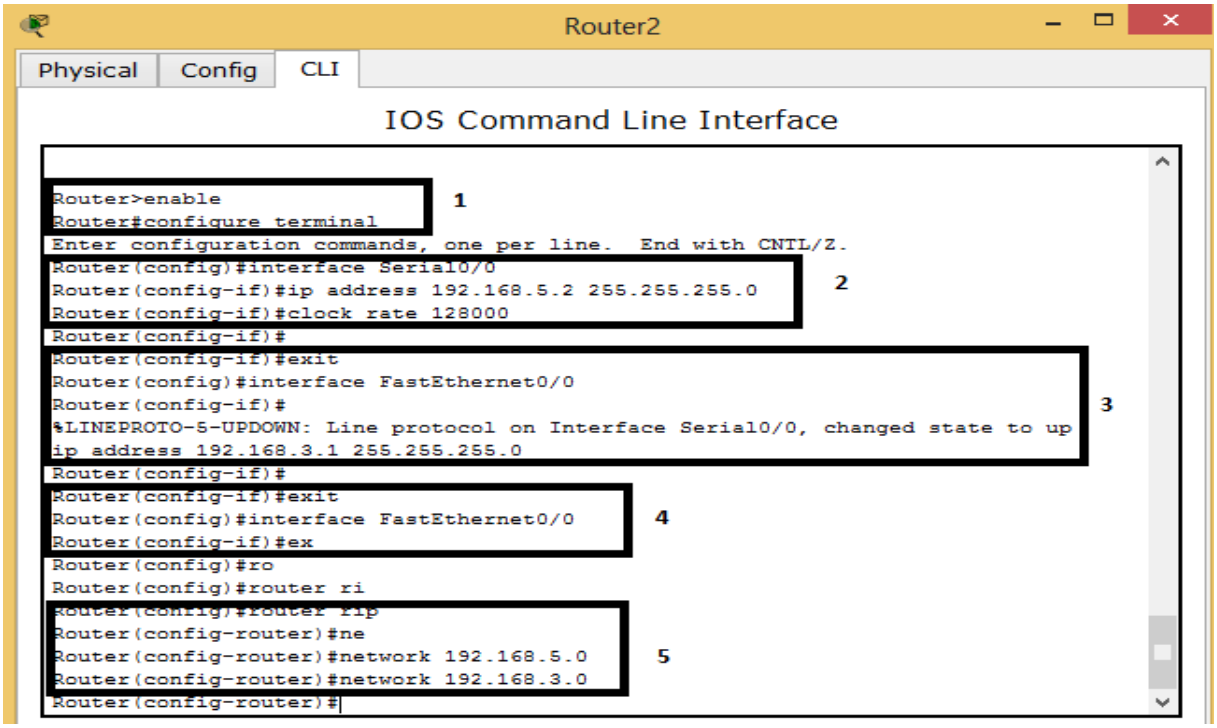
Yukarıdaki topoloji göz önünde bulundurularak basit anlamda RIP konfigürasyonu aşağıda konfigürasyon adımları gerçekleştirilerek RIP konfigürasyonu tamamlanmaktadır.

Router "1" üzerindeki sıfırdan yapılması gereken konfigürasyon adımları aşağıdaki gibidir.



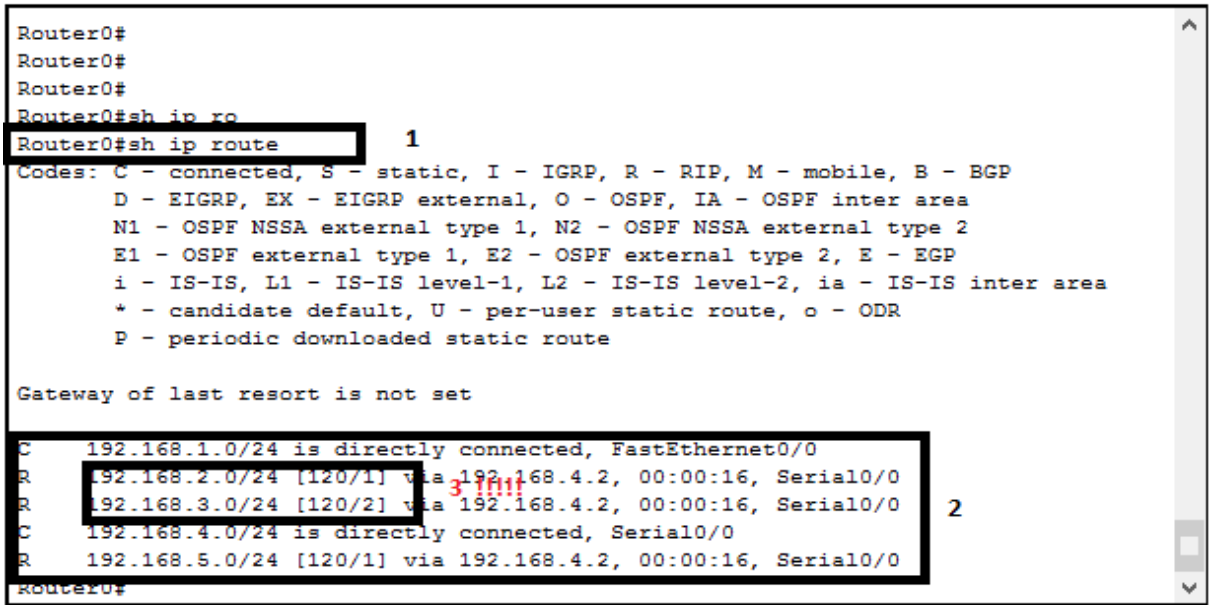
Şekil.19. RIP Konfigürasyonu-Router 1

Router “2” üzerindeki sıfırdan yapılması gereken konfigürasyon adımları aşağıdaki gibidir.



Şekil.20. RIP Konfigürasyonu-Router 2

Yukarıdaki aşamalarda görüldüğü üzere Router’lar üzerinde IP ve RIP konfigürasyonu yapılmıştır. Konfigürasyonların tamamlanmasının ardından Router’ların Yönlendirme tablolarını aşağıdaki gibi görüntüleyip topolojinin genel durumunu görüntülemek mümkün olacaktır.



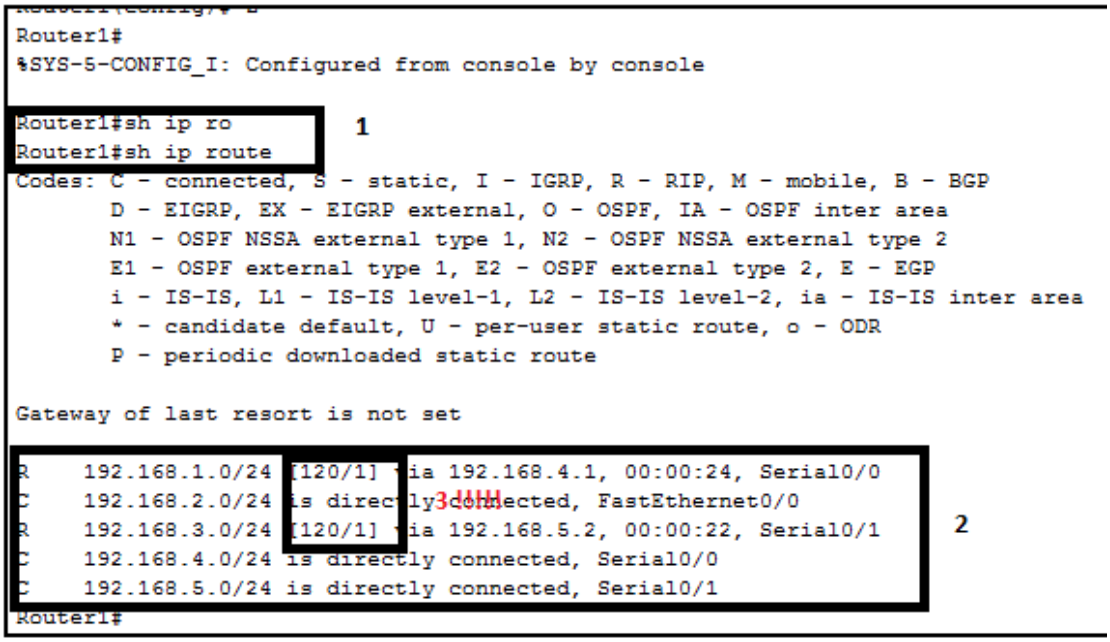
Şekil.21. RIP Konfigürasyonu-Router 0 üzerindeki Routing Tablosu

Yukarıdaki komutlar vasıtası ile "Router0" üzerindeki RIP protokolü ile öğrenilmiş networkler ve Routing tablosu görünmektedir.

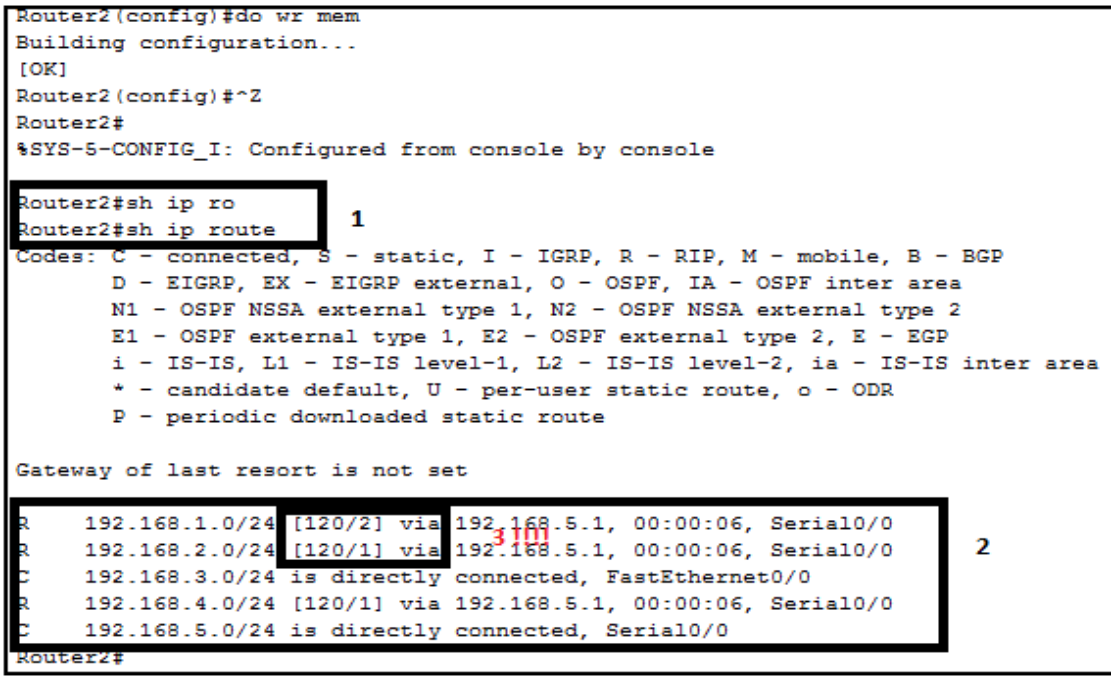
3 Numara ile belirtilmiş başında "R" harfi ile belirtilen networkler RIP ile öğrenilmiş networkler olduğunu ifade eder.

Köşeli parantez içerisindeki 120/1 ve 120/2 bilgileri "120" değeri RIP protokolünü tarif eden Administrative Distance değerini ifade eder varsayılan olarak 120 gelir. V1 ve V2 için değişmez. /1 veya /2 değeri geçilen router sayısını verir. Yani "Router0" üzerinden 192.168.3.0 networküne ulaşılırken toplamda 2 adet router geçildiği anlaşılmaktadır.

Bu bilgiler diğer router için aynı şekilde IP yönlendirme tablosu çıktısına bakılarak yorumlanabilir.

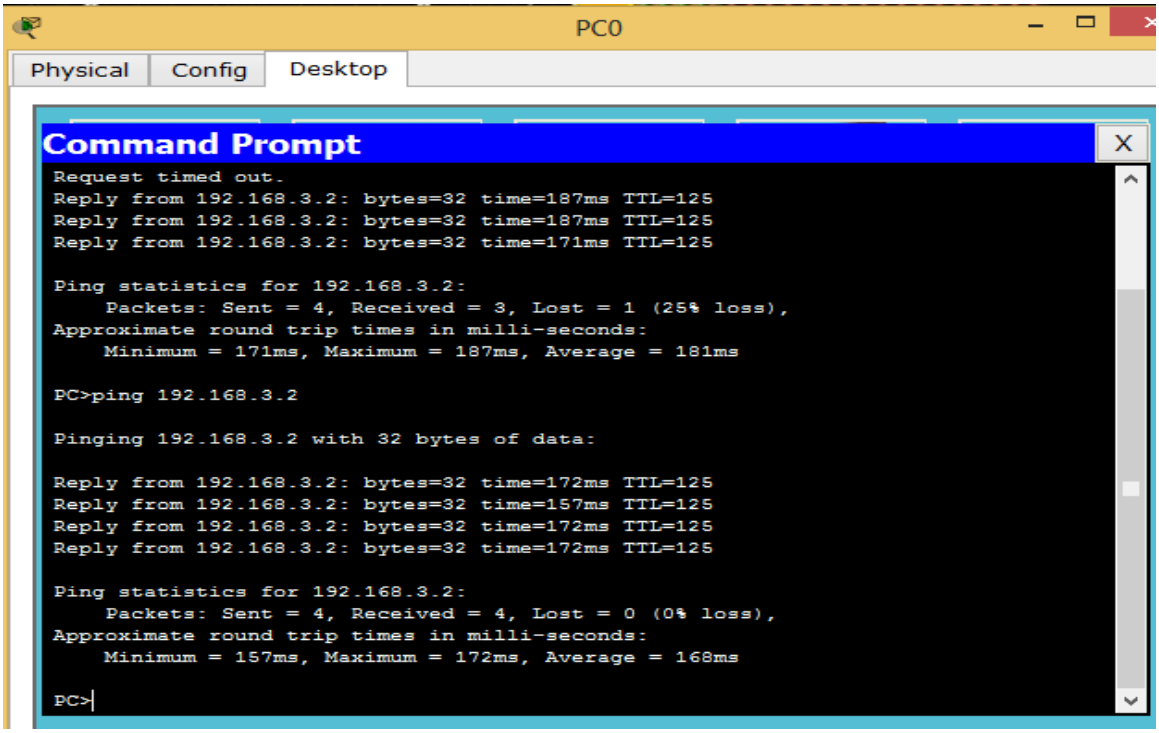


Şekil.22. Router 1 IP Yönlendirme Tablosu



Şekil.23. Router 2 IP Yönlendirme Tablosu

Router “0” ın yorumlarından faydalanarak rakamlandırılmış bilgileri anlamlı hale getirebilmek mümkündür.



Şekil.24. RIP Konfigürasyonu-PC 0

Son olarak Uçtan uca Şekil.11. ’deki topolojiye baktığınızda 192.168.1.0/24 networkünde varolan PC0 (192.168.1.2) IP adresine sahip olan bilgisayardan, 192.168.3.0/24 networkünde yer alan 192.168.3.2 IP adresine sahip PC4’e erişimin sağlandığını ve tüm routerlar arası yönlendirme tablolarının güncellendiğini ve bu tablolardaki IP bilgilerini karşılıklı paylaştıkları için iletişim kurduklarını görüntülemiş olduk.

5. OSPF PROTOKOLÜ MULTI AREA KONFİGÜRASYONU

Open Shortest Path First routing protokolü en çok kullanılan ve yeteneklerinden en fazla yararlanılan protokollerin başında gelmektedir.

OSPF Protokolü Link State çalışır. Yani hattın durumuna göre iletişim kurarlar, küçük hello paketleri yollayarak komşuluk ilişkisinin ayakta kalmasını sağlar.

Link State protokoller, Hattın durumunu kontrol ederler ve hat yoğunluğuna göre cihazlar arası güncelleme paketlerini ve bilgilerini paylaşırlar.

Link State Protokoller, SPF (Shortest Path First) bilgisi sayesinde hedefe gidecek en kısa yolu seçerek, efektif çalışmayı ön görürler.

SPF algoritmasını çıkartan ve iletişim tipine destek veren algoritma "Dijkstra" algoritmasıdır.

OSPF protokolü cihazlar arası bilgi paylaşımını LSA (link state advertisement) paketleri ile sağlarlar.

5.1. OSPF Genel Özellikleri

Open Shortest Path First protokolü kullanan yönlendiriciler, aşağıdaki özellikleri sayesinde karşılıklı olarak iletişim kurarlar.

- 10 Sn'de bir update yaparlar
- Hello paketleri ile komşuluk ilişkisini sürekli ayakta tutarlar
- Dead time süresi (Hello time x 4= 40 Sn'dir)
- Varsayılan olarak tüm networkler Default AREA "0" ile oluşturulur.
- AREA "0" ile farklı AREA konfigürasyonları yapıldığında Multi-AREA OSPF konfigürasyonu gerçekleştirilmiş olur.
- Default Administrative Distance değeri 110'dur.
- Metric değeri olarak "COST" bilgisini referans alır.

- COST= Referance Bandwith / Interface Bandwith ile temel anlamda hesaplanabilir.
- DR ve BDR (Master ve Secondary Router) seçimliliği üzerinden merkezi update yönetimi sağlanabilir.
- 224.0.0.5 ve 224.0.0.6 IP adresleri sayesinde Multicast update yaparlar.
- VLSM desteği vardır.
- Classless(Sınıfsız) veya Classful (Sınıflı) çalışabilirler.
- Authentication desteği vardır.
- Load Balance (Yük Dengeleme) Routerlar arası yük dengeleme desteği vardır.
- Auto ve Manuel Summarization desteği vardır.
- Router'da Priority gibi öncelik belirleme seçimlilikleri vardı.
- OSPF protokolü Frame Relay network'lerde en çok kullanılan protokollerin başında gelirler.
- OSPF protokolü , NBMA , Broadcast ,Point to Point çalışabilirler.

Bu temel bilgilerin aktarımından sonra Frame Relay devresi üzerinde, Multi AREA OSPF konfigürasyonunu aşağıda yer alan topoloji üzerinde sizlere uygulamalı olarak aktarıyor olacağım.

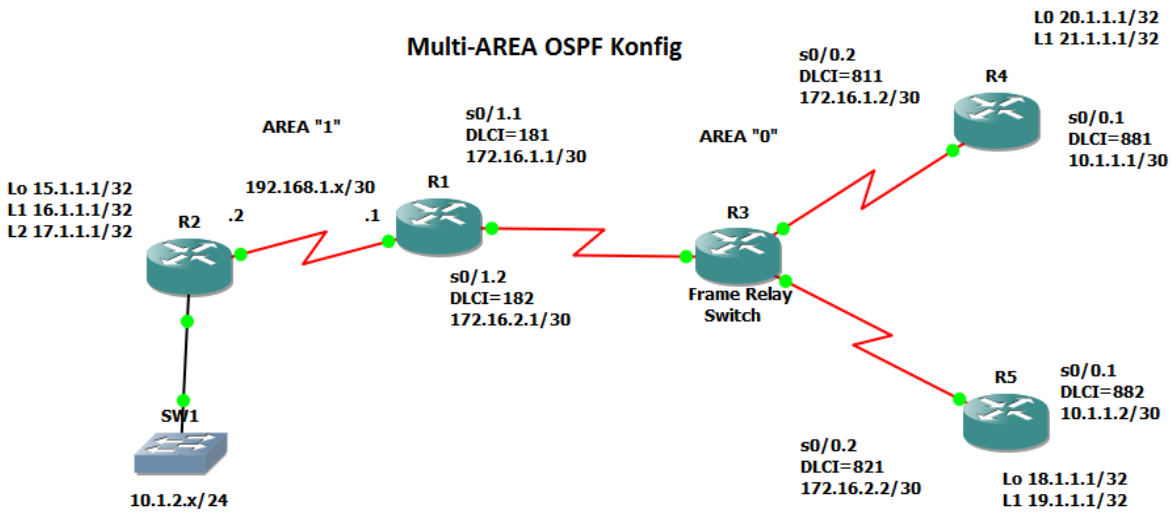
Aşağıdaki konfigürasyonu, GNS3 üzerinde gerçek Cisco IOS işletim sistemi kullanarak 3600 Serisi Routerlar ile 3600 adv.ent. işletim sistemi üzerinde yapılmıştır.

