**T.C.**
**MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ**
**ANABİLİM DALI**

# KABLOSUZ KAMPÜS AĞLARINDA DİNAMİK VLAN YAPILANDIRMASININ AĞ PERFORMANS PARAMETRELERİ ÜZERİNDEKİ ETKİSİ

**YÜKSEK LİSANS TEZİ**

**MUHAMMED FATİH TARLACI**

**TEMMUZ 2018**
**MUĞLA**

## TEZ ONAYI

**MUHAMMED FATİH TARLACI** tarafından hazırlanan **KABLOSUZ KAMPUS AĞLARINDA DİNAMİK VLAN YAPILANDIRMASININ AĞ PERFORMANS PARAMETRELERİ ÜZERİNDEKİ ETKİSİ** başlıklı tezinin, 18/07/2018 tarihinde aşağıdaki jüri tarafından Bilişim Sistemleri Mühendisliği Anabilim Dalı'nda yüksek lisans derecesi için gerekli şartları sağladığı oybirliği/oyçokluğu ile kabul edilmiştir.

---

**TEZ SINAV JURİSİ**

Doç. Dr. Ali Hakan IŞIK **(Jüri Başkanı)** İmza:

Bilgisayar Mühendisliği Bölümü,
Mehmet Akif Ersoy Üniversitesi, BURDUR

Doktor Öğretim Üyesi Gürcan ÇETİN **(Danışman)** İmza:

Bilişim Sistemleri Mühendisliği Anabilim Dalı,
Muğla Sıtkı Koçman Üniversitesi, Muğla

Doktor Öğretim Üyesi Osman ÖZKARACA **(Üye)** İmza:

Bilişim Sistemleri Mühendisliği Anabilim Dalı
Muğla Sıtkı Koçman Üniversitesi, Muğla

---

**ANA BİLİM DALI BAŞKANLIĞI ONAYI**

Prof. Dr. Osman GÖKTAŞ İmza:

Bilişim Sistemleri Mühendisliği ABD.
Muğla Sıtkı Koçman Üniversitesi, Muğla

Doktor Öğretim Üyesi Gürcan ÇETİN İmza:

Danışman, Bilişim Sistemleri ABD.
Muğla Sıtkı Koçman Üniversitesi, Muğla

Savunma Tarihi: 18/07/2018

Tez çalışmalarım sırasında elde ettiğim ve sunduğum tüm sonuç, doküman, bilgi ve belgelerin tarafımdan bizzat ve bu tez çalışması kapsamında elde edildiğini; akademik ve bilimsel etik kurallarına uygun olduğunu beyan ederim. Ayrıca, akademik ve bilimsel etik kuralları gereği bu tez çalışması sırasında elde edilmemiş başkalarına ait tüm orijinal bilgi ve sonuçlara atıf yapıldığını da beyan ederim.

Muhammed Fatih TARLACI

18/07/2018

# ÖZET

## KABLOSUZ KAMPÜS AĞLARINDA DİNAMİK VLAN YAPILANDIRMASININ AĞ PERFORMANS PARAMETRELERİ ÜZERİNDEKİ ETKİSİ

Muhammed Fatih TARLACI

Yüksek Lisans Tezi

Fen Bilimleri Enstitüsü

Bilişim Sistemleri Mühendisliği Anabilim Dalı

Danışman: Doktor Öğretim Üyesi Gürcan ÇETİN

Temmuz 2018, 80 Sayfa

Bu çalışmada Muğla Sıtkı Koçman Üniversitesi kablosuz ağında kullanıcıların tek bir kullanıcı adı ve şifre ile kampüsün her noktasından güvenli bir şekilde ağa dahil olabilmeleri amaçlanmıştır. Gezgin kullanıcıların ağa katılırken hangi yetkilere sahip olacağının belirlenebilmesi için kullanıcılar OpenLDAP veri tabanı içerisinde belirli bir düzene göre gruplandırılmıştır. Yapılan tanımlamalar ile her kullanıcı kablosuz ağa nereden bağlanırsa bağlansın kendisi için tanımlanan VLAN'dan IP adresi alması sağlanmıştır.

Sanal yerel ağ anlamına gelen VLAN, IEEE 802.11Q standardıdır. Yerel ağ içerisinde çalışma grupları oluşturmak ve yerel ağı mantıksal alt ağlara bölmek için kullanılmaktadır. MSKÜ kablosuz ağında, kural tabanlı dinamik VLAN atamaları gerçekleştirilmiş ve ağda oluşan broadcast sayısı, bant genişliği, ağa dahil olan anlık kullanıcı sayıları ve alt ağlar güvenlik açısından incelenmiştir. Yapılan çalışma sonucunda ağ güvenliğinde artış, ağda gerçekleşen broadcast sayısında azalma ve bant genişliğinde artış olmuştur. Ayrıca kablosuz ağ yönetimi açıdan esnek ve yönetilebilir bir yapı oluşturulması amaçlanmıştır.

**Anahtar Kelimeler:** Dinamik VLAN Ataması, Cacti, SNMP, Kablosuz, Kampüs Ağı, Eduroam, FreeRadius, OpenLDAP, Statik VLAN, 802.11, 802.1x, Yayın Adresi Kontrolü, AAA

## ABSTRACT

## EXAMINING THE EFFECT OF DYNAMIC VLAN CONFIGURATION ON NETWORK PERFORMANCE PARAMETERS IN WIRELESS CAMPUS NETWORKS

Muhammed Fatih TARLACI

Master Thesis

Institute of Science and Technology

Information System Engineering

Supervisor: Assistant Professor Gürcan ÇETİN

July 2018, 80 pages

In this study, it is aimed that users in the wireless network of Muğla Sıtkı Koçman University can safely join the network with a single user name and password at every point of the campus. Users are grouped according to a specific scheme within the OpenLDAP database so that mobile users can determine what authority they will have when joining the network. With this configuration, each user is able to get an IP address from the VLAN defined for the connection to where the user is connected to the wireless network. rule based dynamic VLAN architectures were carried out in the wireless network of MSKÜ bandwidth, the number of broadcasts and instant users included in the network were investigated and subnets were examined for security reasons.

VLAN, which means virtual local area network, is referred to as the IEEE 802.11Q standard. It is used to create workgroups within the local network and to divide the local network into logical subnets. In this study, rule-based dynamic VLAN assignments were performed in the Muğla Sıtkı Koçman University wireless network and the effects on the network were examined. As a result of this study, it is expected that network security will increase, decrease the number of broadcasts in the network and increase the bandwidth. It is also aimed to create a flexible structure in terms of network management.



**Keywords:** Dynamic VLAN Assignment, Cacti, SNMP, Wireless, Campus Network Eduroam, FreeRadius, OpenLDAP, Static VLAN, 802.11, 802.1x, Broadcast Control, AAA

“Sedat Mirza ve Elanur’a”

# ÖNSÖZ

Bu çalışma, Muğla Sıtkı Koçman Üniversitesi Fen Bilimleri Enstitüsü Bilişim Sistemleri Mühendisliği Anabilim Dalında yüksek lisans tezi olarak hazırlanmıştır. Muğla Sıtkı Koçman Üniversitesi kablosuz kampüs ağında anons edilen "eduroam" yayını üzerinde yapılan çalışmaları kapsamaktadır. Eduroam ağı küresel ölçekte bir federasyon tarafından yönetilmekte olup, Türkiye'de TÜBİTAK ULAKBİM tarafından desteklenmektedir.

Yüksek lisans eğitimim boyunca benden hiçbir desteği esirgemeyen, iş ahlakı ve bilim insanı tavrı ile çalışkanlığını örnek aldığım, danışmanlığımı yapan değerli hocam Doktor Öğretim Üyesi Gürcan ÇETİN'e, fikir ve önerileri ile bana yol gösteren Doçent Doktor Ali Hakan IŞIK ve Doktor Öğretim Üyesi Osman ÖZKARACA hocalarıma en içten duygularımla teşekkürü borç bilirim.

Ayrıca görüş, önerileri ve destekleri ile her zaman bana yardımcı olan Muğla Sıtkı Koçman Üniversitesi Bilgi İşlem Dairesi Başkanı Osman KELEŞ'e ve mesai arkadaşlarıma şükranlarımı sunarım.

# İÇİNDEKİLER

# ÇİZELGELER DİZİNİ

# ŞEKİLLER DİZİNİ

## SEMBOLLER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

| Kısaltmalar | Açıklama |
|---|---|
| **AAA** | Authentication-Authrization-Accounting |
| **ACL** | Access List |
| **ACS** | Access Control System |
| **AES** | Advanced Encryption Standard |
| **AP** | Accces Point |
| **ARP** | Address Resolution Protocol |
| **AVP** | Attribute Value Pairs |
| **bps** | Bit per second |
| **BSS** | Basic Service Set |
| **CAD** | Computer Aided Design |
| **CBC-MAC** | Cipher Block Chaining Message Authentication Code |
| **CCK** | Complementary code keying |
| **CCMP** | Counter Mode Cipher Block Chaining Message Authentication Code Protocol |
| **CF** | Consolidation Function |
| **CHAP** | Challenge-Handshake Authentication Protocol |
| **CPU** | Central Processing Unit |
| **CSMA** | Carrier Sense Multiple Access |
| **CSMA/CA** | Carrier Sense Multiple Access/Collision Avoidance |
| **CSMA/CD** | Carrier Sense Multiple Access/Collision Detection |
| **CTR** | Counter |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DIT** | Directory Information Tree |
| **DN** | Distinguished Name |
| **DNS** | Domain Name Server |
| **DSSS** | Direct Sequence Spread Spectrum |
| **EAP** | Extensible Authentication Protocol |

| | |
|---|---|
| **EAP-TLS** | Extensible Authentication Protocol-Transport Layer Security |
| **EAP-TTLS** | Extensible Authentication Protocol-Tunneled Transport Layer Security |
| **EEME** | Elektrik ve Elektronik Mühendisleri Enstitüsü |
| **ESS** | Extended Service Set |
| **FHSS** | Frequency Hopping Spread Spectrum |
| **FW** | Firewall |
| **Gbits** | Gigabit per second |
| **GHZ** | Giga Hertz |
| **GPL** | General Public License |
| **GTC** | Generic Token Card |
| **HTTPS** | Hyper Text Transfer Protocol |
| **IAS** | (Internet Authentication Server) |
| **IBSS** | Infrastructure Basic Services Set |
| **ICV** | Integrity Check Value |
| **ID** | Internet Draft |
| **IDS** | Intrusion Detection Systems |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention Systems |
| **IR** | Infrared |
| **ISM** | Industrial Scientific Medical |
| **LAN** | Local Area Network |
| **LDAP** | Lightweight Directory Access Protocol |
| **LDIF** | LDAP Data Interchange Format |
| **LEAP** | Lightweight EAP |
| **MAC** | Media Access Control |
| **MACSEC** | MAC SECURITY |
| **Mbits** | Megabit per second |
| **MD5** | Message Digest |
| **MERNİS** | Merkezî Nüfus İdare Sistemi |
| **MHZ** | Mega Hertz |
| **MIC** | Message Integrity Check |
| **MIMO** | Multi Input Multi Output |

| | |
|---|---|
| **MITM** | Man In The Middle Attack |
| **MKA** | Macsec Key Agreement Protocol |
| **MS-CHAP** | Microsoft-Challenge Handshake Authentication Protocol |
| **MSKÜ** | Muğla Sıtkı Koçman Üniversitesi |
| **MU-MIMO** | Multiple User MIMO |
| **NAS** | Network Access Server |
| **O** | Organization |
| **OFDM** | Orthogonal Frequency Division Multiplexing |
| **OSI** | Open Systems Interconnection |
| **OU** | Organizational Unit |
| **PACS** | Picture Archiving Communication Systems |
| **PAP** | Password Authentication Protocol |
| **PEAP** | Protected EAP |
| **PHP** | Hypertext Preprocessor |
| **PHY** | Physical Layer |
| **PPP** | Point-to-Point |
| **PSK** | Pre-Shared Key |
| **RADIUS** | Remote Authentication Dial-in User Service |
| **RAM** | Random Access Memory |
| **RC4** | Rivest Cipher 4 |
| **RF** | Radio Frequency |
| **RFC** | Request for Comments |
| **RRD** | Round Robin Database |
| **SFP** | Small Form Pluggable |
| **SMS** | Short Message Service |
| **SNMP** | Simple Network Management Protocol |
| **SQL** | Structured Query Language |
| **SSH** | Secure Shell |
| **SSID** | Service Set Identifier |
| **SSL** | Secure Socket Layer |
| **STA** | Station |
| **SU-MIMO** | Single User MIMO |
| **TCL** | Tool Command Language |
| **TCP/IP** | Transmission Control Protocol/Internet Protocol |
| **TELNET** | Telecommunication Network |

| | |
|---|---|
| **TGI** | Task Group I |
| **TGnSycn** | Task Group and Synchronization |
| **TKIP** | Temporal Key Integrity Protocol |
| **TÜBİTAK** | Ulakbim Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| **UCLA** | University Of California Los Angeles |
| **UDP** | User Datagram Protocol |
| **ULAKBİM** | Ulusal Akademik Ağ ve Bilgi Merkezi |
| **VLAN** | Virtual Local Area Network |
| **VoIP** | Voice over Internet Protocol |
| **WAN** | Word Area Network |
| **WEP** | Wired Equivalent Privacy |
| **Wi-Fi** | Wireless-Fidelity |
| **WiMAX** | Worldwide Interoperability for Microwave Access |
| **WLAN** | Wireless Local Area Network |
| **WLC** | Wireless Lan Controller |
| **WMAN** | Wireless Metropolitan Area Network |
| **WPA** | Wi-Fi Protected Access |
| **WPAN** | Wireless Personel Area Network |
| **WWAN** | Wireless Word Area Network |
| **WWISE** | Worldwide Spectrum Efficiency |

# 1. GİRİŞ

Aynı anda en az bir gönderici ve alıcının, bir iletim ortamı aracılığıyla haberleştiği yapıya ağ denir. Temel olarak bilgisayarları ve ağ cihazlarının birbirine bağlayan ve verinin bir istasyondan, başka bir istasyon ya da istasyonlara iletilebilmesini sağlayan yapı bütünüdür (Çetin ve Metin, 2005).

Bir kuruluş, bina, ev gibi belirli bir bölge içindeki bilgisayarların oluşturduğu bilgisayar ağları "Yerel Alan Ağı" (LAN-Local Area Network) olarak adlandırılır. Yerel alan ağ içerisindeki cihazları daha geniş ağlara bağlayan, çoğunlukla TCP/IP (Transmission Control Protocol/Internet Protocol) tabanlı ağa intranet denir. Intranetler ağ geçitleriyle haberleşerek, Geniş Alan Ağlarını (WAN- Wide Area Network) oluşturulur. Bilinen en büyük geniş alan ağı internettir.

İletişimin bakır kablo ve fiber optik gibi kablo üzerinden gerçekleştiği ağ türlerine kablolu ağ denir. İletişimin havada radyo frekansları ve kızıl ötesi ışınlar vasıtasıyla gerçekleştiği ağa ise kablosuz ağ denilmektedir.

Günümüzde kullanılan kablosuz ağların tarihine bakıldığında, ilk olarak 1970'li yıllarda Amerikalı mühendis ve akademisyen Norman Manuel Abramson tarafından Hawaii Üniversitesinde geliştirilen ALOHANET sistemi karşımıza çıkmaktadır. Sistem telefon kablosu kullanmadan merkezi bilgisayarla iletişim sağlayabilmek için 4 adaya konuşlandırılmış 7 bilgisayardan oluşmaktadır (Abramson, 2009).

ALOHA kanalları halen tüm önemli mobil şebekelerde ve neredeyse tüm çift yönlü uydu veri ağlarında kullanılmaktadır. Cep telefonu açıldığında veya bir sesli görüşme, kısa mesajlaşma ya da internet bağlantısı kurmak için telefon her kullanıldığında, ilk gönderilen paket, bir ALOHA rastgele erişimli kanal aracılığıyla gönderilir. Buna ek olarak ilk ALOHA Sistemi araştırması Los Angeles Kaliforniya Üniversitesi'nde (UCLA - University Of California Los Angeles) taşıyıcı duyarlı çoklu erişim (CSMA - Carrier Sense Multiple Access) üzerine yapılan çalışmadır. CSMA Ethernet, Wi-Fi (Wireless-Fidelity) ve WiMAX'te (Worldwide Interoperability for Microwave

Access) çarpışma önleme (CSMA / CA- Collision Avoidance) ve çarpışma algılama (CSMA/CD- Collision Detection) için teorik temel sağlamıştır (Abramson, 2009).

Kablosuz teknolojinin geçmişten günümüze kullanım alanı giderek artmaktadır. Ancak kablosuz ağların gelişimine bakıldığında 1990'lı yılların başlarında kablo kullanılmasının zor olduğu istisnai durumlar dışında, kablosuz cihazlar fazla tercih edilmemekteydi. Bu dönemde üreticiler, hedef kitlesini oluşturan kuruluş ve kampüs ortamlarına ürün satmakta zorlandılar. O günün şartlarında WLAN ürünleri yavaş, çok pahalı, hantal ve güç gereksinimi oldukça fazlaydı. Kablosuz ağ teknolojisinde ısrarcı davranan kurumlar ya iflas ettiler ya da küçülmeye gittiler. Bu noktaya kadar WLAN, LAN'ın yavaş ve güvenilmez bir alternatifi olarak gelişti (Negus ve Petrick, 2009).

Ancak 1990'ların sonlarında WLAN'lar için ilk önemli pazar fırsatı ortaya çıktı. Bu fırsat bugüne kadar WLAN endüstrisinin öngördüğünden büyük ölçüde farklıydı. Özellikle kişisel bilgisayarlar, oyun konsolları, VoIP (Voice over Internet Protocol) telefonlar, ev otomasyonları gibi ağ cihazlarının evlerde kullanılmaya başlanmasıyla, internet bağlantısının paylaşılabilmesi ihtiyacı ortaya çıktı. Bu noktadan sonra kablosuz ağ teknolojisinin şekillenmesinde son kullanıcıların ihtiyaçları önemli rol oynamaya başlamıştır (Negus ve Petrick, 2009).

Günümüzde kablosuz ağlar son kullanıcıların yanı sıra özel sektör ve kamu kurumlarının ihtiyaç ve beklentileri doğrultusunda şekillenmektedir. Bu beklentilerin en başında yönetilebilir ve güvenli kablosuz ağların oluşturulması gelmektedir. Üretici, geliştirici ve akademisyenlerin bu alanda ki çalışmaları durmaksızın devam etmektedir.

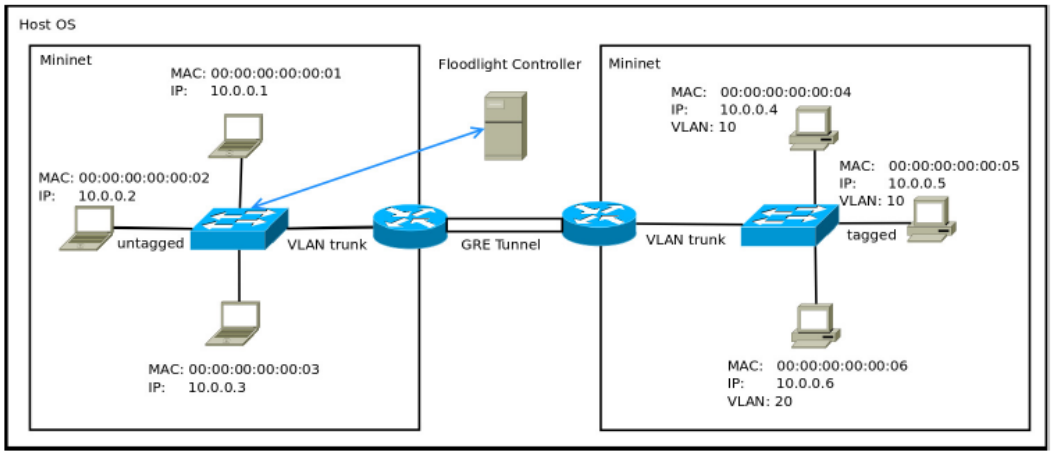
Kablosuz ağa kimin, nereden, nasıl ve hangi yetkilerle bağlanması gerektiği özenli bir planlama gerektirmektedir. Muğla Sıtkı Koçman Üniversitesi'nde Kasım 2009 yılından beri "eduroam" yayını anons edilmektedir (Tübitak, 2018). Bu tez kapsamında eduroam ağına öğrenci, personel ve misafirlerin ağa katılımında kural tabanlı dinamik VLAN ataması gerçekleştirilerek, ağda oluşan kullanıcı sayıları, trafik ve broadcast değerleri analiz edilmiştir.

## 1.1. Literatür Araştırması

Ning Jiang ve arkadaşları 2009 yılında yapmış oldukları çalışmalarında yardımcı VLAN konusu tartışılmış ve kampüs ağlarında IP telefon ve telefonun arkasında bulunan erişim portuna bağlı olarak çalışan bilgisayarın, tek bir port üzerinde farklı VLAN'a atanarak, ses trafiğinin önceliklendirilmesi üzerinde durmuştur (Jiang, Shan, ve Zhao, 2009). Çalışmalarında MAC adresi tabanlı VLAN atama işlemi gerçekleştirmişlerdir. Yardımcı VLAN yapılandırması kullanılarak kampüs ağında iki IP telefon arasında yüksek kaliteli ve kesintisiz ses iletimi sağlanmıştır.

Marc Koernera ve Odej Kaoa 2016 yılında "MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks" isimli çalışmalarında kampüs ağlarında VLAN yapılandırmasının öneminden bahsetmişlerdir. VLAN'ların bir ağın farklı kısımlara bölünmesi ve broadcast boyutunun azaltılması için oldukça yararlı bir araç olduğundan söz edilmiş ve genellikle bir kurum veya üniversitede bilgi işlem birimi tarafından, ağı farklı birimlere ayırmak için kullanıldığından bahsetmişlerdir.

Ayrıca kablolu ağlara bağlanan birçok cihazın (yazıcı, bilgisayar v.b.) sabit bir VLAN'a atandıklarının oysa kablosuz taşınabilir cihazların kampüste sık sık yer değiştirdiklerinden dolayı ilgili VLAN'a atanabilmeleri için dinamik VLAN eşleştirmesi kullanıldığından bahsetmişlerdir. Şekil 1.1.'de dinamik VLAN ataması yapılan network şeması bulunmaktadır. Analizlerin sonucunda mininet test yatağında, wireshark uygulaması ile akış tablolarını gözlemleyerek MAC tabanlı dinamik VLAN etiketlemesinin istikrarlı bir şekilde çalıştığı doğrulanmıştır (Koerner ve Kao, 2016).




**Şekil 1.1 Mininet test yatağı (Koerner ve Kao, 2016)**

Abdul Hameed ve Adnan Noor Mian 2012 yılında sundukları "Finding efficient VLAN topology for better broadcast containment" çalışmalarında dinamik VLAN ataması konusunda bir algoritma önermişlerdir. Daha iyi broadcast önlemesi için, birbirleri ile daha fazla veri alışverişinde bulunan cihazları aynı VLAN'a yerleştirirler. Ancak önceden veri toplanmadan ve trafik istatistiklerine dayanmadan yapılan VLAN atamaları ile daha kötü ağ performansına, dolayısıyla verimsiz VLAN yapısına neden olabileceğinden bahsedilmiştir. "The Simple Set-Based (Ss) Algorithm" adını verdikleri algoritma düğümlerin trafik komşuluklarına ve trafik miktarına göre oluşturulan bir matris üzerinde, birbirlerine yüksek trafik yapan düğümlerin aynı VLAN'da konumlandırılmaları üzerine kuruludur. Bu sayede birbirleri ile etkileşimi yüksek olan cihazların aynı VLAN'da olması, ağ performansında artışa neden olur ve broadcast önlemede verim elde edilir (Hameed ve Mian, 2012).

Asadullah Aktaş 2016 yılında sunduğu "Preventing Campus Network From Excessive Of Unwanted Packet Traffic Using VLAN Technology" isimli Yüksek Lisans tezinde, açık kaynak kodlu uygulamalar ve VLAN yapılandırması ile ağda istenmeyen trafiğin önlenmesi üzerine çalışmıştır. Açık kaynak kodlu ağ izleme yazılımı olarak Cacti ve Nedi uygulamalarından faydalanmıştır. VLAN yapılandırması sayesinde ARP (Address Resolution Protocol) ataklarının tüm networkü değil sadece ilgili VLAN'ı etkileyeceğinden bahsetmiştir (Aktaş, 2016).

Meriç Çetin'e ait 2006 yılında yayınlanan "Kurumsal Kampüs Ağlarında Otomatik Sanal Yerel Alan Ağ Tasarımları Ve Servis Kalitesi Analizleri" isimli yüksek lisans tezinde Pamukkale Üniversitesi Hastanesinde yapılan çalışma anlatılmıştır. Cihazlar hastane ağına dâhil olurken otomatik VLAN yapılandırması ve kimlik kontrolü işlemleri gerçekleştirilmiştir. IEEE (Institute of Electrical and Electronics Engineers) 802.1x protokolü ve Microsoft IAS (Internet Authentication Server) ve Microsoft Active Directory kullanılmıştır. Kullanıcılar ilgili oldukları alan ve departmanlara göre gruplanmış ve VLAN'lara bölünmüştür. 802.1x protokü ile kimlik doğrulayan kullanıcıların bilgisayarları PEAP/MS-CHAPv2 protokolüne göre ayarlanmıştır. Her kullanıcı kendisi ile ilgili VLAN'dan IP adresi almış, bu sayede sadece yetkili oldukları alanlarda ki bilgi ve belgelere ulaşmaları sağlanmıştır. Sonuç olarak yüksek risk oranına sahip hastane verilerinin, hastane içinden ve dışından güvenliği sağlanmış, ağa katılmak isteyen tüm cihazlar kimlik kontrolünden geçirilmiştir (Çetin, 2006).

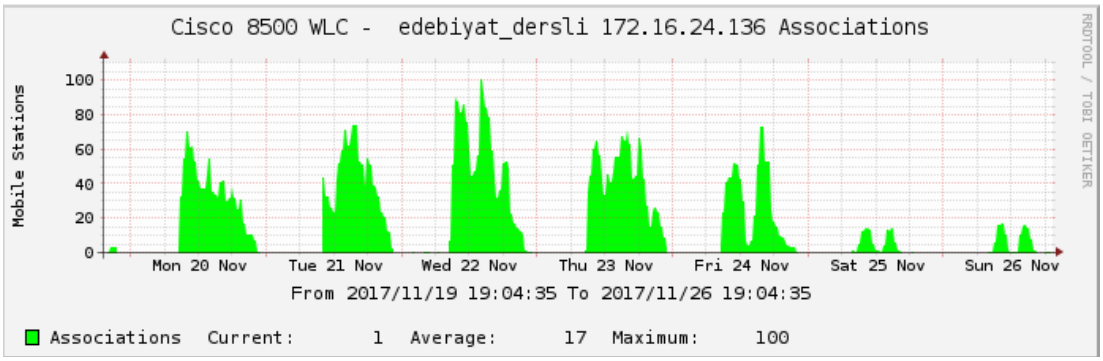
# 2. KABLOSUZ AĞLAR

## 2.1. Kablosuz Yerel Alan Ağının Avantajları:

Kuşkusuz kablosuz bir bağlantının en büyük avantajı, iletişimin gerçekleşebilmesi için kabloya ihtiyaç olmamasıdır. Kablodan bağımsız olunması hareketlilik ve dolaşım özgürlüğünü beraberinde getirmektedir. Özellikle kampüs ağlarında bir binanın mevcut kablolu (fiber optik/bakır vb.) bağlantısının kopması veya revize edilmesi durumunda geçici çözüm olarak noktadan noktaya (P2P-Peer to Peer) kablosuz bağlantı ile kullanıcıların ve ağ cihazlarının kesintisiz şekilde çevrim içi olmaları sağlanabilmektedir. Ayrıca kablo kullanımının mümkün olmadığı ya da fayda/maliyet oranının yüksek olduğu durumlarda kalıcı olarak, noktadan noktaya kablosuz köprü cihazları kullanılabilmektedir. Ayrıca WLAN, yapısal kablolama yapılması mümkün olmayan tarihi yapılarda sıklıkla tercih edilmektedir.

Günümüzde kenar anahtarlar genel olarak en çok 48 adet bakır portla birlikte 4 adet SFP (Small Form Pluggable) portlu üretilmektedir. Bu nedenle bir kenar anahtarına en çok 48 kullanıcı veya 52 (en az 1 port uplink olmalı) adet ağ cihazı bağlanabilmektedir. Ayrıca ağa dâhil olacak her cihaza uygun kabloma yapılması gerekmektedir.

WLAN'da ise bina içine (indoor) veya bina dışına (outdoor) bir erişim noktası (AP-Access Point) konumlandırılarak, belirli bir kapsama alanı içerisinde onlarca kullanıcı ağa bağlanabilmektedir. Şekil 2.1.'de MSKÜ ağında bir AP üzerinde bulunan kullanıcı sayısının grafiği gösterilmekte olup, 22.11.2017 tarihinde 100 adet kullanıcının bir AP üzerinden ağa dâhil olduğu gösterilmektedir.




