İDEAL KAMPÜS AĞ YAPISININ TASARIMI VE GÜVENLİK PERFORMANSININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

İsmail ARIK

Danışman
Doç. Dr. Uçman ERGÜN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ
YÖNETİMİ ANABİLİM DALI

Ocak 2017

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İDEAL KAMPÜS AĞ YAPISININ TASARIMI VE GÜVENLİK PERFORMANSININ DEĞERLENDİRİLMESİ

İsmail ARIK

Danışman
Doç. Dr. Uçman ERGÜN

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

Ocak 2017

TEZ ONAY SAYFASI

İsmail ARIK tarafından hazırlanan "İdeal Kampüs Ağ Yapısının Tasarımı ve Güvenlik Performansının Değerlendirilmesi" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 27/01/2017 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Uçman ERGÜN

İmza

Başkan : Yrd. Doç. Dr. Süleyman A. SULAK
Necmettin Erbakan Üniv., A. K. Eğitim Fak.

Üye : Doç. Dr. Uçman ERGÜN
Afyon Kocatepe Üniv., Mühendislik Fak.

Üye : Yrd. Doç. Dr. Mehmet Eyüp KİRİŞ
Afyon Kocatepe Üniv., Fen Edebiyat Fak.

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. Hüseyin ENGİNAR
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI
Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

30/01/2017

İsmail ARIK

ÖZET

Yüksek Lisans Tezi

İDEAL KAMPÜS AĞ YAPISININ TASARIMI VE
GÜVENLİK PERFORMANSININ DEĞERLENDİRİLMESİ

İsmail ARIK
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Doç. Dr. Uçman ERGÜN

Kampüs ağlarının büyümesi ve ağ cihazlarının artması sebebi ile ağın yönetimi ve problemlere müdahale süreci zorlaşmaktadır. Bu kapsamda; üniversite ağ yapıları incelendiğinde ağ yapısında problemler görülebilmekte, yedeği olmayan ağ yapısı kullanılmakta, kampüs ağında çalışmakta olan cihazların yapılandırma eksikliklerinden kaynaklanan sorunlar bulunabilmekte, ağ güvenliği tam olarak sağlanamamaktadır.

Bu çalışmada, laboratuvar ortamında yedekli bir ağ yapısı kurulmuştur. İç ağ üzerinden yapılabilecek olası saldırılara karşı gerekli güvenlik önlemleri alınarak güvenli bir ağ sistemi kurulmuştur. Kablosuz ağ üzerinde ise kimlik doğrulama yöntemi kullanılarak ağ güvenliği sağlanmaya çalışılmıştır. Böylece güvenlik ve performans bakımından daha verimli ve farklı lokasyonlarda oluşabilecek sorunlara daha kolay çözümler üretilebilecek bir altyapı tasarımı oluşturulmuştur.

2017, xvii + 119 sayfa

Anahtar Kelimeler: Kampüs Ağları, Kablosuz Ağ, Ağ Yönetimi, Ağ Güvenliği, Ağ Cihazları.

ABSTRACT

M.Sc Thesis

DESIGNING AN IDEAL CAMPUS NETWORK STRUCTURE AND EVALUATION OF SECURITY PERFORMANCE

İsmail ARIK

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Assoc. Prof. Uçman ERGÜN

By the growing of campus network and increasing network devices, it becomes more difficult to manage and troubleshoot network problems. When examining university networks in this context there can be seen problems due to non-redundant network system usage, lack of configuration of devices running on the campus network, not fully insured network security.

In this study, in the laboratory environment, established a stable network system by providing backup of network system and taking security measures against possible attacks that could be made over the internal network. On the wireless network, security measures are taken by using the authentication method. In this way, a network system is designed which is more efficient in terms of security and performance, including easy troubleshooting of problem appeared in different location of the campus.

2017, xvii + 119 pages

Key Words: Campus Networks, Wireless Network, Network Management, Network Security, Network Devices.

TEŞEKKÜR

Bu çalışmanın ortaya çıkmasında, çalışmamın yönlendirilmesinde, sonuçların değerlendirilmesinde ve yazımı aşamasında desteğini esirgemeyen tez danışmanım Sayın Doç. Dr. Uçman ERGÜN'e, çalışma konusunda vermiş olduğu desteğinden dolayı Sayın Öğr. Gör. Suikum KARASARTOVA'ya, Bilgisayar Mühendisi Emre AMBARKÜTÜKOĞLU'na ve Bilgi İşlem Daire Başkanlığındaki diğer değerli mesai arkadaşlarıma teşekkürü bir borç bilirim.

Tez süresinde yanımda olan ve beni yalnız bırakmayan aileme teşekkür ederim.

İsmail ARIK

AFYONKARAHİSAR, 2017

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Kısaltmalar

ACL	Access Control List (Erişim Kontrol Listesi)
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standartları)
AP	Access Point (Erişim Cihazı)
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
ARPANET	Advanced Research Projects Agency Network (Gelişmiş Araştırma Projeleri Dairesi Ağı)
ASP	Active Server Pages (Aktif Sunucusu Sayfaları)
ATM	Asynchronous Transfer Mode (Eşzamansız Aktarım Modu)
BGP	Border Gateway Protocol (Sınır Ağ Geçidi Protokolü)
BPDU	Bridge Protocol Data Units (Köprü Protokolü Veri Birimi)
CAM	Content Address Memory (Adres Belleği İçeriği)
CAN	Campus Area Network (Kampüs Alan Ağı)
CENTOS	The Community Enterprise Operating System (Topluluk Kurumsal İşletim Sistemi)
CN	Common Name (Yaygın İsim)
CPU	Central Processing Unit (Merkezi İşlem Birimi)
CRC	Cyclic Redundancy Check (Hata Kontrol Kodu)
DARPA	The Defense Advanced Research Projects Agency (Savunma Bakanlığı İleri Araştırma Projeleri Ajansı)
DC	Domain Controller (Etki Alanı Denetleyicisi)
DCA	Defence Communication Agency (Savunma İletişim Ajansı)
DHCP	Dynamic Host Configuration Protocol (Dinamik Bilgisayar Konfigurasyon Protokolü)
DNS	Domain Name System (Alan Adı Sistemi)
DDoS	Distributed Denial of Service (Dağıtılmış Hizmeti Engelleme Saldırısı)
DoS	Denial of Sevice (Hizmet Reddi)
DPI	Deep Packet Inspection (Derinlemesine Paket Denetimi)
DSL	Digital Subscriber Line (Sayısal Abone Hattı)

DTP	Dynamic Trunk Protocol (Dinamik Gövdem Protokolü)
EAP	Extensible Authentication Protocol (Genişletilebilir Kimlik Doğrulama İletişim Kuralı)
EBYS	Elektronik Belge Yönetim Sistemi
EIA	Electronic Industries Association (Elektronik Sanayicileri Derneği)
FDDI	Fiber Distributed Data Interface (Fiber Dağıtılmış Veri Arabirimi)
FTP	File Transfer Protocol (Dosya İletim Protokolü)
GSM	Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)
G.SHDSL	Symmetric High Bit Rate Digital Subscriber Line (Simetrik Yüksek Bit Hızı Dijital Abone Hattı)
HDSL	High Bit Rate Digital Subscriber Line (Yüksek Bit Hızı Dijital Abone Hattı)
HSRP	Hot Standby Router Protocol (Hızlı Yedekli Yönlendirme Protokolü)
HTTP	Hyper Text Transfer Protocol (Hiper Metin Aktarım Protokolü)
HTTPS	Secure Hypertext Transfer Protocol (Güvenli Hiper Metin Aktarım Protokolü)
ICMP	Internet Control Message Protocol (İnternet Kontrol Mesaj İletişim Kuralı)
ID	Identification (Kimlik)
IDS	Intrusion Detection System (Saldırı Tespit Sistemi)
IEEE	The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IGMP	Internet Group Management Protocol (İnternet Grup Yönetim Protokolü)
IGRP	Interior Gateway Routing Protocol (Dahili Ağ Geçidi Yönlendirme Protokolü)
IIS	Internet Information Service (İnternet Bilgi Servisi)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemi)
IPX	Internetwork Packet Exchange (Ağlararası Paket Değişimi)
IR	Infrared (Kızıl Ötesi)
ISDN	Integrated Services Digital Network (Bütünleşik Hizmetler Dijital Ağı)

ISO	The International Organization for Standardization (Uluslararası Standartlar Organizasyonu)
IPv4	Internet Protocol Version 4 (İnternet Protokolü Sürüm 4)
IPv6	Internet Protocol Version 6 ((İnternet Protokolü Sürüm 6)
JPEG	Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
LACP	Link Aggregation Control Protocol (Hat Birleştirme Kontrol Protokolü)
LAN	Local Area Network (Yerel Alan Ağı)
LDAP	Lightweight Directory Access Protocol (Basit İndeks Erişim Protokolü)
LLC	Logical Link Control (Mantıksal Bağlantı Kontrolü)
L2	Layer 2 (OSI 2.Katman)
L3	Layer 3 (OSI 3. Katman)
M	Meter (Metre)
MAC	Media Access Control (Ortam Erişim Yönetimi)
MAN	Metropolitan Area Network (Kentsel Alan Ağı)
Mbps	Mega Bit Per Second (Saniyede Aktarılan Megabit Miktarı)
MILNET	Military Network (Askeri Ağ)
MITM	Man In The Middle (Aradaki Adam)
MPEG	Moving Picture Experts Group (Hareketli Görüntü Uzmanları Birliği)
NGFW	Next Generation Firewall (Yeni Nesil Güvenlik Duvarı)
NetBEUI	NetBIOS Extended User Interface (NetBIOS Genişletilmiş Kullanıcı Arayüzü)
NetBIOS	Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi)
NFS	Network File System (Ağ Dosya Sistemleri)
OSI	Open Systems Interconnection (Açık Sistemler Bağlantısı)
OSPF	Open Shortest Path First (Öncelikli Olarak Kısa Rotayı Kullan)
OU	Organizational Unit (Kuruluş Birimi)
QoS	Quality of Service (Servis Kalitesi)
RADIUS	Remote Authentication Dial-in User Service (Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti)
RARP	Reverse Address Resolution Protocol (Ters Adres Çözümleme Protokolü)
RF	Radio Frequency (Radyo Frekansı)

RHEL	Red Hat Enterprise Linux
RIP	Router Information Protocol (Yönlendirme Bilgisi Protokolü)
RSA	Rivest-Shamir-Adleman (Rivest-Shamir-Adleman)
SDH	Synchronous Digital Hierarchy (Senkron Sayısal Hiyerarşi)
SMTP	Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SNMP	Simple Network Management Protocol (Basit Ağ Yönetim Protokolü)
SPX	Sequenced Packet Exchange (Sıralı Paket Değişimi)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SSID	Service Set Identifier (Servis Seti Tanımlayıcısı)
SSL	Secure Sockets Layer (Güvenli Soket Katmanı)
STP	Spanning Tree Protocol (Kapsayan Ağaç Protokolü)
TB	Terabyte (Terabyte)
TCP	Transmission Control Protocol (İletim Denetim Protokolü)
TCP/IP	Transmission Control Protocol / Internet Protocol (Geçiş Kontrol Protokolü / İnternet Protokolü)
TIA	Telecommunication Industry Association (Telekomünikasyon Endüstrisi Kurumu)
TIFF	Tagged Image File Format (Etiketli Resim Dosyası Biçimi)
TKIP	Temporal Key Integrity Protocol (Geçici Anahtar Bütünlüğü Protokolü)
TTLS	Tunneled Transport Layer Security (Tünelli Taşıma Katmanı Güvenliği)
UTM	Unified Threat Management (Birleşik Tehdit Yönetimi)
UTP	Unshielded Twisted Pair (Korumasız Bükümlü Kablo)
UDP	User Datagram Protocol (Kullanıcı Veri Bloğu İletişim Protokolü)
URL	Uniform Resource Locator (Standart Kaynak Bulucu)
VPN	Virtual Private Network (Sanal Özel Ağ)
VSS	Virtual Switching System (Sanal Anahtarlama Sistemi)
VLAN	Virtual Local Area Network (Sanal Yerel Alan Ağı)
WAN	Wide Area Network (Geniş Alan Ağları)
WEP	Wired Equivalent Privacy (Kabloluya Eşdeğer Gizlilik)
Wi-Fi	Wireless Fidelity (Kablosuz Bağlantı Alanı)
WLAN	Wireless Local Area Network (Kablosuz Yerel Alan Ağı)
WLC	Wireless LAN Controller (Kablosuz Yerel Alan Ağı Kontrol Cihazı)

WPA	Wi-Fi Protected Access (Wi-Fi Korunmuş Erişim)
WPA-PSK	Wi-Fi Protected Access Pre-Shared Key (Wi-Fi Korunmuş Erişim Ön Paylaşımlı Anahtar)
WMAN	Wireless Metropolitan Area Network (Metropol Kablosuz Ağlar)
WPAN	Wireless Personal Area Network (Kablosuz Kişisel Alan Ağları)
WWAN	Wireless Wide Area Network (Kablosuz Geniş Alan Ağları)

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

RESİMLER DİZİNİ

Sayfa

1. GİRİŞ

Günümüzde internet hedeflere ve amaçlara ulaşmak için kullanılan bir araç niteliği olarak karşımıza çıkmaktadır. Son zamanlarda hızla gelişen teknolojiye insanlar da ayak uydurmaya başlamış son teknoloji ürünler hayatımıza girmiştir.

Hacker adı verilen bilgisayar korsanlarının çoğalması ile siber tehditler artmıştır. Yeterli güvenlik tedbirleri alınmayan üniversite ağları bu saldırılardan en çok etkilenen kurumların başında gelmektedir.

Günümüz teknolojisi ile üretilen ağ cihazları gelişen teknolojiye ve günümüz ihtiyaçlarına göre üretilmekte, güvenlik gereksinimleri şekillenmektedir. Özellikle bilişim suçlarının son dönemlerde artış göstermesi güvenlik zafiyetlerinin gözden geçirilmesi ve bu suçlara karşı yeni önlemler alınması gerekliliğini ortaya koymuştur.

Üniversitelerde kampüs ağları sürekli gelişen teknolojiye göre şekillenmekte ve ihtiyaçlarına göre de yapı olarak değişiklik göstermektedir. Günümüzde geleneksel ağ altyapıları artık güncelliğini kaybetmiştir. Ağ büyüdükçe bu ağın yönetimi ve olası bağlantı problemleri ile oluşan sorunların giderilmesi zorlaşmaktadır.

Bu çalışmanın amacı, kampüs ağlarında ideal bir ağ altyapısı nasıl tasarlanmalı, ağ tasarımı yapılırken dikkat edilecek hususlar ve alınabilecek güvenlik önlemleri vb. konuları inceleyerek laboratuvar ortamında ve örnek mimari projeler üzerinde kablolu ve kablosuz ağ tasarımı kriterlerini belirleyerek optimum kablolu ve kablosuz ağ cihazı yerleşim modeli tasarımı yapmaktır.

Bu çalışmanın, sürekli gelişen teknoloji paralelinde ihtiyaçlara göre çeşitlilik gösteren ve büyüdükçe de yönetimi zorlaşan üniversite ağları için yönetim ve problemlere çözümler üretilmesi bakımından kolaylık sağlayacağı düşünülmektedir. Yapılan çalışma ile tasarım mimarisi, güvenlik ve performans bakımından daha etkin, güvenli ve verimli ağ yapısı ortaya koyulacaktır.

Bu çalışma sonucunda kampüs ağının yönetiminin kolaylaşacağı, kampüs ağının sorunlarının daha rahat çözümlenebilmesi konusunda planlamalar yapılabilecek ve farklı lokasyonlarda oluşabilecek sorunlara daha kolay çözümler üretilebilecek bir altyapı tasarımı oluşması sağlanacaktır.

Çalışma esnasında kullanılan ağ cihazları Hitit Üniversitesi bünyesinde kullanılan gerçek cihazlar olup, cihazların bu çalışmada kullanılması için gerekli izinler alınmıştır.

Bu çalışmanın ikinci bölümünde literatürde ağ çeşitleri ve ağ teknolojileri üzerinde durulmuş, ağ güvenliği ve ağ cihazları ele alınmıştır.

Üçüncü bölümde ise örnek bir binada ideal olabilecek kablolu ve kablosuz ağ altyapısı tasarımı yapılmış, kablosuz ağ cihazları kapsama alanları incelenerek uygun konumlandırma işlemi yapılmıştır. Laboratuvar ortamında kurulan yedekli ağ yapısı adımları üzerinde durulmuş, ağ cihazları üzerinde tanımlanan güvenlik önlemleri ele alınmıştır.

Çalışmanın dördüncü bölümünde ise kurulan yedekli ağ yapısı üzerinde senaryolar kurgulanmış, olası güvenlik zafiyetleri incelenmiş, zafiyetlere karşı alınan tedbirlerin uygulanabilirliği ve sonuçları incelenmiştir. Kampüs bulguları ve ağ trafik analizi ele alınmıştır.

Uygulama sonucunda yedekli ideal olabilecek bir ağ tasarımı yapılmış, ağ yapısı analiz edilmiştir. Böylece yedekli sağlıklı bir yapı kurulmasının yanı sıra güvenlik ve performans bakımından daha etkin, hızlı ve sağlıklı bir ağ yapısı ortaya koyulmaya çalışılmıştır.

2. LİTERATÜR BİLGİLERİ

2.1 Ağ (network) nedir?

Ağ, iki veya daha fazla cihazın bir araya getirilerek veri paylaşımını sağlayan oluşumdur. Bu oluşum iki cihaz ile yapılabileceği gibi ikiden fazla cihazın bir araya getirilmesi ile de oluşturulabilir. Günümüzde bilgisayarların hayatımızda hemen hemen her alana girmesi, internet maliyetinin düşmesi ile ağ kullanımının yaygınlaşmasını sağlamıştır. Kablosuz ağ kullanımı her geçen gün artış göstermesine rağmen kablolu bağlantı ağ yapılarının vazgeçilmezidir. Büyük ya da küçük bütün sistemlerin altyapısında kablo kullanılmaktadır (İnt.Kyn.1).

2.1.1 Ağ Çeşitleri

Bilgisayar ağları büyüklüklerine göre çeşitli türlere ayrılır.

LAN (Local Area Network): Birbirine yakın binalar, birimler veya yerleşkeler içerisinde kullanılan bilgisayar ağı cihazlarının aralarında görüşmesini sağlayan bilgisayar ağı yapısıdır. En az iki bilgisayar ağı cihazından başlayıp yüzlerce bilgisayar ağı cihazını kapsayacak büyüklüklere ulaşabilen bir kapasiteye sahiptir.

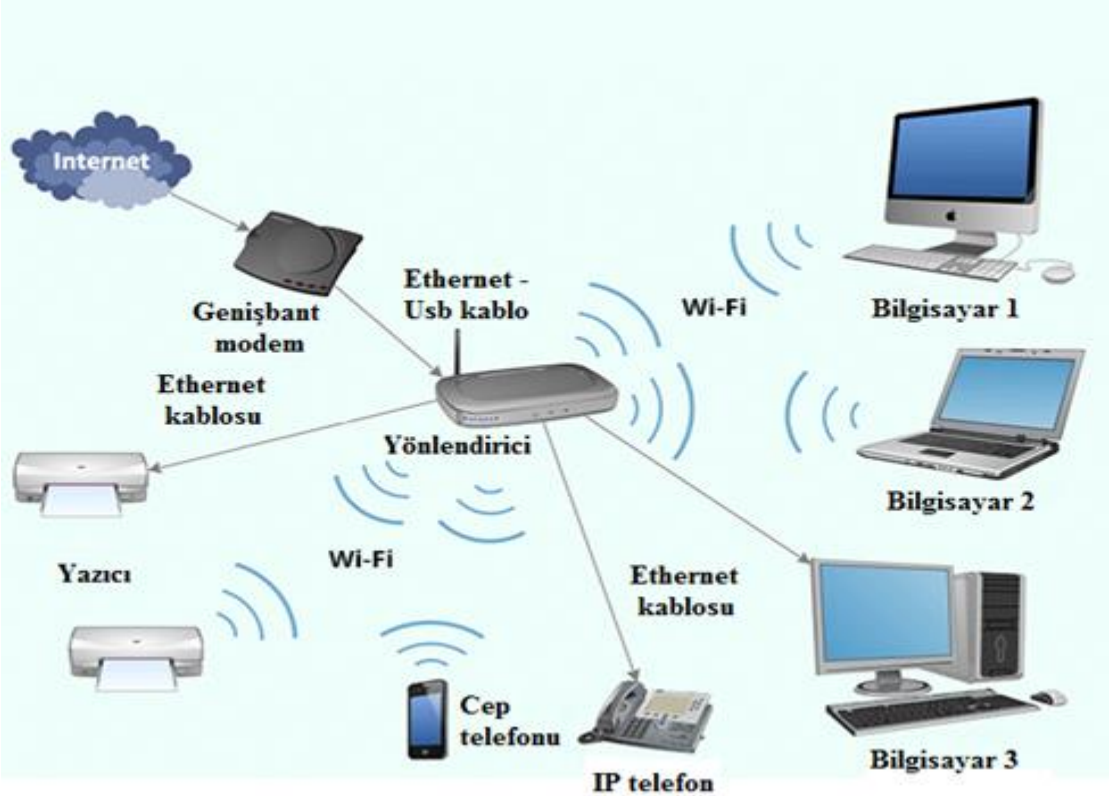
WAN (Wide Area Network): Farklı LAN yapılarının Türk Telekom gibi çeşitli servis sağlayıcılar aracılığı ile iletişim kurmasını sağlayıp uzak mesafelerdeki bilgisayar ağı cihazlarının birbirleri ile görüşmesini gerçekleştiren bilgisayar ağı yapısıdır (Tutkun 2011).

MAN (Metropolitan Area Network): LAN ile WAN arasında bir büyüklüğe sahiptir. Yüksek hızlı bant genişliği sunabilir. Bir kasabayı, şehir içindeki bir alanı ya da şehrin tamamını kapsar. MAN'ın ilk örnekleri olarak kablolu televizyon için tasarlanan kablolu televizyon şebekesi gösterilebilir. Günümüzde bu şebeke aynı zamanda yüksek hızlı internet erişim imkânı da sunmaktadır. Diğer bir örnek ise telefon

şirketleridir. Bu şirketler müşterilerine yüksek hızlı DSL (Digital Subscriber Line) sağlayabilmektedir (Forouzan 2007).

VPN (Virtual Private Network): Paketlerin tünel vasıtası ile iletildiği ve iletim sırasında data paketlerinin şifrelenerek gönderildiği güvenli bir ağdır. Veri paketi iletimi sırasında veri gönderen ve veriyi alan ağ şifrelenmektedir (İnt.Kyn.2).

Kablosuz Ağ: İki nokta arasında veri, ses veya görüntü taşınması işleminin kablosuz olarak yapılması işlemidir (Şekil 2.1). Bina ve kampüs gibi sınırlı alanda kullanılan iletim ortamı olarak IR (Infrared) ve RF (Radio Frequency) kullanan kablosuz ağ, farklı güç ve kapasite ve kapsama alanlarına sahiptir. Kablosuz ağlar WPAN (Wireless Personal Area Network), WLAN (Wireless Local Area Network), WMAN (Wireless Metropolitan Area Network) ve WWAN (Wireless Wide Area Network) olarak sınıflandırılmıştır (Yılmaz ve Öztürk 2007).



Şekil 2.1 Kablosuz ağlar (İnt.Kyn.3).

2.1.2 Kampüs Ağı (Network)

Bir Kampüs ağı, binaları bağlayan ve sınırlı bir coğrafi alanda iki veya daha fazla LAN'dan oluşan bir bilgisayar ağıdır. Kampüs ağı olarak üniversite kampüsü, kurumsal kampüs, endüstriyel kompleks, askeri üs ve ofis binaları olabilir. Kampüs ağlarında eskiden kullanılan ATM (Asynchronous Transfer Mode) ve Token Ring teknolojileri kullanım dışı kalmıştır. Günümüzde Gigabit Ethernet ve Metro Ethernet gibi gelişmiş LAN teknolojileri kullanılır (İnt.Kyn.4).

Kampüs ağı farklı binalarda ya da yerleşkelerde bulunan LAN'ların birleşimi sonucu oluşmuştur. Kolej ve üniversite kampüs ağları ise idari binalar, konut salonları, akademik salonları, kütüphaneler, öğrenci merkezleri, spor tesisleri ve belirli bir kent veya mahallede kurum ile ilişkili diğer binaları birbirine bağlar. Kampüs ağının büyümesi, ağın yönetimini ve ağ içinde oluşan problemlerin çözümünü zorlaştırmaktadır.

İdeal durumda, bir kampüs ağında Gigabit Ethernet veya 10-Gigabit Ethernet teknolojisinin avantajlarından yararlanarak, fiber optik medya vasıtası ile bağlanır. Son kullanıcılarda ise 1 Gigabit Ethernet ya da kablosuz bağlantı yöntemi kullanılır. Üniversite öğrenci merkezleri veya kütüphanelerde pek çok kişi aynı anda ağa dahil olarak dizüstü ve tablet bilgisayarlar gibi taşınabilir ve mobil cihazlar kullanarak araştırma yapabilirler (İnt.Kyn.5).

Birden çok yerleşke içerisinde çok sayıda binadan oluşan kampüs ağlarında belirli toplama noktalarından ana merkeze fiber optik kablolar vasıtası ile bağlantı sağlanmaktadır. Bu bağlantı için Metro Ethernet'in yanında Gigabit Ethernet ve az da olsa Fast Ethernet teknolojileri kullanılmaktadır. Kullanıcı bilgisayarları, UTP (Unshielded Twisted Pair) kablolar vasıtası ile anahtarlayıcı (switch), yönlendirici (router) vb. aktif iletişim cihazlarına bağlanarak LAN'a dâhil olur. Bu aktif cihazlardan oluşan LAN'ların da fiber optik kablolar ve UTP kablolar vasıtası ile ana omurga cihazlarına (backbone) bağlanması sonucunda kampüs yerleşke ağı ortaya çıkar. Son kullanıcıların bu ağa dâhil olması için kablolu bağlantının yanı sıra

kablosuz bağlantı yöntemi de kullanılır. Çok sayıda bilgisayar ve aktif cihazlardan oluşan bu kompleks yapının yönetimi zordur. Yönetiminin kolaylaşması için bu büyük ağ, VLAN (Virtual Local Area Network)'lara bölünür (Karaarslan 2005).

2.1.2.1 Kampüs Ağı Bağlantı Türleri

Kampüs ağları farklı yapıları olan yerleşkelerde oluştuğu için bu yerleşkelerin bağlantı yöntemleri de farklılık göstermektedir. En çok kullanılan bağlantı yöntemleri aşağıdaki gibidir.

- G.SHDSL (Symmetric High Bit Rate Digital Subscriber Line): Farklı lokasyonlar arasında iletişim imkânı sağlayan bu teknoloji, bağlantı maliyeti düşük olmasına karşı sanal devrelerin tanımlanması ile güvenli bir bağlantı olanağı sağlayan bir teknolojidir. Bu bağlantı türünde bağlantı hızı 2 Mbps (Mega Bit Per Second) üzerine çıkamaz.
- Frame Relay: OSI (Open Systems Interconnection) referans modeline göre fiziksel ve veri bağı katmanlarında çalışan, yüksek performansa sahip uzak alan bağlantı protokolüdür. Bant genişliğinin daha esnek kullanımına imkân tanıdığından, kullanıcı açısından daha ekonomik bir çözüm sunar. HDSL (High Bit Rate Digital Subscriber Line) modüllü sayısal modemler ya da mevcut SDH (Synchronous Digital Hierarchy) üzerinden alınan E1'ler vasıtasıyla Frame Relay bağlantısı yapılabilir. Bu teknoloji kullanıldığında en fazla 2 Mbps bağlantı hızına ulaşılabilir.
- Metro Ethernet: Fiber optik kablolar üzerinden internet erişimi sağlanan bu bağlantı yöntemi günümüzde kurumsal firmalar, organize sanayi bölgeleri, oteller, orta ve büyük ölçekli şirketler ile kamu kurum ve kuruluşlarında en çok kullanılan bağlantı yöntemlerinden birisidir. Metro Ethernet ile farklı lokasyonlar arasında fiber üzerinden kesintisiz, hızlı, güvenli ve yüksek kalitede internet bağlantısı sağlanmaktadır.
- Radio Link: İki farklı nokta arasında iletişim kurmak için kullanılan bu sistem elektromanyetik dalgalar kullanılır. İletişimin zor olduğu koşullarda ve santraller arası iletişim kurulması için bu bağlantı yöntemi tercih edilmektedir. Fiber kablonun gidemediği bölgelerde uygulanması daha uygun olan Radio

Link ile yüksek bant genişliği sağlanabilir. Bu bağlantı türünde elektromanyetik dalgalar dar bir koridorun izlenmesi sonucunda hedef noktaya ulaşır. Verinin aktarılması sırasında kullanılan yolun dışına veriler kolay bir şekilde çıkamaz (İnt.Kyn.6).

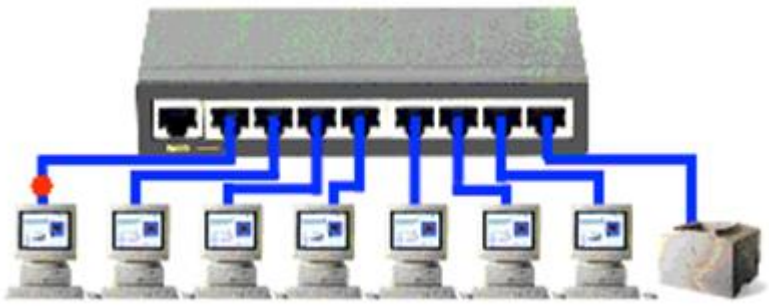
- Kiralık Hatlar: Kiralık hat, herhangi bir telekomünikasyon firmalarından kiralanmış, kablolu uçtan uca veri iletişim hattıdır. Bir noktadan başka bir noktaya bağlantı imkânı sağlayan kiralık devreler, sabit bant genişliğine sahip internet hatlarıdır.

2.1.2.2 Kampüs Ağ Bileşenleri

2.1.2.2.1 Hub

OSI birinci katmanda çalışan bu donanımlar bir porttan aldığı sinyalin genliğini yükselterek sinyali diğer bütün portlardan gönderirler. Bir porttan gelen veri paketini hub'a bağlı tüm bilgisayarlar alabilirler. Aynı hub'a bağlı bilgisayarlar çarpışma alanını oluştururlar.

Port sayısının yetersiz olduğu durumlarda hub kullanma ihtiyacı hissedilir. Fakat arka arkaya bağlanacak birkaç hub sonucunda dolaylı olarak bilgisayarlar birbirine bağlanacağından çarpışma alanı genişleyecektir. Veri sinyalinin defalarca yükseltilmesi ile çarpışma alanı aşırı büyüyecek ve ağda tıkanmalar yaşanacaktır. Bu sebeple ağ trafiğinin yoğun olduğu yerel ağlarda hub yerine anahtarlayıcı (switch) kullanılmalıdır (Şekil 2.2).



Şekil 2.2 Hub (İnt.Kyn.7)

2.1.2.2.2 Anahtarlayıcı (Switch)

Yerel ağlarda bilgisayarları birbirine bağlamak için hub'ların yanında anahtarlayıcıların (switch) da kullanılabilir olması iki ağ cihazının birbirine alternatif donanım cihazları olduğu izlenimini yaratmaktadır. Ancak anahtarlar akıllı cihazlardır. Ağ trafiğinde tıkanmaların oluşmaması için yoğun kullanımın olduğu ağlarda hub yerine anahtarlar kullanılır (Resim 2.1).

Yerel ağ anahtarları gelen bir paketin hangi porttan gönderilmesi gerektiğini bilir. Ağdaki yayın paketlerini anahtarlayıcıların (switch) dinlemesi sonucunda portlara bağlı olan tüm bilgisayarların MAC (Media Access Control) adreslerini öğrenerek bir tabloya yazarlar. Anahtarın bir porttan aldığı veri paketini başka bir porta göndermesi sonucunda paket hedefe iletilmiş olur. MAC adresleri kullanılarak anahtarın yaptığı bu işlem "iletme" (forwarding) olarak tanımlanır. Anahtarlar bir yayın alanı içerisinde birden fazla çarpışma alanı oluşturmak için kullanılır. Hub kullanıldığında tek çarpışma alanı oluşurken, anahtar kullanıldığında her bir port ayrı bir çarpışma alanı oluşturacaktır. Böylece yerel ağın performansı da artacaktır (Özbilen 2005).

Resim 2.1 Anahtarlama cihazı (İnt.Kyn.8).

ACL (Access Control List) yönlendirici çok yönlü ağın parçalarıdır. ACL'leri yapılandırma ve doğru kullanım yönlendirici (router) yapılandırmasının önemli bir parçasıdır. Ağ yöneticilere paket akışları ile ilgili temel istatistikleri toplama, tüm trafiği büyük ölçüde kontrol etmelerine imkân tanıyarak güvenlik politikaları

uygulama imkânı sağlar. Hassas cihazlar yetkisiz erişimlere karşı korunabilir ya da erişimlere izin verilebilir.

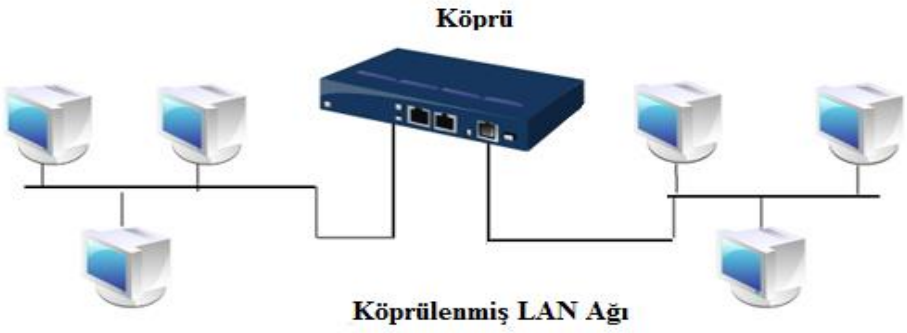
ACL filtreleme sorununu çözmek için etkili bir yoldur. Yönlendirici (router) ve benzer cihazlarda kaynak ve hedef IP (Internet Protocol) adreslerini kontrol ederek trafiğin ağ geçidi üzerinden geçmelerine izin verir ya da engeller. Standart ACL sadece kaynak IP adresine göre filtreleme yapar. Genişletilmiş ACL'ler ise network katmanlarında ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol) ya da IP protokolü kullanarak filtreleme olanağı sağlar. TCP (Transmission Control Protocol) ya da UDP (User Datagram Protocol) ulaşım katmanında belirli port numaraları veya belirli adresler arasında belirli hizmetlere izin vermek ya da engellemek için IP bazlı filtreleme yapılır. ACL'ler ayrıca AppleTalk, IPX (Internetwork Packet Exchange) gibi diğer yönlendirme protokollerini kontrol edebilir. Ayrıca ACL uygunsuz trafiği ortadan kaldırmak için en iyi yoldur (Knipp *et al.* 2002).

2.1.2.2.3 Tekrarlayıcı (Repeater)

Tekrarlayıcılar, iletim ortamında zayıflamış, bozulmuş ya da üzerine gürültü eklenmiş elektriksel işareti tekrar üreterek iletim ortamına yenilenmiş ve gücü yükseltilmiş olarak gönderen ve iki yönlü olarak çalışan donanım aygıtlardır. Tekrarlayıcılar OSI referans modelinin ilk katmanı olan fiziksel katmanında yer almaktadır.

2.1.2.2.4 Köprü (Bridge)

Köprüler, aynı protokolü kullanan iki ya da daha fazla ağı birbirine bağlayan ağ cihazlarıdır (Şekil 2.3). Kendisine gelen çerçeveleri analiz ederek verinin başka bir ağa geçirilip geçirilmeyeceğine karar verir. Bir tekrarlayıcı kendisine gelen mesajı güçlendirerek hedefe bakmadan yollarken, köprülerde ise eğer paket hedefe ulaşamazsa o paketi tekrar göndermezler. Ayrıca OSI modeline göre ikinci katman olan veri bağı katmanında yer alan köprüler, farklı ağları birleştirirken bu ağların birbirleri arasında anlaşmasını da sağlarlar (Uçan ve Osman 2006).



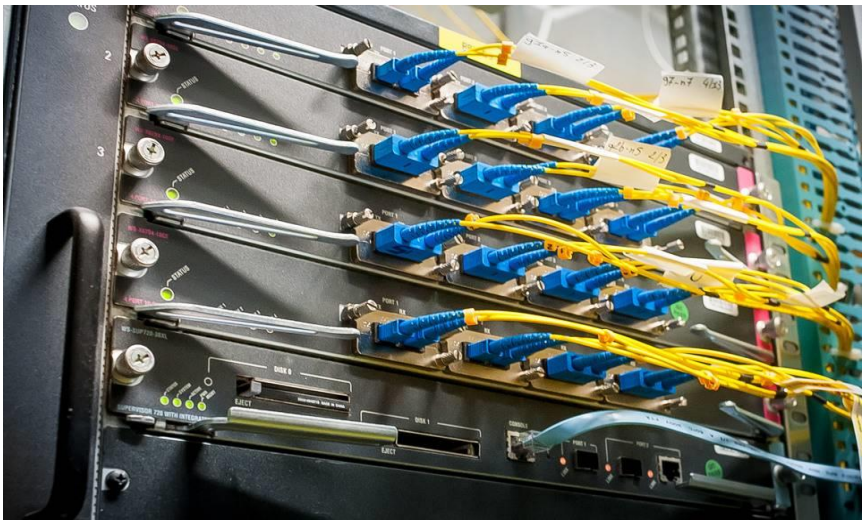
Şekil 2.3 Köprü (İnt.Kyn.9).

2.1.2.2.5 Yönlendirici (Router)

Yönlendirici, ağ katmanda kullanılan bir cihazdır. Yönlendiriciler birden fazla LAN yapısının birbirleri ile haberleşmesi için kullanılır. Yönlendiriciler yol belirleme ve yol seçimi yöntemlerini kullanarak verinin hangi LAN yapısına iletileceğini belirler. Yönlendiriciler mantıksal ağ adresleri yardımı ile verileri hedeflerine yönlendirir. Paketlerin yönlendirilmesi, ağın büyüklüğüne, yapısına ve ihtiyaçlara göre farklılık göstermektedir.

Yol belirleme işi; yol tespiti ve yol tablolarının tutulması ile gerçekleşir. Yol belirleme görevi Yönlendirici cihazına aittir. Yönlendirme tabloları paketlerin hedefe ulaşmak için gideceği bir sonraki Yönlendirici bilgisinin tutulduğu listelerdir. Yönlendirme tabloları; ağ adreslerini, iletişim hattındaki bir sonraki yönlendirici adresini ve hedef ağa ulaşma sırasında etkili olan maliyet bilgilerini içerir (Tutkun 2011).

