T.C.

İSTANBUL AYDIN ÜNİVERSİTESİ

FEN BİLİMLER ENSTİTÜSÜ

KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ YÜKSEK GÜVENLİKLİ KABLOSUZ YEREL ALAN AĞININ TASARIMI

YÜKSEK LİSANS TEZİ

JABRAYİL ALİZADA

Y1313.010031

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Yrd. Doç. Dr. Vassilya UZUN

EYLÜL 2016

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1313.010031** numaralı öğrencisi **JABRAYİL ALİZADA**'nın **"KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ YÜKSEK GÜVENLİKLİ KABLOSUZ YEREL ALAN AĞININ TASARIMI"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 25.08.2016 tarih ve 2016/21 sayılı kararıyla oluşturulan jüri tarafından ..oybirliği.. ile Tezli Yüksek Lisans tezi olarak ..kabul..edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi :29.09.2016	
1)Tez Danışmanı: Yrd. Doç. Dr. Vassilya UZUN	.....
2) Jüri Üyesi : Yrd. Doç. Dr. M. Ahmad SHAH	.....
3) Jüri Üyesi : Yrd. Doç. Dr. Metin ZONTUL	.....

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

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ YÜKSEK GÜVENLİKLİ KABLOSUZ YEREL ALAN AĞININ TASARIMI" 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

Hayatımızın artık vazgeçilmez bir kısmı olan internet ve bilgisayarların iletişim alanında kullanımı her geçen gün daha da büyümektedir. İnternet milyonlarca bilgisayarın bağlandığı ve irili ufaklı binlerce küçük alt ağın olduğu geniş bir alan ağıdır. Bu geniş ağlarında güvenlik ve savunma konusu yöneticilerden teknik personele her kurumun ilgilendiği ve kendini geliştirmek istediği bir alandır. Güvenlik konusu kurumdaki diğer tüm konularla bağlantılı olduğu için karmaşık bir konudur ve organizasyon gerektirir. Diğer bir taraftan alınan güvenlik tedbirlerinin beraberinde yeni güvenlik açıkları ortaya çıkarıyor olması ayrıca ironik bir durumdur.

Bu tez çalışması, kablosuz ağların özellikle de Kablosuz Yerel Alan Ağların (WLAN) tanınması, avantaj ve dezavantajlarının öğrenilmesi, mevcut güvenlik ve saldırı yöntemlerinin öğrenilmesi ve kablosuz ağlarda güvenliğin aslında ne kadar önemli olduğunun anlaşılması için pratik bir kılavuz olacaktır. Bu çalışmadan edinilecek bilgiler sayesinde kablosuz ağ kullanıcıları, ağ güvenliklerini daha da güçlendirmek için neler yapmaları gerektiklerini öğreneceklerdir. Bu sebeple 5 katlı hayali bir ofisin Kablosuz Yerel Alan Ağı tasarlanacaktır. HCNA ve HCNP eğitim seviyesinde kullanılabilecek temel konfigürasyonlar kullanılacaktır. HCNA eğitimi, network alanında Huawei cihazları ile çalışmak isteyenler için ilk basamak olarak değerlendirilebilir. Bu eğitimin amacı temel network bilgilerini, WLAN ve WWAN ağ dizaynını, router ve switch gibi aktif ağ cihazlarının konfigürasyonlarını, ağın optimizasyon ve performans ayarlarının yapılmasını öğretmektir. HCNP eğitimi ise orta ve büyük ölçekli kurumsal Huawei Network sistemlerini kurmak ve yönetmek için gerekli olan bilgi ve yetenekleri verir. Bu eğitim katılımcılara küçük, orta ve büyük ölçekli ağ alt yapılarının, ihtiyaçlarını belirlemek aktif cihaz kurulumları yapmak, cihazları yönetmek, bakım ve hata durumlarına karşı önlemler alma yeterliliklerini sağlayacaktır. Dünyada ağ alanında geçerliliği olan sertifikaları alabilecek bilgi birikimine sahip olmak ve bu alanda kariyer yapmak isteyenler için hazırlanmış bir eğitim programıdır. Bu çalışmada da HCNA ve HCNP tanımları ve becerileri doğrultusunda yüksek güvenlikli yerel alan ağı yapılandırılacaktır.

Geçirdiğimiz eğitim süreci boyunca ilminden ve tecrübelerinden yararlandığım tüm hocalarıma ve bu projenin başarıyla tamamlanması vesile olan kişilere saygılarımı ve şükranlarımı sunuyorum. Ayrıca Yrd Doç Dr. Vassilya UZUN motivasyonundan dolayı teşekkür ediyorum. Rehberlik ve destek, bu projenin başarısı için en önemli unsurdu. Bana sürekli destek verenlere yardımları için minnettarım. En önemlisi, ailem olmadan bu mümkün olmazdı. Bu tez benim aileme, yakınlarıma, dostlarıma, sevgi, ilgi, destek ve kuvvet verenlere adanmıştır.

Eylül, 2016 Jabrayil ALİZADA

İÇİNDEKİLER

Sayfa

KISALTMALAR

ACL :Access List (Erişim Listesi)
AES :Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
AP :Access Point (Erişim Noktası)
ARP :Address Resulotion Protocol (Adres Çözümleme Protokolü)
BBS :Backbone Switch (Omurga Anahtarı)
BPDU :Bridge Protocol Data Units (Köprü Protokolü Veri Birimi)
CBC-MAC :Cipher Block Chaining Message Authentication Code Protocol (Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu)
CCMP :Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu)
CRC :Cyclic Redundancy Check (Döngüsel Yineleme Sınaması)
DDoS :Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DFS :Dynamic Frequency Selection (Dinamik Frekans Seçimi)
DHCP :Dynamic Host Configuration Protocol (Dinamik Ana BilgisayarYapılandırma Protokolü)
DNS :Domain Name Server (Alan Adı Sunucusu)
DoS :Denial of Service (Servis Reddi)
DSSS :Direct Sequence Spread Spectrum (Doğrudan Sıralı Yayılı Spektrumu)
EAP :Extensible Authentication Protocol (Genişletilebilir Doğrulama Protokolü)
EAP-MD5 :Message Digest Five (Mesaj özü)
EAP-TLS :Transport Layer Security (Taşıma Katmanı Güvenliği)
EAP-TTLS :Tunneled Transport Layer Security (Tünellenmiş Taşıma Katmanı Güvenliği)
eNSP : Enterprise Network Simulation Platform
ETSI :European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
FW :Firewall (güvenlik duvarı)
FHSS :Frequency-Hopping Spread Spectrum (Frekans Atlamalı Geniş Spektrum)
Gbps :Gigabit per second (Saniyede bir milyar bit)
Ghz :Gigahertz (Saniyede bir milyar devir)
GSM :Global System for Mobile Communications (Gezgin İletişim için Küresel Sistem)
GPRS :General Packet Radio Service (Genel Paket Radyo Servisi)
HiperLAN :High Performance Radio LAN (Yüksek Performanslı Telsiz LAN)
HTTP :Hypertext Transfer Protocol (Üstmetin Aktarım Protokolü)
ICMP :Internet Control Message Protocol (İnternet Kontrol Mesajı Protokolü)
ICV :Integrity Check Value (Bütünlük Kontrol Değeri)

IEEE :Institute of Electrical and Electronics Engineers (Elektrik Elektronik Mühendisleri Enstitüsü)
IP :Internet Protocol (İnternet Protokolü)
ISM :International Security Management (Uluslararası Güvenlik Yönetimi)
IV :Initialization Vector (Başlangıç Vektörü)
LAN :Local Area Networks (Yerel alan ağları)
LEAP :Lightweight Extensible Authentication Protocol (Sadeleştirilmiş Genişletilebilir Yetkilendirme Protokolü)
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)
MIC :Message Integrity Code (Mesaj Bütünlük Kodu)
MIMO :Multiple Input Multiple Output (Çoklu Giriş Çoklu Çıkış)
MSTP :Multiple Spanning Tree Protocol (Çoklu Genişleme Ağacı Protokolü)
OFDM :Orthogonal Frequency Division Multiplexing (Dikey Frekans Bölüşümü Çoğullama)
OSPF :Open Shortest Path First (En Kısa Yolu Aç)
PC :Personal Computer (Kişisel Bilgisayar)
PEAP :Protected EAP (Korunmuş EAP)
PRNG :Pseudo Random Number Generator
QoS :Quality of Service (Hizmet kalitesi)
R :Router (Yönlendirici)
RADIUS :Remote Authentication Dial-In User Service (Uzaktan Aramalı Kullanıcı Kimlik Doğrulama Servisi)
RC4 :Rivest Cipher 4 (Ron Rivest Simetrik Şifreleme Algoritması)
RF :Radio Frequency (Radyo Frekansı)
RSN :Robust Security Network (Çok güvenli ağ)
RSTP :Rapid Spanning Tree Protokol (Hızlı Kapsayan Ağaç Protokolü)
SSID :Service Set Identifier (Servis Seti Tanımlayıcı)
SSH : Secure Shell (Güvenli Kabuk)
STP :Spanning Tree Protocol (Kapsayan Ağaç Protokolü)
TCP/IP :Transmission Control Protocol/Internet Protocol (İletim Kontrol Protokolü/İnternet Protokolü)
TCN :Topology Change Notification (Topoloji Değişikliği Bildirimi)
TK :Temporal Key (Geçici anahtar)
TKIP :Temporal Key Integrity Protocol (Geçici Anahtar Bütünlüğü Protokolü)
TSC :TKIP Sequence Counter (TKIP Dizi Sayacı)
TPC :Transmission Power Control (İletim Güç Kontrolü)
UDP :User Datagram Protocol (Kullanıcı Datagram Protokolü)
VLAN :Virtual Local Area Netwok (Sanal Yerel Alan Ağı)
WAN :Wide Area Network (Geniş alan ağı)
WEP :Wired Equivalent Privacy (Kabloluya eşdeğer gizlilik)
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)
WPA :Wi-fi Protected Access (Wi-Fi korumalı erişim)
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

KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ YÜKSEK GÜVENLİKLİ KABLOSUZ YEREL ALAN AĞININ TASARIMI

ÖZET

Kablosuz Ağların sağladığı kolay kurulum, esneklik, haraketlilik gibi avantajlarıyla günümüzde makul seviyelere çıkması kablosuz ağ kullanımını yaygınlaştırmıştır. Gelişen teknoloji, artan aktarım hızları ve üretici firmalar arasında giden standardizasyon çalışmaları sonucunda her geçen gün kullanıcı sayısı ve kullanım alanları artmaktadır. Kablosuz ağların geniş bir şekilde yaygınlaşması bazı güvenlik endişelerini de beraberinde getirmiştir. Günümüzde, kablosuz ağ güvenliği için çok sayıda yöntemler vardır ve her geçen gün yeni yöntemler geliştirilmektedir.
Bu tez çalışmasında kullanıcılara hayatımızın vazgeçilmezi olan Kablosuz Ağları özelliklede Kablosuz Yerel Alan Ağları (WLAN) tanıtılmış, kablosuz yerel ağ standartları, avantaj ve dezavantajları anlatılmıştır. Kablosuz yerel ağlarının güvenlik risklerinden ve bu risklere karşı alına bilecek kişisel ve kurumsal yöntemlerden bahsedilmiştir. Ağ güvenliğinde kullanılan bazı yöntemlerin ne gibi zayıflıkları olduğu açıklanmıştır. Ayrıca uygulama kısmında anlatılan güvenlik yöntemleri temel alınarak, Huawei firmasının eNSP programında 5 katlı hayali bir ofis için yüksek güvenlikli kablosuz yerel alan ağı tasarlanmıştır.

Anahtar kelimeler: *Kablosuz Yerel Alan Ağı, IEEE 802.11, WEP, WPA, WPA2, 802.1x, mevcut güvenlik yöntemleri, mevcut saldırı yöntemleri, Huawei, eNSP*

SECURITY AND ATTACK METHODS IN WIRELESS LOCAL AREA NETWORK HIGH SECURITY WIRELESS LOCAL AREA NETWORK DESIGN

ABSTRACT

Wireless Networks, by providing easy setup, flexibility, mobility advantages, has been very common to be used nowadays . The number of users and usage areas of wireless networks have been increasing day by day as a result of standardization work going between producers, emerging technologies and increasing transfer speeds. While the wireless networks being common, they have also brought some security concerns along. Today, there are many methods for the security of wireless network and new methods are being developed every day.

In this thesis work, Wireless Networks, which is indispensable in our lives, especially Wireless Local Area Networks (WLAN) have been introduced to users, and wireless local area network standards, advantages and disadvantages have been described. The security risks of wireless local area network and the personal and organizational methods can be taken against these risks are discussed. What kind of weaknesses that some methods used in network security have are explained in detail. Furthermore based on security methods described in the application part, high security wireless local area network for the fictitious 5 floors office in eNSP program of Huawei has been designed.

Keywords: *Wireless Local Area Network IEEE 802.11i, WEP, WPA, WPA2, 802.1x security methods available, existing methods of attack, Huawei, eNSP*

1 GİRİŞ

Kablosuz ağlar kullanıcılarına iletişim zamanı mekandan bağımsız ve hareket özgürlüğü sunan ağ teknolojisidir. Bu esneklik kablosuz ağ kullanıcıların ihtiyaçları doğrultusunda gün geçtikçe daha da fazla gelişmektedir. Artık hayatımızın her anında istediğimiz bilgiye cep telefonlarıyla veya dizüstü bilgisayarlarla ulaşmamız mümkündür.

Son yıllarda dizüstü bilgisayarlardaki fiyat düşüşü ve ADSL bağlantıların her ortama girmesi yanı sıra kablosuz ağların sunduğu hareket özgürlüğü, bağlantı hızının uygun seviyelere çıkması ve uygulanmasındaki basitlik ile kablosuz ağ kullanımını büyük oranda arttırdı.

Kablosuz ağların bu kadar geniş yaygınlaşması akıllara en çok merak edilen ve çekinilen konuyu, güvenlik konusunu getirdi. Kablosuz ağlardaki güvenlik riskleri kablolu ağlardaki risklerle aynıdır fakat bunlara kablosuz iletişimin hava ortamında kontrolsüz bir şekilde gerçekleştiği için yeni risklerde eklenmiştir. Kablosuz ağlarda güvenliği sağlamak adına çeşitli güvenlik mekanizmaları geliştirilmiştir.

Bu tezin amacı kullanıcılara hayatımızın vazgeçilmezi olan Kablosuz Ağları özelliklede Kablosuz Yerel Alan Ağlarını (WLAN) tanıtmak, avantaj ve dezavantajlarını öğretmek, kablosuz ağlarda güvenliğin aslında ne kadar önemli olduğunu daha iyi anlamalarına yardımcı olmaktır. Bu tezden edinilecek bilgiler sayesinde kullanıcılar kablosuz ağın güvenliğini daha da güçlendirebilecek, güvenlik tehditlerini önceden tespit edebilecek ve karşılaşılan saldırılara karşı önce veya sonra çözüm üretebileceklerdir. Bu nedenle tez 5 bölüme ayrılmıştır. İkinci bölümde kablosuz ağ sistemlerinin teknolojileri ve sınıflandırılması incelenmiştir. Üçüncü bölümde WLAN sistemlerinin tanımlanması, çalışma modları, standartları, avantaj ve dezavantajları incelenmiştir. Dördüncü bölümde WLAN sistemlerinin güvenlik ve saldırı yöntemleri incelenmiştir. Bu başlık altında kablosuz LAN ağlarının güvenlik riskleri, mevcut güvenlik ve saldırı yöntemleri incelenmiştir. Beşinci bölümde ise, anlatılan güvenlik açıkları ve çözümleri göz önüne alınarak Huawei firmasının eNSP

programında 5 katlı bir ofisin yüksek güvenlikli ağ tasarımı yapılmıştır. Son olarak altıncı bölümde ise komutlar kullanılarak tasarlanan ağın güvenlik kontrolü yapılmıştır.

2 KABLOSUZ AĞLAR

2.1 Kablosuz Ağ Sistemleri

Kablosuz ağlar en basit anlamıyla, bir veya daha fazla cihazın kablo olmaksızın haberleşmesi demektir. Kablosuz ağlar hareketli kullanıcılar için mükemmel bir ortam sağlar. Hareketli kullanıcılar denildiğinde akla zamanını çalışma masasından uzakta geçiren, toplantılara katılan, sıklıkla cep telefonlarıyla iletişim kuran kullanıcılar gelir. Kablosuz iletişim ağları bu şekilde çalışan kullanıcılara herhangi bir yerden, toplantı odasından, kafeteryadan, yoldan istedikleri zaman kendi veya şirket bilgilerine ulaşmak imkanı sağlar. Kablosuz iletişim kullanıcılarına kendi aralarında haberleşmek, dosya alış verişi yapmak gibi imkanlar da sunar.

Kablosuz ağ noktaları arasında iletişim aslında çok geniş kullanılan router modemlerle benzer şekilde çalışan ve radyo dalgalarını kullanarak havadan bilgi paylaşımı yapan iletişim sistemleriyle sağlanır. Günümüzde dizüstü bilgisayarların tamamına yakını üzerlerinde varsayılan olarak Wi-Fi alıcıları bulundururlar. Radyo dalgaları ile iletişimin 3 çeşit yolu vardır. Bunlardan kısaca bahsedersek;

- Alıcı (receiver): İsminden de anlaşıldığı gibi radyo dalgalarını alabilen fakat gönderme yetkisi olmayan cihazlardır. Bunlara örnek olarak televizyon antenlerini gösterebiliriz.
- Gönderici (transmitter): İsminden de anlaşıldığı gibi radyo dalgalarını gönderebilen fakat alma özelliği olmayan cihazlardır. Bunlara örnek olarak televizyon verici istasyonlarını gösterebiliriz.
- Alıcı/Gönderici (receiver – transmitter): Radyo dalgalarını hem alabilmek hem de gönderebilmek özelliklerine sahip cihazlardır. Bunlara örnek olarak cep telefonlarını gösterebiliriz.

2.2 Kablosuz Ağ Teknolojileri

Kablosuz iletişim dünyasında baş veren gelişmeler ve değişimler sonucunda kullanıcıların yüksek veri hızı talebi sebebiyle teknolojiler arasındaki rekabette veri hızının en önemli etki olduğu görülmektedir (MEGEP, 2011). Kablosuz ağlarda bant genişliğine ve mesafe oranına uygun olarak çeşitli kablosuz ağ teknolojileri kullanılır. Bunlardan en önemlilerinden ve en çok kullanılanlarından bahsedersek;

2.2.1 RF teknolojisi

İletişim alanında kullanılan RF (Radyo Frekans) ile bir sesi, görüntüyü, veriyi ve ya fotoyu arada bir kablo bağlantısı olmadan başka bir yere göndere bilirsin. RF ile çalışan kablosuz iletişim cihazlarının artıyor olmalarına sebep, cihazların aynı ortam içerisinde çalışırken birbirilerini enterferansa uğratmamalarıdır.

Enterferans terimi, ilgili kanun ve sözleşmeye uygun olarak sağlanan her türlü haberleşme hizmetini engelleyen, haberleşmede kesinti doğuran veya kalitesini bozan her türlü yayın veya elektromanyetik etkiyi ifade etmektedir. En basit tanımıyla, dalgaların kesişmesine enterferans denir (MEGEP, 2011).

RF enterferansı yıldırım, güneş ışıması gibi doğal olaylardan insan yapımı RF yayıcılara kadar çok sayıda sebepten ötürü kaynaklanıyor olabilir. Bunların dışında RF enterferansına istemeden neden olan vericiler de bulunmaktadır. Bunlara örnek olarak mikrodalga fırınları, kablosuz telefonları, bluetooth cihazları, kablosuz video kameraları, mikrodalga hatları, kablosuz oyun joistikleri, floresan lambaları ve daha birçoklarını sayabiliriz.

Belli tipte bir RF iletişimi için kullanılacak frekans bandına karar verilirken, çok sayıda faktörde göze alınmalıdır. Seçilen frekans, çıkış gücü ve bant gibi parametreler, ilgili otoritelerin izin verdiği limit değerlerinin üzerinde olmamalıdır. Aksi durumda başka bir bölgede çalışan diğer kablosuz iletişim cihazlarını olumsuz etkileyecektir. Sinyallerin ulaşacağı mesafelerin büyük önemi vardır. Çünkü kıt kaynak olan RF spektrumunun verimli kullanılması zorunludur. Bu nedenlerle son yıllarda frekans spektrumunu daha verimli kullanan ve enterferanstan daha az etkilenen RF teknolojileri geliştirilmiştir (MEGEP, 2011).

2.2.2 Kızılötesi teknolojisi

Kızılötesi denildiğinde akla, belli bir dalga boyu aralığında ışık türü gelmektedir. Kızılötesi teknolojilerine kızılaltı, IR, enfraruj veya Infrared teknolojilerde denilebilir. Kızılötesi ışınım dalga boyu görünür ışıktan uzun, fakat terahertz ışınımından ve mikrodalgalardan daha kısa olan elektromanyetik ışınımdır. Kızılötesi ışınımın dalga boyu 0.760 µm ile 1000 µm arasında değişiklik gösterebilir (Ansiklopedi, 2013).

Kızılötesinin hayatlarımıza girişi cep telefonlarıyla başlamıştır. Cep telefonumuzdaki şarkıyı, fotoyu veya veriyi başka bir cep telefonuna aktarmak için cep telefonlarını yanyana sabit tutarak kızılötesi teknolojisini kullanırdık. Kızılötesinin gündelik yaşamdaki kullanım alanlarına örnek olarak ise televizyon kumandalarını göstere biliriz.

Kızılötesi teknolojisini kullanan iki donanımın sinyal alıcı kısımları arasında sinyali engelleyen hiçbir engelin olmaması ve aralarındaki uzaklık mesafesinin minimum olması bu teknolojinin en önemli unsurudur.

Kızılötesinin başka bir kullanım alanı ise gece görüşüdür. Genelde askeri amaçla kullanılmakta olan bu yöntem, kızılötesinin insanlar tarafından direk temasta görülememesi özelliğinden yararlanır. Kızılötesinin yaygın olarak kullanıldığı bir başka alan ise belli bir mesafedeki objelerin ya da canlıların ısısının belirlenmesidir. Normalde önemsiz bir bilgi gibi gözükse de bu bilginin kullanım alanı çok geniştir. Uydular bu yöntemle dünyanın belli bölgelerindeki sıcaklık dağılımlarını gözlemleyebilirler ve bu sayede meteorolojiye bilgi sağlayabilirler. Askeri alanda füzelerin kendi hedefini otomatik olarak takip etmesini sağlayan ısıya kilitlenen roketler de kızılötesi ısı ölçüm yöntemini kullanırlar (Ansiklopedi, 2013).

2.2.3 HomeRF teknolojisi

HomeRF evlerde, küçük işyerlerinde veya ofislerde bulunan bilgisayarların, telefonların ve diğer kablosuz cihazlar arasında iletişimi kablosuz şekilde sağlamak için tasarlanmıştır.

Home RF IEEE 802.11 gibi Frequency Hopping Spread Spectrum mekanizmasını kullanıyor. HomeRF'nin IEEE 802.11x standartlarına göre güçlü yanı veri aktarımının yanı sıra ses desteğinin de olmasıdır. Home RF sistemi 10 Mbit/sn'lik veri aktarım

hızına ulaşabiliyor, iletişimi hem peer to peer olarak hem de bir kontrol noktası (Control Point "CP") üzerinden kurmak mümkündür (Yılmaz ve Öztürk).

2.2.4 Bluetooth teknolojisi

Bluetooth teknolojisi, kısa mesafede yüksek hızda veri paylaşımı sağlar. Veri paylaşımı radyo dalgaları kullanılarak yapıldığından kızılötesinde olduğu gibi cihazların arasında veri aktarımını engelleyen başka cisimlerin olması veri aktarımını engellemez. Veri aktarımı yapabilen cihazlarda bluetooth desteği varsa birbirilerini tanıdıktan sonra belli bir alan içinde veri aktarımı yapabilirler. Günümüzde bluetooth'un kullanım alanı çok geniştir. Örneğin, bilgisayarlarımızın farelerini, klavyelerini kablo olmaksızın belli bir mesafeden kontrol ederken, cep telefonlarımızla veri paylaşımı yaparken veya cep telefonlarımız cebimizdeyken, kulağımıza taktığımız kulaklık-mikrofonla gelen aramalara cevap verirken bluetooth teknolojisini kullanabiliriz.

Bluetooth teknolojisinin temeli 1994 yılında hareketli cep telefonu üreticisi Ericsson'un, cep telefonları ve cep telefonu aksesuarları arasında kablosuz iletişim sağlayabilecek düşük güç tüketimli, düşük maliyetli bir radyo arabirimi üzerinde araştırma yapmaya karar vermesine dayanır. Bluetooth haberleşmesi, 2.4 GHz'de ve lisans gerektirmeyen ISM bandında (endüstriyel, bilimsel ve tıp uygulamalarına ayrılmış frekans bandı) gerçekleşmektedir. Maksimum veri akış hızı 1 Mbit / sn'dir (Ansiklopedi, 2013).

2.2.5 GSM (Global System for Mobile - Mobil İletişim için Küresel Sistem) teknolojisi

GSM, cep telefonları arasındaki iletişim protokolüdür. ETSI (European Telecommunications Standards Institute) kurumu tarafından tanımlanmıştır. Daha sonralar sistem küresel bir çapa ulaşmıştır. Kullanıcıların en çok kullandıkları özelliklerinden birisi aynı hat üzerinden sizden kilometrelerce uzaklıktaki değişik ülkelerle görüşme (roaming) yapabilmeleridir. GSM standartlarının hepsi hücresel ağ kullanırlar ve haraketlilik anında bile hücreler arası geçiş yapabiliyorlar. Bu özelliği sayesinde, eğer kapsama alanından çıkmazsak cep telefonu görüşmesi yaparak tüm dünyayı gezebiliriz.

GSM ortaya çıkmasından sonra zamanla yapılan değişiklikler için nesil ifadesi kullanılmıştır. Nesiller ve getirdikleri yeniliklere kısaca bakarsak;

- 0G: Analog veri iletimi.
- 1G: Analog veri iletimi, temel ses, faks, SMS, çağrı yönlendirme ve engelleme.
- 2G: Dijital veri iletimi, CDMA, ses kalitesi artırılması, ücretlendirme geliştirmeleri, çağrı bekletme, konferans çağrıları.
- 2.5G: GPRS (paket anahtarlamalı ağlara bağlanma), MMS, data hızı 114kb/s.
- 3G: Hızlı veri iletimi, mobil internet, video çağrı, mobil TV
- 4G: Yüksek ağ kapasitesi, LTE , UMB , WiMAX, HSPA+, WiMAX, IPv6 desteği, ip tabanlı sistemlerle entegrasyon, farklı ağ ve teknolojilere bağlanma desteği, video chat, IP Telefon servisi (Çamanlı, 2009).

2.2.6 GPRS (General Packet Radio Service - Genel Paket Radyo Servisi) teknolojisi

GPRS, haraketli haberleşme ürünlerinde yaşanan gelişmeler sonucunda GSM için yeni bir taşıyıcı hizmeti olarak geliştirilmiştir. GPRS, paket veri ağlarına kablosuz erişimi kolaylaştıran ve hızlandıran taşıyıcı hizmettir. Harici paket veri ağları ile haraketli istasyonlar arasında veri aktarımında radyo prensibini kullanır. Paket radyo prensibi iletim yöntemiyle çalıştığı için GSM'e göre oldukça hızlıdır ve transfer edilen veri miktarına göre ücretlendirildiğinden GSM'e göre oldukça ucuzdur. GSM bandında normal aktarım hızı 14.4 Kbps (Kilo bit Per Second - Saniyede Kilobayt) iken bu rakam GPRS'de 115 Kbps olarak gerçekleşebilir (Taşpınar ve diğerleri, 2002).

2.3 Kablosuz Ağların Sınıflandırılması

Kablosuz iletişim, evlerde kişisel bilgisayarlarda kullanıldığı gibi şehirlerde ya da ülkelerde binlerce iş istasyonlarında binlerce bilgisayarlar arasında da kullanılır. Oluşturulan bu kablosuz iletişimlerin kapsama alanlarına, kullanım amaçlarına ve yapılarına göre kablosuz ağların sınıflandırılması yapılmıştır (Şekil 2.1).

Şekil 2.1 Kablosuz ağların sınıflandırılması

2.3.1 Kablosuz Geniş Alan Ağları (WWAN - Wireless Wide Area Network)

Coğrafi olarak birbirilerinden uzak olan ülkeler arasında ya da birbirilerinden binlerce kilometre mesafelerde bulunan bilgisayarlar arasındaki iletişimin, uydu veya kablosuz iletişim yöntemleriyle kurulmasına Kablosuz Geniş Alan Ağları denir (Şekil 2.2). En kısa tanımıyla WWAN sistemi, oluşturulan Kablosuz Yerel Alan Ağları ve Kablosuz Metropol Alan Ağları uygulamalarının birleşmesi sayesinde oluşmaktadır. WWAN uygulamalarına örnek olarak interneti veya cep telefonu şebekelerini gösterebiliriz.

WWAN sistemlerinde trafik yükünün en önemli kısmı ses iletişimi ile ilgilidir. Fakat kablosuz ağlara olan ilginin artması beraberinde veri iletişimine ve internet iletişimine ihtiyacı da artırdı. WWAN uygulamaları GSM, GPRS ve 3G gibi teknolojileri kullanır (MEGEP, 2011).

Şekil 2.2 Kablosuz Geniş Alan Ağları (WWAN)

2.3.2 Kablosuz Metropol Alanı Ağları (WMAN - Wireless Metropoliten Area Network)

Bir anakent şehri kapsayacak şekilde oluşturulan ağlara veya birbirilerinden uzak yerlerde yapılandırılmış yerel bilgisayar ağlarının birbirleri ile uydu veya kablosuz iletişim yöntemleriyle bağlanarak oluşturulan ağlara Kablosuz Metropol Alan Ağları (WMAN) denilmektedir (Şekil 2.3). Kablosuz Metropol Alan Ağlarında da genellikle kiralık hatlar veya telefon hatları kullanılmaktadır.

WMAN'lar çok sayıda şubesi bulunan kurum ve büyük şirketler ile dağınık yerleşime sahip üniversiteler gibi yapılarda yaygın olarak kullanılmaktadır. Bu alanda, WiMAX adı altında uygulamalar yapılmaktadır. IEEE 802.16 standardı WMAN için geliştirilmektedir. IEEE 802.16 standardı, 2GHz-11GHz ve 10GHz-66GHz geniş bant frekans aralıklarında 120 Mbps veri hızlarına ulaşabilen uygulamaları kapsamaktadır (Yılmaz ve Öztürk).

Şekil 2.3 Kablosuz Metropol Alan Ağı (WMAN)

2.3.3 Kablosuz Yerel Alan Ağları (WLAN - Wireless Local Area Network)

Bina, ev, ofis, kampüs ya da halka açık alanlar gibi sınırlı alanlarda uydu veya kablosuz iletişim yöntemleriyle kurulan ağlara Kablosuz Yerel Alan Ağları (WLAN) denir (Şekil 2.4) . WLAN sistemleri kullanıcılara kablosuz geniş bant internet erişimi, sunucu üzerindeki uygulamalara ulaşım, aynı ağa bağlı kullanıcılar arasında elektronik posta hizmeti ve dosya paylaşımı gibi çeşitli imkanlar sağlamaktadır. Kablosuz LAN sistemlerinin mesafesi 25-100 metre civarındadır. Dünyada yaygın olarak kullanılan iki tür kablosuz LAN teknolojisi mevcuttur. Bunlardan birisi Amerika tabanlı IEEE 802.11x, diğeri ise Avrupa tabanlı HiperLAN sistemleridir (Dizdar, 2012).

Şekil 2.4 Kablosuz Yerel Alan Ağı (WLAN)

2.3.4 Kablosuz Kişisel Alan Ağları (WPAN - Wireless Personel Area Network)

Ev ya da küçük iş yerlerinde bulunan yakın mesafedeki elektronik cihazları, fare, klavye, cep telefonu, dizüstü bilgisayar vb. kablosuz olarak birbirine bağlayan ağlara Kablosuz Kişisel Alan Ağları (WPAN) denir (Şekil 2.5). Bu tür sistemler, diğer ağlara kıyasla daha düşük veri hızına ve daha kısa iletişim mesafesine sahiptirler. WPAN'ların hızları 1 Mbs ve ulaşım alanları yaklaşık kişiyi 10 metre uzaklığa kadar çevreleyen bir alandır. WPAN uygulamaları Bluetooth ve HomeRF gibi teknolojileri kullanır (Microsoft, tarih yok).

Şekil 2.5 Kablosuz Kişisel Alan Ağı (WPAN)

3 KABLOSUZ YEREL ALAN AĞI (WLAN)

3.1 Kablosuz Yerel Alan Ağlarının Avantajları

Kablosuz Yerel Alan Ağlarının Kablolu Yerel Alan Ağlarına karşı üstünlükleri sayesinde kullanıcılara sağladığı avantajlar incelenerek aşağıda sıralanmıştır.

3.1.1 Esneklik ve Genişletile bilirlik

Kablosuz Yerel Alan Ağ sistemlerinde kablosuz iletişim cihazlarının konumlarını yani yerlerini belirlemeye ve kablo çekmeye ihtiyaç yoktur. Çünkü kablosuz iletişim cihazlarının kapsama alanı içinde olması yeterlidir. Kullanıcı sayısının ve yerinin sabit olmadığı ortamlar için özellikle seyahat halindeki kişiler için Kablosuz Yerel Alan Ağ sistemleri oldukça elverişlidir. Çünkü iş seyahatinde veya normal seyahatte bulunan bir kişi hava alanında bekleme salonunda, otelde, restoranda veya alışveriş merkezinde erişim alanlarını kullanarak kablosuz internet hizmetinden yararlana bilir. Bu hizmetin kablolu sistemlerle yapılması çok zor hatta hemen hemen imkansızdır. Ayrıca, sisteme yeni kullanıcılar katıldığında genişletilmeye ihtiyaç duyulduğunda da ilave işçilik, malzeme ve kablo harcaması yapılması gerekmemektedir. Halbuki geleneksel kablolu ağlarda her katılan yeni kullanıcı için ayrı bir kablo çekilmesi gerekmektedir. Kablosuz erişim özelliğine sahip cihazlar sisteme kolaylıkla ilave edilebilir veya çıkarılabilir (Kadakoğlu, 2010).

3.1.2 Hızlı ve Kolay kurulum

Kablosuz Yerel Alan Ağ sistemleri kablo çekmenin pahalı, zor ve bazen de imkansız olduğu ortamlarda devreye girerek kolay ve düşük maliyetli iletişim imkanı sağlamaktadır. Örneğin kablo çekilmek istenen iki nokta arasında bir nehir, otoyol veya demir yolu bulunuyorsa kablo çekmek hem çok zor hem de çok maliyetli olur. Kablo çekilse bile o kablonun korunması ayrı bir sorun yaratmaktadır. Dağınık yapıya sahip şirketlerin bina içi kullanımında ise Kablosuz Yerel Alan Ağ sistemlerinin

kurulumu oldukça hızlı ve kolaydır. Çünkü duvar ve tavanlardan kablo çekmeden, sadece AP'lerin monte edilmesi sistemi kurmak için yeterlidir.

Tarihi yapılarda özellikle toplantı ve kongre amaçlı kullanılan tarihi binalarda kablo döşenmesine izin verilmiyor. Çünkü bu binalarda kablo çekilerek zarar görmesine ve görüntü bozulmasına izin verilmemektedir. Bu tarihi binalarda iletişim hizmetlerini karşılamak için Kablosuz Yerel Alan Ağ sistemlerinin kullanılması hızlı, kolay ve düşük maliyetli bir çözümdür (Kadakoğlu, 2010).

3.1.3 Mobil iletişim

Mobil iletişim cep telefonlarıyla kurulan iletişimdir. Hareket halinde olmayı gerektiren bazı işlerde mobil iletişiminin olması sağladığı kolaylıklarında ötesinde zorunluluk haline gelmiştir. Örneğin hastanelerdeki doktorların ve hemşirelerin hasta bilgilerine anında ulaşabilmeleri için, ambar, depo, yükleme, boşaltma ve fiyatlandırma çalışanlarının merkezi veri tabanıyla bilgi alış verişi yapmaları için büyük bir rahatlık ve konfor sağlamaktadır. Yine üniversiteler, kurumlar, büyük şirketler ve konferans salonlarında mobil iletişiminin sağlanması iletişim açısından büyük bir kolaylık ve rahatlık sunmaktadır. Günlük hayatımızda da müstakil evlerimizin her yerinden hatta evlerimizin bahçelerinden bile kablosuz internet erişiminden yararlanarak mobil iletişim kurmak bize büyük bir rahatlık ve konfor sağlamaktadır.

3.1.4 Maliyet kazancı

Kablosuz ağların maliyeti, kurulacak sisteme ve kapsayacağı alana göre değişse bile genellikle kablolu ağlardan daha düşük maliyetlidir. Çünkü kablolama işçiliği ücreti ve kablo maliyeti masrafları yoktur. Ayrıca kablo ve konektörlerine potansiyel arıza kaynağı olması düşünüldüğünde, kablosuz ağ sistemlerinin arıza ve bakım giderleri kablolu ağ sistemlerine oranla daha düşüktür. Ağ idaresi açısından bakım maliyetlerinin düşüklüğü ve ağdaki bilgisayarların masrafsız ve kolayca kapsama alanı içinde yer değiştirmesini sağlaması kablosuz ağların maliyetini en az düzeye indirmektedir.

3.2 Kablosuz Yerel Alan Ağlarının Dezavantajları

Kablosuz Yerel Alan Ağ sistemlerinin avantajlarının yanı sıra bazı dezavantajları da mevcuttur. Başlangıçta olan sorunlardan ürün çeşitliliği, standartlaşma, maliyet ve

frekans tahsisi gibi konular zamanla nispeten hal olmuştur. Ancak aşağıda belirtilen sorunlar halen kullanıcılar için dezavantaj olarak durmaktadır.

3.2.1 Güvenlik

Kablosuz sistemler kullanıcılara büyük avantajlar sunarken güvenlik açısından ise dezavantajlar yaratmaktadır. Çünkü havada serbestçe yayılan RF ışınlarının dinlenmesini önlemek, kötü niyetli saldırıları engellemek ve izinsiz kullanımların karşısının alınması için güvenlik sistemine ihtiyaç duyulmaktadır. Yapılan araştırmalara sayesinde bulunan çözümlere rağmen güvenlik tam şekilde sağlanamamaktadır. Fakat son yıllarda geliştirilen güvenlik sistemleri, kablolu ağlardakine eşdeğer bir güvenlik vaat etmektedir (Kadakoğlu, 2010).

3.2.2 Enterferans

Kablosuz çalışma mantığı genellikle enterferansa açıktır fakat özel frekanslar kullanan sistemlerin enterferansa uğrama olasılığı daha azdır. Ayrıca frekanslar enterferansa maruz kaldığında ilgili kurum tarafından sebebi tespit edilerek giderilir. WLAN sistemlerinde çoğunlukla ISM frekans bandı kullanılır ve kullanım şartlarına göre enterferansa uğramaktan şikayet etme hakları da yoktur. WLAN sistemlerinin enterferansa uğramalarına sebep bulundukları bölgeye göre çalışan sistemlerin artması, yakın noktalara AP'lerin kurulması, bölgede başka kablosuz sistemlerin olması ya da bölgedeki WLAN sistemleri olabilir.

3.2.3 Mesafe

WLAN Sistemlerinin bir diğer dezavantajı ise kapsama alanı yani iletişim mesafesinin kısıtlı olmasıdır. WLAN sistemlerinin kapalı alanlarda mesafesi 100 m civarındadır. Açık alanlarda ise bu mesafe 300 m civarına kadar yükselmektedir. Buna sebep kullanılan frekans bandı ve standartların müsaade ettiği kısıtlı çıkış gücüdür. Ayrıca ev ortamlarında duvar ve mobilya gibi fiziksel engellerin fazla olması durumunda mesafe 10 metreye kadar da düşebilmektedir (Kadakoğlu, 2010). WLAN sistemlerinde kesintisiz ve başarılı bir iletişim kurmak için AP'leri uygun yerlere ve yeterli sayıda yerleştirmek lazımdır. Örnek olarak İstanbul İstiklal Caddesinde Cadde boyunca her 30 m aralıklarla konulan 29 adet AP'i göstere biliriz. Daha küçük alanlarda ise bir tane AP'nin yettiği de görülmektedir (Uzun, 2006).

3.3 IEEE 802.11 Çalışma Modları

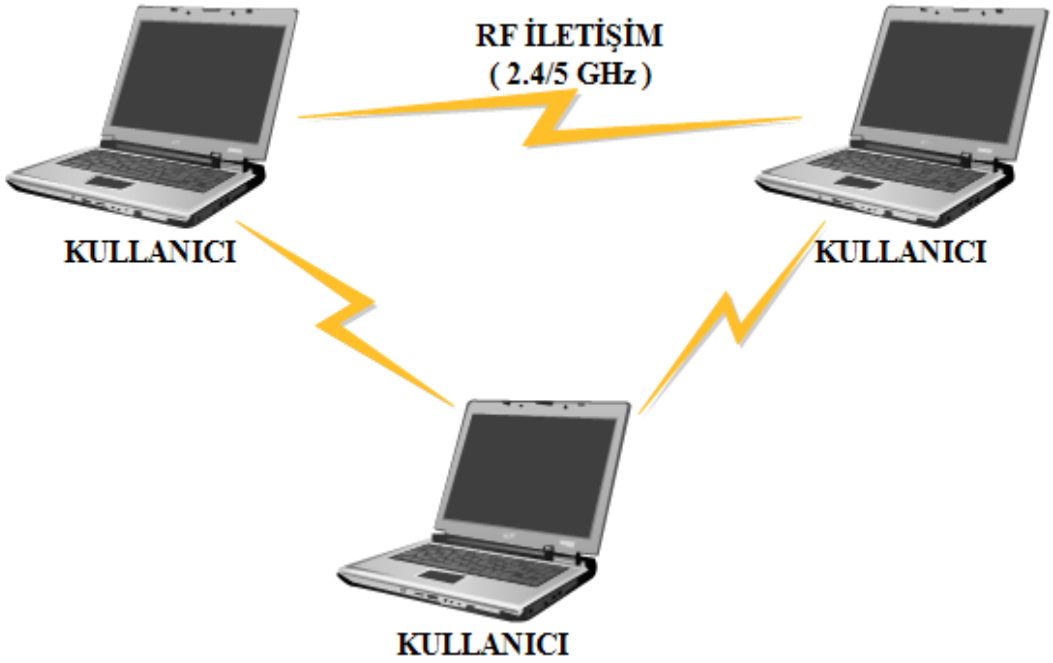
IEEE 802.11 kablosuz yerel alan ağlarında iki farklı çalışma modu bulunmaktadır (BİDB, 2013)

3.3.1 Cihazdan cihaza çalışma (Ad Hoc) modeli

Cihazdan cihaza çalışma modeli iki veya daha fazla kablosuz iletişim özelliği olan bilgisayarların birbirilerine arada sunucu olmadan direkt bağlandıkları ağ yapılarıdır (Şekil 3.1). Bu model, yapı olarak hızlı kurulması ve kablo veya Access Point (AP) gibi herhangi bir altyapıya ihtiyaç duymaması kolaylık ve maliyet bakımından avantajlıdır. Bu yapıda bilgisayarların birbirine bağlanıp veri paylaşımı yapa bilmeleri için sadece kablosuz iletişim özelliğinin olması yeterlidir.

