PERAKENDE SEKTÖRÜNDE GÜVENLİ AĞ ÜZERİNDEN IP TABANLI SES HİZMETİ

Emre Can Güneş
181402201

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Mayıs, 2021

PERAKENDE SEKTÖRÜNDE GÜVENLİ AĞ ÜZERİNDEN IP TABANLI SES HİZMETİ

Emre Can Güneş
181402201

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Mayıs, 2021



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "*Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge*" ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "*Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge*" ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Yüksek Lisans eğitimim boyunca her daim beni destekleyen canım aileme, sabrı ve destekleri için canım eşim Deniz'e, bana bu şansı veren her zaman ilerlememe destek olan Migros Ticaret A.Ş. ailesine ve çok değerli yöneticilerime, bilgisi, tecrübesi, samimiyetini hiç bir zaman esirgemeyen çok kıymetli tez danışmanım Dr. Öğr. Üyesi Önder Şahinaslan'a ve çalışmamda büyük emeği geçen Dr. Ender Şahinaslan'a sonsuz teşekkürlerimi sunarım.

Emre Can Güneş

Mayıs, 2021

ÖZ

PERAKENDE SEKTÖRÜNDE GÜVENLİ AĞ ÜZERİNDEN IP TABANLI SES HİZMETİ

Emre Can Güneş
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2021

Teknolojik ilerlemeler, dijital dönüşüm çalışmaları her sektörde olduğu gibi perakende sektöründe de büyük bir hızda devam etmektedir. Kablolu ağ yapılarından güvenli kablosuz ağ yapılarına doğru dönüşüm çalışmaları bunlardan biridir. IP tabanlı erişimin önem kazanması ve gelişen bilgi teknolojileri sayesinde maliyetler düşürülerek dijital iletişimin hegemonyasını artmıştır. VoIP (İnternet Protokolü Üzerinden Ses) tabanlı iletişim kablolu ve kablosuz ağlar üzerinden sağlanabilecek en ucuz ve hızlı iletişim olmuştur. Bu çalışmada perakende sektöründe faaliyet gösteren bir şirkette var olan bir iletişim problemini çözmek için çalışmalar yapılmıştır. Bu çalışmada, kablolu ve kablosuz ağlar, ağ güvenliği, VoIP tabanlı uygulamalar ele alınarak örnek bir uygulama üzerinden sahadaki kullanıcıların güvenli iletişim problemi çözülmüştür.

Anahtar Sözcükler: VoIP, Kablosuz Ağlar, Ağ Güvenliği, 802.11, SIP, Perakende.

ABSTRACT

IP-BASED VOICE SERVICE OVER SECURE NETWORK IN RETAIL INDUSTRY

Emre Can Güneş
Master Thesis
Department of Computer Engineering
Computer Engineering Programme
Thesis Advisor: Asst. Prof. Önder Şahinaslan
Maltepe University Graduate School, 2021

Technological advances and digital transformation continue at a great pace in the retail sector as in its sector. Conversion tests from wired network structures to secure wireless network structures are one of them. With the increasing importance of IP-based access and reducing the costs of information technologies, the hegemony of digital communication has increased. VoIP (Voice over Internet Protocol) based communication has been the cheapest and fastest communication that can be provided in wired and wireless networks. Efforts have been made to solve a communication problem that exists in a company operating in the retail sector in this market. This cable, wired and wireless networks, network security, VoIP-based applications are handled and the forward communication problem in the field has been solved through a sample application.

Keywords: VoIP, Wireless Networks, Network Security, 802.11, SIP, Retail.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZ v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ ix
ŞEKİLLER LİSTESİ x
KISALTMALAR xii
ÖZGEÇMİŞ xiv
BÖLÜM 1. GİRİŞ 1
Problem 1
Amaç 1
Tanımlar 2
Bilgisayar Ağları 4
Perakende Sektöründe Ağ Altyapıları 4
Kablolu Ağlar 5
Kablosuz Ağlar 6
802.11 Yerel Ağ Standarttı Ailesi 7
Kablosuz 802.11 Yerel Ağlar Hizmet Setleri 19
Bağımsız Temel Hizmet Kümesi (IBSS) 20
Altyapılı Temel Hizmet Kümesi(BSS) 21
Genişletilmiş Servis Setleri (ESS) 22
Mesh Temel Hizmet Setleri (MBSS) 23
Yazılım Tabalı Ağ (SD-WAN) 24
BÖLÜM 2. YÖNTEM 26

Araştırma Modeli 26
Evren ve Örneklem 27
Veriler ve Toplanması 27
Verilerin Çözümlenmesi ve Yorumlanması 27
Kablosuz Ağlarda Güvenlik ve Kimlik Doğrulama Yöntemleri 28
Bilgi Güvenliği Temel Unsurları 29
Kimlik Doğrulama Yetkilendirme Kayıt Tutma (AAA) 31
Açık Sistem Kimlik Doğrulama Yöntemleri (OSA) 33
802.1x Bağlantı Tabanlı Ağ Erişim Kontrol Protokolü 39
Büyüklüklerine Göre Kablosuz Ağlar 48
Kablosuz Yerel Alan Ağların Avantajları 50
Kablosuz Yerel Alan Ağların Dezavantajları 51
İnternet Protokolü Üzerinden Ses Haberleşmesi (VOIP) 52
VoIP Mimarisinde Kullanılan Protokoller 55
Sinyalleşme Protokolleri 57
VoIP Kullanmanın Avantajları 64
VoIP Kullanmanın Dezavantajları 65
BÖLÜM 3. BULGULAR VE YORUMLAR 67
Perakende Sektörüne Yönelik VoIP Tabanlı Uygulamaların İncelenmesi 67
VoIP Tabanlı Çalışan Uygulamaların Karşılaştırılması 72
IPT (Internet Protokol Telefonu) Cihazların Mali Değerlendirilmesi 73
VoIP Uygulaması 74
Uygulama Temini ve Kurulumu 75
Sunucu ve CM Admin Ayarların Yapılması 76
BÖLÜM 4. SONUÇ 87
Özet 87
Yargı 87
Öneriler 88
EK'LER 89
KAYNAKÇA 99

TABLOLAR LİSTESİ

Tablo 1 - Ağ Topolojilerinin Karşılaştırması 6
Tablo 2 - 802.11n MIMO Sayısı ve Bant Genişliği 10
Tablo 3 - 802.11a, 802.11n ve 802.11ac İçin Önemli Veri Hızları 13
Tablo 4 - Wi-Fi Güvenlik Algoritmalarının Karşılaştırılması 39
Tablo 5 - H323 ve SIP Niteliklerinin Karşılaştırması 60
Tablo 6 - Cisco SCCP Call Manager İzi 61
Tablo 7 - SIP İsteği Mesaj Tablosu 64
Tablo 8 - VoIP Tabanlı Uygulama Ana Özellik Karşılaştırılması 71
Tablo 9 - Cihaz Model, Cihaz Adet ve Cihaz Mali Değer Tablosu 74
Tablo 10 - CUCM Cihaz Kurulumu İçin Gerekli Alan Adları 77
Tablo 11 - Rota Bölüm Alanlarına Ait Bir Örnek 80

ŞEKİLLER LİSTESİ

Şekil 1 - OFDM Metodu İle Veri Hızı Artışı 11
Şekil 2 - MIMO VE MU-MIMO Çalışma Prensibi 12
Şekil 3 - Hüzmeleme (Beaforming) Teknolojisi Çalışma Prensibi 15
Şekil 4 - Bir AP ve iki STA ile CSMA / CA Geçici Evrim Örneği 16
Şekil 5 - Hedef Uyanma Süresi (TWT) Yayın Şeması 18
Şekil 6 - OFDMA Çalışma Prensibi 19
Şekil 7 - Kurumsal Yapıda Kullanılan Top 5 SSID Oranları 20
Şekil 8 - IBSS Bağlantı Modeli 21
Şekil 9 - BSS Bağlantı Modeli 22
Şekil 10 - ESS Bağlantı Modeli 23
Şekil 11 - Mesh Ağ Topolojisi 24
Şekil 12 - SD-WAN Ağ Topolojisi 25
Şekil 13 - Bilgi Güvenliği: Bilginin Korunacak Temel Nitelikleri 29
Şekil 14 - Parmak ve Göz Tarama İçin Kullanılan Örnek Cihazlar 32
Şekil 15 - 2020 Ocak-Haziran Ayı Access Point Performans Değerleri 33
Şekil 16 - Açık Sistem Kimlik Doğrulama Prensibi 34
Şekil 17 - Paylaşılan Anahtar Kimlik Doğrulama Prensibi 35
Şekil 18 - Wi-Fi Protected Access 2 (WPA2) Protokolü Çalışma Prensibi 38
Şekil 19 - 802.1x Port Tabanlı Ağ Erişim Süreci 40
Şekil 20 - AP'den RADIUS Sunucusuna Yapılan Ping Testi Çıktısı 41
Şekil 21 - Genişletilebilir Kimlik Doğrulama Protokolü (EAP) Mimarisi 42
Şekil 22 - EAP-FAST Cisco Güvenli Erişim Topolojisi 44
Şekil 23 - Erişim Noktasına Ait Kullanıcı Erişimi/Kimlik Doğrulama Oranı 48
Şekil 24 - Büyüklüklerine Göre WLAN Yapıları 49
Şekil 25 - 2015-2020 Yılları Sektörel IoT Pazar Oranı 51
Şekil 26 - Ortadaki Adam Saldırı Yöntemi 52
Şekil 27 - Kurumsal Bir Yapıya Ait Örnek VoIP Şeması 54
Şekil 28 - H.323 Protokolüne Ait Örnek Bir Şema 58
Şekil 29 - INVITE Mesajının SIP Protokolü Üzerinden İletilmesi 63

Şekil 30 - VoIP Tabanlı Cihazların Envanter Bazında Dağılımı 73
Şekil 31 - Cisco Jabber Android ve iOS kurulumu 75
Şekil 32 - Uygulamanın Ana Ekran Görünümü 76
Şekil 33 - CUCM Aygıt Bilgileri Ayar Ekranı 78
Şekil 34 - Dizin Numarası Tanımları ve Eşleştirmeleri 79
Şekil 35 - CUCM Cihaz Eşleştirme Alanı 81
Şekil 36 - İzin Bilgileri Gruplar ve Roller Alanı 81
Şekil 37 - Hizmet Konumu (SRV) yapılandırma örneği 82
Şekil 38 - Gelişmiş Ayarlar ve Sunucu Ayarlarının Sağlanması 83
Şekil 39 - User Ve Şifrenin Uygulama Tanım Ayarlarına Göre Girilmesi 84
Şekil 40 - Telefon ve Anlık Mesajlaşma Hizmetlerinin Doğrulanması 85
Şekil 41 - Test Mağazaları Problem Geri Dönüş Kayıtları 86

KISALTMALAR

AAA : Kimlik Doğrulama, Yetkilendirme, Kayıt Tutma

AES : Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

ARP : Adres Çözümleme Protokolü (Address Resolution Protokol)

BSS : Temel Hizmet Kümesi (Basic Service Set)

CAGR : Bileşik Yıllık Büyüme Oranı

CIA : Gizlilik, Bütünlük, Erişilebilirlik

CSMA / CA : Çarpışmadan kaçınma özelliğine sahip operatör algılama çoklu erişimi

CUCM : Cisco Birleşik İletişim Yönetimi (Unified Communications Manager)

ESS : Genişletilmiş Servis Setleri (Extended Service Set)

IBSS : Bağımsız Temel Hizmet Kümesi (Independent Basic Service Set)

IEEE : Elektrik ve Elektronik Mühendisleri Enstitüsü

IoT : Nesnelerin İnterneti (Internet Of Things)

IPT : Internet Protokol Telefonu

KVKK : Kişisel Verileri Koruma Kanununu

MBSS : Mesh Temel Hizmet Setleri (Mesh Basic Service Set)

MIMO : Çoklu Giriş ve Çıkış Radyo Terimi

MU-MIMO : Çoklu kullanıcı, Çoklu Giriş ve Çıkış Radyo Terimi

OFDM : Çoklu Taşıyıcı Frekansları Üzerinde Dijital Veri Kodlama Yöntemi

P2P : Noktadan Noktaya

PAC : Korumalı Erişim Kimlik Bilgisi

PHY : İstemcinin Wi-Fi Üzerinden Veri Aktarabileceği En Yüksek Hız

PSTN : Genel Aktarmalı Telefon Şebekesi

RTCP : Gerçek Zamanlı Kontrol Protokolüne

SD-WAN : Yazılım Tabanlı Ağ (Software-Defined Wide Area Networking)

SDP : Oturum Tanımlama Protokolü

SIP : Oturum Davet Protokolü

SSID : Hizmet Seti Kimliği (Service Set Identifier)

TLS : Taşıma Katmanı Güvenliği (Transport Layer Security)

TWT : Hedef Uyanma Süresi

WAN : Geniş Ağ Bağlantısı

WLAN : Yerel Ağ Bağlantısı

WMAN : Yerleşke Ağ Bağlantısı

WPAN : Kişisel Ağ Bağlantısı

ÖZGEÇMİŞ

Emre Can GÜNEŞ

Bilgisayar Mühendisliği Anabildim Dalı

Eğitim

Y.Ls.	2019-21	Maltepe Üniversitesi, Bilgisayar Mühendisliği (Tezli)
Lisans.	2015-18	Anadolu Üniversitesi, Uluslararası İlişkiler
Ön Li.	2012-14	Süleyman Demirel Üniversitesi, İnternet ve Ağ Teknolojileri
Lise	2009-12	Tuzla Teknik Okulları

İş/İstihdam

2020 -	Migros Ticaret Aş - IT Associate
2015-2020	Migros Ticaret Aş - IT Specialist
2015	Turkcell - IT Specialist
2011- 12	Teknosa İç ve Dış Tic. - Stajyer

Mesleki Birlik/Dernek Üyelikleri

2014	Kan Bağışçısı - Kızılay

Alınan Burs ve Ödüller

2012	Tuzla Belediyesi Sportif Faaliyet Belgesi
2020	ICMS 2020
2021	Migros AR-GE Makale Ödülü

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

- A Research on New Generation Technologies to be Used in the Retail Industry After COVID-19., International Conference of Mathematical Sciences (ICMS 2020), Maltepe University
- "Review of The Contributions of Contactless Payment Technologies in the COVID 19 pandemic process," https://doi.org/10.1063/5.0042225, 2021.

BÖLÜM 1. GİRİŞ

Problem

Perakendecilik sektöründe COVID-19 pandemi sonrası çalışma ve iş yapış şekillerinde meydana gelen değişimler (Güneş, Sahinaslan, & Sahinaslan, 2020) uzaktan çalışma ve çağrı merkezlerindeki ani iş yükü artışları mevcut sistemlerle yönetilmez hale gelmiştir. Çalışanlar normalde kurum içinde analog cihazlar üzerinden çağrı yönetimi kullanabilirken, COVID-19 sonrasında kendi mobil cihazlarını bu amaçla kullanma ihtiyacı doğmuştur. Ancak mevcut analog sistemler ile mobil cihaz uyumsuzluk problemleri nedeniyle yetersiz kalmıştır. Aynı zamanda IoT cihazlarındaki hızlı büyüme IoT ağlarının boyutunun yanı sıra potansiyel saldırganların sayısını da artmaktadır (Sahinaslan, 2019). Bu durum kullanım, maliyet ve güvenlik gibi temel ihtiyaçlara uygun yeni teknoloji ve uygulamalar araştırmasını gerekli kılmıştır.

Amaç

Günümüzde havalimanları, kafeler, alışveriş merkezleri, restoranlar, ulaşım araçları ve perakende mağazaları müşterilerine kablosuz internet hizmeti sunmaktadır. Kablosuz teknolojilere olan talep iş, IoT cihazları, enerji sarfiyatının azaltılması sebebiyle yaşamda daha fazla önem kazanmıştır. Nüfus yoğunluğunun ve veri miktarının artmasıyla doğru orantılı olarak hızlı ve kolay erişim talebi artmıştır. Wi-Fi ağları esneklik, mobilite, kullanım kolaylığı, düşük maliyet gibi avantajlar sağladığından sosyal alanlara, ofislere, havaalanlarına, eğitim kurumlarına, ulaşım noktalarına ve diğer konumlara kolayca yerleştirilebilirler. Perakende firmalarının her daim müşteri ile iletişimde olması sebebiyle esnek iletişim yapılarını kullanmaktadırlar. Müşteri memnuniyeti ve büyük pazar payından faydalanmak isteyen kurumlar günümüzdeki teknolojilerin özelliklerine göre yatırım yapmaktadırlar. Bu yatırımlar sürdürülebilirliğin ve gelecek yıllara hâkim olabilmenin en temel yapı taşlarıdır. Dijitalleşmenin zirve yaptığı ve pandemi ile birlikte çevrimiçi görüşmelerin önem kazandığı günümüzde SIP protokolü VoIP etkileşiminin

standart protokolü haline gelmiştir. SIP protokolünün zamanla gelişimi ile birlikte bağlanılan cihazın konumunu belirleme, çoklu ortam içeriklerinin parametre detaylarının belirlenmesi, kullanıcıların toplantı ve davetlere erişiminin belirli kurallara göre belirlenmesi, çağrı süreçlerinin yönetimini ve kurulumunu belirmemek gibi ana kriterler üzerinde düzenleme sağlanabilmektedir. Çoklu ortam verilerinin transferi RTP vasıtasıyla yapılmaktadır. İki istemci arasında oturum tanımı bilgisi ise SDP aracılığıyla sağlanmaktadır.

Tanımlar

Ağ ve internet altyapılarının temeli 1950'li yılların başında nükleer saldırılardan etkilenmeyecek askeri komuta merkezlerinin tasarımına dayanmaktadır. O döneme kadar telefon hatları üzerinden yürütüldüğü için kısa sürede zarar görme özelliğine sahipti.1969 yılında ARPANET adıyla birbirleri ile iletişim kuracak uç nokta yapıları devreye alınmıştır. Daha sonrasında üniversiteler ve farklı kurumların da bu bağlantıya geçiş yapması ile kablolu ağ üzerinden iletişim kurabilen kuruluş sayısı arttı. 1980'li yıllardan itibaren ise kuruluşları ve ticari kurumları kapsayan bir altyapı düzeni haline gelmiştir. Kablolu ağ yapılarında iletişim, bükümlü bakır kablo, koaksiyel kablo ve fiber optik kablolar üzerinden çeşitli ağ cihazlarının entegresi ile çalışmaktadır. Teknolojinin gelişimi ile birlikte kablolu ağ yapısı birçok yönüyle kablosuz ağlara evirilmiştir. Taşınabilen ve teknolojik cihazların artması kablosuz ağ yapılarının daha fazla devreye alınmasını sağlamıştır.

Kablosuz ağ teknolojisi birçok cihazın hava yolu ile herhangi bir elektriksel iletken olmadan verilerin uzaktan iletilmesini sağlayan ağ çeşididir. Kablosuz ağ teknolojisi 1960'lı yılların sonunda başlamış, 1980'li yıllarda yerel bilgisayar ağlarının gelişimi ile kullanım alanı genişlemiştir. 1990'lı yılların sonuna doğru kişisel cihaz kullanımın artması ile geleceğin teknolojilerinden olmaya başlamıştır. Gelişen teknoloji ile birlikte IEEE tarafından farklı dönemlerde 802.11 tabanlı kablosuz ağ standartları oluşturulmuştur. Oluşturulan 802.11 tabanlı standartlar veri hızı ve boyutu ile doğru orantılı olarak geliştirilmiştir. İlk dönemlerinde düşük veri ve kullanıcı ile başlayan süreç daha sonrasında kendini yönetebilen büyük verileri iletebilen kablosuz ağ

yapılarına bürünmüşlerdir. Kablosuz ağ yapıları büyüklüklerine göre Kişisel Ağ Bağlantısı (WPAN), Yerel Ağ Bağlantısı (WLAN), Yerleşke Ağ Bağlantısı (WMAN), ve Geniş Ağ Bağlantısı (WAN) olarak isimlendirilmiştir.

Kablosuz ağ yapılarının büyümesi çeşitli güvenlik zafiyetlerinin de ortaya çıkmasına sebebiyet vermiştir. İnsan faktörünün olduğu her noktada çıkabilecek zafiyetlerin en aza indirgenmesi için kablosuz ağ güvenlik protokolleri de geçmişten günümüze gelişim göstermiştir. Açık sistem kimlik doğrulama ve 802.1x tabanlı kimlik doğrulama yöntemlerinin en sıkı şekilde uygulanması kişi ve kurumların bir görevi haline gelmiştir. CIA (Gizlilik Bütünlük Erişilebilirlik) ve AAA (Kimlik Doğrulama Yetkilendirme Kayıt Tutma) kuralları en iyi şekilde uygulanmalıdır. Kablosuz ağlar üzerinden IP tabanlı ses erişimi VOIP(Voice Over İnternet Protocol –İnternet Protokolü Üzerinden Ses) geçmişten günümüze etkinliğini arttırmıştır. PSTN (Public Switched Telephone Network – Genel Aktarmalı Telefon Şebekesi) tabanlı iletişim altyapısının yerini verim ve maliyet avantajları sebebiyle IP tabanlı sistemler almaya başlamıştır. Günümüzde ses verilerini iletmek için kullanılan IP üzerinden ses teknolojisi; çevrimiçi eğitim, konferans hizmetleri, kurum içi görüşme hizmetleri verebilen kablosuz IP tabanlı araçların üretilmesiyle yaygın olarak kullanılan kablosuz ağlara bütünleşmiş bir şekilde çalışmaya başlamıştır. IP tabanlı sistemlerin kullanımının artmasıyla birlikte VoIP iletişim sistemleri ve VoIP oturumunun organize edilmesini sağlayan SIP protokolü kapsamı geniş bir yapıda kullanılmaya başlanmıştır. Birçok kurum ve kuruluş IP tabanlı yazılım ürünlerini taşınabilir cihazlar üzerinden kullanıcılarına kablosuz erişim altyapıları ses ve görüntü hizmeti sağlamaktadır. VoIP tabanlı hizmetlerin kalitesi ve devamlılığının sağlanması kablosuz ağların güvenliği ile doğru orantılıdır. 2020 yılının başlarında pandemi sürecinin başlaması kablosuz cihaz erişimlerinin artışını da beraberinde getirmiştir. VoIP tabanlı uygulamaların bu dönemde eğitim ve iş tabanlı uygulamalarda kullanılması sebebiyle kişi etkileşimi artmıştır. Çalışmamızda bu etkileşim süreçlerindeki problemi iş tabanlı VoIP uygulaması üzerinden nasıl çözüme kavuşturulduğu ele alınmıştır.

Bu tezin 1.bölümünde tez hakkında bilgiler verilmiş ve amacı açıklanmıştır. 2. bölümde kablolu ağ teknolojileri, Kablosuz ağ teknolojileri standartlarına, büyüklüklerine, avantajlarına ve dezavantajlarına göre incelenmiştir ve literatürdeki araştırmaların özetleri verilmiştir. 3. bölümde ise Kablosuz ağ güvenliği ve kimlik

doğrulama yöntemlerine yer verilmiştir. CIA ve AAA metotları incelenmiştir. Açık sistem ve 802.1x kimlik doğrulama yöntemlerine yer verilmiştir. 4. bölümde ise İnternet protokolü üzerinden ses haberleşmesine ait protokoller incelenmiş ve dezavantajları/avantajlarına yer verilmiştir. Bir uygulama üzerinden çözüm önerisi gerçekleştirilmiştir ve orantısal olarak sonuçları verilmiştir. 5. bölümde ise çalışmaya ait nihai sonuç ifade edilerek daha sonraki çalışmalar için de değerlendirmeler verilmiştir.

Bilgisayar Ağları

Bilgisayar ağları kablolu veya kablosuz olarak geliştirilen sistemlerdir. 1960'lı yıllarda 'mainframe' bir yapıda olan bilgisayarlar daha sonraları kişisel kullanıma evirildikçe iletişim ihtiyacı doğmuştur. Kablolu olarak başlayan bu sistem, zamanla yerel ağların yaygınlaşması ile birlikte farklı metotlar da kullanılmaya başlanmıştır. 1980'li yıllarda kişisel bilgisayarların devreye alınması ile kablolu ağ teknolojileri genişlemiş ve iletişim teknolojileri bu yönde evirilmiştir. Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamıştır. Ancak yerel bilgisayar ağlarının yaygınlaşması 1980'li yıllarda başlamış ve gelişmiştir. 1990'lı yıllar, kişisel bilgisayarların ve internetin çok hızlı yayıldığı, her evde kullanılabilecek duruma geldiği dönemlerdir. Teknolojik gelişmeler sayesinde, ülkeler ve dünya çapında tüm istemcilerin birbirleriyle iletişim kurabilmesi için ağ altyapısı inşa edildi. Kablosuz ağların 1990'lı yıllarda devreye alınması network altyapıları için büyük bir devrim yarattı. Kablolu ve kablosuz ağ entegrasyonları ile geçmişten günümüze her iş modeline göre çeşitli altyapılar oluşturulmuştur.

Perakende Sektöründe Ağ Altyapıları

Perakendenin ilk zamanlarından günümüze uzayan çizgisinde iletişim hep ön planda olmuştur. 1990'lı yılların kırılma noktalarından biri olan e-ticaret sektörünün çıkışı network ağlarının önemini ön plana çıkartmıştır. Amazon'un 1995 yılında basit bir çevrimiçi kitapçı olarak kurulması ile günümüzde en büyük perakendecilerden biri olması arasındaki ilişki internet altyapısının gelişimi ilk sırayı almaktadır. Daha çok kişiye çevrimiçi olarak ulaşabilmek için ağ altyapılarının gelişimi ile sağlanmıştır. Dijitalleşme ile birlikte çevrimiçi alışveriş artmış, SSL güvenlik sertifikalarının devreye alınması ile birlikte de güvenli çevrimiçi alışveriş modeli gelişim göstermiştir. Fiziksel mağaza satışları 2000'lerin başından günümüze düşüş göstermiştir. Çeşitli satış kanallarının etkisi

bu yönde fazladır. Ancak bugün fiziksel bir perakende mağazasında tüm göz önündeki ve arka plandaki cihazların bir ağ altyapısında çalıştığını unutmamak gereklidir. Örneğin; ödeme sistemleri, iBeacon alt yapıları, mobil sistemler, personel yönetim sistemleri ve daha birçok yapı ağ altyapıları sayesinde bütünleşmiş şekilde çalışmaktadır. İnsan müdahalesini en aza indirgeyen akıllı ağ yapıları ile birlikte kendi kendini yönetebilen ağ yapıları fiziksel mağazacılık için vazgeçilmez bir kanıt olmuştur.