Backbone (Omurga anahtarlayıcı) networkün ana omurgasıdır. Ağa bağlı olan tüm bölümler bu omurgaya bağlıdır (Resim2.2).



Resim 2.2 Omurga anahtarlayıcı (Backbone switch) (İnt.Kyn.10).

Backbone genelde tek bir bölümde taşınabilecek veriden daha fazla bilgi taşıyabilir. Yüksek kapasiteli bu cihazlar OSI modelinin L3 (Layer 3) katmanı olan ağ katmanında çalışan network cihazlarıdır. Yönlendirme işleminde kullanılan protokoller Cisco ve IEEE (The Institute of Electrical and Electronics Engineers) tarafından geliştirilmiş olan RIP (Router Information Protocol), OSPF (Open Shortest Path First), IGRP (Interior Gateway Routing Protocol) gibi protokoller ile dinamik yönlendirme ve yük dengeleme işlemleri yapılabilmekte, ayrıca hat kopmalarına karşı yedeklilik de sağlanabilmektedir.

2.1.2.2.6 Firewall (Güvenlik Duvarı)

Güvenlik Duvarı, özel ağ ile internet arasına yerleştirilen ve istenmeyen erişimlerin engellenmesini sağlayan bir sistemdir. Temelinde yazılım tabanlı olarak çalışmakta olup internet üzerinden bir sisteme girişi sınırlayan, gerektiğinde yasaklayabilen ve genellikle bir internet bağlantısını sağlayan ağ geçidi olarak görev yapan güvenlik sistemidir.

Ağ ortamı ile internet arasındaki tüm trafiğin güvenlik duvarı üzerinden geçirilmesi ağın etkin olarak kullanılmasını sağlar. Firewall kullanılmasının esas amacı ağa zarar vermek ya da ağa sızmak isteyenleri engellemektir. Bu sebeple veri merkezleri ve şirketler için sıklıkla güvenlik metodu olarak kullanılmaktadır (Uçan ve Osman 2006).

Yeni nesil tehditlerin ortaya çıkması ve bu tehditlerde artış görülmesi sebebi ile daha ayrıntılı güvenlik ihtiyacını ortaya çıkmıştır. Veri trafiğin engellenmesi yanında bu trafiği sınırlamak ve trafiği düzenleyerek etkin olarak kullanılması önem kazanmakmış, bu ihtiyaçlar sonucunda UTM (Unified Threat Management) sistemleri ve NGFW (Next Generation Firewall) ortaya çıkmıştır. UTM sistemleri, Anti-Spam, Antivirüs, DPI (Deep Packet Inspection), içerik filtreleme, URL filtreleme vb. güvenlik ihtiyaçlarını bir kutu çözümde karşılamakta ve iş gücü ihtiyacını azaltmaktadır. UTM'ler güvenlik işlevlerini yerine getirmek sanal motorlar kullanmaktadırlar. Bir veri paketinin hedefe ulaşması sırasında birkaç kez farklı motordan geçmesi gerekebilmektedir (Şekil 2.4). Böyle bir durumda gecikme süresi uzayarak ağ performansında azalmaya sebep olur (Coşar ve Arık 2014).

Şekil 2.4 UTM firewall (İnt.Kyn.11).

NGFW, paket içeriğini incelerken performanstan ödün vermez, aynı zamanda uygulamaları ve kullanıcı davranışlarını da tanıyabilir. Karmaşık görevleri yerine getirebilen bu cihazlar sayesinde uygulamalar ayrıştırılabilmekte ve kurumsal kullanım politikaları rahatlıkla oluşturulabilmektedir. NGFW veri paketlerini çok detaylı inceleyebilmekte bu özelliği sayesinde paketlerin ikinci bir firewall cihazında kontrol edilmesi ihtiyacını ortadan kaldırmaktadır. Ayrıca paketlerin incelenmesi için başka bir cihaz ihtiyacını ortadan kaldırdığı için de ürün maliyetini aşağı çekmektedir (İnt.Kyn.12).

2.1.2.2.7 AP (Access Point)

Son kullanıcıların kablosuz olarak web sayfalarına ve servislere erişimin sağlanması için kablosuz erişimi sağlayacak bir erişim noktasına ihtiyaç duyulmaktadır. Özellikle kurumsal ağlarda personellerin dışında öğrencilerin de kaynaklara her yerden erişmesi için kampüslerde çeşitli noktalara AP cihazları yerleştirilmektedir. Bu cihazlar kablolu bağlantılarda kullanılan anahtarlayıcı (switch) cihazları gibi bağlantının çoklanması için kullanılır. Kablosuz bağlantı donanımına sahip olan bilgisayar ağı cihazları AP aracılığı ile kablosuz LAN ağını oluşturur. AP'ler tıpkı anahtar cihazlarında olduğu gibi L2 (Layer 2) seviyesinde MAC adresleri üzerinden ve L3 seviyesinde yönlendirme özelliğini kullanarak bilgisayar ağı cihazlarının birbirleri ile iletişime geçmesini sağlar (Tutkun 2011).

Kurumsal ağlarda kullanılan AP cihazları özellikleri bakımından ev ortamında kullanılan cihazlardan farklılık göstermektedir. Farklı protokol desteği, çeşitli kimlik denetleme mekanizmaları, kapsama alanları, frekans aralıkları gibi çok sayıda özellik bu cihazlarda bulunmaktadır. İç ortamda kullanılan cihazların kullanıcı desteği 100 kişiye kadar çıkabilirken dış ortam cihazlarda bu sayı daha da artabilmekte ve daha fazla kapsama alanına sahip olmaktadırlar. Yeni nesil AP cihazları 2.4 Ghz ve 5 Ghz frekanslarında çalışabilmektedir. Bu cihazlar iç ortamlarda 20-30 metre, dış ortamlarda ise 80-100 metre kapsama alanına sahiptir. Kapsama alanları binalarda kullanılan duvarların kalınlıklarına ve kullanılan duvar tipine göre de değişiklik göstermektedir.

2.1.2.2.8 Wireless LAN Controller (Kablosuz Ağ Yönetim Cihazı)

Kablosuz erişim için kullanılan AP cihazlarının tek bir yerden kolay bir şekilde yönetilebilmesi, güvenliğin sağlanması ve kontrol edilmesi için kullanılan cihazlardır. WLC (Wireless Lan Controller) cihazına bağlı olan AP cihazları üzerlerinde konfigürasyon bulundurmazlar, tüm konfigürasyonu WLC'den alırlar. WLC cihazları

AP'ler üzerinden farklı SSID'lerin (The Service Set Identifier Used) yayınlanmasına, AP'lerin yayın yapacağı kanalları otomatik olarak seçmesine ve sinyal kalitesinin arttırılıp azaltılmasını sağlar. Kontrol cihazı ile AP arasında tünelleme işlemi yapılarak oluşan bu tünel içerisinden farklı ağlar kurularak güvenli bir iletişim sağlanmış olur. Kontrol cihazı ile tek bir ekran üzerinden cihazların tüm bilgilerine ulaşılabilmekte ve gerekli güvenlik kriterleri ayarlanabilmektedir.

2.1.2.2.9 Sunucu Sistemleri

Kurumsal bir ağda kullanılan sunucular kurum şubelerine ve son kullanıcılara hizmet ederler. Genellikle bilgi işlem birimlerinde korunaklı olarak özel oluşturulmuş sistem odalarında bulunan sunucular FTP (File Transfer Protocol), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Mail, Web, veritabanı gibi kurumun tüm ihtiyacını karşılayacak sunuculardan ve özel programlar için ayrılan sunucu sistemlerinden oluşmaktadır. Gelen yoğun isteklere cevap verecek ve 7 gün 24 saat çalışacak şekilde dizayn edilen bu sistemler kurumsal ağdaki tüm önemli verilerin tutulduğu merkezlerdir.

Sistem odalarında kullanılan fiziksel sunucu sistemleri günümüzde yerini sanal sunucu sistemlerine bırakmıştır. Yüksek işlemci, yedekli güç kaynağı (power supply) ve yüksek hafızaya sahip olan fiziksel sunucular üzerine çok sayıda fiziksel sunucunun kaldıracağı adette, farklı işletim sistemlerine sahip sanal sunucular kurulabilmektedir. Sanal sunuculara ihtiyaca göre farklı işletim sistemleri yüklenebilmekte ve fiziksel donanımlar eklenip çıkarılabilmektedir. Sunucu cihazları ve depolama cihazları arasında yüksek veri transferini karşılayacak fiber kablolar ile bağlantı sağlanmaktadır.

2.2 Referans Modelleri

2.2.1 OSI Modeli

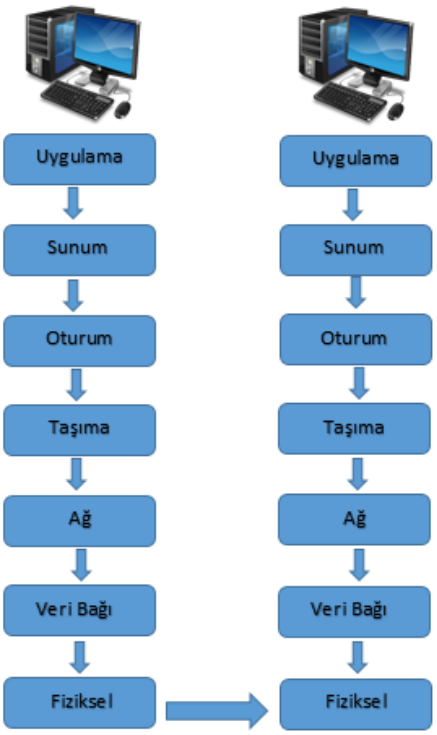
Uluslararası Standartlar Organizasyonu (ISO) tarafından 1977'de oluşturulan bir alt komite tarafından birçok farklı ağ yapıları içinde üreticiden bağımsız olarak iletişimin

sağlanabilmesi için 1984 yılında OSI referans modelini geliştirilmiştir. Bu model günümüzde birçok farklı donanım ve yazılıma sahip bilgisayarların birbirleriyle iletişimini mümkün hale getirmiştir. OSI modeli katmanlardan oluşmaktadır. OSI modeli ile telekomünikasyon mimarisinde ve bilgisayar ağı yapısının tamamında yapılan işlemleri nelerin kapsadığı anlatılmaktadır. Bu sayede bilgisayar ağı cihazları ile onları yönetenler arasında ortak bir dil konuşulması sağlanmış olur.

OSI'nin amacı ağ mimarilerinin ve protokollerinin bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır. Katmanlar arasında kurulan bu iletişim, herhangi bir donanım ya da bilgisayar ağı tipine göre değişiklik göstermez.

OSI modeli 7 katmana ayrılmıştır. İki bilgisayar birbiri ile haberleşirken katmanlar sırasıyla iletişim kurarken üst katmana servis sağlarlar. Eş düzeydeki katmanlar arasında doğrudan bir iletişim kurulmaz ancak iki katman arasında sanal bir iletişim oluşur.

OSI modeli, açık sistemlerin birbirleriyle haberleşmeleri için uymaları gereken katmanlı yapıyı tanımlamaktadır. OSI, açık sistemler arasındaki iletişim işlemlerini katman (layer) adı verilen 7 gruba ayırır. Bu katmanlar bir üst katmana verdikleri hizmet ile tanımlanırlar ve hizmetleri sıra ile takip ederek görev yaparlar (Öner 2003). Eş düzey iki katman arasında sanal bir iletişim kurulur. Bu katmanları ayrıntıları ile incelediğimizde her katmanın farklı bir işlevi olduğunu görmekteyiz (Şekil 2.5).



Şekil 2.5 OSI modeli

2.2.1.1 Physical Layer (Fiziksel Katman)

Verilerin fiziksel olarak gönderilmesi ve alınması bu katmanda vasıtası ile yapılır. Fiziksel katmanda kullanılan konnektör türü, kablo türü gibi elektriksel ve mekanik özellikler ile fiziksel bağlantı için gerekli olan Ethernet kartı ve hub, tekrarlayıcı (repeater) bu katmanda yer alır. Bu katmanda kullanılan iletişim kurallarına 100BASE-TX, ISDN (Integrated Services Digital Network), DSL (Digital Subscriber Line) örnek olarak gösterilebilir (Lammle 2005).

2.2.1.2 Data Link Layer (Veri Bağı Katmanı)

Network katmanından aldığı veri paketlerine hata kontrol bitlerini ilave ederek çerçeve (frame) haline getiren ve bu çerçeveyi fiziksel katmana ileten katmandır. Bu çerçevenin doğru ya da yanlış iletilip iletilmediğini kontrol eder. Eğer iletilen çerçeve hatalı olarak iletilmişse bu katman vasıtası ile yeniden gönderilir. Anahtarlayıcı (switch) ve köprü (bridge)'ler ATM ve Frame Relay servisleri bu katmanda yer alırlar.

Veri bağlantısı katmanı iki alt bölüme ayrılır.

- Media Access Control (MAC) 802.3: Veriyi CRC hata bilgisi yanına alıcı ve gönderici MAC adreslerini ekleyerek paketler ve fiziksel katmana aktarır. Alıcı tarafta da bu işlemleri tersine yapıp veriyi ikinci alt katman olan LLC'ye aktarır.
- Logical Link Control (LLC) 802.2: Bir üst katman olan ağ katmanına geçirilmesinden sorumludur. Ayrıca veri paketlerinden bozuk gidenlerin tekrar gönderilmesinden sorumludur (İnt.Kyn.13).

2.2.1.3 Network Layer (Ağ Katmanı)

Bu katman, bilgiyi ağa yerleştirmekten sorumludur. Bilgisayar ve adres alanından kaynaklı problemleri çözerek verinin sonraki aşamalara iletilmesini sağlar. Verinin uzaklara erişmesi için en kısa ve en iyi yolun bulunması işlemi olan yönlendirme işlemi bu katmanda gerçekleşir. Bu işlemi yapan Yönlendiriciler (router) yine bu katmanda tanımlıdırlar. Yönlendiricilerin güvenliğini sağlamak için erişim kontrol listeleri kullanılır. Veri paketlerinin iletimi için birden fazla rota kullanılabilir. Ağ katmanı, rotalar içindeki en iyi yolu bularak verinin iletilmesini sağlar. Bu işlemleri yaparken ağın durumuna, sunumun önceliğine ve diğer etmenlere bakarak verinin hangi fiziksel yolla iletileceğine karar verir. Bu katmanda rota güncelleme işlemleri için yönlendirme protokolleri kullanılır. En yaygın olarak kullanılan yönlendirme protokolleri olan RIP, OSPF ve IGRP bu katmanda çalışmaktadır.

2.2.1.4 Transport Layer (Taşıma Katmanı)

Taşıma katmanı üst katmandan aldığı paketleri parçalara bölerek bir alt katmana iletilmesini sağlar. Alt katmandan gelen verileri ise gönderildiği sırada birleştirip iletilere dönüştürerek üst katmana iletir. Bu katman ayrıca akış kontrolü ile parçalanarak karşı tarafa iletilen verinin yerine ulaşıp ulaşmadığını da kontrol eder. TCP, UDP, SPX (Sequenced Packet Exchange) ve NetBEUI (NetBIOS Extended User Interface) gibi iletişim kuralları bu katmanda çalışır.

2.2.1.5 Session Layer (Oturum Katmanı)

İletişim içinde olan iki nokta arasındaki oturumların kurulması, yönetilmesi ve sonlandırılmasından sorumludur. Sunum katmanı ile arasındaki diyalog kontrolünü sağlar. İletişimi koordine etmek için simplex, half dublex ve full dublex olarak üç farklı modda verileri iletir. Bu katmanda çalışan protokoller ve protokol ara yüzlerine NFS (Network File System), SQL (Structured Query Language), ASP ve NetBIOS örnek olarak verilebilir.

2.2.1.6 Presentation Layer (Sunum Katmanı)

Bu katman verileri uygulama katmanına sunarken veri üzerinde bir kodlama ve dönüştürme işlemlerinden sorumludur. Dolayısı ile adını bu işlevinden almıştır. Ayrıca bu katmanda veri sıkıştırma yanı sıra şifreleme işlemlerini de yerine getirir. Verilerin uygulama katmanına sunulmasını ve bu katman tarafından okunmasını sağlar. Bu katmanda tanımlanan JPEG (Joint Photographic Experts Group) ve MPEG (Moving Picture Experts Group) gibi grafik ve görsel görüntü sunum standartları kullanılmaktadır.

2.2.1.7 Application Layer (Uygulama Katmanı)

Son kullanıcı tarafından çalıştırılan tüm uygulamalar bu katmanda tanımlıdır. Bu katman kullanıcıya en yakın katman olup sonuçları monitör üzerinden rahatlıkla görülebilmektedir. Bu katmanda çalışan uygulamalara örnek olarak, DNS, HTTP (Hyper Text Transfer Protocol), FTP, SNMP (Simple Network Management Protocol) ve SMTP (Simple Mail Transfer Protocol) protokolünü kullanan tüm e-mail uygulamalarını verebiliriz.

2.2.2 TCP/IP Modeli

TCP/IP 1970'li yıllarda ABD Savunma Bakanlığı'nın bir projesi olarak temelleri atılmış endüstri standardı bir protokoldür. Amerika Savunma Bakanlığı'nın

(Department of Defense) Ocak 1983'te tüm bilgisayarlara bağlı TCP/IP kullanmıştır. DARPA (The Defense Advanced Research Projects Agency) projesi daha sonra ARPANET (Advanced Research Projects Agency Network) olarak adlandırılmıştır. Aynı zamanda, Savunma İletişim Ajansı (DCA), araştırma geliştirme bölümü için ARPANET, askeri iletişim için MILNET (Military Network) kullanılmaya başlamıştır. Bu proje ile daha sonra üniversite ve kamu kuruluşlarının birbirleriyle haberleşmesi amaçlanmıştır (Comer 2000). Günümüzde ağlar arası iletişimde ve internette kullanılan standart ağ haline gelmiştir. Her türlü ağ altyapısında kullanılan bu protokol endüstri standardı haline gelmiştir.

TCP/IP iki internet protokol kümesinden oluşmuştur. Üst katman TCP verinin iletimden önce paketlere ayrılmasını, iletişim sırasında kaybolan bilginin tekrar gönderilmesini ve karışık halde gelen bilginin sıralı hale getirilmesini sağlar. Alt katman IP ise, parçalara (segment) ayrılan bilgilerin ulaşmak istediği IP adresine gönderilmesi için uygun bir rota bularak gönderir. TCP/IP Protokolü dört katmana ayrılmıştır.

2.2.2.1 Uygulama Katmanı

İnternet ortamında kullanılan Telnet, FTP, SMTP, HTTP gibi tüm protokolleri kapsar.

2.2.2.2 İletim Katmanı

Akış kontrolü, hata düzeltme, iletim kalitesi, gibi görevleri üstlenir. İletim katmanında çalışan iki protokol TCP bağlantılı ve güvenli iletişim sağlamak için, UDP ağlar arasında paket aktarımı için tasarlanmıştır. Paketin yerine ulaşıp ulaşmadığını kontrol etmez. Bu sebeple TCP protokolüne göre daha hızlıdır. İletim katmanında yer alan TCP protokolü toplam 32 bit uzunluğa sahip olup TCP başlık yapısı Çizelge 2.1'de görüldüğü gibidir.

Çizelge 2.1 TCP başlık yapısı (Uçan ve Osman 2006).

TCP Başlık Yapısı			
Kaynak Port (16 bit)		Hedef Port (16 bit)	
Sıra Numarası			
Bilgi Numarası			
Başlık Uzunluğu (4 bit)	Rezerve Bölge (6 bit)	Kod Bitleri (Bayraklar) (6 bit)	Pencere Boyu (16 bit)
Hata Kontrolü		Acil Göstergesi	
Opsiyon Bitleri (25 bit)			Doldurma Biti (7 bit)
Veri			

Diğer bir iletim protokolü olan UDP protokolünün başlık yapısı Çizelge 2.2'de görülmektedir.

Çizelge 2.2 UDP başlık yapısı (Uçan ve Osman 2006).

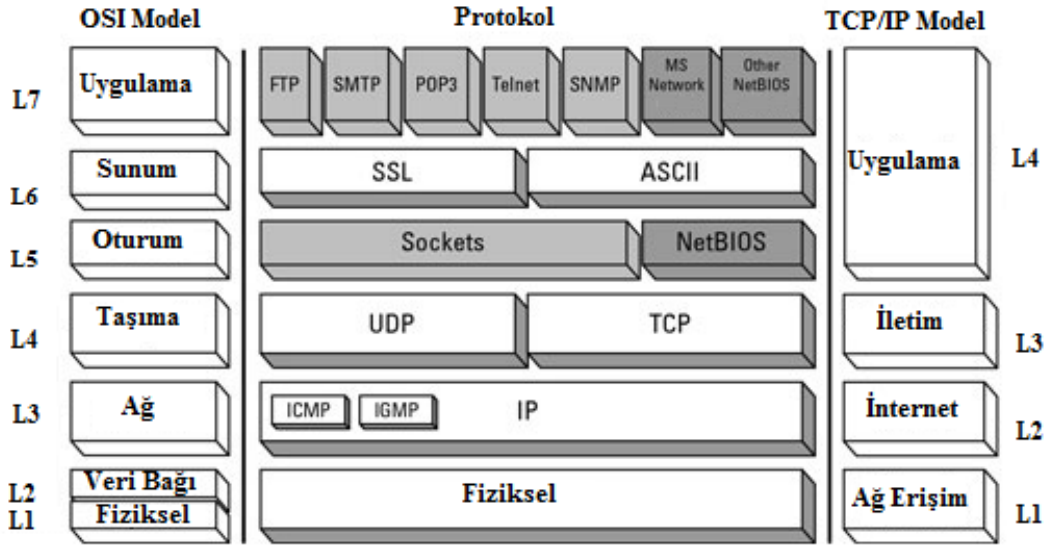
UDP Başlık Yapısı	
Kaynak Port (16 bit)	Hedef Port (16 bit)
Uzunluk (16 bit)	Hata Kontrolü (16 bit)

2.2.2.3 İnternet Katmanı

Kaynak ağdan internet ortamına gönderilecek bilgilerin adreslenmesi ve gönderilmesi ile bu katman sorumludur. İnternet katmanında çalışan protokollerden bazıları IP, ARP (Adres Resolution Protocol) ve RARP (Reverse Address Resolution Protocol)'dır.

2.2.2.4 Ağ Erişim Katmanı

Ağ erişim katmanı, üst katmandan gelen verilerin internet ortamına iletilebilmesi için uç sistem ile alt ağ arasında gerekli olan tüm fiziksel katmanların bilgilerini düzenler. Bu katman Şekil 2.6'da görüldüğü gibi OSI protokolünün fiziksel ve veri bağı katmanı ile aynı işleve sahiptir (İnt.Kyn.14).

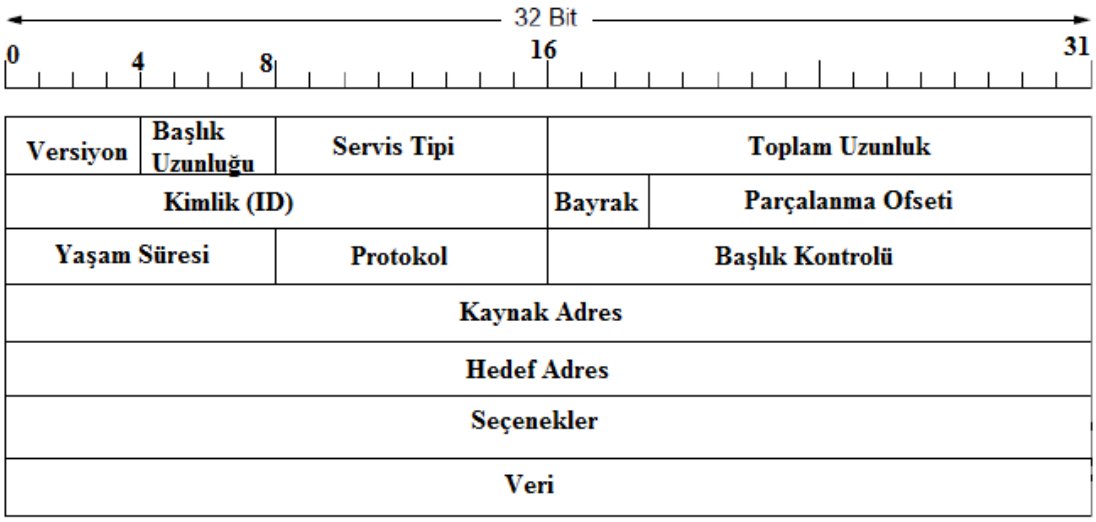


Şekil 2.6 OSI – TCP/IP karşılaştırması (İnt.Kyn.15)

2.3 IP Adres Yapısı ve Desteklenen Protokoller

2.3.1 IP Adres Yapısı

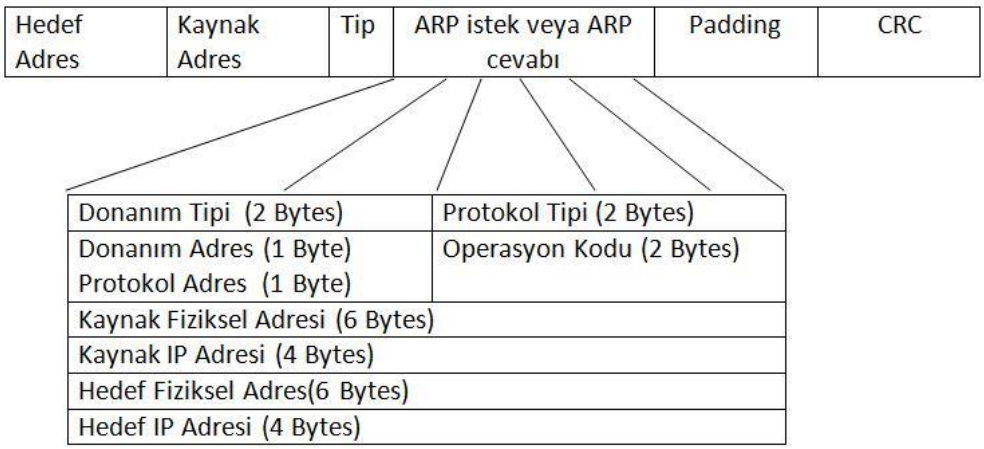
Bir ağa bağlı cihaz ağ üzerinde bulunan başka bir cihaz ile haberleşmek ve veri paketlerini yollamak için IP adresine ihtiyaç duymaktadır. Ağa bağlanan her bilgisayara DHCP sunucusu tarafından bir IP adresi atanır. IP adresleri ile cihazlar iletişim kurarlar. IPv4 (Internet Protocol Version 4) adresleri 32 bitlik bir adresleme yapısına sahiptir. Günümüzde birçok cihazın IP kullanabilir duruma gelmesi ve haberleşmek için IP adresine sahip olması sebebi ile IPv4 adreslemede artık yetersiz duruma gelmiştir. Bu sebeple 128 bitlik adres yapısına sahip olan IPv6 (Internet Protocol Version 6) internet protokolü geliştirilmiştir. (TÜBİTAK ULAKBİM 2011). Bu protokolde her bir oktetde 8 bit bulunmaktadır. IP başlık yapısı Şekil 2.7'de görülmektedir.



Şekil 2.7 IP başlık yapısı (Hunt 2002).

2.3.2 ARP Protokolü

ARP, bir IP adresinden kullanıcıya ait cihazının donanım adresini bulur. Eğer IP üzerinden hedef cihaz bulunamaz ise ARP protokolü vasıtası ile cihaz bulunmaya çalışılır. ARP, sorgulanan IP adresini bir donanım adresine dönüştürerek ağ içine broadcast gönderir ve o cihazın LAN içindeki yeri hakkında bilgi elde eder (Lammle 2007). ARP paket yapısı Şekil 2.8'de görülmektedir.



Şekil 2.8 Arp paket yapısı (İnt.Kyn.16)

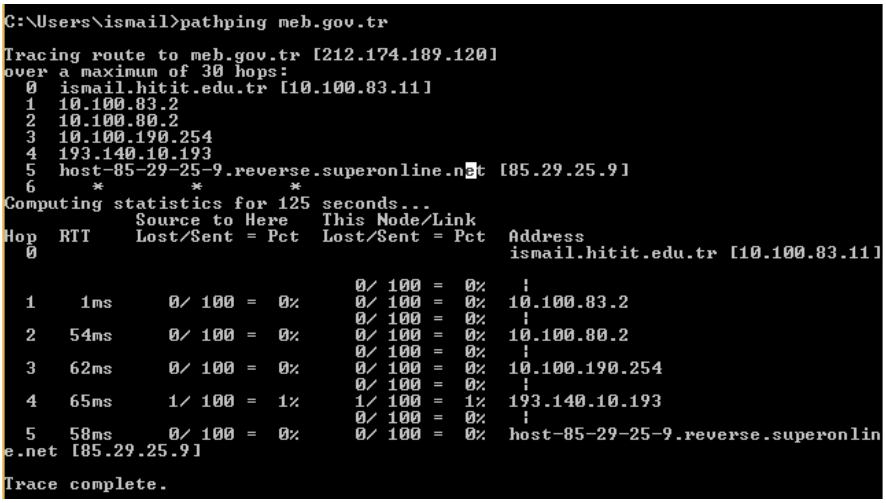
2.3.3 ICMP Protokolü

IP protokolü herhangi bir hata oluştuğunda bunu raporlama ya da oluşan hatayı düzeltme işlevine sahip değildir. ICMP protokolü IP protokolünün bu eksiğini giderir. Daha çok hataları raporlamak amacıyla kullanılan, kontrol amaçlı bir protokoldür. Bazı durumlarda uzakta bulunan bir sistem hakkında bilgi toplamak için de bu protokol kullanılmaktadır. ICMP protokolü yankı isteği (echo request) ve yankı cevabı (echo reply) mesajları kullanılır. Hata tespiti amacı ile en sık kullanılan komutlar ping, tracert ve pathping komutlarıdır.

- *Ping komutu:* Paketlerin hedefe ulaşıp ulaşmadığını gösterir. Gönderilen her paket 32 byte'lık bir ICMP paketi göndererek paketin karşıya ne kadar sürede ulaştığını gösterir.

- *Tracert komutu:* Bir paketin bir bilgisayardan çıktıktan sonra hangi yönlendiriciler (router) üzerinden geçtiğini ve ne kadar sürede geçtiğini gösterir. Eğer internet bağlantısı yoksa ya da bir problem varsa paketlerin hangi yönlendiriciye (router) kadar ulaştığını ve hangi noktada sorun olduğunu tespit etmemize olanak sağlar.

- *Pathping komutu:* Hedefe gönderilen veri paketlerinden hangi yönlendiriciden (router) geçtiğini ve ne kadar paketin ulaşıp, paketlerin ne kadarının ağda kaybolduğunu görebilmenizi sağlar (Resim 2.3).



Resim 2.3 Pathping paket durumu

2.3.4 DHCP Protokolü

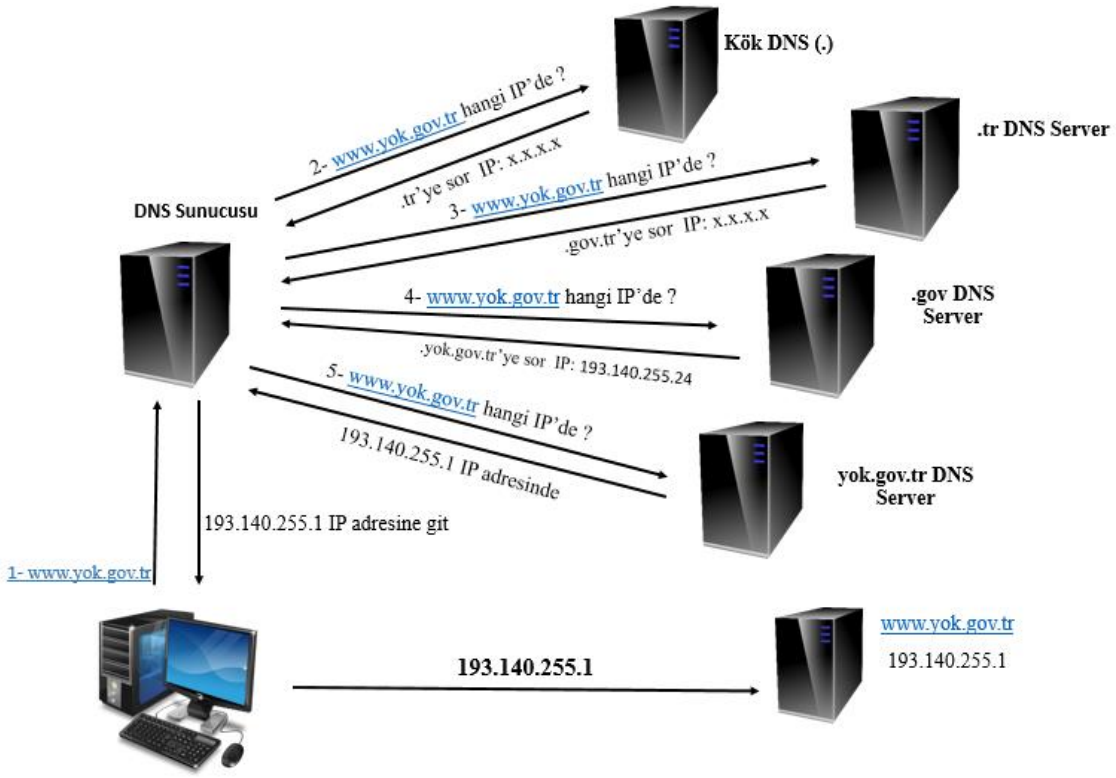
Bir bilgisayarın ağa bağlantısı için ağ bağlantısının yapılandırılması gerekir. Bu protokol ağ üzerinde bulunan bu bilgisayarları yapılandırmak için kullanılır. Ağa bağlanan bilgisayarlar IP ve DNS bilgilerini bu protokol vasıtası ile alırlar. Ağa bağlanan bilgisayarlar DHCP sunucu ile iletişim kurarken UDP protokolünü ile 67 ve 68 portunu kullanırlar.

2.3.5 DNS Protokolü

DNS bir alan adı servisidir. Akılda tutulması zor ve uzun adresleri daha anlamlı hale getirerek akılda tutulabilecek kolay isimler ile servislere ulaşılması amacı ile DNS kullanılır. IP adreslerini bilmek ve hatırlamak zor olduğu için bir servise daha anlamlı ve hatırlanabilir alan adı isimleri ile erişmek daha kolaylaşmaktadır. Alan adının IP adresine çevrilmesi ya da IP adresi bir alan adına çevrilmesi olarak iki yönlü olarak DNS çözümlemesi yapılır (TÜBİTAK ULAKBİM 2012).

İstemci tarafından DNS sunucuya yapılan sorgu özyinelemeli (recursive) sorgu, DNS sunucuların kendi aralarında yaptığı sorguya ise tekrarlamalı (iterative) sorgu olarak isimlendirilir.

Bulunmak istenen bir web adresi kök DNS sunucularına gider. Root sunucuları gelen isteği en üst düzey alan adı DNS sunucularına yönlendirir. Buradan da Alt domain sunucularına istek gönderilerek web adresi tespit edilir. Tespit edilen adres istekte bulunan cihaza gönderilir (Şekil 2.9).



Şekil 2.9 DNS çözümleme işlemi

2.3.6 HTTP Protokolü

HTTP, web üzerinden iletişim sağlanabilmesi için kullanılan en temel protokolüdür. HTTP sayesinde bir web istemcisi sunucularda bulunan bir sayfaya erişebilir. Web talebini yapan istemci cihaz, bu protokol vasıtası ile web sunucu üzerinde yer alan ve web servisleri üzerinden istenilen bilgiyi alabilir. HTTP, protokolü sadece düz metinleri iletmez. Resim, ses, video gibi her türlü çoklu ortam verisini de iletebilecek şekilde tasarımı yapılmıştır (Çetin ve Metin 2005).

İstemci bilgisayarı sunucuya birtakım veriler gönderir. Sunucu da bu verileri yorumlayarak istemciye yorumlanmış veriler ile cevap verir. Gönderilen bu cevapta alınan verinin türünü belirleyen başlık bilgisi (header) ve ana metin (body) bilgisi bulunur.

Kullanılan HTTP metodları;

GET: Sunucudan bir kaynak ister.

HEAD: Get komutuna benzer ancak sadece başlık bilgilerini gönderir

POST: Sunucuda bulunan verinin değişmesi için kullanılır.

DELETE: Sunucuda bulunan bir kaynağı siler.

OPTIONS: Verdiğimiz komutun türünü belirtir.

PUT: Bir web sayfasını saklamak üzere gönderir.

TRACE: Web sunucularını kontrol etme işlemidir.

HTTP protokolüne SSL (Secure Sockets Layer) sertifikası eklenerek HTTPS (Secure Hyper Text Transfer Protocol) protokolü oluşmuştur. Böylece HTTP trafiği güvenli ve daha kullanışlı hale getirilmiştir.

2.3.7 SNMP Protokolü

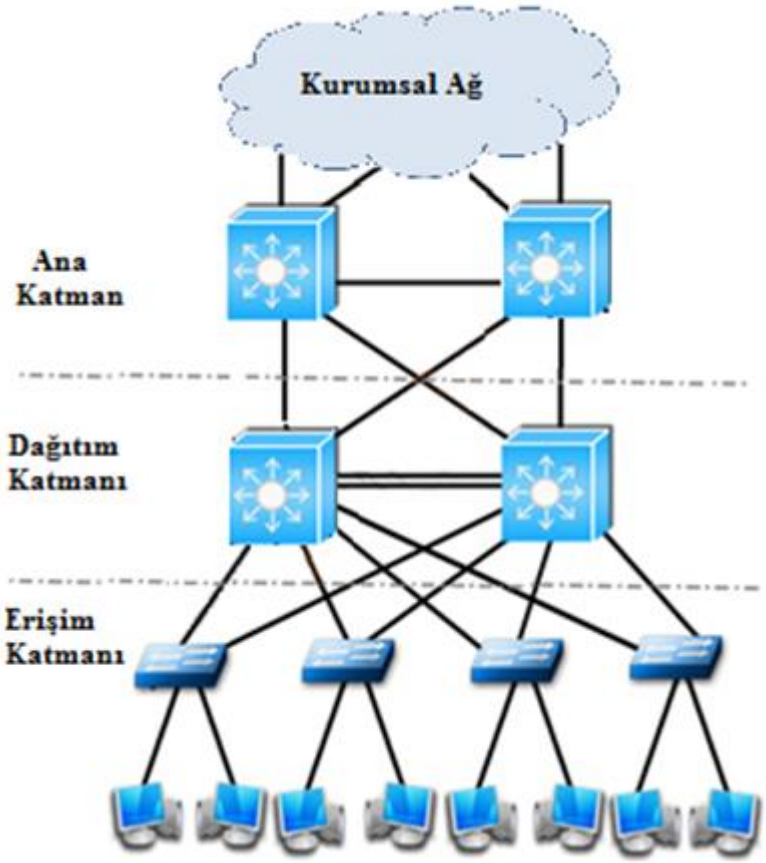
Bu protokol, ağ yöneticisine yardımcı olan basit bir yönetim protokolüdür. Temel amacı bir ağ içinde bağlantıyı sağlayan ağ cihazlarının yönetimini ve bu cihazların denetimini kolaylaştırma için tasarlanmıştır. SNMP ile ağ üzerinden bulunan yönlendirici (router), anahtarlayıcı (switch), sunucu, köprü (bridge) ve hatta bilgisayar gibi cihazlardan bilgiler elde etmek için kullanılır. Bu cihazlardan CPU değerleri, sıcaklık, kullanıcı sayıları, portların yoğunlukları, cihaz çalışma süresi gibi temel bilgiler elde edilebilir. Elde edilen bu bilgiler ile ağda oluşan problemler çözülebilir, ağ performansı artırılabilir ya da ağın büyümesi için önceden bir takım planlamalar yapılabilir.