Bu tür ağlarda bulunan bilgisayarların programlarına, veri veya dosya kaynaklarına ağdaki diğer bilgisayarlar tarafından da erişile bilinmesi güvenlik açısından dezavantajlıdır. Bunun yanı sıra bu modelde ilişki kuran bilgisayarlar arasındaki mesafe kısıtlıdır (MEGEP, 2011). Yani bu model, birbirleri ile iletişim mesafesinde olan bilgisayarlar için tasarlanmıştır. Eğer bir kullanıcı kapsama alanından dışarıya çıkıp da iletişim kurmak isterse, onunla iletişim kurmak istediği kullanıcı arasında başka bir kullanıcı yönlendirici olarak görev yapmalıdır.

Cihazdan cihaza çalışma modeli yapısal ve yapısal olmayan sistemler olarak ikiye ayrılırlar. Yapısal sistemlerde kurulan ağ yapıları belli bir protokolle kurulur. Bu protokol sayesinde toplam bilgiler mantıklı bir sıralamayla sıralanır. Bu sıralama sayesinde kullanıcılar istedikleri bilgilere hızlı ve rahat bir şekilde ulaşırlar. Yapısal olmayan sistemlerde ise mantıklı bir sıralama yoktur. Kullanıcı istediği bilgiye ulaşmak için ağdaki diğer üyeleri teker teker gezmelidir. Buda kullanıcıların istedikleri bilgilere ulaşırken zaman kaybına ve her kişisel kullanıcıdan dolayı çok fazla sinyal dolaşımına sebep olur.

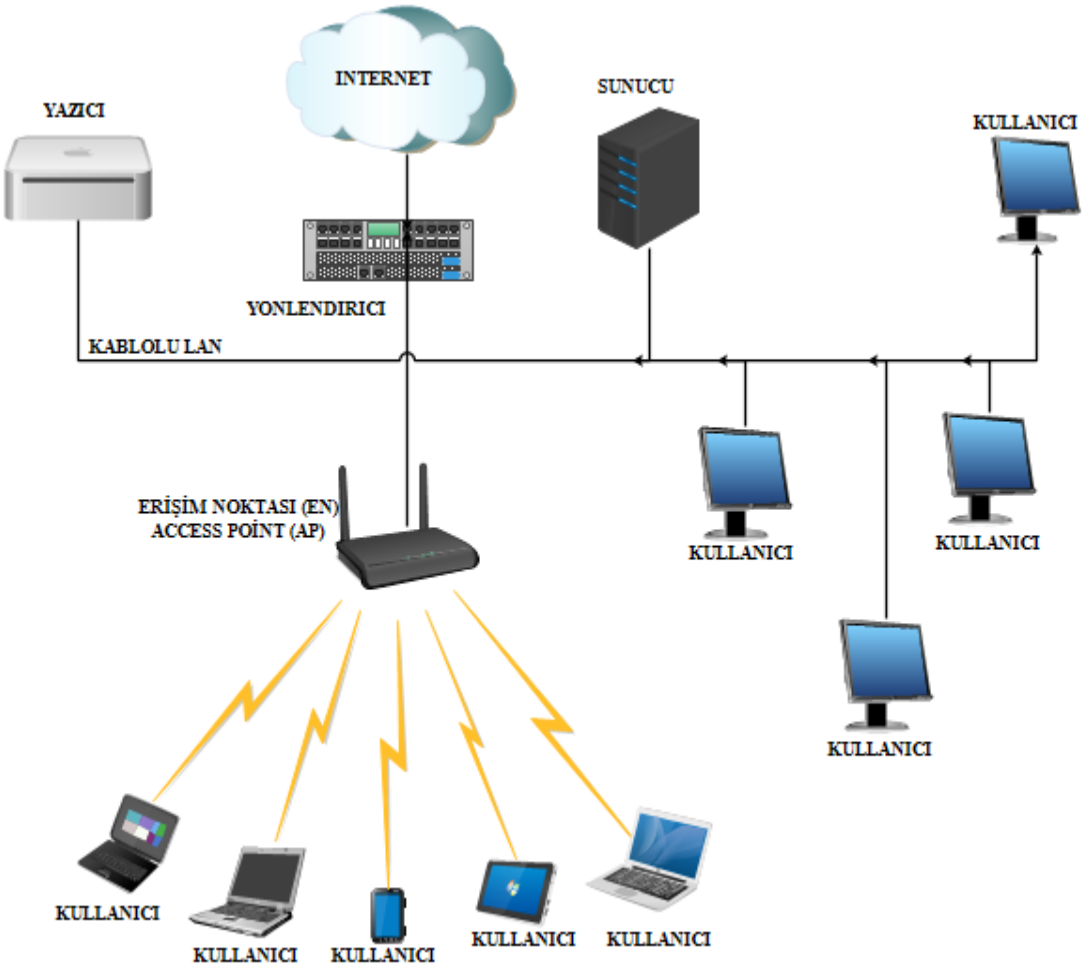


Şekil 3.1 Cihazdan Cihaza Çalışma (Ad Hoc) modeli

3.3.2 Altyapı çalışma (Infrastructure, Client/Server) modeli

Altyapı çalışma modeli kablolu ağa bağlı bir erişim noktası (EN) ve EN'a bağlı istenilen sayıda kablosuz iletişim özelliğine sahip cihazlardan oluşur (Şekil 3.2). Altyapı çalışma modeli ortamında bulunan tüm kablosuz iletişim cihazları EN sayesinde kablosuz olarak internete ve mevcut kablolu ağa bağlanabilirler. Kablolu ağa genellikle sunucu bilgisayarlar ve AP'ler ihtiyaca göre ise yazıcılarda takılabilir. Bu tür temel altyapı çalışma modeli, ev ve küçük iş yerleri için yeterli olacaktır.

Altyapı çalışma modelinde paylaşılan tüm kaynaklar sunucuda saklanır ve isteğe uygun işlemler sunucudan yapılır. Yani kullanıcı erişmek istediği bilgiyi ararken gidip de teker teker ağdaki diğer kullanıcılarda aramaz direkt sunucudan ister ve sunucuda işlemleri hızlı bir şekilde yaparak kullanıcıya yollar. Sonuç olarak işlem hızı ve kapasitesi artırılmış olur. Altyapı çalışma modelinde iletişim kuracak kullanıcı sayısının veya iletişim kapsama alanının artırılması istenen durumlarda sisteme yeni AP'ler ilave edilebilir. AP'lerin sayısı ve montaj yerleri istenilen veri iletişim hızına, kullanıcı sayısına, iletişim alanının kapasitesine ve bunun gibi ölçütlere esasen belirlenir (Kurtuluş, 2011). Örneğin, üniversitenin toplantı salonunda yoğun internet kullanımını karşılamak için ikinci veya üçüncü AP sistemleri ilave edilebilir.



Şekil 3.2 Altyapı Çalışma (Infrastructure, Client/Server) modeli

3.4 Kablosuz Yerel Alan Ağ Standartları

Kablosuz iletişim özelliğine sahip cihazlarının gelişiminin yanı sıra kablosuz yerel alan ağ (WLAN) standartlarında da gelişmeler yaşandı. İlk yıllarda her üretici kendine uygun standart geliştiriyordu. Bu da aynı ortamda birbiriyle uyumsuz birçok bilgisayar ağının oluşmasına neden oluyordu. Bu amaçla WLAN için uluslararası standartlar geliştirilmiştir. WLAN standartlarını tüm öğrenicilerin uyması gereken üniversite kurallarına ya da trafik kurallarına benzete biliriz. Trafik kuralları araçların yolu hangi hızla, nasıl ve neresinden geçmeleri gerektiğini netleştirdiği gibi, WLAN standartları da verilerin nerden, nasıl ve ne kadar hızla gidebileceklerini belirler.

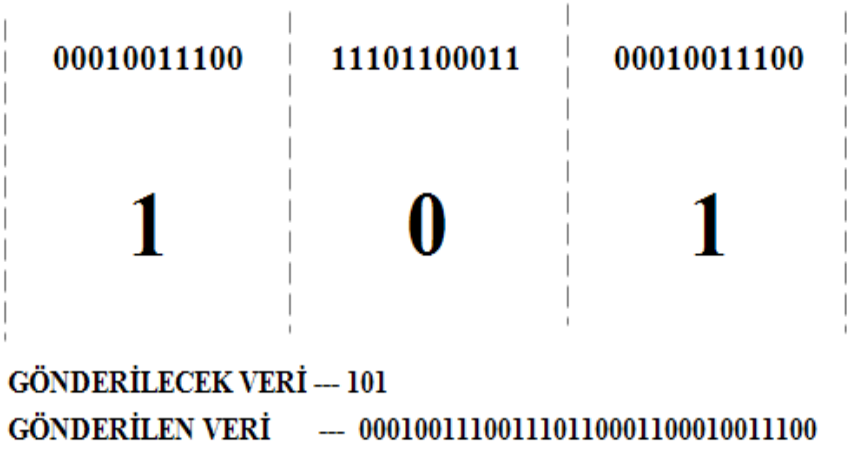
Bu standartlara örnek olarak IEEE'nin (Institute of Electrical and Electronics Engineers - Elektrik Elektronik Mühendisleri Enstitüsü) geliştirdiği 802.11x (x bir harfi temsil etmektedir) adı ile tanımlanmış standartlar ve ETSI (The Eureopean

Telecommunication standards Institute) tarafından tanımlanan HiperLAN1 ve HiperLAN2 standartları gösterilebilir (MEGEP, 2007). Bu standartlar farklı şekilde, farklı alanlarda kullanılmaktadır.

3.4.1 IEEE 802.11 standardı

IEEE 802.11 standartları 1997 yılından başlayarak IEEE tarafından geliştirilmeye başlandı. 802.11 standartları WLAN üzerinden iletişim kurarken kullanılan kuralları temsil eder (BİDB, 2013). Bu temel standartla 2 Mbps'e kadar veri iletişim hızı sağlanmaktadır. IEEE 802.11 standarttın da FHSS (Frenquency Hopping Spread Spectrum-Frekans Atlamalı Yaygın Spektrum) veya DSSS (Direct Sequence Spread Spectrum– Düzgün Sıralı Yaygın Spektrum) teknikleri kullanılıyor.

Düzgün Sıralı Yaygın Spektrum tekniğinde gönderilmek istenen veri uygun değişik frekanslarda küçük paketler halinde gönderilir (Şekil 3.3). Yani gönderilmek istenen veri, özel kodlama yöntemi kullanılarak çok daha geniş frekans bandında dağıtılır. Alıcıda gönderilen verinin anlamlı olarak elde edilmesi için vericide kullanılan kodlama yöntemini kullanır ve veriyi anlamlı bir şekilde elde eder (Köksal, 2007).



Şekil 3.3 DSSS tekniğinde verinin kodlanması

Frekans atlamalı yaygın spektrum tekniğinde ise gönderilecek veriler farklı frekanslarda kısa fakat büyük paketler şeklinde tekrarlanan bir çerçevede gönderilir. Verici veriyi yollayacağı frekans kanalına, frekans değişimini belirleyen bir parametre

kodu seçerek karar verir. Frekans değişimini belirleyen bu kod alıcıya da gönderilir ve alıcı da bu koda göre ayarlanır. Sonuç olarak alıcı doğru frekanstan doğru veriyi almaya hazır duruma gelir.

Zamanla bilgisayar dünyasında yaşanan gelişimler sonucunda 2,4 GHz frekansı, maksimum 75 metre kapsama alan ve 1-2 Mbps aralığında veri iletimi hızı sunan bu standart yetersiz kalmaya başladı. Bu sebepten IEEE, daha iyi frekanslar, daha fazla kapsama alanı, daha yüksek veri iletim hızı vb. ihtiyaçları karşılamak adına 802.11x adı altında bir dizi standart geliştirmeye başlamıştır (Köksal, 2007). Arada bir takım farklar olsa bile 802.11 ailesi temel olarak aynı kuralları kullanırlar.

3.4.2 IEEE 802.11a standardı

802.11a standardı piyasaya 1999 senesinde sürülmüştür. Bu standart 5 GHz'lik bant genişliğini, saniyede 6, 9, 12, 18, 36, 48, 54 Mbps veri iletim hızını ve maksimum 100 metreye kadar kapsama alanını destekler. Yapılan bu değişikliklerin ana amacı sinyal karışıklığının karşısını almaktı. Çünkü kablosuz ev cihazlarından polis telsizlerine kadar birçok cihaz aynı frekans bandını kullandığından sinyal sorunlarıyla sık sık karşılaşılıyordu. Bu sorunu önlemek için 802.11a standardı OFDM (Orthogonal Frequency Division Multiplexing – Ortogonal Frekans Bölümlemeli Çoğullama) tekniğini kullanır.

Ortogonal frekans bölümlemeli çoğullama tekniği veri transferi yaparken radyo sinyalini daha küçük alt sinyallere bölür ve aynı anda farklı frekanslarda alıcıya gönderir. OFDM sinyal iletiminde meydana gelen çapraz karışmayı azaltan ve çoklu yol gecikme yayılmasına ve kanal gürültüsüne tolerans tanıyan bir yöntemdir (Baş, 2014).

802.11a standardında 5 GHz'lik bant genişliği kullanıldığından bu standarda uyumlu ekipmanlar bulmak gittikçe zorlaşmaktaydı ve üstelik maliyet olarak da pahalıya mal oluyordu. Bu standardı yüksek veri iletim hızına ihtiyaç duyan kullanıcılar tarafından veya video dağılım sistemlerinde daha fazla kullanılıyor. İş hayatında da daha çok kurumsal kullanıcılar tarafından tercih edilmektedir (MEGEP, 2011).

3.4.3 IEEE 802.11b standardı

802.11b standardı 802.11a ile aynı tarihlerde yayınlanmıştır. Kullanıcılar arasında 802.11b standardı 802.11a standardıyla kıyasla daha çok kabul görmüştür. IEEE

802.11b standardı 2.5 GHz bant genişliğini, saniyede 1, 2, 5.5, 11 Mbps veri iletim hızını ve yaklaşık olarak kapalı alanlarda 38 metre, açık alanlarda ise 150 metreyi aşacak şekilde kapsama alanını destekler. 802.11b standardı DSSS modülasyon tekniğini kullanır (MEGEP, 2011).

IEEE 802.11b standardının 2.4 GHz banda işleyebilmesinin ana konusu Bluetooth, HomeRF ve Mikrodalga gibi teknolojiler tarafından kullanıla bilinmesidir (MEGEP, 2007). 802.11b standardı kablo çekmenin tehlikeli olduğu alanlarda, hastanelerde, depolarda, fabrikalarda, ofis ortamlarında, konferans salonlarında kısacası taşınabilirliği gerektiren ve orta hızlı ağ bağlantısı yetecek ortamlarda kullanılması için uygundur.

3.4.4 IEEE 802.11g standardı

802.11g standardı IEEE tarafından 2003 yılında geliştirilmiştir. Bu standart temel olarak 802.11b standardının bir uzantısı olmasına rağmen veri iletim hızı ve bant genişliği bakımından önemli gelişmeler sağlanmıştır. Veri iletim hızı olarak 802.11a'da olduğu gibi maksimum 54 Mbps'a ulaşabilmektedir. Kapsama alanı olarak ise 802.11b'nin aynısıdır. 802.11a da olduğu gibi bu standartta da modülasyon tekniği olarak OFDM kullanılmıştır. Sonuç olarak 802.11g standardının 802.11a ve 802.11b'nin en etkin özelliklerinin toplanmış hali olduğu söylenebilir (Soylu, 2011).

Bu standardın fiyatının 802.11b'den yüksek olması ve zaman zaman 802.11b ile çalışan eski cihazlarda uyumsuzluk yaşaması kullanımlığını azaltmıştır.

3.4.5 IEEE 802.11h standardı

Avrupa telsiz düzenlemelerine göre 5 GHz frekans bandında kullanılacak WLAN ürünlerinde TPC (Transmission Power Control) ve DFS (Dynamic Frequency Selection) özelliği bulunması zorunludur. 2002'de yayınlanan bu standart ile Avrupa'da geçerli 5 GHz WLAN düzenlemelerine uygunluk sağlamak için 802.11a standardına ek olarak MAC katmanına ilaveler yapılmıştır (Soylu, 2011).

3.4.6 IEEE 802.11n standardı

802.11n standardı IEEE tarafından 2009 yılında geliştirilmiştir. 802.11n standardı hem 2.4 GHz hem de 5 GHz frekansında haberleşebilmeyi, ortalama 130 Mbps seviyelerinde ve teorik olarak 600 Mbps'ye kadar ulaşabilir bir veri iletim hızını ve

kapalı alanlarda 70 metre, açık alanlarda ise 250 metre kadar kapsama alanını destekler. Bu özellikler sayesinde 802.11n standardı, 802.11a, b, g standartları ile üretilmiş cihazlarda çalışabilmektedir (Soylu, 2011).

802.11n standardının önemli özelliklerinden biride modülasyon tekniği olarak MIMO (Multiple Input Multiple Output–Çoklu Giriş Çoklu Çıkış) teknolojisini kullanmasıdır. Çoklu giriş çoklu çıkış teknolojisinin amacı bir veriyi parçalara ayırarak farklı antenler üzerinden alıcıya göndermektir (MEGEP, 2011). Gönderilen bu veriler duvarlardan ve diğer eşyalardan yansıyarak farklı rotalarda, farklı zamanlarda ve bir defadan fazla kere alıcı antenine varır. 802.11a/b/g standartlarında kullanılan teknolojilerde ise bu kontrolsüz parçalanma durumu alıcı anteninde karışıklığa neden oluyordu ve bu karışıklık sinyalin tekrar bir araya gelmesini zorlaştırarak, yayın performansını azaltıyordu. Fakat MIMO teknolojisiyle bu durum, 802.11n standardının lehine kullanılarak sinyalin güçlenmesi ve daha uzaklara iletilmesi sağlandı. Sonuç olarak MIMO birden fazla anten kullanarak iletişimin sağlandığı teknolojiye verilen isimdir.

3.4.7 IEEE 802.11c standardı

802.11c standardının amacı EN'ları arasında köprüleme yapmaktır. Yani bir ya da daha fazla ağ bağlantılarını yazılım veya donanımsal olarak birbirilerine bağlayarak iletişim sağlamaktır. Bir kablosuz ağ bağlantısını kablolu ağ bağlantısıyla, iki kablolu veya iki kablosuz ağ bağlantılarını köprüleyerek bulunan kullanıcıların birbirileriyle iletişim kurmalarını sağlar. Bir kullanıcı bilgisayarındaki interneti Wi-Fi üzerinden paylaşmak istediğinde köprüleme yaparak rahatça etrafındaki insanların ağa bağlanmasını sağlayabilir. Şirketler, üniversiteler ve oteller ağlarını genişletmek adına bu standardı sıklıkla kullanırlar.

3.4.8 IEEE 802.11d standardı

802.11d standardının amacı kurallar koymak ve bu kurallar dahilinde WLAN uygulamalarını gerçekleştirmektir. Yani amaç, üretici firmaların ürünlerini bu standart kurallarına uygun olarak üreterek farklı ülkelerde farklılık gösteren kablosuz ağ uygulamalarının birbirileriyle uyumlu olmalarını sağlamaktır. Özet olarak 802.11d standardı 802.11 standartlarının yaygınlaşması ve kabul görmesi ile ilgilenmektedir (Karygiannis ve Owens, 2002).

3.4.9 IEEE 802.11e standardı

802.11e standardı bütün 802.11 standartları için veri, ses ve görüntü iletişiminde servis kalitesini (QoS – Quality of Service) geliştirir ve artırır. MAC katmanında çalışan bir standart olmasına rağmen fiziksel katmanda çalışan standartlara destek verir (Karygiannis ve Owens, 2002).

3.4.10 IEEE 802.11f standardı

Bu standardın ana görevi değişik üreticiler tarafından üretilen erişim noktalarının arasındaki uyumluluğu inceleyip çözümlemektedir. Böylelikle kullanıcılar ağ içindeki farklı AP'leri kullanabilmektedir (Karygiannis ve Owens, 2002).

3.4.11 IEEE 802.11i standardı

Bu standart, MAC katmanında çalışır ve 802.11 standartları için güvenlik ve kimlik denetleme mekanizmaları geliştirir (Köksal, 2007).

3.4.12 HiperLAN (High Performance Radio LAN-Yüksek Performanslı Radyo Yerel Ağı)

HiperLAN, ETSI (Europan Telecominications Standarts Institute) tarafından tanımlanmıştır. HiperLAN OFDM modülasyon yöntemini kullanan ve 5 GHz bandında çalışan kablosuz LAN standardıdır. HiperLAN1 ve HiperLAN2 olmak üzere iki tipi vardır. HiperLAN1 20 Mbps'lik bir iletim hızına ulaşırken HiperLAN2 yine aynı frekans bandında 54 Mbps'lik veri iletim hızına erişmektedir.

HiperLAN2 802.11a standardı gibi 54 Mbps'lik veri iletimini 5 GHz'lik bant genişliği kullanarak sağlar. HiperLAN2, Avrupa da yaygın olarak kullanılan bir standarttır.

Hem 802.11b hem de HiperLAN2 yüksek veri hızlarına ulaşmak için OFDM teknolojisini kullanır. HiperLAN2 ağında erişim noktalarından uç sistemlere bağlantıya yönelik bir yaklaşım vardır. Böylece, 802.11 kablosuz LAN uygulamalarının aksine ses ve görüntü aktarımı için gerekli trafik türü desteklenmektedir (Bayraktar, 2005).

4 KABLOSUZ YEREL ALAN AĞLARINDA GÜVENLİK VE SALDIRI YÖNTEMLERİ

Günümüzde artık, bankalarda, mağazalarda, kamu kurumlarında, şirketlerde, hastanelerde hemen hemen her alanda kablosuz ağların kullanımının artması beraberinde kablosuz ağ güvenlik problemlerini doğurmuştur. Güvenlik problemlerini önlemek için çalışmaları hızlandıkça kötü niyetli saldırganlar da saldırı yöntemleri üzerinde çalışmaları hızlandırıyorlar. Bu yüzden daima kablosuz ağımızın güvenliğini kontrol etmeliyiz. Piyasa da ücretli ve ücretsiz bir sürü kablosuz ağlarını zayıflıklarını bulan programlar mevcuttur. Bazıları açıkları bulup çözümler bile öneriyor veya otomatik kendisi açıkları kapatıyor.

Çoğunlukla ev kullanıcıları güvenliğe dikkat etmezler çünkü onlar biz sadece web'te geziniyoruz ve önemli bir işlem yapmıyoruz ki, bize sıkı güvenlik önlemleri gereksin diye düşünürler. Ama bu tamamen yanlış düşüncedir çünkü dışarıdan ağınıza bağlanan kişi artık sizinle aynı haklara sahip olurlar ve ağınızda paylaştığınız her şeye erişebilir, tüm ağ trafiğinizi kaydedip izleyebilir ve illegal işler için kullanabilir.

Kablosuz ağlarda alınabilecek güvenlik önlemlerine geçmeden önce güvenliğin zayıf olması durumlarında ortaya çıkabilecek sorunlara ve risklere kısaca değinilecektir ki, kablosuz ağlarda güvenliğin ne kadar önemli olduğu daha da iyi anlaşılsın.

4.1 Kablosuz Ağların Güvenlik Riskleri

4.1.1 Trafiğin dinlenip verinin çözülmesi

Kablosuz ağlarda iletişimi sağlayan Erişim Noktaları bir hub gibi davranarak, paylaşılan veriyi radyo dalgaları aracılığıyla korumasız hava ortamına gönderirler ve bu veri trafiği ortamdaki diğer kablosuz cihazlar tarafından dinlenip kaydedilebilir. Veri paylaşımında kullanılan şifreleme algoritmalarının zayıf olmaları durumunda kötü niyetli saldırganlar şifrelemenin açıklarını kullanarak veri paketlerini çözebilirler. Bu çözülen paketler sayesinde yazışmalar, parolalar, epostalar, internette sörf yapan kişilerin kişisel bilgileri veya ilgi alanları gibi bilgiler açığa çıkabilir (MEGEP, 2013).

4.1.2 Ağın erişim noktası gibi kullanılması.

Kablosuz ağınıza bağlı olan saldırganlar ortama sahte erişim noktaları ekleyebilirler ya da kendi kablosuz ağ cihazlarını bazı işlemlerle bir erişim noktasına dönüştürebilirler. Kendisini erişim noktasına dönüştüren saldırganlar kablosuz ağın kaynaklarını ya kendileri kullanır ya da yetkisiz kişilerle paylaşarak kullanabilirler. Bu yüzden ağımıza bağlanacak yetkili kullanıcıları bile düzgün bir şekilde konfigürasyon etmemiz gerekir yoksa istenilmeyen kişilerin bağlantı kurmasına sebep olunabilir.

4.1.3 Ağ topolojisinin ortaya çıkması.

Kablosuz ağda şifrelemenin kırılması durumunda iç ağ ile yapılan veri paylaşımı trafiğinin izlenip incelenmesi ile kurumların iç ağ topolojisi ortaya çıkarılabilir. Saldırganların kurumların kablolu ağlarına yaptıkları saldırılarda en önemli etkenlerden biri kurumun ağ topolojisini ortaya çıkarmalarıdır (Özdemir, 2008).

4.1.4 IP'nin illegal işlerde kullanılması

Kablosuz ağınıza erişen saldırganın yaptığı her yasa dışı işlem sizin ağınızdan yapıldığı için suçlu duruma siz düşersiniz. Polisler kapınıza banka dolandırıcılığından, terör işlerine karışmaktan, porno yayımı ve spam yaymak gibi bazı kanunsuz işler yapmaktan dolayı geldiğinde, haberimiz yok deseniz bile suç ağı olarak sizin ağınız tespit edilmiştir denilecektir.

4.1.5 Veri kaybı ve veri kullanması

Elektronik ortamlarda saklanılan verilerin erişilemez veya kullanılamaz hale getirilmesine veri kaybı denilmektedir. Saldırganlar, ağdaki bilgisayarlar üzerinde saklanan veya yedeklenen verileri ele geçirebilirler ya da ağı gizlice izleyerek gönderilen bilgi paketlerini değiştirebilirler. Örneğin, üniversitelerin sistemlerine izinsiz giriş yapabilen bir saldırgan öğrencinin geçersiz notunu geçerli bir nota çevirebilir.

4.1.6 Hizmet aksatılması

Kişisel veya işletmelerdeki kullanıcıların ağ iletişimi zamanı kullandıkları kullanıcı adı ve şifrelerini kullanamamasına ya da kullanıcıların web hizmetine bağlanamamasına hizmet aksatılması denilmektedir. Hizmet aksatılması dışarıdan ağımıza bağlı olan saldırganlar tarafından yapılabilir.

4.2 Mevcut Güvenlik Yöntemleri

Elinde kablosuz iletişim özellikli cihazı olan herkes bir bilgisi olmasa bile kapsama alanındaysa ağınızla bağlantı kurup kullanabilecektir. Çünkü kablosuz ağ ekipmanların başlangıç ayarları müsait erişim noktalarına hiç bir ayar gerektirmeden bağlanabilecek şekilde ayarlanmıştır. Ağımıza rastgele birisinin bağlanmaması için mevcut güvenlik yöntemlerini kullanarak kablosuz ağımızın güvenliğini artırmalıyız.

Güvenli bir kablosuz ağ ortamı kurmak için başlıca şartlar; giriş kontrolü yapmak, kullanıcının kişisel gizliliğini ve veri bütünlüğünü korumak, iyi bilinen saldırılara karşı ağı korumaktır. Bu şartları sağlayan kablosuz ağ ortamında tabii ki de aşağıdaki fonksiyonları uygulayan ağ teknolojileri olmalıdır.

- Kimlik denetimi (Authentication)
- Yetki (Authorization)
- Gizlilik (Confidentiality)
- Giriş kontrollü paket akışı (Overall Framework)
- Bilgi bütünlüğü (Data Integrity)
- Anahtarlama yönetimi (Key Management)
- İyi bilinen saldırılara karşı koruma (Protection Against Well Known Attacks)

Bu güvenlik başlıkları çerçevesinde çeşitli şifreleme algoritmaları geliştirilmiş, zamanla yetersiz kalan algoritmaların yerini daha kuvvetli algoritmalar almıştır (Reisoğlu, 2008).

4.2.1 Başlangıç ayarlarını değiştirmek

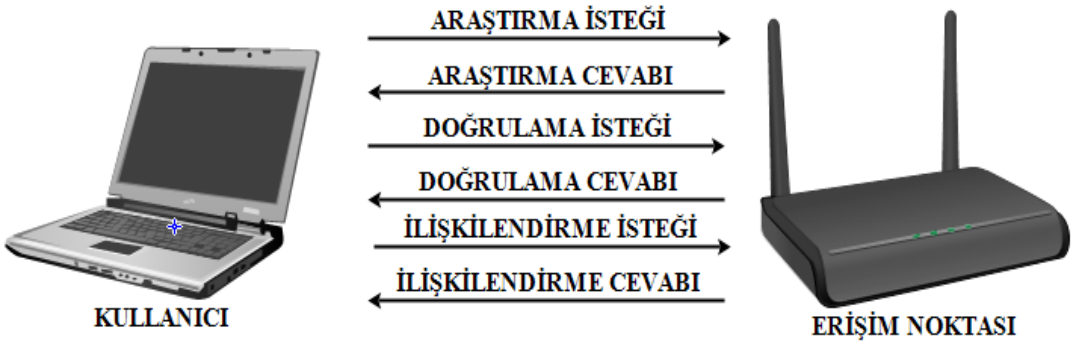
Kablosuz ağlarımıza kapsama alanındaki herkesin erişebilmemesi için ilk yapmamız gereken modemimizin varsayılan başlangıç kullanıcı adını ve admin şifresini değiştirmektir. Çünkü genel olarak kablosuz ağımızın Servis Seti Tanımlayıcısı (SSID) varsayılan olarak üreticiler tarafından verilen erişim noktasının ya da Kablosuz ADSL Router in modeli gibi bir değerdir. Bu konuda biraz tecrübesi olan birisi ağımızın SSID'sini gördüğünde modemin modelini hemen anlar ve o model modemin varsayılan admin şifresini bulup modeminize bağlanarak modeminizi yönetir. Otomatikman bu sorunu çözmek için SSID'yi değiştirmek şarttır. SSID'ye değer verirken telefon numaranızı veya şahsi bir bilginizi vermeyiniz uzmanlar tarafından tavsiye olunmuyor. Çünkü kablosuz ağınız bu isimle yayın yapacaktır ve saldırganlar

tarafından bu şifreleri tahmin etmek zor olmayacaktır. Uzmanlar 25 karakterli ve içinde büyük küçük harfler, rakamlar, özel karakterler kullanılan şifreler koymanızı istiyor. Erişim noktasının yayın yaptığı kanalı da değiştirebilirsiniz.

4.2.2 Servis Seti Tanımlayıcı (SSID-Service Set Identifier)

Servis seti tanımlayıcı, bir kablosuz ağı tanımlayan addır. Yani kablosuz ağın bilgisayar ya da mobil cihazlarda görülen adıdır. Kablosuz bir ağ oluştururken kablosuz cihazların bu ağa bağlanması için onun SSID'sini bilmelidir, aksi takdirde onunla iletişim kuramaz. Bu nedenle kablosuz ağ, etraftaki kablosuz ağların bağlanabilmesi için bir SSID yayınlar. Bir SSID'de en fazla 32 alfasayısal karakter bulunabilir. WAP (Wireless Access Point – Kablosuz Erişim Noktası), SSID'yi genellikle metin olarak tanımlar.

Kullanıcı Kablosuz ağa bağlanmak için önce üye edildiği SSID'yi sorgular. Sorguladığı SSID belirlendikten sonra kullanıcı karşılıklı doğrulama sürecini yerine getirir (Şekil 4.1). Başarılı bir doğrulamadan sonra kullanıcı son duruma gelir ve son ilişkilendirilmiş ve doğrulanmış durumunda bir ortaklık mesajı gönderir ve giriş noktası yanıtı ortaklığı kurar (Reisoğlu, 2008).



Şekil 4.1 802.11 istemci doğrulama süreci

Bazen SSID güvenlik nedenleriyle yayınlanmaz. Wi-Fi ağı SSID'si modem arayüzünden görünmez hale getirilir. Modem arayüzüne girdikten sonra kablosuz (WLAN) sekmesinden Kablosuz Gelişmiş Ayarlara girip SSID Yayınlama seçeneği Devre Dışı olarak işaretlenmelidir (Şekil 4.2). Kablosuz ağ adı gizleme işlemi

yapıldığında modeminiz çevredeki diğer cihazlarda ağ araması yapıldığında bulunmaz, gerekli bilgilerin elle girilmesi gerekir.

Şekil 4.2 TP-LINK modeminin arayüzü

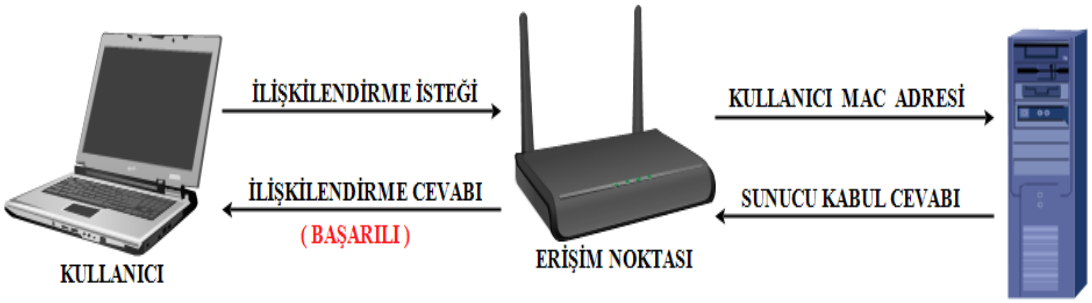
Bu seçeneği kapatmak ağı güvenli hale getirmez çünkü bir kablosuz ağ dinleyicisi WLAN trafiğindeki araştırma istekleri, araştırma istek yanıtları ve bağlantı isteklerini dinleyerek kolayca SSID değerini ele geçirebilir. SSID'ler bir güvenlik özelliği olarak kabul edilmemeliler (Reisoğlu, 2008).

4.2.3 MAC adresi filtreleme

MAC kelimesi anlamını Media Access Control baş harflerinden almıştır ve Ortam Erişim Yönetimi anlamına gelir. MAC adresleri bilgisayarların ağ kartlarının yapıldığı fabrikalarda üretim aşamasında ağ kartlarına atanan ve dünyada bir eşi olmayan seri numaralarıdır. Yani şu anda kullandığımız bilgisayarın ağ kartında kendine özel bir MAC numarası vardır. Bir ağ kartı bir diğer ağ kartına veriyi yollarken alıcıyı diğerlerinden ayırmak için MAC adresini kullanır. Bu yüzden MAC adresleri internete bağlanacak olan her bir bilgisayarda olması gereken adreslerdir. MAC adresleri dolayısı ile değiştirilemez ama kopyalana bilir. MAC adresleri 6 byte uzunluğundadırlar bunlardan ilk 3 byte üretici firmanın kodlarıdır. Örneğin; 52:B8:AX:84:25:AS bir MAC adrestir.

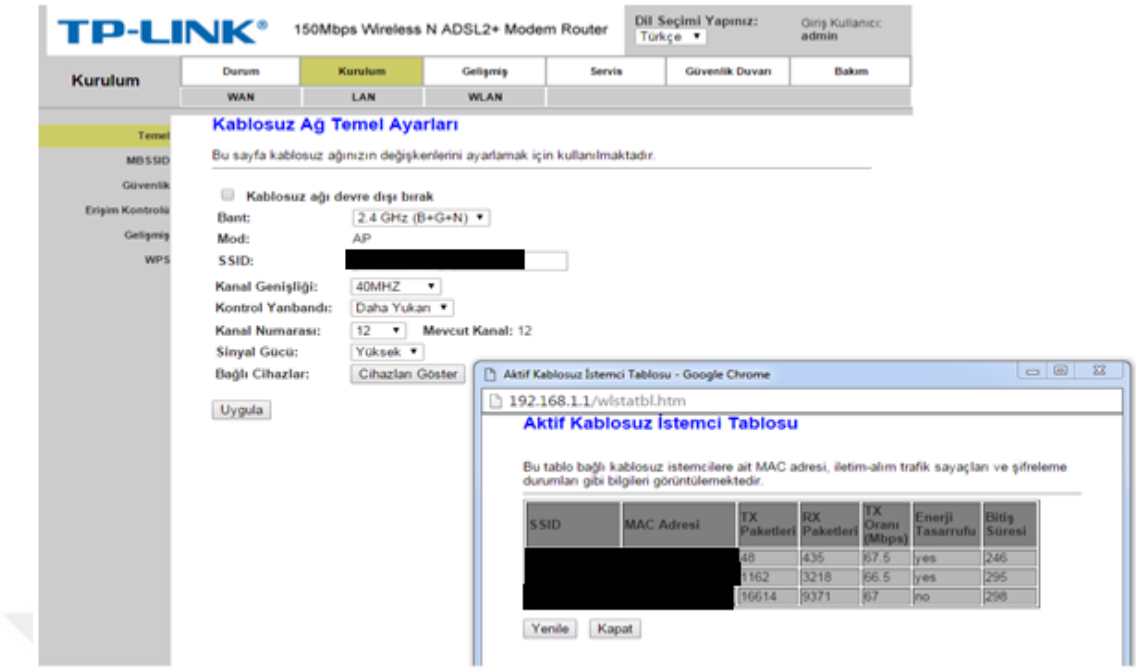
Erişim Noktaları da bu MAC adreslerini kullanarak, sisteme giriş yapmak isteyen kullanıcıların MAC adreslerine göre filtreleyerek erişim izninin olup olmadığını kontrol eder. Bunu için güvenlik kısmında MAC filtrelemeyi etkin hale getirmeliyiz ve sadece erişimine izin vermek istediğimiz bilgisayarların MAC adreslerini eklemeliyiz. Amaç belirlediğimiz MAC adreslerine sahip kablosuz cihazlar dışındaki kablosuz cihazların erişimini engellemektir. MAC filtreleme özelliği, günümüzde kullanılan hemen hemen her modemin üzerinde mevcuttur (Şamlıoğlu, 2011).

Kullanıcı erişim noktasına ilişkilendirme isteğini gönderir. Erişim noktası da MAC adresini doğrulaması için doğrulama sunucusuna gönderir. Doğrulama sunucusu da MAC adresinin erişim izninin olup olmadığını kontrol eder ve kabul ya da ret cevabını erişim noktasına gönderir. Erişim noktası MAC adresinin iznini onaylarsa kullanıcıya erişim izni verir (Şekil 4.3).



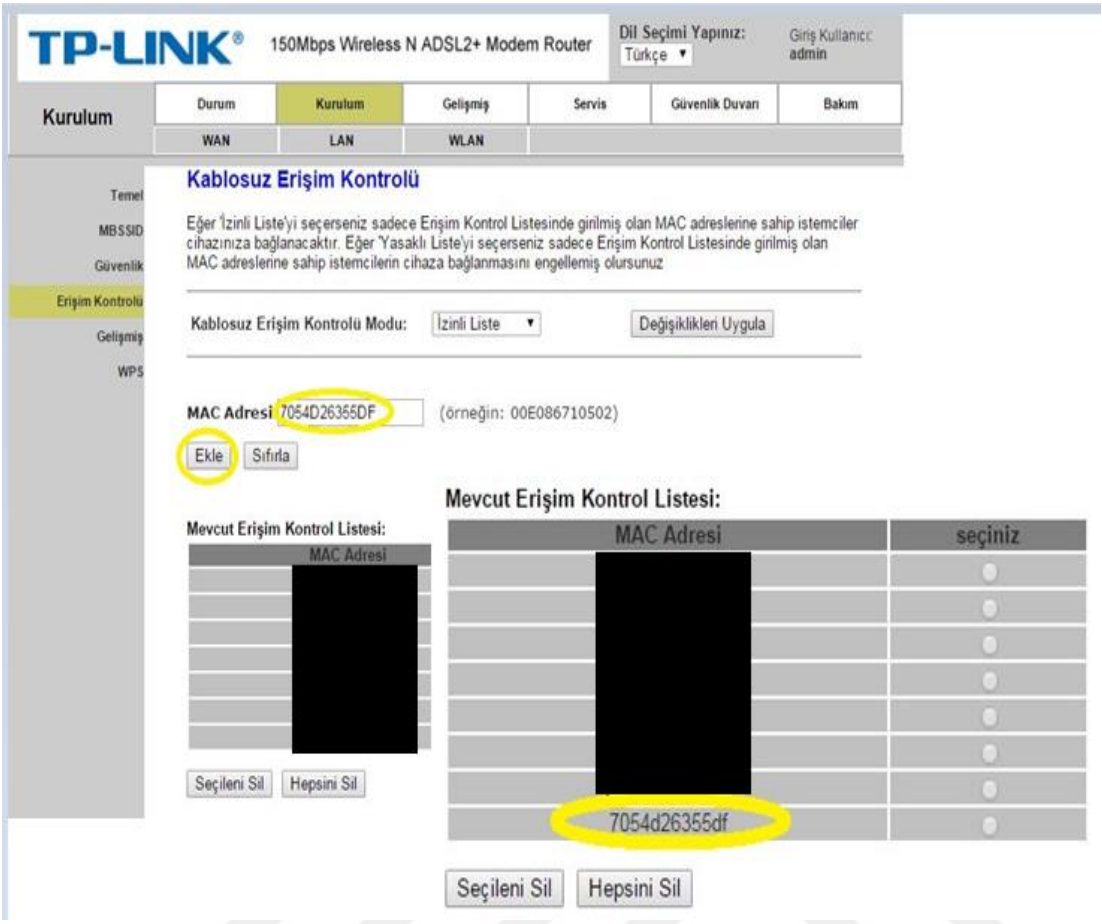
Şekil 4.3 MAC adresi ile doğrulama süreci

Günlük yaşamımızda kullandığımız modemler de MAC filtreleme yapmadan önce ağımız üzerindeki tüm aygıtların MAC adreslerini bilmemiz gerekiyor. MAC adreslerimize bakmanın en kolay yöntemi modem arayüzünden ulaşabileceğimiz Aktif Kablosuz İstemci Tablosuna bakmaktır (Şekil 4.4). İstemci listesinde kablosuz ağımızda bulunan dizüstü bilgisayarlarımızın, cep telefonlarımızın, tabletlerimizin ve başka kablosuz cihazlarımızın MAC adreslerini görebiliriz.



