T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

NS VEYA PAKET İZLEYİCİ GİBİ SİMÜLASYON ARACINI KULLANARAK BİR AĞ PERFORMANSI DEĞERLENDİRMESI

YÜKSEK LİSANS TEZİ

SAYED MANSOOR HASHİMİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI

OCAK, 2017

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 **Y1413.010015** numaralı öğrencisi **Sayed Mansoor HASHIMI**'nın **"NS VEYA PAKET İZLEYİCİ GİBİ BAZI SİMULASYON ARACINI KULLANARAK BİR AĞ PERFORMANSI DEĞERLENDİRMESİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 10.01.2017 tarih ve 2017/01 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi : 26.01.2017	
1)Tez Danışmanı: Prof. Dr. Ali GÜNEŞ	.....
2) Jüri Üyesi : Yrd. Doç. Dr. Köksal MUŞ	.....
3) Jüri Üyesi : Yrd. Doç. Dr. Ferdi SÖNMEZ	.....

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

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "NS VEYA PAKET İZLEYİCİ GİBİ BAZI SİMÜLASYON ARACINI KULLANARAK BİR AĞ PERFORMANS DEĞERLENDİRME (SİMÜLASYON)" 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.

Aday / İmza

ÖNSÖZ

Bu tez çalışması, ağ performans değerlendirilmesinde çeşitli parametreler nasıl bir araya toplanır, nasıl incelenir ve sonuç olarak performansı düşüren sebepleri ortadan kaldırmak için ağ tasarımı yaparken nelere dikkat edilmelisi gerektiğini anlamak için pratik bir kılavuz olacaktır. Bu sebeple hem CISCO Packet Tracer'de hem de eNSP (Enterprise Network Simulation Platform)'de geniş alan ağları tasarlanmıştır. Bu tasarımlar da CCNA, CCNP, HCNA ve HCNP eğitim seviyesinde kullanılabilecek temel konfigürasyonlar kullanılacaktır. Bu eğitimleri bitiren kişiler LAN, WAN, WLAN ve WWAN ağ dizaynını, router ve switch gibi aktif ağ cihazlarının konfigürasyonlarını, ağın optimizasyon ve performans ayarlarının yapabilir ve gerektiğinde ayarların bakımlarını da yapabilirler.

Bu tezin başarısının bir kısmı kendi çabalarım diğer bir kısmı da büyük ölçüde teeşvik ve kurallara bağlıdır.Geçirdiğim eğitim süreci boyunca ilminden ve tecrübelerinden yararlandığım tüm hocalarıma ve bu projenin başarıyla tamamlanması vesile olan kişilere saygılarımı ve şükranlarımı sunuyorum. Ayrıca geniş bilgi birikimi, yol göstericiliği ve tecrübesiyle çalışmam süresince benden desteğini ve yardımını esirgemeyen , Sayın Prof. Dr. Ali GÜNEŞ'e sonsuz saygı ve şükranlarımı sunarak, 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.

Ocak 2017 Sayed Mansoor HASHIMI

İÇİNDEKİLER

Sayfa

KISALTMALAR

ACL :Access List (Erişim Listesi)
AP :Access Point (Erişim Noktası)
ATM :Asynchronous Transfer Mode (Eşzamansız Aktarım Modu)
BBS :Backbone Switch (Omurga Anahtarı)
BPDU :Bridge Protocol Data Units (Köprü Protokolü Veri Birimi)
CCMP :Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu)
CSMA/CD :Carrier sense multiple access/Collision Detection (Taşıyıcı duyarlıklı çoğul erişim/Çarpışma kontrolü)
CLI : Command Line Interface (Komut Satırı Arayüzü)
CME : Call Manager Express (Çağrı Yöneticisi Ekspres)
DDoS :Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DHCP :Dynamic Host Configuration Protocol (Dinamik Ana BilgisayarYapılandırma Protokolü)
DN : Dialed Number(Aranan Numara)
DNS :Domain Name Server (Alan Adı Sunucusu)
DoS :Denial of Service (Servis Reddi)
EIGRP : Enhanced Interior Gateway Routing Protocol (Geliştirilmiş İç Ağ Geçidi Yönlendirme Protokolü)
eNSP : Enterprise Network Simulation Platform
ETSI :European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
FDDI :Fiber Distributed Data Interface (Fiber Dağıtımlı Veri Arayüzü)
FW :Firewall (güvenlik duvarı)
Gbps :Gigabit per second (Saniyede bir milyar bit)
Ghz :Gigahertz (Saniyede bir milyar devir)
HTTP :Hypertext Transfer Protocol (Üstmetin Aktarım Protokolü)
ICMP :Internet Control Message Protocol (İnternet Kontrol Mesajı Protokolü)
IP :Internet Protocol (İnternet Protokolü)
ISP :Internet Service Provider (İnternet Servis Sağlayıcısı)
IGRP : Interior Gateway Routing Protocol (İç Ağ Geçidi Yönlendirme Protokolü)
IT : Information Technology (Bilgi-Bilişim Teknolojisi)
LAN :Local Area Networks (Yerel alan ağları)
LSW :Layer Switch (Katman Anahtarı)
MAC : Media Access Control (Ortam Erişim Yönetimi)
MAN :Metropolitan Area Network (Kentsel alan ağı)
Mbps :Megabit per second (Saniyede bir milyon bit)
MSAU : Multi Station Access Unit (Çoklu İstasyon Erişim Birimi)

MSTP :Multiple Spanning Tree Protocol (Çoklu Genişleme Ağacı Protokolü)
MVRP : Multiple VLAN Registration Protocol (Çoklu VLAN Kayıt Protokolü)
NAT : Network Address Translation (Ağ Adresi Dönüştürme)
NIC : Network Interface Card (Ağ Arabirim Kartı)
NTP :Network Time Protocol(Ağ Zaman Protokolü)
OSPF :Open Shortest Path First (En Kısa Yolu Aç)
PC :Personal Computer (Kişisel Bilgisayar)
PDU : Protocol Data Unit (Protokol Veri Birimi)
R :Router (Yönlendirici)
RIP : Routing Information Protocol(Yönlendzirme Bilgi Protokolü)
ROS : Router on a Stick
SCCP :Skinny Client Control Protocol
SSH :Secure Shell (Güvenli Kabuk)
SSID :Service Set Identifier (Servis Seti Tanımlayıcı)
STP :Spanning Tree Protocol (Kapsayan Ağaç Protokolü)
SW : Switch (Ağ Anahtarı)
TCP/IP :Transmission Control Protocol/Internet Protocol (İletim Kontrol Protokolü/İnternet Protokolü)
TPC :Transmission Power Control (İletim Güç Kontrolü)
UDP :User Datagram Protocol (Kullanıcı Datagram Protokolü)
VTP :VLAN Trunking Protokol (VLAN Kanal Protokolü)
VLAN :Virtual Local Area Netwok (Sanal Yerel Alan Ağı)
VOIP : Voice Over Internet Protocol
WAN :Wide Area Network (Geniş alan ağı)
Wi-Fi :Wireless Fidelity Alliance (Kablosuz sadakat birliği)
WLAN :Wireless Local Area Network (Kablosuz yerel alan ağları)
WMAN :Wireless Metropolitan Area Network (Kablosuz anakent alanı ağları)
WPA2 : Wi-Fi korumalı erişim ikinci sürüm
WPAN :Wireless Personel Area Netwok (Kablosuz kişisel alan ağları)
WWAN :Wireless Wide Area Network (Kablosuz geniş alan ağları)

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

NS VEYA PAKET İZLEYİCİ GİBİ BAZI SİMÜLASYON ARACINI KULLANARAK BİR AĞ PERFORMANS DEĞERLENDİRME

ÖZET

Bilgisayar ağları büyüdükçe Kablolu ve Kablosuz ağ teknolojileri de gelişmeye başlamıştır. Teknolojiler geliştikçe istekler de artmaya başlamıstır. Bu isteklerin en başında, ağların maksimum güvenli ve aynı zamanda maksimum hızlı performanslı olmalarını istemeleri gelmektedir.

Bu çalışmada, ağların performanslı çalışması incelenecektir. Bu sebeple, NS veya paket izleyici gibi bazı simülasyon aracını kullanarak bir ağ performans değerlendirmesinde neler yapılabilir ve türlü türlü parametreler ne kadar başarıyla yanyana getirilebilir gibi bilgiler sunulacaktır. CCNA, CCNP, HCNA ve HCNP eğitim seviyesinde kullanılabilecek önemli ayarlamalar yapılmış olup bunların hepsi teker teker simule edilmiştir. Sonuç olarak başarılacak olan şey bir geniş ağ veya yerel ağ için iyi bir kılavuz olacaktır.

Sanal teknolojiye dayalı teklif edilmiş uzaktan ağ laboratuvarı mimarisi gerçek ekipman kullanan geleneksel laboratuvarlara göre daha fazla fayda gösterdi ki bu lab'de ağ simülasyonları için özellikle önemlidir. Burada kazanılan tecrübe yanı sıra birebir ağ üzerinde işlem yapılabilir. Bizler burada sanal olarak laboratuvar ekipmanlarını yeniden kablolamayı, laboratuvarın topolojisi değiştirmeyi ve sanal laboratuvar ekipmanı ekleyerek yeni bir dizayn uygulayabildik. Sanal bir ortamda çalışıltığında yapılacak ve ispatlanacak konfigürasyonlar kısıtlıdır. Sadece sanal bir lab çözümü çoğunlukla öğretmek için uygundur çünkü ağ trafiği hafiftir ve lab PC yükün üstesinden gelmek için genellikle güçlüdür. Ve önemli bir özellikle eagle sunucusu DHCP, Mail, FTP, Web ve dağıtıcılar, düğmeler, güvenlik cihazları ve PC'ler gibi ağ ekipmanlarını içeren Linux'a dayalı bir makinenin bizlere sağladığı yararlardır. Son olarak anlatılan performans konuları, önlemleri, gerekli parametreler göz önünde bulundurularak hem CISCO Packet Tracer de hem de Huawei'in eNSP simulasyon programında hayali ağlar tasarlanarak performans değerlendirilmeleri yapılmıştır. Fakat unutmamak lazım ki, tasarlanan ağlar gerçek laboratuvarlar da değilde ücretsiz sanal ortamlarda tasarlanmış ve değerlendirilmiştir. Bu yüzden de elimizde gerçek veriler olmadığı için gerçek performans değerlendirilmesi yapmak ve çıktılar almak mümkün değildir. Sadece performans gereksinimleri göz önünde bulundurularak ağlar tasarlanmış ve sanal ortamların izin verdiği kadar değerlendirme yapılarak ağ performans değerlendirilmesi yapılmıştır.

Keywords: *Router,Switch, İnternet Protocols, VLAN Channel Protocols, Network Performance Evaluation, Huawei eNSP, Cisco Packet Tracer.*

NETWORK PERFORMANCE EVALUATION BY USING PACKET TRACER OR NS TOOLS

ABSTRACT

As computer networks are growing, wire and wireless networking technologies are developing, As technology are improving, the requirements of users for fast network performance and security of network are increasing day by day.
In this study, the performance of networks will be examined. Therefore what can be done in a network performance evaluation using some simulation tools such as network simulation or packet tracer. And these information will be presented that how various parameters can be brought side by side together successfully. CCNA, CCNP, HCNA and HCNP educational level has been used and important adjustment has been designed and simulated one by one. As a result this is a usefull guide for a local network and wide network. The proposed remote network in this lab architecture based on virtual technology showed more benefit than traditional laboratories using real equipment, which is especially important for network simulations.
In addition to the experience gained here, operations can be performed on a network. We are re-cabling virtually laboratory equipment here. We could apply a new design by changing the topology of the laboratory and adding virtual laboratory equipment. The virtual laboratory brings all the functions of real equipment. This lab solution is mostly suitable for educational because network traffic is light and lab is usually strong to come from the top of PC load, and a particularly impotant eagle server is DHCP, Mail, FTP, Web buttons and distributors, and networking equipment such as security devices and PCs provided by a linux based machines provides benefits for us. In this study, we tried to integrate virtualization applications such as linux based eagle server and and WMware into virtual cisco device simulation. Finally, the performance issues precautions described. Considering the necessary parameters, imaginary networks were designed and evaluated in both CISCO Packet Tracer and Huawei's eNSP simulation program. But it should not be forgotten that the designed networks were designed and evaluated in free virtual environments, not real laboratories therefore, it is not possible to make actual performance appraisal and output as there is no actual data available. Only the performance requirements are taken into consideration and the network performance is assessed by evaluating as much as the virtual environments permit.

Keywords: *Router, Switch, İnternet Protocols,VLAN Channel Protocols, Network Performance Evaluation, Huawei eNSP, Cisco Packet Tracer.*

1. GİRİŞ

Bilindiği üzere bu çağda bilgisayarlar kablolu veya kablosuz olarak birbirine bağlamak ve bu ağlarla daha geniş ağlar oluşturmak, bu ağlarla bilgi alışverişi yapmak mümkündür. Evimizde, işyerimizde, ofisimizde kullandığımız bilgisayarı veya bilgisayarları hata yazıcı vb. araçları bu ağın bir parçası olarak düşünebiliriz. En önemlisi internette bir ağdır, bu ağda bazı kısıtlamalar mevcuttur.

1.1 Ağ Nedir

İnternet iki veya çok daha fazla sayıda bilgisayarın bir araya gelerek oluşturdukları yapıya ağı denir, bu ağ iki bilgisayar olabileceği gibi, yazıcı vb. Araçlarda olur. Ağa kendine bağlı olan bilgisayarları birbirleri ile iletişime ihtiyaç duymaktadır ve bu da olasıdır, birbirlerine bağlı olan bu cihazlar (PC, Printer, Server) aynı kaynakları paylaşabilirler ve hatta bu ağ üzerinden işlem bile yaparlar. Bir bilgisayarın networke bağlanabilmesi için esas ağ gereksinimlerini sahip olması elzemdi (Olivier Bonaventure 2015). Bu ağlar değişik ağların internet üzerinden birbirleriyle haberleşerek kaynak veya belge paylaşımı yapmasını mümkün kılar.

Veriyi başlatan, yönlendiren ve sonlandıran ağ bilgisayar aygıtlarına ağ düğümleri denir. Düğümler, kişisel bilgisayarlar, telefonlar, sunucular ve ağ donanımı gibi ana makineleri içerebilir. İki cihaz birbirine doğrudan bağlantıları olsun veya olmasın, bir cihaz diğer cihazla bilgi alışverişinde bulunabildiğinde birlikte ağa bağlanmış olarak söylenebilir. Bilgisayar ağları, sinyallerini taşımak için kullanılan iletim ortamı, ağ trafiğini düzenlemek için iletişim protokolleri, ağın boyutu, topoloji ve örgütsel niyet açısından farklılık gösterir. Bilgisayar ağları, World Wide Web, dijital video, dijital ses, uygulama ve depolama sunucularının, yazıcıların ve faks makinelerinin ortak kullanımı ve e-posta ve anında mesajlaşma uygulamalarının kullanımı gibi çok sayıda uygulamayı ve hizmetleri desteklemektedir. Diğerleri. Çoğu durumda, uygulamaya özel iletişim protokolleri daha genel iletişim protokollerine göre katmanlıdır (diğer bir deyişle, yük olarak taşınır).

Sahip olamayacak kişiler işe nörolojik olarak dezavantajlı olacaklar çünkü onlar diğerleri gibi(internete bağlılar)öğrenme ve çalışma yetisine sahip olamayacaklar. Ağların ne olduğu ve ne yapabildiği hakkında temel bir bilgiye sahip olunduğu sürece, onlarla çalışmaya başlanabilir. Aslında, ağ bağlantılarıyla başa çıkmak için geliştirilmiş programlar kullanmak çok mantıklıdır

Ağ özel olarak sadece bir bilgisayardan kontrol edilir ama herhangi bir cihaz tarafından ulaşılabilir. Bu tip ağlar büyük oranda esneklik sağlar. Örneğin, şunları yapmanı sağlar bunlar:

- koltukta diz üstü bilgisayarın ile otururken üst kattaki yazıcıya dosya göndermek.
- cep telefonundan bilgisayarına fotoğraf yükleyebilir.
- bir çevrimiçi yayın sisteminden TV üzerinden film izlemek.

Eğer bunların hepsi sizlere tanıdık geliyorsa, muhtemelen adını söylemeden ve bilmeden evinizde PAN (Personal Area Network) ağına sahipsiniz.

1.2 Yerel Alan Ağı

Bir yerel alan ağı veya diğer adıyla LAN (Şekil 1.1) tek bir yerdeki - özellikle ofislerin bulunduğu bir yapı bilgisayarların oluşumdur. Yerel Alan Ağı veri depolaması ve yazıcılar gibi paylaşma kaynakları için çok kullanışlıdır. Yerel Alan ağları ağ dağıtıcı, ağ adaptörleri ve ethernet kablosu gibi nispeten ucuz donanımlar ile kurulabilir. En küçük Yerel alan ağı sadece 2 bilgisayar kullanır iken, büyük Yerel alan ağlar binlerce bilgisayara internet erişimi sağlamaktadır. Bir Yerel alan ağı genellikle arttırılmış hız ve güvenlik için çoğunlukla kablolu bağlantılara güvenir, ama kablosuz bağlantılarda Yerel alan ağın bir parçası olabilir.

Şekil 1. 1 Yerel Alan Ağı temsili

Yüksek hız ve düşük giderler Yerel alan ağını belirleyen karakteristik özellikleridir. LAN'lar, dar sahaları çevreleyen, genelde çalışma istasyonları, bilgisayarlar, yazıcılar ve server'ler gibi aygıtları birbirine bağlayan ağ çeşididir. Yerel Alan Ağları kullanıcılarına, (ARAT, B) 2014.

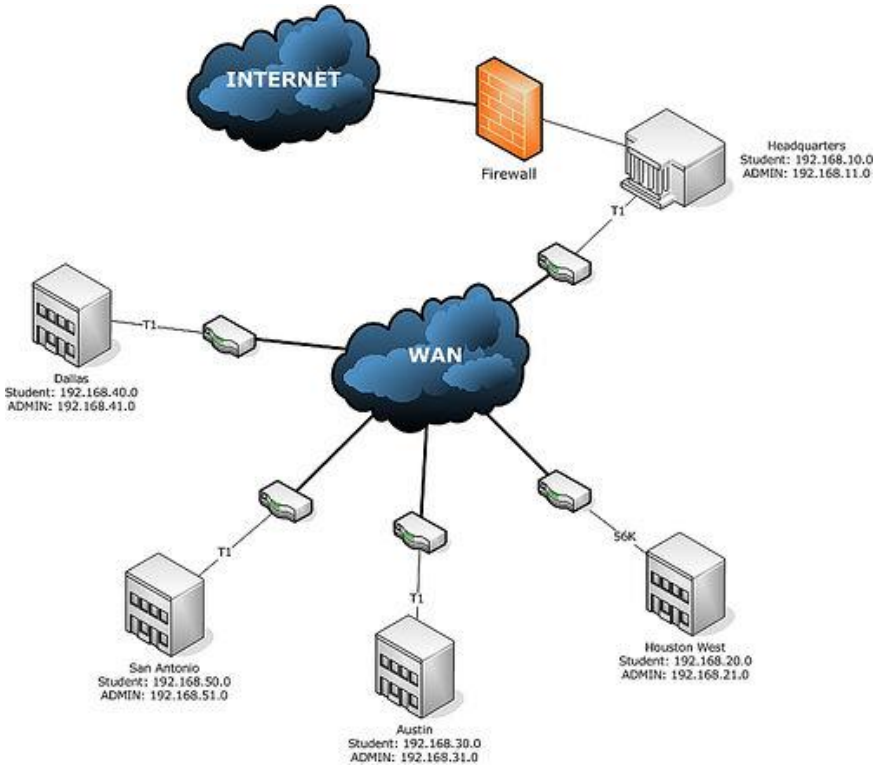
Yerel alan ağlar genellikle insanların kendi aralarında kaynakları paylaşmaları gereken tek bir yerde kullanılır, dünyanın diğer kalanı ile değil herkesin merkez sunucudaki dosyalara veya bir veya daha fazla merkez yazıcısından bir belge yazdırabildiklerini düşün. Bu işler ofiste çalışan herkes için kolay olabilir ama birinin dışarda dolaşarak telefonundan yazıcıya belge yollayabilmesini istemezdin. Eğer bir yerel alan ağı veya LAN tamamen kablosuz ise o kablosuz yerel alan ağı veya WLAN olarak tanımlanır.

1.3 Geniş Alan Ağı

Yerel alan ağlarının (LAN) birbirleriyle haberleşmesi veri alış verişi yapabilmesi için geniş alan ağları diğer tabir ile (WAN-Wide-Area- Network) ile sağlanır. Geniş alan ağı (WAN), geniş bir coğrafi mesafeye yayılmış bir telekomünikasyon ağı veya bilgisayar ağıdır. Geniş alan ağları genellikle kiralık telekomünikasyon devreleri ile kurulur. İş, eğitim ve devlet kurumları, verileri çeşitli coğrafi bölgelerdeki personel, öğrenciler, müşteriler, alıcılar ve tedarikçiler arasında aktarmak için geniş alan ağları kullanmaktadır. Özünde, bu telekomünikasyon modeli bir işletmenin, konumundan

bağımsız olarak günlük işlevini etkili bir şekilde yerine getirmesine olanak tanır. İnternet bir WAN olarak değerlendirilebilir.

Diğer ağ türleri için ilgili terimler, genellikle bir oda, bina, kampüs veya belirli bir metropol için sınırlı olan kişisel alan ağı (PAN), yerel alan ağı (LAN), kampüs alanı ağı (CAN) veya metropolitan alan ağı (MAN) Alanını sırasıyla göstermektedir. (ARISUT, K. (2009, 4 29).