Yönetilen cihazlar üzerinde bulunan SNMP ajanları vasıtasıyla cihazlar üzerinde bulunan bilgiler SNMP yönetim sistemine iletilir. SNMP protokolü haberleşmek için UDP 161 portunu kullanır.

2.4 Hiyerarşik Kampüs Ağı Referans Mimarisi

İnternet servis sağlayıcıları, hastaneler ve üniversiteler gibi büyük yapıdaki kamu kurumlarında kullanıcı sayısının ve verilen hizmetlerin çoğalması, masaüstü bilgisayar, tablet, dizüstü bilgisayar, yazıcı, dijital yayın yapan televizyon sistemleri gibi çok sayıda cihazın da intranet ve internete bağlanması anlamına gelmektedir. Bununla birlikte kampüs ağ kaynaklarını oluşturan web, e-posta, EBYS (Elektronik Belge Yönetim Sistemi), portal uygulamaları, dosya ve yazdırma sunucuları gibi hemen hemen her servis internet üzerinden çalışmaktadır. Dolayısı ile kurulacak kampüs ağı altyapısının genişleyebilen, esnek, işlevsel ve ölçülebilir bir yapıya sahip olmasının yanı sıra network ağındaki cihazların %100'e yakın bir yaşam süresine ulaşması istenen bir özelliktir.

Yangın, deprem gibi doğal afetlerin yaşanması sonucunda, kritik bilgileri üzerinde barındıran sunucu sistemlerinin ve internet iletişim ağının yedeklenmesi ihtiyacını doğurmuştur. Bunun sonucunda internet altyapısında kurum ya da kuruluşların ihtiyaçlarına ve imkânlarına göre farklı tasarımların yapılmasına sebep olmaktadır. Bu noktada kurulacak kampüs ağı fiziki anlamda yedekli olmalı, güvenlik bakımından da gerekli önlemler alınmalıdır. Böyle bir yapı oluşturmaya çalıştığımızda hiyerarşik kampüs ağı mimarisi öne çıkmaktadır. Bu yapı hem kablo olarak hem de donanım olarak yedekli bir yapı sağlar. Son birkaç yıl içinde, veri merkezi mimarileri daha karmaşık bir hale gelmiştir ve çok gelişmiş kampüs ağına bağlı yüksek erişim, düşük gecikme süresi ve yüksek performans gereksinimi ortaya çıkmıştır. 3 katmanlı hiyerarşik ağ tasarımı bu ihtiyaçları karşılayacak yapıdadır (Şekil 2.10).



Şekil 2.10 Hiyerarşik ağ tasarım modeli (İnt.Kyn.17).

2.4.1 Access Layer (Erişim Katmanı)

Son kullanıcı cihazlarının ağ kaynaklarına bağlandığı ve AP cihazlarının bağlı olduğu katmandır. L2 anahtarlama bu katmanda yapılmaktadır. Frame Relay, ISDN veya kiralık hat vb. geniş alan bağlantı teknolojileri kullanılarak ağa erişim yapılması sağlanmaktadır. Port güvenliği, spanning tree vb. güvenlik protokolleri yapılandırması bu katmanda yapılır.

2.4.2 Distribution Layer (Dağıtım Katmanı)

LAN veya WAN bağlantılarının toplandığı ve birbirine bağlandığı noktalardır. LAN'lar arası yönlendirme protokollerinin uygulandığı, ACL kurallarının tanımlandığı, filtreleme ve güveliğin uygulandığı katmandır.

2.4.3 Core Layer (Ana Katman)

Kampüsün çıkış noktasıdır. Bu katmanda merkezi anahtarlama yapan çok-katmanlı (multi-layer) ve yüksek kapasiteli anahtarlar kullanılır. Merkezi anahtarlama yapan bu cihazlar büyük ve pahalı yönlendiriciler olup ağların bel kemiği olarak kabul edilir. Yoğun paket geçişi olduğu için paketler mümkün olabildiği kadar hızlı iletilir. Yüksek hızlı anahtarlama, güvenlik, gözetim, QoS (Quality of Service) hizmet kalitesi önceliklendirmesi bu katmandaki öne çıkan önemli işlemlerdir (İnt.Kyn.18).

2.5 Ağ Standartları

Üniversiteler, hastaneler gibi yoğun kullanıcıların yoğun internet kullandığı ve servislere eriştiği ortamlarda kablosuz ağlar yoğun olarak kullanılmaktadır. Özellikle teknolojinin son zamanlarda hızlı bir şekilde katlanarak ilerlemesi ile teknoloji cihazları ucuzlamıştır. Bugün her birey en az bir tane dizüstü bilgisayar, tablet, cep telefonu vb. kablosuz erişim sağlayan bir cihaza sahiptir. Bu cihazlar ile internet erişimi olan herhangi bir noktadan kablosuz ağa dâhil olarak internete ve servislere erişim sağlanabilmektedir. Erişim noktalarında kullanılan kablosuz erişim cihazlarının özeliklerine göre bağlantı kalitesi değişiklik göstermektedir.

2.5.1 Ethernet Standartları

Uluslararası standartlar geliştiren ve onaylayan IEEE, 802.X LAN standartlarını belirlemiştir. Ağ standartların bir kısmı başarısız olurken bir kısmı da teknolojinin gelişmesi ile kullanım dışı kalmıştır. Sık kullanılan 802.3 Ethernet standartları Çizelge 2.3'te görülmektedir.

Çizelge 2.3 Sık kullanılan IEEE 802.3 standartları (Spurgeon and Zimmerman 2014).

IEEE 802.3 Standartları	**Tanımlama**
802.3	Ethernet
802.3u	Fast Ethernet
802.3z	Fiber optik kablolama veya koaksiyel kablo üzerinden Gigabit Ethernet
802.3ab	Bükülmüş çift kablo üzerinden Gigabit Ethernet
802.3ae	10-Gigabit Ethernet
802.3af	Ethernet Üzerinden Güç

2.5.2 Kablosuz Ağ Standartları

1997 yılında IEEE tarafından standartları belirlenen 802.11 kablosuz iletişim protokolü yıllara göre çok hızlı bir şekilde değişim göstermiştir.

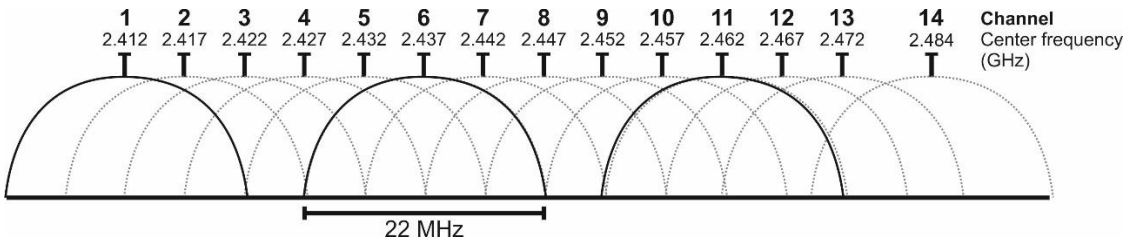
IEEE 802.11 standartlarına ait çizelge Çizelge 2.4'te görüldüğü gibidir. Teknolojinin gelişmesi ile yeni standartlar geliştirilirken bağlantı hızları da artmaktadır. Günümüzde 802.11n standardı 2.4 Ghz ve 5 Ghz destekli cihazlar olup 600 Mb/s hızı desteklerken yeni nesil 802.11ac standardı 5 Ghz frekansında, teoride ise 6.93 Gb/s hızında erişim sağlayan bir teknolojidir. AP bağlantılarında çift yönlü veri alış-verişi yapılamadığı için uygulamada erişilebilecek hız teoride belirtilen değerin yarısına yakındır. Örneğin 802.11n standardını destekleyen bir bağlantıda tek bir kişinin erişebileceğiniz hız 250-280 Mb/s dolaylarındadır. Bu AP cihazına çok fazla kişinin bağlandığında erişilebilecek bu hız bağlanan kişi sayısına ters orantılı olarak düşecektir. Dolayısı ile günümüzde bu teknolojileri destekleyen kablosuz cihaz ile yapılan kablosuz bağlantı

ile kablolu bağlantı karşılaştırıldığında; kablosuz bir bağlantının kablolu bir bağlantıdan daha iyi olduğu söylenemez.

Çizelge 2.4 IEEE 802.11 standartları (İnt.Kyn.19).

Standart	Frekans bandı	Bant genişliği	Maksimum veri aralığı
802.11	2.4 Ghz	20 Mhz	2 Mb/s
802.11b	2.4 Ghz	20 Mhz	11 Mb/s
802.11a	5 Ghz	20 Mhz	54 Mb/s
802.11g	2.4 Ghz	20 Mhz	54 Mb/s
802.11n	2.4 Ghz, 5 Ghz	20 Mhz , 40 Mhz	600 Mb/s
802.11ac	5 Ghz	20, 40, 80, 80+80, 160 Mhz	6.93 Gb/s
802.11ad	60 Ghz	2.16 Ghz	6.76 Gb/s

Bir AP cihazı, iki nokta arasında fiziksel bir bağlantı kullanılmadan elektromanyetik dalgalar vasıtası ile bilgi aktarılması amacı ile kullanılır. Bu dalgalar AP cihazından uzaklaştıkça azalmaktadır. 2.4 Ghz frekans bandı alt kanallara bölünerek Wi-Fi (Kablosuz Bağlantı Alanı) için tahsis edilmiştir. Bu band sınırlı bir kaynağa sahip olduğu için çok sayıda kanal oluşturulması amacı ile Şekil 2.11'de görüldüğü gibi iç içe geçecek şekilde bir yapı oluşturulmuştur. Böylece dar bir frekans bandında çok sayıda kanal sığdırılmış ve frekansın kullanılabilirliği arttırılmıştır.



Şekil 2.11 Wi - Fi kanalları

Tasarımlarda komşu erişim noktaları için birbiri ile çakışmayan kanal mesafesi 5'tir. Bu sebeple başarılı bir cihaz tasarımı için birbirini etkilemeden 3 erişim noktası kullanılarak yapılacak bir konumlandırma sonucunda en az sorunlu kablosuz ağ yapısı kurulmuş olur (İnt.Kyn.20).

2.6 Kampüs Ağ Yönetimi

Hızla büyüyen ağlarda, ağ mühendisleri ve yöneticileri için en çok üzerinde durulması gereken konulardan biri de ağ yönetimidir. Ağdaki uç sayısı arttıkça ağın yönetimi de oldukça zor ve karmaşık bir hal alabilir. Bu yüzden ağ daha tasarlanırken yönetim ile ilgili işlevlerin de yeterince tanımlanması gerekir. Ağ yönetimi sadece ağ cihazlarını uzaktan, merkezi olarak yapılandırılabilmesi olarak algılanmamalıdır. Ağın güncel durumu, trafik dağılımı, trafik türlerinin analizi ileride çözülmesi çok daha zor olabilecek problemlerin zamanında tespiti için hayati önem taşımaktadır (Kaplan 2006).

Kampüs ağı çeşitli bileşenlerden oluşmaktadır. Bu bileşenler içerisinde fiziksel kablolama altyapısından üst yapıda kullanılan ağ cihazlarına kadar geniş bir bileşen yelpazesine sahiptir. Kampüs ağının farklı yerleşkelerde yer alması ulaşım ve arıza durumunda müdahale sürecini uzatmaktadır. Diğer taraftan kurum fonksiyonlarını içeren uygulamaların ağ üzerinde çalışması ağın önemini artırmaktadır. Ağ üzerinde akan uygulama trafiği kritik bir hal almakta ve bütün kurumun çalışma mekanizmasını etkilemektedir. Kurum fonksiyonlarını içeren uygulamaların ve fonksiyonların en az kesintiyle hizmet vermesi, kurum çalışanlarının ve dışarıdan hizmet alan son kullanıcıların da bu uygulamalara kesintisiz ulaşması gerekmektedir.

2.6.1 Kablolu Ağ Yönetimi

Kablolu ağ yönetimi, ağ içinde bulunan ve veri iletişimini sağlayan ağ cihazları ile son kullanıcı cihazları arasındaki veri iletimini kapsar. Burada önemli olan noktaların başında kablolama işlemi gelir. Kablolama işlemi ne kadar kaliteli ve iyi ise ağda oluşacak kablolamadan kaynaklı problemler de o ölçüde azalacaktır.

Kampüs ağının yönetilebilmesi için ağ içinde kullanılan fiziksel altyapının ve ağ içinde kullanılan network cihazlarının tanımlanması gerekir. Kampüs ağ yönetimi; kurulan fiziksel ağ altyapısının sağlıklı olarak çalışması, kampüs ağının yönetimini, ağ tabanlı servislerin yönetilmesini ve ağ güvenliğinin sağlanmasını içerir.
Ağda bulunan cihazlar kontrol altında tutularak ağın sürekli olarak hizmet vermesi sağlanmalıdır. Ağın devamlılığı önemli olduğu için olası herhangi bir cihaz arızasına karşı önceden tedbir alınmalıdır. Ağda oluşabilecek problemlere karşı ağ trafiği sürekli izlenmeli, problem öncesi gerekli tedbirler alınmalı ve herhangi bir problem görüldüğü anda müdahale edilmelidir (İnt.Kyn.21).

L2 Switching (2. katman anahtarlama), ağ yönetimini kolaylaştıran en önemli işlemlerin başında gelmektedir. Donanım tabanlı bir filtreleme yöntemi olup trafik bir filtreden geçirilir. Ethernet kartlarının sahip olduğu MAC adresleri filtreleme için kullanılır ve çok hızlı bir anahtarlama işlemi yapılır.

Ağ üzerinde iki bilgisayar aynı anda ileti göndermeye çalışırsa collision (çarpışma) oluşur. Hub' lar tek bir collision domain (çarpışma alanı) oluştururlar. Çünkü iletilerin kodunu çözemezler, iletinin bozuk olduğunu algılayamazlar ve iletiyi tüm bağlantı noktalarından yinelerler. İki bilgisayar aynı anda very göndermeye çalıştığında çarpışma meydana gelir. Bu sebeple bilgisayarlar sırayla veriyi tekrar göndermek zorunda kalırlar.

Her çarpışma alanındaki bilgisayar sayısını azaltıldığında ve çarpışma alanı sayısı arttığında ağ daha verimli kullanılacaktır (İnt.Kyn.22).

Ağ üzerinde oluşabilecek gereksiz fiziksel bağlantıların önüne geçilerek, oluşabilecek LOOP (döngü) problemlerinin önüne geçilmelidir. Eğer arka arkaya ağ cihazları birbirine bağlanması gerekiyor ise ağ üzerinde darboğaza sebep olmamak için ağ cihazlarının anahtarlama ve toplam kapasite teknik özellikleri bakımından diğerleri ile aynı seviyede olmasına dikkat edilmelidir.

2.6.2 Kablosuz Ağ Yönetimi

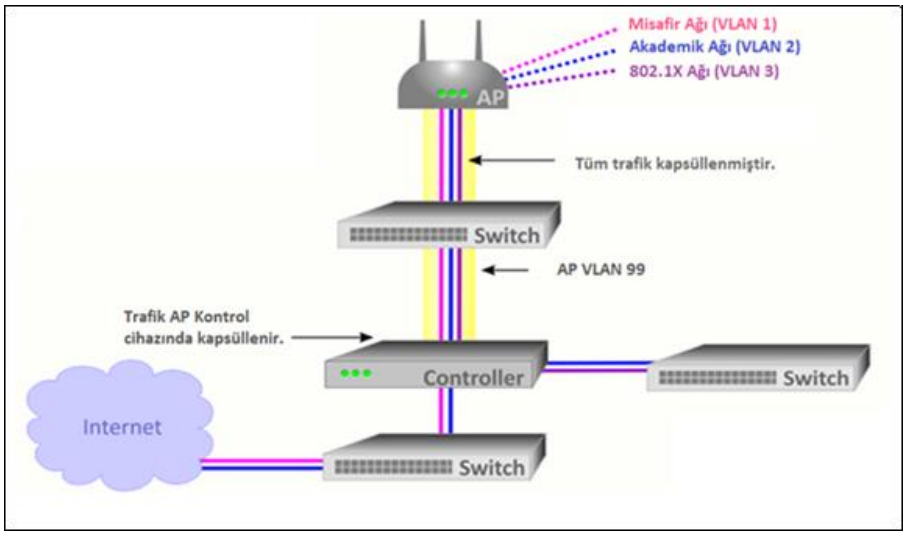
Kurumsal ağlarda kablosuz ağ yönetimi iki farklı şekilde yapılmaktadır. Tekil olarak kablosuz ağ cihazları tek tek yönetilebildiği gibi cihazlar tek bir merkezden de yönetilebilmektedir. Eğer bu iki yapı bir arada kullanılırsa karma bir yapı oluşacak ve yönetim daha güç bir duruma gelecektir. Kablosuz ağ yönetimi için kullanılabilecek yöntemler Çizelge 2.5'te gösterilmiştir.

Çizelge 2.5 Kablosuz ağ yönetimi

Merkezi Çalıştırma (Controlled-base)	**Tekil Çalıştırma (Autonomous)**	**Karma Yapı**
Tüm trafiği merkezi bir yönetici donanıma yönlendirme	Düşük yatırım maliyeti	Yerel trafiği ayırma
Tak çalıştır kullanım	Yönetim zorluğu	Merkezi ve tekil kullanım
Tam merkezi kontrol Kapsüllenmiş trafik Ek yatırım maliyeti	Kısıtlı servisler	Sınırlı kontrol

Merkezi olarak yönetimde kablosuz ağ cihazları basit ya da şifreli olarak bir tünel üzerinden konfigürasyon cihazı ile iletişime geçerler. Bu iletişim şekli normal olabileceği gibi şifreli de olabilir.

AP cihazları çalıştığı zaman merkezi kontrol cihazına bağlanarak güncel konfigürasyon dosyasını kendi üzerlerine çekerler. Bu aşamadan sonra kablosuz ağ cihazı ile kontrol cihazı arasındaki trafik akışı kontrollü bir şekilde kapsüllenmiş olarak iletilmeye başlar. AP cihazları üzerinde kayıtlı herhangi bir konfigürasyon bulunmadığı için çalınma gibi bir durumda cihaz üzerinde herhangi bir kayıtlı konfigürasyon bulunmadığı için ağ hakkında herhangi bir bilgi elde edilemez. Bu sebeple çalınmaya karşı otomatik olarak bir koruma sağlanmış olur (Şekil 2.12).



Şekil 2.12 Merkezi kablosuz ağ yönetimi (İnt.Kyn.23).

Merkezi olarak yönetimin avantajlarında biri de kendi kapsama alanlarında bulunan aynı marka cihazlar ile aynı protokolü kullanarak haberleşme sağlaması ve komşu cihazın kullandığı kanalı anlayarak, kendi yayın yaptığı kanalı otomatik olarak değiştirebilmesidir. Aynı zamanda istenmeyen AP denetimi ve bloklama işlemi yapılabilmektedir.

Kablosuz ağ cihazlarının sayısı arttıkça her cihazın ayrı ayrı yapılandırılması ve yönetilmesi gerekmektedir. Cihazlarda yapılacak en küçük bir değişiklikte kablosuz ağ cihazlarına tek tek bağlantı sağlanarak hepsinde ayar yapılması gerekebilir. Böyle bir durumda network yöneticisinin tüm cihazlarda bu işlemi yapması günlerini alabilir. Bu işlemin daha kısa sürede yapılabilmesi için ise daha fazla nitelikli personele ihtiyaç duyulmaktadır. Fakat merkezi olarak kontrol cihazı ile yönetilen büyük bir kampüste dahi bu yapılandırma çok rahat bir şekilde web üzerinden yapılabilmektedir.

2.7 Kablolama Altyapısının Oluşturulması

Üniversite, hastane, üretim tesisleri gibi büyük yerleşim yerlerinde kablolama altyapısı önemli bir konu haline gelmiştir. Yapılan altyapı yatırımı bazen yüklü bir yatırım olacağı gibi tadilat süreci de zor olacaktır. Bu sebeple iyi düşünülerek oluşturulacak altyapı uzun bir süre sistemi taşıyacaktır.

2.7.1 Kablolu Altyapı

Kablolama altyapısı hazırlanırken dikkat edilmesi gereken noktaların başında, yapılacak kablolama işleminin kalitesini kanıtlamış standartlara uyumlu olması önemlidir. Bu standartlar Amerika'da TIA (Telecommunication Industry Association) tarafından belirlenen TIA/EIA 568, Uluslararası Standardizasyon olarak ISO/IEC – 11801 ve Avrupa Birliği EN 50173 olarak belirlenmiştir. Türkiye'de TIA/EIA 568-B standardı yaygın olarak kullanılmakta ve yapılan işin de bu standarda uygun olarak yapılması önem arz etmektedir.

Bölgesel iletişim ağlarının merkezinde UTP kablolar kullanılmaktadır. UTP kablo içinde sekiz kablo dört çift olacak şekilde bükümlü halde bulunmaktadır. UTP kablo standardında Level-3, Level-4, Level-5 gibi kategorilere ayırırlar. Günümüzde UTP denildiğinde ilk akla gelen Category-5 (CAT5) standardı yerini Category-6 (CAT6) standardına bırakmıştır. CAT6 kablolar daha dayanıklı olup içlerinde parazit oluşmasına karşı bir koruyucu bulunmaktadır. Bu kablolarda veri akışı 1000 Mbps'dir. CAT7 standardı ise ülkemizde yeni kullanıma geçmeye başlamıştır.

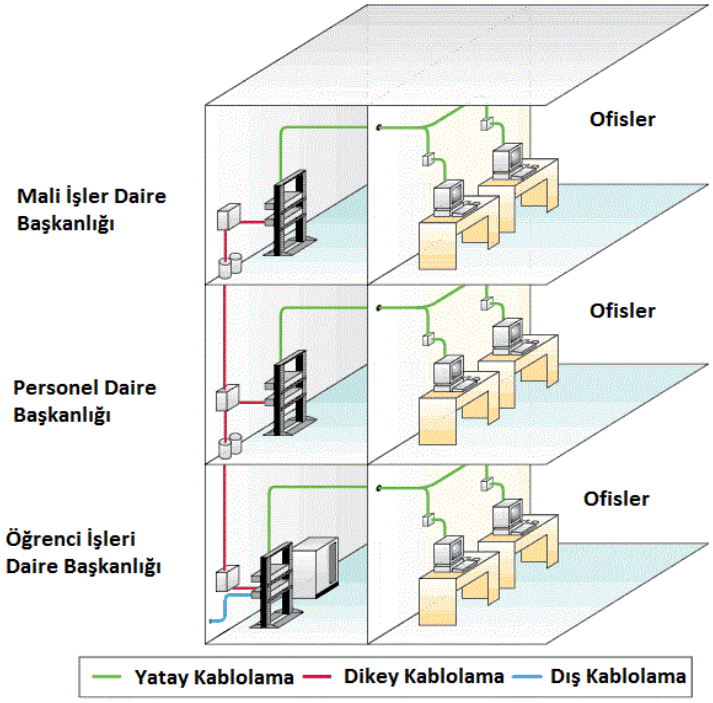
Fiber Optik altyapıların en önemli özelliği, 100 m üzerinde hizmet vermekte zorlanan bakır kabloların yerini almasıdır. Fiber optik kablo kullanılması ile veri kesintileri ve görüntü kayıpları giderilmiş olur. Fiber Optik uygulamalar ile aynı hat üzerinde bulunan birçok kablo tek bir kablo haline getirilerek çevresel etkenlerden etkilenmeden temiz bir iletim sağlayabilir.

Fiber optik kabloların avantajları ise aşağıdaki belirtilmiştir.

- Fiber optik kablonun bilgi taşıma kapasitesi normal data kablosundan daha fazladır.
- Fiber optik kablo ile daha hızlı internet erişimi sağlanabilir. Kullanılabilecek bant genişliği de daha fazladır.
- Bu kabloda sinyal kaybı daha düşüktür. Uzak mesafelerde veri aktarımı yapabilir. Kullanılan kablo türüne göre 90 kilometre mesafeye kadar veri aktarılabilmektedir.

- Bu kablo içerisinden ışık aktarıldığı için elektromanyetik alanlardan etkilenmediği için parazit oluşmaz.
- Fiber optik kabloların dış ortamlardan etkilenmemesi için iyi bir izolasyona sahiptir.
- Bu kablolar su altı gibi zor şartlarda bile rahatlıkla çalışabilmektedir.
- Fiberler, metalik kablolardan daha küçük ve çok daha hafiftir.
- Metal olmadıkları ve kabloların içindeki boşluktan kablo yerine ışık geçtiği için çok daha hafiftir. Bu sebeple nakil maliyeti de azdır (İnt.Kyn.24).

Yapısal kablolama sistemleri ile genişleyebilir sağlıklı bir yapı kurulabilmektedir. Yapılacak kablolama işleminde kullanılan yöntemler ve dikkat edilmesi gereken konuların ana başlıkları aşağıdaki gibidir (Şekil 2.13).



Şekil 2.13 Yatay ve dikey kablolama (Akın ve Bük 2014).

Vertical (Dikey) Kablolama: Dikey kablolama ya da backbone olarak isimlendirilen kablolamada merkez noktadan kenar toplama noktalarına giden taşıyıcı kablo hatlarından oluşur. Haberleşme genellikle dikey olarak kattan kata yapılarak tüm trafik dikey kablolama üzerinden taşınır. Genellikle bu kablolama yöntemi için fiber optik

kablo tercih edilmektedir. Fiber optik kablo kullanılması ile hata oranı düşük olan ve dış ortamdan etkilenmeyen iyi bir veri yolu oluşturulmuş olur (İnt.Kyn.25).

Hortizonal (Yatay) Kablolama: Yatay kablolama kenar toplama noktası ile uç noktalar arasında yatay ya da dikey olarak kablo çekilmesi ile oluşan kablolamadır. Günümüzde planlı yapılarda en çok kullanılan kablolama türüdür.

Doğru Tasarım ve Projelendirme: Bir altyapı tasarlanırken kurulacak ağın büyüyebileceği ihtimali düşünülerek altyapı tasarlanmalıdır. Kablolama altyapısında yapılacak herhangi bir değişikliğin maliyeti yüksek olacağı için birkaç yıllık büyüme düşünülerek altyapı tasarımı yapılmalı ve projelendirilmelidir. Aynı zamanda gerektiğinde büyümeye elverişli bir altyapı tasarımı yapılmalıdır.

Kaliteli İşçilik: Projelendirme kadar önemli diğer bir konu da işçiliktir. İşçiliğin kaliteli yapılması kablolama altyapısının da kaliteli yapıldığı anlamına gelmektedir. Çünkü kaliteli kablo kullanılsa bile eğer yapılan işçilik iyi değilse bu altyapıdan iyi bir performans alınamayacaktır (İnt.Kyn.26). Kaliteli işçilik beraberinde düzenli bir kablolama yapısını beraberinde getirir. Kaliteli işçilik ve düzenli kablolama ile kurulan altyapının uzun ömürlü olması sağlanmış olacaktır. Resim 2.4'de düzenli kablolama örnekleri görülmektedir.

Resim 2.4 Düzenli kablolama örnekleri

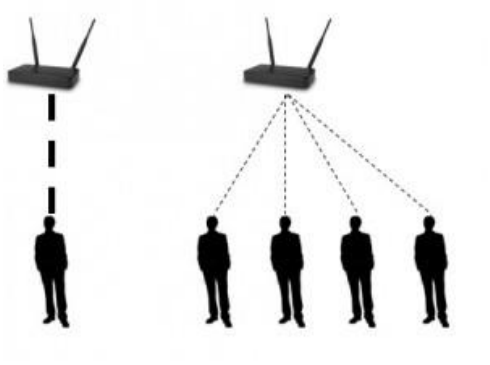
Test, Etiketleme ve dokümantasyon: Kablolama işleminden sonra çekilen tüm kablolar test edilmeli, olası arıza problemlerinde arızalı kablonun tespiti ve problemin giderilmesi için numaralandırma yapılmalıdır. Kablolar belli bir numaralandırma sistemi ile etiketlenmelidir. Etiketleme sonrasında yapılan dokümantasyon arızanın tespiti ya da genişleme durumunda kolaylık sağlayacaktır.

2.7.2 Kablosuz Altyapı

Kablosuz ağ tasarlanırken dikkat edilmesi gereken bazı kriterler bulunmaktadır. Kablosuz ağlarda sinyal gücü zayıfladıkça, veri iletişiminin devam etmesi için düşük performanslı modülasyon teknikleri kullanılmaktadır. Bunun dezavantajı bağlantı hızının düşmesidir. Kablosuz ağ cihazları yerleşiminde tasarım hatası yapılarak erişim noktalarının hatalı konumlandırılması sebebi ile son kullanıcı cihazı ile arasındaki engellerden geçerken emilmeler sonucunda sinyalin zayıflamasına sebep olur. Şekil 2.14'te kablosuz sinyalin zayıflaması görülmektedir.

Şekil 2.14 Sinyalin zayıflaması

Dikkat edilmesi gereken noktalardan biri de AP'ye bağlanacak kişi sayısıdır. Eğer kablosuz erişim cihazına bağlanan kullanıcılardan birisinin bant genişliğini çok tüketmesi diğer kullanıcıları da etkileyecek ve kullanıcıların bağlantı hızı düşecektir. Tek bir erişim noktasına yüz kullanıcı erişim sağlarsa kullanıcılar internetin çok yavaş olduğundan şikâyet edecektir. Kullanıcı sayısı ve uygulamaların tüketeceği bant genişliği miktarı tespit edilerek, ihtiyaç duyulan kapasiteye göre daha fazla sayıda AP kullanılması ve bir erişim noktasına bağlanacak kullanıcı sayısının azaltılması ile bu problem çözülebilir. Kablosuz kullanıcı ile bağlantı hızı ilişkisi Şekil 2.15'te görülebilmektedir.



Şekil 2.15 Kullanıcı – bağlantı hızı ilişkisi

Bir başka önemli husus da ana çıkış hızının gereken kapasiteye sahip olmamasıdır. Kullanılan AP, 450 Mbps hızını destekliyorsa ama ana çıkış hızı daha düşükse iç ağda erişimde bir problem yaşanmazken internete erişim sırasında ana çıkış hızından daha yüksek bir hıza erişilemeyecektir (İnt.Kyn.27).

Anahtarlar (switch) ile AP'ler arasındaki kablolama işleminin sağlıklı olması gerekir. Kalitesiz kablolama yapılması durumunda AP ile haberleşmeyi keseceğinden bağlantıların düşmesine sebep olacaktır. Bu sebeple mümkün olduğunca kaliteli kablo kullanılması gerekmektedir.

Kablosuz ağ cihazlarının kolay yönetilebilmesi hem işgücü tasarrufu hem de zaman tasarrufu sağlayacaktır. Bu sebeple cihazların tek merkezden yönetilmesi zaman ve işgücünün tasarrufunun yanında kablosuz cihazlar üzerinde hâkimiyet sağlayacaktır. Bu sayede denetim ve yapılandırma da kolaylaşacaktır.

Bina içinde kablosuz dolaşım yapılması durumunda internet erişimi kesilmeyecektir. Bu işlem için 2.4 GHz frekansında çakışmayan üç kanalın kullanılması ile mümkün olacaktır. Dördüncü bir AP kullanılması durumunda diğer erişim noktalarının birinin frekans kanalı ile girişim yaratacağından hızın ciddi seviyede düşmesine sebep olacaktır. Bu sebeple tasarım yapılırken kullanılan üç AP'nin farklı kanalları kullanması ve çakışma yapmamasına dikkat edilmesi gerekmektedir.

İstenmeyen AP'ler kontrolünüzde olan AP'lerin sinyal seviyesini bozabilir ve kullanıcıların bağlantı yapmasını engelleyebilir. Bu cihazların tespit edilmesi ve sinyal yaymasının önüne geçilmesi için gerekli tedbirlerin alınması gerekmektedir.

2.8 Ağ Güvenliği

Sistem ve ağ teknolojisi çok çeşitli uygulamalar için önemli bir teknolojidir. Bununla birlikte, ağ güvenliği gelişen ağlarda kritik bir gerekliliktir. Güvenliğin kolayca uygulanamayışı da önemli bir eksikliktir.

Güvenlik teknolojisi ve geliştirici ağlar arasındaki iletişim boşluğunu iyi gelişen OSI modeli doldurmuştur. Ağ tasarımında OSI modeli; modülerlik, esneklik, kullanım kolaylığı ve protokollerin standardizasyonu gibi birçok avantaj sağlar. Farklı katmanlarda yer alan protokolleri haberleştirebilir. Ağ içindeki karmaşıklığı yönetmek için bir yöntem bulunmamaktadır.

Kampüs ağı, kampüs hayatının önemli bir parçasıdır ve ağ güvenliği de kesinlikle olması gerekmektedir. Güvenli ağ, kurumu ağ üzerinden gelebilecek saldırılara karşı korur. Kurum ağında temel hizmetler ve ağ referans tasarımı sağlam bir temel üzerine oturtulmamış ise ağ tarafından sunulan IP telefon, IP video ve kablosuz iletişim gibi uygulamalar performans kaybı ve güvenlik sorunları ile karşılaşacaktır. Ama güvenli bir temel üzerine bu uygulamalar geliştirildiğinde uzun yıllar boyunca ağ geliştirilebilir ve ağın güvenliği sağlanabilir (Ali *et al.* 2015).

Ağ güvenliği göz önüne alındığında tüm ağın güvenliğinden bahsedilmektedir. Ağ güvenliği sadece iletişim ağının sonundaki bilgisayarları içermez. İletişim kanalı saldırılara karşı zayıf olmamalıdır. Potansiyel saldırganları, olası ağ ataklarını ve güvenlik sorunları anlama, etkili bir ağ güvenlik planı ile anlaşılabilir ve geliştirilebilir.

Günümüzde kullandığımız teknolojik cihazların internete bağlı olması, elektronik ticaretin gelişmesi ve internet kullanımının yaygınlaşması sonucunda güncel tehditler

artmakta, sistemler ise bu tehditlere karşı zayıflık göstermektedir. Ağların zayıflıkları sonucunda ise veri ve prestij kaybı yanı sıra maddi olarak da şirketlerin zarar görmesine neden olmaktadır. Web sitesi açıkları, Sıfır gün saldırıları, DoS (Denial of Sevice) saldırıları günümüzde en büyük tehlikeleri oluşturmaktadır. Yapılabilecek bir siber saldırı ise büyük bir sistemin servis dışı bırakılmasına ve verilerin başkalarının eline geçmesine sebep olabilir.

Oluşabilecek bu tehlikelere karşı farklılık gösteren tedbirler alınmaktadır. Ağ güvenliğini sağlamak için birçok yöntem mevcuttur. Bunlar kimlik doğrulama mekanizmaları, şifreleme araçları ve saldırı tespit sistemleri ve güvenlik duvarlarıdır (Daya 2014).

İncelenen bir çalışmada Güvenlik duvarı kullanılarak ağ güvenliği sağlanabilir. Bu çalışmada yerel ve geniş bilgisayar ağlarında firewall tekniği kullanılmış, gerçek dünyadan bir firewall ürünü kullanılarak tespit edilen güvenlik problemleri için belirlenen güvenlik politikalarının mevcut ağlar üzerine kurulan firewall üzerinde nasıl uygulanması gerektiği üzerine çalışma yapılmıştır (Uzun 1999).

Dağ (2001) yaptığı çalışmada, bilgisayar ağlarındaki güvenlik sorunları ve güvenlik sağlama yöntemleri incelenmiştir. Bu amaçla Linux işletim sistemi üzerinde yer alan ağ güvenlik duvarı uygulamaları incelenmiştir. Ayrıca bu tez çalışmasında platform bağımsız olarak çalışabilecek bir vekil güvenlik duvarı yazılım uygulaması gerçekleştirilmiştir (Dağ 2001).

Çakar (2005) yaptığı tez çalışmasında, bilgisayar ağlarındaki güvenlik sorunları, güvenliği sağlama yöntemleri, saldırı türleri, korunma mekanizmaları, güvenlik sınıflamaları ve güvenlik duvarı yapısı incelenmiştir. Güvenlik duvarı uygulaması olarak ISA Server sistemi gerçekleştirilmiş, kurulan küçük ölçekli bir ağ üzerinde bu sistemin etkileri ve özellikleri incelenmiştir. RSA (Rivest-Shamir-Adleman) ve Eliptik Eğri şifreleme algoritmalarıyla ilgili bir yazılım oluşturulmuş, bu algoritmaların çalışması program üzerinde gösterilmiştir (Çakar 2005).

Ertuğrul (2013) yaptığı tez çalışmasında ise kampüs ağında çalışmakta olan cihazların yapılandırılma eksikliklerinden kaynaklanan sorunların olduğu tespit edilerek kampüs içerisindeki ağ cihazları uygun şekilde yapılandırılmış, yönetilebilir cihazların bulunduğu noktalarda 802.1X protokolü ile yönetilemeyen noktalarda ise captive portal uygulaması ile güvenlik sağlanmaya çalışılmıştır. Ağdan kaynaklanan bağlantı problemleri giderilmiş ve internet erişim kayıtları yasada belirtildiği şekilde tutulmaya başlanmıştır (Ertuğrul 2013).

2.8.1 Kablolu Ağlarda Güvenlik

Kablolu ağlarda güvenlik en önemli konuların başında gelmekte ve zaman zaman unutulmaktadır. Her güvenlik önleminin alınması ise veri paketleri içeriğinin de filtrelenmesi anlamına gelebilmektedir. Veri paketlerinin filtrelenmesi ise gereğinden fazla CPU ve hafıza kullanımına ve ağ bağlantısında yavaşlamaya sebep olmaktadır. Bu sebeple makul ölçülerde gerektiği kadar güvenlik önlemleri alınmalıdır.