Kablolu Ağlar

Network topolojileri bir ağın mantıksal ve fiziksel tüm altyapısını ifade etmektedir. Tüm ağı oluşturan bileşenlerin bağlanış şekillerini, kablolama standartlarını iletişim protokol seçimlerini, kullanılacak aygıtları ve bu ağ yapılarının uygulanabilirliği de topolojinin çerçevesini içerisindedir. Ağın donanımsal olarak nasıl görüneceği fiziksel topoloji olarak adlandırılır iken, veri akışının nasıl olacağını ise mantıksal topoloji belirlemektedir. Sırası ile fiziksel katman ve veri iletim katmanı bu rolü üstlenirler.

Fiziksel topolojileri sıralayacak olur isek; yol topolojisi (Bus Topology), Halka topolojisi (Ring Topology), Yıldız topolojisi (Star Topology), Gelişmiş Yıldız topolojisi (Extended Star Topology), Karmaşık topolojisi (Mesh Topology), Ağaç topolojisi (Hierarchical Tree Topology), Çift Halka topolojisi (Dual Ring Topology), Hücresel topoloji (Cellular Topology), Eğri topoloji (Irregular Topology) olarak sıralayabiliriz. Mantıksal topolojiler ise Yayın topolojisi (Broadcast Topology) ve İz topolojisi (Token Passing Topology) olarak ikiye ayrılmaktadır. Tablo 1 üzerinde ağ topolojilerinin 5 farklı başlık altında karşılaştırmaları detaylı biçimde verilmiştir.

Tablo 1 - Ağ Topolojilerinin Karşılaştırması

Topoloji Türü		*Kurulum*	*Maliyet*	*Güvenlik*	*Kablolama Türü*	*Protokol*
TR	*EN*					
Yol	Bus	Çok Kolay	En Ucuz	Zayıf	Koaksiyel, Fiber, Çift Bükümlü	Ethernet ve Localtalk
Halka	Ring	Kısmen Kolay	Ucuz	Zayıf	Fiber, Çift Bükümlü	Token Ring
Yıldız	Star	Kolay	Az Pahalı	Orta	Fiber, Çift Bükümlü	Ethernet ve Localtalk
Gelişmiş Yıldız	Extended Star	Kısmen Zor	Az Pahalı	Orta	Fiber, Çift Bükümlü	Ethernet ve Localtalk
Karmaşık	Mesh	Zor	Pahalı	Güçlü	Koaksiyel, Fiber, Çift Bükümlü	Ethernet ve Localtalk
Ağaç	Tree	Kısmen Zor	Pahalı	Orta	Koaksiyel, Fiber, Çift Bükümlü	Ethernet
Çift Halka	Dual Ring	Kısmen Zor	Az Pahalı	Orta	Fiber, Çift Bükümlü	Token Ring
Hücresel	Cellular	Zor	Pahalı	Zayıf	Koaksiyel, Fiber, Çift Bükümlü	Token Ring, Ethernet ve Localtalk
Eğri	Irregular	Zor	Pahalı	Orta	Koaksiyel, Fiber, Çift Bükümlü	Ethernet ve Localtalk

Kablosuz Ağlar

Kablosuz kelimesi genel anlamda kullanılan bir terimdir, bir uçtan başka bir uca bakır kablo veya saf camdan yapılmış fiber optik gibi fiziksel bir bağlantı kullanmadan yapılan ses, veri veya görüntü aktarımına denir Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan ortama, bilgisayar ağı denir. Bir bilgisayar ağında bulunan ortamın modeline uygun sayıda bilgisayar yer alır. Bu bilgisayarlar; iki bilgisayar olabileceği gibi, tüm dünyaya yayılmış yüzbinlerce bilgisayar da olabilir.

Kablosuz ağlar, geleneksel kablolu ağ yapılarına nazaran sınır olmaksızın bütün imkân ve avantajlarını sağlar. Günümüzde sadece dünya içindeki iletişimi değil, evrende ulaşılabilecek en uzak noktalara kadar kablosuz iletişim kullanılabilmektedir. Kablosuz ağ yapıları tek başlarına değil kablolu ağlar ile bütünleşmiş çalışmaktadırlar.

Kablosuz Ağlar, LAN Düzeyi (IEEE 802.11, Wi Fi ve WLAN), PAN Düzeyi (Bluetooth, IEEE 802.15.1) , MAN Düzeyi (Genişbant Wireless, Wimax, IEEE 802.16) 3G, 4G ve 5G yapılarını içermektedir. Kablosuz ağların en büyük avantajlarının başında esneklik ve düşük maliyet gelmektedir. Kablosuz ağ teknolojilerine uyumlu taşınabilir her cihaz ile internete bağlanabilir ve sınırsız erişim sağlanabilmektedir. NASA gibi büyük şirketler uzaydan kablosuz ağ yapıları sayesinde ses ve görüntü alabilmekte insanlığın geleceği için büyük çalışmalar sağlayabilmektedir. Kablosuz ağ ile bu tür bir işlemin imkânsızlığı bulunur iken gelişen kablosuz ağ teknolojileri ile dünya ve sınırsız evrende erişimler sağlanabilmektedir.

Kablosuz iletim popüler bir kablosuz LAN teknolojisidir. Lisanssız ve 2,4 / 5 GHz frekans bantlarındaki sabit, taşınabilir ve hareketli kullanıcılara geniş bant kablosuz bağlantı sağlar. Kablosuz ağ teknolojisi, dağıtımı çok daha kolay ve daha düşük maliyetli olduğundan, kablolu yerel alan ağına alternatif olarak hızla kabul görmektedir. Yalnızca son 33 yılda, bilgiye erişimin sınırsız erişimi tüm endüstrileri dönüştürerek büyümeyi, verimliliği ve kârı artmaktadır. Günümüzde kablolu, kablosuz ağlar, mobil teknolojiler günlük yaşantımızın vazgeçilmez bir parçası haline gelmiştir (Şahinaslan, Şahinaslan, & Kantürk, 2010)

802.11 Yerel Ağ Standarttı Ailesi

Kablosuz yerel alan ağ yapılarının uyum ve denetleme problemlerinin çözümü için 1997 yılında IEEE tarafından 802.11 standart grubu oluşturulmuştur. IEEE grubu tarafından 802.11x şeklinde çeşitli standartlar geliştirilmiştir. Tez çalışmamızın ilerleyen bölümlerinde geçmişten günümüze en çok kullanılan ana standartlar detayları ile açıklanmıştır.

IEEE grubu, mühendisliğin yaratıcı, geliştirici, bütünleştirici, yönünü 802.1x ağlarını tasarlar iken kullanmıştır. Ayrıca kar amacı olmayan teknik bir mesleki grup

olarak bilinmektedir. Elektronik ve bilgi teknolojisine, insanlığa yararlı bilimlere ve uzmanlık sınıflarına katkıda bulunmaktadır. IEEE, 802.1x yerel alan ağı standartlarını, sonunda bulunan(x'in yerine) a, b, g, n, ac, ax gibi harfler ile özel bir yapıya büründürmüştür. Bu standartlar zamanla oluşan teknolojik gelişmeler ve arz/taleplere istinaden gelişim göstermişlerdir.

802.11a Standardı

802.11 standardı teknolojinin ve iletişim alanlarının gelişmesi ile yetersiz bir hal almaya başlamıştır. Bu gelişmelere paralel olarak 802.11a 1999 yılında tamamlanan ilk başarılı standart olmuştur. 5 GHz bandında ve 54Mbps veri hızına ulaşabilmektedir. 52 alt taşıyıcı kullanan fiziksel OFDM katmanına dayanıyordu. IEEE 802.11a standardının 5 GHz frekansında çalışması farklı avantajlar ve dezavantajlar sağlamaktadır. Kısa mesafede kanal kapasitesi artar ve veri aktarım hızı çok yüksek olur. 5 GHz frekansında gerçekleştirilen yayınların, kapalı alandaki engeller tarafından daha fazla emilim gerçekleştirmesi sebebi ile 802.11a standardının kapalı mekânlardaki kapsama boyutu diğer standartlara göre daha düşüktür.

802.11b Standardı

802.11b standardı 2000 yılının başında piyasaya sürülmüş olup, DSSS sistemi kullanarak 2.4 GHZ bandında çalışmaktadır. 802.11a standardına göre daha kısa sürede dünya üzerinde yaygınlaşmıştır.802.11b 11Mbps hıza çıkabilmektedir. Veri hızı ve uzaklık bakımından daha gelişmiş olması sebebi ile ethernet ağlarına rakip hale gelmiş ve kablosuz ağ standardında büyük gelişmelerin başlangıcını sağlamıştır. 802.11b'nin sağladığı en önemli avantaj kapsama alanı mesafesinin fazla olmasıdır. Bulunduğu dönemde 2.4 GHz bandında bulunması sebebi ile 38 metre kapalı, 150 metrede açık alana ulaşabilecek kapsama alanına sahip idi. Ethernet ağlarının maliyet ve kullanılabilirlik olarak daha zorlayıcı olması sebebi ile kablosuz ağlara yönelimin başlangıcı sayılabilmektedir. Geniş alanlara hükmedebilmesine rağmen en büyük dezavantajlarından biri parazit sorunuydu. Uzaktaki cihazlara erişim sağlar iken aradaki diğer (elektriksel parazitler, bluetooth, mikrodalga ve kablosuz telefon gibi) cihazların parazitlerinden mustarip olabiliyor idi. İletişim hızı düşük olmasına rağmen daha sonra

geliştirilecek teknolojilerin ve standartların önünde büyük bir yol açtığı ve kablosuz kapsama alanlarının gelişimine katkı sağladığı göz önündedir. 802.11a ve 802.11b standardı birbirleri ile uyumlu değillerdir.

802.11g Standardı

2003 yılında 802.11 a ve 802.11b standardından sonra geliştirilen 3. nesil kablosuz ağ standardıdır. 802.11g standardı kendisinden önce geliştirilen 2 standardın en iyi özelliklerini birleştirerek piyasaya sürülmüş kablosuz ağ standardıdır. 802.11 standardında olduğu gibi 5GHz kısa mesafede yüksek hız sağlayabilir iken, 802.11b standardı gibi de 2.4Ghz uzun mesafe erişimi sağlayabilmektedir. 802.11b standardında maksimum 11 Mbps hıza ulaşılan(kapalı alanda 38 açık alanda 150 metre) hızı 22 Mbps çıkartarak uzun mesafede daha verimli hıza ulaşabilmektedir. Çoklu ortam çıkışı ve video altyapılı uygulamalarda dönemine göre en iyi kaliteyi sağlaya bilen standart olarak göze çarpmıştır. Kendisinden önceki standartlara uyumlu şekilde çalışabilmektedir. Daha sonra geliştirilecek standartlar içinde yeni teknolojik gelişmelerin önünü açtığı söylenebilmektedir.

802.11n Standardı

Kullanıcı sayısının artması, teknolojik cihazların gelişimi, hız ve altyapının isteklerine uygun olarak yeni kablosuz altyapılar üzerinde çalışmalar devam etmiştir. Bu isteklere bağlı olarak IEEE ekipleri 802.11g standardından sonra yeni standart çıkarmak için 2003 yılından itibaren çalışmalara başlamışlardır. 802.11g standardını daha hızlı ve kapsama alanını genişletebilecek 802.11n standardını çıkartmışlardır. 802.11n standardı 300 Mpbs hıza çıkabilecek aşamaya gelmiştir. Daha sonra geliştirilen altyapılar ile 600 Mpbs boyutuna kadar gelmiştir. Bunun yanı sıra 802.11n, Çoklu Giriş / Çoklu Çıkış, MIMO (Multiple Input / Multiple Output), adında bir protokol sayesinde 2,4 GHz ve 5 GHz frekanslarının ikisini beraber kullanabilir duruma gelmiştir. Aktarılacak bir verinin parçalara ayrılıp farklı AP'ler üzerinden istemciye gönderilmesini sağlar.

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 çoğullaşma tekniğiyle veri aktarım oranı 4 kat artmıştır (Perahia, 2008)

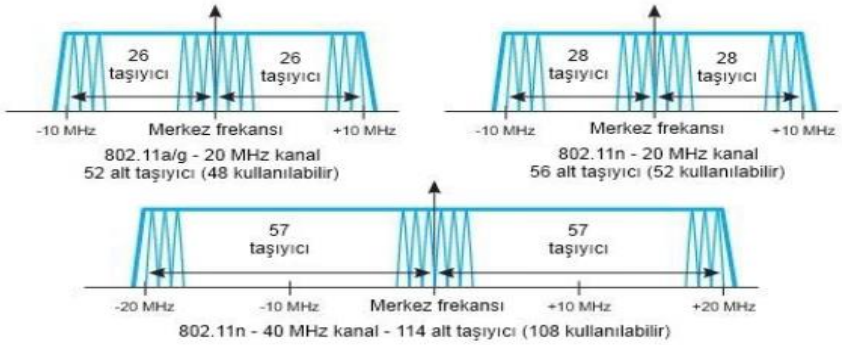
802.11n ile 2.4 GHz ve 5.2 GHz bandı desteği sağlanmıştır. Böylece geriye dönük 802.11a/b/g standardını destekleyen cihazlar ile uyumlu olarak çalışabilmektedir. Ancak bu standartta yakalanabilecek en fazla bant genişliği gönderici ve alıcının MIMO sayısına göre değişmektedir. Farklı MIMO sayısına sahip gönderici-alıcı çiftlerinin oluşturduğu trafik, düşük MIMO sayısına göre gerçekleşmektedir. Tablo 2'de 802.11n standardında, MIMO sayılarına göre ulaşılabilen en düşük ve en yüksek bant genişlikleri gösterilmektedir (Soy, Özdemir, & Bayrak, 2013).

Tablo 2 - 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

Çok taşıyıcılı iletimin özel bir biçimi olan OFDM tekniğinde geleneksel paralel veri iletim sistemlerinde olduğu gibi frekans bant genişliği birbirleriyle örtüşmeyen çok sayıda alt kanallara bölünür. Bu alt kanalların her birinde alt taşıyıcı adı verilen özel bir taşıyıcı sinyal kullanılarak veri sembolleri ile bütünleştirilir. Kanalların birbirlerine girişim etkisi yapmadan verilerin iletilmesi için alt taşıyıcı sinyaller arasında dik genlik (orthogonality) şartının sağlanması gerekir. Alt kanallardaki modülasyon işlemleri sonucunda frekans çoğullaşmalı sinyal elde edilir. Çok taşıyıcılı olma özelliğinden dolayı OFDM tek taşıyıcılı modülasyon tekniklerine göre çok daha fazla veri hızı vaat eder. OFDM tekniğinde gönderilen veriler vericide ters fourier dönüşümüyle (IFFT) bütünleştirilir iken, alıcıda fourier dönüşümü (FFT) ile tekrar de modüle edilir. 802.11n standardında alt taşıyıcı sayısı 20 MHz kanal için 48'den 52'ye yükseltilirken, 40 MHz için 108 alt taşıyıcı kullanılmıştır. Alt taşıyıcı sayısının artması veri taşımak üzere daha fazla sayıda kanal kullanılabilir kanal olduğu anlamını taşır ve böylece veri transfer hızı

artar. Şekil 1'de veri hızı artış sağlanma modülü gösterilmiştir (Perahia, 2008) (Van Nee, 2006)



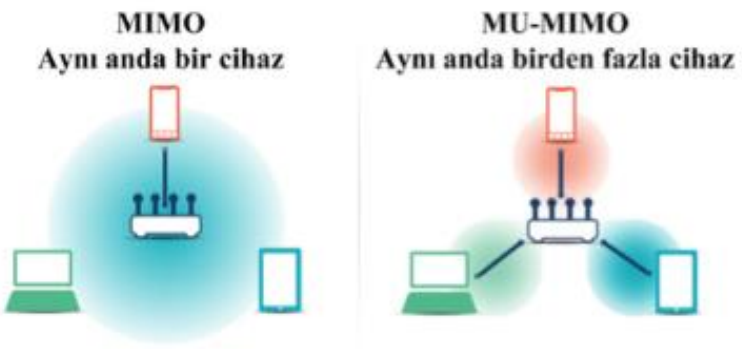
Şekil 1 - OFDM Metodu İle Veri Hızı Artışı (Soy, Özdemir, & Bayrak, 2013)

802.11ac Standardı

802.11ac 5 GHz frekansında çalışır. 3.5 Gbps veri hızına sahip olup, MIMO teknolojisini kullanır ve eski standartlar ile uyumludur. Evlerde kullanılan kablosuz modemler ve yönlendiriciler çoğunlukla bu standardı kullanır. Çoklu-kullanıcı, çoklu-giriş, çoklu-çıkış (MU-MIMO) teknolojisi ile birden fazla kullanıcının aynı anda farklı işlemler yapmasına izin verir. Beamforming teknolojisi ile cihazdan yayılan sinyallerin belirlenen odak noktalarına dağılmadan, kayıpsız ulaşması sağlanır. Önceki standartlarda kullanılan bant genişlikleri 80 MHz ve 160 MHz'e kadar yükseltildi. Veri hızında da 1.7 Gbps ve 3.5 Gbps seviyelerine ulaşıldı. (Cisco, 2018)

Kablosuz yerel alan ağlarının kullanımının yaygınlaşmasına paralel olarak yüksek performans beklentilerinin karşılanması için IEEE 802 Standartları komitesi tarafından oluşturulan yeni bir çalışma grubu (task group, TG) 802.11-2007 standardını oluşturmak amacıyla 2008 yılı Eylül ayında çalışmalarına başlamıştır. 802.11ac olarak bilinen standart tamamladığında kablosuz yerel alan ağlarında spektral verimliliğin iyileştirilmesi sonucunda kablolu ağlarla karşılaştırılabilir performansa ulaşılması hedeflenmektedir. 802.11ac çalışma grubu (TGac) tarafından yapılan çalışmalar sonucunda 2011 yılı Ocak ayında yeni standardın getirdiği teknolojileri tanımlayan ve özelliklerini belirleyen taslak ortaya çıkarılmıştır.

802.11n standardında olduğu gibi 802.11ac standardı da verici huzme biçimlendirme tekniğini destekler. Bunun ötesinde 802.11ac standardında tanımlanan MU-MIMO (Multi- User MIMO) tekniği ile huzme biçimlendirme yeteneği daha ileriye taşınmıştır. Bu şekilde bir erişim noktası uzaysal çoğullaşma tekniğiyle farklı yönlerdeki çok sayıda istemci ile aynı frekans spektrumunda farklı uzaysal akışlar kullanarak eş zamanlı olarak haberleşebilir. Kablosuz ağlarda spektral verimliliğin yükseltilmesi açısından MU-MIMO tekniği büyük önem taşır. Şekil 2 üzerinde MIMO VE MU-MIMO yapılarının prensibi gösterilmiştir (Soy, Özdemir, & Bayrak, 2013).



Şekil 2 - MIMO VE MU-MIMO Çalışma Prensibi

802.11a/n/ac destekli cihazların MIMO sayılarına göre 20,40,80 ve 160 MHz frekanslarında teorik olarak ulaşılabilecek bağlantı değerleri Tablo 3' de gösterilmektedir. 802.11 a standardına göre, 802.11 ac 80 MHz (Wave 2) standardı bant genişliği olarak 8 kat fazla görünmesine rağmen PHY veri hızı (Mbps) olarak 128,3 kat daha hızlıdır. (Cisco, 2018)

Tablo 3 - 802.11a, 802.11n ve 802.11ac İçin Önemli Veri Hızları

802.11a/n/ac ürünler	Bant Genişliği (MHz)	Uzaysal Akış	PHY veri hızı(Mbps)	Modülasyon (QAMr)
802.11a				
Genel	20	1	54	64
802.11n				
Minimum İyileştirme	20	1	65	64
Alt Seviye Ürün(2.4 Ghz)	20	1	72	64
Orta Seviye Ürünler	40	2	300	64
Üst Seviye Ürünler	40	3	450	64
Maksimum İyileştirme	40	4	600	64
802.11 ac 80 MHz (Wave 1)				
Minimum İyileştirme	80	1	293	64
Alt Seviye Ürün(2.4 Ghz)	80	1	433	256
Orta Seviye Ürünler	80	2	867	256
Üst Seviye Ürünler	80	3	1300	256
Maksimum İyileştirme	80	8	3470	256
802.11 ac 80 MHz (Wave 2)				
Minimum İyileştirme	160	1	867	256
Alt Seviye Ürün(2.4 Ghz)	160	2	1730	256
Orta Seviye Ürünler	160	3	2600	256
Üst Seviye Ürünler	160	4	3470	256
Maksimum İyileştirme	160	8	6930	256

802.11ac kablosuz yerel ağ standardı 5 GHz frekansında çalışan 802.11a ve 802.11n standartları arasında çalışan tüm cihazlar ile doğru uyumludur. 802.11ac standardı uyumlu bir bağlantı noktası servis verdiği hücre içinde haberleşme kapasitesini yükselterek aynı sayıda istemciye 802.11n standardına göre kullanıcı başına daha fazla kapasite ile işlem sağlar. Alternatif olarak istemci başına aynı iletişim kapasitesi ile daha fazla kullanıcıya servis sunulabilir. Bu özellikleri üniversite kampüsleri, konferans salonları, stadyumlar, iş yerleri ve diğer açık alanlarda 802.11ac standardına olan ilgiliyi cazip kılmaktadır.

802.11ad Standardı

2016 yılında duyurulan 802.11ad standardı diğer standartlardan farklı olarak 2.4 GHz ve 5 GHz değil, 60 GHz milimetrik frekans çalışır. IEEE 802.11ad, kısa mesafelerde (yaklaşık 10 m) 7 Gbps'ye kadar en yüksek hız sunar. Ayrıca, 60 ve 2,4 / 5 GHz frekans bantları arasında Hızlı Oturum Aktarımını (FST) destekler. IEEE 802.11ad, 60 GHz frekans bantlarının yaşadığı yüksek sinyal zayıflamasıyla başa çıkmak için hüzmelemeden yararlanır. Hüzmeleme sinyali belirli bir yöne odaklar.

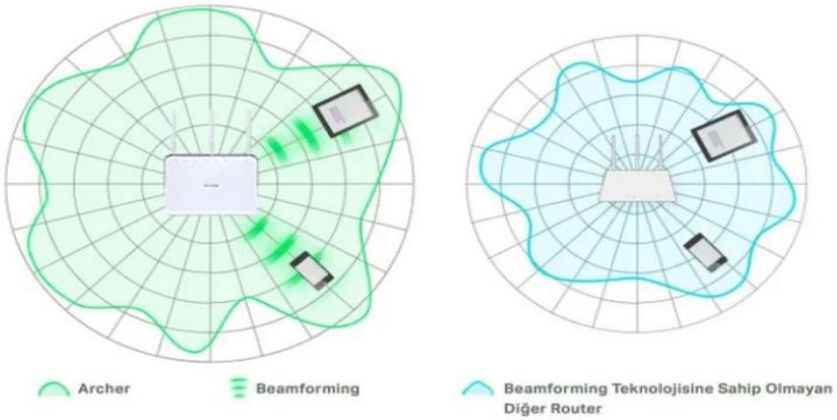
802.11ad aşağıdaki temel özellikleri içerir; Ayrılmış 8 Gbit/sn veri hızları desteği, sağlam modülasyona sahip ancak daha düşük veri hızlarına sahip mod, pille çalışan cihazlar için enerji tasarrufu modu, çok yüksek verim için OFDM teknolojisine sahip yüksek performanslı modu kullanır. 60 GHz lisanssız bandın kullanımı içerisinde; küresel kullanılabilirlik sağlar, aşırı kalabalık 2,4 GHz ve 5 GHz bantlarını önler, anten veya anten dizileri içerisinde kısa dalga boyları kullanır (60 GHz'de 5 mm), bu sayede kompakt ve uygun fiyatlı kullanım avantajı sağlar. 60 GHz aralığında ise, 802.11a, b, g, n, ac, ax'in sorunsuz kullanımı için hızlı oturum aktarımı sağlar.

802.11 ad kablosuz yerel alan ağ standardının kullanıldığı alanlar şunlardır; kablosuz ekranlar, çok fazla HDTV kullanımı olan lokasyonlarda, büyük boyutlu dosyaları iletmek için kullanılan kablosuz PC bağlantılarında, kiosk gibi otomatik eşleme uygulamalarında kullanılmaktadır.

802.11 ad Hüzmeleme (Beaforming)

Beşinci kuşak ışın hüzmeleme teknolojisidir. Bu teknoloji ile cihazdan cihaza gönderilecek veri ortam içinde yayılmadan, sadece alıcı cihazı hedef alarak iletilmektedir (Bıktım, 2016). Şekil 3’ de bu teknolojiyi kullanan cihazların hedef cihazları nasıl odakladığı gösterilmektedir. Gönderici ve hedef arasındaki havayı dar bir koridor gibi görerek veri iletim kalitesini en üst düzeye çıkartmaktadır. Bu sayede en iyi verimliliği sağlanmış olurlar. Sinyal daha yüksek kapasitede, yüksek performans ve daha uzun mesafeye ulaştırılır. Sinyal yayılarak gönderilmediği ve bir ışın gibi dar bir aralıkta

gönderildiği için sinyal kirliliğinden (enterferanstan) arındırılmış bir hizmet seviyesi elde edilir.