**Şekil 2.1 Kullanıcı sayısı grafiği**

Üstelik bir AP'nin ağa dâhil olması için duvara veya tavana montajının yapılıp, en yakın kenar anahtarından 1 adet kablo çekilmesi yeterli olmaktadır. Ayrıca AP'ye kablo çekilmeden, başka bir AP üzerinden örgü (mesh) yapı ile kapsam alanı genişletilebilmektedir.

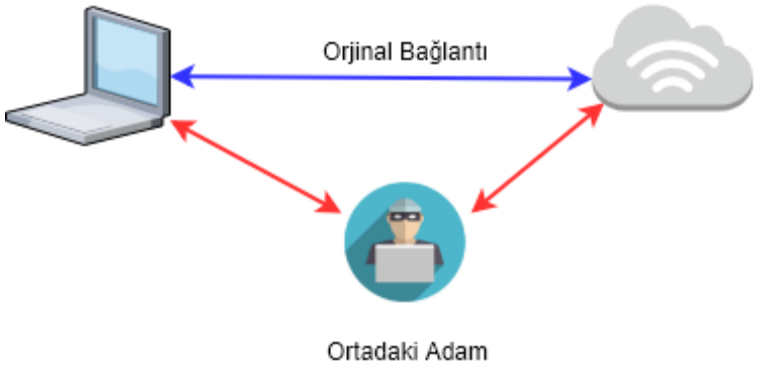
Özellikle son yıllarda gündeme gelen nesnelerin interneti (IoT-Internet of Things) kavramı ile günlük hayatta kullandığımız birçok cihaz akıllı hale gelmektedir. Şüphesiz kablosuz ağların bir başka faydası da, bu cihazlara erişim için kablo yerine kablosuz teknolojinin tercih edilecek olmasıdır.

## 2.2. Kablosuz Yerel Alan Ağının Dezavantajları:

Kullanılmaya başlandığı günden günümüze kadar gelen süreçte, kablosuz ağlar ile ilgili en büyük endişe güvenliktir. Kablosuz ağlarda iletişim radyo frekansları (RF-Radio Frequency) ile gerçekleşir. İletişimin gerçekleştiği ortam hava olduğu için trafiğin dinlenmesi ve çözümlenmesi mümkündür. Her ne kadar geçmişten günümüze değin güvenlik önlemleri ve şifreleme yöntemleri geliştirilmiş olsa da, bilinçsiz kullanım veya yanlış yapılandırmalardan dolayı her zaman bu güvenlik riski bulunmaktadır. Özellikle kurumsal yapılarda kullanıcıların yetkilendirilmesi için kimlik doğrulama senaryoları ve şifre politikaları iyi planlanması gereken konulardır.

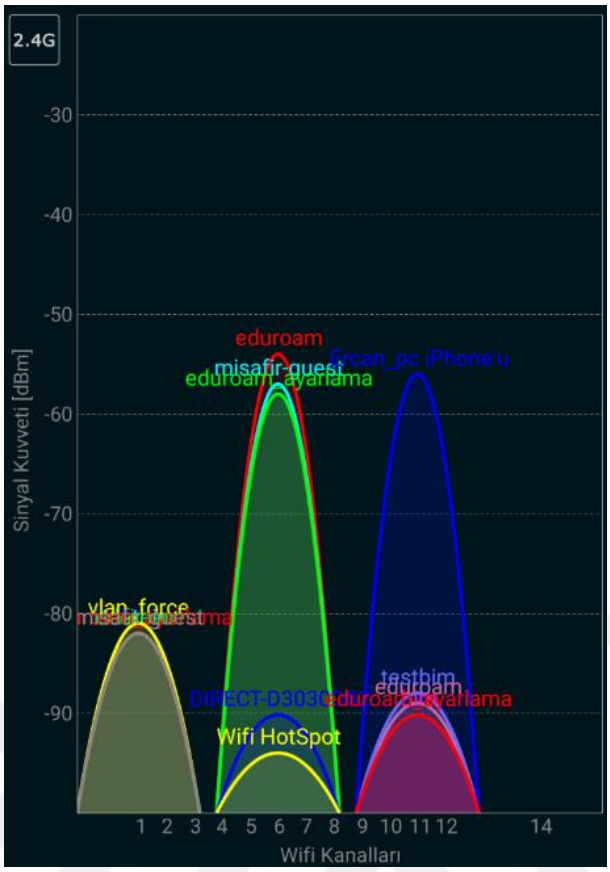
Ekim 2017 tarihinde "Mathy Vanhoef" tarafından "Key Reinstallation Attacks" adı verilen ve WPA2'de bulunan yeni bir açık ile kablosuz ağa dâhil olmadan, araya giren kişilerin "HTTPS" (Hyper Text Transfer Protocol) trafiğini dinleyebildiği ve şifrelerin açık (clear-text) olarak görüntülenebildiği duyurulmuştur. Saldırı yöntemi olarak MITM (Man In The Middle Attack - Ortadaki Adam Saldırısı) yöntemi kullanılmıştır

(Vanhoef, 2018). Bulanan bu yeni açıkla ilgili birçok üretici yeni güncelleme hazırlamakta ve anons etmektedir. Şekil 2.2.'de MITM yönteminin temel çalışma mantığı gösterilmektedir.




**Şekil 2.2 MITM**

Kablosuz ağlar ile ilgili bir diğer sorunda "girişim" yani enterferanstır. Telsiz, kablosuz telefon, uzaktan kontrol cihazları, bleutooth gibi birçok cihaz 2.4 GHz bandında yayın yapmaktadır. Bu band lisans gerektirmemesi, düşük güç tüketimi gibi avantajlarından dolayı çok tercih edilmektedir. WLAN'in bulunduğu ortamda bu bandı kullanan ve 2.4 GHz bandında yayın yapan diğer cihazların yoğunluğu nedeniyle, sinyalizasyonda oluşan karışıklığa "girişim" denir. Ayrıca çok sayıda WLAN cihazının aynı ortamda bulunması da, frekans aralıklarının paylaşılamamasına neden olmaktadır. Yani WLAN cihazları da birbirlerine karşı girişimde bulunabilmektedir. Şekil 2.3.'de, 2.4 Ghz bandında aynı kanallarda yayın yapan cihazların grafiği gösterilmektedir. Bu durum sadece 2.4 GHz bandında değil, 5 GHz bandında da gerçekleşmektedir.




**Şekil 2.3 2.4 GHz WLAN enterferansı**

Bir diğer değerlendirilmesi gereken konu kapsama alanıdır. WLAN'ların kapsama alanı, bina içi duvar kalınlığına, hatta eşyaların yerleşimine göre bile değişebilmektedir. Her ne kadar kazançlı ve yönlendirilebilen antenlerle iyileştirmeler yapılsa da, sistem tasarlanırken maksimum kapsama, minimum girişime göre tasarlanmalıdır. Aksi takdirde iletişim mesafesi ve kalitesi düşecektir.

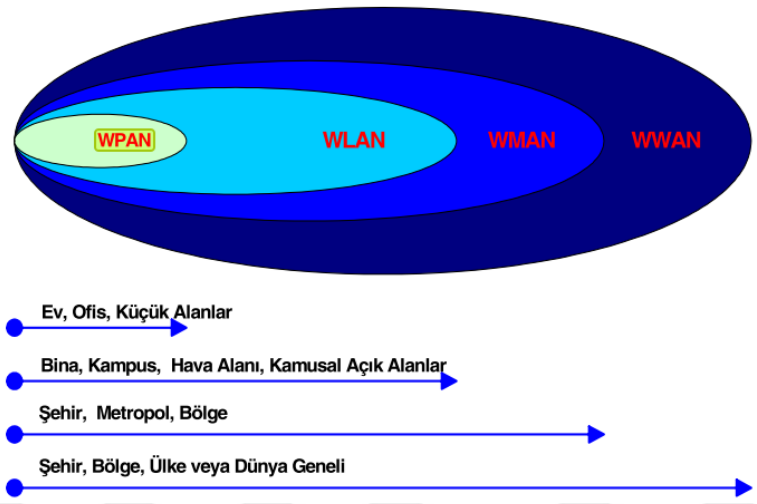
## 2.3. Büyüklüklerine Göre WLAN'lar:

Kablosuz yerel alan ağları tıpkı kablolu ağlarda olduğu gibi kapsamına göre sınıflandırılırlar. Bunlar;

- WPAN (Wireless Personel Area Network): Kişisel kullanım imkânı sağlayan genellikle ev ve ofis tarzı küçük ağlardır.
- WLAN (Wireless Local Area Network): Kurumsal bina, kampüs, havalimanı gibi heterojen kullanıcı ve cihaz yapısından oluşan ağlardır.

- WMAN (Wireless Metropolitan Area Network): Şehir ve bölgesel yayın yapılan ağlardır.
- WWAN (Wireless Word Area Network): Şehirler, bölgeler, ülke veya ülkeler arası yayın yapan ağlardır.

Büyüklüklerine göre WLAN'ların kapsama alanı şekil 2.4.'de verilmiştir.




**Şekil 2.4. Büyüklüklerine göre kablosuz ağlar (Öztürk, 2004)**

## 2.4. Kablosuz Ağ Topolojileri:

IEEE 802.11 standartlarını destekleyen, belirli kurallar ve fiziksel alt yapı mimarisi içerisinde, AP'ler ve kablosuz istasyonlarla (STAs-Stations) oluşturulan farklı kablosuz ağ topolojileri vardır. Her ne kadar kablosuz ağlar fiziksel kablodan bağımsızmış gibi düşünülse de, ağın daha büyük ağlara ve neticede internete ulaşması için ağın belirli bir kısmı için kablo kullanımı gerekmektedir. Bunların dışında kablo kullanılmadan daha dar kapsamda kurulan kablosuz ağ topolojileri de mevcuttur.

802.11 ağını oluşturan en küçük birim Temel Servis Kümesi (BSS-Basic Service Set)'dir. Temel Servis Kümesi birbirleri ile iletişim kuran istasyonlardan meydana gelir. Bir istasyonun diğer istasyonlar ile iletişimde kalabilmesi aynı BSS alanı içerisinde bulunması gerekir (Gast, 2005). 802.11 ağlarında Bağımsız BSS (Independent BSS) ve Alt yapılı BSS (Infrastructure BSS) olmak üzere iki farklı topoloji vardır.

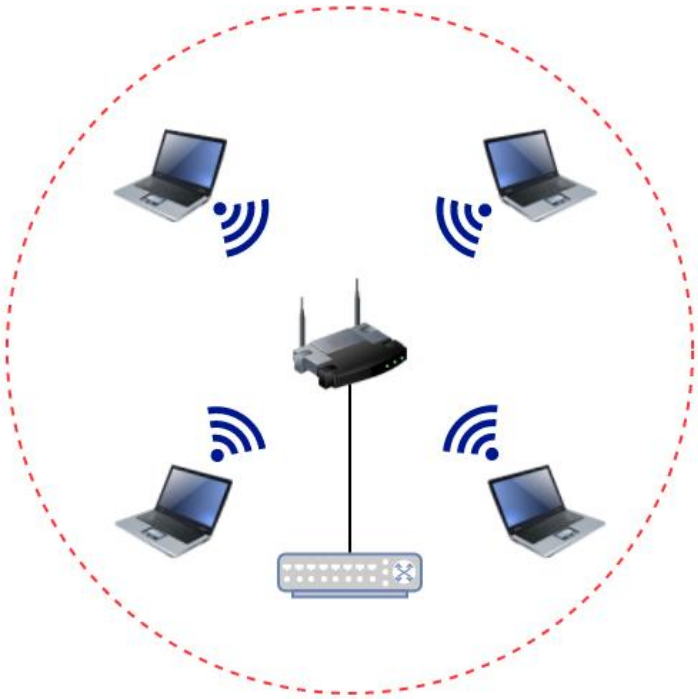
## 2.5. Bağımsız BSS:

Kablosuz bağdaştırıcısı olan en az 2 istasyonun aralarında başka bir ağ cihazı olmaksızın iletişim kurdukları kablosuz ağ tipidir. Ad-hoc ağ olarak da bilinen bu topolojide erişim noktası kullanılmaz. İstasyonların birbirleri ile iletişim kurabilecekleri mesafede bulunmaları gerekmektedir. Genelde geçici ve az sayıda istasyon için kurulan yapılardır (Gast, 2005). Şekil 2.5.'de Bağımsız BSS (Independent BSS/Ad-hoc) bağlantı şekli gösterilmiştir.

**Şekil 2.5. Bağımsız BSS**

## 2.6. Alt yapılı BSS:

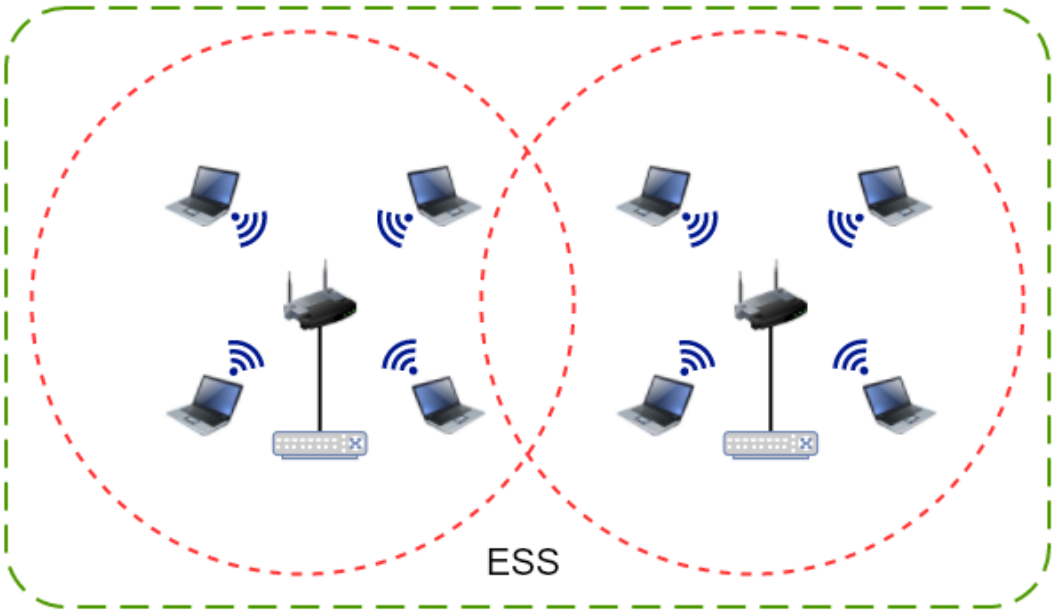
Alt yapılı modda kablosuz istasyonlar birbirleri ve diğer ağ cihazları ile AP üzerinden iletişim kurar. IBSS (Infrastructure Basic Services Set) dışına çıkıldığında ağ ile iletişim kesilir. Genellikle ev ofis gibi küçük ve kısa mesafeli yani dar kapsama alanlarında kullanılır. Şekil 2.6.'da alt yapılı BSS bağlantı şekli gösterilmiştir.



**Şekil 2.6. Alt yapılı BSS**

## 2.7. Genişletilmiş Servis Seti:

Birden fazla altyapılı BSS'nin birbirleri ile iletişim halinde oldukları yapılardır (Gast, 2005). ESS (Extended Service Set)'lerde birden fazla AP bulunur. Bu AP'ler birbirleri ile iletişime geçebilecek şekilde (mesh) ya da alt yapılı olarak hizmet verebilir. Böylece genişletilmiş servis alanı içerisinde kablosuz istasyonların hareket alanı genişler. BSS'ler birbirleriyle farklı alanlarda olabileceği gibi, kısmen de olsa yayın alanları örtüşebilir. Kullanıcıların bir erişim noktasından diğerine geçerek ağdan kopmadan dolaşımı sağlanır. Kampüs ağlarında AP'lerin sayısı yüzlerce olabileceğinden, genellikle kampüs ağlarındaki AP'ler merkezi bir kablosuz yerel ağ kontrolörü (WLC-Wireless LAN Controller) tarafından yönetilir. Şekil 2.7.'de genişletilmiş service setinin yapısı verilmiştir.




**Şekil 2.7. Genişletilmiş servis seti**

## 2.8. Servis Seti Tanımlayıcı:

Servis Seti Tanımlayıcı (SSID- Service Set Identifier) bir kablosuz cihaz tarafından anons edilen yayının adıdır. SSID ile ağa bağlanmak isteyen cihaz ve kullanıcılara ağın temel kimliğini bildirilir. SSID 32 karaktere kadar harf ve rakamlardan oluşabilir (Kösem, 2016). İstasyonlar ağa bu yayın adına göre bağlanırlar.

## 2.9. IEEE 802.11 Standart Ailesi:

İletişim çift yönlü haberleşme ile gerçekleşir. Doğru bir iletişimin gerçekleşebilmesi için tarafların aynı dili konuşması, yorumlaması ve anlayabilmesi gerekmektedir.

Bilgisayar ağlarında da durum farklı değildir. Bu yüzden farklı üreticilerin ürettikleri kablosuz ağ cihazlarının, aynı ağda birbirleri ile uyumlu çalışabilmeleri ihtiyacına binaen, IEEE 802.11 standart ailesi ortaya çıkmıştır. Bu standartlar 1997 yılından bu yana, uluslararası bir sivil toplum örgütü olan, Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE / EEME ) tarafından geliştirilmektedir (Verenkoff, 2011).

IEEE 802.11 bir dizi WLAN standartlarına verilen isimdir. Yıllar içerisinde farklı çalışma grupları ile bazı geliştirme ve düzenlemeler yapılmıştır. Bu düzenlemeler ile

yeni standartlar ortaya çıkmış ve bunlar 802.11x (x- yeni standardın harf grubu.) şeklinde ifade edilmiştir. Aşağıda kablosuz ağ alanında önemli değişiklikleri kapsayan 802.11 standartları anlatılmıştır.

## 2.10. 802.11:

İlk standart olan 802.11, ISM (Industrial Scientific Medical) bandları olarak adlandırılan 2.4 GHz (2.4 -2.4835) ile 5 GHz (5.15 – 5.825) bandındaki düzenlemeler tanımlanmıştır.

Öncelikle fiziksel katman için (PHY-Physical Layer) 3 özellik tanımlanmıştır. Bu özelliklerden ikisi 2.4 GHz taşıyıcıya sahip radyo tabanlı PHY'leri tanımlanmıştır. İlki, frekans atlamalı yayılma spektrumu (FHSS - Frequency Hopping Spread Spectrum) PHY iken, diğeri direkt dizi yayılım spektrumu (DSSS - Direct Sequence Spread Spectrum) PHY' dir. Son olarak da temel bantta çalışan kızıl ötesi (IR- Infrared) PHY tanımlanmıştır. Tanımlanan bu katmanların tümü 1Mbps (Megabits per second) ve 2 Mbps hızlarını desteklemektedir (Paul ve Ogunfunmi, 2008).

## 2.11. 802.11a:

80211a standardı 1999 yılında duyurulmuştur. 802.11b'den farklı olarak 5 GHz bandında çalışmakta ve 54 Mbps'e kadar bant genişliği desteklenmektedir. Hız ve kapasite gerektiren alanlarda kullanılması düşünülen bu standardı destekleyen ürünlerin donanımsal açıdan pahalı olması, 5 GHz bandını kullanması ve 802.11b standardını destekleyen ürünlerin popülerliği nedeniyle son kullanıcı pazarında fazla yer edinememiştir.

## 2.12. 802.11b:

1999 yılında 2 değişiklikle birlikte 802.11b standardı duyurulmuştur. CCK (Complementary Code Keying) modülasyon şeması kullanılarak 5 Mbps'den 11 Mbps'e kadar bağlantı hızı sağlanmıştır (Paul ve Ogunfunmi, 2008). Kullanıcılar

802.11b standardını sağlayan ürünleri ev ve ofis gibi mekânlarda sıklıkla tercih etmiş ve yaygın kabul görmüştür.

### 2.13. 802.11g:

802.11b'nin ardından 2003 yılında 802.11g standardı duyurulmuştur. Bu standartta temel amaç performans artışı sağlarken geriye doğru uyumluluk desteğinin verilmesidir. 2.4 GHz frekansında çalışırken, modülasyon tekniği olarak 802.11a'da olduğu gibi OFDM (Orthogonal Frequency Division Multiplexing) tekniği kullanılmıştır. Sonuç olarak 54 Mbps bant genişliği elde edilmiş ve yaygın olarak kullanılmıştır (Verenkoff, 2011).

### 2.14. 802.11n:

2.4 GHz ve 5.2 GHz'i destekleyebilen cihazların üretim pazardaki 802.11b'den 802.11a ürünlerine geçişi engellemiştir. 2003 yılının sonlarına doğru IEEE tarafından 802.11n için çalışma grupları oluşturulmuştur. Başlangıçta amaç 100 Mbit/s bağlantı hızının sağlanmasıdır (Paul ve Ogunfunmi, 2008).

Teklifler arasında Worldwide Spectrum Efficiency (WWISE) tarafından 802.11b/g standardına benzer (20 Mhz) bant genişliği olan kanallar üzerinden çoklu giriş ve çoklu çıkış (MIMO - Multi Input Multi Output) yöntemi ile 135 Mbps bant genişliği önerilmiştir. Bir diğer çalışma grubu Task Group and Synchronization (TGnSycn) ise 40 MHz (MegaHertz) bant genişliği ile 315 Mbps bant genişliği vadetmiştir. Teklifler arasından sona kalan bu iki öneri grubu arasından oluşturulan ortak bir çalışma grubu ile her iki teklifin faydalı yönlerinin birleştirilmesi kararı alınmıştır (Paul ve Ogunfunmi, 2008).

802.11n standardında temel olarak iki önemli yenilik getirilmiştir. Bunlar 40 MHz bant genişliği frekansı ve MIMO kullanımıdır. MIMO gönderici ve alıcı üzerinde bulunan çoklu antenler aracılığıyla aynı anda farklı sinyallerin gönderilip alınmasına olanak sağlar. Bir anten ve bir uzaysal akıştan 4 anten ve 4 uzaysal akış çoğullama tekniğiyle veri aktarım oranı 4 kat artmıştır (Perahia, 2008).

802.11n ile 2.4 GHz ve 5.2 GHz bandı desteği sağlanmıştır. Böylece geriye dönük 802.11a/b/g standardını destekleyen cihazlar ile uyumlu olarak çalışabilmektedir. Ancak bu standartta yakalanabilecek en fazla bant genişliği gönderici ve alıcının MIMO sayısına göre değişmektedir. Farklı MIMO sayısına sahip gönderici-alıcı çiftlerinin oluşturduğu trafik, düşük MIMO sayısına göre gerçekleşmektedir. Çizelge 2.1.'de 802.11n standardında, MIMO sayılarına göre ulaşılabilen en düşük ve en yüksek bant genişlikleri gösterilmektedir (Soy, Özdemir, ve Bayrak, 2013).

**Çizelge 2.1 802.11n MIMO sayısı ve bant genişliği**

| MIMO Sayısı | Maksimum Hız (20 MHz) | Maksimum Hız (40 MHz) |
|---|---|---|
| 1x1 | 65-72 Mbps | 150 Mbps |
| 2x2 | 130-144 Mbps | 300 Mbps |
| 3x3 | 195-216 Mbps | 450 Mbps |
| 4x4 | 260-288 Mbps | 600 Mbps |

## 2.15. 80211.ac:

Günümüzde taşınabilir cihaz sayısındaki hızlı artış beraberinde yüksek çözünürlüklü video yayınları, bulut depolama ve sosyal medyanın yoğun kullanımı ile kablosuz ağlarda yüksek verimlilik ve bant genişliği ihtiyacını artırmıştır.

Yüksek verimlik ve daha fazla kullanıcıya hizmet verme noktasındaki ihtiyaçların karşılanması için 2008 yılında IEEE 802.11ac çalışma grubu oluşturulmuş ve 2013 yılında standart hale gelmiştir (IEEE, 2018b). 802.11ac ile birlikte kablosuz ağların performansı kablolu ağlar ile kıyaslanabilir hale gelmiştir. Aynı zamanda geriye doğru uyumluluk söz konusu olup 802.11b/g/n destekli cihazlar ile aynı ortamda kullanılabilmektedir (Güleryüz, 2016).

802.11n'de kullanılan MIMO tekniği ile bir cihaz aynı anda birden fazla uzaysal akıştan veri gönderebilir, ancak yalnızca tek bir adrese (cihaza) yönlendirebilir (SU-MIMO - Single User MIMO). 802.11ac ile kullanılmaya başlayan MU-MIMO (Multiple User MIMO) tekniği ile bir AP aynı anda aynı frekans spektrumundan farklı kullanıcılara hizmet verebilmektedir (Cisco Systems, 2018b).

802.11a/n/ac destekli cihazların MIMO sayılarına göre 20,40,80 ve 160 MHz frekanslarında teorik olarak ulaşılabilecek bağlantı değerleri çizelge 2.2.'de gösterilmektedir (Cisco Systems, 2018a).

**Çizelge 2.2. 802.11ac örnek yapılandırmaları**

| 802.11a/n/ac ürünler | Bandwith (MHz) | Uzaysal Akış | PHY Data Rate (Mbps) |
|---|---|---|---|
| **802.11a** | | | |
| Tümü | 20 | 1 | 54 |
| **802.11n** | | | |
| Minimum İyileştirme | 20 | 1 | 65 |
| Alt Seviye Ürün(2.4 Ghz) | 20 | 1 | 72 |
| Orta Seviye Ürünler | 40 | 2 | 300 |
| Üst Seviye Ürünler | 40 | 3 | 450 |
| Maksimum İyileştirme | 40 | 4 | 600 |
| **802.11ac 80 MHz** | | | |
| Minimum İyileştirme | 80 | 1 | 293 |
| Alt Seviye Ürünler | 80 | 1 | 433 |
| Orta Seviye Ürünler | 80 | 2 | 867 |
| Üst Seviye Ürünler | 80 | 3 | 1300 |
| Maksimum İyileştirme | 80 | 8 | 3470 |
| **802.11ac 160 MHz** | | | |
| Alt Seviye Ürünler | 160 | 1 | 867 |
| Orta Seviye Ürünler | 160 | 2 | 1730 |
| Üst Seviye Ürünler | 160 | 3 | 2600 |
| Ultra Üst Seviye Ürünler | 160 | 4 | 3470 |
| Maksimum İyileştirme | 160 | 8 | 6930 |

## 2.16. Kablosuz Ağlarda Güvenlik:

Kablolu ağlarda veri dış ortamdan yalıtılmış olan bir iletim hattı üzerinden iletilir. Kablosuz ağlarda ise radyo frekansları aracılığıyla havada taşınır. Kuşkusuz kablolu ağlara oranla, kablosuz iletişimin güvenliğini sağlamak için daha fazla çaba ve farklı güvenlik önlemleri gerekmektedir.

Güvenli bir iletişimden söz edebilmek için verinin doğruluğu, bütünlüğü ve gizliliğinin sağlanması gerekmektedir. İletişimin gönderici ve alıcı olmak üzere iki paydaşı vardır. Verinin doğruluğunun sağlanabilmesi için iletiminden önce gönderici ve alıcının kimliğinin net bir şekilde doğrulanması gerekir. Gönderilen veya alınan verinin doğru

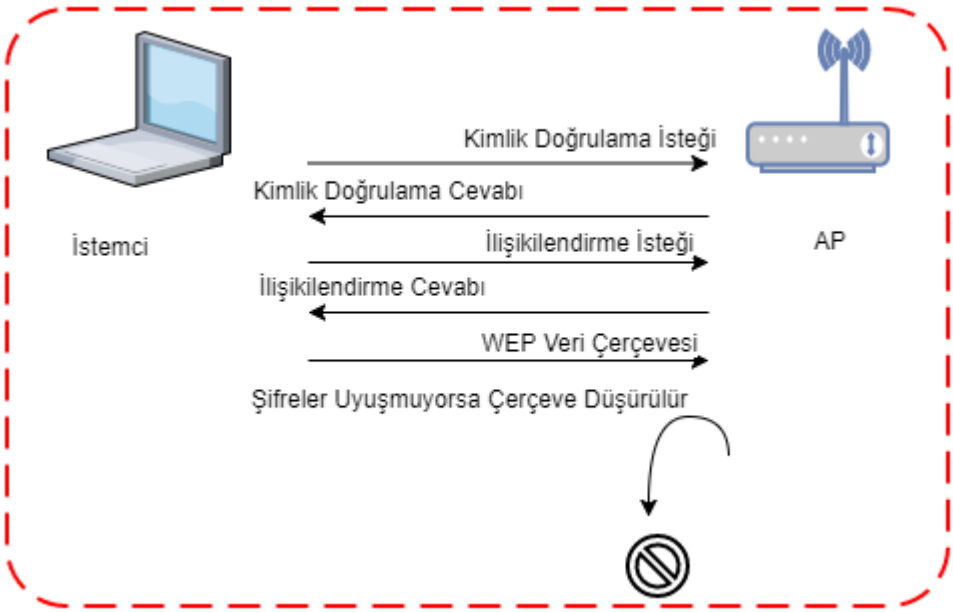
ve eksiksiz olarak iletilmesi, iletişimin bütünlüğü olarak ifade edilir. İletişim esnasında verinin üçüncü bir kaynak tarafından, izlenmeden ve değiştirilmeden gönderilmesi ise iletişimin gizliği ile ilgilidir. Ancak bu şartların sağlanması ile sürdürülebilir ve güvenli bir iletişimden söz edilebilir.