Kablolu ağda alınabilecek güvenlik önlemleri

- Saldırı tespit ve önleme sistemi (IDS/IPS)
- Network tanımlaması - VLAN kullanımı
- Servislerin tanımlanması
- Zararlı yazılım filtreleme (spyware, malware)
- URL kategori, içerik filtreleme
- Kategori Sınırlama / Engelleme
- Kenar anahtarlamalarda (Edge switch) güvenlik
    - Port Security
    - DHCP Snooping
    - Arp Denetlemesi (Inspection)
    - Storm Control
    - MAC Filter

Günümüzde kullanılan ürünler incelendiğinde yukarıda belirtilen güvenlik önlemlerinin alınabildiği görülmektedir. Bu önlemlerin bazıları genellikle kurum ağı

çıkışına konumlandırılan güvenlik duvarı üzerinde, bir kısmı ise ağ içinde kullanılan ağ cihazları üzerinde alınmaktadır.

2.8.2 Kablosuz Ağlarda Güvenlik

Bir kablolu ağda güvenliğin sağlanması için yönetilebilir anahtarlar (switch) ile güvenlik sağlanabilmektedir. Kablosuz ağlarda ise iletişim havadan kurulmakta ve veriler havada dolaştığı için büyük bir güvenlik problemi oluşmaktadır. Kablosuz bir ağda veri paketleri yakalanarak paketlerin içeriğinin görüntülenebilmesi mümkündür. Bu sebeple veri güvenliği için L2 ve L3 düzeyinde yeterli güvenlik önlemleri alınmalıdır.

Kablosuz teknoloji en basit anlamıyla, bir veya daha fazla cihazın fiziksel bağlantı olmaksızın haberleşmesi demektir. Kablosuz ağlar; kablolu iletişime alternatif olarak uygulanan ve RF teknolojisini kullanarak, havadan bilgi alışverişi yapan esnek bir iletişim sistemidir. Kablosuz ağlar sayesinde insanlar, masa başına bağlı kalmadan istedikleri her yerde bilgiye ulaşabilmekte ve sunabilmektedir, Bu sayede insanlara hem hareket özgürlüğü sağlamakta hem de zaman kazandırmaktadır. Kablosuz ağları kurarken dikkat edilmesi gereken en önemli unsur güvenliktir.

Erkinay (2006) yaptığı çalışmada Kablosuz Ağlarda Güvenlik konusunu detaylı olarak inceleyerek, AP üzerinde yapılabilecek güvenlik konfigürasyonlarına değinmiştir. Van Yüzüncü Yıl Üniversitesi kampüs alanında uygulanmakta olan WLAN sistemi, çalışma prensipleri ve güvenlik uygulamaları incelenmiştir. Hali hazırda kullanılan WLAN sisteminin eksikliklerine ve bu eksikliklerin giderilmesi için yapılabileceklere değinilmiştir (Erkinay 2006).

Abdulkareem (2012) yaptığı çalışmada ise, kablosuz ağ güvenliği için kullanılan yöntemlerin güvenlik açıkları incelenmiş, kablosuz ağların korunması için geliştirilen IEEE güvenlik algoritmalarının açıkları anlatılmış ve bu açıklardan yararlanılarak kablosuz bir ağa nasıl dâhil olunacağı, olası saldırılara karşı alınması gereken önlemler

irdelenerek güvenlik anlamında farkındalık yaratılması hedeflenmiştir (Abdulkareem 2012).

Kablosuz ağda alınabilecek güvenlik önlemleri

- WEP (Kabloluya Eşdeğer Gizlilik - Wired Equivalent Privacy), WPA (Wi-Fi Korumalı Erisim- Wi-Fi Protected Access), WPA2 (Wi-Fi Korumalı Erisim II- Wi-Fi Protected Access II) şifreleme
- Captive portal, 802.1X
- MAC Adres filtrelemesi
- İstenmeyen AP denetimi ve bloklama
- 802.1X kimlik doğrulaması (Kuruluş güvenliği)
- EAP-TTLS (Genişletilebilir Kimlik Doğrulama İletişim Kuralı - Tünelli Taşıma Katmanı Güvenliği)

Kablosuz ağ cihazlarının teknik özellikleri incelendiğinde güvenlik için farklı yöntemlerin desteklendiği görülmektedir. Yukarıda bahsedilen yöntemlere ek olarak kablosuz ağ cihazları üzerinde alınabilecek diğer yöntemler aşağıdaki gibidir.

- Fiziksel Güvenlik
- WLAN Yönetimi
- Cihaz şifresinin değiştirilmesi

2.8.2.1 Kabloluya Eşdeğer Gizlilik (WEP - Wired Equivalent Privacy)

Wi-Fi ağlarında yaygın kullanılan ilk şifreleme yöntemi WEP şifreleme yöntemidir. WEP algoritması Kablolu Eşdeğer Gizlilik anlamına gelir ve hemen hemen tüm 802.11/b/g ekipmanları tarafından desteklenir. WEP algoritmasının amacı her türlü harici saldırıdan kablosuz haberleşmeyi korumak ve yetkisiz erişimin engellenmesidir. Kablosuz cihaz ile istemci arasında 40 bitlik ortak bir anahtar kullanılır. Bu anahtarın amacı paket gönderilmeden önce paketleri şifrelemek ve gönderim sonrasında değişikliğe uğrayıp uğramadığının kontrolünü yapmak için kullanılmaktadır. Bu algoritmanın basit olması sebebi ile alternatif algoritmalar geliştirilmiştir. Günümüzde

WEP algoritması üzerinden geçen tüm konuşma ve e-mail trafiği rahatlıkla dinlenebilmektedir. Bu sebeple kullanım alanı azalmıştır.

2.8.2.2 Wi - Fi Korumalı Erişim (WPA - Wi - Fi Protected Access)

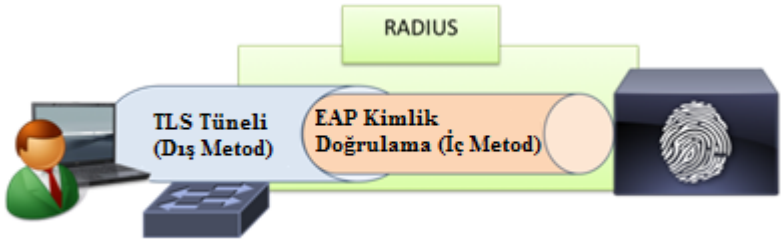
Veri bağlantısında kullanılan diğer bir kimlik doğrulama yöntemi WPA'dır. Bu algoritma WEP'in eksiklerini geçici olarak gidermek için Wi - Fi Alliance tarafından oluşturulmuş bir standarttır. IEEE tarafından 2001 yılında standart olarak kabul edilmiştir. İki farklı modda çalışır. Bunlar TKIP (Temporal Key Integrity Protocol - Geçici Anahtar Bütünlüğü Protokolü) *ve* WPA-PSK (Wi - Fi Protected Access Pre-Shared Key – Wi - Fi Korunmuş Erişim Ön Paylaşımlı Anahtar) korumasıdır. WPA; EAP Protokolünü kullanır. Bu protokol hem kablolu hem de kablosuz ağlarda 802.1X port tabanlı ağ erişim kontrol metodu ile birlikte kullanılmaktadır.

TKIP (Temporal Key Integrity Protocol)
TKIP; WEP'in zayıflıklarını adreslemek ve var olan donanımı kullanarak daha güvenli WLAN için bir çözüm yolu sağlamak için geliştirilmiştir. TKIP; WEP'den daha fazla hesaplama gücü, AES (Advanced Encryption Standard) ve WPA2'den ise daha az hesaplama gücü gerektirir. Anahtarlama boyutu 128 bit olarak kullanılır.

WPA yöntemi ile kimlik doğrulama işlemi mutlaka yapılmalıdır. Bu yöntemde RADIUS (Remote Authentication Dial-in User Service) sunucusu istenilirse kullanılabilir. RADIUS yerine ön paylaşımlı anahtar (pre-shared key – PSK) kullanılarak kimlik doğrulama işlemi de yapılabilmektedir. Bir RADIUS sunucusu kullanıldığında WPA yöntemi tüm 802.1x ve EAP protokollerini desteklemektedir. Kimlik doğrulama sunucusu, bir kullanıcının kimlik bilgilerini kabul ettikten sonra tekil anahtar üretmek için 802.1X'i kullanır. TKIP istemci ve AP'ye bu anahtar dağıtılır. Kullanıcının açmış olduğu oturum (session) süresinde her veri paketi için benzersiz bir şifre oluşturularak şifreli olarak iletim sağlanır (Wi - Fi Alliance 2003).

EAP Protokolü (Extensible Authentication Protocol)

Birçok kablosuz ağ güvenlik metodu EAP protokolünü temel almaktadır (Şekil 2.16). EAP Farklı kimlik doğrulama yöntemlerini desteklemektedir. Aynı zamanda Noktadan noktaya hatlarında, kablosuz ağlarda ve VPN erişiminde kullanılır. EAP-TLS, EAP-TTLS ve EAP-FAST protokollerinde veri güvenliği ve tünelleme özelliği mevcuttur. Kullanıcı doğrulamasını SQL, LDAP (Lightweight Directory Access Protocol) ya da Active Directory sunucularından yapabilmekte, kimlik doğrulama işlemi için ağırlıklı olarak RADIUS sunucuları kullanılmaktadır.



Şekil 2.16 EAP - TTLS bağlantısı (İnt.Kyn.28).

WPA2-PSK (WPA2 Pre-Shared Key) Protokolü

WPA2, kablosuz modemlerde yeterli güvenlik sağlanamadığında kablosuz ağları daha iyi korumak için geliştirilmiştir. 128 bitlik onaltılı sayı sistemi (hexadecimal) olarak bir şifreleme yöntemi kullanır. WPA2 şifrelemesi hem teorik hem de pratik açıdan WPA ile benzer özellikler göstermektedir.

WPA şifrelemesi ile birlikte kullanılmaya başlanan kimlik tanımlama, anahtar yönetimi ve AES, WPA2 protokolünde de kullanılır. Veri alışverişi başlamadan önce ön kimlik denetimi yapılır. Bu bilgiler önbellekte saklanır. Tüm özellikler şifreli haberleşmenin hızlanmasını sağlamaktadır.

AES (Advanced Encryption Standard)

Kablosuz ağı diğer kullanıcılardan gelebilecek saldırılara ve korsan saldırılara karşı korunması amacı ile WPA ve WPA2 protokolleriyle birlikte TKIP ve AES şifreleme standartları geliştirildiği için saldırılardan etkilenme olasılığı en aza indirilmiştir (İnt.Kyn.29). TKIP şifreleme standardında açıkların bulunması sebebi ile AES standardı oluşturulmuştur. 128 bit, 256 bit ve 512 bit uzunluğa sahip anahtarları

destekleyebilmektedir. AES standardı uluslararası olarak kullanılan ve günümüzün en güvenli şifreleme standardıdır. Şifreleme standartlarının karşılaştırılması Çizelge 2.6'da görülmektedir.

Çizelge 2.6 WEP, WPA ve WPA2 'nin karşılaştırılması

Özelik	**WEP**	**WPA**	**WPA2**
Giriş Kontrolü	Yok	802.1x	802.1x
Kimlik Denetimi	Yok	EAP	EAP
Şifreleme Algoritması	RC4	TKIP	AES
Anahtar Bit Uzunluğu	40 bit veya 104 bit	128 bit şifreleme. 64 bit kimlik denetimi için kullanılır	128 bit

2.8.2.3 Captive Portal

Bu güvenlik yönteminde özel programların yerine kimlik doğrulamak için web tarayıcısı kullanılır. İnternet tarayıcısı olan tüm bilgisayar, dizüstü ve mobil cihazlar üzerinden rahatlıkla kimlik doğrulama yapılması sureti ile oturum açılabilir. Kimlik bilgileri girildiğinde kullanıcı bilgileri Kimlik Doğrulama Sunucusuna (Authentication Server) iletilir. Kimlik bilgileri doğrulanmadığı durumda kullanıcı internete çıkamaz. Oteller, kafeler, bilgisayar laboratuvarları için uygulanabilir bir çözümdür.

2.8.2.4. 802.1X Protokolü

Kurumsal ağlarda ve kampüs ağlarında ikinci katmanda en fazla kullanılan güvenlik yöntemlerinden bir tanesi IEEE tarafından geliştirilmiş olan 802.1X'tir. Kullanıcı kimlik doğrulaması için RADIUS sunucu kullanılmaktadır. Şifreleme yöntemi olarak tünellenmiş EAP protokolü kullanılmaktadır. Bu sayede şifrelenmiş ve tünelden geçen veri tamamen koruma altına alınmış olur.

Bu kimlik doğrulama yöntemi hem kablolu hem de kablosuz bağlantı yöntemlerinde kullanılabilmektedir. Kablosuz bağlantıda AP ya da merkezi kontroller üzerinden

ayarların yapılması ve client cihazları üzerinde de 802.1X ayarlarının yapılması gerekmektedir. Kablolu bağlantıda bu yöntemin kullanılabilmesi için kullanılan anahtar (switch) cihazlarının bu yöntemi desteklemesi gerekmektedir. Bu sebeple kablosuz bağlantı yönteminde daha fazla kullanılmaktadır (Butler *et al.* 2013).

2.9 Ağa Yapılan Başlıca Saldırılar

Ağ güvenliği politikaları belirlenirken, sadece kurum dışından gelecek saldırılar düşünülmemeli, kurum dışından gelebilecek saldırılara karşı önlem alınmamalıdır. Bilişim kaynaklarına ya da kurum verilerine yönelik güvenlik tehditleri, kurum dışından olduğu kadar kurum içinden de kaynaklanabilmektedir. Bu noktada çoğu zaman göz ardı edilen bu durum zaman zaman ciddi sorunlara sebep olabilmektedir. Bu nedenle, kurumsal güvenlik politikaları belirlenmeli ve bu politikalar uygulanmalıdır. Bu politikalar kurum içinde bilişim kaynaklarının daha verimli kullanılmasını sağlamayacaktır (Can ve Akbaş 2014).

Aşağıda ağ güvenliği konusunda çeşitli saldırı tiplerinden örnekler verilmiştir.

2.9.1 VLAN Atlama (VLAN Hopping)

VLAN Hopping atakları, önlenmesi en basit, ancak en çok unutulan güvenlik açıklarından birini kullanarak yapılır. VLAN Hopping, son kullanıcı cihazları ile VLAN'lara ulaşabilecekleri normal şekilden farklı bir şekilde ağa bağlanarak portlara paketlerin gönderilmesi vasıtası ile VLAN bilgilerinin elde edilmesidir. DTP protokolünde portların hangi modda çalışacağı anahtarlayıcılar (switch) arası anlaşmalar (negotiation) aracılığıyla karar verilmektedir. Eğer portların trunk ayarların düzgün yapılmamışsa çerçevelerin (frame) değiştirilerek gönderilmesi vasıtası ile saldırı yapılabilir. Bu da saldırganın tüm ağa ulaşması anlamına gelir. Kötü niyetli bir kişi anahtarlayıcının (switch) bir portuna bağlanan bilgisayarında DTP paketlerini dinleyerek ya da anahtarlayıcının (switch) bu ucuna bağlanarak bu hattın trunk olmasını sağlar. Hat trunk olduğunda network üzerindeki tüm ağa erişebilir duruma gelir ve ağ paketleri kötü niyetli kişinin eline geçmiş olur. Bu yöntem ile saldırgan

kendisinin bağlı olduğu VLAN bilgisi yanında ağda kullanılan diğer VLAN'ların bilgisine de ulaşır.

2.9.2 MAC Taşması (MAC Flooding)

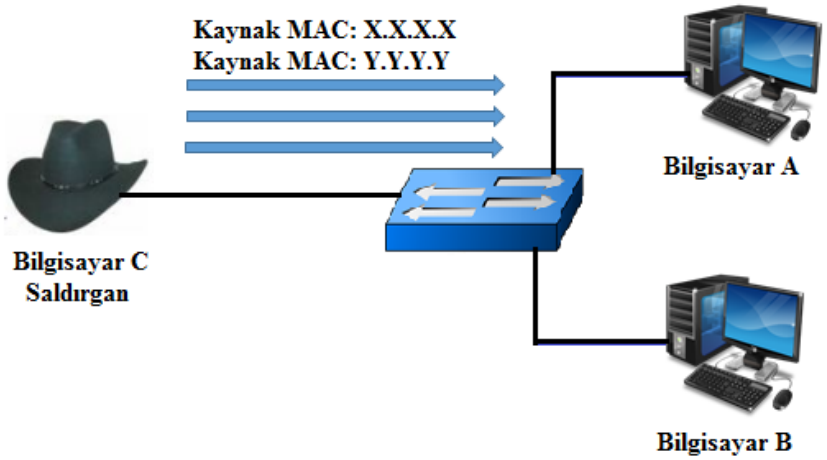
Her anahtarın (switch) üzerinde, anahtar (switch) üzerindeki portlar ile bu portlara bağlı cihazlarının MAC adreslerinin eşleştirildiği bir tablo bulunur. Portlar arasındaki veri iletişimi için bu tablodaki bilgiler kullanılır. Bu tablo MAC adres tablosu ya da CAM (Content Address Memory) tablosu olarak isimlendirilir. Örnek bir MAC adres tablosu Resim 2.5'de görülmektedir.

Vlan	Mac Address	Type	Ports
60	0000.2106.314d	DYNAMIC	Gi1/1/3
60	0002.f154.5e20	DYNAMIC	Gi1/1/2
60	0002.f157.1a28	DYNAMIC	Gi1/1/1
60	001b.0d47.dac1	DYNAMIC	Gi1/0/17
60	001c.0fc3.cc00	DYNAMIC	Gi1/1/1
60	0025.1136.9c7a	DYNAMIC	Gi1/1/2
60	08cc.686f.d5b0	DYNAMIC	Gi1/0/5
60	08cc.686f.d5c1	DYNAMIC	Gi1/0/5
60	08cc.6875.b431	DYNAMIC	Gi1/1/3
60	08cc.6875.b441	DYNAMIC	Gi1/1/3
75	08cc.6875.f9b0	DYNAMIC	Gi1/0/8
75	08cc.6875.f9c1	DYNAMIC	Gi1/0/8
75	08cc.6899.e2b1	DYNAMIC	Gi1/1/2
75	08cc.6899.e2c1	DYNAMIC	Gi1/1/2

Resim 2.5 MAC adres tablosunun ekran görüntüsü

MAC taşması saldırısı yapan bilgisayar tarafından anahtarlayıcıya (switch) hızlı bir şekilde ard arda sahte MAC adresleri gönderilir. Bu işlem MAC Adres tablosu devam edene kadar devam eder. MAC adres tablosunda çok fazla kayıt yapıldığından dolayı erişilmesi istenen bilgisayarlara erişim sağlanamaz ve gerçek isteklerin dışında bir veri trafiği oluşur. Kontrolsüz oluşan bu trafik normal ağ trafiğini de olumsuz yönde etkilenmesine ve diğer bilgisayarların erişimlerinin kısıtlanmasına da sebep olabilmektedir. Anahtarlayıcı (switch) üzerinde bulunan MAC adres tablosu tamamen dolduktan sonra artık anahtarlayıcı (switch) bir "hub" gibi bir porta gelen çerçeveleri (frame) diğer tüm portlara aynen gönderir. Artık bu anahtarlayıcının (switch) bağlı

tüm portların trafiği rahatlıkla dinlenebilir. MAC flooding saldırısı Şekil 2.17'de görünmektedir.



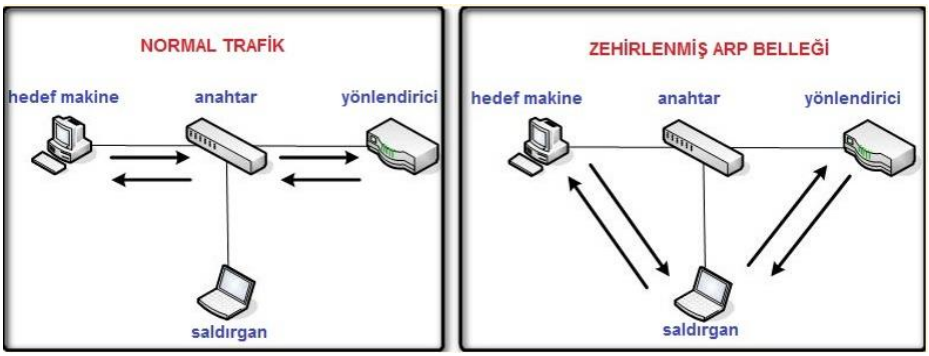
Şekil 2.17 MAC flooding saldırısı

Anahtarlayıcılar (switch) üzerinde her portta MAC adresi güvenliği uygulaması zor olan bir güvenlik çözümdür. Önce bütün kullanıcıların MAC adresleri toplanmalı, her porta kullanıcı MAC bilgileri portlara girilmelidir. Bu bilgilerin sürekli olarak güncel tutulması da kolay değildir. Günümüzde MAC adresi rahatlıkla değiştirilebilmektedir. MAC adresi sabitlenen bir porttan aynı MAC adresini tanımlayan başka bir kullanıcı rahatlıkla erişim sağlayabilir. Bu sebeple belirli kurallarla anahtarlayıcı (switch) portlarında kısıtlama yaparak, sadece tanımlama yapılan cihazların ilgili portları kullanmalarına izin verilebilir. Eğer, izin verilmeyen bir cihaz porta bağlanırsa, anahtarlayıcı (switch) durumu bilgi mesajı olarak kayıt yapabilir, o cihazdan gelen çerçeveleri engelleyebilir ya da ilgili portu kapatabilir (İnt.Kyn.30).

Yönetilebilir anahtarlayıcılarda bazı güvenlik kuralları ile ağda yapılabilecek saldırılara karşı önlem alınabilir. MAC flood saldırılarına karşı olarak port security (port güvenliği) uygulaması kullanılır. Anahtar (switch) portlarına MAC adreslerini atayarak portu belirtilen MAC adresi dışında başka bir ağ cihazının kullanması engellenmiş olur. Port security ile saldırganlar tarafından MAC flood (MAC adres taşması) saldırıları ve anahtarın (switch) MAC adres tablosu doldurulup hub gibi çalışması engellenir. Malware gibi yazılımlar ise bir yazılım veya kullanıcı bilgisi dahilinde MAC adresini değiştirip izini kaybettiremez.

2.9.3 ARP Zehirlemesi (ARP Poisoning)

ARP poisoning saldırısı ağı kullanılamaz duruma getirme ya da ağ üzerinden geçen trafiği dinlenmesi için yapılan saldırı yöntemlerinden birisidir. Çoğu zaman göz ardı edilen bu yönteme karşı alınmayan önlemler sonucunda networkta darboğaz oluşarak kesintiye uğrayabilir ya da bu network trafiği istenmeyen bir adres üzerine yönlendirilebilir. Bu saldırılara karşı ağ cihazları üzerinde yapılacak basit işlemler ile yerel ağlarda gerçekleştirilen sahte ARP istekleri engellenebilmektedir. Arp zehirlenmesi saldırısı Şekil 2.18'de gösterilmiştir.



Şekil 2.18 ARP zehirlenmesi saldırısı (İnt.Kyn.31).

ARP protokolü vasıtası ile yerel ağ üzerinde ARP poisoning saldırısı yapılabilir. Bu saldırı türünde saldırgan ARP tablosunu zehirlenerek ortadaki adam saldırısını yapar. Saldırgan ağ üzerindeki her iki kullanıcıya da sahte ARP paketleri göndererek kendisini kullanıcı gibi tanıtır. Eğer yapılan saldırı başarılı olursa kullanıcıları zehirleyerek ARP tablosunu değiştirmiş olur. Bu sayede iki kullanıcı arasındaki tüm veri trafiği saldırgan üzerinden diğer kullanıcıya aktarılır (İnt.Kyn.32)

2.9.4 DHCP Protokolüne Yapılan Saldırılar

DHCP, istemci cihazlara, IP adresi, alt ağ maskesi, varsayılan alt ağ geçidi ve DNS adresi bilgilerini otomatik olarak dağıtan bir protokoldür. Bu protokol sayesinde, ağdaki tüm bilgisayarlara tek tek bilgi girmeye gerek kalmaz, IP çakışması gibi durumlar ortadan kalkar. İstemciler, DHCP sunucusundan gerekli bilgileri alabilmek için istek yollar; DHCP sunucusundan gelen bilgileri kullanarak internete

erişmeye çalışır. Yalnız bunu yaparken kendisine ilk cevap dönen DHCP sunucusunun gönderdiği bilgileri tercih eder.

Bu sisteme yönelik saldırılarda kendini DHCP dağıtıcı olarak ortama tanıtılan bilgisayar bütün trafiği üzerinde geçirebilir. Yapay MAC adreslerinden IP rezerve istekleri yapılarak IP havuzu doldurulur. DHCP sunucu isteklere cevap veremez duruma gelir. Aynı zamanda anahtarın (switch) MAC adresi de dolar ve anahtar (switch) hub gibi davranmaya başlar.

2.9.5 Hizmet engelleme saldırısı (Denial of Service - DoS)

DoS saldırıları bir sisteme birden çok paket yollayarak sistemi yavaşlatıp durdurmaya yönelik olarak yapılan saldırı türüdür. Bu paketler bazen çok büyük olmaktadır. Bazen de içerisinde çalıştırılması istenen zararlı kodları içerebilir. Bu paketler sistemin yükünü artmasına, kaynakları tüketerek sistemin durmasına ve hatta hizmet veremez duruma gelmesine yol açabilir.

2.9.6 Dağıtılmış hizmet engelleme saldırısı (Distributed Denial of Service - DDoS)

DDoS saldırıları DoS saldırılarının gelişmiş bir türevidir. Günümüzde, dağıtılmış hizmet reddi (DDoS) saldırıları, en yaygın güvenlik tehditlerinden biri olup özellikle kamu kurumlarına yönelik çok büyük bir tehdit oluşturmaktadır. DDoS'un diğer bir yönü ağ donanım cihazlarında kaynak tüketiminin IPS ağlarında tüketilen miktarlara kadar çıkabilmesidir. Bir web sitesine yapılan küçük bir DDoS atağı tüm IIS'in ağını servis dışı bırakabilir ve binlerce kullanıcının bu olaydan etkilenmesi sebep olabilir (Farraposo *et al.* 2005).

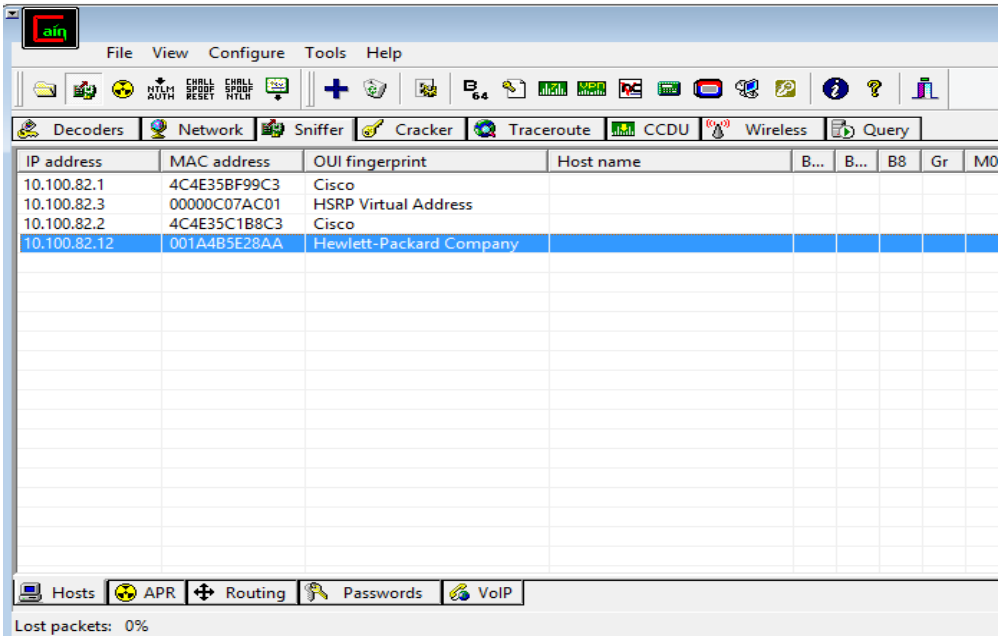
Bu yöntemde saldırgan girmek istediği bir ağın dışarıya açık bir servisini veya güvenlik duvarını, zombi bilgisayarlar kullanarak durdurup, ağa sızmaya olanak hazırlar. Zombiler, trojan ve virüs bulaştırılmış bilgisayar gruplarıdır ki saldırganlarca belli bir amaç için programlanabilir ve uzaktan kullanılabilirler. Zombi bilgisayarlar belli bir zamanda önceden belirlenmiş bir sisteme sürekli olarak sahte paket yollamaya

başlarlar (Gupta *et al.* 2012). DDoS saldırısı ile amaç bant genişliği tüketmek ve ağ güvenlik sistemlerinin kapasitesini zorlayarak kaldıramayacakları kadar yük bindirmektir.

2.10 Saldırı Araçları

Commview for Wi-Fi: Kablosuz ağ paketlerini görüntülemeye ve incelemeye yarayan bu program saldırganlar tarafından kablosuz ağ paketlerinin yakalanması amacı ile kullanılmaktadır. Yakaladığı bilgiler arasında erişim noktalarına ait, sinyal gücü, ağ bağlantısı ve protokol, ve bağlı olan istemciler gibi birçok bilgi bulunur.

Cain & Abel: ARP zehirleme (ARP poisoning), ve MITM (Man in the middle) gibi saldırı türlerinde ve siber güvenlik testlerinde kullanılabilecek araçlardan biridir (Resim 2.6).

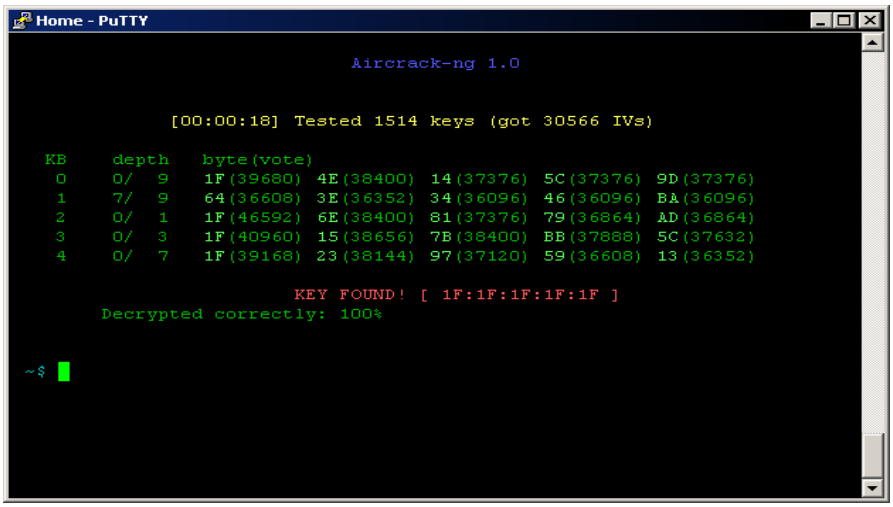


Resim 2.6 Cain&Abel programı

Kismet: Pasif ağları ve SSID yayınlanmayan erişim noktalarını bulmak için kullanılan kablosuz ağ programıdır.

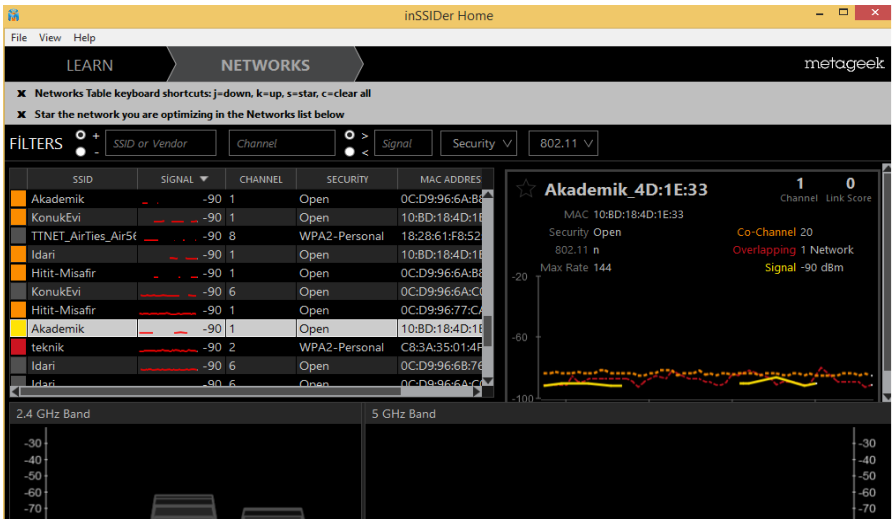
Kali Linux: İçerisinde birçok güvenlik aracını içerisinde barındıran ve güvenlik incelemeleri ve sızma testlerinde kullanılan Linux türevidir.

Aircrack: Kablosuz ağ WEP ve WPA şifre kırma konusunda en fazla kullanılan araçlardan bir tanesidir. Ethernet kartı ve sürücü yeteneklerini kontrol etmek ve paketleri yakalayarak algoritmalar ile paketler içerisindeki parolayı kurtarmak için kullanılır. Saldırganlar (hacker) tarafından wordlist (kelime listesi) ya da bruteforce (kaba kuvvet) atak yapılarak SSID parolasının kırılması amacı ile kullanılır (Resim 2.7).



Resim 2.7 Aircrack programı

InSSIDer: Kablosuz ağların tespit edilmesi, ağ problemlerinin tespit edilmesi için kullanılan araç yakında bulunan ağlar hakkında detaylı bilgi de vermektedir. MAC adresini, yönlendirici (router) üreticisini, kullandığı kanalı, SSID ismini ve sinyal seviyesini tespit edebilmektedir (Resim 2.8).



Resim 2.8 InSSIDer programı

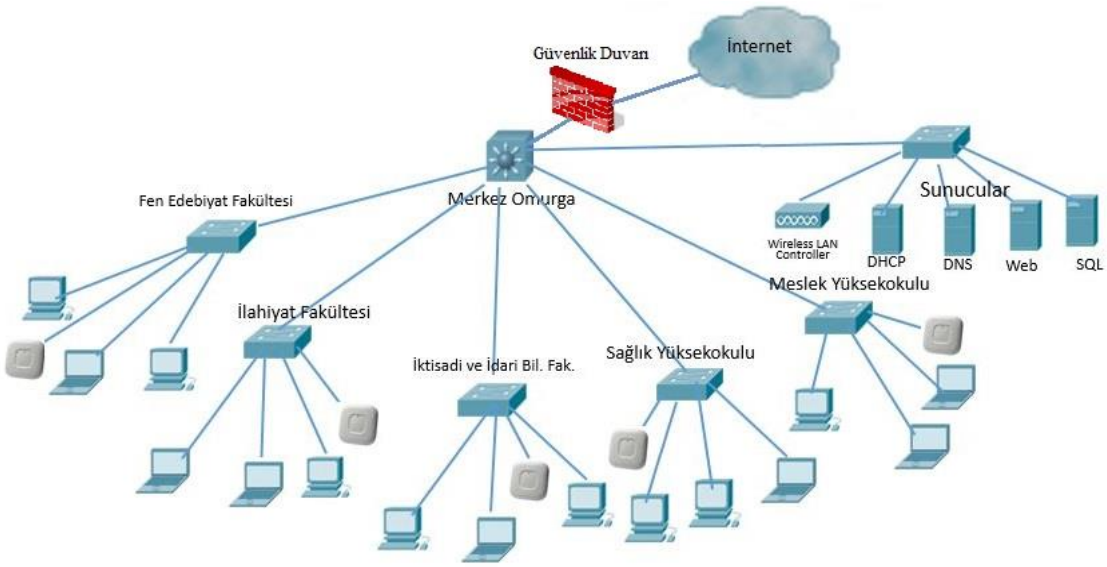
3. MATERYAL ve METOT

3.1 Kampüs Ağ Altyapısı

Büyük bir kampüs ağında farklı kullanıcı profillerine sahip kullanıcılar bulunmaktadır. Bu kullanıcıların ise farklı işletim sistemine sahip laptop, tablet, cep bilgisayarı, cep telefonu vb. farklı kullanıcı cihazları bulunmaktadır. Kampüs ağına dâhil olan bir virüslü bilgisayar network ağını kontrol dışı bırakabilir. Ağdaki bilgisayara ve önemli verilere bulaşabilir. Bu sebeple ağdaki cihazların ve kullanıcıların tiplerine göre kategorize edilmeli ve yetkilendirilmedir. Bu işlem bilgisayar ağlarının yönetilmesini kolaylaştıracaktır.

Bir ağ ne kadar küçük olursa, o ağın yönetimi, problemlere müdahale süreci ve problem çözme süreci de o kadar kolay olur. Örneğin bir personel, muhasebe ve misafirlerden oluşan bir ağ düşündüğümüzde personellerin özel yazışmalarını misafirlerin ve muhasebe biriminin görmeleri istenmeyen bir durumdur. Aynı şekilde de muhasebe birimindeki kullanıcıların da özel yazışmaları görmeleri istenmez. Misafirlerin ise ağdaki her yere ulaşmaları ve internette her siteye erişmeleri istenmez. Üç gruptan oluşan bu küçük ağ, eğer gruplandırılmaz ve yetkilendirilmez ise yönetimi zorlaşacak ve oluşacak problemlere müdahale ve çözüm süreci normalden çok daha fazla zaman alacaktır.

Hitit Üniversitesi Aralık 2016 itibariyle 8 fakülte, 2 yüksekokul, 7 meslek yüksekokulu, 3 enstitü ve 11 araştırma merkezine sahip olup yaklaşık olarak 18.000 öğrenciye hizmet vermektedir. Bilgi işlem merkezi Kuzey Kampüs yerleşkesinde bulunmakta ve bu yerleşkede yeni fakülte binaları yapım aşamasındadır. Bu farklı yerleşkeler merkeze noktadan noktaya metro ethernet (fiber) ile bağlanmış durumdadır. Kampüs ağ altyapısı geleneksel yıldız topolojisi tasarımına sahiptir (Şekil 3.1).



Şekil 3.1 Kampüs ağ altyapısı

3.2. Materyal

Yapılan tez çalışmasında aşağıdaki materyaller kullanılmıştır.

- Omurga Anahtar (Backbone Switch)
- Dağıtım Anahtarı (Distribution Switch) (2 adet)
- Kenar Anahtar (Edge Switch) (2 Adet)
- Güvenlik Duvarı (Firewall)
- Erişim Cihazı (AP) (4 Adet)
- WLC (Wireless Lan Controller)
- İnternet Trafik İzleme ve Analiz Yazılımları (4 adet)
- RADIUS Sunucusu

Yapılan bu çalışmada üç farklı anahtarlama cihazından faydalanılmıştır.