Şekil 3 - Hüzmeleme (Beaforming) Teknolojisi Çalışma Prensibi (Bıktım, 2016)

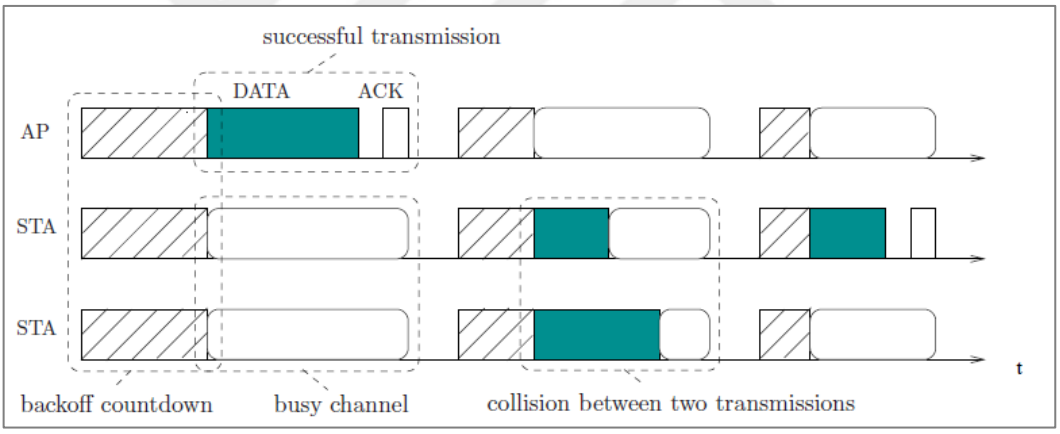
60 GHz aralığındaki iletim, 2.4 GHz ve ya 5 GHz den daha fazla iletim kaybına uğramaktadır. Bir bağlantı sırasında kanal koşulları önemli ölçüde değişebilir. Her ikisi de hüzmeleme kullanılarak gerçek zamanlı olarak yönetilebilir. 60 GHz bandındaki anten boyutu çok kompakt, küçük ve kullanılabilir olduğu için tercih edilebilmektedir. 802.11ad gerçek zamanlı olarak hüzmeleme oluşturmayı destekler. Her durum için en iyi anten ağırlıkları sonra ayarlanabilir. (Rohde-Schwarz, 2017)

802.11ax Standardı

2020-2030 on yılı içerisinde tahmini internete bağlı ağ cihazı sayısı, trafik yoğunluğu ve kullanıcı talepleri yeni bir PHY / MAC IEEE 802.11 kablosuz yerel alan ağ değişikliğinin geliştirilmesini ön görmüştür. Bu sebeple yüksek boyutta tanımlı video uygulamalarının internet kullanımına büyük oranda hükmetmeye başlamıştır. Maliyetli ve mücbir (pandemi, deprem, heyelan vb.) sebeplerden dolayı uzaktan çalışma, webinar, iş toplantıları, konferanslar ve bunun yanında eğitimin devamlılığını sağlamak için video tabanlı uygulamaların kullanımı artmıştır. Ayrıca, sanal gerçeklik eğlence uygulamaları, filmler, oyunlar, webde gezinme, zengin metin, görüntü, ses ve video içeriğinin etkileşime girdiği bir multimedya deneyimine doğru çok hızlı bir şekilde ilerlemektedir. Bunun yanında dosya depolama, bulut yönetimi ve eşleme içerik açısından standart haline

gelmiştir. Bu uygulamalar yüksek bant genişliğinin yanında güvenirlik ve sınırlı gecikme yapıları üzerine kurgulanmaktadır.

Kablosuz yerel ağların en uç özelliklerinden biri, MAC Protokolü olarak CSMA/CA('carrier sense multitiple access with collision avoidance') kullanımıdır. Şekil 4 üzerinde görüleceği üzere, bu protokol performans düzeyini arttırarak maliyeti düşürmektedir. Düğüm için hazır bir paket olduğunda CSMA / CA iletim kanalını dinler. Kanal iletimi serbest olarak algılandıktan sonra düğüm geri çekilme sayacı için rastgele bir başlangıç değeri seçerek geri çekilmeyi başlatır. Düğüm daha sonra kanalı algılarken geri çekilme sayacını azaltmaya başlar. Ne zaman bir iletim, aynı WLAN içindeki diğer düğümlerden veya diğer WLAN'lara ait kanalda algılanır ise, kanal tekrar serbest algılama moduna kadar geri çekilir ve sayacı duraklatılır, daha sonra geri sayım devam eder. Geri çekilme sayacı sıfıra ulaştığında, düğüm verici üzerinde tekrar başlar. (Boris, 2016)



Şekil 4 - Bir AP ve iki STA ile CSMA / CA Geçici Evrim Örneği

IEEE 802.11ax standardını bu kadar ilgi çekici yapan şeylerden biri de mobil ve IoT cihazlar için, güç ve zaman verimliliğini en üst düzeyde arttırmasıdır. 802.11ax standardında geliştirilmiş olan sadece teorik sistem seviye çıktıları değil, aynı zamanda yüksek kullanıcı yoğunluklu senaryolarda son kullanıcılar tarafından elde edilen gerçek gerçek zamanlı çıktılardır. IEEE 802.11ax kablosuz yerel ağ protokolü, tüm olası senaryolarda son kullanıcılara çok daha iyi bir kullanıcı deneyimi vaat ediyor. Bunlar, genellikle yoğun bir Wi-Fi kullanıcısı olan (örneğin stadyumlar, iş yerleri, kampüsler toplu taşıma) yoğun ortamlarda çalışmak için en iyi verimliliği ve hızı sağlamaktadır.

IEEE 802.11ax, tüm bu işlemleri yapabilmek bir dizi farklı teknolojiyi kullanmalıdır. Standardın OFDM'ye temel alacağı öngörülmekle birlikte, şu anda OFDMA, MU-MIMO ve daha yüksek dereceli modülasyon dâhil olmak üzere diğer bazı teknolojiler dikkate alınmaktadır. OFDM'ye göre geriye dönük uyumlu olarak çalışmaktadır. OFDM'de toplam kanal bant genişliği (20 MHz, 40 MHz, 80 MHz vb.) Birden fazla OFDM alt taşıyıcı içerir. Halen OFDM'de, herhangi bir çerçeve aktarımı bant genişliğindeki tüm alt taşıyıcıları kullanmak zorundadır. (Boris, 2016)

Birlikte yaşama: Kablosuz yerel alan ağları Uluslararası Telekomünikasyon Birliği (ISM)'nde lisanssız cihaz olarak çalışır. Bu nedenle, IEEE 802.11ax 2019 ortalarından itibaren hem aktif çalışan diğer kablosuz ağlarla hem de lisanslı cihazlarla ve son kullanıcı cihazlar ile entegre olarak çalışacak şekilde bütünleştirmiştir.

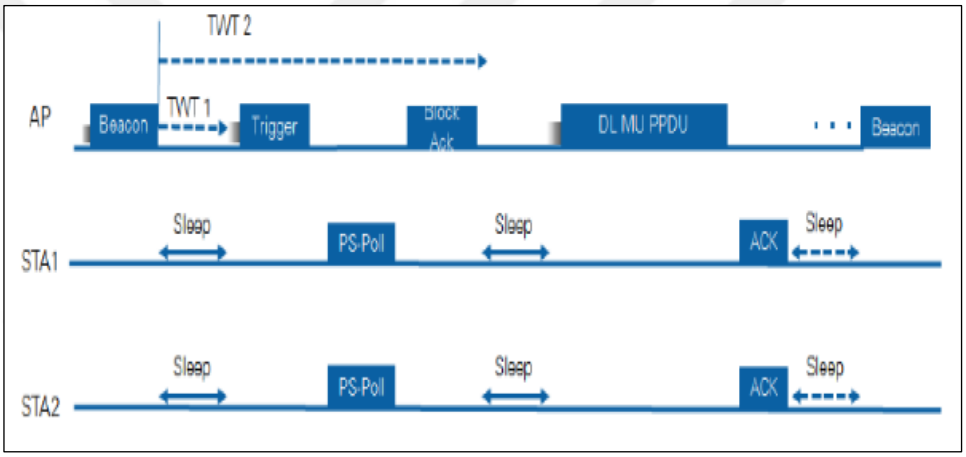
Daha yüksek verim: Hem sistem hem de kullanıcı veriminin iyileştirilmesi, kanal kaynaklarının iyileştirilmiş kullanımını gerektirir. IEEE 802.11ax 2019 ortalarından itibaren, IEEE 802.11ac-2013'e kıyasla 4 kat daha yüksek bir verim artışı hedeflemiştir. Bu amaca ulaşmak ve ilerisi için geliştirmek için Dinamik CCA, OFDMA (Ortogonal Frekans Bölmeli Çoklu Erişim) ve gelişmiş çoklu anten teknikleri gibi bazı yeni kablosuz teknolojiler kullanmaktadır.

Enerji verimliliği: IEEE 802.11ax'in 2019 un ortalarından sonraki hedefi, hem yeni düşük güçlü donanım mimarileri hem de yeni düşük güçlü fiziksel katman verimliliği gerektirir. Bir üst maddede belirtilen 4 kat verimlilik artışı göz önüne alındığında, en azından MAC üzerinde önceki standart değişikliklerden daha fazla tüketmemek önem arz etmektedir.

Geriye Dönük Uyumluluk: IEEE 802.11ax modelini kullanan kablosuz yerel alan ağ yapıları, önceki IEEE 802.11 standartları üzerinde PHY / MAC değişikliklerini kullanan cihazları desteklediğinden, geriye dönük olarak uyumlu hale getirmek için mekanizmalar da uygulanmalıdır. (Boris, 2016)

IEEE 802.11ax Hedef Uyanma Süresi (Target Wakeup Time -TWT)

IEEE 802.11ax Access Point(AP), katılımcı istasyon(STA)'larla belirli istasyonların ortama erişmesi için belirli bir zamanı veya süreyi tanımlamak için Hedef Uyanma Süresi (TWT) işlevinin kullanılması teknolojisini kullanmaktadırlar. STA'lar ve AP, beklenen aktivite süresini içeren bilgi alışverişinde bulunabilir. Şekil 5 üzerinde uygulama şeması paylaşılmıştır. Bu şekilde AP, ortama erişmesi gereken STA'lar arasındaki çekişme ve örtüşme seviyesini kontrol eder. 802.11ax STA'lar enerji tüketimini azaltmak için TWT kullanabilir ve TWT gelene kadar uyku durumuna girebilir. Dahası, bir AP ek olarak zamanlamaları tasarlayabilir ve aralarında bireysel TWT anlaşmaları olmadan STA'lara TWT değerleri atayabilir. (Boris, 2016)

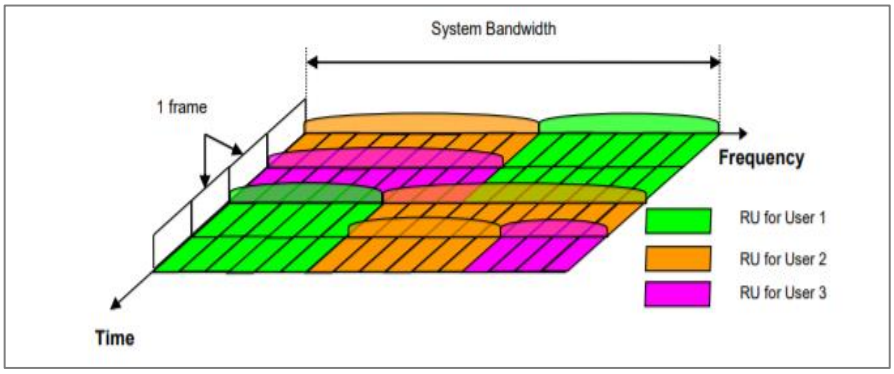


Şekil 5 - Hedef Uyanma Süresi (TWT) Yayın Şeması (Boris, 2016)

IEEE 802.11ax OFDMA Teknolojisi

802.11ax OFDMA adı verilen daha verimli bir veri iletim modu sunar. Bu mod OFDMA olarak da adlandırılabilir. Farklı kullanıcıları alt taşıyıcılara ayırarak ve birden çok kullanıcı ekleyerek kanal kaynaklarını yeniden kullanmak için birden fazla kullanıcı OFDM sistemine erişir. Şimdiye kadar, bu teknoloji 3GPP, LTE gibi birçok kablosuz teknoloji tarafından kullanılmıştır. Ayrıca, 802.11ax standardı en küçük alt kanalı bir kaynak birimi (resource unit- RU) olarak tanımlar. Her kaynak birimi en az 26 alt taşıyıcı içerir ve kullanıcılar zaman frekanslı kaynak birimleri ile ayırt edilir. Şekil 6 da gösterildiği gibi kaynaklar tüm kanalın içerisinde küçük sabit zaman frekanslı kaynak birimlerine bölünür. Kullanıcı verileri bu modda her kaynak birim üzerinden devam eder.

Bu nedenle, toplam zaman frekansı kaynaklarında, birden fazla kullanıcı aynı anda ve aynı zaman diliminde iletim sağlar. (Huawei, 2020)



Şekil 6 - OFDMA Çalışma Prensibi (Huawei, 2020)

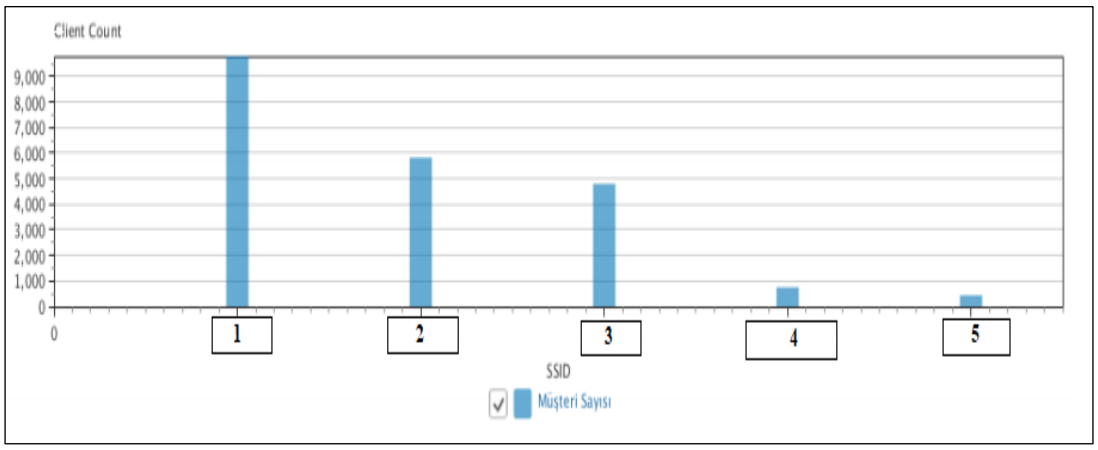
Hız ve trafik ihtiyaçları temelinde çalışan AP, kanalın nasıl kullanılacağına karar verir ve her zaman mevcut tüm kaynak birimlerine talimat verir. Tüm kanalı aynı anda tek bir kullanıcıya devredebilir (IEEE 802.11ac olarak) veya birçok kullanıcıya aynı anda iletim hizmeti vermek için parçalara bölünebilir. Birçok son kullanıcının normalde verim iddia edemeyeceği yoğun ortamlarda, OFDMA aynı anda daha küçük ancak etkili bu alt kanala hizmet sağlar, bu şekilde kullanıcı başına ortalama verimi en üst düzeyde artırır.

Bu senaryolarda, Wi-Fi ağına bağlı STA sayısı kısa sürede büyük ölçüde artar. Artan ses ve video trafiği, Wi-Fi ağına da uyum sağlar. İletim gecikmesi genellikle ağ tıkanıklığı veya yeniden iletimden kaynaklanır. Mevcut Wi-Fi 5 (802.11ac) ağı büyük bant genişliği sağlayabilir. Ancak, erişim olarak yoğunluk artar, verim performansı bir darboğazla karşılaşır. Wi-Fi 6 (802.11ax) ağı bu hizmetlerin daha fazla olmasını sağlamak için OFDMA, MU-MIMO ve 1024-QAM gibi teknolojiler kullanır. Daha geniş bir erişim kapasitesine ek olarak, ağ her birinin bant genişliğini kullanıcı bazında dengeleyebilir. (Huawei, 2020)

Kablosuz 802.11 Yerel Ağlar Hizmet Setleri

Kablolu ağlar gibi, kablosuz ağlar da çeşitli fiziksel ve mantıksal topolojilere sahiptir. 802.11 kablosuz yerel ağ standardında kendi içerisinde hizmet setlerine bölünmüştür. Bir servis seti, bir kısım kablosuz cihazın birbiriyle nasıl iletişim kurduğunu ve haberleştiğini açıklamaktadır. Arz/talep içeriğine göre bu servis setleri kurgulanır.

AP'ler ve kablosuz istasyonlarla (STAs-Stations) kurulan çeşitli kablosuz ağ topolojileri vardır.



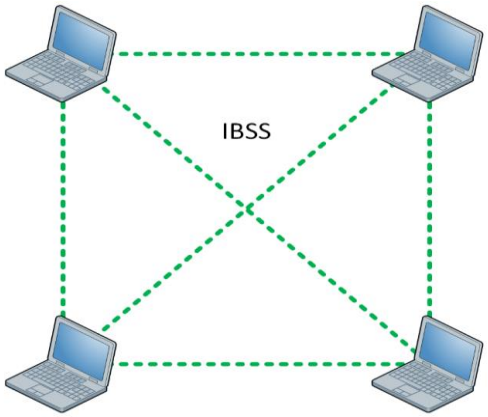
Şekil 7 - Kurumsal Yapıda Kullanılan Top 5 SSID Oranları

Şekil 7 üzerinde en çok kullanılan 5 SSID gösterilmiştir. SSID-1'e günlük 9000 ile 10500 arası cihaz erişim sağlamaktadır. Bu cihazlar yoğun olarak sahada kullanılan RF el terminalleri, e-ticaret ürün toplama cihazları, teraziler, e-etiket cihazları ve operasyonda kullanılan diğer kablosuz cihazları kapsamaktadır. SSID-2'e günlük 5000 ile 7500 arası cihaz erişim sağlamaktadır. Bu cihazlar yoğun olarak dizüstü, şirket telefonu, ipad, terazi ve kurumsal LDAP yetkisi tanımlı olan tüm cihazlar erişebilmektedir. SSID-3e 4000 ile 5500 arası cihaz erişim sağlamaktadır. Dışarıdan belirli kısıtlar ile kurum dışı kişiler erişebilmektedirler. OTP ve mail onayı ile sıkı güvenlik politikaları altında wireless erişimi sağlanabilmektedir. SSID-4 ve SSID-5 ise yük dengeleme (load balancing) sağlamak için açılmıştır ve belirli dönemlerde devreye girerek network yükünü diğer SSID'ler üzerinde azaltmaktadırlar. İstemci isteklerini veya ağ trafiğinin verimli şekilde dağıtılmasını sağlar.

Bağımsız Temel Hizmet Kümesi (IBSS)

İki veya daha fazla kablosuz aygıtı erişim noktası (AP) olmadan doğrudan bağlamak için kullanılan bir yöntemdir. Adhoc bağlantı olarak da adlandırabiliriz. Cihazlardan biri bir SSID yayını yapar ve diğer cihaz bu SSID'yi kullanarak bağlantı sağlar. İzin verilmesi durumunda daha sonra diğer cihazlar ağa katılabilir. IBSS popüler bir bağlantı yöntemi değildir. Erişim noktalarına bağlanmadan iki veya daha fazla dizüstü bilgisayar, akıllı telefon, tablet, akıllı saat arasında dosya aktarmak istiyorsanız bunu

kullanabilirsiniz. Şekil 8 üzerinde ikiden fazla cihaz bağlanılarak IBSS bağlantı modelinin gösterimi bulunmaktadır.

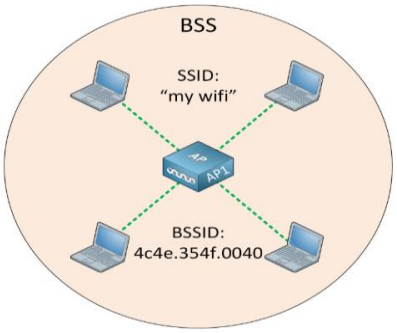


Şekil 8 - IBSS Bağlantı Modeli (NetworkLessons, 2020)

Altyapılı Temel Hizmet Kümesi(BSS)

Altyapılı temel hizmet kümesi modunda tüm kablosuz istemci cihazları merkezi bir cihaz olan erişim noktası(AP)'na bağlıdır. Tüm veriler erişim noktası üzerinden geçer. Genellikle ofis ev gibi küçük ve kısa mesafeli kapsama alanları dar alanlarda kullanılır. 802.11 kablosuz yerel ağ standarttı içerisinde çok farklı hizmet küme modelleri yer almaktadır.

Erişim noktası Temel Hizmet Kümesi Tanımlayıcısını (BSSID) da tanıtır. Bu, AP'nin radyosunun MAC adresidir, AP'yi tanımlayan benzersiz bir adrestir. Tüm kablosuz istemcilerin AP'ye bağlanması gerekir. Bu, AP'nin sinyal aralığının BSS boyutunu tanımladığı anlamına gelir. Bu alana ise Temel Hizmet Alanı (BSA) denilmektedir. Şekil 9 üzerinde BSS yayın yaptığı alan ve bağlı olan istemcilerin iletişimi görülmektedir. (NetworkLessons, 2020)



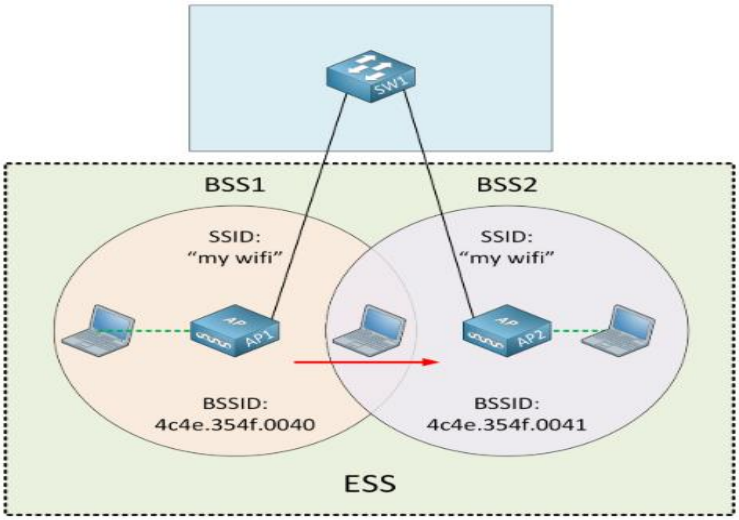
Şekil 9 - BSS Bağlantı Modeli (NetworkLessons, 2020)

Bu topolojide en önemli nokta her şeyin AP üzerinden geçmesidir. AP ana noktamız olarak kabul edilmektedir. BSS'in boyutunu ve kapsama alanını tanımlayan AP'dir. Konum, cihaz modeli, duvar ve istemci cihazların özelliklerine göre iletim boyutu farklılık gösterebilir.

Genişletilmiş Servis Setleri (ESS)

Bir BSS tek bir AP kullanmaktadır. Ancak gelişen teknolojiyle birlikte bu AP sayısı yetersiz kalmaktadır. Mobil kullanımın arttığı her ortamda kablosuz yapıların önemi de artmaktadır. Bu nedenle kapsam bazında baktığımızda tek bir AP'nin yetersiz kaldığı noktada yapıları genişletmemiz gerekmektedir. Ayrıca yoğun noktalarda tek AP verimsiz çalışacaktır. İstemci sayısı arttıkça AP üzerinde yük ve ısı miktarı yükselir. Bu sebeple AP birbiriyle iletişim halinde olan AP'leri arttırarak bant genişliği noktasında AP'ler üzerinde balans sağlayabilir.

Genişletilmiş Servis Setleri birbirleriyle farklı alanlarda olabileceği gibi, kısmen de olsa yayın alanları kesişebilmektedir. 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. (Tarlacı, 2018)



Şekil 10 - ESS Bağlantı Modeli (NetworkLessons, 2020)

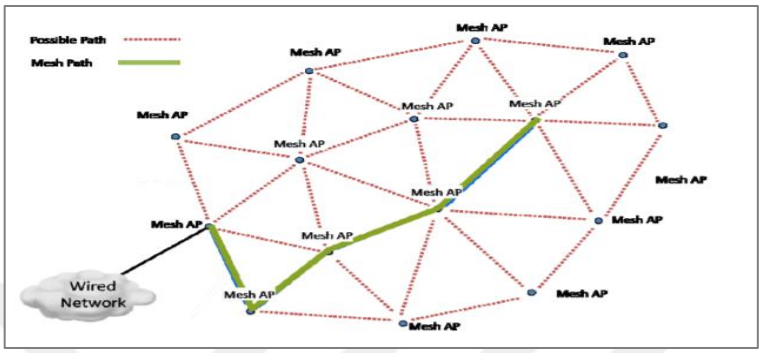
AP'ler birbirleriyle bütünleşik olarak çalışmaktadır. Şekil 10 üzerinde görüleceği üzere BSS1 ve BSS2'yi birbiri ile ilişkilendirme durumunda kablosuz istemci bağlantısı kesilmeden bir AP üzerinden diğerine otomatik geçiş sağlamaktadır. Buna kısaca dolaşım diyebiliriz. Bu yapının kesintisiz bir şekilde işleyebilmesi için birbiriyle örtüşmesi gerekmektedir.

Mesh Temel Hizmet Setleri (MBSS)

Mesh ağ yapısı, kablolu ağın mümkün olmadığı yerlerde birçok AP üzerinden erişim sağlamak kullanılmaktadır. Erişim noktaları üzerinden, kablolu altyapıya en yakın erişim noktasına kablosuz ağ bağlantısı oluşturur. Kablolu ağa bir veya daha fazla AP bağlanabilir ve geri kalanı erişim alanı içerisinde kablosuz olarak birbirine bağlanabilir

Mesh ağ yapısı günümüzde kablosuz ağ kullanımının çok hızlı büyümesiyle birlikte, kablolu ağın erişimindeki maliyet ve esneklik zorluğunun yaşanması kablosuz bağlantının artırılması gibi çeşitli yararlar sağlar. Kablosuz bağlantılar ile bir anahtara ve kablolu ağa bağlanmak için bir ilk erişim noktasına ihtiyacınız vardır. Daha sonra birçok AP bu bağlantı üzerinden bağlanabilir. Bu bağlantı anahtardan ve ilk erişim noktasından kilometrelerce uzakta, hatta hareketli nesneler (tren, otobüs, gemi) olsa bile erişim kesintisi yaşamadan işlevlerine devam edebilmektedirler. Bir başka avantaj ise, kablosuz bağlantının izlediği yoldur. Bir kablolu bağlantıyla belirli bir esneklik sağlanabilir. Ancak kablosuz bağlantı birkaç AP aralığında çalışmaktadır ve istemci erişim yolunu radyo frekansları üzerinden gerçekleştirir. Mesh bağlantı yapısı üzerinden çok örgülü AP

bağlantısı, birden fazla kullanıcının verilerini bulut depolama üzerinde eşleştirerek kesintisiz olarak işlevsellik sağlamaktadır. Şekil 11'de mesh topoloji çalışma prensibi gösterilmektedir. En hızlı ve sabit yol seçilerek iletişimin en hızlı şekilde sağlanması amaçlanmaktadır. En yakın komşu metodu ile en yüksek verim alınmaktadır.