Şekil 4.4 Aktif Kablosuz istemci tablosu

MAC adreslerimizi bir yere not ettikten sonra modemimizin Kablosuz Erişim Kontrolü kısmına gelerek, Kablosuz Erişim Kontrolü Modu'nu İzinli Liste yapıyoruz. Sonra MAC Adresi kısmına ağımıza bağlanmasına izin vermek istediğimiz kablosuz cihazın MAC adresini yazıp Ekle butonuna tıklayarak Mevcut Erişim Kontrol Listesine ekliyoruz (Şekil 4.5).



Şekil 4.5 Mevcut Erişim Kontrol Listesine cihazın eklenmesi

Bu işlemi bitirdikten sonra artık dışarıdan biri bizim şifreyi bilse bile ağımıza bağlanma izni olmadığından bağlanamayacaktır.

Ne yazık ki bu da güvenlik adına tam olarak bir çözüm değildir. Çünkü saldırgan bazı yöntemlerle veya programlarla izinli listedeki MAC adresini öğrenebilir ve kendi MAC adresini o adresle değiştirip ağımıza bağlanabilir. MAC adresi değiştirme basit bir kayıt değişimidir. Birçok yardımcı program ile kolaylıkla yapılabilir. Belirli durumlarda MAC adres doğrulaması güvenlik özelliklerinin eksiklerini giderebilir, fakat bu hiçbir zaman kablosuz güvenlik sağlamanın ana metodu olmamalıdır (Reisoğlu, 2008).

4.2.4 Kabloluya Eşdeğer Gizlilik (WEP-Wired Equivalent Privacy)

WEP, kablosuz yerel alan ağlarının güvenlik standartlarından biridir. WEP'in amacı radyo dalgaları üzerinden dağıtılan verileri şifrelemektir. Eylül 1999 yılından beri WEP, Wi-Fi güvenlik standardı olarak kabul edilmiştir. WEP'in ilk sürümlerinin geliştirildiği dönemlerde Amerika, bazı kriptografik teknolojilerin şifre kullanımına

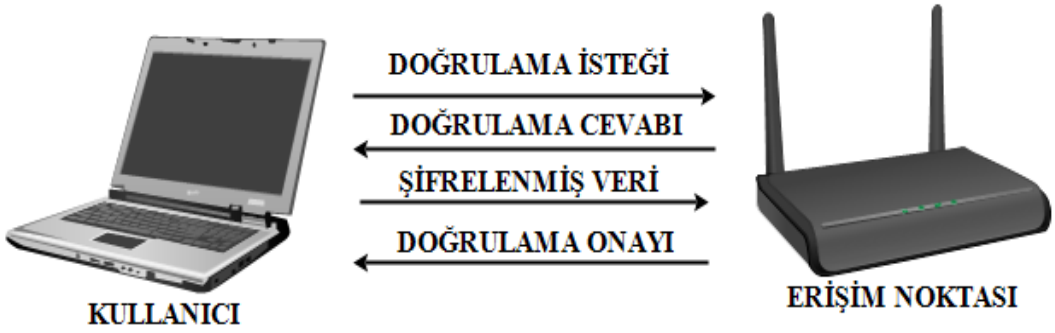
sınır koymuştu ve bu yüzden üretici firmalar sadece 64 bit şifreleme kullanabiliyorlardı. Sınırlamalar kaldırıldıktan sonra üreticiler şifrelemeyi 128 bit'e daha sonra ise 256 bit'e çıkardılar. Günümüzde 256 bit WEP şifrelemesi mevcuttur ama 128 bit şifreleme daha yaygın kullanılır (Tatlı ve diğerleri, 2013).

4.2.4.1 WEP kimlik doğrulama

WEP güvenlik standardı kimlik doğrulama işlemi için iki seçenek sunmaktadır.

Açık Sistem Kimlik Doğrulama (Open System Authentication) : İsminden de anlaşılacağı gibi istemci ve erişim noktası arasındaki iletişim herhangi bir kimlik doğrulama yapılmadan sağlanır. Kullanıcı Erişim Noktasına (EN) bağlanmak istediğinde kablosuz ağ kartının MAC adres bilgisi erişim noktasına gönderilir ve EN bu bilgiyi kaydederek kullanıcıya kendisine bağlanması için kablosuz erişim hakkı verir (Özdemir, 2008).

Paylaşılan Anahtar ile Kimlik Doğrulama (Shared Key Authentication) : Kullanıcıyla erişim noktası arasında kimlik doğrulama anahtarı belirlenir ve kullanıcı erişim noktasına bağlanmak istediğinde erişim noktasına bağlanma (doğrulama) isteği gönderir. Erişim noktası bu isteğe karşın doğrulama cevabı olarak kullanıcıya şifresiz bir sorgu paketi gönderir. Kullanıcı gelen bu sorgu paketini WEP anahtar ile şifreler ve şifrelenmiş veri olarak erişim noktasına gönderir. Erişim noktası gelen paketin doğru WEP anahtarı ile şifrelenip veya şifrelenmediğini kontrol eder. Doğru WEP anahtarı ile şifrelenmişse erişim noktası kullanıcıya kendisine bağlanması için kablosuz erişim hakkı verir (Şekil 4.6) (Özdemir, 2008).



Şekil 4.6 Paylaşılan anahtar ile kimlik doğrulama süreci

4.2.4.2 WEP şifreleme algoritmaları

WEP güvenlik protokolünün şifreleme algoritması RC4 (Rivest Cipher), anahtar uzunluğu 40 bit (veya 104 bit), IV (Initialization Vector) uzunluğu 24 bit, veri bütünlüğü yöntemi ise ICV (Integrity Check Value)'dir (Harmankaya ve diğerleri).

RC4 (Rivest Cipher 4) şifreleme: RC4 şifreleme algoritması, RSA'da çalışan Ronald Rivest tarafından 1987 yılında geliştirilmiştir (Kartal, 2010). RC4 şifreleme simetrik şifreleme algoritması olduğundan veriyi şifrelemek ve çözmek için aynı anahtarı kullanır. RC4'ün amacı, verilen bir gizli anahtar ile geniş uzunlukta rasgele sayılar üretmek ve daha sonra bu akışla göndericide düz metin mesajı şifrelemektir. Alıcı, verilen anahtarla aynı akışı üretebilecek ve alınan mesajın şifresi çözülebilecektir (Bayraktar, 2005).

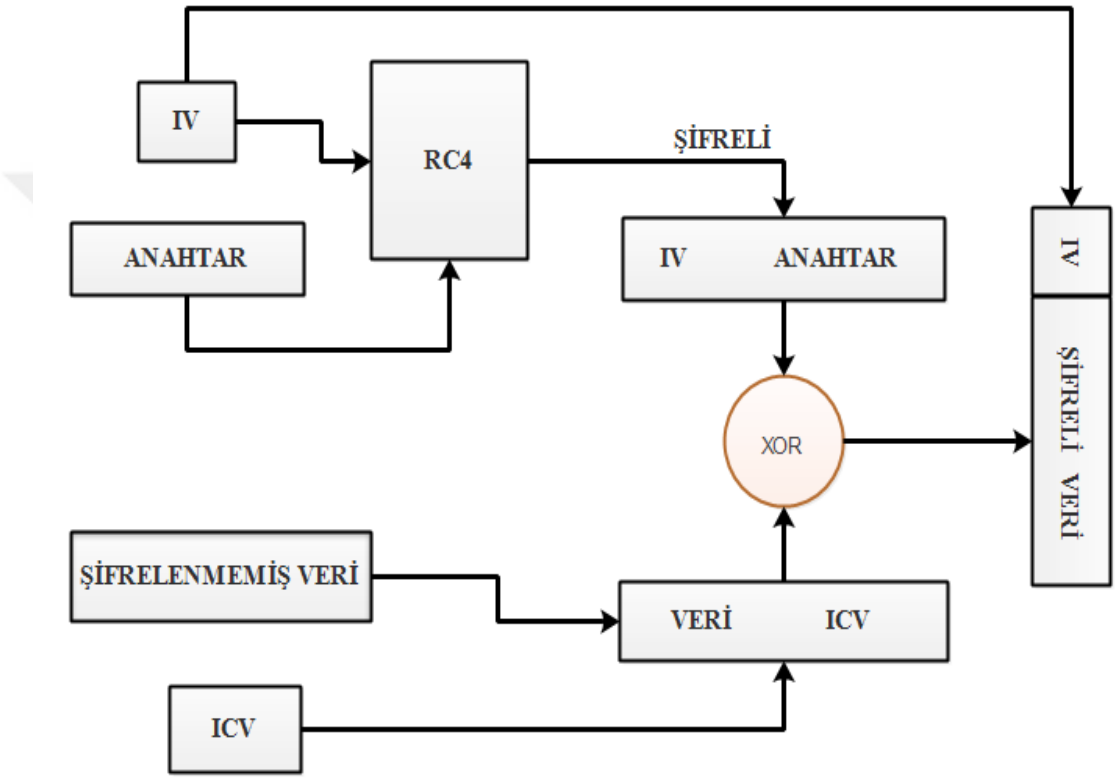
IV (Initialization Vector): IV başlangıç vektörü, 64 bitlik WEP şifreleme algoritmasının 24 bitlik başlangıç kısmını oluşturur. IV'nin kullanılmasında amaç WEP'te gönderilen şifreli verinin veya metnin başlangıc durumlarının tekrar oluşmasını önlemektir. IV değeri şifreli paketin içerisinde tekrardan şifrelenmez çünkü alıcı tarafında şifre çözme işleminde aynı değer kullanılır. IV için ayrılan 24 bitlik küçük alan tekrardan aynı akış şifresinin üretilmesine sebep olur ve bu güvenlik adına istenmeyen bir durumdur.

ICV (Integrity Check Value): Bu yöntemde veri paketinin 32-bit CRC(Cyclic Redundancy Check)'si oluşturulmakta ve WEP anahtarı ile şifrelenerek alıcıya gönderilmektedir (Özdemir, 2008). ICV, gönderilen paket ya da mesajların ulaşım esnasında bir değişikliğe uğrayıp uğramadığının kontrolünü yapar. Bu kontrol için gönderilen paketler içerisine bir Integrity Check Vector alanı kullanılır.

4.2.4.3 WEP şifreleme

WEP şifreleme şu şekilde çalışmaktadır; Gönderme ünitesi 24 bit'lik bir başlangıç vektörü (IV-Initialization Vector) üretir ve daha sonra 40 bit'lik ya da 104 bit'lik gizli anahtara (ortak anahtar) eklenir. Bu anahtarın uzunluğu, IV + Gizli Anahtar uzunluğu kadardır (24 + 40=64 bit ya da 24 + 104=128 bit). Oluşan bu yeni anahtar RC4 algoritmasına girdi olur. Bu şekilde, her kullanımda, RC4 algoritmasına farklı bir anahtar girecektir. Daha sonra, RC4 algoritması, sahte rastgele sayı üreteci kullanarak girdi parametresinin uzunluğu (64 bit ya da 128 bit) kadar bir akış anahtarı üretir. Bu sırada veri bütünlüğü sağlamak için şifrelenmemiş veri üzerinden bütünlük kontrol

değeri (ICV-Integrity Check Value) hesaplanır ve verinin sonuna eklenir. Elde edilen akış şifresi ile (veri + ICV) XOR işlemine girer ve sonuç olarak şifreli veri hazırlanmış olur. Son olarak şifreli verinin başına alıcı tarafın şifreyi çözmesi için bilmesi gereken IV, şifrelenmeden eklenir. Böylece WEP şifreleme yöntemi kullanılarak şifreli veri elde edilir (Şekil 4.7). Şifre çözmede ise alıcı taraf IV'yi çerçeveden okur anahtar kendinde olduğu için akış şifresini elde eder ve şifreleme işlemlerini ters sıra ile gerçekleştirerek açık veriye ulaşır (Kadakoğlu, 2010).



Şekil 4.7 WEP şifreleme akış diyagramı

4.2.4.4 WEP'in zayıflıkları

WEP'in tasarlanmasının üç önemli amacı güvenilirlik, erişim kontrolü ve veri bütünlüğü olmasına rağmen bu alanlarda maalesef eksikleri zamanla ortaya çıkmaya başladı. Algoritmanın ortaya çıkan sorunlarına karşın yapılan düzeltmeler ve artırılan anahtar boyutuna rağmen, ortaya çıkan güvenlik açıkları saldırganlar tarafından kötüye kullanılmaya başlandı. Zamanla bilgisayar gücünün artmasıyla ise artık bu açıkları kötüye kullanmak oldukça kolay duruma geldi. Uzmanlar WEP'in zayıflığını insanlara anlatabilmek için, ücretsiz yazılımlarla WEP şifrelerinin ne kadar kolay

kırılabildiğini göstermeye başladılar (Mert Tatlı ve diğerleri, 2013). Bu eksiklere kısaca bakacak olursak;

WEP'in ilk zayıflığı anahtar paylaşımında gizliliği yönetmesindeki eksikliğinden gelmektedir. Bu eksikliğin en açık sebebi otomatik anahtar yönetiminin olmamasıdır. WEP'in anahtar dağılımı elle yapılır. Her kullanıcı, aynı gizli anahtarı bilmek zorundadır. Geniş kullanıcı topluluğuna anahtar dağılımı yapılır. Anahtarın değişmesi, her bilinen kullanıcının güncelleştirmeden haberdar edilmesi demektir ve hiç pratik bir durum değildir. Bunun sonucunda, WEP'in kullanıldığı birçok yerde anahtar uzun zaman aynı kalmaktadır. Geniş bir topluluk gizli anahtarı bildiği zaman, anahtarın uzun süre gizli kalması oldukça zordur.

RC4 algoritmasına parametre olarak giren IV değeri başlangıçta sıfır değerindedir ve her paket için işleme girdiğinde değeri bir artar. IV'nin 24 bit uzunluğunda olması 224 farklı değer alabilmesi demektir. Dolayısıyla 224 paket sonra RC4 algoritmasında aynı IV değerleri tekrar kullanılacaktır. Ağı dinleyen saldırganların anahtarın yeniden kullanıldığı zamanı bilmeleri, aynı anahtarla şifrelenmiş çoklu paketleri elde etmeleri anlamını gelir. Aynı akış şifresi ile şifrelenen mesajlar elde edildikten sonra analiz yöntemleri kullanılarak veri deşifre edilebilir (Köksal, 2007).

Paylaşılan Anahtar ile Kimlik Doğrulama da kimlik doğrulama için kullanılan anahtar aynı zamanda veri şifrelemesi için de kullanıldığından güvenlik açığı oluşturmaktadır. Böylece şifreyi ele geçirmek daha da kolaylaşır (Kadakoğlu, 2010).

WEP anahtarlarının şifrelerinin çözülmesinin bir başka yolu da RC4 (Rastgele Sayı Üretici – Pseudo Random Number Generator – PRNG) algoritması ile oluşturulan akış şifrelerinin doğrusal bir yöntemle oluşturulması ve dolayısıyla bu şifrelerin çözülmesinin kolay olmasıdır (Reisoğlu, 2008). Bu zayıf anahtarlar tespit edilerek çözülebilmektedir.

WEP'te iletilen verinin baş kısmındaki MAC adres bilgileri şifrelenmediğinden saldırganlar bu adresleri istediği şekilde değiştirerek verileri farklı bir adrese yönlendirebilir (Reisoğlu, 2008).

WEP'te veri tekrarı saldırılarını önlemek için herhangi bir güvenlik önlemi olmadığından saldırganlar aynı mesajı alıcılar tarafından bile anlaşılamayacak şekilde defalarca gönderebilir.

4.2.5 Wi-Fi Korumalı Erişim (WPA - Wi-fi Protected Access)

WEP standardının zayıflıklarının ortaya çıkması sonucunda IEEE yeni bir güvenlik standardı oluşturmak zorunda kalmıştır. Fakat bu standardın oluşmasının gecikmesi sebebiyle üretici firmalar, çeşitli sistemlerin birlikte çalışmasına olanak veren geçici bir standart üzerinde anlaşmak kararını almıştır. Böylelikle WEP'in zayıflıklarını gidermek amacıyla 2004 yılında WiFi Alliance (üretici firmaların oluşturduğu organizasyon) tarafından Wi-Fi Korumalı Erişim (WPA) standardı geliştirilmiştir. WPA, ek bir donanım gerektirmez kullanıcı yazılım veya cihaz yazılım güncellemeleriyle bu protokolü kullanabilir. Günümüzde cihazlarda desteği eklenmiş durumdadır (Gezgin ve Buluş, tarih yok).

WPA'nın WEP'e tercih edilmesinin sebebi WEP'in zayıflıklarını büyük oranda kapatmasıydı. WPA da kullanılan 128 bit uzunluklu anahtar her oturum ve her paket için değişir ve böylelikle de daha yüksek bir güvenlik sağlanmış olur. Anahtar yönetimi için 802.1x kullanılır. WPA kimlik doğrulama için 802.1x EAP yöntemini kullanır. Veri bütünlüğü kontrolü ise MIC (Message Integrity Code) mekanizması ile sağlanır (Gezgin ve Buluş, tarih yok).

4.2.5.1 WPA kimlik doğrulama

WPA kimlik doğrulama işlemi için iki seçenek sunmaktadır.

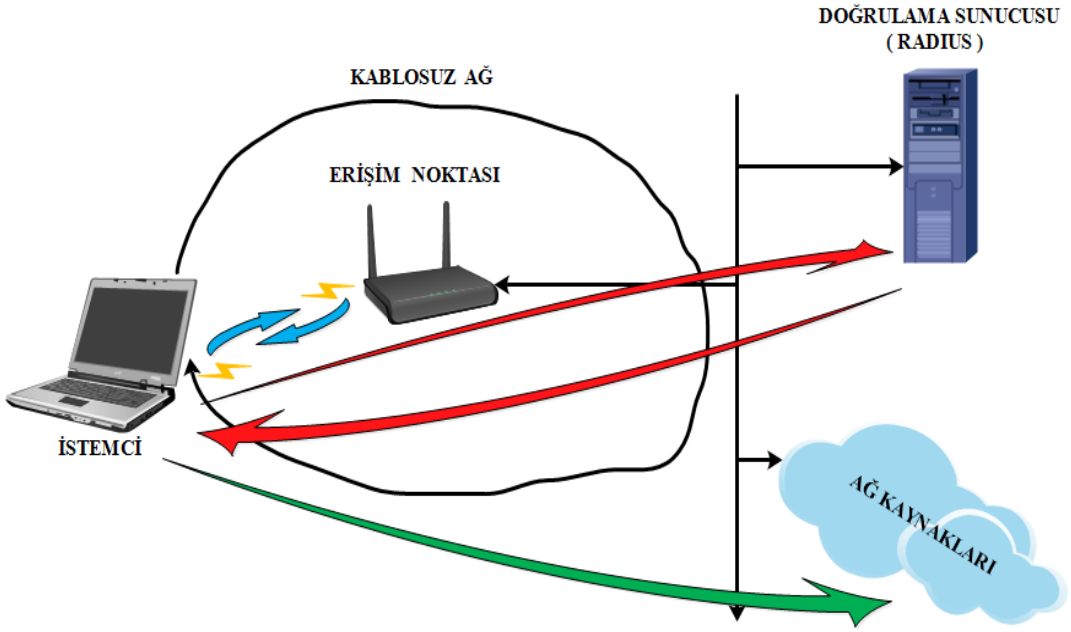
WPA-PSK yapısı: Kablosuz ağ bağlantı özelliklerinden kimlik doğrulama metodu olarak WPA-PSK seçilerek uygulanır. Ev kullanıcıları ve küçük işletmeler kullanabilir ama kurumsal kablosuz ağlarda kullanımı uygun değildir (ALTAI, 2013). WPA-PSK da kimlik doğrulama EN ve istemci tarafında girilmesi gereken 8 ile 63 karakter arası bir paylaşılan anahtar ile gerçekleştirilir.

802.1x yapısı: Kablosuz ağlar için 802.1X kimlik doğrulamasının üç ana bileşeni vardır:

- Kimliği doğrulayan (erişim noktası)
- Talepte bulunan (istemci yazılım)
- Kimlik doğrulama sunucusu

802.1X kimlik doğrulaması, EAP (Extensible Authentication Protocol - Genişletilebilir Kimlik Doğrulama İletişim Kuralı) olarak bilinen bir kimlik doğrulama iletişim kuralı kullanımından yararlanır. 802.1X kimlik doğrulamada istemci EN'na

bir kimlik doğrulama isteği gönderir ve EN istemciyi EAP uyumlu RADIUS (Remote Authentication Dial-In User Service) sunucusunda doğrular. Kablosuz istemci, RADIUS sunucusundan onay cevabı gelene kadar ağa bağlanamaz (Şekil 4.8).



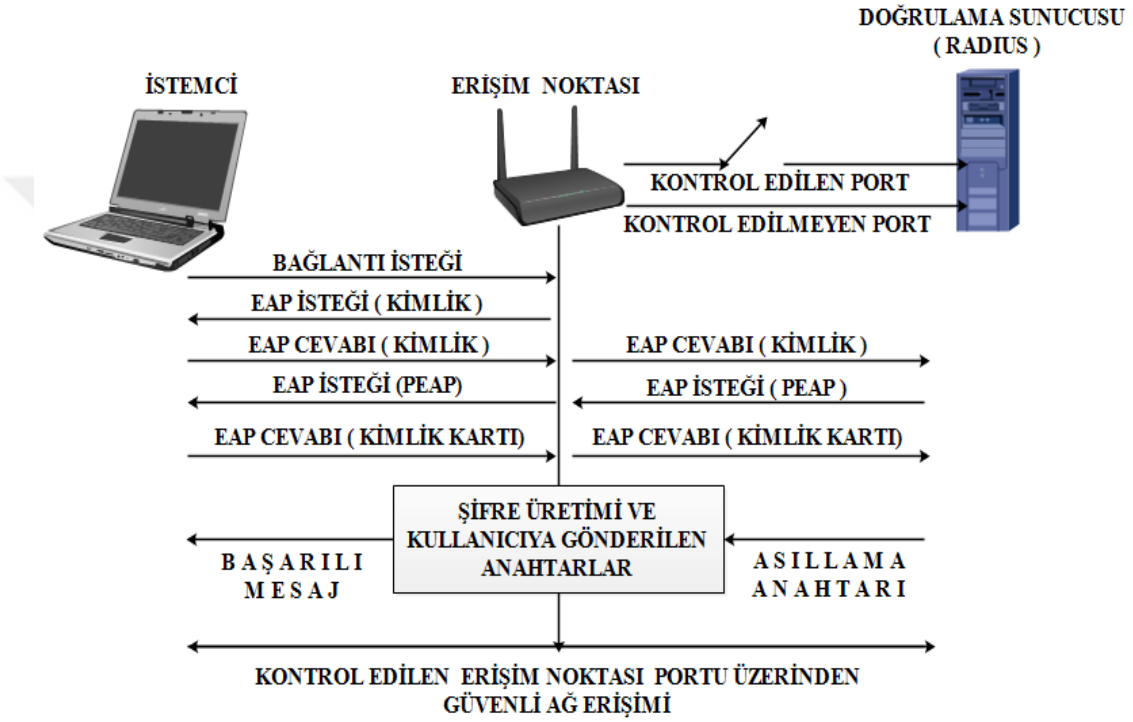
Şekil 4.8 802.1X yapısı

802.1X kimlik doğrulamasında (EAP-TLS, EAP-TTLS) , Protected EAP (PEAP) ve EAP Cisco Kablosuz Genişletilebilir Hafif Kimlik Doğrulama İletişim Kuralı (LEAP) gibi kimlik doğrulama algoritmaları kullanılır. Bu algoritmalar istemcinin kendini RADIUS sunucusunda doğrulama yollarıdır. RADIUS, AAA (Authentication, Authorization, Accounting - Kimlik Doğrulama, Yetkilendirme, Hesap Yönetimi) olarak anılan standartlar takımından oluşur ve bu takımın ana amacı kullanıcı kimliklerini veri tabanlarıyla karşılaştırmaktır (Şekil 4.9).

RADIUS sunucusunun, örneğin Protected EAP (PEAP) mekanizmasını kullanarak 802.1x asıllama işlemini yapması şu şekilde gerçekleşir (Köksal, 2007).

- İstemci kimlik bilgilerini göndererek EN'dan bağlantı isteğinde bulunur.
- EN, bu isteği kimlik kontrolü yapılmayan bir porttan RADIUS doğrulama sunucusuna gönderir.
- RADIUS doğrulama sunucusu EN üzerinden Protected EAP (PEAP) mekanizmasını kullanarak istemciden talepte bulunur.

- İstemci, EN üzerinden RADIUS sunucusuna kimlik bilgilerini cevap olarak iletir.
- Kimlik bilgileri doğru ise, RADIUS sunucusu EN'na şifrelenmiş bir asıllama anahtarı gönderir.
- EN, sadece o oturumda kullanılabilecek şifrelenmiş bir asıllama anahtarını istemciye gönderir.
- İstemci, asıllama anahtarını aldıktan sonra veri trafiğine başlaya bilir.



Şekil 4.9 802.1x asıllama işlemi adımları

4.2.5.2 WPA şifreleme algoritmaları

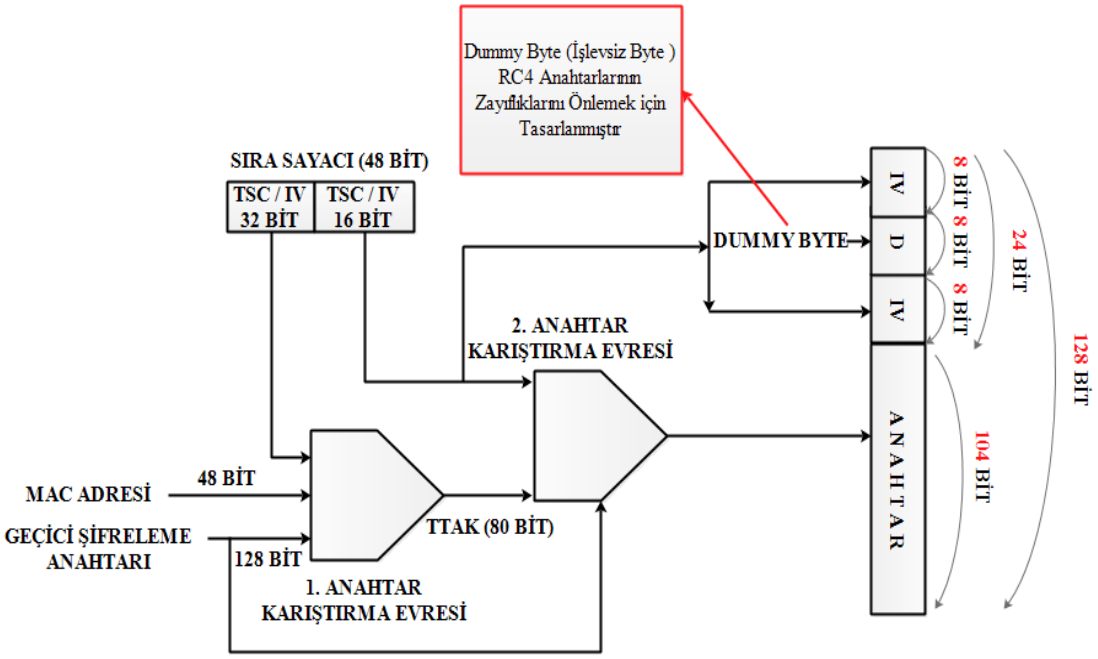
WPA şifreleme yöntemi olarak TKIP, mesaj bütünlüğü kontrolü için ise MIC algoritmalarını kullanır. WPA geçici olarak tasarlandığı için basit kablosuz donanım güncellemeleri ile elde edile bilinsin değe hazırlanmıştır. Ama AES desteği, güncellemeler ile eklenemeyeceğine göre isteğe bağlı olarak kullanılır.

Geçici Anahtar Bütünlüğü Protokolü (TKIP - Temporal Key Integrity Protocol): TKIP, WEP tabanlı çözümlere karşılık bir yazılım güncellemesi olarak tasarlandığından WEP'in temel yapısına ve işlemlerine sahiptir. Fakat WEP'in var

olan zayıflıklarına çözüm olarak tasarlandığından ve isim olarak ayırabilmek adına yeniden adlandırılmıştır.

TKIP ile IV 24 bitten 48 bite çıkarılmıştır ve IV hem paketlere sıra numarası vermede hem de her paket için yeni bir anahtar oluşturmada kullanılır. Her pakete sıra numarası verilmesinin sebebi tekrar saldırılarının karşısını almaktır. Bu mantıkla sırasız gelen paketler alıcı tarafından kabul edilmeyecektir ve WEP'e yapılan tekrar saldırılar WPA da yapılamayacaktır.

WPA, tekrar saldırılarına karşı TSC (TKIP Sequence Counter) kullanır. TSC'nin çalışma mantığı gelen paketin sıra numarası, bir önce gelen paketten 1 fazla değilse, o paketi kabul etmemektir (Şekil 4.10). TSC, oturum anahtarından oluşturulan geçici şifreleme anahtarını ve MAC adresini kullanarak her paket için ayrı bir şifreleme anahtarı üretir (Köksal, 2007).



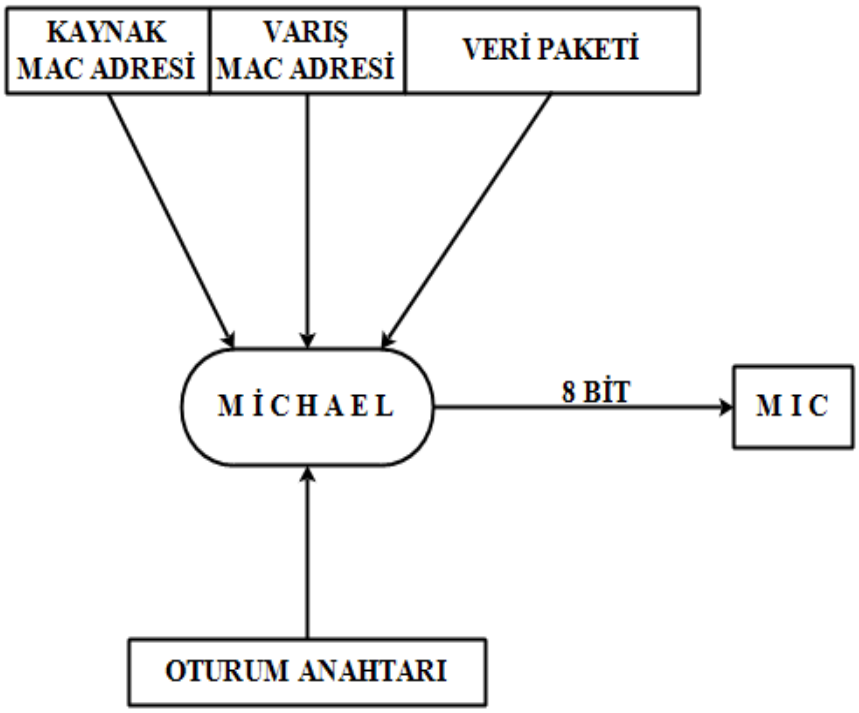
Şekil 4.10 Paketlerin şifrelenmesi için farklı anahtarların oluşturulması

TSC, 1. anahtar karıştırma evresinde giriş olarak belirtildiği gibi verici MAC adresi, 48 bitlik sıra sayacının yüksek anlamlı 32 bitlik parçası (IV) ve 128 bitlik geçici şifreleme anahtarıdır. Çıktı olarak ise TTAK 80-bitlik bir ara anahtar değerini verir. Anahtar karıştırma işleminin evre ikisi, her yapı için yeniden hesaplanmalıdır. Giriş olarak, ikinci evre, birinci evrenin verdiği TTAK değerini, geçici şifreleme anahtarını ve sıra sayacının düşük anlamlı 16 bitini alır. Yapıda şifrelemek için değiştirilen tek

giriş, sıra sayacıdır. Sonuç olarak anahtarlar her oturum ve paket için değişir (Deniz Mertkan Gezgin).

Her paket için oluşturulan anahtarın uzunluğunun 48 bit olması ile tekrarlanma sıklığını yaklaşık olarak 100 yıla çıkartmıştır. Dolayısıyla WPA da IV'lerin dinlenerek anahtarın ele geçirilmesi çok güçtür.

Mesaj Bütünlük Kodu (MIC-Message Integrity Code): WPA'da veri bütünlüğünü kontrol etmek için Michael algoritması kullanılır. Michael veri bütünlük kodu alıcı ve verici MAC adreslerini alarak sağlama bitleri oluşturur (Şekil 4.11). MAC adresleri de WEP'te olduğu gibi açık bir şekilde gönderilmez. Sağlama bitleri verinin sonuna şifreli şekilde eklenir. Şifrelenerek eklenme saldırganlar tarafından mesaj içeriğinin değiştirilmesini önler. Michael algoritmasına girdi olarak MAC adreslerinin yanı sıra oturum anahtarı ve veri paketi de girer. Bu girdiler sonuç olarak 8 bitlik bir sağlama verisi oluşturur (Köksal, 2007).



Şekil 4.11 MIC kodunun elde edilmesi

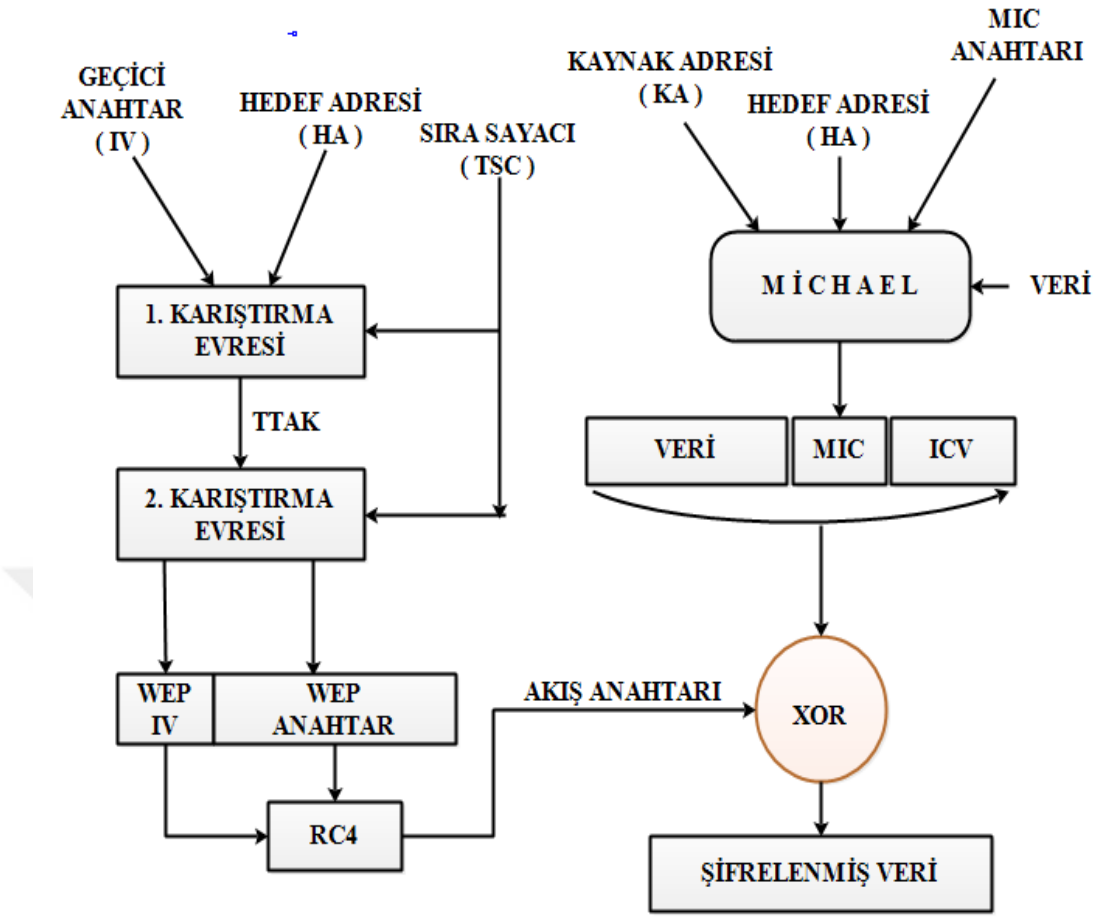
4.2.5.3 WPA şifreleme

WPA şifrelemede veriyi şifrelemek ve bütünlüğünü sağlamak için özetle, aşağıdaki değerlere ihtiyaç vardır;

- Veri şifreleme anahtarı ya da grup şifreleme anahtarı.
- Veri ya da grup bütünlüğünü kontrol eden MIC anahtarı.
- Sıfırdan başlayan ve her veri paketi için bir bir artan IV değeri.
- Kablosuz veri çerçevesinin kaynak (KA) ve hedef (HA) adresi.
- Sıfırdan başlayarak artan ve gelecek işlemin belirtilmesi için ayrılan özellik alanının değeri.

Şekil 4.12'de gösterilen WPA şifreleme mekanizmasında uygulanması gereken aşamalar aşağıda belirtilmiştir (Yüksel ve diğerleri).

- IV, HA ve veri şifreleme anahtarı TKIP anahtar karıştırma evrelerine girerek her paket için şifreleme anahtarı oluşturur.
- KA, HA, veri ve veri bütünlük anahtarı Michael veri bütünlük algoritmasına girerek MIC bütünlük sağlaması oluşturulur.
- CRC-32 sağlaması ile ICV değeri hesaplanır ve MIC in sonuna eklenir.
- IV değeri ile şifreli her paket anahtarı RC4 PRNG fonksiyonuna girer ve sonuç olarak MIC ve ICV ile aynı veri genişliğinde bir akış anahtarı üretir.
- Veri, MIC ve ICV üçlüsünün oluşturduğu kombinasyon ile akış anahtarı XOR işlemine girerek şifrelenmiş metini oluşturur.
- Şifrelenmiş metne IV ve genişletilmiş IV bilgileri eklenerek bir 802.11 kablosuz veri paketi elde edilmiş olur.



Şekil 4.12 WPA şifreleme mekanizması

WPA her ne kadar WEP'in eksiklerini kapatmak için tasarlansa da WEP'in zayıflıkları WPA'nın da peşini bırakmadı. Çünkü WPA'nın temel amacı ayrı bir donanım gerektirmeden basit WEP güncellemeleriyle cihazlara uygulanmasıydı. Öyle ki, WEP de kullanılan sistemlerin bazı unsurları tekrar kullanılmak zorunda kalındı ve bunlarda zamanla açıklar vermeye başladı. Uzmanlar WEP gibi WPA'nın da saldırılara karşı ne kadar açık olduğunu göstermek adına videolar yayınlamaya başladı (CHIP, 2013).

4.2.6 Çok Güvenli Ağ (RSN-Robust Security Network, WPA2)

WPA2 veya Robust Security Network (RSN) olarak bilinen bu standart IEEE 802.11i çalışma grubu tarafından WEP'in açıklarını tamamen ortadan kaldırmak için oluşturulmuştur. WPA2 WPA gibi WEP tabanlı ağlarla aynıdır fakat WPA'da olduğu gibi güncellemelerle WPA2'ye geçilemez. WPA2'ye bağlanmak için kablosuz cihazların WPA2 uyumlu olması şarttır. Bu uyumluluk cihaz güncellemeler ile de

sağlanamaz. Ancak üretim aşamasında bu uyumluluk eklenebilir. Bu yüzden de WPA2 teknolojisini kullanabilmek için mevcut kablosuz cihazların WPA2 uyumlu cihazlarla değiştirilmesi zorunludur.

Geçici olarak oluşturulan WPA'da kullanılan yöntemler genel kısımlarıyla WPA2'de de kullanılmıştır. Fakat WPA'nın eksik yönlerini kapatmak amacıyla farkı ve daha güçlü güvenlik önlemleri de alınmıştır. WPA2'de RC4 şifreleme algoritmasından ortaya çıkan zayıflıkları gidermek amacıyla AES (Advanced Encryption Standard) şifreleme algoritması kullanılır. AES şifreleme algoritması CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) protokolünü veya TKIP protokolünü kullanır. WPA2'de CCMP zorunlu iken, TKIP ise seçeneklidir. WPA2, doğrulama yöntemini IEEE 802.1x standartları ile gerçekleştirir. Veri bütünlüğü kontrolünü ise WPA'da olduğu gibi MIC algoritmasıyla sağlanır (Harmankaya ve diğerleri).

4.2.6.1 WPA2 kimlik doğrulama

WPA2'de kimlik doğrulama için WPA'da olduğu gibi 802.1X EAP standardı kullanılır. WPA kısmında 802.1X asıllama işleminin nasıl gerçekleştiği anlatıldı. Bu kısımda ise 802.1X standardında doğrulama için kullanılan EAP yöntemleri incelenecektir.

EAP kimlik doğrulama yöntemleri: EAP, aslında bir kimlik doğrulama yöntemi değil, kimlik doğrulama için geliştirilmiş bir kimlik kanıtlama protokolüdür. Bunun yanı sıra, kimlik kanıtlama sunucusu ile istemci arasında arabuluculuk yaparak tarafların hangi kimlik kanıtlama yöntemini kullanacakları konuşmasında da kullanılır. EAP kimlik kanıtlamanın kırktan fazla yöntemi vardır. Aşağıda, bunlardan en sık kullanılanlara değinilecektir.