Şekil 1. 2 WAN Gösterimi

1.4 Tez Amaçları

Bu çalışmanın amacı Cisco Packet Tracer veya Net Simulator benzeri bir benzetim kullanarak ağ performansını değerlendirmektir. Bu değerlendirme soncunda varılan istatistik verileri karşılaştırma bu verilerden yararlı yöntemleri sunmaktır. Bu amaçla gerçekleştirilen çalışmada, katılımcıların interneti hangi hızda veya hangi topolojilerde kullanmasına yardımcı olmaktır.

2. AĞ TOPOLOJİSİ

Topoloji ağdaki bilgisayarların nasıl bağlandığını belirleyen ağın fiziksel yapılandırılmasıdır. Topoloji kelimesi farklı anlam ve açıklamalara sahiptir, örnek olarak matematiğe göre topoloji şekli veya figürlerin boyutu sürekli değişimden etkilenmeyen geometrik özelliklerin ve mekânsal ilişkilerin çalışmasıdır. Bu başlıkta ağ alanındaki ağ topolojileri hakkında genel kesin bilgiler yer almaktadır. Ağ topolojisi bir ağın düzeni, planı demektir. Bir ağdaki farklı düğümlerin birbirlerine nasıl bağlandıkları ve nasıl iletişim kurdukları ağ topolojisi tarafından belirlenir. Ağ topolojisi bir bilgisayar ağındaki çeşitli elementlerin (bağlantılar, düğümler vs.) ayarlanmasıdır. Esasen, bu bir ağın topolojik yapısıdır ve fiziksel veya mantıksal olarak anlatılabilir. Mantıksal topoloji verinin fiziksel tasarımı dışında bir ağın içinde nasıl dolaştığını gösterirken, fiziksel topoloji cihazların yeri ve kablo kurulumunda içeren ağın farklı yapı malzemelerinin yerleştirilmesidir. Bağlar arasındaki mesafeler, fiziksel bağlantılar, iletim oranları veya sinyal tipleri iki ağ arasında değişiklik gösterebilir ama onların topolojileri aynı olabilir. Bir örnek yerel alan ağıdır (LAN): LAN'daki her hangi bir düğüm diğer cihazlar ile bir veya daha fazla bağlantısı vardır; grafiksel olarak bu bağlantıları haritalamak bir ağın fiziksel topolojisini açıklayan bir geometrik şekil olarak sonuçlanır. Tam tersine, parçalar arası veri akışını haritalamak ağın mantıksal topolojisini belirler. Ağ topolojilerinin iki temel kategorisi vardır: fiziksel topolojiler ve mantık topolojiler.

Topoloji ile ilgili olarak tasarlayıcı, topoloji alakalı bilgileri ilişkisel bilgi veritabanına eklemek amacıyla ilk örnek içinde kullanılan bir araçtır (KÖSAL,A.S.) 2007.

2.1 Fiziksel Topoloji

Bir ağın fiziksel topolojisi iş alanlarının asıl geometrik planıdır. Bir ağdaki cihazların fiziksel tasarımıdır. Her LAN bir topolojiye sahiptir veya bir ağdaki cihazlar ayarlanmış ve onlar nasıl birbirleri ile iletişim kurduklarının yolu. Veriyi ileten asıl kablolar üzerinden istasyonlarının ağa bağlanması fiziksel topoloji olarak adlandırılır. Bir ağın fiziksel planına referans olarak, düğümlerin ve onları bağlayan

kabloların belirli bir şekilde fiziksel olarak konumlandırılması. LAN ve WAN topolojileri çeşitli olarak veri yolu, şebeke, kısmi şebeke, halka, yıldız ve ağaç içerir.

2.2 Mantıksal Topoloji

Sinyal topolojisi olarak da adlandırılır. Her LAN bir topolojiye sahiptir veya cihazların ayarlanmaları ve birbirleri ile nasıl iletişim kurduklarının yoluna sahiptir. Mantıksal topoloji tam tersine, sinyallerin ağ medyasında rolünün yolu veya cihazların fiziksel olarak bağlanmalarını umursamaksızın verinin ağ üzerinden diğer cihaza aktarımının yoludur. Bir ağın mantıksal topolojisi fiziksel topolojisi kadar aynı derecede gerekli değildir. Örnek olarak, bükülmü çift ethernet bir fiziksel yıldız topoloji içinde bir mantıksal veri yolu topolojisidir. IBM'nin jeton halkası bir mantıksal halka topolojisi iken, bu fiziksel yıldız topolojisi planı ile kurulmuştur. Mantıksal topolojisi, tam tersine, sinyallerin ağ medyasındaki hareketlerinin yoludur veya verinin ağ üzerinden fiziksel bağlantı olmadan cihazlar arası geçişinin yoludur. Mantıksal topolojiler verinin ağ içinde nasıl hareket ettiğini ayarlayan ağ protokollerine bağlı ve mecburdur. Ethernet protokolü yaygın bir veri yolu topolojisi protokolüdür. IBM'nin jeton halkası yaygın bir mantıksal halka topoloji protokolüdür (MEGEP, 2011). Bir ağın mantıksal topolojisi onun fiziksel topolojisi kadar aynı derecede gerekli değildir. Örnek olarak, bükülmüş çift ethernet bir fiziksel yıldız topoloji içinde bir mantıksal veri yolu topolojisidir. IBM'nin jeton halkası bir mantıksal halka topolojisi iken, bu fiziksel yıldız topolojisi planı ile kurulmuştur. Mantıksal topolojiler sık sık medya erişimi kontrol metot ve protokolleri ile bağdaştırılır. Mantıksal topolojiler dağıtıcı ve düğüm gibi özel donanımlar ile etkin olarak yeniden ayarlanma yetisine sahiptir. Ağ topolojisi konusu bu yazıda ilerledikçe göreceğimiz beş adet temel topoloji tanır.

3. AĞ PAKETİ

Geleneksel noktadan noktaya olan iletişim linkleri gibi paketleri desteklemeyen bilgisayar iletişim bağlantıları veriyi bit akışı olarak aktarır. Ama bilgisayar ağlarındaki çoğu bilgi paketler içinde taşınır. Verinin biçimlendirilmişi olanı bir ağ paketi(bitlerin bir listesi) bir açılmış paket ile taşınır. Paket ağlarında, veri hedefe yollanılan paketlere biçimlendirilir. Paketler vardığı zaman yeniden orijinal mesaja dönüşürler (CISCO, 2015).

Paketler ile iletim ortamının bant genişliği ağın dairesel olarak açılmasından kullanıcılar arasından daha iyi paylaşılır. Bir kullanıcı paket yollamıyor ise, bağlantı aşırı kullanılmadan azıcık kurcalama ile diğer kullanıcılar tarafından doldurulabilir ve bu sayede giderler paylaşılabilir. Paketler iki türlü veriden oluşur: kontrol bilgisi ve kullanıcı verisi.

Kontrol bilgisi ağın kullanıcıya ulaştırması gereken bilgiyi sağlar örnek olarak: kaynak ve hedef ağ adresleri, hata bulma kodları ve sıralama bilgisi. Genellikle, kontrol bilgisi yük verileri ile paket başlıkları ve römorklar arasında bulunur (ITS, 2011). Genellikle paket bir ağ üzerinden alması gereken rota hemen mevcut olmaz. Bu durumda paket sıraya girer ve bağlantı boşalana kadar bekler.

Bunun dışında client ile server üzerinde ölçünlü olarak Gigabit NICs olmadığı için fazladan 10/100/1000 Mbit çalışabilen rtl8169 chipsetli network interface cards PCI 32bit 33MHz slotlara yerleştirlmiştir. Attaklar için kullanılan bu yöntemde veya sistemde 10/100/1000 Mbit çalışabilen rtl8169 chipsetli network interface cards dahildedir. Güvenlik Duvarı sisteminde ise iki adet 10/100/1000 Mbit hızlarda çalışabilen nvidia nForce 3 ve rtl8169 chipsetli anakarta network interface cards bulunmaktadır bu da daha hızlı çalışma ve paylaşım yapma anlamına gelir (Seral).

4. AĞ BİLEŞENLERİ

İletim ortamından ayrı olarak, ağlar arayüz kontrolcüsü, merkezler, köprüler, düğümler, dağıtıcılar, modemler ve güvenlik duvarı gibi temel sistem kurma blokları içerebilir. Bir ATM ağı arayüzü bir aksesuar kardı formundadır. Bir sürü ağ arayüzü gömmedir. Ağ arayüz kontrolcüsü bilgisayara iletim medyasına katılma kabiliyeti ve düşük seviye ağ bilgisini işlemesini sağlar (İTÜBDB, 2013). Örnek olarak, NIC bir kabloyu kabul etmek için veya kablosuz iletişim için bir anten ve ilgili devreler için bir bağlayıcısı olabilir. NIC bir ağ adresine gönderilmiş trafiğe NIC ve tüm bir bilgisayar olarak cevap verir. Ethernet ağlarında, her ağ arayüzü kontrolcüsü kendisinin sonsuz hafızasından saklanan kendine özel bir ortam erişim kontrolü (MAC) vardır. Cihazlar arası adres çarpışmalarından korunmak için, Elektrik ve Elektronik Mühendisler Enstitüsü MAC adres benzersizliğini korur ve yönetir. Bir ethernet MAC adresinin boyunu 6 bayttır. En önemli 3 bayt NIC üreticilerini tanımlamak için saklanıyor. Bu üreticiler, sadece kendilerine atanan önek kullanarak, benzersiz ürettikleri her Ethernet arabiriminin en az üç önemli baytı atarlar.

4.1 Tekrarlayıcılar (Repeater)

Tekrarlayıcı sinyali gereksiz seslerden arındırarak ve yeniden üreterek sinyali alan bir cihazdır. Yani repeaterlar, herhangi bir ethernet parçasından ayrılmış olan bir kısımdan ve bu parçadan aldığı elektriksel veriyi yeniler (Şekil 4.1). Sinyal yüksek güç seviyesine veya engelin diğer tarafına yeniden iletilir bu sayede sinyal uzun mesafeleri bozulmadan katledebilir. Çoğu bükülmüş çift Ethernet yapılandırmasında, tekrarlayıcılar 100 metreden uzun kablolara ihtiyaçları vardır. Fiber optikler ile tekrarlayıcılar onlarca veya bazen yüzlerce kilometre uzakta olabilirler. Çoklu girişli tekrarlayıcılar merkez olarak bilinirler.

Şekil 4. 1 Repeater

Tekrarlayıcılar OSI modelinin fiziksel katmanında çalışırlar. Tekrarlayıcılar sinyali yeniden üretebilmek için küçük bir zamana ihtiyaç duymaktadırlar. Bu ağın performansını etkileyen yayılma gecikmesine neden olur. Sonuç olarak, çoğu mühendis Ethernet 5-4-3 kuralı gibi tekrarlayıcıların kullanım sayısını limitlerler. Merkezler çoğu zaman modern düğümler ile eski kalmışlardır; âmâ tekrarlayıcılar uzun mesafe bağlantıları için kullanılıyorlar, en göze batanı deniz altı kablolaması.

4.2 Hub

"Hub"lar birer basit ağ aygıtı olduğu söylenebilir. Kendinde bulunan güç kaynağı sayesinde hem çalışır hem de bundan destek alır. Ağ sistemlerinde sinyal yenileme veya sinyalin baştan oluşum zamanlamasını sağlar. Hub'a bağlanan bilgisayarlar ortak kullandıkları bir paylaşım yolu vardır. Mesela aynı zamanda haberleşme eyleminde bulunmak isteyen networke bağlı aygıtların, hattın boşta kalmasını beklemesi gerekmektedir. Bunlar sekiz ile yirmi dört sayıları bulunduran değişken port sayısı bulunduran portlardır.

Hub'lar ağ yapılarda genelde merkezde bir nokta meydana getirir. Hub'lar OSI modeli üzerinde 1.layerda bulunmalarının sebebi ise, bu cihazların bit level'da işlem yapabilme özelliklerindendir. Hub'lar için 2 tür sınıflandırmadan bahsedilir. Bunlar genellikle edilgen ya da etken sınıflardır (Linksys, 2012). Edilgen olanlar gelen sinyalleri olduğu gibi bırakarak herhangi bir güçlendirme işlemine girişmeden çok kullanıcılı ortam için bölerler, etken olan tür ise gelen sinyali destekleyip güçlendirir ve çok kullanıcılı ortam için bölerler.

4.3 Köprüler (Bridges)

Ağ köprüsü OSI modelindeki iki bağlantı parçasını tek bir bağlantı yapmak için bağlar ve süzer. Bu ağın çarpışma alanını kırar ama birleşik bir yayın alanını korur. Ağ bölümlendirmesi büyük ve karışık bir ağı daha küçük ve verimli ağa dönüştürür.

Şekil 4.2'de görüldüğü üzere köprüler üç temel tipte gelir:

Yerel köprüler: LAN'lara direkt bağlanma

Uzak köprüler: LAN'lar arası geniş alan ağı (WAN) üretmek için kullanılabilir. Bağlanma bağlantısının son ağlardan daha yavaş olduğu yer olan uzak köprüler büyük oranda yönlendiriciler ile değiştirilmiştir. Kablosuz köprüler: LAN'lara bağlanmak veya uzak cihazları LAN'a bağlamak için kullanılabilir.

Şekil 4. 2 Köprüler

4.4 Anahtar (Switch)

Switch cihazlarında hub'da olduğu gibi bağlı olan bilgisayarlara yol gösterir (Şekil 4.3). Yolun şifreli olarak sunulması Switch'i Hub'dan ayırır. Switch ağ düğmesi OSI katmanını hedefteki MAC adresinin portları arasında yollayarak ve süzerek iki datagram yapan bir cihazdır. Bir düğüm sadece tüm bağlı portlardan ziyade iletişimde yer alan fiziksel port çerçevelerine iletir ki buda bir merkezden farklıdır. Bu çoklu girişi olan bir köprü olarak düşünülebilir. Bu alınan çerçevelerin kaynak adreslerini inceleyerek MAC adreslerine fiziksel portları ilişkilendirmesini öğrenir. Eğer bilinmeyen bir nokta hedeflenmiş ise, düğüm tüm portlara yayımlar ama kaynağa yapmaz. Düğümeler normalde cihazlara yıldız topolojisini kolaylaştıran bir sürü girişi ve basamaklı olarak ek düğümleri vardır. Çok katmanlı düğümler katman 3 adresleme veya ek mantıksal düzeylerine göre yönlendirme yeteneğine sahiptir.

Şekil 4. 3 Switch

Düğüm terimi genellikle dağıtıcılar, köprüler ve yüke bağlı olarak veya uygulama içeriğine göre trafik üretebilen cihazlar gibi cihazları içerir(örneğin Web URL tanımlayıcısı) Şayet şaseli switchlerden yararlanıyorsak biz buna port ekleyip çıkarabilirzi. OSI modelinde bu aygıtlar 2.layer cihazlardır. (Güvenlik, 2008).

4.5 Yönlendiriciler (Routers)

Genel bir ev veya küçük ofis yönlendiricisi ADSL telefon girişini ve Ethernet ağ kablo bağlantılarını gösteriyor. Bir yönlendirici paket veya datagram dâhil yönlendirme bilgileri işleyerek ağlar arasında paketler ileten bir internetworking cihazdır(katman 3 den internet protokolü bilgisi).yönlendirme bilgileri genellikle yönlendirme tablosunda birlikte işlenir. Bir yönlendirici paketleri nereye yollayacağına karar vermek için kendisinin yönlendirme tablosunu kullanır (Wait, 2005). Yönlendirme tablosundaki bir hedef diğer adıyla kara delik olan 'null' arayüzü içerebilir çünkü veri oraya gidebilir ama daha sonra veri için söylenen hiçbir söz yerine getirilmez. Örneğin paketlerin düşmesi gibidir.

4.6 Modemler (Modem)

Modemler ağ düğümlerini kablo aracılığı ile bağlamak için ürettirilmiştir orijinal olarak dijital ağ trafiği veya kablosuz için değil. Bunu yapmak için bir veya daha fazla taşıyıcı sinyal. Sinyal iletimi için gerekli özellikleri elde uygun olabilir bir analog sinyali üretmek üzere, dijital sinyal ile modüle edilmektedir. Modemler yaygın Dijital Abone Hattı teknolojisi kullanılarak, telefon hatları için kullanılır.

4.7 Güvenlik Duvarları (Firewalls)

Güvenlik duvarı ağ güvenliğini ve geçiş kurallarını kontrol eden bir cihazdır. Güvenlik duvarları genellikle bilinen kaynaklardan gelen giriş isteklerini kabul ederken bilinmeyenlerden gelenleri reddetmeye programlanmıştır. Güvenlik duvarlarının ağ güvenliğindeki hayati önemi siber atakların sürekli artmasına paralel olarak artmaktadır.

4.7.1 Ağ yapısı

Ağ topolojisi bir ağın bağlanmamış düğümlerinin düzeni veya organize hiyerarşisidir. Farklı ağ topolojileri veriyi etkileyebilir ama güvenilirlik genellikle daha kritik. Bus ağları gibi yeni teknolojilerde küçük bir hata tüm ağın çökmesine neden olabilir. Genel olarak ne kadar ara bağlantı varsa ağda o kadar güçlü olur ama inşa edilmesi o kadarda pahalı olur.

4.7.2 Ortak düzenler

Ortak düzenler; bir Bus ağı: tüm düğümler bu ortam bünyede ortak bir ortama bağlıdır. Bu 10BASE5 ve 10BASE2 denilen تامorijinal ethernet'in düzeniydi bir yıldız ağı: tüm düğümler merkezdeki özel bir düğüme bağlıdır. Bu her kablosuz kullanıcının merkezde bulunan kablosuz giriş noktasına bağlandığı WLAN'da bulunan genel bir düzendir. Bir ring ağı: her düğüm solundaki ve sağdaki komşu düğüme bağlıdır, bu sayede tüm düğümler birbirlerine sağlı ve sollu çapraz hareketlerle ulaşabilir. FDDI böle bir topolojinin kullanılmasını sağladı (Wait, 2005). Bir mesh ağı: her düğüm keyfe bağlı sayılı olan düğümlere her düğümün en az bir tane geçiş yapabileceği düğüme yakın olması yoluyla bağlanmıştır. Bir tamamen bağlı ağ: her düğüm ağdaki diğer tüm ağlara bağlıdır. Bir tree ağ: düğümler hiyerarşik olarak yerleştirilmiştir. Unutulmamalıdır ki düğümlerin fiziksel düzeni ağ topolojisini yansıtmıyor olabilir. FDDI ile bir örneğe göre, ağ topolojisi bir ring (aslında çift yönlü halkalar) ama fiziksel topolojisi genellikle yıldız topolojisidir çünkü tüm komşu bağlantılar fiziksel merkez konumu tarafından yönlendirilebilir.

4.8 Bindirme Ağı

Bir bindirme ağı diğer bir ağın üstüne kurulmuş bir sanal bilgisayar ağıdır. Bindirme ağındaki düğümler sanal veya mantıksal bağlantılarla bağlanmışlardır. Her bağlantı, ağın altında yatan yolun, belki de daha fazla fiziksel ağın karşılığıdır. Bindirme ağın

topolojisi altta yatan topolojiden farklı olabilir. Örnek olarak, çoğu "peer to peer" ağları bindirme ağlarıdır. Onlar internetin üzerindeki bağlantıların sanal sisteminin düğümleri gibi organize edilmişlerdir. Bindirme ağları daha hiç bir veri ağının olmadığı bilgisayarların modem kullanılarak telefon kabloları ile bağlandığı zaman olan ağın icadından beri vardır (İTÜBDB, 2013). Bindirme ağlarının en dikkat çekici örneği internetin kendisidir. İnternet kendisi başta bir telefon ağına bindirme ağ olarak kurulmuştur. Bugün bile, her internet düğümü çılgınca farklı topolojileri ve teknolojileri olan altta yatan alt ağlar üzerinden iletişim kurabilir. Adres çözünürlüğü ve yönlendirme bir bindirme ağın kendisinin altındaki yatan ağın haritasını yapma izni anlamına gelirler. Bindirme ağın bir diğer örneği ise düğümlerin anahtarlarını haritalayan dağıtılmış hash tablosudur. Bu durumda, altta yatan ağ bir IP ağıdır ve bindirme ağ ise anahtarlardan oluşmuş bir tablodur. Bindirme ağları internet yönlendirmesini daha yüksek yayınlama ortamına ulaşmak için servis garantilerinin kalitesi yoluyla geliştirilmesi önerilmiştir.

Önceki IntServ, Diffserv ve IP Multicast tasarıları genel bir kabul görmedi çünkü onlar bir ağın içindeki tüm router'lerin modifikasyonunu gerektiriyorlardı. Diğer elden, bir bindirme ağı internet servisi sağlayıcılarının yardımı olmadan aşamalı olarak bindirme protokol yazılımını çalıştıran uç bilgisayarlar üzerine kurulabilir (MEGEP, 2011). Bindirme ağı iki bindirme düğümünün arasında yatan ağın içindeki paketlerin nasıl yönlendirildiği üzerinde kontrolü yoktur ama o örneğin bir mesajın hedefine ulaşmadan önce üzerinden geçtiği bindirme düğümleri dizisini kontrol edebilir. Örnek olarak,

AKAMAI TCHS güvenli ve verimli içerik ulaştırışını yönetir. Akademik araştırma sos sistem multicasti, esnek yönlendirme diğerleri arasında servis çalışmalarının kalitesini içerir.

4.9 İletişim Protokolleri

TCP/IP modeli veya internet katman düzeni ve onun yaygın protokollere ilişkisi genellikle onun üstüne katmanlandırılmıştır. Mesaj figürü bir yönlendirici(R) varlığı ile A-B arasında süzülür, kırmızı süzülmeler efektif iletişim yolları, siyah yollar ise asıl yollardır. Bir iletişim protokolleri ağ bağlantıları arasındaki alışveriş kurallarının bir dizisidir. Protokol yığınında (OSI modelinde görün), her protokol altındaki protokol servislerine baskı yapar.