GNS3 yazılımını temin edebileceğiniz site;

http://www.gns3.net/download/ ilgili windows versiyonunu seçerek indirebilirsiniz.

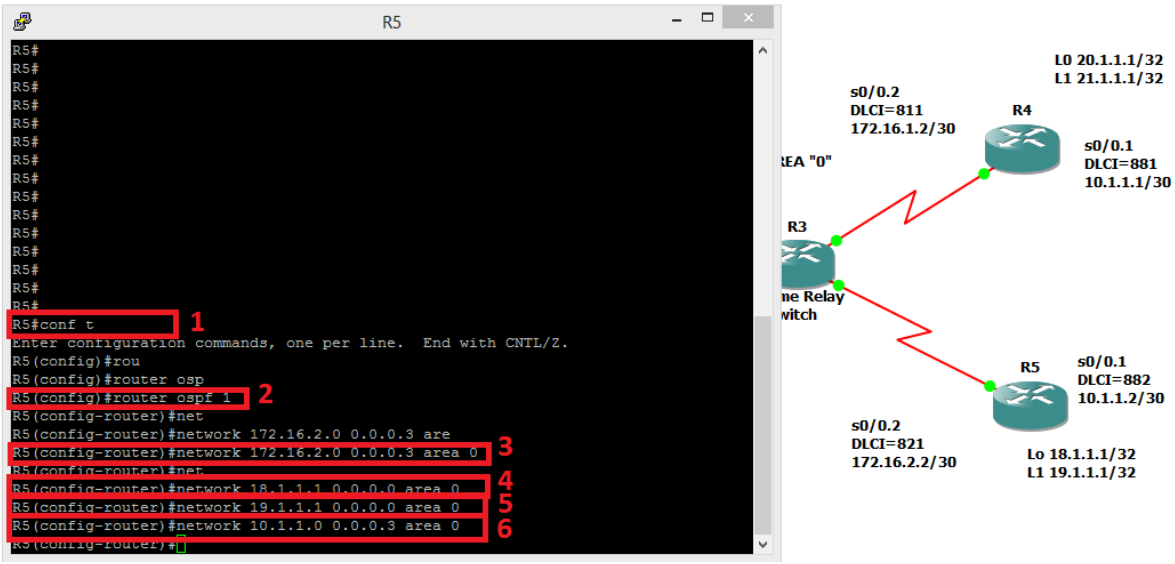
GNS3 yazılımını kurduktan sonra, temel ayarlamaları yapmanız gerekmekte aksi takdirde kurulum tamamlandıktan hemen sonra simulatörden yararlanamazsınız.

IPNetStudy (22.02.2010) GNS3 Temel ayarlarının yapılması' ndan alıntıdır.



Şekil.25. Multi-AREA OSPF Konfigürasyonu

Temel anlamda aşağıdaki resim'de "R4" cihazının OSPF implementasyonunu mevcuttur. Tüm cihazlarda temel konfigürasyon anlamında benzer adımlar uygulanarak konfigürasyon neticelendirilir.



Şekil.26. Multi-AREA OSPF Konfigürasyonu-2

Yukarıdaki temel operasyonların tamamını Şekil 24'te yer alan genel topoloji dizaynımıza göre, IP ve AREA standartlarını yerine getirdikten sonra, Şekil 25 'de yer

alan standart OSPF implementasyon komutlarından destek alarak her Router'ın kendisine direkt olarak bağlı olan networklerini, OSPF Routing modunda iken tek tek networkler yazılarak tüm routerların network anons işlemi tamamlanır.

Burada dikkat edilmesi gereken durum, Router OSPF komutundan sonra verilmiş olan Process ID değerini tüm routerlarda aynı yapılması gerekmektedir.

Area Bilgisini ortak yani her iki "AREA" bağlantısı olan Router'da Hem AREA"0" , hemde AREA"1" bilgisini paylaşmasını sağlayarak topolojinin genel resmine bakıldığında sol tarafı AREA "1" networkü, Sağ tarafı ise AREA "0" networkü (Backbone) veya Omurga AREA kısmıdır.

Bu bilgilerin ardından "R5" cihazında konfig bilgisi paylaşılan tüm cihazların Show- Running çıktılarını aşağıda sırası ile R1, R2, R3, R4 ve R5 olmak üzere aşağıda çıktıları bulunmaktadır.

R1 Router show running çıktısı

```
interface Loopback1
 ip address 22.1.1.1 255.255.255.255
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
```

```
!
interface Serial0/1.1 point-to-point
 ip address 172.16.1.1 255.255.255.252
 frame-relay interface-dlci 181
!
interface Serial0/1.2 point-to-point
 ip address 172.16.2.1 255.255.255.252
 frame-relay interface-dlci 182
!
router ospf 1
 log-adjacency-changes
 network 22.1.1.1 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 1
```

Burada yalnızca ilgili komutlara ait çıktılar paylaşılmıştır.

R2 Router show running çıktısı

```
interface Loopback0
 ip address 15.1.1.1 255.255.255.255
!
interface Loopback1
 ip address 16.1.1.1 255.255.255.255
!
interface Loopback2
```

```
 ip address 17.1.1.1 255.255.255.255
!
interface Serial0/0
 ip address 192.168.1.2 255.255.255.252
 serial restart-delay 0
!
interface FastEthernet1/0
 ip address 10.1.2.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 10.1.2.0 0.0.0.255 area 1
 network 15.1.1.1 0.0.0.0 area 1
 network 16.1.1.1 0.0.0.0 area 1
 network 17.1.1.1 0.0.0.0 area 1
 network 192.168.1.0 0.0.0.255 area 1
```

Burada yalnızca ilgili komutlara ait çıktılar paylaşılmıştır.

R3 Router Show Running çıktısı (Frame Relay Switch)

```
frame-relay switching
!
!
 interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 181 interface Serial0/1 811
```

```
 frame-relay route 182 interface Serial0/2 821
!
interface Serial0/1
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 811 interface Serial0/0 181
 frame-relay route 881 interface Serial0/2 882
!
interface Serial0/2
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 821 interface Serial0/0 182
 frame-relay route 882 interface Serial0/1 881
-----------------------------------------------------------------
```

Burada yalnızca ilgili komutlara ait çıktılar paylaşılmıştır.

Bu cihaz üzerinde sadece Frame Encapsulation teknolojisi aktif hale getirilmiştir. Topoloji üzerinde Layer 2 encapsulation sağlayabilmek için farklı ortamdaki routing protokolleri bir araya getirebilmek için Frame Relay switch kullanabiliriz.

Frame Relay Switch'e direkt bağlı olan router'larda ve ilgili interface'lerde de Frame Relay konfigürasyonu yapıldığını unutmayınız. Mevcut olarak router'ların show-running çıktılarınıda yer verilmektedir.

R4 Router show running çıktısı;

```
interface Loopback0
 ip address 20.1.1.1 255.255.255.255
!
interface Loopback1
 ip address 21.1.1.1 255.255.255.255
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
!
interface Serial0/0.1 point-to-point
 ip address 10.1.1.1 255.255.255.252
 frame-relay interface-dlci 881
!
interface Serial0/0.2 point-to-point
 ip address 172.16.1.2 255.255.255.252
 frame-relay interface-dlci 811
!
router ospf 1
 log-adjacency-changes
```

```
 network 10.1.1.1 0.0.0.0 area 0
 network 20.1.1.1 0.0.0.0 area 0
 network 21.1.1.1 0.0.0.0 area 0
 network 172.16.1.0 0.0.0.255 area 0
```

Burada yalnızca ilgili komutlara ait çıktılar paylaşılmıştır.

R5 Router show running çıktısı

```
interface Loopback0
 ip address 18.1.1.1 255.255.255.255
!
interface Loopback1
 ip address 19.1.1.1 255.255.255.255
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
!
interface Serial0/0.1 point-to-point
 ip address 10.1.1.2 255.255.255.252
frame-relay interface-dlci 882
```

```
!
interface Serial0/0.2 point-to-point
 ip address 172.16.2.2 255.255.255.252
 frame-relay interface-dlci 821
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 18.1.1.1 0.0.0.0 area 0
 network 19.1.1.1 0.0.0.0 area 0
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.255 area 0
```

Burada yalnızca ilgili komutlara ait çıktılar paylaşılmıştır.