Mesaj Özü ile EAP (EAP-MD5 - Message Digest Five): EAP-MD5 kimlik doğrulaması, kullanıcı adı ve şifreler kullanan tek yönlü bir kimlik doğrulama yöntemidir. Bu yöntemde kimlik doğrulamasının yapılabilmesi için şifrenin doğrulama sunucusunun veri tabanında açık metin olarak tutulması şarttır. MD5, doğrulanacak istemciden kullanıcı adı ve şifre alır ve bunu MD5 mesaj hashing algoritması ile şifreleyerek bu veriyi RADIUS sunucusuna gönderir (Reisoğlu, 2008). RADIUS sunucusu istemcinin kimliğini doğrulamak için, istemcinin gönderdiği şifreli veriyi veri tabanında tuttuğu açık metin kullanıcı adı ve şifre verisi ile karşılaştırır.

İstemci gönderdiği verileri doğru sunucuya gönderdiğini kontrol edemez çünkü MD5 yöntemi tek yönlü bir kimlik doğrulama yöntemidir. Bu yöntem, özellikle kablosuz ağda kullanılmak için oldukça güvensiz bir yöntemdir. Çünkü anahtar yönetimini desteklemez ve kablosuz ağ yeterince uzun dinlendiğinde, kırılması çok kolay olmaktadır.

Taşıma Katmanı Güvenliği ile EAP (EAP-TLS-Transport Layer Security): EAP-TLS kimlik doğrulaması yönteminde, istemci ve sunucu arasında bir TLS oturumu oluşturulur. TLS iletişim kuralı, kamuya açık bir ağda güvenliği sağlamak için verileri şifrelemek üzere tasarlanmıştır. Hem sunucu hem de istemci doğrulama için geçerli bir sertifika ve PKI (public key infrastructure) kullanmalıdır. EAP-TLS de doğrulama çift yönlü yapılabildiği için EAP yöntemleri içerisinde en güvenilir kimlik doğrulama yöntemi olarak bilinir. Fakat her istemciye ayrı bir sertifika üretip ve bu sertifikaları güvenli bir şekilde istemcilere dağıtılmasının yaratmış olduğu sıkıntılar sebebiyle çokta kullanılan bir yöntem değildir (Reisoğlu, 2008).

Tünellenmiş Taşıma Katmanı Güvenliği ile EAP (EAP-TTLS-Tunneled Transport Layer Security): EAP-TTLS kimlik doğrulama yönteminde, kimlik doğrulama bilgisinin güvenli bir şekilde iletile bilinmesi için sunucu ve istemci arasında tünellenmiş bir TLS oturumu oluşturulur. TLS tünelinin içinde kimlik doğrulama başka bir kimlik doğrulama yöntemiyle de yapılabilir. RADIUS sunucusu istemciyi doğrulama verisiyle doğrularken, sunucu da doğrulama yapma yetkisi olduğunu sertifikasıyla kanıtlar. Sonuç olarak, sunucu sertifikası, kullanıcı adı ve şifre verisi kullanılarak çift yönlü doğrulama yapılmış olur.

Korunmuş EAP (PEAP-Protected EAP): EAP-TTLS'te olduğu gibi PEAP kimlik doğrulaması yönteminde de şifreli bir TLS oturumu oluşturulur. PEAP da sertifikalar istemcilerde değil de yetkilendiricilerde olması karmaşıklığı ve maliyeti azaltır. PEAP, en uygun ve en güvenli doğrulama yöntemlerinden biri sayılır. Fakat hem Cisco hem de Microsoft farklı yöntemleri uyguladığından çokta kabul görülmemiştir (Reisoğlu, 2008).

Sadeleştirilmiş Genişletilebilir Yetkilendirme Protokolü (LEAP - Lightweight Extensible Authentication Protocol): LEAP kimlik doğrulaması yönteminde istemci, kimlik kanıtlama için kullanıcı adı ve şifre verisini açık metin olarak RADIUS kimlik sunucusuna gönderir. LEAP, Cisco tarafından geliştirilmiş bir protokoldür

(Reisoğlu, 2008). LEAP da bir birilerinde bağımsız oturumlar oluşturularak bir oturuma saldırı yapılsa bile diğer oturumları güvende tutmak amaçlanır. Ancak, sözlük saldırıları ile kırılabildiği için güvenli olduğu düşünülmüyor.

Yukarıda sözü geçen yöntemlerin özet niteliğinde bir karşılaştırılması Tablo 4.1'de verilmiştir.

Çizelge 4.1 EAP yöntemlerinin karşılaştırılması

	MD5	TLS	TTLS	PEAP	LEAP
Standart	Açık	Açık	Açık	Açık	Firma
İstemci Sertifikası	×	✓	×	×	×
Sunucu Sertifikası	×	✓	✓	✓	×
Güvenlik	Yok	Güçlü	Güçlü	Güçlü	Zayıf
Kullanıcı Veritabanı	"Açık Metin" Parola	"Active Directory"	Token Systems, SQL, LDAP	Active Directory, NT Etki Alanı	Active Directory, NT Etki Alanı
Dinamik Anahtar Değişimi	×	✓	✓	✓	✓
Karşılıklı Doğrulama	×	✓	✓	✓	✓

4.2.6.2 WPA2 şifreleme yöntemleri

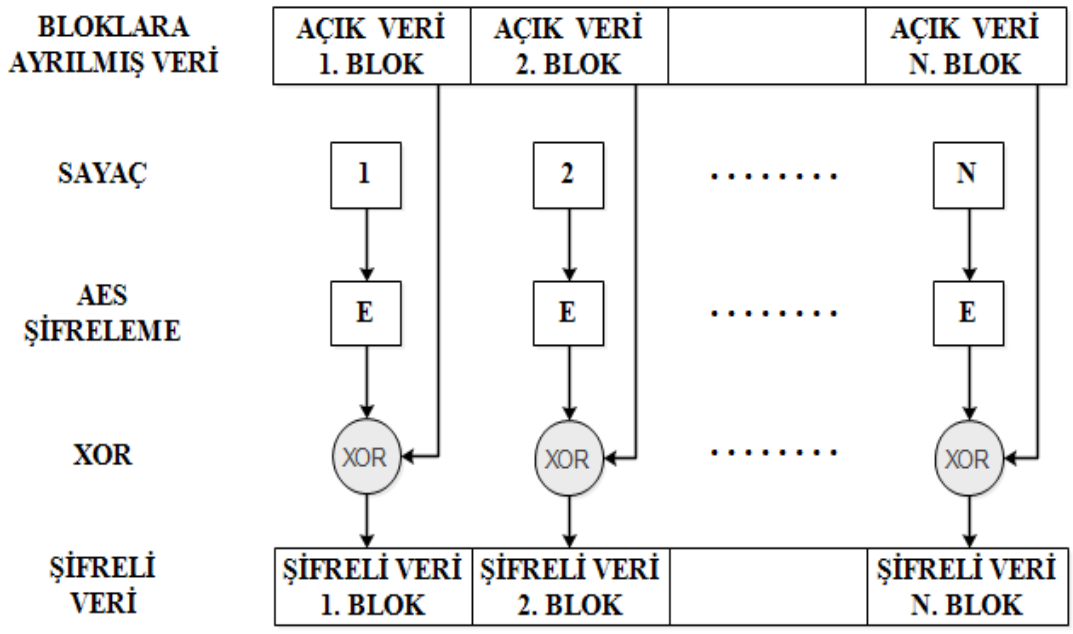
Yukarıda da belirtiğimiz gibi WPA2'de şifreleme TKIP veya CCMP ile gerçekleşir. CCMP protokolü TKIP'in aksine bir geçiş protokolü değil 802.11 ağları için nihai güvenlik mekanizmalarını tanımlar ve önceden yapılmış güvenlik amaçlı uygulamaları (WEP kapsülleme) geçersiz kılarak kullanmaz. CCMP protokolü TKIP' e oranla daha güvenilir kabul edilmektedir. Bunun nedeni eskiye olan bağımlılığının olmaması ve telsiz bilgisayar ağları üzerinde koşturulacağı da göz önüne alınarak baştan tasarlanmış olmasıdır.

Şifreleme algoritması kurulacak güvenlik mekanizmasının kalbi olarak tanımlanacağından bilinen problemlerinden dolayı RC4 algoritması yerine daha güvenilir bir algoritma olan AES seçilmiştir. RC4 algoritması temelde şifreleme amaçlı olarak değil rastgele sayı üretme amaçlı tasarlanmış olması da algoritma değişiminin bir nedenidir.

Sayaç Modu ile Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (CCMP): CCMP, şifreleme algoritması olarak AES'i kullanır. AES algoritmasında simetrik anahtarlar kullanıldığı için güvenilir ve hızlı bir algoritma olarak kabul görülmüştür. AES algoritmasında birçok kullanım modu bulunmaktadır (Harmankaya ve diğerleri). CCMP içinde kullanılan kullanım modları aşağıdakilerdir;

Sayaç Modu (Counter Mode): Sayaç Modunun amacı, aynı veriyi içeren bloklar aynı şifre ile şifrelendiğinde şifrelerin değiştirilmesinin istenmesidir. Çünkü ayni şifre ile şifrelenirse verinin tekrar eden bloklardan oluştuğu bilinir ve bu da güvenlik açısından istenmeyen bir durumdur. Sayaç madunda şifreleme anahtarının uzunluğu 128 bittir (Reisoğlu, 2008).

Sayaç modunda istediğimiz bir değerle başlayıp, istediğimiz bir değerle artacak bir sayaca ihtiyaç vardır. Örneğin, sayaç 3 değerinden başlar ve her blok için 2 artar. Birbirilerini takip eden mesajlar kendinden sonraki mesaj için başlangıç değeri üretir. Sonuç olarak sayaç modu ile şifrelemede, önce sayaç bir anahtar akışıyla şifrelenir daha sonra 128 bitlik bu AES şifreleme, bloklara ayrılmış 128 bitlik veri ile XOR işlemine girerek şifreli veri elde edilir (Şekil 4.13).



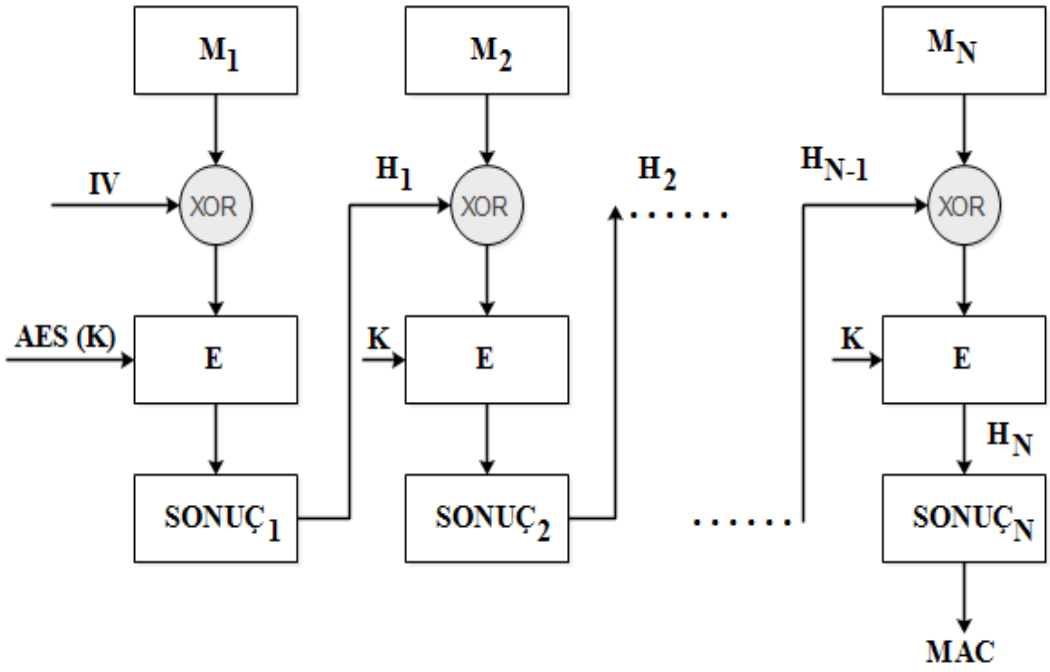
Şekil 4.13 Sayaç Modu ile şifreleme

Zincirleme Blok Şifreleme Mesaj Doğrulama Kodu (CBC-MAC- Cipher Block Chaining Message Authentication Code): Cipher Block Chaining (CBC)-MAC

işleminin amacı veri bütünlüğünü sağlamaktır. CBC, veri bütünlüğünü sağlamak için MIC kullanır. Çünkü MIC'de 1 bit değiştiğinde bile sonuçta çok büyük değişiklikler olur ve saldırganlar tarafından mesaja uygun bir MIC hesaplanması çok zordur.

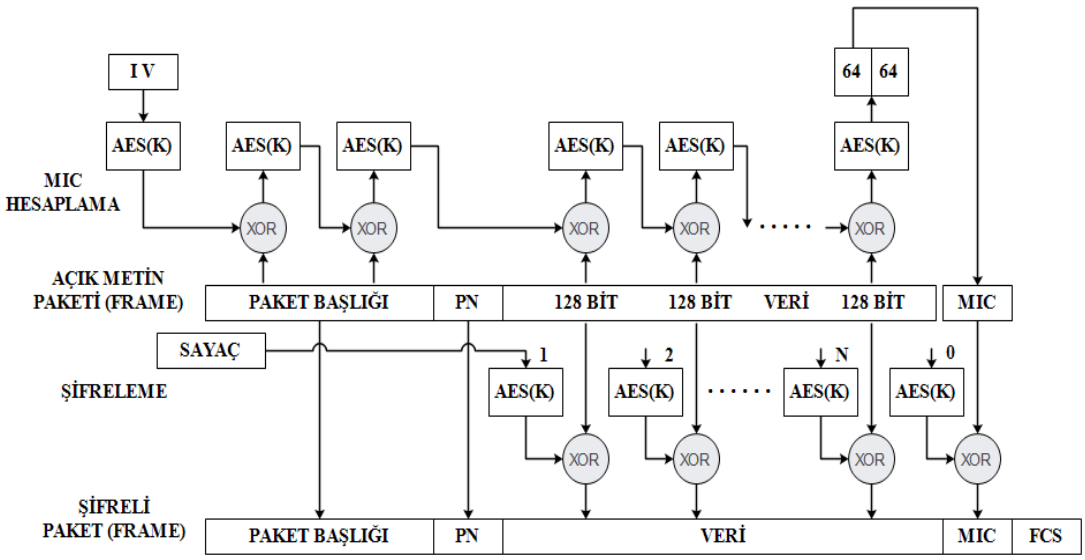
CBC-MAC işleminin çalışma şekli şu şekildedir (Şekil 4.14).

- Mesajın ilk bloğu ile IV XOR işlemine girer ve sonrasında çıktı, AES kullanılarak bir anahtar ile şifrelenir.
- İlk bloktan elde edilen ilk sonuç ikinci blok ile XOR işlemine girer ve daha sonra elde edilen çıktı yine AES ile şifrelenir.
- Elde edilen bu sonuç da, takip eden blokla XOR işlemine tabi tutulur ve çıktısı şifrelenir. Bu işlem son bloğa kadar devam eder ve sonuç olarak son blokta tek blok uzunluğunda şifrelenmiş bir veri elde edilir (Köksal, 2007).



Şekil 4.14 CBC-MAC işleminin çalışma yapısı

CCMP çalışma yapısında, öncelikle CBC-MAC kullanılarak MIC değeri hesaplanır. Sonra sayaçtan bir değer alınır ve AES algoritması ile şifrelenir ve çıkan sonuç mesajın 128 bitlik ilk bloğu ile XOR işlemine girer (Şekil 4.15). Daha sonraki bloklarda sayaç birer arttırılarak elde edilen veriler şifrelenir (Olgun, 2015).



Şekil 4.15 CCMP çalışma yapısı

4.3 Mevcut Saldırı Yöntemleri

Kablosuz ağlara çok çeşitli saldırılar yapılabilir. Bu konudaki sınırsızlık protokollerin çalışmaları incelendiğinde ortaya çıkar. Yapılabilecek saldırıları genel olarak kurum içerisinden ve kurum dışından yapılan saldırılar olarak ikiye ayırabiliriz. Bu iki tip saldırının dinamikleri birbirinden çok farklıdır.

Günümüzde kurumlara karşı yapılan saldırılar sonucunda meydana gelen bilgi sızmaları ve mali kayıpların büyük bir bölümü kurum içinden yapılan saldırılar sonucunda oluşmaktadır. Amerika'da bilgisayar güvenliği kurumu ve FBI'ın (CSI/FBI) 2012 de yaptığı araştırmaya göre Amerika da şirketlere zarar veren elektronik suçların %37 sinin şirket içinden %35 inin şirket sistemlerine daha önce hiç bağlanmamış bir kişi tarafından %28 inin ise kim tarafından yapıldığının anlaşılmadığı tespiti yapılmıştır (Usta, 2015).

Piyasada çok popüler saldırı tipleri olmasına rağmen daha bahsedilmeyen karmaşık sayısız saldırı tipi vardır. Bu tezde seçilen saldırı tipleri görece popüler saldırı tipleridir

4.3.1 Harici ve Dahili saldırılar

Ağ dışında çalışan çalışanlardan ya da ağ dışındaki saldırganlardan gelen saldırılara harici saldırılar denir. Harici saldırganların ağa erişim izni yoktur ve genellikle saldırılarını kablosuz ağlar üzerinden yaparlar. Harici saldırılar çok büyük zararlara

yol açabilir bu yüzden sıkı güvenlik önlemleri alınmalıdır. Şirket içinde çalışanlardan ya da şirket içindeki saldırganlardan gelen saldırılara ise dahili saldırılar denir. Dahili saldırganların ağ üzerinde bulunduğu konuma göre bazı izinleri vardır. Şirketin ilkelerini ve kişilerini çok iyi tanıdığından çalışanların hangi bilgilerinin savunmasız olduğunu ya da hangi bilgilere nasıl ulaşabileceğini çok iyi bilir.

Kurum yerel alan ağından yapılabilecek saldırılar, kuruma dışarıdan yapılabilecek saldırılar ile karşılaştırıldığında, kurum yerel alan ağından yapılan saldırıların çok daha tehlikeli ve etkili olduğu, engellenebilmesi için bilinmesi ve bakılması gereken noktaların sayısının daha fazla olduğu görülmektedir (Usta, 2015).

Dahili saldırılar her zaman saldırganlar tarafından yapılmaz bazen güvenilir bir çalışan bile farkında olmadan ağ için güvenlik tehdidi oluşturabilir. Örneğin, yeterli güvenlik önlemleri alınmayan bir yerel alan ağında bulunan kötü niyetli bir kişi isterse, hedef bir kişinin veya bütün kullanıcıların trafiğini dinleyebilir, kim hangi sitelere giriyor veya maillerinde ne yazıyor görebilir, ağda akan şifreleri ele geçirebilir, istediği kullanıcıların ağ bağlantısını kesebilir, sunuculara erişip verileri çalabilir, bütün ağı çalışmaz duruma getirebilir ve eğer yeterli önlem alınmamışsa kimliğini tamamen gizleyebilir.

Kurum içerisinden gerçekleştirilebilecek çok sayıda saldırı tipi ve bunlar için alınabilecek farklı tip önlemler bulunmaktadır. Saldırılara karşı alınacak etkili tedbirler genelde ya yerel alan ağı yöneticisinin ya da kullanıcıların işlerini zorlaştırıcı etkilere sahiptir. Bu nedenle bu güvenlik tedbirleri uygulanmaya başlandıktan sonra zaman içerisinde yıpranmakta uygulanabilirliğini yitirmektedir. Bazı önlemler ise başlangıçta uygulanabilir ve yönetilebilir iken zaman içerisinde kullanıcı sayısının artması ağ fiziksel yapısının değişmesi gibi etkiler ile yönetilebilirliğini yitirmektedir.

4.3.2 Sosyal Mühendislik saldırısı

Bu tür saldırılarda saldırganlar, teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanları etkileme ve ikna etme yöntemlerini kullanarak insanlardan faydalanırlar. Kısacası, sosyal mühendislik saldırısı insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarına ikna etme sanatıdır. Sosyal mühendislerin en büyük silahı insanların zafiyetlerini kullanmaktır. Bunun birçok yöntemleri vardır. Örneğin, çalışanların kullanıcı şifresini öğrenmek için kendisini sistem görevlisiymiş gibi göstermek, teknisyen ya da çalışan kılığında kurumun içerisine fiziksel olarak

sızmak ve bilgisayar başına geçip o, kullanıcının yetkisi çerçevesinde dosyaları karıştırmak ya da çöp tenekelerini karıştırarak bilgi toplamak gibi farklı yöntemler kullanılır. Her bir kurumda çalışanlara kimliğini kanıtlamayan insanlara güvenmemeleri ve bilgi vermemeleri gerektiğini aktarmalı, gerekli uyarılar yapılmalı ve önlemler alınmalıdır (MEGEP, 2013).

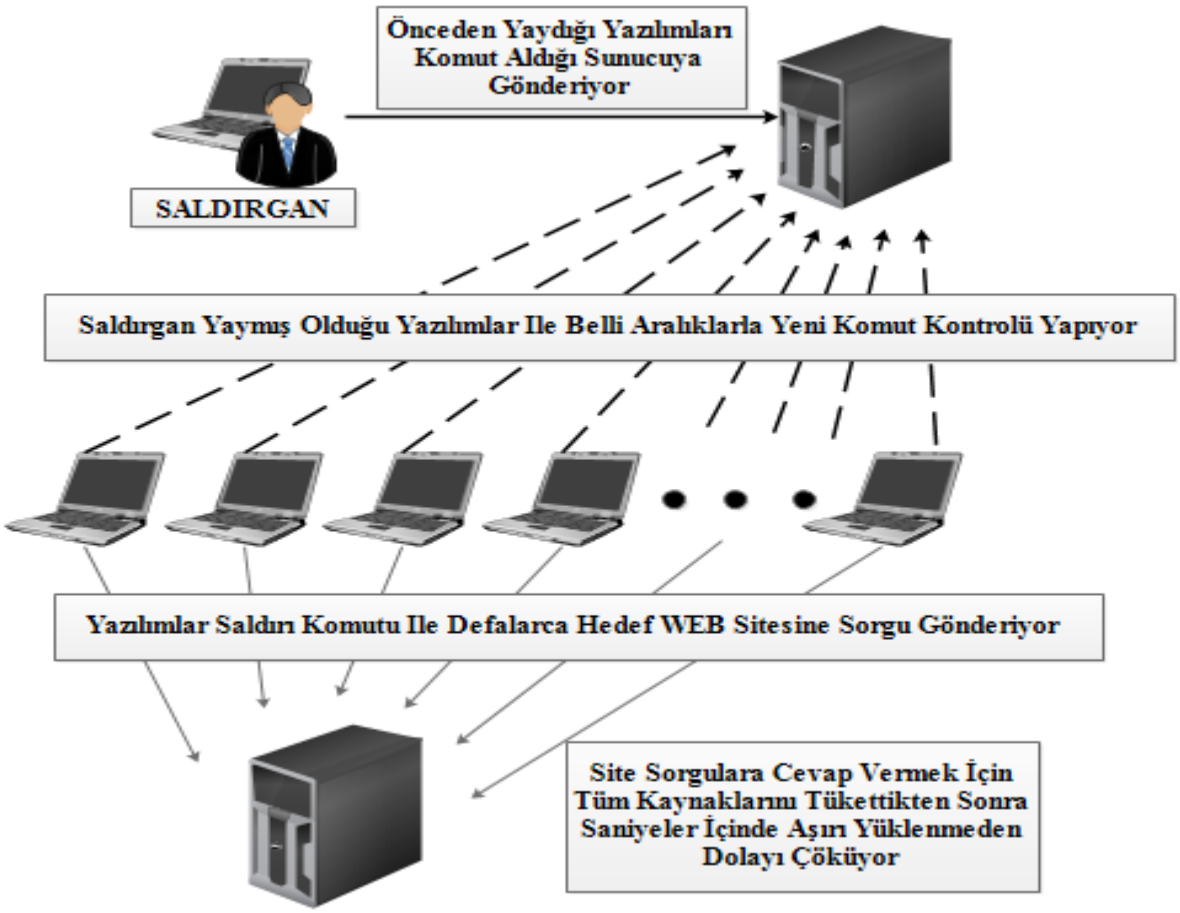
4.3.3 Hizmet Reddi (Denial of Service-DoS) saldırısı

Hizmet reddi saldırısı, hizmeti aksatmaya yönelik bir saldırı çeşididir. DoS saldırısının amacı şifre kırmak veya bilgi çalmak değildir. Bu saldırıların asıl amacı ağ sistemlerine eş zamanlı ve mümkün olduğunca çok sayıda istek göndererek sistem kapasitesinin aşılması durumunda o sistemin, hizmet veremez hale getirilmesidir. Ayrıca DoS saldırılarıyla kurban sisteme ait kaynaklar tüketilerek erişilemez hale getirilebilir. Kaynak tüketimi önemli sunucuların servis vermesini durdurabilir ve buda çok büyük sıkıntılar çıkarabilir (MEGEP, 2013).

Teknik anlamada, DoS saldırısında saldırgan, bilgisayar web sitesine sürekli tekrarlanan istekler gönderir ve sonuçta ana bilgisayarda oluşan aşırı yüklenme hizmete erişimi engeller çünkü bütün kaynaklar saldırgan tarafından tüketilmiştir. Dahası, spam mailler göndermek yoluyla kotaları doldurarak üyelerden gelecek e-posta mesajlarının alınmasını da engelleyebilmektedir.

4.3.4 Dağıtılmış Hizmet Reddi (Distributed Denial of Service–DDoS) saldırısı

DDoS saldırısında DoS saldırısından farklı olarak kurbana tek bir kaynaktan değil de birçok farklı kaynaktan saldırılar yapılır. Bunun sebebi saldırının şiddetini artırmaktır. Saldırganlar tasarladıkları bazı yazılımlarla internet kullanıcılarına virüs bulaştırarak zombi haline getirirler ve bu zombi bilgisayarların yetkilerini ellerine geçirerek hedef sunucu bilgisayarına eş zamanlı ve mümkün olduğunca çok sayıda istek göndermek için kullanırlar. Sonuç olarak sunucunun kapasitesi aşılır ve hizmet veremez hale gelir (Şekil 4.16).



Şekil 4.16 DDoS saldırısının çalışma yapısı

DDoS saldırısını önlemek çok zordur, zira çok sayıda zombi bilgisayarlarla yapılan DDoS saldırılarının bilinen bir yöntemi yoktur. Yüzbinlerce zombi bilgisayardan gelen istekler öncelikle cevaplanmaya çalışılır ve bir süre sonra kapasite aşılarak devre dışı kalır. Saldırılar zombi bilgisayarları üzerinden yapıldığından kaynak saldırgan çoğu zaman tespit edilemiyor. Tam olarak önlenemese bile bazı yöntemlerle DDoS saldırılarının karşısı alınabilir.

DDoS saldırısına maruz kalındığında yapılması gereken, saldırının yapıldığı ip adreslerinden gelen istekleri kabul etmemektir. Ancak, bu yapılırken sistem kapatılmadan açık ve çalışır şekilde kalmasını içerecek yöntemler kullanılmalıdır. Zira sistemin kapatılması zaten saldırganın ana amacıdır.

DDoS saldırılarının karşısını alabilmek için kullanılan yöntemlerden biride, Rate Limit yöntemidir. Bu yöntemin amacı bir hedef bakımından, belli zamanlarda trafik miktarının sınırlandırılmasıdır. Bunun için öncelikle normal zamandaki trafik yoğunluğu tespit edilir ve bu trafiğe uygun bir değer limit olarak kabul edilir. Kabul

edilen limitin üzerindeki trafik kabul edilmez ve DDoS saldırısının sistemi devre dışı bırakması önlenmiş olur.

DDoS saldırılarının karşısını alabilmek için başka bir yöntemde, IP engelleme yöntemidir. Bu yöntemde sisteme erişmesi gereken kaynakların IP adresleri tek tek bilinebilecek durumdaysa, bu IP adreslerinden liste oluşturulur ve bu liste dışındaki bütün IP adresleri engellenir. Böylece, sisteme bilinmeyen IP adresleri üzerinden saldırılar yapılması engellenir (Ural, 2015).

Başka bir yöntemde, saldırı sırasında kullanılan zombi bilgisayarların tehlikeyi fark edip saldırganın bilgisayarına gönderdiği komutları kaldırmasıdır. Ancak birbirinden bağımsız çok sayıda zombi bilgisayarlar kullanıldığından birkaç zombiye uygulanacak bu yöntem yeterli olmamaktadır (MEGEP, 2008).

4.3.5 Deneme Yanılma (Brute Force) saldırısı

Deneme Yanılma saldırılarının amacı, hazırlanmış bir yazılım sayesinde, deneme yanılma işlemlerini yaparak şifreyi çözmektir. Saldırganlar tarafından hazırlanan bu yazılımlar, deneme yanılma işlemlerini önceden belirlenmiş tahmini şifrelerin yer aldığı txt dosyaları sayesinde yaparlar. Bu txt dosyalarına sözlük dosyaları denir.

Deneme yanılma işlemlerini sözlük dosyalarıyla yapılabilindiği gibi tüm şartlar kontrol edilerek de yapılabilir. Yani, şifrenin her karakteri için olabilecek tüm ihtimaller kontrol edilir. Bu yöntemle kırılamayacak şifre yoktur. Ancak, bilgisayar sistemlerinde her bir karakter 8 bitten (11001100) oluşur ve bu 8 bitlik sayının 1'leri ve 0'ları değiştirilerek farklı karakterler oluşturulur. Böylece, deneme yanılma işlemlerini tüm şartlar için kontrol etmek, saniyeler içinde sonuçlanabileceği gibi günler, haftalar, aylar hatta yıllar içerisinde de sonuçlanabilir. Yani tüm şartları kontrol etmek hem maliyetli hem de zaman isteyen bir yöntemdir. Bu yüzden pek kullanılmaz. Genelde deneme yanılma saldırıları daha önceden belirlenmiş yüzlerce, binlerce hatta milyonlarca şifrelerin yer aldığı sözlük dosyaları üzerinden yapılır. Eğer saldırgan şanslıysa doğru şifreyi tutturarak başarıya ulaşır.

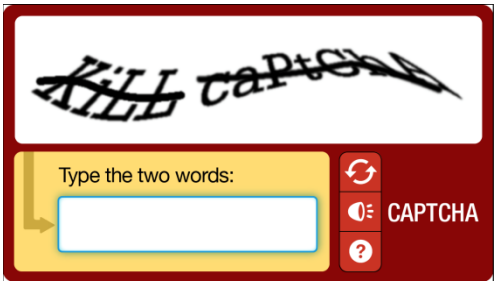
Deneme Yanılma saldırılarından korunmanın yolu bu işlemler sonucunda ele geçirilmesi oldukça zor olan şifreler kullanmaktır. Kullanılan şifrelerin güçlü yani kırılması zor olması için aşağıdaki şartlara dikkat edilmelidir:

- En az 8 karakterli şifre oluşturulmalıdır.

- Şifrelerde harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler kullanılmalıdır (Murt, 2014).
- Büyük ve küçük harfler bir arada kullanılmalıdır.
- Doğum tarihi, isim ve soyisim gibi kişisel bilgiler saldırganlar tarafından çok kolay tahmin edilebilineceği için kullanılmamalıdır.
- Sözlükte bulunabilecek kelimeler şifre olarak kullanılmamalıdır.
- Çoğu kişi tarafından bilinen yöntemlerle geliştirilen şifreler kullanılmamalıdır.

Çoğu kişiye göre bu şartlara uyarak belirlenen şifreleri akılda tutmak zordur. Bu yüzden hem güçlü hem de akılda tutulabilecek bir şifre oluşturmak için günlük hayatımızdan kolayca hatırlayabileceğimiz atasözlerinden, şarkı sözlerinden veya şiirlerden cümleleri kullanabiliriz. Örneğin: 1Env,2Esv. (bir elin nesi var, iki elin sesi var.), B91y11.28'D (ben 1991 yılının 11. ayının 28'inde doğdum) .

Günümüzde deneme yanılma saldırılarının önüne geçebilmek için kayıt formlarının neredeyse hepsinde Captcha kullanılıyor. Captcha'nın kullanılma amacı kayıt yapmak isteyen kişinin robot olmadığını netleştirmektir. Bunun için kullanıcı adı ve şifre ile birlikte toplama, çıkarma işlemlerinin sonuçları, ülkelerin başkentleri ya da yazılan bir metinin aynısının girilmesi isteniyor. Böylece deneme yanılma saldırıları yapan yazılımların denemeler yapmaları engelleniyor (Şekil 4.16).



Şekil 4.17 Captcha örneği

Bunların yanı sıra deneme yanılma saldırıları DoS ve DDoS saldırıları gibi aşırı trafik oluşması sebebiyle veya kullanıcı hesaplarının kilitlenmesiyle hizmet reddine yol açabilir (Murt, 2014).

4.3.6 Kötü niyetli yazılım (Malware) saldırıları

Kötü niyetli yazılımlar, sistemlere sızarak açık yaratma, bilgi hırsızlığı yapma veya açığı olan bir sistemi çökertme gibi birden fazla davranışları kendinde toplayan yazılımlardır. Bu tür yazılımlar genellikle kullanıcıların haberi olmayacak şekilde sistemlere sızarak yerlerini alırlar. Kullanıcılar kötü niyetli yazılımların farkına, bilgisayarlarının hızı düştüğünde, kişisel bilgilerinin değiştiğini fark ettiklerinde veya normal kullandıkları programların artık kullanılamaz duruma geldiklerini gördüklerinde varırlar. Bazı kötü niyetli yazılımların farkına varsak bile bilgisayardan kaldırmak bizi çok zorlayabilir. Bu tür kötü niyetli yazılımların sistemimize bulaşması bize çok ciddi sorunlar çıkarabilir, daha da kötüsü kullanıcıların çoğunluğu olayın ciddiyetini bilmediklerinden, değişikliklere aldırmazlar ve hiçbir önlem almadan bilgisayarlarını kullanmaya devam ederler.

Kötü niyetli yazılımların birçok türü vardır. Aşağıda bu türlerin içerisinde günümüzde en sık rastlananlarına değinilecektir:

4.3.6.1 Casus yazılımları (Spyware)

Casus yazılımlar bilgisayarımıza bizim bilgimiz veya isteğimiz olmadan girip yerleşirler. Casus yazılımlarının amacı, bizi istediği sitelere yönlendirmek, bize istediği dosyaları indirtmek ya da bilgisayarımızdaki bilgilere ulaşmaktır. Daha gelişmiş casus yazılımları, web site şifrelerimizi, kullanıcı adlarımızı, kredi kartları numaralarımızı ya da kişisel bilgilerimizi toplayarak saldırganlara aktarabiliyor.

Casus yazılımlarının bilgisayarımıza bulaşması çok kolaydır ve hatta genellikle dosya veya program indirdiğimizde ya da bir açılır pencereye tıkladığımızda haberimiz olmadan kendi ellerimizle bulaştırıyoruz. Bilgisayarımıza bulaşan bu yazılımlar, bilgisayarımızı yavaşlatabilir ve dahili ayarlarımızı değiştirerek başka saldırılar için zayıf bir ortam yaratabilir. Casus yazılımların çok yaygın olduğu aşağıdaki birkaç istatistikte de görülmektedir (Wikipedia, 2016).

- Geniş bant bağlantısı olan bilgisayarların yaklaşık %90'ında casus yazılım bulunduğu tahmin edilmektedir (Wikipedia, 2016).
- Casus yazılımlar bütün Windows uygulama çökmelerinin üçte birinden sorumludur (Wikipedia, 2016).
- 2003 yılında virüslerin iş dünyasına verdiği zarar yaklaşık 55 milyar ABD $'dır (Wikipedia, 2016).

- 3 milyon işyeri bilgisayarının ele alındığı bir araştırmada, bilgisayarlar üzerinde 83 milyon casus yazılım saptandı (Wikipedia, 2016).

Casus yazılımlar genellikle kaldırılması zor olacak şekilde oluşturulur. Bu yazılımları kaldırmak için Ekle/Kaldır yapmak yeterli değildir. Çünkü bu yazılımlar kaldırılsa bile casuslar içeride kalır ve bilgisayarı yeniden başlattığımızda program yeniden görülebilir. Bu yüzden, çeşitli şirketler casus yazılımlarını ve başka istenmeyen yazılımları aramamıza ve bunları bulduktan sonra kaldırmamıza yardımcı olacak ücretsiz veya ucuz yazılımlar oluşturmaktadır.

Casus yazılımlarından korunmak için aşağıda bazı öneriler verilmiştir;

— İşletim sistemlerimiz güvenlik duvarlarını etkinleştirerek İnternet'e erişmek isteyen programları görüp bloke edebiliriz. Fakat ne güvenlik duvarı nede virüs korunma yazılımları tam olarak casus yazılımlarını engellemek için tam bir çözüm değildir.

— Ücretsiz bir program indirirken "Kabul ediyorum" düğmesine basmadan önce lisans sözleşmesini dikkatlice okumak gerekir. Çünkü bazı lisans sözleşmelerinde bilgilerimiz toplamasına farkında olmadan izin veririz. Bu yüzden casus yazılımları kanundışı değildir. Yetkililer kendilerini direkt olarak: “Bunlar bedava yazılımlar ve kullanıcıyla programcı arasındaki özel bir ikili anlaşmadır” diye savunuyorlar.

— Tıklatılabilir reklamlara karşı dikkatli olmak gerekir. Çünkü bu reklamlara tıkladığımız anda saldırganlar arka planda bizin görmeyeceğimiz bir şekilde casus yazılımlarını bilgisayarımıza yerleştirebilirler veya birileri bizim bu reklamlara nasıl yanıt verdiğimizi izliyor olabilirler.

— Bilgisayarlarımızda virüslere karşı virüs korunma yazılımları kullandığımız gibi casus yazılım önleme (antispyware) ürünleri de güncel şekilde kullanılmalıdır.

Bunların dışında kullanıcılar, casus yazılımlarının sistemlere bulaşma tekniklerini çok iyi bilmelidir. Bilgisayar sisteminin, yama ve güncellemelerle sürekli güncel tutulması ve internet üzerinde bilinmeyen programların indirilip çalıştırılmaması gibi önlemler de casus yazılımlarına karşı korunma sağlayacaktır (Canbek ve Sağıroğlu, 2007).

4.3.6.2 Reklam yazılımları (Adware)

Reklam yazılımlarını basitçe yorumlamak gerekirse üzerinde bulundukları bilgisayarların sahiplerine özel reklamlar göstermek için oluşturulmuş yazılımlardır. Bu tür yazılımların özelliği yazılımların ücretsiz olarak dağıtılması ve yazılımlara gömülen reklamları bize göstermesinden ve bizim de gördüğümüz bu reklamlara tıklamamızdan kazanç sağlamasıdır. Bu tür rahatsız edici yazılımlar aynı zamanda sistemimizdeki kişisel veya istatiksel verilerimizi bizim haberimiz veya iznimiz olmadan üçüncü kişilere aktarabilir.

Reklam yazılımları, bilgisayarlarımıza çoğunlukla ücretsiz paylaşılan programları indirmemizle veya virüslü web sitelerini ziyaret etmemizle bulaşırlar. Bilgisayarlarımızın sistem tarafında programla ilgili bir işaret görünmez hatta program menüsünde dosyaların bilgisayara yüklenmesiyle ilgili hiçbir iz bulunmaz. Bu tür yazılımlar bilgisayarlarımızda yasal nedenlerle de bulunabileceğinden antivirüs programları bizi tam anlamıyla koruyamaz. Bu yüzden casus yazılımlarında olduğu gibi reklam yazılımlarından da korunmak için çeşitli programlar kullanılmalıdır

4.3.6.3 Virüs

Virüs, diğer kötü niyetli yazılımlar gibi bilgisayarlarımıza haberimiz veya iznimiz olmadan bulaşan ve bilgisayarlarımızı çalıştırdığımızda değişik zararlar veren küçük programcıklardır. Virüs yazılımları bilgisayarlarda çok yer kaplamazlar. Virüslerin bulaştığı programlar bir süre normal çalışırlar ama daha sonra kendi kendilerine yeni virüsler üretmeye başlarlar. Virüsler bulaştığı programları kullanılamaz hale getirdiği gibi bilgisayarlarımız da tekrar kullanılamaz hale getirebilirler. Bilgisayar virüslerini, genel olarak dosyalara bulaşan ve bilgisayarın sistem alanlarına bulaşan virüsler olarak iki grupta toplamak mümkün (Canbek ve Sağıroğlu, 2007).

Virüsler, CD, internet, e-posta, disket veya bellek kartlarını kullanarak bilgisayarlarımıza bulaşırlar. Virüs yazarları virüslerin bulaştığı sistemlerde göze çarpmaması için kodlarını kısa tutarlar. Sadece belirlenen şartlardan sonra kendilerini göstermeye başlarlar. Virüsler bulaştığında, programların boyutunda artış olabilir, RAM eksikliği olabilir, bazı programlar RAM'ı daha fazla kullanmaya başlayabilir, bazı programlar çökebilir veya bazı programlarda yavaşlamalar ve kitlenmeler olabilir.

Virüslerden korunmak için mutlaka bir anti-virüs programı yüklenmeli ve güncel tutulmalıdır. Günümüzde var olan en popüler anti-virüs programlarının veri

tabanlarında binlerce virüs ve varyantlarının imzası vardır. Bu veri tabanlarına yeni çıkan virüslerde eklenerek sık sık güncellenir. Anti-virüs programlarının amacı virüsleri arayıp bulmak, bulunan virüsleri temizlemek ve bilgisayarlarda virüslerden korunmak için koruyucu kalkan oluşturmaktır. Virüs kalkanları, bilgisayarımız her açıldığında kendiliğinden devreye girer ve bilgisayara bir şey kopyaladığımızda veya indirdiğimizde bunları kontrol eder ve veri tabanında bulunan virüslere rastladığında bizi uyararak, virüs temizleme modülünü harekete geçirir.