Şekil 11 - Mesh Ağ Topolojisi (Henry, 2011)

Kendi kendini şekillendirme: Mesh temel hizmet setinin çok önemli artısı kendi kendini oluşturmasıdır. Genellikle bir algoritma, ağdaki en iyi yolu algılamak için AP'ye gömülür. Kablosuz ağ üzerinde bir AP eklemek veya düzenlemek bu algoritma sayesinde çok kolay bir yolla olabilir. Bunu sağlayabilmek için AP çekim alanı içerisinde olması yeterlidir. Kalan her şey Mesh AP'lerinde çalışan gömülü mesh uygulamaları ile halledilir.

Kendi kendini iyileştirme: Kablosuz ağ, içinde bulunan birden fazla kablosuz yol üzerinden kablolu ağ / anahtar yolu için yedeklik sunar. Bu, kablosuz ağın kendi kendini iyileştirme özelliğidir. Bir erişim noktasının kablolu bağlantı için birkaç olası yolu varsa ve AP otomatik olarak en iyi yolu seçebilir. Mesh yapısı üzerinde bir erişim noktasını kaldırmak basitçe kablosuz yapının dağıtılmasına gerek kalmadan kablolu ağa giden yeni en iyi yolu bulmak için diğer erişim noktaları üzerinden erişim sağlar.

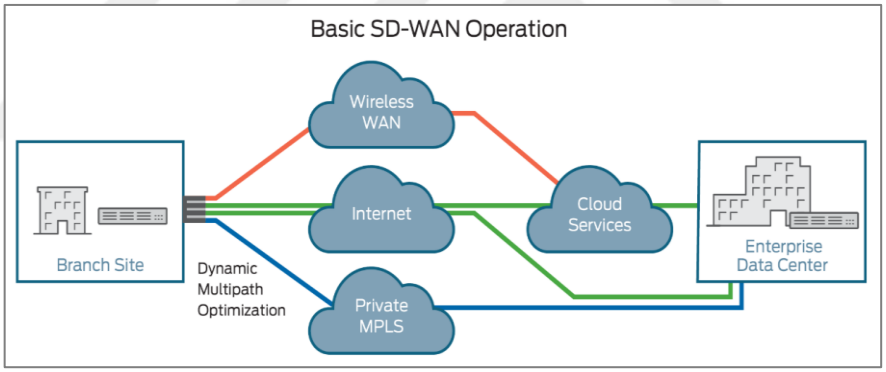
Yazılım Tabalı Ağ (SD-WAN)

Dijitalleşen dünyada modern işgücü giderek artmaktadır. Kullanılan uygulamalar merkezi yapıdan daha çok, veri merkezi tabanlı bulutlara taşınmaktadır. Artan son kullanıcı sayısı göz önüne alındığında bulut tabanlı yapılara erişim sayısı artmaktadır ve bu BT birimleri için karmaşıklığa yol açabilmektedir. Bu yapıyı daha basite indirgeyebilmek ve hızlı çözümlere ulaşmak için WAN yapılarından basit SD-WAN

yapılarına geçiş gözle görülür bir şekilde artmaktadır. Kısacası artan bant genişliği, artan performans, çalışma süresinin uzatılması ve kendi kendine öğrenen bir yapıda olması yazılım tabanlı ağların kullanımında ön plana çıkmaktadır.

SD-WAN Çalışma Prensibi

Yazılım tanımlı geniş alan ağı (SD-WAN) çözümü işletmelere sunulan yazılım, internet ve bulut destekli bir ağ hizmetidir. Ağ hizmetini sanal hale getirir ve kurumsal ağı yapılandırma ve ağ yöneticisinin karmaşıklığını en aza indirger. Kullanıcı trafiği en üst düzey koruma altına alır. Kurumdaki mevcut ağ yapıları üzerinden iletildiği SDN yer paylaşımı modeline dayanır. Mevcut ağ yapısında herhangi bir değişiklik gerektirmez; bunun yerine, trafiği koruma altına alarak uç cihaza gerekli yapılandırma ve algoritmayı ekler. Uç cihazlar, mevcut altyapının üzerinde mantıksal olarak ayrı bir ağ oluşturur. Mantıksal ağ, temel erişim teknolojilerine bakılmaksızın herhangi bir IP ağı üzerinden oluşturulabilir.



Şekil 12 - SD-WAN Ağ Topolojisi (Juniper, 2020)

SD-WAN, kritik görev uygulamaları için daha iyi hizmet kalitesi sunarken, ağ noktaları arasında daha hızlı yönlendirme ve WAN yollarına daha fazla görünürlük sağlamaktadır. Bu avantajlarıyla, ağ yöneticileri sorunları daha kolay giderebilir ve maliyet düşüşlerini gerçekleştirebilirler.

BÖLÜM 2. YÖNTEM

Bu çalışmada uygulanan yöntemde kablosuz ağ yapıları ve VoIP teknolojisinin en kolay yoldan ve maliyet düşürücü şekilde entegrasyonun sağlanması hedeflenmiştir. VoIP teknolojisinin kablosuz ağ teknolojisi ile entegrasyonunun düşük maliyetli hızlı iletişim ağının oluşmasına yönelik yöntem benimsenmiştir. Ayrıca dolar bazındaki yükseliş ve pandemi sebebiyle artan maliyeti en aza düşürerek iletişimi sağlayabilme yetisi kazanmak da amaçlanmıştır. Bunu sağlayabilmek amacıyla örnek bir 'Kurumsal Perakende Şirketinde' eldeki şartlar ile araştırma yapılmış ve özgün bir projeye dönüştürülerek gerçekleştirilmiştir.

İşlemelerde amaçlanan VoIP çözümleri; çalışanların gittikleri yerlere ofisteki dâhili hatlarını götürebilmesi için internet konferansı, mevcudiyet, faks ve e-postaya eklenen sesli mesaj, anlık sohbet ve daha pek çoğu kadar akıllı telefon istemcilerini içeren birleşik iletişimler özelliklerini de kapsar. Akıllı telefon istemcileri, ofislerindeki dâhili numarayı çeviriyormuş gibi bir kullanıcının cep telefonundan arama yapıp aramaları cevaplandırmak üzere de VoIP'i kullanır.

Araştırma Modeli

Söz konusu IoT olduğunda olasılıklar sonsuzdur ve istatistikler kesinlikle bunu yansıtmaktadır. McKinsey, küresel olarak her saniyede bir 127 cihazın internete bağlı olduğunu belirtiyor. 2025 yılına kadar dünya çapında 75 milyardan fazla IoT cihazının olması bekleniyor. Çin, Kuzey Amerika ve Batı Avrupa, IoT'nin kurulu tabanının% 67'sini oluşturuyor. IDC, IoT küresel pazar gelirinin 2025 yılına kadar yaklaşık 1,1 trilyon ABD dolarına ulaşacağını tahmin ediyor. Bağlantıların 2017'den 2025'e kadar yaklaşık 7 milyardan 25 milyara % 17 CAGR (Bileşik Yıllık Büyüme Oranı) ile artması bekleniyor.

5G teknolojisi IoT ve diğer uygulamalar için kullanılan mevcut kablosuz iletişim yöntemlerini yeniden şekillendirecek ve fayda/maliyet açısından ön plana çıkacak gibi görünüyor. Tüm cihazların birbirleri ile etkileşimi sayesinde iletişim kurmanın değeri daha fazla artmaktadır. Bu değeri en az maliyet ve en üst verim ile iletişimi sağlayabilmek

için çalışma gerçekleştirilmiştir. Kendi iç kaynak taramalarımız (sertifikasyon, zaman, kullanıcı cihazları, lokasyon uygunluğu) ile birlikte teknolojinin kablosuz ağ ve internet protokolü üzerinden ses erişimi (VoIP) yönü ile maliyeti düşük ve çok hızlı şekilde devreye alabilecek modeli geliştirmek için çalışma gerçekleştirdik.

Evren ve Örneklem

Kablosuz ağ yapıları çok büyük bir alanlara hitap etmektedir. VoIP teknolojileri de çeşitli uygulamalar üzerinden kablosuz ağ yapıları ile birleşerek etkileşimi arttırmıştır. Çalışmamızın yapısı olan perakende de iletişim hem iç hem de dış alanda çok önem kazanmaktadır. Kısmi olarak yayılıma gidilen çalışmamızda 20.000 üzerinde cihaz bulunmaktadır. Masaüstü, telsiz, mobil cihaz ve dizüstü cihaz modelleri düşünüldüğünde evren büyüklüğü artmaktadır. Tüm evrende ki VoIP yapısını birbirine entegre edebilmek ve cihaz sayılarını arttırabilmek kablosuz ağ yapıları sayesinde olabilmektedir. Lokasyon ve kişiler üzerinde yapılan çalışmalar ile örneklem büyüklüğünü daha da genişletebilir.

Veriler ve Toplanması

Kurumsal firma üzerindeki VoIP tabanlı cihaz verilerinin toplanması gerçekleştirilecektir. Bunun yanında kendi iç kaynaklarımızda bulunan döküm, bağlı cihaz sayısı, görüşme zamanları ve veri trafiğinin belirli dashboard ekranları üzerinde toplanması hedeflenmiştir. Önemli araştırma firmaları McKinsey, IDC ve Gartner gibi özgün firmaların anket ve araştırmaları da incelenecektir.

Verilerin Çözümlenmesi ve Yorumlanması

Çalışmanın yürütüldüğü örnek kuruma ait iç envanter ve dashboard ekranlarındaki verilerin MS Excel'e aktarımı (export) gerçekleştirilerek bu verilerin çeşitli başlıklar altında bir arada toplanması sağlanmıştır. Ortalama cihaz, kullanıcı, veri trafiği, mali olarak gösterimi ve kısa/uzun vadede getirisi hesaplanarak bu somut veriler üzerinden yorumlanacaktır.

Kablosuz Ağlarda Güvenlik ve Kimlik Doğrulama Yöntemleri

Kuruluşların müşterileri ve şirket içi bireylerinin tüm bilgilerinin güvende tutma ve yönetmelerine yardımcı olan belge ISO/IEC 27001'dir. Bu belge sayesinde kurum ve kuruluşlar iç ve dış tüm kritik seviyeden en alt seviyeye kadar bilgileri yönetebilir ve çeşitli esnekliklere göre paylaşabilirler. Risklerin azaltılması ve yönetilmesinde önemli rol oynayan ISO/IEC 27001, ayrıca kurumların itibarını ve güvenirliğini arttırmaktadır. Teknolojik gelişmelere istinaden bilgi gizliliğinin, bütünlüğünün ve yanı sıra doğru kullanılabilirliği önem arz etmektedir. Kasıtlı veya bilmeyerek gerçekleştirilecek güvenlik ihlalleri kişi kurumların veri ihlallerine neden olabilmekte ve büyük kayıplara yol açabilmektedir. Her ne kadar teknolojik gelişmeler yaşansa da insanlar bilgi güvenliğini ihmal etmenin bir yolunu bulmuştur. Bu noktada zayıf halkanın teknolojik altyapılar değil, insanlar olduğunu söyleyebiliriz. Tek bir ürün ve teknolojinin kurum ve kişilerin güvenlik açıklarını kapatmaya yetmeyeceği göz önündedir. Çeşitli bilgi güvenliği birleştirmeleri ile güvenliği üst düzeye çıkarmak kurum ve kişilerin görevidir.

Sayısal ortamlarda verilerin korunmasına ilişkin oluşan bilgi güvenliği kavramı, bilgi varlıklarının ortamdaki tehditlerden, zarar görmeden kullanılabilmesi üzerinde çalışır. Bilgi güvenliğinin temel amacı, elektronik veya diğer ortamlarda bulunan her türlü bilginin; gizliliğin, bütünlüğünü, kullanılabilirliğini sürekli olarak sağlamaktır. Ağa bağlı kullanıcılara ait kullanıcı adı, parola, yüksek güvenlik seviyesi gerektiren, özel veya hassas verilere ait bilgilerin gizliliğinin en önemli ölçütlerindendir. İletişim ortamın da yetkisiz erişim, modifikasyon, veri tekrarı dinlemeleri, hizmet reddi ve paket üretimi gibi tehditlere karşı savunmak her daim önem arz etmektedir. Güvenli olduğunu iddia eden ağ protokollerinin sağlaması kullanıcıdan başlayarak tüm döngüdeki cihazları kapsamaktadır. Örneğin bir kablosuz iletişim sisteminin güvenlik gereksinimleri açık alanda akan verilerin gizliliğini, kullanıcı bilgileri gizliliğini ve en önemlisi de kullanıcı kimlik doğrulamayı sağlamayı içerir.

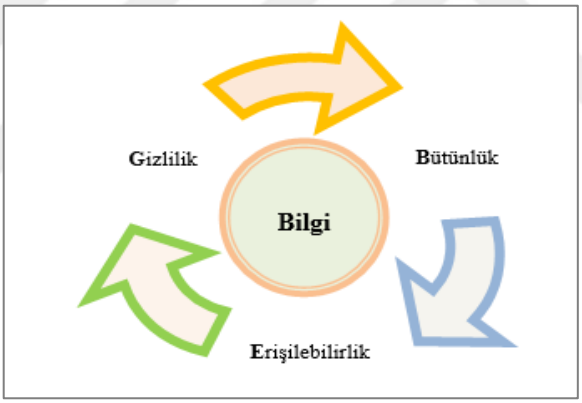
Kablosuz ağlar, verilerin fiziksel bir koruma olmadan hava ortamında iletilmesi sebebiyle saldırılara en açık iletişim şeklidir. Bu durumun bir zafiyet oluşturmaması ve

olası tehditlerin önlemesine yönelik kablolu ve kablosuz ağlarda güvenli iletişim için kullanılan kavram ve teknolojiler gelecek konularda ayrıntılı şekilde açıklanmıştır.

Bilgi Güvenliği Temel Unsurları

Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması, ek olarak doğruluk, açıklana bilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar (TS ISO/IEC 17799, 2002).

Bilgiye olabilecek yetkisiz erişimlerin engellenmesine gizlilik, yetkili erişim sonucunda kendine özgü bilgi mahremiyetinin korunmasına bütünlük, ihtiyaç halinde kolay ulaşılabilir olması erişilebilirlik denir. Şekil 13'de gösterilen bu bileşenler korunacak bir bilginin üç temel özelliğini teşkil eder (Şahinaslan, Kantürk, Şahinaslan, & Borandağ, 2009).



Şekil 13 - Bilgi Güvenliği: Bilginin Korunacak Temel Nitelikleri (Şahinaslan, E. 2010)

Bilgi güvenliğinin birinci amacı bilginin dışarıya erişimini engellemektedir, yani gizliliğini sağlamaktır. Bilgi güvenliği, bilgilerin izinsiz erişimlerden, farklı amaçlarla kullanımından, ifşa edilmesinden, kaybedilmesinden, değişme uğramasından veya hasar verilmesinden korunması ve engellenmesi işlemidir. Bilgi güvenliğinin temelinde gizlilik, bütünlük ve erişilebilirlik yatmaktadır (Boris, 2016).

Gizlilik (Confidentiality)

Bilginin yetkisi olmayan kişilerin eline geçmesini belirli yollar ile engellemeyi amaçlamaktadır. Bilgi hem bilgisayar sistemleri üzerinde her saniye işlenirken, hem depolama ortamlarında saklanırken, hem de network üzerinde istemci ve gönderici arasında taşınırken yetkisiz girişimlerden korunmalıdır. ISO standartları tarafından; Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi olarak adlandırılır. Bu yöntemde dikkat edilmesi gereken kritik nokta, bilginin tamamen gizlenmesini sağlamak değildir. Yetkisiz erişimlerin çeşitli güvenlik politikaları ile engellemesi ve erişimin gerçekleştiği durumlarda da ise uyarı mekanizmalarıyla bu durumdan haberdar olunabilmektir. Bu kapsamda gizliliği sağlamak için çeşitli kriptolama yöntemleri kullanılmaktadır.

Bütünlük(Integrity)

Bilgiyi tamamıyla kaybetmeden ve bir tam halinde tutabilmek bütünlüğü ifade etmektedir. Bilginin değiştirilmesini, bozulmasını, üzerine yeni veriler eklenmesini, tamamının veya bir kısmının silinmesini en katı şekilde engellemeyi hedefler. Bu amaçla kritik olarak belirlenen yapıların yedeklenmesi sağlanmalıdır. Bu yedekleme süreçleri bilginin önem derecesine göre anlık, saatlik ve günlük olarak yapılmasını hedefler. Bu kapsamda veri iletim halinde iken kesintiye uğramaması, bozulmaması ve güvenli bir şekilde erişimi gerçekleşir. Verinin izinsiz olarak veya yanlışlıkla bozuntuya uğraşması, silinmesinin veya veriye ekleme yapılmasının engellenmesi, verinin göndericiden alıcıya, göndericiden ilk çıktığı haliyle değişmeden tam bir bütün olarak erişmesini sağlar.

Erişilebilirlik (Availability)

Kullanılabilirlik, yetkili aktörlere verilen bilgi sistemlerine ve hizmetlere zamanında ve kesintisiz erişim anlamına gelir. Bir güvenlik mekanizmasında kullanılabilirlik, kaynakların ve verilerin yetkili kullanıcılar için erişilebilirliği konusunda kapsamlı bir güvence sağlar. Doğru birleştirmeler ile öngörülemeyen kesintilerle başa çıkılabilir. Veri imhasını ve kaybını önlemek ve güvenilir bir yedeklemeyi sürdürmek için yeterli düzeyde performans ve uygunluk sağlar. Erişilebilirliğe yönelik tehditler, yazılım ve elektrikli cihazlardaki arıza ve hatalar, kimyasalların ve sıvıların dökülmelerinin yanı sıra yüksek sıcaklık, hava sistemi hataları, su baskını gibi doğal faktörleri içerir. DDoS

saldırıları, veri imhası ve iletişim kesintileri dâhil olmak üzere bazı saldırı türleri kullanılabilirliği kesintiye uğratmaya odaklanır.

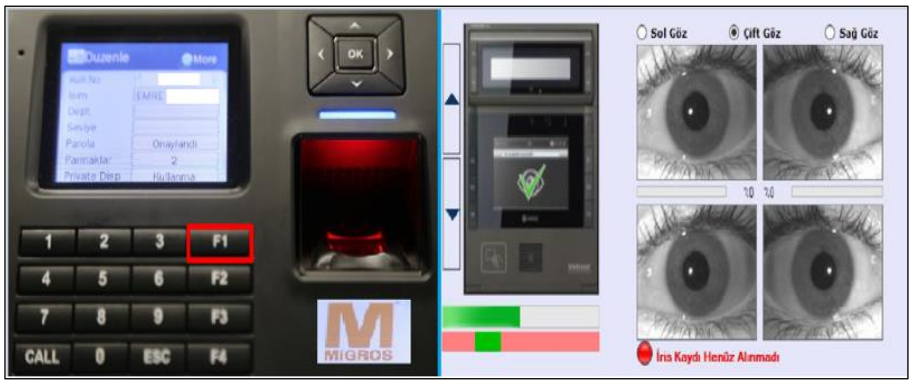
İnsan faktörleri, kullanılabilirlik için başka bir tehdit oluşturmaktadır. Hata, gözetim, yorgunluk, yetersizlik, stres vb. gibi etkenler ve hassas bilgilerin yetkisiz değiştirilmesi yoluyla erişilebilirlik sağlanamayabilir. Erişilebilirlik ihlalleri, kullanıcıların eylemleri, güvenlik politikasındaki yanlışlık veya güvenlik kontrolünün yanlış uygulanması nedeniyle de ortaya çıkabilir.

Kimlik Doğrulama Yetkilendirme Kayıt Tutma (AAA)

Ağ ve bilgi güvenliği genel tanımlamasında; Kimlik Doğrulama, Yetkilendirme, Kayıt Tutma terimlerinin İngilizce baş harflerinden oluşan, ağda dolaşan tüm veri paketlerinin çeşitli standartlara göre inceleyerek kayıt altına alan, gerektiğinde yetkilerini kısıtlayan ve bilgi güvenirliğini zedeleyici olanları da engelleyen sistemlerin bütünüdür.

Kimlik Doğrulaması (Authentication)

Erişimlerde kimlik (Idendity) tek başına güvenliği sağlayabilen bir unsur değildir. Kullanıcının gerçekten o kişi olduğunu kanıtlaması için ilk birincil olarak yapması gereken işleme ‘Kimlik Doğrulaması’ adı verilir. Kullanıcının bir cihaza veya uygulamaya ilk giriş sağlarken gerçekten o kişi olduğunu kanıtlaması işlemidir. Bu işlem adımı ile kullanıcının gerçek kişi olup olmadığı sistem üzerinden eşleştirilir. Daha sonra sistem tarafından kullanıcıya verilen parola ile doğrulama işleminin ikinci adımı gerçekleştirir. Bu eşleştirmeler doğru şekilde sağlanır ise sisteme giriş işlemi sağlanmış olacaktır. Bilgisayar yapıları ve bilgisayar ağları dışında kullanılan fiziksel sistemler için de çok fazla önem taşımaktadır. Bu sebep ile göz tarama, akıllı kart, parmak izi taraması, avuç içi biyometrik doğrulamalar ve dijital imza gibi teknolojilere dayalı kimlik sınama sistemleri kullanılamaya başlanmıştır. Şekil 14’de parmak ve göz tarama cihaz model örnekleri verilmiştir. Biyometrik fiziksel cihazlar kimlik doğrulama için birçok alanda kullanılmaktadır. Kopyalanması çok zor hatta imkânsıza yakın olan retina ve parmak izi bilgileri ile yetkili kişilerin kimlik doğrulaması yapılabilmektedir.



Şekil 14 - Parmak ve Göz Tarama İçin Kullanılan Örnek Cihazlar

Yetkilendirme (Authorization)

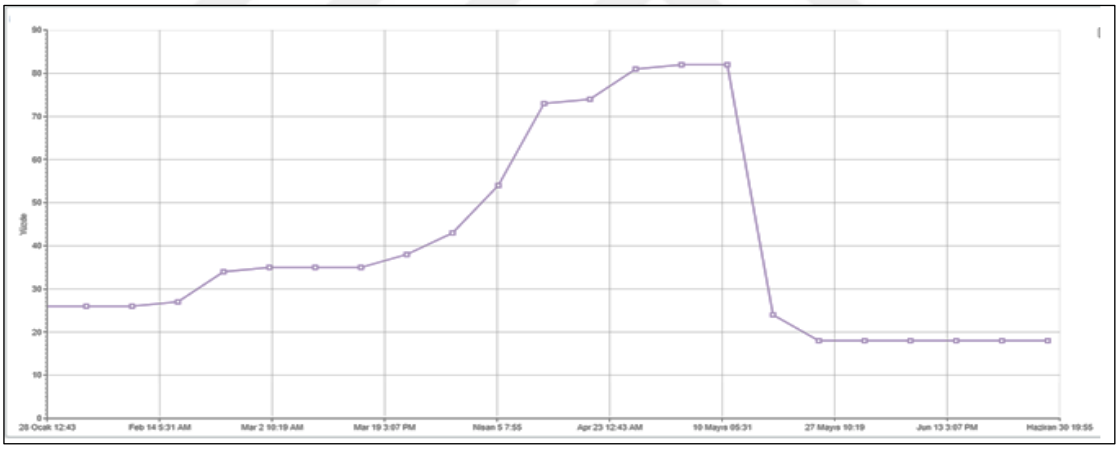
Kimlik doğrulamadan sonra ki en önemli adımdır, kullanıcı adı ve parolası ile sisteme erişim sağlayan kişinin hangi yetkilere sahip olacağını belirlemek çok önemli bir ölçüttür. Sisteme kayıtlı olan kullanıcılar belirli organizasyon gruplarına (OU) taşınır. Bu gruplara çeşitli yetkilendirmeler sağlanabilir. Örneğin; A grubu internete erişebilsin ancak haber sitelerine giremesinler. B grubu ise insan kaynakları ortak alanına erişebilsin, dosyaları görüntüleyebilsin ancak değişiklik yapamasın gibi çeşitli gruplar içerisine taşınan kullanıcılar sayesinde yönetim ve bilgi güvenliği daha kolay şekilde sağlanabilmektedir. Kullanıcılar birden fazla grup içerisinde de bulunabilirler. Kullanıcıların görev tanımlarına, bağlı bulunduğu bölüme, misafir olarak bağlanacakları ağ üzerinden erişecekleri tüm alanların belirlemesi yapılabilir. Hiçbir kullanıcıya fazladan yetki verilmemelidir. Bu yetkiler daha sonrasında bilgi güvenliği ihlallerine sebep olabilmektedir.

Kayıt Tutma (Auditing)

Kimlik doğrulama ve yetkilendirme adımları ne kadar sıkı da olsa sistemler üzerinde yetkisiz erişimler gerçekleşebilir. Bu erişimlerin geriye dönük ve anlık tespitleri için kayıt tutma işlemleri her an çalışır vaziyettedir. Sistemdeki tüm aktiviteleri takip ederek izin erişim ve yetkisiz kullanımların hangi aşamada yapıldığını ve ne kadar zarara neden olduğunu gözlemlerler. Sistemde bulunan kullanıcıların yaptıkları bütün aktiviteler ve erişim saatleri anlık olarak kayıt altına alınır. 5651 Sayılı Bilişim Hukuku Kanunun ve Kişisel Verileri Koruma Kanununun (KVKK) kapsamlarını zedeleyici tüm suçların

tespiti sağlanabilmektedir. Gerçek zamanlı kayıt tutma, network kaynaklarının tüketim ve kullanım kapasitelerini belirlemektedir. Bu kaynakların doğru dağıtımı kişisel ve sistemsel olarak performansa doğrudan etkisi bulunmaktadır.