Show- Running çıktılarının ardından R4 cihazında IP Route Table görüntülemek için aşağıdaki komut çalıştırılmıştır ve IP Table R4 cihazı için aşağıdaki gibidir.

```
R4#sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

17.0.0.0/32 is subnetted, 1 subnets

O IA 17.1.1.1 [110/129] via 172.16.1.1, 00:38:28, Serial0/0.2 (Farklı AREA ile komşuluk ilişkisi kurduğunu O IA bilgisi sayesinde anlayabiliyoruz.

16.0.0.0/32 is subnetted, 1 subnets

O IA 16.1.1.1 [110/129] via 172.16.1.1, 00:38:28, Serial0/0.2

19.0.0.0/32 is subnetted, 1 subnets

O 19.1.1.1 [110/65] via 10.1.1.2, 00:38:28, Serial0/0.1

18.0.0.0/32 is subnetted, 1 subnets

O 18.1.1.1 [110/65] via 10.1.1.2, 00:38:28, Serial0/0.1

21.0.0.0/32 is subnetted, 1 subnets

C 21.1.1.1 is directly connected, Loopback1

20.0.0.0/32 is subnetted, 1 subnets

C 20.1.1.1 is directly connected, Loopback0

172.16.0.0/30 is subnetted, 2 subnets

C 172.16.1.0 is directly connected, Serial0/0.2

O 172.16.2.0 [110/128] via 172.16.1.1, 00:38:32, Serial0/0.2

[110/128] via 10.1.1.2, 00:38:32, Serial0/0.1

22.0.0.0/32 is subnetted, 1 subnets

O 22.1.1.1 [110/65] via 172.16.1.1, 00:38:32, Serial0/0.2

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

O IA 10.1.2.0/24 [110/129] via 172.16.1.1, 00:38:32, Serial0/0.2

C 10.1.1.0/30 is directly connected, Serial0/0.1

192.168.1.0/30 is subnetted, 1 subnets

O IA 192.168.1.0 [110/128] via 172.16.1.1, 00:38:32, Serial0/0.2

15.0.0.0/32 is subnetted, 1 subnets

O IA 15.1.1.1 [110/129] via 172.16.1.1, 00:38:32, Serial0/0.2

Bu bilgi sayesinde R4 cihazının IP Routing tablosunu görüntülemekteyiz.

Tüm cihazlarda aynı komut sayesinde (Rx# show ip route) ile IP Tabloları görüntülenebilir.

Bu detaylı bilgilerin ardından son olarak cihazlar arasında konfigürasyon bilgisinin tamamlanıp, uçtan uca erişimin olup olmadığını anlamak adına,

R2 cihazı üzerinden en uç noktada bulunan R4 Router'ı üzerindeki 20.1.1.1 Ip adresine erişim denetimini Ping komutu ile aşağıdaki gibi gerçekleştirebiliriz.

R2#ping 20.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.1.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 80/92/100 ms

Aynı şekilde aynı cihaz üzerinden, aynı IP adresine tracertroute komutu ile 20.1.1.1 IP adresine giderken geçilen network'lerin takibini yapmak mümkündür.

R2#traceroute 20.1.1.1

Type escape sequence to abort.

Tracing the route to 20.1.1.1

1 192.168.1.1 56 msec 32 msec 28 msec

2 172.16.1.2 84 msec 72 msec *

Bu komut çıktılarının ardından, genel topoloji konfigürasyonu ve test komutlarının detayları ile birlikte detaylıca incelenmiştir.

Multi AREA OSPF konfigürasyonu senaryoları yapıya eklenecek Router ve Network ID'leri sayesinde genişletilebilir.

Dinamik Routing protokolleri içerisindeki ikinci protokolümüzün konfigürasyonunuda tamamlamış bulunmaktayız.

6. EIGRP PROTOKOLÜ

Enhanced Interrior Gateway Routing Protocol Cisco firmasının geliştirmiş olduğu bir protokoldür. Eski versiyon ismi IGRP'dir.

EIGRP protokolü sadece Cisco cihazlarda kullanılabilecek bir protokoldür. HP, Juniper vb firma cihazlarında kullanılması mümkün değildir.

EIGRP Hybrid Routing protokoller sınıfına girerler. Yani duruma göre Link State, hattın durumuna göre çalışırlar. Duruma göre Distance Vector çalışırlar (Geçilen Router sayısı).

RIP ve IGRP gibi protokollerde topoloji güncellemelerini bir çok Router'a yeniliklerin dışında tüm network bilgisini update ederler. EIGRP protokolü tam tersi şekilde çalışıp sadece yeni gelen topoloji değişikliklerini diğer router'lar ile paylaşırlar.

EIGRP protokolü TCP protokolü yardımı ile çalışır. Bu durumda hedeflenen amaç olumlu-olumsuz durum değişikliklerinin yapılıp yapılmadığından haberdar olmaktır. Bu durum için Hello ve ACK mesajlarını Router'lar birbirlerine yollarlar. Bu mesajları yollama işlemini TCP protokolü ile gerçekleştirirler.

6.1. EIGRP Paket Tipleri

EIGRP çalışan Router'lar 5 farklı mesaj ile komşuluk ilişkisini sürdürürler.

- Hello
- Acknowledgement
- Update
- Query
- Reply

Bu paketlerdeki karşılıklı olarak Router'lar arasında paylaşılmasının ardından, gerekli güncellemeler veya komşuluk ilişkisinin durumunu öğrenmek ve iletişim kurmak mümkün olacaktır.

Hello: Her 5 'snde bir hattın durumuna göre yollanır. Komşuluk ilişkisinin varlığından haberdar olmak için kullanılır.

Acknowledgement: Bu paket içerisinde veri barındırmaz. Olumlu veya Olumsuz şekilde iletişimin sonlanıp –sonlanmadığını kontrol etmek için kullanılır. Unicast çalışırlar.

Update: Topoloji üzerinde olumlu- olumsuz değişiklikler olduğunda, Metric değeri değiştirildiğinde, Successor veya Feasible Succesor değiştirildiğinde oluşan güncellemeleri Router'lar arası bilgi vermek için kullanılır.

Query ve Reply: Query paketi komşu router herhangi bir bilgiye ihtiyaç duyduğunda yollar. Bu pakete cevaben Router'ların yolladıkları paketlere Reply paketleri denilir. Reply paketleri Unicast, Query paketleri Multicast iletişim kurarlar.

6.2. EIGRP Protokolü Özellikleri

EIGRP protokolü kullanan yönlendiriciler aşağıdaki özellikleri kullanarak, yönlendiriciler arası iletişimi ve bilgi paylaşımını gerçekleştirirler.

- Bant genişliği 1.44 Mbps'dan düşük olan yerlerde "Hello" paketleri komşularına 60 Sn'de bir yollanır. Yüksek olan yerlerde 5 Sn'de bir yollanır.
- Hold Time Süresi = 3 x hello interval = 3 x 5 = 15 Sn'dir.(Örnek)
- EIGRP protokolü topoloji değişiklik bilgilerini ve iletişimi Multicast kurarlar.
- Multicast iletişim'de kullandığı IP adresi 224.0.0.10 'dur.
- EIGRP Dual Algorithm denilen bir algoritma kullanır.(Hedef aynı anda aktif iki yol)
- EIGRP protokolünde Master ve Secondary yol kavramı vardır.(Successor, Feasible Successor)
- VLSM desteği vardır.
- Authentication Desteği vardır.

- Summarization destekler.
- Yük Dengeleme (Load Balance) desteği vardır.

6.3. EIGRP Metric Parametreleri

EIGRP protokolü kaynak Router'dan hedef Router'a giderken metric parameter değerlerine göre yol seçimine karar verirler.

Metric Parametreleri;

- Bandwith
- Delay
- Reliability
- Loading
- MTU

EIGRP protokolü varsayılan olarak Metric değerine şu şekilde karar verir.

Metric= Bandwith (slowest link) + Delay (sum of delays)

Bandwith =(10^7 / Kilobit cinsinden minumum bant genişliği) *256

Delay = Aynı yol üzerindeki tüm interface'lerin mikro saniye cinsinden toplamı

Varsayılan olarak Yukarıdaki 5 farklı değer "K" harfi ile simgelenir.

K değeri (K1=1, K2=0, K3=1, K4=0, K5=0)

Metric = K1 * BW + ((K2*BW)/ (256 –Load)) + K3* Delay)

Eğer K5 değeri "0" a eşit değilse;

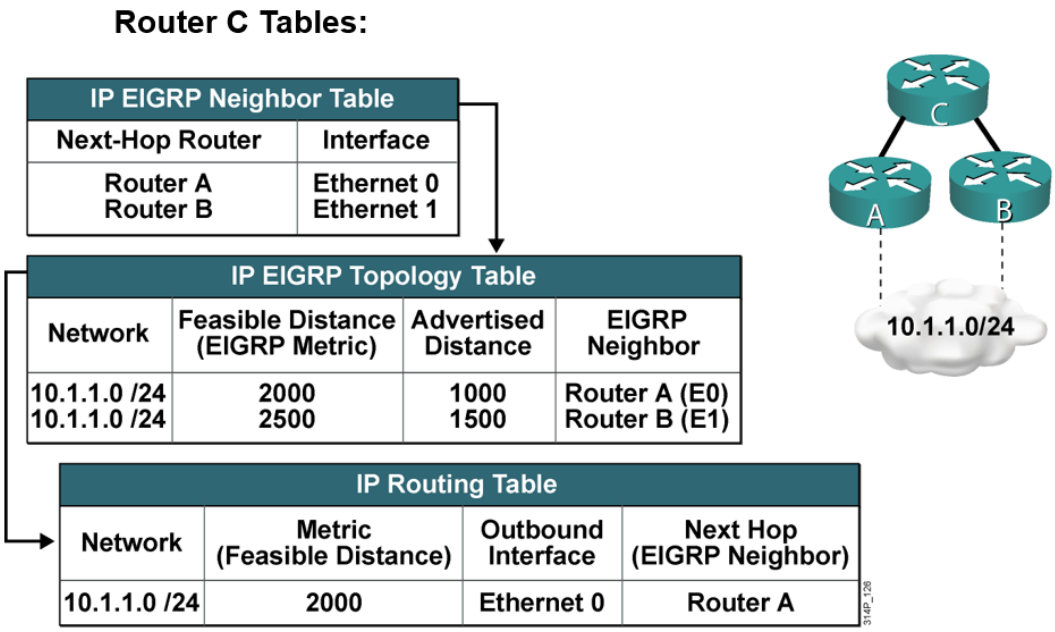
Metric = metric *(K5 /reliability + K4)

Yukarıdaki bilgiler ışığında metric değerlerinin belirlenmesi ve hesaplanması durumunu açığa çıkartmak mümkündür.

EIGRP protokolü 3 Adet tabloya bakarak, network dizaynını tanımlar.

IP Tablosu, Komşuluk Tablosu ve Topoloji Tablosu'dur.

EIGRP Protokolünde, Successor ve Feasible Successor seçimi aşağıda resmedilmiştir.

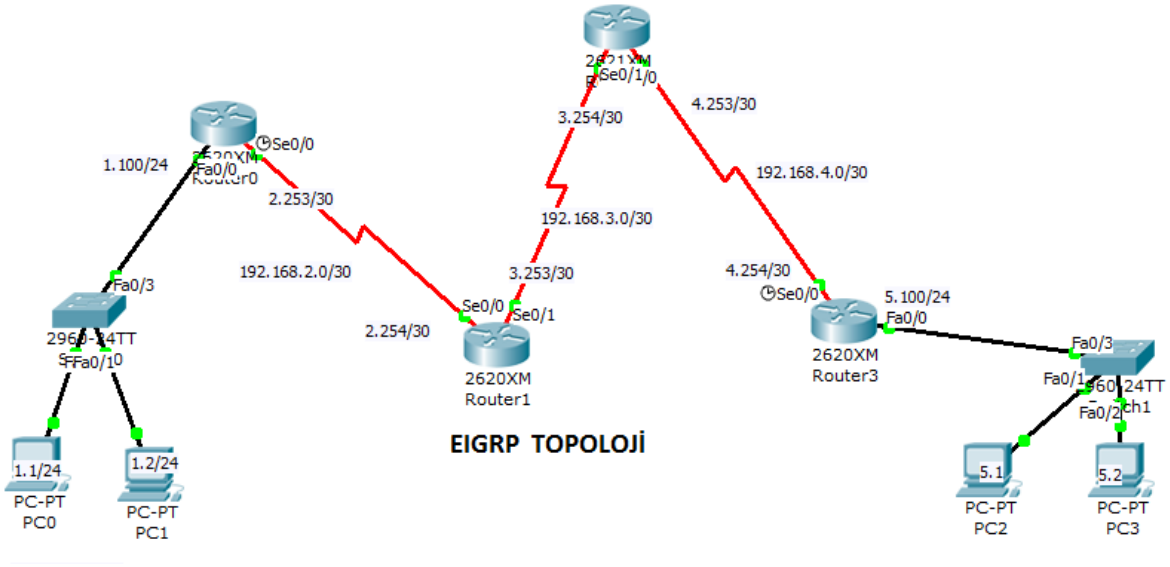


Şekil.27. EIGRP Tablosu

Yukarıdaki bilgiler ışığında Router A ve B 'ye giden yollar içerisinde FS ve Successor yolları belirlenir.

FD ve AD değerleri toplandığında ortaya çıkan bilgiler ışığında, İki değerin toplamında düşük olan değer Successor, ondan sonraki Successor'a en yakın çıkan değer Feasible Successor'dır.

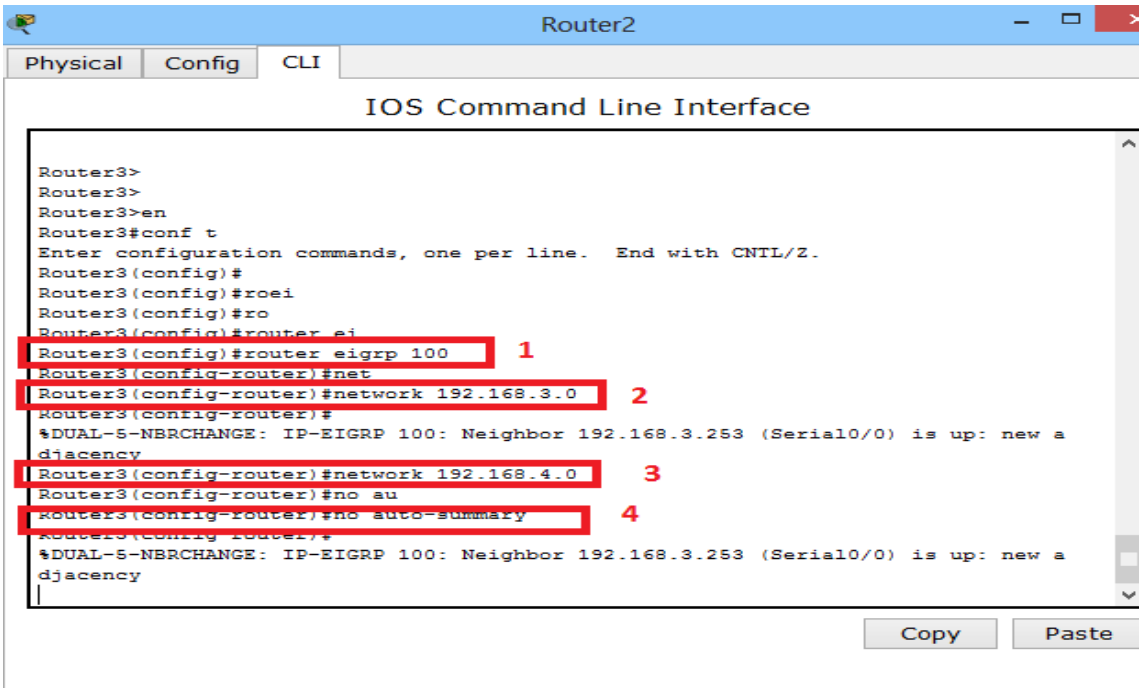
Bu bilgilerin ardından EIGRP protokolü kullanılarak oluşturulmuş olan aşağıdaki topoloji üzerinden uygulamalı olarak EIGRP konfigürasyonunu tamamlamanız mümkündür.



EIGRP TOPOLOJİ

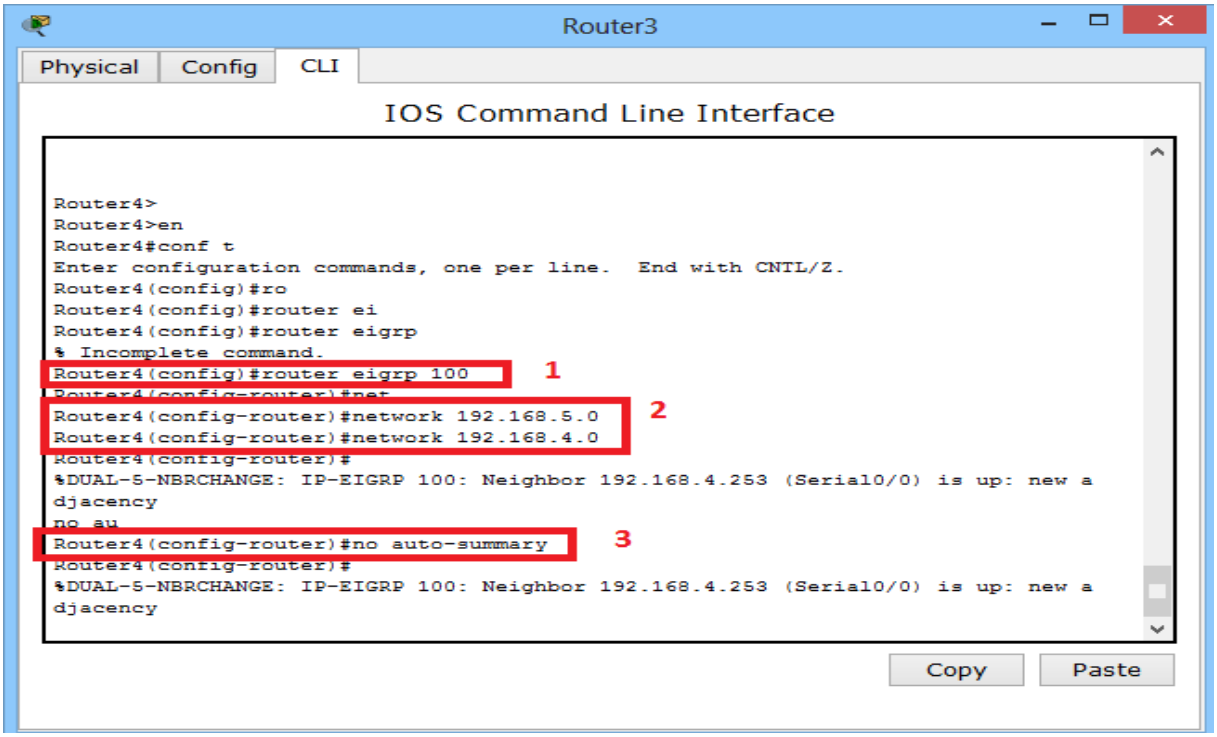
Şekil.28. EIGRP konfigürasyonu

Yukarıda verilmiş IP networkleri interface tabanlı olarak birebir konfigürasyonu yapılarak, ardından EIGRP konfigürasyonu gerçekleştirilmiştir.



Şekil.29. EIGRP konfigürasyonu - Router 2

Router 2 için şekil 27'de örnek EIGRP konfigürasyonu yapılmıştır.

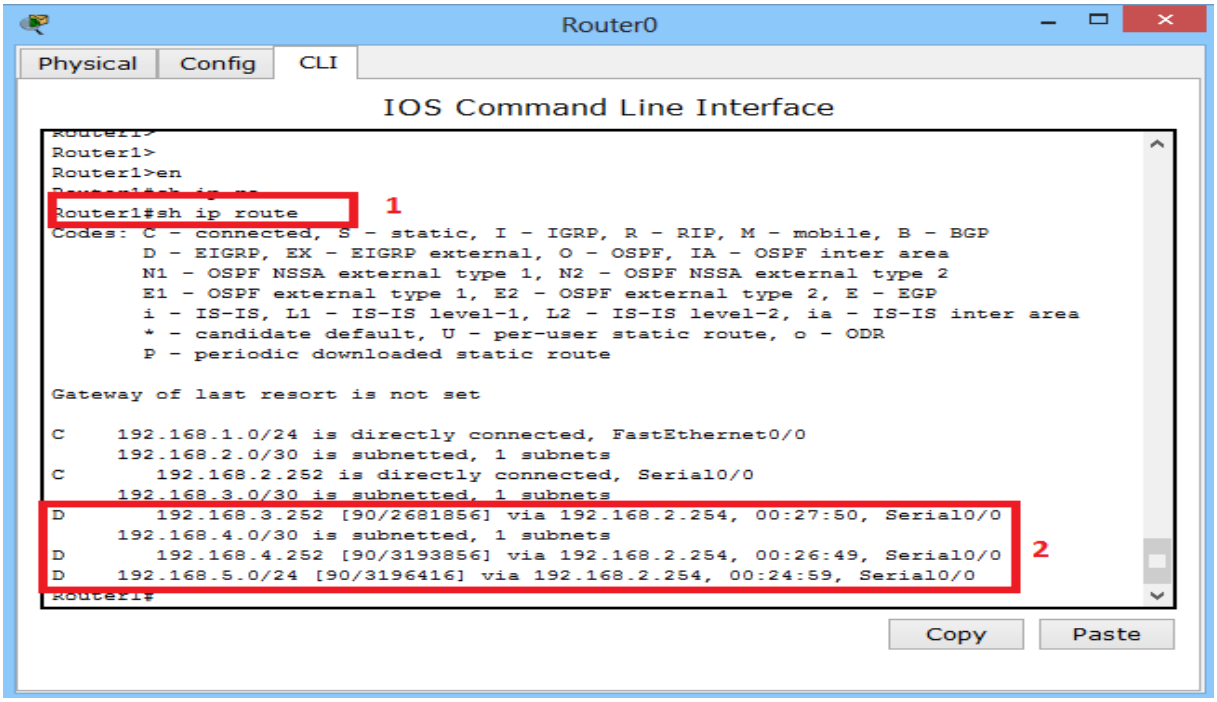


Şekil.30. EIGRP konfigürasyonu- Router 3

Router 3 için şekil 28'de örnek EIGRP konfigürasyonu yapılmıştır.

Yukarıdaki örneklerde yalnızca "2" Router için EIGRP konfigürasyon bilgisini paylaştım. Topoloji üzerindeki IP adreslerini göz önünde bulundurarak, her Router üzerindeki direkt bağlı olan İnterface'ler üzerindeki IP network adresleri girilerek konfigürasyonu tamamlayabilirsiniz.

EIGRP Routing Tablosunu, aşağıdaki ekrandan faydalanarak öğrenebilirsiniz.



Şekil.31. EIGRP Rouiting Tablosu

Aşağıdaki konfigürasyon çıktısında Router2 için detaylı üzerinde tutmuş olduğu konfigürasyonun görüntülenmesi mümkündür.

Router2#show running-config

Building configuration...

Current configuration : 536 bytes

!

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