Protokol yığının bir örnek IEEE 802.11nin (wifi protokolü) üzerinde olan IP üzerinde olan TCP'nin (internet protokolleri) üzerinde olan http yani dünya kapsamı internet protokolüdür. Bu protokol kablosuz yönlendirici arasında ve ev kullanıcısının internette sörf yaptığı zaman kullanılır. Protokol kaplaması bilgisayar ağlarında her yerde bir bulunan bir şey iken, bu tarihsel zaman boyunca bir sürü araştırmacı tarafından iki baş neden yüzünden eleştirilmiştir. İlki, protokol yığınını soyutlamak üstteki katmanın alttaki katmanın işlevselliğini ikiye katlar ve bu bağlantı bazında ve uçtan uca esasında düzelme hatası olan başlıca bir örnektir.

İkincisi, tek bir katmandaki protokol uygulamasının sadece başka bir katmanda sunulan bir veri, yer veya adres bilgisini gerektirmesi yaygındır, böylece ilk etapta dağılan katmanların noktası engellenir. Örneğin TCP bir tıkanıklık göstergesi olarak IPv4 başlığında ECN alanı kullanır; TCP taşıma katmanı protokolü iken IP bir ağ katmanı protokolüdür. İletişim protokolleri çeşitli karakteristiklere sahiptir. Onlar bağlantı-amaçlı veya bağlantısız olabilir, onlar daire modu veya paket açmayı kullanabilirler ve onlar hiyerarşik adresleme veya düz adresleme kullanabilirler.

4.10 VLAN (Virtual Local Area Netwok)

Zamanla şirket ağları büyüdükçe karmaşık hal almıştır ve doğal olarak bu karmaşıklık performans düşüklüğüne, karışık ağ topolojilerine ve güvenlik açıklarına yol açmıştır. Bu sorunları gidermek amacıyla bir çok kurum tarafından VLAN kullanılmaya başlanmıştır. Bunların yanı sıra VLAN yapısını kullanmak için bir sıra sebepler vardır (CISCO, 2014). Bunların en önemlilerine bakacak olursak:

- Güvenlik ve izlenebilirlik: Önemli bilgileri barındıran sistemler VLAN yapılarıyla bir birilerinden ayrılarak daha kolay izlene bilinir ve olası bir saldırı zamanı daha çabuk görülerek karşısı alınabilinir.
- Performans ve bant genişliği: Ağ tarfiğinin performans ve bant genişliği daha dikkatli bir şekilde izlenebilinir ve olası bir değişiklik tüm topolojiye değilde sadece o VLAN a yapılır.
- Aşırı yüklenmelere: : Şirket cihazlarını gerekenden daha fazla kullanan ofisleri ve çalışanları ayırabilmek için VLAN'lar kurulur.

4.11 OSPF (Open Shortest Path First) Protokolü

OSPF protokolü, bir bağlantı durumu yönlendirme protokolüdür; bu, yönlendiricilerin, en yakın komşuları ile topoloji bilgisi alışverişinde bulunduğu

anlamına gelir. Topoloji bilgisi Özerk sistem boyunca taşmaktadır, böylece Özerk sistemdeki her yönlendirici Bağımsız Sistemin topolojisinin tam bir resmini elde eder

Açık Kısa Yol İlk İlkinin (OSPF) başlıca dezavantajları, Açık İlkeler Yoludur (OSPF komşuları listesi), topoloji (tüm yönlendiricileri ve yollarını içeren bir bağlantı hali veritabanını) tutmak için daha fazla bellek gerektirir ve Yönlendirme tabloları, Açık Kısa Yol İlk (OSPF), SPF algoritmasını çalıştırmak için fazladan CPU işlemeyi gerektirir ve OSPF (Open Shortest Path First) kompleks bir yönlendirme protokolüdür.

SPF (Shortest Path First - Önce En Kısa Yol) mantığını kullanarak yollar arasındaki en iyi olan yola karar verirler. Ayrıca Link-state Refresh (Hat Durumu Güncellemesi) olarak bilinen, 30 dakikada bir periyodik güncellemeler gönderir. Loopback adres ayarlanmış ise en büyük loopback ip adresi router id si olarak seçilir.
Loopback adresş yok ise router üzerinde verilmiş en büyük ip adresi router id si olarak seçilir ve komşuluk bu router id üzerinden kurulur (Baydar, 2013). OSPF, yol bilgisini hızlı bir şekilde öğrenme, büyük ve karmaşık ağlarda daha iyi çalışabilme ve güvenilirlik konularında oldukça başarılıdır. Ayrıca OSPF bu önemli özellikler dışında başka özelliklere de sahiptir. OSPF'nin EIGRP üzerindeki en büyük avantajı, herhangi bir aygıta açık standart temelli olarak çalışmasıdır.

Avantajları

• Açık bir standarda dayandığı için, çoğu yönlendirici üzerinde çalışacaktır.

• Döngüsiz bir topoloji sağlamak için Dijkstra tarafından geliştirilen SPF algoritmasını kullanır.

• Sınıfsız bir protokoldür ve VLSM ve rota özetlemesi ile hiyerarşik bir tasarıma izin verir.

Dezavantajları:

• Bitişiklik (OSPF komşularının listesi), topoloji ve yönlendirme tablolarını tutmak için daha fazla bellek gerekir

• SPF algoritmasını çalıştırmak için ek CPU işlemesi gerekir

• Yapılandırılması daha karmaşıktır ve sorun gidermek daha zor.

4.12 STP (Spanning Tree Protokol-Kapsayan Ağaç Protokolü) protokolü

Switchler, ona gelen broadcast paketlerini gelen interface dışındaki tüm portlarından gönderir. Bu şekilde yapılan yayınlar zamanı oluşan duruma broadcast storms (broadcast fırtınası) denilmektedir. Broadcast paketinde hedef MAC adresine gidecek olan paket switchin iki portundan broadcast yaptığında karşıdaki switch aynı paketi bir a portundan bir b portundan aldığı zaman sürekli ben bu switchle a portundan konuşcam diye mac adresi tablosuna yazacak. sonra b portundan bir paket geldiğinde b portundan konuşcam diye yazacak ve sanki switchin portunu biri sürekli söküp takıyor gibi yapacaklar ve switch sapıtacak. Bu tür sorunları gidermek amacıyla STP protokolü kullanıyoruz (Admin, 2011). Bu sayede topolojimiz her türlü şartlarda duraksama yaşamadan ve performans düşüklüğü olmadan çalışmaya devam eder.

STP 802.1D uyumlu köprüler ve anahtarlar üzerinde çalışır. STP'nin farklı aromaları var, ancak 802.1D en popüler ve yaygın şekilde uygulanmaktadır. Ağdaki döngüleri önlemek için STP'yi köprüler ve anahtarlar üzerine uygularsınız. Gereksiz bağlantıları, ancak döngüleri istemediğiniz durumlarda STP'yi kullanın. Yedek linkler, bir ağdaki yük devretme durumunda yedekleme kadar önemlidir. Birincil sürücünün başarısızlığı, kullanıcıların ağı kullanmaya devam edebilmesi için yedek bağlantıları etkinleştirir. Köprüler ve anahtarlar üzerinde STP olmadan, böyle bir arıza bir döngüye neden olabilir.

Bağlanan iki anahtar STP'nin farklı lezzetlerini çalıştırırsa, birbirlerine yakınsamaları için farklı zamanlamaları gerektirirler. Anahtarlarda farklı lezzetler kullanıldığında, Engelleme ve İletme durumları arasında zamanlama sorunları yaratır. Bu nedenle, aynı aroma STP'yi kullanmanız önerilir. Bu şebekeyi düşünün:

Fiziksel bağlantılardan birinin VLAN gövdesi olması durumunda, STP, VLAN'larda sorunlara neden olabilir. Bunun nedeni, yalnızca tek bir kapsayan ağaçla birlikte, VLAN gövdesiyle olan bağlantının engellenmesi olasılığıdır. Bu, belirli bir VLAN için kendi LAN'ının geri kalanına hiçbir bağlantıya neden olmayabilir. Bunu çözmek için VLAN başına alan ağaçlarını (PVST) etkinleştirin. PVST etkinleştirildiğinde, bir köprü, köprü üzerindeki VLAN başına bir örtüşen ağaç örneği çalıştıracaktır.Bir baglanti baglantisi VLAN 1, 2 ve 3 içeriyorsa, VLAN 1 ve 2'nin bu yoldan girmemesine, ancak VLAN 3'ün kullanmasına izin vermeye karar verebilir.

Yığın Ağacı Protokolü (STP) işlemlerini izlediğinizde, istatistik günlüğünde artış gösteren topoloji değişiklik sayaçlarını gördüğünüzde endişelenebilirsiniz STP'de topoloji değişiklikleri normaldir. Ancak, bunların çoğunun ağ performansları üzerinde bir etkisi olabilir. Bu belge, bu topolojinin amacının:

- VLAN başına alan ağacı (PVST) ve PVST + ortamlarındaki mekanizmayı değiştirin.
- Bir topoloji değişikliği olayını tetikleyen şeyin belirlenmesi.
- Topoloji değişim mekanizmasına ilişkin konuları açıklayın.

4.13 ACL (Access Control List) Erişim Kontrol Listesi

Erişim kontrol Listesi (ACL), bir ağın içinde veya dışında hangi yönlendirme güncellemelerinin veya paketlerin izin verildiğini veya hangilerinin engellendiğini kontrol etmenizi sağlayan filtrelerdir. ACL'ler, ağınıza giren ve çıkan trafiği kontrol etmek için güçlü bir yol sağlar. Bu kontrol, ağın ana makinelerine veya adreslerine izin vermek veya reddetmek kadar basit olabilir. ACL'leri tüm yönlendirilen ağ protokolleri için yapılandırabilirsiniz. ACL'leri yapılandırmanın en önemli nedeni, ağımız için güvenlik sağlamaktır. Ancak ACL'ler, kullanılan TCP bağlantı noktasına bağlı olarak ağ trafiğini kontrol edecek şekilde de yapılandırılabilir.ACL'lerin kullanılmasının sebepleri aşağda anlatılmıştır.

- Ağ performansını artırmak için ağ trafiğini sınırlar. ACL'ler, yönlendirme güncellemelerinin dağıtımını kısıtlayarak trafik akış denetimini sağlar.
  - Ek güvenlik olarak kullanılabilir.
  - Bir hangi alanlara erişeceğini kontrol edebilme.
  - Hangi trafik türünün yönlendirici tarafından yönlendirildiğini veya engellendiğini denetler.

5. AĞ TEKNOLOJİLERİ VE YAPISI

5.1 Ethernet

Ethernet, yerel ağlarda (LAN) ve metropolitan alan ağlarında (MAN) yaygın olarak kullanılan bilgisayar ağı teknolojilerinin bir ailesidir. Ticari olarak 1980 yılında piyasaya sürüldü ve ilk olarak IEEE 802.3 olarak 1983'te standartlaştırıldı ve daha yüksek bit hızlarını ve daha uzun bağlantı mesafelerini desteklemek için rafine edildi. Zamanla, Ethernet, token ring, FDDI ve ARCNET gibi rakip kablolu LAN teknolojilerinin yerini aldı. Ethernet mimarisi, IEEE 802.3 ölçülerine göre standardize edilmiştir. Bundan dolayı network Cisco'da CSMA/CD erişim yönteminindin yararlanmaktadır. CSMA/CD'de istemci PC'ler, veriyi iletmek için beli bir sırayı takip eder yani ilk hangi veri gidecek veya son hangi veri iletilecek bunu da ağın topolojisi belirler. Aslında Ethernetler, kendisiyle beraber çalışan iletişim ve kabloların hızına göre sınıflandırırlar.1000 Mbps hız ile haberleşebilenler Gigabit Ethernet, 10 Mbps hız ile bildirişen (haberleşebilenler) Bu topolojiler mantıksal veri yolu ile yıldız topolojileridir. Bir ağ genelde 100 Mbps gibi bir sayıya tekabül eder. Yeni olan standart ise 1 Gbps hızına kadar çıkarılabilir. Bir ağ dâhilinde bilgisayarlar ortak kullanılan taşıyıcı hat üzerinde birbirleriyle iletişimlerini kurarlar. Çok fazla bilgisayarın olduğu bir network, bilgisayarların aynı anda veri iletiminde bulunması collision olabileceğinden veri transferi başarısızlıkla sonuçlanır. OSI modelinde 2. layer da çalışan CSMA/CD protokolü bu çakışmayı durdurmak için kullanılır. Veri iletmeye başlamak isteyen PC, öncel ağı elden geçirir. Network boş ise frame gönderebilir. Network dolu ise hattın boşta kalmasını beklenir (Bayburtlu, 2010).

Carrier sense (Hat Dinleme) : Ethernet'e merbut tüm bilgisayarlar aynı anda hattı dinler ve hattın boş olduğunu gördükten sonra paketi hedefine gönderir. Lakin aynı anda çok daha fazla bilgisayar hattı dinlenir ve aynı anda paketi gönderir ise hatta çakışmalar meydana gelebilir. Ethernet rürleri Çizelge 5.1'de anlatılmıştır.

Çizelge 5.1 Ethernet Çeşitleri:

Ethernet Tipi	Kablo Türü	Data Hızı	Standart Aralık
1000 Base	CAT5, CAT6	1 GB/Sn	100 metre
1000 Base SX	Fiber optik	1 GB/Sn	**tre**

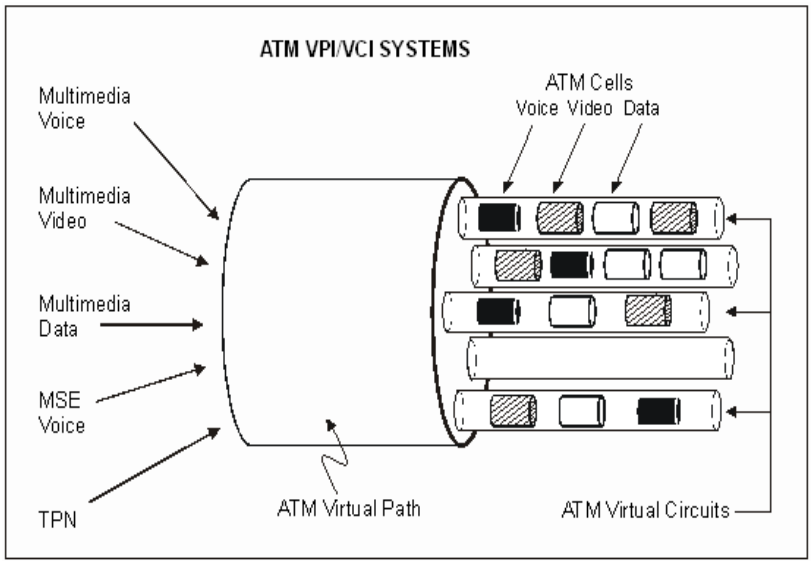
5.2 Token Ring

Token Ring node'ler birbirine halka şeklinde bağlandığından herbir node fiziksel olarak komşu iki node bağlıdır. Token halka yerel ağ (LAN) teknolojisi yerel alan ağları için bir iletişim protokolüdür. İş istasyonlarının veya sunucuların mantıksal bir "yüzüğü" etrafında dolaşan "işaret" adı verilen özel üç baytlık bir çerçeve kullanır. Bu belirteç geçişi, tüm istasyonlar için adil erişim sağlayan ve çekişme tabanlı erişim yöntemlerinin çarpışmalarını ortadan kaldıran bir kanal erişim yöntemidir. (Özhan, 2006). Bahsi geçen sistem, Token Passing ulaşım tekniğinden yararlanır ve IEEE 802,5 standart ölçüsüdür. Bu ağlar yıldız topolojine benzer bir şekilde tasarlanır. Bilgisayarlar ana bir Hub'a bağlı olarak çalışırlar. Lakin bu PC'ler bir Halka üzerine yerleştirilmiş gibi birbiriyle mütemadiyen veri alış veriş imkânı doğurur. Bu mantıksal olarak ring diye isimlendirilir. Bunun gibi ring network fiziksel olarak bir Star topoloji ağa benzemektedir. Fakat logical yani mantıksal olarak bir ringe topolojiye benzer. Bütün bilgisayarlar Ana bir adla (MSAU) münasebet içindeler. Bu hemen hemen tüm istasyonlardan alıp sinyalleri bir sonraki istasyona göndererek veri alış verişi yapar. Datayı alacak olan PC gelen veri paketini alır. Ardından yeni bir Jeton ağ üzerinde gezinmeye başlar. Token Ring network'ler orijinalde dört Mbps'dir. Fakat günümüzde kullanılan Token Ring ağlar onaltı Mbps hızına kadar çıkabilirler. Bu ağlarda ağa erişebilecek sonraki bilgisayar bilinmektedir (Doğru, 2006).

5.3 Asynchronous Transfer Mode

ATM belli bir boyuttaki (ki bu 53 gibi bir rakama tekabül eder) hücreler şeklinde data ileten bir network çeşididir. Bu teknolojinin temeli bağlantılara dayanmaktadır. Paket anahtarlamanın çeşidi de varsayılan "cell relay" yöntemi datanın taşınması sağlar. Asenkron aktarım modu hücreleri göz önünde bulundurarak tasarlanmıştır. Bunun nedeni, ses verisi paketlere dönüştürülmesi ve aynı ortamdan geçen veri gönderme verileri (büyük paket veri) ile bir ağ paylaşmaya zorlanmasıdır. Böylece, ses paketleri ne kadar küçük olursa olsun, her zaman tam boyutlu veri paketleriyle

karşılaşırlar ve maksimum kuyruklama gecikmeleri yaşayabilirler. Bu nedenle tüm veri paketleri aynı büyüklükte olmalıdır. ATM'nin sabit hücre yapısı, yönlendirilen çerçeveler ve yazılım değiştirme ile ortaya çıkan gecikmeler olmadan kolayca donanımla değiştirilebileceği anlamına gelir. Bu nedenle bazı insanlar, ATM'nin İnternet bant genişliği sorununun anahtarı olduğuna inanıyor. ATM, veri aktarımı başlamadan önce iki nokta arasında sabit rotalar oluşturur; bu, verilerin paketlere bölünmüş olduğu TCP / IP'den farklıdır ve bunların her biri hedefine ulaşmak için farklı bir yol alır. Bu, veri kullanımını fatura etmeyi kolaylaştırır. Bununla birlikte, bir ATM ağı, ani bir ağ trafiğinin artmasına daha az uyarlanabilir. (Yücel).



Şekil 5. 1 ATM bağlantı modeli

ATM'ler bu tarz networklerin ana temelli olduğundan, bilgisayarlardan herhangi biri data transferi yapabilmesi için ilk önce bağlantı kurulumu yapması için şart olan paketi yolar. Bu paket ihtiyaç duyduğu kaynaklar ile ilişkin ve geçtiği ATM anahtarlarına bağlantının varlığı hakkında ve bilgileriyle alakadardır. Bağlantının sanal devre path bilgisi de sanal path olarak isimlendirilir. sanal devre path olarak isimlendirilir. Bütün bağlantıların sadece kendilerine özgü kimlik bilgileri sahiptirler.

5.4 Fiber Dağıtık Veri Arayüzü (FDDI)

Bu çağda yararlandığımız optik fiber kablo yoluyla yüksek hızla çalışabilen Token halka yerel ağlardır. Çift kablolama yöntemi bu kablolamada kullanılır. Burada şu kastedilmekte, bir yönü saat yönünde ise diğer tarafı tam tersi istikamette iletim

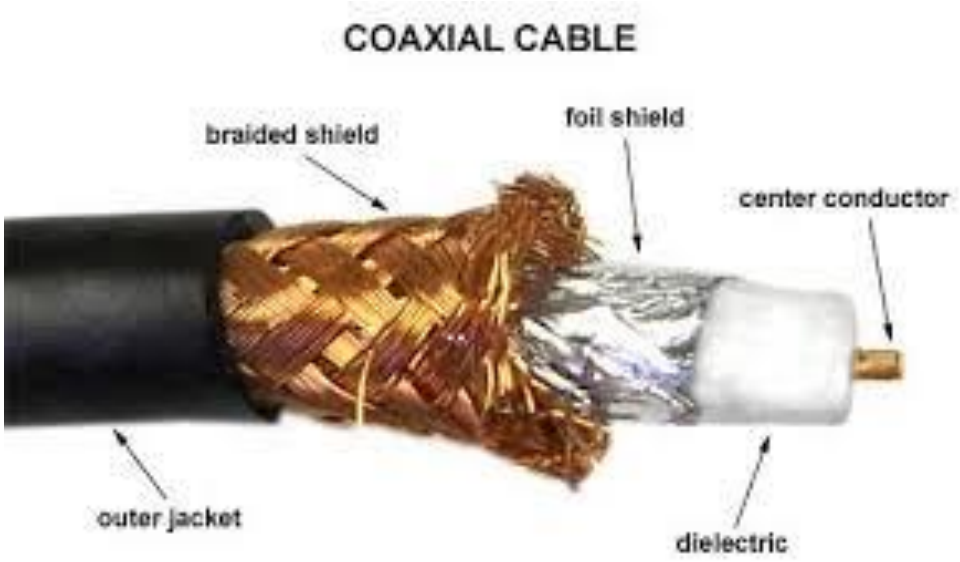
yapar. IEEE 802,5 Token Ring ve FDDI arasında birçok farklı nokta vardır. 802.5'te bir istasyonun yolladığı paketin varacağı yer paket gidene ve geriye dönene kadar herhangi yeni bir Token meydana gelmez fakat FDDI' de ise istasyonda yeni Token üretilmesi için tek şart eski Token'nin geri gelmesine ihtiyaç yoktur yani gelse de gelmese de yeni Token üretilir

6 AĞ BAĞLANTILARINDA KULLANILAN KABLOLAR

Bu günlerde bilgisayar networkte yararlanılan kablo üç türdür. Bu tipler; (Coaxial)cable,(Twisted Pair) ve (Optic fiber) kablo türleridir

6.2 Koaksiyel Kablo

Şekil 6.1'de gösterildiği gibi Koaksiyel kablo elektro manyetik pis ortamların olduğu yani kirli olan ortamlar da az güçte sinyallerini iletsin diye geliştirilmiş olan kablo çeşididir. Bu kablo çeşidi birçok alanda kullanılabilir. Bunun yanında ses ve video transferinde de bu Koaksiyel kablodan yararlanılır.

