T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

CISCO PACKET TRACER KULLANARAK AĞ PERFORMANSI DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

Muhammet Emin KAMİLOĞLU
Y1313.010030

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Bilim Dalı

Tez Danışmanı: Yrd. Doç. Dr. Vassilya ABDULOVA

EYLÜL,2015

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1313.010030** numaralı öğrencisi **Muhammet Emin KAMİLOĞLU**'nun **"CISCO PACDET TRACER KULLANARAK AĞ PERFORMANSI DEĞERLENDİRİLMESİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 30/06/2015 tarih ve 2015/13 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul edilmiştir.

Öğretim Üyesi Adı Soyadı	İmzası
Tez Savunma Tarihi :14/09/2015	
1)Tez Danışmanı: Yrd. Doç. Dr. Vassılya ABDULOVA	.....
2) Jüri Üyesi : Prof. Dr. Ali GÜNEŞ	.....
3) Jüri Üyesi : Yrd. Doç. Dr. Hasan TINMAZ	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum “CISCO PACKET TRACER KULLANARAK AĞ PERFORMANSI DEĞERLENDİRİLİMESİ” adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya’da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (14/09/2015)

Aday / İmza

ÖNSÖZ

Bu tez çalışması, ağ performans değerlendirmesinde çeşitli parametreler nasıl bir arada toplanır, incelenir ve sonuç olarak ne gösterir bunu incelemek için pratik bir kılavuz olacaktır. Geniş alan ağı tanımlanmıştır.CCNA ve CCNP eğitim seviyesinde kullanılabilecek temel konfigürasyonlar kullanılacaktır. CCNA : Cisco System firması kendi bünyesinde oluşturmuş olduğu yeni network cihazlarının bakım kurulum onarım gibi alt yapılarının iyileştirilmesi için dünya çapında oluşturduğu bir akademi ağı vardır. Bu ağ içerisinde öncelikli eğitim sırası üniversitelerde daha sonra özel eğitim kurumlarında verilmektedir (Bayrakçı, 2010). CCNP : CCNP sertifikasyon programı, ağ teknolojileri konusunda çalışan kişilerin konularında gerçek bir profesyonel olmasını sağlayacak ileri düzey programdır. Bu programı bitiren kişiler büyük ölçekli organizasyonlarda LAN, WAN ve dial access servislerini kurabilir, gerekli ayarları ve bakımları yapabilir düzeye ulaşırlar. Bu programa katılan kişiler, 500 veya daha fazla şubeli bir LAN ve WAN üzerinde ana omurga ve kenar cihazları voice (ses), kablosuz ve güvenlik bileşenleriyle entegre şekilde çalışması için gerekli ayar ve bakımlarını yapabilecek, gerekli durumlarda sorunları çözebilecek bilgi ve beceriyi kazanırlar (Btegitim, 2012). Bu tanımlar doğrultusun da geniş alan ağı yapılandırılacaktır.

Bir projenin başarısı kendi çabalarınun bir kısmı, büyük ölçüde teşvik ve diğerleri kurallara bağlıdır. Bu projenin başarıyla tamamlanması vesile olan kişilere şükranlarımı sunuyorum. Ayrıca Yrd Doç Dr. Vassilya ABDULOVA motivasyonundan dolayı teşekkür ediyorum. Rehberlik ve destek, bu projenin başarısı için en önemli unsurdu. Bana sürekli destek verenlere yardımları için minnettarım. En önemlisi, ailem olmadan bu mümkün olmazdı. Bu tez benim aileme, yakınlarıma, dostlarıma, sevgi, ilgi, destek ve kuvvet verenlere adanmıştır.

Eylül 2015 Muhammet Emin KAMİLOĞLU

İÇİNDEKİLER

Sayfa

KISALTMALAR

KBIT : KILOBIT
MBIT : MEGABIT
GBIT : GIGABIT
NIC Network Interface Card (Ağ Arabirim Kartı)
SSH Secure Shell (Güvenli Kabuk)
V-LAN Virtual Local Area Netwok (Sanal Yerel Alan Ağı)
PC Personal Computer (Kişisel Bilgisayar)
DNS Domain Name Server (Alan Adı Sunucusu)
DHCP Dynamic Host Configuration Protocol (Dinamik Ana Bilgisayar Yapılandırma Protokolü)
VTP VLAN Trunking Protokol (VLAN Kanal Protokolü)
STP Spanning Tree Protocol
CME Call Manager Express
IT Information Technology (Bilgi-Bilişim Teknolojisi)
SW Switch (Ağ Anahtarı)
RTR Router (Yönlendirici)
CLI Command Line Interface (Komut Satırı Arayüzü)
IP Internet Protocol (Internet Protokolü)
VOIP Voice Over Internet Protocol
MSAU Multi Station Access Unit
LAN Local Area Network (Yerel Alan Ağı)
WAN Wide Area Network (Geniş Alan Ağı)
CSMA/CD Carrier sense multiple access/Collision Detection (Taşıyıcı duyarlıklı çoğul erişim/Çarpışma kontrolü)
ATM Asynchronous Transfer Mode (Eşzamansız Aktarım Modu)
FDDI Fiber Distributed Data Interface
MVRP Multiple VLAN Registration Protocol
PDU Protocol Data Unit (Protokol Veri Birimi)
ISP Internet Service Provider (İnternet Servis Sağlayıcısı)
NAT Network Address Translation (Ağ Adresi Dönüştürme)
ACL Access List (Erişim Listesi)
ROS Router on a Stick
SCCP Skinny Client Control Protocol
DN Dialed Number(Aranan Numara)
RIP Routing Information Protocol(Yönlendirme Bilgi Protokolü)
EIGRP Enhanced Interior Gateway Routing Protocol
IGRP Interior Gateway Routing Protocol
OSPF Open Shortest Patfh First
NTP Network Time Protocol(Ağ Zaman Protokolü)
HTTP Hyper Text Transfer Protocol
ICMP Internet Control Message Protocol(İnternet Kontrol Mesaj Protokolü)

CCNA Cisco Certified Network Associate
CCNP Cisco Certified Network Professional

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

CISCO PACKET TRACER KULLANARAK AĞ PERFORMANSI DEĞERLENDİRİLMESİ

ÖZET

Bu çalışma da bir geniş alan ağı tasarlanmış ve simülasyonu yapılmıştır. Bu ağda kullanılan cihazlar, kablolar, yerel alan ağı topolojisi hakkında bilgiler verilmiş, bu bilgilerin uygulaması olan ağ, Packet Tracer yazılım ortamında benzetime tabi tutulmuştur. Veri iletimi metotları üçe ayrılır: Tekli iletim (unicast), çoklu iletim (multicast) ve yayındır (broadcast). Tekli iletimde veri tek bir hedef adrese, çoklu iletimde veri birden çok hedef adrese gönderilir. Yayın ise verinin ağda bulunan tüm düğümlere iletilmesidir. Bu iletimlerin hepsinde gönderilen tek bir pakettir. Sonuç olarak ağ üzerindeki cihazlar birbirlerine gerektiği şekilde bağlandıktan sonra bir ağ oluşacaktır ve ağ üzerinde her zaman veri iletimi olacaktır. Bunun iletimin nasıl olacağı nasıl bir fiziksel yola sahip olacağı belirlenmiş kurallar çerçevesinde sağlanacaktır.

Anahtar Kelimeler : Yölendirici**,**Anahtar**,**İnternet Protokolü**,**VLAN Kanal Protokolü**,**İnternet Denetim İletisi Protokolü

CISCO NETWORK PERFORMANCE EVALUATION USING PACKET TRACER

ABSTRACT

In this study, a wide area network designed and simulated. These devices are used in the network, cables, provides information about the local area network topology, the application of this information network, Packet Tracer software environment has been subjected in the simulation. Data transmission methods are divided into three: unicast, multicast, and broadcast multiple transmission. Individual data for transmission to a single destination address, sent me multiple messages to multiple destination addresses data. The broadcast is transmitted to all nodes in the network's data. All of these transmissions are sent in a single packet. Consequently, a network will be composed as required after each other connected devices on the network and will always transmit data over the network. How will my message that will be provided in the context of how it would have established rules of physical way.

Keywords : Router**,**Switch**,**Internet Protocol**,** Vlan,Trunking Protocol**,**Internet Control Message Protocol

1. GİRİŞ

Günümüzde bilgisayarları kablolu veya kablosuz olarak birbirine bağlayarak ağ oluşturulabilir. Evimizde kullandığımız bilgisayarı veya bilgisayarları bir ağın parçası olarak düşünebiliriz. Çünkü internette bir ağdır, sadece üzerinde hız sınırlamaları ve kotalar bulunmaktadır. Farklı ağların internet üzerinden birbirleriyle kaynak veya belge paylaşımı yapmasını sağlanabilir. Genel olarak bakıldığında birden fazla bilgisayarı birçok kablo ile birbirine bağlayıp görsel ara yüzler vasıtasıyla ağ oluşturmak mümkündür. Fakat bu hem fazladan fiziksel alan hem gereksiz kablo fazlalığı hem fazladan ara yüz kullanmamızı gerektirecektir.

Bunu gidermek amacıyla anahtarlar (switch) üretilmiştir. Bu anahtarlar sayesinde tek bir ara yüz ile birden fazla bilgisayarı birbiriyle haberleştirip paylaşım yapmalarını sağlayabiliriz. Anahtarlar (yani switch'ler) ağı çakışma (yani collision) domain'lerine ayıran ve layer 2'de çalışan cihazlardır. Üzerlerinde bulunan CAM Table'ları (MAC Adres Tablosu) yardımıyla network içerisinde cihazlar arasında unicast iletişim yaparlar (Yaşar, 2011). Bilgisayarlar NIC(Network Interface Card)'ler aracığıyla RJ-45 konnektörler aracılılığı ile kablolarla switch'lere bağlanırlar ve bu bilgisayarların başka ağlara yönlendirilmesini sağlayan router adı verilen cihazlar vardır. Bu cihazların yönetimi için cihazların başında olmak gerekmez SSH(Secure Shell) protokolüyle uzaktan Telnet yapılarak yönetilebilirler. Telnet; Internet üzerinden farklı bir cihaza bağlanmanıza yardımcı olan metin tabanlı basit bir yazılımdır.

Şekil 1.1 Switch , RJ45 KONNEKTÖR KABLO , ROUTER

Farklı firmalar bu cihazları üretmektedir. Bu çalışmada bu cihazları inceleyebilmek adına Cisco Packet Tracer adlı program ile sanal olarak birebir bu cihazların kurulumunu sağlayıp birbirleriyle haberleşmeleri için gerekli komutlar uygulanarak farklı ağlar birbririne bağlanacaktır.

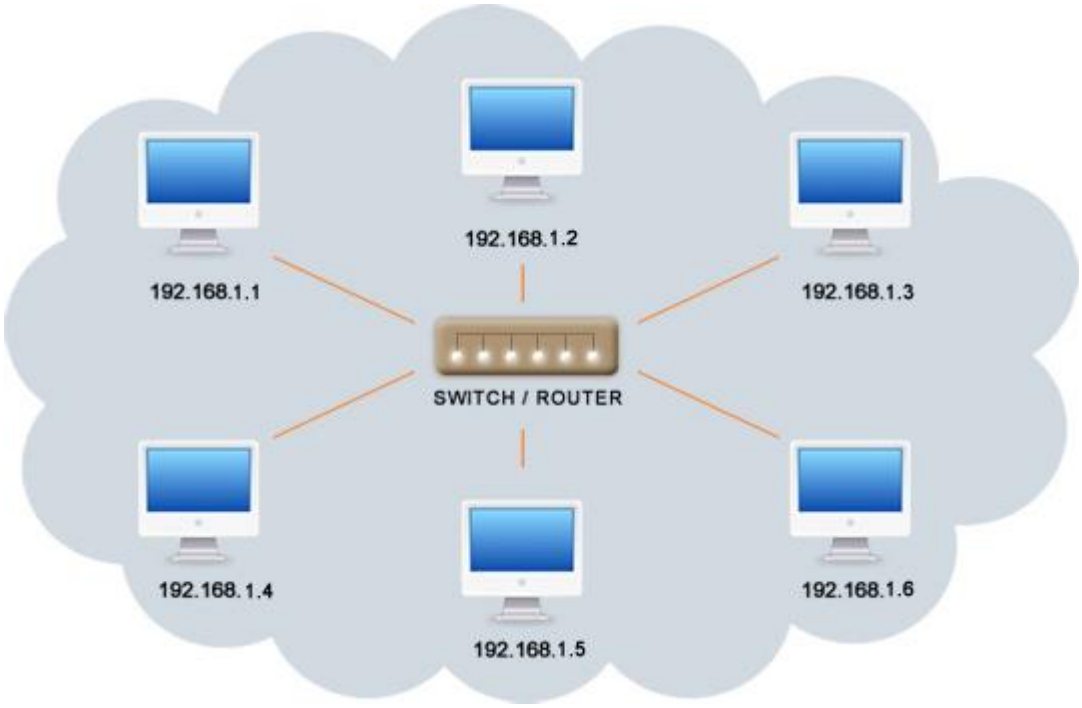
Son olarak yine bu program aracılığı ile ağların haberleşmesini gösteren bir simülasyon oluşturup görsel olarak performansı değerlendirilecektir.

2. AĞ YAPILARI, TOPOLOJİLERİ ve BİLEŞENLERİ

2.1 Ağ Yapıları

2.1.1 Yerel Alan Ağı

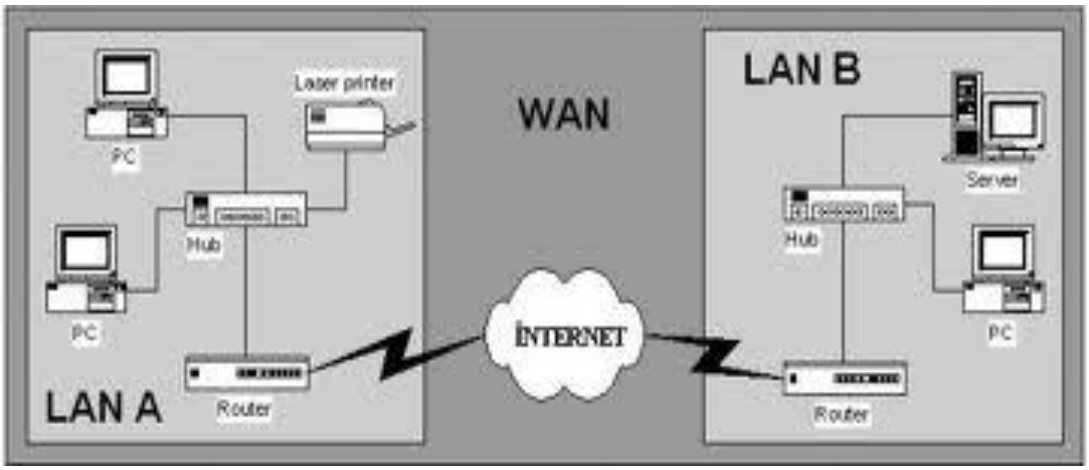
LAN(Local Area Network) yerleşim olarak birbirine yakın olan birden fazla bilgisayarın birbirleriyle bağlanması sonucu oluşan küçük çaptaki ağ sistemine verilen isimdir (**Şekil2.1**). Daha geniş ağların ölçeklendirilmesi için kullanılır. Bilgisayar, yazıcı, mobil aygıt gibi kişisel cihazlar ve bunları birbirine bağlayan anahtarlayıcı (switch) gibi cihazlardan oluşur. Yerel ağlarda Ethernet (10 Mbps), FastEthernet (100 Mbps), GigabitEthernet ve 10 Gigabit Ethernet olmak üzere 4 farklı ethernet hızı vardır (Başkanlığı B. İ., 2013).



Şekil 2.1 Yerel Alan Ağı

2.1.2 Geniş Alan Ağı

Yerel alan ağlarının (LAN) birbirleriyle haberleşmesi geniş alan ağları (WAN-Wide Area Network) ile sağlanır **(Şekil 2.2)**. WAN adından da belli olduğu gibi geniş bir alanda yer alır ve birden çok bağlantı türünün yardımı ile iletim ortamını yerel alan ağlarına sunar. Geniş alan ağı teknolojilerinin yerel alan ağından farklı olarak layer 3 ve layer 2′yi kullanarak iletimi gerçekleştirir. Bundan dolayı yapılandırılması ve hata gidermesi LAN'a göre çok daha zordur (Hoşgör, 2014).



Şekil 2.2 Geniş Alan Ağı

2.1.3 Ağ Topolojileri

Bütün bilgisayar ağları, verinin ağlar arasında gidip gelmesini sağlayan bir yapıya gerek duyar. Aralarındaki bu yapı çoğunlukla kablolarla sağlanır. Günümüzde kablosuz yapılar daha çok yaygınlaşmaya başlamıştır. Ama kablosuz yapılar kablolu yapılara göre çok daha az rağbet görmektedir. Birçok yerel alan ağı barındıran geniş alan ağlarının alt yapıları yinede kablo şeklindedir. Ağı yapılandırmaya başlamadan önce yapılacak en önemli şey ağın yapısının nasıl olacağına karar vermektir. Öncelikle ağın yapısını belirleriz.

Herhangi bir ağ topolojisi bir ağ üzerinde bulunan ağların ve sistemlerin nasıl düzenleneceğini gösterir. Topoloji oluşturmak farklı ağ sistemlerinin yapısını ve çalışma şekillerini anlamada yardımcı olucak ilk basamaktır. Bu ağ içindeki bilgisayarın ya da düğümlerin, düzenlenmiş ve birbirine bağlı olduğunu tanımlar. Ağ topolojisi üzerindeki bilgisayarlaırn yerlerinin nasıl oalcağını, nasıl bağlı olacağını,

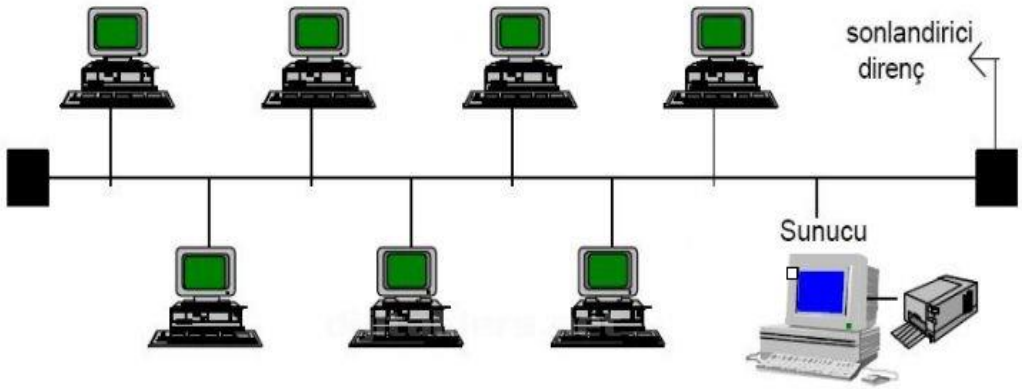
veri iletiminin nasıl yapılacağını sağlayan genel yapıya topoloji denir. Bazı yaygın ağ topolojileri yıldız, halka, karmaşık, doğrusal ve ağaç yapılandırmalarıdır.

Topolojiyi anlayabilmek için en basit yöntem iki değişik ve birbirine bağlı olmayan parçaya ayırarak gözlemlemektir;

- Fiziksel Topoloji : Birbirleri arasında bir ağ yapısı tasarlanmış bir grup bilgisayara bakıldığında gözle görülen yapıdır. Yani kablolar bilgisayarlar arasında nasıl bir bağlantıya sahip, bilgisayarlar birbirlerine hangi yolla bağlanmışlar gibi gözle görülen kısım fiziksel topolojinin ne olduğunu belirler.
- Mantıksal Topoloji : Bilgisayar ağlarının veriyi kabloların bağlantı şeklinden bağımsız olarak nasıl ilettiklerini gösterir.

2.1.4 Doğrusal (Bus) Topoloji

Belirlenmiş bir çizgi doğrultusu üzerinde bilgisayarlar birbirine bağlanır. Bu hattın en başında ve en sonunda sonlandırıcı konnektörler vardır (**Şekil 2.3**). Coaxial kablo ve BNC konnektör kullanılır. Bütün bağlantıların noktası düğüm (node) olarak adlandırılır. Aralarında broadcast bir haberleşme gerçekleşir. Sonuçta bir bilgisayardan gönderilen paketler ağa bağlı bütün bilgisayarlara iletilmiş olur.



Şekil 2.3 Doğrusal Topoloji

Doğrusal topolojinin avantajları :

- Kurulum kablo yapısı açısından güvenlidir.
- Kolaylıkla yeni bir istasyon eklenebilir.
- Merkezde bir birime gerek yoktur.
- Yapıya herhangi bir bilgisayar eklemek kolaydır.
- Kablo uzunluğu çok fazla değildir.

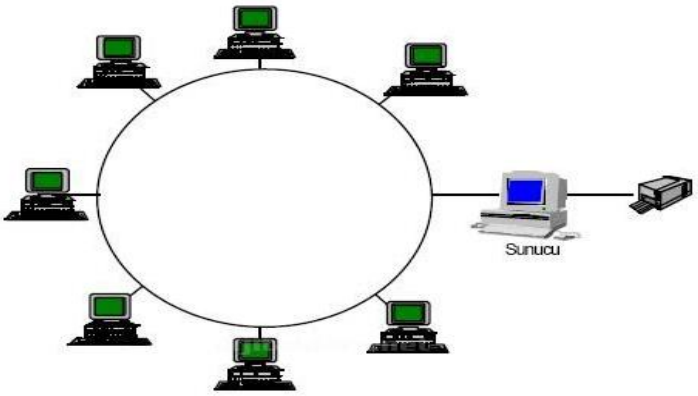
Dezavantajları :

- En fazla 30 adet istasyon bağlanır.
- Networkun uzunluğu ince coaxialde 185, kalın coaxialde 500 metredir
- Eğer bir istasyon arızalanırsa bütün ağ devre dışı kalır.
- Eğer backbone bir kablo da herhangi bir bozukluk veya kesilme olur ise bütün ağın bağlantısı kopar.
- Kablo hattının sonunda sonlandırıcı (Terminator) konnektör olması gerekir.
- Ağda bir sorun olduğu zaman sorunun nerden kaynaklı olduğunu bulmak zaman alır.
- Genellikle yanlız bütün bir binanın ağ yapısı olarak kullanılmaz.
- Çakışma (Collision) çok fazla olur.

Çakışmayı bulmak (Collision Detect) : Bir ethernet kartı veri yollayacağı an ağdaki trafiği kontrol eder. Eğer ağ kablosun üzerinde veri yok ise veriyi kablo üzerine bırakırlar. Kablo üzerinde veri var ise kablo üzerinde olan veri hedefine ulaşıncaya kadar bekler. Daha sonra üzerindeki datayı yollar. Bunlar başarısız olduğu takdirde collision oluşur (Aslantaş, 2013).

2.1.5 Halka (Ring) Topoloji

Mantıksal bir yapı olarak daire şeklinde tüm nodeların birbirine bağlanması halinde oluşur(**Şekil 2.4**). Tüm bilgisayarlar ağı oluşturan ve halka şeklinde dolaşan bir kabloya bağlıdırlar. Günümüzde halka topolojilerinde UTP, STP kablo kullanılmaktadır.