```
no service password-encryption
!
hostname Router2
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0
 ip address 192.168.2.254 255.255.255.252
!
interface Serial0/1
 ip address 192.168.3.253 255.255.255.252
!
router eigrp 100
 network 192.168.3.0
 network 192.168.2.0
 no auto-summary
!
ip classless
!
!
```

line con 0

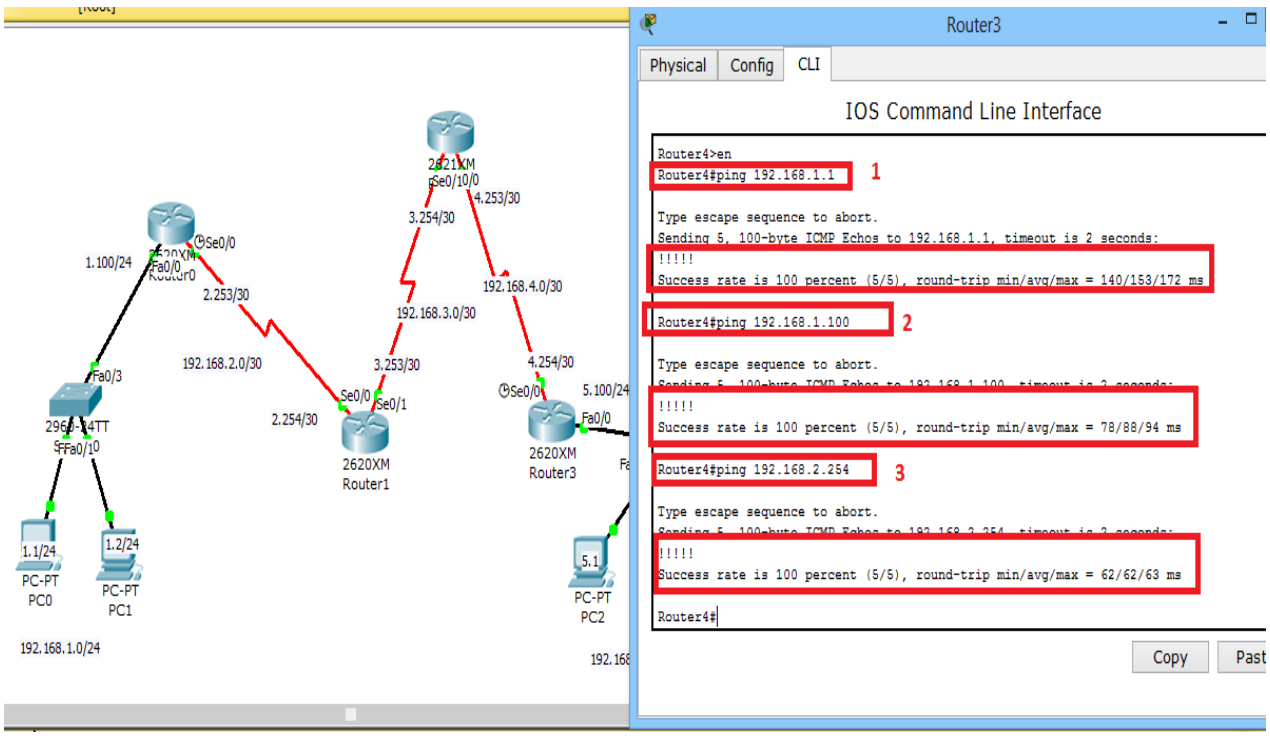
line vty 0 4

login

!

end

Son olarak aşağıdaki ekranda uçtan uca cihazlar arası iletişimde sorun olup olmadığını ve Routing tablosunun tüm topoloji için tutulduğundan emin olmak için "PING" komutu ile ulaşılabilirlik testini tamamlayabilirsiniz.



Şekil.32. EIGRP Rouiting (Ping Komutu)

Son olarak yukarıdaki örnekte görüldüğü üzere doğruluk ve çalışırlık testlerimizide tamamlayarak işlemlerimizi sonlandırdık.

7. BGP PROTOKOLÜ DETAYLARI

7.1. BGP Nedir ?

Border Gateway Protocol günümüzde İnternet bağlantılarının kurulmasında ve genişletilmesinde kullanılan en temel protokollerin başında gelmektedir.

Kullanım alanı bir hayli yaygındır, fakat küçük ve orta boy tipteki işletmelerin network dizaynı yaptığında kullanmak isteyeceği bir protokol değildir.

Sebebi çok kapsamlı olmasından ve genel olarak internet servis sağlayıcılarının, internet servislerini kullanıcılara sunmak ve işletmeleri internet servisi ile buluşturmak, servis sağlayıcıların bir başka servis sağlayıcı ile iletişim kurmasına imkan tanıyan kapsamı büyük ölçekte olan, operasyonel olarak ciddi deneyim gerektiren, internet servis sağlayıcılarında Veri Merkezi Yönlendirici seviyesindeki Cihazların üzerinde kullanılan protokoldür.

BGP, "exterior gateway protocol" harici ağ geçidi protokolü olarak sınıflandırılmaktadır. "Autonomous System" (AS) Otonom sistemler arasında IP rotaları taşımak için kullanılmaktadır. BGP hedef seçiminde, elle müdahele edilerek gidilmesi istenilen yollara, rota manipülasyonu yaparak, gidilmesi tercih edilen tüm networklere ait rotalar yazılarak istenildiği gibi tüm yönledirme işlemlerine detaylı olarak müdahele ettirmeye olanak tanır.

Bu operasyonların gerçekleştirilmesi için deneyimlerin servis sağlayıcı düzeyinde olması şarttır.

BGP protokolü RFC 1771 standartlarına göre çalışması IETF tarafından açıklanmıştır.

7.2. Autonomous System Nedir?

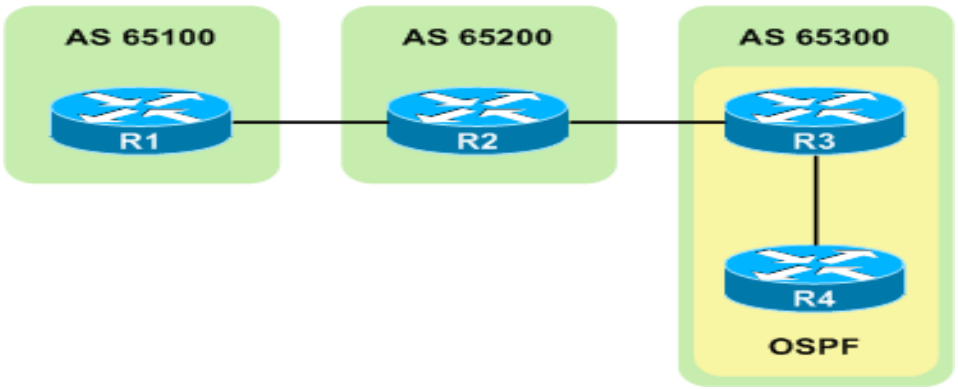
Otonom Sistem; Otonom sistem kavramını aslında IP network havuzları oluşturur. Otonom sistemlerde amaç IP networklerinin coğrafi konumlarına göre gruplara bölünmesi ve IP network'lerinin yönetimini kolaylaştırılması ve sınırların çizilmesi maksadı ile kullanılır.

Otonom Sistemler 16 bit ile ifade edilebilirler. Diğer bir ifade ile 0 ile 65535 arasında değerler alabilirler. Otonom Sistem kavramı "AS" olarak ingilizce kısaltma olarak ifade edilirler. "AS" numaraları ripe, arin gibi kuruluşlardan satın alınabilirler. 64512-64534 arasında bulunan "AS" numaraları "private range" olarak rezerve edilmiştir ve "Private" IP blokları yalnızca iç networklerde belli amaçlar için kullanılabilirler. Aşağıdaki resimde de "AS" numaralandırması topoloji üzerinde örneklendirilmiştir.

BGP protokolü sınıfsız bir yönlendirme protokolüdür. "CIDR" ve "VLSM" desteği vardır. "CIDR ve VLSM" kavramlarını IP protokol başlığında detaylarını görebilirsiniz.

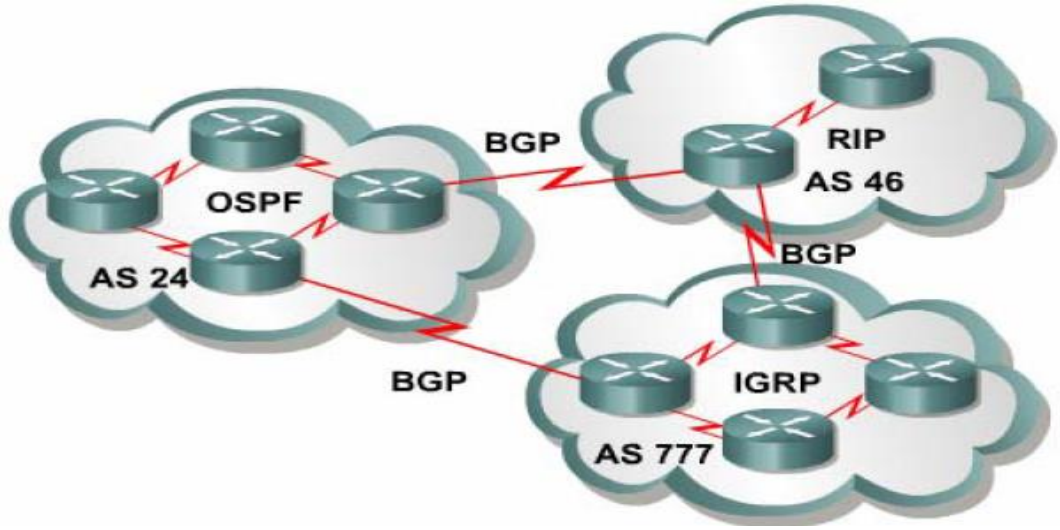
"CIDR" kullanılmadan network anonsları BGP ile yapıldığında yaklaşık olarak 2.000.000 civarı IP yönlendirilmesi yapılabilir. "CIDR" kullanıldığında bu rakam 170.000 civarına düşmektedir.

Ipv4 ve Ipv6 ile BGP protokolünü kullanmak mümkündür.



Şekil.33. AS" Numaralandırması Örneklendirilmesi

Aşağıdaki resimde de “BGP” protokolünün büyük ölçeklerde kullanımını resmeden bir topoloji yer almaktadır.



Şekil.34. BGP Topolojisi

7.3. Büyük Ölçekli Networklerde BGP Kullanımı

BGP protokolü her firmanın kullanacağı ölçekte bir protokol değildir. BGP ölçeğini anlamak ve kullanmak için işletmenin çok şubeli ve merkezden oluşan bir organizasyon yapısına sahip olmalı veya hizmet sağlayıcı bir firma olmalıdır. Aksi halde yönetim zorluğu ve uygulamasının büyük ölçekte deneyim gerektiren durumlar olduğundan problem yaşanması ve çözümü zor olacaktır.

Aşağıdaki networkümüzde “multihomed” bgp kullanımı söz konusudur. “AS” lere olan bağlantılardan herhangi biri koptuğu vakit bir diğer bağlantı üzerinden “AS” ler iletişim kurmaya devam ederler.

Ayrıca hedef network'lere hangi yolu kullanarak gideceğimize dair bize rota tanımlaması imkanı sağlayarak hangi network'e hangi yol izlenerek gidileceğine karar vermemize yardımcı olur ve performans artırmaya olumlu katkısı olacaktır.

Peki bu durumda hangi durumlarda "BGP" protokolünü kullanmalıyız veya ihtiyaç olduğunu nasıl anlayabiliriz sorusunu soralım?

BGP Kullanmayı Gerektiren Durumlar;

- AS'den bir başka AS'e paket iletmeniz gerektiren durumlarda kullanılırlar.
- Kullanıdığımız AS'in birden fazla AS'e bağlantısı var ise kullanılırlar.
- AS üzerindeki trafik farklı rotalara yönlendirilmesi, yani rota manipülasyonu gerektiren durumlarda kullanılırlar.

BGP Kullanmayı Gerektirmeyen Durumlar;

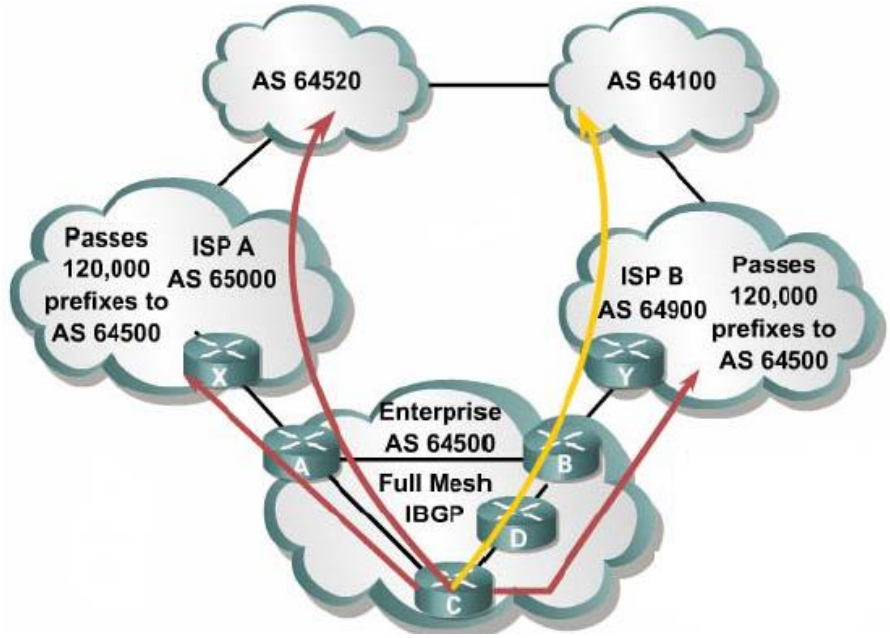
- İnternet bağlantısına yalnıza tek bir network veri hattı ile bağlı iseniz kullanmaya gerek yoktur.
- Rota yazmak, Rota filtreleme yapmak gibi konularda deneyiminiz veya detaylı bilginiz yok ise kullanılmamalıdır.
- BGP protokolünü aktif edeceğiniz "Router" larınızda BGP detaylarını kullanabileceğiniz kadar RAM ve İşlemciye sahip değillerse kullanılmamalıdır.

7.3.1. BGP Varsayılan Rotalar Üzerinden Güncelleme Metodları

BGP protokolü varsayılan olarak rota seçiminde aşağıdaki metodları kullanırlar.

- Her internet servis sağlayıcı yalnızca varsayılan olarak kullanılan rotaların bilgisini kabul ederler.
- Tüm AS'ler yönlendirme tablolarının tamamını internet servis sağlayıcılarına yönlendirirler.

- İç networklerde çalışan tüm yönlendiriciler, yönlendirme tablolarına bakarak en iyi yolu seçerler.
- Statik veya Dinamik yönlendirmeler sayesinde direkt veya dolaylı yoldan internet servis sağlayıcılarına bağlantı sağlanabilir.
- Yönlendirme güncellemeleri 3 şekilde anons edilirler varsayılan güncelleme, bölümsel ve ful güncelleme.
-



Şekil.35. BGP Protokolü Rota Seçimi

Tüm Servis Sağlayıcıların Tam Yönlendirilmesi

- Tüm servis sağlayıcılar tüm yönlendirmeleri "AS" lere yönlendirir.
- Tüm iç network yönlendiricileri "IBGP" çalışırlar.
- Bu işlemleri yaparken kaynak kullanım gereksinimleri gayet düşüktür.

7.4. BGP Protokolü Özellikleri

BGP protokolü “Path-Vector” çalışırlar. “Distance Vector” özelliklerinden daha evvel ki RIP protokolü başlığında değinmiştik.

İnternet üzerindeki tüm yönlendiricilerin BGP konfigürasyonu yapıldığını düşündüğümüzde ve her saniye, yönlendiriciler üzerindeki rotaların up/down olduğu göz önünde bulundurulduğunda “distance vector” protokolü bir dezavantaj gibi görünebilirler.

Fakat “Link-State” çalışmış olsalardı her saniye rotalar güncellendiğinde her yönlendirici üzerlerindeki protokol vasıtası ile güncellemeleri protokolün kullandığı algoritmalardan dolayı, bu algoritmaları yüklerken bir hayli performans harcayacağından, yönlendircilerin yönlendirme kapasitesinde ciddi düşüşler olduğu gözlemlenecektir.

Bu olumsuz durum göz önünde bulundurulduğunda gecikmeleri minumum seviyeye indirmek adına BGP protokolü “distance-vector” çalışırlar.

BGP protokolü güncellemeleri RIP protokolüne nazaran çok daha yavaş yollarlar. RIP protokolü gibi Hop Count sayısına bakarak güncelleme yaptıkları bi çok kaynakta yazılıdır fakat bu protokol AS’lere bakarak güncellemelerini yollarlar.

BGP protokolü güncellemelerini yollarken, IP prefixleri ve autonomous system bilgisini paylaşırlar.

BGP protokolünün diğer protokollerin çalışması göz önünde bulundurulduğunda en büyük farklarından biri OSI referans modelinde 4.katmanda çalışmalarıdır.

BGP TCP 179 nolu portdan güncellemelerini paylaşır. ACK işlemi BGP protokolünde mevcur değildir. Varsayılan olarak TCP kullandığı için TCP protokolüde ACK işlemini varsayılanda yaptığı için harici olarak bu operasyona ihtiyaç duymazlar.

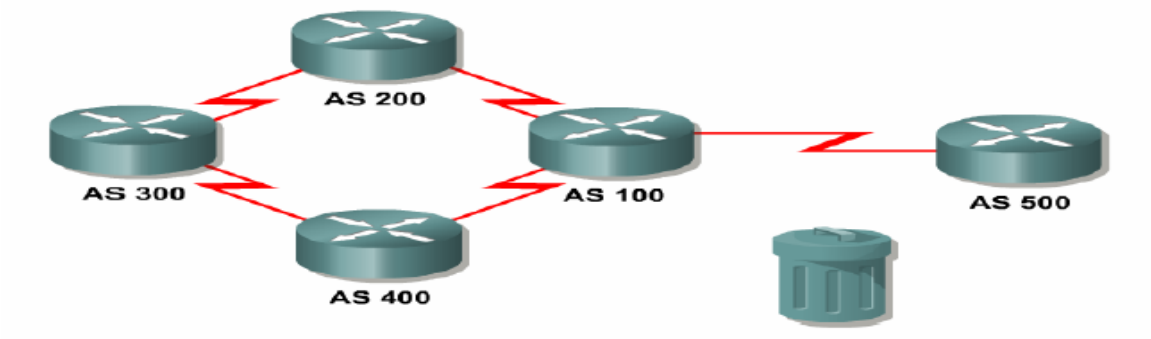
BGP protokolü RIP protokolüne benzer davranışlar sergilerler fakat RIP gibi güncellemelerini her defasında topluca yollamazlar sadece değişen bilgileri paylaşırlar.

Şekil.36. BGP Protokolü 1

BGP komşularına "keepalive" mesajları gönderirler, "keepalive" mesajları diğer protokollerdeki "hello" mesajlarına benzerler.

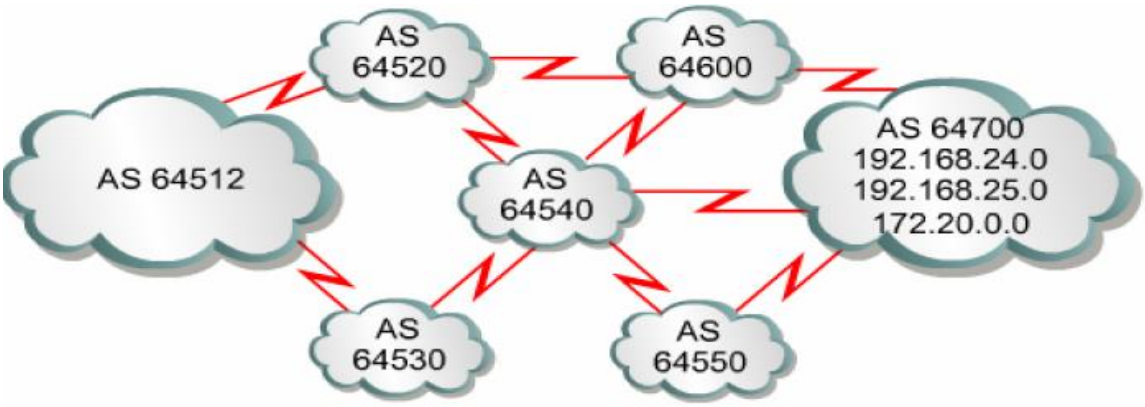
BGP protokolü varsayılan olarak 60 saniye de bir "keepalive" mesajı yollarlar.

BGP protokolü RIP ile benzer davranışları sergilemesinden kaynaklanan "Split Horizon with Poison Reverse" özelliği sayesinde, Kısır döngüye girmiş olan paketleri çöpe atarak güncellemelerin olumsuz yönde etkilenmemesi adına aksiyon alırlar.



Şekil.37. BGP Protokolü 2

BGP protokolü ilke tanımlamalarından AS by AS veya Hop by Hop ilke tanımlamalarına destek sunarlar.



Şekil.38. BGP Protokolü 3

7.5. BGP Protokolü Veritabanları

BGP tabloları aşağıdaki gibidir;

1. Komşuluk tablosu(Neighbor Table): BGP konfigürasyonu yapılmış yönlendiricilerin bilgisini gösteren tablodur. BGP komşuluğu kurulması için elle ile konfigürasyonun yapılmış olması gereklidir. Varsayılan olarak 179 nolu porttan iletişim kurarlar ve periyoduk olarak bu porttan güncellemelerini yollarlar.
2. BGP veritabanı yönlendirilmesi(Forwarding Database): Komşuluk kurulduktan sonra BGP rota yönlendirmelerini gönderip – alırlar, diğer cihazlardan alınan bilgiler yönlendirme tablosuna konumlandırıldıktan sonra diğer rotalar için birden fazla yol bilgisi tutarlar.
3. IP Yönlendirme Tabloları(IP Routing Table): BGP yönlendirme tabloları en iyi rotaları IP yönlendirme tablolarına koyarlar. “Autonomous System” içerisinde BGP ile öğrenilen rotalar aynı zamanda diğer yönlendirme protokolleri ilede öğrenilebilir.

Bu durumda yönetimsel değerlerine bakılır. IGP protokoller içerisinde en yüksek yönetimsel değere BGP sahip olduğu için BGP protokolü ile yönlendirme yapılamaz. IBGP'de yönetimsel değer "200" EBGP'de ise "20" dir.

7.6. BGP Protokolü Mesaj Tipleri

BGP protokolünde 4 tip mesaj vardır.

1. Açık Mesaj (Open Message): Komşular arası anlaşmanın gerçekleşmesi için gönderilen mesajdır. Mesaj paketinin içerisinde;
   - BGP versiyon numarası
   - AS numarası
   - Zaman tutma süresi
   - Router kimlik bilgisi, ospf protokolünde olduğu cihaz üzerindeki IP adresleri ile tanımlanır.
2. Mesaj tutma süresi (Keep Alive): Merhaba mesajlarını algılarlar. Her 60 saniyede bir güncelleme mesajları yollarlar. 3 kere 60 sn mesaj içeriği tamamlanırsa ardından bir daha "keepalive" mesajı yeniden güncelleme olmadığı sürece yollamazlar.

3. Uyarı Mesajları (Notification Message): Bu mesaj tipi güncellemelerde herhangi bir uyarı veya hata bilgisini paylaşmak için kullanılır.

1 Message Header Error	1 Connection Not Synchronized 2 Bad Message Length 3 Bad Message Type
2 OPEN Message Error	1 Unsupported Version Number 2 Bad Peer AS 3 Bad BGP Identifier 4 Unsupported Optional Parameter 5 Authentication Failure 6 Unacceptable Hold Time
3 UPDATE Message Error	1 Malformed Attribute List 2 Unrecognized Well-Known Attribute 3 Missing Well-Known Attribute 4 Attribute Flags Error 5 Attribute Length Error 6 Invalid Origin Attribute 7 AS Routing Loop 8 Invalid NEXT_HOP Attribute 9 Optional Attribute Error 10 Invalid Network Field 11 Malformed AS_path

Şekil.39. Uyarı Mesajları

4. Güncelleme Mesajı (Update Message): Güncelleme mesajını 3 başlık altında yollayabilirler. NLRI (network layer reachability information) Network bilgisinin erişelebilirliğini kontrol eder. Yol erişim bilgisini tutar. Yönlendirmeleri yeniden yapılandırır.

Şekil.40. Güncelleme Mesajı

7.7. BGP Bağlantı Durumları

BGP protokolü 4 paket ile bağlantıyı gerçekleştirir ve topoloji üzerindeki değişiklikleri paylaşırlar. Bu bilgilere istinaden 6 adet bağlantı durumunu anlatan aşamalar mevcuttur.

Idle State(Boşta durumu): BGP çalışmaya ilk başlangıç adımıdır. Komşu ile TCP bağlantı kurulması için beklemeye geçilir. BGP durumlarından herhangi birinde sorun olması durumunda tcp oturumu kapatılır ve "ıdle" durumuna geçerler.

Bu aşamanın geçilememesinin sebebi TCP 179 nolu portun açık olmamasıdır.

AS veya IP adresi yanlış konfigüre edilmiş olabilir.

Connect State(Bağlantı durumu): Komşu yönlendirici ile TCP bağlantısının tam anlamıyla kurulması beklenir.

SYN, SYN-ACK, ACK işlemi ile TCP oturumu kurulması kısa sürer ve oturum gerçekleştirilir.

Open paketi bu aşamada yollanır, bu aşamada herhangi bir sorun yaşanırsa, BGP aktif oturuma geçer.

Active State(Aktif durum): TCP oturumu gerçekleştirilmediğinde bu duruma geçerler. Yönlendirici komşu cihaz ile yeniden bağlantı kurulması denenir başarılı olunursa, "Open" mesajı yollanır.

Tekrar başarısız olunduğunda "ıdle state" e düşerler.

Cihazlar arası bant genişliği yeterli değilse veya hatta tıkanıklık varsa BGP aktif ve boşta kalma durumları arasında sürekli gider gelir. Acilen düzeltilmesi gereken bir durumdur.

OpenSent State (Açık yollama durumu): Yönlendiricinin komşusundan "Open" mesajı aldığı durumdur. Alınan paketin doğruluğuna bakar, paketin içerisindeki MD5 parola, AS numarası değerleri uyuşmazlık gösteriyorsa, "Notification" mesajı yollanır. Eğer hata yoksa "Keepalive" mesajı yollanır.

Open Confirm State (Açık Onaylama Durumu): Komşu yönlendiriciden KEEPALIVE mesajının beklendiği durumdur, bu mesaj alındığında "Established" durumuna geçilir. "Keepalive" gelmezse yönlendirici "Idle State" e düşer.

Established State (Bağlantı Sağlanma Durumu): BGP komşularının güncelleme mesajlarını göndereceği durumdur. Komşuluk ilişkileri yerine oturmuştur. Güncelleme mesajlarında sorun çıkarsa tekrar "Notification" mesajı yollanır ve "Idle" durumuna dönülür.

Cisco cihazlarda Established State'de iken established görülmez komşulardan öğrenilen "prefix" bilgileri gösterilir.

7.8. BGP Komşuluk İlişkisi

BGP protokolünün detaylarının ardından, komşuluk ilişkisinin incelenmesi konusunda bilgi verelim. İki cihaz TCP bağlantısı kullanarak BGP konuşması sağlanır ve komşuluk kurulur. BGP komşularına "peer" adı verilir. Komşulukların sınıflandırılması IBGP ve EBGP olarak incelenir.

BGP komşulukları manuel olarak kurulur. Diğer yönlendirme protokollerinde komşuluk ilişkisi dinamik olarak kuruluyor idi.

IBGP (Internal BGP):

IBGP aynı “AS” içerisindeki yönlendiricilerin komşuluk ilişkisi kurduğu durumdur.

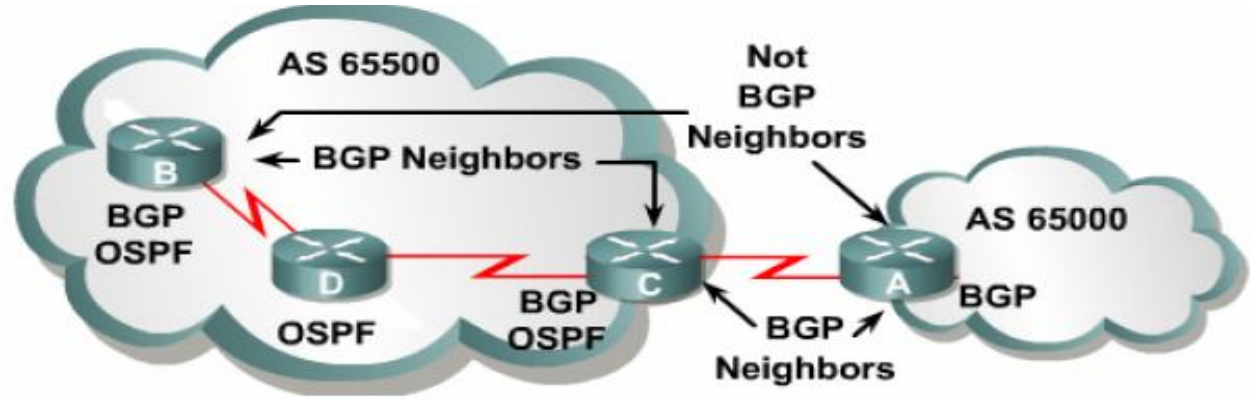
EBGP(External BGP):

Farklı AS’ler arasında yapılan bağlantılar sayesinde EBGP oluşturulur.

BGP konuşan cihazlar, dış otonom sistemlerdeki, tüm cihazlar ile komşuluk kuramazlar. İnternet üzerinde 21.000 den fazla AS bulunduğu ve binlerce BGP çalışan yönlendiriciler olduğu göz önünde bulundurulursa bu durumun imkansıza yakın olduğu anlaşılabilir.

EBGP komşuluğu için direkt bağlı olmaları gerekmektedir.

EBGP komşuluğu aşağıdaki gibi resmedilmiştir.



Şekil.41. EBGP Komşuluğu

7.9. BGP Konfigürasyonu

Basit BGP Konfigürasyonu;

Router (config)# router bgp *autonomous-system* komutu ile bgp"AS" bilgisi yönlendiriciye atanır.

Router (config-router)# neighbor ip-address | peer-group-name remote-as autonomous-system komut seti ile komşu network'e ait "AS" bilgisi tamamlanarak next-AS bilgisi tanımlanır.

Örnek olarak yukarıdaki iki komut özetlendiğinde;

Router (config)# router bgp 65100

Router (config-router)# neighbor 10.1.1.2 remote-as 65101

Router (config-router)# neighbor 10.1.1.2 65001 shutdown komutu ile yönetimsel olarak bakım yapılması gereken veya istenen routerlarda "shutdown" komutu kullanılır.

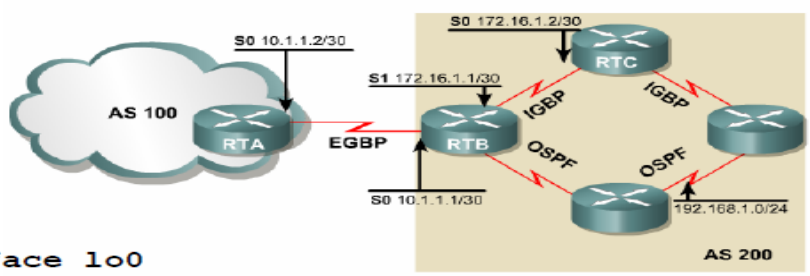
Router (config-router)#no neighbor 10.1.1.2 65001 shutdown komutu ile ilgili "AS" için komşuluk bilgisi komple kaldırılır.

Router(config-router)# neighbor 10.1.1.2 update-source *interface-type interface-number* komutu ile update'lerin yapılacağı loopback interface router üzerinde tanımlanır.

Bu komut kullanım amacı IBGP içerisinde BGP konuşan router'ların updatelerini Loopback interface'ler üzerinden yaparak fiziksel interface'leri update bilgisi için meşgul etmemesi için yapılır.

Bu durumun amacı IBGP networklerinde update bilgisini zenginleştirmek, bu komut yalnızca direkt birbirlerine bağlı olan router'larda ve IBGP networklerde çalışırlar, EBGP networklerde çalışmazlar.

Aşağıdaki topolojide Loopback source tanımlamasını detaylı uygulamaya yarayacak bilgi paylaşılmıştır.