Şekil 15 üzerinde örnek bir konumda bulunan erişim noktası (Access Point-AP) cihazının Ocak-Haziran 2020 arasındaki yüzdelik performans grafiği verilmiştir. Ocak ve Şubat aylarının ortalarında yüzde %20 ile yüzde %30 seyreden bir grafik çizmiştir. Şubat ayının son zamanlarında başlayan %35 üzeri performans artışı Mayıs ortalarına gelindiğinde yüzde %80 üzerini bulmuştur. Mayıs ayının son zamanlarında ise keskin bir düşüş yaşayarak Ocak ayındaki ilk performans grafiği olan yüzde %20'nin altına gerilemiştir. Performans artışının en büyük sebebi pandeminin ilk zirve zamanlarındaki saha ve e-ticaret operasyonlarının da zirve yapmış olmasıdır. AP ye erişen cihaz artmış ve yük artışı gerçekleşmiştir. Bu dönemde VoIP tabanlı görüşmeler lokasyonlar içerisinde artmış kablosuz erişimlerin performanslarının yükselmesine sebebiyet vermiştir.

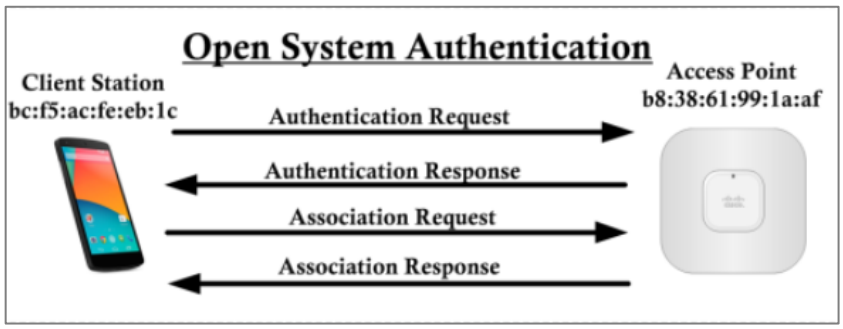


Şekil 15 - 2020 Ocak-Haziran Ayı Access Point Performans Değerleri

Açık Sistem Kimlik Doğrulama Yöntemleri (OSA)

Açık sistem yapısında kullanıcı ile AP arasında MAC adresi temeline dayanan bir kimlik iletimi söz konusudur. Şekil 16 üzerinde açık kimlik doğrulamasının çalışma prensibi verilmiştir. 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. Açık kimlik doğrulama, ağınızdaki bir RADIUS sunucusuna bağlı değildir (Cisco, 2008).



Şekil 16 - Açık Sistem Kimlik Doğrulama Prensibi

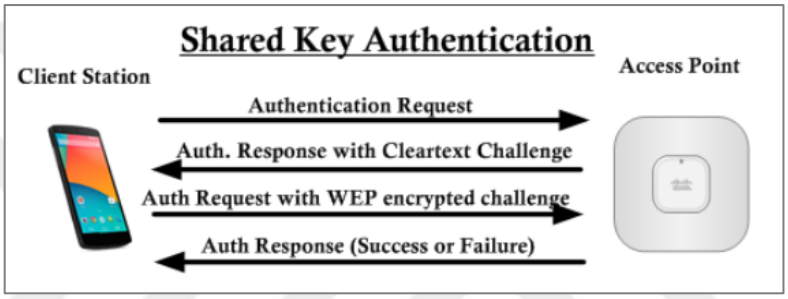
Açık sistem kimlik doğrulamanın çalışması için, bilgisayarın hizmet kümesi tanımlayıcısının kablosuz erişim noktasının SSID'si ile eşleşmesi gerekir. SSID, bir kablosuz yerel alan ağını benzersiz şekilde adlandıran bir karakter dizisidir. İşlem üç adımda gerçekleşir. İlk olarak, bilgisayar erişim noktasına bir kimlik doğrulama isteği gönderir. Daha sonra erişim noktası, yalnızca o oturum sırasında kullanılması amaçlanan, genellikle rastgele bir kimlik doğrulama kodu oluşturur. Son olarak, bilgisayar kimlik doğrulama kodunu kabul eder ve oturum devam ettiği ve bilgisayar orijinal erişim noktasının kapsama alanında kaldığı sürece ağın bir parçası olur. 802.11 ağlarının ilk ortaya çıktığı zamanlarda kullanılan bu yöntem daha sonrasında geliştirilerek kullanılmaya başlanmıştır. Ağa dâhil olacak cihazların MAC adresleri cihaz içerisinde tanımlanır. Bir nevi şifreleme ile güçlendirilmiştir. Bu yöntem güvenlik için yeterli değildir. MAC adresleri günümüzde yazılımlarla değiştirilebilmektedirler. Bu sebeple ağa erişen biri ağ trafiği dinleyerek paketleri çözümleyebilir. Araştırmalarımızın ilerleyen konularında bahsettiğimiz çeşitli güvenlik algoritma ve tasarımları ortaya çıkmıştır.

Paylaşılan Anahtar Kimlik Doğrulaması

Paylaşılan anahtar kimlik doğrulaması sırasında erişim noktası, erişim noktasıyla iletişim kurmaya çalışan herhangi bir aygıta şifrelenmemiş bir sınama metni dizesi gönderir. Kimlik doğrulama isteyen cihaz, sınama metnini şifreler ve onu erişim

noktasına geri gönderir. Sınama metni doğru şifrelenmişse, erişim noktası, istekte bulunan cihazın kimliğini doğrulamasına izsin verir.

Şekil 17 üzerinde paylaşılan anahtar kimlik doğrulamasının çalışma prensibi verilmiştir. Hem şifrelenmemiş sorgulama hem de şifrelenmiş meydan okuma izlenebilir, ancak bu, şifrelenmemiş ve şifrelenmiş metin dizelerini karşılaştırarak WEP anahtarını hesaplayan bir saldırganın erişim noktasını saldırıya açık bırakır. Saldırıya karşı bu güvenlik açığı nedeniyle, paylaşılan anahtar kimlik doğrulaması, açık kimlik doğrulamasından daha az güvenli olabilir. Açık kimlik doğrulama gibi, paylaşılan anahtar kimlik doğrulaması da ağınızdaki bir RADIUS sunucusuna dayanmaz (Cisco, 2008).



Şekil 17 - Paylaşılan Anahtar Kimlik Doğrulama Prensibi

Paylaşılan anahtar sistem kimlik doğrulamasında yanlış anahtar kullanım sınırlaması bulunmadığından iyi bir şifre sözlüğü bulunan kaba güç (brute force) saldırıları ile şifrelenmiş anahtarı elde etmek mümkündür.

Kabloluya Eşdeğer Gizlilik (WEP)

(Yao, Chong, & Xingwei, 2010)'a göre kablosuz aygıtlarda kullanılan 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 rastgele erişimli bellek alanı (RAM - Random Access Memory) gerekir.

WEP'de kimlik doğrulama tek taraflı çalışmaktadır. Erişim noktası istemcinin kimlik doğrulamasını sağlamaktadır. Erişim izni isteyen bir istemciye şifresiz bir paket gönderilir. İstemci aldığı paketi WEP anahtarı ile şifreler ve erişim noktası bu şifreli paketi doğrularsa istemcinin üye olması veya paket göndermesi izni verilir. Görüldüğü gibi erişim noktası istemciyi doğrulamaktadır ancak istemci erişim noktasını doğrulaması gibi bir kural yoktur. Ağ trafiğine zarar vermek isteyen biri istemciye yakın bir yerde erişim noktası ekleyip sabit çalışan ağa zarar verebilir ve istemciler fark etmeden bu erişim noktasına bilgi gönderebilir.

İstemci aldığı paketi WEP anahtarı ile şifreler ve erişim noktası bu şifreli paketi doğrularsa istemcinin üye olması veya paket göndermesi izini verilir. Erişim noktası istemciyi doğrulamaktadır ancak istemci erişim noktasını doğrulaması gibi bir kural yoktur. Ağ trafiğine zarar vermek isteyen biri istemciye yakın bir yerde erişim noktası ekleyip sabit çalışan ağa zarar verebilir ve istemciler fark etmeden bu erişim noktasına bilgi gönderebilir.

Wi - Fi Protected Access (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. 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, 2005).

WPA, güvenli kablosuz ağlar oluşturmak için oluşturulmuş bir güvenlik protokolüdür. WEP protokolüne benzer, ancak güvenlik anahtarlarını işleme biçiminde ve kullanıcıların yetkilendirilme biçiminde daha gelişmiş seçenekler sunar.

Şifrelenmiş bir veri aktarımının çalışması için, bir veri aktarımının başlangıcındaki ve sonundaki her iki sistemin de aynı şifreleme ve şifre çözme anahtarını kullanması gerekir. WEP her istemciye aynı anahtarı sağlarken, WPA, sistemlerin kullandığı anahtarı dinamik olarak değiştiren geçici anahtar bütünlüğü protokolünü

(TKIP) kullanır. Bu, dışarıdan erişimi engeller ve güvenli ağ tarafından kullanılanla eşleştirmek için kendi şifreleme anahtarlarını oluşturmalarını engeller.

(Klein, 2008)'e göre RC4, muhtemelen bir geri bildirim kaydırma yazmacına dayanmayan en popüler akış şifresidir. 1987'de Ron Rivest tarafından geliştirildi, ancak algoritma 1994'e kadar gizli tutuldu. Algoritmanın ilk yayını, şifreli posta listesindeki isimsiz bir postaydı. Bu yayından sonra RC4 tarafından oluşturulan sözde rastgele dizide birkaç zayıflık keşfedildi.

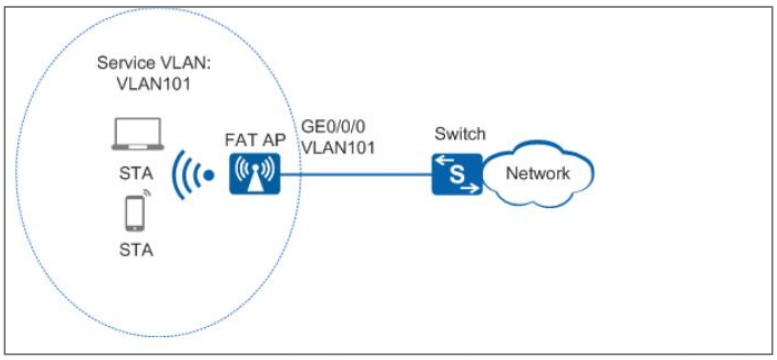
WPA ayrıca, kullanıcıları yetkilendirmek için Genişletilebilir Kimlik Doğrulama Protokolü (EAP) adı verilen protokollüde kullanır. Bilgisayarları MAC adreslerine göre yetkilendirmek yerine, WPA her istemcinin kimliğini doğrulamak için başka yöntemler kullanır. Bu, yetkisiz sistemlerin kablosuz ağa erişimini zorlaştırır.

Wi-Fi Protected Access 2 (WPA2)

IEEE tarafından 2004 yılında, Wi-Fi korumalı erişim II (WPA2) olarak anılan 802.1 standardı onayladı. WPA2, farklı donanımlar gerektiğinden WEP ve WPA ile geriye doğru uyumlu değildir. Bu standart, WEP ve WPA'daki zayıflıkları gidermek için tamamen yeniden tasarlanmıştır. WPA'da olduğu gibi, WPA2'yi iki modda kullanmak mümkündür: önceden paylaşılan anahtar (PSK) modu veya IEEE 802.1X kimlik doğrulamasını kullanabilmektedir. 256 bitlik bir PSK oluşturmak için 8 ila 63 karakter uzunluğunda bir parola kullanır. Ağa bağlanan her istemci cihaz aynı parolayı kullanır. Bu, bir ev ağında kullanımı kolaylaştırır, ancak aynı zamanda bir güvenlik sorunu oluşturur. Birisi bir WPA2 ağının parolasını biliyorsa, alabileceği trafiğin şifresini çözebilir.

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. Anahtar şifresi ile hem şifreleme, hem de şifre çözme işlemleri gerçekleştirilir. 128 bitlik veriler 128, 192 ve 256 bit olarak işlem görürler. AES şifreleme, bir turu oluşturan 4 aşamayı içerir. Her geçiş, bit anahtar boyutuna bağlı olarak 10, 12 veya 14 kez yinelenir. AES'in WPA2/802.11i uygulaması için, her tur 10 kez

yinelenir. Şekil 18'de WPA2-PSK-AES güvenlik politikasını yapılandırmak için ağ şeması prensibi görülmektedir. İstemcilerden çıkan paket güvenli alan içerisinde switch üzerinden işlem sağlamaktadır.



Şekil 18 - Wi-Fi Protected Access 2 (WPA2) Protokolü Çalışma Prensibi (Huawei, 2020)

Wi - Fi Protected Access 3 (WPA3)

Ocak 2018 itibariyle Wi-Fi ittifakı (Wi-Fi Alliance) tarafından WPA2'nin yerini alacak olan WPA3 standardını geliştirmiştir. WPA3, Wi-Fi aygıt kaydı protokolü (DPP) ile çalışmaktadır. Bu protokoldeki metod şifreyi açık ortama aktarmadan sisteme nasıl erişeceklerini belirtmektedir. DPP metodu ile kullanıcılar 'quick response' metodu veya NFC etiketlerini kullanmaktadırlar. WPA3 şifreleme metodu ev, ofis ve halka açık tüm ortamlarda gizliliği ve siber saldırıları önlemek için daha fazla koruma katmanı sağlamaktadır.

WPA3, şifre paylaşım metodu yerine, şifrenin paylaşımına gerek duymayan yöntemler ile network üzerinde işlem sağlar. Wi-Fi Aygıt Kaydı Protokolü (DPP) olarak adlandırılan bu yeni sistem, şifreyi ortam içerisinde paylaşmadan sisteme nasıl erişim sağlanacağını ileterek çalışır. WPA3 algoritma olarak 256-bit ile korunur. Bu metod Galois-Counter Mode Protokolü (GCMP-256) ile encapsüle edilir. Diğer Wi-Fi erişim protokollerinde 128 bit şifreleme metodu kullanır iken, WPA3'de 256 bitlik şifreleme metodu kullanılmaktadır. 256 bit şifreleme 3.048x 10^38'e denk gelmektedir. Bu metod ile şifrenin çeşitli programlar ve hesaplamalar ile kırılması neredeyse imkânsızdır.

Tablo 4'de WEP, WPA, WPA2 ve WPA3 güvenlik algoritmaları hakkındaki farklar detaylı olarak verilmiştir. Önceki tüm değerlendirmelerden elde edilen en önemli sonuç, birçok kusur keşfedildiği için WEP'ten her zaman kaçınılması gerektiğidir. Eski donanıma sahip cihazlar WPA'yı kullanacak şekilde güncellenmelidir. Bu kadar sık anahtar çarpışmalara izin vermez ve geçici anahtarlar getirir. Öte yandan, bir cihaz WPA2 için donanım desteği sağlıyorsa, her zaman kullanılmalıdır. Mesaj bütünlüğü ve şifreleme açısından en iyi güvenliği sunar. WPA3 ile birlikte güvenlik yöntemlerinin daha fazla gelişeceği öngörülmektedir. Saldırı yönetmeleri arttıkça bunlara karşı güvenlik önlemleri de doğru orantıda artmaktadır.

Tablo 4 - Wi-Fi Güvenlik Algoritmalarının Karşılaştırılması

	WEP	*WPA*	*WPA2*	*WPA3*
Anlamı	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
Çıkış Tarihi	1997	2003	2004	2018
Güvenlik Seviyesi	Çok Zayıf	Zayıf	Güçlü	Çok Güçlü
Şifreleme Standardı	RC4	TKIP ile RC4	AES-CCMP	AES-CCMP AES-GCMP
Anahtar Boyutu	64 Bit 128 Bit	128 Bit	128 Bit	128 Bit 256 Bit
Kimlik Doğrulama Standardı	Açık Sistem ve Paylaşılan Anahtar	PSK, 802.1x ve EAP	PSK, 802.1x ve EAP	AES – CCMP AES-GCMP
Bütünlük	CRC-32	64 Bit	CCMP ve AES	SHA-2

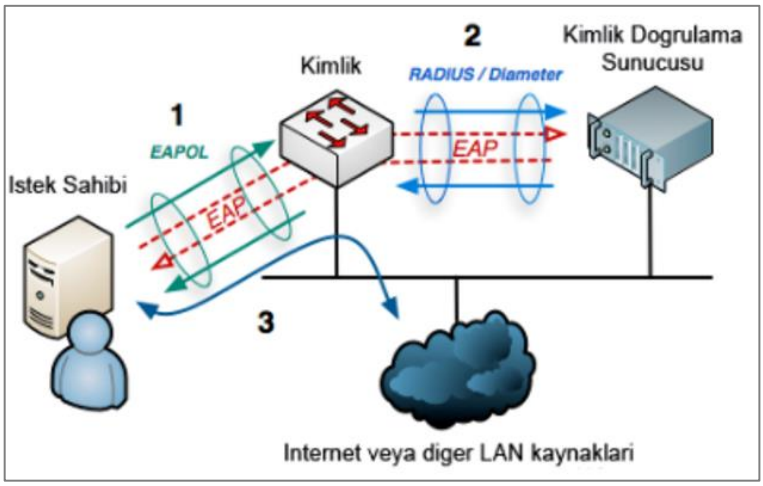
802.1x Bağlantı Tabanlı Ağ Erişim Kontrol Protokolü

Port tabanlı ağ erişim denetimi, noktadan-noktaya bağlantı özelliklerine sahip bir yerel ağ portuna takılan cihazların kimlik doğrulaması ile sağlanır. Kimlik doğrulaması ve yetkilendirmesi başarısız olması durumunda o portu erişime kapatır. IEEE 802 yerel ağ altyapılarının fiziksel erişim özelliklerinin kullanımına olanak sağlayan, port tabanlı

ağ erişim denetimi 802.1X teknolojisidir. Ağda port tabanlı kullanıcı doğrulayabilmek, herhangi bir kullanıcıya ya da gruba ağ erişim politikaları uygulamaya imkân tanır. Kullanıcı doğrulama; MAC adresi, switch portu ya da harici bir yetkilendirme politikası ile sağlanır. Ağa kullanıcıların hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirmesi sağlanır. Bu süreç kullanıcı odaklı ve ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir.802.1x protokolü Yetkilendirme (Authentication), kimlik doğrulama (Authorization) ve hesap yönetimi (Accounting) kısaca AAA düzeni ile çalışır. Şekil 19'da 802.1x genel ağına erişmek isteyen kullanıcının izlediği yol ve doğrulama protokolleri gösterilmiştir. Yapı üzerindeki süreç maddeler halinde açıklanmıştır.

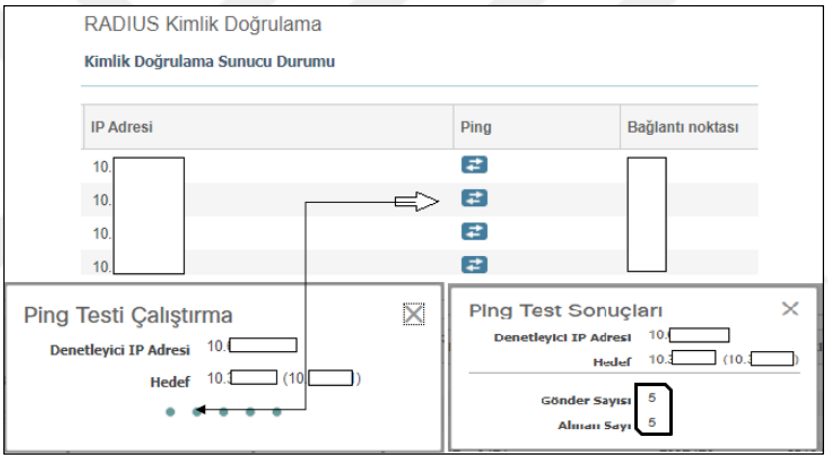
I. İstemci ve kimlik denetiminin yapıldığı sunucu arasında bulunan denetleyici cihaz, bağlantı durumunda istemciye EAP-Request/Identity paketi göndererek kimliğini belirlemesini ister
II. İstemci, kimliğini doğrulayan EAP-Response/Identity paketi ile bu talebe cevap verir.
III. Bu paket encapsulation yapılarak sunucuya tekrar geri gönderilir.
IV. Sunucu bu aşamada denetleyiciye şifreli token davetiyesi gönderir. Denetleyici bu paketi açıp EAPOL (LAN üzerinden EAP) içerisinde istemciye tekrar geri gönderir. İstemci davetiyeye denetleyici üzerinden cevap gönderir.

Son aşamada istemci gerekli kullanıcı tanımına ve haklarına sahipse, sunucunun gönderdiği doğrulayıcı mesaj denetleyicinin istemciye internet ve diğer LAN kaynaklarına erişim izni vermesiyle sonuçlanır.



Şekil 19 - 802.1x Port Tabanlı Ağ Erişim Süreci (Wikipedia, 2020)

Şekil 20 üzerinde AP yönetim ekranında RADIUS sunucusuna erişim doğrulaması (ping) testi yapılmıştır. Ağ cihaz yönetim ekranında seçilen herhangi bir AP içerisinde güvenlik ekranından RADIUS kimlik doğrulama adımına geçiş yapılmıştır. RADIUS kimlik doğrulama adımında sunucu dizini, IP adresi, doğrulama kolonu (ping), bağlantı noktası ve yönetici kontrol durum ekranı bulunmaktadır. Bu alan içerisinde RADIUS kimlik doğrulama ping'i gönderimi sağlanarak, güvenlik noktalarının ne kadar verimli ve istikrarlı çalıştığı test edilebilir. Ping adımına geçildikten sonra, ping testi çalıştırma ekranı açılacak ve denetleyici IP adresi ile hedef IP adresini doğrulamak için bir önceki maddelerde belirtilen doğrulama yöntemlerini kullanacaktır. Gönderilen ve alınan sayıların eşit olması (5/5) RADIUS sunucusu ile istikrarlı çalıştığını göstermektedir.



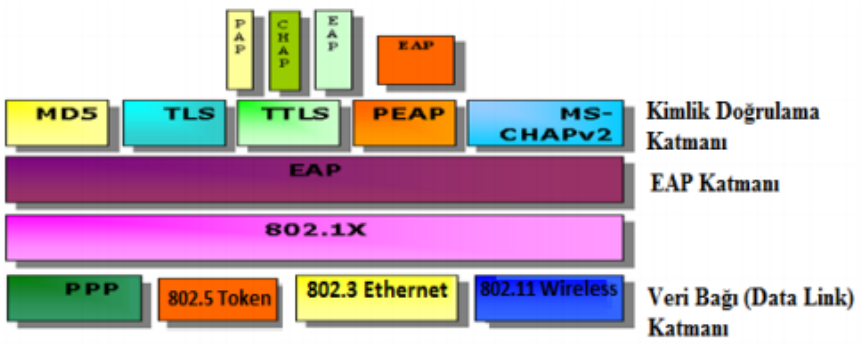
Şekil 20 - AP'den RADIUS Sunucusuna Yapılan Ping Testi Çıktısı

Genişletilebilir Kimlik Doğrulama Protokolü (EAP)

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. EAP protokolü; belirteç kartları, akıllı kartlar, sertifikalar, tek kullanımlık parolalar ve gibi birden çok kimlik doğrulama mekanizmasını destekleyebilir. Bunun yanı sıra, kimlik kanıtlama sunucusu ile istemci arasında arabuluculuk yaparak tarafların hangi kimlik kanıtlama yöntemini kullanacakları konuşmasında da kullanılır.

İşleyiş şekilli şu şekildedir; EAP kullanan iletişimlerde, bir kullanıcı bir erişim noktası (bazen alıcı-verici olarak da bilinen veri ileten ve alan bir istasyon) aracılığıyla kablosuz bir ağa bağlantı ister. Erişim noktası, kullanıcıdan kimlik verilerini ister ve bu verileri bir kimlik doğrulama sunucusuna iletir. Kimlik doğrulama sunucusu, erişim noktasından kimliğin geçerliliğinin kanıtını ister. Erişim noktası bu doğrulamayı kullanıcıdan aldıktan ve doğrulama sunucusuna geri gönderdikten sonra, kullanıcı istendiği gibi ağa bağlanır.

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 istinaden çeşitli algoritmalar geliştirilmiştir (Tarlacı, 2018). EAP'ın kullanıldığı yapı katman olarak Şekil 21'de verilmiştir.



Şekil 21 - Genişletilebilir Kimlik Doğrulama Protokolü (EAP) Mimarisi (Kurt, 2013)

EAP- MD5 (Message Digest 5)

MD5 kriptografik özet algoritmasıdır, MIT Profesörü Ronald Rivest tarafından tasarlanmıştır. 128 bitlik bir karma değer üretmektedir. MD5 algoritması, 32-bit makinelerde oldukça hızlı olacak şekilde tasarlanmıştır. MD5 algoritması tablolar içerisinde büyük bir alan gerektirmez ve algoritma oldukça kompakt bir şekilde kodlanabilir. MD5 algoritması, MD4 mesaj özet algoritmasının bir uzantısıdır. MD5, MD4'ten biraz daha yavaştır, ancak daha güvenilir bir tasarımdır. MD5, MD4 e göre daha yavaş olması ilk çıktığı zamanlarda eleştirilmiştir. Ancak MD4 olağanüstü hızlı olacak

şekilde tasarlandığından kriptografik olarak saldırılara daha açıktır. MD5 bu sebeple daha yüksek güvenlik sağlamaktadır (Rivest, 1992).

EAP kimlik doğruma yöntemlerinin içerisinde en basit denetleme yöntemi EAP-MD5'tir. Kablosuz ağ üzerinden açık şekilde şifrenin iletilmesinden olayı kullanımı önerilmez. Kablosuz ağ üzerinden kullanımı açısından güvensiz olduğundan kablolu üzerinden kullanılmaktadır. MD5 tek yönlü olarak kimlik denetimi yapmaktadır. MD5'in en önemli zafiyeti kimlik denetleyicisine giriş ve tek yönlü olarak işlem sağlamasıdır. Kimlik denetleme modunda açık metin olarak şifreyi içermesidir. Bu sebep ile kablosuz ağ üzerinden yapılan Ortadaki Adam (MITM) saldırısı için çok zayıf bir güvenlik sağlamaktadır. MD5 anahtar denetimi sağlamamaktadır. Özellikle ilk çıkan eski sistem WEP sürümünün anahtarlarının şifresini çok rahatlıkla kırabilirler.

LEAP (Lightweight EAP)

Cisco tarafından geliştirilen LEAP Kablosuz ağlarda kullanılan çift yönlü kimlik denetimini destekleyen bir EAP kimlik denetleme yöntemidir. Yaygın kullanılan kimlik denetleme sunucusu (RADIUS) sunucusu sayesinde kullanıcı adı ve şifre eşleştirmesini erişim noktası (AP) üzerinden sağlar.