Şekil 2.4 Halka Topoloji

Halka Topoloji avantajları :

- Eğer ağ büyütülürse, ağdaki toplam sistem performansını pozitif yönde etkiler.
- Ağdaki bütün istasyon ağa eşit erişim hakkına sahiptir.

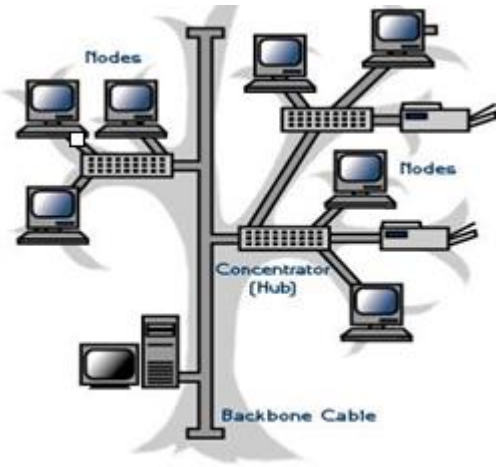
Dezavantajları :

- Topoloji çeşitleri arasında en pahalısıdır.
- Karmaşık bir yapısı vardır.
- Eğer bir istasyon arızalanırsa bundan bütün istasyonlar etkilenir.

Halka topolojisi genellikle twisted pair ve fiber optik kablo tipleri kullanır. Bu toplojiye en uygun protokol Token Ring'dir (Arısüt, 2009).

2.1.6 Tree (Ağaç) Topoloji

Star topolojsine sahip ağları birbirine bağlayarak oluşturulur. Yıldız topolojisine sahip ağlar böyle dahada büyütülebilir (**Şekil 2.5**). Tree yapısının dallarında değişik topolojilerin ağlarını görebiliriz, tree gövdeside bu ağları birbirlerine bağlar. Bus topolojisinin ile star topolojinin karakteristik yapısının karışımı şeklinde böyle bir topoloji ortaya çıkmıştır.



Şekil 2.5 Ağaç Topoloji

Ağaç Topoloji Avantajları :

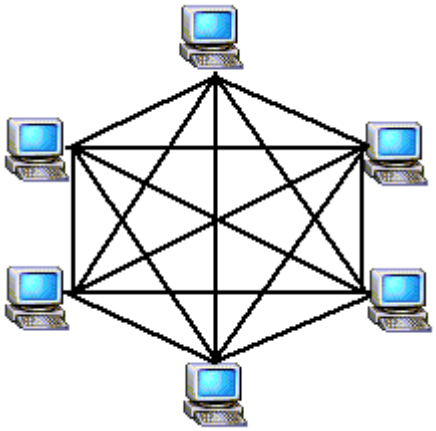
- Bütün ayrılan parçalar için point to point bir kablolama türü kullanılırlar, böylece ayrılan parçalarda bir kesinti olursa diğer parçalar etkilenmemektir.
- Birbirinden farklı yazılım ve donanım üreticileri ürettikleri ürünler birbirleriyle uyumlu olarak bu yapıda çalışabilirler.

Dezavantajları :

- Kabloların tiplerine göre her ayrılan parçanın ortalama uzunluğu belli bir sınırda kalır.
- Eğer trunk yapısın da bir kesinti olur ise bütün network çalışabilirliğini kaybedebilir.
- Toplojiler arasında Kablolama türlerine göre en zor konfigürasyona sahip topolojidir. (Aslantaş, 2013).

2.1.7 Mesh (Karmaşık) Topoloji

Bütün noktaların birbrilerine bağlanıldığı çok güvenli ağ yapısı olan mesh yerleşik düzeni tam olarak ya da biraz oluşturulur (**Şekil 2.6**). Karmaşık yapıya genelde rastlanmaz. Genelde geniş alan ağlarında kullanılır. Karmaşık topoloji de bütün nodelar network üzerinde birbirlerine bağlıdırlar. Yerel alan ağlarında kullanıldığında tüm noderların birbirlerine bağlı bir yapı zorunlu değildir.



Şekil 2.6 Karmaşık Topoloji

Karmaşık Topoloji Avantajları :

- Bütün istasyonların kendi başına diğer istasyonlarla poitn to point bağlantısı kurulduğundan, multiple bağlantı oluşur, eğer bir bağlantı koparsa, diğer bağlantılar sinyalin hedefe gidebilmesi için kullanılır. Bu da bu topolojinin en önemli avantajıdır.

Karmaşık Topoloji Dezavantajları :

- Mesh networkde az miktarda node bulunan yapılarda ve ağ ortamının boyutu küçük ise ortaya çıkan bağlantı miktarı çıkar ve bundan dolayı ağ hızının yavaşlar (Aslantaş, 2013).

2.1.8 Yıldız (Star) Topoloji

Yıldız topolojisi, bütün cihazların (Serverlar, istasyonlar ve öteki çevre birimlerin) merkezi konnektörlere (switch veya hub) doğrudan bağlantısı ile oluşan topolojidir (**Şekil 2.7**). Gönderilen data, hedefindeki adrese gidebilmek için switch veya hub üzerinden geçerek gider. Hub veya switch networkun bütün fonksiyonlarını yönetebilir ve kontrol edebilir. Ek olarak yıldız topoloji kullanılan ağda bir repeater/sinyal güçlendirici benzer çalışırlar.

Şekil 2.7 Yıldız Topolojisi

Yıldız topolojisinin avantajları ;

- Yeni bir istasyon kolaylıkla eklenebilir.
- Hatalar kolay tespit edilebilir ve yönetimi basittir. Ayrıca fazla zaman almaz.
- Farklı kablolama metotları ile birbirine bağlanabilir.
- Bir istasyonda arıza olursa veya yeni bir birim eklenirse bütün ağ bu durumdan etkilenmez.

Dezavantajları ;

- Diğer toplojilere göre kablo ihtiyacı fazladır.
- Hub veya Switch ‘de herangi bir problem olduğu zaman bütün ağ etkilenir.
- Hub ve switch kullanıldığı için, bus topolojiye göre maliyet daha yüksektedir.

Twisted pair ve fiber optik kablo türleri günümüzde yaygın olan bu topoloji de kullanılır. Bu topolojinin yaygın olarak kullanılan protokol tipleri Ethernet ve Localtalktur. (Arısüt, 2014).

Genel olarak yıldız topoloji kullanılır. Bu yüzden bu çalışmada bu topoloji kullanılacaktır.

2.2 Ağ Teknolojileri ve Mimarileri

2.2.1 Ethernet

Ethernet mimarisi, IEEE 802.3 standardına dayanır. Bu ise, bir ağ CSMA/CD erişim yöntemini kullanır. CSMA/CD'de client bilgisayarlar, veriyi iletmek için önce hangisini ve sonra hangisinin gideceğinin sırasını, ağın topolojisine göre belirlerler. Ethernetler, beraberinde iletişim ve kablo hızına göre de sınıflara ayrılırlar. 1000 Mbps hız ile haberleşebilenler Gigabit Ethernet, 10 Mbps hız ile haberleşebilenler Ethernet, 100 Mbps hızıyla haberleşebilenler Fast Ethernet olarak adlandırılır. Ethernetin genelde kullandığı iki topoloji vardır. Bunlar; mantıksal veri yolu ve yıldız topolojisidir. Ağ büyüdükçe hiyerarşi düzenine gelir. Bu ağ genel olarak hız 100 Mbps kadardır. Yeni getirilen standarda göre 1 Gbps hızına kadar çıkarılabilir.
Herhangi bir network içindeki bilgisayarlar ortak kullanılan taşıyıcı hat üzerinde birbirleriyle iletişimlerini kurarlar. Birden fazla bilgisayarın bulunduğu bir ağda, bilgisayarların aynı zamanda veri iletiminde bulunması collision olabileceğinden başarılı bir data iletimi olmayacaktır. OSI modelinde 2. Katmanın da çalışan CSMA/CD protokolü bu çakışmayı engellemek için kullanılır. Data iletmeye başlamak isteyen bilgisayar, öncel networku kontrolden geçirir. Ağ boş ise frame gönderebilir. Ağ boş değil ise hattın boşta kalmasını bekler. Frame iletimi yapılırken collision olursa, frame yollayan bilgisayar, ağ üzerindeki öteki bilgisayarlara "jam" sinyali yayınlar ve buda networkde çakışma oluştuğunu gösterir (Yıldırım, 2010).

Hat Dinleme (Carrier sense) : Ethernete bağlı bütün bilgisayarlar aynı zamanda hattı dinler ve hattın boş olduğunu gördükten sonra paketi hedefine yollar. Ama aynı zamanda birden fazla bilgisayar hattı dinler ve aynı zamanda paketi gönderir ise hatta çakışmalar olabilir.
Ethernet Türleri :

Çizelge 2.1 Ethernet Türleri

Ethernet Türü	Kablo Tipi	Veri Hızı	Standart Mesafe
1000BaseT	CAT5 , CAT6	1 Gb/Saniye	100 m
1000BaseCX	Twinaxial	1 Gb/Saniye	25 m
1000BaseSX	Fiber optik	1 Gb/Saniye	500 m

1000BaseLX	Fiber optik	1 Gb/Saniye	5000 m

2.2.2 Token Ring

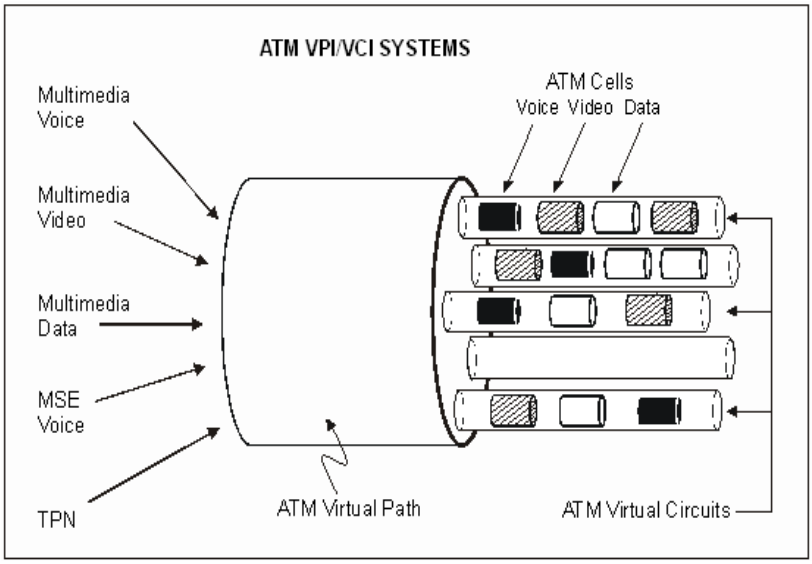
Bu yapı, token passing erişim yöntemini kullanır ve IEEE 802.5 standardındadır. Bu networkler star topoloji gibi yapılandırılırlar. Bilgisayarlar merkezde bir huba bağlı olarak çalışırlar. Fakat bilgisayarlar bir ring üstüne yerleştirilmiş gibi birbiriyle ardışık haberleşme sağlarlar. Bu mantıksal olarak halka diye adlandırılır. Bu halka ağlar fiziksel olarak bir yıldız toploji ağ görünümündedir. Ancak mantıksal olarak bir halka topolojiyi andırır. Bütün pc'ler MSAU (merkezi bir birime) bağlıdır. Bu bütün istasyonlardan alıp sinyalleri bir sonraki istasyona aktarıp haberleşmeyi sağlar.

İlk tokenın ağ üzerinde dolaşmaya başlaması bir pc veri iletimine başladığında sağlanır. Network üstünde sadece bir adet token aynı zamanda dolaşır. Data iletmek isteyen pc'ler kendi tokenını network üzerine göndererek verisinin iletimini sağlar. Veriyi alacak olan bilgisyarlar veri paketini yakalarlar. Bunun peşinden yeni bir token ağ üzerinde dolaşmaya başlar. Token Ring ağlar orjinalde 4 Mbps'dir. Ama günümüzde kullanılan Token Ring ağlar 16 Mbps hızındadır. Bu ağlarda ağa erişebilecek sonraki bilgisayar belirlidir. İstasyon tarafından döngünün hangi yönde olacağı belirlenir. Çakışma olamaz. Bundan dolayı Ethernete göre sistematik bir network şeklindedir. Modern, Token Ring networklerde STP ve UTP kablolarla kullanılmaktadır (Çubukçu, 2012).

2.2.3 Asynchronous Transfer Mode(ATM)

53 byte sabit büyüklükte hücreler halindeki verleri ileten bir ağ türüdür. Temeli bağlantıya dayanan bir teknolojidir. Paket anahtarlamanın türü sayılan cell relay tekniğini veriyi iletimek için kullanılır. Devre anahtarlamanın avantajlarından sanal devreler oluşturarak hücre aktarımı tekniği de faydalanabilir. Paket anahtarlamada olduğu gibi; örnek olarak, Frame Relay, X. 25, ATM çoğullama, TCP/IP ve anahtarlama işlevlini bütünler, patlamalı trafiğe göre uygundur, devre anahtarlama uygun değildir ve değişik hızlarla çalışabilen aygıtların haberleşmesine müsaade eder. Fakat paket anahtarlamaya göre, ATM yüksek performanslı çoklu ortam networklere göre tasarlıdır (**Şekil 2.8**). Yerel ağlarda kullanışı kısıtlı olan, yaygın

olarak genelde haberleşme ve pc networkleri arasında hızlı omurga yapısı oluşturabilmek için kullanılır.



Şekil 2.8 ATM Bağlantı Modeli

Bu ağlar bağlantı temelli olduğundan, pc'lerden biri veri iletişimini başlatabilmek için öncelikle bağlantı kurulumu için gerekli paketi gönderir. Bu paket ihtiyaç duyduğu kaynaklar ile alakalı ve geçtiği ATM anahtarlarına bağlantının varlığı hakkında ve bilgilerin kaydolmasınıyla ilgilenir. Bağlantının sanal devre yol bilgisi de sanal yol olarak adlandırılır. Eğer bağlantının ağ üzerindeki ihtiyacı geçici değilse, bilgiler sürekli anahtarlama tablolarının üzerinde tutulur. Böyle devamlı bağlantılar kalıcı sanal devre olarak adlandırılır. Bütün bağlantıların sadece kendilerine has kimlik bilgileri bulunur. İki tarafta bağlantı kurulduğu vakir hemen veri gönderme işlemi yapabilir. Bu veriler 53 byte'lık yani 5 byte başlık ve 48 byte bilgi şeklinde celllere dönüştürülür. Başlık bağlantının kimliğinide içerir, bu nedenle Bu anahtarlar aldığı hücrelerin nereye iletecekleri anlarlar. Bundan dolayı tüm hücreler aynı yoldan giderler. Celller belirli bir şekilde sıra takip etseler bile, celllerin hedefine ulaşıp ulaşmadığı genel olarak kontrol edilmez.

2.2.4 FDDI(Fiber Distributed Data Interface)

Günümüzde kullandığımız optik fiber kablo aracılığıyla yüksek hızla çalışabilen (100 Mbpsnin üstünde) token ring LANlarıdır. Çift kablolama tekniği bu kablolamada kullanılır. Yani bir tarafı saatin yönün de iletimi yapar iken diğer tarafı saate tam tersi yönde iletim yapar. A ve B sınıfı olarak iki adet istasyon çeşidi bulunur. A sınıf istasyon çeşitleri çok önem taşıyan dataların iletimini sağladığından iki fiber

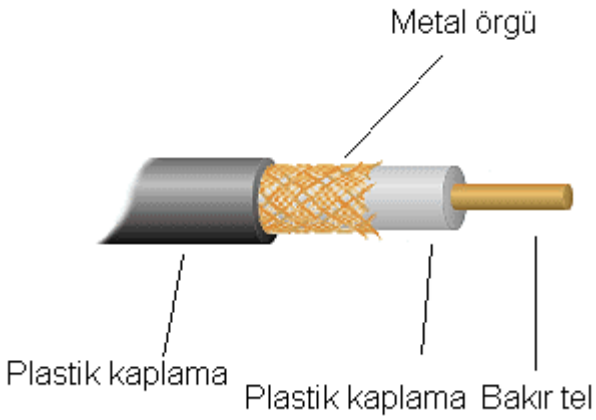
kabloyada bağlanmalıdır. B sınıf istasyon çeşitleri ise fiber kablolardan bir tanesine bağlanmalıdır. IEEE 802.5 Token Ring ve FDDI arasında fark bulunur. 802.5te herhangi bir istasyonun gönderdiği paketin gideceği yere gidene ve geriye dönene dek yeni token üretemezler fakat FDDIda istasyonda yeni token üretilmesi için eski tokenın geriye denmesini beklemesine gerek kalmaz.

2.3 Ağ Bağlantıları

Günümüzde bilgisayar ağlarında kullanılan kablo tipleri 3 çeşittir. Bunlar; koaksiyel (coaxial) kablo, çift burgulu kablo (twisted pair cable) ve fiber optik (optic fiber) kablodur.

2.3.1 Koaksiyel kablo

Coaxial kablo elektro manyetik kirlilik fazla olan ortamlar da az güçte sinyallerini iletebilmek için geliştirilen kablo türüdür (**Şekil 2.9**). Bu kablo türü birçok alanda kullanıabilir. Bunun yanında ses ve video iletimindede kullanılır.



Şekil 2.9 Koaksiyel kablonun yapısı

2.3.2 Çift Burgulu Kablo (Twisted-Pair Lines)

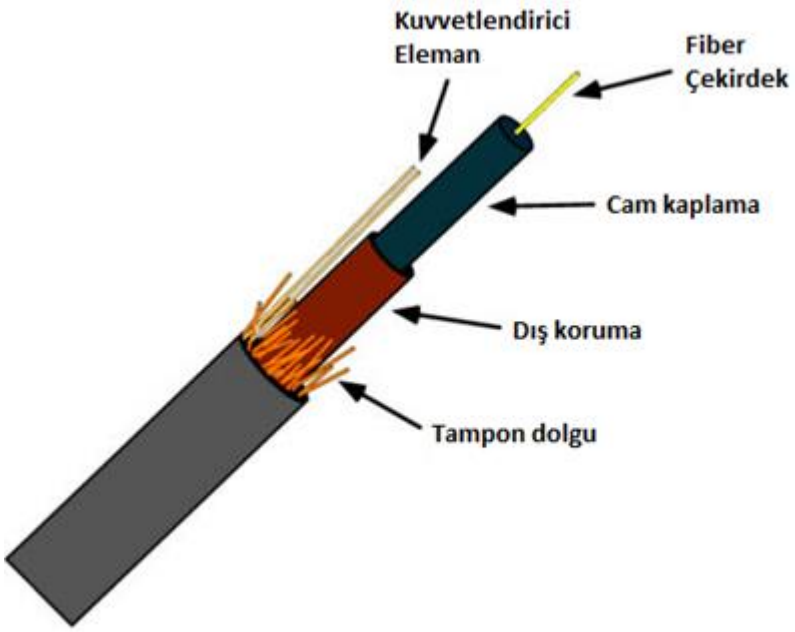
Çift burgulu kablo le yaplın kablo bağlantısı genelde LAN için en çok kullanılan ve en basit yöntemlerdendir. Bu kablolarda birebir aynı izolasyon maddelesiyle kaplanmış tel çiftlerinin birbirine sarılması ve helezonik olarak döndürülmesiyle oluşur (**Şekil 2.10**). Bu kabloların bükülerek sarılması gürültünün azalmasını sağlar. Bu tür kabloların bundan dolayı iki telli açık hatlara göre yapay gürültü (parazit,hata)

sinyallerine karşı dirençleri yüksektir. Bir gürültü sinyalini iki hat tarafındanda toplanması, yani fark sinyalinin yaptığı etkinin azalması sinyal ve toprak hatlarının birbirine yakınlığından kaynaklanır. Kablo içindeki her çiftin bükülmesinin çapraz bağlantıyı azaltmasının nedeni aynı kablo içerisinde birkaç tane bükülmüş çift olmasıdır (Güler, 2008).

Şekil 2.10 Çift Burgulu Kablo

2.3.3 Fiber Optik Kablo

Günümüzde internet erişimde en ileri son kullanıcı teknolojisi fiber optik kablolardır. Datayı ışığın darbeleriyle saydam bir hat içerisinden iletir dersek en basit şekliyle anlatmış oluruz. Optik fiber teknolojisi çalışması ışığın değişik yoğunlukta olan ortamların arasında geçiş yaparken kırılmasıdır. Ortamlar arasında yoğunluğun farkı ve ışığın gelişinin açısı gerektiği kadar yüksek ise ışık bulunduğu ortamdan daha düşük yoğunluktaki ortama geçmez sadece geriye yansıma yapar. Plastik fiber hattının etrafına iletken cam veya daha düşük kırılma indisi olan kaplama yapılırsa eğer bu çalışma şekli kullanılarak, ışık içerdeki fiber hattının içeirisinden çıkamaz ve fiber hattının içindeki duvarlardan yansıyarak ilerler. Bu hatların yapısı en iç tarafta cam veya plastik den yapılmış, yarıçapı mikrometrelerle ölçülecek şekilde olan iletim kısmı bulunur (**Şekil 2.11**). Bu parçalar iletim için yeterlidir; ama fiber optik kabloyu fiziksel etkilerinden koruyabilmek ve dayanıklı olabilmesi için en dışa koruyucu belli bir katman eklenir. Her iki uca da fiber optik arayüzü girişleri bağlanır. (Badur, 2013).



Şekil 2.11 Fiber Optik Kablo

2.4 Ağ Bileşenleri

Günümüzde ağ cihazlarının amacı ağ bandını genişletmek ve bilgisayarların birbiriyle iletişimini sağmaktır.

Temel olarak ağ cihazları şunlardır;

2.4.1 Hub

Basit ağ cihazlarındandır. Kendine ait bir güç kaynağı vardır ve bundan beslenerek çalışır. Network sistemlerde sinyallerin yeni baştan oluşturmasını ve yeni baştan zamanlamasını yapar. Bu cihaza bağlanan pc'lere birbirleriyle paylaştıkları bir yol verir. (Bütün portlara kendine gelen veriyi gönderir.) Yani aynı zamanda haberleşme yapmak isteyen ağa bağlı aygıtların, hattın boşta kalmasını beklemesi gerekmektedir. Üzerinda 8 ve 24 sayıları içinde değişken port sayısı bulunduran aygıtlardır. Hub'lar network yapılarda genelde merkezde bir nokta oluştururlar ya da o networkun güvenliğinin arttırılmasına benzer amaçlarlada kullanabililer. OSI modeli üzerinde 1. katman cihaz olmalarının nedeni bit seviyesinde işlem yapmalarındandır. Bu cihazlar için iki çeşit sınıflandırma yapılır; Yani Hub aygıtlar genelde pasif ya da aktif olarak

iki grup şekline incelenirler. Pasif olanlar gelen sinyali güçlendirmeksizin çok kullanıcılı ortam için bölerler, aktif olanlar gelen sinyali güçlendirip çok kullanıcılı ortam için bölerler. Bu yüzdem pasif göbekler kablo uzunluğunu arttırmak amaçlı kullanılmazlar (Dikici, 2013).

Şekil 2.12 Hub

2.4.2 Repeater

Repeaterlar, herhangi bir ethernet ayrılmış parçasından aldığı elektriksel veriyi yeniler ve binary koda dönüştürerek diğer ayrılmış parçalara iletir. Bundan dolayı repeater, hem elektriksel olarak bozulmuş sinyallerin iyileştirilmesinde, hem de sinyal gücünün arttırılmasında rol alır. Repeaterlar, mikrodalga, telgraf, optik haberleşme, telefon benzeri birçok sistem üzerinde kullanılır. Bunlarında OSI modelinde 1. katman cihazlar olmasının nedeni hublar gibi sadece bit seviyesinde işlem yaptıklarındandır (Dikici, 2013).