```
RTB
RTB(config)# interface lo0
RTB(config-if))# ip address 1.1.1.1 255.255.255.0
RTB(config)# router bgp 200
RTB(config-router)# neighbor 10.1.1.2 remote-as 100
RTB(config-router)# neighbor 2.2.2.2 remote-as 200
RTB(config-router)# neighbor 2.2.2.2 update-source lo0
RTC
RTB(config)# interface lo0
RTB(config-if))# ip address 2.2.2.2 255.255.255.0
RTB(config)# router bgp 200
RTB(config-router)# neighbor 1.1.1.1 remote-as 200
RTB(config-router)# neighbor 1.1.1.1 update-source lo0
```

Şekil.42. Loopback Source

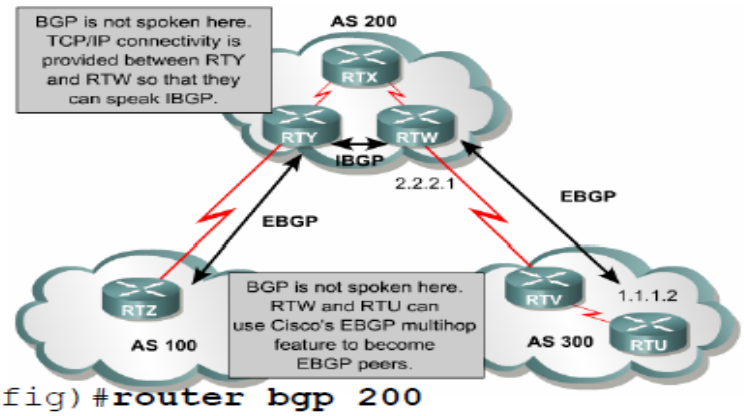
7.10. EBGP Çalışan Router'larda Komşuluk İlişikisi

EBGP güncellemeleri yapılırken normal şartlarda, Router'ların (Yönlendiriciler) direkt olarak birbirlerine bağlı olması gerekmektedir. Fakat bu durumun tersi durumlarda söz konusu olabilir. Yani direkt olarak bağlı olma gerekliliğinin ortadan kaldırıldığı durumlarda olabilir.

IBGP çalışan router'larda bu durum zaten sağlandığı için ve aynı "AS" içinde olduğu için bu durum IBGP çalışan routerlar için otomatik olarak sağlanmış bulunmaktadır.

Eğer EBGP çalışan routerlar direkt olarak birbirlerine bağlı şekilde çalışmıyorlarsa, Cisco cihazların işletim sistemi olan IOS (Internetwork Operating System) lerde aşağıdaki komut syntax'ı sayesinde güncellemelerin yollanması sağlanabilir.

Router(config-router)# neighbor *ip-address* ebgp-multihop (hops)