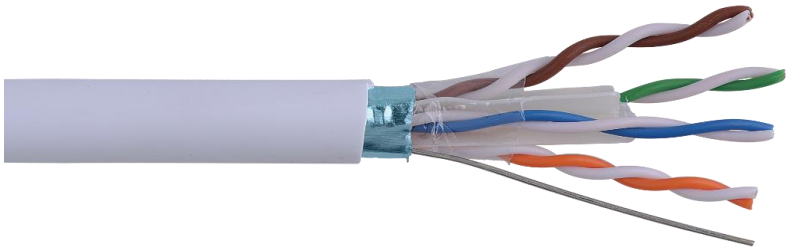


Şekil 6. 1 Koaksiyel kablonun yapısı

6.3 Bükümlü Çift Kablo

Twisted Pair Cable diye bilinen bükümlü çift kablo Şekil 6.2'de görüldüğü gibi, genellikle yerel ağlarda en çok tercih edilen ve yaygın olarak kullanılan en basit metottur. Bu tür kablolarda birebir aynı yalıtım maddelisiyle kaplanmış tel çiftlerinin birbirine sarılması sonucunda meydana gelmiştir. Bu kabloların bükülerek sarılması gürültünün azalmasını sağlar. Bu kablo çeşidi birbirini helezonik olarak dolandırıldığından dolayı iki telli açık hatlara göre yapay gürültü sinyallerine karşı dirençlidir yani parazitlere karşı etkilidir. Parazitler sinyalini her 2 hat tarafından da

toplanması sinyal ve toprak hatlarının birbirine yakınlığının neden olduğundan bilinen bir gerçektir. Sırf koruma kalkanı olsun diye birbirine sarılmış 2 kablodan oluşan kablo tipidir. Daha düzü, bu çiftlerden 4 âdetini içeren ethernet kablosunun diğer bir adıdır. Günümüzde “Cat 5” diye de adlandırılır.



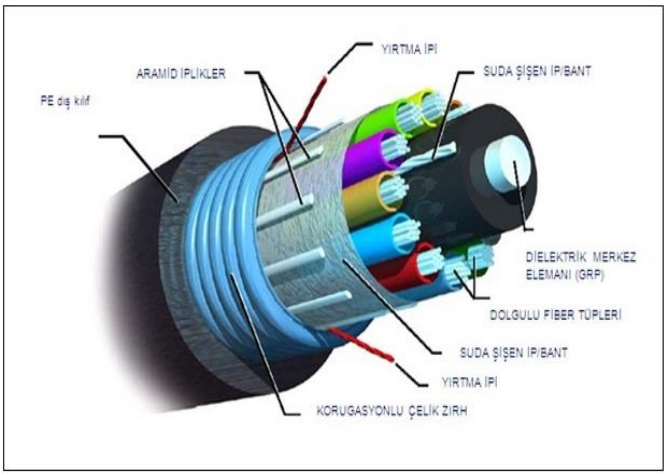
Şekil 6. 2 Bükümlü çift kablo

6.4 Fiber Optik Kablo

Şuana kadar internet erişimde en ileride olan teknolojisi fiber optik kablo çeşididir. Veriyi ışığın darbeleriyle saydam bir hat içerisinden transfer eder. Bir optik fiber kablo, ışığı taşımak için kullanılan bir veya daha fazla fiber optik içeren bir kablodur. Optik fiber elemanlar tipik olarak plastik tabaka (Şekil 6.3) ile ayrı ayrı kaplanır ve kablonun konuşlandırılacağı ortam için uygun bir koruyucu boru içinde bulunur. Farklı kablo türleri, örneğin uzun mesafe telekomünikasyon gibi farklı uygulamalar için veya bir binanın farklı bölümleri arasında yüksek hızlı veri bağlantısı sağlamak için kullanılır. (Pekküçük ve Ünverdi).

Fiber optik kablo10 km içinde veri kaybı olmayan dünyadaki tek kablo türüdür.100 megabayt hızında data iletimini sağlar. “Wireless sistemler tümden kablosuz değildir. Böyle sistemler ananevi olarak beli başlı ağlara bağlanmak üzere sayısal devrelerden yararlanırlar. Bir fiber optik iletişimin önemli bir özelliği, fiber optik kabloların uzatılması ve böylece iki farklı kabloya bağlanarak oluşan kayıpların asgari düzeyde tutulmasıdır. Optik fiberin birleştirme uzunlukları genellikle elektrik kablosuna bağlanmaktan daha karmaşıktır ya da Kabloyu ve liflerin dikkatle parçalanmasını gerektirir. Elyaf çekirdeğinin mükemmel hizalanması ve bu hizalanmış elyaf çekirdeğinin birleştirilmesi. Kalıcı bir bağlantı isteyen uygulamalar için, elyaf uçlarını mekanik olarak tutan mekanik bir birleştirme kullanılabilir veya elyaf uçlarını bir araya getirmek için ısı kullanan bir füzyon ek yeri kullanılabilir. Geçici

veya yarı kalıcı bağlantılar, özel fiber optik konektörler vasıtasıyla yapılır. (Baykara ve Karadoğan, 2013).



Şekil 6. 3 Fiber Optik kablo

Fiberde iletilen kanal başına ışık sinyalleri, konuşlandırılmış sistemlerde tipik olarak 10 veya 40 Gbit / s olmasına rağmen, NTT ile 111 gigabite (Gbit / s) kadar yüksek oranlarda modüle edilmiştir. Haziran 2015'te araştırmacılar, 4-modlu yörünge açısal momentum çoklama kullanarak tek bir kanal üzerinden 400 Gbit / s iletim gösterilmiştir.

7 AĞ PERFORMANS DEĞERLENDİRİLMESİ

7.1 Performans

Verilen bir görevin başarısı önceden hazırlanmış bilinen doğruluk, bütünlük, gider ve hız ile ölçülür. Bir sözleşmede, tüm yükümlülükleri işi yapanın üzerinden kaldırırcasına bir yoldan yaparak, performansın tüm zorunlulukları tamamen yerine getirmesi var sayılır. Performans terimi son yıllarda sanatta, edebiyatta ve teknolojideki sosyal bilimlerde son derece popüler oldu. Onun kullanımı ve popülaritesi büyüdü, bu nedenle onun performansı hakkında yazmak ve hangi insan aktivitesi olduğunu analiz etmeye ve anlamaya kalkışmak karmaşık bir vücuda sahiptir.

Hayatımız, davranış olarak onaylanmış ve tekrar eden normlara göre yapılandırılmış olmasından dolayı "performans" tüm insani faaliyetler için potansiyel bir değerlendirme olarak düşünülebilme olasılığını doğurur veya en azından var olan bütün faaliyetler iç disiplinden etkilenerek kendi iç değerlendirmesini geliştirerek performans ölçütüne girebilir. Aslında muğlak olan performans kavramını ele alacak olursak veya düşünecek olursak, bu bize bir aktörün veya öğrencinin ya da arabanın performansını kapsayan boş beyhude, malayani işlerle uğraşmış olacağımız anlamına gelir.

7.2 Ağ Performansını Değerlendirmek için Gerekli olan Faktörler

Son on yılda, iletişimdeki gecikmenin düzeltilmesinde ve yüksek uç makinelerdeki iletişimin yazılım overheadları işlemci performansındaki üstel artışların çok gerisinde kalmıştır. Bunun için bir neden en güncel büyük ölçekli paralel makineler iş istasyonlarının veya kişisel bilgisayarların kümeleri olarak kurulmasıdır aynı zamanda, âmâ düzensiz veri yapıları ve iletişim kalıpları kullanarak bilimsel uygulama toplumuna süregelen bir ilgi vardır. Çözüm zamanını, doğruluğu ve hafıza kullanımı iyileştirmek için, geliştiriciler genellikle yoğun matrislerden seyrek olanlara, yapılandırılmış yapılardan yapılanmamışlara ve statik algoritmalardan zamana veya uzaya adapte olmuşlara yönelirler. bu algoritmalar doğal olarak

yapılandırılmamış ağ hayalet düğümleri, adaptif ağ dikdörtgeninin sınırlarını doldurur veya olay kaynaklı simülasyon olayları gönderme gibi talebe bağlı az miktarlardaki verilerin iletişimini içerir. Çift taraflı iletişimle olan bulk senkronize programlama modelleri bu algoritmalar için kullanılabilir, ama programlama karışıklığından dolayı yüksek bir giderle, çünkü küçük mesajlar büyük olanlarına paketlenir ve noktadan noktaya eşleme küresel eşleme ile değiştirilir, burada biz hem küçük hem de büyük mesajların performanslarını çağdaş süper bilgisayar ağlarında değerlendiririz. Logp'nin modelini ve uzantısını büyük mesajlar için kullanarak, loggp testlerimiz ve analizlerimiz için başlangıç noktasıdır, biz bir kaç tane katı teklif ediyoruz; biz geniş bir ağ çeşitliliğin üzerinde hayata geçirdiğimiz ağ kıyaslamaları dizisini bant genişliği, gecikme ve yazılım yükünü ölçmek için açıkladık.- hem küçük hem büyük mesajların süper bilgisayar ağlarındaki performansı için bu kıyaslamalardan veri sağlıyoruz ve uygulamaların bir alt seviyesi olan MPİ'nin performansını onla karşılaştırıyoruz.- bizim sonuçlarımızı kullanarak, iletişim ile üst üste gelme hesaplaması, boru hattı mesajları ve mesaj paketlemenin kullanımı gibi ağ optimizasyonu ile elde edilebilecek çeşitli uygulama hızlandırmalarını inceliyoruz. biz son 10 yıldaki küçük mesaj performansı trendlerinin tarihsel bir portresini sunuyoruz. Genellikle iletişim ağda devam ederken iletişimcinin internet erişiminin ortalama performansı ağ performansından etkilenir, oda aşağıdaki faktörlere bağlıdır:- cihaz hızı: bir cihazın rota veya filtre gönderme ve ağdaki veriyi almada ne kadar hızlı olduğunu gösterir. Ağ hızı: ağın bant genişliğini veya ağ arayüzlerinin bit oranını ve cihazların veya sunucu girişlerinin bağlanılır olup olmamasını gösterir.- veri filtreleme: bu eylem paketlerin osi modelinin seviye3'ün üzerindeki paketlerin denetletmesine yapılmaktadır. Filtrelemenin ne kadar yüksek seviyesi, performansı arzulanan seviyeye getirmek için CPU kaynağının eklenmesi gerekirken, o kadar düşük performans. veri şifreleme: eğer bu overhead çok iyi olduğunu kanıtlarsa ve ağ performansı belli kabul edilebilir bir seviyeye düşer isse , VPN cihazlarda ağ trafik performansı kötüleşir, ek CPU kaynakları şifrelememe yapan cihazlara performansı arzulanan seviyeye getirmek için eklenmelidir.- cihazların sayısı: gecikmenin ortalama performansa sunulan performans cihazların sayısı artarsa artar.

Kötü uygulamalara cevap verme zamandan kaynaklanan sorunların çözülmesi tüm ağ mühendislerinin her zaman atlatması gereken anahtar bir görevdir. Uygulamanın kendisini veya kullanıcıları sinir eden yavaş bir ağ mı, yoksa ağın yavaşlamasına

neden olan başka sorunlar mı? Belki de bu kadar geciktiren şey sunucudur? Kullanıcıların hüsranına sebep olan şeyi bulmak önemlidir çünkü tam olarak nereye bakılacağını bilmek yavaş olan networkler için cevaptaki çözümünün ilk adımıdır. İşte burada ağ sorunları ile karşılaştığınız zaman bakmak isteyeceğiniz ağı etkileyen en önemli dört faktör:

7.2.1 Gecikme

Gecikmeyi bir anayoldaki hız limiti gibi düşünün. Bir anayoldaki trafik hızı hava durumu, diğer trafik ve yol işaretleri gibi çeşitli şeylerden baya etkilenir. Bunun gibi ağda seyahat eden veri paketlerinde çoğu şeyden etkilenir. Gecikmeyi azaltmanın ilk yolu ortalama gecikmeyi ağa, uygulamaya ve onunla alakalı sunuculara yıkmaktır. Bu tespitin yapılması ile görsel olarak uygulama ve ağ gecikmesini yakın ilgi gerektiren anormallik ve sorunları bulmak için grafikler ve sonra bu sayede işin içine girebilirsin ve neyin darboğaz yaptığını tespit edebilirsin.

7.2.2 Throughput

Throughput bir ağın bir anda taşıyabileceği trafik miktarıdır. Trafik analojisi yukarda gecikmeyi açıklamak için kullanıldığı gibi, Throughput'u bir anayoldaki şeritlerin sayısı gibi düşün. Ne kadar fazla şerit, o kadar fazla anayolun ev sahipliği yapabileceği trafik. Ağları düşünürken, ne kadar yüksek bit oranı, o kadar hızlı dosya transferi. Yavaş cevap süresi yeterli Throughput olmaması nedeniyle olabilir. Eğer bu yoldaki şerit sayısı az ve yol kötü ise arabanız (benzetim) ne kadar lüks olursa olsun, hızında her daim sorun yaşanacaktır. İşte Throughput bu yoldaki şerit sayısı gibidir.

7.2.3 Paket kaybı

Kusurlar, hatalar veya aşırı ağ yüklenmesi veri paketlerinin kaybı ile sonuçlana bilir. Bazen router ve switchler genel ağ performansını korumak için ya da belirli hizmet seviyesine zorlamak için bilerek trafik tutabilir. İyi ayarlanmış bir ağda kasıtlı paket kaybı nadir bir olaydır, ama paket kaybı diğer nedenlerden dolayı host'un başına yine de gelebilir ve ortalama ağ performansından emin olmak için yakından incelenmelidir.

7.2.4 Tekrar iletim

Bir paket kaybı oluştuğunda, kayıp olan paketler yeniden yollanmıştır. Bu yeniden yollama işleme iki türlü gecikmeye neden olur: birincisi verinin tekrar yollanmasından, ikinci gecikme ise verinin protokol yığınına gitmesinden önce doğru sırayı beklemesinden kaynaklanır. Bu faktörler özel değildir ama onlar yavaş bir ağa katkı yapabilen birçok şeyin resminin yapılmasına yardım eder. Umarım, bu bilgi ile donanarak, performans problemleri çıkmadan önce onları tam olarak teşhis edebilirsiniz. Tarihsel performans değerlendirme başlangıçta 1970ler ve 80lerde bilgisayar sistemleri ile ilgilendi ve bu değerlendirme hız ve eş zaman yüzünden bilgisayar biliminin önemli bir parçası olarak ortaya çıktı. Modern bilgisayarların karışıklığını artıran ortaya çıkan şey, bilgisayar sistemlerinin anlanabilmesini ve değerlendirmesini daha da zorlaştırdı. Performans değerlendirmenin amacı bilgisayar sistemlerinin efektifliğini ve hakkaniyetini belirlemektir ve performans değerlendirmesi bilgisayar araştırmalarının bilimsel metodunun uygulamasıdır. Bu teknikler tüm müşteri sınıflarına adil bir servisi sağlamak için uğraşırken bilgisayar sistem kaynaklarının yönettikleri ile efektifliği tam olarak hesaplamak için geliştirilmiştir.

7.3 Performans Modellemesi

Performans modellemesi modelin çalışmasının matematiksel bir yaklaşımını kullanarak değişik sistem konfigürasyonlarına karşı çeşitli kullanıcı ve sistem yükleri simüle etme işlemidir. Genellikle bu yük test ortamının kullanımını gerektirmez. Bu genellikle performans testinden daha ucuzdur ve daha yaklaşık sonuçlar üretir. Örneğin, sunucular düşük seviye kullanıcı işlemleri sisteme karşı gerçekleştirilirken görüntülenir. Tipik performans modelleme sonuçları:1. sunucu sayaçları işlem tepki süreleri ile ilişkilidir.2.sistem özellikleri ile bilgi bir matematiksel modelleme aleti haline beslenir.3.veri girildikten sonra çeşitli modeller farklı konfigürasyonlarda ve kullanıcı veya sistem yükleri sistemin davranışını göstermek için üretilmektedir.4.performans modelleme çıkışları kapasite planlaması için kullanılır.

7.4 Ağ Performansı Ölçümü

Ağ performansının ölçümü her zaman zor ve belirsiz bir görev olmuştur, başlıca nedeni çoğu mühendis ve yöneticiler kendi LAN veya WLAN ağına hangisinin daha uygun olacağından emin değiller. Bir yaygın (ve çok kolay) ağ performansının test

edilmesi metodu bir sunucuya basit bir dosya aktarımını başlatmaktır, âmâ bu metot sık sık mühendisler tarafından tartışılmıştır ve bunun için güzel bir neden: dosya transferleri olurken, biz sadece hızı ölçmüyoruz, aynı zamanda yayının iki tarafındaki hard disk gecikmelerini de ölçüyoruz.

Hedefin kaynağın atabileceğinden daha fazla iletim oranları kabul etme yeteneğine sahip olması muhtemeldir veya başka bir yoldan. Hard disk (HDD) sürücülerinden kaynaklanan bu darboğazlar, işletim sistemi mekanizma veya diğer donanımları sıraya sokar, istenmeyen gecikmeler yapar, sonuç olarak tutarsız sonuçlar sağlar. Maksimum verimlilik ve ağın diğer yönlerini ölçmenin en iyi yolu teste katılan makinelerden gelen gecikmeyi en aza indirmektir. Test sırasında başka işlerle uğraşmadıkları sürece yüksek/orta uç makineler(sunucular, iş istasyonları veya laptoplar) bu testleri gerçekleştirmek için kullanılabilirler. Büyük şirketler yukardaki tüm sorunların üstesinden gelmek ve ağ testi çevresine adanmış donanımları satın almak için gerekli finansal kaynaklara sahip iken, bizler çoğu açık kaynak topluluğundan bedava olan metotlara ve araçlara güveniriz.

Bulunduğunuz yerle diğer uzak yerler arasında testler yapmak uçtan uca performansı anlamanın ilk yoludur ağ değerlendirmesi, tabanlar kurulur ve grafiksel form olarak alınabildiği zaman: ağ yolu gerçeklerine karşı karşılaştır. Kullanıcı beklentilerine dayalı olarak performansı değerlendir aşağıdaki bölümler ölçme araçlarının muhtemel sonuçlarını tartışıyor, farklı tür sonuçlar için makul açıklamalar sunuyor. Çoğu zaman lan çevresinde gerçekleşen testler için bile personar araçları kapasite sayısının %99 unu rapor etmez. Bu şunları içeren birçok faktörden dolayıdır:- başlatılan testin türü- testin süresi- test aracı ayarı- test sırasında ağ faktörleri

7.5 DHCP (Dynamic Host Configuration Protocol)

Yerel ağdaki bir bilgisayar, bir yazıcı veya bir ip kamera ya da her hangi bir IP adresi alarak çalışmak zorunda olan cihaz ağa bağlanmak için IP almak zorundadır. DHCP, böyle cihazları ağa bağlamak için bir ağ yapılandırma protokolüdür. Yani DHCP, ağdaki cihazlara ip adresi, ağ maskesi, ağ geçidi ve dns adresleri gibi bilgileri otomatik olarak atamak için kullanılan servistir. Bir ağda bulunan cihazlara tek tek gezip benzer ip parametrelerinin defalarca elle girilmesini engelleyerek zamandan tasarruf etmeye yarar. Bu sayede sistem yöneticisinin işini kolaylaştırır. DHCP, ağ yönetimini azaltmak için aşağıdaki özellikleri içerir:

- Merkezi ve otomatik TCP / IP yapılandırması.
- Merkezi bir konumdan TCP / IP yapılandırmalarını tanımlama özelliği.
- DHCP seçenekleri aracılığıyla bir dizi ek TCP / IP yapılandırma değeri atama olanağı.
- Sık sık güncellenmesi gereken istemciler için IP adresi değişikliklerinin verimli bir şekilde kullanılması. Kablosuz ağdaki farklı konumlara taşınan taşınabilir bilgisayarlar gibi.
- DHCP aktarma aracısı kullanarak başlangıç DHCP iletilerinin iletilmesi, Böylece her alt ağda bir DHCP sunucusu olması gereğini ortadan kaldırır.

7.6 DNS (Domain Name System)

DNS ya (Etki Alanı Adı Sistemi) Alfabetik isimleri sayısal IP adreslerine ve IP adreslerine alfabetik olarak dönüştürmek için kullanılan Internet sistemidir. Örneğin bir tarayıcıya bir Web adresi (URL) girildiğinde, DNS sunucuları bu adla ilişkilendirilmiş olan Web sunucusunun IP adresini döndürür. Bu hazırlanmış örnekte DNS, www.google.com URL'sini IP adresi 200.10.10.1'e dönüştürür. DNS olmadan, Web sitesini almak için tarayıcınıza dört sayı ve nokta dizisini yazmanız gerekmektedir. O zaman bütün müşteriler için tüm şirketlerin IP adreslerini ezberlemek çok zor olacak bu kolaylık özeliğini DNS servisindedir.