4.3.6.4 Solucan (Worm)

Solucanlar da virüsler gibi sistemimizdeki dosyaları tahrip etmek, bilgisayarlarımızı yavaşlatmak ve bazı programları çökertmek için tasarlanmıştır. Solucanların virüsten farkı kendi başlarına yayılabilmeleridir. Yani bir taşıyıcı dosyaya ihtiyaç duyamadan, ağ bağlantılarını kullanarak otomatik yayılabilirler. Solucanlar sistemimize bulaştıktan sonra kendi başlarına ilerler. Bu da solucanların nasıl tehlikeli olduğunun bir göstergesidir. Örneğin bilgisayarımıza bulaşan bir solucan, e-posta adres defterimizdeki herkese kopyalarını gönderebilir ve aynı şekilde gittiği adreste de bunu yapabilir. Böylece işyeri ağlarını ve internetin tümünü yavaşlatarak web sayfalarının görüntülenmesini uzun süre geciktirebilir (Akçay, 2006).

4.3.6.5 Truva Atı (Trojan)

Truva Atı, programların içine gizlenen ve bilgisayarlarımızın arka planında gizli işlemler yapan bir yazılımdır. Genellikle, e-postaların içine yerleştirilerek kullanıcılara yollanırlar ve kendilerini yükletmek için kullanıcıları, faydalı bir program olduğuna inandırır. İçine saklanıldığı program çalıştırılana kadar aktif duruma geçemezler. Bu tür yazılımlar kendilerinde iki farklı dosya barındırırlar. Bu dosyalardan biri kullanıcıya yollanılan dosyadır. Kullanıcı bu dosyayı çalıştırdığı zaman farkında olmadan saldırgana bilgisayarından bir port açarak erişebilme imkan verir. Saldırgan ikinci dosyayı çalıştırarak kullanıcının bilgisayarına erişim sağlar. Bilgisayarımıza erişim sağlayan saldırgan, bilgisayarımızın içine çok rahatlıkla girebilir, dosyalarımızı açarak içeriğinde istediği değişiklikleri yapabilir, dosyalarımızı silebilir hatta dosyalarımızı kendi bilgisayarına bile kopyalayabilir veya kredi kartı gibi önemli bilgilerimize de erişebilir. Kısacası bizim kendi bilgisayarımızda yapabileceğimiz her şeyi bilgisayarımıza erişen saldırganda yapabilir. Bu yüzden de truva atı yazılımları kullanıcılara virüs ve solucandan daha fazla zarar verebilir. Ayrıca truva atları

sistemimizde bilmediğimiz bir açık port bıraktığından başka kötü niyetli yazılımlar içinde müsait ortam yaratırlar (Şeremet, 2014).

4.3.7 Spam

Spam mesajları, birçok kişiye aynı anda, istekleri olmadan zorla gönderilen reklam içerikli e-posta mesajlarıdır. Spamlar genellikle ticari reklam niteliğindedir ve bu reklamlar çoğunlukla güvenilmeyen ürünlerin duyurulması amacına yöneliktir. Bir iletiyi spam mesaj olarak nitelendirmek için iletide kullanılan başlığın iletinin içeriği ile hiçbir alakası olmaması da yeterlidir. Ayrıca spamlar, e-posta sunucularını ve kısıtlı kullanıcı sistemlerini aşırı yükleyebilen bir ağ tehdididir.

E-posta spam listeleri genellikle grup paylaşımlarının üye listelerinin çalınmasıyla veya web üzerinde paylaşılan adres taranmalarıyla oluşturulur. Spam listelerini oluşturmanın diğer bir yolu da virüsler yoluyla oluşturmaktır. Bilgisayarlarımıza bulaşmış bir virüs adres defterimizdeki adreslere mesajlar göndermekle beraber o e-postaları spamlara kaydeder. Oluşturulan e-posta listelerine mesaj gönderme yöntemlerinden biride e-posta sahibinin bilgisayarını ele geçirmektir. Bu yüzden spamlar virüs, solucan ve truva atı gibi yazılım yöntemlerini kullanır. Denetim altına alınan bu bilgisayarlar daha sonra spam göndermek için kullanılır. Spam, İnternet bant genişliğinin büyük miktarını tüketir ve bugün birçok ülkenin spam kullanımıyla ilgili yasa çıkarmasına neden olacak kadar ciddi bir sorundur (MEGEP, 2013).

Spam yazılımlarından korunmak için aşağıda bazı öneriler verilmiştir;

- E-posta adresimizi tanımadığımız veya güvenmediğimiz web sitelerine veya şirketlere vermemeliyiz.
- Web sayfalarına üye olduğumuzda daima gizlilik politikalarını okumalıyız.
- Asıl iletişimimiz için kullanacağımız e-posta adresimizi genel kullanımlı adresimizden ayrı tutmalıyız.
- İstenmeyen mesajları spam olarak işaretlemeliyiz.
- E-posta adresimizi kişisel web sayfamızda açık bir şekilde paylaşmamalıyız. E-posta adreslerini web sayfalarında gizlemenin birçok yöntemi vardır. Örneğin e-posta adresimizi resim olarak paylaşa biliriz.

Çok sayıda e-posta adreslerinin birlikte ileti yöntemi ile iletişim kurulan ortamlardan uzak durmak veya dikkatli olmak gerekir. Çünkü bu tür ortamlar spam gönderen kişiler için önemli kaynaktır.

4.3.8 Spoofing (Sahte) saldırıları

Spoofing saldırılarını basitçe kaynak yanıltma olarak tanımlayabiliriz. Genellikle hedef üzerinde ek haklar kazanmak için kullanılır. Aynı zamanda kendilerini gizleyerek, saldırı suçunu başka kişilerin veya kurumların üzerine atarlar. Spoofing saldırılarının yapılmasının en sık rastlananlarına tekniklerine bakacak olursak;

4.3.8.1 Sahte MAC (MAC Spoofing, MAC Flooding) atağı

Her bir ethernet anahtar cihazı MAC tablolarında sınırlı sayıda MAC adresi tutabilmektedir. Ethernet anahtarları bir portundan aldığı Ethernet paketini, hafızasında bulunan MAC tablosuna ve konfigürasyona bakarak diğer bir portundan veya portlarından çıkaran cihazlardır. MAC adres tabloları dolan Ethernet anahtarları, modellerine göre farklı şekillerde davranmaya başlarlar. Bazıları öğrenilen yeni MAC adreslerini en yaşlı MAC adresinin üzerine yazarken, bazıları ise yani bir MAC adresi eklemek için eski kayıtların yaşlanma sürelerinin bitmesini beklerler. Fakat her iki durumda da Ethernet anahtarına hafızasında bulunmayan bir MAC adresini hedef alan bir paket gelirse, Ethernet anahtarı bu paketi tüm portlarından gönderir. Bu duruma Bilinmeyen Unicast Taşması (Unknown Unicast Flooding) denir (Usta, 2015).

Ethernet anahtarlarının MAC tablosunu doldurmak için cihazın bir portuna bağlı bilgisayar üzerinde çalışan ve bilgisayarın MAC adresini devamlı bir artırarak paket yollayan bir program yeterlidir. Bu durumu gerçekleştirerek, ethernet anahtarlarının saldırganların istediği gibi davranmasını sağlayan saldırılara MAC flooding atağı denir. MAC flooding atağında hedef bilgisayar diğer bilgisayarlarla konuşmaya devam edeceği için hedef bilgisayarın trafiği elde edilebilir. Fakat ethernet anahtarları üzerinde birden fazla sanal yerel alan ağı (VLAN) varsa saldırgan sadece kendisinin de olduğu VLAN'daki bilgisayarların paketlerini ele geçirebilir.

Sanal yerel alan ağına ait MAC tablosundaki MAC adresleri eşsiz olmalıdır. Bir Mac adresi birden fazla portta görüldüğünde son gelen kayıt geçerli sayılır ve ondan önce gelen kayıt silinir. MAC tablolarının bu özelliğini kullanarak hedef bilgisayarın yerine geçmeye yönelik yapılan saldırılara ise MAC spoofing atağı denir. MAC spoofing

atağına maruz kalmış hedef bilgisayara gidecek tüm talepler saldırgana gider ve bu taleplere saldırganın makinesi cevap verir. MAC spoofing atağının MAC flooding atağından farkı MAC flooding atağında hedef makine diğer makinelerle haberleşmeye devam eder ama MAC spoofing atağında hedef bilgisayarın trafiği ona gönderilen paketler saldırı yapılan porta gönderildiğinden tamamen kesilir.

Yönetilebilir tüm Ethernet anahtar cihazları yani switch'ler bu ataklar sırasında oluşan MAC tablosunun taşması veya bir MAC adresinin birden fazla portta görülmesi gibi durumları önlemek için loglar üretebilir. Örneğin statik olarak bir porttan geçebilecek MAC adresleri sınırlana bilir ya da dinamik MAC kilidi konfigürasyonu ile belli bir kontenjan sayısı kadar bilgisayarın bir porttan geçebilmesine izin verilebilir (Usta, 2015).

4.3.8.2 Sahte ARP (ARP Spoofing) atağı

Aynı sanal yerel alan ağındaki bilgisayarların birbirileriyle iletişim kurabilmeleri için birbirlerinin MAC adreslerini bilmeleri gerekir. Bu yüzden de ağdaki bir bilgisayar, paket göndereceği bilgisayarın MAC adresini öğrenmek adına anahtarlayıcıya ARP isteği (ARP request) gönderir. Anahtarlayıcı gelen paketi tüm portlara yollar fakat yalnızca hedef bilgisayar bu pakete ARP yanıtı (ARP reply) verir. ARP istek paketini yollayan bilgisayar da IP adresi ile MAC adresi arasındaki eşleşmeni kendi ARP tablosuna kaydeder (Usta, 2015).

ARP protokolü kimlik doğrulaması yapmayan kontrolsüz ve zayıf bir süreçtir. Saldırganlar, ARP protokolünün zayıflıklarını kullanarak sahte ARP atağını gerçekleştirirler. Sahte ARP ataklarında saldırgan, hedef bilgisayarın yerine ARP istek paketine cevap verir ve paketi gönderen bilgisayar cevabın hedeften geldiğini kabul ederek, saldırganın MAC adresini kendi ARP tablosuna kaydeder. Bundan sonra hedef bilgisayara gönderilecek paketler artık saldırganın üzerinden geçer ve saldırgan bu trafiği dinleyebilir veya değiştirebilir.

Saldırgan varsayılan ağ geçidinin (default gateway) yerine ARP isteklerine cevap verirse, ağdan çıkan tüm paketler saldırgan tarafından dinlenebilir ve bunun yanı sıra saldırganın bilgisayarının donanım özelliklerine göre ağda performans zayıflıkları olabilir.

ARP saldırısı çok tehlikeli ve önlenmesi zor bir saldırı olmasına rağmen bu kadar kolay gerçekleştirile bilinmesinin nedeni ARP protokolünün, kimlik doğrulama

mekanizmasının olmamasıdır. ARP spoofing ataklarının zayıf tarafı saldırı yapan bilgisayarla izlenen bilgisayarın aynı sanal yerel alan ağlarında bulunması şartıdır. Buda kurum içerisinde çalışanların bilgisayarlarını seviyelerine göre sınıflandırmanın ve bu seviyeler için ayrı sanal yerel alan ağları oluşturmanın ne kadar gerekli olduğunu göstermektedir.

4.3.8.3 Sahte DHCP (DHCP Snooping) atağı

Bilgisayar sayısı 20'yi geçen veya dağınık yapıya sahip bütün yerel alan ağlarında DHCP protokolünün kurulması, yöneticilerin işlerini çok kolaylaştırır. DHCP sunucuları çok basit çalışan programlardır ve kurumsal ağlarda herhangi bir bilgisayar üzerinde kurularak kullanılabilinir. En basit tanımıyla DHCP, yerel ağdaki ister bir bilgisayarın, ister bir yazıcının veya başka bir cihazın ağa bağlanması için gereken IP'leri dağıtır. Yani, DHCP, ağa bağlanmaya çalışan cihazlara otomatik olarak IP adresi verir. Ağa bağlanmak isteyen cihazlara, o anda bir alt ağdan (subnet) veya dağıtım hovuzunda boşta olan bir IP adresini tahsis etmesi kurumsal ağlarda çok avantajlı bir durumdur. Örneğin DHCP olmaksızın, bir şirket içerisinde sık sık yer değiştiren bilgisayarlar veya dizüstü bilgisayarlar her ağa bağlanmak istediklerinde kendilerine çakışmayan bir IP bulmaları gerekirdi. Fakat DHCP böyle bilgisayarlara her açılıp kapatıldığında otomatik bir IP adresi tahsis ederek güvenli bir şekilde ağa bağlanmasını sağlar. DHCP protokolünün en zayıf tarafı güvenlik düşünülmeden ve kimlik doğrulama gibi mekanizmalar kullanılmadan tasarlanmış olmasıdır (Sesli, 2015).

DHCP snooping ataklarında saldırganlar yerel alan ağımızda mevcut olan DHCP servere ek olarak kendi sahte DHCP serverlerini kurarlar ve DHCP'den IP isteğinde bulunan bilgisayarları kendi kurdukları sahte DHCP'ye yönlendirerek, bilgisayarlara, DNS sunucusunun adresini kendi bilgisayarının adresi gibi öğretirler. Böylece, saldırganlar akan trafikteki bilgileri istedikleri gibi toplayıp izleyebilirler. Bunun yanı sıra artık kullanıcı internet tarayıcısına hangi adresi yazarsa yazsın saldırgan onu istediği siteye yönlendirebilir. Örneğin saldırganın duyurduğu DNS sunucusu www.bank.com adresini kendi hazırladığı sahte www.bank.com sitesine yönlendirerek kullanıcının siteye girerken kullandığı kimlik bilgilerini ele geçirebilir.

DHCP snooping görüldüğü üzere çok ciddi bir saldırı türüdür. Bu tür saldırıları engellemek için yönetilebilir switch'ler üzerinden DHCP snooping özelliğini aktif etmek gerekmektedir (Usta, 2015).

DHCP snooping, switch üzerindeki portları Güvenilir (Trusted) ve Güvenilmeyen (Untrusted) olarak gruplama özelliğine sahiptir. DHCP serverimiz hangi portlar üzerinden yayın yapacaksa switch'e öğretilir ve öğretilen yani güvenilir portundan gelen DHCP istekleri incelenerek porttan geçirilir. Güvenilmeyen yani öğretilmeyen porttan gelen istekler ise direk çöpe gönderilir ve atak yapılan port kapatılır. Böylece sahte DHCP ataklarını, switch üzerinden engellemiş oluruz.

4.3.8.4 Sahte DNS (DNS Spoofing) atağı

DNS (Domain Name System), internet ve TCP/IP ağlarında isimleri (Hostname) çözme protokolüdür. Bir DNS server, bilgisayarlar birbirileriyle haberleştiği anda kullandıkları IP adreslerini kayıt altına alır. Kullanıcı bir bilgisayar ismine karşılık gelen IP adresini bulmak istediğinde DNS servere başvurur ve eğer DNS serverin veritabanında öyle bir isim varsa, bu isme karşılık gelen IP adresini kullanıcının bilgisayarına gönderir. Kısacası, bilgisayarlar normalde sayısal bir adres kullanarak iletişim kurarlar. DNS servisi de bu ağ kaynaklarının kullanımını kolaylaştırmak için bir hizmet sağlar. Örneğin bir arkadaşımızın vatandaşlık numarasını öğrenmek yerine ismini öğrenmek daha kolaydır. DNS server bu konuda çok etkili ve profesyonel hizmet sunan bir servistir.

İnternet adresleri ilk önce ülkeler göre ayrılır. Adreslerin sonundaki az, tr, uk gibi ifadeler adresin bulunduğu ülkeyi gösterir. Örneğin az Azerbaycan'ı, tr Türkiye'yi, uk İngiltere'yi gösterir. ABD adresleri için bir ülke takısı kullanılmaz, çünkü DNS'i oluşturan ülke ABD'dir. ABD'ye özel kuruluşlar için us uzantısı oluşturulmuştur. İnternet adresleri ülkelere ayrıldıktan sonra com, edu, gov, gibi daha alt bölümlere ayrılır. Örneğin www.aydın.edu.tr şeklinde oluşur (Bülent Gür, 2015).

Sahte DNS ya da DNS zehirlenmesi olarak Türkçe'ye çevrilen DNS spoofing atağı, DNS sunucusunun veritabanına veri ekleyerek veya oradaki verileri değiştirerek bilgisayarlarımızı yanlış IP adreslerine yönlendirilmesine neden olan saldırılardır. Genellikle de saldırıyı yapan kişi kendi bilgisayarındaki sahte IP'lere yönlendirir. Böyle bir saldırıya uğradığımızda, biz bankadaki hesabımız yerine, saldırganın hazırladığı sahte banka hesabına gideriz ve kendi ellerimizle banka şifrelerimizi

saldırgana veririz. Aynı zamanda saldırgan, bizi yönlendireceği sitede bilgisayarımıza virüsler ve casus yazılımları gibi zararlı yazılımları yükleyerek tüm bilgilerimize sahip olabilir.

DNS zehirlenmesine karşı önlem almak için DNS ön belleğini sık sık temizlemek gerekir. Fakat bu tür saldırılara karşı en etkili çözüm DNSSEC kullanımıdır. DNSSEC, DNS verisinin kaynağını doğrulayan ve veri bütünlüğünü sağlayan yöntemleri içerir. Yani, DNSSEC, yukarıda bahsedilen senaryoları önlemek için birden fazla kimlik kontrol yöntemleri kullanır (Özçelik, 2014).

5 AĞ HARİTASININ TASARLANMASI VE AĞIN KONFİGÜRASYONUNUN YAPILMASI

Yukarıdaki 4 bölümde anlatılan kablosuz yerel alan ağlarının güvenlik ve saldırı yöntemlerinden yola çıkarak 5 katlı bir kurumun yüksek güvenlikli ağ tasarımı yapılacaktır. Tasarım Huawei'in eNSP V1.2.00.380 serili sürümünde yapılacaktır. Özel laboratuvarlarda değil de kendi kişisel bilgisayarımda yapacağım için bazı cihazlar sınırlı seviyede kullanılacaktır. Sınırlı seviyeden kastım girilen konfigürasyonlar doğru olsa bile cihazın gereksinimleri dolayısıyla çalışmaması veya doğru çalıştığının ispatının yapılamamasıdır. Bu yüzden çalışacak kadarının konfigürasyonu yapılacaktır. Bunun yanı sıra eNSP programının simülasyon desteği olmadığından tasarlanan ağın güvenliği komutlar ile kontrol edilecektir.

Güvenlik konusuna girerken iki önemli gerçeğin farkına varmak gerekir. İlki her şeyi koruyamayacağımız ya da her şeyin korunmaya değmeyeceği gerçeğidir. Her şeyin korunması, maddi problemlerin yanında çoğu zaman bazı teknik imkansızlıklara da bağlıdır. İkincisi ise güvenliğin normalde var olan akışa ters hareket eden bir olgu olduğudur. Bu nedenle güvenlik devamlı yıpranmaktadır, devamlı uygulanışının denetlenip kontrol edilmesi gereklidir.

5.1 Tasarım Bileşenleri

Bir ağ tasarlarken öncelikle amaç her türlü şartta çalışmasını sağlamaktır. Bunu sağlamak adına sunucu, switch, firewall vb. ağ bileşenleri üzerinde kümeleme (cluster) yapıları kullanılmalıdır. Her türlü kesinti durumunda ağımızın haberleşmeye devam etmesi için network tarafında ise ring, star, mesh gibi topolojiler kullanılmalıdır. Yapılan yedekli hatların aktif kullanılabilir halde bekletmek, en kısa ve en hızlı yoldan iletişimlerini sağlamak ve rastlanan ağ döngülerini (loop) engellemek adına STP (Spanning Tree Protokolü) protokolünün kullanılmasının büyük faydası vardır. Tasarıma geçmeden önce kullanılacak protokollerden, cihazlardan ve tabii ki de tasarımın yapılacağı programdan bahsetmekte fayda var.

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

STP, 7 seviyeli OSI modelinin L2 (2. katman) seviyesinde yani veri bağlantı katmanında yer alan bir yöntem protokolüdür. En basit tanımıyla STP, karışık ağ yapısını bir ağaç yapısında düzenler ve paketlerin cihazlar arasında sonsuz döngüye girmesine engel olur. Paketlerin döngüye girmelerini engellemek için STP bazı portları kapatır ve iki anahtar cihaz arasında yalnız bir geçerli bağlantının var olmasını sağlar (Usta, 2015).

STP protokolünde konuşan cihazlar birbirleri ile BPDU (Bridge Protocol Data Units) paketleri vasıtasıyla haberleşirler. BPDU paketlerinin içerisinde MAC adresi, port id, root id gibi bilgiler bulunur. STP protokolü kullanılan ağ yapılarında switch'ler birbirilerine her iki saniyede bir BPDU paketi gönderirler ve bridge id'si küçük olan cihaz ortamda Root Bridge olarak seçilir. Bridge id'ler eşit olduğu durumlarda MAC adresi küçük olan cihaz ağ üzerinde root bridge seçilir. Diğer switch'ler root bridge seçilen switch'e en yakın yolu açık tutarlar. Switch'ler bu yakın yolu belirlerken ağ yolunun mesafesine, hop sayısına ve gidilen yolun bant genişliğine bakarlar (Kaya, 2014).

STP protokolünün STP (Spannig Tree Protokol-Kapsayan ağaç protokolü), RSTP (Rapid Spanning Tree Protokol-Hızlı kapsayan ağaç protokolü), MSTP (Multiple Spanning Tree Protocol-Çoklu kapsayan ağaç protokolü) olmak üzere üç çeşidi vardır. Bu protokollerden kısaca bahsetmek gerekirse:

STP'nin geliştirilme amacı L2 seviyesinde oluşan döngüleri engellemektir. STP de root porttan başka diğer portlar bloklanarak bekletilir. Aktif root portta herhangi bir kesinti olması halinde yeniden bir rota hesaplanır ve rota hesaplama süresi ortalama 55 saniyedir (Kaya, 2014).

RSTP'nin geliştirilme amacı STP'nin 55 saniyelik rota hesaplama süresine çözüm bulmaktır. Çünkü bazı yeni kurulan ağlar 55 saniyelik bir süreyi tolere edemiyordu. RSTP de portlar bloklanmak yerine port cost hesabı yapılarak designated durumunda bekletilir. Aktif root portta herhangi bir kesinti olması durumunda designated port devreye girer. Designated portun devreye girme süresi 1 saniye ile maksimum 15 saniye arasında değişir (Kaya, 2014).

MSTP, STP ve RSTP'nin geliştirilmiş halidir. MSTP'nin çalışma mantığı RSTP'le aynıdır fakat MSTP'de switch üzerinde bulunan diğer linkler bloklanmaz ve her

linkten farklı VLAN'lar geçirerek yük dengeleme imkanı sağlar. Çalışan linklerde problem olduğunda ise VLAN'ı diğer linkler üzerine aktarır (Çizelge 5.1).

Çizelge 5.1 STP protokollerinin Port Rolleri

Port Durumu	Durum Açıklaması
Forwarding	Port iletim durumunda, BPDU ve trafiği iletilir.
Learning	Port öğrenme modunda, cihaz kullanıcı trafiğine göre MAC tablosu oluşturur, trafik yoktur.
Listening	Port dinlenme durumunda, Root port, Root Bridge, Designed port seçimi yapmaya çalışıyor.
Blocking	Port engelleme durumunda, BPDU paketlerini alır ve iletir fakat trafiği geçirmez.
Disabled	Port devre dışı durumda, BPDU yada trafik iletilmez.
Discarding	Bloklanan porttur, sadece BPDU paketleri alabilirsiniz.
Root	Root Bridge'ye veri göndermekten sorumlu porttur, cost değeri en düşük olan porttur.
Designated	Switch üzerinde belirlenen portlardan BPDU paketlerini iletir.
Alternate	Başka bir switch üzerinden gönderilen BPDU paketlerini aldıktan sonra, göndermek için alternatif bir port olarak bloke'de bekletilir. Root Bridege'ye yeniden bağlantı için alternatif yoldur.
Backup	Yedek port olarak bekletilir. BPDU paketlerini alır.
Master	MST region içerisinde aldığı BPDU paketlerini Root Bridge'ye gönderir. Root Bridge'e en yakın porttur.
Edge	Portlara doğrudan bağlanan terminal cihazlardır

5.1.2 Router (Yönlendirici)

Router en basit tanımıyla yönlendirme yapan cihazdır veya iki farklı ağı birbirine bağlayarak aralarında köprü görevi yapan cihazdır. Günümüzdeki modemler de bizi internete yönlendirdiği için aslında birer router'dir. ADSL modemler, verileri ses sinyaline, ses sinyallerini verilere çevirerek uzak bilgisayarlarla iletişim kurmamızı sağlarlar, router'lar ise bilgisayarlar arasında sorgulamalar yapıldığında bu sorgulamaların hangi bilgisayara yapıldığını yönlendirilmesini sağlarlar. Router, modem olmadan internet bağlantısı sağlamaz. Şimdiki zamanda internete telefon hattından bağlanıldığı için ve telefon hattı da modeme bağlı olduğu için asıl internet bağlantımız modem sayesindedir (Akmenek, 2013).

Router'lar genelde statik ve dinamik olmak üzere ikiye ayrılır. Statik router'larda yönler elle şekillenir ve hep aynı yön kullanılır. Statik router'lar, dinamik olanlara göre daha güvenlidir. Dinamik routerlarda, rotalar otomatik olarak şekillenir ve veri için en iyi yönü router seçer. Dinamik routerlarda güvenliği arttırmak için elle şekillendirme yapılır (Dikici, 2013).

5.1.3 Hub

Hub'lar bir ağdaki hangi bilgisayarların kendisine bağlı olduğunu bilmeyen, maliyeti düşük akılsız cihazlardır. Akılsız denilmesine sebep, kaynak veya hedef bilgisayara ait bir ağ doğrulaması gerçekleştirmeden, verileri bağlı olduğu tüm bilgisayarlara göndermesidir. Kendisine gelen verinin ne olduğunu anlayarak alıp almama kararını ise bilgisayarlar verir. Bu da network ağını çok yorar ve performans düşüklüğüne sebep olur (Aslantaş, 2013).

Hub'lar özellikleri yüzünden büyük ve karmaşık ağlarda kullanılmazlar fakat ev gibi küçük ağları bulundurabileceğimiz ortamlarda kullanılabilir. Ağda hub'a yazıcı, kamera gibi cihazlar da bağlanabilir. Hub'lara en basit tanımıyla akılsız switch de denmektedir.

Performans düşüklüğüne sebep olması, güvensizliği ve ağı fazladan gereksiz meşgul etmesi göz önüne alınarak bu tasarımda hub cihazı kullanılmayacaktır.

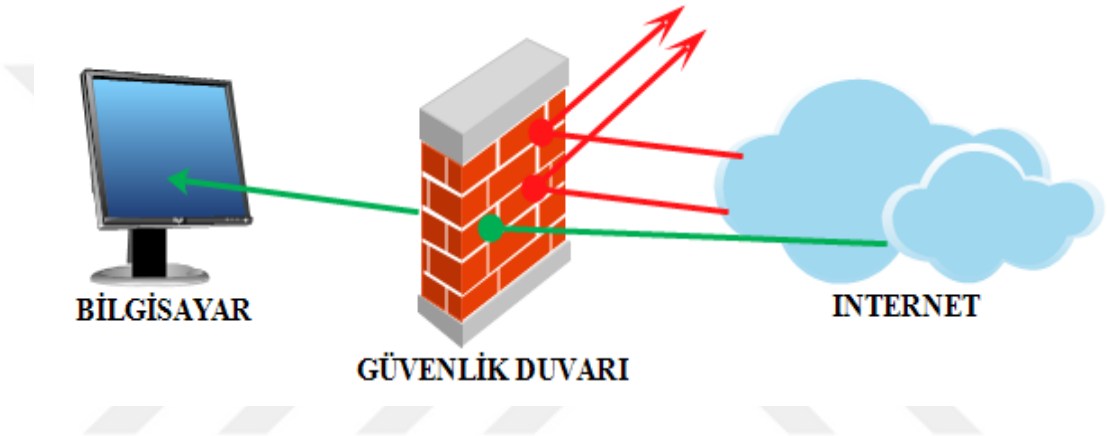
5.1.4 Switch (Anahtar)

Switch'ler hub'larla aynı mantıkla çalışırlar. Fakat switch'ler hub'lardan farklı olarak hangi cihaza ne ileteceğini bilirler. En basit tanımıyla hub'ların akıllı halidir. Akıllı sayılmasına sebep iletim yapacağı cihazların MAC adreslerini veri tabanında tutması ve veri ileteceği zaman direkt hedefe göndere bilmesidir. Yani gereksiz yayın trafiğini engelleyebilir. Bunun yanı sıra kullanıcıya, yönetim panelinde nelerin çalıştığını veya ne olup bittiğini gösterir. Doğal olarak hub'lara göre daha maliyetlidir. Fakat zaman ve performans açısından çok daha avantajlı olduğu için çoğu iş yeri switch kullanır (Aslantaş, 2013).

Bu tasarımda kenar (LSW1, LSW2, LSW3, LSW4, LSW5) ve merkez (BBS1, BBS2) switch'ler kullanılacaktır. Kenar switch, direk olarak bilgisayar ve benzeri cihazların bağlandığı switch'lerdir. Kenar switch tüm ağdan sorumlu olmadığı için, kendi altındaki bağlantıların kontrolünü yapması yeterlidir. Merkez switch, kenar switch'lerle beraber tüm ağı kontrol eden ve kapasitesi kenar switch'lerden çok daha yüksek olan switch'lerdir. Merkez switch ağdaki tüm MAC adreslerini tutar ve gelen paketi hangi kenar switch üzerinden hangi PC'ye gidecekse, uygun olan adrese gönderir.

5.1.5 Firewall (Güvenlik Duvarı)

Güvenlik duvarı, gelen ve giden ağ trafiğini kontrol eden ve ardından güvenlik duvarı ayarlarınıza göre engelleyen veya geçişine izin veren bir yazılım veya donanımdır (Şekil 5.1). Güvenlik duvarı, bilgisayarı saldırganlara karşı gizlemek ve taramak, kötü niyetli internet erişimlerini ve Truva yazılımlarını engellemek, hırsızlığa karşı kişisel verileri korumak, bilgisayar ve ağ için son nokta güvenliğini sağlamak gibi özelliklere sahiptir. Ayrıca, güvenlik duvarı bilgisayarımızın diğer bilgisayarlara zararlı yazılım göndermesine de engel olur (Admin, 2011).



Şekil 5.1 Güvenlik Duvarının çalışma yapısı

5.1.6 VLAN (Virtual Local Area Netwok)

Zamanla ağlar genişledikçe daha da karmaşık bir hal almaya başlamıştır. Birçok kurum ağ yapısını lojik olarak büyütmek için VLAN kullanmaktadır. Temel olarak VLAN diğerlerinden fiziksel yer olarak ayrılmış tekil bir broadcast domain üzerinde bir araya gruplanmış düğümler bütünüdür. VLAN birçok farklı sebeplerden dolayı kullanılabilir, aşağıda bu sebeplerin en önemlilerinden kısaca bahsedilmiştir.

- Güvenlik: Önemli bilgileri barındıran sistemleri birbirlerinde ayırarak olası bir sızma zamanı yapılabilecekleri azaltır.
- Projeler ve özel uygulamalar: Bütün gerekli düğümler bir arada kullanıldığı için proje yönetimini ve özel uygulamaları daha da basitleştirir.
- Performans ve bant genişliği: Ağ trafiğinin performans ve bant genişliği daha dikkatli bir şekilde izlenebilir.

- Yayın ve trafik akışı: Yapılan yayın miktarını otomatik olarak azaltmak için trafik akışının VLAN üyesi olmayan diğere düğümlere geçirmez.
- Departmanlar ve özel iş türleri: Ağı fazlasıyla kullanan departmanlar ayrılabilmek için şirket içindeki farklı departmanlar farklı VLAN'lara kurulur.

Bir switch'te birden fazla VLAN kurula bilindiği gibi bir VLAN da birden fazla switch'e dallanabilir (Turksan, 2009).

5.1.7 eNSP (Enterprise Network Simulation Platform)

Ağ tasarımı yaparken veya ağ sistemleri ile çalışırken yaptıklarımızı test edecek sanal yazılımlara ihtiyaç duyarız. Günümüzde bu ihtiyaçları karşılamak adına bir çok simülatör programı mevcuttur. Simülatör programları kullanmamıza sebep her zaman laboratuvar ortamı oluşturmak imkanımızın olmaması veya yapacağımız iş için laboratuvar ortamına ihtiyaç duyulmaması. Bu simülatör programlarından biride Huawei firmasının geliştirdiği ve ücretsiz olarak kullanıcılarına sunduğu eNSP programıdır. Görsel ara yüzü sayesinde topolojinizi sürükle bırak yöntemiyle rahat bir şekilde oluşturabilirsiniz.

eNSP yazılımında Router, Switch, Access Controller, Access Point, Firewall ve Cloud Engine ürün ailesini bulabilirsiniz. Yazılım gerçek cihazların yazılımları ile aynı özelliklere sahiptir. Her şeyi komut satırı arayüzü üzerinden yönetebiliyorsunuz ama Access control ve firewall'ları komut satırı üzerinden yönetmek sıkıntı çıkarıyor bu yüzden tek eksiği Access Controller ve Firewall için web arayüz bağlantısı yapılamaması diyebiliriz (Savaşal, 2015).

Yazılımı ücretsiz olarak internetten en son sürümünü seçerek indirip kurabilirsiniz. Kurulum esnasında firewallunuz açık olsun ve izin istediğinde gerekli izinleri veriniz. Firewall kapalı iken program kurulduğunda elle tek tek izin açmanız gerekecektir. Bu yazılım kendiyle beraber WinPcap, Wireshark ve Oracle VM VirtualBox yazılımlarını da kuruyor. Bu yazılımların ne işe yaradığını kısaca anlatmak gerekirse;

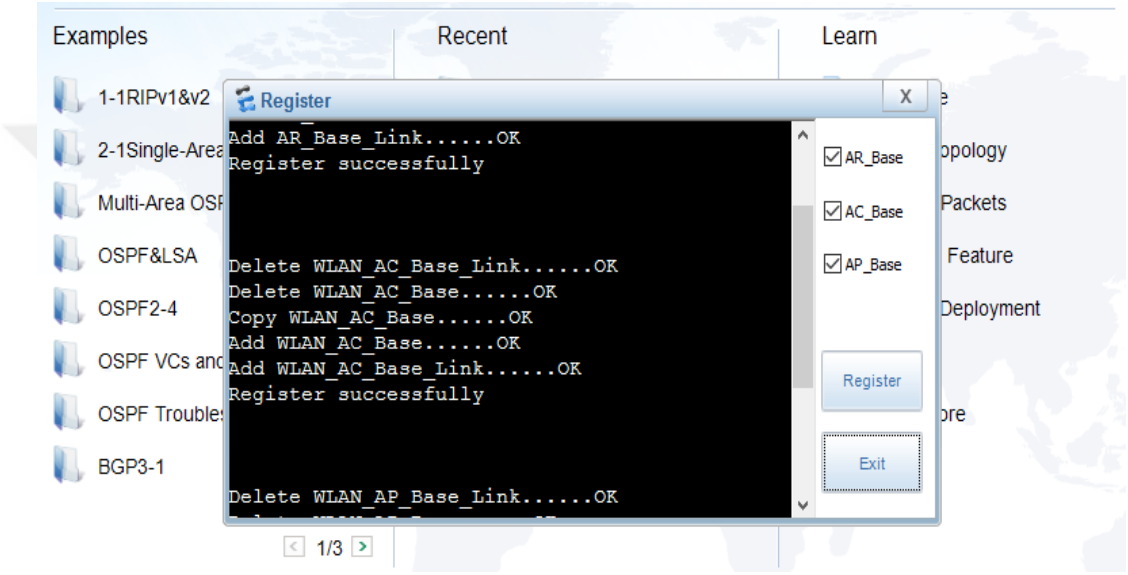
— WinPcap, bağlı olduğunuz ağla ilgili çeşitli verileri analiz etmeye yarayan Wireshark, Nmap, Snort gibi bazı programların çalışması için gereken bir kütüphanedir.

— Wireshark, bilgisayara bağlı olan Ethernet kartlarındaki veya modem kartlarındaki tüm TCP/IP mesajlarını analiz edebilen bir yazılımdır. Wireshark

programı, şebeke problemlerinde sorunu tespit etmek, güvenlik problemlerini kontrol etmek, uygulamaya konan protokollerde oluşan hataları tespit etmek veya onarmak, ağ protokolünün içerisindeki bilgileri öğrenebilmek gibi amaçlar için kullanılır.

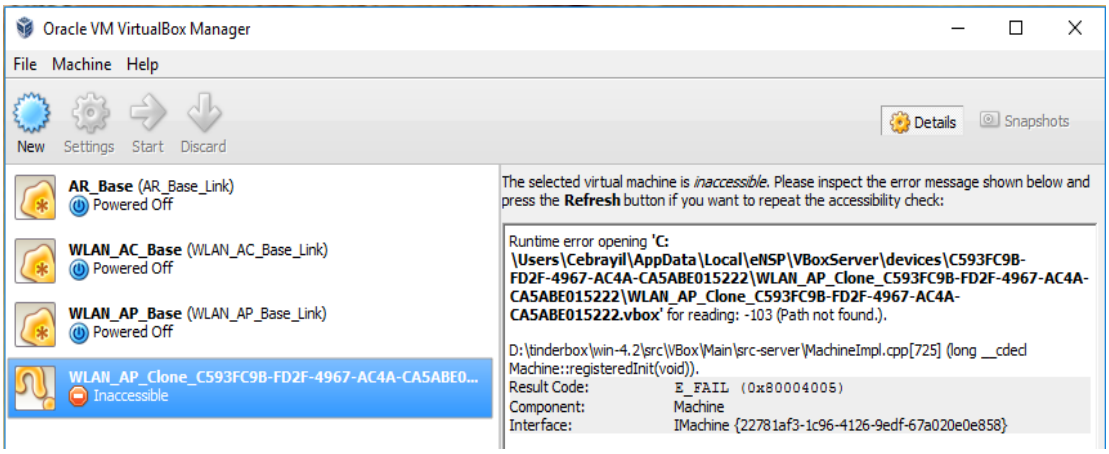
— Oracle VM VirtualBox, işletim sistemi içinde bir veya daha fazla sanal makineler oluşturarak, sistem içinde sanal sistemler oluşturan bir programdır.

Kurulum bittikten sonra programı açın ve hiçbir cihaz eklemeden önce Menu sekmesinden TOOLS sekmesi seçilir ve REGISTER DEVICE sekmesine tıklanır daha sonra tüm cihazlar seçilip register butonuna tıklanmalı (Şekil 5.2).



Şekil 5.2 Register işleminin tamamlanması

Şekil 5.2'deki gibi register successfully yani kayıt işlemi başarılı yazısını gördükten sonra artık eNSP'yi kullanabilirsiniz. Fakat cihazları çalıştırırken yine hata alırsanız, eNSP programını kapatıp Oracle VM VirtualBox yazılımını açın ve BASE olmayan örneğin, WLAN_AP_Clone_XXXXXXXX gibi gözüken sanal makinaları silin (Şekil 5.3). Daha sonra Virtual Box'u kapatıp eNSP programını çalıştırın ve yeniden Register Device sekmesini tıklayıp register successfully yazısını görmeyi bekleyin (Savaşal, 2015).



Şekil 5.3 BASE oturmamış sanal makine

5.1.8 OSPF (Open Shortest Path First - İlk Açık Yöne Öncelik) Protokolü

OSPF Protokolü, tasarlanan büyük ağlarda kullanılan ve sınırsız hop atlayan bir Link State (Hata Durumu) protokolüdür. Bu protokol Dijkstra algoritmasını kullanarak hedefe gidecek en kısa yolu hesaplayıp bulmaya çalışır. OSPF, enable router'lara her 10 saniyede bir Hello paketi göndererek komşularını keşfeder ve OSPF Veritabanını oluşturur. Ağdaki tüm yolların bilgisine ulaştıktan sonra SPF algoritmalarını kullanarak en kısa ve en iyi yolun hangisi olduğuna karar verir. Link-state Refresh protokolü sayesinde 30 dakikadan bir periyodik güncellemeler göndererek ağ değişikliklerinden tüm router'ları haberdar ediyor (Baydar, 2013).

OSPF, büyük ve karmaşık ağlarda yol bilgisini çabuk ve iyi öğrenme, iyi çalışabilme ve güvenlik konularında daha başarılıdır.

5.1.9 SSH ve Telnet bağlantısı

SSH ve Telnet internet ağı üzerinde bulunan sunucudan uzaktaki başka bir sunucuya bağlanmak için geliştirilen bağlantı programlarıdır. Bağlantı yapıldıktan sonra sanki o makinenin karşısında oturuyormuş gibi komutlar yazılabilir veya programlar çalıştırılabilir. SSH açık haliyle Secure Shell yani Güvenli Kabuk anlamını veriyor. Telnet ise güvensiz bir protokoldür. Çünkü kullanıcı adınız ve şifrenizle bağlı bulunduğunuz ağda veriler Plain Text yani düz metin olarak gönderilmektedir. SSH'nın Telnet gibi bağlantı protokollerinden farkı sunucu arasındaki iletişimi kriptografik şifreleme sistemiyle anlaşılmaz bir hale dönüştürerek bilgileri şifrelemesidir. Uzaktaki bilgisayarlara SSH bağlantısı yapılması için şifreleme ve

doğrulama algoritmaları kullanılmaktadır. SSH sunucusu default olarak 22, Telnet ise default olarak 23 numaralı portları kullanırlar (Dündar, 2010).