Şekil 2.13 Repeater

2.4.3 Switch

Switch cihazlarıda hub görevi gibi bağlı pc'lerine yol sunar. Anahtarlamalı olarak yol sunmaları hub cihazlarından farkıdır. Ağın içerisindeki 2 pc birbiriyle haberleşmek isterlerse anahtarlama özelliği olduğundan dolayı diğer pclerle de iletişimi sağlayabilirler. Bu yüzden hub cihazlarına göre daha fazla yüksek performans gösterirler. Bu cihazlar 8 ve 48 sayıları içinde değişen port sayısına sahiptir ve şaseli modelleride bulunur. Eğer şaseli anahtarlar kullanıyorsak gerekiyorsa port ekleyebiliriz. OSI modelinde bu cihazlar 2.katman cihazlardır. İletecekleri paketlerin MAC adreslerine bağlı çarpışma alanlarını ayırırlar ve MAC adreslerine göre yönlendirirler (Dikici, 2013).

2.4.4 Router

Yönlendirici yönetilebilir ve gerekli konfigürasyonlar yapıldığı zaman uzaktaki herhangi network erişebilmek istediğinde o an bulunan bir den çok yol arasından kullanılabileği Best Determination Path (en iyi yolun) seçebilirler. Routerlar, bütün ağları ya da ağ parçalarını birbirine bağlarlar. OSI modelinde 3.katman cihazlardır. Buna rağmen gereken interface modülü kullanılırsa OSI modelinde 2.katmanda çalışabilen ayrı 2 network aygıtınıda birbirlerine bağlar. Yalnız network adresinin bildği verinin aktarılımına onay verirler bu sayede network trafiğinide azaltmış olurlar. Genelde statik routerlar ve dinamik routerlar olmak üzere 2ye ayrılır. Statik routerlarda yönler elle şekillenir ve hep aynı yön kullanılır. Statik routerlar, dinamik olanlara göre daha güvenlidir. Dinamik routerlarda, rotalar otomatik olarak şekillenir ve veri için en iyi yönü router seçer. Dinamik routerlarda güvenliği arttırmak için elle şekillendirme yapılır (Dikici, 2013).

3. CISCO PACKET TRACER

Ağ sistemleri ile çalışan her insanın takıldığı zaman yardımına en başta faydası şey ağ simülatörleridir. Çünkü bir anda routerları, switchleri hemen bağlayabilecek laboratuvar ortamı oluşturmak mümkün olmayabilir, eğer olmuş olsa bile her zaman gerekli değildir. Günümüzde artık bunu test edecek sanal yazılımlar oluşturulmuştur. Bunlardan biride Cisco firmasının geliştirdiği ve ücretsiz olarak kullanıcıların hizmetine sunduğu Packet Tracer adlı programdır. Kolay bir kullanımı vardır, görsel ara yüzü sayesinde topolojinizi sürükle bırak yöntemiyle rahat bir şekilde oluşturabilirsiniz.

Cihazlarda istediğiniz şekilde ara yüzleri basitçe eklersiniz ve çıkarabilirisniz ve ara bağlantıları da cihazları seçerek basitçe belirleyebilirsiniz. Cihazların UP&Running (yani çalışır durumda) olup olmadığını anlamak için ping komutu yazmanıza bile gerek kalmaz, bir zarf resmini cihazlar üzerine tıklayıp ping atmanızı sağlıyor. Test edilmesi gereken hemen hemen tüm ağ ekipmanlarını ve bağlantıları da destekliyor.

Cisco Packet Tracer programı, hiç bir fiziki makine veya araç kullanmadan Cisco işlemlerinin veya uygulamalarının yapılmasının sağlayan ve bize adeta bir ağ laboratuvar ortamı sunan bir simülasyon programıdır. Lan routing uygulamalarının çoğu bu simülasyon programı yardımı ile gerçekleştirilebilir .

Cisco Packet Tracer programının avantajları şunlardır:

- Rahat ve iyi bir şekilde öğreneceğiniz ortamı sağlar.
- Birden fazla kullanıcılı, real time(gerçek zamanlı) eğitim laboratuvarı sağlar.
- Öğrenciler için sınavlar hazırlanabilir ve yaptıklarına göre puan verilmesini sağlar.
- Sanal ekipmanlar kullanılarak network ortamı tasarlanır ve network cihazları yapılandırılır

Yazılımın kurulumunun düzgün olması ve cihaz üzerinde çalışabilmesi için aşağıdaki minimum sistem gereksinimlerinde bilgisayara ihtiyaç vardır. Ayrıca önerilen sistem

gereksinimleri kısmındaki referansa göre bir bilgisayara yüklenecek olursa daha az sorunla çalışacaktır (Şanlı, 2013).

Minimum sistem gereksinimleri :

Çizelge 3.1 Cisco Packet Tracer Minimum Sistem Gereksinimleri

İşlemci :	Intel Pentium III 500 MHz veya üstü
İşletim Sistemi :	Microsoft Windows XP, Microsoft Windows Vista,Microsoft Windows 7, Fedora 11, or Ubuntu 8.04 LTS
RAM :	256 MB boş alan
Sabit Disk :	256 MB boş alan
Ekran Çözünürlüğü :	800 x 600
Ek Yazılım :	Adobe Flash Player

Önerilen sistem gereksinimleri :

Çizelge 3.2 Cisco Packet Tracer Önerilen Sistem Gereksinimleri

İşlemci :	Intel Pentium III 1.0 GHz veya üstü
RAM :	512 MB
Sabit Disk :	300 MB boş alan
Ekran Çözünürlüğü :	1024 x 768
Ek Yazılım :	Ses kartı ve hoparlör, İnternet bağlantısı (Çok kullanıcı özelliği kullanılacaksa)

Programın basit bir kurulumu vardır. Yükleme sihirbazını açıp, lisans sözleşmesini kabul ettikten sonra kuracağımız yeri bilgisayar içinde seçeriz ve kurulumu tamamlarız.

4. AĞ HARİTASININ OLUŞTURULMASI ve KURALARIN BELİRLENMESİ

Yukarıda da belirtildiği gibi öncelikle ağ haritasını oluşturulacak ve daha sonra ağ üzerinde olacak kurallar belirlenecektir. Harita üzerinde birbirinden bağımsız ama gerekli araçları birbirine bağlı farklı V-LAN'lar oluşturulacaktır.

4.1 V-LAN :

Netwokde switch üzerindeki portları gruplandırarak her bir grubun sadece birbiri arasında ieltişiminin sağlanması VLAN olarak adlandırılır. Portların gruplanmasıyla bir switch üzerinde birden fazla ağ anahtarı varmış gibi davranabilir. Network genişledikçe ve network trafik çoğaldıkça VLAN'a ihtiyaç duyulur. VLAN broadcast sınırlandırarak trafiği azaltır. Bundan dolayı farklı VLAN'lar üzerindeki cihazlar birbirlerine veri gönderimi yapamazlar ve birbirlerinden veri alamazlar. Yani farklı VLAN grubundaki cihazların IP'leri aynı olmasında bir sakınca yoktur. Farklı VLAN'lar birbirleriyle haberleşemedikleri için birbirlerinin çalışmalarını etkilemezler. Herhangi bir port farklı iki VLAN içerisinde olmasında bir sakınca yoktur. Bununla iki VLAN trafiğinide alabilir. Fakat gelen veriyi hangi VLANdan alıyorsa, yalnız veriyi aldığı VLAN grubuna dağıtır. Ne kadar içinde bulunsada halde diğer VLAN grubu o veriyi alamaz.

VLAN ağ üzerindeki kullanıcılar ve kaynaklar bir SW üstündeki portlara bağlanıp yapılır ve mantıksal bir grup oluşturur. VLANlar üstünden subnetler ya da yayın domainleri oluşturulabilir. Yani yayın yapılan alan sadece aynı VLAN içindeki portlardır. VLANlar üzerindeki, kaynaklar ve kullanıcılar düzenine bakılmadan, yerleşime, işleve, departmana ya da kullanılan uygulama protokolüne göre düzenlenir. 2. katmanda çalışan ağlarda, gerekli olsun yada olmasın her yayın paketi ağ üzerindeki her cihaz tarafından görünebilir. Bunun haricinde bütün kullanıcılar network üzerindeki her cihazada ulaşabilirler. Bunun güvenlik sorunu oluşturması

muhtemeldir. Sonuçta VLANlar sayesinde layer 2 ağlarındaki birçok sorun çözülür (Eryol, 2002).

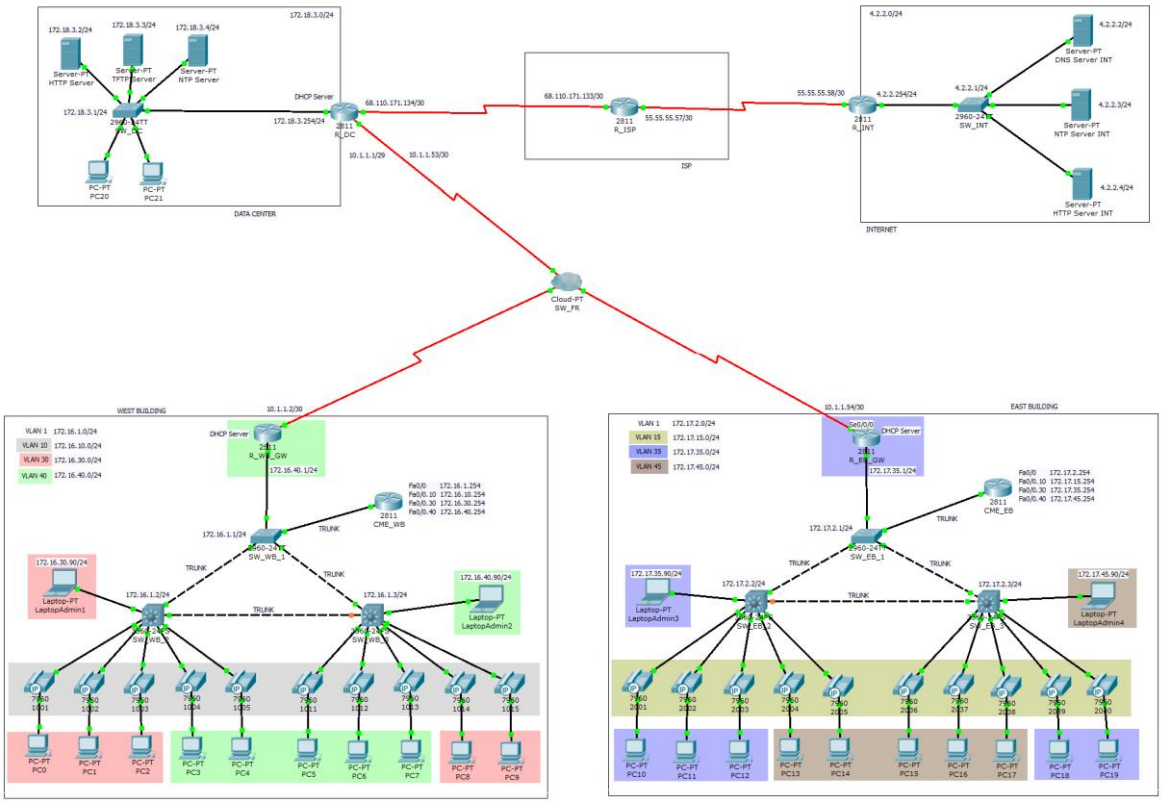
VLAN, LAN üzerindeki network kullanıcılar ve kaynaklar mantıksal bir şekilde gruplandırılır, değişik yayın domainlere ataması ve network aygıtları üzerine farklı portlara ataması ile yapılır. VLAN olan bir ağ üzerinde, VLANda olan kullanıcıların yanlız kendi yayın domainine sahip olduğundan, birbirleriyle iletişim kurabilirler.

Oluşturulan farklı bir VLAN üzerinde bulunan kullanıcılar ile kesinlikle haberleşme yapamazlar. Geniş networklerde bu yüzden VLAN ihtiyacı belirmiş ve ağ Mühendislerini çok kalabalık işlerden yardımcı olmuştur. Ağda bir cihaz OSI 3. katmanda çalışıyorsa, herhangi VLAN'a üye network kullanıcısının değişik herhangi VLANa üye network kullanıcısı ile iletişimi sağlanır.

Cisco Systems'in ürettiği Layer-3 sw'ler, yönlendirici modun da çalışabildikleri için bunu yapabilirler. VLAN adaptasyonundan sonra yayın trafiği azalır ve bandwith artıtırılır.

4.2 Ağ Haritası

Bu çalışmada konfigürasyonu yapılacak ağ haritası aşağıdadır ;



Şekil 4.1 Ağ Haritası

Harita üzerinde 4 adet layer2 switch , 4 adet layer3 switch , 7 adet router , 22 adet pc 2 adet HTTP , 2 adet NTP , 1 ader TFTP , 1 adet DNS Server ve 1 adet cloud bulunmaktadır. Bu cihazların ne olduğunun ve görevlerinin ne olduğunun konfigürasyon yaptıkça sırası geldikçe açıklanacaktır.

4.3 Ağ Kuralları

Belirlenen ağ kuralları aşağıdadır ;

1. SW'lerin IP blokları haritada belirtilmiştir. Bu şekilde konfigürasyonu yapılmalıdır ve bütün cihazlara haritadaki gibi isimleri verilmelidir.

2. TRUNK olacak portlar harita belirtilmiştir bunlar bu şekilde yapılandırılacaktır. Haritada VLAN'lar belirtilmiştir. WB için VLAN 10, VLAN 30, VLAN 40 VE EB için VLAN 15, VLAN 35, VLAN 45 olacaktır. İsimleri sırasıyla DATA1_WB, DATA_WB, VOICE_WB, DATA1_EB, DATA2_EB, VOICE_EB olacaktır. VTP domain kurulacaktır. WB için domain adı 'WB', EB için domain adı 'EB' olacaktır ve şifreleri '1234' olacaktır. PC'lerin hangi VLAN da olacağı renklerle belirtilmiştir. SW'lerin arabirimlerini buna göre yapılandırmak gerekecektir.

3. SW_WB1 ve SW_EB1 root SW olacaktır. VLANlar bu SW üzerinde oluşturulacaktır. Layer3 SW'ler client olacaktır. SW'ler STP yapısı olacaktır.

4. VLAN'lar için CME Routerlar üzerinde Rouer-on-a-stick yapısı oluşturulmalıdır ve aynı router üzerinde Cisco ip telefonları için CME oluşturulmalıdır yani VOIP yapısı kurulmalıdır.

5. DHCP olacak WB ve EB routerları VLAN40 ve VLAN35 üzerinde olmalıdır. VLAN30 ve VLAN40 için havuzlar burada oluşturulacaktır.

6. WB ve EB routerları üzerinde birbirleriyle haberleşebilmeleri için router protokolü tanımlanmalıdır.

7. Data Center ağında herhangi bir VTP ve STP yapısı kurulmayacaktır. Ağdaki PC'ler için bir DHCP havuzu oluşturulacaktır. ISP Router ile DC Router arasında router protokolü yapılancırılacaktır. Ve bu Router üzerinde konsola, enable moda ve bu cihaza başka bir cihaz TELNET yapmak istediğinde şifre soracaktır. Ayrıca açılışta bir mesaj verecektir. Herhangi bir porta bir açıklama mesajı oalcaktır.

8. Sadece INTERNET ve DATA CENTER network bilecektir. NAT yapısı daha sonra kurulacaktır.

9. Yapının INTERNET ağıyla haberleşebilmesi için sadece INT ve ISP Router arasında static route tanımalanacaktır.

10. Bulut üzerinde bütün ağların haberleşebilmesi için frame –relay yapısı kurulacaktır.

11. Son olarak Data Center ağının bulunduğu Router üzerinde NAT yapısı kurulacaktır. VLAN40 ve VLAN35 Router'lar ve yönetici bilgisayarları hariç hiçbir cihaz erişemeyecektir. Bunun için ACL yapısı kullanılacaktır

5. AĞIN KONFİGÜRASYONU

5.1 VLAN ve IP Bloklarının Belirlenmesi

Ağ haritası oluşturulup, kurallar belirlendikten sonra konfigürasyona başlanır. Öncelikle VLAN numaralarını belirleyip bunların hangi IP bloğundan IP alacağı seçilir. Harita üzerinde ayrıntılı bir şekilde belirtilmiştir.

5.2 Ağ Kurallarının Uygulanması

5.2.1 Birinci Kural

SW'lerin IP blokarını haritada verildiği şekilde yapılandırılacaktır ve cihazların isimlerini verilecektir.

5.2.2 İkinci Kural

Bu kuralda VTP domain kurulmasını ve bazı SW'lerin TRUNK olarak belirlenmesini istiyor. Öncelikle bunların ne olduğu aşağıda tanımlanmıştır.

5.2.3 VTP(VLAN Trunking Protocol)

Birden fazla mesela 100 VLAN üzerinde konfigürasyonu yapmak istenirse bunu her VLAN'ı elle tek tek ayarlayıp her porta tek tek atamak zorunda kalırsınız. Ayrıca kullanıcı sayısına bağlı olarak çok SW kullanmak zorunda kaldığınızı düşünürseniz iş yükünün ne kadar artacağını daha iyi anlayabilirsiniz. Bu noktada VTP bize kolaylık sağlamaktadır. VTP kullanarak, bir yada ihtiyaca bağlı olarak (logical tasnife bağlı olarak) birden fazla SW server olarak tanımlanmakta ve SW'ler üzerinde VLAN tanımları yapılarak VTP Client olarak tanımlanan Switchler üzerinde dağılması sağlanmaktadır. VTP tasarımında Switch server, client, transparent gibi üç farklı modda çalışabilmektedir. Böylece farklı amaçlar için farklı switch ayarları kullanabilmektedir. VTP, Cisco tarafından geliştirilmiş ve kullanılan

bir protokoldür. VTP standardı 802.1Q‘dur. VTP standardının IEEE tarafından açık kaynaklı olarak geliştirileni Multiple VLAN Registration Protocol(MVRP)‘dur. MVRP standadı 802.1Q eklentisi olan 802.1ak‘dır. Cisco tarafından VTP 2003 yılında geliştirilmiştir, IEEE 802.1Q‘ya ak eklentisini 2005 yılında geliştirmiştir. Her iki protokol de aynı amaç için kullanılmaktadır.

Multiple VLAN Registration Protocol(MVRP); VLAN’ların portlar üzerinde ağ köprüsü içinde dinamik olarak kaydı ve kaydının silinmesini destekler. MVRP’nin, sadece bir porta tüm VLAN durumunu içeren bir Protocol Data Unit (PDU) göndermesi gerekir (Cisco, 2012)

VTP Prunning özelliği ile VLAN’larda karşılaşılan Broadcast Flooding problemlerinin önüne geçer. Pruning yapıldığında VTP kullanılmayan durumlardaki gibi bir VLAN içerisinde broadcast paketi gönderildiğinde diğer VLAN’lar içerisine dağılmaz böylece gereksiz paket dolaşımının önüne geçilmiş olur. Sadece serverda enable edilir, Server bunu her cihaza iletir, her cihaz VTP Join Message ları ile, kendi üzerinde bulunan VLANlardan hangisinin aktif olarak kullanıldığını tüm cihazlara iletir, böylece gereksiz broadcast engellenmiş olur.

VTP mesajları ;

Özet Bildirileri (Summary Advertisements): VTP etki alanı adı, güncel revizyon numarası ve diğer VTP konfigürasyon detayları gibi bilgileri içerir. Her 5 dakikada bir komşu olan sunucu ya da istemci modda çalışan ve VTP özelliği olan anahtarlayıcılara gönderilir.

Altküme Bildirileri (Subset Advertisements): VLAN bilgilerini içerir. Bir VLAN oluşturulması ya da silinmesi, bir VLAN kapatılması ya da aktif hale getirilmesi, VLAN ismi değiştirilmesi ve VLAN paketinin boyutu değiştirilmesi gibi değişikliklerde değişiklik yapılan anahtarlayıcı aynı etki alanında bulunan diğer anahtarlayıcılara değişiklik yapıldıktan hemen sonra gönderir.

İstek Bildirileri (Request Advertisements): VTP etki alanı ismi değişikliği, kendi revizyon numarasından yüksek bir summary advertisement alınması, herhangi bir sebepten dolayı subset advertisement mesajı gelememesi ve anahtarlayıcı kapatılıp açılması durumunda anahtarlayıcı etki alanında bulunan anahtarlayıcılara istek

bildirisinde bulunur. Bir request advertisement alan anahtarlayıcı önce summary daha sonra subset advertisement gönderir (Başkanlığı, 2013).

VTP Katılım Mesajları (VTP Join Messages) : Bu mesaj türü istek bildirileri türüyle benzerdir ama farklı bir mesaj türü, alan ve daha fazla parametre özelliği vardır. Adından da belli olduğu gibi vtp clientler domaine ilk katıldığında vtp server üzerine bilgisi yollanır (Administrator, 2012).

VTP çalışma modları;

VTP Server mode; Sunucu modda ki switch'in VLAN bilgilerininin değiştirilme yetkisi bulunur. Yeniden VLAN ekler var olan VLAN'ı siler. Sunucu mod da VTP değişiklikler yollar ve alır. Ve VLAN yapılandırmasını hafızada tutar.

VTP Client mode; VLAN bilgilerini değiştirme hakkı yoktur. Yeniden VLAN eklenmez, silinmez. VTP güncelleme gönderip alabilir. VLAN bilgisini hafızada tutmaz.

VTP Transparent mode; Transparent moddaki SW'in VLAN bilgisini değiştirme hakkı vardır. Yeniden VLAN eklenebilir var olan VLAN silinebilir fakat yapılacak bu değişikler yalnız o SW'de etkin olur. Bu modda olan VLAN değişikliklerinin hiçbiri diğer SW'leri etkilemeyecktir. VTP güncellemeleri iletir. VTP duyuruları dinlemez çünkü kendi veritabanı vardır. Bundan dolayı aldığı bilgiye hiçbir ideğişiklik yapmadan diğer SW yollar VLAN bilgilerini hafızada tutar (Elohab, 2014).

VTP, VLAN'ların yönetiminde bizlere çok büyük avantajlar sağlayan bir teknoloji standartıdır. İyi anlaşılması ve kullanılması güvenlik, yönetim ve bağlantı tutarlılığı konularında katma değer sağlar (Hoşgör, 2014).

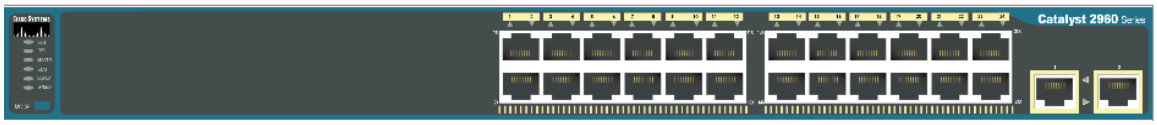
Bir VTP domain (aynı zamanda bir VLAN yönetim alanı denir) aynı VTP etki alanı adı paylaşan aynı idari sorumluluğu altında bir anahtar veya birkaç birbirine bağlı anahtarlar oluşur. Bir anahtar, sadece bir VTP etki olabilir (Configuring VTP, 2009). 2960-24TT model switch kullanılmıştır. 24TT'nin o SW'nin 24 portlu olduğunu gösterir. Mouse ile SW üzerine gelip beklenildiğinde o SW üzerindeki portlar ve VLAN'lar görülebilir. Seçilen SW üzerinde 24 tane FastEthernet ve 2 adet GigabitEthernet bulunmaktadır. FastEthernet'ler 100 mbit GigabitEthernet'ler ise 1 gbit'tir. Ayrıca default 1 VLAN bulunmaktadır. Hepsi defaultta downdır yani çalışmıyordur (**Şekil 5.2**).