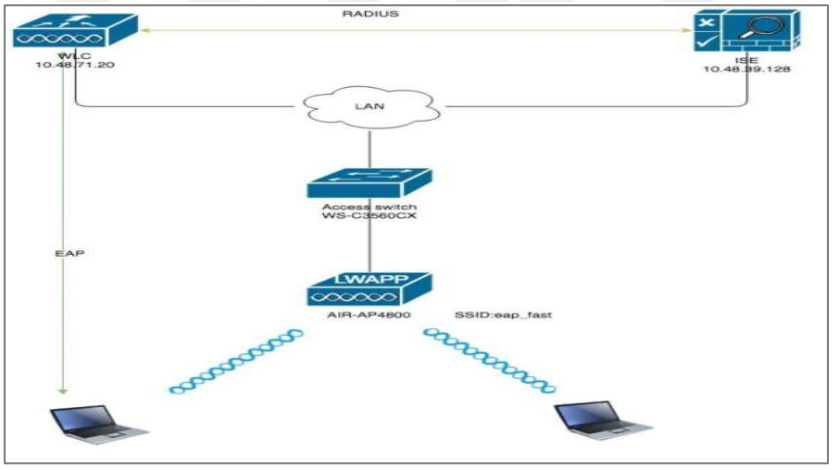
LEAP, oturum eşleştirmesi sağlamak için tek zamanlı WEP anahtarı oluşturmaktadır. Veri transferi her şifreleme aşamasında değişir. WEP üzerinden karşılıklı kimlik doğrulama işlemi gerçekleşir. Ağ üzerinde erişim sağlamak isteyen her kullanıcı farklı WEP anahtarı oluştur. Güçlü şifrelerin kullanımına özel dikkat gösterilmelidir. Cisco LEAP, parola tabanlı bir algoritmadır. Başarılı bir sözlük saldırısı olasılığını en aza indirmek için tahmin edilmesi zor olan güçlü parolalar kullanın. Güçlü parolaların bazı özellikleri şunlardır: En az on karakter, büyük ve küçük harflerin karışımı, en az bir sayısal karakter veya alfa sayısal olmayan bir karakter, kullanıcı adı veya kullanıcı kimliğinin hiçbir biçimi, sözlükte bulunmayan bir kelime (Cisco, 2020).

LEAP'ın saldırılara açık olmasının en büyük sebebi, çift yönlü kimlik denetimi için MS–CHAPv1 protokolünü kullanıyor olmasından kaynaklanmaktadır. LEAP

algoritmasının en büyük eksikliği Cisco ağlar üzerinden uçtan uca olarak kullanılıyor olmasıdır.

EAP – FAST

EAP-FAST protokolü, Cisco'nun 802.1X EAP türü dağıtmak isteyen müşterileri desteklemek için geliştirdiği, genel erişime açık bir IEEE 802.1X EAP türüdür. Kimliği Doğrulanmış Diffie-Hellman Protokolünü (ADHP) kullanır. Bu aşama diğer aşamalardan bağımsızdır. Cisco tarafından da geliştirilen doğrulama yöntemi olarak çok yaygın bir şekilde kullanılmaktadır. EAP-FAST, bir Korumalı Erişim Kimlik Bilgisi (PAC) kullanılarak oluşturulan bir Taşıma Katmanı Güvenliği (TLS) tüneli üzerinden kimlik doğrulama işlemi gerçekleştirir. Şekil 22 üzerinde EAP FAST çalışma protokolü gösterilmiştir. İstemciler ve erişim noktası arasında oluşan TLS tüneli dışarıdan erişimi engellemektedir.



Şekil 22 - EAP-FAST Cisco Güvenli Erişim Topolojisi (Cisco, 2019)

PAC: PAC'ler, ISE ve bir EAP-FAST son kullanıcı istemcisinin birbirlerinin kimliğini doğrulamasını ve EAP-FAST ikinci aşamada kullanılmak üzere bir TLS tüneli oluşturmasını sağlayan güçlü keydir. ISE, aktif ana anahtar ve bir kullanıcı adı kullanarak PAC'ler oluşturur. (Cisco, 2019)

PAC şunları içerir:

- **PAC-Key:** Bir istemciye (ve istemci cihaza) ve sunucu kimliğine bağlı paylaşılan anahtar (Cisco, 2019).
- **PAC-Opaque**: İstemcinin önbelleğe aldığı ve sunucuya aktardığı Opaque alanı. Sunucu, istemciyle karşılıklı olarak kimlik doğrulaması yapmak için PAC Anahtarını ve istemci kimliğini kurtarır (Cisco, 2019).
- **PAC-Bilgisi**: Asgari olarak, istemcinin farklı PAC'leri önbelleğe almasını sağlamak için sunucunun kimliğini içerir. İsteğe bağlı olarak, PAC'nin sona erme süresi gibi diğer bilgileri içerir (Cisco, 2019).

EAP – TLS

EAP-TLS, RFC 2716'da açıklanmıştır. Aralarında karşılıklı kimlik doğrulaması sağlamak için istek sahibi için ortak anahtar altyapısı (PKI) dijital sertifikası ve kimlik doğrulama sunucusu kullanır. PKI sertifikası, sunucunun adı veya kullanıcının bilgileri hakkında bilgi içerecektir. Kullanılan güvenli yöntemlerden biridir, çünkü talep eden ile kimlik doğrulama sunucusu arasında TLS tüneli sertifika alışverişi sırasında oluşturulur. Burada dikkat edilmesi gereken bir diğer husus, EAP mesajlarını korumak için bir tünel oluşturulsa bile, sertifika değişim süreci başlamadan önce kullanıcı kimliğinin açık bir düz metin olarak gönderilmesidir. Karşılıklı olarak kimlik doğrulama ve sertifika için güvenli taşıma tüneli oluşturur. Dinamik yeniden anahtarlama mümkündür. Bakım maliyeti fazladır, güvenli olmasına rağmen ağ yöneticileri arasında popüler değildir. Talepte bulunan ve taraflar arasında karşılıklı sertifika değiş tokuş edilmelidir ve uygulamayı zorlaştıran kimlik doğrulama sunucusudur.

EAP-TLS karşılıklı doğrulama işlemi şu şekilde yapılır:

I. İstemci erişim noktası (AP)'na bağlanır olur.
II. Bu sürede diğer tüm erişimler bloklanır ve doğrulanana kadar işlem sağlanmaz
III. İstemci, dijital sertifika ile sunucuyu doğrular.
IV. Sunucu, dijital sertifika ile kullanıcıyı doğrular.

V. Sunucuda ve istemci fiziksel kartında dinamik WEP işlem anahtarı oluşturulur.

VI. Sunucu bu işlem anahtarını güvenli kablolu ağ yapısı üzerinden erişim noktasına gönderir.

VII. Erişim noktası ve istemci tek kullanımlık bu doğrulama anahtarını aktif hale getirirler ve birbiri ile iletişim kurar iken kullanır.

EAP-TTLS

EAP-TTLS, IETF RFC 5281' de ilk olarak açıklanmıştır. EAP-TTLS, EAP-TLS'nin devamı niteliğindedir ve PKI dijital sertifikasını kaldırmak için ve TLS uygulanırken karşılaşılan uygulama zorluğunu en aza indirgemek için oluşturulmuştur. EAP- TTLS'nin ortaya çıkmasından sonra kimlik doğrulama sunucusunun tek başına istek sahibinin kimliğini doğrulaması gerekir. İstemci isteğe bağlı olarak sunucuya kendi kimliğini doğrulayabilir. Bu sebeple, bir veya iki yönlü kimlik doğrulama yön yöntemi olarak rol almaktadır. EAP-TTLS istemci kimlik doğrulaması için PAP, CHAP, MSCHAP ve MSCHAPv2 gibi birçok dâhili protokolü desteklemektedir. Kimlik doğrulama süreci güvenli ağ tünelinin içerisinde gerçekleşmektedir. TTLS'nin TTLSv1 ve TTLSv2 ve TTLSv3 olmak üzere üç sürümü vardır. SSL tüneli oluşturmak, geriye dönük tüm eski kimlik doğrulama yöntemlerini desteklemek, önceki sürüm TLS üzerindeki gibi dinamik yeniden anahtarlama ve kullanıcı kimliği koruması gibi önemli avantajlar sağlamaktadır.

PEAP (Protected Extensible Authentication Protocol)

EAP-PEAP, TLS'ye benzer şekilde çalışır. Kimlik doğrulaması için özel anahtar altyapısı (PKI) dijital sertifikaları kullanır. TLS'den farklı olarak, EAP-PEAP, istemciye kendi kimliğini doğrulamak için yalnızca bir sertifika gerektirir (yani, yalnızca sunucunun istemciye kendi kimliğini doğrulaması gerekir. Bu nedenle, isteğe bağlı istemcinin kimlik doğrulama sunucusunda kimliğini doğrulaması için TTLS'den farklı olarak tek yönlü bir kimlik doğrulama yöntemidir. EAP-PEAP, istek sahibi ile kimlik doğrulama sunucusu arasında, aralarında EAP iletilerini geçirmek için güvenli bir tünel oluşturur. PEAP'de, iç güvenli tünel içinde yalnızca EAP-MD5, EAP MSCHAPv2,

PEAPv1/EAP-GTC vb. gibi değişken yöntemler kullanılabilir. PEAP, çeşitli eski protokolleri kullandığından, kimlik doğrulayıcı yalnızca paketleri arasında aktarmak için kullanılır. Avantajları; Güvenli SSL tüneli oluşturur, kullanıcı kimliği korumalıdır, hızlı yeniden bağlantıları destekler, mesaj doğrulama ve şifreleme sağlar. Dezavantajları; Mesaj alış verişinin çok fazla olması sebebiyle daha fazla ek yük getirmektedir. Sunucu kimliği doğrulaması için sertifika yetkisi (CA) gerekmektedir.

PEAPv0/EAP-MSCHAPv2: İç kimlik doğrulama yöntemi MSCHAPv2'nin açılımı Microsoft's Challenge Handshake Authentication Protocol'dür yani "Microsoft Karşılıklı Kimlik Doğrulama Protokolü"dür. Bu form Microsoft NT ve Microsoft Active Directory'de bulunan ve MS-CHAPv2 destekleyen database'e kimlik doğrulama yetkisi verir (NetworkKampus, 2018).

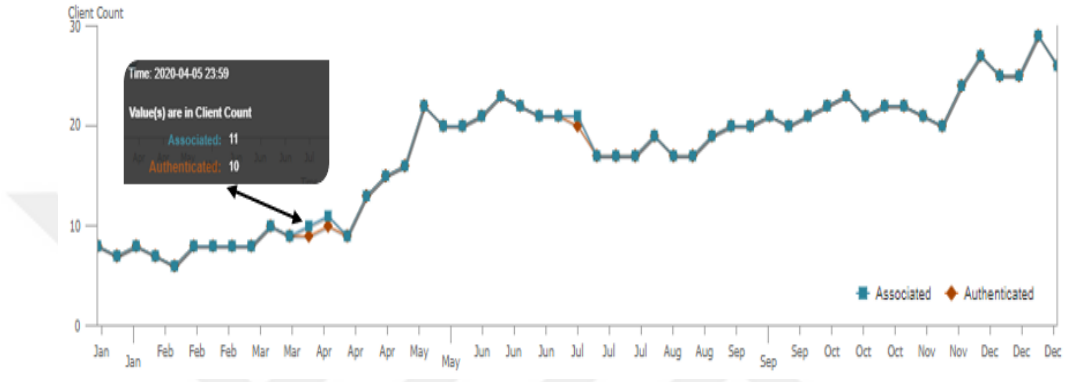
PEAPv0/EAP-MSCHAPv2, PEAP yönetimin en eski ve en yaygın formudur. Dünyada EAP-TLS 'den sonra ikinci en çok kullanılan şifreleme yöntemidir. Dolaysıyla Microsoft, Apple ve Cisco gibi birçok istemci/sunucu firması ve Open1x.org projesinden xsupplicant ve WPA supplicant gibi diğer uygulamalar tarafından desteklenmektedir. Ayrıca bu yöntem, diğer EAP şifreleme yöntemleri ile birlikte dinamik şekilde kullanılabilmektedir (NetworkKampus, 2018).

PEAPv0/EAP-MSCHAPv2 ile art niyetli bir istemcinin CA (Certificate Authority) sertifikası onaylanmaz ve böylece örneğin MS-CHAPv2 handshake sağlayan sahte bir wireless access point ağa alınmamış olur (NetworkKampus, 2018).

PEAPv1/EAP-GTC: Bu yöntem Cisco firması tarafından var olan diğer korunmuş bir kanal vasıtasıyla yapılan kimlik doğrulama temelli dizinler ve token card'ları ile birlikte ortak çalışıla bilirliği sağlamak amacıyla oluşturulmuştur. Bu yöntemi Windows İşletim sistemleri desteklememektedir (NetworkKampus, 2018).

Şekil 23'de örnek bir lokasyona ait AP'de kullanıcı erişim oranları ve erişen kullanıcıların kimlik doğrulama oranları verilmiştir. Belirli noktalarda erişimler ile kimlik doğrulama oranlarının eşit olmadığı görülmektedir. Nisan ayının 5'inde erişim sağlayan 11 cihazdan 10 u doğru ve protokollere uygun erişim sağlamış iken 1 cihazın erişiminde

kimlik doğrulaması tam olarak gerçekleşmediği görülmektedir. Erişim noktası (AP)'na erişen cihazların kimlik doğrulama oranlarına eşit olması beklenmektedir. Bu eşitlik sağlanmadığı durumlarda güvenlik zafiyetleri ortaya çıkmaktadır. Kimlik doğrulama adımlarında erişim noktasına doğru ve güvenli bağlantı sağlanabilmesi için kurumsal kimlik doğrulama adımları tam olarak uygulanması gerekmektedir. Cihazlara yüklenen sertifikalar bu yönde önem arz etmektedir.

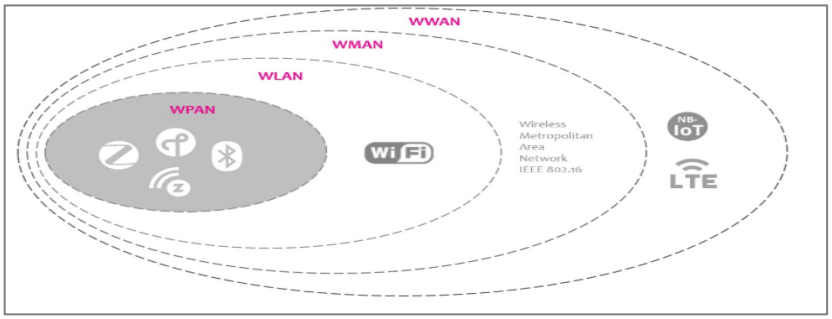


Şekil 23 - Erişim Noktasına Ait Kullanıcı Erişimi/Kimlik Doğrulama Oranı

Kablosuz yapıların gelecek yıllarda daha çok devreye alınacağı göz önünde iken, Açık sistem kimlik doğrulama ve 802.1x tabanlı kimlik doğrulama yöntemlerinin en sıkı şekilde uygulanması kişi ve kurumların bir görevi haline gelmiştir. İnsan faktörünün olduğu her noktada CIA (Gizlilik Bütünlük Erişilebilirlik) ve AAA (Kimlik Doğrulama Yetkilendirme Kayıt Tutma) kuralları en iyi şekilde uygulanmalıdır

Büyüklüklerine Göre Kablosuz Ağlar

Kablosuz ağlar ihtiyaca ve büyüklüklerine göre tasarlanmıştır. Şekil 24'de genel kapsamıyla belirtilen bir yapıya göre hazırlanmış bir sistemsel üründür. Bu sebeple de farklı açılardan bakıldığı zaman da çeşitli kablosuz ağ türlerini de görmek mümkündür. Bu ağ yapılarının oluşturulmasında fiziksel olanaklar, tasarım, arz/talep oranları ve erişilebilirlik ön plana çıkmaktadır. Maliyet ve fayda oranlarının en iyi şekilde sağlanabilmesi için çeşitli kablosuz yerel alan ağ yapıları oluşturulmuştur. Bunları WPAN, WLAN, WMAN, WPAN olarak sıralayabiliriz.



Şekil 24 - Büyüklüklerine Göre WLAN Yapıları (Computer Controls, 2020)

WPAN (Kişisel Ağ Bağlantısı)

PAN kişisel cihazların birbiriyle bağlanması sonucu elde edilen kişisel ağdır. Infared (IR) ve Bluetooth (BT) günümüzde PAN ağlarında en çok kullanılan teknolojilerdir. BT 10 ile 200 metre arasında bağlantı sağlarken (700 kbps) IR ancak bir kaç metre içerisinde bağlantı sağlar (115 kbps). PAN bağlantısı sağlandığında PAN'ın parçası olan tüm etkin aygıtlar (cep telefonu, USB, fotoğraf makinesi, yazıcı gibi) ve bilgisayarlar arasında erişim sağlanır. Kişisel ağ bağlantısı, bilgisayar ile ağ dâhilindeki diğer bilgisayar ve cihazlar arasında otomatik olarak bağlantı kurulmasını sağlar (İTÜBİDB, 2013).

WLAN (Yerel Ağ Bağlantısı)

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

WMAN (Yerleşke Ağ Bağlantısı)

Bünyesinde birden çok LAN sistemi barındıran, coğrafi ölçekte LAN ve WAN arasında büyüklüğe sahip bir ağ sistemidir. LAN'ları birbirine bağlayarak Wide Area hizmetini LAN'a ulaştırır. Tek bir kuruma veya kuruluşa ait olabildiği gibi kamuya açık

bir hizmet şeklinde de olabilir. Gigabit, 10 Gigabit veya kablosuz teknolojileri kullanabilir. Bir şehri tamamen kaplayacak büyüklüğe ulaşabilir (İTÜBİDB, 2013).

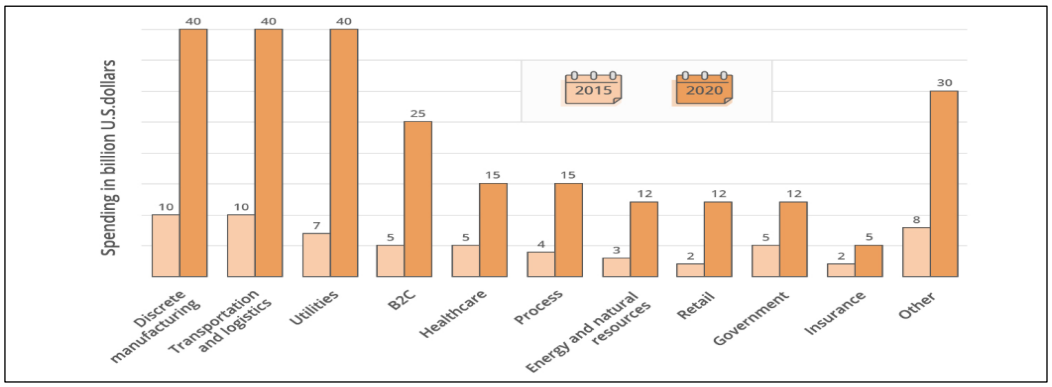
WAN (Geniş Ağ Bağlantısı)

Coğrafi olarak en geniş alanı kapsayan ağ çeşididir. Dünya üzerine yayılmış ağ yapılarını ifade eder. Genellikle WAN teknolojileri LAN'a göre daha yavaştır. Son kullanıcıdan gelen talep doğrultusunda DSL (Digital Subscriber Line - Sayısal Abone Hattı) ve kablo ve fiber teknolojileri ile yüksek hızlar sağlanabilmektedir. Kurum ve kuruluşların uzaktaki şubelerini birbirine bağlamak için WAN teknolojileri kullanılabilir. Ethernet teknolojisinin WAN'da kullanılmaya başlamasıyla kuruluşların yüksek bant genişliği ihtiyacı karşılanmıştır (İTÜBİDB, 2013).

Kablosuz Yerel Alan Ağların Avantajları

Kablosuz bir ağ yapısının en büyük avantajı, iletişimin gerçekleşebilmesi için en az donanım yapısına ihtiyaç olmamasıdır. Donanımı en aza indirgemesinden ve dolaşım özgürlüğünü beraberinde getirmektedir. Özellikle büyük yapıdaki ağların mevcut kablolu (fiber/bakır vb.) bağlantısının kesilmesi veya değişmesi durumunda anlık çözüm olarak noktadan noktaya (P2P-Peer to Peer) kablosuz bağlantı ile kullanıcıların erişimlerinin devam etmesini sağlamaktadır. Buna ek olarak belirli dönemlerde yenilenmesi gereken kablolu ağların maliyet oranlarında azaltılmış olur. Fiziksel kablolama işleminin uygun olmadığı tarihi eser niteliği taşıyan yapıların korunması içinde kablosuz ağlar kullanılmaktadır.

IoT cihazların gelişimi, veri miktarının artması, yapay zekâ ürünlerinin küresel pazarda önem kazanması ve bulut teknolojilerindeki gelişimler sebebiyle Wi-Fi ile bütünleşmiş iş modelleri oluşturma ihtiyacı duyulmaktadır. Özellikle Wi-Fi 6 ve 5G iletişim modellerinin yaygınlaşmasıyla beraber güvenlik sorunları, performans, enerji sarfiyatı azlığı ve kurulum bakım maliyeti açısından her noktanın büyük aşamada bilinmesinden dolayı kablosuz ağlar her sektörde ilgi çekici olmaktadır.



Şekil 25 - 2015-2020 Yılları Sektörel IoT Pazar Oranı (Ipropertymanagement, 2019)

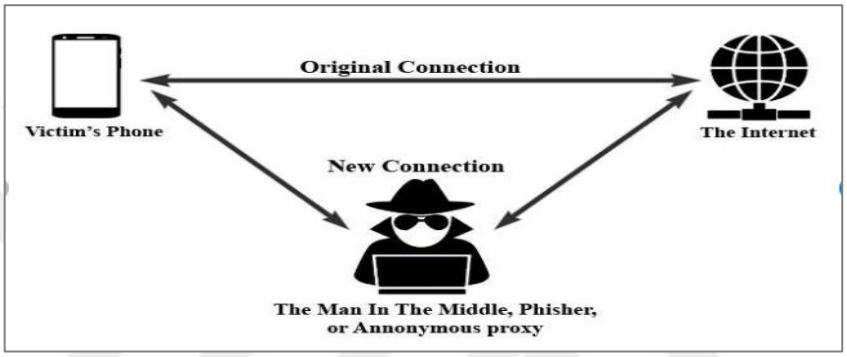
Şekil 25 üzerindeki IDC araştırmalarına göre, 2016 yılında Nesnelerin İnternet(IoT)'inin pazarlar arasında küresel harcamaları 737 milyar dolar olduğu bilinmektedir. 2020 yılına kadar bu sayının 1,29 trilyon dolara ulaşması ve %15,6'lık bir Bileşik Yıllık Büyüme Oranı (CAGR) elde etmesi beklenmektedir.

McKinsey, küresel olarak her saniyede bir 127 cihazın internete bağlı olduğunu belirtiyor. 2025 yılına kadar dünya çapında 75 milyardan fazla IoT cihazının olması bekleniyor. Çin, Kuzey Amerika ve Batı Avrupa, IoT'nin kurulu tabanının %67'sini oluşturuyor. IEEE 802.11 standart kuruluşu tarafından yönetilen kablosuz teknolojisi, kullanıcılara yüksek veri hızı kablosuz bağlantılarına yaygın, düşük maliyetli erişim sağlayan bu dönüşümde önemli bir rol oynamıştır.

Kablosuz Yerel Alan Ağların Dezavantajları

1999 yılından günümüze kadar gelen süreçte, kablosuz ağlar ile ilgili en büyük kuşku güvenliktir. Radyo frekansları (RF- Radio Frequency) üzerinden kablosuz olarak iletişim gerçekleşir. Bu iletişimin sağlandığı ortam hava ve boşluk olduğu için belirli metotlar ile bu havada süzülen paketler dinlenebilir ve çözümlenebilir. Her ne kadar geçmişten günümüze uzanan süreçte güvenlik algoritmaları geliştirilmiş olsa da, güvenlik algoritmalarını kırma yöntemleri ile istenmeyen kişiler kablosuz ağlara erişebilmektedir. Son kullanıcının insan olduğu yapılarda hata oranında artmaktadır. Özellikle kurumsal yapılarda kullanıcıların yetkilendirilmesi için kimlik doğrulama algoritmaları, şifre politikaları ve güvenli erişim eğitimleri iyi planlanması gereken başlıklardır.

Şekil 26'da bu saldırı yönteminin nasıl işlediği görülmektedir. Orijinal bağlantı kesilerek Ortadaki Adam (MITM) yöntemiyle paketler dinlenerek veriler çalınabilir. 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 (Mathy & Piessens, 2017).



Şekil 26 - Ortadaki Adam Saldırı Yöntemi (Ahvanooey, Li, Hou, Mazraeh, & Zhang, 2018)

Saldırgan orijinal bağlantının gerçekleştiği OSI katmanının 2. seviyesinde ARP protokolünden faydalanmaktadır. Bu yönteme ARP Spoofing denilmektedir. Saldırgan iki bağlantı arasına erişim sağlar. Sonrasında geçit (gateway) üzerinden orijinal bağlantı kendisi imiş gibi ağa yayın yapar. Kurban olan hedef MITM saldırısını gerçekleştiren kişinin saldırısını anlamaz ve ağ üzerindeki işlemlerine devam eder. Bu süre zarfında ağ üzerindeki tüm izleri toplanabilir ve saldırıyı gerçekleştiren kişi kurbanın internet üzerindeki mesajlarını manipüle edebilir. Ahvanooey ve arkadaşlarına (Ahvanooey, Li, Hou, Mazraeh, & Zhang, 2018) göre ASCII veya Unicode standardına dayanan TCP ve HTTP protokolünün özelliği nedeniyle çok etkilidir.