## 2.17. Kablosuz Ağlarda Kimlik Doğrulama Yöntemleri:

Kablosuz ağ standartlarının gelişmesiyle birlikte hız kazanan kablosuz ağ kullanımı, gizlilik ve güvenlik gereksinimlerini de beraberinde getirmiştir. Geçmişten günümüze kadar birçok şifreleme yöntemi geliştirilmiştir. Bu yöntemlerin zafiyetlerinin tespit edilmesinin ardından, daha güvenli şifreleme algoritmalarını geliştirilmiştir. IEEE tarafından 802.11 ağları için açık sistem (Open System) ve Paylaşılan anahtar (Shared Key) olmak üzere iki farklı kimlik doğrulama yöntemi tanımlanmıştır (Chen, Jiang, ve Liu, 2005).

## 2.18. Açık Sistem Kimlik Doğrulama:

Açık sistem yapısında kullanıcı ile AP arasında MAC adresi temeline dayanan bir kimlik iletimi söz konusudur. Kullanıcı kimlik bilgisini içeren bir doğrulama isteği gönderir ve AP kimlik doğrulama isteğini yanıtlar. Bu süreç cihazların birbirleri ile iletişime geçmesi, kimliklerini paylaşması, yani tanışmasıdır. Kullanıcının ağa erişimi için bir WEP anahtarına sahip olup olmadığı kontrol edilir. WEP anahtarı eşleşmesi başarılı olursa ağda oturum açılır, aksi halde iletişim sonlandırılır (Cisco Systems, 2018c). Açık sistem kimlik doğrulamasının çalışma prensibi şekil 2.8'de verilmiştir.



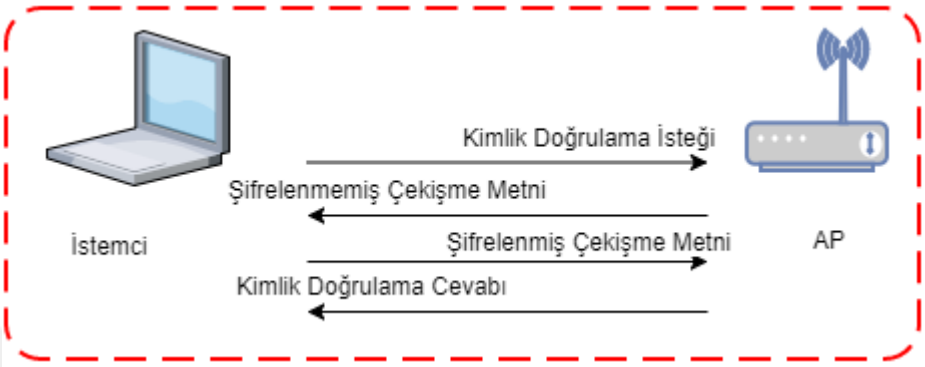

**Şekil 2.8. Açık sistem kimlik doğrulama**

802.11 ağlarının erken dönemlerinde kullanılan bu yöntemin zayıflıkları nedeniyle ilave bazı önlemler ile birlikte kullanılmıştır. Bazı erişim noktaları güvenliği artırmak için MAC adresi doğrulaması gerçekleştirmektedir. Ağa dahil olacak cihazların MAC adresleri cihaz içerisinde tanımlanır. Ancak bu yöntem de güvenliği sağlamakta yetersizdir. MAC adresleri günümüzde kolay ulaşılabilen yazılımlarla değiştirilebilmektedirler. Ayrıca arada gerçekleşen veri trafiğinde herhangi bir şifreleme gerçekleşmediği için kolaylıkla dinlenebilmektedirler. Bu yüzden tam anlamıyla bir kimlik doğrulama yöntemi olduğu söylenemez.

## 2.19. Paylaşılan Anahtar Kimlik Doğrulaması:

Paylaşılan anahtar kimlik doğrulamasında istemci (Supplicant) ile AP arasında 4 farklı mesaj iletimi gerçekleşir (Chen vd., 2005). İstemci kimlik bilgilerini içeren bir mesajı AP'ye gönderir. AP bir sınama metni ile kimlik doğrulaması isteyen istemciye yanıt verir. İstemci gelen metni paylaşılan WEP anahtarını kullanarak metinden elde ettiği sonucu şifreleyerek AP'ye geri gönderir. Eğer istemci WEP anahtarını yanlış girerse ya da anahtara sahip değilse kimlik doğrulama başarısız olur ve istemcinin ağa dahil olmasına izin verilmez. Şayet gelen yanıt doğru anahtarla şifrelenmiş ise oturum açma başarılı bir şekilde gerçekleşir.

Paylaşılan kimlik doğrulaması yöntemi gizli bir anahtarın kullanılarak metinlerin şifrelenmesi ve çözümlenmesi ile gerçekleşir. Yanlış anahtar kullanım sınırlaması bulunmadığından iyi bir sözlüğü bulunan brute force (kaba güç) saldırıları ile gizli anahtarı elde etmek mümkündür. Ayrıca WEP anahtarı kullanılması nedeniyle WEP algoritmasının tüm zaaflarından etkilenmektedir. Paylaşılan Anahtar Kimlik Doğrulamasının çalışma mantığı şekil 2.9'da verilmiştir.




**Şekil 2.9. Paylaşılan anahtar kimlik doğrulaması (Cisco Systems, 2018c)**

## 2.20. Kabloluya Eşdeğer Gizlilik:

Kullanılmaya başlandığı zamandan günümüze kadar 802.11 ağlarında en büyük endişeler güvenlik ve gizliliktir. WEP (Wired Equivalent Privacy) şifrelemesi 802.11 ağların da gizlilik, erişim denetimi ve veri bütünlüğünü sağlamak için IEEE gönüllülerince geliştirilmiştir (Wong, 2003).

Genellikle, kablosuz aygıtlarda kullanılan çoğu şifreleme RC4 (Rivest Cipher 4) gibi simetrik anahtar şifrelemesine dayanır. RC4, 1987'de Ron Rivest tarafından tasarlanan bir akış şifresidir ve 802.11 WEP'de kullanılmıştır. Verileri şifrelemek için 40 bitlik WEP anahtarı ve 24 bitlik rastsal olarak üretilen başlangıç vektörü (IV- Initial Vector) birleştirilerek 64 bitlik bir akış elde edilir. Gönderilecek olan veri (plaintext) bu 64 bitlik anahtar ile XOR işlemine tabi tutulur ve şifrelenmiş veri (ciphertext) elde edilir. RC4 hızlı ve etkili bir algoritmadır, yalnızca birkaç satırlık kod kullanılarak yazılabilir ve 256 bayt rasgele erişimli bellek alanı (RAM - Random Access Memory) gerekir (Yao, Jiang, ve Wang, 2010).

Bununla birlikte, Fluhrer ve birçok araştırmacı RC4 algoritmasında bazı güvenlik açıkları keşfetmişlerdir. 2001 yılından itibaren ciddi zafiyetler bulunmuş ve WEP

şifrelemesinin birçok alanda savunmasız olduğu görülmüştür. 40 bitlik veya 104 bitlik anahtarın iki veya üç saat içerisinde kırılabildiği belirtilmiştir ( Yao, Jiang, ve Wang, 2010). Sonuç olarak kabloya eşdeğer gizliliği hedefleyen WEP, bu amaca ulaşamadığı için, zafiyetlere çözüm getirmek amacıyla WPA şifrelemesi geliştirilmiştir.

## 2.21. WPA:

802.11 WEP şifrelemesinde bulunan güvenlik açıkları nedeniyle IEEE tarafından 802.11i standardı için 2001 Mayıs ayında Görev Gücü I isimli çalışma grubu oluşturulmuştur (IEEE, 2018c). Ancak kablosuz endüstrisi yeni standardın onaylanmasını beklemeden, 802.11'in güvenlik açıklarını kapatabilecek ara bir çözüm arayışına girmişlerdir. IEEE ile birlikte Wi-Fi Alliance, WPA (Wi-Fi Protected Access) olarak bilinen güvenlik protokolü üzerinde anlaşmıştır. Wi-Fi Alliance 1999 yılında kurulan, kâr amacı gütmeyen ve endüstride üretilen farklı kablosuz cihazların bir arada çalışabilirliğini amaçlayan bir kuruluştur. 2018 Mart ayı itibariyle 720'nin üzerinde cihaz üreticisi kuruluşa üye olmuştur ve 30.000'nin üzerinde ürün Wi-Fi sertifikası almıştır (Wi-Fi Alliance, 2005).

WPA ile donanımsal bir güncelleme yapılmaksızın, sadece yazılım güncellemesi ile daha güvenli bir kablosuz iletişim hedeflenmiştir. Bunu yaparken WEP'te kullanılan RC4 algoritması gibi Geçici Anahtar Bütünlük Protokolü (TKIP -Temporal Key Integrity Protocol) ve Mesaj Bütünlüğü Kontrolü (MIC - Message Integrity Check) kullanılmıştır. Ayrıca, IEEE 802.1x Genişletilebilir Kimlik Doğrulama Protokolü (EAP - Extensible Authentication Protocol) veya önceden paylaşılan anahtar (PSK-Pre-Shared Key) mimarisi kullanılarak, karşılıklı kimlik doğrulama şeması sağlanmaktadır. 802.1X ile kurumsal yapılar için kimlik doğrulama sunucusu marifetiyle, kullanıcı veri tabanı üzerinden doğrulama imkanı sunarken, PSK mimarisi ev, ofis ve küçük işletmeler gibi az kullanıcısı olan yerler için tasarlanmıştır (Wi-Fi Alliance, 2005).

WPA'da WEP'in aksine başlangıç vektörü 48 bite, geçici anahtar ise 128 bite çıkarılmıştır. Her paket için ayrı başlangıç vektörü ve ayrı geçici anahtar üretilerek şifrelenir. Mesaj bütünlüğünü sağlamak için Michael (MIC-Message Integrity Code) adı verilen sağlama algoritmasını kullanır. Ara bir çözüm olarak geliştirilen WPA,

dönemin güvenlik ihtiyaçlarını en az maliyetle karşılamayı başarsa da, yapılan incelemelerde bazı güvenlik açıkları tespit edilmiştir. IEEE 802.11i'nin duyurulmasıyla birlikte yerini WPA2'ye bırakmıştır. Ancak günümüzde 802.11i standardından önce üretilmiş olan donanımlar hala kullanılmaya devam edilmektedir.

## 2.22. WPA2:

IEEE TGi grubu tarafından geliştirilen 802.11i standardı 2004 Haziran ayında onaylanmıştır (IEEE, 2018c). WPA gibi 802.1X ve PSK'yı desteklemekle birlikte, yeni şifreleme ve kimlik doğrulama algoritmaları ile oldukça güvenilir bir alt yapı sağlamıştır. Gerçek anlamda kimlik doğrulaması sağlayan bir yapıya göre tasarlanmıştır. WPA2-Enterprise ile kurumsal yapılarda her kullanıcı için ayrı ayrı kimlik doğrulama ve yetkilendirme imkânı sağlar. Kullanıcılar cihazlarına kurulan 802.1X destekli bir yazılım ile (supplicant), ağ yöneticisi tarafından belirlenen EAP versiyonuna göre ağa dahil olurlar. Supplicant ile AP arasında karşılıklı kimlik doğrulaması gerektiren 802.1x kimlik doğrulama yöntemi kullanılmaktadır.

WPA2 Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard) ile kullanıcı ile AP arasındaki veriyi şifreler. AES sabit uzunlukta bit gruplarından oluşan simetrik blok şifre yapısındadır. 128 bitlik veriler 128, 192 ve 256 bit olabilen anahtar şifresi ile hem şifreleme, hem de şifre çözme işlemleri gerçekleştirilir. AES şifreleme, bir turu oluşturan 4 aşamayı içerir. Her tur, bit anahtar boyutuna bağlı olarak 10, 12 veya 14 kez yinelenir. AES'in WPA2/802.11i uygulaması için, her tur 10 kez yinelenir.

Ayrıca AES, Sayaç Modu isimli (CCMP- Counter Mode Cipher Block Chaining Message Authentication Code Protocol) hem şifreleme hem de kimlik doğrulama için tek bir anahtarın kullanılmasına olanak tanıyan bir protokoldür**.** Gönderici ve alıcı tarafından bilinen anahtar ile şifreleme ve çözümleme yapılır. Veri bütünlüğünü sağlamak için veri şifrelemeyi Sayıcı modu (CTR-Counter) gerçekleştirir. Doğrulamayı ise Şifreleme Blok Zincirleme Mesaj Doğrulama Kodu (CBC-MAC-Cipher Block Chaining Message Authentication Code) sağlar (Öztürk, 2004).

Bir donanımın WPA2'yi destekleyebilmesi için üretilirken bu yapıya uygun olarak üretilmesi gerekir. WPA'da olduğu gibi yazılım güncellemesi ile destek sağlanamaz. 802.11i geriye dönük WPA-EAP, WPA-PSK yapılarını desteklemekle birlikte,

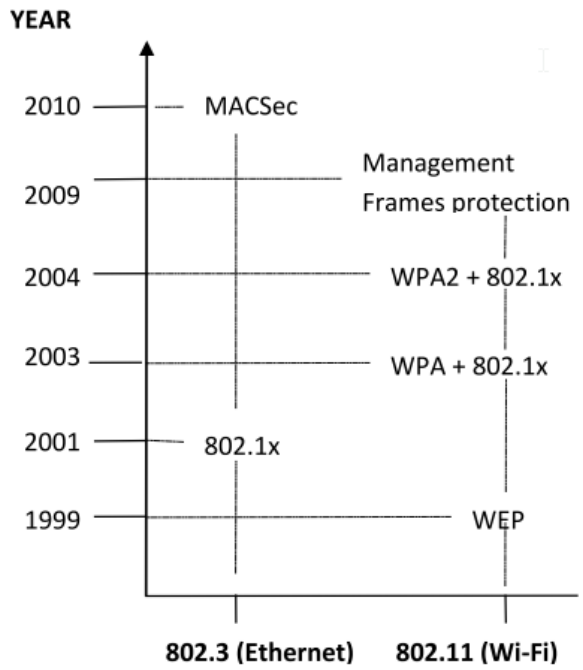
WPA'dan WPA2'ye geçiş sürecinde olan ağlar için Mixed Mode (Karma Mod) denilen her iki yapıyı da destekleyen CCMP veya TKIP ağları oluşturmak mümkündür (Wi-Fi Alliance, 2005).

WPA2'nin başka bir özelliği de kablosuz ağlarda dolaşım imkanı sağlamasıdır. Özellikle kurumsal kampüs ağlarında kablosuz cihaz bir AP'ye bağlı ve hareket halindeyken, kendisine yakın diğer bir AP'yi algılarsa 802.1x anahtar değişimi ile yeni AP için anahtarları elde eder ve hafızaya alır. Böylece 802.1x kimlik denetiminin yeniden yapılmasına gerek kalmaz (Köksal, 2007).

## 2.23. 802.1x Port Tabanlı Ağ Erişim Kontrol Protokolü:

Bilgisayar ağlarının yaygın olarak kullanılmaya başlanması ile birlikte açıkların bulunmasında bilimsel araştırmaların yanı sıra, saldırgan (hacker) kişi ve grupların maddi kazanç beklentisi veya bilişim vandalizmi duygularını tatmin etme isteği de rol oynamaktadır. Bulunan bu açıklara IEEE yıllar boyunca güvenlik standartları geliştirmiştir. Her bir standart bir sonraki standardın basamağını oluşturmuştur.

IEEE tarafından geliştirilen 802.1x, port tabanlı ağ erişimi ve kontrolü sağlayan standarttır. 2001 yılında kablolu ağlar için tasarlanmış ve 2004 yılında 802.11 ağlarının yaygınlaşması ile birlikte 802.1x-2004 projesi ile güncellenmiştir. 802.1x-2004 ile 802.11 ağlarında karşılıklı kimlik doğrulamada Genişletilebilir Kimlik Doğrulama Protokolü (EAP- Extensible Authentication Protocol) kullanımına başlanmıştır. WG802.1 - Higher Layer LAN Protocols Working Group tarafından 2010 yılında 802.1x-2010 projesi ile yeniden düzenlenmiştir. 802.1x-2010, IEEE 802.1AE (MACSec olarak bilinir) MAC güvenliğini desteklemiştir. Bu güncelleme ile kimliği doğrulanmış anahtar desteği (MKA - Macsec Key Agreement Protocol) getirilmiştir (IEEE Computer Society: LAN/MAN Standards Committee, 2010). 2014 yılında yapılan yeni bir iyileştirme ile numaralandırılmış paket özelliği sağlayan 802.1AEbw desteği, ek güvenlik ve yönetilebilirlik özelliklerini desteklemek amacıyla MKA genişletilmiştir (IEEE Computer Society: LAN/MAN Standards Committee, 2014). Kablolu ve kablosuz ağlarda geçmişten günümüze kadar kullanılan güvenlik standartlarının yıllara göre değişimi Şekil 2.10' da gösterilmektedir.




**Şekil 2.10. Yıllara göre güvenlik standartlarının gelişimi (Abreha, 2016)**

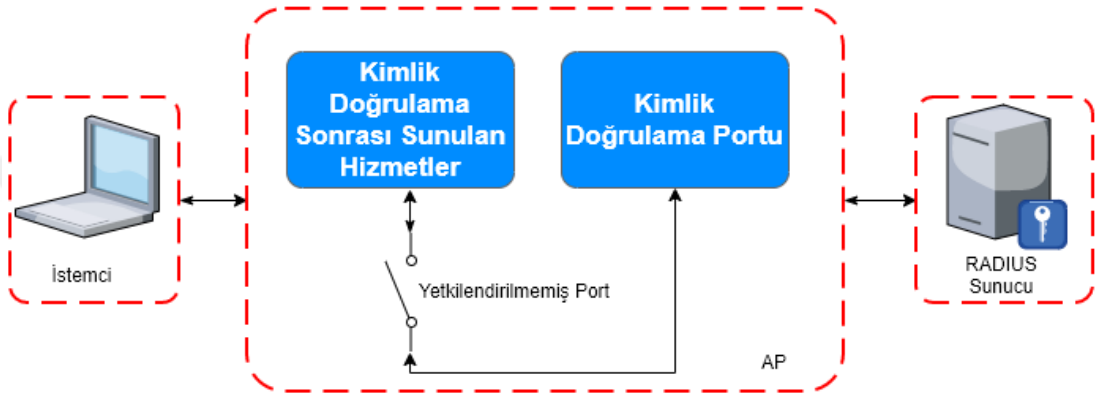
Kablosuz ağlarda kullanılan kimlik doğrulama şifre ve algoritma standartlarının karşılaştırması çizelge 2.3.'de verilmiştir.

**Çizelge 2.3 Standartların karşılaştırılması**

| | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| **Şifreleme Algoritması** | RC4 | TKIP/RC4 | CCMP/AES CCMP/TKIP |
| **Şifreleme Anahtarı** | 40 Bit | 128 Bit | 128 Bit |
| **Başlangıç Vektörü** | 24 Bit | 48 Bit | 48 Bit |
| **Anahtar Değişikliği** | Sabit Anahtar | Her oturum için anahtar değişir. | Anahtar değişimine ihtiyaç yoktur |
| **Anahtar Yöntemi** | Yok | 802.1x | 802.1x |
| **Kimlik Doğrulama** | Zayıf | 802.1x EAP | 802.1x EAP |
| **Veri Bütünlüğü** | ICV | MIC | MIC |

Güvenli bir ağın temel bileşenleri kimlik doğrulama, erişim kontrolü ve veri bütünlüğüdür. Veri bütünlüğünün sağlanması ilk iki parametre olan kimlik doğrulama ve erişim kontrolü ile mümkün olabilir. 802.1x kuruluş modunda kullanıldığında 802.1x / EAP mekanizması ile karşılıklı kimlik doğrulama, anahtar üretimi ve değişimi hiyerarşisi sağlanır. IEEE 802.1x mimarisi, kimlik doğrulayıcı (AP), istemci ve kimlik doğrulama sunucusu (genellikle RADIUS- Remote Authentication Dial-in User Service) olmak üzere üç temel bileşenden oluşur. Kimlik doğrulayıcı istemciyi kimlik doğrulamaya zorlar. Kimlik doğrulayıcı ile istemci arasında birisi kontrol edilen,

diğeri kontrol edilmeyen iki mantıksal port bulunur. Kontrolsüz port (Unauthrized Port) istemcinin yetkilendirilmesine bakmaksızın kimlik doğrulama sunucusu gibi belirli cihazlar ile iletişime geçmesine olanak tanır. Bu port aracılığıyla istemci EAP mekanizması ile kimlik bilgilerini, kimlik doğrulama sunucusuna gönderebilir. Kimlik doğrulama sunucusu, istemcinin kimlik bilgilerini genellikle önceden tanımlanmış kullanıcı veri tabanı üzerinden karşılaştırır. Eşleştirme başarılı ise yetkilendirme portu kapatılarak ağa erişim sağlanır. 802.1x çalışma prensibi Şekil 2.11.'de gösterilmektedir (Abreha, 2016).




**Şekil 2.11. 802.1x çalışma prensibi (Abreha, 2016)**

## 2.24. AAA:

Güvenli bir ağ denilince ilk akla gelen IETF (Internet Engineering Task Force) tarafından geliştirilen AAA (Authentication-Authrization-Accounting) standardıdır. Şubat 1999 yılında çalışmaya başlayan AAA çalışma grubu, ağda kimlik doğrulama gereksinimlerinin geliştirilmesine odaklanmıştır ve Ocak 2007'de çalışma tamamlanmıştır (IETF, 2018a).

## 2.25. Kimlik Doğrulama(Authentication):

Ağı dışarıdan gelecek saldırılara karşı güvenlik duvarı gibi cihaz ve yazılımlarla korumaya çalışmak elbette önemlidir. Ancak güvenliği sağlamanın ilk adımı kuşkusuz ağa dahil olacak kullanıcı ve cihazların kimliğinin doğrulanması olmalıdır. Hiçbir ağ yöneticisi kurumsal ağına kimlik doğrulaması yapılmadan, rast gele erişilebilmesini

istemez. Kimlik doğrulama işlemi son kullanıcının, kullanıcı adı-şifre, MAC adresi gibi gizli bilgilerini ihtiva eder. Bu bilgiler kimlik doğrulama sunucusu aracılığıyla ilgili veri tabanı üzerinden karşılaştırılır. Bilgiler eşleşiyorlarsa ağa erişime izin verilir, aksi halde kullanıcı ağda oturum açamaz (Ventura, 2002).

## 2.26. Yetkilendirme (Authorization):

Bir kampüs ağında, güvenlik kamera görüntüleri, ip telefon sistemleri, PACS (Picture Archiving Communication Systems) arşivleri, elektronik posta sunucuları, öğrenci bilgi sistemi veri tabanları ve elektronik belge yönetim sistemleri gibi çok sayıda veri çeşidi bulunabilir. Ayrıca birden çok kullanıcı tipi ağda bir arada çalışmaktadır. Kullanıcının ağa erişimi sağlandıktan sonra hangi hak ve yetkilere sahip olacağı planlanmalıdır. Kullanıcı, IP veya sanal yerel alan ağı tabanlı filtreler kullanarak trafik ve port izinleri belirlenebilir.

## 2.27. Kayıt Tutma (Accounting):

AAA'nın son kısmı olan Accounting işlemi kullanıcı ve cihazların ağa dahil olma sürecinden başlayarak, ağdaki yaptıkları aktivitelerin belirli bir düzen içerisinde kayıt altına alınması ve gerektiğinde izlenmesi işlemidir. Bu işleme kısaca loglama ya da log tutma işlemi de denir.

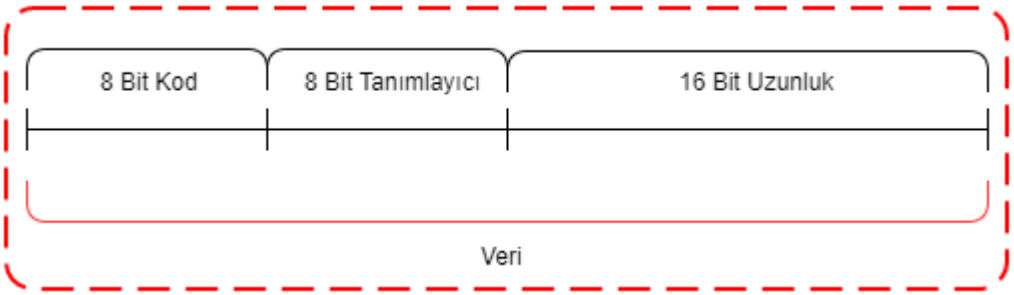
## 2.28. Genişletilebilir Kimlik Doğrulama Protokolü:

Genişletilebilir Kimlik Kanıtlama Protokolü sadece kimlik doğrulama için geliştirilmiş bir iletim protokolüdür. Kendisi bir kimlik doğrulama yöntemi olmamakla birlikte esnek bir kimlik doğrulama çerçevesi sunar. Point-to-Point (PPP), IEEE 802 ve IEEE 802.11i ağlarında kullanımı elverişlidir ve verinin kapsüllenerek iletimini sağlar.

EAP kimlik doğrulaması işlemi, kimlik doğrulayıcı tarafından başlatılır ve istemci kimlik doğrulamaya zorlanır. Kimlik doğrulama aşamaları aşağıda belirtildiği gibi özetlenebilir:

1. İstemci EAP oturumunu başlatmak için EAPOL-Start paketi gönderir.
2. Kimlik doğrulayıcı, istemciye ilk önce kimlik doğrulama türü belirtilir (örneğin MD5-challenge gibi).
3. İstemci, tür alanına karşılık gelen bir yanıt paketi gönderir. Geçerli bir yanıt paketi alınana kadar bu işlem devam eder. Geçerli bir paket alınmaması halinde belirlenen yeniden deneme aşımı süresince istek ve yanıt paket alışverişi devam eder. Geçerli bir yanıt paketi gelmezse iletişim sonlandırılır.
4. Geçerli bir yanıt gelmesi halinde kimlik doğrulayıcı istemcinin kimlik bilgilerini Radius Erişim İsteğine dönüştürerek (Radius-Access-Request) kimlik doğrulama sunucusuna iletir.
5. Kimlik doğrulama sunucusu istemcinin kimliğini kanıtlamasını ister (Radius-Access-Challenge).
6. İstemci kimlik kanıtlama için gerekli olan bilgileri gönderir. Bu süreç içerisinde kimlik doğrulayıcı, aradaki iletişimi 802.1x'de bahsedilen kontrolsüz port üzerinden taraflara aktarır.
7. Kimlik kanıtlama işlemi başarılı olursa Radius-Access-Accept paketi gönderilir, başarısız olursa Radius-Access-Denied ile yanıt verilir.

Kimlik doğrulanana kadar istemcinin ağ kaynaklarına erişimine izin verilmez. Hatta bu işlemler gerçekleşirken istemcinin bir IP adresi bile yoktur. EAP oturumu boyunca istemcinin bir IP adresine ihtiyacı olmaması, EAP'ın en önemli avantajlarından birisidir. EAP paket yapısı şekil 2.12.'de, başlık yapısı çizelge 2.4.'de verilmiştir.

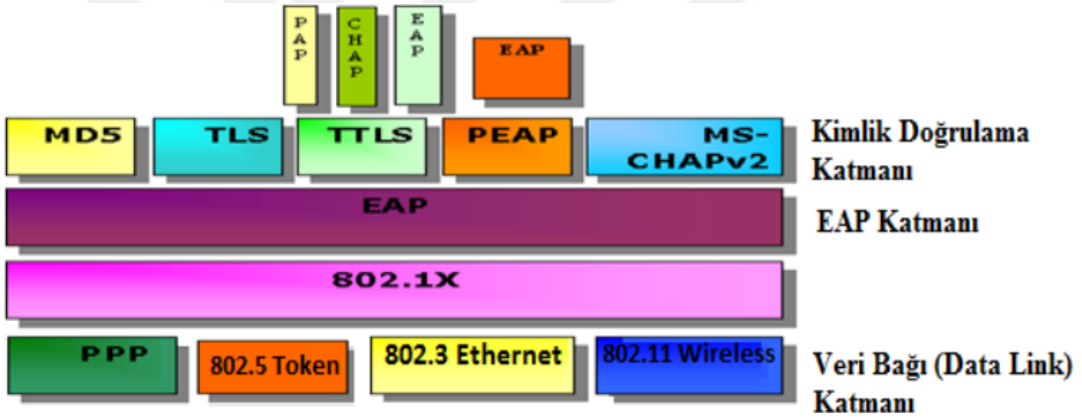



**Şekil 2.12. EAP paket yapısı**

**Çizelge 2.4 EAP başlık yapısı**

| Kod | Açıklama | Referans |
|---|---|---|
| **1** | Request | RFC 3748 |
| **2** | Response | RFC 3748 |
| **3** | Success | RFC 3748 |
| **4** | Failure | RFC 3748 |
| **5** | Initiate | RFC 5296 |
| **6** | Finish | RFC 5296 |

Ağ yöneticisinin ihtiyacına ve ağın yapısına göre farklı kimlik doğrulama yöntemleri tercih edilebilir. Kimlik doğrulama yöntemleri tercih edilirken ağdaki cihazların işletim sistemleri, destekledikleri kimlik doğrulama yöntemleri, kimlik doğrulama yönteminin güvenlik seviyesi gibi faktörler göz önünde bulundurulur. Farklı ihtiyaçlara binaen çeşitli algoritmalar geliştirilmiştir. EAP'ın kullanıldığı yapı katmansal olarak şekil 2.13.'de verilmiştir.