5.1.10 ACL (Access Control List)

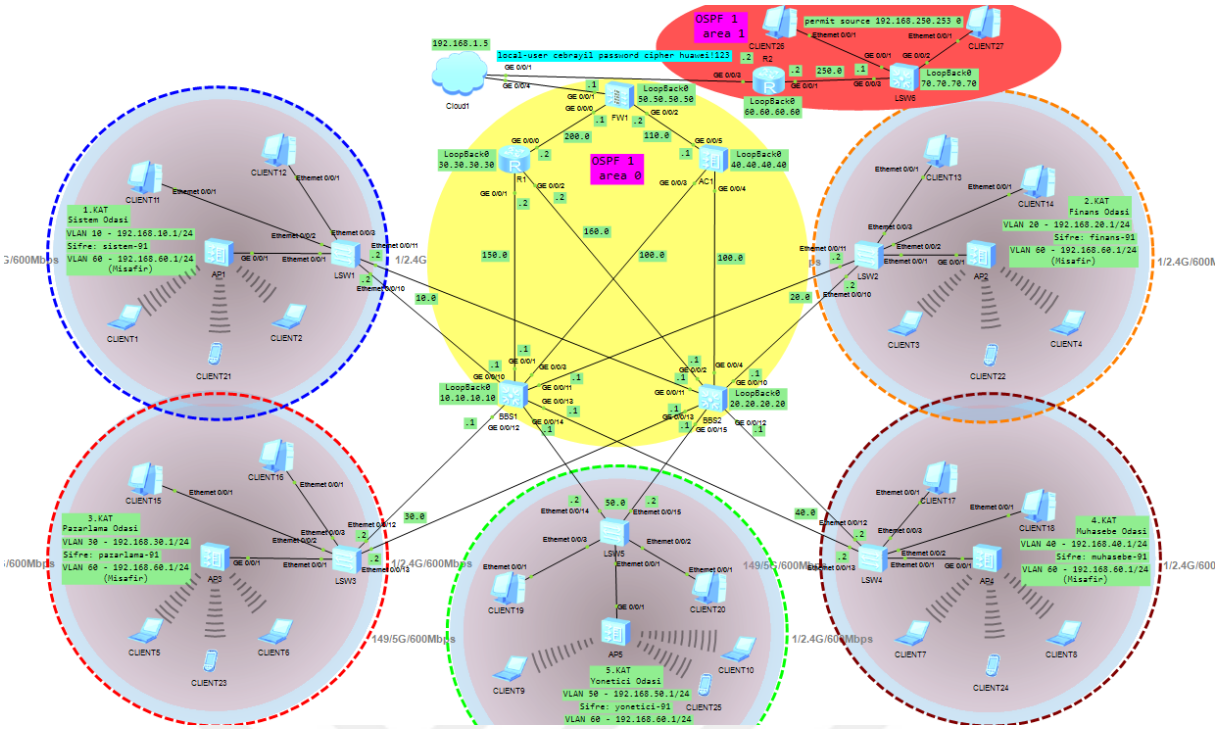
ACL, farklı networkler üzerinde gelen ve giden iletişim trafiğini kaynak ip bazında ya da port bazında filtreleme yapmayı sağlayan kontrol mekanizmasıdır. ACL kuralları sayesinde kaynak ip filtrelemesi yapmakla beraber gelişmiş listeler yaparak hedef ip, port numarası ve protokol bazında filtreleme işlemleri yapabilmekteyiz. ACL kural listeleri oluşturulurken aşağıdaki parametreler kullanılır:

- Access list numarası: 2000 – 2999 (Temel erişim), 3000 – 3999 (Gelişmiş erişim), 4000 - 4999 veya 6000 - 6999 arasında bir numara seçilmelidir.
- Deny: Yasaklamak için kullanılır
- Permit: İzin vermek için kullanılır
- Source IP: Kaynak ip adresi
- Destination IP: Hedef ip adresi
- Wildcard Mask: Kaynak veya hedef ip adresinin subnet maskesinin tam tersi olarak yazılması gereken değerdir.

5.2 Ağ Haritası

Tasarım bileşenleri başlığı altında bahsedilen cihazlardan ve protokollerden yola çıkarak 5 katlı bir ofis için yüksek güvenlikli Kablosuz ve Kablolu Yerel Alan Ağı haritasının tasarımı yapılacaktır.

Bu tez çalışmasında konfigürasyonu yapılacak Yerel Alan Ağının ağ haritasının tasarımı aşağıdadır;



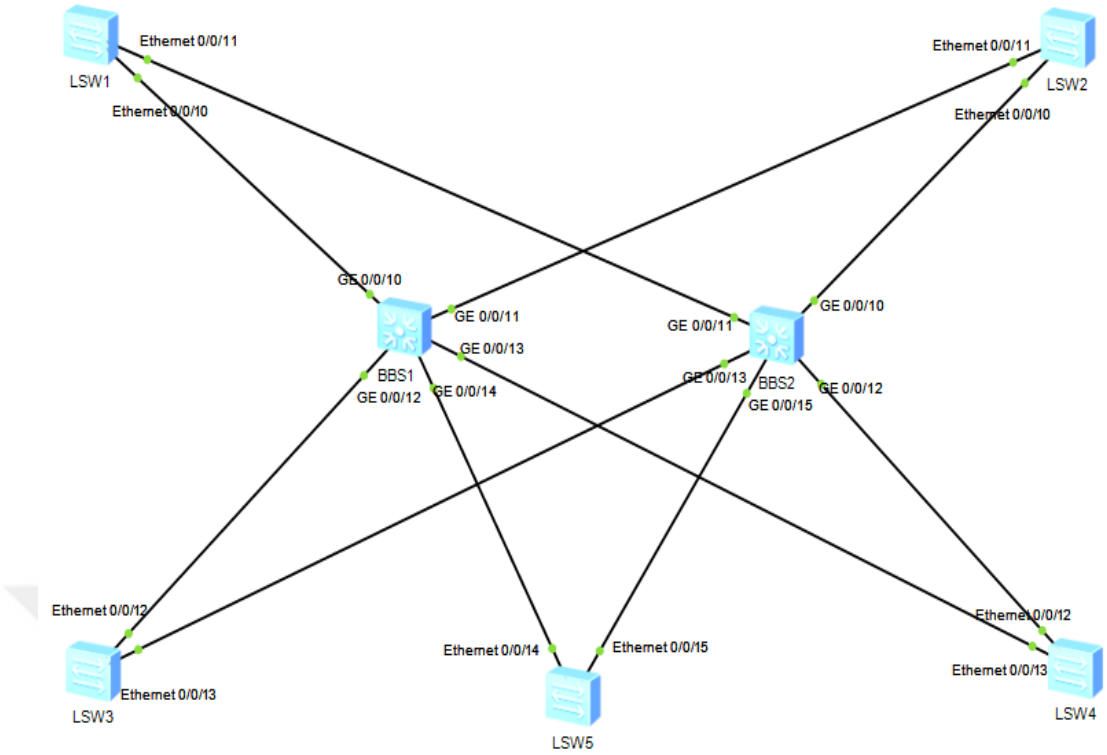
Şekil 5.4 Ağ haritası

Tasarımda 3 adet merkez switch, 5 adet kenar switch, 12 adet kablolu bilgisayarı, 10 adet dizüstü bilgisayar, 5 adet cep telefonu, 2 adet router, 5 adet Access Point, 1 adet Firewall ve 1 adet Cloud kullanılmıştır. Bu cihazların görevlerinin ne olduğu ve güvenlikleri açısından neler yapılması gerektiği konfigürasyonları yapıldıkça anlatılacaktır.

5.3 Ağın Konfigürasyonu

5.3.1 Birinci kısım

Tasarımın ilk kısmında merkez ve kenar switch'ler ağ haritasında gösterildiği gibi yerleştirilecek ve isimleri verilecektir. Daha sonra yukarıda da belirtildiği sebeplerden dolayı switch'lere MSTP protokolü uygulanacaktır. Bu protokolün konfigürasyonu yapılırken, STP protokolüne yapılan saldırılardan ve bu saldırılara karşı alınabilecek önlemlerden de bahsedilecektir ve bahsedilen önlemler göz önüne alınarak cihazların konfigürasyonları yapılacaktır (Şekil 5.5).



Şekil 5.5 MSTP protokolünün uygulanacağı switch'lerin haritası

— Öncelikle VLAN'lar ve MSTP protokolünü oluşturulacak ve MSTP protokolü aktif duruma getirilecektir. Sonra BBS1 switch'ine atanan instance değerlerinin öncelik sırası belirlenecektir. Instance 1'i root primary yapmakta amaç BBS1 switch'ini instance 1 VLAN'ları için devreye giren ilk switch olarak belirlemektir. Aynı şekilde instance 2'yi root secondary yapmakta amaç instance 2 VLAN'ları için BBS1 switch'ini ikincil switch olarak belirlemektir.

— Switch kendisinde bulunan bağlantıda hata tespit ederse root porta TCN (Topology Change Notification) gönderir. TCN mesajını alan switch'ler mevcut MAC tablolarını yeniler ve toplamda 2'şer dakika kesintilerle tekrar tekrar yeniden hesaplamalar yaparak ağı kullanılamaz hale getirebilir. Bu tür atakları engellemek adına Tc Protection özelliğini ağımıza bağlı olan tüm switch'ler üzerinde etkinleştirmemiz gerekmektedir. Tc Protection özelliğini kullandığınızda saldırı yapan MAC adres ve ARP kayıtlarını silerek tekrar tekrar MAC adresi girişini engeller (Kaya, 2014).

— STP protokolünde aldığımız daha düşük bridge ID'li BPDU paketleri ağda kullanılan Root Bridge'yi değiştirir. Sonuç olarak, paket kendi iletim yolunu bırakarak kendisine daha uzak ve performans bakımından daha kötü olan root bridge üzerinden

iletişim kurmaya devam eder ve bu durumdan ağımızın performansı olumsuz etkilenir. Ayrıca saldırı sonucu root bridge olan switch'in enerjisinde kesintiler yaparak ağımızı tekrar tekrar root bridge seçimine zorlayabilirler. Bu durum hedefe gitmeyen paketler anlamına gelir. Bu tür durumları engellemek adına ağımızda bulunan primary ve secondary root bridge durumundaki switch'lerin portlarına root-protection fonksiyonun eklenmesi gerekir (Kaya, 2014).

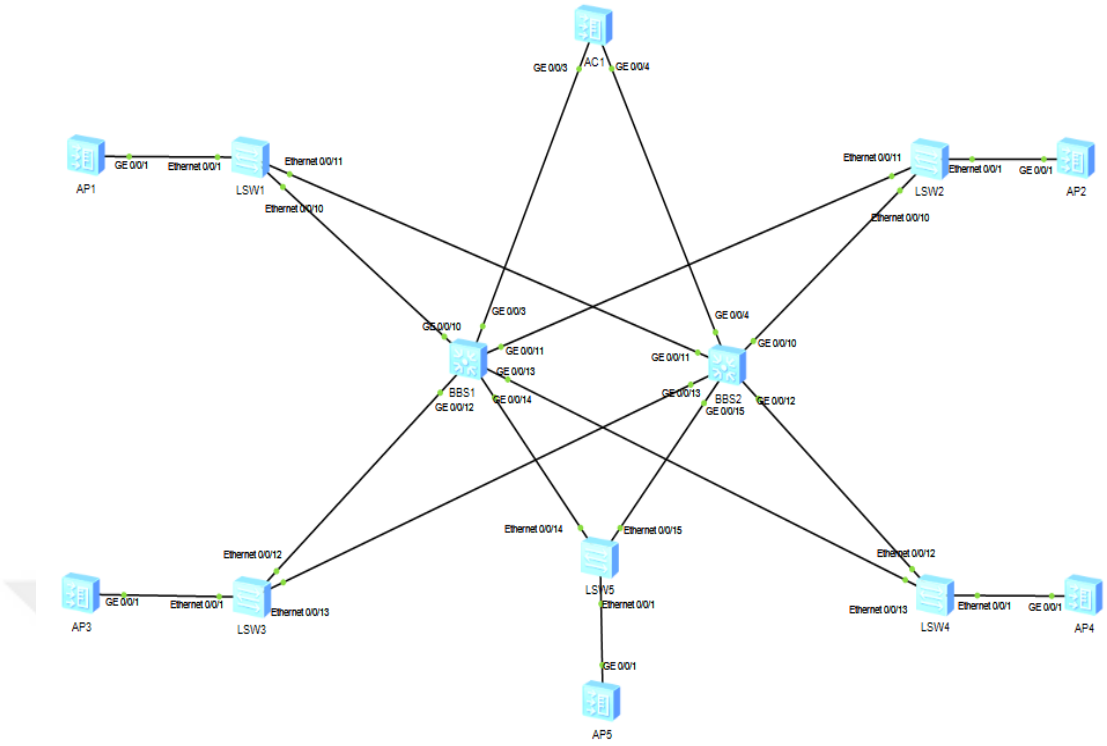
— BBS1 switch'inde yaptığımız konfigürasyonların aynısı BBS2 switch'inde de yapmamız gerekir. Fakat BBS1 ve BBS2 swith'lerini kenar switch'lere bağlayan portların numaralarına dikkat etmemiz gerekir. Ayrıca BBS2 switch'inde root primary olarak instance 2'i atanacaktır ve böylece BBS2 yedek switch olarak hazır durumda bekletilecektir. BBS1 switch'inde veya her hangi bir portunda sorun çıktığı zaman BBS2'i veya BBS2'inin sorun çıkan porta denk gelen yedekli portu devreye girecektir.

— LSW1, LSW2, LSW3, LSW4, LSW5 kenar switch'lerinde de BBS1 ve BBS2 de olduğu gibi öncelikle VLAN'lar oluşturulacak ve daha sonra MSTP protokolü uygulanacaktır.

— STP protokolü BPDU mesajını alamadığı durumlarda ağ içerisindeki kenar switch'ler alternate durumunda bulunan portunu açarak designated durumunu getirir ve sonuç olarak ağımız sonsuz döngüye girer. Bu tür durumları engellemek adına loop-protection fonksiyonu geliştirilmiştir. Loop protection fonksiyonu STP yapısında root ve alternate portlarında aktif edilecektir (Kaya, 2014).

5.3.2 İkinci kısım

Tasarımın ikinci kısmında merkez switch'lere bir tane AC (Access Controller) ve her kattaki kenar switch'lere birer tane AP eklenerek yayın yapmaları sağlanacaktır. Güvenlik açısından yapılması gerekenler tasarım yapıldıkça anlatılacak ve ona göre tasarım yapılacaktır (Şekil 5.6).



Şekil 5.6 AP'lerin eklenmiş durumu

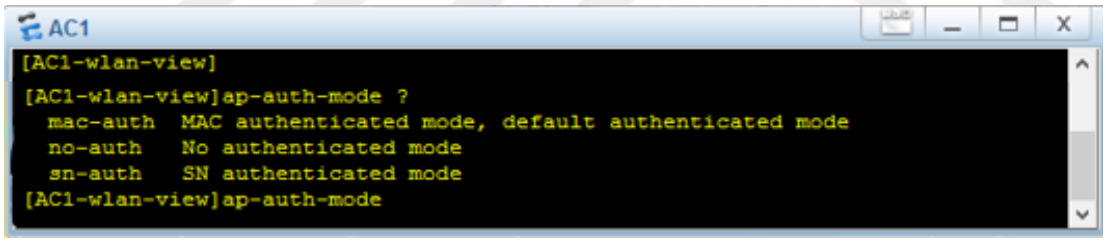
— Öncelikle merkez switch'leri AC1 ve kenar switch'leri AP'lere bağlayacak portların konfigürasyonları girilecektir. Daha sonra AC1 cihazında yayının yapılaması için gerekli konfigürasyonlar yapılacaktır.

— 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. AP'lere bu değerleri atamak için normalde Router cihazı kullanılır fakat bu tasarımda Router'da fazladan yük trafiği oluşmaması adına AC cihazından yayın yaptırılarak BBS1 ve BBS2 merkez switch'lerinden IP adresi atamaları yaptırılacaktır. Öncelikle AC1'e MSTP protokolünü kullandığımızı iletmek gerekir yani MSTP protokolünü AC cihazına uygulamamız ilk şarttır. Yoksa AC1'i merkez switc'lere bağlayan portlar loop'a girecektir (Huawei, 2014).

— IP dağıtımı BBS1 ve BBS2 merkez switch'lerinden yapılacağı için öncelikle merkez switch'lerde DHCP serveri aktif hale getirilecektir daha sonra hangi katta hangi VLAN'dan ve hangi ip adresleri dağıtılacağı girilecektir. Son olarak ise DNS server IP'si (8.8.8.8) girilecektir.

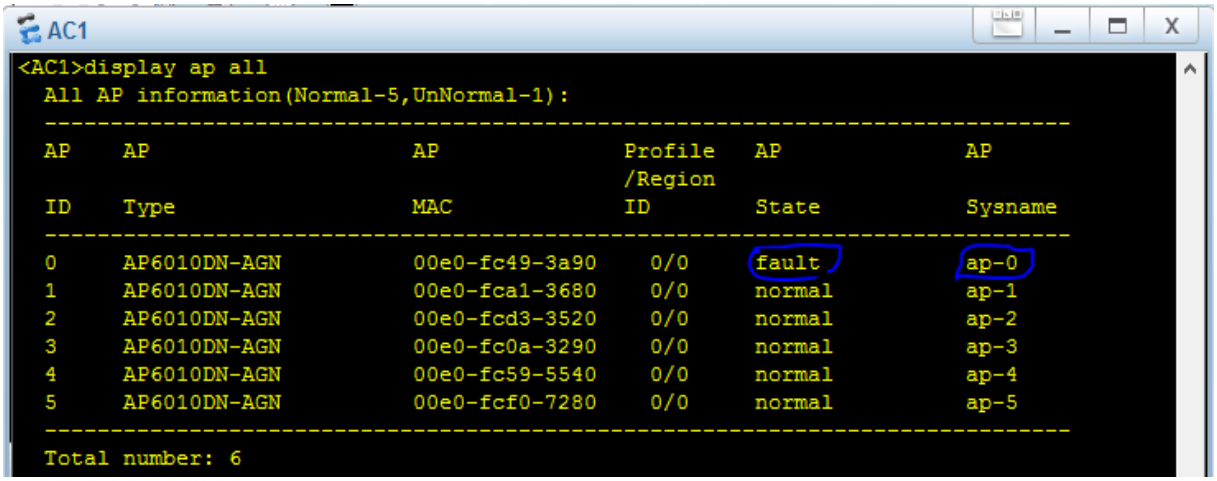
— Varsayılan giriş (Default gateway) olarak VLAN'lara girdiğimiz IP'lerin atanması için her bir VLAN'a dhcp select interface komutunu girmek yeterlidir. Bu özellik sadece Huawei cihazlarında vardır. Ayrıca Huawei cihazlarında DHCP server IP dağıtımına sonuncu IP'den başlar. Örneğin VLAN 10'dan bağlanan cihazlara DHCP server, 192.168.10.254'ten başlayarak IP dağıtmaya başlayacaktır.

— Kenar switch'leri AP'lere bağlayan portlara default vlan 100 girildiğinden dolayı AC1'in ağdaki AP'leri tanımaları veya AP'lerin AC1'e atanması için öncelikle "wlan ac source interface vlanif100" komutu daha sonra ise "ap-auth-mode no-auth" komutu girilecektir. Aşağıda da görüldüğü üzere no-auth değil de mac-auth veya sn-auth da girilebilirdi. Fakat mac-auth gireceğimiz taktirde ağımıza bağlayacağımız AP'lerin MAC adreslerini bilmemiz ve elle girmemiz gerekecekti ve ayni şekilde sn-auth komutunu gireceğimiz zaman da AP'lerin seri numaralarını teker teker elle girmemiz gerekecekti. No-auth komutu girilerek, hiçbir işlem gerekmeden AC1'in ağımızdaki AP'leri tanıması sağlanmıştır. Son olarak "commit all" komutuyla şimdiye kadar yapılanlar AC1'in üzerine atanmıştır. Bazen bu komutu kullanmadığımız takdirde AP'lerin tanınmasında sıkıntı çıkabiliyor. AP'lerin tanınma süresinin yaklaşık olarak 3-4 dakika sürebilme ihtimali vardır (Huawei, 2014).



Şekil 5.7 AP'leri tanıtma çeşitleri

— Display ap all komutuyla AP'lerin oturup oturmadığı kontrol edilir (Şekil 5.8).



Şekil 5.8 AP'lerin AC1 tarafından tanınması

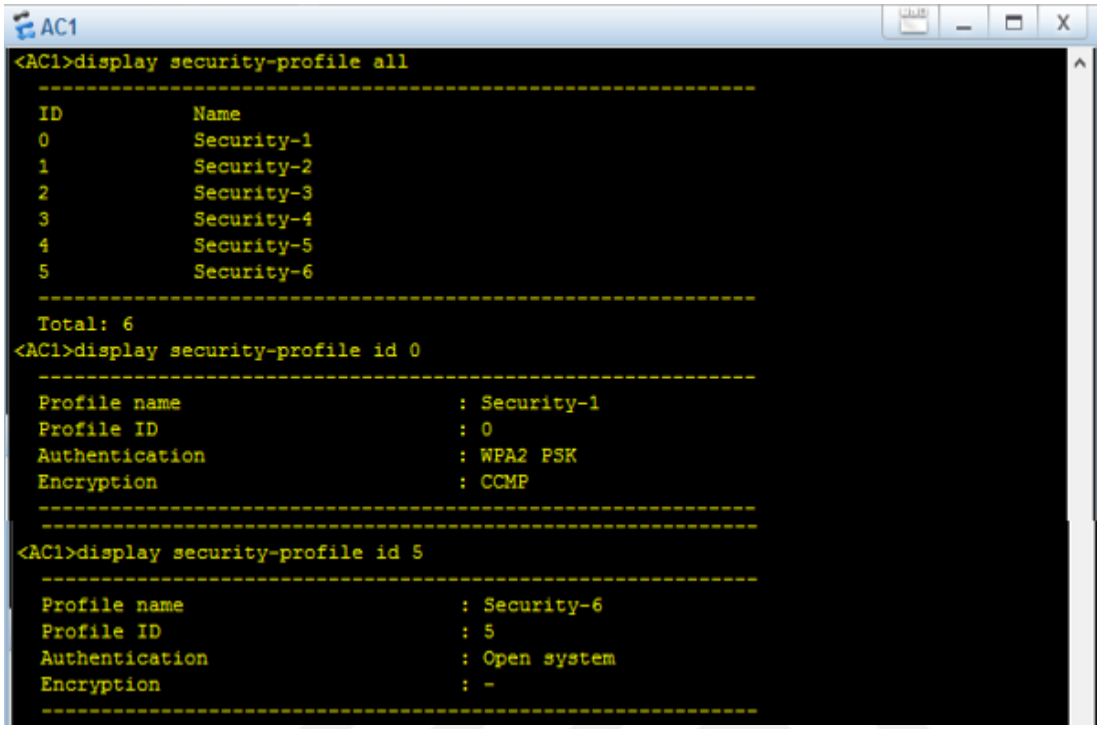
— Şekil 5.8'de görüldüğü üzere 5 adet AP kullanacağımıza rağmen 6 adet AP tanıtılmıştır. Buna sebep AP numaralarının (ap-1, ap-2, ap-3, ap-4, ap-5) tasarlanacak 5 katlı ofisin kat numaralarıyla aynı olmasını ayarlamaktır.

— AP'ler doğru bir şekilde tanıtıldıktan sonra AP'lerin yayın yapmasını yapmasını sağlayacak yapılandırma yapılacaktır. Bir AP'nin yayın yapması için sırasıyla WMM profili, radio profili, WLAN-Ess'i, traffic profili ve security profili oluşturulmak zorundadır. WMM (Wireless Multi Media) teknolojisi, ağ üzerinde audio, video ve ses uygulamalarına öncelik tanıyarak diğer uygulamaların veya trafiğin bu uygulamaları yavaşlatma ihtimalini en az indirir. Sadece audio, video ve ses uygulamalarını değil, herhangi bir trafiğe düşük veya yüksek öncelik verebilme özelliğine de sahiptir. WMM, diğer WMM donanımları ile daha iyi çalıştığından dolayı, sistemi oluşturan her bir parçanın WMM uyumlu olması toplam sistem performansını artıracaktır (Huawei, 2012).

— Bu çalışmada iki tip yayın yapılacağı için iki adet radio profili oluşturulacaktır. Yayın tipleri 802.11bgn (2.4Ghz) ve 802.11an (5Ghz) olarak ayarlanıp, VMM profiline atanacaktır. WMM profiline verilen ismi her defasında yazmamak için id değerini 0 (sıfır) yazmakta yeterlidir. Çünkü program kendisi id 0 değerini gördüğünde bunun yapılan ilk WMM profili olduğunu anlayabiliyor (Huawei, 2012).

— Oluşturulan radio profilleri AP'lere atanacak, WLAN-Ess'ler, traffic profilleri ve security profilleri oluşturulacaktır. Security profilleri oluşturulurken

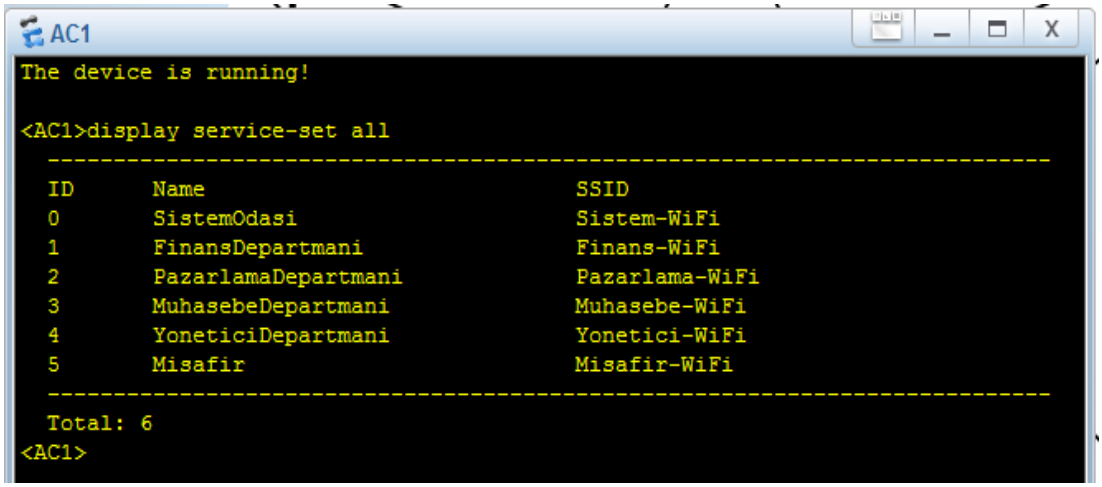
güvenlik bölümünde anlatılan güvenlik yöntemlerine dikkat edilmesi gerekir (Şekil 5.9).



Şekil 5.9 Security profillerinin görüntülenmesi

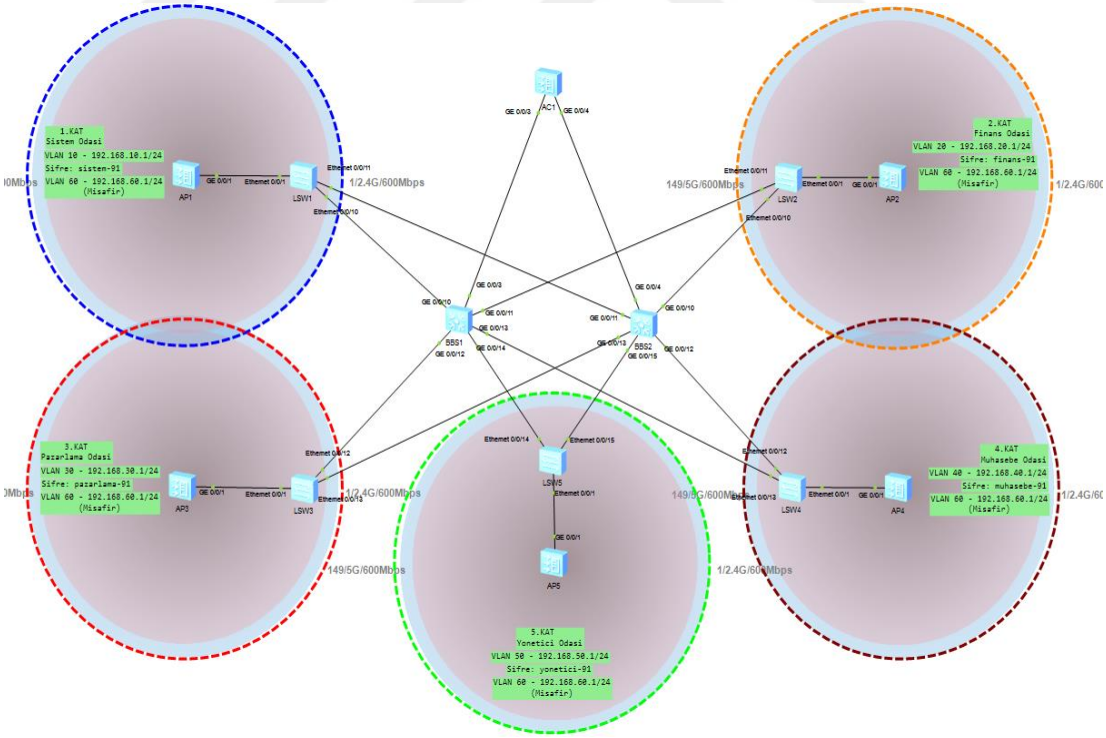
— Şekil 5.8'de görüldüğü üzere 6 adet security profili oluşturulmuştur. Bunlardan ilk 5'i katlarda çalışanların yayınında kullanılacağı için şifreli sonuncusu ise misafirlerin yayınında kullanılacağı için şifresiz olarak oluşturulmuştur.

— Bir sistemin çalışması için gerekli olan wmm-profile, radio-profile, traffic profile ve security-profile oluşturuldu. Son olarak oluşturulan profillerin hangisinin hangi kata ait olduğu, hangi isimle ve hangi VLAN'la yayın yapacağı konfigürasyonları yapılacaktır. Yani service-set'leri oluşturulacaktır. (Şekil 5.10)



Şekil 5.10 Service setlerinin görüntülenmesi

— AP'lerin yayının yapması için son olarak yapılması gereken, hangi AP'nin hangi service set'inden yani hangi kattan yayın yapacağını ayarlamak. En sonda "commit all" komutuyla WLAN adına yapılanların tümünü programın algılamasını sağlarız. Yaklaşık olarak 1-2 dakika bekledikten sonra AP'ler yapılan konfigürasyonları algılayarak yayın yapmaya başlar (Şekil 5.11).

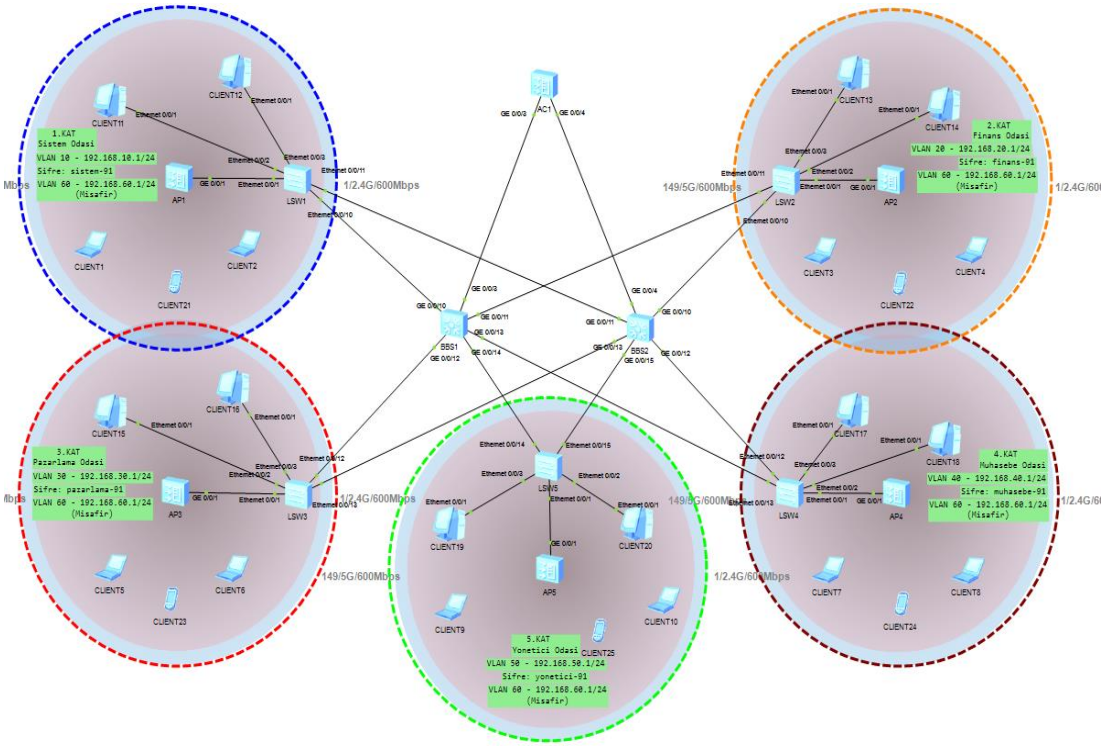


Şekil 5.11 AP'lerin yayın yapması

5.3.3 Üçüncü kısım

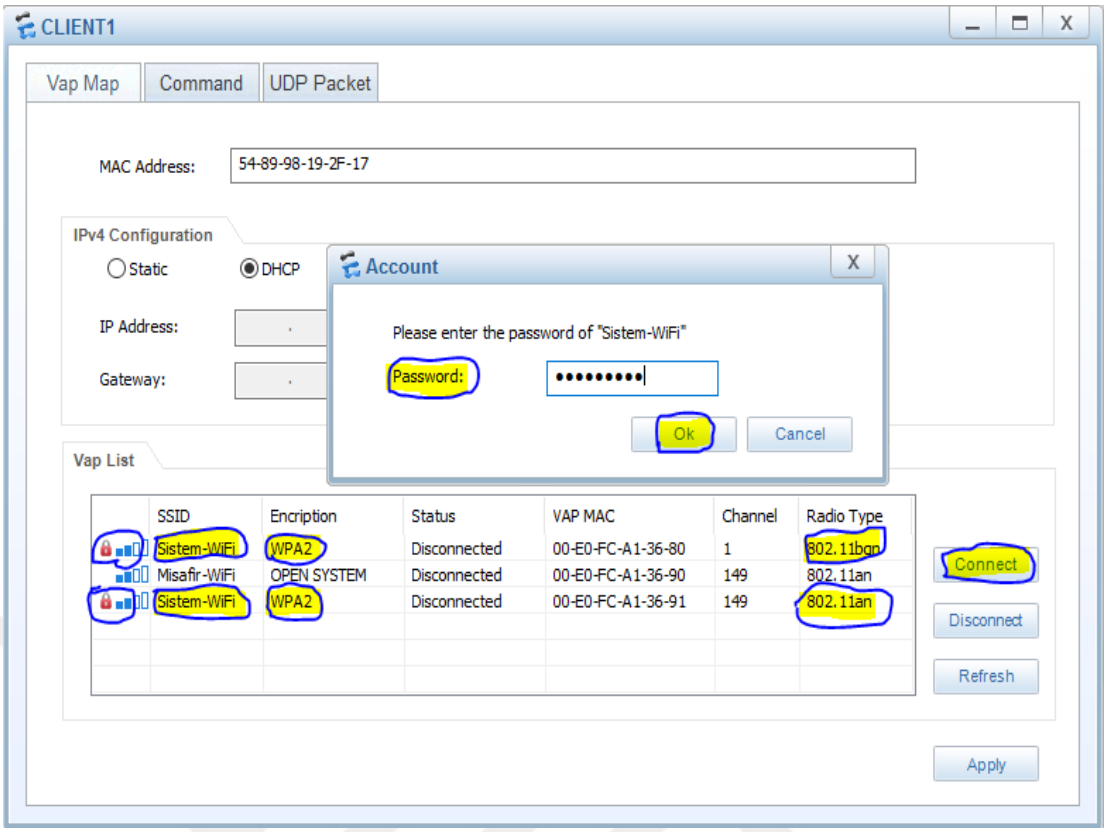
Tasarımın üçüncü kısmında yayın yapan AP'lere kablosuz ve kablolu cihazların nasıl bağlandığı anlatılacaktır.

— Sürükle bırak yoluyla her kata iki kablosuz (dizüstü bilgisayar ve cep telefonu) ve iki kablolu cihaz eklenecektir. Daha sonra eklenen cihazlar seçilerek start butonuna tıklanıp, çalışır duruma getirilecektir (Şekil 5.12).

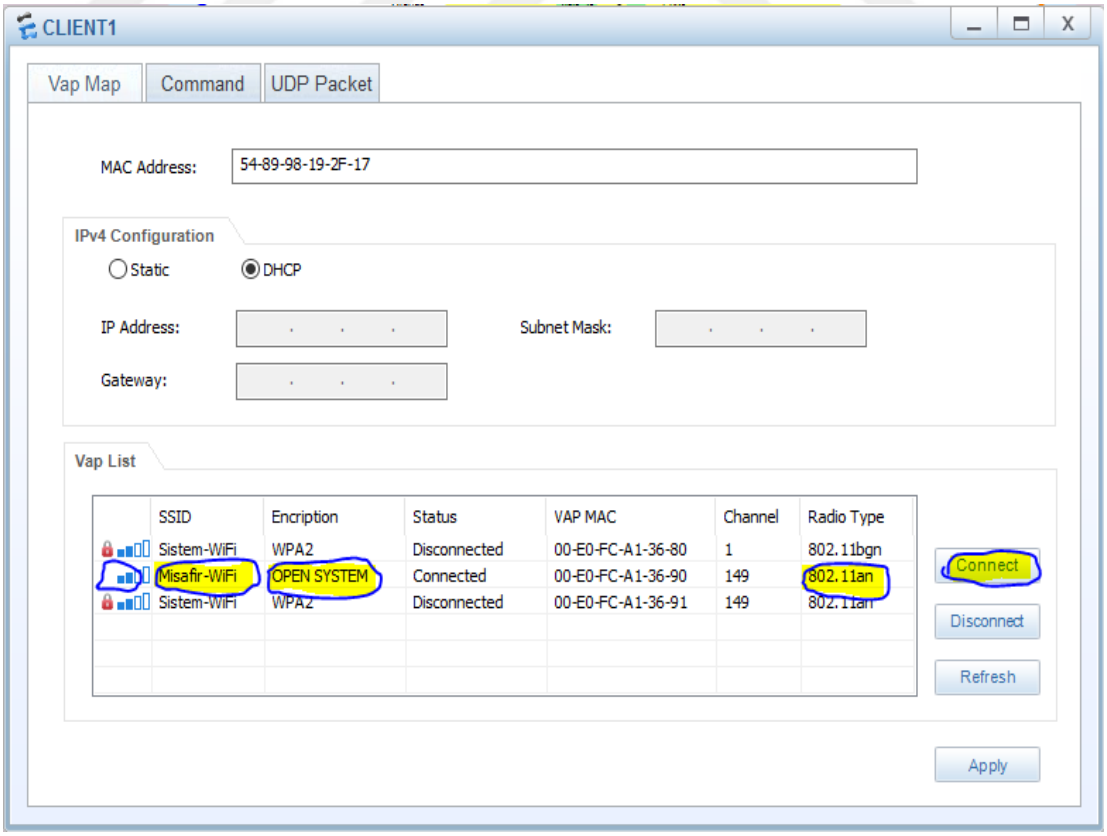


Şekil 5.12 Cihazların hepsinin çalışması

— Cihazların hepsi çalıştırıldıktan sonra kablosuz cihazlardan herhangi birinin üzerine iki kere tıklayarak, açılan pencereden bağlanmak istenen yayını seçip, Connect butonuna tıklanır. Bağlanmak istediğimiz ağ, şifreli yayın yapıyorsa, o ağın güvenlik şifresini doğru bir şekilde yazıp ok butonuna tıklayarak, ağa bağlanmasını beklenmelidir. (Şekil 5.13) Ağ şifresiz yayın yapıyorsa, yayını seçtikten sonra sadece Connect diyerek, ağa bağlanması beklenmelidir. (Şekil 5.14)

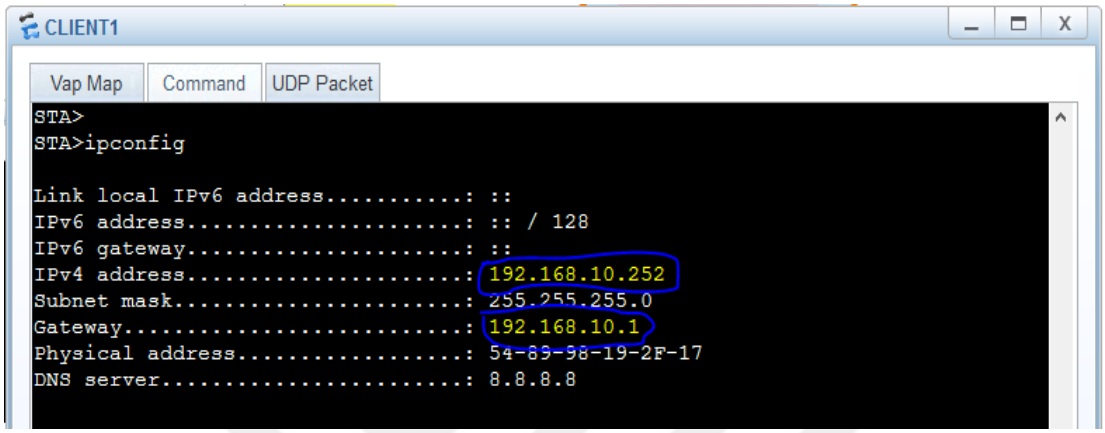


Şekil 5.13 CLIENT1'in şifreli ağa bağlanması



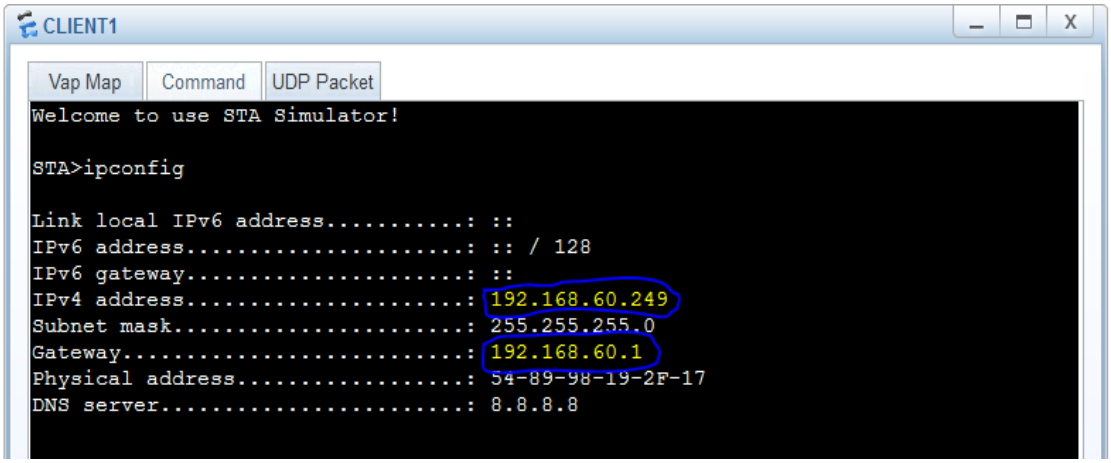
Şekil 5.14 CLIENT1'in şifresiz ağa bağlanması