3.2.1 Cisco 6509

Laboratuvar çalışmasında Omurga anahtar görevi görmüştür. Tüm üniversite trafiğini kaldırabilecek yüksek anahtarlama kapasitesine sahiptir. Tüm internet trafiği bu cihaza yönlendirilmekte ve internet çıkışı bu cihaz üzerinden yapılmaktadır (Şekil 3.2).

Şekil 3.2 Cisco 6509 anahtar (İnt.Kyn.33).

3.2.2 Cisco 3750

Dağıtım anahtarı olarak Cisco 3750 cihazları kullanılmıştır. Bu cihazlar L3 seviyesinde yönlendirme yapılabilmesine ve VLAN'lar arasın haberleşme yapabilmesine olanak tanımaktadır. Teknik özellik bakımından yüksek anahtarlama kapasitesine sahiptir. Laboratuvar çalışmasında DHCP sunucu görevi bu cihazlara verilmiştir.

3.2.3 Cisco 2960

Kenar noktalarda kullanılmak için Şekil 12.2'de görülen Cisco 2960 model anahtarlama cihazı kullanılmıştır. L2 seviyesinde yönlendirme kabiliyetine sahip bu cihazlar, her portu için özel ayarlar yapılmasına imkan veren yönetilebilir anahtarlama cihazlarıdır (Şekil 3.3).

Şekil 3.3 Cisco 2960 anahtar (İnt.Kyn.34).

3.2.4 Fortigate 1000C

Güvenlik duvarı (firewall) olarak kullanılan bu cihaz ağ güvenliğini sağlayarak dış ağdan iç ağa yapılacak saldırılara karşı korunması amacı ile kullanılan ağ cihazıdır. Sadece saldırılara karşı bir önlem değil aynı zamanda saldırı tespiti, antivirüs, uygulama kontrolü, web filtreleme özelliklerini de içerisinde barındırmaktadır. Ağ güvenliğinin sağlanması amacı ile internet çıkış noktasına güvenlik duvarı konumlandırılmıştır.

3.2.5 Cisco 1700 AP

Kablosuz ağ bağlantısı için kullanılan ağ cihazı hem özerk olarak hem de kontrol cihazı destekli olarak yapılandırılmıştır. Uygulamada yönetim bakımından farkları incelenmiştir.

3.2.6 Cisco WLC 5508

Kablosuz ağ cihazı yönetimi için kullanılmıştır. Tek bir ara yüzden kablosuz ağ cihazlarının yönetimini bu cihaz üzerinden yapılmış ve bazı bilgilere bu cihaz üzerinden ulaşılabilmektedir.

3.2.7 Cactiez Yazılımı

Network üzerinde konumlandırılmış aktif cihazlarınızın bellek, port yoğunluğu, işlemci kullanım durumu gibi bilgileri gözlemlemeye olanak sağlayan açık kaynak kodlu bir yazılımdır. Cihaz bilgilerini almak için SNMP protokolünü kullanır. Aldığı bilgileri ise rrdtool aracı vasıtası ile grafiksel hale getirir. Bu yazılımın diğer özellikleri ise aşağıdaki gibidir.

- SNMP vasıtası ile oluşturulan grafiksel verilere web arayüzü üzerinden erişmeye imkan verir. Bu grafiksel verilere geçmişe yönelik olarak

erişilebilmekte ve port yoğunluğu ve darboğaz durumları tespit edilebilmektedir.

- Network cihazlarının bant genişliği kullanımı, Throughput değerleri gibi bilgileri tarihsel ve grafiksel olarak web arayüzü üzerinden görüntüleyebilir (İnt.Kyn.35).

3.2.8 Solarwinds Real Time Bandwidth Monitor Yazılımı

Ağ cihazları üzerinde bulunan portlardan geçen trafik yükü bilgilerini gerçek zamanlı olarak almak için kullanılan ücretsiz bir yazılımdır. Bu bilgileri almak için SNMP protokolünü kullanır.

3.2.9 Scrutinizer Netflow Analiz Yazılımı

Yönlendirici (router) olarak çalışan yönlendirici cihaza gerekli tanımlamalar yapıldıktan sonra trafik veri akış bilgisi Netflow analiz yazılımına iletilir. Bu yazılım ile kullanıcıların erişim performansının düşmesi ve olası güvenlik risklerine tespit edilebilmesi ve kullanıcıların ve uygulamaların ağ kullanım yoğunluklarını saptayarak ağ yöneticilerine yardımcı olması amacı ile kullanılır.

3.2.10 Wireshark Protokol Analiz Yazılımı

Ağ trafiğinin izlenmesi, paketlerin analiz edilmesi ve ağdaki problemlerin tespit edilmesi amacı ile kullanılan ağ protokol analiz yazılımıdır. Ağ problemlerinin giderilmesi, paket hatalarının tespit edilmesi amacı ile kullanılmaktadır. Ayrıca ağ içinde olağan dışı trafik olduğu anlaşıldığında bu trafiğin ne olduğunu anlamaya yardımcı olur.

3.2.11 Linux İşletim Sistemi

Çalışma içinde kullanılan RADIUS sunucu için açık kaynak kodlu işletim sistemi olan CENTOS (The Community Enterprise Operating System) tercih edilmiştir. Linux

türevi olan CENTOS, RHEL (Red Hat Enterprise Linux) kaynak kodları üzerinde geliştirilmiştir. Bağımsız bir yazılımcı grubu tarafından geliştirilen CENTOS sunucularda gösterdiği yüksek performans nedeniyle birçok web geliştiricisinin ilk tercihleri arasında yer almaktadır. Linux tabanlı yazılan Cpanel, Plesk Panel, Direct Admin gibi yönetim panelleri de CENTOS ile uyumlu olarak çalışmaktadır.

3.2.12 Kimlik Denetimi

RADIUS, Livingston Enterprise tarafından geliştirilmiş kimlik denetleme sunucusudur. Uzaktan bağlanan kullanıcılar için bir istek aldıktan sonra gelen isteğe sahip kullanıcı bilgisinin doğru olup olmadığını kontrolünü yapar. RADIUS, istemci sunucu tabanlı olarak çalışır. Mesaj bilgilerinin değişimi için UDP protokolünü kullanır. Sunucu ve kullanıcı arasında oluşan iletişim birincil anahtar ile şifrelenir. Bu sayede şifre hiçbir zaman ağ üzerinden gönderilmez. Eğer sunucu ve kullanıcı şifreleri uyuşmazsa kurulan bağlantı sona erdirilir. RADIUS sunucuya birden fazla LDAP ve SQL tanımlanabilmektedir. Bu işlemler sonunda yönetim kolaylığının yanı sıra sistem güvenliği de sağlanmaktadır.

3.2.13 Kullanıcı Bilgileri

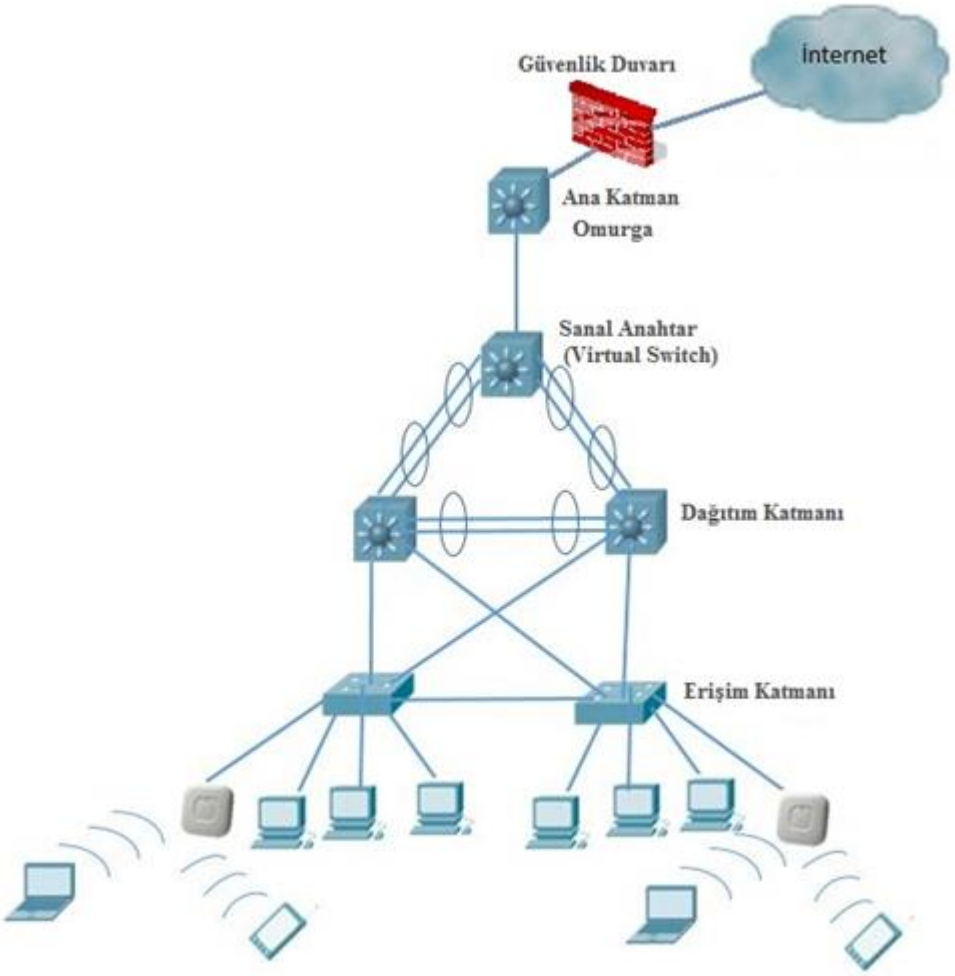
Sistemi kullanacak kişilerin kullanıcı bilgileri Microsoft dizin hizmeti olan Active Directory üzerinde tutulmaktadır. LDAP, Active Directory içerisinde sorgulama (query) ve güncelleme (update) için kullanılan, temel bir dizin servis protokolüdür. LDAP protokolü sayesinde network içerisindeki kaynaklara ulaşım daha da hızlandırılmış olur. LDAP, Aktive Directory içerisindeki objeleri isimlendirirken X.500 isimlendirme standardını kullanmaktadır.

Tüm Active Directory objeleri, Network ortamında kendilerine ulaşılmasını sağlayan komple dizin komponenti kullanan DN (Distinguished Name)' e sahiptir. Burada grup ve kullanıcı adları için CN (Common Name) , Organizasyon bilgisi için OU (Organizational Unit) ve Domain hiyerarşisini belirtmek için DC (Domain Controller) terimleri kullanılır.

Relative Distinguished Name ise AD içinde tek olan Domain ismini belirtir. DN sayesinde bir objenin tam olarak yeri belli olur. Objelerin yedekten dönülmesi, yetkilendirilmesi ya da silinmesi gibi önemli adımlarda obje ismi yerine DN kullanılır, bu sayede bu objenin gerçekte hangi obje olduğu kesin olarak tanımlanmış olur (İnt.Kyn.36).

3.3 Metot

Bu tasarım modelinde hem kablolama hem de fiziksel cihaz olarak yedekliliğin sağlanması amaçlanmıştır. Bu tasarımda 4 farklı VLAN oluşturulmuş, anahtarlar üzerinde yedeklilik ve güvenlik için gerekli tanımlamalar yapılmıştır (Şekil 3.4).



Şekil 3.4 Hiyerarşik ağ tasarımı uygulaması

3.3.1 Firewall Yapılandırması

Laboratuvar ortamında kullanılacak IP blokları Resim 3.1'de görüldüğü şekilde güvenlik duvarı üzerinde tanımlanmıştır.

Name	Type	Details	Interface
LAB-82	Subnet	10.100.82.0/24	Any
LAB-83	Subnet	10.100.83.0/24	Any
LAB-84	Subnet	10.100.84.0/24	Any
MANAGEMENT	Subnet	10.99.16.0/24	Any
MANAGEMENT_2	Subnet	192.168.1.0/24	Any
MISAFIR	Subnet	10.27.0.0/16	Any
MUHENDISLIK	Subnet	10.100.20.0/22	Any
MVCServer	Subnet	79.123.184.98/32	Any
MYO Isıtma Sogutma Sis. SRV	Subnet	10.100.4.54/32	Any

Resim 3.1 Firewall yapılandırması ekran görüntüsü - 1

İlgili ağların internete çıkabilmesi için içeriden dışarıya doğru çıkabilmesi için ilgili kurallar güvenlik duvarında tanımlanmıştır. Resim.3.2'de görüldüğü üzere sadece HTTP, HTTPS ve ICMP protokollerine izin verilmiştir. Böylece farklı portlardan dışarıya doğru yapılabilecek tehlikelerin önüne geçilmiştir.

Seq.#	Source	Destination	Service	Action	IPS	AV
port5 (INSIDE) - port3 (OUTSIDE) (98 - 147)						
110	BILGIISLEM	nvi.gov.tr KamuSM NES IP	ALL	✓ ACCEPT	webserver-ips	default
111	BILGIISLEM	all	ALL	✓ ACCEPT	default	default
112	LAB-82 LAB-83 LAB-84	all	HTTP HTTPS icmp4	✓ ACCEPT	default	default
113	REKTORLUK	all	ALL	✓ ACCEPT	default	default
114	GENEL_SEKRETERLIK	all	ALL	✓ ACCEPT	default	default
115	OGRENCI_ISLERI	all	ALL	✓ ACCEPT	default	default

Resim 3.2 Firewall yapılandırması ekran görüntüsü - 2

İç IP adresine sahip bilgisayarların dış ortama gerçek bir IP adresi üzerinden çıkmaları gerekmektedir. Bu sebeple güvenlik duvarında tanımlanan ilgili kural Resim 3.3'te görüldüğü gibidir.

IPv4 Pool (39)	
10.200.0.2_NAT	193.255.107.221 - 193.255.107.221
10.200.0.3_NAT	193.255.107.222 - 193.255.107.222
ALACA	193.255.107.100 - 193.255.107.100
BAP-DONERSERMAYE	193.255.107.218 - 193.255.107.218
LAB_NAT	193.255.107.185 - 193.255.107.185
BOGAZKALE_ARSMER	193.255.107.200 - 193.255.107.200
ENSTITU	193.255.107.120 - 193.255.107.120
FEF	193.255.107.70 - 193.255.107.70
GENEL_SEKRETERLIK	193.255.107.187 - 193.255.107.188
GLOBAL	193.255.107.201 - 193.255.107.212

Resim 3.3 Firewall yapılandırması ekran görüntüsü - 3

3.3.2 Ağ Cihazlarının Yapılandırılması ve Güvenliği

Öncelikli olarak ağ cihazları konumlandırılmıştır. Anahtarlara (switch) yönetim konsol portlarından bağlantı sağlandıktan sonra trunk ve access portlar belirlenmiştir. IP tanımlamaları, DHCP tanımlamalarının ardından diğer yapılandırma ayarları yapılmıştır. Cihaz güvenliğinin sağlanması için kullanıcı tanımlaması yapılmış ve güvensiz olan Telnet ve HTTP protokolleri kapatılmıştır. Ağ trafiğinin ve cihaz güvenliğinin sağlanması amacı sadece SSH erişimine izin verilmiştir. SSH trafiği 1024 bit ile şifrelenmiştir. Yapılandırma ayarları Çizelge 3.1'de görüldüğü gibi yapılmıştır.

Çizelge 3.1 Cihaz SSH yapılandırması

Kullanılan Komutlar
Switch3(config)#ip domain-name test.local.hitit.edu.tr
Switch3(config)#username admin password labtest
Switch3(config)#enable password labtest
Switch3(config)#line vty 0 4
Switch3(config-line)#transport input ssh
Switch3(config-line)#login local
Switch3(config-line)#crypto key generate rsa modulus 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

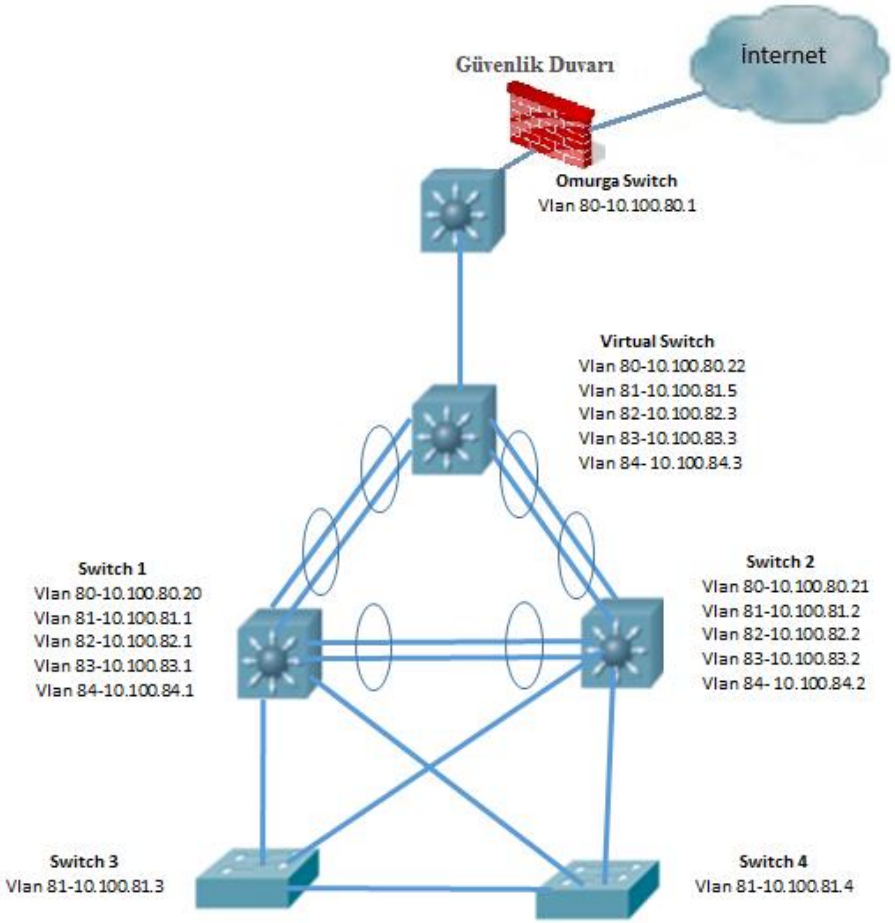
Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu işlemin yapılabilmesi için erişim kontrol listesi kullanarak yapılabilir. Uygulamada access-list yazılarak sadece 10.100.81.3 ve 10.100.81.4 IP'lerin erişimine izin verilmiş ve diğer IP adresleri engellenmiştir.

Çizelge 3.2 Cihaz erişim güvenliği

Kullanılan Komutlar
Switch3(config)#access-list 3 permit 10.100.81.3
Switch3(config)#access-list 3 permit 10.100.81.4
Switch3(config)#access-list 3 deny any log

3.3.2.1 Anahtarlarda (Switch) VLAN ve IP Dağılımı

L3 anahtarlarda (switch) VLAN arayüzleri oluşturulmuş, her ağ için birer IP adresi tanımlaması yapılmıştır. Benzer bir yapı sanal anahtar (switch) üzerinde de uygulanmış ve bu VLAN'lardan gelen trafikler omurgaya yönlendirilmiştir (Şekil 3.5).



Şekil 3.5 Anahtar (switch) VLAN ve IP yapıları

Anahtarların (switch) komşuları Resim 3.4'te görülebilmektedir.

```
Switch1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch3          Gig 0/22          129          S I   WS-C2960S Gig 1/0/24
Switch4          Gig 0/21          129          S I   WS-C2960S Gig 1/0/24
6509.hitit.edu.tr
                 Gig 0/1           164            R S I WS-C6509- Gig 1/4
6509.hitit.edu.tr
                 Gig 0/2           164            R S I WS-C6509- Gig 1/5
Switch2.hitit.edu.tr
                 Gig 0/24          179            R S I WS-C3560X Gig 0/24
Switch2.hitit.edu.tr
                 Gig 0/23          179            R S I WS-C3560X Gig 0/23
```

Resim 3.4 Anahtar (switch) komşuluk durumları ekran görüntüsü

3.3.2.2 VLAN Yapılandırması

Belirli ağlara kurallar tanımlayabilmek ve yönetimin daha iyi yapılabilmesi için VLAN kullanılarak ağ küçük parçalara ayrılmıştır. Erişim katmanında ve dağıtım katmanında bulunan tüm anahtarlarda (switch) VLAN tanımlaması Resim 3.5'te gösterildiği şekilde yapılmıştır.

```
Switch3#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28
81   MANAGEMENT                       active    Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21
82   MUHASEBE                         active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/14
83   PERSONEL                         active    Gi1/0/6, Gi1/0/7, Gi1/0/8
                                                Gi1/0/9, Gi1/0/10
84   MISAFIR                          active    Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/15, Gi1/0/16, Gi1/0/22
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Resim 3.5 VLAN yapısı ekran görüntüsü

VLAN'lar tanımlandıktan sonra ilgili portlar tanımlanan anahtarlar (switch) üzerindeki ana portlar Resim 3.6'da görüldüğü şekilde trunk olarak belirtilmiştir.

```
Switch1#sh running-config interface gigabitEthernet 0/23
Building configuration...

Current configuration : 188 bytes
!
interface GigabitEthernet0/23
 switchport trunk allowed vlan 80-84
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip access-group 100 in
 channel-group 2 mode active
end

Switch1#sh running-config interface gigabitEthernet 0/24
Building configuration...

Current configuration : 188 bytes
!
interface GigabitEthernet0/24
 switchport trunk allowed vlan 80-84
 switchport trunk encapsulation dot1q
 switchport mode trunk
 ip access-group 100 in
 channel-group 2 mode active
end
```

Resim 3.6 Trunk port yapısı ekran görüntüsü

3.3.2.3 Spanning Tree Yapılandırması

L2 seviyesinde yönetim sağlayan STP (Spanning Tree Protokol) protokolü ile ağ döngüleri (loop) oluşması engellenebilmektedir. Aynı hedefe giden iki veya daha fazla kablo sonsuz döngüye girerek ağ içerisinde Broadcast Storm (Yayın Fırtınası) oluşturabilir. Bunun sonucunda tüm bant genişliği işgal edilebilir ve ağ kullanılamaz hale gelebilir. STP protokolünü kullanma amacımız, yedek hatların kullanabilir halde bekletilerek, en kısa ve en hızlı yoldan iletişimin devam edebilmesi ve ağ üzerinde döngülerin oluşmasının engellenmesidir.

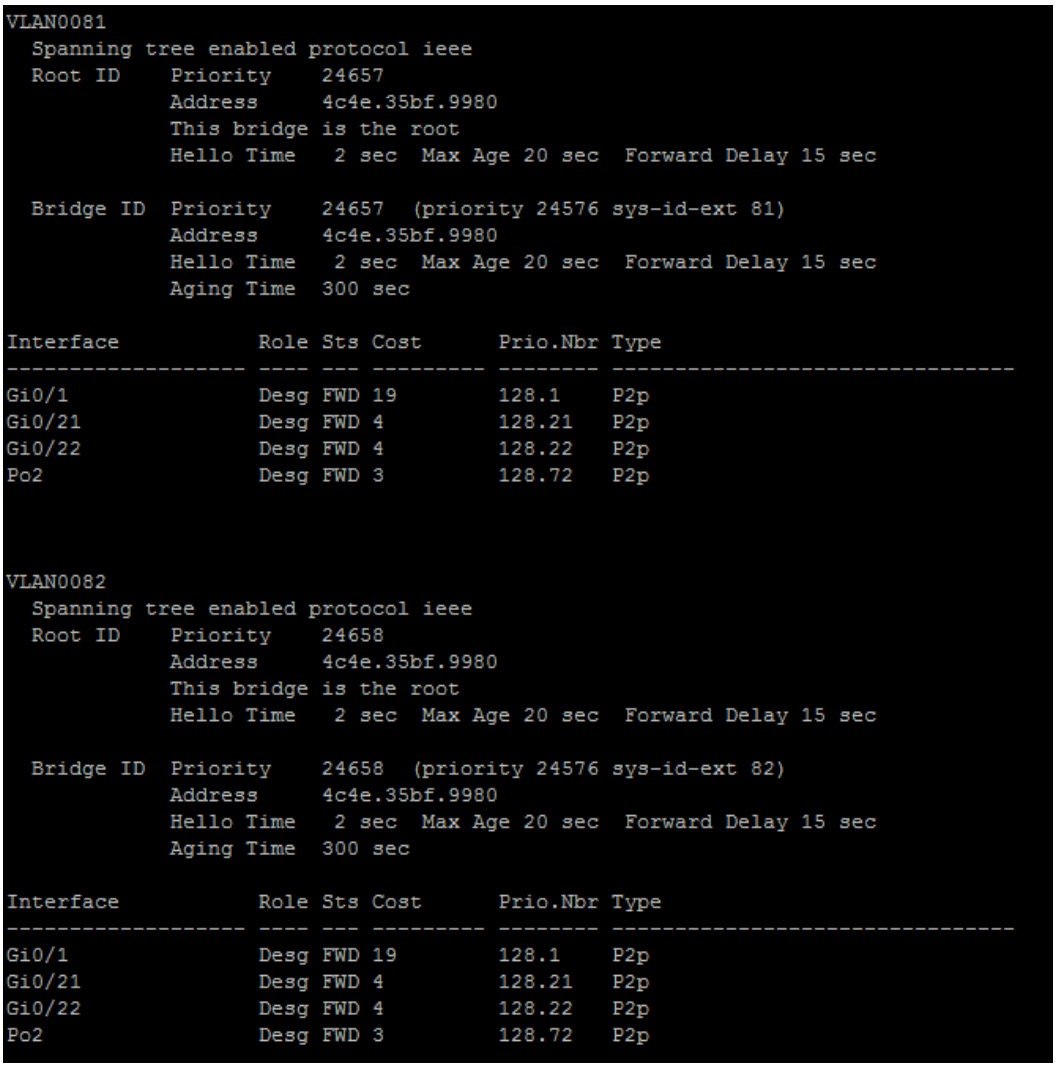
STP protokolü vasıtası ile anahtarlayıcılar (switch) ağ içerisinde, iki saniyede bir kez BPDU (Bridge Protocol Data Units) mesajı gönderirler, BPDU paketinin içerisinde ID (Identification) bilgileri bulunur. Köprü kimliği (bridge ID) en küçük olan cihaz ağda kök köprü (root bridge) olarak tanımlanır.

Uygulamamızda STP protokolü kullanılarak VLAN'lar için kök köprü (root bridge) belirtilmiştir. Bu seçim işleminde uygun yolun seçilmesi ve network yükünün paylaştırılması için gerekli yapılandırma ayarları Çizelge 3.3'te görüldüğü gibi yapılmıştır.

Çizelge 3.3 Spanning-tree yapılandırması

Kullanılan Komutlar
Switch1#spanning-tree vlan 81-82 root primary
Switch1#spanning-tree vlan 83-84 root secondary
Switch2#spanning-tree vlan 81-82 root secondary
Switch2#spanning-tree vlan 83-84 root primary

L3 anahtarlarda yapılandırma sonucunda VLAN'lar için kök (root) durumları ve öncelik değerleri Resim 3.7'de görüldüğü gibidir.



Resim 3.7 Spanning-tree ekran görüntüsü

3.3.2.4 Hat Birleştirme (Etherchannel) Yapılandırması

Etherchannel veya Link Aggregation yapılandırması sayesinde hem yedeklilik (redundancy), yük dengeleme (load balancing) ve yüksek bant genişliği sağlanmış olur. Bu işlem en az 2 en fazla 8 hat birleştirilebilir. Etherchannel yapılacak olan portlar aynı hıza sahip olmalı ve aynı VLAN da yer almalıdır.

Uygulamada anahtarlar (switch) üzerinde ikişer port etherchannel port olarak belirlenmiş ve ayarları karşılıklı olarak aynı olacak şekilde yapılmıştır (Resim 3.8).

```
Switch1(config)#interface Port-channel1
Switch1(config-if)#switchport trunk allowed vlan 80-84
Switch1(config-if)#switchport trunk encapsulation dot1q
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
Switch1(config)#interface Port-channel2
Switch1(config-if)# switchport trunk allowed vlan 80-84
Switch1(config-if)#switchport trunk encapsulation dot1q
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
Switch1(config)#interface range GigabitEthernet0/1-2
Switch1(config-if-range)#channel-group 1 mode active
Switch1(config-if-range)#end
Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#interface range GigabitEthernet0/23-24
Switch1(config-if-range)#channel-group 2 mode active
Switch1(config-if-range)#exit
```

Resim 3.8 Switch1 Etherchannel yapılandırması örneği

Komutlar anahtarların (switch) ilgili portlarında uygulandıktan sonra konfigürasyon çıktısına bakıldığında portların L2 olarak LACP (Link Aggregation Control Protocol) protokolü ile Etherchannel ayarlarının yapıldığı görülmektedir (Resim 3.9).

```
Switch1#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)         LACP      Gi0/1(P)    Gi0/2(P)
2      Po2(SU)         LACP      Gi0/23(P)   Gi0/24(P)
```

Resim 3.9 Switch1 Etherchannel yapılandırma durumu

3.3.2.5 Yönlendirme İşlemi

Veri paketlerinin bir ağdan başka bir ağa gönderilmesi işlemine yönlendirme (routing) denir. Yönlendirme işlemini üçüncü katmanda yönlendiriciler (router) yapar. Yönlendirmeler genellikle hedef ağa bağlıdır. Yönlendiricilerin (router) paketleri yönlendirme yaparak hedef ağa göndermeyi başarabilmesi için yönlendirme tablosuna (routing table) ihtiyacı vardır.

Yönlendirici (router) farklı networklerin birbirleriyle haberleşmesi için hangi yolu kullanması gerektiğini hesaplayarak uygun yolu seçebilir ya da paketlerin hangi

yoldan gideceği static olarak belirtilebilir. Dinamik Routing protokolleri olarak RIP, OSPF ve BGP (Border Gateway Protocol) ve IGRP protokolleri kullanılmaktadır. Dağıtım anahtarları (switch) ve omurga anahtar (switch) üzerinde tanımlanan arayüzlere IP adresleri verilmiştir. Sonrasında yönlendirme işlemi yapılmıştır.

Çizelge 3.4'te görülen yapılandırma tanımlamaları sonucunda kenar anahtarlarda oluşan gereksiz yayın (broadcast) trafiği ve iç ağ trafiği omurgaya kadar ulaşmayacak ve dağıtım anahtarlarında sonlanacaktır. Sadece bu VLAN'lar dışındaki trafik omurgaya ulaştırılmayacaktır.

Çizelge 3.4 L3 anahtar komutları tablosu

Switch1	Switch2
interface Vlan81	interface Vlan81
ip address 10.100.81.1 255.255.255.0	ip address 10.100.81.2 255.255.255.0
ip default-gateway 10.100.81.1	ip default-gateway 10.100.81.2
ip routing	ip routing
ip route 0.0.0.0 0.0.0.0 10.100.80.22	ip route 0.0.0.0 0.0.0.0 10.100.80.22

Omurga anahtardan (switch) kenar anahtarlara (switch) doğru olan trafik ise Çizelge 3.5'te görüldüğü şekilde yönlendirilmiştir.

Çizelge 3.5 Omurga anahtar komutları tablosu

Kullanılan Komutlar
interface Vlan 80
ip address 10.100.80.1 255.255.255.0
ip routing
ip route 10.100.81.0 255.255.255.0 10.100.80.22
ip route 10.100.82.0 255.255.255.0 10.100.80.22
ip route 10.100.83.0 255.255.255.0 10.100.80.22
ip route 10.100.84.0 255.255.255.0 10.100.80.22

3.3.2.6 DHCP Konfigurasyonu

Switch1 ve Switch2 üzerinde DHCP havuzları oluşturularak ağ geçidi ve DNS sunucu tanımlamaları yapılmıştır. Bu anahtarlar (switch) yedekli çalışacağı için iki anahtar (switch) üzerinden de aynı komutlar çalıştırılmış ve Resim 3.10'da görüldüğü şekilde aynı yapı oluşturulmuştur. Her havuzdan 10 (on) IP adresi dağıtım dışında bırakılmıştır.

```
ip dhcp excluded-address 10.100.82.0 10.100.82.10
ip dhcp excluded-address 10.100.83.0 10.100.83.10
ip dhcp excluded-address 10.100.84.0 10.100.84.10
!
ip dhcp pool VLAN_82
 network 10.100.82.0 255.255.255.0
 default-router 10.100.82.3
 domain-name hitit.edu.tr
 dns-server 79.123.184.24 79.123.184.26
!
ip dhcp pool VLAN_83
 network 10.100.83.0 255.255.255.0
 default-router 10.100.83.3
 domain-name hitit.edu.tr
 dns-server 79.123.184.24 79.123.184.26
!
ip dhcp pool VLAN_84
 network 10.100.84.0 255.255.255.0
 default-router 10.100.84.3
 domain-name hitit.edu.tr
 dns-server 79.123.184.24 79.123.184.26
!
!
ip dhcp snooping
ip flow-cache timeout active 5
ip domain-name hitit.edu.tr
vtp mode transparent
```

Resim 3.10 DHCP yapılandırması ekran görüntüsü

3.3.2.7 HSRP (Hot Standby Router Protocol) Konfigurasyonu

HSRP, Cisco tarafından geliştirilen bu protokol, aynı işi yapan birden fazla yönlendirici (router) ya da L3 anahtarın (switch) ağda bulunan son kullanıcılara tek bir yönlendirici (router) gibi görünmesini sağlar. HSRP'de iki yönlendiriciden (router) birisi 'Active' diğeri ise 'Standby' olarak çalışır. Bunlardan biri aktif işlemleri yerine getirerek paketleri hedeflerine ulaştırırken, diğeri aktif olan yönlendiricide (router) herhangi bir aksaklık olması durumunda aktif olanın yerine geçmek için yedekte bekler. HSRP protokolünü kullanarak anahtarlardan (switch) biri yanıt vermese bile

trafik diğer anahtar (switch) üzerinden akacak, kullanıcılar bu durumdan en az şekilde etkilenecektir. Bu protokolü kullanarak hem yedekli yapı kurulmuş, hem de yük dengeleme işlemi yapılmıştır. L3 olarak tanımlanan anahtarlar (switch) için HSRP konfigurasyonu Çizelge 3.6'da görüldüğü gibidir.

Çizelge 3.6 HSRP konfigurasyonları

Switch 1	Switch 2
interface Vlan80	interface Vlan80
ip address 10.100.80.20 255.255.255.0	ip address 10.100.80.21 255.255.255.0
standby 4 ip 10.100.80.22	standby 4 ip 10.100.80.22
standby 4 priority 150	!
standby 4 preempt	interface Vlan81
!	ip address 10.100.81.2 255.255.255.0
interface Vlan81	standby 5 ip 10.100.81.5
ip address 10.100.81.1 255.255.255.0	!
standby 5 ip 10.100.81.5	interface Vlan82
standby 5 priority 150	ip address 10.100.82.2 255.255.255.0
standby 5 preempt	standby 1 ip 10.100.82.3
!	!
interface Vlan82	interface Vlan83
ip address 10.100.82.1 255.255.255.0	ip address 10.100.83.2 255.255.255.0
standby 1 ip 10.100.82.3	standby 2 ip 10.100.83.3
standby 1 priority 150	standby 2 priority 150
standby 1 preempt	standby 2 preempt
!	!
interface Vlan83	interface Vlan84
ip address 10.100.83.1 255.255.255.0	ip address 10.100.84.2 255.255.255.0
standby 2 ip 10.100.83.3	standby 3 ip 10.100.84.3
!	standby 3 priority 150
interface Vlan84	standby 3 preempt
ip address 10.100.84.1 255.255.255.0	
standby 3 ip 10.100.84.3	

Varsayılan olarak öncelik (priority) değeri 100 olarak tanımlıdır. Yüksek öncelik (priority) olan anahtar (switch) aktif durumda olur. Preempt komutu ise anahtarı (switch) kapanıp tekrar açıldığında aktif duruma geri alabilmek için kullanılır.

Yaptığımız konfigurasyon çıktıları Resim 3.11 ve Resim 3.12'de görüldüğü gibidir. Bu çıktılar incelediğimizde VLAN 80, 81 ve 82 için Switch1'in birincil olarak aktif durumda olduğu VLAN 83 ve 84 için ise ikincil durumda standby (hazırda bekleme) durumunda olduğu görülmekte, Switch2 için ise VLAN 83 ve 84'ün aktif olduğu ve VLAN 80, 81 ve 82 için ise standby (hazırda bekleme) durumunda olduğu görülmektedir.

```
Switch1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl80        4    150 P Active  local           10.100.80.21    10.100.80.22
Vl81        5    150 P Active  local           10.100.81.2     10.100.81.5
Vl82        1    150 P Active  local           10.100.82.2     10.100.82.3
Vl83        2    100   Standby 10.100.83.2     local           10.100.83.3
Vl84        3    100   Standby 10.100.84.2     local           10.100.84.3
Switch1#
Switch1#
```

Resim 3.11 HSRP ayarları çıktısı – örnek 1

```
Switch2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Vl80        4    100   Standby 10.100.80.20    local           10.100.80.22
Vl81        5    100   Standby 10.100.81.1     local           10.100.81.5
Vl82        1    100   Standby 10.100.82.1     local           10.100.82.3
Vl83        2    150 P Active  local           10.100.83.1     10.100.83.3
Vl84        3    150 P Active  local           10.100.84.1     10.100.84.3
Switch2#
```

Resim 3.12 HSRP ayarları çıktısı – örnek 2

3.3.2.8 AP Yapılandırması

Ağ üzerindeki AP cihazlar iki şekilde yönetilebilmektedir. Özerk Kablosuz Erişim Cihazı (Autonomous Access Point) ve Hafif Kablosuz Erişim Cihazı (Lightweight Access Point) olarak isimlendirilir. Özerk AP cihazlarının tek tek yapılandırılması gerekmektedir. Hafif AP cihazlar ise kontrol cihazı ile tek bir merkezden yönetilebilmektedir.

Özerk AP üzerinde yapılan uygulama ayarları yapılmıştır. Resim 3.13'te görüldüğü üzere BVI1 arayüz (interface) üzerinde IP tanımlaması yapıldıktan sonra gerekli SSID ismi verilmiş, parola ataması yapılarak şifreleme türü seçilmiştir. Yine SSID yayını için tüm yapılandırma ayarları yapılmalıdır. Bu ayarların tüm AP'lerde tek tek yapılması gerekmektedir. Ayarlarda yapılması gereken en küçük bir değişiklikte yine cihazlara teker teker bağlanılması ve ilgili değişikliklerin yapılması gerekmektedir.