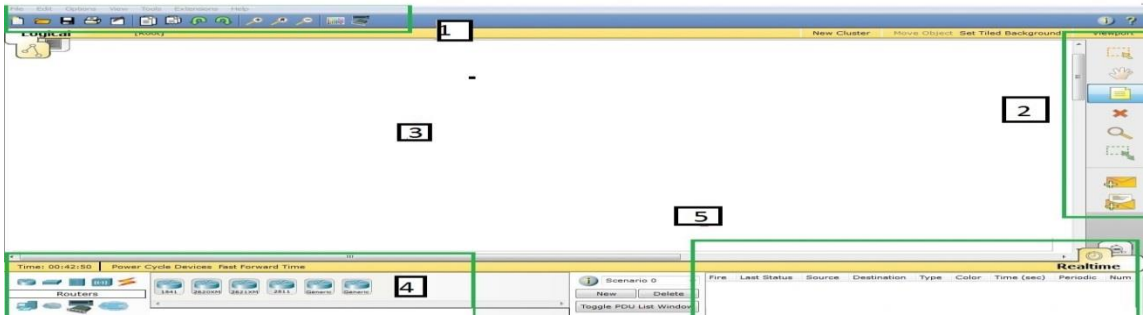
DNS Sunucusu hizmetini çalıştıran bir etki alanına birden çok etki alanı denetleyicisi yükleyerek, bir etki alanı denetleyicisi başarısız olursa veya bakım için çevrimdışı duruma getirildiğinde DNS'nin çalışmaya devam etmesini sağlayabilirsiniz. Birden çok etki alanı denetleyicisine sahip olmak, sunucuları, DNS istemcileri tarafından en verimli şekilde ulaşılabilecek sitelerde bulma olanağı da verebilir. Buna ek olarak, ortaya çıkan yük dengelemesi genel DNS performansını artırabilir.

8 CISCO PACKET TRACER

Ağ konusunda çalışan tüm uzmanların hemen hepsinin kendilerine yardımcı olan ağ simülatörleri bulunur çünkü laboratuvar ortamında çalışmak her zaman mümkün olmayabilir. Bunlar NS (Network simülatör) veya Cisco paket izleyici (Cisco Packet Tracer) gibi simülatörleridir. Ezcümle aniden router'leri, switch'leri hemencecik bağlayabilecek laboratuvar ortamı oluşturmak çok da kolay bir iş değildir. Bu işler uzun zaman ve enerji gerektirir bu da bizleri bu tarz simülatörlere yönlendirir. Bu çalışmamızda biz daha çok Cisco programları üzerinde yoğunlaşacağız.

İşte bunun en güzel örneği Cisco firması tarafından geliştirilen ve herkesin kullanıma sunulan Packet Tracer adlı programdır. Cisco Packet Tracer programı, herhangi bir fiziki makine veya araç kullanımına gerek bırakmadan, Cisco işlemlerinin veya uygulamalarının yapılmasının imkan tanıyan ve kullanıcılara bir ağ laboratuvar ortamı sunan bir benzetim programıdır(Şekil 8.1).

Cisco'nun geliştirdiği bu yazılım sayesinde ağlar sanal olarak modellenebilir ve üzerine çok da kolay işlem yapılabilir durumuna gelir. Bu Cisco programları hemen hemen bütün platformlarda çalışır ve kullanıcı dostu olduğundan kurulumu ve kullanımı basittir. Cisco Packet Tracer basit bir arayüze sahiptir işte bunun sayesinde yaratığınız topolojiyi sadece sürükleyip bırakarak işlem yapabilir ve paket ölçümüne girebilirsiniz. Cihazlarda istenildiği gibi arayüzleri kolayca başvurulabilir. Bu arayüz sayesinde ağda yapılması gerek tüm işlemler yapılabilir.



Şekil 8. 1 Cisco Packet Tracer

Günümüzde Cisco Packet Tracer interface'i işi o kadar basitleştirmiş ki bir ağ aygıtının çalışıp çalışmadığını ping komutu yazmaya dahi gerek yok, bu kontrolü cihaz üzerinde bulunan bir zarf resmini cihazlar üzerine tıklayıp ping atmanıza olanak sağlar böylece cihazının durumunu buradan anlayabilirsiniz. Cisco Packet Tracer rakiplerine göre farkı kılar.

1) Cisco Packet Tracer kullanıcı dostu ve ağ bağlantılarını daha iyi bir şekilde öğrenmek için sanal ortamlar sunar.

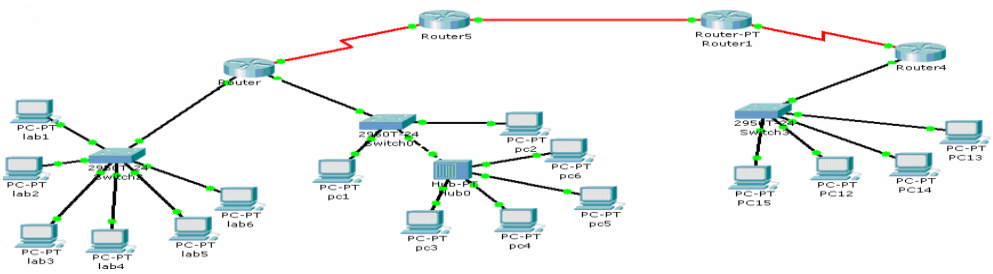
2) Birden çok kullanıcılı (mutliusers), gerçek zamanlı eğitim laboratuvarı sunar.

3) Öğrencilere yönelik aktivite geliştirebilir ve sınav hazırlanabileceği gibi bu sınavların sonuçları değerlendirilir.

Görüldüğü gibi, bu çalışmada TCP ve OSI referans modelini bütün ayrıntılarıyla kapsayacak seviyede reel hayata olduğu gibi ağların tasalanması yapıldı herhangi bir sorunla karşılaşmadan başarıyla tamamlandı. Ağ benzetimlik yazılımlarının çoğu, ağ ürünleri geliştiren firmaların eğitim ve tasarım amacıyla kullandıkları yazılımlardır. CİSCO system, tarafından geliştirilen CCNA, CCNP benzeriseviye eğitimlerin büyük bir bölümünde laboratuvar kullanımı yerine geliştirdiği benzetimlik programlarından yararlanmaktadır. Cisco Packet Tracer kapsamlı olmasına rağmen gayet güzel bir kullanıcı dostu arabirimi vardır. Ağ modellerin çoğu bu uygulama ile tasarlanmaktadır.

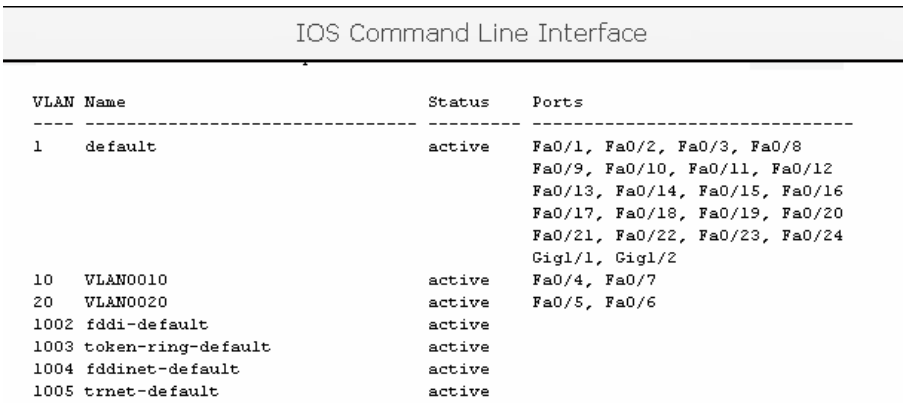
8.1 Alan Ağı Modellemesi

Dizayn edilen Network Topolojisi Sekil 8.2'de gösterildiği gibi 2 ana parçadan meydana gelmektedir. Görülen iki kısımda da fiber optik kablo kullanılmıştır. Bu sanal ağda bilgisayarlar, yönlendiriciler, switch'ler, Hub'lar, Modemler ve dizüstü bilgisayarlar kullanılmıştır.



Şekil 8. 2 Tasarlanan Ağ Topolojisi

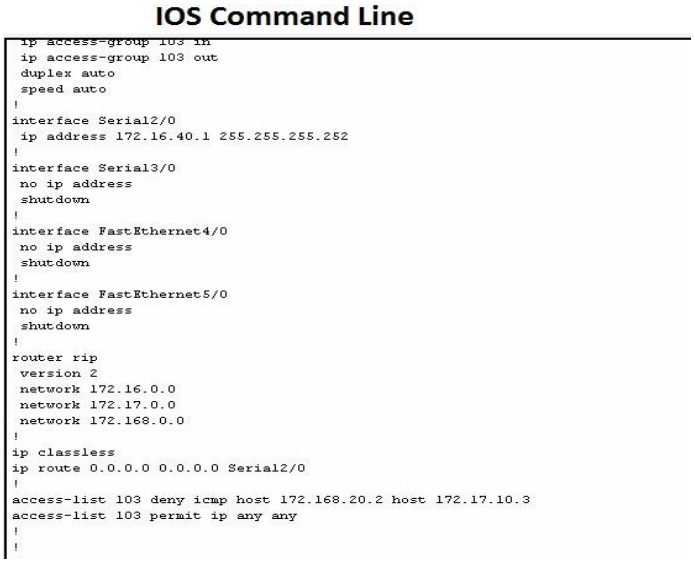
Burada ana router seri kablo ile bağlı yönlendiriciyi yani router ve ona bağlı 2 adet switch mevcuttur. Switch'lere 4 adet bilgisayar bağlanmıştır. Bu PC'lerden part1 switch' ine bağlı durumunda olanlar 192.168.2.10/24 subnetinde ve diğerlerine gelince 192.168.2.0/24 subnetinde yer almaktadırlar. Switch'lere bağlı PC'ler IP adreslerini canlı (dynamic) olarak ana router'inde kurulu olan DHCP havuzundan sağlamaktadırlar (Şekil 8.3).



Şekil 8. 3 VLAN konfigürasyonu

Router' da bir yönlendirme protokolü için RIP'den yararlanmaktadır. Karşılıklı bir statik yönlendirme meydana gelebilecek herhangi bir döngüyü engelleyeceğinden statik yönlendirmeden faydalanmıştır. Switch ile router'ler arasında düz kablo ve hub ile switch arasında cross kablodan yararlanılmış olup bilgisayaralar bu hub ve switch'lere düz kablo ile bağlanmıştır. Tahmin edileceği gibi bilgisayarlar ana router'a seri kablo ile bağlanmıştır. Layer1 Switch'i altı adet bilgisayara dağıtım sağlamaktadır. Bağlı olan PC'lerin IP adresleri statik olarak manuel girilmiştir. Meydana gelebilecek trafiği azaltmak ve kontrol altına almak için Layer1 de switch üzerinde üç adet VLAN yaratılmıştır. Bu VLAN sayesinde aynı switch bağlı olan birbirlerinin oluşan broadcast trafiğinden en asgari düzeyde etkilenmekte ya da hiçbir şekilde etkilenmemektedirler. Yaratılmış olan sanal LAN'ların veri alış verişi yapabilmeleri için switch' in ana router'a bağlı f0/1 interface trunk modundadır.

Router switch'e bağlı interface ve altarayüz (subinterface) diye kendi aralarında sınıflara ayrılırlar. Bu arada PC2, PC lab5 bilgisayarına ICMP protokolüyle erişimini engellemek için access-list kullanılmıştır ve şekil 8.4'de bariz bir şekilde görülmektedir.

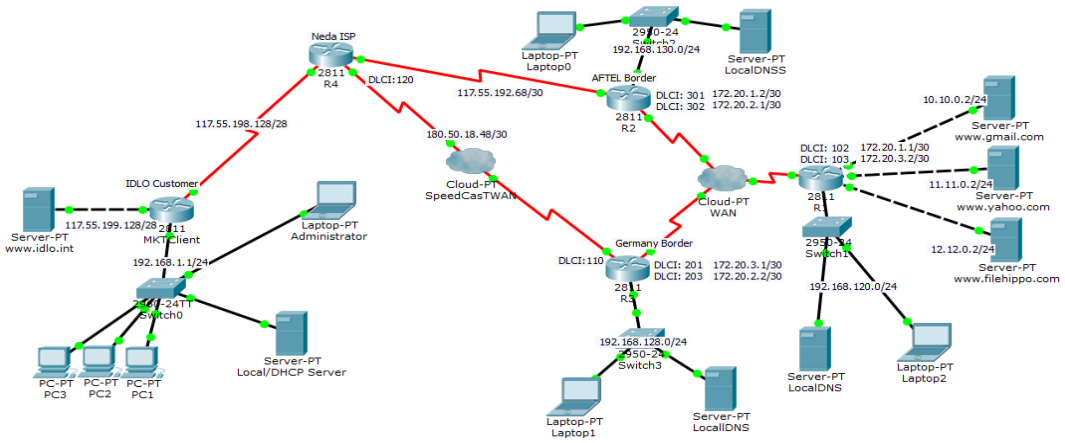


Şekil 8. 4 Router konfigürasyonu

8.2 Simulasyon

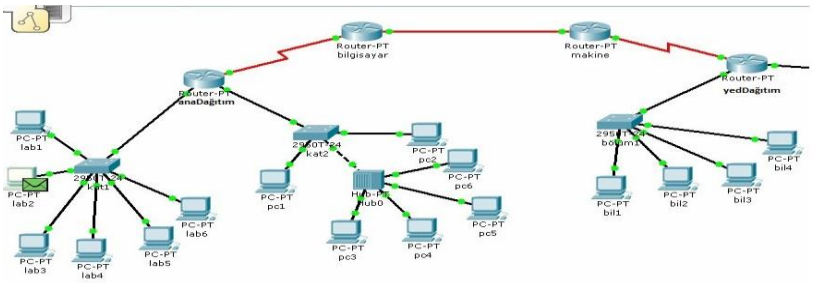
Bu benzetim çizimi için Cisco Packet Tracer ve Cisco system tarafından ağ performans ölçüm ve ağ laboratuvarı işlemleri yapabilen Packet Tracer 6.0.2 net benzetim programında vasıtasıyla yapılmıştır. Temel ağ olarak da görüleceği gibi şekil 8.5'de detaylı olarak çizilmiştir. Dört ana bölümden oluşan şemamızda birçok aygıt bulunmaktadır.

Bu işlem için router, switch, PC, IP phone, Tablet PC, wireless router gibi aygıtlar kullanılmıştır. Kablo olarak router'leri optik fiber kablo ile seri porta bağlı şekilde ayarlanmıştır. Diğer switch ve router'leri bilgisayarlara düz kablo da diyebileceğimiz Twisted Pair tipi kablodan yararlanılmıştır. Ethernet olarak Fast ethernet tercih edilmesine karşın Giga Ethernet'te yarar sağlamaktadır.



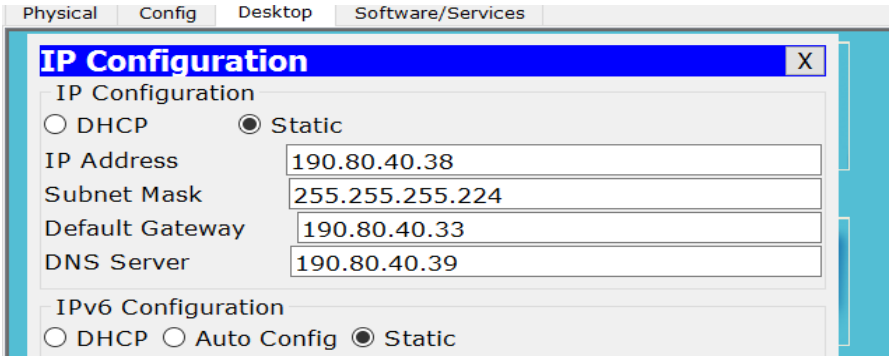
Şekil 8. 5 Temel ağ şeması

Gerekli konfigürasyonlar yapılmış, serverler eklenmiş, erişim kontrolleri ACL kuralları vasıtasıyla dizginlenmiş ve frame relay bağlantıları ayarlanmıştır.



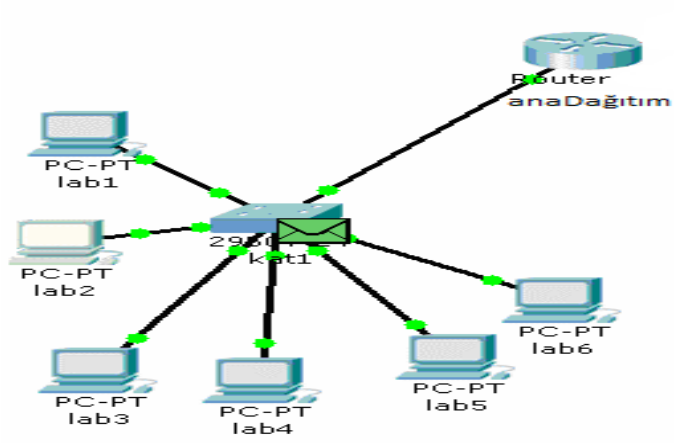
Şekil 8. 6 ICMP paket konfigürasyonu

Ayriyeten Şekil 8.6'da olduğu gibi birinci ICMP paketi gibi l2 bilgisayarından, pc8 bilgisayarına gönderilmek üzere tasarlanan bir paket bulunmaktadır. Burada pc8 PC'leri ana Dagitim router' ine bağlı, DHCP sunucusu yoluyla IP adresleri manuel olarak girilmiştir.



Şekil 8.7 Manuel statik IP girişi

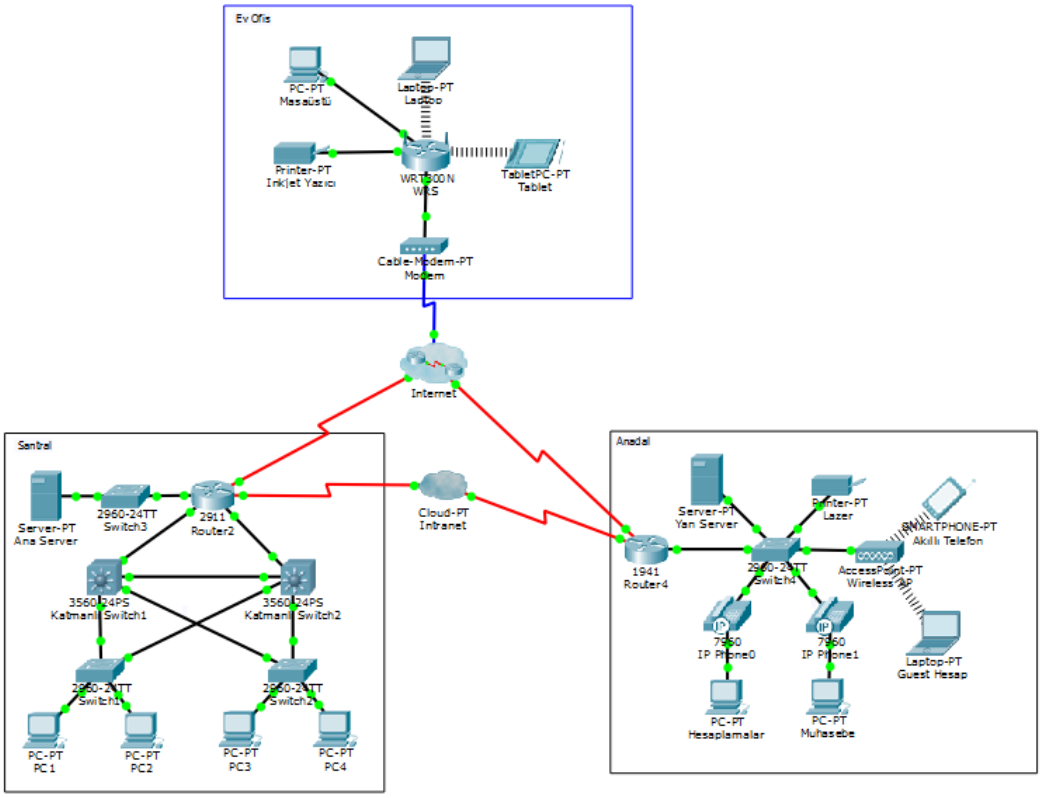
Şekil 8.7'de görüldüğü gibi IP adresler statik ve manuel olarak girilmiştir lakin IPv6 adresleri kolaylık olsun diye otomatik olarak da yapılabilir.



Şekil 8. 8 Katman 1 switch paket

Şekil 8.8'de görülüğü gibi Layer1 Switch'i gelen paketin MAC adresini kendi MAC adres char'tında bulunup bulunmadığını kontrol eder ve makro hedef olan bilgisayar kendine doğrudan bağlı olmadığından dolayı paketi yönlendirilmek üzere yed Dağıtım router'ına yönlendirir. Bir ISP ve router, modem ile bilgisayarlar kullanılmıştır. Router'a bağlı kablolar fiber optik iken diğer kablolar Twisted Pair yani çift burgulu kablo tercih edilmiştir. Seri portlar ve router ip adresleri manuel girilmiş olup hepsi statik olarak ayarlanmıştır. Fast ethernet giriş için kullanılmıştır ve şekilde verildiği gibi IP adresleri ile MAC adresler uyumu sağlanmıştır. Ayrıca bu çalışmada, birçok senaryo simüle edilmiştir.

Ağda kullanılan bu cihazlar, kablolar yerel alan ağı topolojisi hakkında bilgi sağlar, bu bilgi ağının uygulaması, paket takipçisi çevre yazılımı bu simülasyonun içinde bulundurulmuştur. Veri transferi metotları 3 e bölünür: tek noktaya, çok noktaya yayın ve çoklu aktarımlara yayın. Bir veriyi tek bir hedef adrese iletimi için, çoklu adres verilerine çoklu mesajlar yollanması gerekir. Yayın ağın verisindeki tüm düğümlere iletilir. Tüm bu iletimler tek bir paket içinde gönderilir. Sonuç olarak, bir ağ ağdaki bağlanmış diğer cihazlardan sonra gerekli olarak oluşacaktır ve veriyi her zaman ağ üzerinden iletecektir.



Şekil 8.9 Ağ ölçümü temsili

Şekil 8.9'da ağ ölçümü temsili olarak sunulmuştur. Ofis, ev, santral diye 3 ana bölümden oluşan bu WLAN'da router, switch, hub, modem ile bilgisayarlar ve santral kullanılmıştır. Modemden giden kablo wireless modem sayesinde wireless cihazlar arasında paylaşılmıştır. Simulasyon denemeleri yapılarak topolojinin doğru bir şekilde çalıştığı ispatlanmıştır.