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	0090.2B65.CC01
FastEthernet0/2	Down	1	--	0090.2B65.CC02
FastEthernet0/3	Down	1	--	0090.2B65.CC03
FastEthernet0/4	Down	1	--	0090.2B65.CC04
FastEthernet0/5	Down	1	--	0090.2B65.CC05
FastEthernet0/6	Down	1	--	0090.2B65.CC06
FastEthernet0/7	Down	1	--	0090.2B65.CC07
FastEthernet0/8	Down	1	--	0090.2B65.CC08
FastEthernet0/9	Down	1	--	0090.2B65.CC09
FastEthernet0/10	Down	1	--	0090.2B65.CC0A
FastEthernet0/11	Down	1	--	0090.2B65.CC0B
FastEthernet0/12	Down	1	--	0090.2B65.CC0C
FastEthernet0/13	Down	1	--	0090.2B65.CC0D
FastEthernet0/14	Down	1	--	0090.2B65.CC0E
FastEthernet0/15	Down	1	--	0090.2B65.CC0F
FastEthernet0/16	Down	1	--	0090.2B65.CC10
FastEthernet0/17	Down	1	--	0090.2B65.CC11
FastEthernet0/18	Down	1	--	0090.2B65.CC12
FastEthernet0/19	Down	1	--	0090.2B65.CC13
FastEthernet0/20	Down	1	--	0090.2B65.CC14
FastEthernet0/21	Down	1	--	0090.2B65.CC15
FastEthernet0/22	Down	1	--	0090.2B65.CC16
FastEthernet0/23	Down	1	--	0090.2B65.CC17
FastEthernet0/24	Down	1	--	0090.2B65.CC18
GigabitEthernet1/1	Down	1	--	0007.ECDD.8901
GigabitEthernet1/2	Down	1	--	0007.ECDD.8902
Vlan1	Down	1	<not set>	0001.64D3.13BD

Hostname: Switch

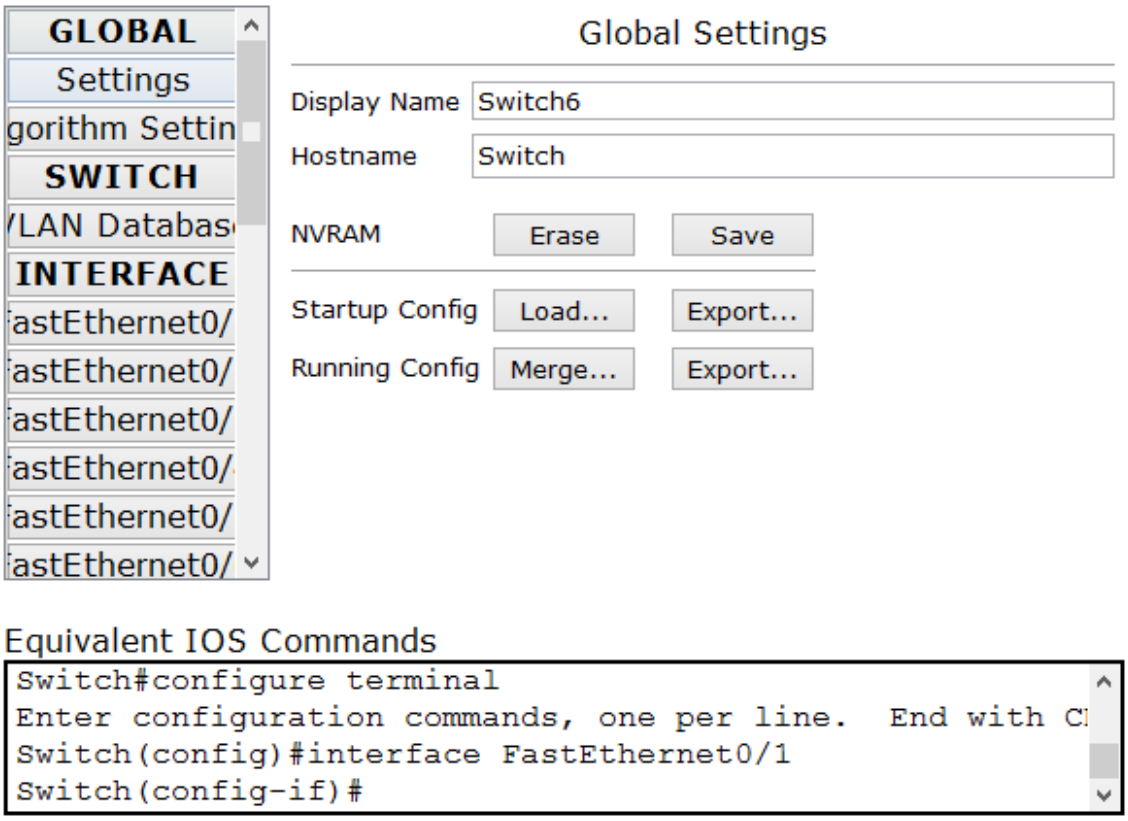
Şekil 5.1 SW Deafult Bilgileri

SW üzerine tek tıklandığında 3 tane sekme gelir. İlk o cihazın fiziksel görünüme ulaşılır (**Şekil 5.3**).



Şekil 5.2 SW Fiziksel Görünümü

İkinci sekme arayüz kullanarak konfigürasyon yapma sekmesidir (**Şekil 5.4**). Alt kısımda da arayüz kullanıp konfigürasyon yaptıktan sonra hangi kodların kullanıldığını görülebilir.



Şekil 5.3 Arayüz Konfigürasyon Sekmesi

Kodlarla konfigürasyon yapılacağı için üçüncü sekmeye yani CLI sekmesine gelinir. Bu arayüz üzerinde önce ‘enter’ tuşuna basarak komut satırının gelmesini sağlanır. Bu arayüzde 4 adet mod bulunmaktadır.

Kullanıcı Modu (User EXEC Mod) : Kullanıcı modudur yönlendirci üzerindeki konfigürasyonları yanlız görülmesini sağlar. Bu kısımda konfigürasyon yapma özelliği yoktur.

Özel Mod (Privileged mode) : Yönlendirinin konfigürasyonunun görülevileceği ve yapılandırılabileceği kısımdır (Karaalioğlu, 2008).

Yapılandırma Modu (Global Configuration Mode) : Yapılandırma komutları bir bütün olarak cihazı etkileyen özellikleri uygular.

ArayüzKonfigürasyon Modu (Interface Configuration Mode) : Arayüz yapılandırma komutları; arabirimi değiştirme işlemi yapar (Cisco, 2012).

İlk olarak gelinen mod kullanıcı modudur. Burda soru işareti yazarak uygulanabilecek komutlar görülebilir. Gerçek bir SW’de uygulanacak komutlar daha fazladır fakat simülatör üzerinde çalışıldığı için uygulanacak komutlar sınırlıdır. Bu kısımda uygulanacak kodun baş harfini yazıp klavye üzerinde ‘tab’ tuşuna basıldığı

zaman kodu otomatik tamamlar. Fakat aynı harfle başlayan bir kod varsa sırasıyla diğer harflerin yazılması gerekir. Çünkü ikisini birden ekrana getiremeyeceği için ek bir harfe ihtiyaç duyacaktır. Kullanıcı modunda‘ enable’ yazarak özel moda geçilir. Bu moddayken konfigürasyona başlamak için için ‘configure terminal’ komutunu yazarak yapılandırma moduna geçilir.

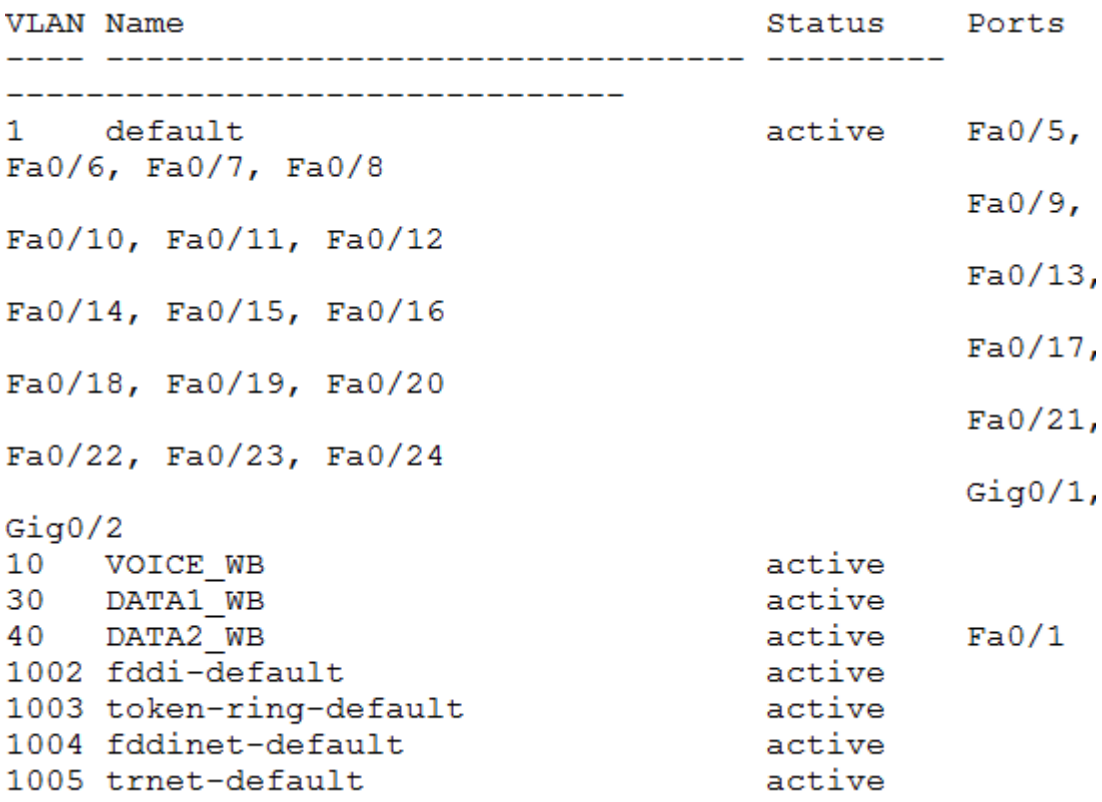
SW_WB_1 VE SW_SW_EB_1, SW’leri üzerinde VLAN’ları oluşturulur.

Daha önce VTP durumunu belirlenecektir. Eğer gerçek bir cihaz üzerinde çalışıyor olunsaydı burdaki durumlara ek olarak pruning olacaktı.

VTP’nin versiyon 1, versiyon 2 ve son olarak versiyon 3 olmak üzere 3 adet versiyonu vardır. Versiyon 1 ve 2 arasındaki belirgin olan tek fark version 2 Token Ring VLAN destekler. Versiyon 3’ün önceki versiyonlara göre oldukça yeni özellikler getirmiştir. Bu özelliklerden bazıları;

- VTP version 3 diğer switchlerin VLAN bilgilerini güncellemek için kullanılan switch üzerinde etkili bir yönetim görülür. Networkde yanlış yapılan değişikliklerin büyük ölçüde azalmasını sağlar ve kullanılışı artar.
- 1-1001 arasındaki ISL VLAN’leri ile birlikte 4095’e kadar olan Dot1q (802.1Q) VLAN’lerinin de taşınması ve VLAN’lerin yanında Privat VLAN(PVLAN) yapılarını da desteklemesi ile VLAN ortamında fonksiyonellik önemli ölçüde artmıştır.
- VTP version 3 VLAN haricinde değişik veritabanlarının da aktarımını sağlar (Başkanlığı, 2013).

VTP version2 kullanılacaktır. Daha sonra TRUNK olarak belirlenecek portları bütün portları belirlenecektir. Bu işlemi yaptıktan sonra o portlar aktif olması için yeniden başlar ve defaultta gelen VLAN bilgisi silinir (**Şekil 5.5**).



Şekil 5.4 CLI Arayüzü VLAN Bilgisi

'show vlan brief' komutuyla VLAN bilgisini görebiliriz. Bu komut privilege modda iken çalışır. Eğer herhangi bir konfigürasyon modunda isem bu komutun başına 'do' komutunu ekleyerekte çalıştırabilr.

Yapılan konfigürasyonu kaydetmek amacıyla 'write' komutunu kullanılır. PC'lerin bağlı olduğu portlarda hangi VLANlarda olacaklarını belirlenir.

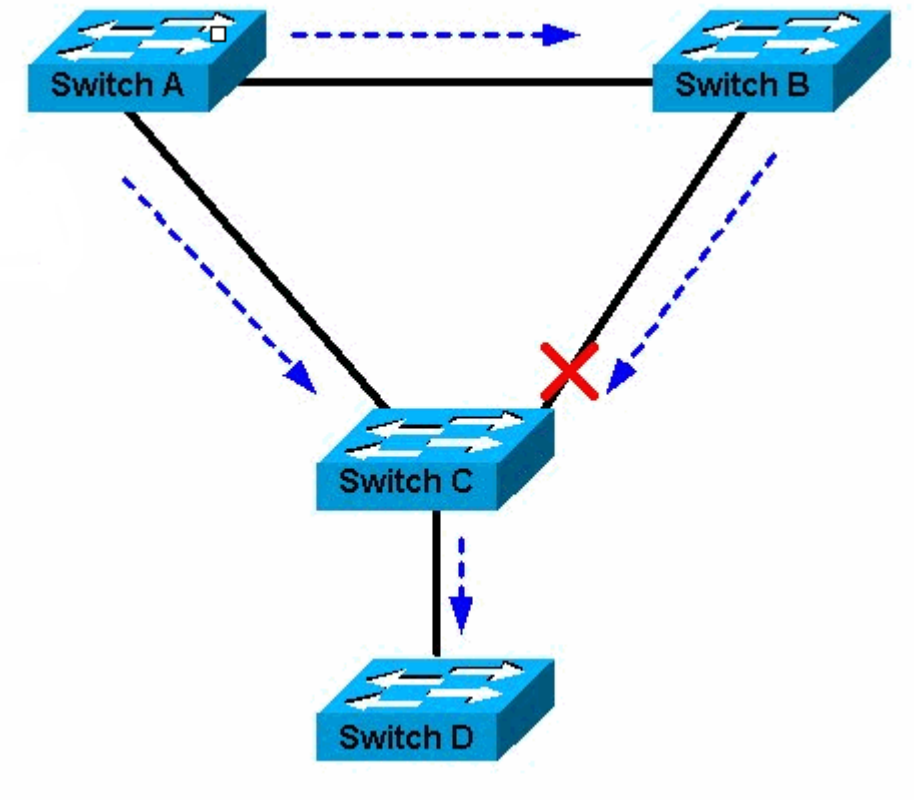
5.2.4 Üçüncü Kural

Bu kural bize STP yapılandırmamızı söylüyor. STP'nin tanımı aşağıda yapılmıştır.

5.2.5 STP (Spanning-Tree Protocol)

Çok fazla fiziksel bağlantı olan networklerde, STP yapılandırmadan önce frameler belli olmayan bir süre boyunca dolaşıyorlardı. STP, herhangi bir yerel alan ağ çarpışma etki alanı arasında tek bir aktif bağlantı kalabilmesi için bazı portları bloklar. STP'nin hem iyi ve kötü sonucu: Frameler döngüye girmez ve buna göre yerel alan ağı kullanılabilir. Fakat network, framelerin döngüye girmesin diye bloklanan bağlantıların getireceği avantajları kaybeder.

STP algoritması, Bütün bridge ve switch portunu bloklar veya iletim durumuna getirir. İletim durumundaki portların, etkin spanning tree içinde bulunur. İletim portlarının hepsi, framelerin yolladığı bir yol oluşturur (System, 2008).



Şekil 5.5 Spanning Tree Protocol

Kuralda belirtiği gibi yapı kurulur. İsteğe bağlı olarak burda spanning-tree komutu kullanılabilir. Fakat defaultta o şekilde geldiği için kullanma gereği duyulmaz.

5.2.6 Dördüncü Kural

Bu kuralda öncelikle yapılması gereken router-on-astick yapısını kurmaktır. Bu yapının ne olduğu aşağıda tanımlanmıştır.

5.2.7 ROS(Router on a Stick)

Router on a Stick Inter-VLAN Routing, Inter Vlan Routing'in fazla sayıda arabirime ihtiyaç duymasından dolayı ortaya çıkan Inter Vlan yapısıdır (Ağcıyız Ekibi, 2013). VLAN'ları birbirleriyle haberleştirmek için bu yapıya ihtiyaç olacaktır. Router'ın SW bağlı arabirminde bir adet interface bulunmaktadır. Fakat bu haritada 2 ağdada 3 adet VLAN bulunmaktadır. Bunun için sub-interface oluşturmak gerekir. Yani o

arabirim içinde 1den fazla alt arabirim oluşturabilir. Önce VOICE VLAN'ları hariç bütün VLAN'larım için oluştur ve IP atamaları yapılır.

Daha sonra VOICE VLAN için bir tanımlama yapmak gerekir ki IP telefonları ile ağı haberleştirilir. Burda CME yapısı kurulması gerekir. Yani burada VOIP kullanılacaktır. Bu yapı aşağıda tanımlanmıştır.

5.2.8 CCME(Cisco Call Manager Express)

CME Cisco router üzerinde çalışan ve ağa hizmet vermektedir. Bir switch aracılığıyla ağa bağlı IP Telefonlar gelen ve giden çağrıları için kullanılır. IP telefonlar ve CallManager Express router ile iletişim kurmak için SCCP adlı özel bir protokol kullanır. Bir çağrı CallManager Express kontrolü altında iki IP telefon arasına yerleştirildiğinde, SCCP protokol çağrıyı almak için kullanılır. SCCP protokolü sadece IP telefon ve Cisco CME sistemi arasında kullanılır, iki IP telefon arasında kullanılmaz (Administrator, 2012).

5.2.9 VOIP(Voice Over Internet Protocol)

Internet üzerinde belli noktalar arasında sesli görüşmeyi sağlayan bir teknoloji olarak görülmektedir (Sarıyar, 2008).

Türkçesi internet üzerinden ses olarak çevirilebilir. VoIP genelde telefon şebekesi ağ yapısında uygulanan geliştirmeler sonucuyla ortaya çıkmıştır, İnternetin alt yapısını kullanıp arama yapabilmeyi ve faks çekebilmeyi sağlar (Güngörür, 2009).

Yapılandırmaya başlamadan önce telefonlara dağılacak IP grubunu oluşturulur Yani bir DHCP havuzu oluşturulur ve tabi router IPleri dağılmasın diye onları havuzun içinden çıkartılır.

5.2.10 DHCP(Dynamic Host Configuration Protocol)

DHCP, pclere en başta IP adresi ve subnet maskesi olarak TCP/IP parametrelerini otomatik dağıtan yapıdır. DHCP şu şekilde kurulur; Önce bir makine DHCP server olarak kurulur. Sonra DHCP serverda diğer cihazlara dağıtılacak adresler için bir adres aralığı ve bir subnet maskesi tanımlanır (Öçkoymaz, 2012).

Havuzu tanımlarken birde TFTP sunucusu tanımlamak gerekir. Bu haritada Data Center ağında bulunuyor. Bu sunucu aşağıda tanımlanmıştır.

5.2.11 TFTP(Trivial File Transfer Protocol) Sunucusu

Bir TFTP sunucusu, genellikle VoIP Cihazlar için standart yapılandırma şablonları backend olarak kullanılır. Mevcut VoIP Cihazlar ve yeni nesil cihazların iyi bir kısmı cihazlara kendi yapılandırma dosyaları ve ayarları iletmek için TFTP sunucuları kullanır. Bellekte çok az yer kaplar. Genellikle gerçek dünyada bakıldığında kilometrelerce uzakta istemciler olabilir. Mesela 50 adet telefonunuz ve bunlar IP adreslerini bir sunucudan sabit IP üzerinden alıyorlarsa o sunucunun IP adresi değiştiğinde telefonlara erişim sağlanamaz fakat TFTP sunucu sayesinde bu yaklaşık 15 saniye içinde bulur ve değiştirir (Bench, 2009).

Burada TFTP sunucusu temsili olarak kullanılmıştır. Çünkü IP telefonlara IP dağıtmak ve VoIP yapısını tanımlamak için DHCP havuzu oluştururken bunu kod ile belirtmek gerekiyor ve telefonların hangi port aralığında olacağını belirtmek gerekir. Telefonların hepsine bir DN atanır. Yani aranacağı numara atanır ve port numarası verilir. Bu port numaraları aynı port aralığında farklı numaralar olmalıdır.

'show ephone' komutuyla IP telefonların bilgisi görülebilir (**Şekil 5.6**).

```
ephone-1 Mac:0030.F20D.EAD6 TCP socket:[1] activeLine:0
REGISTERED in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0
paging 0 debug:0 caps:8
IP:172.16.10.102 1025 7960   keepalive 43 max_line 2
 button 1: dn 1  number 1001 CH1   IDLE

ephone-2 Mac:0030.A37A.3914 TCP socket:[1] activeLine:0
REGISTERED in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0
paging 0 debug:0 caps:8
IP:172.16.10.101 1025 7960   keepalive 43 max_line 2
 button 1: dn 2  number 1002 CH1   IDLE

ephone-3 Mac:0001.6475.B61D TCP socket:[1] activeLine:0
REGISTERED in SCCP ver 12 and Server in ver 8
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0
paging 0 debug:0 caps:8
IP:172.16.10.105 1025 7960   keepalive 43 max_line 2
 button 1: dn 3  number 1003 CH1   IDLE
```

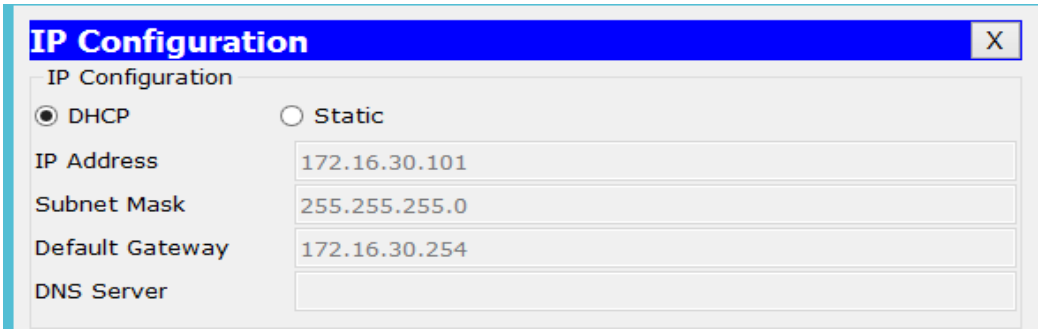
Şekil 5.6 IP Telefonların Bilgileri

Şekil 5.7 1001 portlu IP telefonun 1002 portlu IP telefonuna ulaşması

Burda VLAN30 ağına 'ip helper-address' komutu ile VLAN40 ağının Router gateway IPsi eklenir. Çünkü o Router üzerinde VLAN'lar DHCP havuzunu oluştulacaktır. O ağ VLAN40 ağı olduğu için yardımcı IP adresi ataması gerekir.