İnternet Protokolü Üzerinden Ses Haberleşmesi (VOIP)

İnternet Protokolü üzerinden ses haberleşmesi (VoIP) yapısı, dijitalleşme ve internetin gelişimi ile birlikte görüntülü görüşme, konferans, eğitim, sunum, anlık sohbet ve toplantı gibi birçok yeteneği sebebiyle PSTN ağların yerini çok hızlı bir şekilde

almışlardır. Çağımızda İnternet protokolü çoklu ortam iletişim sistemleri aslında içeriğinde birden fazla yapı ve protokolü barındırmaktadır. VoIP sistemlerinde ise TCP/IP katmanlarından uygulama katmanında SIP ve H.323 protokolü kullanılmaktadır. Bu iki protokolün kabul yılı 1996'dır. Özellikle SIP protokolü VoIP sistemlerinin standardı haline gelmiştir.

(Handley, Schulzrinne, Schooler, & Rosenberg, 1999).'ye göre Oturum başlatma protokolü bir uygulama katmanı protokolüdür. Sinyal göndererek bir veya daha fazla katılımcı ile oturumları oluşturmak değiştirme ve sonlandırmak için kullanılır. Bu oturumlar internet ağı üzerindeki oturumları ifade etmektedir. Oturumdaki kişiler, çok noktaya yayın veya tek noktaya yayın yaparak veya ikisinin karışımını kullanarak SIP protokolünden faydalanırlar

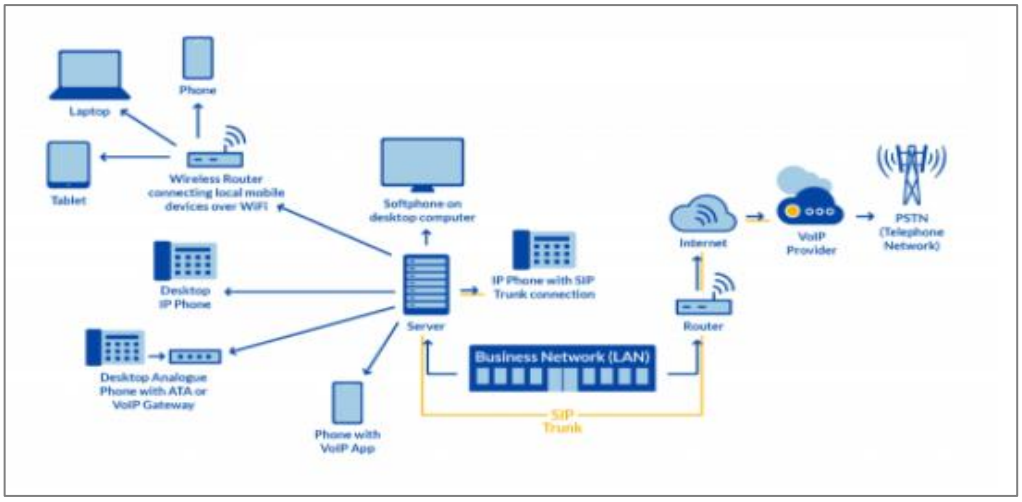
SIP çalışmalarında ilk hedef internet üzerinden çoklu yayın gerçekleştirmek idi. Bu kapsamda oluşturulan ilk taslaklar "draft-ietf-mmusic-scip-00" ve "draft-ietf-mmusic-sip-00" isimleriyle bilinmektedirler. İlk oluşturulan yapıda çağrı kurulumunu sağlayan tek bir talep tipi (request type) mevcut idi (Schulzrinne H. , 1996). Daha sonra Aralık 1996'da "draft-ietf-mmusic-sip-01" ve Ocak 1999'da "draft-ietf-mmusic-sip-12" taslakları oluşturuldu. Oluşturulan taslakta bugün SIP protokolünde kullanılan altı SIP talep tipi mevcuttu. Mart 1999'da ise bugünkü SIP standartlarının temeli olan RFC 2543 standartları yayınlandı (Handley, Schulzrinne, Schooler, & Rosenberg, 1999).

Dijitalleşmenin zirve yaptığı ve pandemi ile birlikte çevrimiçi görüşmelerin önem kazandığı günümüzde SIP protokolü VoIP etkileşiminin standart protokolü haline gelmiştir. SIP protokolünün zamanla gelişimi ile birlikte bağlanılan cihazın konumunu belirleme, çoklu ortam içeriklerinin parametre detaylarının belirlenmesi, kullanıcıların toplantı ve davetlere erişiminin belirli kurallara göre belirlenmesi, çağrı süreçlerinin yönetimini ve kurulumunu belirmemek gibi ana ölçütler üzerinde düzenleme sağlanabilmektedir. Çoklu ortam verilerinin transferi RTP (Gerçek Zamanlı İletim Protokolü – Real Time Transport Protocol) vasıtasıyla yapılmaktadır. İki uçbirim arasında oturum tanımı bilgisi ise SDP (Oturum Tanımlama Protokolü – Session

Description Protocol) aracılığıyla sağlanmaktadır. VoIP kullanım çeşitlerini maddeler halinde sıralarsak;

- Telefondan Telefona VoIP
- Telefondan Bilgisayara VoIP
- Bilgisayardan Bilgisayara VoIP
- Mobil VoIP
- Kablosuz VoIP

Küresel firmalar VoIP altyapısını birçok cihazda bütünleşmiş şekilde kullanmaktadır. Taşınabilir cihazların 2010 lu yıllardan sonra daha sık kullanılmasıyla ve kablosuz ağ seğmentinin genişlemesi VoIP yapısının büyümesinde en önemli etkenlerdendir. Şekil 27'de VoIP diyagramının küresel bir firma üzerinde çalışması gösterilmiştir. Bir kullanıcının telefonu arandığı zaman ipad, dizüstü, mobil telefon ve masaüstü VoIP telefonunun aynı anda çalması sağlanabilmektedir. Kullanıcı istediği cihazdan telefonu açabilmekte, yönlendirebilmekte, meşgule atabilmekte, konferansa dâhil edebilmekte ve sesli postaya yönlendirebilmektedir. Esneklik açısından VoIP'in avantajı burada devreye girmektedir.



Şekil 27 - Kurumsal Bir Yapıya Ait Örnek VoIP Şeması (Tech, 2020)

VoIP Mimarisinde Kullanılan Protokoller

İnternet Protokolü (IP)

Internet protokolü, verilerin paketler halinde ilgili ağ adreslerine yönlendirilmesini sağlayan protokoldür. Internet Protokolü OSI referans modelinin 3. Katmanı olan ağ (Network) katmanında çalışır. Network katmanı gelen verilerin doğru adreslere yönlendirilmesini sağlamaktadır. Bu yönlendirme sağlanır iken gelen veri paketinin içeriği önem arz etmez, sadece iletilecek hedef adrese temel alınarak veri iletilir. İletilecek yol belirlendikten sonra İnternet Protokolüne yönlendirilecek IP başlığı eklenir. İnternet Protokolünün bir paketinin içerisinde kaynak/hedef adresi, iletim sırasında hataları tespit edebilmek için sağlama alanı, atlama sınırı, uzunluk, hizmet kalitesi önceliklendirme ve yük dengesi alanları bulunmaktadır.

İletim Kontrol Protokolü (TCP)

TCP, uçtan uca bağlantılı güvenli bir protokoldür. TCP protokolü sayesinde verinin doğru, kayıpsız ve denetimli bir ortamda aktarımı sağlanmaktadır. Verinin denetimli ve kayıpsız bir ortamda iletilmesini sağlayan ise kabul (acknowledgement) mesajlarıdır. Alıcı tarafından ilgili veri paketi için bir onay mesajı gönderilmediği takdirde, o veri paketinin alıcıya iletilmediği belirlenmiş olur ve ilgili veri paketinin tekrar gönderilmesi sağlanır. Bu sayede ilgili veri paketlerinin alıcıya ulaşıp ulaşmadığı belirlenmektedir.

İki cihaz arasında TCP ile bağlantı kurulmak istenildiğinde bu kullanıcılar arasında mesaj değişimi gerçekleşir. Literatürde TCP üç yollu el sıkışması (handshake) olarak açıklanmaktadır. TCP çoklu ağ katmanına sahip hiyerarşilere uyumludur. TCP bu hiyerarşiler ve bilgisayar ağları arasındaki güvenli bağlantıyı sağlar. TCP prensip olarak kablolu, kablosuz paket anahtarlamalı veya devre anahtarlamalı ağlarla birlikte geniş bir yelpazede çalışabilmektedir.
TCP 3 yollu el sıkışma, bir TCP / IP ağında sunucu ile istemci arasında bağlantı sağlamak için kullanılan bir işlemdir.

- SYN: bir bağlantı başlatmak ve kurmak için kullanın
- ACK: diğer tarafın SYN'yi aldığını doğrulamaya yardımcı olur.

- SYN-ACK: yerel cihazdan gelen bir SYN mesajı ve önceki paketin ACK'sıdır.
- FIN: bir bağlantıyı sonlandırmak için kullanılır.

TCP el sıkışma süreci, bir istemcinin sunucuyla bir iletişim oturumu talep ederek konuşmayı başlatması gerekir. İlk adımda, istemci bir sunucu ile bağlantı kurar. Bu ikinci adımda, sunucu istemci isteğine SYN-ACK sinyal seti ile yanıt verir. Bu son adımda, müşteri sunucunun yanıtını kabul eder. TCP, iki ayrı uç nokta arasındaki bağlantıyı otomatik olarak sonlandırır.

Kullanıcı Veri Bloğu İletim Protokolü (UDP)

Kullanıcı Datagram Protokolü (UDP), bir önceki maddede bahsettiğimiz TCP Protokolü gibi OSI referans modeli üzerinde çalışmaktadır. OSI referans modelinin dördüncü katmanı olan taşıma katmanında rol almaktadır. Kullanıcı Datagram Protokolü ile ses, video ve görüntü gibi yüksek boyutlu verilerin anlık olarak en hızlı şekilde iletilmesi sağlanmaktadır. Bu protokol, İnternet Protokolünün (IP) temel protokollerindendir.

UDP ve TCP arasındaki en büyük fark güvenliktir. TCP de el sıkışma metodu var iken UDP de böyle bir mekanizma yoktur. Verilerin alıcıya ulaşıp ulaşmadığını kontrol etmez ve tekrar iletilmesi için bir işlem yapmaz. Gönderim / onay mekanizması çalışması için veriler hızlı bir şekilde ve yüksek boyutlu olarak iletilebilir. Veri gönderim hızı üst seviyeye çıkar iken, kontrol mekanizması olmadığı için güvenlik zafiyetlerinin ortaya çıkması muhtemeldir.

Gerçek Zamanlı İletim Protokolü (RTP)

(Schulzrinne, Casner, Frederick, & Jacobson, 1996).'e göre RTP protokolü, anlık iletilmesi gereken ses, video, görüntü, çevrimiçi toplantı ve telekonferans gibi anlık çoklu ortam verileri ağ üzerinden en hızlı şekilde iletebilmek için geliştirilmiş bir protokoldür. İlk olarak H. Schulzrinne ve arkadaşları tarafından RFC 1889 de ortaya çıkan bu protokol daha sonrasında RFC 3550 ile geliştirilmiştir. RTP yoğun olarak UDP protokolü üzerinden çalışmaktadır

Gerçek zamanlı iletim protokolü, UDP protokolüne sıra numarası ve zaman bilgisi bitlerinin eklenmesini sağlar. Kaynaktan çıkan pakete eklenen sıra numarası bilgisi, hedef adreste sıraya koyularak doğru bir şekilde alınır. Bu sayede paket kaybı yaşanıp yaşanmadığı tespit edilir. UDP protokolünün ağ üzerinde yaşadığı veri kayıplarının daha aza indirgemesi RTP protokolü sayesinde olur.

Gerçek Zamanlı Denetim İletim Protokolü (RTCP)

Gerçek zamanlı denetim iletim protokolü, belirli aralıklar ile RTP katmanına kontrol paketleri iletir. Bu paketler ile hizmet kalitesinin izlenmesi ve sabit hale gelmesi için senkronize olarak denetim sağlar. Bu gönderilen paketler RTP protokolü devre de iken kullanıcı bilgileri, kullanıcısı sayısı, oturuma katılan/ayrılan kullanıcıları denetler ve hizmet kalitesini arttırır. RTCP protokollüde UDP protokolünün maksimum kaliteli ve kesintisiz şekilde çalışmasını sağlamak için rol alır. RTP, RFC-3550'de tanımlanan RTP Kontrol Protokolü (RTCP) ile birlikte kullanılır.

RTCP, periyodik olarak kontrol paketlerinin bir RTP oturumunun tüm üyelerine iletir. Geri bildirim raporları alım kalitesi, paket kaybı, gecikme, titreme veya arızalarla ilgili kaynak alıcılarda problem olup olmadığını tespit eder. RTCP, akış kontrolünü ve çok noktaya yayın oturum gözetimini kolaylaştırır. Bu raporlar akışın ağ koşullarına ve oturum üyelerine uyarlanmasına yardımcı olur. Örnek olarak, oynatma hızı, bir alıcıdaki paket varış hızına eşit olmalıdır. Bir medya oynatıcı, gelen paketlerden daha fazla paket tüketir ve bu da oynatma kesintisine neden olur. Tam tersi, bir kullanıcının gönderdiği paket miktarından daha fazla gelen paket olduğunda tamponda yeterli alan yoksa bu aşırı yükleme paket kaybına neden olur. Bunda durumda alıcı, gönderene RTCP paketleri göndermek ister ve gönderenin iletim hızını oynatma hızı değerine düşürmelidir.

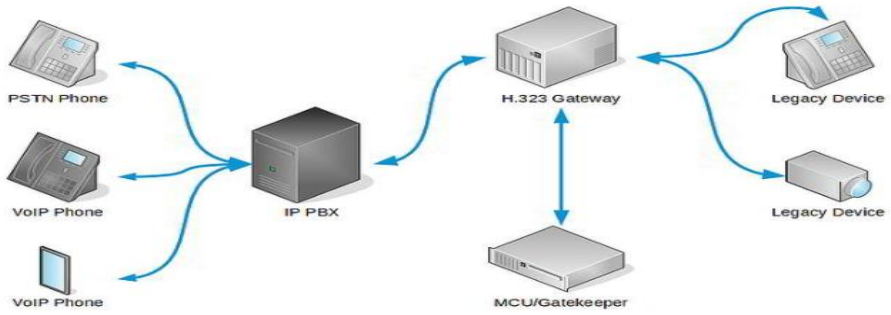
Sinyalleşme Protokolleri

İnternet Üzerinden Ses İletişimi (VoIP) teknolojisinin temelinde sinyalleşme için kullanılan protokoller; H.323, SIP, SCCP, MGCP olarak sıralanabilir. En çok kullanılan protokollerin başında gelmektedirler.

H.323 Protokolü

H.323 protokolü, tüm paket ağlarında görsel ve işitsel iletişim oturumlarının sağlanması için çalışan protokolleri açıklayan bir Uluslararası Telekomünikasyon Birliği (ITU-T) önerisidir. H.323 protokolü, paket tabanlı ağlar üzerinden multimedya iletişimi için donanım, bilgisayar ve hizmetler için standartlar sağlar ve gerçek zamanlı video, ses ve veri ayrıntıları için iletim protokollerini belirtir.

H.323, İnternet Protokolü üzerinden Ses Erişimi (VoIP), IP tabanlı video konferans ve İnternet telefonunda yaygın olarak kullanılmaktadır. Kullanıcılar İnternet üzerinden iletişim kurabilir ve H.323 standardıyla uyumlu çeşitli ürünlerden yararlanabilirler. H.323 standardı temel olarak İnternet Mühendisliği Görev Gücü'nün (IETF) Gerçek Zamanlı Kontrol Protokolüne (RTCP) ve Gerçek Zamanlı Protokol'e (RTP), veri iletişimi, çağrı sinyalleşmesi ve A/V için çeşitli diğer protokollerin kullanımıyla bağlıdır. Şekil 28'de H.323 protokolüne ait şema örneği verilmiştir ve detayları ile açıklanmıştır.



Şekil 28 - H.323 Protokolüne Ait Örnek Bir Şema (İletişim3xc, 2020)

Ekim 1996'da resmi olarak tanınan H.323 standardı, çeşitli ağlarda multimedya iletişim hizmetleri sağlayan bir ITU-T öneriler ailesi olan H.32x'in bir parçasıdır. Bu standartlar, H.323 uyumlu bileşenlerin aramaları nasıl oluşturduğunu, sıkıştırılmış video ve sesi nasıl paylaştığını, çok üniteli konferanslara nasıl katıldığını ve H.323 olmayan uç noktalar ile nasıl çalıştığını belirtir (ITU, 2001).

Terminaller: H.323 terminali, H.323 yığınını ve multimedya uygulamalarını çalıştıran bir bilgisayar veya gerçek zamanlı LAN ağı kullanan istemci uç noktaları olabilir.

Ağ geçitleri: Anlık iki farklı ağı bağlamak için kullanılan H.323 ağ geçidi, H.323 ve H.323 olmayan ağlar arasında iletişim sağlar. Bu farklı ağ bağlantısı, arama kurulumu ve yayınlanması için işlem sağlar. Ek olarak tasarlanan protokollerin çevrilmesi, çeşitli ağlar arasındaki ortam formatlarının dönüştürülmesi ve ağ geçidi ile birbirine bağlanan ağlar arasında ayrıntıların değiştirilmesi ile kurulur.

Ağ geçidi denetleyicileri: H.323'nin en kritik bileşeni olarak kabul edilen ağ geçidi denetleyicisi, arama kontrol hizmetleriyle kayıtlı H.323 uç noktaları sağlar. Kendi bölgesi içindeki her arama için çekirdek nokta görevi görür. H.323 ağlarında, ağ geçidi denetleyicileri isteğe bağlı olarak görev alır.

Çok Noktalı Kontrol Birimleri (MCU) : Üç veya daha fazla H.323 uç noktasını ifade eder. Terminal ile konferans görüşmesi için destek sağlar. Bir konferansa katılım sağlayan her istemci bir MCU bağlantısı kurar.

H.323 telekomünikasyon odaklı ses ve video iletimi gerçekleştirir. Görüntü ve sesi telekomünikasyon odaklı iletir. SIP protokolü ise internet taban odaklı çalışmaktadır. H.323 ve SIP protokolü arasında bu sebeple farklar bulunmaktadır. Tablo 5 üzerinde bu farklar detaylı olarak gösterilmiştir.

Tablo 5 - H323 ve SIP Niteliklerinin Karşılaştırması

	H.323 Standardı	*SIP*
Erişim Yöntemi	Telefon tabanlı	İnternet tabanlı
Düzenleyici Kurum	ITU	IETF
Uç nokta konumu	Takma adı kullanır	SIP URL'lerini kullanır.
Çağrı yönlendirme	Ağ geçidi bilgilerini sağlar.	Yönlendirme bilgilerini sağlar
Mesaj Formatı	İkili	ASCII
İnternet ile uyumluluk	Hayır	Evet
Mimari	Monolitik	Modüler
Anlık mesajlaşma	Sağlanmadı	Anlık mesajlaşma olanağı sağlar
Ölçeklenebilirlik	Sınırlı	Daha Gelişmiş
Esneklik	Yeterince esnek değil.	Oldukça esnek.
Birlikte çalışabilirlik	Geriye dönük uyumluluk.	Birlikte çalışabilirlik sağlamaz.
Uygulama kolaylığı	Dağıtımı karmaşıklaştırır.	Dağıtımı kolaylıkla gerçekleştirir.
Karmaşıklık	Karmaşık	Orta

Skinny Client Control Protocol- (SCCP)

SCCP(Basit Müşteri Denetimi Protokolü) protokolü, IP üzerinden gerçek zamanlı aramalar ve konferanslar için bir Cisco protokol standardıdır. SCCP protokolünü kullanarak skinny istemcisi ile iletişim kurmak için bir H.323 proxy kullanılabilir. H.225 ve H.245 sinyallemesi için bir proxy kullanılır. SCCP protokol mimarisiyle, H.323 işlem gücünün çoğu bir H.323 proxy de bulunur. Uç istasyonlar (IP telefonlar), daha az işlem yükü tüketen skinny istemcisini çalıştırır. İstemci, başka bir H.323 uyumlu uç istasyonla bir arama kurmak için bağlantı odaklı (TCP / IP tabanlı) iletişim kullanarak CallManager ile iletişim kurar. Cisco CallManager aramayı oluşturduktan sonra, iki H.323 uç istasyonu, ses iletimleri için bağlantısız (UDP / IP tabanlı) iletişimi kullanır.

Tablo 6'da gösterilen CallManager izi, Cisco CallManager'ın SCCP uç noktasına '2' gönderdiğini gösterir.

Tablo 6 - Cisco SCCP Call Manager İzi (Cisco, 2006)

03/01/2006 16: 43: 19.808 CCM | İstasyonD:
(0000044) **CallState callState = 2** lineInstance = 1
callReference = 16777296 | <CLID :: 496_Evoice-R5-CM1> <NID :: 172.18.110.96>
<CT :: 1,100,119,1.213986> <IP :: 14.48.40.131> <DEV :: SEP000A41F97CC4>

MGPC (Ortam Geçit Kontrol Protokolü) Protokolü

Medya Ağ Geçidi Kontrol Protokolü (MGCP), IP telefon ağ geçitlerini yönetmek için arama kontrol cihazları tarafından kullanılan RFC2705 de tanımlanan düz metin protokolüdür. Bir çağrı kontrol cihazının bir ağ geçidindeki belirli bir portun kontrolünü ele geçirmesine izin veren bir ana bağımlı protokolüdür. Bu, merkezi ağ geçidi yönetimi avantajına sahiptir ve büyük ölçüde ölçeklenebilir IP telefon çözümleri sağlar. Bu protokol ile ağ geçidindeki her bir portun durumunu bilir ve kontrol eder. Arama planının tam kontrolüne izin verir. Master – Slave mimarisinde çalışmaktadır.

SIP (Oturum Başlatma Protokolü) Protokolü

SIP (Session Initiation ProtocoL), Internet Protokolü üzerinden bir multimedya oturumu oluşturmak, değiştirmek ve sonlandırmak için kullanılan bir sinyal iletişim kuralıdır. Oturum, iki uç nokta arasındaki basit bir çağrıdan çağrı isteğidir. Bitiş noktası akıllı telefon, dizüstü bilgisayar veya Internet üzerinden multimedya içeriği alıp gönderebilen herhangi bir aygıt olabilir. SIP, IETF (Internet Engineering Task Force) standardı tarafından tanımlanan bir uygulama katmanı protokolüdür. RFC 3261'detanımlanır. SIP istemci-sunucu mimarisi ve HTTP URL ve URI kullanımı ve bir metin kodlama düzeni ve SMTP bir başlık tarzı temsil eder. SIP, IP ağı üzerinden ses ve video sunmak için kullanılan bir oturumu ve RTP'yi (Gerçek Zamanlı Taşıma Protokolü) tanımlayan SDP (Oturum Açıklama Protokolü) yardımıyla alır. SIP iki taraflı (unicast) veya çok taraflı (çok noktaya yayın) oturumlar için kullanılabilir. Diğer SIP uygulamaları

arasında dosya aktarımı, anlık mesajlaşma, video konferans ve çevrimiçi oyunlar ve yer alır. SIP response mesaj kodları 6 gruba ayrılmıştır. SIP mesaj kodları maddeler halinde belirtilmiştir.

Bilgilendirme (Information) Mesajları (100-199) : İstemci tarafından sunucuya gönderilen isteğin, sunucu tarafından alındığını ve işlemde olduğunu detaylandırmak amacıyla istemciye iletilen mesajdır. 182 Call Queued; 'Çağrı kuyruğa alındı' mesajı örnek olarak gösterilebilir.

Başarı (Successful) Mesajları (200-299) : İstemci tarafından gönderilen talebin başarılı bir şekilde kabul edildiğini belirtmek için gönderilen mesajdır. 202 Accepted; 'Kabul' cevabı örnek olarak gösterilebilir.

Yönlendirme (Redirection) Mesajları (300-399) : İşlemin tamamen devreye alınmadığını belirten mesajlardır. Ek işlem yapılması gerektiğini belirtir. 302 Moved Temporarily; 'Geçici olarak konum değişti' mesajı örnek olarak gösterilebilir.

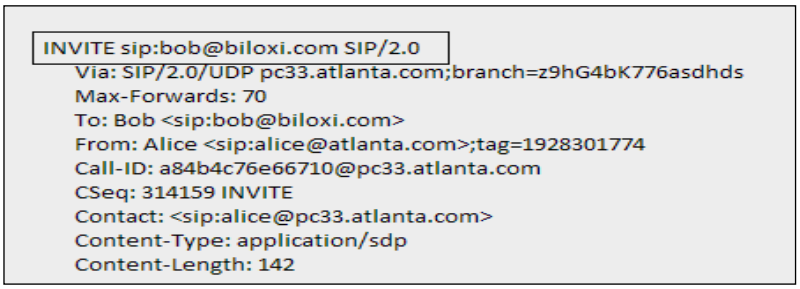
Kullanıcı (Client Error) Hata Mesajları (400-499) : Talep mesajındaki hatalar sebebiyle işlemin devreye alınamayacağını belirten mesaj türüdür. 403 Forbidden; Yasaklanmış ve 404 Not Found; 'Hedef bulunamadı' mesajları örnek olarak gösterilebilir.

Sunucu (Server Error) Hata Mesajları (500-599) : Kullanıcı tarafından gönderilen talebin alındığını ancak sunucudaki hata sebebiyle işlemin sağlanamayacağını belirten mesajlardır. 501 Not Implemented; 'Mesaja ait uygulama yok' ve 502 Bad Reques; 'Hatalı talep' örnek olarak gösterilebilir.

Genel Başarısızlık (Global Failure) Hata Mesajları (600-699) : İletilen talebin sistemdeki hiçbir sunucu tarafından gerçekleştirilemeyeceğini belirten mesaj türüdür. 603 Decline; 'Çağrı reddedildi' mesajı örnek olarak gösterilebilir.

Şekil 29'da SIP INVITE işleminin nasıl yapıldığını göstermektedir. INVITE mesajı arama yapan telefon mesajı veya sistem tarafından gönderilen ilk mesajdır. Çağrıyı

başlatmak için kullanılmaktadır. Invite sip, mesajı ile çağrı başlatıldıktan sonra kime (To:) ve kimden (From:) adımları sırasıyla devreye alınır.