**Şekil 2.13. EAP ile kullanılan mimariler (Kurt, 2013)**

## 2.29. EAP Tabanlı Kimlik Doğrulama Mekanizmaları:

### 2.29.1. EAP-MD5:

MD5 en temel EAP yöntemlerinden birisidir. 1992 yılında ta Ronald L. Rivest tarafından geliştirilen MD5 (Message Digest) algoritmasına (RFC1321) göre çalışır ve veriyi "hash" fonksiyonu aracılığıyla sabit uzunlukta (128 bit) değerlere dönüştürülür. Tersine döndürülemez bir algoritmadır ancak internette denenmiş MD5 şifrelerinin tutulduğu geniş veri tabanları bulunmaktadır. Ayrıca sözlük temelli brute force saldırıları ile kırılabilmektedir (IETF, 2018d).

Uygulaması kolay olmakla birlikte, kimlik doğrulama tek yönlü gerçekleşir. Veri tabanında şifreler açık metin olarak saklanır ve MD5'e dönüştürülerek gelen istek ile karşılaştırılır. İstemci kimlik doğrulayıcının kimliğini doğrulamaz, bu yüzden MITM ataklarına karşı zayıf bir yapıdır. Anahtarın sabit olmasından dolayı günümüzde güvenli bir EAP yöntemi olarak kabul edilmez.

### 2.29.2. LEAP

Cisco System tarafından Aralık 2000'de duyurulan LEAP (Hafif EAP- Lightweight EAP), kablosuz ağlar için tasarlanmıştır. LEAP istemci ve RADIUS sunucu arasında karşılıklı kimlik doğrulaması sağlayan 802.1x yöntemidir. WPA ve WPA2 ile birlikte kullanılabilen LEAP, kullanıcı adı ve şifre ile kimlik doğrulamayı destekler. Kullanıcının her oturumunda dinamik ve şifrelenmiş anahtar kullanmasını sağlar. Dinamik şifreleme anahtarı kimlik doğrulama sırasında türetilir ve RADIUS güvenli bir kanaldan anahtarı istemciye iletir. Kullanıcı adı ve şifre bilgileri bu anahtar ile şifrelenmeden gönderilmez. Hemen hemen tüm işletim sistemleri ve ağ kartları tarafından desteklenmektedir (Cisco Systems, 2017). Ancak açık bir standart olmadığı ve bir firma tarafından üretildiği için farklı ağ cihazlarından oluşan WLAN'lar için kullanımı sorun yaratabilir.

### 2.29.3. EAP-TLS:

IETF tarafından RFC (Request for Comments) 5216 koduyla Mart 2008 tarihinde tanımlanmış açık bir standarttır. SSL (Secure Socket Layer - Güvenli Giriş Katmanı) sertifikası ve anahtar ile taraflar arası karşılıklı doğrulamayı sağlar. EAP-TLS güvenlik ve gizlilik için SSL' den yararlanır. Daha önce EAP başlığında anlatıldığı gibi kimlik doğrulayıcı, istemciden kimlik bilgilerini ister ve EAP türünü belirten TLS Start isteğini gönderir. İstemci TLS client_hello mesajıyla yanıt gönderir. Client_hello iletisi TLS sürüm numarasını, sessionId (oturum kimliği), rastgele üretilmiş bir sayı ve istemci tarafından desteklenen şifreleme seti bilgisini içerir. Bu noktadan sonra oturumun SSL ile şifrelemesi üzerine mutabakat sağlanması amacıyla, EAP sunucusu EAP-Request isteği gönderir. Bu isteği yanıtlayan istemciye mutabakatın sağlanması halinde, EAP-Success mesajı ile yanıt verilir. EAP-TLS ile birlikte kullanılan sessionId ile istemcinin araya giren başka kişiler ile iletişim kurmasının önüne geçilir (IETF, 2018b). Birçok işletim sistemi ve ağ cihazı tarafından desteklenmektedir.

### 2.29.4. EAP-TTLS:

EAP-TLS üzerine geliştirilmiş olan EAP-TTLS (Tünellenmiş Taşıma Katmanı Güvenliği - Tunneled Transport Layer Security), IETF tarafından Ağustos 2008 tarihinde RFC3748 açık standardı olarak duyurulmuştur. EAP-TLS'de olduğu gibi karşılıklı kimlik doğrulama işlemi gerçekleşir ve istemci ile kimlik doğrulama sunucusu arasında kurulan SSL tüneli vasıtasıyla güvenli bir yapı amaçlanmıştır. Bu sayede MITM saldırılarını önlemede daha avantajlıdır. Ayrıca EAP-TLS'de bulunan, istemci tarafında sertifika sahibi olma zorunluluğunu ortadan kaldırmak için tasarlanmıştır.

EAP-TTLS kimlik doğrulaması TLS el sıkışma aşaması ve TLS tünel fazı olmak üzere iki aşamadan oluşur. Birinci fazda EAP-TLS'de olduğu gibi el sıkışma ve karşılıklı kimlik doğrulama süreci tamamlanır. İkinci Fazda ise tünel oluşturulur ve kimlik doğrulama aşamasında EAP'ın yanı sıra PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft-Challenge Handshake Authentication Protocol) , MS-CHAP-V2 ve GTC (Generic Token Card) kullanılabilir. RADIUS'ta olduğu gibi AVPs (Nitelik Değer Çiftleri- Attribute Value Pairs) karşılaştırması yoluyla farklı kimlik doğrulama seçenekleri oluşturulabilir. EAP-TLS'den farklı olarak istemci tarafında sertifika zorunluluğu olmadığı için, sertifika dağıtımı ve takibi işlemlerini ortadan kaldırarak, hem yönetim açısından, hem de maliyet açısından daha avantajlı olduğu düşünülebilir. EAP-TTLS'in paket biçimi Şekil 2.14.'de gösterilmektedir (IETF, 2018c).


**Şekil 2.14. EAP-TTLS paket biçimi**

### 2.29.5. PEAP:

Microsoft Corporation, Cisco System ve RSA Security tarafından 802.11 ağlarında erişim noktaları ve istasyonların kimlik doğrulaması amacıyla tasarlanmıştır. PEAP (Protected EAP), IETF internet taslağı (ID-Internet Draft) olarak yayınlanmış ancak herhangi bir RFC standardı haline dönüşmemiştir. EAP mekanizması kullanarak kimlik doğrulaması gerçekleştirir. Verinin bütünlüğü ve gizliliği TLS tarafından korunmaktadır. Ancak istemci tarafında bir sertifikaya ihtiyaç duyulmaz, kimlik doğrulama sunucusuna güvenilir sertifika (trusted certificate) yüklenmesi gerekmektedir. EAP-TTLS'den farklı olarak PAP ve CHAP gibi kimlik doğrulama yöntemleri yerine daha güvenli olan MS-CHAP-V2 kullanımı zorunludur. PEAP'ın ilk aşamasında TLS oturumu oluşturulur, faz 2'de TLS kanalı üzerinden MS-CHAP-V2 kimlik doğrulaması gerçekleştirilir.

Geçmişten günümüze kadar en sık tercih edilen EAP yöntemlerinin belirli ölçütlere göre karşılaştırılması çizelge 2.5.'de gösterilmektedir.

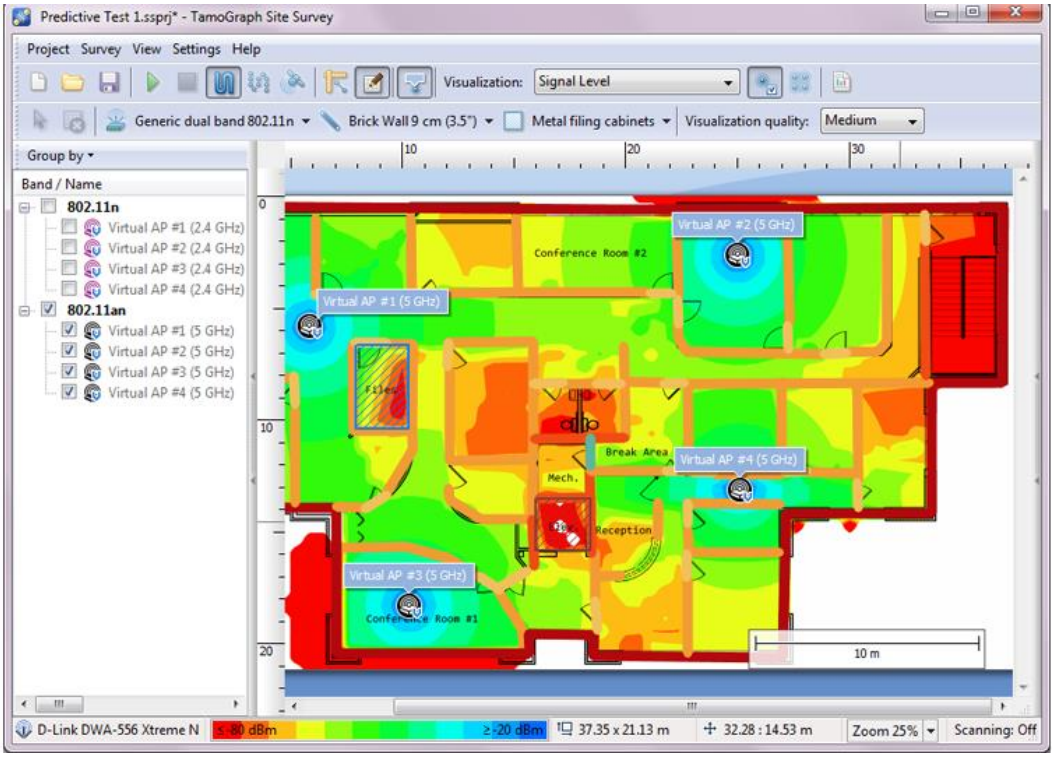
**Çizelge 2.5 EAP Yöntemleri karşılaştırması**

| 802.1x EAP Özellikleri | MD5 | TLS | TTLS | LEAP | PEAP |
|---|---|---|---|---|---|
| **İstemci Sertifikası** | Yok | Var | Yok | Yok | Yok |
| **Sunucu Sertifikası** | Yok | Var | Var | Var | Var |
| **Anahtar Değişimi** | Yok | Gerekli Değil | Var | Var | Var |
| **Kimlik Doğrulama Şekli** | Tek Yönlü | Karşılıklı | Karşılıklı | Karşılıklı | Karşılıklı |
| **Dağıtım Zorluğu** | Kolay | Zor | Orta | Orta | Orta |
| **Güvenlik Seviyesi** | Zayıf | Çok Yüksek | Yüksek | Yüksek | Yüksek |

# 3. WLAN ÜZERİNDE 802.1X VE DİNAMİK VLAN YAPILANDIRMASI

## 3.1. Kablosuz Kurumsal Kampüs Ağları:

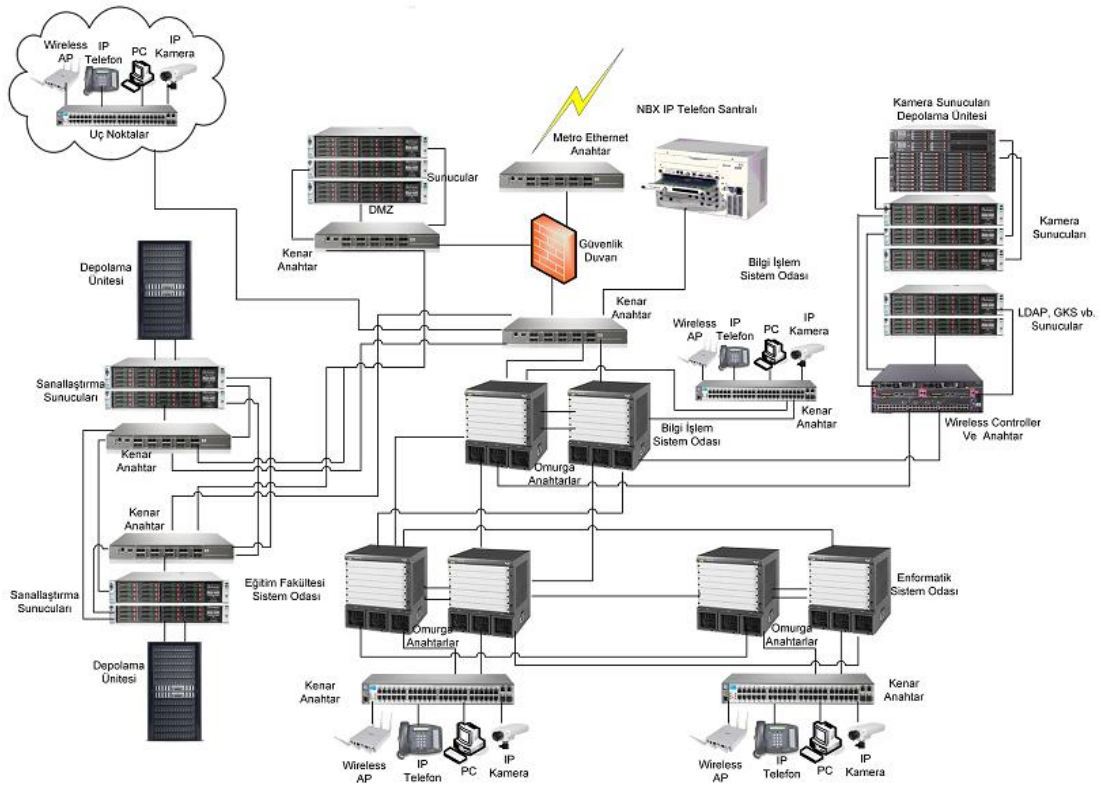
Kurumsal kampüs ağları genellikle bir veya daha çok yerleşkede birden çok binası bulunan dağıtık yapılardır. Kampüs ağlarında kablosuz hizmetler genellikle mevcut kablolu ağ alt yapısı üzerinden gerçekleştirilir. Kablosuz ağ cihazlarının bir bina ve yerleşke içerisinde nasıl konumlandırılacağı önemli bir konudur. Erişim noktaları arasında girişim olmamasına gayret edilmelidir. Bunun için bazı ağ üreticilerinin geliştirdiği konumlandırma yazılımları mevcuttur. Binanın CAD (Computer Aided Design) çizimleri programa yüklenir ve en uygun yer ve AP sayısı program tarafından belirlenebilir (Predictive Site Survey-Tahmini Mevki Araştırması). Şekil 3.1.'de tahmini mevki araştırması yazılımı ve AP'lerin nasıl konumlandırıldığı gösterilmektedir.




**Şekil 3.1. Örnek tahmini mevki araştırması yazılımı (TamoSoft, 2018)**

Ancak kablosuz ağları etkileyen birden çok faktör olduğundan en iyi sonucu gerçek ortamda yapılacak olan testler belirlemektedir. Testler gerçek ortamda 2 şekilde, aktif ve pasif olarak gerçekleştirilir. Pasif testlerde WLAN trafiği pasif olarak dinlenir. Test yapılırken test yapılan cihaz herhangi bir WLAN'a bağlı değildir. Gürültü ve sinyal takibi yapılır. Aktif testlerde test yapılan cihaz ağda konumlandırılan erişim noktasına bağlanır. Ağın performansı paket kayıpları, bant genişliği, kapsama alanları ve sinyal ölçümleri yapılır. Çıkan sonuçlara göre erişim noktası sayısı ve konumları belirlenir.

Şekil 3.2.'de görüldüğü gibi kampüs ağı çok sayıda aktif cihaz barındırmakta ve TCP/IP protokolü üzerinden çeşitli servisler ağ üzerinde koşmaktadır. Bu servislerin veri trafiği aynı fiziksel katmanda iletilmektedir. Kampüs ağında IP telefon ile ses trafiği, IP kamera ile video akış trafiği ve bilgisayarların oluşturduğu veri trafiğinin aynı anda çalışması gerekmektedir.




**Şekil 3.2. Kampüs ağı**

Yapının sağlıklı çalışabilmesi için mevcut ağ alt ağlara bölünür ve yönetilir. Ağ bölümlemesi için VLAN (Virtual Local Area Network – Sanal Yerel Ağ ) yapılandırılması kullanılır.

## 3.2. VLAN-Sanal Yerel Ağ:

Sanal yerel ağ anlamına gelen VLAN IEEE 802.11Q standardı olarak anılır. Yerel ağ içerisinde çalışma grupları oluşturmak ve yerel ağı mantıksal alt ağlara bölmek için kullanılır. Fiziksel olarak aynı ağ içerisinde bulunsalar bile farklı VLAN'larda bulunan cihazlar, yönlendirme yapılmaksızın birbirleri ile doğrudan iletişim kuramazlar.

Ağda bulunan cihazların sayısı arttıkça, ağdaki yerel yayın (broadcast) sayısı da doğru orantılı olarak artar. Bir kampüs ağında bulunan ağ cihazı sayısı binlerce olabilmektedir. Ayrıca aynı ağ anahtarı üzerinde ses, video ve veri trafiği yapılabilmektedir. Ses ve video paketleri UDP (User Datagram Protocol) protokolü ile gerçek zamanlı iletilmektedir. Bu servislerin hizmet kalitesinde yaşanacak bir gecikmenin telafisi mümkün olmamaktadır. Bu servisler aynı ağ anahtarı üzerinde gerçekleşse bile farklı VLAN yapılandırması ve trafik önceliklendirmesi ile gecikmelerin önüne geçilmeye çalışılmaktadır. Kullanıcılar ve cihazlar belirli VLAN'lar altında genellikle yerleşim yerine, departmana, güvenlik seviyesine, sunucu ve kaynakların işlevine göre gruplanırlar.

## 3.3. VLAN Türleri:

Kampüs ağlarında ağ içerisinde koşan verinin türüne göre farklı VLAN grupları oluşturulmaktadır. Bu durum yönetimsel açıdan kolaylık sağlamakla birlikte, verinin tasnifi, izolasyonu, internete açık olup olmaması, servis kalitesi, kimlerin bu ağa ulaşıp ulamayacağına kadar detaylandırılabilir. Teknik açıdan VLAN türleri arasında pek fark olmasa da, terminoloji açısından aşağıdaki gibi isimlendirilirler;

### 3.3.1. Varsayılan VLAN (Default VLAN):

Anahtarın fabrika ayarlarında tanımlanan ve cihazın ilk açılışında tüm portlarının üye olduğu VLAN'dır. VLAN ID'sine ön tanımlı olarak 1 değeri atanmıştır. Bu değer değiştirilemez. Bunlar dışında veri VLAN'ı gibi çalışır.

### 3.3.2. Veri VLAN'ı (Data VLAN):

Verilerin özelleştirilmeden toplandığı, genellikle internete veya yazıcı gibi diğer ağ cihazlarına doğru gerçekleşen VLAN türüdür. Her türden ses, görüntü vb. verinin taşınmasında kullanılabilir.

### 3.3.3. Yerel VLAN (Native VLAN):

Yerel ağ içerisinde işaretlenmemiş (untagged) verinin taşındığı VLAN'dır. Yani herhangi başka bir VLAN'dan gelmeyen veridir. Trunk portlar aracılığıyla hem işaretlenmiş (tagged), hemde işaretlenmemiş veri taşınabilir. Bir trunk porta gelen işaretlenmemiş (untagged) veri native VLAN'a yönlendirilir.

### 3.3.4. Yönetim VLAN'ı (Manangement VLAN):

Genellikle ağ cihazlarına ulaşmak için tanımlanır. Ağ cihazının desteklediği sınırda herhangi bir ID atanabilir. Son kullanıcıların cihazların yönetimsel arayüz kaynaklarına (TELNET, SSH, WEB v.b.) erişimini kısıtlamak ve cihazların belirli bir alt ağ altında tasnif edilmesini sağlamak amacıyla kullanılır.

### 3.3.5. Ses VLAN'ı (Voice VLAN):

Kampüs ağlarında ses VLAN'ı IP telefon iletişimi için kullanılır. Bunun için anahtarlarda veri VLAN'ı ile birlikte ses VLAN'ıda oluşturularak ilgili portun altında tanımlanır. IP telefonun yapılandırılması yapılarak ilgili VLAN telefon içerisine kaydedilir. Bazı üreticiler tarafından üretilen ağ cihazları, kendi markası olan telefon üzerinde herhangi bir yapılandırma yapmaksızın, ağa dahil olan cihazın IP telefon olduğunu algılayabilir ve telefondan gelen paketleri ses VLAN'ı olarak işaretler.

Ağ cihazlarının kabiliyetleri doğrultusunda bu ve benzeri tüm VLAN'lar farklı amaçlara hizmet etmek için oluşturulabilir. Örneğin IP kameralar, erişim noktaları, kart okuyucular vb. cihazlar için ayrı ayrı VLAN'lar oluşturulabilir. Temelde veri VLAN'larından bir farkı olmayacaktır. VLAN'lar aracılığıyla yönetimsel kolaylık sağlamakla birlikte, erişim listeleri (ACL-Access List) ve güvenlik duvarı kuralları gibi denetimlerle, ağın üzerinde hâkimiyet sağlanması kolaylaşacaktır.

## 3.4. VLAN Atama Yöntemleri:

### 3.4.1. Statik VLAN atamaları:

Günümüzde birçok üretici tarafından yönetilebilir ve 802.11q destekli cihazlar ağlarda konumlandırılmıştır. Farklı arayüz ve komutlara sahip olsalar da, temel olarak aynı mantık üzerine yapılandırılırlar. Statik VLAN atamaları ağ cihazları üzerinde belirli portların gruplanması ile oluşur. Ağ yöneticisi tarafından manuel olarak atanır ve değiştirilmediği sürece aynı kalır. Bu tarz VLAN atamalarına "Port Based VLAN'da denir. Özellikle kablolu ağlarda ve ağa dahil olan cihazların sık sık değişmediği, durağan ağlarda tercih edilir. Yer değiştiren kullanıcılar için yeniden VLAN tanımlaması yapılması gerekmektedir. Bir port yalnızca bir veri VLAN'ına üye olabilir.

### 3.4.2. Dinamik VLAN atamaları:

Cihazların ve kullanıcıların sık değiştiği ortamlarda kullanılan VLAN atama yöntemleridir. Kablosuz istasyonun bir kampüs ağı içinde hareket ederken aynı VLAN üzerinde kalmasına izin vermek için kullanılır. Bu işlemin gerçekleştirilebilmesi için üretilmiş yazılım ve donanımlar vardır. Bununla birlikte Linux tabanlı yazılımlarla da bu işlemler gerçekleştirilebilmektedir. Dinamik VLAN atamasının ne şekilde yapılacağının belirlenebilmesi için önceden bilgi toplanması gerekir. Başlıca dinamik VLAN atama yöntemleri aşağıda listelenmiştir.

### 3.4.3. MAC tabanlı VLAN atama:

Ağ Cihazları veri bağı katmanında (Layer 2) birbirleri ile MAC (Media Access Control) adresleri üzerinden iletişim kurarlar. Ağ cihazı üretilirken, her ethernet portu için benzersiz bir MAC adresi tanımlanır. Birçok ağ cihazı üreticisi MAC tabanlı doğrulamayı destekler. MAC adresi doğrulamasında ağa dâhil olmak isteyen cihaz ilişkilendirme isteği gönderir. Bir doğrulama sunucusu veya bir MAC listesi aracılığıyla yetkilendirme ve VLAN ataması yapılır.

### 3.4.4. Protokol tabanlı VLAN'lar:

Protokol tabanlı VLAN'lar belirtilen protokol türünün yayınlarını kabul ederler. İlgili port için ayarlanan protokollerin oluşturduğu trafik kabul edilir. Böylece ağda istenmeyen başka trafiklerin önüne geçilmiş olur. Böylece ağ protokol kümelerine göre homojen olarak tasnif edilebilir. Alt ağların birbirleri ile izin verilen etkileşimi, yönlendirme ihtiyacından dolayı katman 3 seviyesinde gerçekleşebilir. Bu işlemlerin tamamı ağ yöneticisi tarafından el ile yapılabilir. Portların tek tek ayarlanması gerekmektedir (Jiang vd., 2009).

### 3.4.5. Kural tabanlı VLAN'lar:

Ağ yöneticisinin belirlediği kurallar çerçevesinde yapılan VLAN atama işlemleridir. VLAN ataması yapılmadan önce kullanıcıların sisteme ne şekilde dâhil olacağı belirlenmiştir. Kullanıcıların profiline, cihaz tipine veya departmanına gibi kurallar çerçevesinde VLAN ataması yapılabilir. Esnek ve kolay değiştirilebilir bir yapı olmakla birlikte, ilk yapılandırma aşamasında iyi planlama gerektirir.

## 3.5. Kablosuz Kampüs Ağlarında Dinamik VLAN Ataması:

Kablosuz kampüs ağları açısından değerlendirildiğinde dinamik VLAN ataması, ağ yöneticisi tarafından belirlenen kriterler doğrultusunda esnek bir yapı sağlamaktadır. Büyük bir alanda sürekli hareket halinde bulunan kullanıcıların ne zaman ve nereden ağa katılacağını öngörmek güçtür. Aynı bölgede birden farklı kullanıcı tipi ağa katılmak isteyebilir. Çok sayıda kullanıcı tipi ve cihazının bulunduğu bir ortamda tek bir ağda (1 VLAN içinde) tüm kullanıcıların konumlandırılması birçok sorunu beraberinde getirecektir. VLAN kullanımının bu sorunlara getireceği çözümler 5 başlık altında toplanabilir;

### 3.5.1. Güvenlik:

Kampüs ağlarında öğrenci, akademik personel, idari personel, yönetici, teknik personel gibi çok sayıda kullanıcı tipi bulunmaktadır. Bu kullanıcıların ağa dâhil oldukları zaman hangi yetkilerle bağlanabilecekleri belirlenmek istenir. Günümüzde siber güvenliğin önemi göz önüne alındığında, aynı VLAN'da farklı kullanıcı

tiplerinin bulunması istenmeyen bir durumdur. VLAN'lar arası veri trafiği OSI (Open Systems Interconnection) referans modelinin 3. Seviyesi olan ağ katmanında gerçekleşirken, aynı VLAN içerisinde trafik 2. seviye olan veri bağı katmanında MAC adresleri vasıtasıyla gerçekleşir. Ağa katılan bir kullanıcı ağ trafiğini dinleyerek ağ paketlerinin çözümlemesini yapabilir. Bu yüzden VLAN yapılandırılmasının dikkatle yapılması gerekmektedir. Bu sayede yapılacak bir saldırı veya virüs yayılması sadece ilgili VLAN'da kalacak, tüm ağın dinlenmesinin ve zarar görmesinin önüne geçilerek, ağ üzerinden yayılabilen zararlı yazılımların kontrol altına alınması kolaylaşacaktır. Ayrıca VLAN'lar arası bir noktaya konumlandırılacak IPS (Intrusion Prevention Systems), IDS (Intrusion Detection Systems), FW (Firewall) gibi güvenlik cihazları ile ağ daha denetlenebilir hale getirilebilmektedir.

### 3.5.2. Broadcast (yayın adresi) sayısı:

Broadcast bir mesajın ağdaki tüm cihazlar tarafından alınmasını sağlayan bir protokoldür. Bir alt ağda cihaz sayısı ne kadar artarsa broadcast sayısı üstel olarak o oranda artmaktadır. Kontrol altına alınmazsa bu durum bir süre sonra broadcast storm (yerel yayın fırtınası) oluşmasına neden olur ve ağda iletişimin başarılı bir şekilde devam etmesine engel olabilir. Doğru yapılandırılmış VLAN atamaları ile broadcast kontrolü sağlanmış olacaktır (Ulakbim, 2018).

### 3.5.3. Bant genişliği:

Bilgisayar ağları açısından değerlendirildiğinde bant genişliği, iletim ortamının toplam kapasitesini gösteren değerdir. Bant genişliği ne kadar büyükse, anlık olarak iletilebilecek veri miktarı o kadar artar. Günümüzde bant genişliği değerleri Mbit/s (Megabit per Second), Gbit/s (Gigabit per Second) gibi değerler ile ifade edilmektedir. Bu birimler saniyede iletilebilen bit sayısını ifade eder. Kampüs ağlarında alt ağların oluşturduğu çıkış trafiği, genel çıkış hattının toplam bant genişliğini oluşturur. Bu yüzden alt ağların gözlemlenmesi, aşırı trafik üreten kullanıcı ve uygulamaların kontrol edilmesi gerekmektedir.

### 3.5.4. Ağ izleme ve arıza takibi:

Kablosuz kampüs ağının alt ağlara bölünmesi ağda oluşabilecek sorun ve arızaların ağ izleme yazılımları ile gözlemlenerek tespitini kolaylaştıracaktır.

### 3.5.5. Esneklik:

Kullanıcı nereden ağa dâhil olursa olsun, kendisi için belirlenen VLAN'a ataması yapılacaktır. Kullanıcı profilinde oluşabilecek bir değişiklikte (yönetici değişiklikleri v.b.) yeni bir VLAN tanımlaması ile kullanıcı ağdaki yaşamına kesintisiz devam edebilmektedir. Kullanıcının kurumsal yapı ile bağının kesilmesi durumunda kısıtlanmış misafir VLAN'ına alınması işlemi kolaylıkla yapılabilmektedir.