5.2.12 Beşinci Kural

EB ve WB, GW Routerları üzerinde kalan VLAN'lar için DHCP havuzu oluşturulur. PC üzerinde aldığı IPler görülebilir (**Şekil 5.8**).



Şekil 5.8 DHCP üzerinden IP alan PC

5.2.13 Altıncı Kural

Routerların biribiriyle haberleşmeleri için protokol tanımlanır.

5.2.14 Router Protokolleri

Static Routing : Static routing protokolünde sistem yöneticisi routing tablosundaki bilgileri kendisi eliyle girer. Static routing protokolünün avantajları şunlardır:

- Yönledirici işlemcisine gerek duyulmaz.
- Yönlendiriciler arasında bandwith kullanımaz.

Bununla birikte static routing protokolünün dezavantajları şunlardır:

- Routerlar ağların route protokolünü bilmelidirler.
- Yeni ağ eklendiğinde yönetici el ile yolunu bütün ağa eklemelidir.
- Geniş ağlarda el ile bu bilgilerin girilmesi çok vakit alır, mümkün bile olmayabilir (Ciscotr, 2008).

Dynamic Routing : Router üzerinde çalıştırılan bir protokol aynı protokol ile çalışan diğer Router'lar ile belirli tanımlamalar ve kısıtlar çerçevesinde kalmak şartıyla haberleşerek routing table'ı oluşturur/doldurur (Hoşgör, 2014).

RIP: Distance vector routing protokolünü kullanır. Uzaklık vektörü yönlendiriciler yönlendirme tablolarınını komşu yönlendiricilere yollar böylece router komuşularından aldığı yönlendirme bilgileri ile kendi bilgilerini birleştirerek yönlendirme tablosunu oluşturur. RIP kullanılan bir ağda her 30 saniyede bir yönlendiriciler yönlendirme tablosunu bütün aktif arabirimlere yollar. Bu protokolün en iyi yolu hesaplamak için hop sayısına bakar. En fazla geçilebilecek hop sayısı 15'dir. Bu yüzden küçük ağlar için RIP kullanışlıdır fakat büyük ağlarda ve geniş alan ağlarında yapıda yetersiz kalır. Rip version 1 ve version 2 diye iki çeşittir. Rip version 1 'i tercih edilirse version 1 classfull dur yani ağda ki tüm cihazlar aynı subnet'e sahip olmak durumundadır. Version 2 ise classlessdır yani route güncellemeleriyle beraber subnet masklarıda gönderir ve aynı zamanda prefix routing sağlar. Rip'in administartive distance numarası ise 120 dir (Türkeri, 2011).

IGRP (Interior Gateway Routing Protocol) : Protokolu Rip V1 gibi classfull çalışır. Packet tracer bu protokolu desteklemez. IGRP protokolu sadece Cisco Routerlarında kullanılabilir. Bu Protokol Cisco cihazlarına özeldir. IGRP protokolu classfull olduğu

için routing bilgisinde subnetmask bilgileri içermez, Sadece IP Routingi destekler. Classless veya VLSM networkleri desteklemez (Şener, 2014).

EIGRP: EIGRP, Cisco Systems tarafından yapılmış ve IGRP'nin gelişmiş versiyonudur. EIGRP, Interior Gateway Protocol ailesindendir. Metodu distance vector protokoldür ama link state yapısınıda barındırır. Bir network üzerinde EIGRP yapılandırılabilmesi için iyi bir ağ tasarlanması gerekir. EIGRP alternatif yollar arasında yüksek bir geçiş hızı sağlar. EIGRP, Diffusing Update Algorithm kullanır. DUAL algoritmasıyla yedek yönlendirmeler hesaplanır ve gerektiğinde zaman kaybı olmadan yedek yolların kullanılmasını sağlar. Routing tablosunda değişiklik olursa bütün tabloyu göndermez, yalnız değişen kısmı gönderir. Böylelikle routera gelen ek yük de çok az olur ve ağ trafiğini de optimum kullandırır. Ayrıca EIGRP; IP, IPX, AppleTalk protokollerini de destekler. (Taşkıran, 2006).

OSPF: OSPF Link state Protocol olan ve ulaşılmak istenen ağa giden en kısa yolu Dijikstra algoritması kullanarak bulmaktadır. Hello protokolu yardımıyla OSPF yönlendirmesi kullanana yönlendiriciler komşularını bulurlar. Hello paketleri 10 saniyede bir gönderilir ve burdan gelen sonuçlara yardımıyla OSPF veritabanı oluşur. OSPF metrik icin cost adı verilen degeri kullanırlar Standart bir tanımı yapılmamakla birlikte Cisco Routerlar da öngörülen OSPF metriği bant genisliği ile ters orantılıdır.

Bu yönlendirmede ağdaki routing verileri kendi üzerinde toplayıp diğer cihazlara dağıtan bir yönlendirici vardır. Bu yönlendiricye Designated Router denir. DR aktif değilse eğer Backup Designated devreye girer.

Hello paketinin içerdiği bölümler;

Yönlendirici ID: Yönlendiricide yapılandırılan en yüksek IP adresidir.
Network Mask: Yönlendirici ID'yi belirleyen arabirimin ağ maskesidir.
Area ID: Hello paketi yollayan yönlendriricinin arabiriminin alan ID'sidir. Hello paketindeki verilerin geçerli olması için bu paketi alan yönlendiricinin arabirimi ile aynı olması gerekir. Router Priority: Routerin DR veya BDR seçiminin nasıl olacağını sağlar.
Hello Paket Aralığı: Süresi 10 saniyedir.

OSPF Area ; OSPF çalışma sistemi alanlar üzerine tasarlanmıştır ve bundan dolayı bir dizayn hiyeraşisi sağlanır. Bu yapının convergencesi hızlandırır.

OSPF merkezi area 0'dır. Area 0 backbone area olarak adlandırılır. Farklı arealar olduğunda o arealar içinde area 0 ile konuşan interface'e sahip routerlar olmalıdır (DİKAY, 2010).

EIGRP kullanılmıştır. Bundaki mantık aynı işlem ID sinde olanlarla haberleşir diğerleriyle haberleşmez. OSPF'e göre biraz daha hızlı çalışır. Başka bir Router protokolü ile haberleşmek isterse eğer cihaz yöneticisine sorar.

'show ip route' komutuyla routerların hangi arabirimlerle haberleştiğini görebiliriz (**Şekil 5.9**).