9 eNSP (ENTERPRİSE NETWORK SİMULATİON PLATFORM)

Ağ sistemleri ile çalışırken veya ağ tasarımı yaparken yaptıklarımızı test edecek sanl bir yazılımlara ihtiyaç duyarız ve bu ihtiyaçları kaşılmak adına bir çok simülatör programı mevcuttur. Çalıştığımızda eNSP Simülatör programında kullanılmıştır.

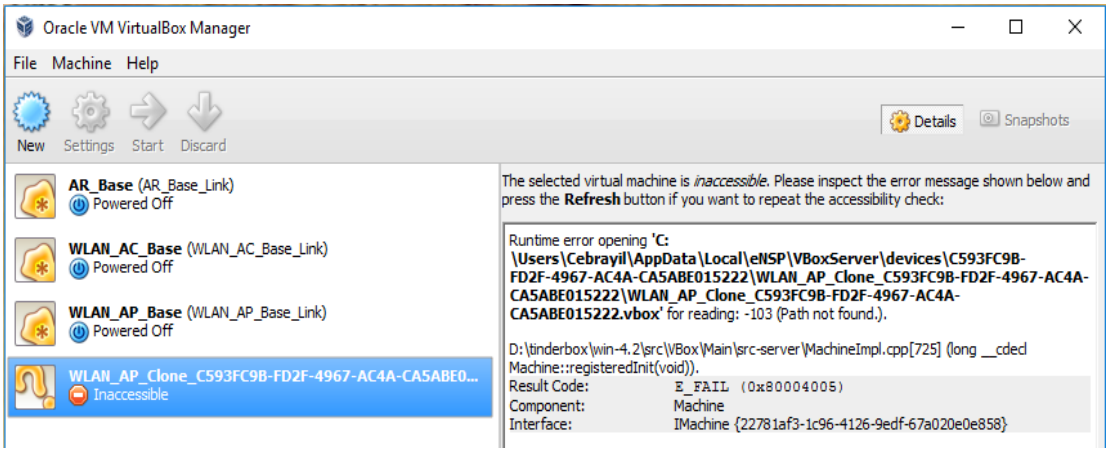
(eNSP)ya Enterprise Network Simulation Platform, Huawei tarafından geliştirilen, ücretsiz, genişletilebilir ve grafik ağı simülasyon platformudur. Huawei kurumsal yönlendiricilerini ve anahtarlarını simüle ederek, aygıt dağıtım senaryolarını gösterir. ENSP, büyük boyutlu ağları simüle edebilir. Kullanıcılar gerçek cihazlar kullanmadan deneme testleri yapabilir ve ağ teknolojilerini öğrenebilir. (Huawei, 2012). (eNSP) programını internet üzerinden ücretsiz olarak indirip kurabilirsiniz. Kurulum zamanı güvenlik duvarının açık olması lazım çünkü programı çalıştırırken Router, Switch,AccessPoint,AccessController,ya Erişim Kontrol Cihazı ,Firewall ve Cloud Engine cihazlarını çalıştırmak için teker teker izin vermek gerekir. Bu programı kurarken kendiğle birlikte Wireshark WinPcap, ve Oracle VM VirtualBox yazılımlarını da kuruyor (Savaşal, 2015).

WinPcap, bağlı olduğunuz ağla ilgili çeşitli verileri analiz etmeye yarayan Wireshark gibi bazı programların çalışması için gereken bir kütüphanedir.

Wireshark, ethernet veya modem kartlarındaki bütün TCP/IP veya UDP mesajlarını analiz edebilen bir protokoldür. Wireshark yazılımı, şebeke problemlerinde sorunu tespit etmek, güvenlik problemlerini kontrol etmek, performansı düşürecek her hangi bir sorunun olup olmadığını tespit etmek veya onarmak, ağ protokolünün içerisindeki bilgileri öğrenebilmek için kullanılır.

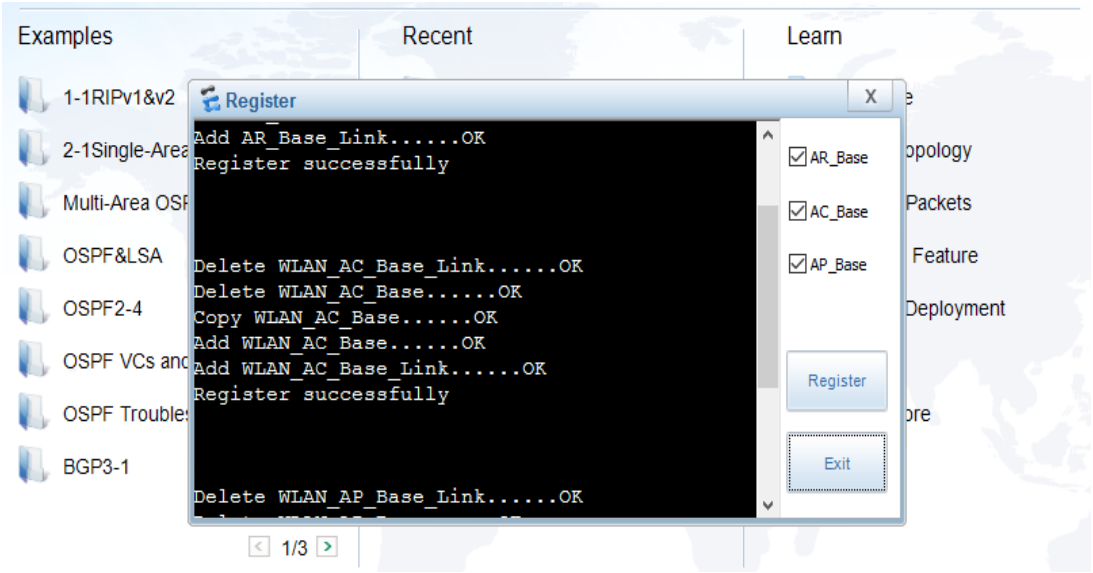
Oracle VM VirtualBox, işletim sistemi içinde bir veya daha fazla sanal makineler oluşturarak, sistem içinde sanal sistemler oluşturan bir programdır. eNSP de çalıştıracağımız her cihaz için Oracle VM VirtualBox birer sanal makine kurar. Bazen sanal makinelerden biri her hangi bir sebepen dolayı patlak verdiğinde yani çalışmayı durduğunda eNSP de o cihaz da çalışmaz (Huawei, 2014). Bu zaman

Oracle VM VirtualBox u yönetici olarak çalıştırarak o sanal makineyi kaldırıp yeniden o cihaz için sanal makine oluşturmak lazım.



Şekil 9.1 Oracle VM VirtualBox görüntüsü

Bunları bittikten sonra hiçbir cihaz eklemeden önce Menu sekmesinden TOOLS sekmsi seçip Ragister Device sekmsine AR, AC, ve AP seçilip butonuna tklanmalıdır. (Kaya, 2014).

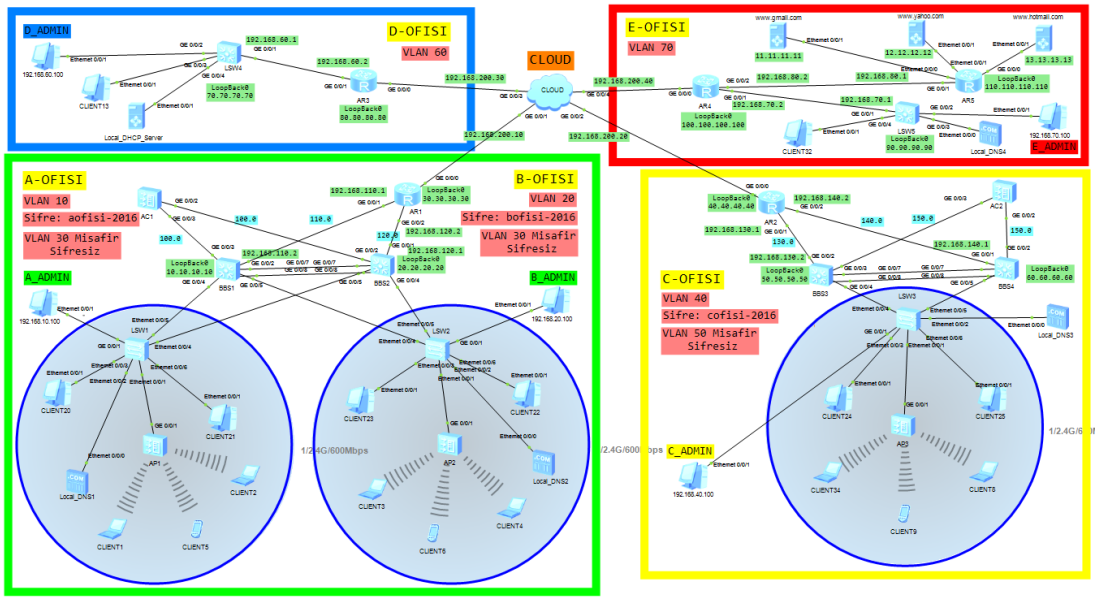


Şekil 9.2 Register işleminin tamamlanması

Yukarıda gösterildiği gibi kayıt işlemleri başarılı bir şekilde yapıldıktan sonra eNSP yi kullanabiliriz.

9.1 Tasarlanan Ağın Haritası

eNSP de yapılan tasarımda 5 adet router, 9 adet switch, 2 adet acces controller, 12 adet kablolu bilgisayar, 6 adet dizüstü bilgisayar, 2 adet cep telefonu, DHCP ve DNS serverler kullanılmıştır.



Şekil 9.3 Ağ haritası

9.2 Tasarlanan Ağın Konfigürasyonu

Tasarımın ilk kısmında cihazlar gösterildiği gibi ağ haritasında yerleştirilerek bütün offislerin ve cihazlarin isimleri verilecektir. İsimleri verdikten sonra yukarıda da belirtilen karışık tasırım oldoğundan dolayı switch'lere ve access controller'e STP protokolü uygulanacaktır. STP uygulanırken performansı etkileyecek durumlara karşı önlemler alınacaktır.

Tasarımın ikinci kısmında ağ haritasında gösterildiği gibi VLAN'lar oluşturulacak ve ip adresleri verilecektir. Her ofis için farklı VLAN'ların oluşturulmasında ana amaç iletişim zamanı performans düşüklüğünün karşısının alınmasıdır. Aynı zamanda her hangi bir VLAN'a sızma olduğu durumlarda sadece o VLAN'a zarar vere bilirler ve böylece güvenlikde sağlanmış olur.

Tasarımın üçüncü kısmında merkez switch'lere bir tane AC (Access Controller) ve her ofisteki kenar switch'lere birer tane AP eklenerek yayın yapmaları sağlanacaktır. Performans açısından yapılaması gerekenlere konfigler yazılırken göz önünde bulundurulacaktır. Öncelikle merkez switch'leri (BBS1, BBS2, BBS3, BBS4) AC1

ve AC2'ye, kenar switch'leri AP'lere bağlayacak portların konfigürasyonları girilecektir. Daha sonra AC1 ve AC2 cihazlarında yayının yapılaması için gerekli konfigürasyonlar yapılacaktır.

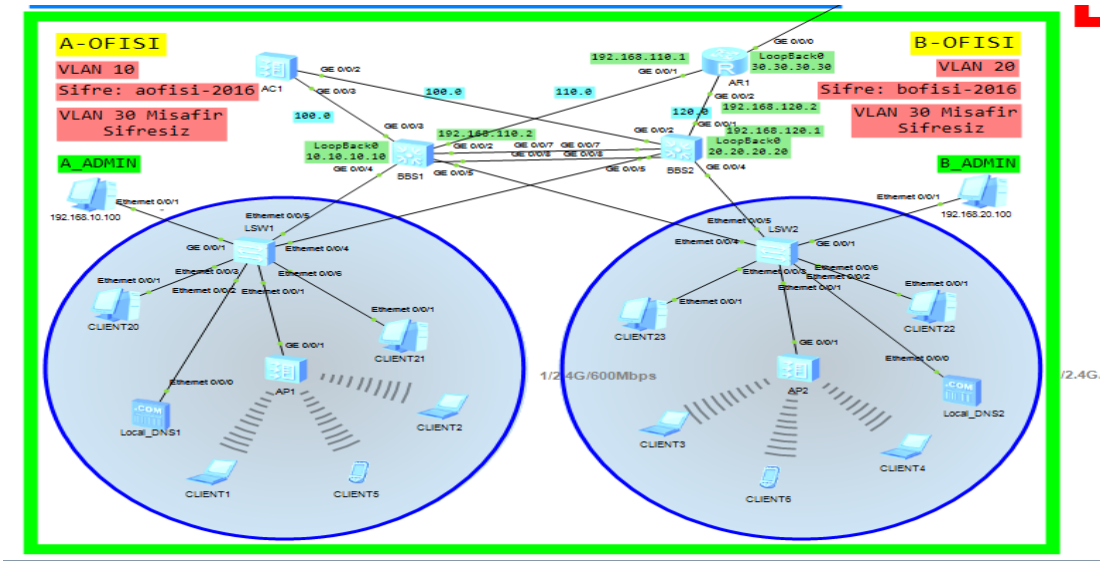
Bilindiği üzere kablosuz bir cihazın erişim noktasına bağlanması için IP adresi, alt ağ maskesi (Subnet mask), varsayılan giriş (Default gateway) ve DNS server adresi gereklidir. AC cihazlarından yayın yaptırılarak BBS1, BBS2, BBS3 ve BBS4 merkez switch'lerinden IP adresi atamaları yaptırılacaktır. Öncelikle AC1 ve AC2'ye MSTP protokolünü kullandığımızı iletmek gerekir yani MSTP protokolünü AC cihazlarına uygulamamız gerekir aksi halde AC'leri merkez switc'lere bağlayan portlar loop'a girecektir (Huawei, 2014).

Huawei cihazlarında DHCP server IP dağıtımına sonuncu IP'den başlar (Huawei, 2014). Örneğin VLAN 20'dan bağlanacak olan her hangi bir bilgisayara DHCP server, 192.168.20.254'ten başlayarak IP dağıtımı yapmaya başlayacaktır.

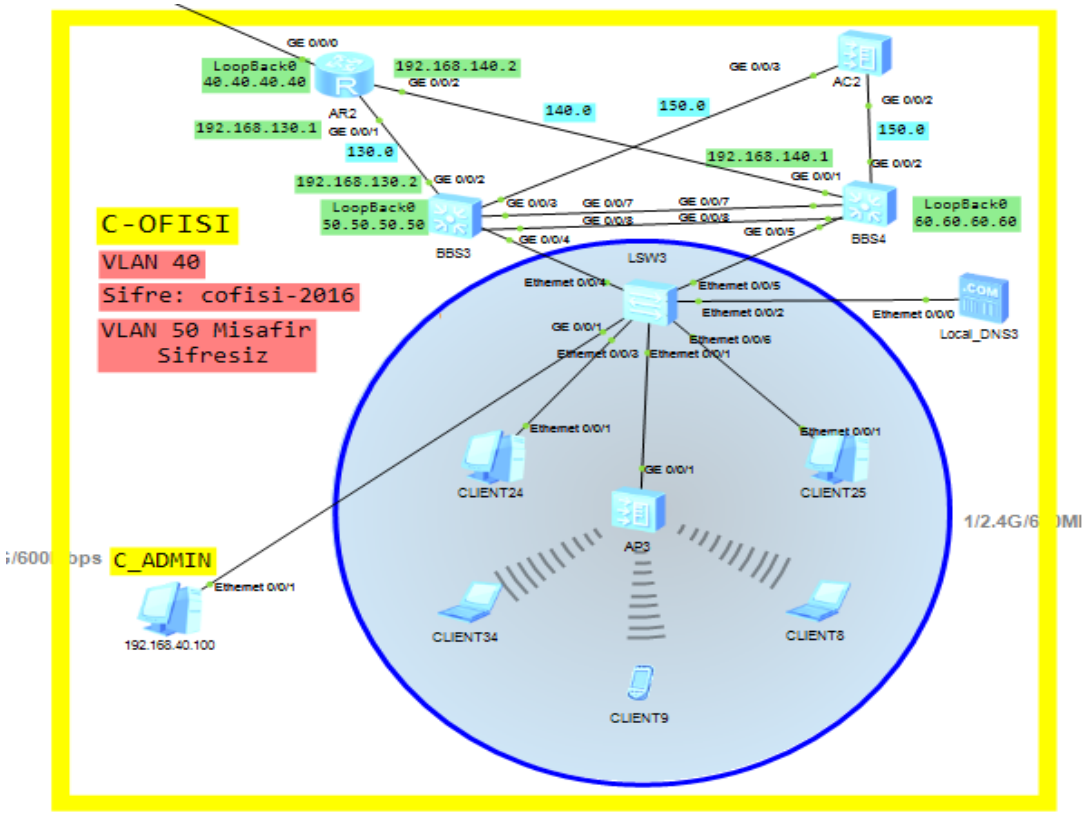
LSW1 ve LSW2'i kenar switch'lerini AP'lere bağlayan portlara default vlan 100, LSW3 kenar switch'ini AP'ye bağlayan porta ise default vlan 150 girildiğinden dolayı AC1'in ve AC2'nin ağdaki AP'leri tanımaları için öncelikle "wlan ac source interface vlanif100" ve "wlan ac source interface vlanif150" komutu daha sonra ise "ap-auth-mode no-auth" komutu girilecektir(Huawei, 2014).

AP'ler tanıtıldıktan sonra AP'nin yayın yapması için sırasıyla WMM profili, radio profili, WLAN-Ess'i, traffic profili ve security profili oluşturulacaktır(Huawei, 2014).

AP'lerin yayının yapması için son olarak hangi AP'nin hangi service set'inden yani hangi ofisden yayın yapacağını ayarlamak gerekir.



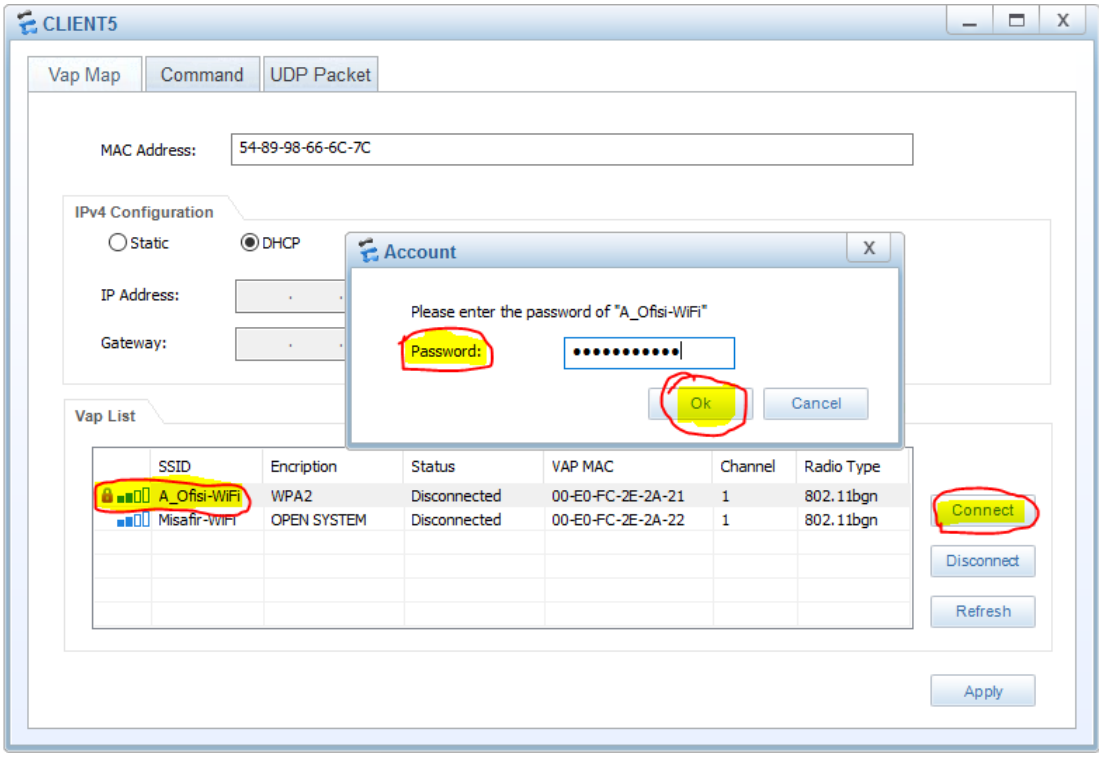
Şekil 9.4 A ve B ofislerinin AP'lerinin yayın yapması



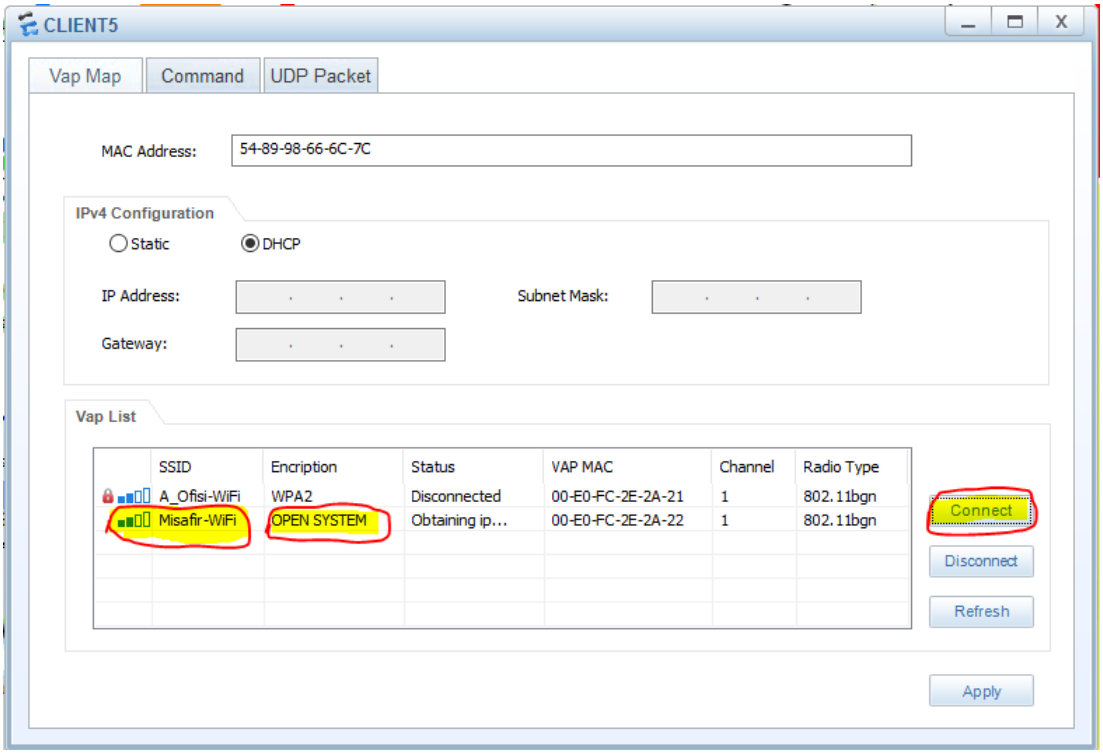
Şekil 9.5 C ofisinin AP'sinin yayın yapması

Tasarımın dördüncü kısmında şekil 9.4 ve şekil 9.5 de görüldüğü üzere Local DNS'ler, admin PC'ler, kablolu ve kablosuz cihazlar bağlanacaktır. LİNKSYS, D. (2012)

Cihazların hepsi çalıştırıldıktan sonra kablosuz cihazlardan herhangi birinin üzerine tıklıyarak ve açılan pencereden bağlanmak istenen yayını seçilerek Connect butonuna tıklanmalıdır. Bağlanmak istediğimiz ağ, şifreli yayın yapıyorsa, o ağın güvenlik şifresini doğru bir şekilde yazılmalıdır(Şekil 9.6) Ağ şifresiz yayın yapıyorsa, yayını seçtikten sonra sadece Connect yapmak ağa bağlanmak için yeterli olacaktır (Şekil 9.7).