## 3.6. Sistem Tasarımı:

### 3.6.1. Mevcut yapı:

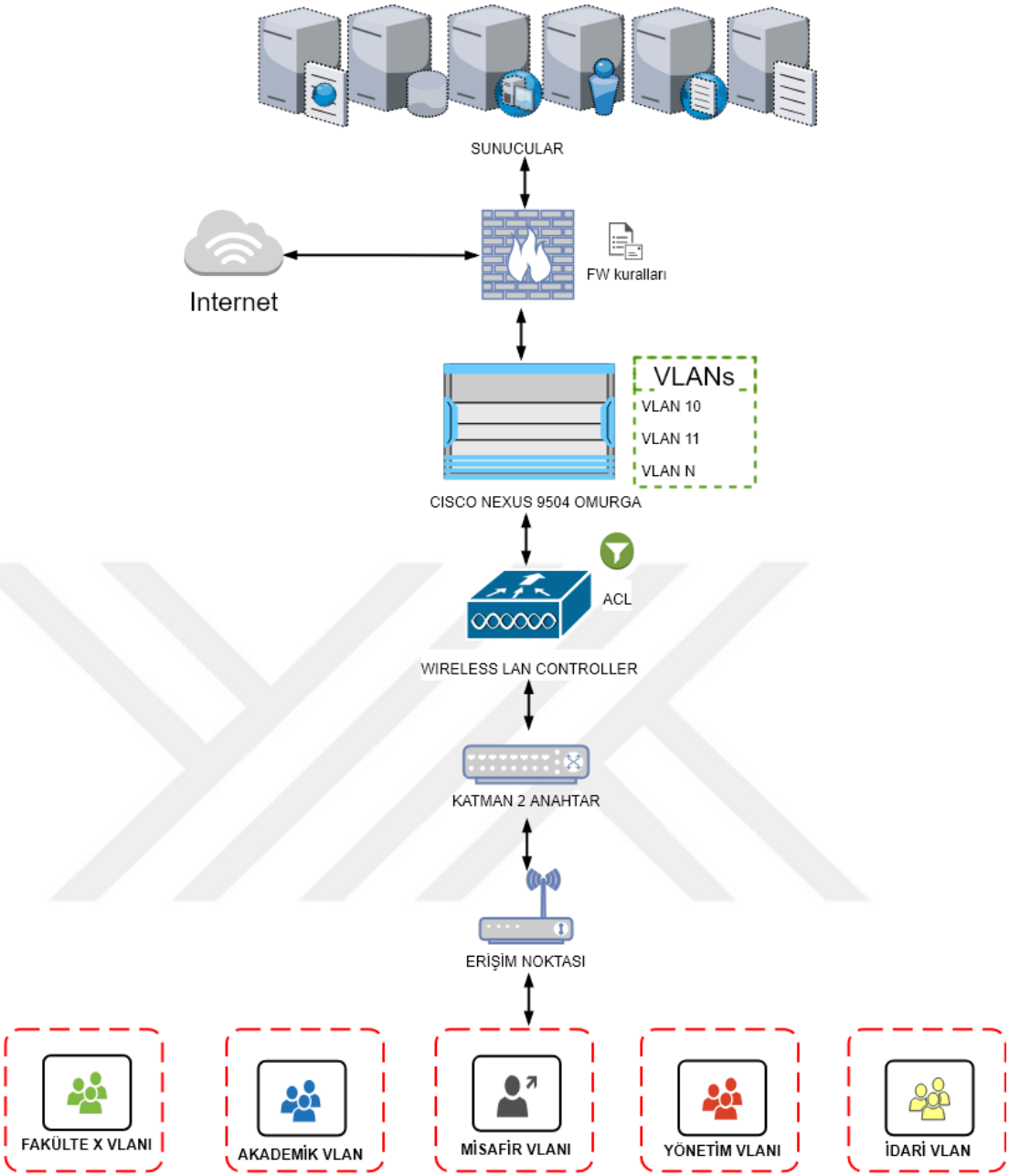
Mevcut kullanılan yapıda tüm kullanıcılar tek bir VLAN içerisinde alınarak ağda konumlandırılmaktadır. Ağda oluşabilecek bir sorun ya da kablosuz ağ için uygulanacak bir güvenlik kuralı tüm kullanıcıları etkilemektedir. Tek bir alt ağ içerisinde kullanıcı cihazlarında bulunan güvenlik uygulamaları dışında (Antivirüs, güvenlik duvarı v.b.) kullanıcıları birbirinden izole edecek başka bir katman bulunmamaktadır.

Şayet bir bölge veya AP için ayrı bir VLAN ataması yapılmak istenirse, ilgili VLAN arayüzünün tanımlı olduğu cihazdan (genellikle omurga anahtar), AP'nin bağlı olduğu kenar anahtar portuna kadar taşınması ya da katman 3 olarak yönlendirme yapılması gerekmektedir.

### 3.6.2. Yeni yapı:

Yeni tasarlanan yapıda kullanıcılar kural tabanlı olarak gruplandırılarak ağa katılmaları sağlanmıştır. Gruplandırma işlemi kullanıcı tipine göre belirlenerek ilgili VLAN'a ataması gerçekleştirilmektedir.

Kullanıcının AP'den WLC'ye kadar olan trafiği kapsüllenerek getirilmektedir. Böylece kullanıcının başka bir yerel VLAN'a ulaşmasının önüne geçilmiştir. Bunların yanı sıra WLC'de ve FW'da alt ağlara yönelik detaylı kurallar yazılabilmektedir. VLAN grupları arasından hem iç sunuculara hem de internet yönüne denetim ve yetkilendirme imkânı artırılmıştır. Şekil 3.3'de yeni yapının tasarımı verilmiştir.




**Şekil 3.3. Yeni yapının tasarımı**

### 3.6.3. OpenLDAP:

Haziran 2006'da OpenLDAP Foundation tarafından geliştirilen LDAP (Lightweight Directory Access Protocol) protokolü IETF RFC 4510 açık standardı ile dizin hizmetlerine erişim için kullanılır. LDAP dizini, Dizin Bilgileri Ağacı (DIT - Directory Information Tree) olarak adlandırılan hiyerarşik bir yapıdadır. Dizin yapısı bir veri tabanı gibi çalışır. Bilinen birçok veri tabanı hızlı yazma ve okuma üzerine tasarlanmıştır. LDAP dizin yapısı ise bir adres defterine benzer ve ulaşılacak verinin indeksi bellidir. Burada amaç ulaşılmak istenen kayıta en kısa sürede ulaşmaktır. Bu

nedenle okuma işlemi yazma işlemine göre çok daha hızlıdır. Dizinde bulunan her kayıtın kendine ait özellikleri vardır. ObjectClass denilen tanımlamalar ile her bir kayıt için kullanılabilecek özellikler belirlenir. Tüm özellikler RFC standartlarında açık olarak belirtilen şemalar aracılığıyla tanımlanmıştır.

LDAP dizin yapısında gerçekleştirilen işlemler şunlardır;

**Kayıt Arama işlemi (ldapsearch):** Dizindeki bir girdiye veya herhangi özellik değerine ulaşmak için kullanılır.

**Kayıt Ekleme işlemi (slapadd):** Dizine bir girdi eklemek için kullanılır.

**Kayıt Silme İşlemi (ldapdelete):** Dizindeki bir girdiyi silmek için kullanılır.

**Kayıt Değiştirme İşlemi (ldapmodify):** Dizindeki bir girdiyi değiştirmek için kullanılır.

**Kayıt Karşılaştırma İşlemi (ldapcompare):** Dizindeki iki farklı girdinin karşılaştırması için kullanılır.

Dizin içerisine veri yazılırken veya bir sorgu aracılığıyla veri çekilirken LDIF (LDAP Data Interchange Format- LDAP Veri Değişim Biçimi) denilen metin tabanlı dosyalar kullanılır (IETF, 2018e). Dizin içerisinde bulunan her nesnenin benzersiz bir DN'i (Distinguished Name- Benzersiz Ad) bulunmaktadır. Ulaşılacak olan veriye bu benzersiz ad ile ulaşılır ve LDIF dosyalarında her nesne için bu adres en başta bulunur.

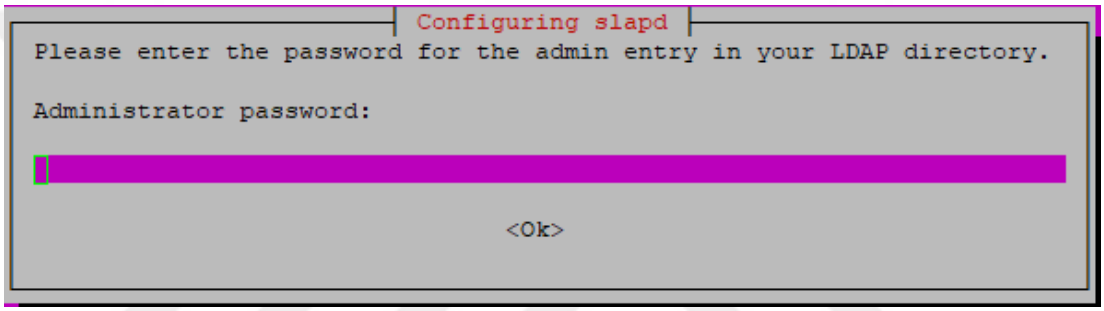
Örnek bir LDIF dosyası aşağıdaki gibidir;

```
dn: uid=fatihtarlaci, ou=Ogrenci, dc=mu, dc=edu, dc=tr
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Fatih TARLACI
givenName: Fatih
sn: TARLACI
uid: fatihtarlaci
mail: fatihtarlaci@mu.edu.tr
telephoneNumber: +90 252 123 45 67
```

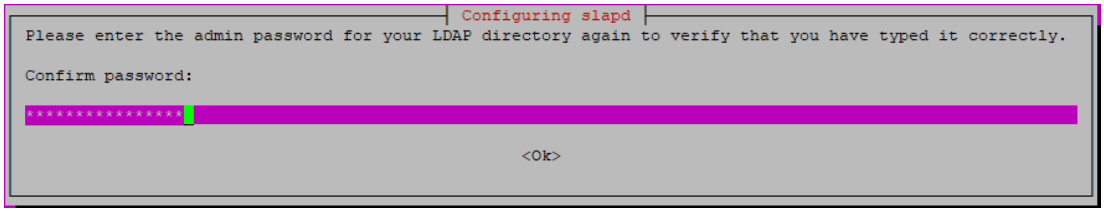
### 3.6.4. OpenLDAP kurulumu:

OpenLDAP tıpkı FreeRadius gibi birçok Linux dağıtımının depolarında bulunur. Açık kaynak kodlu ve GPL lisansı ile kamunun hizmetine sunulmuştur. Mart 2018 tarihi itibariyle, Ubuntu işletim sistemi depolarında güncel sayılabilecek versiyonu bulunmaktadır. Kaynak çeşitliği oluşturması amacıyla kurulum için işletim sistemi depoları kullanılmıştır. Kurulum adımları aşağıda verilmiştir:

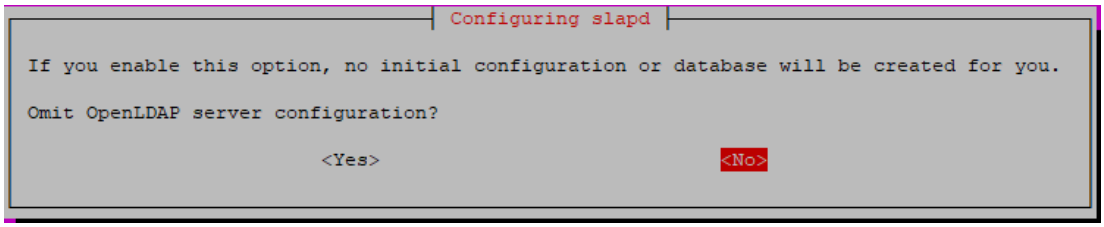
```
$sudo apt-get update
$sudo apt-get upgrade
$sudo apt-get install slapd ldap-utils
$dpkg-reconfigure slapd
```



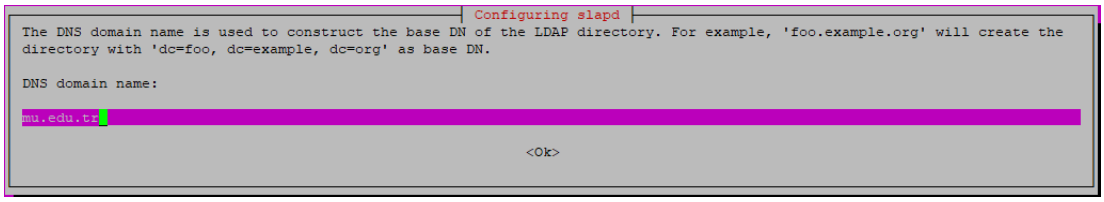

**Şekil 3.4. Adım 1: Admin şifresinin belirlenmesi**



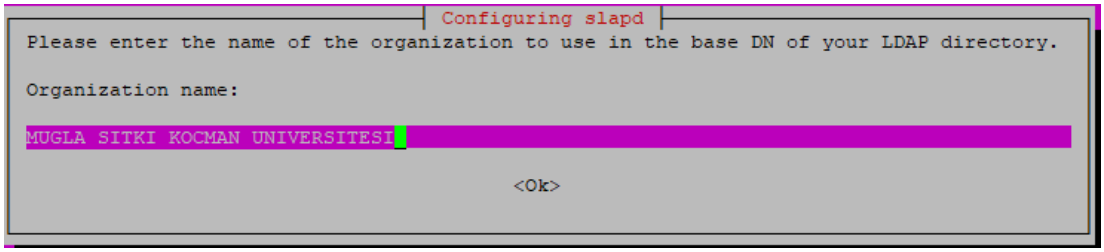

**Şekil 3.5. Adım 2: şifrenin doğrulanması**



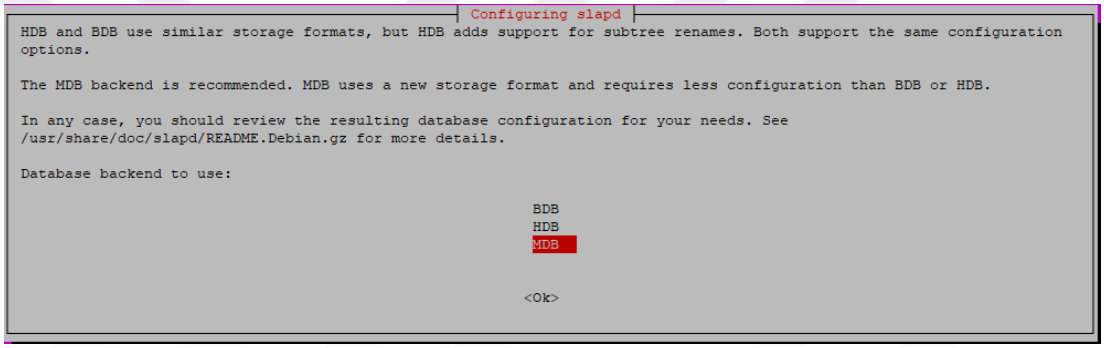

**Şekil 3.6. Adım 3: Ayarlara geçiş**



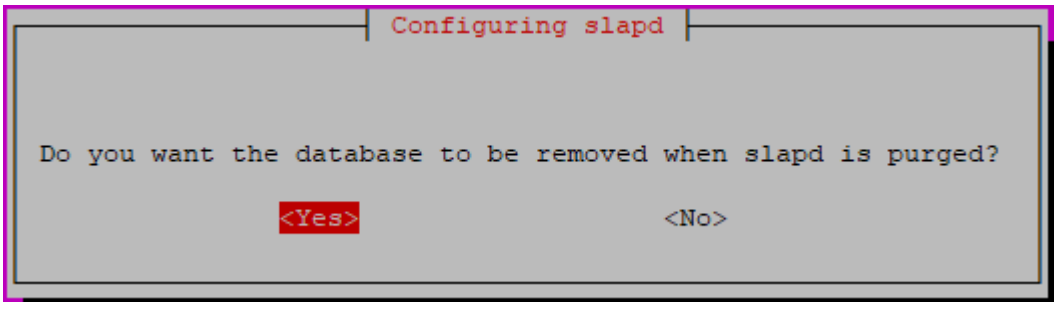

**Şekil 3.7. Adım 4: Domain adresinin belirlenmesi**



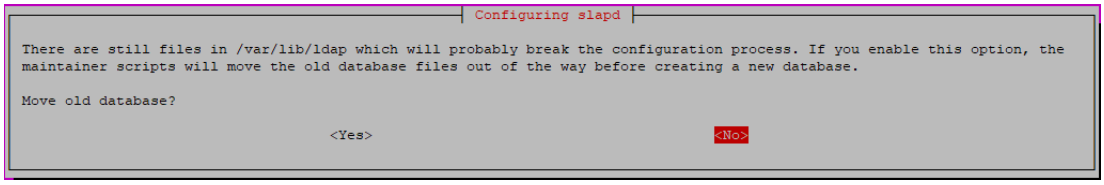

**Şekil 3.8. Adım 5: Organizasyon adının belirlenmesi**



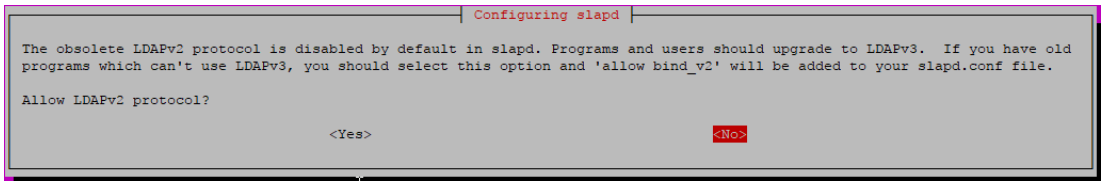

**Şekil 3.9. Adım 6: Veri tabanı türü seçilmesi**




**Şekil 3.10. Adım 7: OpenLDAP ile birlikte veri tabanı kaldırma seçeneği**




**Şekil 3.11. Adım 8: Eski veri tabanının taşınma/taşınmama işlemi**




**Şekil 3.12. Adım 9: LDAPv2 izin verme/vermeme işlemi**

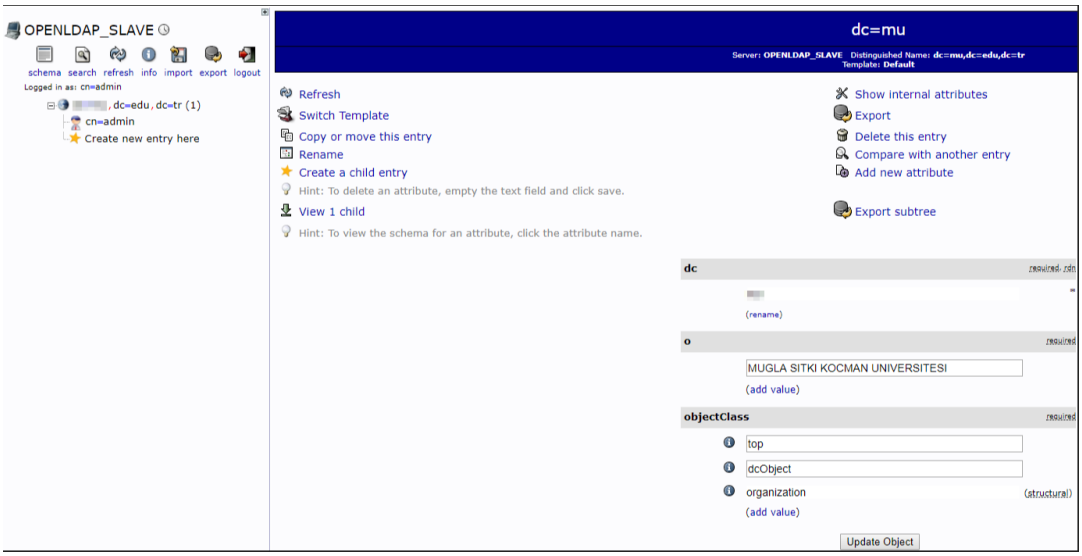
Temel olarak OpenLDAP'ın kurulumu yukarıdaki gibidir. Bu noktadan sonra ağaç yapısının temel taşlarından olan organizasyon (O - Organization) ve organizasyon birimleri (OU - Organizational Unit) oluşturulur. Bir O ve OU eklemek için gerekli LDIF dosyası aşağıdaki gibidir;

```
dn: o=organization.edu.tr,dc=organization,dc=edu,dc=tr
o: organization.edu.tr
objectClass: top
objectClass: organization
dn: ou=student,o= organization.edu.tr,dc=organization,dc=edu,dc=tr
objectClass: top
objectClass: organizationalUnit
ou: student
description: Mugla Sıtkı Koçman Universitesi Ogrenci OU
dn: ou=employee,o=mu.edu.tr,dc= employee,dc=edu,dc=tr
objectClass: top
objectClass: organizationalUnit
ou: employee
description: Mugla Sıtkı Koçman Universitesi Personel OU
```

LDIF biçiminde kaydedilen dosyanın komut satırı aracılığıyla dizin içerisine aktarılması aşağıdaki gibidir. Veri yazılırken başlangıçta belirlenen domain admin şifresi girilmesi gerekmektedir.

ldapadd -x -D cn=admin,dc=mu,dc=edu,dc=tr -W -f base.ldif

Bu işlemler komut satırından yapılabileceği gibi OpenLDAP için geliştirilen "PhpLDAPAdmin" uygulaması ile arama, ekleme, silme vb. işlemler kullanılabilir. Şekil 3.13'de phpldapadmin yazılımının WEB arayüzü verilmiştir.




**Şekil 3.13. PhpLDapAdmin WEB arayüzü**

### 3.6.5. Phpldapadmin kurulumu:

Phpldapadmin uygulaması Ubuntu işletim sistemi depolarında bulunmaktadır. Kurulum için komut satırından aşağıdaki komut çalıştırılmalıdır;

```
sudo apt-get install phpldapadmin
```

Kurulum tamamlandıktan sonra phpLDAPadmin yazılımını, LDAP sunucusuna göre yapılandırmak için config.php dosyasında aşağıdaki satırlar organizasyona göre düzenlenmelidir;

```
sudo nano /etc/phpldapadmin/config.php
$servers->setValue('server','host','sunucu adı veya IP adresi');
$servers->setValue('server','base',array('dc=organizasyon,dc=edu,dc=tr'));
$servers->setValue('login','bind_id','cn=admin,dc=organizasyon,dc=edu,dc=tr ');
$config->custom->appearance['hide_template_warning'] = true;
```

### 3.6.6. Kimlik doğrulama ve yetkilendirme sunucusu:

Kablolu ve kablosuz ağlarda 802.1x ile kimlik doğrulama, yetkilendirme ve kayıt tutma gibi özen gerektiren işlemler için en yaygın kullanılan servistir. RADIUS (Remote Authentication Dial-in User Service) protokolü Livingston Enterprise tarafından geliştirilmiş, IETF tarafından Haziran 2000'de RFC2865 koduyla açık standart haline getirilmiştir.

Radius sunucu/istemci tabanlı çalışır. İstemcilerin istekleri NAS (Network Access Server) adı verilen cihaz üzerinden RADIUS sunucuya iletilir. NAS cihazı

kullanıcıların bağlanmak istedikleri AP, ağ anahtarı vb. cihazlardır. RADIUS sunucusu gelen kimlik doğrulama isteklerini belirlenen yapılandırmaya göre doğrulamaya çalışır ve sonucu NAS'a geri bildirir. Ayrıca RADIUS sunucusu gelen istekleri başka bir kimlik doğrulama sunucuna ileterek proxy görevi de yapabilir. İletişim genellikle UDP 1812 (Authentication) ve UDP 1813 (Accounting) portları üzerinden gerçekleştirilir. RADIUS protokolünü kullanarak kimlik doğrulaması gerçekleştiren pek çok ürün ve yazılım bulunmaktadır. Bunlardan en çok bilinen ve kullanılanı Freeradius'tur.

Haziran 1999'da Miquel Van Smoorenburg ve Alan Dekok tarafından geliştirilen Freeradius'un "alfa" yayımı Ağustos 1999'da yapılarak, Mayıs 2001'de ilk kararlı sürümü olan 0.1 versiyonu yayınlanmıştır. İlk sürümünden günümüze kadar pek çok güncelleme yapılmıştır. Mart 2018 tarihi itibariyle en son kararlı sürümü 3.0.16 sürümüdür. Freeradius ekibi tarafından gerçekleştirilen bir anket çalışmasında 50 binin üzerinde servis sağlayıcının günlük 100 milyondan fazla kullanıcının internete erişirken, kimlik doğrulama işlemlerinin, freeradius sunucuları tarafından gerçekleştirildiği ortaya çıkmıştır (The FreeRADIUS Server Project, 2018).

Ankete katılanlar arasında kullanıcı sayısı 10 ile 10.000.000 arasında olan kurumlar bulunmaktadır. Ankete katılan kurumların kullanıcı sayısı istatistikleri çizelge 3.1.'de verilmiştir (The FreeRADIUS Server Project, 2018).

**Çizelge 3.1 FreeRadius kullanıcı istatistikleri**

| Kullanıcı Sayıları | |
|---|---|
| **1-10** | %14 |
| **11-100** | %17 |
| **100-1000** | %25 |
| **$10^3$-$10^4$** | %25 |
| **$10^4$-$10^5$** | %13 |
| **$10^5$-$10^6$** | %4 |
| **$10^6$-$10^7$** | %1'den az |
| **$10^7$'den fazla** | %1 |

Freeradius kimlik doğrulamasını metin dosyası içerisine tanımlanan kullanıcı bilgilerine göre yapabilir. Bu yöntem az sayıda kullanıcısı olan kurumların tercih edebileceği bir yöntemdir. Kullanıcı sayısı arttıkça, LDAP (Lightweight Directory Access Protocol) ve SQL (Structured Query Language) gibi protokoller aracılığıyla

veri tabanı ve dizin servisleri kullanılarak kimlik doğrulama işlemi gerçekleştirilir. Ankete katılan kurum ve işletmelerin tercih ettikleri kullanıcı veri tabanı istatistikleri çizelge 3.2.'de gösterilmektedir.

**Çizelge 3.2 Veri tabanı istatistikleri**

| VERİ TABANI KULLANIMI | |
|---|---|
| **MySQL** | %32 |
| **User File** | %22 |
| **OpenLDAP** | %15 |
| **Active Directory** | %13 |
| **PostgreSQL** | %8 |
| **Oracle** | %5 |
| **Diğer** | %4'den az |

Freeradius dışında ürün ve yazılım kullananların istatistikleri çizelge 3.3.'de verilmiştir. Buna göre freeradius dışında pazarda en çok Cisco System ve Microsoft'un ürünleri tercih edilmiştir.

**Çizelge 3.3 Freeradius dışında kullanılan ürünler**

| KULLANILAN DİĞER YAZILIMLAR | |
|---|---|
| **Cisco ACS** | %24 |
| **Microsoft IAS** | %23 |
| **Cistron** | %12 |
| **Funk** | %11 |
| **OpenRADIUS** | %10 |
| **Radiator** | %10 |
| **Diğer** | %10 |

Freeradius'un kurum ve sistem yöneticileri tarafından bu kadar çok tercih edilmesinin nedenleri arasında, en başta açık kaynak kodlu ve GPL (General Public License - Genel Kamu Lisansı) lisansa sahip olması yer almaktadır. Bunların yanı sıra Freeradius, birçok kimlik doğrulma türünü ve kullanıcı veri tabanını desteklerler. Her kurum kendi ihtiyacına uygun olanı kullanabilmektedir.

### 3.6.7. Freeradius sunucusunun kurulumu:

Muğla Sıtkı Koçman Üniversitesi kablosuz ağında (eduroam) kimlik doğrulama sunucusu olarak Freeradius kullanılmaktadır. İşletim sistemi olarak Ubuntu Server

16.04.4 tercih edilmiştir. Freeradius Linux dağıtımlarının birçoğunun depolarında bulunmaktadır. Depolardan kurulum yaparken Freeradius'un için gerekli olan paketler otomatik olarak kurulur. Ubuntu depolarında bulunan paketlerin versiyonları

*#apt-cache policy <paket_adı>*

komutuyla kontrol edilebilir. Mart 2018 tarihi itibariyle Ubuntu depolarında freeradius 2.2.8 sürümü bulunmaktadır.


**Şekil 3.14. Ubuntu Server Depolarında Bulunan Freeradius Sürümü**

Ancak freeradius 2.x sürümlerine olan destek Eylül 2015 tarihinde sona ermiştir. Depolardan kurulum yapmak yerine 3.0.16 paketinin kaynak kodlarının derlenerek kurulması tercih edilmiştir. Freeradius TLS desteği için OpenSSL'i kullanır. OpenSSL tıpkı Freeradius gibi açık kaynak kodlu bir yazılımdır ve işletim sistemi ile birlikte 1.0.2g versiyonu kurulu gelir.


**Şekil 3.15. Ubuntu Server Depolarında Bulunan OpenSSL Sürümü**

Her yazılımda olduğu gibi OpenSSL'de de zafiyetler bulundukça güncellemeler yayınlanır. Mart 2018 tarihi itibariyle en kararlı sürüm 1.1.0'dır. 1.0.2 sürümünün 31 Aralık 2019 tarihine kadar destekleneceği duyurulmuştur (OpenSSL Management Committee., 2018).