```
hostname LAB_TEST_AP1
ssid Personel
!
encryption mode ciphers tkip
!
dot11 ssid Personel
  authentication open
  authentication key-management wpa version 2
  guest-mode
  wpa-psk ascii 7 14380112014A180605
!
ssid Misafir
!
dot11 ssid Misafir
  authentication open
  authentication key-management wpa version 2
  guest-mode
  wpa-psk ascii 7 14380112014A182964
!
interface BVI1
 ip address 10.100.81.28 255.255.255.0
 no ip route-cache
```

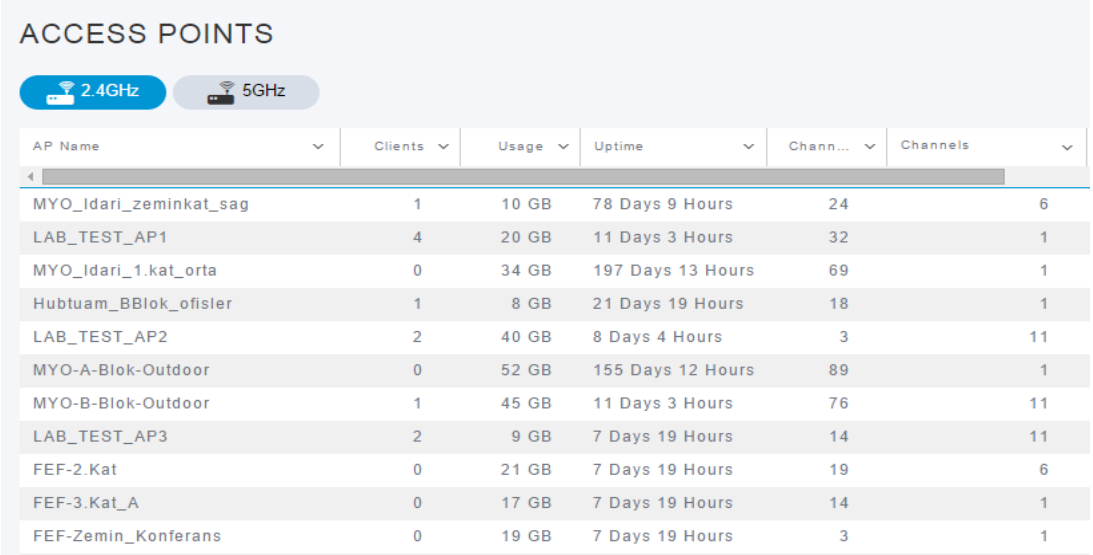
Resim 3.13 AP yapılandırma örneği

Kontrol cihazı destekli AP'ler ise yapılandırma işlemi çok daha basittir. Tek bir yerden yapılan değişiklik ilgili tüm AP'lere uygulanmaktadır. Aynı zamanda AP'ler üzerinde herhangi bir yapılandırma bulundurmaz (Resim 3.14).

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
2	WLAN	Misafir	Misafir	Disabled	Web-Passthrough
3	WLAN	eduroam	eduroam	Enabled	[WPA + WPA2][Auth(802.1X)]
4	WLAN	Idari	Idari	Enabled	Web-Auth
5	WLAN	Akademik	Akademik	Enabled	Web-Auth
6	WLAN	Ogrenci	Ogrenci	Enabled	Web-Auth
7	WLAN	Personel	Personel	Disabled	[WPA2][Auth(PSK)]

Resim 3.14 Kablosuz yönetim cihazı WLAN tanımlamaları

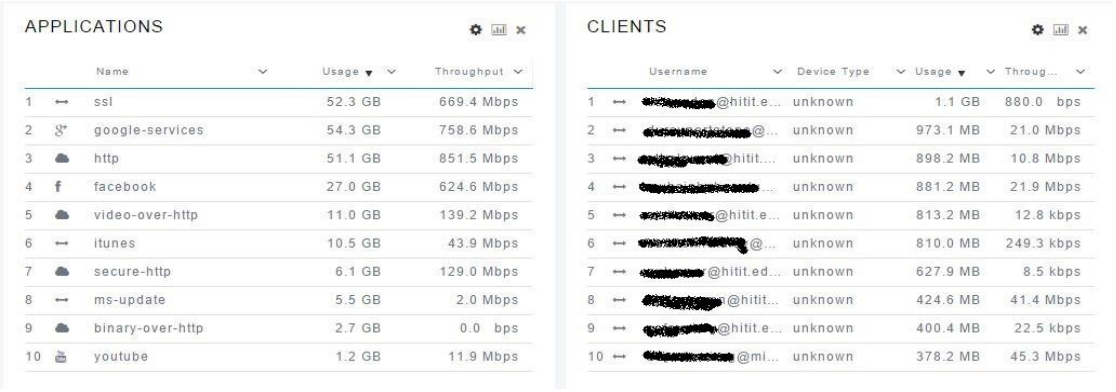
Kontrol cihazı kullanmanın faydalarından biri de istatistiki raporların tek bir arayüzde rahatlıkla görüntülenebilmesidir. Resim 3.15 ve Resim 3.16'de görüldüğü üzere kullanılan AP'ler, uygulamalar ve kullanıcılara ait anlık istatistiki bilgilere ulaşılabilmektedir.



AP Name	Clients	Usage	Uptime	Chann...	Channels
MYO_Idari_zeminkat_sag	1	10 GB	78 Days 9 Hours	24	6
LAB_TEST_AP1	4	20 GB	11 Days 3 Hours	32	1
MYO_Idari_1.kat_orta	0	34 GB	197 Days 13 Hours	69	1
Hubtuam_BBlok_ofisler	1	8 GB	21 Days 19 Hours	18	1
LAB_TEST_AP2	2	40 GB	8 Days 4 Hours	3	11
MYO-A-Blok-Outdoor	0	52 GB	155 Days 12 Hours	89	1
MYO-B-Blok-Outdoor	1	45 GB	11 Days 3 Hours	76	11
LAB_TEST_AP3	2	9 GB	7 Days 19 Hours	14	11
FEF-2.Kat	0	21 GB	7 Days 19 Hours	19	6
FEF-3.Kat_A	0	17 GB	7 Days 19 Hours	14	1
FEF-Zemin_Konferans	0	19 GB	7 Days 19 Hours	3	1

Resim 3.15 AP istatistikleri - 1

Kontrol cihazına bağlı AP isimleri, bu AP'ler üzerindeki kullanıcı sayıları, çalışma süreleri, kullanılan kanallar ve hangi AP'nin ne kadar veri kullandığı vb. bilgilere ulaşılabilmektedir. Resim 3.15'de görüldüğü gibi LAB_TEST_AP1 isimli AP cihazına 4 (dört) kullanıcı bağlı olduğu, kullanıcıların 20 GB veri kullandığı görülürken, LAB_TEST_AP3 isimli AP cihazına ise 2 (iki) kullanıcının bağlı olduğu ve bu kullanıcıların da 9 GB veri kullandığı görülmektedir.



Resim 3.16 AP istatistikleri - 2

Resim 3.16'nın Aplications bölümünde hangi uygulamanın kullanım miktarları ve toplam kullanım miktarları görülebilmektedir. SSL uygulaması 52.3 GB kullanıldığı, faceboook uygulamalarının 27 GB kullanım oranı bulunmakta iken youtube 1.2 GB ile en az kullanılan uygulama konumundadır. Resim 3.16'nın Clients bölümünde ise hangi kullanıcının ne kadar veri kullandığı görülebilmektedir. Kişisel hakların korunması açısından şahsi bilgiler gizleniştir.

3.3.3 Ağ Üzerinde Alınan Güvenlik Önlemleri

Günümüzde OSI'nin tüm katmanlarında ağ güvenliği düşünülerek bir yapı kurulması gerekmektedir. Birçok kurum, bir güvenlik duvarı (firewall) kullanıldığında güvenlik ile ilgili problemlerin çoğunun çözüldüğü sanılmakta ve diğer önlemler önemsememektedir. Oysa güvenlik terimi ile anlaşılması gereken ağ üzerinde çalışan bütün cihazların güvenliği olmalı ve süreklilik arz etmelidir.

Kurulan ağın kesintisiz olarak hizmet vermesi için de sağlıklı bir altyapı kurulmalı ve kurulacak bu yapının oluşması için ise saldırılara karşı birtakım güvenlik önlemleri alınmış olmalıdır.

3.3.3.1 Access List (Erişim Kontrol Listesi) Yapılandırması

Anahtarlar (switch) üzerinde access-list komutları erişime izin vermek ya da engellemek için kullanılmaktadır. Yapılan uygulamada misafir ağına bağlanan bir

kullanıcının Personel ve Muhasebe ağlarına erişmesi engellenmiştir. L3 olarak çalışan anahtarlarda (switch) bu komutlar Resim 3.17'de görüldüğü gibi uygulanmıştır.

```
Switch1#sh access-lists
Extended IP access list 100
    10 deny ip 10.100.84.0 0.0.0.255 10.100.82.0 0.0.0.255
    20 deny ip 10.100.84.0 0.0.0.255 10.100.83.0 0.0.0.255
    30 deny ip 10.100.84.0 0.0.0.255 10.100.81.0 0.0.0.255
    40 deny ip 10.100.84.0 0.0.0.255 10.100.80.0 0.0.0.255
    50 permit ip any any (22820 matches)
```

Resim 3.17 Erişim kontrol listesi kuralları

3.3.3.2 Port Security Yöntemi

Bu güvenlik önlemi kenar anahtarın portlarına uygulanan bir güvenlik önlemidir. Büyük bir ağda port bazında MAC adres güvenliği sağlanması oldukça zor bir iştir. Tüm kullanıcıların MAC adres bilgilerinin toplanması ve tüm portlarda sınırlamaların el ile yapılması ve bilgisayarların değişmesi durumunda MAC adres bilgisi değişeceğinden bu işlemlerin tekrar yapılması gerekmektedir. MAC flood atakları yapılarak anahtarların (switch) mac adres tablosu doldurulup hub gibi çalışması engellenebilir.

Uygulamada anahtarlarda (switch) son kullanıcı cihazlarının takılacağı tüm portlara bu güvenlik önlemi uygulanmıştır. Bir porta en fazla 3 (üç) adet cihaz takılabilecek durumdadır. Belirlenen sayıdan daha fazla cihazın takılması durumunda son takılan cihazlar port tarafından engellenecek ve cihazların ağa bağlanması engellenmiş olacaktır (Resim 3.18).

```
interface GigabitEthernet1/0/5
 switchport access vlan 82
 switchport mode access
 switchport port-security maximum 3
 switchport port-security
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/6
 switchport access vlan 83
 switchport mode access
 switchport port-security maximum 3
 switchport port-security
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Resim 3.18 Switch3 port güvenlik ayarları

3.3.3.3 DHCP Snooping Yöntemi

Bu güvenlik önlemi son kullanıcı cihazlarının DHCP sunucu olarak kullanılmasını ve kötü niyetli kişilerin ağ trafiğini dinlemesini önleyecek yöntemlerden biridir.

Uygulamada kenar anahtarlar üzerinde bu kural aktif duruma getirilerek DHCP sunucusunun bağlı olduğu portlar güvenilir (trust) olarak işaretlenmiştir (Çizelge 3.7).

Çizelge 3.7 DHCP tanımlaması

Kullanılan Komutlar
ip dhcp snooping ip dhcp snooping trust

3.3.3.4 Arp Inspection

Ağ cihazları üzerinden 2 farklı şekilde Arp poisoning saldırısının tespit edilmesi mümkündür (Resim 3.19).

```
Switch3#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)#ip arp inspection vlan 81-84
Switch3(config)#inter
Switch3(config)#interface gigabitethernet 1/0/23
Switch3(config-if)#ip arp inspection trust
Switch3(config-if)#ip dhcp snooping trust
Switch3(config-if)#exit
Switch3(config)#
```

Resim 3.19 Arp yapılandırma örneği - 1

VLAN bazında güvenlik önlemi alınabilir. Arp saldırısına karşı koruma alınmış, trunk port dışındaki tüm portlar güvenilmez olarak işaretlenmiş ve bu portlarda Vlan 81 ile Vlan 84 arası için ilgili güvenlik önlemi aktif duruma getirilmiştir. Diğer bir yöntem ise port bazında güvenlik önlemi almaktır (Resim 3.20).

```
Switch3(config)#errdisable
Switch3(config)#errdisable recovery cause arp-inspection
Switch3(config)#interface gigabitethernet 1/0/21
Switch3(config-if)#ip arp inspection limit rate 25 burst interval 3
Switch3(config-if)#
```

Resim 3.20 Arp yapılandırma örneği - 2

Bu yöntem ile Resim 3.20'de görüldüğü üzere ilgili portta 3 saniye içinde 25'ten fazla ARP mesajı geldiğinde bu ARP mesajlarını saldırı olarak algılayacak ve üzerinden geçen trafiği kesecektir. Daha sonra port anahtarlama görevini yapmaya devam edecektir.

3.3.3.5 Bpdu Guard Özelliği

STP, aktif olduğunda anahtarlar arasından bir tanesi root bridge olarak seçilir ve döngüye neden olabilecek portlar otomatik olarak bloklanır. STP ataklarına karşı önlem alınmadığı durumda yapılabilecek bir atak cihazlar arasında sonsuz döngülerin oluşmasına sebep verebilir.

Yönetilebilir anahtarlar portlarına herhangi bir cihaz takıldığında, takılan cihazın ne olduğunu algılayarak cihaza ait IP, MAC vb. bilgileri alması ve portun aktif duruma gelmesi süresine listening-learning süresi denir. İstendiği durumda bu süre kısaltılarak

bekleme yapılmadan port aktif duruma getirilebilir. Bu yöntem için spanning-tree portfast yöntemi kullanılır. Bu durumda ilgili portta hiçbir işlem yapılmayarak port aktif duruma getirilir. Bu durumda ilgili porta anahtar (switch) takılmasına izin verilmiş olur. Böyle bir durumda mevcut topoloji bozulacak ve ağ saldırılara açık duruma gelecektir. Saldırgan ilk başta ağı dinleyerek root bridge'in "bridge ID" değerini öğrendikten sonra kendisinin ağa bağladığı ağa BPDU çerçevelerini gönderir. Bu işlem sonunda eğer bağlanan anahtar (switch), root (kök) duruma gelirse artık saldırgan ağ trafiğini dinleyebilir.

"BPDU guard" özelliği aktif hale getirilmiş olan portlara/anahtarlara BPDU mesajı gelirse bu port error-disabled duruma gelecektir ve hiçbir şekilde STP'ye dahil olmayacaklar. Bu yöntemle BPDU saldırılarından korunmuş olunacaktır.

Laboratuvar uygulamasında kontrolümüz dışında anahtar (switch) takılmasını önlemek için "BPDU guard" özelliği aktif duruma getirilmiştir. Son kullanıcı cihazlarının takıldığı Switch3 ve Switch4'ün acccess portlarında yapılan tanımlamalar aşağıdaki gibidir (Resim 3.21).

```
Switch3#
Switch3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)#interface range Gigabitethernet1/0/1-20
Switch3(config-if-range)#spanning-tree portfast
Switch3(config-if-range)#spanning-tree bpduguard enable
Switch3(config-if-range)#exit
Switch3(config)#
```

Resim 3.21 BPDU guard yapılandırma örneği

3.3.3.6 Storm Control Yöntemi

Networkun kullanılamaz hale gelmesinde networkun herhangi bir noktasında LAN'da sorunsuz işleyen paket trafiğinin, belli bir zaman diliminde olması gerekenden çok daha fazla sayıda istek gönderilerek cihazın cevap veremez hale gelmesi sağlanır. Normalden çok daha fazla sayıda gelen broadcast, multicast ya da unicast paketler sebebiyle network kullanılamaz duruma gelebilir. Bu paketler sebebi ile oluşabilecek

problemlerin önüne geçebilmek için Storm control yöntemi kullanılır. Bu yöntem her porta uygulanarak kullanılabilir. Anahtarlama cihazlarında 1s. içinde bir portun bant genişliği kapasitesinin istenen bir yüzdeyi geçmesi ya da saniyede belirlenen bir paket sayısını aşması durumunda bu değer üzerindeki trafik bloklanabilir. Yapılan tanımlama örneği Çizelge 3.8'de gösterildiği gibidir.

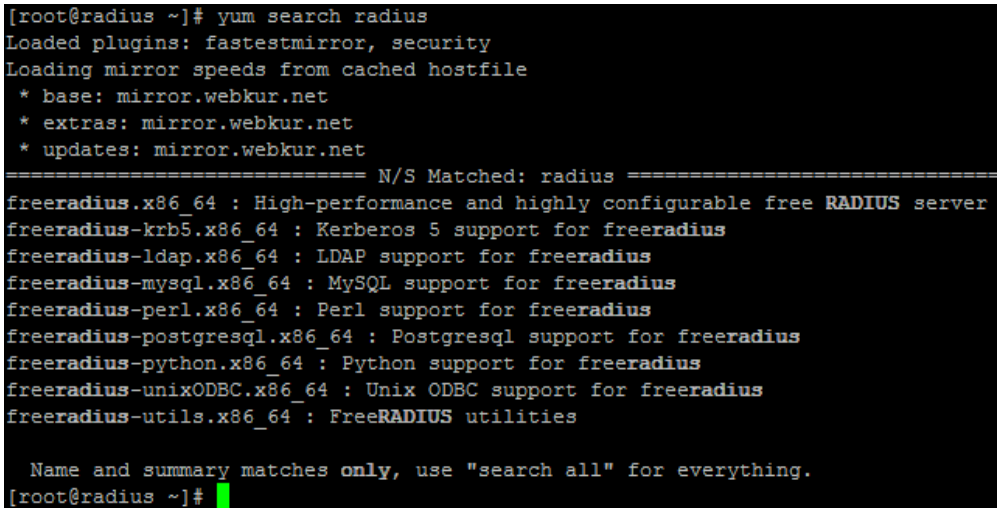
Çizelge 3.8 Storm control tanımlaması

Kullanılan Komutlar
storm-control broadcast level pps 500 storm-control action shutdown

3.3.4 Kimlik Doğrulama Sunucusu Oluşturulması

Günümüzde kullanılan sistemlerin çoğalması ve kullanılan cihazları farklılaşması dolayısı ile kullanıcı kimliğiniz doğrulanması yöntemlerinde de farklılıklar getirmeye başlamıştır. Sistemleri farklı cihazlar ile kullanan kullanıcıların ortak protokol ve yöntemler ile kimlikleri doğrulanabilir. Bu noktada Active Directory, LDAP ve RADIUS ile kimlik doğrulama yöntemleri öne çıkmaktadır.

Çalışmada kullanıcı kimlik denetimi için Freeradius kullanılmıştır. RADIUS sunucu CENTOS 6.5 işletim sistemi üzerine kurulumu yapıldıktan sonra sistem güncellemeleri yapılmış ve gerekli olan Freeradius, Freeradius-ldap ve Freeradius-utils paketleri yüklenmiştir (Resim 3.22).

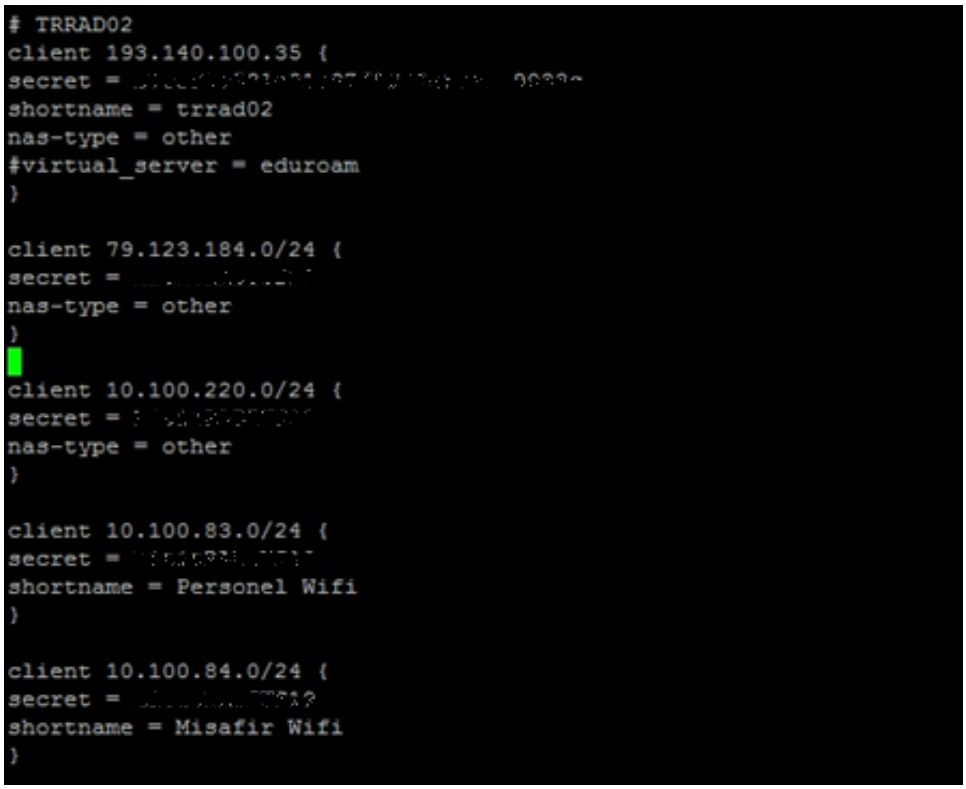


Resim 3.22 Freeradius kurulum paketleri

Gerekli paketlerin kurulum işlemi tamamlandıktan sonra yapılandırma dosyaları üzerinde gerekli ayarların yapılması gerekir. Yapılandırma dosyaları RADIUS sunucuda /etc/raddb klasörü altında yer almaktadır.

3.3.4.1 Clients.conf yapılandırılması

RADIUS sunucuya hangi IP bloklarından gelen isteklerin kabul edileceği client.conf dosyasında yer alır. Yine sunucu üzerine bağlantı şifresi ve sunucu bilgisi de bu dosyada tanımlanmaktadır. Resim 3.23'te görüldüğü üzere kurum içinde bulunan IP blokları ile Ulakbim eduroam sunucularına ait IP tanımları bu dosya içerisinde tanımlanmıştır.



Resim 3.23 Client ayarları

3.3.4.2 Doğrulama metodlarının tanımlanması

RADIUS sunucuda yetkilendirme ve kimlik doğrulama için gerekli tanımlamalar yapılması gerekir. Sunucu üzerinde bu ayarlar /etc/raddb/sites-enabled klasörü içerisinde default dosyasında yer almaktadır. RADIUS sunucuda doğrulama metodları Resim 3.24'te görüldüğü gibi yapılmıştır. Yapılandırma işlemine göre gelen kullanıcı bilgisi eğer "öğrenci.hitit.edu.tr" domainine aitse öğrenci kimlik doğrulama yöntemi yapılacak, kullanıcı öğrenci bilgisine sahip değilse personel doğrulama yöntemi yapılacaktır.

```
authorize {

        if (User-Name =~ /ogrenci.hitit.edu.tr/) {

           ldapogrenci
}
        else {
               ldapad

}

authenticate {
         if (User-Name =~ /ogrenci.hitit.edu.tr/) {

             ldapogrenci
}
        else {
                ldapad
}
```

Resim 3.24 Doğrulama metodları

3.3.4.3 Eap.conf yapılandırması

Bağlantı aşamasında kullanılacak şifreleme sistemi ve kullanılan parametrelere ait bilgiler ise eap.conf dosyasında yer alır (Resim 3.25).

```
#  EAP types NOT listed here may be supported via the "eap2" module.
#  See experimental.conf for documentation.
#
       eap {
               #  Invoke the default supported EAP type when
               #  EAP-Identity response is received.
               #
               #  The incoming EAP messages DO NOT specify which EAP
               #  type they will be using, so it MUST be set here.
               #
               #  For now, only one default EAP type may be used at a time.
               #
               #  If the EAP-Type attribute is set by another module,
               #  then that EAP type takes precedence over the
               #  default type configured here.
               #
               default_eap_type = ttls

               #  A list is maintained to correlate EAP-Response
               #  packets with EAP-Request packets.  After a
               #  configurable length of time, entries in the list
               #  expire, and are deleted.
               #
               timer_expire     = 60
               auth_type = PAP
               certificate_file = ${certdir}/server.pem
```

Resim 3.25 Eap yapılandırması

3.3.4.4 LDAP yapılandırması

RADIUS sistemi birden fazla LDAP veya Active Directory ile bağlantı kurabilmektedir. Bu bilgilerin tanımlanacağı yapılandırma dosyası ldap.conf dosyasıdır. Çalışmada iki farklı LDAP parametresi kullanılarak Akademik ve Öğrenci Active Directory sistemleri ile bağlantı sağlanmıştır. Bağlantı bilgileri Resim 3.26'da görülmektedir.

```
ldap ldapad {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = "  .30"
        identity = "                ,DC=hitit,DC=edu,DC=tr"
        password = .
        basedn = "OU=IA_Akademik,DC=hitit,DC=edu,DC=tr"
        filter = "(mail=%{%{Stripped-User-Name}:-%{User-Name}})"
        #base_filter = "(objectclass=radiusprofile)"

}

ldap ldapogrenci {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.

        server = "  .144"
        identity = "CN=                 ,DC=ogrenci,DC=hitit,DC=edu,DC=tr"
        password = .
        basedn = "OU=OGRENCI,DC=ogrenci,DC=hitit,DC=edu,DC=tr"
        filter = "(mail=%{%{Stripped-User-Name}:-%{User-Name}})"
        base_filter = "(objectclass=radiusprofile)"


        #  How many connections to keep open to the LDAP server.
        #  This saves time over opening a new LDAP socket for
        #  every authentication request.
        ldap_connections_number = 5
```

Resim 3.26 LDAP yapılandırması

3.3.5 Ağ Cihazları Yerleşimi

Ağ cihazlarının yerleşiminde dikkat edilmesi gereken noktalar bulunmaktadır. Kullanılan kablonun kaliteli olması ve belirli standartlara uyması önem arz etmektedir. Özellikle uzun mesafelerde çekilen kablonun kalitesiz olması veri iletiminde kesilmelere sebep olabilmektedir. Her kablonun taşıyabileceği belli bir kapasite ve veri iletim mesafesi bulunmaktadır. UTP kabloda da bu mesafe 100 m. sınırındadır. Kullanılan internet kablosu bu sınır üzerinde ise yine veri kayıplarının yaşanması

muhtemeldir. Bu sebeple ağ cihazları konumlandırılırken bu mesafeye dikkat edilmesi gerekir.

Anahtar (switch), yönlendirici (router) gibi ağ cihazları konumlandırılırken dikkat edilecek diğer bir konu ise kablolamanın cihazlar arasında nasıl yapılması gerektiğidir. Bu noktada ağda herhangi bir problem olduğunda ağ üzerindeki cihazların ve kullanıcıların bu problemden en az derecede etkilenmesi için bir ağaç ve ağaca bağlı dallar şeklinde yapıyı oluşturmak gerekir. Eğer her anahtar (switch) ana omurgaya bağlı olursa olası bir problem durumunda kullanıcılar ve ağ üzerindeki diğer cihazlar bu problemden en az şekilde etkilenecektir.

3.3.5.1 Kablolu Ağ Cihazları Yerleşimi

İyi bir ağ altyapısında ağ cihazlarının konumları önemlidir. Bir merkezin ya da birden fazla merkezin toplama noktası olarak belirlenmesi gerekir. Bu noktaların belirlenmesinde maliyet, ölçeklenebilirlik ve arıza tespit kolaylığı dikkate alınmalı, cihaz adedi ve uygun cihaz konumları tespit edilmelidir.

UTP kablolar pratikte 100 metre ve daha yukarısında veri taşıyabilse de kullanılan kablo çok kaliteli değilse veri kayıpları yaşanabilmektedir. Bu sebeple data kabloların 100 metre üzerinde olmamasına dikkat edilmelidir.

3.3.5.2 Kablosuz Ağ Cihazı Yerleşimi

Kablosuz ağ cihazlarının çekim alanları kapalı ve açık alanlarda farklılık göstermektedir. İç ortam kablosuz ağ cihazlarının birçoğu 50 metreden daha uzak bir mesafeden bağlantı şansı sunmaz. Dış ortam cihazlarda ise 100-150 metreye kadar kapsama alanı genişleyebilmektedir. Öte yandan sıvalı ve pürüzlü duvarlar, kablosuz olarak gönderilen sinyali, alçıpan duvarlara göre daha çok bloke ederler. Cam, ytong ve alçıpan kullanılan bir yapıda sinyal rahat bir şekilde duvarlardan geçerken tuğla ve çelik kullanılan bir yapıda sinyal rahatlıkla geçemeyecek ve sinyal seviyesi düşecektir. Kablosuz ağ cihazları genellikle Wi-Fi sinyalini her yöne otomatik olarak

dağıtmaktadır. Yeni nesil kablosuz ağ cihazlarında ise kullanıcı yoğunluğuna bağlı olarak sinyal bir tarafa yönlenmekte ve sinyal seviyesini yoğunluk durumuna göre artırarak azaltabilmektedir. Bir antenin sinyal gönderme ve alma (dBi) değeri -75 dBi altında ise sinyal kaybolur. Anten kazancı (dBi) değeri arttıkça kapsama alanı da genişler.

4. BULGULAR

Yedekli bir ağ mimarisi kurulması amacı ile laboratuvar ortamında ağ cihazları konumlandırılmış, bu cihazlar üzerinde alınan güvenlik tedbirleri ile laboratuvar ortamında ağ güvenlik testleri yapılmıştır. Kurulan yedekli yapının ve güvenlik önlemlerinin uygulanabilirliği incelenmiştir. Yedekli sağlıklı bir yapı kurulması ile güvenlik ve performans bakımından sağlıklı bir ağ yapısı ortaya koyulmaya çalışılmıştır.

4.1 Laboratuvar Bulguları

İlk önce laboratuvar içerisinde anahtarlar (switch) ve AP'ler konumlandırılmıştır. Ana katman anahtarı olarak üniversitede kullanılan mevcut omurga anahtar kullanılmıştır. Mevcut üniversite ağını etkilememek için omurga anahtar ile dağıtım anahtarları arasına bakır kablolama yapılmıştır. Anahtarlar (switch) arası kablolama işlemi için CAT6 yama kabloları (patch cord) kullanılmıştır. Sonrasında cihazların konfigürasyonları yapılmıştır. Nihayetinde ise laboratuvar ortamında oluşturulan ağ üzerinde güvenlik testleri yapılmıştır. Yapılan testler sonucunda elde edilen bulgular ağadaki gibidir.

4.1.1 Senaryo 1 (Ağ güvenliğinin test edilmesi)

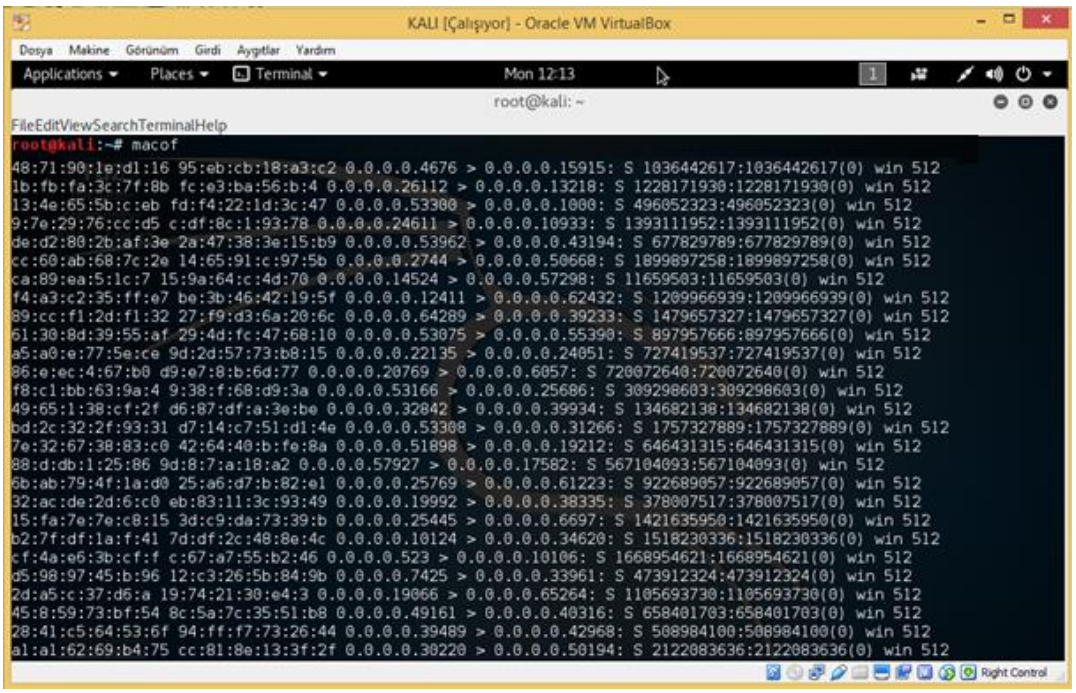
Porta birden fazla cihaz bağlanarak port güvenlik kuralı ihlal edilmesi durumu laboratuvar ortamında test edilmiştir. Port security kuralları aktif olan portlarda testler yapılmıştır. Port üzerine birden fazla cihaz bağlandığında port güvenlik kuralı sebebi ile portun engellendiği ve yapılan testin başarılı olduğu görülmüştür (Resim 4.1).

```
Switch4#show int status err-disabled

Port      Name               Status       Reason              Err-disabled Vlan
s
Gi1/0/3                      err-disabled psecure-violation
```

Resim 4.1 Port security güvenlik uygulaması

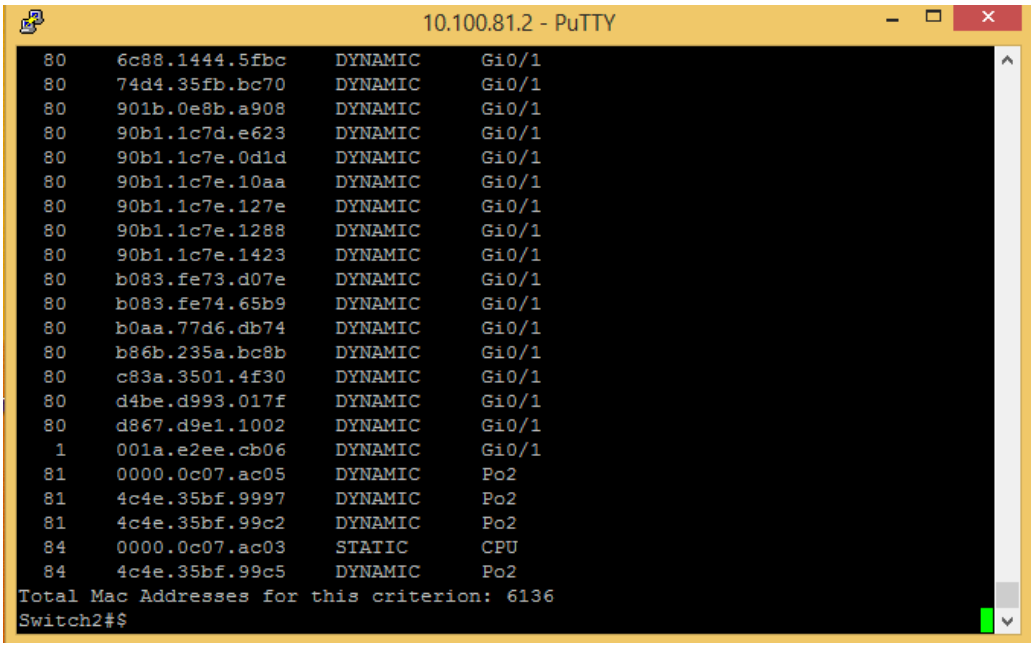
4.1.2 Senaryo 2 (MAC tablosunun doldurulmaya çalışılmasının test edilmesi)

Gerekli güvenlik kuralları uygulandıktan sonra MAC adresleri taklit edilerek Resim 4.2'de görüldüğü şekilde Kali Linux 2016.1 sürümü içerisinde yer alan macof programı ile anahtarın (switch) MAC adres tablosu doldurulmaya çalışılmıştır (İnt.Kyn.37). Doldurulan MAC tablosu Resim 4.3'te görülmektedir.



Resim 4.2 MAC flooding uygulaması

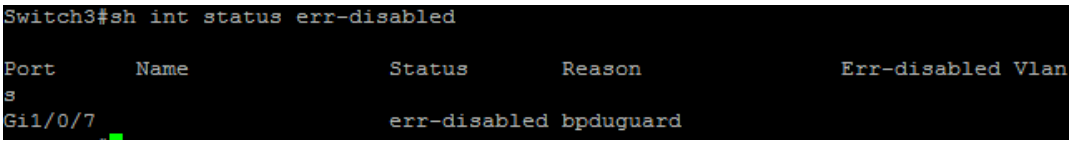
Port güvenliği yapılmayan arayüzlerdeki bu açık ile anahtarın MAC adres tablosu doldurularak switch işlevsiz duruma getirilmiştir. Port güvenliğinin sağlandığı durumda ise MAC tablosu doldurulamamış ve switch normal fonksiyonlarını yapmaya devam etmiştir.



Resim 4.3 MAC tablosu ekran görüntüsü

4.1.3 Senaryo 3 (Port çoklamayı engelleme işleminin test edilmesi)

Kenar anahtarlardan birine ağa daha önce dahil olmayan ve habersiz olarak takıldığı varsayılan bir anahtar (switch) takılması ile port çoklama işlemi test edilmiştir. Port üzerine takılan anahtar üzerinden trafiğin geçmesine izin verilmeyerek portun bloklandığı görülmüştür. BPDU guard özelliği sayesinde ağ yöneticisinin istemediği kontrol dışı internet çoklama işlemi başarısız olmuştur (Resim 4.4).