— CLIENT1 Sistem-WiFi yayınına bağlandıktan sonra Command sekmesine gelerek, ipconfig komutuyla VLAN10'dan IP alıp almadığı kontrol edilecektir. (Şekil 5.15)



Şekil 5.15 CLIENT1'in VLAN10'dan IP alması

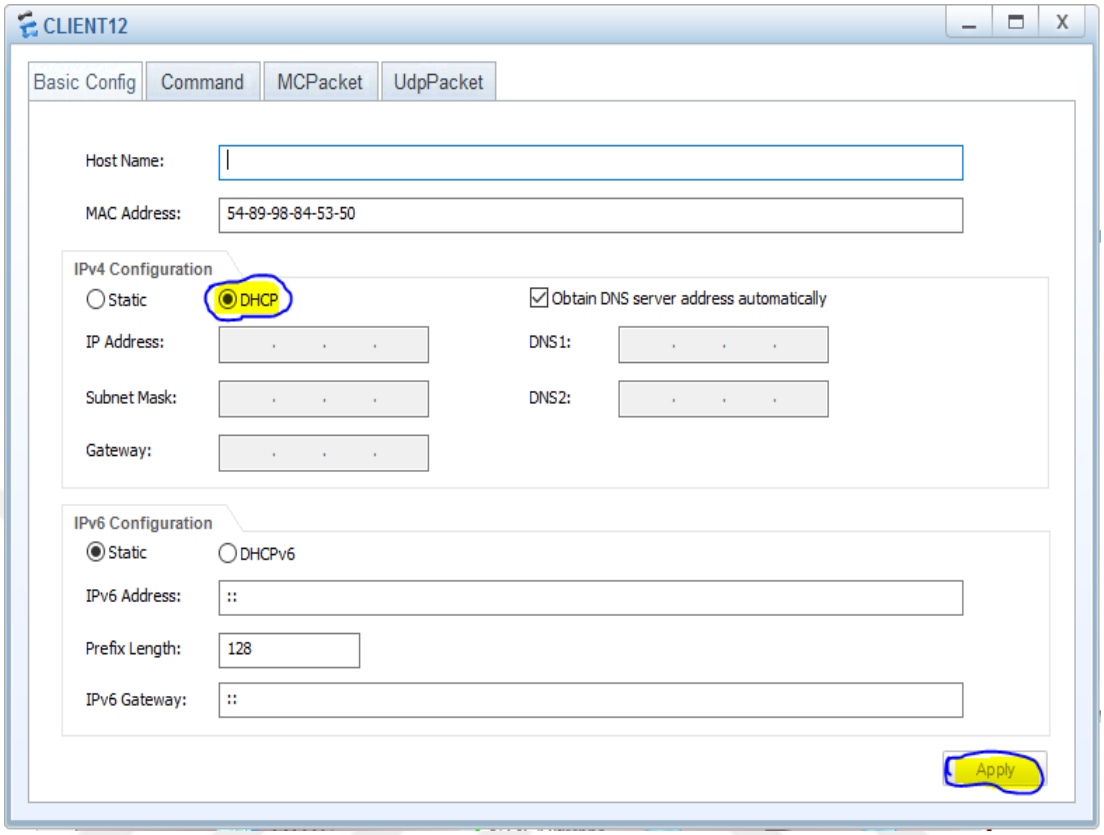
— CLIENT1 Misafir-WiFi yayınına bağlandıktan sonra Command sekmesine gelerek, ipconfig komutuyla VLAN60'dan IP alıp almadığını kontrol edilecektir. (Şekil 5.16)



Şekil 5.16 CLIENT1'in VLAN60'dan IP alması

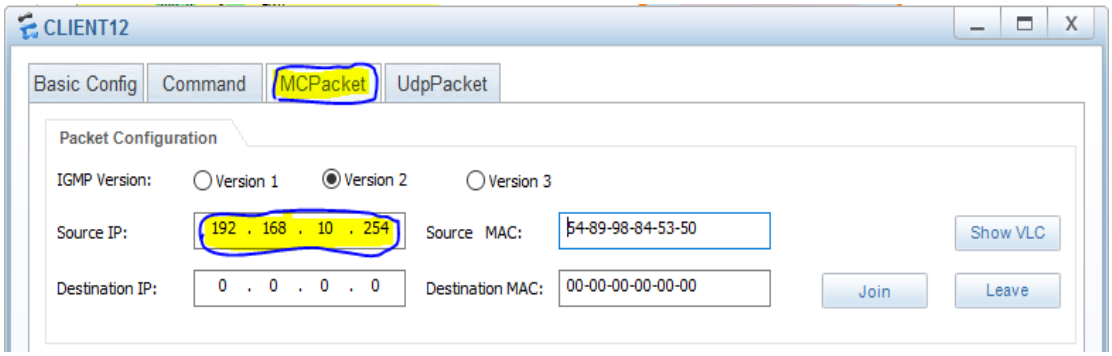
— Kablolu cihazların ağa bağlanıp DHCP server'den doğru IP almaları için kablolu cihazları kenar switch'lere bağlayan portlarına default vlan olarak hangi vlan'dan IP almasını istiyorsak o vlan girilecektir. Sonra her hangi bir kablolu cihazın üzerine iki

kere tıklayarak, açılan pencereden DHCP seçeneğini seçip Apply butonuna tıklanmalıdır. (Şekil 5.17)



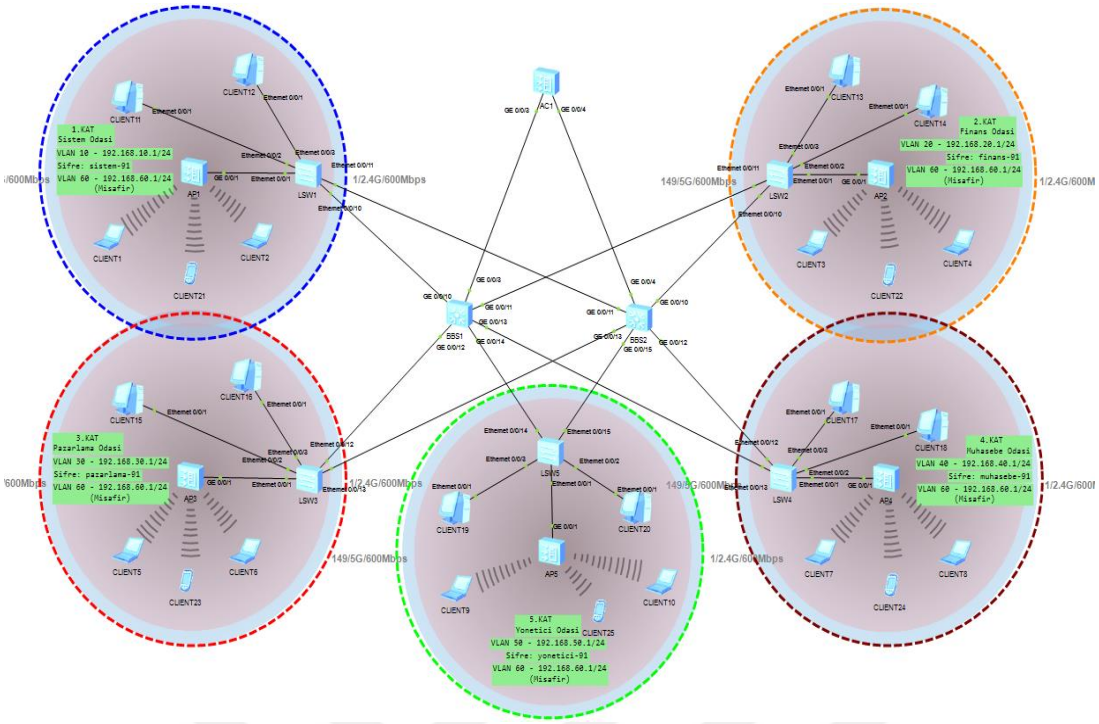
Şekil 5.17 CLIENT12'nin bağlantı arayüzü

— Daha sonra MCPaket butonuna tıklayarak, CLIENT12'nin DHCP'den IP alması beklenmelidir. (Şekil 5.18)



Şekil 5.18 CLIENT12'nin VLAN10'dan IP alması

— Kablolu ve kablosuz cihazlar şekil 5.18'de görüldüğü üzere doğru bir şekilde bağlanarak çalışır durumda.

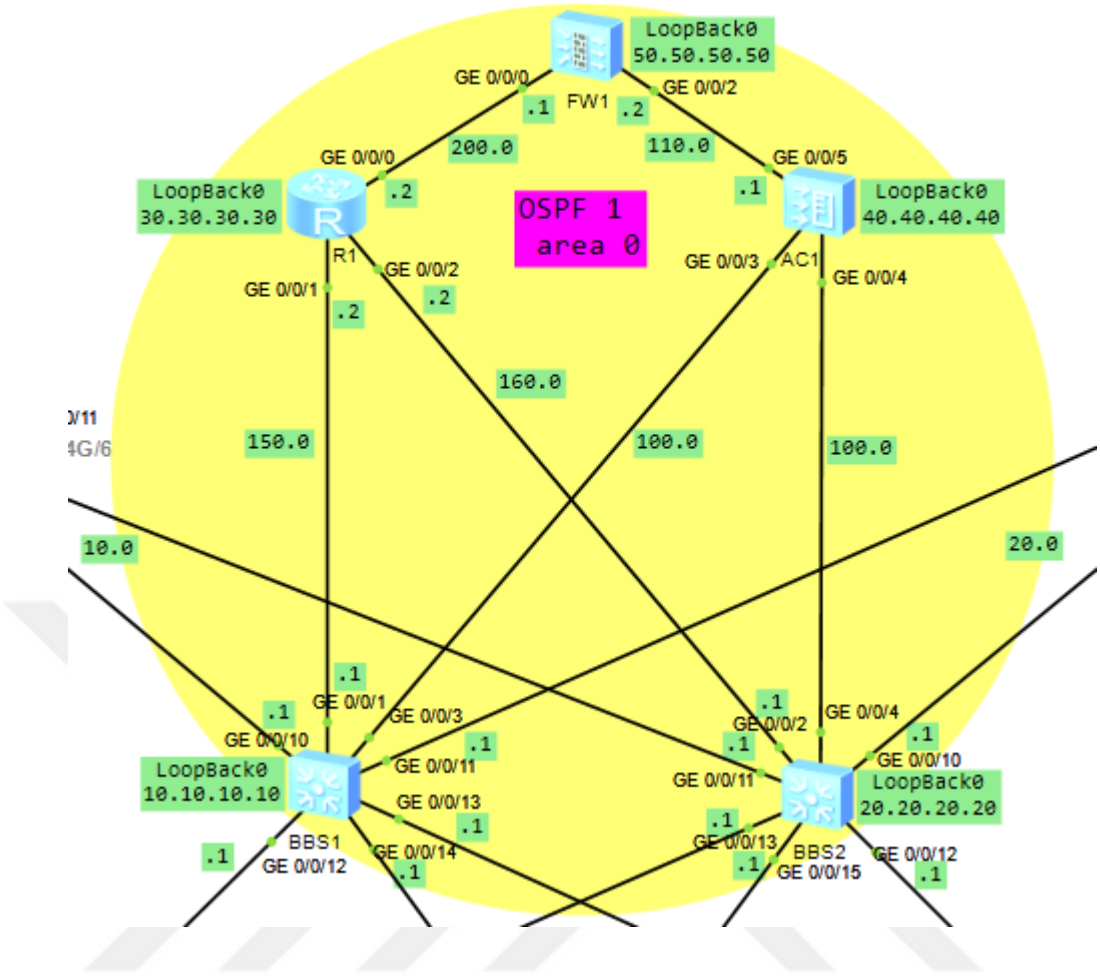


Şekil 5.19 Kablolu ve kablosuz cihazların bağlanarak çalışması

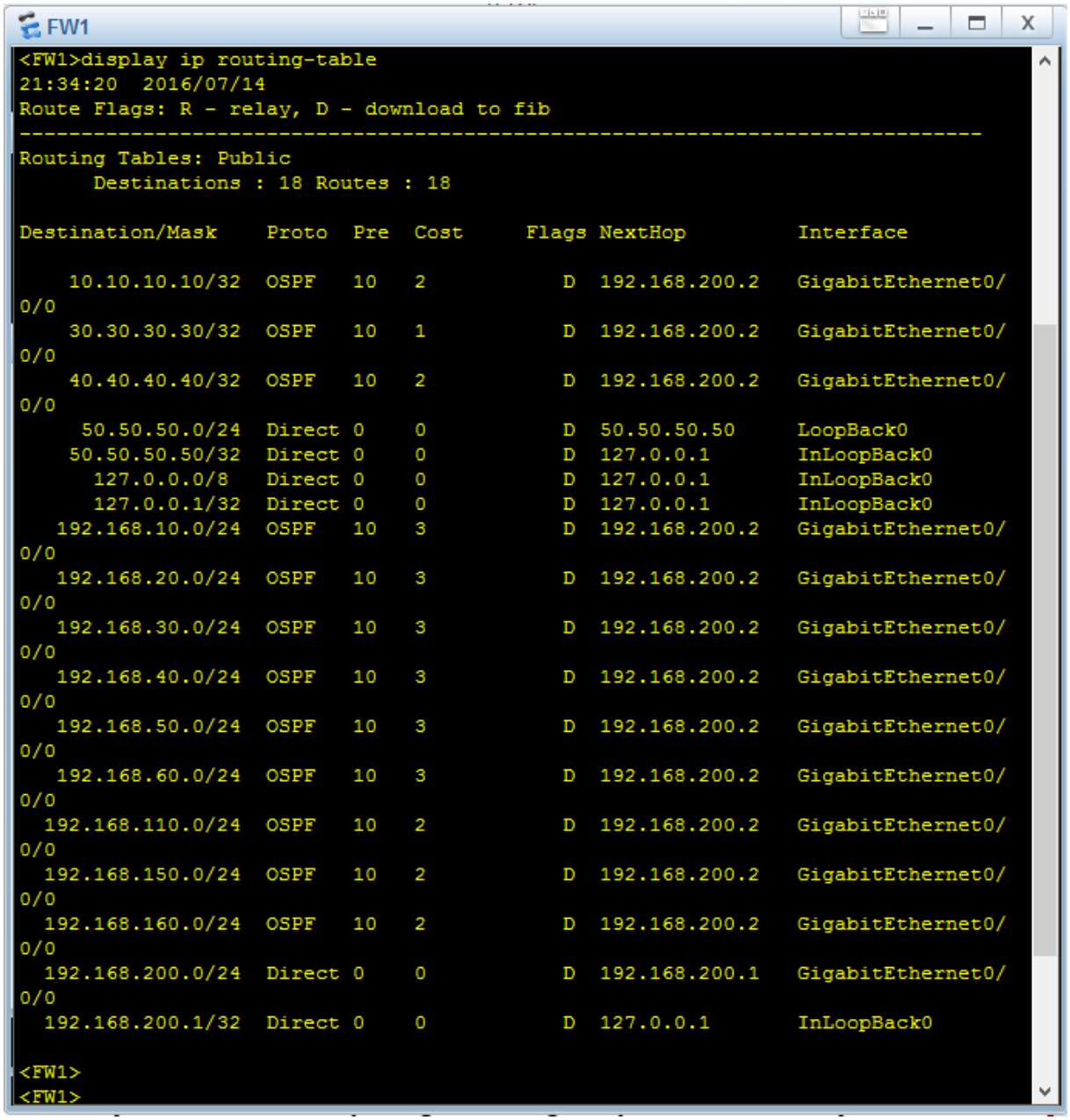
5.3.4 Dördüncü kısım

Tasarımın dördüncü kısmında Router (R1) ve Firewall (FW1) cihazları eklenecektir ve eklenen cihazların ağımızla haberleşmesi için OSPF protokolü uygulanacaktır. Firewall, router ve merkez switch'lerde saldırı yöntemleri kısmında anlatılan saldırılardan korunmak adına temel konfigürasyonlar yapılacaktır. Cihazlar üzerinde hem SSH hem de Telnet bağlantı protokolleri aktif edilecek ve bağlantı onayı için kullanıcı adı ve şifre belirlenecektir. Bunların yanı sıra ağımızın güvenliği adına gerekli cihazlarda gerekli ACL kuralları uygulanacaktır.

— Öncelikle sürükle bırak yoluyla Router ve Firewall cihazları eklenecek ve ağ haritasına uygun olarak isimlerinin ve bağlantı portlarının IP'lerinin konfigürasyonları yapılacaktır. Daha sonra Router ve Firewall cihazlarının ağımızdaki cihazlara erişmesi için OSPF protokolü uygulanacaktır. (Şekil 5.19) Tasarım bileşenleri kısmında OSPF protokolünün ne olduğu ve çalışma yapısının nasıl olduğu açıklanmıştır. OSPF protokolünü kullanmadığımız taktirde Firewall'a gideceği adrese ulaşırken, hangi yolu kullanacağını el ile teker teker girmemiz gerekecekti. Buda hem kullanışsız hem de güvensiz bir metottur. (Şekil 5.20)



Şekil 5.20 OSPF protokolünün uygulanması



Şekil 5.21 Firewall'ın (FW1) ağdaki IP'leri tanıması

— Saldırganlar, trafiği meşgul etmek için bir sunucuya gereksiz verileri büyük miktarda gönderirler. Trafiğin karışması sonucunda sunucu yetkili kullanıcılardan gelen isteklere cevap vermekte başarısız olur. SYN flood saldırıları, TCP full-connection saldırıları, HTTP flood saldırıları, UDP flood saldırıları ve ICMP flood gibi taşma saldırılarına karşı ağımızı korumak için firewall üzerinde trafik saldırılarına karşı savunmayı etkinleştirmek adına temel konfigürasyonlar yapılacaktır.

— Firewall üzerinde Bozuk Paket (Malformed Packet) saldırılarına, ICMP (Internet Control Message Protocol) Paket saldırılarına ve Smurf, Land, Fraggle gibi DoS saldırı

programlarına karşı savunmayı etkinleştirmek adına temel konfigürasyonlar yapılacaktır.

— DHCP snooping saldırılarına karşı alınacak önlem komutlarının başında dhcp snooping enable komutu gelir. Çünkü bu komut sayesinde switch'ler hangi porttaki kullanıcıya hangi ip atanmış şeklinde bir veritabanı tutmaya başlarlar. Tasarladığımız ağda IP dağıtımı AC1'in GigabitEthernet 0/0/3 portundan BBS1 switch'ine, GigabitEthernet 0/0/4 portundan ise BBS2 switch'ine yapıldığı için BBS1 ve BBS2 merkez switch'lerinde GigabitEthernet 0/0/3 ve GigabitEthernet 0/0/4 portlarına dhcp snooping trusted komutu girilecektir. Trusted yapılmasındaki amaç ağımıza sahte DHCP server bağlandığında ve bize ip dağıtımı yapmak istediğinde untrusted portlardan yaptığı için DHCP istek teklifleri cihazlar tarafından kabul edilmeyerek geri çevrilecektir. Trusted mantığına dayanarak kenar switch'leri merkez switch'lere bağlayan portlara da trusted komutu girilecektir. Çünkü kenar switch'ler IP'yi merkez switch'lerden alarak, ona bağlı olan cihazlara aktarıyor.

— DHCP snooping saldırılarına karşı bunların yanı sıra, DHCP'den bağlanan kullanıcıları kontrol etmek için merkez switch'leri kenar switch'lere bağlayan portlarında, bağlanan kullanıcıların MAC adreslerinin kontrolü, bağlantı izin verilen kullanıcı sayısı, atılabilecek mesaj yüzdesi gibi temel konfigürasyonlar yapılacaktır.

— ARP saldırılarına karşı ilk önce anti-attack özelliği aktif edilecektir. Daha sonra gelen ARP paketlerinin kontrol edilmesi adına temel konfigürasyonlar yapılacaktır.

— Uzaktaki bir makinenin ağımızdaki makinelere bağlanabilmesi için SSH ve TELNET bağlantı protokolleri aktif edilecektir. Bağlantı onay izni için her cihaza ayrı ayrı kullanıcı ismi ve şifre vermek yerine tüm cihazlara aynı kullanıcı isimi (cebrayil) ve şifre (huawei!123) atanacaktır. Daha sonra teker teker tüm cihazlara SSH ve TELNET bağlantıları yapılarak konfigürasyonların doğru yapılıp yapılmadığı kontrol edilecektir.

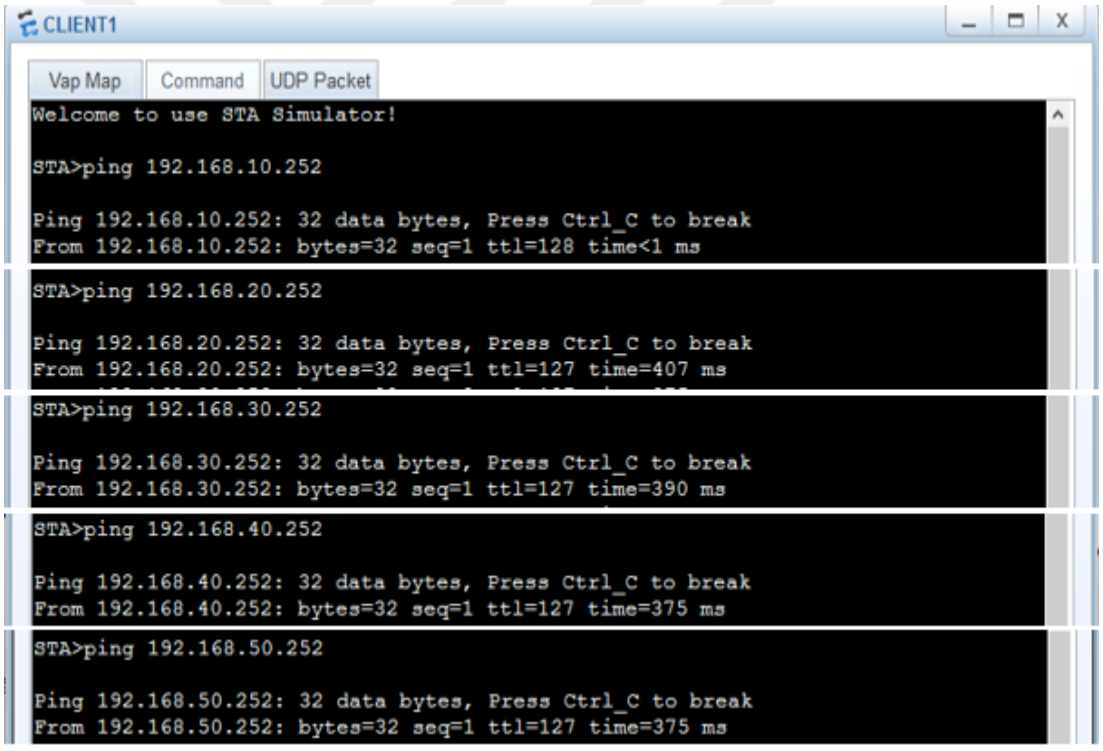
— Son olarak tasarımımıza ACL kuralları uygulanacaktır. ACL kural listelerinin önemi ve hazırlanırken kullanılması gereken parametreler tasarım bileşenleri kısmında anlatılmıştır. İlk önce VLAN 20'nin (Finans odası), VLAN 30'un (Pazarlama odası), VLAN 40'ın (Muhasebe odası) ve VLAN 50'nin (Yönetici odası) birbirilerine ICMP paketi göndermemeleri için gerekli ACL kuralları yazılarak bu VLAN'ların IP dağıtımının yapıldığı merkez switch'lere (BBS1 ve BBS2)

uygulanacaktır. Sonra VLAN 60'ın (Misafir) VLAN 20'e, VLAN 30'a, VLAN 40'a ve VLAN 50'ye erişememeleri için gerekli ACL kuralları yazılarak misafir yayınının yapıldığı AC1 (Access Controller) cihazına uygulanacaktır. Daha sonra ise Router'a güvenlik duvarı ve dışarıdan erişimine izin vereceğimiz bilgisayar veya cihaz dışında hiçbir cihazın erişmemesi için gerekli ACL kuralları yazılacaktır ve bu ACL kuralları Router'ın (R1) dışarıya bakan GigabitEthernet0/0/0 portuna uygulanacaktır. Dışarıdan ağımıza bağlanmak isteyen saldırganın IP'si Router cihazından geçemeyeceği için ağımıza erişemeyecektir.

6 KOMUTLARLA AĞIN GÜVENLİK KONTROLÜNÜN YAPILMASI

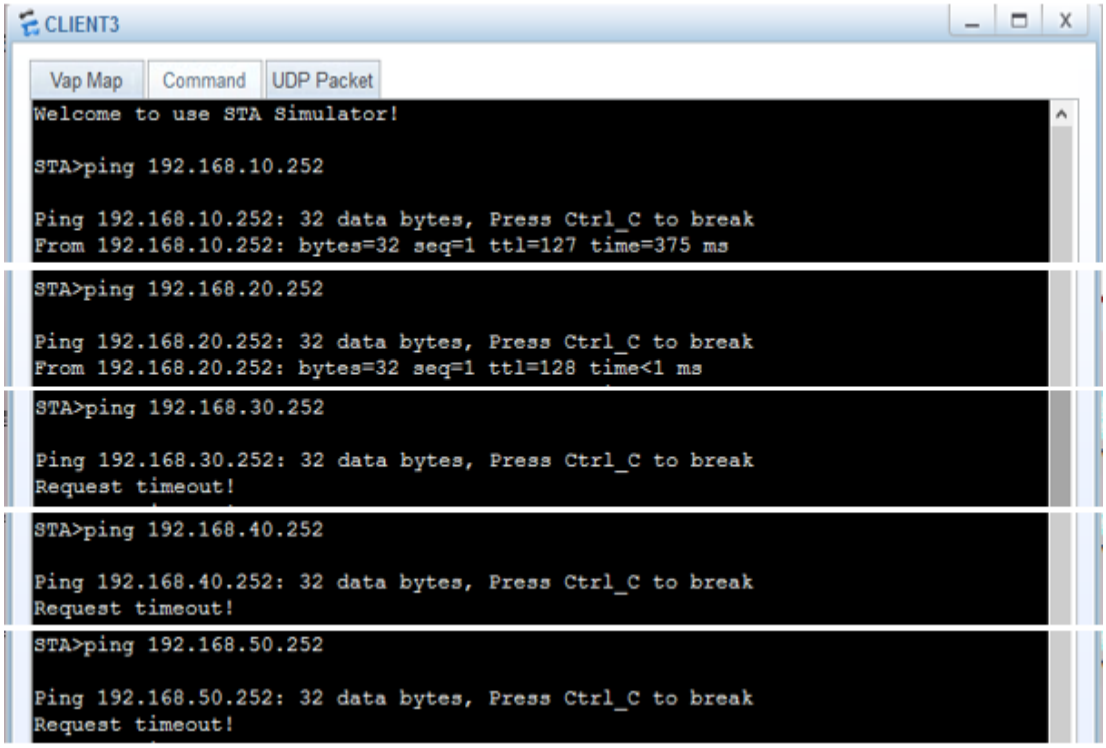
Huawei firmasının eNSP programı hakkında bilgi verirken simülasyon desteğinin olmadığından bahsedilmişti. Bu yüzden yapılan konfigürasyonların kontrolü komutlar kullanılarak yapılacaktır.

— VLAN 10'dan diğer kat VLAN'larına ICMP paketi gönderilerek yani ping atılarak, erişebilme durumları kontrol edilmelidir. Bu sebeple 1.kattaki CLIENT1 bilgisayarından diğer kattaki CLIENT bilgisayarlarına ping atılarak erişebilme durumlarının tasarımda belirlendiği gibi olduğu gözlemlenmiştir. (Şekil 6.1)



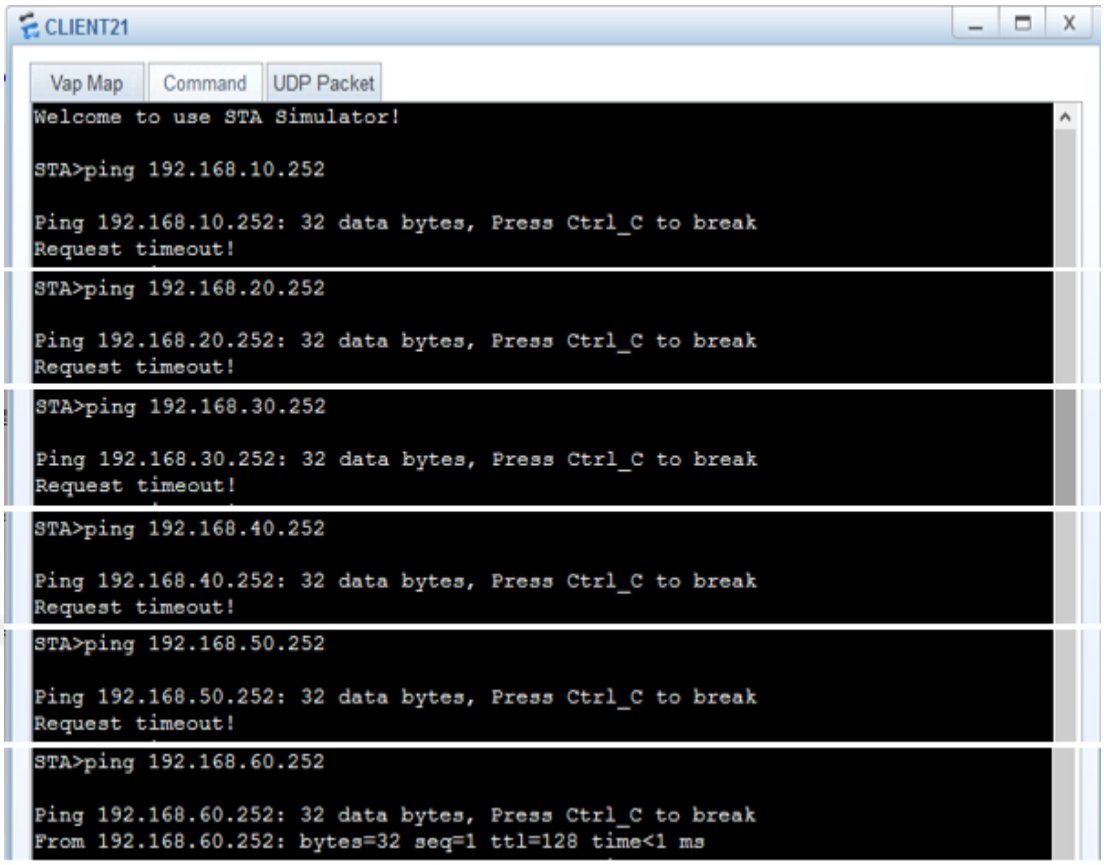
Şekil 6.1 CLIENT1'in tüm kattaki bilgisayarlara ping atma durumu

— VLAN 20, 30, 40 ve 50'den birbirilerine ICMP paketleri gönderilerek erişebilme durumları kontrol edilmelidir. Bu sebeple 2.kattaki CLIENT3 bilgisayarından diğer kattaki CLIENT bilgisayarlarına ping atılarak erişebilme durumlarının tasarımda belirlendiği gibi olduğu gözlemlenmiştir. (Şekil 6.2)



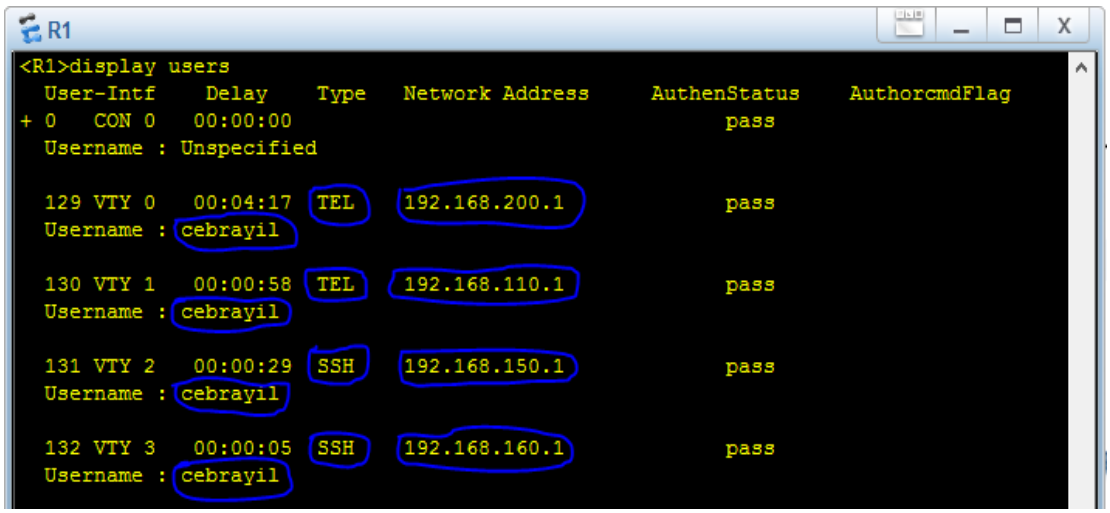
Şekil 6.2 CLIENT3'ün tüm kattaki bilgisayarlara ping atma durumu

— VLAN 60'tan kat VLAN'larına ICMP paketleri gönderilerek erişebilme durumları kontrol edilmelidir. Bu sebeple CLIENT21 bilgisayarından diğer kattaki CLIENT bilgisayarlarına ping atılarak erişebilme durumlarının tasarımda belirlendiği gibi olduğu gözlemlenmiştir. (Şekil 6.3)



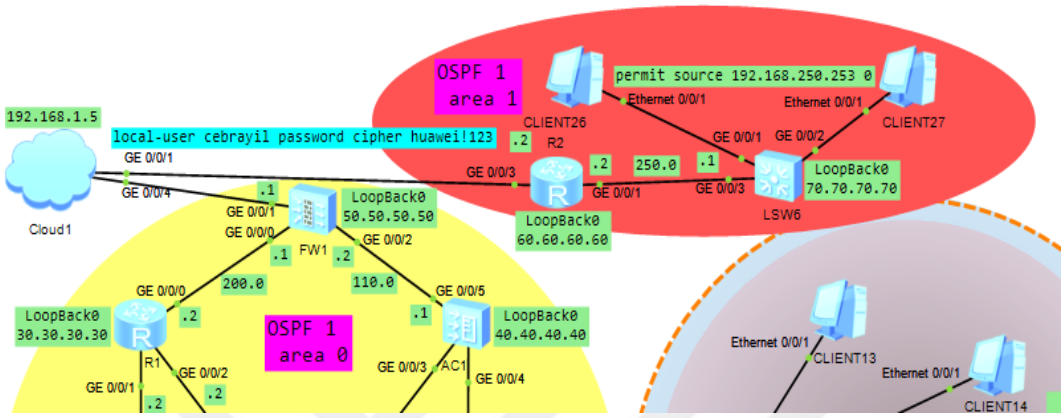
Şekil 6.3 CLIENT21'in tüm kattaki bilgisayarlara ping atma durumu

— SSH ve Telnet bağlantılarının kontrolü için tüm cihazlardan birbirilerine bağlantı yapılarak hepsinin doğru çalıştığı kontrol edilmelidir. Tüm cihazların bağlantılarını göstermek yerine aşağıda sadece FW1 ve AC1 cihazlarından TELNET, BBS1 ve BBS2 cihazlarından ise SSH bağlantılarıyla R1'e bağlantı yapıldığı gösterilmiştir. (Şekil 6.4)



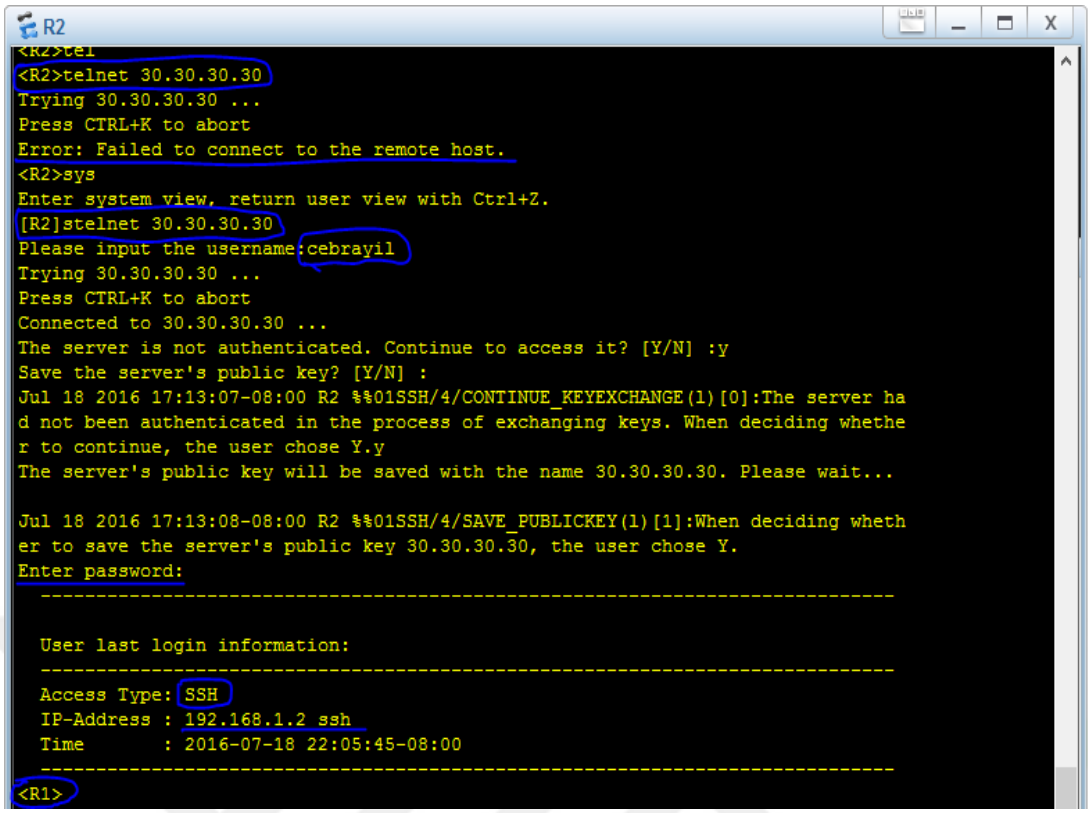
Şekil 6.4 FW1, AC1, BBS1 ve BBS2 cihazlarının R1'e bağlantı durumları

— Router'a (R1) dışarıdan yapılan bağlantılar için belirlenen ACL kurallarının doğru çalışıp çalışmadığı kontrol edilmelidir. Bu sebeple öncelikle tasarıma yeni bir küçük ağ tasarımı eklenecektir. (Şekil 6.5)



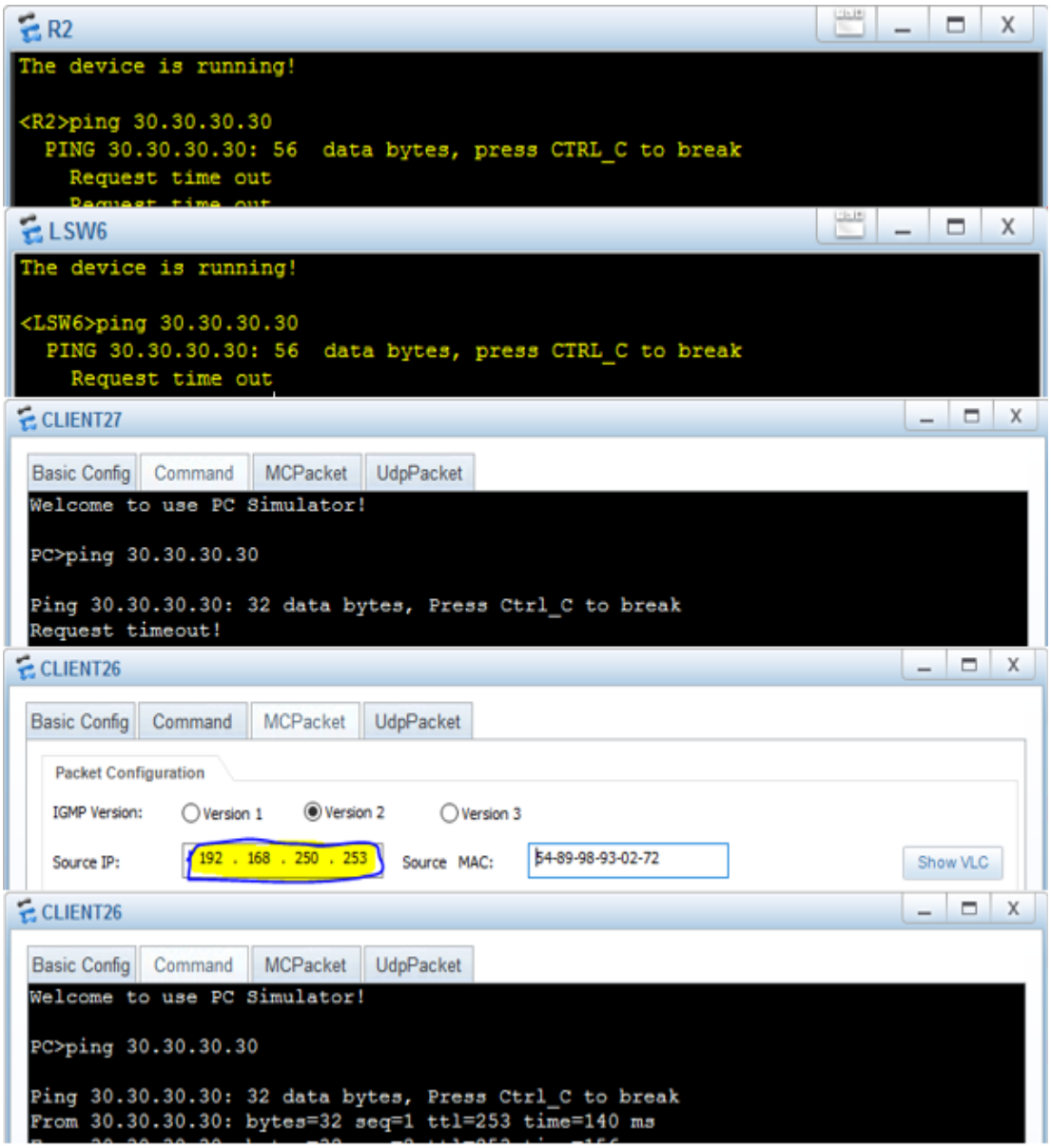
Şekil 6.5 Yeni ağın eklenmiş hali

— R1'de belirlenen ACL kurallarıyla tasarlanan ağa dışarıdan erişim yasaklanmıştı. Fakat belirlenen ACL kurallarının doğruluğunu kontrol etmek sebebiyle sadece R2 Router'ından ağımıza yani R1'e SSH bağlantısı yapılması için gerekli izin verilmiştir. (Şekil 6.6)