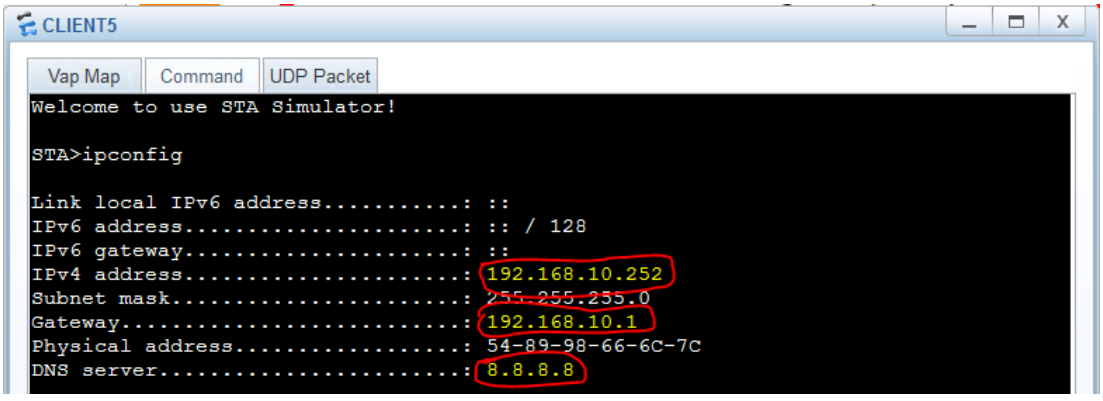


Şekil 9.6 CLIENT5'in şifreli ağa bağlanması



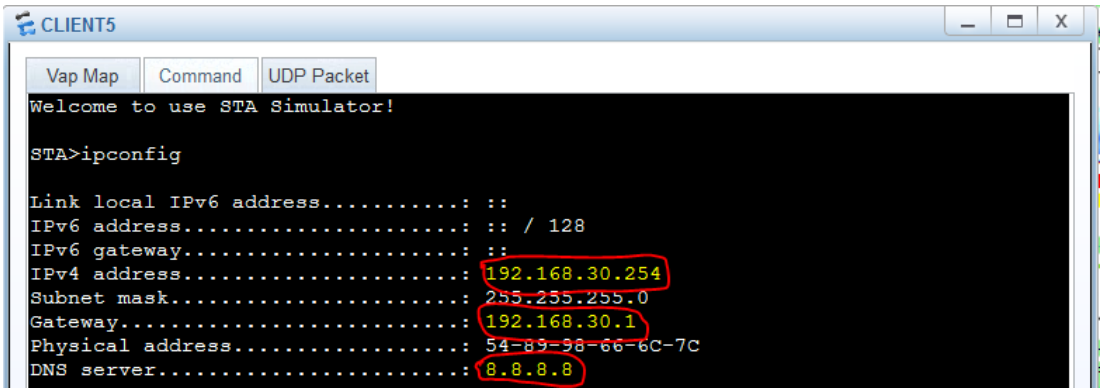
Şekil 9.7 CLIENT5'in şifresiz ağa bağlanması

CLIENT5 A_Ofisi-WiFi yayınına bağlandıktan sonra Command sekmesine gelerek, ipconfig komutuyla VLAN10'dan IP alıp almadığı kontrol edilecektir. (Şekil 9.8)



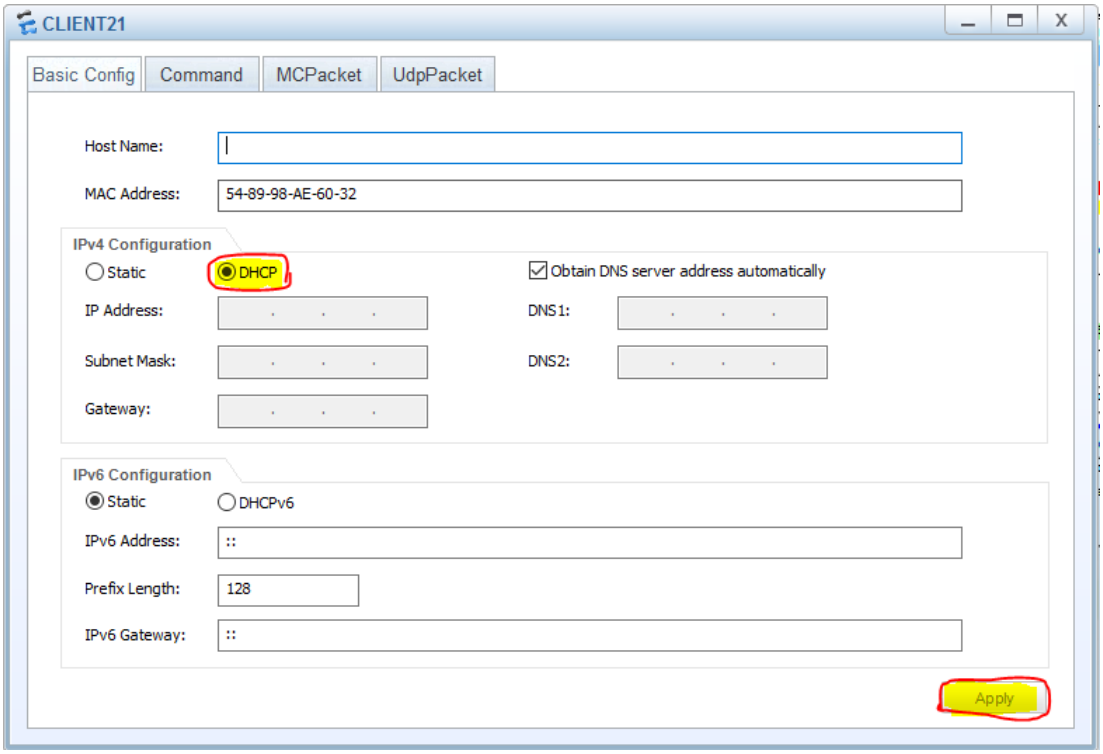
Şekil 9.8 CLIENT5'in VLAN10'dan IP alması

CLIENT5 Misafir-WiFi yayınına bağlandıktan sonra Command sekmesine gelerek, ipconfig komutuyla VLAN30'dan IP alıp almadığını kontrol edilecektir. (Şekil 9.9)



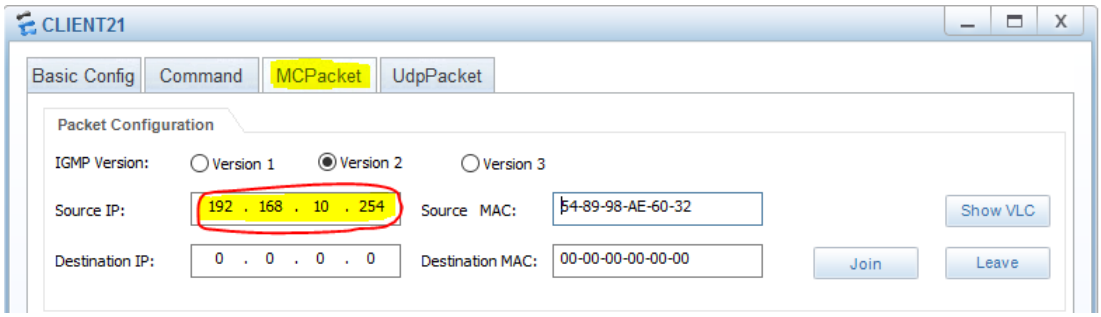
Şekil 9.9 CLIENT5'in VLAN30'dan IP alması

Kablolu cihazların ağa bağlanıp DHCP server'den doğru IP almaları için kablolu cihazları kenar switch'lere bağlayan portlarına default vlan olarak hangi vlan'dan IP almasını istiyorsak o vlan girilmelidir (Şekil 9.10).



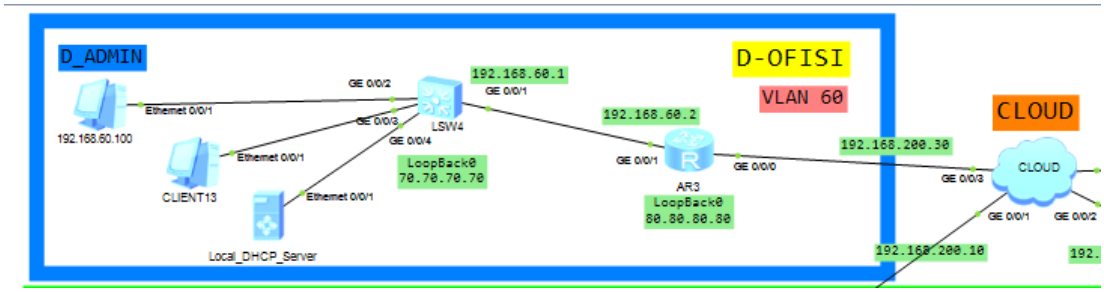
Şekil 9.10 CLIENT21'in bağlantı arayüzü

sonradan MCPaket butonuna tıklayıp, Nodon DHCP'den IP alması beklenmelidir. (Şekil 9.11)

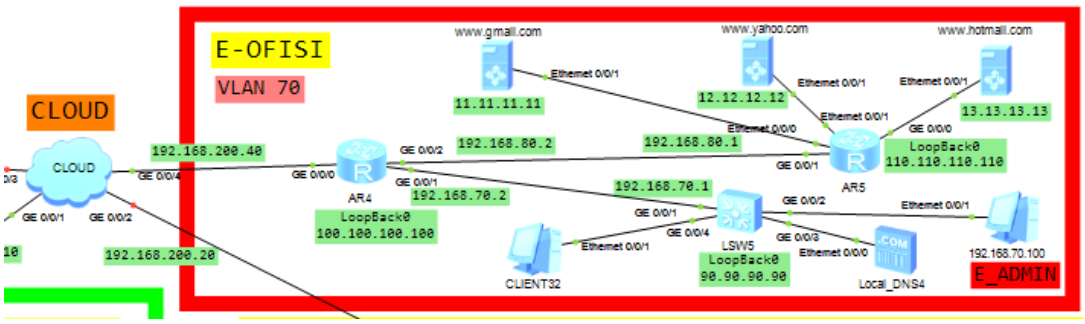


Şekil 9.11 CLIENT21'in VLAN10'dan IP alması

Tasarımınn beşinci kısmında ise sadece kablolu yayınlar yapan D (Şekil 9.12) ve E (Şekil 9.13) ofisleri tasarlanacaktır. Router'lar switch'lere switch'ler ise PC'lere aynı A, B ve C ofislerinde bağlandığı gibi bağlanarak konfigurasyonları yapılacaktır.



Şekil 9.12 D ofisinin çalışır hali



Şekil 9.13 E ofisinin çalışır hali

Tasarımın altıncı kısmında ise A, B, C, D ve E ofislerinin bir birileriyle performanslı şekilde yani veri kaybı olmadan ilteşim kurabilmeleri için OSPF protokolü uygulanacaktır. OSPF protokolü uygulandıktan sonra tüm cihazlar bir birileriyle iletişim kura biliyor olacaktır. Fakat bu istenmeyen bir durumdur. Çünkü örneğin A ofisinden bağlanan çalışan istediği zaman D ofisindeki admine, router'a veya switch gibi cihazlara erişe bilirse bu hem performans düşüklüğüdür hem de çok büyük güvenlik güvenlik açığıdır. HUAWEİ. (2014) Bu sorunları aradan kaldırmak için ACL kurallarının yazılması ilk şarttır. Yukarıda da belirtildiği gibi unutmamamız

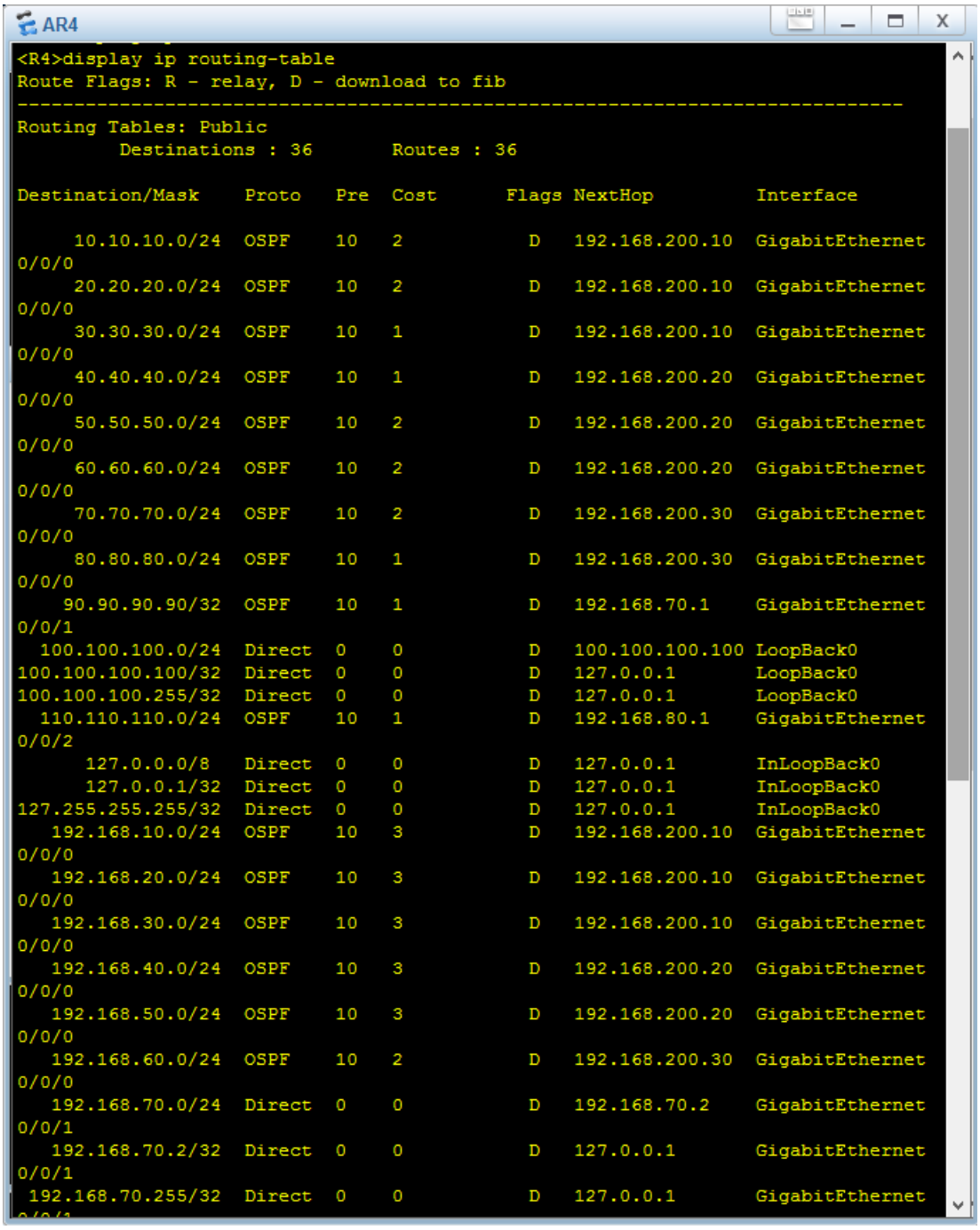
lazım ki, bu tasarım gerçek labaratuvar ortamlarında değilde ücretsiz paylaşılan sanal labaratuvarlarda tasarlanmıştır. Bu yüzden de yapabileceğimiz konfigurasyonlar ve çalıştırabileceğimiz cihazlar kısıtlıdır.

Daha sonra cihazlara TELNET bağlantısı yapılabilinmesi için gerekli konfigürasyonlar yapılacaktır.

9.3 Ağın Performans Kontrolünün Yapılması

Ağ performans değerlendirilmesi kısmında ağ topolojisinin performans değerlendirilmesi için gerekli olan faktörlere, modellemelere ve gerekli ölçümlere değinmiştik. Fakat aynı zamanda gerçek ağ üzerinde değilde sanal ortamda kurulmuş hayali bir ağ topolojisi üzerinde değerlendirme yapacağimiz için alına bilecek veriler kısıtlıdır. Bunun yanı sıra eNSP'nin CISCO Packet Tracere göre eksik bir yanı simülasyon özelliğinin olmaması. Bu yüzden de değerlendirmeyi ispatlamak için cihazları çalıştırarak ICMP paketi yolayarak erişim kontrolleri yapılacaktır.

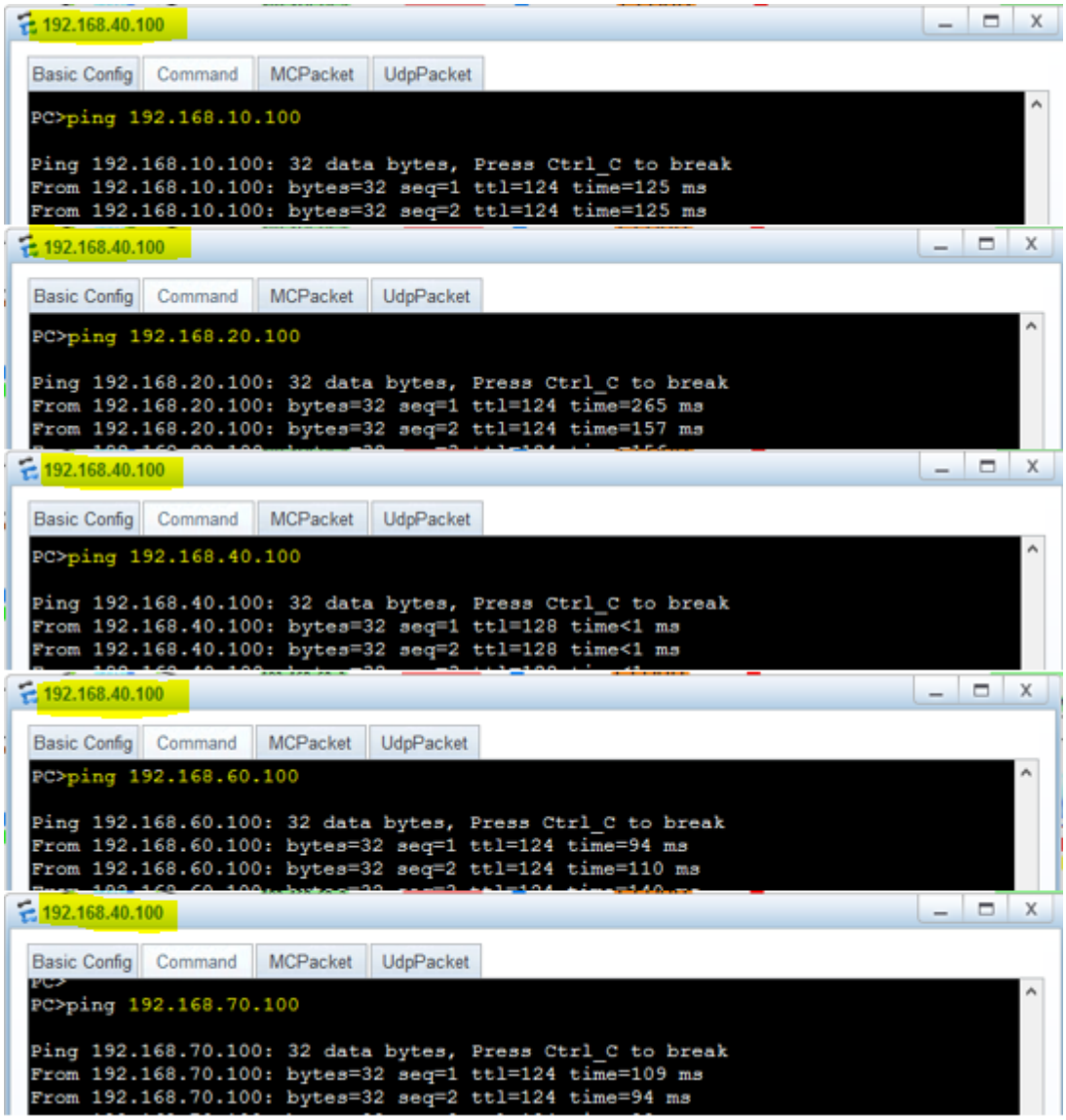
Öncelikle bir ağ tasarlarken göz önünde bulundurulması gereken ilk şart topolojimizin tüm şartlarda performans şekilde çalişmasını sağlanmasıdır. Yani olurda bir hata sonuçu her hangi bir portta sıkıntı çıkar veya merkez switch'lerden her hangi biri bozulur veya döngüye girerse topolojimizin durmadan çalışmasını sağlamak için yedekli portlar oluşturmak lazımdır. Bu sebepten topolojimize Öncelikle STP protokolü uyguladık. Daha sonra gerekli konfigürasyonlar yapılarak her türlü toleranslı durmlarda performanslı iletişim sağlanmıştır. Ağımıza OSPF protokolü uygulanarak ağımaza eklenecek her hangi bir cihaz veya ip adresi gerektiren her hangi bir kablosuz cihaz bağlandığın da şirketimizin tüm ofislerine bildiri giderek o ip adresini öğrenmeleri sağlanmıştır. Örneğin E ofisindeki router (AR4) ağımızdaki tüm cihazlardan haberdardır. TURGUT,H.(2005) Bunu 'display ip routing-table' komutuyla ispatlaya biliriz. (Şekil 9.14)