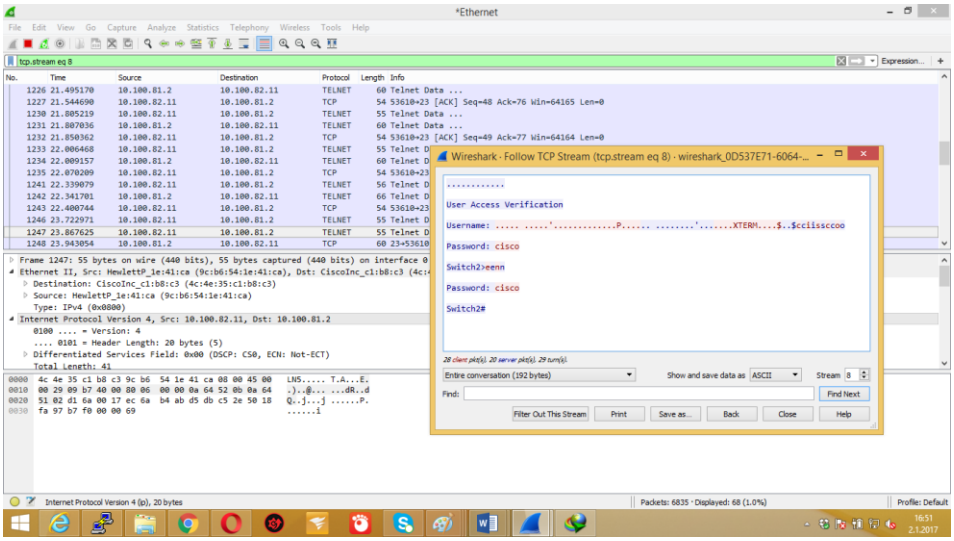


Resim 4.4 BPDU guard testi

4.1.4 Senaryo 4 (Trafik analizinin yapılması)

Ağ üzerindeki paketlerin analiz edilmesi ve kullanılan protokollerin tespit edilmesi amacı ile Wireshark programının 2.2.3 sürümü kullanılarak ağ trafiği incelenmiştir. (İnt.Kyn.38). Ağ üzerinde iletilen paketler yakalanarak paketlerin içerikleri analiz edilmiştir. Şifrelenmeden iletilen paketlerde kullanıcı bilgisine erişilmiştir. Telnet

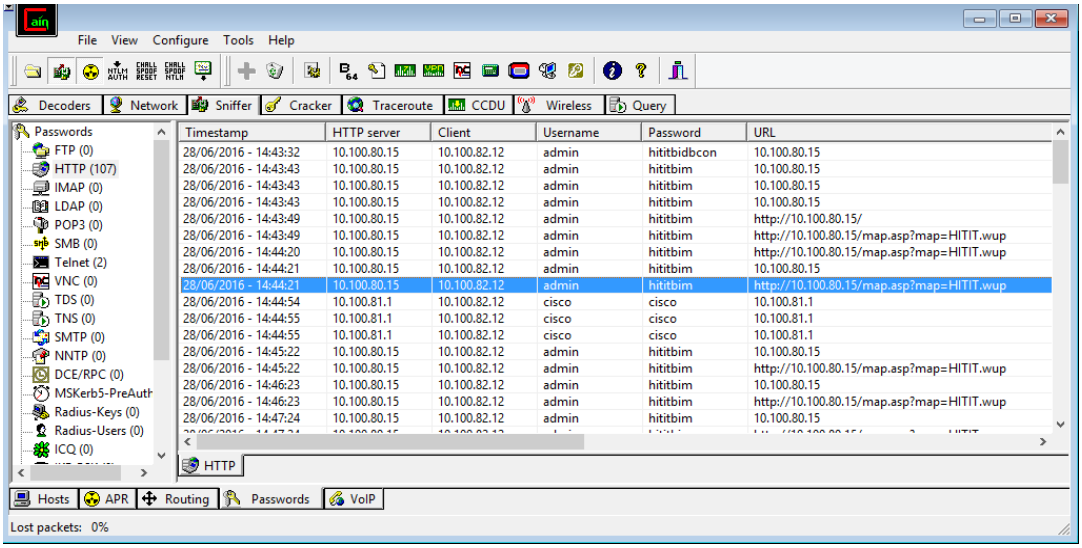
protokolünde Resim 4.5'te görüldüğü gibi kullanıcı adı ve şifre bilgisinin açık bir şekilde iletildiği görülmektedir.



Resim 4.5 Paket analizi

4.1.5 Senaryo 5 (Arp poisoning saldırısı önlenebilirlik testi)

Hub kullanılan ya da anahtarlayıcı port güvenliği alınmayan bir ağda bilgisayarın gönderdiği paketlerin anahtarlayıcı yerine saldırgan bilgisayara gönderilir. Çalışmada Cain&Abel programının 4.9.56 sürümü kullanılarak arp poisoning saldırısı yapılmış ve Resim 4.6'da görüldüğü gibi kullanıcı bilgileri ele geçirilmiştir (İnt.Kyn.39).



Resim 4.6 Arp poisoning ile ağ dinleme

Dinamik arp tespit kuralları uygulanan anahtar üzerinde tekrar aynı saldırı yapıldığında anahtara ulaşan paketlerinin geçersiz olduğu ve bu paketlerin engellendiği Resim 4.7'de görülmektedir.

```
Switch3#
.Jun 29 13:30:10.589: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/
0/4, vlan 82.([9cb6.541e.41ca/10.100.82.11/0000.0000.0000/10.100.82.3/13:30:09 U
TC Wed Jun 29 2016])
.Jun 29 13:30:11.595: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/
0/4, vlan 82.([9cb6.541e.41ca/10.100.82.11/0000.0000.0000/10.100.82.3/13:30:10 U
TC Wed Jun 29 2016])
.Jun 29 13:30:12.602: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/
0/4, vlan 82.([9cb6.541e.41ca/10.100.82.11/0000.0000.0000/10.100.82.3/13:30:12 U
TC Wed Jun 29 2016])
.Jun 29 13:30:13.609: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/
0/4, vlan 82.([9cb6.541e.41ca/10.100.82.11/0000.0000.0000/10.100.82.3/13:30:12 U
TC Wed Jun 29 2016])
.Jun 29 13:30:14.615: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/
0/4, vlan 82.([9cb6.541e.41ca/10.100.82.11/0000.0000.0000/10.100.82.3/13:30:13 U
TC Wed Jun 29 2016])
```

Resim 4.7 Arp poisoning testi

Engellenen arp paketlerine ait istatistiki bilgilere de ulaşılabilir. Resim 4.8'de görüldüğü gibi 245 arp paketi engellenmiştir.

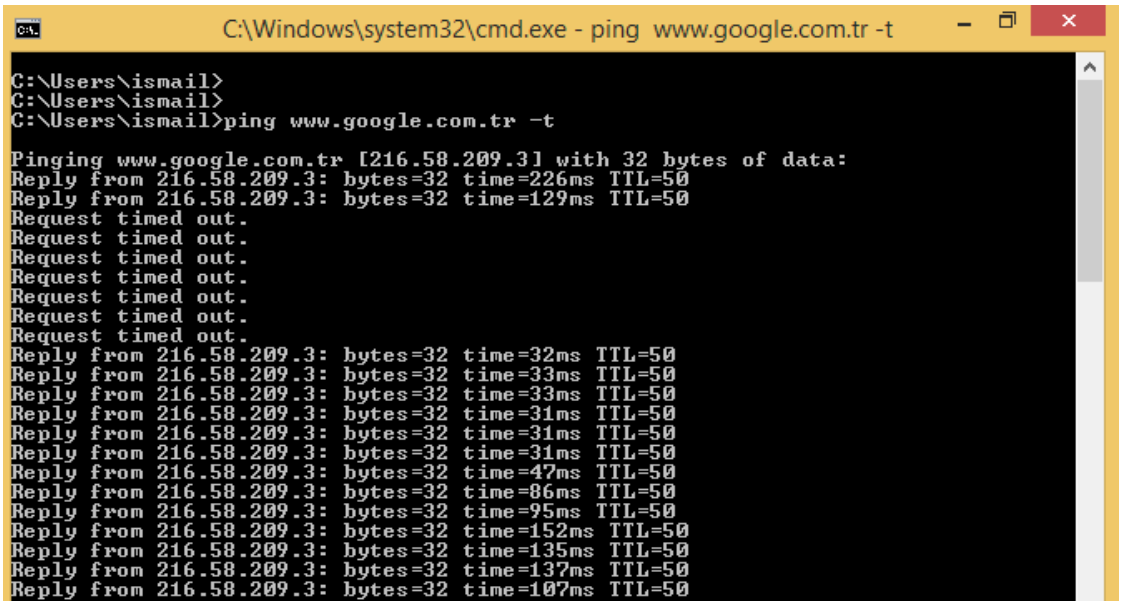
```
Switch3# show ip arp inspection statistics

 Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
 ----      ---------        -------     ----------      ---------
   83              6            245            245              0

 Vlan   DHCP Permits    ACL Permits  Probe Permits   Source MAC Failures
 ----   ------------    -----------  -------------   -------------------
   83              0              0              0                     0

 Vlan   Dest MAC Failures   IP Validation Failures   Invalid Protocol Data
 ----   -----------------   ----------------------   ---------------------
   83                    0                        0                      0
Switch3#
```

Resim 4.8 ARP istatistikleri

4.1.6 Senaryo 6 (Yedekli yapının kararlı çalışmasının test edilmesi)

Laboratuvar ortamında kurulan yedekli yapıda son kullanıcı bilgisayarından www.google.com.tr sitesine ping atılmış ve paket kayıpları incelenmiştir. Anahtarlardan (switch) bir tanesinin arızalanmış olduğu varsayılmış, bu anahtar devreden çıkarılarak ping kaketleri incelenmeye devam etmiştir. Resim 4.9'da görüldüğü ping paketlerinde 5-7 arasında kayıp oluştuğu, sonrasında ise paket kaybı

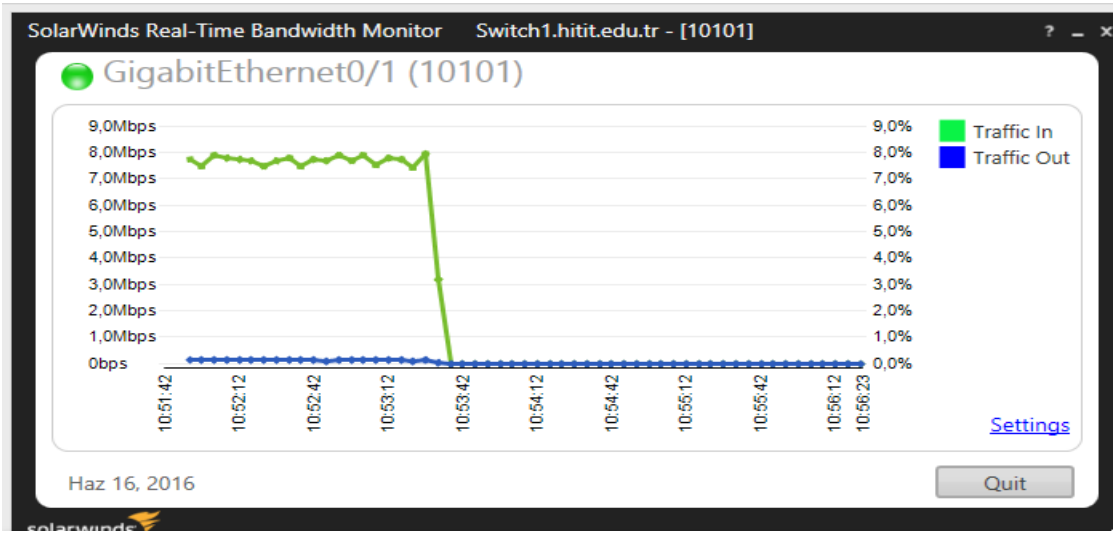
oluşmayarak ikinci yedek anahtar üzerinden internet trafiğinin akmaya devam ettiği görülmüştür.



Resim 4.9 Ping durumu

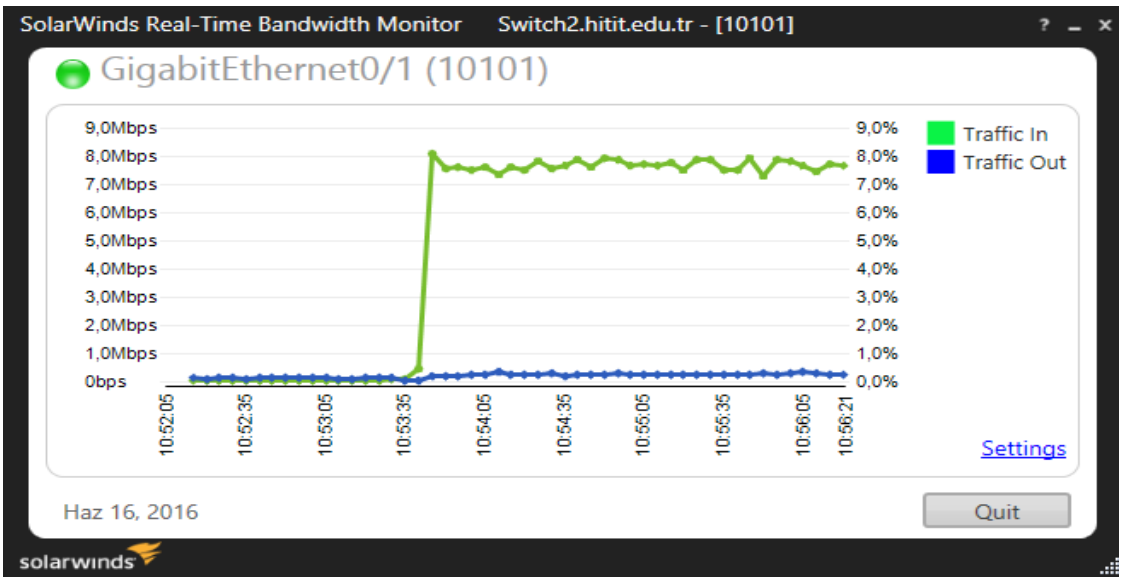
Ağ içerisinde hangi trafiklerin oluştuğu ve trafik yoğunluğunun izlenebilmesi için ağ istatistiklerine ihtiyaç duyulmaktadır. Bu amaçla oluşturulan ağın analizi yapılarak hangi anahtar (switch) üzerinden ne kadar trafiğin geçtiği de incelenmiştir. Uygulama üzerinde internet trafiklerinin anlık olarak oluşturulması için Solarwinds Real Time Bandwith Monitor programı kullanılmıştır (İnt.Kyn.40).

Laboratuvar ortamında oluşturulan yedekli mimaride yapıda dağıtım anahtarları (distribution switch) üzerinden geçen aynı zaman dilimine ait trafikler izlenmiştir. Şekil 4.1'de görüldüğü aktif durumda Switch1 isimli anahtarın (switch) kullanıldığı ve Gigabitethernet 0/1 arayüzünden 8 Mbps trafiğin geçtiği gözlemlenmiştir.



Şekil 4.1 İnternet trafiği - 1

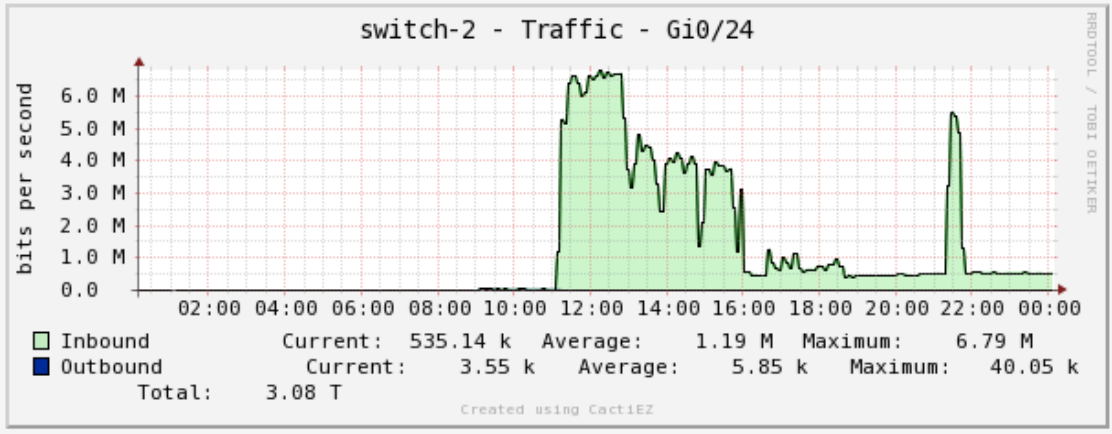
Uygulama test esnasında Switch1 kapatılarak cihazlar üzerinden geçen trafik Şekil 4.2'de görüldüğü gibi analiz edilmeye devam etmiştir. Switch1 üzerinden akan trafiğin durduğu ve 8 Mbps internet trafiğinin Switch2 üzerindeki Gigabitethernet 0/1 arayüzünden akmaya devam ettiği görülmüştür.



Şekil 4.2 İnternet trafiği - 2

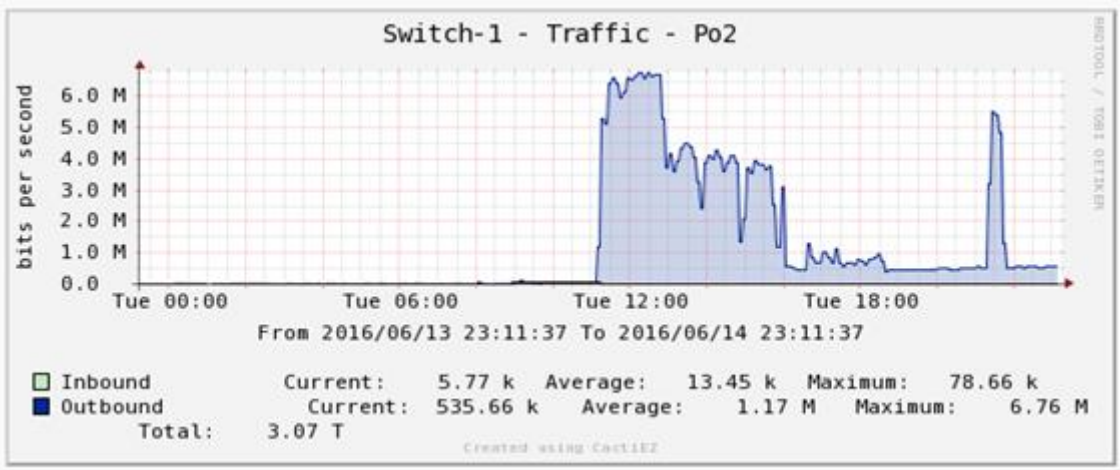
4.1.7 Senaryo 7 (Arayüz kullanım miktarlarının analiz edilebilirliğinin test edilmesi)

Başka bir analiz programı olan Cactiez programının 0.7 versiyonu ile internet trafiği analizi yapılmıştır (İnt.Kyn.41). Switch2'nin Gigabitethernet 0/24 arayüzü üzerinden 6 Mbps trafik geçtiği Şekil 4.3'te görülmektedir.



Şekil 4.3 İnternet kullanım oranları - 1

Dağıtım anahtarları üzerindeki portlar incelendiğinde Gi 0/24 trunk portunda upload yönünde trafik oluştuğu görülmüştür. Etherchannel yapılandırılması sonucu Şekil 4.4'te görüldüğü gibi birleştirilen portlardan trafiğin geçtiği ve 6 Mbps internet trafiğinin oluştuğu görülmektedir.



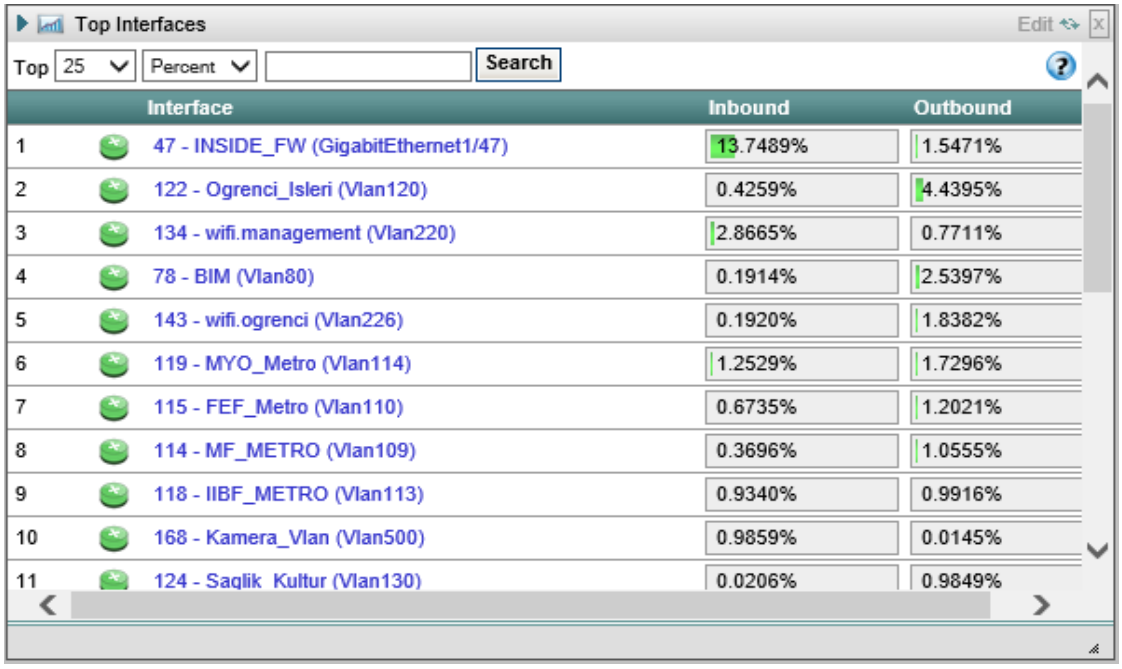
Şekil 4.4 İnternet kullanım oranları - 2

4.1.8 Senaryo 8 (Ağ trafiğinin tamamıyla izlenebilirliğinin mümkün olup olmadığının araştırılması)

Kurumsal ağ trafiğinin analiz edilerek bu ağ içinde olup bitenleri incelenmesi gerekmektedir. Bu sayede ağ içindeki problemlere ve olası problemlere daha kolay müdahale edilebilir. Normalin dışında iç ağda oluşabilecek yüksek trafik miktarı iç ağda yayılan bir virüs ya da kötü niyetli olarak yapılan bir saldırının habercisi olabilir. Netflow ile ağ trafiği hakkında detaylı bilgi elde edilir. Netflow ile ağ trafiği izlenerek ağ hakkında detaylı bilgiler elde edilebilir. QoS'nin (Quality of Service) hangi noktada uygulanacağı ve DoS (Denial of Service) ataklarının tespit edilmesinde Netflow kullanılmaktadır.

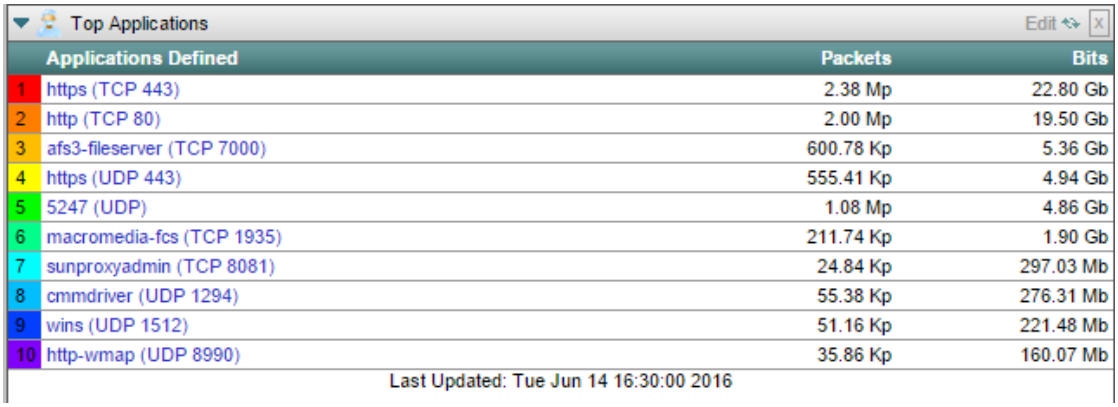
Kampüs ağı içindeki ağ trafiğinin izlenebilmesi için Scrutinizer 9.0.1.19989 versiyonunun 30 günlük kısıtlı sürümü kullanılmıştır (İnt.Kyn.42). Scrutinizer netflow analiz programı ile tüm trafik izlenerek kullanılan protokoller ve kullanıcıların anlık yapmış olduğu iç ve dış trafik bilgilerine ulaşılmaya çalışılmıştır. Omurga anahtar (backbone switch) üzerinden geçen trafik analiz edildiğinde elde edilen bulgular Resim 4.10 ve Resim 4.11'de görüldüğü gibidir.

Omurga üzerinde tanımlı olan ağların anlık olarak ne kadar trafik yarattığı Resim 4.10'da görülmektedir. Trafik anlık olarak incelendiğinde en fazla trafiği Öğrenci İşleri biriminin yarattığı, içeriden dışarıya doğru tüm trafiğin %4'ünü bu trafiğin oluşturduğu görülmektedir.



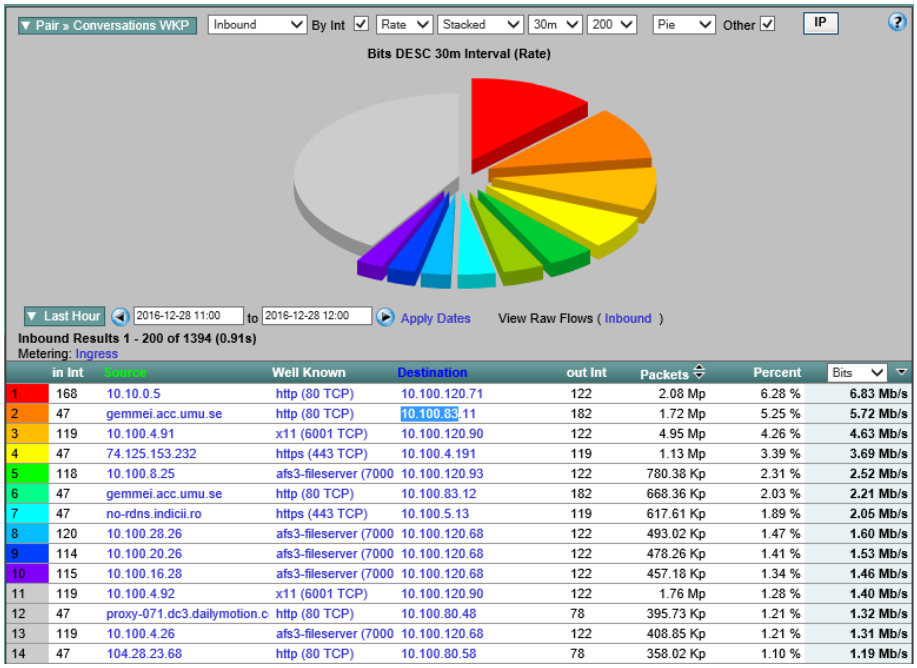
Resim 4.10 Netflow analizi - 1

Netflow analizi ile protokoller ve kullanım oranları Resim 4.11'de görülmektedir. En fazla HTTPS ve HTTP protokollerinin kullanıldığı tespit edilmiştir. HTTPS protokolünde 22.80 Gb, HTTP protokolünde ise 19.50 Gb veri kullanıldığı görülmektedir.



Resim 4.11 Netflow analizi - 2

Netflow sonucunda iç ve dış ağ ile yapılan veri trafik miktarları Resim 4.12'de görülmektedir. Anlık olarak yapılan trafiğe bakıldığında; 10.100.120.68 IP adresinin farklı IP adresleri ile iletişimde olduğu ve TCP 7000 portu üzerinden kamera görüntüsü aktarıldığı, 10.10.0.5 IP adresi 10.100.120.71 IP adresleri arasında 6.83 Mbit'lik trafik oluştuğu görülmektedir. 10.100.83.11 IP adresinin Debian internet sitesi ile TCP 80 portundan iletişim sağladığı, 10.100.80.48 IP adresinin ise video trafiği yarattığı görülmektedir.



	in Int	Source	Well Known	Destination	out Int	Packets	Percent	Bits
1	168	10.10.0.5	http (80 TCP)	10.100.120.71	122	2.08 Mp	6.28 %	6.83 Mb/s
2	47	gemmei.acc.umu.se	http (80 TCP)	10.100.83.11	182	1.72 Mp	5.25 %	5.72 Mb/s
3	119	10.100.4.91	x11 (6001 TCP)	10.100.120.90	122	4.95 Mp	4.26 %	4.63 Mb/s
4	47	74.125.153.232	https (443 TCP)	10.100.4.191	119	1.13 Mp	3.39 %	3.69 Mb/s
5	118	10.100.8.25	afs3-fileserver (7000	10.100.120.93	122	780.38 Kp	2.31 %	2.52 Mb/s
6	47	gemmei.acc.umu.se	http (80 TCP)	10.100.83.12	182	668.36 Kp	2.03 %	2.21 Mb/s
7	47	no-rdns.indicii.ro	https (443 TCP)	10.100.5.13	119	617.61 Kp	1.89 %	2.05 Mb/s
8	120	10.100.28.26	afs3-fileserver (7000	10.100.120.68	122	493.02 Kp	1.47 %	1.60 Mb/s
9	114	10.100.20.26	afs3-fileserver (7000	10.100.120.68	122	478.26 Kp	1.41 %	1.53 Mb/s
10	115	10.100.16.28	afs3-fileserver (7000	10.100.120.68	122	457.18 Kp	1.34 %	1.46 Mb/s
11	119	10.100.4.92	x11 (6001 TCP)	10.100.120.90	122	1.76 Mp	1.28 %	1.40 Mb/s
12	47	proxy-071.dc3.dailymotion.c	http (80 TCP)	10.100.80.48	78	395.73 Kp	1.21 %	1.32 Mb/s
13	119	10.100.4.26	afs3-fileserver (7000	10.100.120.68	122	408.85 Kp	1.21 %	1.31 Mb/s
14	47	104.28.23.68	http (80 TCP)	10.100.80.58	78	358.02 Kp	1.10 %	1.19 Mb/s

Resim 4.12 Netflow analizi - 3

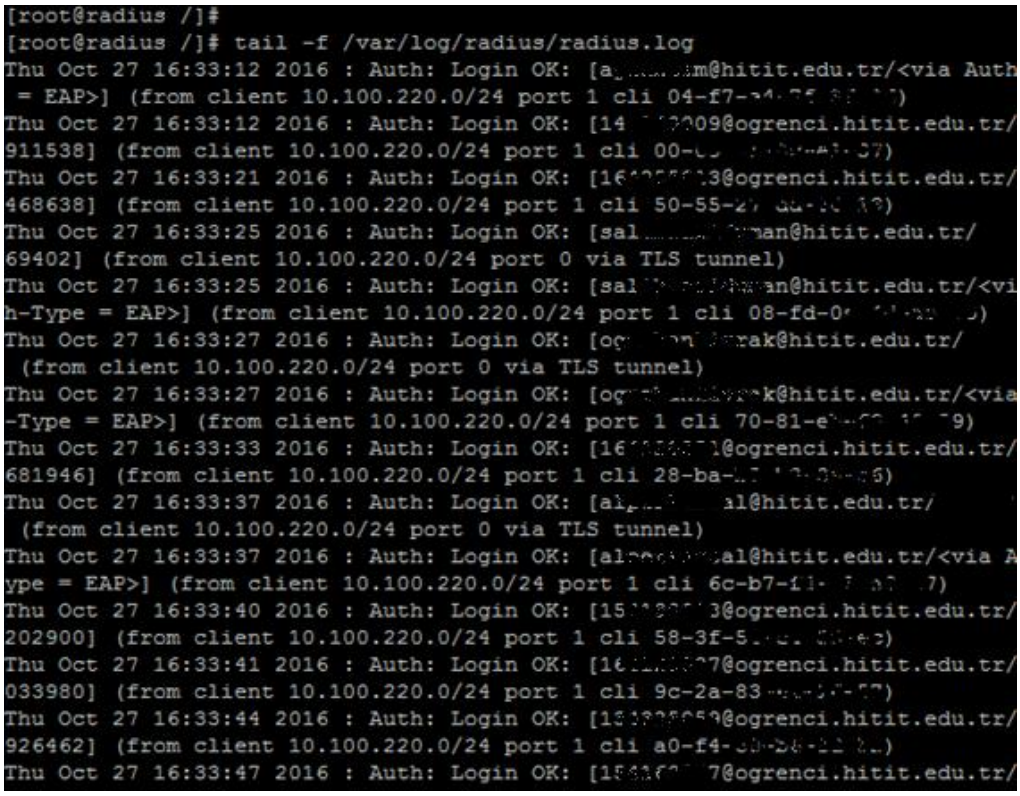
Güvenlik duvarı internet trafik kayıtları gerektiğinde kullanılmak üzere tutulmaktadır. Güvenlik duvarı üzerinden geçen trafik kayıtları Resim 4.13'te görülmektedir.

#	Date/Time	Source IP	Destination IP	Service	Sent/Received	Application
1	12:50:00	10.100.83.12	37.59.195.0	HTTP	1 KB / 1 KB	HTTP
2	12:50:00	10.100.83.12	172.217.17.193	HTTP	176 B / 132 B	HTTP
3	12:50:02	10.100.83.12	104.96.135.139	HTTP	0 / 0	HTTP
4	12:50:03	10.100.83.11	79.123.184.14	santral-port	132 B / 244 B	santral-port
5	12:50:03	10.100.83.12	178.250.0.100	HTTP	3 KB / 3 KB	HTTP
6	12:50:03	10.100.83.12	199.96.57.6	HTTP	164 B / 132 B	HTTP
7	12:50:06	10.100.83.12	199.96.57.6	HTTPS	982 B / 491 B	Twitter
8	12:50:08	10.100.83.12	93.184.220.113	HTTP	164 B / 128 B	HTTP
9	12:50:10	10.100.83.12	79.123.184.14	santral-port	132 B / 284 B	santral-port
10	12:50:12	10.100.83.11	172.217.17.174	443/udp	17 KB / 5 KB	443/udp
11	12:50:13	10.100.83.12	104.96.135.139	HTTP	164 B / 128 B	HTTP
12	12:50:13	10.100.83.11	79.123.184.14	santral-port	132 B / 284 B	santral-port
13	12:51:04	10.100.82.13	172.217.17.194	HTTP	3 KB / 3 KB	HTTP
14	12:51:05	10.100.82.13	193.140.13.72	HTTP	1 KB / 2 KB	HTTP
15	12:50:00	10.25.57.252	216.58.212.40	HTTPS	1 KB / 4 KB	Google.Analytics
16	12:50:00	10.25.21.58	79.123.184.31	DNS	72 B / 126 B	DNS
17	12:50:00	180.107.126.63	79.123.185.40	23231/tcp	0 / 0	23231/tcp
18	12:50:00	79.123.184.153	10.100.4.36	SNMP	478 B / 1 KB	SNMP

Resim 4.13 Güvenlik duvarı trafik kayıtları ekran görüntüsü

4.1.9 Senaryo 9 (Kimlik denetimi yapılabilirliğinin test edilmesi)

Kimlik denetimi sayesinde hangi kullanıcıların hangi tarih ve saatte istekte bulunduğu, hangilerinin oturum açabildiği ve bir kullanıcının hangi MAC adresine sahip cihaz ile erişim yaptığı rahatlıkla tespit edilebilmektedir. RADIUS sunucu üzerindeki erişim logları incelendiğinde kimlik doğrulama metodu sayesinde kullanıcıların internet erişimlerinin sağlandığı Resim 4.14'te görülmektedir. Kişisel hakların korunması açısından şahsi bilgiler gizleniştir.



Resim 4.14 RADIUS erişim logları

4.2 Kampüs Bulguları

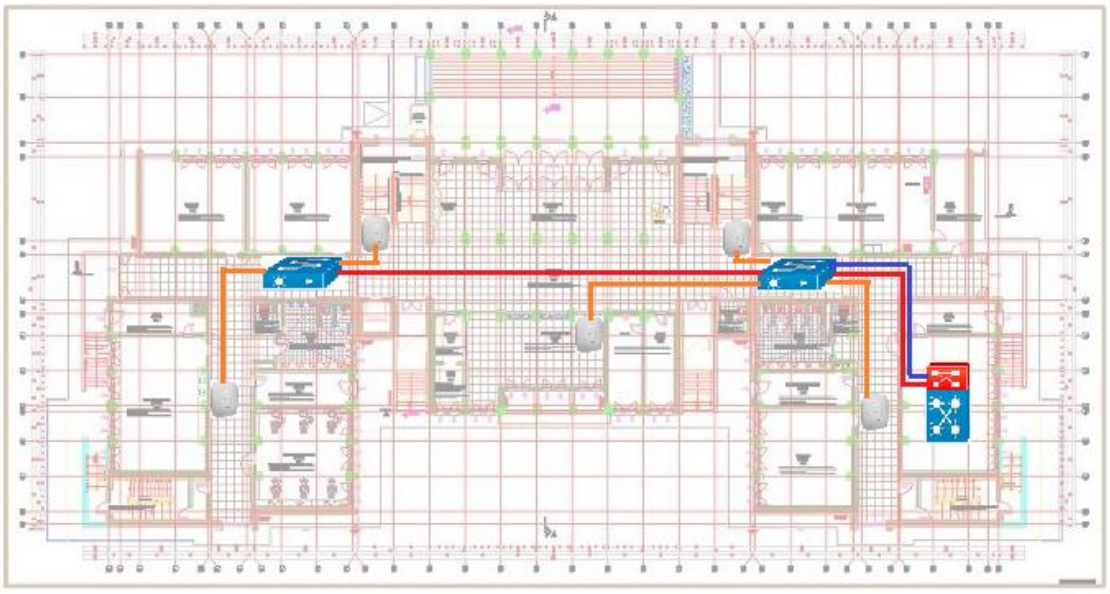
Hitit Üniversitesi Kuzey Kampüs yerleşkesi içerisinde bulunan Rektörlük ve Mühendislik Fakültesi binalarında yapılan incelemeler sonucunda kablolu ve kablosuz ağ yapısı ile ilgili yapılan tespitler aşağıdaki gibidir.

4.2.1 Cihaz Yerleşimi

Hitit Üniversitesi Rektörlük binası 11.555 m^2 kapalı alana sahiptir. Betonarme yapıya sahip olup yapı malzemesi olarak tuğla kullanılmıştır. Ağ cihazları planlaması yapılırken kullanıcı yoğunluklarına ve çekilen kabloların uzunluklarına dikkat edilmiştir.

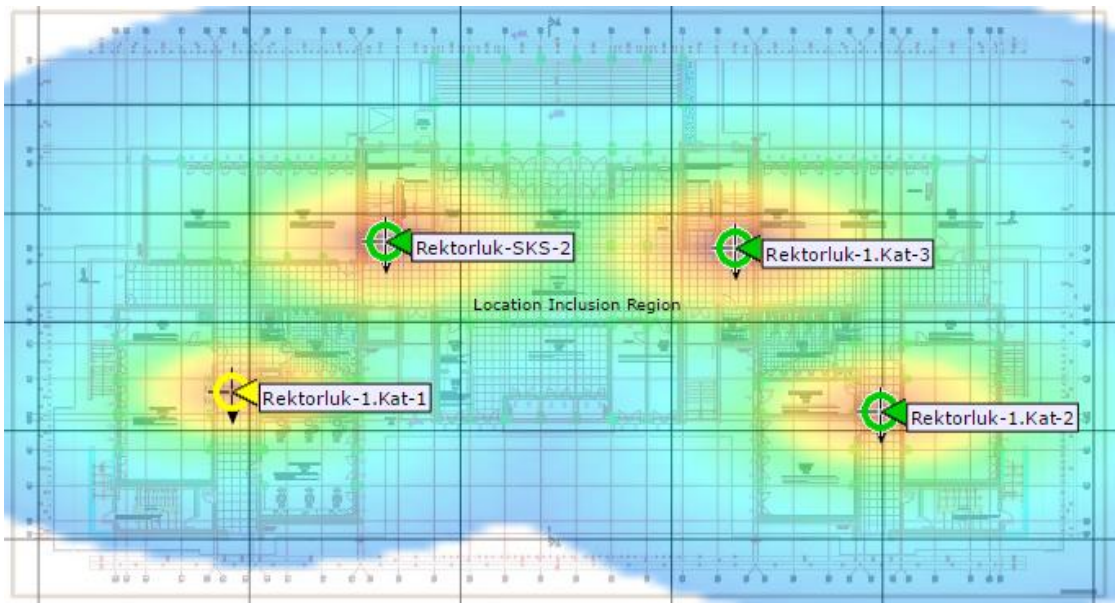
Rektörlük binası içerisinde kablolu ağ için çekilen en uzun kablo 90 metre uzunluğundadır. Katlara konumlandırılan anahtarlar (switch) yönetilebilir L2 anahtarlar (switch) olup multi mode fiber optik kablo kullanılarak direk olarak merkez omurgaya bağlanmıştır. AP'ler kendisine en yakın anahtara (switch) bağlanarak elektrik gücünü kendisine bağlanan enjektör vasıtası ile almaktadır. Katlarda bulunan anahtarlar (switch) binayı besleyen güç kaynağına ve jeneratör cihazına bağlı durumdadır. Cihaz yerleşimi doğru olup cihazlar arası kablolama metrajı normaldir.