```
RTW(config)#router bgp 200
RTW(config-router)#neighbor 1.1.1.2 remote-as 300
RTW(config-router)#neighbor 1.1.1.2 ebgp-multihop 2
RTU(config)#router bgp 300
RTU(config-router)#neighbor 2.2.2.1 remote-as 200
RTU(config-router)#neighbor 2.2.2.1 ebgp-multihop 2
```

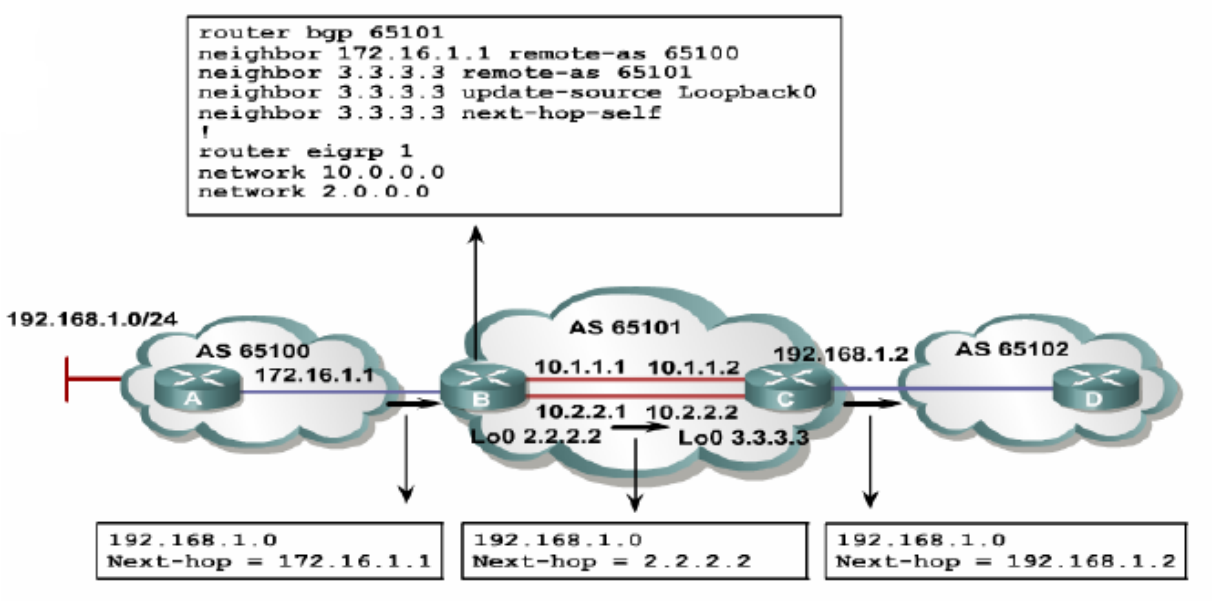
Şekil.43. EBGP Komşuluk İlişkisi

7.11. BGP Komşu Router Seçiminde Kullanılan Parametreler

BGP protokolü komşu router seçiminde veya komşu router üzerinden hedef network'e gitmek isterken kullandığı yol, geçtiği router sayısı ve bu routerların topoloji üzerindeki bağlantı durumlarına bakarak karar verir.

Komşu router ve hedef network seçimindeki rota güncellemelerini sessizce arka planda çalışan, bgp anons komutları ile gerçekleştirmek mümkün.

Komşu routerların Frame Relay devreleri üzerinden, hedef network'e giderken sıradaki veya komşu router seçimine ait örnek konfigürasyon aşağıdaki gibi verilmiştir.



Şekil.44. BGP Komşuluk İlişkisi

7.12. BGP Senkronizasyonu

BGP protokolü çalışan router'larda BGP network bilgileri anons edilirken normal şartlarda sadece IBGP konfigürasyona sahip olan router'lar arasında topoloji ve network bilgisi paylaşılır.

Bir diğer haliyle EBGP router'lara herhangi bir IBGP router'dan güncelleme bilgisi direkt olarak paylaşılmaz, dolaylı yoldan güncelleme bilgisi paylaşılması istendiğinde bu bilgiyi paylaşıcak olan ve EBGP AS'e direkt bağlı olan router üzerinde senkronizasyon aktif hale getirilir.

Varsayılan olarak Cisco IOS'larda senkronizasyon kapalı durumda gelir.

Router(config-router)# no synchronization komutu kullanılarak senkronizasyon durumu değiştirilebilir.

7.13. BGP Protokolü Komşular Arasında Güvenlik Doğrulama Temelleri

Güvenlik konusu tartışılmaz olarak network dünyasında çok önemli bir yere sahiptir. BGP protokolü'de diğer yönlendirme protokolü gibi karşılıklı olarak güvenlik bilgilerini doğruladıktan sonra üzerindeki güncellemeleri karşı router ile paylaşabilir.

BGP protokolü varsayılan olarak güvenlik denetimi aktif değildir.

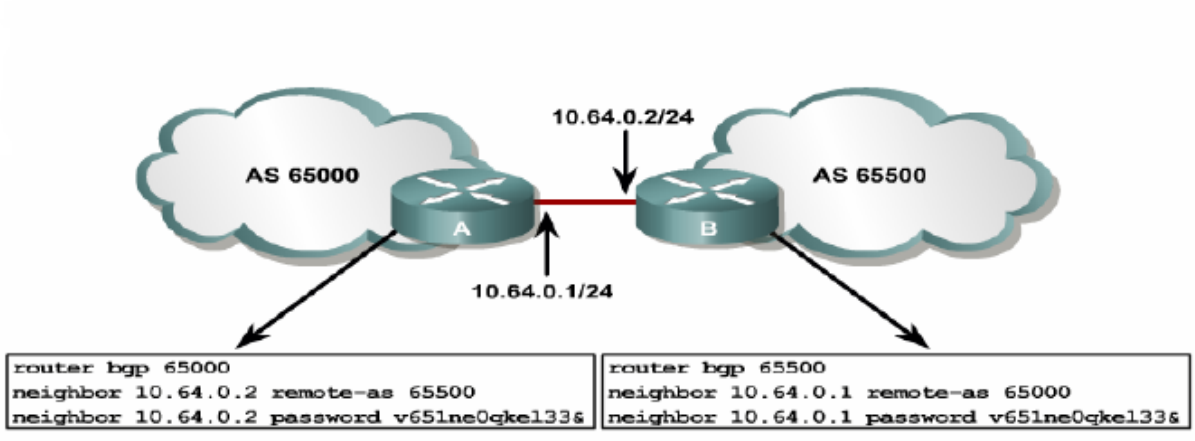
BGP protokolü MD5 güvenlik doğrulama metodunu kullanır.

Güvenlik anahtarı router'lar üzerinde bir anahtar bilgisi girilerek oluşturulur ve karşıdaki router'dan da aynı güvenlik anahtarına sahip olması beklenir.

Message Digest (MD5) metodu routerlar arasında anahtar bilgisi yollamazlar.

Router'lar üzerinde oluşturulan MD5 keyleri, BGP protokolünün TCP çalışmasından ötürü TCP segmentinde MD5 bilgisini çift yönlü olarak gönderip/alırlar.

Örnek konfigürasyon aşağıdaki gibidir.



Şekil.45. BGP Senkronizasyonu

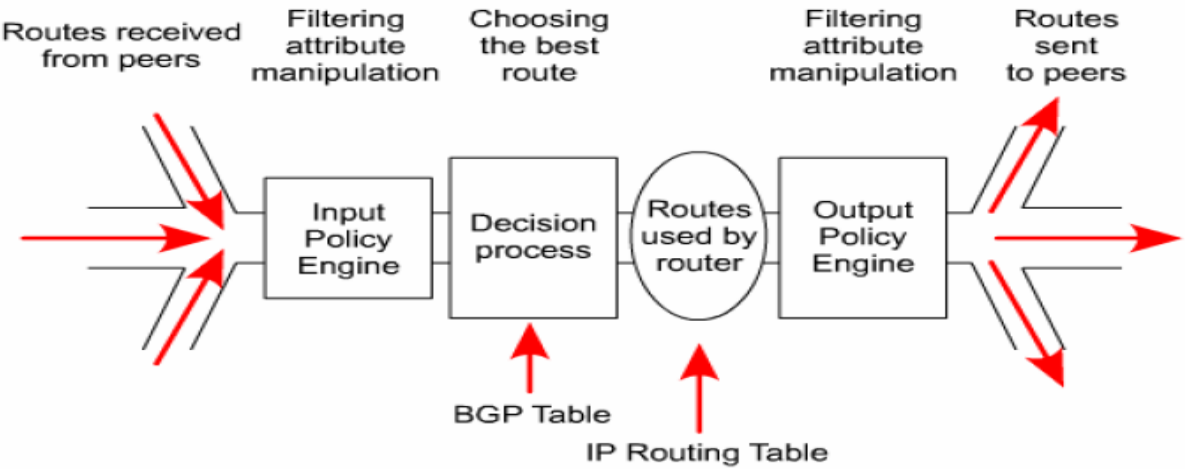
7.14. BGP Protokolü Oturumlarının Yenilenmesi

BGP protokolü aktif hale getirilmiş olan router'larda Erişim Denetim Listeleri (ACL) veya herhangi bir başlık, özellik eklendiğinde yapılan ayarların etki etmesi için BGP komşuluk ilişikisinin ve router üzerine yeni eklenen bilgilerin güncellenmesi, etkisini göstermesi için, BGP oturumlarının güncellenmesi gerekmektedir.

BGP oturumları 3 farklı yolla güncellenebilir.

Hard reset, Soft reset, Route refresh.

Aşağıdaki resim'de BGP protokolü için oturumu güncelleme aşamaları ve süreçleri yer almaktadır.



Şekil.46. BGP protokolü güncelleme aşamaları

Hard Reset :

Bu durumun anlamı BGP konuşan router'ların komşuluk ilişkisinin yeniden kurulup, yapılan değişiklikler ile birlikte yeni bilgiler ile komşuluk ve topoloji bilgileri diğer router'lar ile paylaştırılması için hard reset yapılır.

Router# clear ip bgp *

Komutunun anlamı tüm BGP bağlantılarının yeniden başlatılması ve komşuluk ilişkisinin yeniden gözden geçirilmesi sağlanır. Yalnızca BGP protokolü aktif olan cihazlarda çalışacaktır.

BGP protokolünün üzerindeki tüm yönlendirme tablosuda silinip yeniden oluşturulmak üzere hesaplanacaktır.

Router# clear ip bgp ip-address komutu ile sadece yazılan ip adresi ile komşuluk ilişkisi hesaplanması için kullanılır.

Soft Reset :

Bu durumda sadece BGP ile kurulan oturumlar yeniden başlatılacaktır. Bu operasyonda yeniden hesaplama veya BGP tablosu üzerindeki yönlendirme bilgilerinin silinmesi söz konusu değildir.

Bu komut ve uygulama genellikle kritiklik seviyesi yüksek olan İnternet Servis Sağlayıcılar veya Finans kuruluşlarında kullanılabilir.

Soft Reset sayesinde sadece dış ortama aktarılan bilgilerde bir değişiklik gerçekleştiyse onlarla ilgili operasyon yapıldığı için, oturumu kopartma işlemi yoktur.

Soft reset işlemini hem "inbound" hemde "outbound" segment'de kullanımı mümkündür.

Router# clear ip bgp * *ip-address (soft out)*

Router# clear ip bgp * *ip-address (soft in)*

Router(config-router) # neighbor *ip-address* soft-reconfiguration inbound

Route Refresh:

Router# clear ip bgp * *ip-address (peer-group-name) in*

Komutu sayesinde sadece yönlendirilmiş tablolar yenilenebilir. Route refresh komutu ilk olarak Cisco IOS12.0 (2)S and 12.0(6)T işletim sistemi versiyonları ile kullanılmaya başlanmıştır.

8. ÇOK PROTOKOLLÜ ETİKETLEME (MULTI-PROTOCOL LABEL SWITCHING-MPLS)

MPLS Protokolü OSI hiyerarşi modelinde 2. ve 3. katman arasında yer alır. İlerleyen zamanla beraber ağlarda artan kullanıcı sayılarına istinaden, ağlar üzerinde artan trafik hacmi daha yüksek bant genişliği ve hızlı iletim ihtiyacını beraberinde getirmiştir. Router'ların paket iletiminde routing tablosuna bakıp iletimi gerçekleştirmesi hem routerların yükünü arttırıyor hem de işlemlerin süresini uzatıyordu.

Bununla beraber ATM, Frame Relay veya Ethernet protokollerinin birlikte çalışması sistemde gecikmelere ve sorunlara sebep oluyordu. Tüm bunlara çözüm olarak 1997 yılında IEFT (Internet Engineering Task Force), MPLS protokolünü geliştirmeye başladı ve etiket anahtarlama iletim metodu ortaya çıkartıldı. İletim her IP paketi ya da ATM hücresinin başına eklenen etiketlerle gerçekleştirilmeye başlandı.

MPLS Protokolü detaylarını anlayabilmek için MPLS terminolojisini bilmek gerekmektedir.

8.1. MPLS Terminolojisi

8.1.2. MPLS Etiketleri

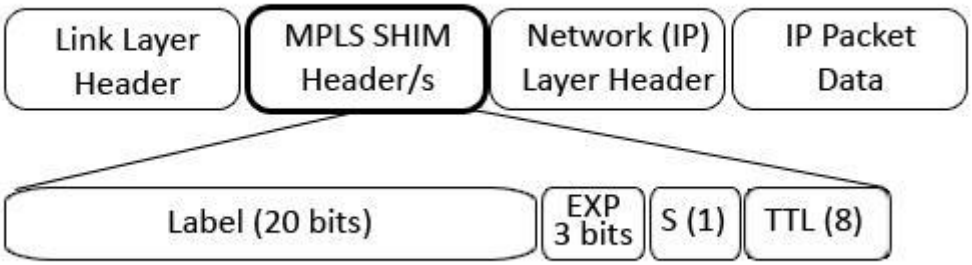
Label (Etiket) 4 byte uzunluğunda, yerel önem taşıyan bir tanımlayıcıdır, bu tanımlayıcı Forwarding Equivalence Class'ı belirler. 2.katman ve 3.katman arasına yerleşen bu 4 bytelik bu etiketin içinde;

20bit Label (Etiket) ; Label değerini belirtir.

3bit TC; Başlangıçta deneysel amaçlarla ayrılmıştır, günümüzde Class of Service alanı olarak kullanılmaktadır. (Bu kısım eskiden EXP olarak anılırdı fakat Şubat 2009'da yayınlanan RFC 5462 incelenirse artık TC olarak belirtilmektedir.)

1bit S; Bottom of Stack (Alt Yığın) biti olarak anılır, 1 değeri için etiketin bittiğini, 0 değeri için arkasından başka bir Label (etiket) daha geldiğini belirtir.

Aşağıda yer alan örnekte MPLS VPN paketi için iki farklı etiketin "S" değerleri görünmektedir.



Şekil.47. MPLS VPN Etiketi

Forwarding Equivalence Class (FEC) (Denklik Yönlendirme Sınıfıları);

Aynı rotadan yönlendirilen benzer işlem gören paketlerin bütününe verilen isim.

MPLS Label Switch Router (LSR) (Etiket Anahtarlama ve Yönlendirme);

Anahtarlamayı MPLS etiketlerine göre yapan routerdır. LSR paketi aldığında göndereceği "interface"'i belirledikten sonra Label'ı çıkartır ve yeni Label'ı pakete ekler sonrasında paketi belirtilen interface'den yollar.

MPLS Edge Label Switch Router (E-LSR) (Uç Etiketleme Anahtarlama ve Yönlendirme)

MPLS domainlerinin sınırlarında bulunurlar, paketler "MPLS" domainine girdiği noktada pakete etiketin eklenmesi ve domaini terk eden paketin ip bazlı yönlendirmesi bu routerlarda üzerinden yapılır.

MPLS Label Switched Path (LSP) (Etiket Anahtarlanmış Yol)

MPLS protokolünde veri iletimi "LSP" üzerinden yapılır, "LSP" kaynaktan hedefe kadar gidilecek yolun her noktasındaki etiketlerin dizisidir. Farklı bir deyişle iki nokta arasında kurulan sanal bir yol olarak da belirtebiliriz. "LSP" üzerinde etiketler "LDP" veya "RSVP" gibi protokollerle dağıtılır. (Etiketleme eğer "RSVP" ile yapılırsa bir traffic-engineering özelliği olan LSP 'ler ile A ile B noktası arasındaki yol şu noktalardan geçerek gitsin diye belirtebilir, eğer etiketleme protokolu olarak "LDP" kullanılıyorsa "TE" yapamazsın, dolayısıyla "LSP" 'lerin yoktur, yolu "OSPF" belirler ve "OSPF" çalışma metodolojisine göre trafik akışı devam eder.)

Label Distribution Protokol (LDP) (Etiket Dağıtımlı Protokol)

Bu protokol MPLS ağlarında etiketlerin “LSR” ’lara dağıtılmasını sağlamak için kullanılır. “LDP” sayesinde “FEC” ’ler etiketler ile eşlenir ve “LSP” ‘ler oluşturulur. LDP protokolü çift yönlü çalışır her oturumda “LDP” komşuları karşılıklı olarak birbirlerinin etiket eşleştirmesini öğrenebilirler. “LDP” komşu etiket bilgilerini eşleştirmek için “LDP” kullanan iki “LSR” ‘a verilen isimdir.

Label Information Base (LIB) (Etiket Anahtarlama Temelli)

IP/MPLS router’ların da “LDP” sayesinde oluşturulan, içerisinde network etiket bilgileri “LSR” ve etiket bilgileri yer alır.

Label Forwarding Information Base (LFIB) (Etiket Yönlendirme Bilgisi)

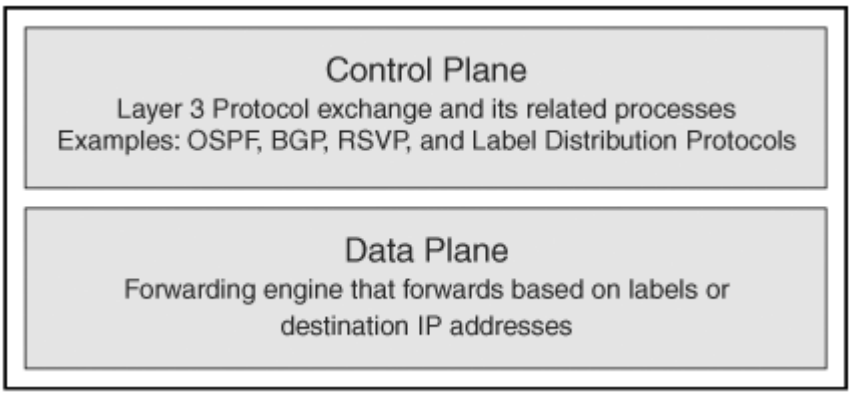
Network bilgileri, etiketleri ve yapılacak değişme işlemi vardır. Gelen etiketlerin bir sonraki router’a nasıl gönderileceğini belirler.

Control Plane (Kontrol Erişimi) ve Data Plane(Veri Erişimi)

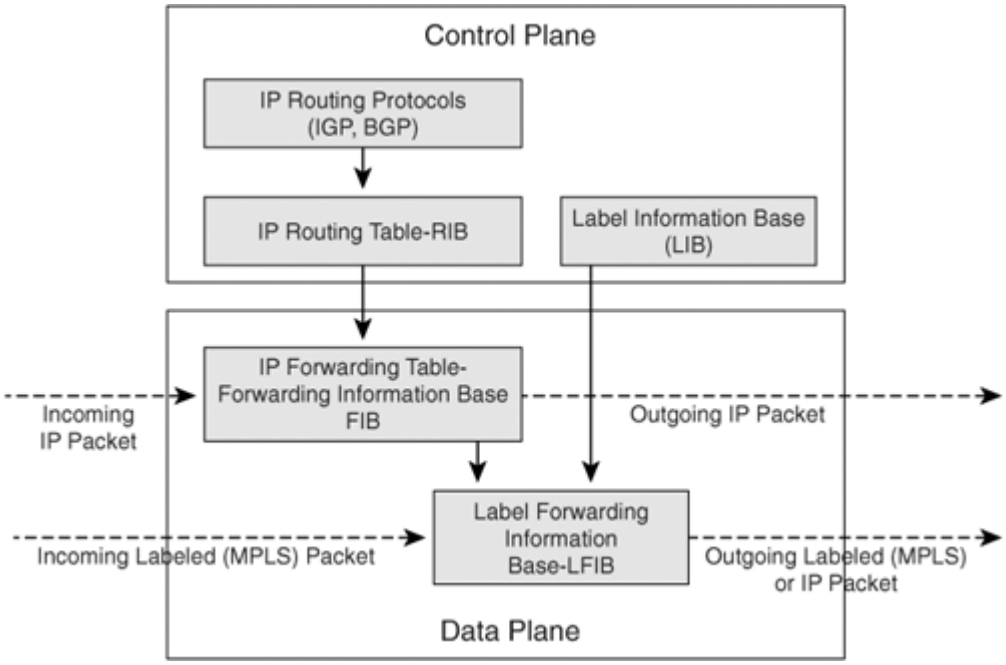
MPLS işlemi Cisco cihazlarda iki farklı mimari blokta çalışır,

Control Plane: 3. Katman protokoller burada çalışırlar, bu sebeple 3. Katman yönlendirme bilgilerini burada tutarlar. LDP, RSVP gibi protokoller de bu blokta çalışır.

Data Plane: Etiket tabanlı yönlendirmenin yapıldığı yerdir, yönlendirme işlemi control plane de tutulan tabloya göre yapılır.



Şekil.48. MPLS Control ve Data Plane



Şekil.49. Control Plane ve Data Plane Metodolojisi

Yukarıda belirtilen çalışma metodolojisi Control Plane ve Data Plane çalışmasını açıklamaktadır.

Resim'e bakıldığında LSR'a gelen bir paket Data Plane tarafından alınmakta ve ControlPlane'deki "LIB" bilgilerine göre iletilmekteydi. Ayrıca yukarıdaki şekilde açıkca görünmektedir ki Cisco routerlarda "MPLS" ve "CEF" hemen hemen aynı

şekilde çalışmaktadır. Resimde MPLS paketinin dışında Cisco Router'a gelen bir IP paketinin yönlendirilmesi de gözükmektedir.

8.2. MPLS'in FAYDALARI

- Tek elden yönetilebilen, coğrafi sınırları ortadan kaldıran bir alt yapı hazırlanmasına olanak tanır.
- IP üzerinden ATM teknolojisinin veya diğer network topolojilerinin entegrasyonunun kolaylaştırılması.
- İnternet servis sağlayıcılarının omurga networklerde BGP protokolü çalıştırılması zorluğunun ortadan kaldırılması.
- Uçtan-Uca, noktadan – noktaya network iletişim modellerine izin vermesi.
- Network'deki trafik akışına detaylar ile müdahele edilmesi.

MPLS protokol sayesinde entegre edilmiş tek bir network yönetilmesi amaçlanmaktadır. MPLS paketlerini taşıyan omurga cihazlar MPLS paketinin içerisinde ne taşıdığına bakmazlar.

MPLS protokolü sayesinde Ipv4, Ipv6, Ethernet, HDLC, PPP ve OSI referans modelinde 3.katmanda çalışan protokollerin tamamı MPLS ile taşınabilir.

ATM teknolojisi üzerinden IP paketlerini taşımak MPLS'den de önce kullanılmaktaydı. Bilinen metodlardan bir tanesi RFC 1483'de açıklanmış olan "Multiprotocol Encapsulation over ATM Adaptation Layer 5" . Bu oluşturulan devrelerin tamamı elle oluşturulduğu için bütün yollar, geçilecek bir sonraki yönlendirici cihazları tek tek tarif etmek gerekliydi.

Omurga networklerde yönlendiriciler IP yerine etiket anahtarlama yaptığından BGP protokolünün getirdiği yüklerden kurtulurlar. Tam yedekli yönlendirme

tablosunda 150.000 civarı satır olduğunu düşünürsek omurga cihazların işlemci, bellek ihtiyaçları ciddi ölçüde azalacaktır.

Servis sağlayıcılar müşterilerine VPN (Sanal Özel Ağlar) hizmeti vermek için iki tip VPN kurulumu yapabilirler.

8.3. MPLS VPN

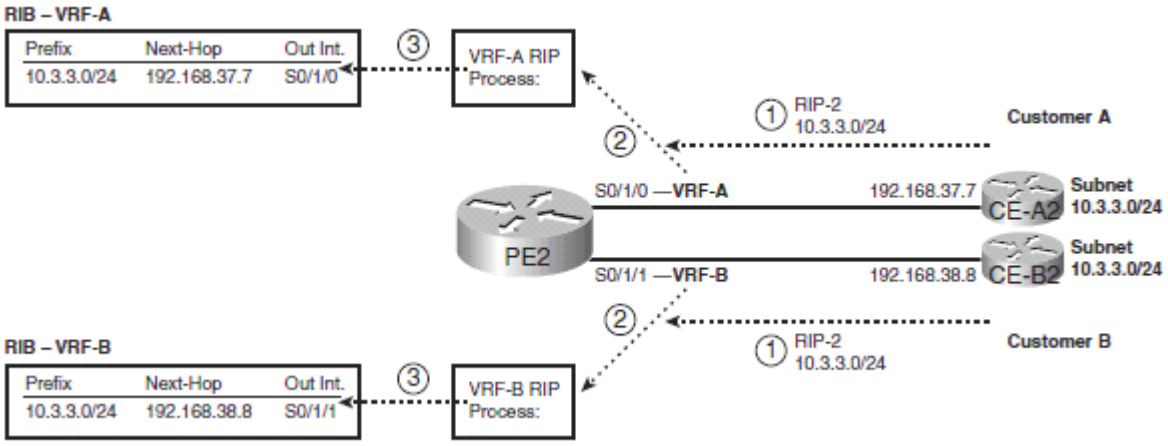
MPLS VPN'i anlamak için BGP, IGP(OSPF, RIP, IS-IS), MPLS ve MP-BGP konusunda fikir sahibi olmak gereklidir. MPLS VPN'in altyapısını sağlayan temel bilgiler aşağıdaki gibidir.

- VRF (Sanal Yönlendirme Tablosu)
- Route Distinguisher (RD) (Rota Ayırma)
- Route Target (RT) (Hedef Rota)

8.4. VRF

Aynı IP adres gruplarını kullanan farklı müşterileri desteklemek için MPLS VPN içerisinde sanal router konsepti kullanılır. Sanal routerları oluşturmak için "VRF" tabloları oluşturulur, bu sayede istenilen yönlendiricide birbirinden izole edilmiş farklı IP tabloları tutulur. VRF'ler üzerinde MPLS çalışan "PE" routerlarında tanımlanıp kullanılır.

Konsepti bir örnek ile açıklayacak olursak aşağıda A ve B müşterilerine bağlı PE2 yönlendirici vardır. Müşteri ve Servis sağlayıcı routerı arasında RIPv2 (Herhangi başka bir protokolde olabilir) kullanılmaktadır. PE2 yönlendiricisi A ve B yönlendiricilerinde aynı ip adresi gruplarını öğrenmektedir. Şekilde belirtilen 1, 2, 3 numaralı adımları açıklayacak olursak;



Şekil.50. VRF Örneği

1. CE routerları PE routerına RIP-2 kullanarak 10.3.3.0/24 networkunu anons ederler.
2. PE routerında A ve B müşterisi için VRF-A ve VRF-B tanımlanmış olduğundan bu portlardan gelen anonsları uygun VRF içine sokar. A müşterisi için S0/1/0 portundan gelen updateleri VRF-A altında diğer işlemlerden ayrı bir şekilde RIP prosesine sokar. Aynı işlemi S0/1/1 porttundan gelen B müşterisi içinde VRF-B içerisinde yapar.
3. RIP hesaplamaları yapıldıktan sonra VRF-A altında RIB tablsouna bu rota için gerekli satır eklenir. Aynı işlem B müşterisi içinde tamamlanır. Her VRF için RIB ve FIB tabloları tutulur.

8.5. Multi Protocol BGP (MP-BGP) ve Route Distinguishers (RD)

PE2 yönlendiricisi yukarıda verilen örnekte A ve B müşterisinden gelen anonsları değerlendirerek birbirinden bağımsız iki farklı RIB oluşturdu. Şu an bu bilgilerin Servis sağlayıcıdaki diğer yönlendiriciler aracılığıyla diğer sağlayıcı routerlara ve müşterinin diğer noktalarına ulaştırılması gerekiyor. BGP yinelenen prefixlerinin iletilmesi için tam olarak bir çözüm sağlamamaktadır.

Yinelenen ip adreslerinin birbirinden ayrılabilmesi için "BGP NLRI" önüne bir ekleme yapılarak müşterinin "NLRI" değerlerinin istenildiği gibi birbirinden farklı olması sağlanır. Bunu sağlamak için BGP güncellemerinde NLRI değerlerini güncellenmeye izin veren MP-BGP (RFC 4760) kullanılır. IPv4 adreslerinin ayrıştırılabilmesi için başına eklenen bu ayrıştırıcıya da Route Distinguisher (RD) denir.

RD kullanım konseptini özeleyecek olursak anonslarda her "NLRI" için geleneksel ip adresinin başına 64bitlik RD değeri eklenir ve aynı IPv4 adreslerinin başına gelen farklı RD değerleri sayesinde yepyeni birbirinden farklı "NLRI" formatı ortaya çıkar.

64bitlik RD'nin, ilk 16bit i BGP extended commmunity tipini belirtmek için ayrılmıştır, bu yüzden RD tanımlamak için elimizde 48bit vardır. RD değeri iki farklı şekilde girilebilir.

16bit:32bit (Autonom Sistem Numarası: XXX)

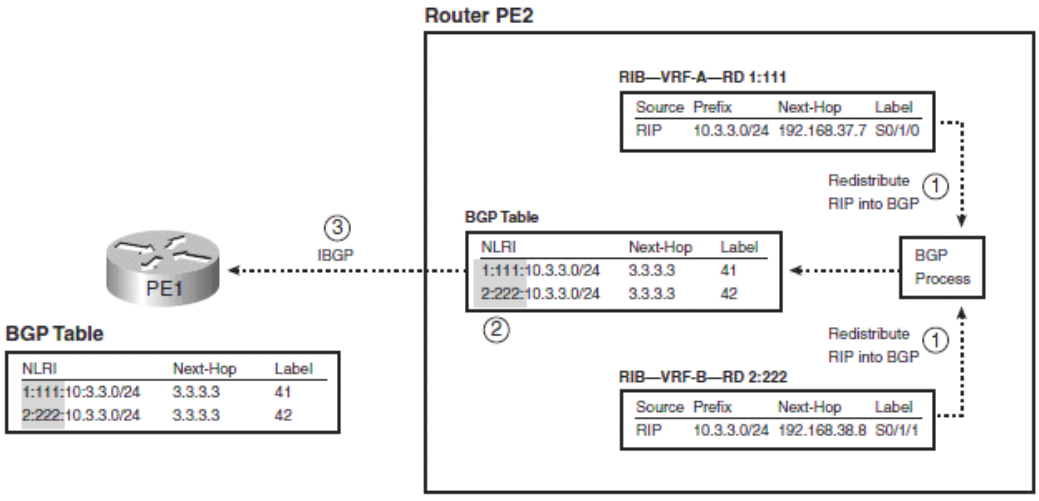
32bit:16bit (Ip Adresi: XXX)

Her iki yöntemde uygulanabilir olmasına rağmen ilk verilen yöntem daha sık kullanılmaktadır.

VRF örneğinde farklı müşterilerden RIP-2 ile anonsları alan VRF-A ve VRF-B için ayrı RIB tabloları oluşturan PE2 üzerinden konuyu açıklamaya devam edelim. VRF-A için RD 1:111, VRF-B için RD 2:222 kullanılmış olsun. RD değeri olmasaydı PE2 routerı 10.3.3.0/24 ile ilgili aldığı anonsu BGP üzerine redistribute (RIP ile

öğrendiği rotaları BGP üzerine aktarıp BGP ile dışarıya anons etmesidir.) sağlayıcının başka noktasındaki PE1 routerı bunlardan sadece bir tanesini en iyi yol olarak değerlendirip onu kullanırdı.

RD değeri eklendiği zaman BGP tablosunda aynı IPv4 adresinin ayrıştırılması sağlanır. Aşağıda görülen 1,2 ve 3 numaralı adımların açıklamaları aşağıda paylaşılmıştır.



Şekil.51. BGP Tablosu ve RIB

1. PE2 öğrendiği rotaları VRF-A ve VRF-B için oluşturduğu RIB'de tutmaktadır. Bu rotalar BGP üzerinde redistribute edilsin.
2. BGP tablosu oluşturulurken NLRI değeri olarak VRF-A ve VRF-B de tutulan satırların başına bu VRF'e ait RD değeri eklenir. Şekilde verilen BGP tablosuna bakıldığında aynı ip adres grubu için yeni NLRI değerleri ortaya çıktığı görülmektedir.

   A müşterisi için = 1:111:10.3.3.0/24
   B müşterisi için = 2:222:10.3.3.0/24

3. PE2 IBGP ile bu bilgileri PE1 routerına ilettiği anda, PE1 farklı RD değerleri sebebiyle bu iki rotayı da öğrenir.

Üzerinden hareket edilen örnekte PE1 routerı 10.3.3.0/24 networkü için VPN-A ve VPN-B için olmak üzere iki farklı rota öğrendi. Sonraki aşamada PE1 routerı BGP tablosunda bulunan bu rotaları kendi üzerinde doğru VRF'lerin içerisine sokması gerekmektedir. Bunu sağlamak için Router Targetler kullanılır.

8.6. Route Targets (RT) (Yönlendirme Hedefleri)

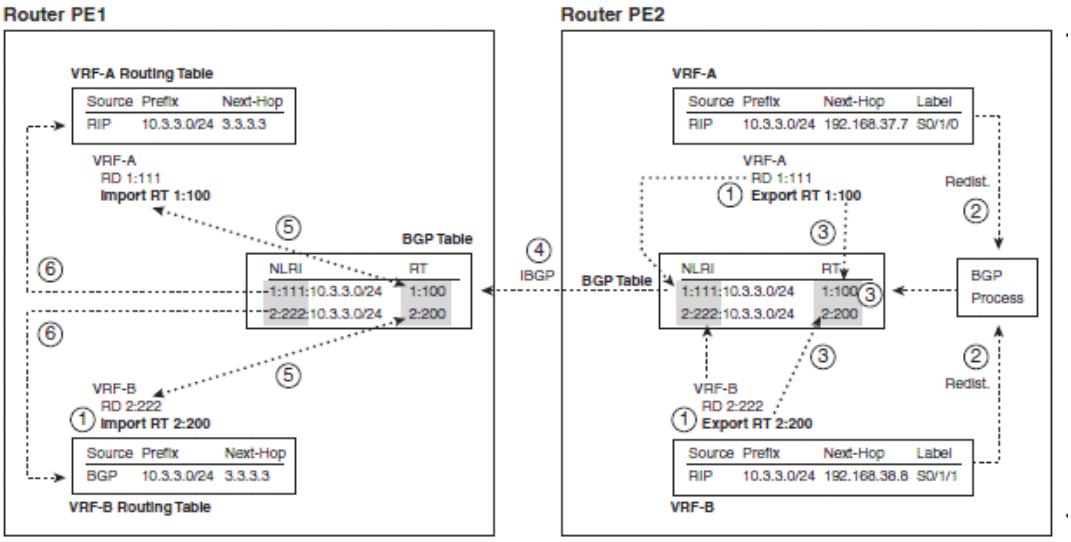
RT'nin anlaşılması için öncelikle basit bir şekilde nasıl çalıştığının bahsedilmesi gereklidir.

MPLS RT'yi IBGP ile öğrendiği rotaları PE üzerindeki hangi "VRF" üzerine aktaracağını belirlemek için kullanır. RT temel olarak RD ile aynı formattadır. Fakat belirli bir prefix sadece bir RD değerine sahip olabilirken, aynı prefixe birden fazla RT değeri atanabilir.

PE yönlendiricileri RT değerlerini BGP updateleri içerisinde BGP "Extended Community Path Attribute" olarak dağıtırlar.

RT değerini açıklamaya VRF ve RD'de kullandığımız topoloji üzerinden açıklanmaktadır.

Şekilde VRF A ve B için verilen RD, RT import ve export değerleri yer almaktadır.



Şekil.52. VRF A ve B için verilen RD, RT Değerleri

1, 2, 3, 4, 5, 6 numaralı adımları sırasıyla aşağıda sırası ile açıklanmaktadır.

1. PE2 üzerinde iki VRF üzerinde Export RT değerleri verilmiştir. VRF-A için 1:100 VRF-B için 2:200. PE1 üzerinde Import RT değerleri VRF-A için 1:100 VRF-B için 2:200 olarak verilmiştir.
2. RIP üzerinden BGP'ye redistribution gerçekleşir.
3. RD ile NLRI oluşturulmasından önceki aşamada bahsedilmişti bu aşamada dikkatimizi vermemiz gereken kısım BGP tablosunda eklenen RT değeridir. Export işlemi VRF'den BGP üzerine redistribution yaparken kullanılır, bu sebeple konfigurasyonda export RT değeri girilmiştir. BGP tablosuna ise VRF'ler için verilen RT export değerleri eklenmiştir.
4. PE2 IBGP kullanarak rotaları RT değerleriyle birlite PE1'e anons eder.
5. PE1 IBGP ile rotaları ve RT değerlerini öğrenir
6. PE1 her rota için RT değerlerini bilmektedir. Bu rotaları VRF'ler üzerine BGP den redistribute ederken izin verilen Import değerlerine bakar ve VRF-A içerisindeki RIB'e A müşterisinin rotalarını, VRF-B içerisindeki RIB'e de B müşterisinin rotalarını yazar.

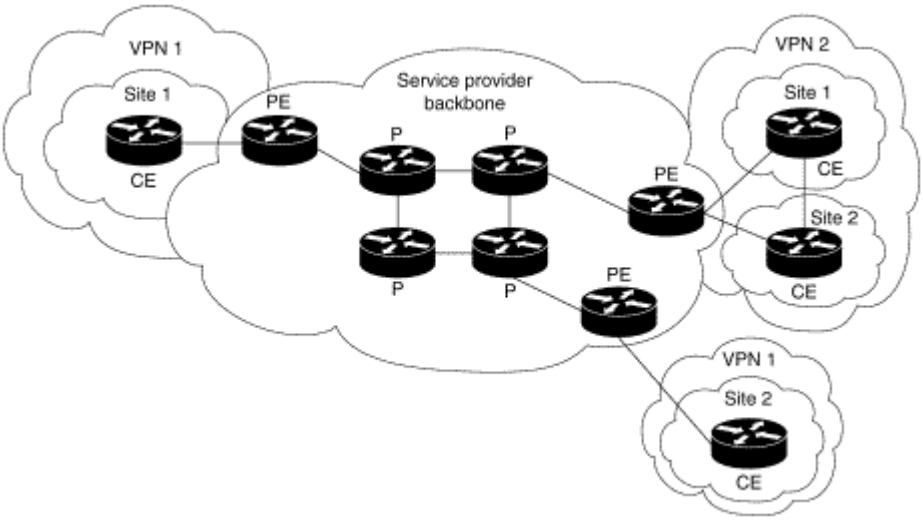
Yukarıda anlatılan işlemde PE1'e bağlı A müşterisinin routerı PE2'deki A müşterisinin routerın'daki adres grubunu öğrenmiştir. PE2 deki A müşterisi

Routerının PE1 deki A müşterisinin rotalarını öğrenmesi için aynı şekilde PE1'de bulunan VRF-A üzerinde RT export, PE2 de bulunan VRF-A üzerinde RT import işlemi yapması gerekmektedir.

RT ve RD değerleri aynı veya farklı olarak tanımlanabilir.

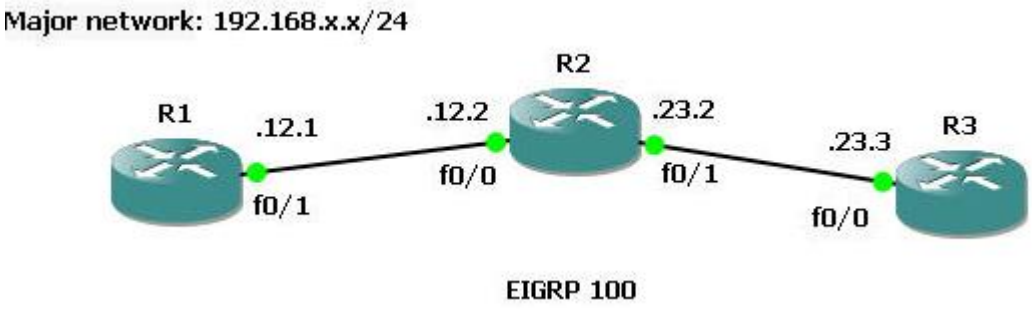
Verilen bu genel bilgilerin ardından MPLS protokolü ile ilgili olarak temel konfigürasyon yapabilecek duruma gelmiş bulunmaktayız.

Örnek MPLS yönlendiricilerinin konumlandırılması açıklayan resim aşağıdaki gibidir.



Şekil.53. MPLS Yönlendiricilerinin Konumlandırılması

Temel MPLS konfigürasyonu ve topolojisi aşağıdaki gibidir.



Şekil.54. Temel MPLS Konfigürasyonu

Yukarıdaki topoloji göz önünde bulundurulduğunda, cihazların örnek konfigürasyonları aşağıdaki gibidir.

Öncelikle cihazlar üzerinde EIGRP protokolü ile temel konfigürasyonlarını tanımlayacağım.

EIGRP AS 100 bilgisi dahilinde R1,R2 ve R3 cihazlarına tek tek temel ayarlar tanımlanacak.

R1:

R1#configure terminal
R1(config)#interface f0/1
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router eigrp 100
R1(config-router)#network 192.168.12.0 0.0.0.255

R2:

R2#configure terminal
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router eigrp 100
R2(config-router)#network 192.168.12.0 0.0.0.255
R2(config-router)#network 192.168.23.0 0.0.0.255

R3:

R3#configure terminal
R3(config)#interface f0/0
R3(config-if)#ip address 192.168.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router eigrp 100
R3(config-router)#network 192.168.23.0 0.0.0.255

Bu adımları cihazlar üzerinde tek tek yazdığımızda temel ip yapılandırması ve EIGRP yönlendirme protokolü konfigürasyonu tamamlandıktan sonra, cihaz üzerindeki konfigürasyonun doğruluğunu ispatlamak adına, her yönlendirici cihaza ait ekran görüntülerini her cihaz için aşağıdaki gibi sırası ile paylaşılmıştır.

R1 başlangıç konfigürasyonu;

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, FastEthernet0/1
D    192.168.23.0/24 [90/30720] via 192.168.12.2, 00:05:12, FastEthernet0/1
R1#
```