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
D       10.1.1.52 [90/2681856] via 10.1.1.1, 03:35:07,
Serial0/0/0
     172.16.0.0/24 is subnetted, 4 subnets
D       172.16.1.0 [90/30720] via 172.16.40.254, 03:35:06,
FastEthernet0/1
D       172.16.10.0 [90/30720] via 172.16.40.254,
03:35:06, FastEthernet0/1
D       172.16.30.0 [90/30720] via 172.16.40.254,
03:35:06, FastEthernet0/1
C       172.16.40.0 is directly connected, FastEthernet0/1
     172.17.0.0/24 is subnetted, 4 subnets
D       172.17.2.0 [90/2686976] via 10.1.1.1, 03:35:07,
Serial0/0/0
D       172.17.15.0 [90/2686976] via 10.1.1.1, 03:35:06,
Serial0/0/0
D       172.17.35.0 [90/2684416] via 10.1.1.1, 03:35:06,
Serial0/0/0
```

Şekil 5.9 RB_WB_GW Router'ın haberleştiği arabirimler

5.2.15 Yedinci Kural

Data center ağı yapılandırılacaktır. Burda küçük hayali bir data center yapılandırılmıştır. TFTP, NTP, HTTP sunucular bulunuyor ve 2 adet PC bulunuyor.

Data Center: İçinde kullanılanz hosting veya server çeşitlerini barındıran üst düzey teknolojilerin kullanıldığı sunucu deposudur diye açıklayabiliriz. İnternet kullanımının artması ile internet üzerindeki verilar daha fazla önem oldu ve daha fazla güvenlik önlemi almak gerekti. Bundan dolayı bu verilere ev sahipliği yapacak verimerkezleri kuruldu ve geliştiriliyor (Arat, 2014).

Router üzerinde DHCP havuzu oluşturulur default VLAN için yani VLAN1 için data center üzerindeki PC'lere IP dağıtılır. Daha sonra ISP ile haberleşmesi için router RIP tanımlanır bilmediği bütün ağları o router üzerinden öğeniyor.

5.2.16 Sekizinci Kural

Burda hayali bir ISP tanımlanır.

ISP(Internet Service Provide) : ISS, genelde belli bir mikater ücret karşılığında Internet'e erişiminizi sağlayan belli şirketlerdir. Bir internet servis sağlayıcısına bağlanmanın genel yolları telefon hattı (çevirmeli) veya geniş bant bağlantısı (kablolu veya DSL) kullanmaktır. Birçok internet servis sağlayıcısı, e-posta hesapları, web tarayıcıları gibi ek hizmetler ve web sitesi oluşturmanız için alan sağlar (Windows, 2014).

Bu router üzerinde static routing tanımlanır çünkü sadece data center ve internet ağını bilmesi gerekiyor.

5.2.17 Dokuzuncu Kural

Internet ağı üzerinde de DNS, NTP VE HTTP sunucusu bulunmaktadır. Burdaki router üzerinde sadece ISP ile haberleşmesi için static routing tanımlanır ve NTP sunucu tanımlanır.

NTP Sunucu : Bu sunucuda 'Log' kayıtları için zaman bilgisi çok önemlidir. Yönlenirici üzerinde zaman değerleri doğru ayarlanmalıdır. Yönlendirici üzerinde zaman bilgisini gösteren iki saat vardır;

- Hardware Clock : Donanımsal bir saattir ve pil ile beslenir. Yönlendirci reset atıldığında zaman bilgisinin kaybolmaması için kullanılır. Bütün Cisco cihazlarda olmak zorunda değildir. IOS'da CALENDAR olarak belirtilir.
- Software Clock: Bütün Cisco cihazlarda vardır. Eğer cihaz üzerinde hardware Clock yok ise cihaza reset atıldığında zaman bilgisi gider. Cihazlardaki sistemler zaman bilgisini almak için bu kaynağı birincil olarak kullanır. IOS 'da CLOCK olarak belirtilir. Birden fazla seçenek ile Software Clock değerleri ayarlanabilir.
- El ile konfigüre edilebilir.
- NTP Master sunucu ile senkron çalışabilir (Altaner, 2013).

HTTP (Hyper Text Transfer Protocol) Sunucu : Web server yada network serverın, İnternet üzerinde bir web sitesinin yayınını yapması gereken serverdır. Web servisi internet üzerinde genelde kullanılan servisdir. Temelde HTTP kullanılarak verilen bir servistir (Sarıgöz, 2011).

DNS Server : DNS günümüzde en basit anlatımıyla isim çözümleme için kullanılır. Internet veya intranet ortamını bakarsak her bir cihazın sayısal olarak bir adı vardır ama genelde alphanumeric isimleri biliriz çünkü akılda kalması zordur. DNS bu manada alphanumeric isimleri bilerek sayısal isimlere ne olduğunu görmemizi sağlar. Ağ üzerindeki cihazların DNS'te isim karşılığına Hostname denir . FQDN'de DNS serverındaki bir nesnenin tam adıdır. Ağda olan cihazlar hostname ile iletişim saglarlar, ama mutlaka bir DNS server içinde bu hostname karşılık gelen IP adresi bulunur (Solmaz, 2008).

5.2.18 Onuncu Kural

Cloud üzerinde frame-relay point-to-point tanımlayarak ve bağlı routerlar üzerindede tanımlayarak yapının haberleşmesini sağlanır. Çünkü internet simülasyonu yapmak için WAN kullanılacaktır.

Frame Relay : Bütün dünyada genelde kullanılan paket anahtarlamalı teknolojidir. Leased Line'dan daha az masraflı olduğu için genellikle tercih edilen iletişim teknolojisidir. Bu bağlantı için en yakın Türk Telekom Frame Relay SW'ine yüksek bandwith(bant genişliği) sahip modem ve yönlendirici ile bağlanılması gerekir. Anahtarlanmış paket teknolojisine dayanan Frame Relay datayı küçük paketlere bölerek yollar. Bu paketler gönderilecek olan adresi, gönderenin adresini ve orijinal mesajın bir parçasını içerir (Şahan, 2009).

Point to point olarak tanımlamamın nedeni farklı ağlar olması ve merkezin bunlara tek arabirim üzerinden erişmesidir.

Öncelikle SW_FR üzerinde gerekli tanımlamaları yapılır. Daha sonra data center router üzerinde DLCI 102 (WB), 103 (EB) olarak tanımlanır ve WB DLCI-201-EB DLCI-301 olarak tanımlanacaktır.

5.2.19 On birinci Kural

Data center router üzerinde NAT yapısı tanımlanır.

NAT (Network Address Translation) : Ağ adresi çevirisi, bir ağ üzerindeki bilgisayarların Internet Protokolü sürüm 4 (IPv4) adreslerinin farklı bir ağ üzerindeki bilgisayarların IPv4 adreslerine çevrilmesine yönelik bir yöntemdir. Şirket ağı gibi özel bir ağın Internet gibi ortak bir ağ ile buluştuğu sınırda dağıtılan NAT etkinleştirilmiş bir IP yönlendiricisi, bu çeviri hizmetini sağlayarak özel ağ üzerindeki bilgisayarların ortak ağ üzerindeki bilgisayarlara erişmesine izin verir.

NAT teknolojisi, IPv4 adreslerinin tükenmesi sorununa geçici bir çözüm sunmak amacıyla geliştirilmiştir. Kullanılabilir genel benzersiz (ortak) IPv4 adreslerinin sayısı, Internet erişimine gerek duyan bilgisayarların hızla artan sayısını karşılayamayacak kadar azdır. Internet Protokolü sürüm 6 (IPv6) adreslerinin geliştirilmesine yönelik uzun vadeli çözüm mevcut olsa da IPv6 henüz yaygın şekilde benimsenmemiştir. NAT teknolojisi herhangi bir ağ üzerindeki bilgisayarların, Internet üzerinde genel benzersiz ortak adreslere sahip bilgisayarlara bağlanmak için yeniden kullanılabilir özel adresler kullanmasına olanak tanır (Technet, 2015).

Şimdi son olarak ACL yapılandırılacaktır. Bu yapı aşağıda tanımlanmıştır.

ACL(Access List) : Cisco IOS, bir erişim kontrol listesini tanımlar ve trafiği yöneten bir kaydıdır. Trafik belirledikten sonra, bir yönetici bu trafiği olabilir çeşitli etkinlikler belirleyebilirsiniz.

IP ACL'leri erişim listeleri en popüler türü IP trafiğinin en yaygın türüdür. Burada iki şekilde Ip Access List vardir, Standart ve Extended Standart IP ACL'leri Sadece kaynak IP adresine dayalı trafik kontrol edilebilir. Extended IP ACL'leri çok daha güçlüdür; burada kaynak IP, kaynak portu, hedef IP tabanlı ve hedef port trafik saptanabilir (Kenber, 2009).

ACL şu şekilde yapılandırılmıştır;

WB’de VLAN40 subnetine hiçbir cihaz erişemeyecek tabi router ve admin PC’ler erişebilecek. EB’de VLAN35 subnetine hiçbir cihaz erişemeyecek tabi router ve admin PC’ler erişebilecek. Diğer alt ağlara erişilebilicek.

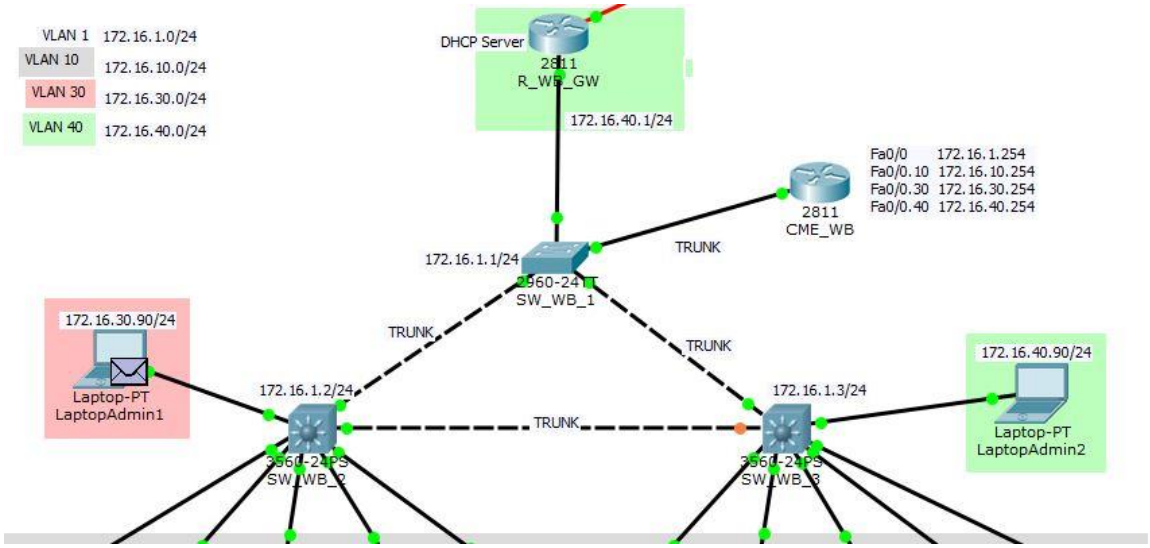
Kurallar tanımlandı. Artık ağ belirlenen kurallar çerçevesinde birbirleriyle haberleşebilir.

6. SİMÜLASYON

Simülasyonu Cisco Packet Tracer üzerinde gerçekleştirilecektir. Bu programın özelliğidir. Bir ICMP paketi gönderip her bir adım resimlerle gösterilmiştir.

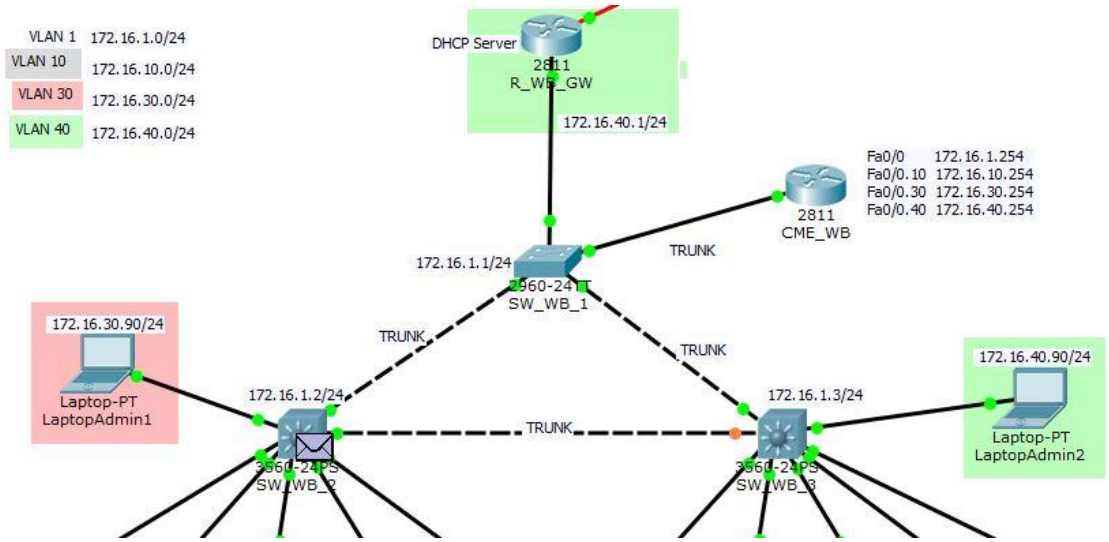
ICMP(Internet Control Message Protocol) : IP'nin görevi datagram paketlerini ilgili yerlere adreslemek ve yönlendirmektir. IP paketi ilettikten sonra, bir sonraki alacağı veya vereceği pakete bakar. Çünkü IP bağlantısız (connectionless) bir protokoldür ve paketin hedefe ulaşıp ulaşamayacağı konusunda hiçbir garanti vermez. Paketler, hedef hosta/hostlara zaman aşımı ya da benzeri bir sebeple ulaşmayabilir (Webstar, 2014).

VLAN30 admin PC'den VLAN35 admin PC'ye bir ICMP mesajı gönderilecektir. Yani ping atılır. Hem NAT çalışıyor mu o kontrol edilecektir hem de tanımlanan ACL çalışıyor mu o kontrol edilecektir. VLAN 40 Admin bilgisayarından ICMP çıkışı gerçekleşir (**Şekil 6.1**).



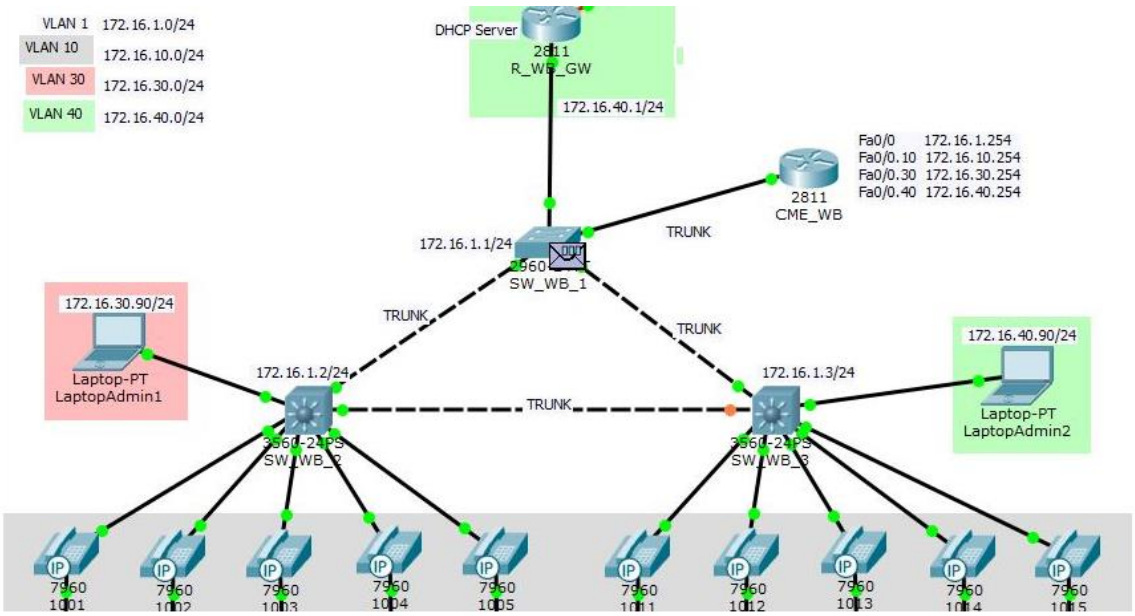
Şekil 6.1 VLAN40 admin PC'den ICMP çıkışı

ICMP client olarak belirlenen layer3 SW ulaşır (**Şekil 6.2**).



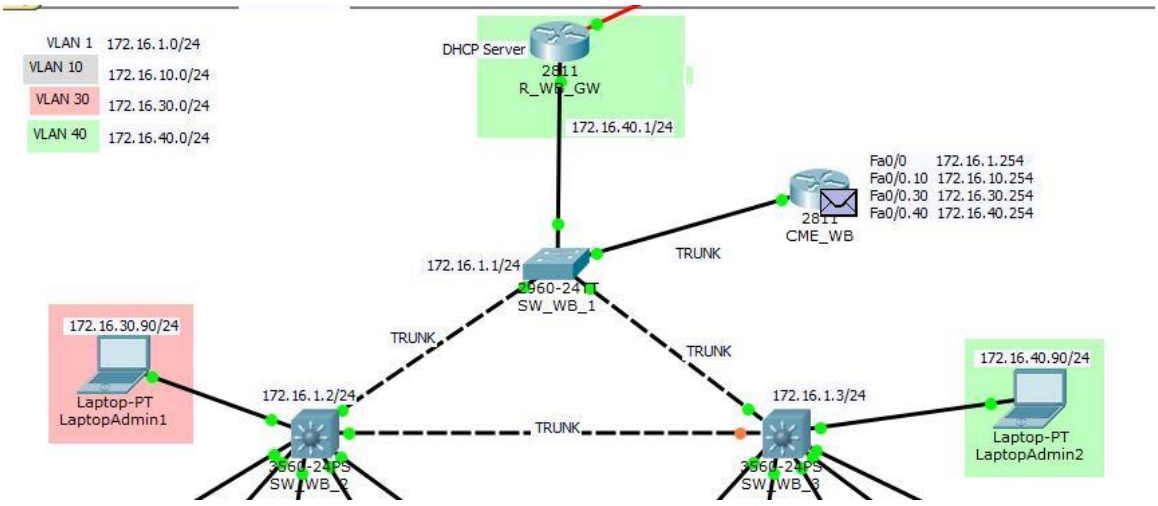
Şekil 6.2 ICMP client olan layer3 SW ulaşması

ICMP daha sonra root SW ulaşır (**Şekil 6.3**).



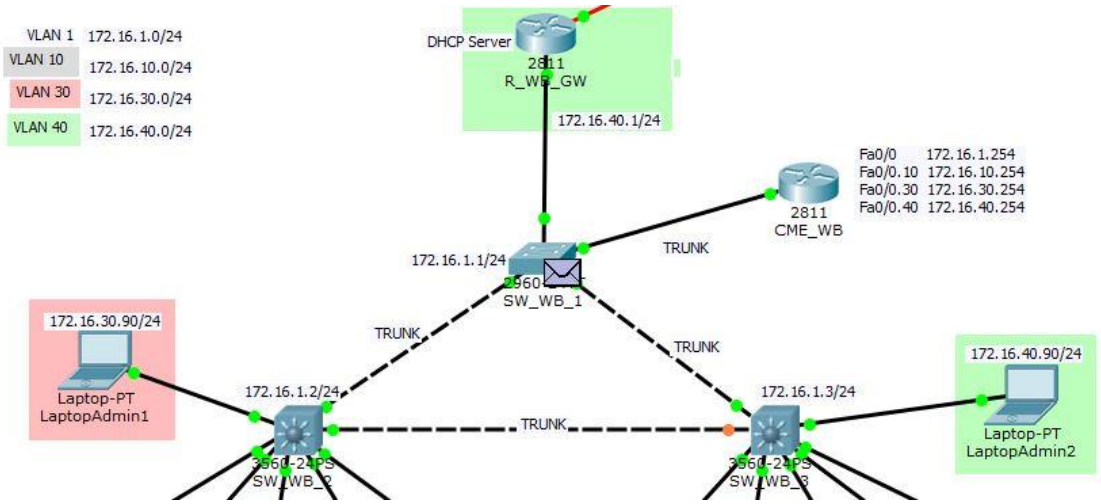
Şekil 6.3 ICMP root SW ulaşması

ICMP, VLAN40 ağının gateway router üzerine ulaşır (**Şekil 6.4**).



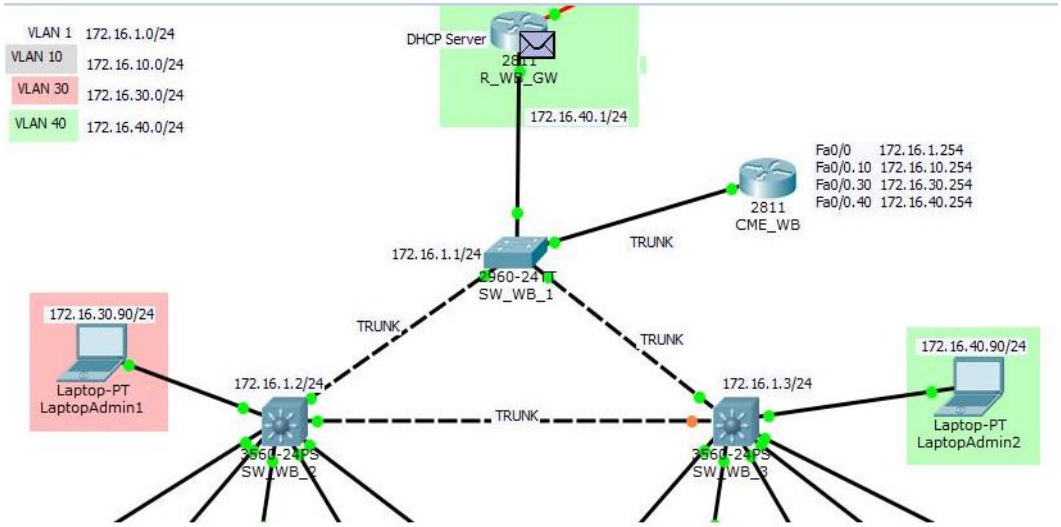
Şekil 6.4 ICMP VLAN40 gateway router ulaşması

ICMP geçiş iznini aldıktan sonra tekrar root SW döner (**Şekil 6.5**).



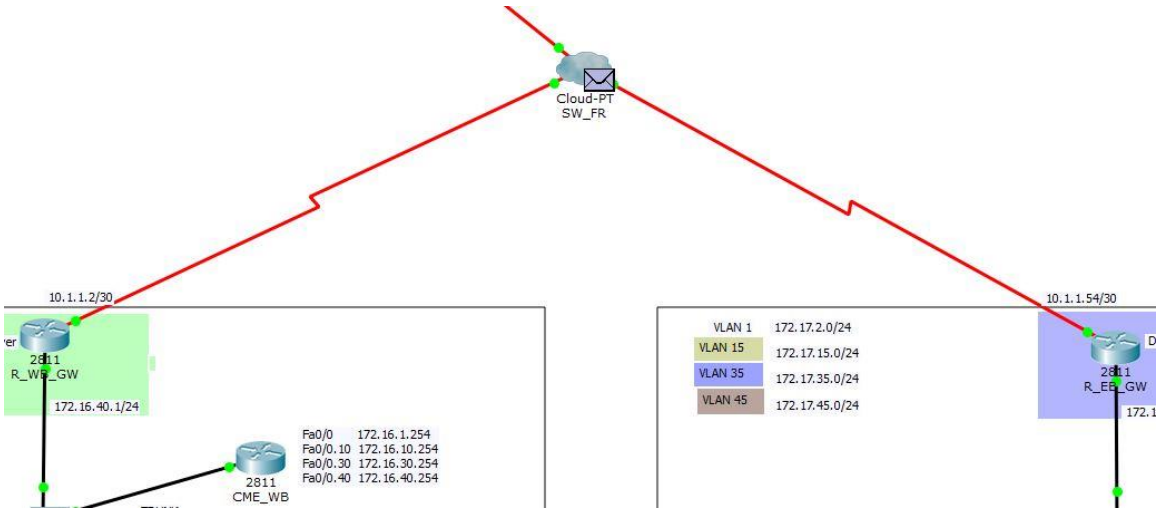
Şekil 6.5 ICMP tekrar root SW dönmesi

ICMP, WB ağının gateway router üzerine ulaşır (**Şekil 6.6**).



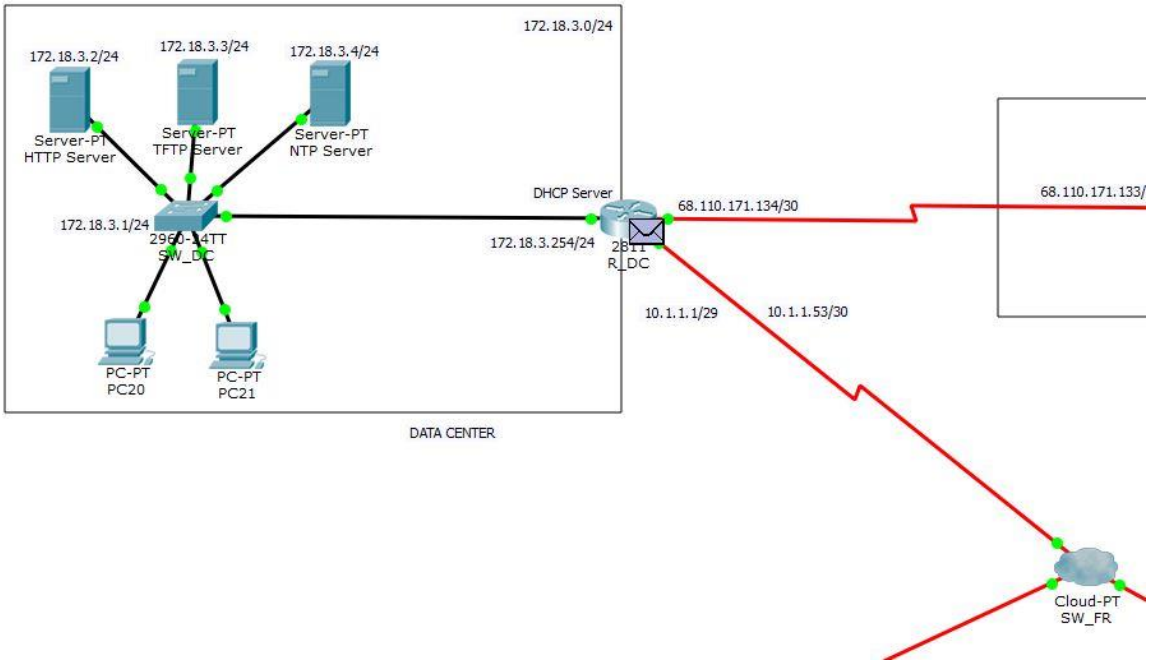
Şekil 6.6 ICMP ağın gateway router ulaşması

ICMP bulut üzerine frame-relay SW ulaşır (**Şekil 6.7**).



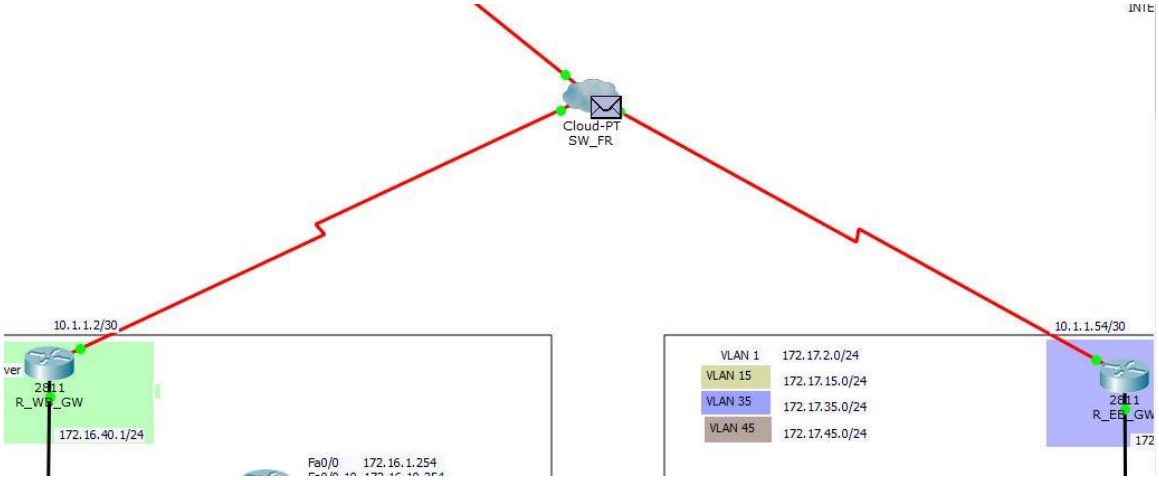
Şekil 6.7 ICMP frame-relay SW ulaşması

ICMP data Canter router üzerine ulaşır (**Şekil 6.8**).



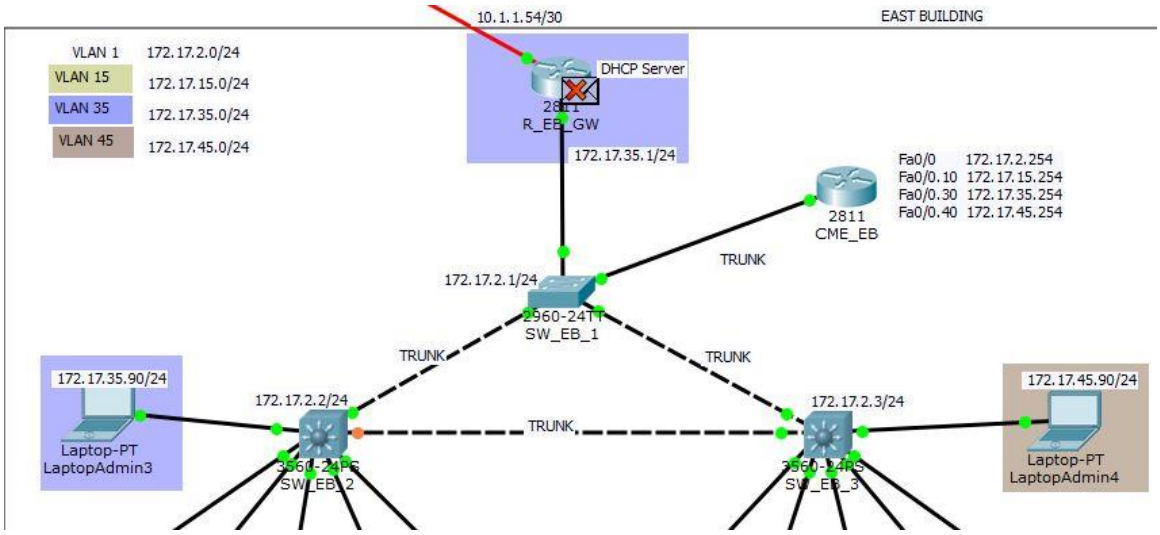
Şekil 6.8 ICMP data center router ulaşması

ICMP, NAT yapısından data center router üzerinden izin aldıktan sonra tekrar frame-relay SW döner. Bu şekilde NAT yapısının çalıştığını görebiliriz. Inbound yada outbound konrolünü yapıyor (**Şekil 6.9**).



Şekil 6.9 ICMP frame-relay SW dönmesi

ICMP, oradan diğer ağın gateway router gidiyor ve burdan geçemiyor. Bu şekilde de ACL çalıştığını görebiliriz. Çünkü Adminler sadece kendi ağlarına erişebiliyordu (**Şekil 6.10**).



Şekil 6.10 ICMP VLAN35 router üzerinden geçmemesi

Son olarak frame-relay yapısının çalıştığını da routerların haberleşip paketi iletmesinden görebiliriz.

7. SONUÇ

Bu çalışmada Router, switch, hub, IP telefon, frame-relay ve gerekli sunucular içeren bir geniş alan ağı ve yerel alan ağları gerçekleştirilmiştir. Yapılan topolojinin gerçekleştirilmesi sırasında Cisco Packet Tracer programı kullanılmış ve gerçek Router, switch konfigürasyonu ile aynı cihaz konfigürsyonu sağlanmıştır. VLANlar tanımlanmış bu VLANlar gerekli cihazlara konfigüre edilmiştir. PC'ler için DHCP havuzları tanımlanmış ve PC'lerin IP'leri aldığı gözlemlenmiştir. IP telefonlar için VoIP tanımlanmış CEM router üzerinden DHCP havuzu oluşturulmuştur ve TFTP sunucu tanımlanmıştır. IP telefonların IP aldığı gözlemlenmiş ve birbirlerini arayabildikleri görülmüştür. Routerlar üzerinde EIGRP, static ve RIP routing protokolleri tanımlanmıştır. Frame-relay SW üzerinde ve routerlar üzerinde gerekli yapılandırma yapılıp ağların birbirleriyle haberleştiği gözlemlenmiştir. NTP sunucu master ve client data center ve internet ağında tanımlanmıştır. DNS sunucu tanımlanmıştır ve DHCP havuzları üzerinden PC'lere dağıtılmıştır. HTTP sunucu tanımanmış ve erişim gözlemlenmiştir. Local Area Netwokler ve Wide Area Network tam anlamıyla çalışmaktadır. NAT tanımlanmıştır. İç ağ ve dış ağ kontrolü sağlanmıştır. Başka bir deyişle basit bir firewall görevi yapmaktadır. Erişim listeleri tanımlanmıştır. Hangi ağlara erişilecek hangilerine erişilmeyecek belirlenmiştir ve hangi cihazlar hangi cihazlara erişeceği belirlenmiştir. Trunk yapılarım ve spanning tree yapılarım tanımlanmış ve çalıştığı gözlemlenmiştir. Son olarak bu çalışmada CCNA ve CCNP seciyesine ulaşılmıştır. Cisconun bu eğitimlerinde yapılabilecek her şey bu sisteme uygulanmıştır. Hayali bir geniş ağ tasarlanmıştır. ISP tanımlanmıştır. Geniş bir ağda ve yerel bir ağda olması gereken temel cihazlar ve protokoller kullanılmıştır.

Statik ve dinamik IP yapılandırılmalarının eş zamanlı simülasyonu hazırlanmıştır. Simülasyonun sonuçlarında network de bir paketin kaynak ile hedef arasında sorunsuz gidip geldiği görülmüştür.

Belirlenen kurallar çerçevesinde konfigürasyonlar eksiksiz yapılmış ve geniş alan ağı oluşturulmuştur. Günümüz teknolojisine göre tabi eksikleri vardır. Örnek olarak

geniş bir alan ağı yapılandırıldığı için bulut üzerinden paket geçiyor ve hayali bir ISP var. Bundan dolayı frame-relay SW gelmeden firewall tanımlanması gerekir. Tabi sonuçta simülasyon programı kullanıldığı ve gerçek bir labarotuvar ortamı olmadığı için bu tanımlama yapılamamıştır.

Ek olarak bu çalışmaya kablosuz ağlar ve mobil ağlarda eklenebilir. Şunu unutmamak gerekir, sanal bir ortamda çalışıldığı için yapılacak konfigürasyonlar kısıtlıdır.

Cisco Packet Tracer haricinde, Cisco cihazlarla birebir çalışan farklı programlarda vardır. Böyle bir çalışma o programlar üzerinde gerçekleştirip simülasyonu yapılabilir. Ama konu Cisco olduğu için firmanın kendi yazılımını kullanmak daha mantıklıdır.

KAYNAKLAR

ADMINISTRATOR. (2012, 5 10). Cisco CallManager Express Basic Concepts. 4 9, 2015 tarihinde firewall: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-voice/371-cisco-ccme-part-1.html adresinden alındı

ADMINISTRATOR. (2012, 7 14). In-Depth Analysis Of VTP. 4 4, 2015 tarihinde firewall: http://www.firewall.cx/networking-topics/vlan-networks/virtual-trunk-protocol/224-vtp-analysis.html adresinden alındı

ALTANER, C. (2013, 10 25). ntp-network-time-protocol. (cemaltaner, Dü.) 4 9, 2015 tarihinde http://www.cemaltaner.com.tr/2013/10/25/ntp-network-time-protocol/: http://www.cemaltaner.com.tr/2013/10/25/ntp-network-time-protocol/ adresinden alındı

ARAT, B. (2014, 9 7). Datacenter (Veri Merkezi) Nedir ? 4 9, 2015 tarihinde isimtescil: http://blog.isimtescil.net/datacenter-veri-merkezi-nedir/ adresinden alındı

ARISUT, K. (2009, 4 29). Temel Ag Topolojileri. 11 18, 2014 tarihinde cozumpark: http://www.cozumpark.com/blogs/network/archive/2008/04/29/temel-ag-topolojileri.aspx adresinden alındı

ASLANTAŞ, M. (2013, 9 4). Network Ağ Topolojisi. 12 9, 2014 tarihinde bilgievim: http://www.bilgevim.com/network/network-ag-topolojisi.html adresinden alındı

BADUR, B. (2013, 4 17). optik fiber nedir nasıl çalışır. 12 16, 2014 tarihinde mshowto: http://www.mshowto.org/optik-fiber-nedir-nasil-calisir.html adresinden alındı

BAŞKANLIĞI, B. İ. (2013, 9 7). PAN, LAN, MAN, WAN karşılaştırması. 4 9, 2015 tarihinde itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/pan-lan-man-wan-kar%C5%9F%C4%B1la%C5%9Ft%C4%B1rmas%C4%B1 adresinden alındı

BAŞKANLIĞI, İ. B. (2013, 9 7). VLAN Trunking Protocol - Sanal Yerel Ağ Aktarım Protokolü. 4 4, 2015 tarihinde itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/vtp-%28vlan-trunking-protocol---sanal-yerel-a%C4%9F-aktar%C4%B1m-protokol%C3%BC%29 adresinden alındı

BAYRAKÇI, E. V. (2010, 3 27). CCNA (Cisco Certified Network Associate) Nedir? 4 9, 2015 tarihinde sanalkurs: http://sanalkurs.net/ccna-cisco-certified-network-associate-nedir-4067.html adresinden alındı

BENCH, T. (2009, 6 16). How to: Setup and Configure a TFTP Server. 4 9, 2015 tarihinde 888voip: http://www.888voip.com/how-to-setup-and-configure-a-tftp-server/ adresinden alındı

BTEGİTİM. (2012, 10 2). CCNP R&S_egitimi. 4 9, 2015 tarihinde btegitim: http://www.btegitim.com/CCNP%20R&S_egitimi.html adresinden alındı

CISCO. (2009, 9 1). Configuring VTP. 3 16, 2015 tarihinde Cisco: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html adresinden alındı

CISCO. (2012). Configuring IEEE 802.1ak MVRP and MRP. CISCO içinde, Cisco Security Appliance Command Line Configuration Guide (s. 876). Kaliforniya: Cisco Systems. 3 16, 2015 tarihinde http://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd.pdf adresinden alındı

CISCO. (2012, 3 1). Using the Command-Line Interface. 4 2, 2015 tarihinde cİSCO: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_2_JA/command/reference/i1232cr/cr32cli.html adresinden alındı

CISCOTR. (2008, 7 2). Routing (Yönlendirme) - IP Routing - Static Routing - Routing. 4 9, 2015 tarihinde ciscotr: http://ciscotr.blogcu.com/routing-yonlendirme-ip-routing-static-routing-routing/2736731 adresinden alındı

CUBUKCU, F. (2012, 4 11). token ring. 12 16, 2014 tarihinde bilgisayar dershanesi: http://www.bilgisayardershanesi.com/Y5504-token-ring.html adresinden alındı

DİKAY, N. (2010, 5 4). Cisco Router Protokoller. 4 9, 2015 tarihinde nebildikay: http://www.nebildikay.com/ciscoprotokol.html adresinden alındı

DİKİCİ, B. (2013, 9 7). temel ag cihazları. 12 16, 2014 tarihinde itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/temel-a%C4%9F-cihazlar%C4%B1 adresinden alındı

EKİBİ, A. (2013, 6 9). Router-on-a-Stick Inter Vlan Konfigürasyonu. 4 9, 2015 tarihinde agciyiz: http://www.agciyiz.net/index.php/switching/router-on-a-stick-inter-vlan-konfigurasyonu/ adresinden alındı

ELOHAB. (2014, 9 30). VTP Vlan Trunking Protocol Nedir? 3 16, 2015 tarihinde ehaberlesme: http://ehaberlesme.com/vtp-vlan-trunking-protocol-nedir/ adresinden alındı

ERYOL, G. (2002, 12 1). VLAN. 11 18, 2014 tarihinde odtu: http://www.cisn.odtu.edu.tr/2002-7/vlan.php adresinden alındı

GÜLER, P. D. (2008). Bilgisayar Ağları. Gazi Üniversitesi, Elektronik Bilgisyar Bölümü. Ankara: Gazi Üniversitesi.

GÜNGÖRÜR, A. (2009, 7 8). voip. 4 9, 2015 tarihinde firat: web.firat.edu.tr/bilmuh/gaydin/dersler/0809/bmu401/ppt/VOIP.ppt adresinden alındı

HOŞGÖR, E. (2014, 2 17). Bilgisayar Ağı Nedir, Çeşitleri Nelerdir ?, Network . 4 9, 2015 tarihinde get-itlabs: http://get-itlabs.com/bilgisayar-agi-nedir-cesitleri-nelerdir-network-lab-0-2/ adresinden alındı

HOŞGÖR, E. (2014, 5 21). Routing (Yönlendirme) Temelleri Nedir, Bir Network'ler Arasında Nasıl Yönlendirme Yapılır, . 4 9, 2015 tarihinde get-itlabs: http://get-itlabs.com/routing-yonlendirme-temelleri-nedir-bir-networkler-arasinda-nasil-yonlendirme-yapilir-routing-giris-lab-8-1/ adresinden alındı

HOŞGÖR, E. (2014, 5 11). VLAN Trunking Protocol (VTP) Nedir. 3 16, 2015 tarihinde get-itlabs: http://get-itlabs.com/vlan-trunking-protocol-vtp-nedir-lab-7-1/ adresinden alındı

KARAALIOGLU, F. (2008, 3 30). Basit Router Konfigurasyonu. çözümpark. doi:http://www.cozumpark.com/blogs/cisco_system/archive/2008/03/30/basit-router-konfigirasyonu.aspx

KENBER. (2009, 5 4). Cisco IOS Access List (ACL). 4 9, 2015 tarihinde ciscotr: http://www.ciscotr.com/forum/cisco/4079-cisco-ios-access-list-acl.html adresinden alındı

ÖÇKOYMAZ, Ö. (2012, 5 19). dhcp nedir nasıl oluşturulur. 4 9, 2015 tarihinde sistem-ag: http://sistem-ag.blogspot.com.tr/2012/05/dhcp-nedirnasl-olusturulur.html adresinden alındı

SARIGÖZ, M. (2011). web sunucusu. İstnabul: Fatih Üniversitesi. 4 9, 20105 tarihinde www.fatih.edu.tr/~msarioz/source%20224/apache.doc adresinden alındı

SARIYAR, M. (2008, 3 28). voip-nedir-nasil-kurulur. CZOUMPARK, 5. 4 9, 2015 tarihinde https://www.cozumpark.com/blogs/network/archive/2008/03/28/voip-nedir-nasil-kurulur.aspx adresinden alındı

SOLMAZ, E. (2008, 5 12). Domain Name System. czodumpark, 10. 9 4, 2015 tarihinde http://www.cozumpark.com/blogs/windows_server/archive/2008/05/12/dns-domain-name-system.aspx adresinden alındı

SYSTEM. (2008, 7 24). stp-spanning-tree-nedir-spanning-tree-konfigurasyonu-stp-nedir. 4 9, 215 tarihinde ciscotr: http://www.ciscotr.com/stp-spanning-tree-nedir-spanning-tree-konfigurasyonu-stp-nedir.html adresinden alındı

ŞAHAN, A. A. (2009, 4 18). frame relay. 4 9, 2015 tarihinde sahhan: http://www.sahhan.com/cisco/teknolojiler/FrameRelay/Frame%20Relay.pdf adresinden alındı

ŞANLI, Y. (2013, 3 10). Cisco Packet Tracer. 11 18, 2014 tarihinde slideshare: http://www.slideshare.net/yildiraysanli/cisco-packet-tracer-17085371 adresinden alındı

ŞENER, A. (2014, 3 27). IGRP ROUTING (Dinamik Routing). 4 9, 2015 tarihinde ccnaegitimi: http://www.ccnaegitimi.com/2014/03/27/igrp-routing-dinamik-routing/ adresinden alındı

TASKIRAN, A. (2006). İstanbul: EnderUnix Yazılım Geliştirme Takımı. 4 9, 2016 tarihinde http://www.enderunix.org/docs/Cisco_Networks_Routing.pdf adresinden alındı

TECHNET. (2015, 1 2). NAT Nedir? 4 9, 2015 tarihinde microsoft: https://technet.microsoft.com/tr-tr/library/cc753373%28v=ws.10%29.aspx adresinden alındı

TÜRKERİ, N. (2011, 7 21). Routing Information Protocol (RIP). 4 9, 2015 tarihinde mshowto: http://www.mshowto.org/routing-information-protocol-rip.html adresinden alındı

WEBSTAR, O. (2014, 1 20). ICMP (Internet Control Message Protocol) Nedir? 4 2015, 9 tarihinde reitix: http://www.reitix.com/Makaleler/ICMP-%28Internet-Control-Message-Protocol%29-Nedir/ID=1543 adresinden alındı

WINDOWS. (2014, 5 9). İnternet Servis Sağlayıcısı (ISS) nedir? 4 9, 2015 tarihinde microsoft: http://windows.microsoft.com/tr-tr/windows/what-is-internet-service-provider#1TC=windows-7 adresinden alındı

YAŞAR, F. (2011, 5 4). mshowto. 11 13, 2014 tarihinde Switch Nedir Nasil Calisir Ilk Ayarlar Nasil Yapilir: http://www.mshowto.org/switch-nedir-nasil-calisir-ilk-ayarlar-nasil-yapilir.html adresinden alındı

YILDIRIM, Z. (2010, 10 1). ciscotr. 12 16, 2014 tarihinde Ethernet Yapisi: http://www.ciscotr.com/ethernet-yapisi.html adresinden alındı

EKLER

EK A : Konfigürasyon Kodları

Ağda oluşturulan konfigürasyonun kodları cihaz isimlerine göre ekte verilmiştir.

SW_WB1;

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config)#hostname SW_WB1
SW_WB1(config-if)#ip address 172.16.1.1 255.255.255.0
SW_WB1(config-if)#no shutdown
SW_WB1(config-if)#exit
SW_WB1(config)#ip default-gateway 172.16.1.254
SW_WB1(config)#vlan 30
SW_WB1(config-vlan)#name DATA1_WB
SW_WB1(config-vlan)#vlan 40
SW_WB1(config-vlan)#name DATA2_WB
SW_WB1(config-vlan)#vlan 10
SW_WB1(config-vlan)#name VOICE_WB
SW_WB1(config)#vtp mode server
SW_WB1(config)#vtp domain WB
SW_WB1(config)#vtp password 1234
SW_WB1(config)#vtp version 2
SW_WB1(config)#interface range fastEthernet 0/2-4
SW_WB1(config-if-range)#switchport mode access
SW_WB1(config-if-range)#switchport mode trunk
SW_WB1(config)#interface fastEthernet 0/1
SW_WB1(config-if)#switchport mode access
SW_WB1(config-if)#switchport access vlan 40
```