### 3.6.8. OpenSSL'in kurulum aşamaları:

İşletim sisteminin yayınlandığı günden sonra yapılan güncellenmelerin alınması için;

```
$sudo apt-get update
$sudo apt-get upgrade
```

komutları kullanılır.

Kuruluma geçmeden önce paket derleyicilerinin kurulması gerekmektedir. Bunun için;

```
$sudo apt-get install build-essential
```

komutuluyla gcc/g++ derleyicileri yüklenmelidir.

freeradius'un bağımlı olduğu diğer paketlerin kurulması için;

```
$sudo apt-get install libssl-dev libtalloc-dev libpq-dev
```

**OpenSSL'in güncellenmesi:**

Kurulmak istenen openssl paketinin /home/kullanıcı dizinine indirilmesi için;

```
$cd /home/kullanıcı
$sudo wget https://www.openssl.org/source/openssl-1.0.2n.tar.gz
```

Paketin klasöre açılması için;

```
$sudo tar –zxvf openssl-1.0.2n.tar.gz
```

Paketin derlenmesi ve kurulması için;

```
$cd openssl-1.0.2n
$sudo ./config
$sudo make install
```

Paket derlenip kurulduktan sonra, işletim sistemine OpenSSL kütüphanelerinin yeni yerini bir sembolik bağlantı ile belirtmek gerekmektedir. Bunun için;

```
$ sudo ln -sf /usr/local/ssl/bin/openssl /usr/bin/openssl
```

Böylece Freeradius kurulumu için gerekli olan paketler yüklenmiş olur.

### 3.6.9. Freeradius'un indirilmesi ve derlenmesi:

Son kararlı sürümün /home/kulanıcı dizinine indirilmesi için;

```
$ sudo wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-3.0.16.tar.gz
```

Paketin klasöre açılması için;

```
$ sudo tar –zxvf freeradius-server-3.0.16.tar.gz
```

```
$ cd freeradius-server-3.0.16
```

Paketin derlenmesi ve kurulması için;

```
$ ./configure
$ sudo make
$ sudo make install
```

Kurulum tamamlandıktan sonra radiusd –X komutu ile varsayılan ayarlar ile hata ayıklama (debug) modunda freeradius çalıştırılır ve test edilir. Kullanılacak kimlik doğrulama yöntemi belirlendikten sonra ayarların yapılandırılması gerekmektedir. Muğla Sıtkı Koçman Üniversitesi'nde kimlik doğrulama yöntemi olarak eduroam federasyonunun tercih ettiği EAP-TTLS/PAP kimlik doğrulama yöntemi seçilmiştir.

TTLS yapısı gereği istemci ve sunucu arasında oluşturulan tünel vasıtası ile kimlik doğrulama işlemi gerçekleştirir. Kurulan tünelin güvenliği SSL ile sağlanmaktadır. Freeradius için gerekli SSL sertifikası, güvenilir sertifika otoritelerinden temin edilen sertifikalar olabilir. Sertifika temin etmek yerine OpenSSL marifetiyle kuruma özel sertifika üretilip, imzalanabilir. Bu tarz sertifikalara "Self-Singed" sertifikalar denilmektedir. Freeradius kurulurken varsayılan olarak üretilen sertifikalar "/usr/local/etc/raddb/certs" klasöründe bulunur. Varsayılan sertifikaların silinerek özelleştirilmiş yeni sertifikanın üretimi şöyle gerçekleştirilir.

```
# rm -f  *.crt *.der *.key *.csr *.p12 serial* *.pem index.txt* dh random
```

ca.cnf, client.cnf ve server.cnf dosyalarının, nano, pico veya vi gibi herhangi bir metin editörü ile bu dosyaların düzenlenmesi gerekmektedir.

ca.cnf dosyasının düzenlenmesi gereken satırları;

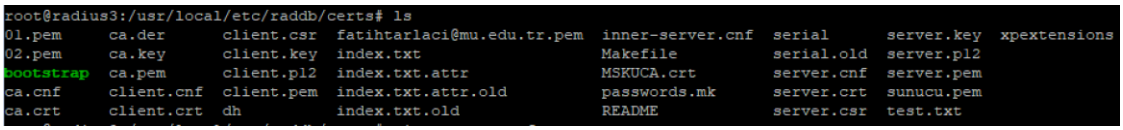
```
[ req ]
prompt                  = no
distinguished_name      = certificate_authority_adı
default_bits            = 2048
input_password          = ca_şifresi_input_şifresi
output_password         = ca_output_şifresi
x509_extensions         = v3_ca

[certificate_authority]
countryName             = TR
stateOrProvinceName     = MUGLA
```

```
localityName            = MUGLA
organizationName        = MUGLA SITKI KOCMAN UNIVERSITESI
emailAddress            = eposta_adresi@mu.edu.tr
commonName              = "MSKU Authority"

#server.cnf dosyasının düzenlenmesi gereken satırlar;
[ req ]
prompt                  = no
distinguished_name      = sunucu_adı
default_bits            = 2048
input_password          = input_sifresi
output_password         = output_sifresi
[server]
countryName             = TR
stateOrProvinceName     = MUGLA
localityName            = MUGLA
organizationName        = MUGLA SITKI KOCMAN UNIVERSITESI
emailAddress            = eposta_adresi@mu.edu.tr
commonName              = "MSKU AUTHORITY"
#client.cnf dosyasının düzenlenmesi gereken satırlar;
[ req ]
prompt                  = no
distinguished_name      = client
default_bits            = 2048
input_password          = input_sifresi
output_password         = output_sifresi
[client]
countryName             = TR
stateOrProvinceName     = MUGLA
localityName            = MUGLA
organizationName        = MUGLA SITKI KOCMAN UNIVERSITESI
emailAddress            = eposta_adresi@mu.edu.tr
commonName              = eposta_adresi@mu.edu.tr
```

Bu düzenlemeler yapıldıktan sonra *./bootstrap* scripti çalıştırılarak sertifikalar oluşturulur. Sertifika oluşturma işlemi bittiğinde "certs" klasöründe üretilen sertifikalar görülmektedir. Şekil 3.16'da üretilen sertifikalar verilmiştir.




**Şekil 3.16. OpenSSL certs klasörü**

### 3.6.10. Sanal sunucu (virtual server) kavramı:

Sanal sunucu kavramı, ağ üzerinde farklı politikalara ihtiyaç duyulması halinde tek bir RADIUS sunucu ile bu ihtiyaçların karşılanabilmesini sağlamak amacıyla geliştirilmiştir. Örneğin ağdaki bir bölgede TTLS-PAP ile kimlik doğrularken başka bir bölgede PEAP-MSCHAPv2 kimlik doğrulaması gerekebilir. Sanal sunucular bu gibi durumlarda oldukça esnek bir yapı sağlayarak, istenilen şekilde yapılandırılabilirler.

Sanal sunucu tanımlamaları /usr/local/etc/raddb/sites-available dizini içerisinde bulunur. Aktif olabilmesi için /usr/local/etc/raddb/sites-enabled dizinine sembolik link ile bağlanması gerekir.

Muğla Sıtkı Koçman Üniversitesi'nde kimlik doğrulama işlemleri OpenLDAP dizin servisi üzerinden gerçekleştirilmektedir. Bu nedenle RADIUS sunucusu ldap modülüne göre yapılandırılmıştır. OpenLDAP'ın kurulum ve yapılandırması bir sonraki başlıkta anlatılacaktır.

EAP dosyasında belirtilen eduroam sanal sunucusunun yapılandırılması;

```
server eduroam {
#sunucunun dinleyeceği portlar belirlenir
        listen {
                type = "auth"
                ipaddr = *
                port = 1812
        }
        listen {
```

```
            type = "acct"
            ipaddr = *
            port = 1813
        }
#yetkilendirme için kullanılacak modüller belirtilir.
      authorize {
            auth_log
            suffix
            ldap
            eap
            pap
            files
}
#kimlik doğrulama yöntemi belirtilir.
       authenticate {
       Auth-Type PAP {
       pap
                    }
       eap
      }
#kimlik doğrulama yapılırken ldap modülü ve dizin servisi tercih edilmiştir.
Auth-Type LDAP {
       ldap
       }
       preacct {
            suffix
       }
       accounting {
       }
       post-auth {
            # detaylı loglama için
            reply_log
            exec
            detail
            Post-Auth-Type REJECT {
```

```
                reply_log
            }
        }
        pre-proxy {
            # detaylı loglama için
            pre_proxy_log
            detail
            if("%{Packet-Type}" != "Accounting-Request") {
                attr_filter.pre-proxy
            }
        }
        post-proxy {
            # detaylı loglama için
            detail
             post_proxy_log
            attr_filter.post-proxy
        }
}
```

### 3.6.11. LDAP modülünün yapılandırılması:

LDAP modülü dizin servisleri ile iletişimi sağlayan modüldür ve /usr/local/etc/raddb/mods-enabled/ dizini içerisinde yer alır. LDAP sunucu tanımları aşağıdaki gibi yapılır;

```
ldap
{
server = IP_yada_hostname_adresi'
identity = "cn=admin,dc=domain,dc=edu,dc=tr"
password = admin_şifresi
base_dn = 'dc=domain,dc=edu,dc=tr'
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"#istenilen başka filtreler varsa düzenlenebilir.
ldap_connections_number = 5
timeout = 4
timelimit = 3
net_timeout = 1
```

```
tls {
start_tls = no# İstenirse iki sunucu arası TLS yapılandırması ilave güvenlik sağlanabilir.
}
```

### 3.6.12. Freeradius'un EAP-TTLS için yapılandırılması:

```
#/usr/local/etc/raddb/radius.cnf dosyasının düzenlenmesi
stripped_names = yes #kullanıcı_adının_loglanması
auth = yes# kimlik_doğrulamaların_loglanması
```

Freeradius 2.X serisinde eap.cnf dosyası raddb dizinindeyken, 3.X sonrası tüm modüller raddb/mods-available dizini altında toplanmıştır. Modülleri etkinleştirmek için raddb/mods-enabled dizin ile sembolik bağlantı ile bağlanması gerekmektedir.

### 3.6.13. EAP dosyasının düzenlenmesi:

```
#/usr/local/etc/raddb/mods-available/eap dosyasının düzenlenmesi
eap {
default_eap_type = ttls
tls {
certs private_key_password = sertifika_keyi
private_key_file = ${certdir}/server.pem
ttls {
default_eap_type = md5
copy_request_to_tunnel = yes
use_tunneled_reply = yes
virtual_server = "eduroam"
```

### 3.6.14. Proxy.conf dosyasının düzenlenmesi:

```
#/usr/local/etc/raddb/proxy.cnf dosyasının düzenlenmesi:
proxy server {
#
default_fallback = yes
}
home_server üst_otorite_adi {
type = auth+acct
```

```
ipaddr = ulakbim_sunucu_ipv4_adresi
# ipv6addr = ulakbim_sunucu_ipv6_adresi #ipv6 adresi dağıtılıyorsa tanımlanır.
port = 1812
secret = üst_sunucuda_tanımlanan_şifre
response_window = 20
zombie_period = 40
revive_interval = 120
status_check = status-server
check_interval = 30
num_answers_to_alive = 3
}
home_server trrad02 {
type = auth+acct
ipaddr = ulakbim_sunucu_ipv4_adresi
# ipv6addr = ipv6_adresi #ipv6 adresi kullanılıyorsa tanımlanır.
port = 1812
secret = üst_sunucuda_tanımlanan_şifre
response_window = 20
zombie_period = 40
revive_interval = 120
status_check = status-server
check_interval = 30
num_answers_to_alive = 3
}
home_server_pool EDUROAM-FTLR {
type = fail-over
home_server = birincil_sunucu_adi
home_server = ikincil_sunucu_adi
}
realm domain.edu.tr {
strip
}
realm "~\\.domain\\.edu\\.tr$" {
strip
}
```

```
realm DEFAULT {
pool = EDUROAM-FTLR
nostrip
}
realm LOCAL {
}
realm NULL {
}
```

### 3.6.15. Client.cnf dosyasının düzenlenmesi:

Client.cnf dosyası ağ üzerinde kimlik doğrulayıcı olarak çalışan, AP, ağ anahtarı vb. cihazlarını ve üst yetkilendirici sunucusunun tanımlandığı dosyadır. Kimlik doğrulama yapacak cihazın, IP adresi ve kimlik doğrulama yaparken kullanılan şifresi gibi bilgilerin girilmesi zorunludur. Aksi halde kimlik doğrulama istekleri reddedilecektir. Tek bir IP adresine izin verilebileceği gibi bir alt ağ için de tanımlama yapılabilmektedir.

```
client localhost {
ipaddr = 127.0.0.1
secret = belirlenen_şifre
require_message_authenticator = no
nas-type = other
}
client 172.16.0.0/16 {
secret = belirlenen şifre
shortname = eduroam
virtual_server = eduroam
nas-type = other
}
```

Freeradius sunucusunun EAP-TTLS ve faz 2'de PAP kimlik doğrulamasına ilave olarak kullanıcı veri tabanı OpenLDAP kimlik doğrulaması olacak şekilde uygulanacak ayarlar tamamlanmıştır.

### 3.6.16. Kablosuz ağ kontrolörü:

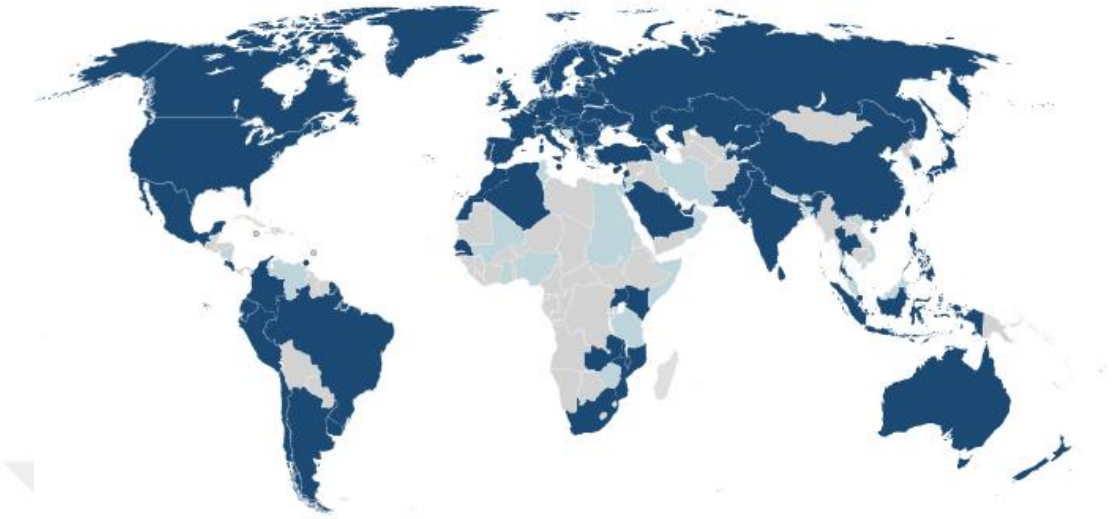
Kablosuz ağların geniş ölçekli alan ve yerleşkelerde kullanılmaya başlanması ile birlikte ağda konumlandırılan AP sayısı önemli ölçüde artmıştır. Öyle ki bu sayı, ortalama bir kampüs ağında yüzlerce AP'ye tekabül etmektedir. Her bir AP'nin yönetimini ayrı ayrı yapmak oldukça güç olacaktır. Birçok üretici ağdaki tüm AP'lerin merkezi bir cihaz üzerinden yönetilmesi amacıyla, kablosuz ağ kontrolörü (WLC-Wireless LAN Controller) çözümü sunmaktadır.

Bu çözümler genelde donanım (appliance) veya sanallaştırılmış yazılım (virtual appliance) olabilmektedir. Ağa konumlandırılan AP, DNS (Domain Name Server) sorgusu veya DHCP (Dynamic Host Configuration Protocol) option 43 yöntemiyle WLC'ye kendisini kayıt eder. Kayıt işleminin ardından ağdaki tüm AP'lerin, kimlik doğrulama yöntemi, WLAN'lar ve yazılım güncellemeleri gibi pek çok yapılandırma WLC üzerinden yapılır. Muğla Sıtkı Koçman Üniversitesi merkez kampüsünde Cisco 8540 WLC ile birlikte 300'ün üzerinde AP'nin yönetimi yapılmaktadır.

## 3.7. Eduroam Altyapısı:

Eduroam (Education Roaming- Eğitim Gezgini), uluslararası araştırma ve eğitim topluluğu için geliştirilmiş güvenli, dünya çapında internet dolaşım ve erişim hizmetidir. Eduroam üyesi olan kurumlar hem kendi kurumundaki kullanıcıların internete bağlanmasını, hem de diğer eduroam üyesi kurum kullanıcılarının internete erişimini sağlar. Eduroam'un hizmeti hiyerarşik federasyon yapısı ile sağlanır. Her ülkenin veya bölgenin ana RADIUS sunucusu bulunur. Türkiye'de bu sunucu TÜBİTAK ULAKBİM'dedir. Bu sunucu, üst yetkilendirme sunucuları olan Avrupa Eduroam Konfederasyonu ve Asya-Pasifik Eduroam Konfederasyonu sunucuları ile iletişim halindedir. Mart 2018 tarihi itibariyle Dünya genelinde 89 ülkede aktif kullanımda, 26 adet ülkede pilot eduroam yetkilendirmesi yapan ana sunucu

bulunmaktadır. Bünyesinde eduroam üyesi barındıran ülkeler Şekil 3.17.'de koyu mavi renkte gösterilmektedir (Eduroam, 2018).

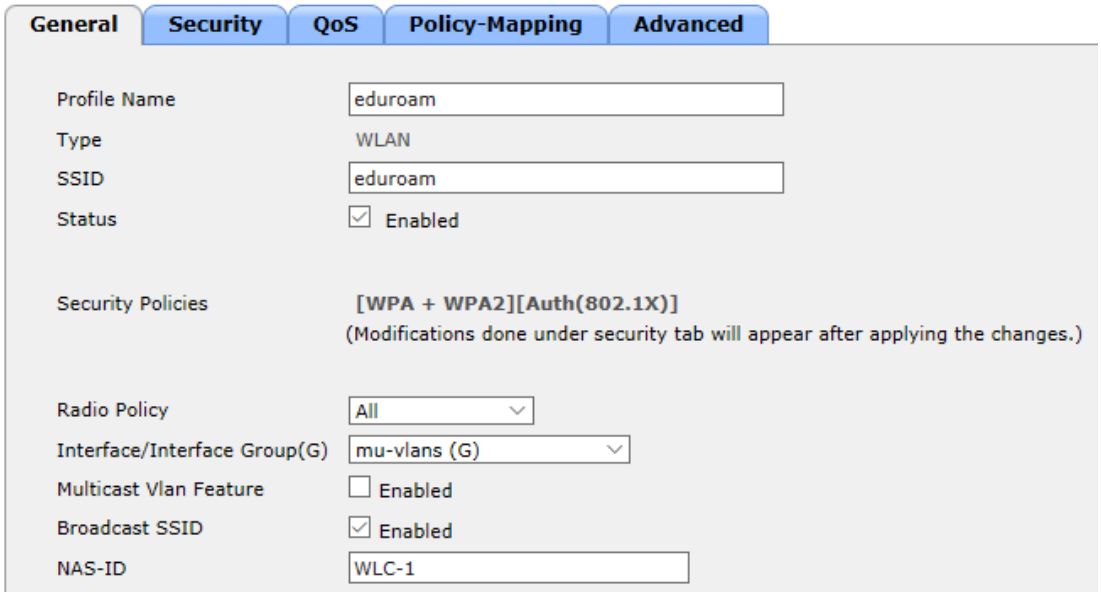


**Şekil 3.17. Eduroam üyesi olan ülkeler (Eduroam, 2018)**

Domain eki (@domain.edu.tr) ile misafir ağda oturum açmaya çalışan kullanıcının isteği federasyonun üst otoritesi olan ana RADIUS sunucusuna proxy edilir. Ana sunucu isteğin domain ekine göre kullanıcının kendi kurum sunucusuna bu isteği iletir. Yetkilendirmenin başarılı olup olmadığına kullanıcının kendi kurumunda ki RADIUS sunucusu karar verir. Böylece kullanıcının kimlik ve şifre bilgileri misafir olduğu RADIUS sunucusu tarafından bilinmez. Eduroam alt yapısındaki RADIUS sunucularının büyük bir çoğunluğu FreeRADIUS'tur. Proxy işlemi bir kullanıcının kimlik doğrulamasını yapmak için uzak bir RADIUS sunucusuna danışabileceği anlamına gelir. Bunun için FreeRadius'un proxy.cnf doyası düzenlenmeli ve RADIUS sunucularının karşılıklı olarak client.cnf dosyalarına eklenmesi gerekmektedir.

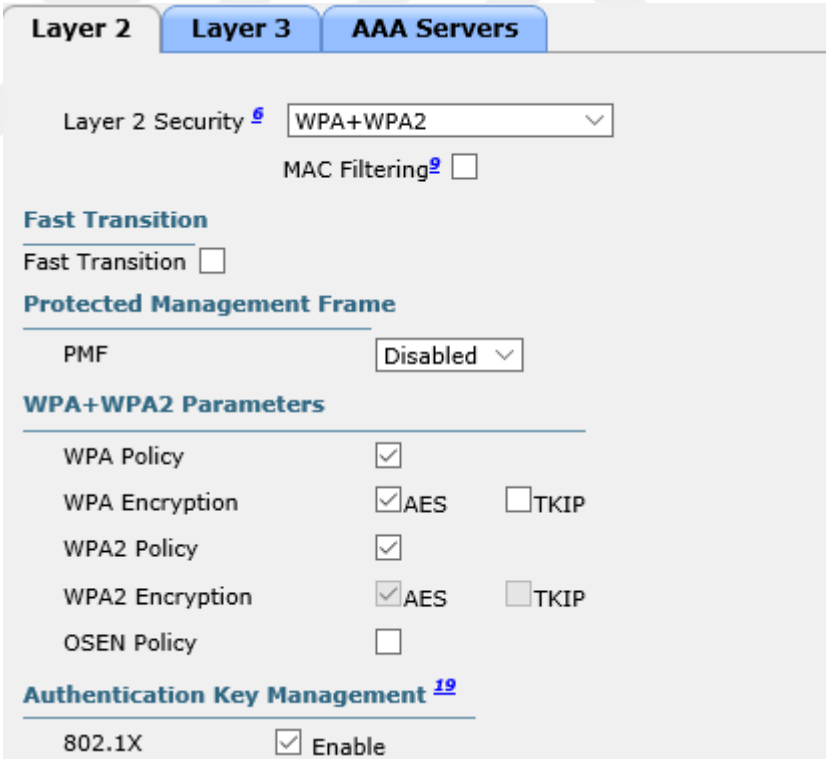
## 3.8. Cisco 8540 WLC'de Yapılan Ayarlar:

WLAN sekmesinden oluşturulmak istenen SSID ve profil adı belirtilerek yeni bir WLAN oluşuturulabilir veya mevcut WLAN'lar üzerinde düzenleme yapılabilir.Şekil 3.18'de SSID oluşturma işlemi verilmiştir.



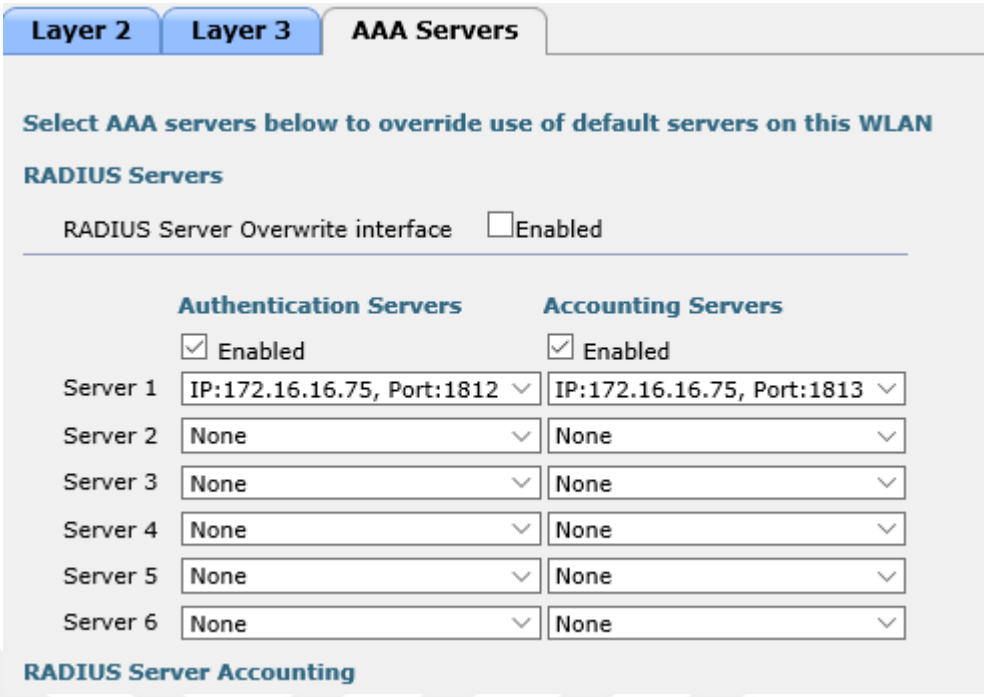

**Şekil 3.18. SSID oluşturma işlemi**

Kimlik Doğrulama yöntemi 802.1x seçilmiştir. Şifreleme algoritması AES olarak belirlendiği şekil 3.19'da gösterilmiştir.



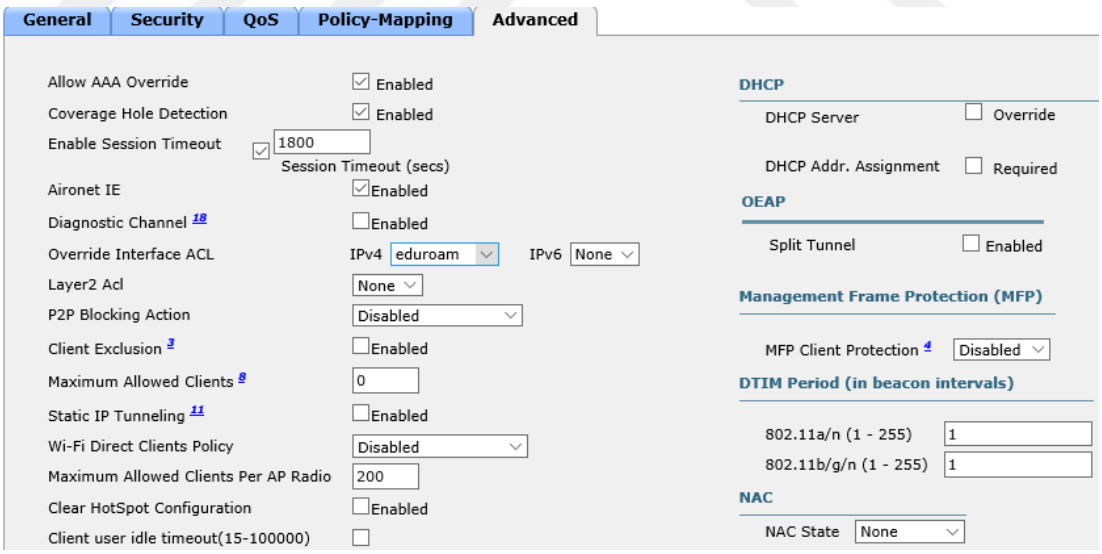

**Şekil 3.19. Kimlik doğrulama ayarları**

Kimlik doğrulaması yapılacak olan RADIUS sunucusu seçilir. Daha önce bir RADIUS sunucu tanımlanmadıysa, SECURITY→AAA→Authentication/Accounting menüleri ile şekil 3.20'deki gibi tanımlama yapılabilir.




**Şekil 3.20. WLC RADIUS ayarları**

Kullanıcıların ilgili VLAN'lara atanabilmesi amacıyla, AAA Override özelliği aktif edilmelidir. Oluşturulmuş bir ACL varsa Override Interface ACL menüsünden ilgili ACL şekil 3.21'deki gibi seçilmelidir.




**Şekil 3.21. SSID ACL ayarları**

Kullanıcıların atanacağı VLAN'ların CONTROLLER→Interfaces altında tanımlanması gerekmektedir. WLC'nin bağlı olduğu uplink portu, ilgili VLAN'ların tamamına Trunk port olarak tanımlanması gerekmektedir.

## 3.9. CACTI

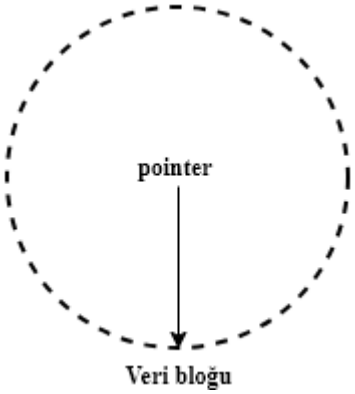
CACTI popüler ve kullanışlı bir ağ izleme yazılımıdır. GPL lisanslı ile ücretsiz olarak kamunun hizmetine sunulmuştur. Ağın grafiksel olan izlenebilmesi için RRDTool (Round Robin Database Tool), MySQL, PHP (Hypertext Preprocessor) kullanılır. Ağ cihazının band genişliği, CPU (Central Processing Unit-Merkezi İşlem Birimi), RAM ve daha birçok donanımsal kapasitenin ölçümü gerçekleştirilir. Bunun için SNMP protokolü aracılığıyla cihazın CACTI sunucusuna tanımlanması gerekir.