Şekil.55. R1 Başlangıç Konfigürasyonu

R2 başlangıç konfigürasyonu;

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.12.0/24 is directly connected, FastEthernet0/0
C    192.168.23.0/24 is directly connected, FastEthernet0/1
R2#
```

Şekil.56. R2 Başlangıç Konfigürasyonu

R3 başlangıç konfigürasyonu;

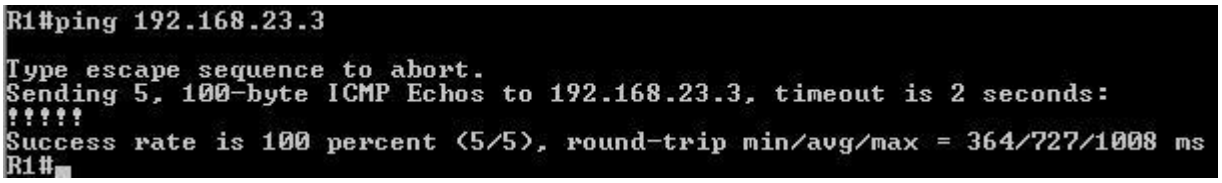
```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.12.0/24 [90/30720] via 192.168.23.2, 00:08:13, FastEthernet0/0
C    192.168.23.0/24 is directly connected, FastEthernet0/0
R3#
```

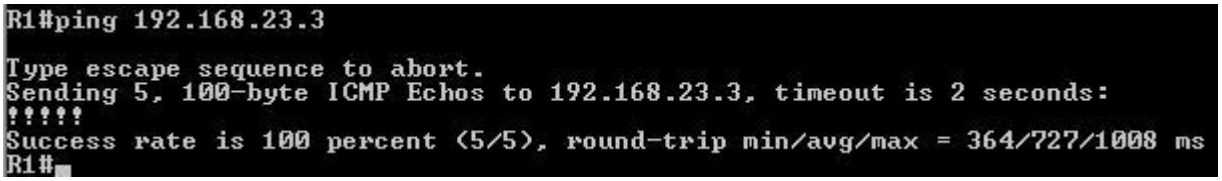
Şekil.57. R3 Başlangıç Konfigürasyonu

Bu doğrulama komutlarının ardından herhangi bir cihaz'da örneğin R1 cihazında komşuluk durumunu sorgulamak için aşağıdaki gibi bilgi alınabilir.



Şekil.58. R1 Komşuluk Durumunu

Cihazlar arasındaki iletişim durumunu test etmek içinse aşağıdaki ekran görüntüsündeki komut kullanılır.



Şekil.59. R1 Komşuluk Durumunu 2

Temel ayalarının tamamlanmasının ardından cihazlar üzerinde MPLS protokolünü aktif edebilmek için aşağıdaki adımları sırası ile cihazlar üzerinde uygulamak gereklidir.

R1:

R1(config)#interface f0/1

R1(config-if)#mpls ip

R2:

R2(config)#interface f0/0

R2(config-if)#mpls ip

R2(config)#interface f0/1

R2(config-if)#mpls ip

R3:

R3(config)#interface f0/0

R3(config-if)#mpls ip

Cihazlar üzerinde yukarıdaki konfigürasyonları uyguladıktan kısa bir süre sonra mpls protokolünün aktif edildiğini ekran görüntüsünde gözlemleyebilirsiniz.

Şekil.60. MPLS Protokolünün Aktivasyonu

Cihazlarda sırası ile MPLS protokolünün interface bazlı olarak durumunu görüntülemek için aşağıdaki adımları sırası ile takip etmek gerekli.

R1

Şekil.61. MPLS R1

R2

```
R2#show mpls interfaces
Interface              IP             Tunnel   Operational
FastEthernet0/0        Yes (ldp)      No       Yes
FastEthernet0/1        Yes (ldp)      No       Yes
R2#
```

Şekil.62. MPLS R2

R3

```
R3#show mpls interfaces
Interface              IP             Tunnel   Operational
FastEthernet0/0        Yes (ldp)      No       Yes
R3#
```

Şekil.63. MPLS R3

Son olarak yönlendiriciler üzerinde MPLS komşuluk ilişkisini cihazlarda sırası ve detayları ile aşağıda görüntülemek mümkündür.

R1

```
R1#show mpls ldp neighbor
    Peer LDP Ident: 192.168.23.2:0; Local LDP Ident 192.168.12.1:0
        TCP connection: 192.168.23.2.32009 - 192.168.12.1.646
        State: Oper; Msgs sent/rcvd: 17/17; Downstream
        Up time: 00:10:57
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 192.168.12.2
        Addresses bound to peer LDP Ident:
          192.168.12.2    192.168.23.2
R1#
```

Şekil.64. MPLS komşuluk ilişkisi R1

R2

```
R2#show mpls ldp neighbor
    Peer LDP Ident: 192.168.12.1:0; Local LDP Ident 192.168.23.2:0
        TCP connection: 192.168.12.1.646 - 192.168.23.2.32009
        State: Oper; Msgs sent/rcvd: 18/18; Downstream
        Up time: 00:11:41
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.12.1
        Addresses bound to peer LDP Ident:
          192.168.12.1
    Peer LDP Ident: 192.168.23.3:0; Local LDP Ident 192.168.23.2:0
        TCP connection: 192.168.23.3.21141 - 192.168.23.2.646
        State: Oper; Msgs sent/rcvd: 17/17; Downstream
        Up time: 00:11:20
        LDP discovery sources:
          FastEthernet0/1, Src IP addr: 192.168.23.3
        Addresses bound to peer LDP Ident:
          192.168.23.3
R2#
```

Şekil.65. MPLS komşuluk ilişkisi R2

R3

```
R3#show mpls ldp neighbor
    Peer LDP Ident: 192.168.23.2:0; Local LDP Ident 192.168.23.3:0
        TCP connection: 192.168.23.2.646 - 192.168.23.3.21141
        State: Oper; Msgs sent/rcvd: 18/18; Downstream
        Up time: 00:11:52
        LDP discovery sources:
          FastEthernet0/0, Src IP addr: 192.168.23.2
        Addresses bound to peer LDP Ident:
          192.168.12.2    192.168.23.2
R3#
```

Şekil.66. MPLS komşuluk ilişkisi R3

Temel MPLS protokolü üzerindeki tanımlamalara interface tabanlı veya tüm mod'lar için mpls protokolünün "tdp" özelliğini aktif edebiliriz.

R(config)#mpls label protocol tdp (Genel olarak aktif etmek için)

R(config-if)#mpls label protocol tdp (interface tabanlı aktif etmek için)

Temel olarak tüm cihazlar üzerindeki MPLS ve EIGRP protokolü tanımlamalarını gerçekleştirmiş bulunduk.

9. BGP PROTOKOLÜ İLE İNTERNET YÖNLENDİRME ÜZERİNDE ROTA MANİPÜLASYONU

BGP Protokolü hakkında detayları ile paylaşmış olduğumuz yönlendirme temellerinin ardından;

Rota Manipülasyonu nedir?

BGP protokolünü kullanarak rota manipülasyonu nasıl yapılır?

Sorularının cevaplarını uygulamalı olarak aşağıda detayları ile paylaşılmış bulunmaktadır.

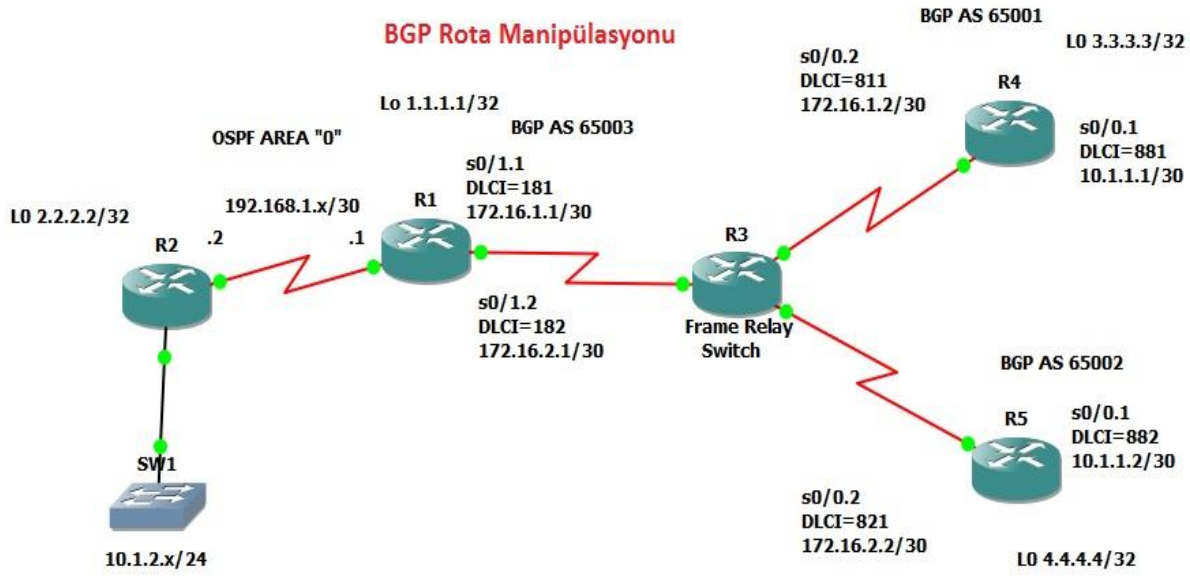
9.1. Rota Manipülasyonu Nedir ?

Rota Manipülasyonu, yönlendirme protokollerini kullanarak kaynak ağ yolunun, hedef ağ yoluna giderken kullandığı tüm ip trafiğinin yönünün farklı rotalar üzerinden, elle veya dinamik olarak ağ trafiğine istenildiği gibi müdahale edilmesine ve ağ trafiğinin optimizasyonun yapılarak performans artışı sağlanması için kullanılan metoda verilen isimdir.

9.2. Rota Manipülasyonu Nasıl Yapılır ?

BGP Protokolü kullanılarak rota manipülasyonunu aşağıdaki aşamalarda, sırası ile uygulanmış ve çalışan BGP ve OSPF protokolü konfigürasyonlarının ardından, rota manipülasyonun elle ayarlanmasının ve sonucunun normal trafik ile rota manipülasyon ayarlarının tamamladıktan sonraki halini görüntüleyebiliriz.

Aşağıdaki topolojimizin üzerinde BGP Rota Manipülasyonu uygulamasını gerçekleştireceğim.



Şekil.67. BGP Rota Manipülasyonu Genel Topoloji

Temel BGP konfigürasyonu ve topoloji özelinde minumum olması gereken konfigürasyon çıktıları aşağıda tüm yönlendiriciler için yer almaktadır.

R1 cihazı konfigürasyon çıktısı ;

R1#sh run

Building configuration...

Current configuration : 1442 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