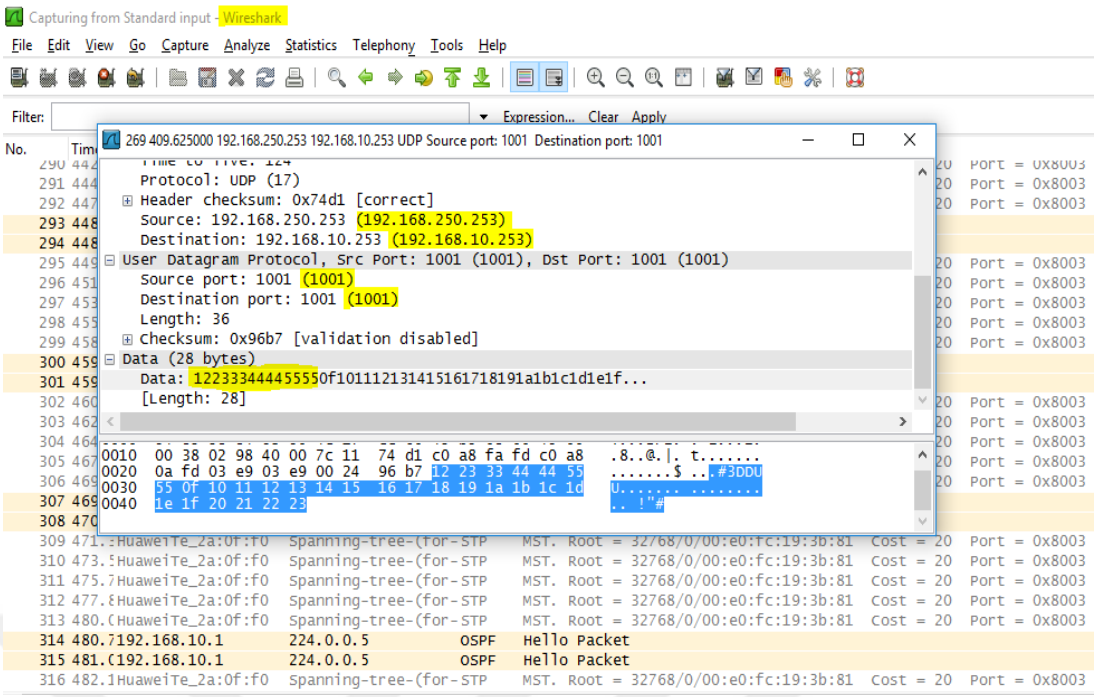
Şekil 6.6 R2'nin TELNET ve SSH bağlantı durumları

— R1'e dışarıdaki ağdan sadece IP adresi 192.168.250.253 olan bilgisayarın ICMP paketi göndermesine ve erişimine izin verilmiştir. (Şekil 6.7)



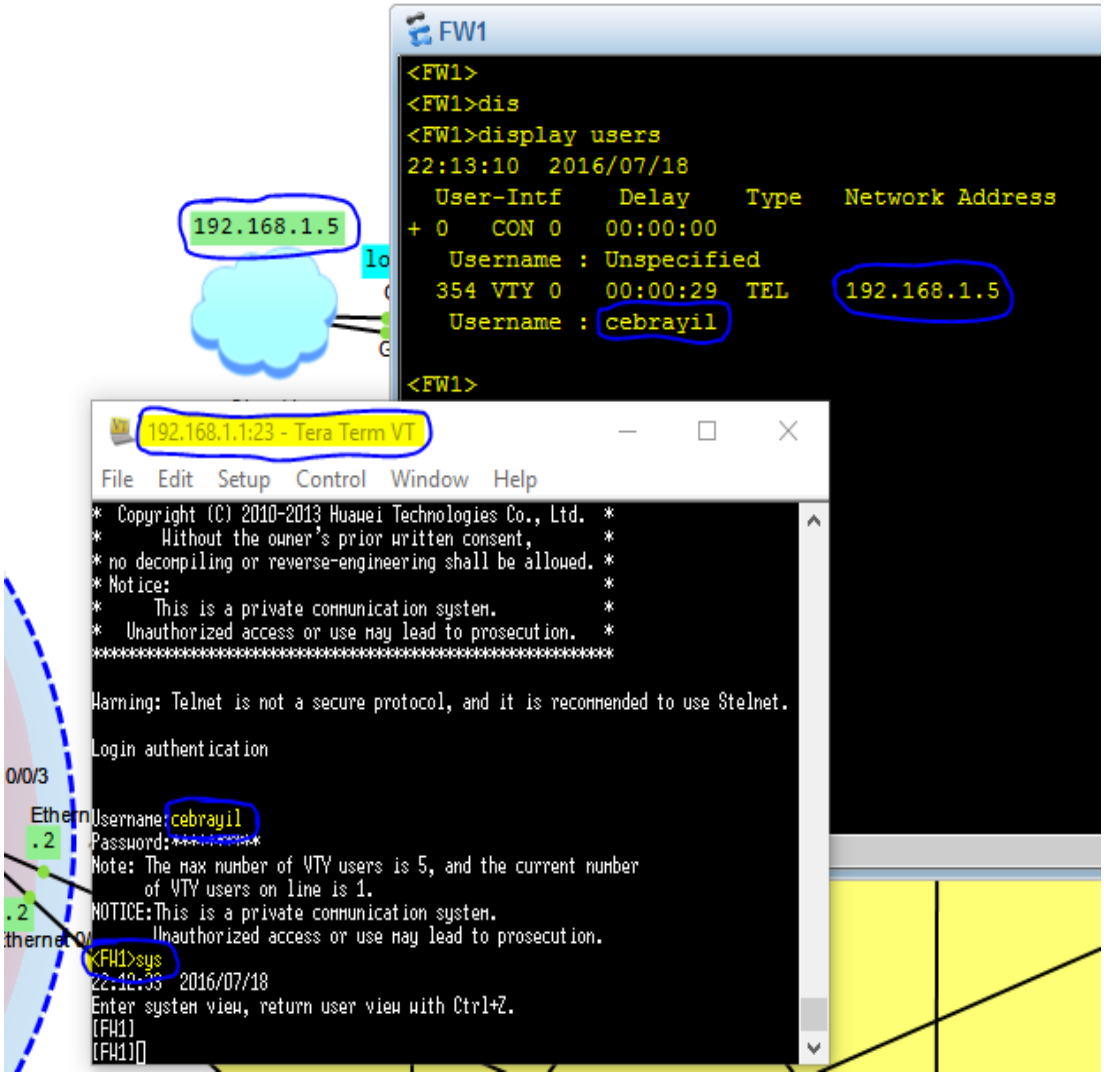
Şekil 6.7 R1'e dışarıdaki ağdan ICMP paketi gönderilmesi durumu

— IP adresi 192.168.250.253 olan bilgisayardan IP adresi 192.168.10.253 olan bilgisayara UDP paketi göndererek Wireshark ağ izleme programıyla paketin geldiği gözlemlenmiştir. (Şekil 6.8)



Şekil 6.8 Wireshark görüntüsü

— Son olarak uzaktaki sunucuya terminal üzerinden bağlantı sağlayan yazılımlardan olan Tera Term programıyla güvenlik duvarına (FW1) bağlantı yapılarak, ağımıza bulut üzerinden erişimin olduğu gözlemlenmiştir (Şekil 6.9).



Şekil 6.9 FW1 cihazına Tera Term bağlantısının yapılması

7 SONUÇ

Kablosuz ağlar sağladığı avantajlar sayesinde günümüzde olduğu kadar gelecekte de vazgeçilmez iletişim teknolojisi olarak kalmaya devam edecektir. Fakat kablosuz ağların avantajlarının yanı sıra bazı dezavantajları da vardır. Bu dezavantajların en önemlisi güvenlik açısından tam olarak istenen seviyenin sağlanamamasıdır. Bu yüzden kablosuz ağlar üzerinde sürekli olarak araştırmalar yapılarak yeni güvenlik yöntemleri geliştirilmeye çalışılmaktadır. Yapılan çalışmalar ile en hızlı ve en güvenilir bir ağ iletişimi hedeflenmektedir.

Bu tez çalışmasında kablosuz ağların özelliklede Kablosuz Yerel Alan Ağlarının gelişim süreci, teknolojileri, çalışma modları, standartları, avantaj ve dezavantajları, mevcut güvenlik ve saldırı yöntemleri incelenmiş ve en basit anlamlarıyla anlatılmağa özen gösterilmiştir. Uygulama kısmında sistem, finans, pazarlama, muhasebe ve yönetici katlarından ibaret 5 katlı hayali bir ofisin yüksek güvenlikli kablosuz yerel alan ağının tasarımı gerçekleştirilmiştir. Bu tasarımın ana amacı bireysel kullanımdan en kapsamlı ve gelişmiş kurumsal kullanıma kadar, güvenli bir kablosuz yerel alan ağını oluşturmak için izlenmesi gereken politikaları ve olası saldırılara karşı alınması gereken en güvenilir temel yöntemleri belirlemektir. Bu sebeple bu çalışmada firewall, router, switch, kablolu ve kablosuz cihazlar ve gerekli sunucuları ve protokolleri içeren yerel alan ağı oluşturulmuştur. Oluşturulan topolojinin gerçekleştirilmesi için Huawei firmasının eNSP programı kullanılmış ve konfigürasyonlar gerçek router, switch cihazlarının konfigürasyonları ile aynı şekilde yapılmıştır. VLAN'lar tanımlanmış ve bu VLAN'lar gerekli cihazlarda MSTP protokolü kullanılarak konfigüre edilmiştir. AC (Access Controller) cihazında ağımıza bağlı olan AP'lerin yayın yapmaları adına sırasıyla WMM profili, radio profili, WLAN-Ess'i, traffic profili ve security profili oluşturulmuştur. Daha sonra service set'leri oluşturularak bu profiller uygun servislere atanmıştır. PC'ler için DHCP havuzları ve DNS sunucusu tanımlanmış ve PC'lerin yerleştikleri veya oldukları kata göre hangi Wi-Fi yayınına bağlanıyorsalar o, kata veya yayına uygun IP adresleri aldıkları gözlemlenmiştir. DNS ve Gateway IP adresleri DHCP havuzları üzerinden dağıtılmıştır. Router ve Firewall cihazları

eklenmiş ve ağımızdaki IP adreslerine ve kullanılan cihazlara erişebilmeleri için Router, firewall, Access controller ve merkez switch'ler üzerinde OSPF protokolü uygulanmıştır. Display ip routing komutuyla router ve firewall cihazlarının ağımızdaki tüm IP'leri ve ağımızdaki cihazlara erişebilmeleri için gerekli tüm yolları otomatik öğrendikleri gözlemlenmiştir. Firewall cihazı üzerinde trafik, bozuk paket, ARP snooping, DHCP snooping, MAC flooding ve bir sıra DoS saldırı programlarına karşı önlem almak adına gerekli konfigürasyonlar yapılmıştır. Uzaktaki bir sunucunun ağımızdaki makinelere bağlanabilmesi için SSH ve Telnet bağlantı protokolleri aktif edilmiş ve bağlantı onay izni için cihazlar üzerinde kullanıcı ismi ve şifreler belirlenmiştir. Son olarak ağın güvenliği için gerekli ACL kuralları yazılarak, hangi cihazın hangi cihaza ya da hangi porta erişebileceği veya erişemeyeceği belirlenmiştir.

Tasarlanan ağın güvenliğinin kontrolü simülasyon yapılarak yapılamadığı için cihazlar üzerinde bazı komutlar kullanılarak yapılmıştır. Kontroller sonucunda tasarlanan ağın konfigürasyonlarının doğru çalıştığı gözlemlenmiştir.

Tasarlanan ağın günümüzdeki teknolojilere göre tabi ki de eksikleri vardır. Çünkü unutmamak gerekir ki tasarım gerçek laboratuvar ortamında değil de internet üzerinde ücretsiz paylaşılan Huawei'in eNSP programında yapılmıştır. Bu yüzdende sanal bir ortamda çalışıldığı için yapılacak konfigürasyonlar kısıtlıdır.

KAYNAKLAR

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

Akçay, B. (2006, 7 7). *Bilgisayar Virüslerinden ve Saldırılarından Korunma Önerileri*. 6 5, 2016 tarihinde bidb: http://www.bidb.hacettepe.edu.tr/viruslere-karsi-korunma.shtml adresinden alındı

Akmenek, B. (2013, 7 19). *Modem'le Router Arasındaki Fark Nedir?* 6 4, 2016 tarihinde fragtist: http://www.fragtist.com/masaustu/modemle-router-arasindaki-fark-nedir/ adresinden alındı

ALTAI. (2013). *Evaluation of Wireless Security using altai A8N Super Wifi Solution.* 6 2, 2016 tarihinde altaitechnologies: http://www.altaitechnologies.com/wp-content/uploads/2013/08/Whitepaper-Evaluation-of-Wireless-Security-130822.pdf adresinden alındı

Ansiklopedi. (2013, Eylül 29). *Bluetooth, Kızılötesi, Wireless İnfrared Nedir Arasında Ne Fark Var*. 4 25, 2016 tarihinde bilgilersitesi: http://www.bilgilersitesi.com/bluetooth-kizilotesi-wireless-infrared-nedir-arasinda-ne-fark-var.html adresinden alındı

Aslantaş, M. (2013, 10 15). *Hub, Switch ve Router nedir görevi nelerdir?* 6 7, 2016 tarihinde bilgevim: http://www.bilgevim.com/network/hub-switch-ve-router-nedir-nasil-calisir.html adresinden alındı

Baş, T. (2014, 5 30). *WiFi, 802.11 a/b/g standartları ve Telsiz Örgüsel Ağlar.* 5 27, 2016 tarihinde tuncaybas: http://www.tuncaybas.com/index.php/wifi-802-11-abg-standartlari-ve-telsiz-orgusel-aglar/ 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

Bayraktar, Z. (2005, Mayıs). *802.11 Telsiz Yerel Bilgisayar Ağlarında Güvenlik*. İstanbul: İstanbul Teknik Üniversitesi Yüksek Lisans Tezi. 5 25, 2016 tarihinde alındı

BİDB. (2013, 9 7). *Kablosuz Ağ Modları.* 5 2, 2016 tarihinde itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/kablosuz-a%C4%9F-modlar%C4%B1 adresinden alındı

BİDB. (2013, 9 7). *Kablosuz Ağ Standartları*. 5 20, 2016 tarihinde bidb.itu: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/kablosuz-a%C4%9F-standartlar%C4%B1 adresinden alındı

Canbek, G. ve Sağıroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, 121-136. 6 5, 2016 tarihinde http://www.mmfdergi.gazi.edu.tr/article/download/1061000244/1061000214 adresinden alındı

Canbek, G. ve Sağıroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 7-8. 6 5, 2016 tarihinde alındı

CHIP. (2013, 8 7). *Wi-Fi Şifreleme Sistemleri Arasındaki Farklar.* 6 2, 2016 tarihinde chip: http://www.chip.com.tr/haber/kablosuz-aginizi-sifreleyin-wi-fi-protected-access-wpa_41795_4.html adresinden alındı

Çamanlı, T. (2009, 10 18). *GSM Nedir ?* 3 22, 2016 tarihinde xing: https://www.xing.com/communities/posts/gsm-nedir-gsm-in-tanimlamasi-dot-dot-dot-1002692612 adresinden alındı

Dikici, 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-cihazlar%C4%B1 adresinden alındı

Dizdar, E. (2012, 2 25). *Kablosuz Ağlar.* 4 22, 2016 tarihinde slideshare: http://www.slideshare.net/edizdar/kablosuz-alar adresinden alındı

Dündar, M. (2010, 8 9). *SSH Nedir ? SSH Komutları Nelerdir ?* 6 5, 2016 tarihinde serhatdundar: http://www.serhatdundar.com/ssh-nedir-ssh-komutlari-nelerdir adresinden alındı

Gür, B., Şayf, V., Yüksel, A. ve Kantar, M. İ. (2015). Domain Name System (DNS). *Windows Server 2012 R2* (s. 253-254). içinde İstanbul: KODLAB Yayınları. 5 7, 2016 tarihinde alındı

Gezgin, D.M. ve Buluş, E. (tarih yok). *RC4 Tabanlı WPA(Wi-Fi Protected Access)'da Kullanılan TKIP (Temporal Key Integrity Protocol) Şifrelemesinin Incelenmesi.* 6 2, 2016 tarihinde emo: http://www.emo.org.tr/etkinlikler/itusem/etkinlik_bildirileri_detay.php?etkinlikkod=122&bilkod=4727 adresinden alındı

Harmankaya, A.O, Demiray, H.E., Ertürk, İ., Bayılmış, C. ve Bandırmalı, N. (tarih yok). *Kablosuz Ağlarda Güvenlik Protokollerinin Karşılaştırmalı İncelenmesi.* 6 1, 2016 tarihinde emo: http://www.emo.org.tr/ekler/3101d7f52390c29_ek.pdf adresinden alındı

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

Huawei. (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

Huawei. (2014, 4 20). *HCNA-WLAN Course Experiment Guide for WLAN Engineers.* 4 2, 2016 tarihinde huawei: http://support.huawei.com/learning/trainFaceDetailAction?courseId=Node1000004789&pbiPath=term1000025181&lang=en adresinden alındı

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

Kadakoğlu, S. (2010). Kablosuz Yerel Alan Ağlarında (WLAN) Güvenlik Uygulamaları ve Ses Haberleşmesi (VoIP). Yüksek Lisans Tezi. Trabzon 4 10, 2016 tarihinde alındı

Kartal, S. (2010, 5 14). *Şifreleme Algoritmaları.* 6 1, 2016 tarihinde savaskartal: http://www.savaskartal.com/2010/04/14/sifreleme-algoritmalari/ adresinden alındı

Karygiannis, T. ve Owens, L. (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices. *NIST Special Publication.* 5 25, 2016 tarihinde alındı

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

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

Kurtuluş, F. (2011, 9 5). *Altyapı Çalışma (Infrastructure, Client/Server) Modeli*. 5 14, 2016 tarihinde blogcu: http://teknikpcdersleri.blogcu.com/altyapi-calisma-infrastructure-client-server-modeli/11082304 adresinden alındı

MEGEP. (2007). *Kablosuz Ağ Sistemleri.* 5 20, 2016 tarihinde meb: http://hbogm.meb.gov.tr/modulerprogramlar/kursprogramlari/elektrik/modduller/kablosuzagsistemleri.pdf adresinden alındı

MEGEP. (2008). *Ağ protokolleri ve ağ güvenliği.* MCU (Multipoint Conferencing Unit): http://hbogm.meb.gov.tr/modulerprogramlar/kursprogramlari/elektrik/modduller/agprotokolleriveagguvenligi.pdf adresinden alındı

MEGEP. (2011). *Bilişim Teknolojisi Kablosuz Ağlar.* 3 28, 2016 tarihinde megep: http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/Kablosuz%20A%C4%9Flar.pdf adresinden alındı

MEGEP. (2011). *Kablosuz Ağ Sistemleri.* 3 27, 2016 tarihinde megep: http://www.megep.meb.gov.tr/mte_program_modul/moduller_pdf/Kablosuz%20A%C4%9F%20Sistemleri.pdf adresinden alındı

MEGEP. (2013). *Bilişim Teknolojileri, Ağ Güvenliği.* 5 28, 2016 tarihinde meb: http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/A%C4%9F%20G%C3%BCvenli%C4%9Fi.pdf adresinden alındı

Microsoft. (tarih yok). *Kablosuz Ağlara Genel Bakış*. 4 13, 2016 tarihinde microsoft: https://technet.microsoft.com/tr-tr/library/cc784756(v=ws.10).aspx adresinden alındı

Murt, M. (2014, 6 28). *Güvenli ve Güçlü Şifre Oluşturma Yöntemleri*. 6 4, 2016 tarihinde mesutmurt: http://www.mesutmurt.com/12763-Guvenli-ve-Guclu--Sifre-Olusturma-Yontemleri.html adresinden alındı

Olgun, O. (2015, 5 15). *Kablosuz Ağ teknolojileri ve Şifreleme*. 6 3, 2016 tarihinde cyber-warrior: https://www.cyber-warrior.org/forum/kablosuz-ag-teknolojileri-ve-sifreleme_549583,2.cwx adresinden alındı

Öcal, F. (2014). *Bilgisayar ağları.* Ağ topolojileri: http://www2.cbu.edu.tr/users/fatihocal/dosyalar/konu_ekleri/ag-sistemleri-1-1.pdf adresinden alındı

Özçelik, S. (2014, 1 4). *DNS zehirlenmesi (Spoofing) Nedir ?* 5 8, 2016 tarihinde wordpress: https://soykanozcelik.wordpress.com/2014/04/01/dns-zehirlenmesispoofing-nedir/ adresinden alındı

Özdemir, B. (2008, 3 3). *Kablosuz Yerel Alan Ağı Güvenliği Kılavuzu*. UEKAE. 5 28, 2016 tarihinde alındı

Reisoğlu, E. (2008, Ocak). *Kablosuz Ağlarda Güvenlik.* İstanbul: Bahçeşehir Üniversitesi, Yüksek Lisans Tezi. 5 28, 2016 tarihinde alındı

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

Sesli, M. (2015, 5 31). *DHCP Starvation ve DHCP Spoofing Saldırıları*. 6 8, 2016 tarihinde blogspot: http://msesli.blogspot.com.tr/2015/05/dhcp-starvation-ve-dhcp-spoofing.html adresinden alındı

Soylu, T. (2011). *Kablosuz Ağ Teknolojileri.* Edirne: Paralel Mimariler. 5 25, 2016 tarihinde alındı

Şamlıoğlu, H. (2011, 2 19). *ADSL Modem Üzerinde Mac Filtrelemesini Aktif Etmek.* 5 28, 2016 tarihinde teakolik: http://www.teakolik.com/adsl-modem-uzerinde-mac-filtrelemesini-aktif-etmek/ adresinden alındı

Şeremet, Ö. (2014, 11 27). *Bilgi ve Veri Güvenliği*. 6 6, 2016 tarihinde ozgurseremet: http://ozgurseremet.com/bitin-gizlilik-ve-guvenlik-boyutlari/ adresinden alındı

Taşpınar, N., Koçak, Y., Sabah, A. M. (2002). Genel Paket Radyo Servisi (GPRS) Yapısı, Protokolleri ve Kaynak Yönetimi. *Erciyes Üniversitesi Fen Bilimleri Ensitüsü Dergisi*. 3 20, 2016 tarihinde http://fbe.erciyes.edu.tr/MKA-2005/Dergi/2001-vol17-no-1-2/3-taspinar.pdf adresinden alındı

Tatlı, M. Z., Teke, A., Uslu, Y. ve Çeğil, B. (2013, 8 7). *Çevirmeli Uzaktan Erişim Nedir ?* 6 1, 2016 tarihinde anadolu: http://ceng.anadolu.edu.tr/emrekacmaz/BTP106/Konular/10_Hafta_Bilgisayar_Aglari.pptx adresinden alındı

Turksan. (2009, 1 3). *Network Switch Nedir? Nasıl Çalışır?* 6 5, 2016 tarihinde turksan: http://www.turksan.com/network-switch.html adresinden alındı

Ural, A. (2015, 1 13). *Botnet, Dos, DDos Nedir?* 6 4, 2016 tarihinde onedio: http://onedio.com/haber/16-maddede-internette-saati-10-dolara-kiralanabilen-siber-ordular-gercegi-435279 adresinden alındı

Usta, G. (2015). *Bilgisayar Ağlarında Saldırı ve Savunma.* Ankara: Seçkin Yayıncılık. 6 5, 2016 tarihinde alındı

Uzun, K. (2006, 7). Kablosuz İletişim Sistemleri Bina İçi Yayılımında Engellerin Etkilerin İncelenmesi. *Zonguldak Karaelmas Üniversitesi*. Zonguldak. 4 29, 2016 tarihinde alındı

Yüksel, E., Soytürk, M., Ovatman, T., Örencik, B. (tarih yok). *Telsiz Yerel Alan Ağlarında Güvenlik Sorunu.* 6 2, 2016 tarihinde marmara: http://mimoza.marmara.edu.tr/~mujdat.soyturk/papers_web/bag_05.pdf adresinden alındı

Yılmaz, E. ve Öztürk, E. (tarih yok). *Yeni Nesil Kablosuz İletişim Teknolojileri Karşılaştırmalı Analizi.* 4 20, 2016 tarihinde emo: http://www.emo.org.tr/ekler/31a0d8b9f7e04e3_ek.pdf adresinden alındı

Wikipedia. (2016, 5 30). *Casus Yazılım*. 6 5, 2016 tarihinde wikipedia: https://tr.wikipedia.org/wiki/Casus_yaz%C4%B1l%C4%B1m adresinden alındı

EKLER

EK A: Konfigürasyon Kodları

Ağda oluşturulan konfigürasyonun kodları cihaz isimlerine göre ekte verilmiştir.

LSW6;

```
<LSW6>display current-configuration
#
sysname LSW6
#
dhcp enable
#
interface Vlanif1
 ip address 192.168.250.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface LoopBack0
 ip address 70.70.70.70 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 70.70.70.70
 area 0.0.0.1
  network 192.168.250.0 0.0.0.255
#
return
```

Router 2;

```
<R2>display current-configuration
#
sysname R2
#
rsa peer-public-key 192.168.200.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
interface GigabitEthernet0/0/1
 ip address 192.168.250.2 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.2 255.255.255.0
#
```

```
interface LoopBack0
 ip address 60.60.60.60 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 60.60.60.60
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 60.60.60.60 0.0.0.0
  network 192.168.250.0 0.0.0.255
#
ssh client first-time enable
ssh client 192.168.200.2 assign rsa-key 192.168.200.2
#
return
```

Firewall;

```
<FW1>display current-configuration
#
sysname FW1
#
rsa peer-public-key 192.168.200.2
  public-key-code begin
  public-key-code end
 peer-public-key end
#
interface GigabitEthernet0/0/0
 ip address 192.168.200.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 192.168.110.2 255.255.255.0
#
interface LoopBack0
 ip address 50.50.50.50 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
 add interface GigabitEthernet0/0/1
 add interface GigabitEthernet0/0/2
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil service-type telnet ssh
 local-user cebrayil level 15
#
ospf 1 router-id 50.50.50.50
 area 0.0.0.0
```

```
  network 50.50.50.50 0.0.0.0
  network 192.168.200.0 0.0.0.255
  network 192.168.250.0 0.0.0.255
  network 192.168.110.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
 ssh client first-time enable
 ssh client 192.168.200.2 assign rsa-key 192.168.200.2
#
 firewall blacklist enable
 firewall blacklist item 192.168.250.1
 firewall blacklist item 192.168.250.254
#
user-interface con 0
 authentication-mode none
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
 vlan batch 250
#
return
```

Router 1;

```
<R1> display current-configuration
#
 sysname R1
#
vlan batch 110 150 160 200
#
rsa peer-public-key 192.168.160.1
  public-key-code begin
  public-key-code end
 peer-public-key end
#
 rsa peer-public-key 192.168.150.1
  public-key-code begin
  public-key-code end
 peer-public-key end
#
acl number 3010
 rule 5 permit icmp source 192.168.200.1 0
 rule 10 permit icmp source 192.168.110.1 0
 rule 15 permit icmp source 50.50.50.50 0
 rule 20 permit icmp source 40.40.40.40 0
 rule 25 permit icmp source 192.168.250.253 0
 rule 30 deny tcp source 192.168.1.2 0 destination 192.168.200.2 0 destination-port eq
telnet
```

```
 rule 35 deny tcp source 192.168.1.2 0 destination 30.30.30.30 0 destination-port eq
telnet
 rule 40 deny icmp
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
 interface GigabitEthernet0/0/0
 ip address 192.168.200.2 255.255.255.0
 traffic-filter inbound acl 3010
#
interface GigabitEthernet0/0/1
 ip address 192.168.150.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 192.168.160.2 255.255.255.0
#
interface LoopBack0
 ip address 30.30.30.30 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 30.30.30.30
 area 0.0.0.0
  network 30.30.30.30 0.0.0.0
  network 192.168.150.0 0.0.0.255
  network 192.168.160.0 0.0.0.255
  network 192.168.200.0 0.0.0.255
#
 ssh client 192.168.160.1 assign rsa-key 192.168.160.1
 ssh client 192.168.150.1 assign rsa-key 192.168.150.1
 ssh client first-time enable
 stelnet server enable
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
user-interface vty 16 20
#
return
```

AC;

```
<AC1> display current-configuration
#
 sysname AC1
#
vlan batch 10 20 30 40 50 60 70 100 110
```

```
#
stp enable
#
dhcp enable
#
acl number 3060
 rule 5 deny icmp source 192.168.60.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
 rule 10 deny icmp source 192.168.60.0 0.0.0.255 destination 192.168.40.0 0.0.0.255
 rule 15 deny icmp source 192.168.60.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 deny icmp source 192.168.60.0 0.0.0.255 destination 192.168.30.0 0.0.0.255
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet
#
interface Vlanif60
 ip address 192.168.60.1 255.255.255.0
 traffic-filter inbound acl 3060
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif100
 ip address 192.168.100.100 255.255.255.0
 dhcp select interface
#
interface Vlanif110
 ip address 192.168.110.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/5
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 2 to 4094
#
interface Wlan-Ess1
 port hybrid pvid vlan 10
```

```
 port hybrid untagged vlan 10
#
interface Wlan-Ess2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface Wlan-Ess3
 port hybrid pvid vlan 30
 port hybrid untagged vlan 30
#
interface Wlan-Ess4
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
interface Wlan-Ess5
 port hybrid pvid vlan 50
 port hybrid untagged vlan 50
#
interface Wlan-Ess6
 port hybrid pvid vlan 60
 port hybrid untagged vlan 60
#
interface LoopBack0
 ip address 40.40.40.40 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 40.40.40.40
 area 0.0.0.0
  network 40.40.40.40 0.0.0.0
  network 192.168.60.0 0.0.0.255
  network 192.168.110.0 0.0.0.255
#
user-interface con 0
 authentication-mode password
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
wlan
 wlan ac source interface vlanif100
 ap-auth-mode no-auth
 ap id 0 type-id 19 mac 00e0-fc49-3a90 sn 2102354483107915F322
 ap id 1 type-id 19 mac 00e0-fca1-3680 sn 210235448310280AD511
 ap id 2 type-id 19 mac 00e0-fcd3-3520 sn 210235448310E008F644
 ap id 3 type-id 19 mac 00e0-fc0a-3290 sn 2102354483101D408F2E
 ap id 4 type-id 19 mac 00e0-fc59-5540 sn 2102354483109B481415
 ap id 5 type-id 19 mac 00e0-fcf0-7280 sn 210235448310D85A8814
 wmm-profile name WMM-1 id 0
 traffic-profile name Traffic-1 id 0
 security-profile name Security-1 id 0
```

```
 security-policy wpa2
 wpa2 authentication-method psk pass-phrase cipher sistem-91 encryption-method ccmp
security-profile name Security-2 id 1
 security-policy wpa2
 wpa2 authentication-method psk pass-phrase cipher finans-91 encryption-method ccmp
security-profile name Security-3 id 2
 security-policy wpa2
 wpa2 authentication-method psk pass-phrase cipher pazarlama-91 encryption-method ccmp
security-profile name Security-4 id 3
 security-policy wpa2
 wpa2 authentication-method psk pass-phrase cipher muhasebe-91 encryption-method ccmp
security-profile name Security-5 id 4
 security-policy wpa2
 wpa2 authentication-method psk pass-phrase cipher yonetici-91 encryption-method ccmp
security-profile name Security-6 id 5
service-set name SistemOdasi id 0
 forward-mode tunnel
 wlan-ess 1
 ssid Sistem-WiFi
 traffic-profile id 0
 security-profile id 0
 service-vlan 10
service-set name FinansDepartmani id 1
 forward-mode tunnel
 wlan-ess 2
 ssid Finans-WiFi
 traffic-profile id 0
 security-profile id 1
 service-vlan 20
service-set name PazarlamaDepartmani id 2
 forward-mode tunnel
 wlan-ess 3
 ssid Pazarlama-WiFi
 traffic-profile id 0
 security-profile id 2
 service-vlan 30
service-set name MuhasebeDepartmani id 3
 forward-mode tunnel
 wlan-ess 4
 ssid Muhasebe-WiFi
 traffic-profile id 0
 security-profile id 3
 service-vlan 40
service-set name YoneticiDepartmani id 4
 forward-mode tunnel
```

```
 wlan-ess 5
 ssid Yonetici-WiFi
 traffic-profile id 0
 security-profile id 4
 service-vlan 50
service-set name Misafir id 5
 forward-mode tunnel
 wlan-ess 6
 ssid Misafir-WiFi
 traffic-profile id 0
 security-profile id 5
 service-vlan 60
radio-profile name Radio-1 id 0
 radio-type 80211bgn
 wmm-profile id 0
radio-profile name Radio-2 id 1
 radio-type 80211an
 wmm-profile id 0
ap 1 radio 0
 radio-profile id 0
 service-set id 0 wlan 1
ap 1 radio 1
 radio-profile id 1
 service-set id 5 wlan 1
 service-set id 0 wlan 2
ap 2 radio 0
 radio-profile id 0
 service-set id 1 wlan 1
ap 2 radio 1
 radio-profile id 1
 service-set id 5 wlan 1
 service-set id 1 wlan 2
ap 3 radio 0
 radio-profile id 0
 service-set id 2 wlan 1
ap 3 radio 1
 radio-profile id 1
 service-set id 5 wlan 1
 service-set id 2 wlan 2
ap 4 radio 0
 radio-profile id 0
 service-set id 3 wlan 1
ap 4 radio 1
 radio-profile id 1
 service-set id 5 wlan 1
 service-set id 3 wlan 2
ap 5 radio 0
 radio-profile id 0
 service-set id 4 wlan 1
ap 5 radio 1
```

```
 radio-profile id 1
 service-set id 5 wlan 1
 service-set id 4 wlan 2
#
return

BBS1;
<BBS1>display current-configuration
#
sysname BBS1
#
vlan batch 10 20 30 40 50 60 70 100 150
#
stp instance 1 root primary
stp instance 2 root secondary
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
dhcp snooping enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
rsa peer-public-key 192.168.10.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.20.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.30.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.40.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.50.2
```

```
 public-key-code begin
 public-key-code end
peer-public-key end
#
acl number 3020
 rule 5 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.30.0 0.0.0.255
 rule 10 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.40.0 0.0.0.255
 rule 15 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
acl number 3030
 rule 5 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
 rule 10 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.40.0 0.0.0.255
 rule 15 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
acl number 3040
 rule 5 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
 rule 10 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.30.0 0.0.0.255
 rule 15 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif30
 ip address 192.168.30.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif40
 ip address 192.168.40.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif50
 ip address 192.168.50.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
```

```
interface Vlanif150
 ip address 192.168.150.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 150
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 dhcp snooping trusted
#
interface GigabitEthernet0/0/10
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/11
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/12
 port hybrid pvid vlan 100
```

```
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/13
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/14
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
#
```

```
interface LoopBack0
 ip address 10.10.10.10 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 10.10.10.10
 area 0.0.0.0
  network 192.168.150.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
  network 192.168.30.0 0.0.0.255
  network 192.168.40.0 0.0.0.255
  network 192.168.50.0 0.0.0.255
  network 10.10.10.10 0.0.0.0
#
traffic-filter vlan 20 inbound acl 3020
traffic-filter vlan 30 inbound acl 3030
traffic-filter vlan 40 inbound acl 3040
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
ssh client first-time enable
ssh client 192.168.10.2 assign rsa-key 192.168.10.2
ssh client 192.168.20.2 assign rsa-key 192.168.20.2
ssh client 192.168.30.2 assign rsa-key 192.168.30.2
ssh client 192.168.40.2 assign rsa-key 192.168.40.2
ssh client 192.168.50.2 assign rsa-key 192.168.50.2
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

BBS2;

```
<BBS2> display current-configuration
#
sysname BBS2
#
vlan batch 10 20 30 40 50 60 100 160
#
stp instance 1 root secondary
stp instance 2 root primary
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
```

```
#
dhcp snooping enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
rsa peer-public-key 192.168.10.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.20.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.30.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.40.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
rsa peer-public-key 192.168.50.2
 public-key-code begin
 public-key-code end
peer-public-key end
#
acl number 3020
 rule 5 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.30.0 0.0.0.255
 rule 10 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.40.0 0.0.0.255
 rule 15 deny icmp source 192.168.20.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
acl number 3030
 rule 5 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
 rule 10 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.40.0 0.0.0255
 rule 15 deny icmp source 192.168.30.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
acl number 3040
 rule 5 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
 rule 10 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.30.0 0.0.0.255
 rule 15 deny icmp source 192.168.40.0 0.0.0.255 destination 192.168.50.0 0.0.0.255
 rule 20 permit icmp
#
```

```
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif30
 ip address 192.168.30.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif40
 ip address 192.168.40.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif50
 ip address 192.168.50.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 8.8.8.8
#
interface Vlanif160
 ip address 192.168.160.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 160
 port trunk allow-pass vlan 2 to 4094
#
interface GigabitEthernet0/0/4
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 dhcp snooping trusted
#
interface GigabitEthernet0/0/10
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
```

```
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/11
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/12
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/13
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
```

```
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface GigabitEthernet0/0/15
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp root-protection
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping alarm dhcp-request enable
 dhcp snooping alarm dhcp-request threshold 200
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr enable
 dhcp snooping alarm dhcp-chaddr threshold 200
 dhcp snooping alarm dhcp-reply enable
 dhcp snooping alarm dhcp-reply threshold 200
 dhcp snooping max-user-number 20
#
interface LoopBack0
 ip address 20.20.20.20 255.255.255.0
 ospf network-type broadcast
#
ospf 1 router-id 20.20.20.20
 area 0.0.0.0
  network 192.168.160.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
  network 192.168.30.0 0.0.0.255
  network 192.168.40.0 0.0.0.255
  network 192.168.50.0 0.0.0.255
  network 20.20.20.20 0.0.0.0
#
traffic-filter vlan 20 inbound acl 3020
traffic-filter vlan 30 inbound acl 3030
traffic-filter vlan 40 inbound acl 3040
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
```

```
ssh user cebrayil service-type stelnet
ssh client first-time enable
ssh client 192.168.10.2 assign rsa-key 192.168.10.2
ssh client 192.168.20.2 assign rsa-key 192.168.20.2
ssh client 192.168.30.2 assign rsa-key 192.168.30.2
ssh client 192.168.40.2 assign rsa-key 192.168.40.2
ssh client 192.168.50.2 assign rsa-key 192.168.50.2
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
Return
```

LSW1;

```
<LSW1> display current-configuration
#
sysname LSW1
#
vlan batch 10 20 30 40 50 60 70 100
#
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif10
 ip address 192.168.10.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
```

```
interface Ethernet0/0/3
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/10
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
interface Ethernet0/0/11
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

LSW2;

```
<LSW2> display current-configuration
#
sysname LSW2
#
vlan batch 10 20 30 40 50 60 70 100
#
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
aaa
 local-user cebrayil password cipher huawei!123
```

```
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif20
 ip address 192.168.20.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 20
#
interface Ethernet0/0/10
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
interface Ethernet0/0/11
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

LSW3;

```
<LSW3> display current-configuration
#
sysname LSW3
#
vlan batch 10 20 30 40 50 60 70 100
#
stp bpdu-protection
```

```
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif30
 ip address 192.168.30.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 30
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 30
#
interface Ethernet0/0/12
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
interface Ethernet0/0/13
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
#
user-interface con 0
user-interface vty 0 4
```

```
 authentication-mode aaa
 protocol inbound all
#
return

LSW4;
<LSW4> display current-configuration
#
sysname LSW4
#
vlan batch 10 20 30 40 50 60 70 100
#
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif40
 ip address 192.168.40.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 40
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 40
#
interface Ethernet0/0/12
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
```

```
interface Ethernet0/0/13
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

LSW5;

```
<LSW5> display current-configuration
#
sysname LSW5
#
vlan batch 10 20 30 40 50 60 70 100
#
stp bpdu-protection
stp pathcost-standard legacy
stp tc-protection
#
dhcp enable
#
stp region-configuration
 region-name MSTP1
 instance 1 vlan 10 20 30 40 50 60 100
 instance 2 vlan 70
 active region-configuration
#
aaa
 local-user cebrayil password cipher huawei!123
 local-user cebrayil privilege level 15
 local-user cebrayil service-type telnet ssh
#
interface Vlanif50
 ip address 192.168.50.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 100
#
interface Ethernet0/0/2
```

```
 port link-type access
 port default vlan 50
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 50
#
interface Ethernet0/0/14
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
interface Ethernet0/0/15
 port hybrid pvid vlan 100
 port hybrid tagged vlan 10 20 30 40 50 60 70
 port hybrid untagged vlan 100
 stp loop-protection
#
stelnet server enable
ssh user cebrayil
ssh user cebrayil authentication-type password
ssh user cebrayil service-type stelnet
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

ÖZGEÇMİŞ

Ad-Soyad **:** Jabrayil ALİZADA
E-Posta **:** cebrayilelizade@gmail.com

KİŞİSEL BİLGİLER

Doğum Tarihi ve Yeri **:** 28/11/1991/ Azerbaycan, Lenkeran
Medeni Durum **:** Bekar
Askerlik Durumu **:** Tamamlandı (2012-2013)

EĞİTİM BİLGİLERİ

Lisans **:** Azerbaycan Devlet Petrol Akademisi / Otomatik ve Yönetim
Yüksek Lisans **:** İstanbul Aydın Üniversitesi / Bilgisayar Mühendisliği

SERTİFİKA BİLGİLERİ

Microsoft Certified Professional : Microsoft Certified Professional (29/03/2016)
Microsoft Certified Solutions Associate : Windows Server 2012 (08/06/2016)
Microsoft Certified Solutions Expert : Messaging (08/06/2016)
Microsoft Certified Solutions Expert : Server Infrastructure (17/08/2016)
Network Academy Information Technology : MCSE (23/05/2016)

BİLGİSAYAR BİLGİSİ

Windows server 7-8-10
Windows Server 2012r2
Exchange Server 2016
HTML, CSS
JavaScript
CISCO