SW_WB2;

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_WB2
SW_WB2(config)#interface vlan 1
SW_WB2(config-if)#ip address 172.16.1.2 255.255.255.0
SW_WB2(config-if)#no shutdown
SW_WB2(config-if)#exit
SW_WB2(config)#interface fastEthernet 0/24
SW_WB2(config-if)#switchport mode access
SW_WB2(config-if)#switchport mode trunk
SW_WB2(config)#vtp mode client
SW_WB2(config)#vtp domain WB
SW_WB2(config)#vtp password 1234
SW_WB2(config)#interface fastEthernet 0/7
SW_WB2(config-if)#switchport mode access
SW_WB2(config-if)#switchport access vlan 30
SW_WB2(config-if)#do write
SW_WB2(config)#interface range fastEthernet 0/2-6
SW_WB2(config-if-range)#switchport mode access
SW_WB2(config-if-range)#switchport mode trunk
SW_WB2(config-if-range)#switchport trunk allowed vlan 30,40
SW_WB2(config-if-range)#switchport voice vlan 10
```

SW_WB3;

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_WB3
SW_WB3(config)#interface vlan 1
SW_WB3(config-if)#ip address 172.16.1.3 255.255.255.0
SW_WB3(config-if)#no shutdown
```

SW_WB3(config-if)#exit
SW_WB3(config)#interface fastEthernet 0/24
SW_WB3(config-if)#switchport mode access
SW_WB3(config-if)#switchport mode trunk
SW_WB3(config)#vtp mode client
SW_WB3(config)#vtp domain WB
SW_WB3(config)#vtp password 1234
SW_WB3(config)#interface fastEthernet 0/7
SW_WB3(config-if)#switchport mode access
SW_WB3(config-if)#switchport access vlan 40
SW_WB3(config-if)#do write
SW_WB3(config)#interface range fastEthernet 0/2-6
SW_WB3(config-if-range)#switchport mode access
SW_WB3(config-if-range)#switchport mode trunk
SW_WB3(config-if-range)#switchport trunk allowed vlan 30,40
SW_WB3(config-if-range)#switchport voice vlan 10

CME_WB;

Router>enable
Router#configure terminal
Router(config)#hostname CME_WB
CME_WB(config)#interface fastEthernet 0/0
CME_WB(config-if)#ip address 172.16.1.254 255.255.255.0
CME_WB(config-if)#no shutdown
CME_WB(config-if)#exit
CME_WB(config)#interface fastEthernet 0/0.10
CME_WB(config-subif)#encapsulation dot1Q 10
CME_WB(config-subif)#ip address 172.16.10.254 255.255.255.0
CME_WB(config-subif)#exit
CME_WB(config)#interface fastEthernet 0/0.30

```
CME_WB(config-subif)#encapsulation dot1Q 30
CME_WB(config-subif)#ip address 172.16.30.254 255.255.255.0
CME_WB(config-subif)#ip helper-address 172.16.40.1
CME_WB(config-subif)#exit
CME_WB(config)#interface fastEthernet 0/0.40
CME_WB(config-subif)#encapsulation dot1Q 40
CME_WB(config-subif)#ip address 192.168.40.254 255.255.255.0
CME_WB(config-subif)#exit
CME_WB(config)#ip dhcp pool VLAN10
CME_WB(dhcp-config)#network 172.16.10.0 255.255.255.0
CME_WB(dhcp-config)#default-router 172.16.10.254
CME_WB(dhcp-config)#dns-server 4.2.2.2
CME_WB(dhcp-config)#lease 8 0 0
CME_WB(dhcp-config)#option 150 ip 172.18.3.3
CME_WB(config)#ip dhcp excluded-address 172.16.10.254 255.255.255.0
CME_WB(config)#ip dhcp excluded-address 172.16.10.1 255.255.255.0
CME_WB(config)#telephony-service
CME_WB(config-telephony)#max-dn 10
CME_WB(config-telephony)#max-ephones 10
CME_WB(config-telephony)#ip source-address 172.16.10.254 port 1000
CME_WB(config-telephony)#exit
CME_WB(config)#ephone-dn 1
CME_WB(config-ephone-dn)#number 1001
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 2
CME_WB(config-ephone-dn)#number 1002
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 3
CME_WB(config-ephone-dn)#number 1003
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 4
CME_WB(config-ephone-dn)#number 1004
CME_WB(config-ephone-dn)#exit
```

```
CME_WB(config)#ephone-dn 5
CME_WB(config-ephone-dn)#number 1005
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 11
CME_WB(config-ephone-dn)#number 1011
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 12
CME_WB(config-ephone-dn)#number 1012
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 13
CME_WB(config-ephone-dn)#number 1013
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 14
CME_WB(config-ephone-dn)#number 1014
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone-dn 15
CME_WB(config-ephone-dn)#number 1015
CME_WB(config-ephone-dn)#exit
CME_WB(config)#ephone 1
CME_WB(config-ephone)#button 1:1
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 2
CME_WB(config-ephone)#button 1:2
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 3
CME_WB(config-ephone)#button 1:3
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 4
CME_WB(config-ephone)#button 1:4
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 5
```

```
CME_WB(config-ephone)#button 1:5
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 11
CME_WB(config-ephone)#button 1:11
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 12
CME_WB(config-ephone)#button 1:12
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 13
CME_WB(config-ephone)#button 1:13
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 14
CME_WB(config-ephone)#button 1:14
CME_WB(config-ephone)#exit
CME_WB(config)#ephone 15
CME_WB(config-ephone)#button 1:15
CME_WB(config-ephone)#exit
CME_WB(config)#router eigrp 101
CME_WB(config-router)#no auto-summary
CME_WB(config-router)#network 172.16.1.0 0.0.0.255
CME_WB(config-router)#network 172.16.10.0 0.0.0.255
CME_WB(config-router)#network 172.16.30.0 0.0.0.255
CME_WB(config-router)#network 172.16.40.0 0.0.0.255
```

R_WB_GW;

```
Router>enable
Router#configure terminal
Router(config)#hostname R_WB_GW
R_WB_GW(config)#interface fastEthernet 0/1
R_WB_GW(config-if)#ip address 172.16.40.1 255.255.255.0
R_WB_GW(config-if)#no shutdown
R_WB_GW(config)#ip dhcp pool VLAN40
```

R_WB_GW(dhcp-config)#network 172.16.40.0 255.255.255.0

R_WB_GW(dhcp-config)#default-router 172.16.40.254

R_WB_GW(dhcp-config)#dns-server 4.2.2.2

R_WB_GW(dhcp-config)#lease 8 0 0

R_WB_GW(config)#ip dhcp excluded-address 172.16.40.254 255.255.255.0

R_WB_GW(config)#ip dhcp excluded-address 172.16.40.1 255.255.255.0

R_WB_GW(config)#ip dhcp excluded-address 172.16.40.90 255.255.255.0

R_WB_GW(config)#ip dhcp pool VLAN30

R_WB_GW(dhcp-config)#network 172.16.30.0 255.255.255.0

R_WB_GW(dhcp-config)#default-router 172.16.30.254

R_WB_GW(dhcp-config)#dns-server 4.2.2.2

R_WB_GW(dhcp-config)#lease 8 0 0

R_WB_GW(config)#ip dhcp excluded-address 172.16.30.254 255.255.255.0

R_WB_GW(config)#ip dhcp excluded-address 172.16.30.1 255.255.255.0

R_WB_GW(config)#ip dhcp excluded-address 172.16.30.90 255.255.255.0

R_WB_GW(config)#router eigrp 101

R_WB_GW(config-router)#no auto-summary

R_WB_GW(config-router)#network 192.168.40.0 0.0.0.255

R_WB_GW(config-router)#network 10.1.1.1.0 0.0.0.252

R_WB_GW(config)#interface Serial0/0/0

R_WB_GW(config-if)#clock rate 2000000

R_WB_GW(config-if)#ip address 10.1.1.2 255.255.255.252

R_WB_GW(config-if)#no shutdown

R_WB_GW(config)#interface serial 0/0/0.103 point-to-point

R_WB_GW(config-subif)#ip address 10.1.1.54 255.255.255.252

R_WB_GW(config-subif)#frame-relay interface-dlci 103

R_WB_GW(config-subif)#bandwith 64

R_WB_GW(config-subif)#exit

R_WB_GW(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.54

SW_EB1;

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_EB1
SW_EB1(config)#interface vlan 1
SW_EB1(config-if)#ip address 172.17.2.1 255.255.255.0
SW_EB1(config-if)#no shutdown
SW_EB1(config-if)#exit
SW_EB1(config)#ip default-gateway 172.17.2.254
SW_EB1(config)#vlan 35
SW_EB1(config-vlan)#name DATA1_EB
SW_EB1(config-vlan)#vlan 45
SW_EB1(config-vlan)#name DATA2_EB
SW_EB1(config-vlan)#vlan 15
SW_EB1(config-vlan)#name VOICE_EB
SW_EB1(config)#vtp mode server
SW_EB1(config)#vtp domain EB
SW_EB1(config)#vtp password 1234
SW_EB1(config)#vtp version 2
SW_EB1(config)#interface range fastEthernet 0/2-4
SW_EB1(config-if-range)#switchport mode access
SW_EB1(config-if-range)#switchport mode trunk
SW_EB1(config)#interface fastEthernet 0/1
SW_EB1(config-if)#switchport mode access
SW_EB1(config-if)#switchport access vlan 35
```

SW_EB2;

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_EB2
SW_EB2(config)#interface vlan 1
```

SW_EB2(config-if)#ip address 172.17.2.2 255.255.255.0
SW_EB2(config-if)#no shutdown
SW_EB2(config-if)#exit
SW_EB2(config)#interface fastEthernet 0/24
SW_EB2(config-if)#switchport mode access
SW_EB2(config-if)#switchport mode trunk
SW_EB2(config)#vtp mode client
SW_EB2(config)#vtp domain EB
SW_EB2(config)#vtp password 1234
SW_EB2(config)#interface fastEthernet 0/7
SW_EB2(config-if)#switchport mode access
SW_EB2(config-if)#switchport access vlan 35
SW_EB2(config-if)#do write
SW_EB2(config)#interface range fastEthernet 0/2-6
SW_EB2(config-if-range)#switchport mode access
SW_EB2(config-if-range)#switchport mode trunk
SW_EB2(config-if-range)#switchport trunk allowed vlan 35,45
SW_EB2(config-if-range)#switchport voice vlan 15

SW_EB3

Switch>enable
Switch#configure terminal
Switch(config)#hostname SW_EB3
SW_EB3(config)#interface vlan 1
SW_EB3(config-if)#ip address 172.17.2.3 255.255.255.0
SW_EB3(config-if)#no shutdown
SW_EB3(config-if)#exit
SW_EB3(config)#interface fastEthernet 0/24
SW_EB3(config-if)#switchport mode access
SW_EB3(config-if)#switchport mode trunk

SW_EB3(config)#vtp mode client
SW_EB3(config)#vtp domain EB
SW_EB3(config)#vtp password 1234
SW_EB3(config)#interface fastEthernet 0/7
SW_EB3(config-if)#switchport mode access
SW_EB3(config-if)#switchport access vlan 45
SW_EB3(config-if)#do write
SW_EB3(config)#interface range fastEthernet 0/2-6
SW_EB3(config-if-range)#switchport mode access
SW_EB3(config-if-range)#switchport mode trunk
SW_EB3(config-if-range)#switchport trunk allowed vlan 35,45
SW_EB3(config-if-range)#switchport voice vlan 15

CME_EB

Router>enable
Router#configure terminal
Router(config)#hostname CME_EB
CME_EB(config)#interface fastEthernet 0/0
CME_EB(config-if)#ip address 172.17.2.254 255.255.255.0
CME_EB(config-if)#no shutdown
CME_EB(config-if)#exit
CME_EB(config)#interface fastEthernet 0/0.15
CME_EB(config-subif)#encapsulation dot1Q 15
CME_EB(config-subif)#ip address 172.16.15.254 255.255.255.0
CME_EB(config-subif)#exit
CME_EB(config)#interface fastEthernet 0/0.35
CME_EB(config-subif)#encapsulation dot1Q 35
CME_EB(config-subif)#ip address 172.16.35.254 255.255.255.0
CME_EB(config-subif)#ip helper-address 172.16.35.1
CME_EB(config-subif)#exit
CME_EB(config)#interface fastEthernet 0/0.45
CME_EB(config-subif)#encapsulation dot1Q 45

CME_EB(config-subif)#ip address 192.168.45.254 255.255.255.0

CME_EB(config-subif)#ip helper-address 172.16.35.1

CME_EB(config-subif)#exit

CME_EB(config)#ip dhcp pool VLAN15

CME_EB(dhcp-config)#network 172.16.15.0 255.255.255.0

CME_EB(dhcp-config)#default-router 172.16.15.254

CME_EB(dhcp-config)#dns-server 4.2.2.2

CME_EB(dhcp-config)#lease 8 0 0

CME_EB(dhcp-config)#option 150 ip 172.18.3.3

CME_EB(config)#ip dhcp excluded-address 172.16.15.254 255.255.255.0

CME_EB(config)#ip dhcp excluded-address 172.16.15.1 255.255.255.0

CME_EB(config)#telephony-service

CME_EB(config-telephony)#max-dn 20

CME_EB(config-telephony)#max-ephones 20

CME_EB(config-telephony)#ip source-address 172.16.15.254 port 2000

CME_EB(config-telephony)#exit

CME_EB(config)#ephone-dn 1

CME_EB(config-ephone-dn)#number 2001

CME_EB(config-ephone-dn)#exit

CME_EB(config)#ephone-dn 2

CME_EB(config-ephone-dn)#number 2002

CME_EB(config-ephone-dn)#exit

CME_EB(config)#ephone-dn 3

CME_EB(config-ephone-dn)#number 2003

CME_EB(config-ephone-dn)#exit

CME_EB(config)#ephone-dn 4

CME_EB(config-ephone-dn)#number 2004

CME_EB(config-ephone-dn)#exit

CME_EB(config)#ephone-dn 5

CME_EB(config-ephone-dn)#number 2005

CME_EB(config-ephone-dn)#exit

```
CME_EB(config)#ephone-dn 36
CME_EB(config-ephone-dn)#number 2036
CME_EB(config-ephone-dn)#exit
CME_EB(config)#ephone-dn 37
CME_EB(config-ephone-dn)#number 2037
CME_EB(config-ephone-dn)#exit
CME_EB(config)#ephone-dn 38
CME_EB(config-ephone-dn)#number 2038
CME_EB(config-ephone-dn)#exit
CME_EB(config)#ephone-dn 39
CME_EB(config-ephone-dn)#number 2039
CME_EB(config-ephone-dn)#exit
CME_EB(config)#ephone-dn 40
CME_EB(config-ephone-dn)#number 2040
CME_EB(config-ephone-dn)#exit
CME_EB(config)#ephone 1
CME_EB(config-ephone)#button 1:1
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 2
CME_EB(config-ephone)#button 1:2
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 3
CME_EB(config-ephone)#button 1:3
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 4
CME_EB(config-ephone)#button 1:4
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 5
CME_EB(config-ephone)#button 1:5
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 36
CME_EB(config-ephone)#button 1:36
CME_EB(config-ephone)#exit
```

```
CME_EB(config)#ephone 37
CME_EB(config-ephone)#button 1:37
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 38
CME_EB(config-ephone)#button 1:38
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 39
CME_EB(config-ephone)#button 1:39
CME_EB(config-ephone)#exit
CME_EB(config)#ephone 40
CME_EB(config-ephone)#button 1:40
CME_EB(config-ephone)#exit
CME_EB(config)#router eigrp 101
CME_EB(config-router)#no auto-summary
CME_EB(config-router)#network 172.17.2.0 0.0.0.255
CME_EB(config-router)#network 172.16.15.0 0.0.0.255
CME_EB(config-router)#network 172.16.35.0 0.0.0.255
CME_EB(config-router)#network 172.16.45.0 0.0.0.255
```