```
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
!
interface Serial0/1.1 point-to-point
 ip address 172.16.1.1 255.255.255.252
 frame-relay interface-dlci 181
!
interface Serial0/1.2 point-to-point
 ip address 172.16.2.1 255.255.255.252
 frame-relay interface-dlci 182
!
```

```
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate
!
router bgp 65003
 no synchronization
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 172.16.1.0 mask 255.255.255.252
 network 172.16.2.0 mask 255.255.255.252
 redistribute ospf 1
 neighbor 172.16.1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 no auto-summary
!
ip http server
no ip http secure-server
!
control-plane
!
```

```
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R2 cihazının konfigürasyonu aşağıdaki gibidir;

```
R2#sh  run
Building configuration...
Current configuration : 1442 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface Serial0/0
```

```
 ip address 192.168.1.2 255.255.255.252
 serial restart-delay 0
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface FastEthernet1/0
 ip address 10.1.2.1 255.255.255.0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
ip http server
no ip http secure-server
control-plane
!
```

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

R3 (Frame Relay) cihazının konfigürasyonu aşağıdaki gibidir;

```
R3#sh  run
Building configuration...
Current configuration : 1442 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
frame-relay switching
!
interface Serial0/0
 no ip address
```

```
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 181 interface Serial0/1 811
 frame-relay route 182 interface Serial0/2 821
!
interface Serial0/1
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 811 interface Serial0/0 181
 frame-relay route 881 interface Serial0/2 882
!
interface Serial0/2
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 clock rate 128000
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 frame-relay route 821 interface Serial0/0 182
 frame-relay route 882 interface Serial0/1 881
!
interface Serial0/3
 no ip address
 shutdown
```

```
 serial restart-delay 0
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R4 cihazının konfigürasyonu aşağıdaki gibidir;

```
R4#sh  run
Building configuration...
Current configuration : 1442 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R4
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
```

```
!
ip cef
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
!
interface Serial0/0.1 point-to-point
 ip address 10.1.1.1 255.255.255.252
 frame-relay interface-dlci 881
!
interface Serial0/0.2 point-to-point
 ip address 172.16.1.2 255.255.255.252
 frame-relay interface-dlci 811
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 network 3.3.3.3 mask 255.255.255.255
 network 10.1.1.0 mask 255.255.255.252
 network 172.16.1.0 mask 255.255.255.252
 neighbor 10.1.1.2 remote-as 65002
 neighbor 172.16.1.1 remote-as 65003
 no auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Null0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R5 cihazının konfigürasyonu aşağıdaki gibidir;

```
R5#sh  run
Building configuration...
```

```
Current configuration : 1442 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R5
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
!
 interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface Serial0/0
 no ip address
 encapsulation frame-relay
 serial restart-delay 0
 frame-relay lmi-type ansi
!
interface Serial0/0.1 point-to-point
 ip address 10.1.1.2 255.255.255.252
 frame-relay interface-dlci 882
!
interface Serial0/0.2 point-to-point
```

```
 ip address 172.16.2.2 255.255.255.252
 frame-relay interface-dlci 821
!
interface Serial0/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial0/3
 no ip address
 shutdown
 serial restart-delay 0
!
router bgp 65002
 no synchronization
 bgp log-neighbor-changes
 network 0.0.0.0
 network 4.4.4.4 mask 255.255.255.255
 network 10.1.1.0 mask 255.255.255.252
 network 172.16.2.0 mask 255.255.255.252
 neighbor 10.1.1.1 remote-as 65001
 no auto-summary
!
ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 Null0
```

!

control-plane

!

line con 0

line aux 0

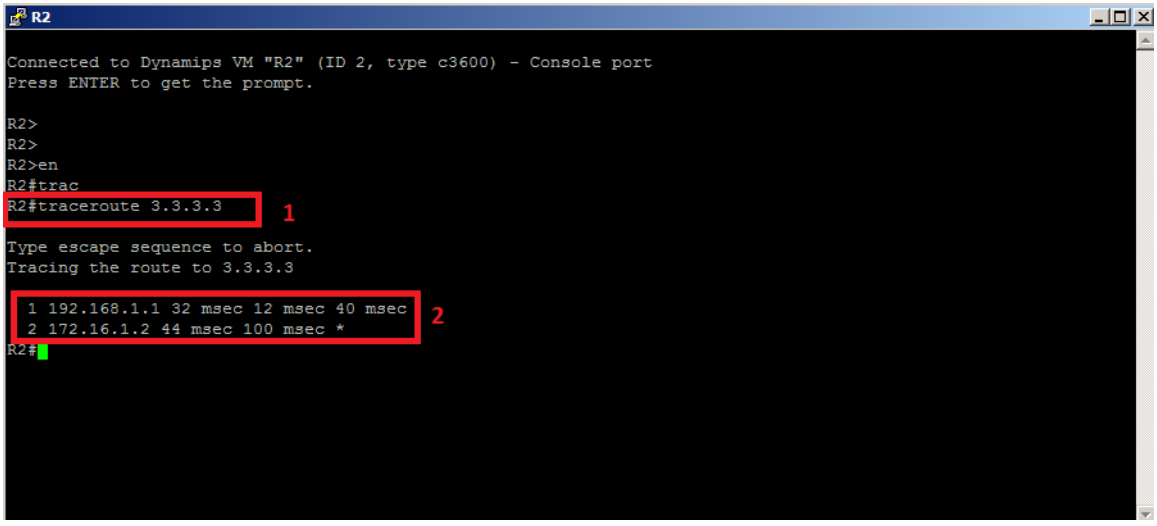
line vty 0 4

login

!

end

Rota manipülasyonu yapılmadan evvel R2 cihazı üzerinden, R4 cihazı üzerinde bulunan 3.3.3.3 Ip adresine ulaşmak için traceroute komutu kullanıldığında geçilen ağ rotası çıktısı aşağıdaki gibidir.



Şekil.68. Rota Manipülasyonu yapılmadan evvel 2 farklı cihaz üzerindeki iletişimin testi

Ekran çıktısından da görüldüğü üzere topolojimizin en sol tarafında bulunan cihazdan en sağ üst taraftaki taraftaki R4 cihazının üzerindeki 3.3.3.3 ip adresine ulaşılmak istenildiğinde, R4 cihazı önünde yer alan 172.16.1.2 interface ip adresinden sonra 3.3.3.3 ip adresine erişim sağlanabiliyor.

Bu durumu değiştirip alternatif yol olan R5 cihazı üzerindeki sanal link üzerinden gitmesini sağlayıp mevcut rota üzerinde manipülasyon işlemini gerçekleştirmiş olacağız.

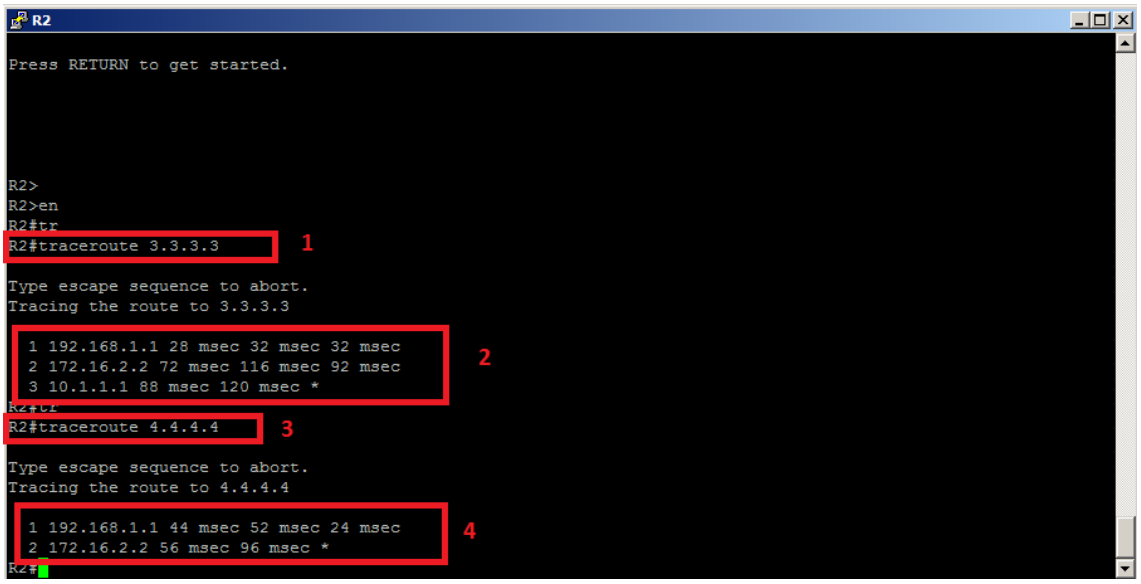
Rota Manipülasyon işlemini gerçekleştirmiş olduğumuz cihaz R1 cihazıdır. R1 cihazı manipülasyon işlemi için yapılan temel konfigürasyon aşağıda yer almaktadır.

R1 cihazı rota manipülasyonu için önemli alt başlıkların çıktısı;

```
interface Serial0/1.1 point-to-point
 bandwidth 64
 ip address 172.16.1.1 255.255.255.252
 frame-relay interface-dlci 181
!
interface Serial0/1.2 point-to-point
 bandwidth 128
 ip address 172.16.2.1 255.255.255.252
 frame-relay interface-dlci 182
router bgp 65003
 no synchronization
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 172.16.1.0 mask 255.255.255.252
```

```
 network 172.16.2.0 mask 255.255.255.252
 redistribute ospf 1
 neighbor 172.16.1.2 remote-as 65001
 neighbor 172.16.1.2 route-map LOCALPREF-R4 in
 neighbor 172.16.2.2 remote-as 65002
 neighbor 172.16.2.2 route-map LOCALPREF-R5 in
 neighbor 172.16.2.2 route-map ASPATH out
 no auto-summary
!
route-map LOCALPREF-R5 permit 10
 set local-preference 200
!
route-map LOCALPREF-R4 permit 10
 set local-preference 100
!
route-map ASPATH permit 10
 set as-path prepend 65003 65003
!
```

Bu konfigürasyon adımlarının ardından daha evvel test işlemini gerçekleştirmiş olduğumuz R2 cihazı üzerinden, yeniden R4 cihazı üzerindeki 3.3.3.3 ip adresine erişim denendiği zaman, aşağıdaki ekran çıktısından faydalanarak rota manipülasyon işleminin başarı ile gerçekleştirildiğini ve alternatif yollar üzerinden yönlendirme işleminin tamamlandığını görebilirsiniz.



Şekil69. Rota Manipülasyonu yapıldıktan sonra 2 farklı cihaz üzerindeki iletişimin testi

Rota manipülasyonu işlemi yukarıdaki örnek'de yalnızca 1 Adet internet çıkışı olan fakat 2 farklı lokasyona erişilmesi istenen rotalar üzerinde elle uygulanmıştır.

Rota'ların artırılması, performans artırımı işlemlerinde farklı kombinasyonlar'la BGP protokolü ile MPLS devreleri üzerinden binlerce rota manipülasyonu işlemine tek bir yönlendirici cihaz üzerinden destek vermektedir.

10. SONUÇ

Günümüzde çalışan internet servis sağlayıcı firmaların tamamı, BGP ve MPLS protokolleri ile rota manipülasyonu uygulamasını kullanmaktadır. Fakat gerek cihazların işletim sistemlerinin güncel olmamasından, gerekse bu metod'ların uygulandıktan sonra etkisini internet ağları üzerinden göstermesi uzun zaman dilimlerine sebep olmasından dolayı, tam anlamıyla rota manipülasyon işlemlerinden performans alınamamaktadır.

Bu konu ile alakalı olarak, yetişmiş personel açığı ve ar-ge çalışmalarının yetersiz olmasından kaynaklanan, olumsuz sebeplerden ötürü rota manipülasyonu çalışması dinamik hale getirelemediğinden, bu uygulama alanından tam olarak fayda sağlanamamaktadır.

Bu tez çalışması ile ortaya atılan çalışmanın özünde, rota manipülasyon işlemleri, internet üzerindeki özellikle türkiye'de yaşanan bağlantı sorunlarını farklı rotalar üzerinde daha evvel tanımlanan veya tanımlanmış rotaların hayata geçirilmesinin ardından iletişim devrinde, haberleşme ve bilgiye ulaşma anlamında kesintisizlik veya kesintileri minumum seviyeye indirmek imkanlı duruma getirilmesi amaçlanmış ve test ortamında gerçekleştirilmiştir.

Çalışmanın devamı ve sürekliliği göz önünde bulundurulduğunda, rota manipülasyon işini dinamik hale getirerek, işlevselliği artırmak ve rota değişikliklerinin otomatik olarak devreye alınmasını sağlamaktır.

Bu çalışma sonucunda internet üzerinde ulaşılan veya ulaşılması planlanan rotaların ve kaynakların tamamına eskiye oranla daha kısa yollar kullanılarak internet erişiminin daha efektif kullanılması ve alternatif rotalar üzerinden kesintisizlik sağlanması sonucuna ulaşılmış ve tez amacına uygun bir şekilde test edilerek gerçekleştirilmiştir.

KAYNAKLAR

Internet Society,(b.t.) , Brief History of the Internet. 10.03.2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Internet Society,(b.t.) , History of the Internet,10.03.2013, http://www.internetsociety.org/internet/what-internet/history-internet

ALTUN, A.(29.04.2003). Yurdum Internet'i 10 Yaşında !,10.04.2013, http://www.internetarsivi.metu.edu.tr/10yil.php

Technet, (28.03.2003), How DNS Works , 15.04.2013, http://technet.microsoft.com/en-us/library/cc772774(v=ws.10).aspx

Internet Systems Consortium, (b.t.), 10.04.2013, https://www.isc.org/wordpress/

TürkTelekom,(2013) Kurumsal, Ürün & Hizmetler,25.03.2013, http://www.turktelekom.com.tr/tt/portal/Kurumsal/Urun-ve-Hizmetler

Balchunas, A. (2007). Border Gateway Protocol. 15.03.2013, http://www.routeralley.com/ra/docs/bgp.pdf

Barry M. (b. t.) Brief History of the Internet. 15.02.2013, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

Yumuşak. I. G. (b.t.), Elektronik ticaretin gelişmekte olan ülkelere etkileri ve türkiye üzerine bir değerlendirme, 20.05.2013, http://128.118.178.162/eps/mac/papers/0404/0404032.pdf

CISCO Systems. (23.11.2011). MPLS Label Distribution Protocol, 17.05.2013, http://www.cisco.com/en/US/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-overview.pdf

CISCO Systems. (16.11.2007). Configuring a Basic MPLS VPN, 17.05.2013, http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00800a6c11.shtml

CISCO Systems. (18.07.2012). Border Gateway Protocol (BGP). 20.05.2013, http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html

CISCO Systems. (2013). Enhanced Interior Gateway Routing Protocol. 15.04.2013, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps6630/qa_C67-726299.html

EE6367. (04.2006). Multi-Protocol Label Switching, 18.05.2013, http://www-ee.uta.edu/online/wang/MPLS.pdf

Iptut. (04.04.2011). Simple MPLS GNS3 Lab, 05.04.2013,
http://www.iptut.com/ccip-knowledge/practice-ccip-gns3- lab/simple-mpls-gns3-lab

Karagöl, M. (10.06.2010). BGP.05.04.2013,
http://www.agciyiz.net/index.php/routing/bgp-nedir/

Molenaar, R. (25.06.2010). Basic MPLS, 15.03.2013,
http://gns3vault.com/MPLS/basic-mpls-vpn.html

Rouse, M.(Kasım 2010). Fast Guide to DSL (Digital Subscriber Line). 10.04.2013,
http://whatis.techtarget.com/reference/Fast-Guide-to-DSL-Digital-Subscriber-Line

The Internet Society. (2006). Border Gateway Protocol 4. 05.04.2013,
http://www.ietf.org/rfc/rfc4271.txt

The Internet Society. (1998). RIP Version 2. 05.04.2013,
http://www.ietf.org/rfc/rfc2453.txt

UNCU, A. (11.03.2011). L2 IP/MPLS VPN Servisleri,14.04.2013,
http://www.agciyiz.net/index.php/mpls-wan/l2-ipmpls-vpn-servisleri/

UNCU, A. (11.10.2010). MPLS VPN, 14.05.2013,
http://www.agciyiz.net/index.php/mpls-wan/mpls-vpn/

Whatis.com, (b.t). Computing-Fundamentals, 14.03.2013,
http://whatis.techtarget.com/glossary/Computing-Fundamentals

Wikipedia. (2013). History of the Internet. 05.02.2013,
http://en.wikipedia.org/wiki/History_of_the_Internet

IPNetStudy (22.02.2010) Howto: Setup GNS3,25.05.2013,
http://www.youtube.com/watch?v=DDcRladdpZc

Wikipedia. (01.2013). Multiprotocol Label Switching, 07.02.2013,
http://en.wikipedia.org/wiki/Multiprotocol_Label_Switching

Internet Society (03.2013) Internet Technologies Development,
10.03.2013 http://www.internetsociety.org/what-we-do/internet-technology-matters?gclid=CMrD_e7qpLcCFUld3god50IAVA

Internet Society, (02 2013) What is The Internet ?, 18.02.2013

http://www.internetsociety.org/internet/what-internet/history-internet

ODTU, (01.2013), Türkiyede İnternet Kullanımı, 12.01.2013

http://www.internetarsivi.metu.edu.tr/10yil.php