## 3.10. RRDTool:

RRDTool, Round Robin Veritabanı aracıdır ve CACTI'nin omurgasını oluşturur. Perl, Python, TCL (Tool Command Language - Araç Komut Dil Aracı), PHP gibi birçok dil ile veri bağlantısı yapabilir.

RRD aracının temel amacı, bir veya daha fazla değerin belirli bir periyot içindeki eğilimini gösteren zaman grafiğinin oluşturulmasıdır. Zaman grafiğinde, X ekseni değişkenlerin değerini, Y ekseni de zaman değerini gösterir. RRD grafikleri, RRD veri tabanından çıkarılan verilerinden oluşturulur. RRDTool ayrıca bu veri tabanını oluşturma ve besleme yeteneğine de sahiptir (Luteus Sarl, 2018).

RRD veri tabanının yapısı diğer doğrusal veri tabanlarından farklıdır. RRDTool veri tabanları öncelikli olarak izleme için kullanılır ve yapı bakımından çok basittir. Doğrusal veri tabanlarında veri oluşturulan tabloların alt kısmına eklenir. Böylece veri tabanının boyutu artarak devam eder. RRDTool veri tabanında ise dairesel bir yapı söz konusudur. Okuma ve yazma işlemleri bir pointer aracılığıyla, başlangıç ve bitiş noktası olmayan, dairesel bir yapı üzerinde gerçekleştirilir. Veri bu çember üzerine kaydedilir. Böylece RRD'nin boyutu her zaman sabit kalır. Round Robin ismi de buradan gelmektedir (Oetiker, 2018). RRD'nin çalışma mantığı şekil 3.22'de verilmiştir.




**Şekil 3.22. RRD veri tabanı yapısı**

RRDTool yeni bir değer almazsa, o aralık için UNKNOWN değerini saklar. Bu nedenle, RRDTool veri tabanını kullanılırken, veri tabanını güncelleştirmek için sürekli bir veri akışı sağlamak gerekir. Geçmişe yönelik verilerin saklanması için ağ cihazından alınan örneklerin saklanması gerekir. Alınan her örneğin saklanması, sunucu üzerinde önemli miktarda disk kapasitesinin kullanılmasına neden olacaktır. Bunun için CF (Consolidation Function - Konsolidasyon Fonksiyonu) tanımlanır. AVERAGE (Ortalama), MAX (En Yüksek), MIN (En Düşük), LAST (En Son) olmak üzere 4 farklı CF kullanılarak, veriler tasnif edilir ve RRA (Round Robin Archive) üzerinde saklanabilir (Luteus Sarl, 2018).

# 4. BULGULAR

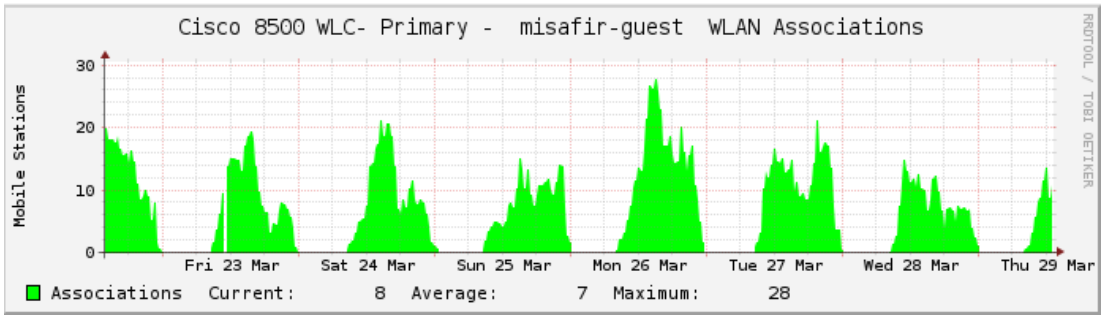
## 4.1. Kampüs Ağında Sanal Yerel Ağ Tasarımı:

Yerel sanal ağ tasarımı yönetimsel ve teknik açıdan değerlendirilebilir. Yönetimsel açıdan ağda oturum açacak kullanıcı tipi ve sayısı gibi değerler göz önünde bulundurulur. Teknik açıdan ise ağda konumlanacak cihazların en yüksek verimle ağda çalışabilmeleri amaçlamaktadır.

## 4.2. Kablosuz Kampüs Ağında Sanal Yerel Ağ Tasarımı:

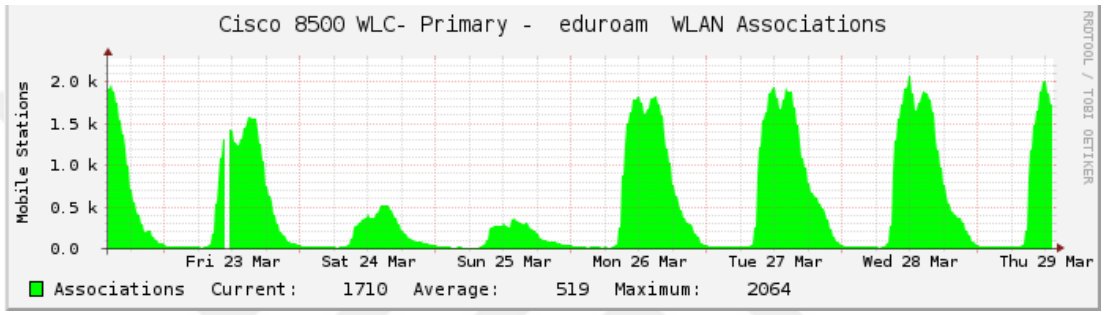
Muğla Sıtkı Koçman Üniversitesinde kullanıcılar akademik personel, idari personel, öğrenci ve misafir olmak üzere 4 farklı başlık altında ele alınmıştır. Kablosuz ağda sadece anlatılan "eduroam" ve misafir-guest yayını yapılmaktadır.

Misafir yayını bir hotspot yayınıdır. Kısıtlı alanlarda yapılan bu ağa dahil olmak isteyen kullanıcılar sisteme kendilerini SMS (Short Message Service- Kısa Mesaj Servisi) veya MERNİS (Merkezî Nüfus İdare Sistemi) doğrulamasıyla kayıt ederler. Ağa dahil olan kullanıcıların kimliği tam olarak belirlendikten sonra 5651 sayılı "internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun" kapsamında internet trafiği kayıt altına alınır. Hotspot yayın bu tezin kapsamı dışında tutulmuştur. Kampüs içerisinde konuk evi ve kütüphane gibi kamuya açık yerler dışında yayını yapılmamaktadır. Haftalık kullanıcı grafiği Şekil 4.1'de gösterilmektedir.



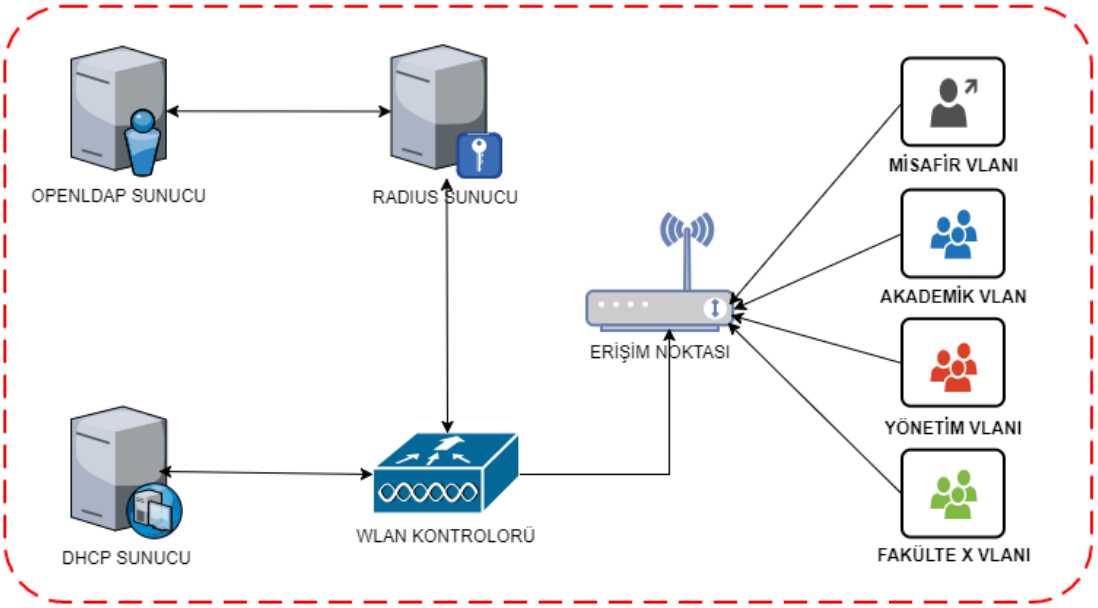

**Şekil 4.1. Misafir-Guest yayını haftalık kullanıcı sayıları**

MSKÜ kablosuz ağının neredeyse tamama yakını eduroam yayını ile sağlanmaktadır. Eduroam ağı haftalık kullanıcı istatistiklerini gösteren grafik Şekil 4.2.'de verilmiştir.




**Şekil 4.2. . Eduroam yayını haftalık kullanıcı sayıları**

Bölüm 3'de kurulum ve yapılandırmaları anlatılan sunucuların oluşturdukları genel yapı Şekil 4.3.'de gösterildiği gibi tasarlanmıştır. Tüm kullanıcılar için toplamda 45 adet VLAN oluşturulmuştur.

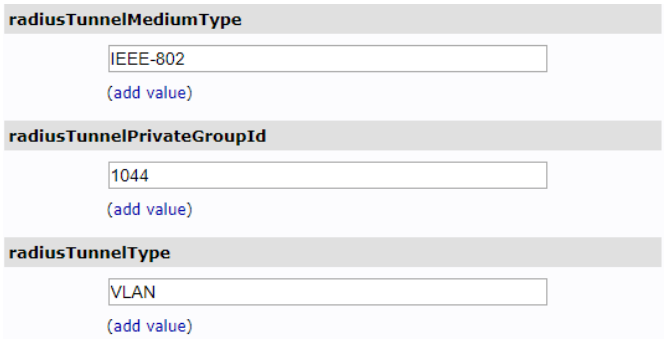



**Şekil 4.3. Genel yapı**

## 4.3. Uygulama:

İki farklı senaryo hazırlanarak ağdaki değerler SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü) protokolü ve CACTI yazılımı ile takip edilmiştir (IEEE, 2018a). Senaryo 1'de tüm öğrenciler tek bir VLAN içerisinde gruplanmış ve ağda oluşan kullanıcı sayıları, broadcast paket sayıları, kimlik doğrulama yöntemleri, toplam yapılan trafik incelenmiştir. Güvenlik nedeniyle akademik ve idari personel VLAN'ları ayrı tutulmuştur. Senaryo 2'de tüm kullanıcıların için 45 adet VLAN oluşturulmuş ve ağda gruplanmışlardır. Ağda oluşan kullanıcı sayıları, broadcast paket sayıları, kimlik doğrulama yöntemleri, toplam yapılan trafik incelenmiştir. Tüm kullanıcılar, kendileri için oluşturulan VLAN grubu altında ağa dahil olurken, ağdaki kullanıcı sayıları, broadcast paket sayıları, kimlik doğrulama yöntemleri ve WLC portlarındaki toplam yapılan trafik incelenmiştir. WLC 2 adet 10 Gbit/s'lık portlar üzerinden Cisco Nexus 9504 omurga anahtara bağlanmıştır. Port channel ile toplamda 20 Gbit/s lık bir hat elde edilmiştir. Tüm ağ istatistikleri ve raporlar bu portlar üzerinden alınmıştır.

Öncelikli olarak kullanıcılar için tasarlanan VLAN'lar ve VLAN arayüzleri omurga anahtar ve WLC üzerinde oluşturulmuştur. Daha sonra fakülte ve birimine göre OpenLDAP'ta kayıtlı kullanıcı özellikleri Şekil 4.4.'de ki gibi düzenlenmiştir.




**Şekil 4.4. OpenLDAP kayıt özellikleri**

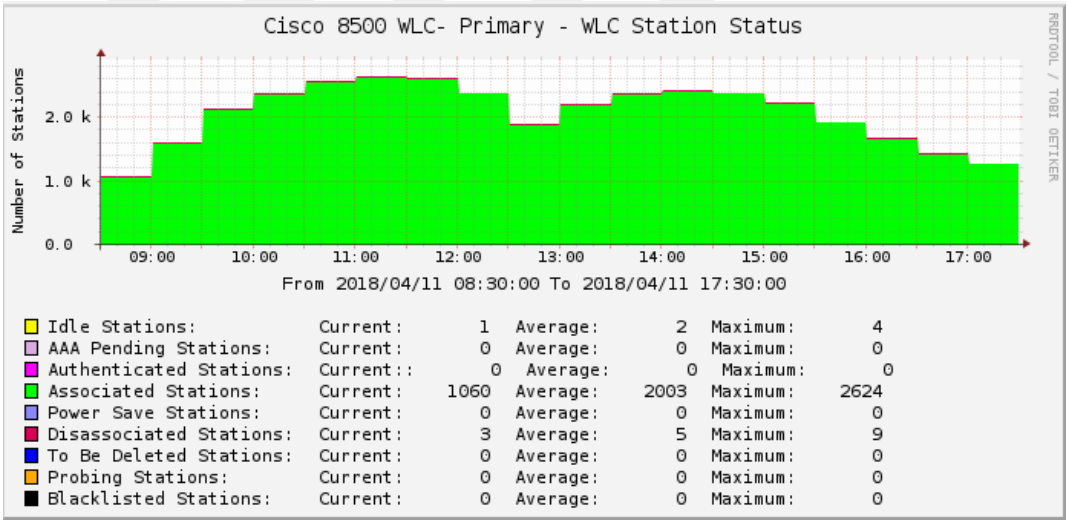
Her eğitim öğretim dönemi başında üniversiteye kaydolan öğrencilerin kendilerini sisteme kayıt edebilecekleri bir internet arayüzü geliştirilmiştir (SARIMAN, 2018). Bu kayıt esnasında öğrencinin e-posta hesabı oluşturulur ve fakültesine göre VLAN bilgisi OpenLDAP sunucusuna otomatik olarak yazılır. Öğrenci mezun olana kadar hesabını aktif olarak kullanabilmektedir. Freeradius schema'larına eklenen AgErisimi

(Network Access) özellik değeri öğrencinin mezuniyeti sonrası “False” olarak değiştirilir ve ağa dahil olması engellenir.

```
filter="(&(agErisimi=TRUE)(mail=%{%{Stripped-User-Name}:-%{User-Name}}))"
```

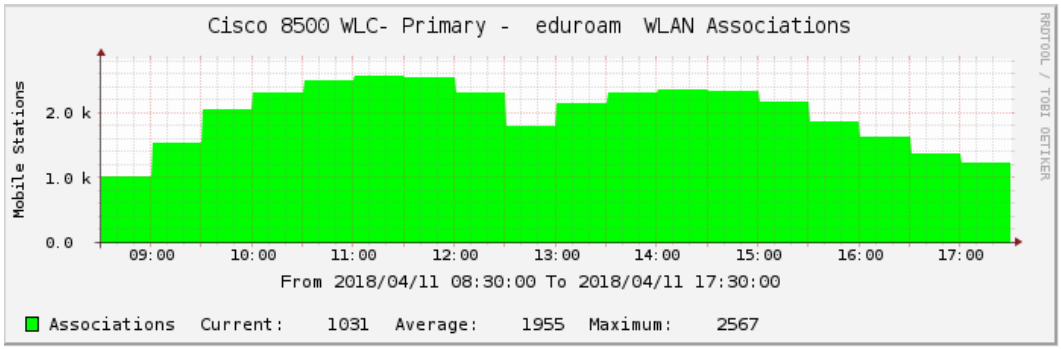
### 4.4. Senaryo 1: Statik Vlan Ataması:

Kullanıcılar WLC’de statik olarak tek bir VLAN altında gruplanmışlardır. Testler kablosuz ağın en yoğun kullanıldığı sabah 8:30 ile akşam 17:30 arasında ve 9-13 Nisan 2018 tarihlerinde gerçekleştirilmiştir. Belirlenen saatler arasında ağa 1773 ile 2624 arasında kullanıcı dahil olmuştur. En yüksek bağlantı sağlanan tarih 11 Nisan 2018 günü olmuştur. Kablosuz ağda başarılı bir şekilde oturum açan kullanıcıların sayısı Şekil 4.5.’de verilmiştir.



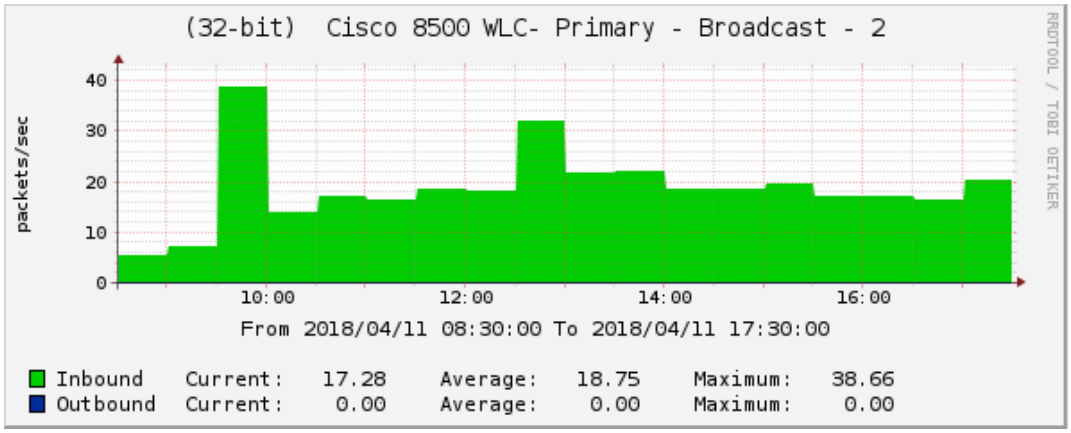

**Şekil 4.5. Senaryo-1 Ağ ile ilişkilendirilen kullanıcı sayıları**

Ağa katılan kullanıcıların 2567 adeti eduroam ağına dahil olmuştur.



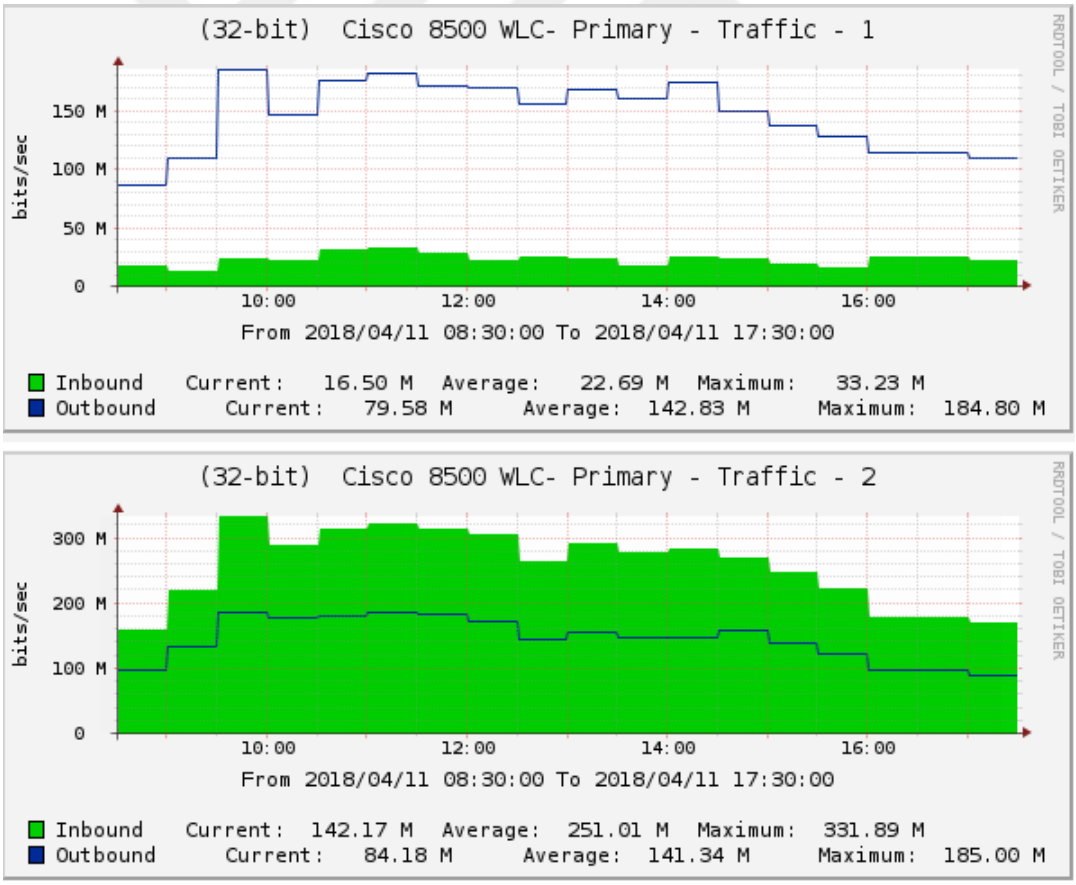

**Şekil 4.6. Senaryo-2 eduroam ağına bağlanan kullanıcı sayısı**

Günlük olarak WLC'nin portlarında saniyede oluşan broadcast sayısı ölçülmüş ve şekil 4.7'de verilmiştir.




**Şekil 4.7. Senaryo-1 Broadcast paket sayısı**

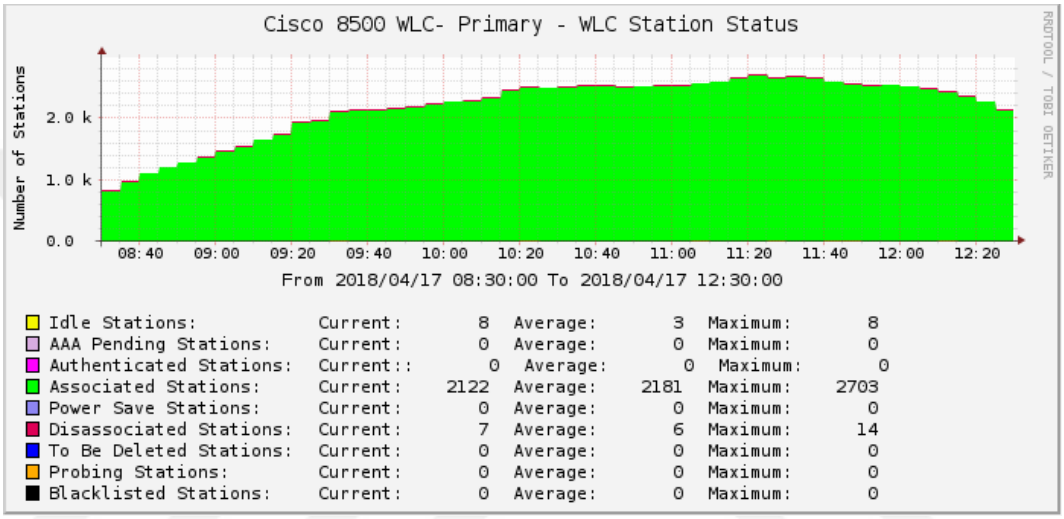
Günlük olarak WLC'nin portlarında saniyede oluşan trafik ölçülmüş ve şekil 4.8'de verilmiştir.




**Şekil 4.8. Senaryo-1 TenGigabit port trafik grafikleri**

## 4.5. Senaryo 2: Dinamik VLAN Ataması

Kullanıcılar departman ve fakültelerine göre 45 adet VLAN'a atanarak ağa dahil olmuşlardır. Yapılan testler 6-20 Nisan 2018 tarihinde günün en yoğun olduğu sabah 8:30 ile akşam 17:30 arasında gerçekleştirilmiştir. Belirlenen saatler arasında ağa 1774 ile 2678 arasında kullanıcı dahil olmuştur. Kullanıcıların tamamına yakını başarılı bir şekilde ağda oturum açmış ve internet erişimi bulunmaktadır. Kullanıcıların tamamına yakını eduroam ağında katılmışlardır.




**Şekil 4.9. Senaryo-2 Ağ ile ilişkilendirilen kullanıcı sayıları**

Senaryo 1'de olduğu gibi Günlük olarak WLC'nin portlarında saniyede oluşan broadcast sayısı ve giriş-çıkış trafikleri ölçülmüş ve kaydedilmiştir. Elde edilen sonuçlar, değerlendirme bölümünde tartışılmıştır.

## 4.6. Dinamik VLAN Uygulaması ve Güvenlik:

WLC'de oluşturulan ACL(Access Control List-Erişim Kontrol Listeleri) ile istenilen kaynak ve hedef adresleri belirtilerek erişim denetimi sağlanabilmektedir. Şekil 4.10.'da WLC üzerinde yazılan ACL görüntülenmektedir. VLAN kullanımı kurum içerisinde kullanılan Firewall, IPS/IDS için daha detaylı kurallar yazabilme imkanı tanımaktadır. Öğrenci VLAN'larından, TELNET (Telecommunication Network), SSH (Secure Shell), RDP (Remote Desktop Connection) gibi bazı portların yanı sıra, sadece personelin kullanması gereken servislere erişim kısıtlanmıştır.

Deny Counters 3024780

| Seq | Action | Source IP/Mask | | Destination IP/Mask | | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 0.0.0.0 | / 0.0.0.0 | 10.2.2.2 | / 255.255.255.255 | UDP | Any | Any | Any | Inbound | 1377208 |
| 2 | Permit | 10.2.2.2 | / 255.255.255.255 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | Any | Any | Outbound | 1347416 |
| 3 | Permit | 0.0.0.0 | / 0.0.0.0 | 10.2.2.3 | / 255.255.255.255 | UDP | Any | Any | Any | Inbound | 188713 |
| 4 | Permit | 10.2.2.3 | / 255.255.255.255 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | Any | Any | Outbound | 173828 |
| 5 | Permit | 172.0.0.0 | / 255.0.0.0 | 172.16.16.75 | / 255.255.255.255 | UDP | RADIUS | RADIUS | Any | Inbound | 0 |
| 6 | Permit | 172.16.16.75 | / 255.255.255.255 | 172.0.0.0 | / 255.0.0.0 | UDP | RADIUS | RADIUS | Any | Outbound | 0 |
| 7 | Permit | 172.0.0.0 | / 255.255.255.255 | 10.2.2.6 | / 255.255.255.255 | Any | Any | Any | Any | Inbound | 0 |
| 8 | Permit | 10.2.2.6 | / 255.255.255.255 | 172.0.0.0 | / 255.0.0.0 | Any | Any | Any | Any | Outbound | 0 |
| 9 | Permit | 172.22.240.0 | / 255.255.248.0 | 0.0.0.0 | / 0.0.0.0 | Any | Any | Any | Any | Inbound | 13494408 |
| 10 | Permit | 172.22.224.0 | / 255.255.248.0 | 0.0.0.0 | / 0.0.0.0 | Any | Any | Any | Any | Inbound | 18071037 |
| 11 | Permit | 0.0.0.0 | / 0.0.0.0 | 172.22.224.0 | / 255.255.248.0 | Any | Any | Any | Any | Outbound | 31905703 |
| 12 | Permit | 0.0.0.0 | / 0.0.0.0 | 172.22.240.0 | / 255.255.248.0 | Any | Any | Any | Any | Outbound | 23412233 |
| 13 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | FTP Control | Any | Any | 120 |
| 14 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | FTP Control | Any | Any | 6384 |
| 15 | Deny | 0.0.0.0 | / 0.0.0.0 | 10.1.1.75 | / 255.255.255.255 | Any | Any | Any | Any | Inbound | 0 |
| 16 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | 22 | Any | Any | 5147 |
| 17 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | 22 | Any | Any | 0 |
| 18 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | Telnet | Any | Any | 2730 |
| 19 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | Telnet | Any | Any | 5081 |
| 20 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | UDP | Any | 3389 | Any | Any | 0 |
| 21 | Deny | 0.0.0.0 | / 0.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | 3389 | Any | Any | 5075 |
| 22 | Deny | 0.0.0.0 | / 0.0.0.0 | 10.1.1.73 | / 255.255.255.255 | Any | Any | Any | Any | Any | 0 |
| 23 | Deny | 0.0.0.0 | / 0.0.0.0 | 10.1.1.71 | / 255.255.255.255 | Any | Any | Any | Any | Any | 0 |
| 24 | Deny | 0.0.0.0 | / 0.0.0.0 | 10.2.2.26 | / 255.255.255.255 | Any | Any | Any | Any | Any | 0 |
| 25 | Deny | 0.0.0.0 | / 0.0.0.0 | 10.1.1.82 | / 255.255.255.255 | Any | Any | Any | Any | Any | 1962 |
| 26 | Permit | 0.0.0.0 | / 0.0.0.0 | 172.0.0.0 | / 255.0.0.0 | TCP | HTTP | Any | Any | Outbound | 69273329 |
| 27 | Permit | 172.0.0.0 | / 255.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | HTTPS | Any | Inbound | 128157788 |
| 28 | Permit | 0.0.0.0 | / 0.0.0.0 | 172.0.0.0 | / 255.0.0.0 | TCP | HTTPS | Any | Any | Outbound | 193798825 |
| 29 | Permit | 172.0.0.0 | / 255.0.0.0 | 0.0.0.0 | / 0.0.0.0 | TCP | Any | HTTP | Any | Inbound | 23952651 |

**Şekil 4.10. Eduroam ağı için oluşturulan ACL**

MSKÜ eduroam ağına gelen misafir kullanıcılar freeradius virtual server'ı aracılığıyla misafir VLAN'ına atanırlar. Freeradius virtual server'da ki tanımlama aşağıdaki gibidir;

```
if ((Realm == 'mu.edu.tr') || (Realm == 'posta.mu.edu.tr')) {
        noop
    }
else {
    update reply {
        Tunnel-Type = "VLAN",
        Tunnel-Medium-Type = "IEEE-802",
        Tunnel-Private-Group-Id := "1020",
        Reply-Message= "WELCOME TO GUEST VLAN"
         }
            }
```

Örneğin 1 Haziran 2018 tarihinde Akdeniz Üniversitesi hesabıyla kampüs ağına bağlanan kullanıcının Misafir VLAN'ına alınma kaydı aşağıda verilmiştir;

*Fri Jun  1 00:00:16 2018*

*User-Name = " anonymous@ogr.akdeniz.edu.tr"*

*NAS-Port = 8*

*NAS-IP-Address = 172.16.168.2*

*Framed-IP-Address = 172.22.112.151*

*Framed-IPv6-Prefix = fe80::/64*

*NAS-Identifier = "MU-WLC-8540"*

*Airespace-Wlan-Id = 1*

*Acct-Session-Id = "5b0ffe99/7c:c3:a1:f0:63:14/748312"*

*NAS-Port-Type = Wireless-802.11*

*Cisco-AVPair = "audit-session-id=02a810ac000985c499fe0f5b"*

*Acct-Authentic = RADIUS*

***Tunnel-Type:0 = VLAN***

***Tunnel-Medium-Type:0 = IEEE-802***

***Tunnel-Private-Group-Id:0 = "1020"***

*Event-Timestamp = "May 31 2018 16:59:52 +03"*

*Acct-Status-Type = Stop*

*Acct-Input-Octets = 9287*

*Acct-Input-Gigawords = 0*

*Acct-Output-Octets = 9164*

*Acct-Output-Gigawords = 0*

*Acct-Input-Packets = 101*

*Acct-Output-Packets = 41*

*Acct-Terminate-Cause = Idle-Timeout*

*Acct-Session-Time = 316*

*Acct-Delay-Time = 0*

*Calling-Station-Id = "7c-c3-a1-f0-63-14"*

*Called-Station-Id = "50-0f-80-a0-11-fb"*

*Timestamp = 1527800416*

FW ve IPS tarafında yazılan kurallar ile VLAN temelli erişim yetkileri tanımlanmıştır. Şekil 4.11. yazılan kurallara göre engellenen uygulama ve trafik istekleri verilmiştir.