R_EB_GW

```
Router>enable
Router#configure terminal
Router(config)#hostname R_EB_GW
R_EB_GW(config)#interface fastEthernet 0/1
R_EB_GW(config-if)#ip address 172.16.35.1 255.255.255.0
R_EB_GW(config-if)#no shutdown
R_EB_GW(config)#ip dhcp pool VLAN35
R_EB_GW(dhcp-config)#network 172.16.35.0 255.255.255.0
```

R_EB_GW(dhcp-config)#default-router 172.16.35.254

R_EB_GW(dhcp-config)#dns-server 4.2.2.2

R_EB_GW(dhcp-config)#lease 8 0 0

R_EB_GW(config)#ip dhcp excluded-address 172.16.35.254 255.255.255.0

R_EB_GW(config)#ip dhcp excluded-address 172.16.35.1 255.255.255.0

R_EB_GW(config)#ip dhcp excluded-address 172.16.35.90 255.255.255.0

R_EB_GW(config)#ip dhcp pool VLAN45

R_EB_GW(dhcp-config)#network 172.16.45.0 255.255.255.0

R_EB_GW(dhcp-config)#default-router 172.16.45.254

R_EB_GW(dhcp-config)#dns-server 4.2.2.2

R_EB_GW(dhcp-config)#lease 8 0 0

R_EB_GW(config)#ip dhcp excluded-address 172.16.45.254 255.255.255.0

R_EB_GW(config)#ip dhcp excluded-address 172.16.45.1 255.255.255.0

R_EB_GW(config)#ip dhcp excluded-address 172.16.45.90 255.255.255.0

R_EB_GW(config)#router eigrp 101

R_EB_GW(config-router)#no auto-summary

R_EB_GW(config-router)#network 192.168.35.0 0.0.0.255

R_EB_GW(config-router)#network 10.1.1.1.0 0.0.0.252

R_EB_GW(config)#interface Serial0/0/0

R_EB_GW(config-if)#clock rate 2000000

R_EB_GW(config-if)#ip address 10.1.1.54 255.255.255.252

R_EB_GW(config-if)#no shutdown

R_EB_GW(config)#interface serial 0/0/0.102 point-to-point

R_EB_GW(config-subif)#ip address 10.1.1.2 255.255.255.252

R_EB_GW(config-subif)#frame-relay interface-dlci 102

R_EB_GW(config-subif)#bandwith 64

R_EB_GW(config-subif)#exit

R_EB_GW(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

R_DC;

Router>enable

Router#configure terminal

```
Router(config)hostname R_DC
R_DC(config)#banner motd #Data Center Gateway - Access with Password#
R_DC(config)#line console 0
R_DC(config-line)#password 1234
R_DC(config-line)#login
R_DC(config-line)#do wr
R_DC(config-line)#line vty 0
R_DC(config-line)#password 1234
R_DC(config-line)#login
R_DC(config-line)#do wr
R_DC(config-line)#enable password 1234
R_DC(config-line)#enable secret 1234
R_DC(config)#interface fastEthernet 0/0
R_DC(config-if)#ip address 172.18.3.254 255.255.255.0
R_DC(config-if)#no shutdown
R_DC(config)#ip dhcp pool VLAN1
R_DC(dhcp-config)#network 172.16.3.0 255.255.255.0
R_DC(dhcp-config)#default-router 172.16.3.254
R_DC(dhcp-config)#dns-server 4.2.2.2
R_DC(dhcp-config)#lease 8 0 0
R_DC(config)#ip dhcp excluded-address 172.16.3.254 255.255.255.0
R_DC(config)#ip dhcp excluded-address 172.16.3.1 172.16.3.10
R_DC(config)#interface Serial0/2/0
R_DC(config-if)#description Encrypted Port
R_DC(config-if)#clock rate 2000000
R_DC(config-if)#ip address 68.110.171.134 255.255.255.252
R_DC(config-if)#no shutdown
R_DC(config)#interface serial 0/0/0.201 point-to-point
R_DC(config-subif)#ip address 10.1.1.2 255.255.255.252
R_DC(config-subif)#frame-relay interface-dlci 201
R_DC(config-subif)#bandwith 64
```

R_DC(config-subif)#exit

R_DC(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2

R_DC(config)#interface serial 0/0/0.301 point-to-point

R_DC(config-subif)#ip address 10.1.1.54 255.255.255.252

R_DC(config-subif)#frame-relay interface-dlci 301

R_DC(config-subif)#bandwith 64

R_DC(config-subif)#exit

R_DC(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.54

R_DC(config)#ip nat pool recep 85.5.5.1 85.5.5.1 netmask 255.255.255.0

R_DC(config)#ip nat inside source list 1 pool recep overload

R_DC(config)#interface FastEthernet0/0

R_DC(config)#ip nat inside

R_DC(config)#interface Serial0/0/0

R_DC(config)#ip nat outside

R_DC(config)#access-list 1 permit 10.1.1.0 0.0.0.252

R_DC(config)#ip access-list standard 40

R_DC(config-std-nacl)#deny 192.168.40.0 0.0.0.255

R_DC(config-std-nacl)#permit host 172.16.30.90

R_DC(config-std-nacl)#permit host 172.16.40.90

R_DC(config-std-nacl)#permit 10.1.1.0 0.0.0.252

R_DC(config)#ip access-list standard 35

R_DC(config-std-nacl)#deny 192.168.35.0 0.0.0.255

R_DC(config-std-nacl)#permit host 172.16.35.90

R_DC(config-std-nacl)#permit host 172.16.45.90

R_DC(config-std-nacl)#permit 10.1.1.0 0.0.0.252

R_DC(config)#ip access-list standard 1

R_DC(config-std-nacl)#permit any

R_DC(config)# ntp server 4.2.2.3

R_DC(config)# end

SW_DC;

Switch#configure terminal

Switch(config)#hostname SW_DC
SW_DC(config)#interface vlan 1
SW_DC(config-if)#ip address 172.16.3.1 255.255.255.0
SW_DC(config-if)#no shutdown
SW_DC(config-if)#exit
SW_DC(config)#interface Serial0/2/0
SW_DC(config-if)#clock rate 9600
SW_DC(config-if)#ip address 68.110.171.134 255.0.0.0
SW_DC(config-if)#ip address 68.110.171.134 255.255.255.0
SW_DC(config-if)#no shutdown

R_ISP;

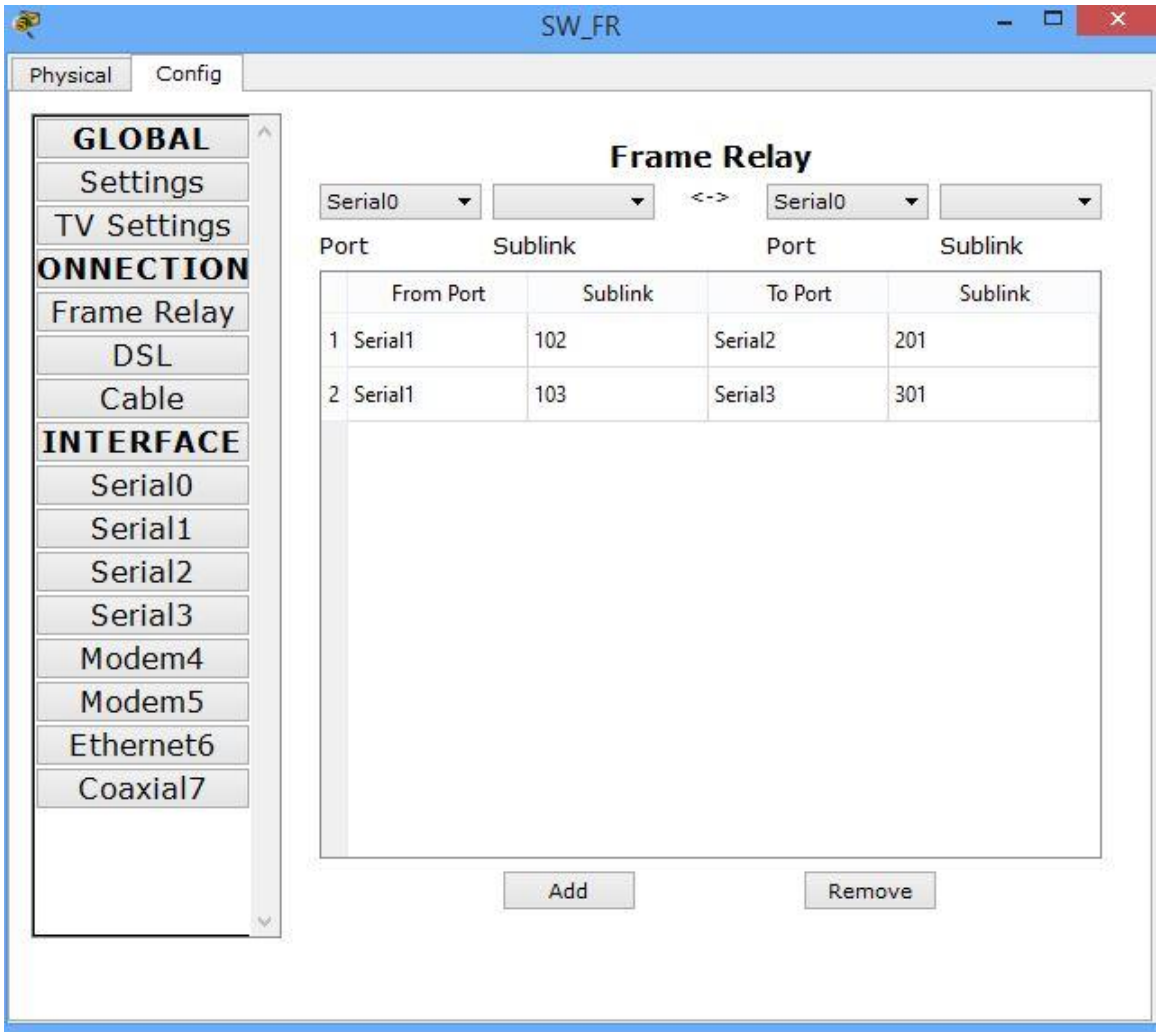
Router>enable
Router#configure terminal
Router(config)#hostname R_ISP
R_ISP(config)#interface Serial0/1/1
R_ISP(config-if)#clock rate 2000000
R_ISP(config-if)#ip address 68.110.171.133 255.255.255.252
R_ISP(config-if)#no shutdown
R_ISP(config-if)#no exit
R_ISP(config)#ip route 172.18.3.0 255.255.255.0 68.110.171.134
R_ISP(config)#interface Serial0/1/0
R_ISP(config-if)#clock rate 9600
R_ISP(config-if)#ip address 55.55.55.57 255.255.255.252
R_ISP(config-if)#no shutdown
R_ISP(config)#ip route 4.2.2.0 255.255.255.0 55.55.55.58

R_INT;

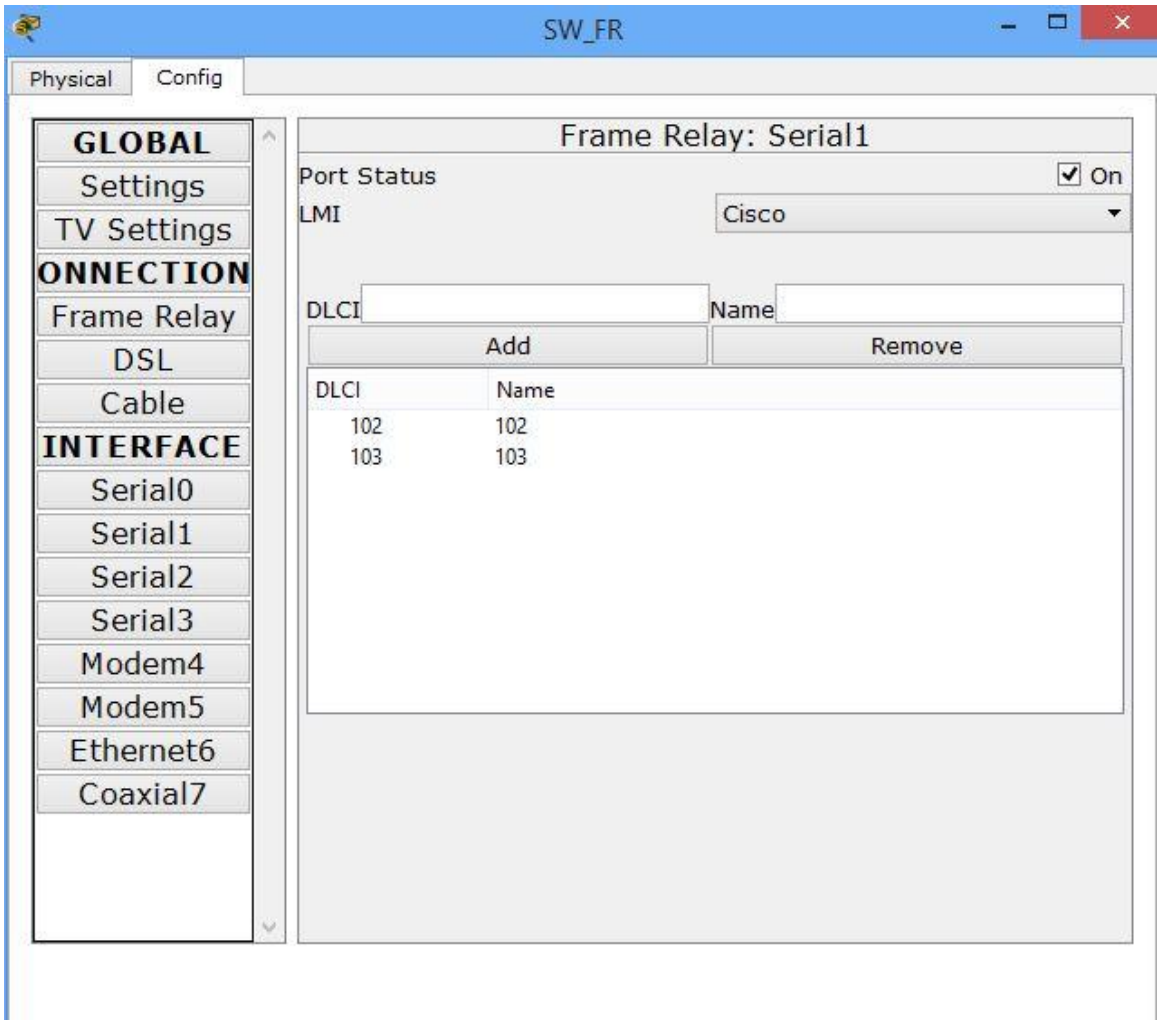
Router>enable

```
Router#configure terminal
Router(config)#hostname R_INT
R_INT(config)#interface Serial0/3/0
R_INT(config-if)#clock rate 2000000
R_INT(config-if)#ip address 55.55.55.58 255.255.255.252
R_INT(config-if)#no shutdown
R_INT(config)#interface fastEthernet 0/0
R_INT(config-if)#ip address 4.2.2.254 255.255.255.0
R_INT(config-if)#no shutdown
R_INT#clock set 18:21:00 apr 8 2015
R_INT(config)# clock time EST -5
R_INT(config)# clock summer-time EST recurring
R_INT(config)# ntp master 3
R_INT(config)# end
```

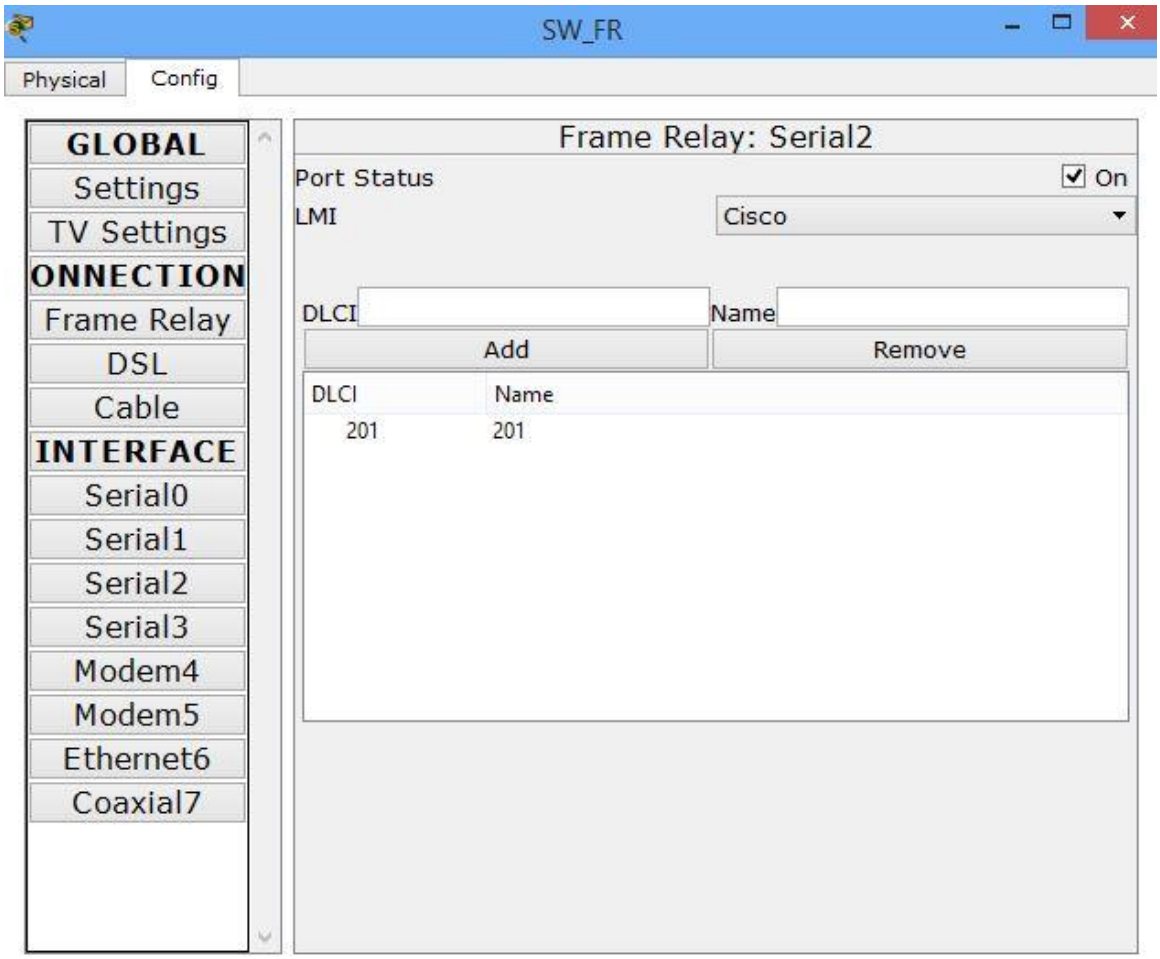
SW_FR;



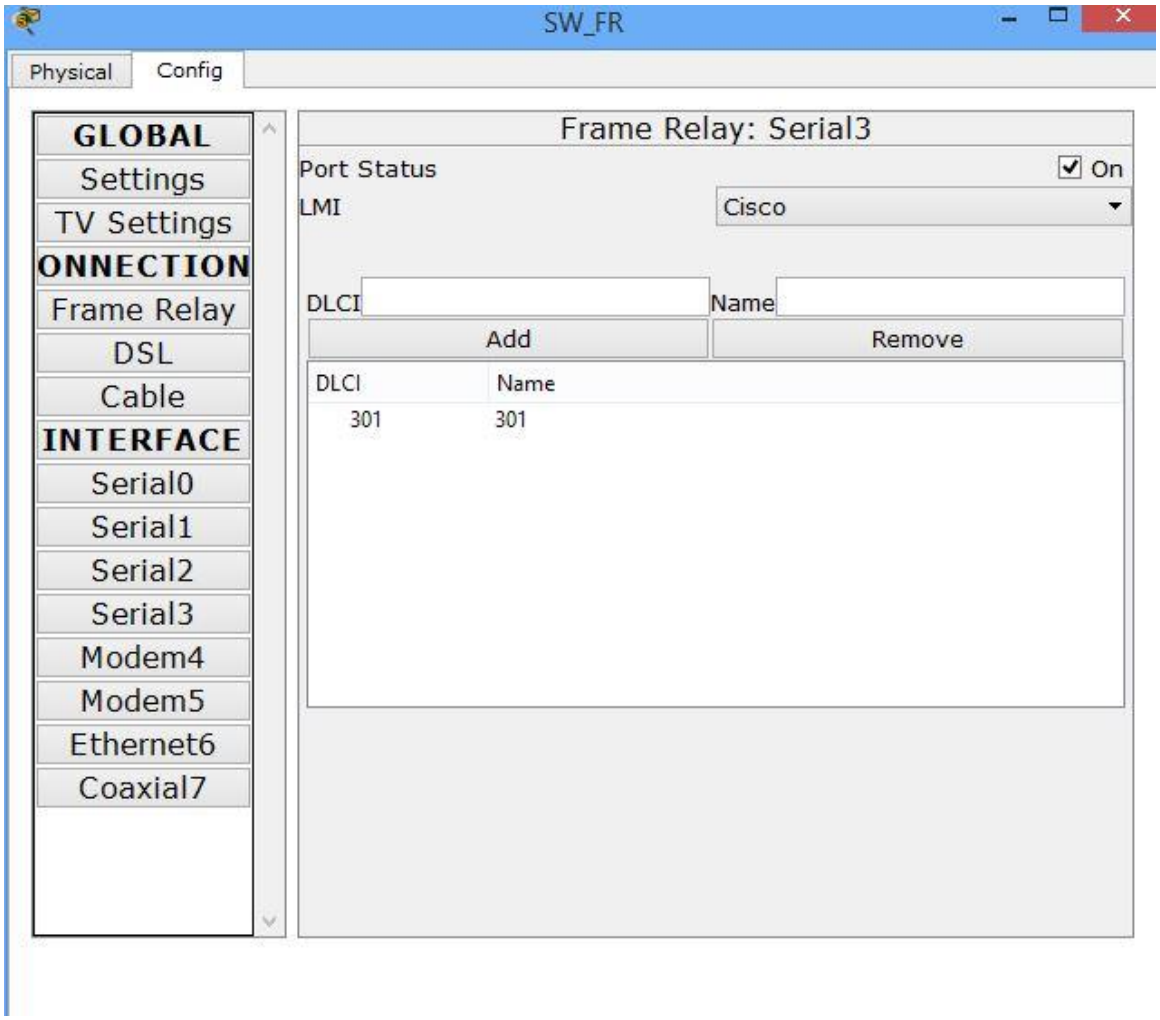
Şekil 7.1 Frame-relay konfigürasyonu 1



Şekil 7.2 Frame-relay konfigürasyonu 2



Şekil 7.3 Frame-relay konfigürasyonu 3



Şekil 7.4 Frame-relay konfigürasyonu 4

ÖZGEÇMİŞ

Ad-Soyad **:** Muhammet Emin KAMİLOĞLU
Doğum Tarihi ve Yeri : 1988/Istanbul
E-Posta **:** m.emin.kamiloglu@hotmail.com

ÖĞRENİM DUERUMU

Ön Lisans **:** T.C. İstanbul Arel Üniversitesi / Bilgisayar Teknolojisi ve Programlama
Lisans **:** T.C. İstanbul Arel Üniversitesi / Matematik-Bilgisayar
Yüksek Lisans : T.C. İstanbul Aydın Üniversitesi / Bilgisayar Mühendisliği