Rektörlük binası betonarme yapıya sahip olup yapı malzemesi olarak tuğla kullanılmıştır. Bina içinde iç ortam 802.11 a/b/g/n desteğine sahip kablosuz ağ cihazları konumlandırılarak kablosuz ağ ölçümleri yapılmış, kablosuz ağ cihazlarının ortalama 25 metre çekim alanına sahip olduğu tespit edilmiştir. Rektörlük binasında Wi-Fi çekim alanı ile ilgili testler yapılmıştır. Yapılan ölçümlerde, zemin katta köşelerde bulunan dip odalarda sinyal gücünün -75 dBi seviyesi altına düştüğü, bu sebeple bu odalarda kablosuz Wi-Fi sinyalinin çok az çektiği ve bağlanma ve kopma sorunları yaşandığı tespit edilmiştir.



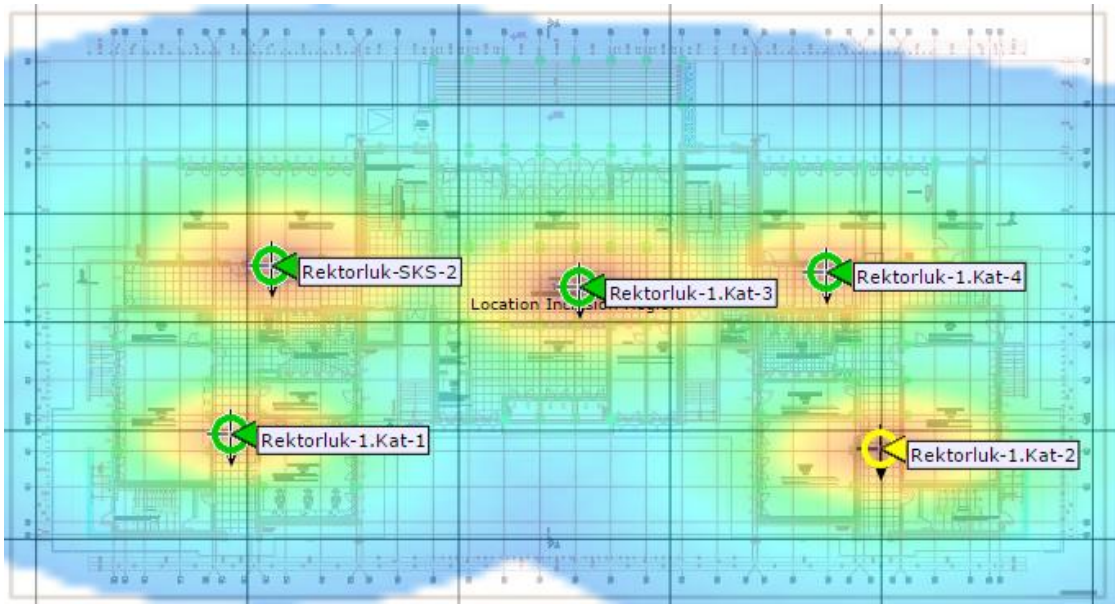
Şekil 4.5 Ağ cihazları yerleşim planı örneği

Optimum kablosuz çekim alanı oluşması için kablosuz ağ cihazlarının konumlarında değişiklik yapılması gerekmektedir. Hatalı bir AP yerleşimi Şekil 4.6'da görülmektedir.



Şekil 4.6 AP yerleşim planı örneği - 1

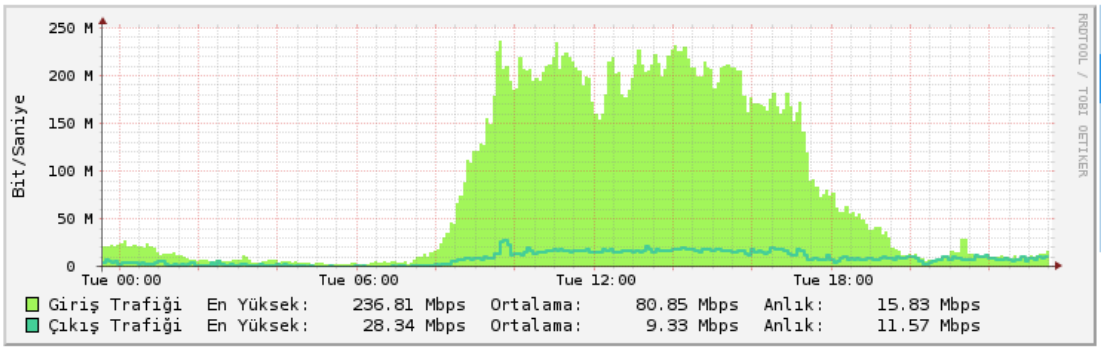
Optimum çekim alanı oluşturulması için ise AP Şekil 4.7'de gösterildiği şekilde konumlandırılması gerekir.



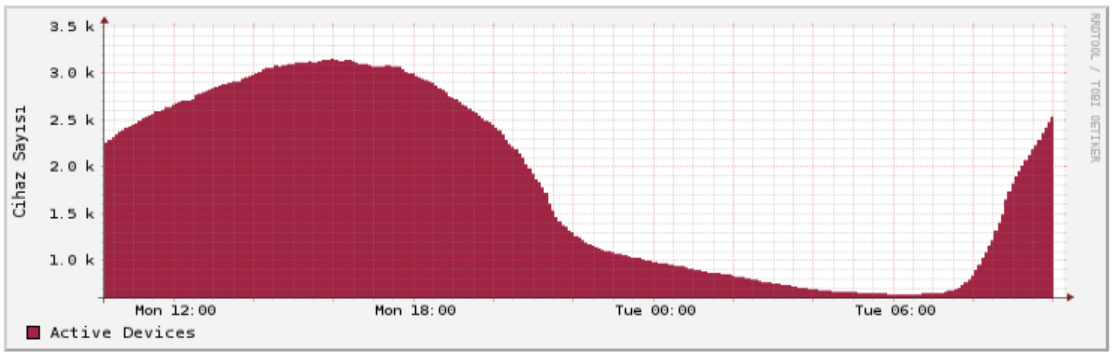
Şekil 4.7 AP yerleşim planı örneği - 2

4.2.2 İnternet Kullanım Oranları

2016 yılı internet trafiği üzerinde yapılan genel gözlemler sonucunda ise;
Üniversite genelinde oluşan günlük internet trafiği ise Şekil 4.8'de görülebilmektedir. Trafiği oluşturan cihaz sayıları ise Şekil 4.9'da görüldüğü gibidir.

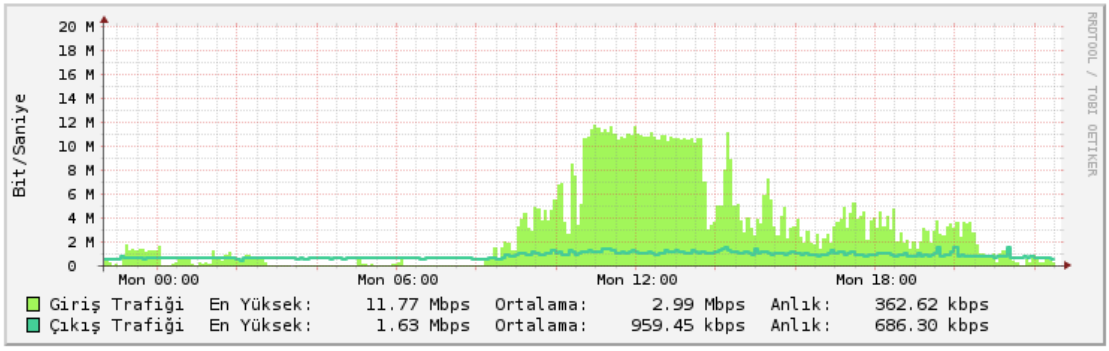


Şekil 4.8 Toplam trafik istatistiği



Şekil 4.9 Anlık toplam aktif cihaz sayısı

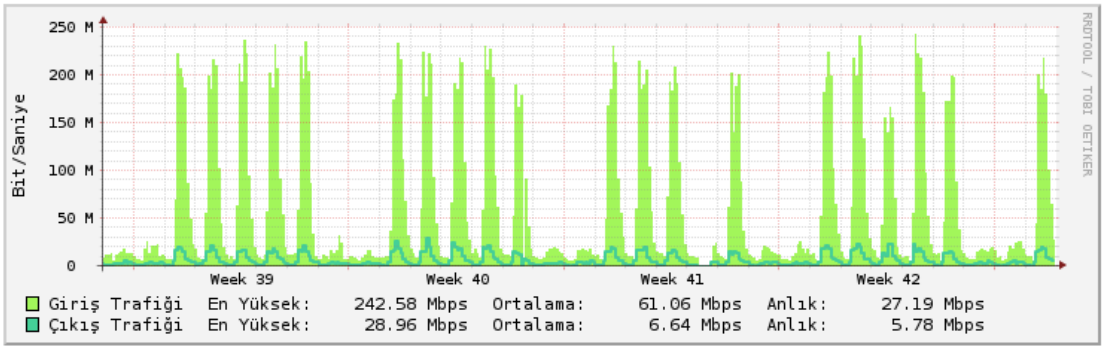
İnternet kullanım istatistikleri incelenerek ileriye yönelik yatırım planlaması yapılması sağlanabilir. Şekil 4.10'da İskilip ilçesinde üniversiteye bağlı İskilip Meslek Yüksekokulu günlük internet kullanım istatistiği görülmektedir.



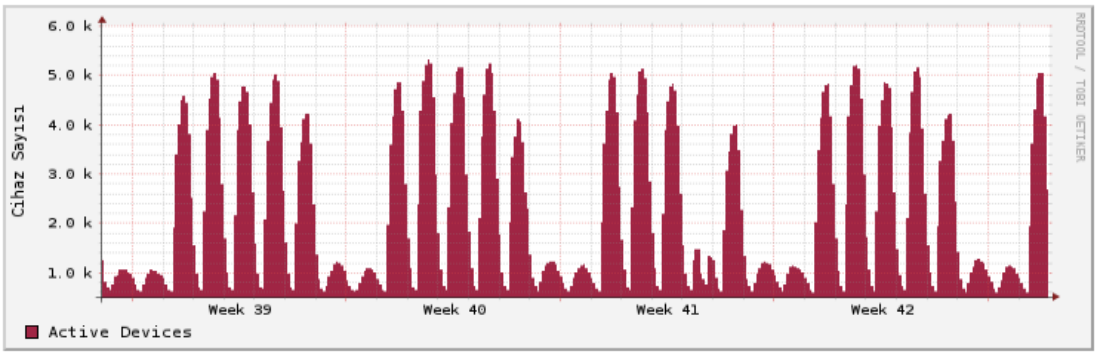
Şekil 4.10 İskilip MYO trafik istatistiği

İskilip Meslek Yüksekokulu trafik istatistiği incelendiğinde özellikle Eylül – Ekim aylarında hafta içi öğle saatlerinde internetin yoğun olarak kullanıldığı görülmektedir. İnternet kullanımının 10 Mbps doymuşluk sınırına ulaşmış ve kullanıcılardan gelen taleplere zaman zaman karşılık veremez duruma gelmiştir. Ulakbim uç yönetim sistemi üzerinden hız artışı yapılması için gerekli girişimlerde bulunulmuştur.

Bilgisayar laboratuvarları sayısında meydana gelen artış ve bir kullanıcının birden fazla internete bağlanabilecek cihaza sahip olması sonucunda, yıl içinde internet kullanım miktarı artmaktadır. Özellikle öğrencilerin interneti yoğun olarak kullanmaya başladığı Eylül - Ekim dönemlerinde toplam kullanılan cihaz sayısı 5000'e, internet kullanım oranı ise 200 Mbps'a ulaştığı Şekil 4.11 ve Şekil 4.12'de görülmektedir.



Şekil 4.11 Toplam trafik istatistiği



Şekil 4.12 Toplam aktif cihaz sayısı

İnternetin yoğun olarak kullanılmadığı gece saatlerinde makine işletim sistemi güncellemeleri ile makine yedekleme ve çoğaltma işlemleri yapılabilir. Ayrıca makine bakımlarının da gece saatlerinde yapılması da kullanıcıların en az şekilde etkilenmesi anlamına gelecektir.

Ulakbim ağ istatistikleri merkezi üzerinden alınan 2014 ve 2015 yıllarına ait veri kullanım istatistikleri Çizelge 4.1 ve Çizelge 4.2'de görülebilmektedir.

Çizelge 4.1 2014 yılı veri kullanım istatistikleri (Birim/TB)

2014	Ocak	Şubat	Mart	Nisan	Mayıs	Haziran	**Toplam**
İçeri	13.05	13.02	16.38	12.34	10.98	8.11	73.88
Dışarı	2.26	2.83	3.34	1.65	1.93	1.87	13.88
En Fazla	13.05	13.02	16.38	12.34	10.98	8.11	73.88
Toplam	15.31	16.02	19.72	13.99	12.91	9.98	87.93

Çizelge 4.2 2015 yılı veri kullanım istatistikleri (Birim/TB)

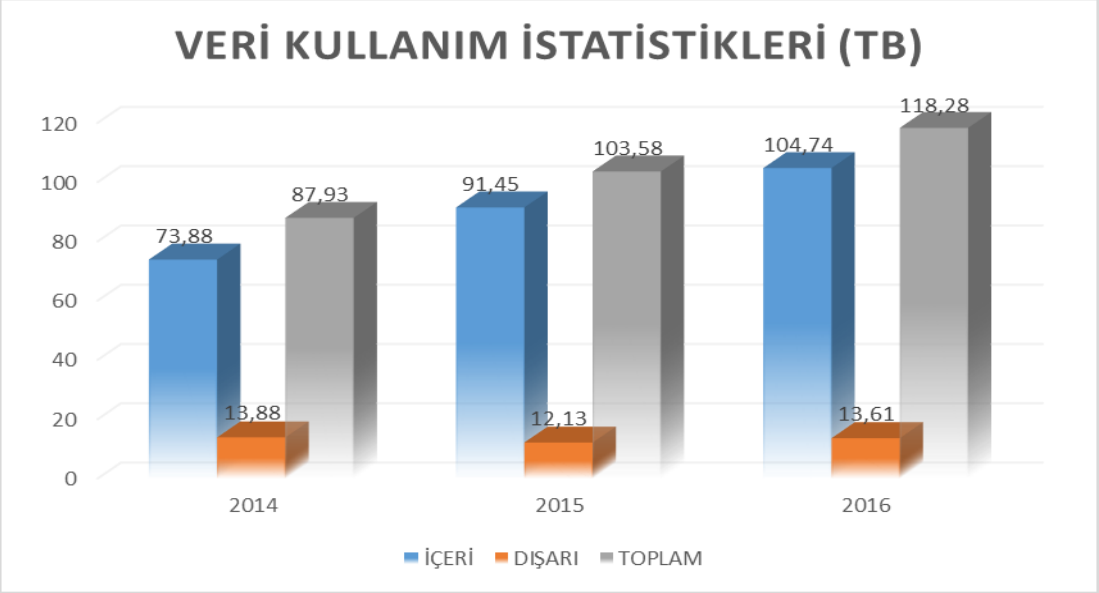
2015	Ocak	Şubat	Mart	Nisan	Mayıs	Haziran	**Toplam**
İçeri	11.89	12.79	18.04	16.19	17.34	15.20	91.45
Dışarı	2.43	1.87	1.96	1.96	1.82	2.09	12.13
En Fazla	11.89	12.79	18.04	16.19	17.34	15.20	91.45
Toplam	14.32	14.65	20.00	18.15	19.15	17.28	103.58

2014 yılında ilk altı aylık toplam 87.93 TB veri işlenirken 2015 yılında aynı dönemde internetten toplam 103.58 TB veri işlendiği gözlemlenmektedir (Çizelge 4.3).

Çizelge 4.3 2016 yılı veri kullanım istatistikleri (Birim/TB)

2016	Ocak	Şubat	Mart	Nisan	Mayıs	Haziran	**Toplam**
İçeri	14.36	16.34	21.62	16.9	19.12	16.38	104.74
Dışarı	2.37	2.02	2.6	2.05	2.18	2.39	13.61
En Fazla	14.36	16.34	21.62	16.9	19.12	16.38	104.74
Toplam	16.73	18.36	24.22	18.95	21.3	18.77	118.28

2016 Yılı içinde ilk altı ayda ise 104.74 TB verinin indirildiği, 13.61 TB verinin ise internet ortamına yüklendiği görülmektedir. İlk altı aylık veri kullanımı toplamına bakıldığında ise 2014 ve 2015 yıllarına göre artış olduğu gözlemlenmektedir. İnternet kullanım miktarları Resim 4.15'te grafiksel olarak görünmektedir.



Resim 4.15 Yıllara göre veri kullanım istatistikleri

Artış oranlarını incelendiğinde 2017 yılının ilk altı ayında; veri indirme yönünde 120.38 TB, veri yükleme yönünde 13.75 TB toplamda ise 134.13 TB veri işleneceği tahmin edilmektedir.

4.2.3 Yapılan Saldırıların İzlenmesi

Kötü niyetli olarak sistemlerin açıklarından faydalanılarak yapılmaya çalışılan saldırılar firewall (güvenlik duvarı) tarafından engellenmiştir. Yapılan saldırıların türleri ve hangi IP adresleri üzerinden saldırının yapıldığı loğlardan görülebilmektedir. Resim 4.16'de görüldüğü gibi dış IP adreslerinden hem de iç IP adreslerinden atakların yapıldığı, güvenlik duvarı tarafından ise bu atakların engellendiği görülmektedir.

#	@	Date/Time	Source	Destination	Protocol	Action	Attack Name
1		16:16:16	130.193.37.5	79.123.184.71	tcp	dropped	PHP.Function.CRLF.Injection
2		16:15:01	141.8.142.162	79.123.184.71	tcp	dropped	PHP.Function.CRLF.Injection
3		16:14:18	62.210.181.123	79.123.184.137	tcp	dropped	WordPress.Slider.Revolution.File.Inclusion
4		16:13:38	5.255.253.39	79.123.184.71	tcp	dropped	PHP.Function.CRLF.Injection
5		16:12:23	141.8.183.21	79.123.184.71	tcp	dropped	PHP.Function.CRLF.Injection
6		15:35:48	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
7		15:35:46	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
8		15:35:11	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
9		15:35:02	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
10		15:04:07	10.100.32.117	79.123.184.180	tcp	dropped	TCP.Inconsistent.Retransmssion
11		15:03:16	10.100.32.117	79.123.184.180	tcp	dropped	TCP.Overlapping.Fragments
12		14:38:37	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
13		14:36:52	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
14		14:05:18	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution
15		14:05:05	10.25.25.206	146.0.4.18	tcp	dropped	STUNSHELL.Web.Shell.Remote.Code.Execution

Resim 4.16 Saldırı önleme sistemi ekran görüntüsü

Firewall sistemi anormal trafik olarak isimlendirilen saldırıları da engellememiştir. Resim 4.17'de görüldüğü gibi DoS saldırısı türevi olan udp_flood ve icmp_flood atakları tespit edilmiş ve saldırı engellenmiştir.

#	Date/Time	Source	Source Port	Destination	Destination Port	Attack Name	Action	Count
1	00:14:41	77.238.84.223	63231	193.255.107.185	44162	udp_flood	clear_session	101
2	00:14:36	74.125.154.107	443	193.255.107.90	57469	udp_flood	clear_session	140
3	00:14:30	74.125.153.59	443	193.255.107.140	60956	udp_flood	clear_session	104
4	00:14:25	74.125.154.107	443	193.255.107.90	57469	udp_flood	clear_session	182
5	00:14:20	74.125.153.55	443	193.255.107.30	53647	udp_flood	clear_session	198
6	00:14:19	219.158.30.145		193.255.107.121	11	icmp_flood	clear_session	1
7	00:14:13	74.125.154.107	443	193.255.107.90	57469	udp_flood	clear_session	168
8	00:14:08	74.125.153.55	443	193.255.107.30	53647	udp_flood	clear_session	123
9	00:14:03	74.125.154.107	443	193.255.107.90	57469	udp_flood	clear_session	108
10	00:13:57	74.125.154.106	443	193.255.107.30	52136	udp_flood	clear_session	354
11	00:13:52	216.58.212.1	443	193.255.107.90	52066	udp_flood	clear_session	132
12	00:13:47	92.223.0.13	32810	193.255.107.140	59899	udp_flood	clear_session	365
13	00:13:41	74.125.154.107	443	193.255.107.90	57469	udp_flood	clear_session	131
14	00:13:35	74.125.153.59	443	193.255.107.140	60956	udp_flood	clear_session	221
15	00:13:30	74.125.153.204	443	193.255.107.160	51553	udp_flood	clear_session	207

Resim 4.17 Anormal trafik ekran görüntüsü

5. TARTIŞMA ve SONUÇ

Laboratuvar ortamında yaptığımız çalışmada güvenlik önlemleri kenar anahtarlar üzerinde alınmıştır. Tüm trafiğin firewall üzerinden geçirilmesi durumunda güvenlik sağlanabilir. Bu durumda firewall üzerinde aşırı fazla yük oluşur. Amacı güvenliğin sağlanması olan bir cihaza bu kadar yüklü bir görev verilmesi firewall cihazının kolay kolay taşıyamayacağı bir yük durumundadır. Tüm trafiğin firewall üzerinde sonlandırılmaması ve anahtarlar (switch) üzerinde güvenlik ayarların yapılmadığı durumunda ise trafik diğer ağ cihazları üzerinden dolaşacağı için tek başına firewall koruması yetersiz kalmaktadır. Bu sebeple yapılan çalışmada yönetilebilir anahtarlar (switch) kullanılarak ağ trafiğinin rahat dolaştığı kenar anahtarlar (switch) üzerinde güvenlik kriterleri artırılmış, yedekli bir yapı kurularak da yük dengelemesi yapılması sağlanmıştır.

Kapsama alanının genişleyerek daha iyi bir kablosuz altyapının kurulabilmesi için kablosuz ağ cihazlarının yerleşim planlaması yapılarak yönetim kolaylığı sağlayacak merkezi kontrollü bir yapı kurulması gerekmektedir.

Kablosuz ağ cihazlarını merkezi olarak yönetimi ile cihazlarda kolay yapılandırma yapılması sonucunda iş gücü ve zamandan tasarruf sağlanmıştır. Aynı zamanda kablosuz ağ cihazları üzerindeki kullanıcı yoğunluğu ve kullanıcılara ait bilgilere merkezi yönetim sayesinde rahatlıkla erişilebilmektedir.

Üniversiteye bağlı birimlerin internet kullanım oranları incelenmesi sonucunda İskilip Meslek Yüksekokulu internet kullanım istatistiklerinde görülen doymuşluk seviyesine ulaşması sebebi ile internet hızının artırılması, hız artışının yapılması için ise yatırım yapılması gerekmektedir.

Yapılan bu çalışmada ideal ağ tasarımı ve ağ güvenliği ele alınmıştır.

İdeal ağ tasarımı;

- Anahtarlar arası yatay ve dikey olarak yedekli kablo kullanılarak hatlar birleştirilmiştir. İki katı performans sağlanmış ve fiziksel altyapının yedekli olması sağlanmıştır.
- HSRP Protokolü kullanılarak aktif ve bekleme durumunda olmak üzere iki adet L3 anahtar (switch) üzerinden gelen trafiğin tek bir sanal ağ geçidine yönlendirilmesi sağlanmıştır.
- Etherchannel yöntemiyle bant genişliği genişletilmiş ve bağlantı yedekliliği sağlanmıştır.
- Yedekli bir yapı kurulmuştur. Kurulan yedekli yapı test edilmiştir. Switch1 kapatıldıktan sonra tüm trafiğin Switch2 üzerine geçtiği gözlemlenmiştir. Son kullanıcılar bu işlemden en az şekilde etkilenmiş ve normal çalışmalarına devam etmiştir. Arıza oluşması durumunda dahi gönderilen paketlerin hedefe ulaşması sağlanmıştır.
- Kablosuz ağ cihazları kullanılan frekanslarda çakışma olmayacak ve en fazla kapsama alanı oluşturacak şekilde konumlandırma yapılmıştır.
- Kullanıcı trafiğinin farklı anahtarlar üzerinden geçmesi sağlanarak anahtarlar üzerindeki yük azaltılmıştır.

Ağ güvenliği;

- Kullanıcı ağı sanal ağlara bölünerek ağlar arası güvenlik sağlanmış, ağ içine istenmeyen kullanıcı gruplarının girişi engellenmiştir.
- Ağ güvenliği için alınan güvenlik önlemleri laboratuvar ortamında test edilmiş ve test sonuçları incelenmiştir.
- Port bazlı yapılandırma ayarları sonucunda broadcast trafiği sınırlandırılmıştır. Arp trafiğinin de sınırlandırılması ile istenmeyen paketlerin dolaşması engellenmiştir.
- Port bazlı güvenlik önlemi alınarak son kullanıcı portlarına istenmeyen cihazların bağlanmasının ve oluşabilecek loop probleminin önüne geçilmiştir.
- Ağ içinde sahte arp istekleri ve kullanılan protokol kaynaklı zafiyetler engellenerek yapılabilecek atakların önüne geçilmiştir.

- Ağ içinde sahte DHCP sunucuları kurularak mevcut yapıya zarar verebilecek sahte DHCP sunucuları kullanılması ile mevcut yapıyı zarar verilmesi önlenmiş, bu yöntem ile yapılabilecek saldırılar da engellenmiştir.
- Son kullanıcı ya da virüslerin ağda sahte MAC adresleri üreterek anahtarların MAC tablosunu doldurarak anahtarlara ya da DHCP sunucuya yapılabilecek saldırılar önlenmiştir.
- Kullanıcılardan merkeze doğru kontrolsüz bir trafiğin önüne geçilmesi ve daha güvenli bir ağ yapısı oluşturulması için ağ cihazları üzerinde güvenlik önlemleri alınmıştır.
- Son kullanıcı portlarında Bpdu-guard özelliği aktif edilerek bu portlara anahtarlayıcı (switch) takılması engellenmiştir. Portlara takılacak cihaz sayısına sınırlama getirilmiştir. Böylece bu portlara bilinçsiz ya da istem dışı takılan bilgisayarlar engellenmiştir.
- Kullanıcıların tüm bant genişliğini meşgul etmesini engellenmesi için broadcast, unicast trafiği sınırlanmıştır.
- Misafir kullanıcıların muhasebe ve personel ağından yalıtılarak sadece internete çıkmalarına izin verilmiştir.
- Netflow analizi ile anlık olarak veri trafiği incelenmiş, kullanılan protokoller ile veri kullan miktarlarında herhangi olumsuz bir durumla karşılaşılmamıştır. Netflow ile iç ağda oluşan tüm trafiğin izlenebildiği görülmüştür.
- Ağ üzerindeki paketlerin analiz edilmiş, şifrelenmeden gönderilen paketlerde kullanıcılara ait kritik bilgilerin tespit edilebileceği görülmüştür.
- Ağın dışarı bakan tarafında güvenlik duvarı kullanılması ve dışarıdan gelebilecek saldırılara karşı mutlaka önlem alınması gerektiği görülmüştür.

Bu çalışmada donanım cihazlarının maliyetinin yüksek olması sebebi ile yedek olarak düşünülen ikinci bir omurga cihazı temin edilememiştir. Bu sebeple tek omurga cihaz kullanılmış, HSRP protokolü ile yedekli bir ağ yapısı oluşturulmuştur.

Gelecekte yapılacak çalışmalarda iki omurga cihazı kullanılması durumunda VSS (Sanal Anahtarlama Sistemi) teknolojisi ile tam yedekli bir yapı kurulması sağlanabilir. VSS teknolojisi ile iki omurga anahtar üzerinde ağ geçidi yedekliliği

sağlanacağından anahtarlar (switch) aktif / aktif olarak çalışacaktır. VSS ile STP bağımlılığı da ortadan kalkacaktır. Aynı zamanda iki omurga anahtarın (switch) tek bir anahtar (switch) olarak görülmesi ile yönetim anlamında da kolaylık sağlayacaktır.

Gelecek çalışmalarda IPv4 internet protokolü yerine biraz daha karmaşık yapıya sahip olan IPv6 internet protokolü kullanılabilir.

6. KAYNAKLAR

Abdulkareem, M. (2012). IEEE 802.11 Kablosuz Ağlarda Güvenlik. Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara.

Akın, G. ve Bük O. (2014). Kampüs Ağlarında Ağ Yöneticiliğine Giriş. Akademik Bilişim Konferansı, Mersin, 5-7 Şubat.

Ali, M. N. B., Hossain, M. E. and Parvez, M. M. (2015). Design and Implementation of a Secure Campus Network. *International Journal of Emerging Technology and Advanced Engineering*, **5**: 370-374.

Anonim, 2011. ULAKBİM IPv6 Geçiş Eğitim Notları. TÜBİTAK ULAKBİM, Ankara,

Anonim, 2012. IPv6 El Kitabı, TÜBİTAK ULAKBİM, Ankara.

Butler, J. (2013). Wireless Networking In The Developing World. wndw.net, Third Edition, Copenhagen, DENMARK.

Can, Ö. ve Akbaş, M. F. (2014). Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması. *TUBAV Bilim Dergisi*, **7(2)**: 16-31.

Comer, D. E. (2000). Internetworking With TCP/IP. Prentice Hall, Forth Edition, New Jersey, USA.

Coşar, M. ve Arık, İ. (2014). Yeni Nesil Güvenlik Duvarlarında Olması Beklenen Özellikler ve Uygulama Bazlı Filtreleme. Türkiye'de İnternet Konferansı, Yaşar Üniversitesi, İzmir, 24-27 Kasım, 259-265.

Çakar, H. (2005). Bilgisayar Ağ Güvenliği ve Güvenlik Duvarları. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

Çetin, G. ve Metin, B. (2005). Linux Ağ Yönetimi, Şeçkin Yayıncılık, 5. Baskı, Ankara.

Dağ, B. (2001). Ağ Güvenliği ve Güvenlik Duvarları. Yüksek Lisans Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli.

Daya, B. (2013). Network Security: History, Importance and Future, University of Florida Department of Electrical and Computer Engineering, 13.

Ertuğrul, A. (2013). Açık Kaynak Kodlu Yazılımlarla Ağ Güvenliğinin Sağlanması Afyon Kocatepe Üniversitesi Örneği. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, Afyonkarahisar.

Farraposo, S., Gallon, L. and Owezarski, P. (2005). Network Security and DoS Attacks. Technical Report, http://www.laas.fr/METROSEC/Security_and_DoS.pdf.

Forouzan, B. A. (2007). Data Communications and Networking. Mc Graw Hill, Forth Edition, New York, USA.

Gupta, B. B., Joshi, R. C. and Misra, M. (2012). Ann Based Scheme to Predict Number of Zombies in DDoS Attack. *International Journal of Network Security*, **14 (2)**: 61-70.

Hunt, C. (2002). TCP/IP Network Administration, O'Reilly Media, Third Edition, Sebastopol, USA.

Kaplan, Y. (2006). Network Veri Haberleşmesi Uygulamaları. Papatya Yayınları, 2. Baskı, İstanbul.

Karaarslan, E. (2005). Kampüs Ağ Yönetimi, Akademik Bilişim Konferansı, Gaziantep, 2-4 Şubat, 1-3.

Knipp, E., Browne, B., Weaver, W., Baumrucker, C. T., Chaffin, L., Caesar, J., Osipov, V. and Danielyan, E. (2002). Managing Cisco Network Security. Syngress, Second Edition, Rockland, USA.

Lammle, T. (2005). CCNA: Cisco Certified Network Associate Study Guide. Sybex, Fifth Edition, San Francisco - London, ENGLAND.

Lammle, T. (2007). CCNA: Cisco Certified Network Associate Study Guide. Wiley Publishing, Sixth Edition, Indiana, USA.

Öner, B. D. (2003). Bilgisayar Ağları. Papatya Yayıncılık, İstanbul.

Özbilen, A. (2005). Bilgisayar Ağları ve Güvenliği. Pusula Yayıncılık, İstanbul.

Spurgeon, E. C. and Zimmerman J. (2005). Ethernet: The Definition Guide. O'Reilly Media, Second Edition, USA.

Tutkun, H. K. (2011). Network Sistemleri. Seçkin Yayınları, Ankara.

Uçan, O. N ve Osman, O. (2006). Bilgisayar Ağları ve Ağ Güvenliği. Nobel Yayın Dağıtım, Ankara.

Uzun, M. (1999). Bilgisayar Ağlarında Firewall ile Güvenlik. Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Mühendislik ve Fen Bilimleri Enstitüsü, Gebze.

Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, Standards-based, Interoperable security For Today's Wi-Fi Networks, 4-5.

Yılmaz, E. ve Öztürk, E. (2007). Yeni Nesil Kablosuz İletişim Teknolojileri Karşılaştırmalı Analizi, EMO III. İletişim Teknolojileri Ulusal Sempozyumu, Adana, 18-19 Ekim, 1-2.

İnternet Kaynakları

1) http://www.elektrikport.com/teknik-kutuphane/network-topolojileri-ve-calisma-sekilleri-bolum-1/15282#ad-image-0, 09.11.2015
2) http://www.vpnnedir.org/vpn/sanal-ozel-ag, 15.11.2015
3) https://myassignmenthelp.com/computer_network_assignment_help.html, 22.11.2016
4) http://www.conceptdraw.com/How-To-Guide/campus-area-networks, 07.11.2015
5) http://searchsdn.techtarget.com/definition/campus-network, 08.11.2015
6) http://shiftdelete.net/radyolink-nedir-ve-ne-ise-yarar-34785, 27.10.2015
7) http://www.nbbc.org.uk/hub-churches/, 08.11.2015
8) http://www.handoli.com/internet-cok-yavas-cozuldu/, 25.11.2015
9) http://ecomputernotes.com/computernetworkingnotes/communication-networks/bridges, 26.11.2015
10) https://www.ovh.com/us/about-us/network.xml, 26.11.2015
11) http://www.netgear.com/images/UTM25s%20overview118-63541.png, 27.11.2015
12) http://labrisnetworks.com/tr/blog-tr-yeni-nesil-guvenlik-duvari-ngfw-next-generation-firewall/, 19.11.2015
13) http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/osi-katmanları, 21.11.2015
14) http://mimoza.marmara.edu.tr/~hkaptan/tcp-ip.htm, 20.12.2015
15) http://www.dummies.com/how-to/content/network-basics-tcpip-and-osi-network-model-compari.html, 15.11.2015
16) http://www.batuhanduzgun.com/post/2010/10/13/ARP-Protokolu-ve-Detaylarc4b1.aspx, 16.11.2015
17) http://www.omnisecu.com/cisco-certified-network-associate-ccna/three-tier-hierarchical-network-model.php, 16.12.2015
18) http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4, 20.12.2015
19) http://electroniccomputerinformation.blogspot.com.tr/2015/09/wireless-lans.html, 15.10.2015
20) http://www.ozengen.com/kablosuz-cekim-gucunu-arttirmak/, 15.01.2016

21) http://btechbilisim.com/ag-yonetimi/, 21.11.2015
22) http://www.belgeci.com/layer-2-switching.html, 21.12.2015
23) http://securityuncorked.com/2011/11/the-4-wireless-controller-architectures-you-need-to-know/, 10.02.2016
24) http://www.simsekpc.com.tr/fiber-optik-altyapi, 08.12.2015
25) https://evrak.wordpress.com/2011/12/09/yapisal-kablolama-ve-standartlar/, 08.12.2015
26) http://www.ultekege.com.tr/yapisalkablolama.html, 08.12.2015
27) http://blog.vitel.com.tr/2014/02/kablosuz-ag-tasarim-hatalari/, 28.12.2015
28) http://www.networkworld.com/article/2223672/access-control/which-eap-types-do-you-need-for-which-identity-projects.htm, 24.02.2016
29) https://technet.microsoft.com/tr-tr/en-%20us/library/bb878054.aspx, 20.02.2016
30) http://www.ertandonmez.com/ikinci-katman-saldirilari-2.html, 11.02.2016
31) http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasil-yapilir.html, 05.01.2016
32) http://ekaragol.blogspot.com.tr/2015/02/arp-zehirlemesi-ile-bilgi-edinme.html, 12.01.2016
33) http://www.cisco.com/c/en/us/support/switches/catalyst-6509-e-switch/model.html, 20.01.2016
34) http://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tc-l-switch/model.html, 10.01.2016
35) http://www.muratturkyilmaz.com.tr/?p=40, 20.01.2016
36) http://sozluk.cozumpark.com/goster.aspx?id=1405&kelime=distinguished-name, 30.02.2016
37) https://www.kali.org/downloads/, 14.07.2016
38) https://www.wireshark.org/download.html, 28.09.2016
39) http://www.oxid.it/cain.html, 12.06.2016
40) http://www.solarwinds.com/free-tools/real-time-netflow-analyzer, 05.06.2016
41) http://cactiez.cactiusers.org/download/, 18.05.2016
42) https://www.plixer.com/products/scrutinizer/download/, 10.05.2016

ÖZGEÇMİŞ

Adı Soyadı : İsmail ARIK

Doğum Yeri ve Tarihi : AFYONKARAHİSAR-Emirdağ / 10.12.1981

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : 05354561548 / ismailarik@hitit.edu.tr

Eğitim Durumu (Kurum ve Yıl)

Lise : Bilecik Anadolu Ticaret Meslek Lisesi
Bilgiişlem Bölümü (1996- 2000)

Önlisans : Uludağ Üniversitesi, Teknik Bilimler Meslek Yüksekokulu,
Bilgisayar Programcılığı Bölümü (2001-2003)

Lisans : Anadolu Üniversitesi, İşletme Bölümü (2003-2010)

Çalıştığı Kurum/Kurumlar ve Yıl :

Hitit Üniversitesi, Bilgi İşlem Daire Başkanlığı, ÇORUM, 2007 – …

Yayınları (SCI ve diğer) :

Diğer konular :