Kampüs içerisinde konumlandırılan DNS sunucuları dışında harici DNS sorgulamaları engellenmiştir. Ayrıca VPN ile proxy edilen trafiklerin de engellendiği gösterilmiştir.

| Time | .. | .. | .. | .. | Origin | Source | Source User... | Destination | Service | .. | Application Name | Primary Category |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Today, 16:11:53 | | | | | MU-FW2 | | | 138.68.92.190 | https (TCP/443) | 5 | TouchVPN | Anonymizer |
| Today, 16:11:51 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:11:29 | | | | | MU-FW2 | | | 217.69.139.42 | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:11:02 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:10:33 | | | | | MU-FW2 | | | 69.171.255.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:10:25 | | | | | MU-FW2 | | | 178.237.20.200 | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:10:09 | | | | | MU-FW2 | | | 188.132.178.... | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:09:54 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:09:47 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:09:28 | | | | | MU-FW2 | | | 69.171.255.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:09:07 | | | | | MU-FW2 | | | 107.167.115.... | http (TCP/80) | | mini5.opera-mini.... | Computers / Internet |
| Today, 16:08:17 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:08:01 | | | | | MU-FW2 | | | 31.222.68.36 | https (TCP/443) | 2 | Badoo | Personals / Dating |
| Today, 16:07:49 | | | | | MU-FW2 | | | 87.240.129.130 | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:07:39 | | | | | MU-FW2 | | | 104.155.82.30 | http (TCP/80) | 1 | Socks Protocol | Network Protocols |
| Today, 16:07:06 | | | | | MU-FW2 | | | 87.240.129.74 | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:06:35 | | | | | MU-FW2 | | | 188.132.178.... | https (TCP/443) | 3 | Film_Dizi_Domain | Custom Application/... |
| Today, 16:05:39 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:04:39 | | | | | MU-FW2 | | | 69.171.239.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |
| Today, 16:03:52 | | | | | MU-FW2 | | | 69.171.255.13 | quic (UDP/443) | 1 | DNSCrypt | Anonymizer |

**Şekil 4.11. FW'da engellenen uygulamalar**

Şekil 4.12.'de yazılan kurallara göre BotNet ağına doğru yapılan trafiklerin engellendiği görüntülenmektedir.

| Time | .. | .. | .. | .. | Origin | Source | Source User... | Destination | Service |
|---|---|---|---|---|---|---|---|---|---|
| Today, 15:33:38 | | | | | MU-FW2 | | | static.183.75.63.178.clients.your-server.de (178.63.75.183) | https (TCP/443) |
| Today, 15:33:38 | | | | | MU-FW2 | | | static.183.75.63.178.clients.your-server.de (178.63.75.183) | https (TCP/443) |
| Today, 15:28:56 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 15:28:56 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 15:28:50 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 15:28:50 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 15:28:47 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 15:28:47 | | | | | MU-FW2 | | | BotNet-17 (141.8.224.169) | http (TCP/80) |
| Today, 14:28:09 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:28:09 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:28:03 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:28:03 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:28:00 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:28:00 | | | | | MU-FW2 | | | static.248.71.63.178.clients.your-server.de (178.63.71.248) | http (TCP/80) |
| Today, 14:07:55 | | | | | MU-FW2 | | | de717.cxense.com (178.63.13.144) | https (TCP/443) |
| Today, 14:07:55 | | | | | MU-FW2 | | | de717.cxense.com (178.63.13.144) | https (TCP/443) |
| Today, 14:07:22 | | | | | MU-FW2 | | | de717.cxense.com (178.63.13.144) | https (TCP/443) |
| Today, 14:07:07 | | | | | MU-FW2 | | | de717.cxense.com (178.63.13.144) | https (TCP/443) |
| Today, 14:06:59 | | | | | MU-FW2 | | | de717.cxense.com (178.63.13.144) | https (TCP/443) |

**Şekil 4.12. FW'da engellenen trafik istekleri**

# 5. SONUÇLAR VE ÖNERİLER

Senaryo 1'de ağa dahil olan kullanıcı sayıları, tengigabit portlarında oluşan broadcast ve trafik değerleri ölçülerek, en yüksek ve ortalama değerler cinsinden çizelge 5.1.'de verilmiştir. Broadcast sayısı saniye/paket ve trafik değerleri Mbit/s cinsinden ölçülmüştür.

**Çizelge 5.1 Senaryo-1 İstatistikleri**

| SENARYO 1- STATİK VLAN ATAMASI | | | | | |
|---|---|---|---|---|---|
| **ÖLÇÜLEN DEĞERLER** | **9.04.2018** | **10.04.2018** | **11.04.2018** | **12.04.2018** | **13.04.2018** |
| Kullanıcı Sayısı Maximum | 2364 | 2615 | 2624 | 2278 | 1773 |
| Kullanıcı Sayısı Ortalama | 1995 | 2027 | 2003 | 1806 | 1410 |
| Broadcast Sayısı Maximum | **39,91** | **60,43** | **38,66** | **50,52** | **35,88** |
| Broadcast Paketi Ortalama | **31,64** | **23,79** | **18,75** | **20,68** | **16,21** |
| 1/0/1 Outbound Maximum | 263,33 | 198,83 | 184,8 | 211 | 150,53 |
| 1/0/1 Inboud Maximum | 39,22 | 45,72 | 33,23 | 30,42 | 36,71 |
| 1/0/1 Outbound Ortalama | 165,18 | 151,12 | 142,83 | 145,81 | 100,84 |
| 1/0/1 Inboud Ortalama | 22,92 | 24,24 | 22,69 | 19,44 | 18,02 |
| 1/0/2 Outbound Maximum | 196,84 | 212,94 | 185 | 239,82 | 134,37 |
| 1/0/2 Inboud Maximum | 404,03 | 344,19 | 331,89 | 381,86 | 232,86 |
| 1/0/2 Outbound Ortalama | 150,74 | 135,66 | 141,34 | 137,31 | 97,29 |
| 1/0/2 Inboud Ortalama | 280,8 | 251,81 | 251,01 | 252,21 | 172,6 |
| Outbound Ortalama Toplamı | 315,92 | 286,78 | 284,17 | 283,12 | 198,13 |
| Inbound Ortalama Toplamı | 303,72 | 276,05 | 273,7 | 271,65 | 190,62 |
| In/out Ortalama Toplamı | 619,64 | 562,83 | 557,87 | 554,77 | 388,75 |
| Ortalama Kullanıcı Başına Ortalama Outbound Trafiği | **0,15835589** | **0,14148002** | **0,141872192** | **0,156766334** | **0,14051773** |
| Ortalama Kullanıcı Başına Ortalama Inbound Trafiği | **0,1522406** | **0,136186482** | **0,136645032** | **0,150415282** | **0,135191489** |
| Ortalama Kullanıcı Başına OrtalamaIn/Out Toplamı Trafiği | **0,31059649** | **0,277666502** | **0,278517224** | **0,307181617** | **0,27570922** |

Senaryo 2'de ağa dahil olan kullanıcı sayıları, tengigabit portlarında oluşan broadcast ve trafik değerleri ölçülerek, en yüksek ve ortalama değerler cinsinden çizelge 5.2.'de verilmiştir. Broadcast sayısı saniye/paket ve trafik değerleri Mbit/s cinsinden ölçülmüştür.

**Çizelge 5.2 Senaryo-2 İstatistikleri**

| SENARYO 2 DİNAMİK VLAN ATAMASI | | | | | |
|---|---|---|---|---|---|
| **ÖLÇÜLEN DEĞERLER** | **16.04.2018** | **17.04.2018** | **18.04.2018** | **19.04.2018** | **20.04.2018** |
| Kullanıcı Sayısı Maximum | 2393 | 2678 | 2673 | 2493 | 1811 |
| Kullanıcı Sayısı Ortalama | 1890 | 2084 | 2066 | 1915 | 1411 |
| Broadcast Sayısı Maximum | **38,14** | **46,61** | **24,36** | **42,06** | **22,63** |
| Broadcast Paketi Ortalama | **16,45** | **10,84** | **17,11** | **18,2** | **11,84** |
| 1/0/1 Outbound Maximum | 192 | 203,59 | 257,13 | 247,7 | 247,15 |
| 1/0/1 Inboud Maximum | 59,5 | 330,83 | 255,64 | 57,18 | 93,03 |
| 1/0/1 Outbound Ortalama | 137,34 | 153,44 | 179 | 159,22 | 121,14 |
| 1/0/1 Inboud Ortalama | 26,73 | 206,96 | 51,66 | 25,18 | 21,69 |
| 1/0/2 Outbound Maximum | 211,43 | 230,39 | 226,42 | 219,12 | 196,91 |
| 1/0/2 Inboud Maximum | 319,55 | 321,82 | 390,48 | 391,73 | 294,15 |
| 1/0/2 Outbound Ortalama | 149,66 | 159,37 | 146,32 | 138,44 | 107,44 |
| 1/0/2 Inboud Ortalama | 250,2 | 93,97 | 260,91 | 260,88 | 198,26 |
| Outbound Ortalama Toplamı | 287 | 312,81 | 325,32 | 297,66 | 228,58 |
| Inbound Ortalama Toplamı | 276,93 | 300,93 | 312,57 | 286,06 | 219,95 |
| In/out Ortalama Toplamı | 563,93 | 613,74 | 637,89 | 583,72 | 448,53 |
| Ortalama Kullanıcı Başına Ortalama Outbound Trafiği | **0,151851852** | **0,150100768** | **0,157463698** | **0,155436031** | **0,161998583** |
| Ortalama Kullanıcı Başına Ortalama Inbound Trafiği | **0,14652381** | **0,144400192** | **0,151292352** | **0,14937859** | **0,155882353** |
| Ortalama Kullanıcı Başına OrtalamaIn/Out Toplamı Trafiği | **0,298375661** | **0,29450096** | **0,30875605** | **0,304814621** | **0,317880936** |

Belirlenen saatler arasında tengigabit portlarının oluşturduğu in/out ortalama toplam trafiğinin, ortalama kullanıcı sayısına bölümü ile ortalama kullanıcı başına düşen trafik değeri elde edilmiştir. Değerlerin karşılaştırmaları mesai günleri olan Pazartesi-Cuma günleri birebir olarak gerçekleştirilmiştir.

## 5.1. Ölçülen Broadcast Sayıları:

Kullanıcıların tek bir VLAN altında toplandığı Senaryo 1'de oluşan broadcast sayısı, tüm karşılaştırmalarda Senaryo 2'ye göre daha fazla çıktığı gözlemlenmiştir. Kullanıcıların alt ağlara bölünerek, tasnif edilmesi ile oluşan broadcast sayılarında önemli ölçüde azalma izlenmiştir. Bu durumun ağa dahil olan kullanıcı sayısının daha fazla ya da daha az olmasından bağımsız olduğu tespit edilmiştir. Elde edilen sonuçlar çizelge 5.3.'de verilmiştir.

**Çizelge 5.3 Senaryo-1 ve Senaryo-2 Broadcast karşılaştırması**

| Tarih | Broadcast Sayısı |
|---|---|
| **9 Nisan-16 Nisan** | Senaryo 1 > Senaryo 2 |
| **10 Nisan-17 Nisan** | Senaryo 1 > Senaryo 2 |
| **11 Nisan-18 Nisan** | Senaryo 1 > Senaryo 2 |
| **12 Nisan-19 Nisan** | Senaryo 1 > Senaryo 2 |
| **13 Nisan-20 Nisan** | Senaryo 1 > Senaryo 2 |

## 5.2. Ölçülen Toplam Ortalama Trafik:

9 Nisan-16 Nisan Pazartesi günü haricinde dışında diğer tüm günlerde Senaryo 2'de oluşan Toplam Ortalama Trafik, Senaryo 1'e göre daha fazla oluşmuştur. Elde edilen sonuçlar çizelge 5.4.'de verilmiştir.

**Çizelge 5.4 Senaryo-1 ve Senaryo-2 Toplam ortalama trafik karşılaştırması**

| Tarih | Toplam Ortalama Trafik |
|---|---|
| 9 Nisan-16 Nisan | Senaryo 1 > Senaryo 2 |
| 10 Nisan-17 Nisan | Senaryo 1 < Senaryo 2 |
| 11 Nisan-18 Nisan | Senaryo 1 < Senaryo 2 |
| 12 Nisan-19 Nisan | Senaryo 1 < Senaryo 2 |
| 13 Nisan-20 Nisan | Senaryo 1 < Senaryo 2 |

## 5.3. Ölçülen Kullanıcı Başına Düşen Ortalama Trafik:

9 - 16 Nisan ve 12 - 19 Nisan Senaryo 1' oluşan trafik, Senaryo 2'ye göre daha fazladır.12-19 Nisan karşılaştırmalarında oluşan kullanıcı başına ortalama trafik sayıları birbirlerine oldukça yakındır. Senaryo 1'de kullanıcı başına 0,307181617 Mbit/s, Senaryo 2'de ise kullanıcı başına 0,304814621 Mbit/s trafik elde edilmiştir. İki gün arasında kullanıcı başına 0,002366996 Mbit/s'lık bir fark söz konusu olmuştur. 10-17 Nisan, 11-18 Nisan ve 13-20 Nisan karşılaştırmalarında, Senaryo 2'de oluşan ortalama kullanıcı başına düşen, ortalama trafik Senaryo 1'e göre daha yüksektir. Elde edilen sonuçlar çizelge 5.5.'de verilmiştir.

**Çizelge 5.5 Senaryo-1 ve Senaryo-2 Kullanıcı başına düşen ortalama trafik**

| | Kullanıcı Başına Düşen Ortalama Trafik |
|---|---|
| 9 Nisan-16 Nisan | Senaryo 1 > Senaryo 2 |
| 10 Nisan-17 Nisan | Senaryo 1 < Senaryo 2 |
| 11 Nisan-18 Nisan | Senaryo 1 < Senaryo 2 |
| 12 Nisan-19 Nisan | Senaryo 1 > Senaryo 2 |
| 13 Nisan-20 Nisan | Senaryo 1 < Senaryo 2 |

Sonuç olarak kullanıcıların kural tabanlı VLAN gruplarına bölünerek ağa dahil olmaları ile oluşan broadcast sayılarında düşüş, toplam ve ortalama kullanıcı başına düşen trafikte ise çoğunlukla artış olduğu gözlemlenmiştir. VLAN yapısının esneklikleri sayesinde kullanıcılar güvenlik seviyesine göre ait oldukları ağda yaşamına devam etmesi sağlanarak, ACL, FW, IPS ve IDS kuralları vasıtasıyla ağın daha denetlenebilir hale gelmesi sağlanmıştır.

## 5.4. Öneriler:

Bu tez çalışması kapsamında yapılacak olan önerileriler şöyle sıralanabilir;

- Sistemde yapılacak değişiklikler tüm ağa uygulanmadan önce daha küçük ölçekli bir deneme ağında test edilmelidir.
- Kablolu ya da kablosuz ağda bir değişiklik yapılmadan önce ağda oluşabilecek sorunlar öngörülmeli, ağ izlenerek en az kullanıcının bulunduğu saatlerde operasyonlar gerçekleştirilmelidir.
- Sistemin her parçası mümkün olduğu kadar yedekli bir yapıda tasarlanmalıdır. Örneğin kimlik doğrulama sunucusu, kullanıcı veri tabanı, WLC v.b. cihazlar aktif-aktif olarak çalışabilecek şekilde en az 2 sunucu veya cihazdan oluşturulmalıdır. Birincil ve ikincil sunucular ayrı bölgelere konumlandırılarak olası elektrik kesintisi veya yangın, sel v.b. felaket durumlarında sistemin devamlılığı sağlanmalıdır.
- Sistem devreye alınmadan ve alındıktan sonra sunucu ve cihaz yapılandırmaları günlük olarak yedeklenmelidir.

- Şayet sunucular sanal sistemler üzerinde çalışıyorsa, sanallaştırmanın getirdiği tüm imkânlardan faydalanılarak işletim sistemleri ve tüm veriler günlük hatta belirli saatler aralığında mutlaka yedeklenmelidir (snapshot, image backup v.b.).
- Sunucular sadece yapacakları işe adanmış olmalı, üzerlerinde başka servislerin koşmaması sağlanmalıdır.
- Kurumda sistem ve network birimi ayrı birimlerden oluşuyorsa yapılacak işlemler öncesi tüm personel detaylı olarak bilgilendirilmelidir.
- Kullanıcıların ağa nasıl dahil olabileceklerine dair bir web sitesinin oluşturulması iş yükünü azaltacaktır.
- Kurumsal ağ kullanım politikasının oluşturulması ve bu politikaların tüm personele duyurulması işleyiş açısından faydalı olacaktır.
- Kullanıcılara verilecek olan şifrelerin güçlü şifreler olması ve şifre değiştirme işlemlerinde yine güçlü şifrelerin belirlenebilmesi sağlanmalıdır.
- Ağ tasarımı ne kadar iyi olursa olsun kural tabanlı yapılan VLAN atamaları neticesinde gerçekleşecek iletişim, alt ağlara yönelik yazılan FW, IPS veya IDS kuralları çerçevesinde olacaktır.
- VLAN gruplandırmaları yapılırken öğrenci, idari personel, akademik personel gibi kullanıcıların unvanı ve yaptığı işlere göre gruplandırmalar yapılmalıdır.

# KAYNAKLAR


Abramson, N. (2009). The alohanet-surfing for wireless data. *IEEE Communications Magazine*, *47*(12), 21–25. Retrieved from http://dl.comsoc.org/livepubs/ci1/public/2009/dec/abramson.html

Abreha, M. (2016). History and implementation of IEEE 802 security architecture. Retrieved from http://www.standardsuniversity.org/wp-content/uploads/History-and-implementation-of-the-IEEE-802-security-architecture-Abreha.pdf

Aktaş, A. (2016). *Preventing Campus Network From Excessive Of Unwanted Packet Traffic Using Vlan Technology*.

Çetin, G., Metin, B. (2005). *Linux Ağ Yönetimi* (5. Baskı).

Çetin, M. (2006). *Kurumsal Kampüs Ağlarında Otomatik Sanal Yerel Alan Ağ Tasarımları Ve Servis Kalitesi Analizleri*.

Chen, J. C., Jiang, M. C., Liu, Y. I. W. (2005). Wireless LAN security and IEEE 802.11l. *IEEE Wireless Communications*, *12*(1), 27–36. http://doi.org/10.1109/MWC.2005.1404570

Cisco Systems, I. (2017). Aironet-1200-series wireless. Retrieved from https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-series/prod_qas0900aecd801764f1.html

Cisco Systems, I. (2018a). 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf

Cisco Systems, I. (2018b). 802.11ac Wave 2 FAQ. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-a-c67-734152.html

Cisco Systems, I. (2018c). Authentication Types for Wireless Devices. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#wp1035025

Eduroam. (2018). What is eduroam. Retrieved from https://www.eduroam.org

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide*. Retrieved from http://books.google.com/books?id=9rHnRzzMHLIC&pgis=1

Güleryüz, M. C. (2016). *Kablosuz Ağ Standartlarının Karşılaştırılması*.

Hameed, A., Mian, A. N. (2012). Finding efficient VLAN topology for better broadcast containment. *2012 3rd International Conference on the Network of the Future, NOF 2012*, 108–113. http://doi.org/10.1109/NOF.2012.6464001

IEEE. (2018a). A Simple Network Management Protocol. Retrieved from https://tools.ietf.org/html/rfc1157

IEEE. (2018b). Official IEEE 802.11 Working Group Project Timelines - 2018-07-06. Retrieved from http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm#tgac

IEEE. (2018c). Superseded Or Withdrawn - Standards, Amendments, and Recommended Practices. Retrieved from http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm#tgi-121

IEEE Computer Society: LAN/MAN Standards Committee. (2010). *IEEE Standart for Local and metropolitan area networks- Port Based Network Access Control-802.1x-2010*. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5409813

IEEE Computer Society: LAN/MAN Standards Committee. (2014). *IEEE Standard for Local and metropolitan area networks -- Port-Based Network Access Control Amendment 1 : MAC Security Key Agreement Protocol (MKA) Extensions* (Vol. 2014). Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6994208

IETF. (2018a). Authentication, Authorization and Accounting (aaa). Retrieved from https://datatracker.ietf.org/wg/aaa/about/

IETF. (2018b). EAP-TLS Authentication Protocol. Retrieved from https://tools.ietf.org/html/rfc5216#page-4

IETF. (2018c). Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0. Retrieved from https://tools.ietf.org/html/rfc5281

IETF. (2018d). Network Working Group Request for Comments: 1321.

IETF. (2018e). The LDAP Data Interchange Format (LDIF) - Technical Specification. Retrieved from https://tools.ietf.org/html/rfc2849

Jiang, N., Shan, L., Zhao, J. (2009). Application of dynamic port VLAN membership with auxiliary VLAN in campus area network. *Proceedings - 2009 9th International Conference on Hybrid Intelligent Systems, HIS 2009*, *2*, 279–282. http://doi.org/10.1109/HIS.2009.168

Koerner, M., Kao, O. (2016). MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks. *Procedia Computer Science*, *94*, 497–501. http://doi.org/10.1016/j.procs.2016.08.077

Köksal, A. S. (2007). *802.11 Kablosuz Yerel Alan Ağlarında Güvenlik Sorunu*.

Kösem, M. (2016). *Kablosuz Ağ Standartlarının Karşılaştırılması Ve 802.1x Standardı İle Bir Üniversitede Kablosuz Ağ Güvenliği Tasarımı*.

Kurt, Ç. (2013). Kablosuz Ağlarda Eap Tabanlı Bir Kimlik Doğrulama Protokolü.

Luteus Sarl. (2018). Introduction to RRD - Round Robin Database. Retrieved from https://www.loriotpro.com/Products/On-line_Documentation_V5/LoriotProDoc_EN/V22-RRD_Collector_RRD_Manager/V22-A1_Introduction_RRD_EN.htm

Negus, K. J., Petrick, A. (2009). History of wireless local area networks (WLANs) in the unlicensed bands. *Info*, *11*(5), 36–56. http://doi.org/10.1108/14636690910989324

Oetiker, T. (2018). rrdtool. Retrieved from https://oss.oetiker.ch/rrdtool/doc/rrdtool.en.html

OpenSSL Management Committee. (2018). OpenSSL Download. Retrieved from https://www.openssl.org/source/

Öztürk, E. (2004). WLAN Kablosuz Yerel Alan Ağları (Wireless Local Area Networks) Teknolojisinin İncelenmesi, Mevcut Düzenlerin Değerlendirilmesi ve Ülkemize Yönelik Düzenleme Önerisi, *2*(2), 65–73.

Paul, T. K., Ogunfunmi, T. (2008). Wireless LAN comes of age: Understanding the IEEE 802.11n amendment. *IEEE Circuits and Systems Magazine*, *8*(1), 28–54. http://doi.org/10.1109/MCAS.2008.915504

Perahia, E. (2008). IEEE 802 . 11n Development : History , Process , and Technology. *IEEE Standards in Communications and Networking*, *46*(7), 48–54. http://doi.org/10.1109/MCOM.2008.4557042

SARIMAN, G. (2018). Muğla Sıtkı Koçman Üniversitesi Öğrenci Kimlik Yönetim Sistemi. Retrieved from https://aktivasyon.mu.edu.tr/

Soy, H., Özdemir, Ö., Bayrak, M. (2013). *Kablosuz Yerel Alan Ağlarında Güncel Gelişmeler: IEEE 802.11ac ile Yeni Nesil Gigabit Wi-Fi*. ANTALYA. Retrieved from http://ab.org.tr/ab13/bildiri/108.pdf

TamoSoft. (2018). Predictive Wi-Fi Surveys: Easy WLAN Planning with TamoGraph. Retrieved from https://www.tamos.com/products/wifi-site-survey/wlan-planner.php

The FreeRADIUS Server Project. (2018). No Title. Retrieved from https://freeradius.org/about/

Tübitak, U. (2018). eduroam Türkiye Katılımcıları. Retrieved from http://www.eduroam.org.tr/participants.php

Ulakbim, T. (2018). Sanal Yerel Ağları (VLAN'lar) ve Uygulamaları. Retrieved from http://blog.csirt.ulakbim.gov.tr/?p=48

Vanhoef, M. (2018). Key Reinstallation Attacks. Retrieved from https://www.krackattacks.com/

Ventura, H. (2002). Diameter next generation's AAA protocol, 57.

Verenkoff, B. (2011). Understanding and Optimizing 802.11n, (July).

Wi-Fi Alliance. (2005). Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise, (March).

Wong, S. (2003). The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards. *GSEC Practical v1.4b*.

Yao, Y., Jiang, C., Wang, X. (2010). Enhancing RC4 algorithm for WLAN WEP Protocol. *2010 Chinese Control and Decision Conference, CCDC 2010*, 3623–3627. http://doi.org/10.1109/CCDC.2010.5498536

# ÖZGEÇMİŞ

**Kişisel Bilgiler**


Ad Soyad :Muhammed Fatih TARLACI

Uyruk : T.C.

Doğum Yeri ve Tarihi : Çivril-1982

Medeni Hali : Evli

Telefon : 90 252 211 12 62

E-posta : fatihtarlaci[at]mu.edu.tr

fatihtarlaci[at]gmail.com


**Eğitim**

| Alınan Derece | Aldığı Kurum/Üniversite | Mezuniyet Yılı |
|---|---|---|
| Lise | Antalya Mesleki ve Teknik Anadolu Lisesi-Bilgisayar Donanımı Bölümü | 1998 |
| Ön Lisans | Ege Üniversitesi Ege MYO-Bilgisayar Donanımı Bölümü | 2002 |
| Lisans | Anadolu Üniversitesi-İşletme Fakültesi-İşletme | 2008 |
| Lisans | Hoca Ahmet Yesevi Uluslararası Türk-Kazak Üniversitesi-Mühendislik Fakültesi-Bilgisayar Mühendisliği | 2015 |

**İş Tecrübesi**

| Yıl | Yer | Görev |
|---|---|---|
| 2002-2003 | Elips Elektronik San. Tic. Ltd. Şti.-Antalya | Bilgisayar Teknikeri |
| 2003-2005 | Barbaros İlköğretim Okulu-Antalya | Bilgisayar Öğretmeni |
| 2005-Halen | Muğla Sıtkı Koçman Üniversitesi Bilgi İşlem Dairesi Başkanlığı | Bilgisayar Teknikeri |

**Yabancı Dil**

| Dil (İngilizce) | Başlangıç | Orta | İleri |
|---|---|---|---|
| Okuma/Yazma | | X | |
| Konuşma/Anlama | | X | |