Şekil 9.14 AR4'ün IP routing tablosu

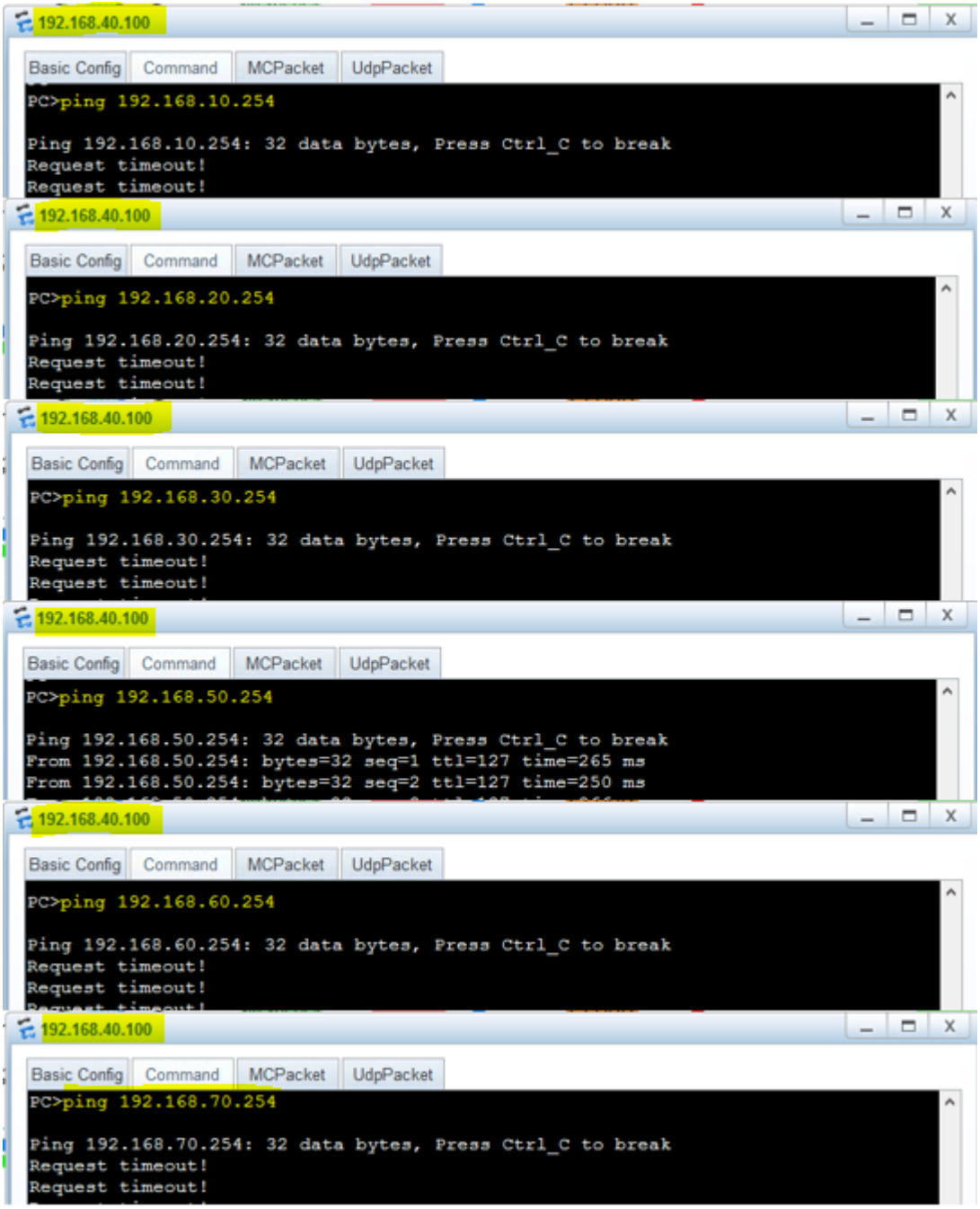
Erişim sağlandıktan sonra önemli olan güvenlik ve performans açısından erişimlerin doğru şekilde kısıtlanmasıdır. Yani örneğin A ofisindeki her hangi bir çalışan diğer ofisdeki çalışanlara özellikle de admin PC'lere erişimi kısıtlı olmalıdır. Bu yüzden topolojimizde ICMP paketlerini ACL kuralları yazarak engellemeler koyduk. Bu engellemeleri ispatlamak için cihazları çalıştırıp ping komutu sayesinde ICMP paketi yollayarak ispatlaya biliriz.

Öncelikle C ofisinin adminin diğer adminlerle ilişki durumuna bakalım (Şekil 9.15). Şekil 9.15'den de görüldüğü üzere C_Adminin ağımızdaki diğer adminlerle iletişim kurma yetkisi vardır.



Şekil 9.15 C_Adminin diğer adminlere erişim durumu

Daha sonra C_Adminin ağımızdaki diğer çalışanlara ve misafir yayınlarına bağlantı durumlarına bakalım (Şekil 9.16). Şekil 9.16'dan görüldüğü üzere C_Admin istenildiği gibi sadece kendi ağındaki çalışanlara ve misafirlere bağlana biliyor. Her hangi bir ofis adminin bile diğer ofis çalışanlarına ping bağlantısı yoktur. Çünkü bu istenmeyen bir durumdur. En basit anlatımla zira iletilmesi gereken bir paket olursa öncelikle o ofisin adminine ulaşması gerek daha sonra o admin vasıtasıyla her hangi bir çalışana ulaşabilir.

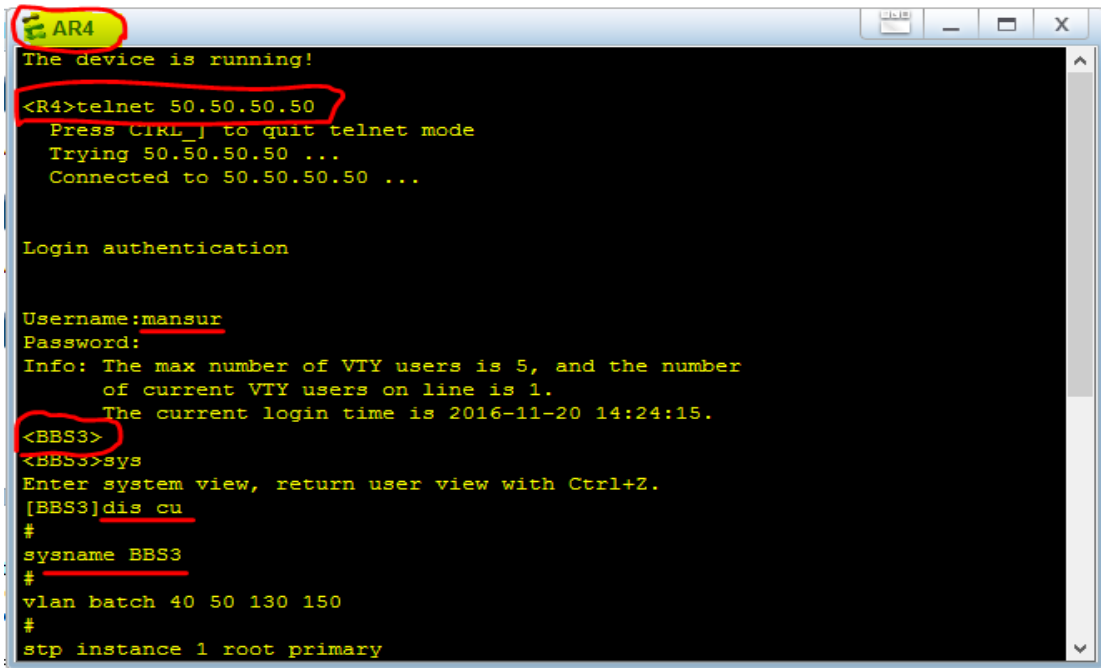


Şekil 9.16 C_Adminin diğer VLAN'lara erişim durumu

Aynı şekil de diğer adminlerin (A_Admin, B_Admin, D_Admin ve E_Adim) bağlantı durumları da kontrol edilerek aynı C_Admin gibi performanslı çalıştıkları gözlemlenmiştir. WAİT, J. (2005)

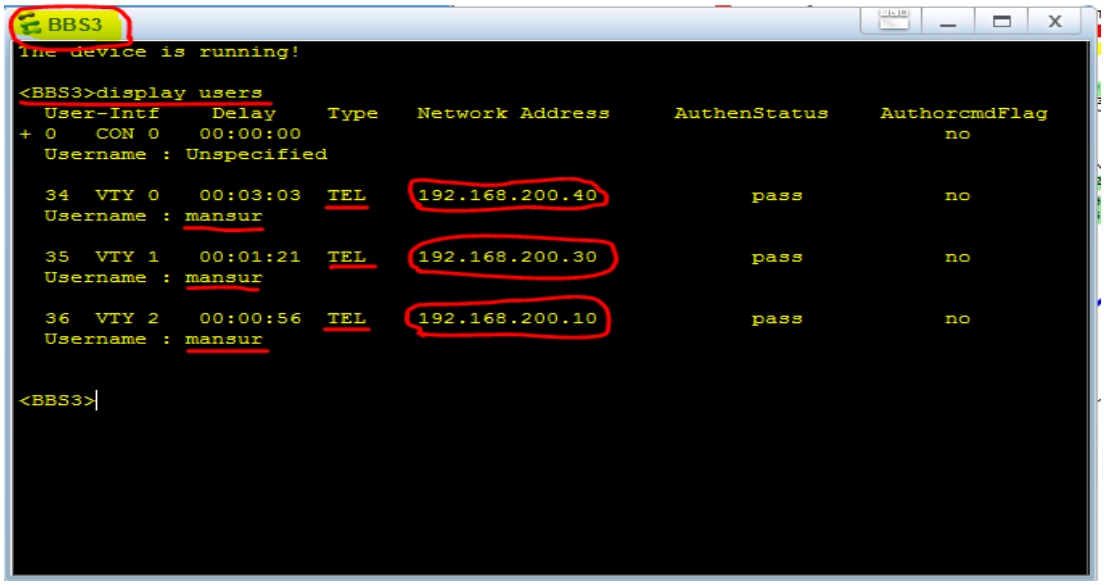
Uzaktaki bir sunucu başka bir sunucuya bağlana bilmesi için TELNET bağlantısı konfigüre edilmiştir. Bunun için kullanıcı ismi 'mansur' şifre ise 'huawei' atanmıştır. Teker teker tüm cihazlardan bağlantı yapılarak doğru bir şekilde ve ağın

performansını düşürmeden bağlantı sağlandığı gözlemlenmiştir. Örneğin E ofisinin router'inden BBS3'e TELNET bağlantısı yapalım (Şekil 9.17).



Şekil 9.17 AR4'ün BBS3'e TELNET bağlantısı yapması

Daha sonra aynı şekilde diğer routerlardan da BBS3'e bağlantı yapalım ve BBS3 switch'ini çalıştırarak 'display users' komutuyla sağlanan bağlantıları görüntüleyerek bağlantıların sağlanıp sağlanmadığını kontrol edelim.



Şekil 9.18 BBS3'e bağlanan sunucuların görüntülenmesi

10 SONUÇ

Bu tez çalışmasında ağ performans değerlendirilmesinde çeşitli parametreler nasıl bir araya toplanır, nasıl incelenir ve sonuç olarak performansı düşüren sebepleri ortadan kaldırmak için ağ tasarımı yaparken nelere dikkat edilmelisi gerektiğini anlatılmıştır. Bu sebeple performans konuları, önlemleri, gerekli parametreler göz önünde bulundurularak hem CISCO Packet Tracer de hem de Huawei'in eNSP simulasyon programında hayali ağlar tasarlanarak performans değerlendirilmeleri yapılmıştır. Fakat unutmamak lazım ki, tasarlanan ağlar gerçek laboratuvarlar da değilde ücretsiz sanal ortamlarda tasarlanmış ve değerlendirilmiştir. Sanal bir ortamda çalışıldığı için yapılacak ve ispatlanacak konfigürasyonlar kısıtlıdır. Bu yüzden de elimizde gerçek veriler olmadığı için gerçek performans değerlendirilmesi yapmak ve çıktılar almak mümkün değildir. Sadece performans gereksinimleri göz önünde bulundurularak ağlar tasarlanmış ve sanal ortamların izin verdiği kadar değerlendirme yapılarak ağ performans değerlendirilmesi yapılmıştır. Bu çalışmaların sonucunda CCNA ve CCNP konfigürasyonları yapılmıştır. Statik ile dinamik IP simülasyon programı hazırlanmıştır. Bunu yanı sıra LAN ve WLAN ağları ile yönlendirici, Switch'ler, Hub'lar, IP telefonlar, frame-relay ve ihtiyaç duyulan bütün server'ler üzerinde işlem yapılmıştır. Bunların simülasyonu yapılmış olup hepsi teker teker test edilmiştir ve en önemli konusu bu ağların birbirleri ile bağlantı yaparken ağın performansını değerlendirmesi yapmaktadır.Ve simülasyon programları kullanılarak bire bir gerçek benzetim yapılarak birçok topoloji gerçekleştirilmiştir. Bunlar gerçek Router, Switch ve Hub'lar ile aynı konfigürasyona sahiptirler. Buna ilaveten çalışmada hayali olarak bir `şirketin ayrı ayrı şehirlerde yerleşen A, B, C, D ve E ofislerinden oluşan ağ topolojisi tasarlanmıştır. Bu tasarımın ana amacı kapsamlı ve gelişmiş kurumsal kullanıma kadar, performanslı bir kabulolu ve kablosuz yerel alan ağını oluşturmak için izlenmesi gereken politikaları ve temel yöntemleri belirlemektir. Bu sebeple bu çalışmada Router, Switch, kablolu ve kablosuz cihazlar ve gerekli sunucuları ve protokolleri içeren bir ağ tasarlanmıştır. Ve sonuç olarak sanal bir ortamda hazırlanan ağ olduğu için belirlediği kuraller çerçevesinde ağin çalıştığını göstermek

ağ performans değerlendirmesidir. Umarım, bu bilgiler ile donanarak, performans problemleri çıkmadan önce onları tam olarak teşhis edebilirsiniz.

KAYNAKLAR

OLİVİER BONAVENTURE, Computer Networking: Principles, Protocols Practice October30, 2015 tarihinde http://www.computerhope.com/jargon/n/network.htm.pdf adresinden alındı

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

PEKKÜÇÜK, G. İ. Uzar, and N.Ö. Ünverdi, Optik Filtrelerde Performans Analizi
Performance Analysis of the Optical Filters.
https://www.researchgate.net/.../NS-VEYA-PAKET-IZLEYICI-GIB.

BAYKARA, M. R. Daş, and İ. **KARADOĞAN**. Bilgi Güvenliği Sistemlerinde
Kullanılan Araçların İncelenmesi. in 1st International Symposium on Digital Forensics
https://www.journals.elsevier.com/**digital**-investigation

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 cozum park: http://www.cozumpark.com/blogs/network/archive/2008/04/29/temel-ag-topolojileri.aspx adresinden alındı

ADMİN (2011, 1 11) Güvenlik Duvarı Nedir?6 5, 2016 tarihinde cyber warrior: https://www.cyber-warrior.org/forum/guvenlik-duvari-nedir_412479,0.cwx adresinde

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

BAYDAR, S. (2013, 11 13). OSPF Hakkında Herşey. 6 , 12, 2016 tarihinde btyardım: http://www.btyardim.com/ospf-hakkinda-hersey.php adresinden alındı,

DİKİCİ, B. (2013, 9 7). Temel Ağ Cihazları. 5, 14, 2016 tarihinde itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/temel- a%C4%9F

HUAWEİ. (2012, 7 20). Feature Description - Security. 4 6, 2016 tarihinde huawei: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC0100534396 adresinden alındı

HUAWEİ. (2014, 1 16). Configuration Guide - Security. 4 6, 2016 tarihinde huawei: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000019451&idPath=7919710%7C9856750%7C7923148%7C9858988%7C6078839 adresinden alındı

HUAWEİ. (2014, 4 20). HCNA-WLAN Course Experiment Guide for WLAN Engineers.42,2016tarihindehuawei:

http://support.huawei.com/learning/trainFaceDetailAction?courseId=Node1000004789&pbiPath=term1000025181&lang=en adresinden alındı

HUAWEİ. (2014). Huawei Certified Network Associate -WLAN Edition v1.6. 4 5, 2016tarihindehuawei: http://support.huawei.com/learning/Certificate!showCertificate?lang=en&pbiPath=term1000025450&id=Node1000004563 adresinden alındı

KAYA, M. (2014, 5 25). Spanning Tree Protokolü Saldırı Ve Korunma Yöntemleri. 5,16,2016tarihinde,cozumpark: http://www.cozumpark.com/blogs/network/archive/2014/05/25/spanning-tree-protokolu-saldiri-ve-korunma-yontemleri.aspx adresinden alındı

KÖSAL,A.S.(2007, Mayıs). 802.11 Kablosuz Yerel Alan Ağlarında Güvenlik Sorunu. Sakarya: Sakarya Üniversitesi Yüksek Lisans Tezi. 5 20, 2016 tarihin

MEGEP.(2011).Kablosuz Ağ Sistemleri. 3 27, 2016 tarihinde megep: http://www.megep.meb.gov.tr/mte_program_modul/moduller_pdf/Kablosuz

SAVAŞAL,S.(2015, 12 3). Huawei eNSP. 6 10, 2016 tarihinde selcuk.savasal: http://www.selcuk.savasal.com/?p=255 adresinden alındı

BAŞ, F. (2008, Nisan). Cisco ağ teknolojileri yönetimi. (B. Üçüncüoğlu, Dü.) İstanbul. https://docs.google.com/file/d/0B9trw0kbT3aPOGZBX1dISmVmQjg/edit?pli

CİSCİ.(2008). Campus Network for High Availability Design Guide. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_cam

CİSCİ.(2008, 21 Mayıs).Yönlendirme protokollerinin yeniden dağılımı. http://www.cisco.com/cisco/web/support/RU/9/92/92190_redist.pdf adresinde

CİSCİ.(2014).VLANTrunkProtocol.: http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

CİSCİ.IPtelephonybasicconfiguration. (2015,Şubat). VoIP: http://www.packettracernetwork.com/tutorials/voipconfiguration.html adresinden alındı

ITS. (2011). Campus Network Report. Texas: The University of Texas at Austin. https://www.utexas.edu/its/network/reports/Campus%20Network%20Report%202011.pdf adresinden alındı

İTÜBDB. (2013,Eylül). Frame Relay yapısı: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/frame-relay adresinden alındı

İTÜBİDB.(2013,Eylül7). CaptivePortal (KısıtlamaPortalı).İstanbul. http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/captive-portal-(k%C4%B1s%C4%B1tlama-portal%C4%B1) adresinden alındı

LİNKSYS, D. (2012). Linksys configuration. http://www.linksys.com/ca/support-article?articleNum=142912 adresinden alındı

P, C. (tarih yok). Fiber Distributed Data Interface . Yüksek hızlı bilgisayar ağı: http://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2408.htm adresinden alındı

TURGUT, H. (2005). Ağ Teknolojileri , OSPF Protokolü. https://en.wikibooks.org/wiki/Routing_protocols_and.../Open_Shortest_Path_First

WAİT, J. (2005). Network Protocols and OSI model. Indiana. https://en.wikibooks.org/wiki/CCNA_Certification/Network_Layer

ÖZGEÇMİŞ

Ad-Soyad **:Sayed Mansoor HASHIMI**

E-Posta **: mansoor.man777@yahoo.com**

KİŞİSEL BİLGİLER

Doğum Tarihi ve Yeri **: Kabul, AFGHANİSTAN**

Date of Birth: **:18.11.1988**

Medeni Durum **: Bekar**

Askerlik Durumu **: Hayır**

EĞİTİM BİLGİLERİ

Lisans **: Kabil Eğitim Üniversitesi / Bilgisayar Mühendisliği**

Yüksek Lisans **: İstanbul Aydın Üniversitesi / Bilgisayar Mühendisliği**

SERTİFİKA BİLGİLERİ

BİLGİSAYAR BİLGİSİ

- ✓ **Microsoft Office**
- ✓ **A+ Hardware Comp (TIA)**
- ✓ **MCSE (MCITP)**
- ✓ **CCNA (Online Certified)**
- ✓ **CCNA (Online Certified)**
- ✓ **IT Essential 1 (Online Certified)**
- ✓ **IT Essential 2 (Online Certified)**