Şekil 29 - INVITE Mesajının SIP Protokolü Üzerinden İletilmesi (IETF, 2002)

Tablo 7 üzerinde SIP istekleri detaylı bir şekilde iletilmiştir. Bu istekler SIP protokolünün temelini oluşturmaktadır. Oturum başlatma, güncelleme, kayıt olma, sonlandırma mesajlarının tümünü barındırmaktadır. SIP Mesaj yapısı ile alakalı bilgiler RFC 3261'de detaylı bir şekilde ifade edilmiştir. SIP Mesajlarında her bir isteğe karşılık, o mesaja bağlı olarak verilen son yanıt (response) süresine kadar süreci içeren mesajlaşmaya SIP İşlemi (SIP Transaction) denir.

Tablo 7 - SIP İsteği Mesaj Tablosu

SIP İSTEĞİ		
TR	*EN*	*AÇIKLAMA*
DAVET ET	INVITE	Kullanıcı veya hizmeti oturuma davet eder
ONAY	ACK	INVITE komutu tarafından başlatılan işlemi sonuçlandırır
HOŞÇAKAL	BYE	Çağrı, arayan veya aranan tarafından oturumu serbest bırakır
İPTAL ETMEK	CANCEL	Bekleyen istekleri iptal edin.
SEÇENEKLER	OPTIONS	Ağ sunucusu özelliklerini sorgulamanızı ve toplamanızı sağlar
KAYIT OL	REGISTER	Konum bilgilerini SIP sunucularına kaydetmek için kullanılır
GEÇİCİ ONAY	PRACK	ACK'ya benzer, ancak geçici bir onay sunar
ABONE OL	SUBSCRIBE	Cihaza bir olay bildirimine abone olur.
BİLDİR	NOTIFY	Bir olayın tüm abonelerini bilgilendirir.
YAYINLA	PUBLISH	Bir sunucuya bir olay yayınlar.
BİLGİ	INFO	Oturumun durumunu değiştirmeyen bir oturumun ortasında bilgi gönderir.
BAŞVUR	REFER	İstemciden bir SIP isteği, genellikle bir çağrı aktarımı yapmasını ister.
İLETİ	MESSAGE	SIP kullanarak anlık mesaj gönderir.
GÜNCELLEME	UPDATE	Diyalog durumunu değiştirmeden bir oturumun durumunu değiştirir.

VoIP Kullanmanın Avantajları

İnternet protokolü üzerinden ses haberleşmesi (VoIP) kullanmanın belli başlı avantajları aşağıda maddeler halinde sıralanmıştır.

- Ses kalitesi tüm mesafeler arasında kalitesini korur

- VoIP yapılarda, her ağ soketinde bir dizi sanal kullanıcı tanımlanabileceği için çok fazla esneklik sağlar.
- LDAP üzerinden isim ve tanımlara yönelik değişim rahatlıkla yapılabilir.
- Geleneksel kablolu yapılarla karşılaştırıldığında fazlasıyla kolaylık sağlamaktadır.
- VoIP kullanılan sistemler yazılıma dayalı olduğu için bakım, yönetim ve değişimi sağlamak çok daha kolaydır. Bu sebeple az envanter ile çok fazla cihaz üzerinden etkileşim sağlanabilmektedir. Bu sayede maliyeti düşürmektedir.
- VoIP kablosuz ağ üzerinden çalışabildiğinden hareket kabiliyeti yüksek şekilde kullanılabilir. Bir firmaya ait VoIP uygulaması çok farklı cihazlara (mobil telefon, dizüstü, ipad, masaüstü telefon vb.) kurularak internet erişiminin olduğu her noktada iletişim sağlanabilir.
- Mobil olarak Android ve IoS cihazlarda kolaylıkla kullanılabilir.
- VoIP sadece sesli görüşme bazında çalışmadığından görüntülü görüşme avantajı da sağlamaktadır. Pandemi ve dijitalleşmenin artması ile birlikte birçok firmanın bu yöndeki çalışmaları öncelik kazanmıştır. Microsoft Teams, Cisco Jabber, Google Meet, Adobe Connect, Zoom başta olmak üzere eğitim ve iş sürekliliği kullanımları çok fazla artmıştır.

VoIP Kullanmanın Dezavantajları

İnternet protokolü üzerinden ses haberleşmesi (VoIP) kullanmada karşımıza çıkan dezavantajlara ait belli başlı hususlar aşağıda sıralanmıştır.

- Bu çalışmanın yapıldığı sırada VoIP desteği olan IP telefon maliyeti çok yüksektir.
- PSTN telefonlar sadece santral bağımlı olduğundan elektrik kesintisinde çalışabilirler fakat IP telefonları elektrik ve internet bağlantısına bağımlıdırlar.
- Sesli ve özellikle görüntülü görüşmeler anlık erişimlerle sağlandığından, internet erişiminin hızına bağlı olarak iletişim kalitesinde düşüşler olabilmektedir. Bu görüntülü görüşmeye katılan katılımcı sayısına ve altyapıya bağlı olarak da değişiklik göstermektedir

Geleneksel ses erişiminde hedef ve kaynak arasında standart bir çizgide ilerleyen iletişim biçimi kullanılmaktadır. Birbirleri ile erişecek paketler belirli bir yol üzerinden ilerleyerek erişeceği hedefe varırlar. VoIP tabanlı erişimde ise hedef ve kaynak arasında internet protokolü devreye girer. Hedef ve kaynak arasında paketler internet protokolü sayesinde hızlı ve sıralı biçimde iletişim gerçekleştirilirler. Geleneksel yapıda paketler birbirlerini bekler iken, VoIP tabanlı yapıda paketler birbirini beklemeden hızlı biçimde hedef kaynak arasında yol alırlar.

BÖLÜM 3. BULGULAR VE YORUMLAR

Perakende Sektörüne Yönelik VoIP Tabanlı Uygulamaların İncelenmesi

Güçlü bir perakende organizasyonu işletmek, üst düzey teknolojik ürünlere sahip olmaktan daha fazlasını gerektirir. Maksimum verimliliğe ulaşmak için, kurum yapısının teknolojik gelişmeleri benimsemesi ve proaktif olması gerekir. Yeni teknolojiler ile daha fazla işlevsellik ve en iyi sonuca odaklanmak için daha fazla iletişim ve zaman gereklidir.

Perakende kurumları daha iyi iletişimden yararlanabilirler. Günümüz şartlarına göre yoğunluklu olarak kablosuz çözümlere etkili şekilde ulaşabilir ve VoIP tabanlı iletişimi sağlayabilirler. Kablosuz ağların yanı sıra PSTN bağlantılar ile bütünleşmiş her noktada üst düzey iletişim sağlanabilmektedir. IP tabanlı telefonlar ise birçok üreticiden temin edilebilmektedir. Başlıca Aastra, Cisco, Grandstream ve Snom geleneksel telefon modellerine uygun (ahizeli) cihazlar üretmektedirler. Ethernet kablosunun takılması yeterlidir, ekstra şebeke elektriğine ihtiyaç duyulmamaktadır. Tüm bu yapı ile bilgisayar ve mobil cihazlar bütünleşmiş olarak çalışmaktadır. Bu sebep ile hareket halinde iken iletişim kurabilmenin önem arz ettiği perakende sektöründe VoIP kilit noktada bulunmaktadır.

Üretkenliği arttırmada da VoIP tabanlı cihaz ve uygulamaların kullanılmasının rolü bulunmaktadır. Meşgul bir anda en uygun iş arkadaşına yönlendirme yaparak müşteri ile görüşme kesintiye uğramadan sağlanabilmektedir. Ekip üyeleri birbirleri arasında yönlendirme özelliklerini kullanarak kurum dışında olduklarında otomatik olarak sesli posta veya başka bir ekip arkadaşına yönlendirme sağlayabilirler. Kayıt tutma özelliği sayesinde lokasyon, dâhili ve kişi bazlı istenilen özellikte iz kaydı (log) tutabilmektedir.

Standart telefon faturaları, cep telefonu aramak ve kurum dışı diğer görüşmeler ek olarak maliyet demektir. VoIP ise gelişmiş altyapı ile otomatik çağrı dağılımı, herhangi bir noktaya en ucuz ve hızlı şekilde ulaşım, esnek bir çalışma ortamı sağlamak için en önemli araçtır. PBX yapıdaki telefon donanımı kullanma ihtiyacını ortadan kaldırır. Kurumların büyümesi ve geniş bir ağa yayılmasını en hızlı karşılayacak olan yapı bulut tabanlı VoIP'tir. Buna uygun olarak kullanılan Cisco Jabber, Teams gibi PSTN ile uyumlu çalışacak uygulamalar kullanılabilir. Dünya üzerinde kullanılan VoIP tabanlı başlıca 4 uygulama bir sonraki adımda karşılaştırılmıştır.

Cisco Jabber

Cisco Jabber, anında mesajlaşma, görüntülü/sesli iletişim, masaüstü paylaşımı, web konferansını mobil ve sabit cihazlar üzerinden tek noktada derleyerek toplu bir deneyime dönüştürür. Cisco Jabber tüm mobil cihazlar, Ios/Android altyapılı teknolojiler, Mac ve Windows cihazlarda kullanılabilir. Hangi cihazın erişilebilir olduğu gözetmeksizin, tek bir arama veya anlık ileti ile kullanıcıları arasında güvenli iletişimi sağlar.

Cisco Jabber çözümü, UC (Birleşik İletişim) client olarak sunulmaktadır. Cloud üzerinde çalışan hizmetleri kadar, bizzat şirket tarafından hazırlanmış uygulamalar da müşteri nezdinde kullanılabilmektedir. Kullanıcılar ofiste, yolda, toplu yerlerde ve evde kısacası erişim sağlanan her yerde anında mesajlaşma ses veya video araması başlatabilir. Bunun yanında belgeler üzerinde ortak çalışma ve sunumlar yapabilirler. Jabber tüm Cisco video çözümleriyle bir arada, sorunsuz çalışır. Jabber tüm platform sınırlarını aşar, şirket iletişimini kuvvetlendirir ve karar süreçlerini hızlandırır. Cisco Jabber uygulamasının en büyük artılarından biri çağrı yönetimi ve PSTN uyumluluğudur. Çağrı yönetiminin çok geniş çaplı olması (cevapsız çağrı yönlendirme, meşgul çağrı yönlendirme, çağrıyı kuyruğa alma, çağrıyı bekletme, aynı anda çağrı alma, çağrı kayıt, arayan kullanıcı kimliği, engelleme, konferans, rahatsız etmeyin modu, dizin listesi yapısı) büyük kurumsal yapılarda uyum sorununu ortadan kaldırmaktadır. Her kurumun kendi operasyon ve iş süreçlerine göre yapacağı tanımları Cisco Jabber uygulaması barındırmaktadır.

Adobe Connect

Bulunulan konumdan bağımsız olarak uzaktan eğitim ve sanal görüşmeler sağlayan bir platformdur. Mobil cihaz üzerinden erişim imkânı sağladığı için dünya üzerinde sanal sınıf uygulaması olarak birçok şirket ve eğitim kurumunun tercihi halindedir. Sanal toplantı ve uzaktan eğitim için gereken tüm temel yapıtaşlarını bünyesinde barındırmaktadır. Adobe Connect XML bir API'ye sahiptir, bu sebep ile kolay genişletilebilir. Adobe Connect uygulamasının özellikleri; özelleştirilebilir toplantı odaları, kişi başına birden fazla toplantı odası, toplantı sırasında ara oturumlar ana hizmetleri barındırır. Buna ek olarak VoIP, sesli ve görüntülü konferans, toplantı kaydı alma, ekran paylaşımı, beyaz tahta uygulaması, kullanıcı raporlama, kullanıcı yönetimi, merkezi içerik kitaplığı, iş birliği oluşturucu SDK, mobil uygulama (Android ve iOS) tabanlı destekleme ve HTML 5 istemcileri olarak sıralanmaktadır.

Google Meet

Google'ın gerçek zamanlı etkileşim sağlayan yeni görüntülü sohbet platformu Google Meet'tir. Uzaktan eğitim, kurum içi sanal görüşme, arkadaşlarınızla görüşme veya ailenizle çevrimiçi görüşme sağlayabilirsiniz. Google Meet, sadece G-Suite kullanan kullanıcılara açık iken yakın bir dönemde tüm standart Google aboneleri tarafından ücretsiz erişilebilir ve kullanılabilir hale gelmiştir. Google Meet, mobil olarak android ve iOS cihazlar üzerinde kullanılabilmektedir. Bu sayede esnek kullanım avantajı sunmaktadır. Google Meet üzerinden standart gmail hesabı ile toplantı ve görüşme sağlayabilirsiniz. Mobil olarak üst düzey ve kaliteli çalışmaktadır. Google Workspace Essentials, Google Workspace Enterprise olarak hesaplarınızı belirli bir ücret karşılığında yükselterek kullanılan özellikleri daha üst düzeye çıkartabilirsiniz. İlgili yükseltmeleri kurum ve kişi ihtiyacına göre ayarlayabilirsiniz. Ücretsiz sürümde 100 kişi ile sınırlı olan katılımcı sayısı ücretli versiyonda maximum 250 kişiye kadar çıkabilmektedir. İzleyici sayısı olarak ise 100.00 kişiyi bulabilmektedir. Google Meet'in başlıca özellikleri, sınırsız sayıda toplantı, canlı altyazı, mobil kullanım, görüntü ve ses önizileme ekranı, mesajlaşma, ekran paylaşımı, Google ve Microsoft Office uygulamaları ile uyum sağlama ve diğer birçok konferans uygulaması ile benzer özellikleri taşımaktadır.

Google Meet görüşmelerin güvenliğini sağlamak için 2 adımlı doğrulama seçeneği sunmaktadır, Görüşmeler kullanıcılar arasında şifreli olarak iletilmektedir. Google Meet, Datagram Taşıma Katmanı Güvenliği (DTLS) ve Güvenli Gerçek Zamanlı Aktarım Protokolü (SRTP) için IETF güvenlik standartlarına uyar. Güvenlik, gizlilik ve uygunluk denetimleri, her daim güncellenir ve bağımsız kuruluşlar tarafından kontrol edilir.

Microsoft Teams

Microsoft 365 ürün ailesinin bir parçası olarak microsfoft tarafından geliştirilen iletişim platformudur. Teams platformu Azure Active Directory'de depolanan kullanıcı kimliklerinden yararlanmaktadır. Teams çevrimdışı olunsa dahi belirli koşullarda çalışmaya devam etmektedir. Teams Skype çevrimiçi sürümün yerini alması beklenmektedir. 14 Mart 2017 Tarihinde ortaya çıkmıştır. Node.js ve JavaScpript platformlarının bir araya gelmesi ile oluşturulmuştur. Microsoft Teams içinde birçok özellik barındırmaktadır. Bunların başında sohbet ve paylaşılan dosyaların kalıcı olmasıdır. Kurumların belirli kurallarına göre süreler uzatılabilir ve kısaltılabilir. Kullanıcılar grup oluşturarak sohbet, video konferans ve toplantı özelliklerini kullanabilirler.

Bir URL gönderilerek veya kişiler seçilerek takımlar oluşturulabilir. Oluşturulan takımlar içerisinde yöneticilerin veya öğretmenlerin belirleyeceği kurallara uygun olarak görüşmelere sağlanabilir. Kullanıcılar sohbetlere GIF, resim ve metin ile cevap verebilmektedir. Etiketleme özelliği ile direk kişiye veya gruba mesaj gönderilebilmektedir.

Arama şu şekilde sağlanır: anlık ileti, IP üzerinden ses (VoIP) ve istemci yazılımı içinde video konferans. Teams ayrıca, kullanıcıların istemciden telefon numaralarını aramasına izin veren ortak anahtarlı telefon ağı (PSTN) konferansını da destekler. Microsoft Teams, öğretmenlerin Eğitim için Office 365 abonelerinin kullanabileceği ödevler sekmesini kullanarak Teams aracılığıyla teslim olan öğrenci ödevlerini dağıtmasına, geri bildirim sağlamasına ve not vermesine olanak tanır (Wikipedia, 2019).

Teams üzerinden toplantı daveti gönderilebilmesi için Outlook uygulamasında eklenti bulunmaktadır. Binlerce kullanıcıya bu eklenti üzerinden erişebilmeleri için toplantı daveti gönderilebilir. Mobil platformlar üzerinden kullanım sağlanabilmektedir. Teams office uygulamaları ile bütünleşmiş biçimde çalışmaktadır. Buna ek olarak One Drive üzerinde içeriklerin Teams üzerinde kullanılabilmesi için bir taslak sunmaktadır.

Microsoft Teams, Microsoft'a özgü bir dizi iletişim kuralını temel haline gelir. Video konferanslar, Skype tüketici sürümünden bilinen MNP24protokolü üzerinden gerçekleştirilir. Skype Kurumsal'dan MS-SIP protokolü artık Teams istemcilerini bağlamak için kullanılmaz. SIP ve H.323 tabanlı VoIP ve video konferans istemcilerinin Microsoft Teams sunucularına bağlanmak için özel ağ geçitlerine ihtiyacı vardır. Etkileşimli Bağlantı Kuruluşu (ICE) yardımıyla, eşler arası mümkün değilse, Ağ adresi çeviri yönlendiricilerinin ve kısıtlayıcı güvenlik duvarlarının arkasındaki istemciler de bağlanabilir (Wikipedia, 2019).

Tablo 8 - VoIP Tabanlı Uygulama Ana Özellik Karşılaştırılması

Ana Özellikleri	**Adobe Connect**	**Cisco Jabber**	**Google Meet**	**Microsoft Teams**
Çağrı Yönetimi	-	+	-	+
Mobil Erişim	+	+	+	+
Sunu Araçları	+	-	-	+
Ekran Paylaşımı	+	+	+	+
Sohbet	+	+	+	+
PSTN Bağlantı	-	+	-	+
Gizlilik	+	+	+	+
Deneme Sürümü	+	-	+	+
Konferans	+	+	+	+
Dosya Paylaşımı	+	-	+	+
Organizasyon Şeması	-	+	-	+

VoIP Tabanlı Çalışan Uygulamaların Karşılaştırılması

VoIP Tabanlı çalışan 4 uygulamanın karşılaştırılması üzerinde detaylandırılmıştır. Tablo 8 üzerindeki ana özellikler üzerinden değerlendirecek olur isek, Cisco Jabber uygulamasının Adobe Connect, Google Meet, Microsoft Teams uygulamalarına oranla üstünlüğü bulunmaktadır. Çalışmamızda Cisco Jabber uygulamasının seçilmesinin en uç nedeni PSTN bağlantı özelliğinin daha ön planda olmasıdır. PSTN bağlantı özelliği sayesinde mobile, masaüstü Bilgisayar, masaüstü telefon, dizüstü ve IPT cihazların birbiri ile erişimi sağlanabilmektedir.

Wireless IP telefonu, IP'nin paket anahtarlamalı bağlantılarını kullanarak sesli arama, sesli posta, görüntülü arama, video konferans, faks, mesajlaşma ve telefonla ilgili diğer hizmetleri etkinleştiren teknolojileri, ürünleri ve hizmetleri kapsar. Bu tür bilgiler geleneksel olarak, aynı zamanda düz eski telefon hizmeti olarak da bilinen kamusal anahtarlamalı telefon ağının (PSTN) ayrılmış devre anahtarlamalı bağlantıları üzerinden geçer. Bunun yerine, IP telefon teknolojisi aramaları, faksları ve metin mesajlarını bilgisayar ağ hatlarında dolaşan veri paketlerine dönüştürerek PSTN yapılardaki veri ücretlerini çok düşüğe çekmektedir.

Cisco Jabber, anında mesajlaşma, görüntülü/sesli iletişim, masaüstü paylaşımı, web konferansını mobil ve sabit cihazlar üzerinden tek noktada derleyerek toplu bir deneyime dönüştürür. Cisco Jabber tüm mobil cihazlar, Ios/Android altyapılı teknolojiler, mac ve windows cihazlarda kullanılabilir. Hangi cihazın erişilebilir olduğu gözetmeksizin, tek bir arama veya anlık ileti ile kullanıcıları arasında güvenli iletişimi sağlar (Techtarget, 2020).

Bu cihazların birbiri ile olan erişimleri en uygun fiyat ve verimde sağlayabilmek bugün birçok kurumsal yapının önceliğidir. Teknik ve Operasyonel olarak bu süreçleri gerçekleştirmek için en iyi analizler yapılmalıdır. Uzun vadede kurum ve kişiler için getirisi olacağı ön görülmektedir.

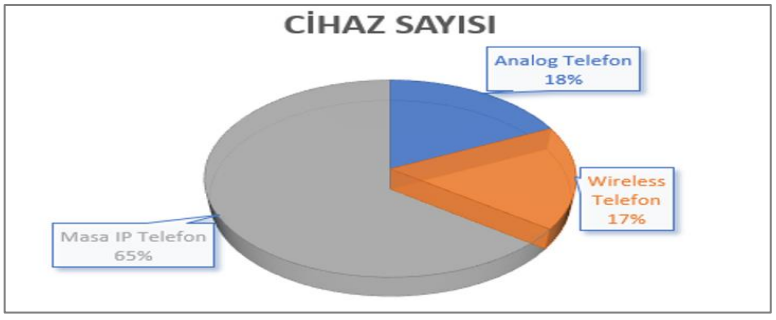
IPT (Internet Protokol Telefonu) Cihazların Mali Değerlendirilmesi

IP telefon, kurum merkezlerinde, şubelerde, uzaktan çalışan veya mobil olarak çalışan kullanıcılar için son derece güvenli bir iletişim hizmeti sunar. Güvenli bu hizmeti tutarlı ve basit bir biçimde genişletebilmek için altyapıya sahip çalışır. IP telefon, internet protokolü kullanarak network üzerinden ses iletişimi gerçekleştirir. Cisco IP telefon çözümleri; sabit ve mobil ağlardaki ses, video, veri ve mobil uygulamaları birleştiren Cisco Unified Communications'ın ayrılmaz bir parçasıdır.

Kullanıcıların herhangi bir ortam, cihaz veya işletim sistemini kullanarak herhangi bir çalışma alanında kolayca iletişim kurmasını sağlar. Ağı platform olarak kullanan Cisco IP telefon çözümleri, her boyuttaki kuruluşun, taşıma ve ara bağlantı için en üst düzey güvenlik, esneklik ve ölçeklenebilirlik elde etmesini sağlar (Cisco, 2014).

IPT cihazların döviz olarak satışının gerçekleştirilmesi mali yükü çok fazla arttırmaktadır. 2018 yılındaki döviz krizinden sonra bu cihazlara verilen desteklerin azalmasına ve bitmesine sebebiyet vermektedir. Kurumsal firmaların bu cihazların kendi ham maliyetleri dışında; saha desteği ve yan ürünlerinin (pil, güç kablosu, güç adaptör) de maliyetlerinin artması sebebiyle farklı çözüm arayışlarına sebebiyet vermiştir.

2018 Yılının ortalarında başlayan ve kayıt altına alınan bu sürecin çözümü için en doğru yolun BYOD (Kendi cihazını getir) hizmetinin kullanılması olacağına karar verilmiştir. Şekil 30 üzerinde cihazların envanter bazında dağılımı detaylı olarak verilmiştir. Masa IP telefonları %65 Envanter yoğunluğu yaşatır iken, analog telefon %18 ve wireless telefonda ise %17'lik envanter yoğunluğu gözlemlenmektedir.



Şekil 30 - VoIP Tabanlı Cihazların Envanter Bazında Dağılımı

BYOD yapısında öncelikli olarak hedeflenen yapılar Wireless Telefonlardır. Bu telefonların maliyetlerinin yüksekliği ve sahada kullanım gerekliliği fazladır. Ortalama bu cihazların sayısı 1800 adettir. 1800 cihazın mali olarak yük hesabı; cihaz maliyeti + servis maliyeti + yan ürün (pil, güç kablosu, güç adaptör) olarak USD bazında hesaplanmaktadır. Tablo 9 üzerinde Cihaz Modeli 8821-K9 Wireless Cisco Telefon baz alınmıştır. Full cihaz + Servis maliyeti yaklaşık $650' dolara tekabül etmektedir (RouterSwitch, 2021).

Tablo 9 - Cihaz Model, Cihaz Adet ve Cihaz Mali Değer Tablosu

Cihaz Modeli	Cihaz Adedi	Cihaz Maliyeti (Full Cihaz + Servis Maliyeti)
8821-K9	1800	$650,00

Bu mali yükün aşılması için dünyanın en büyük perakende şirketi Wallmart'ın kendi şirket uygulamalarına erişim için kullandığı BYOD (kendi cihazını getir) hizmeti üzerinden çalışmalar yapılmıştır.

VoIP Uygulaması

Cisco Jabber çözümü, UC (Birleşik İletişim) Client olarak sunulmaktadır. Cloud üzerinde çalışan hizmetleri kadar, bizzat şirket tarafından hazırlanmış uygulamalar da müşteri nezdinde kullanılabilmektedir. Kullanıcılar ofiste, yolda, cafede ve evde kısacası her yerde anında mesajlaşma ses veya video araması başlatabilir. Bunun yanında belgeler üzerinde ortak çalışma ve sunumlar yapabilirler. Jabber tüm Cisco video çözümleriyle bir arada, sorunsuz çalışır. Jabber tüm platform sınırlarını aşar, şirket iletişimini kuvvetlendirir ve karar süreçlerini hızlandırır. Cisco Jabber uygulamasının en büyük artılarından biri çağrı yönetimi ve PSTN uyumluluğudur. Çağrı yönetiminin çok geniş çaplı olması (Cevapsız çağrı yönlendirme, meşgul çağrı yönlendirme, çağrıyı kuyruğa alma, çağrıyı bekletme, aynı anda çağrı alma, çağrı kayıt, arayan kullanıcı kimliği, engelleme, konferans, rahatsız etmeyin modu, dizin listesi yapısı) büyük kurumsal yapılarda uyum sorununu ortadan kaldırmaktadır. Her kurumun kendi operasyon ve iş süreçlerine göre yapacağı tanımları Cisco Jabber uygulaması barındırmaktadır.

Uygulama Temini ve Kurulumu

Problem çözümümüzün ana uygulaması olan Cisco Jabber'ın kurulumu için kişi telefonundan Google Play veya Apple Store üzerinden uygulama indirme ekranına giriş sağlanması gerekmektedir. Uygulama indirme ekranında Cisco Jabber bulunduktan sonra Şekil 31 üzerinde gösterildiği gibi INSTALL butonu tıklanarak indirme işlemi başlatılır.



Şekil 31 - Cisco Jabber Android ve IOS Kurulumu

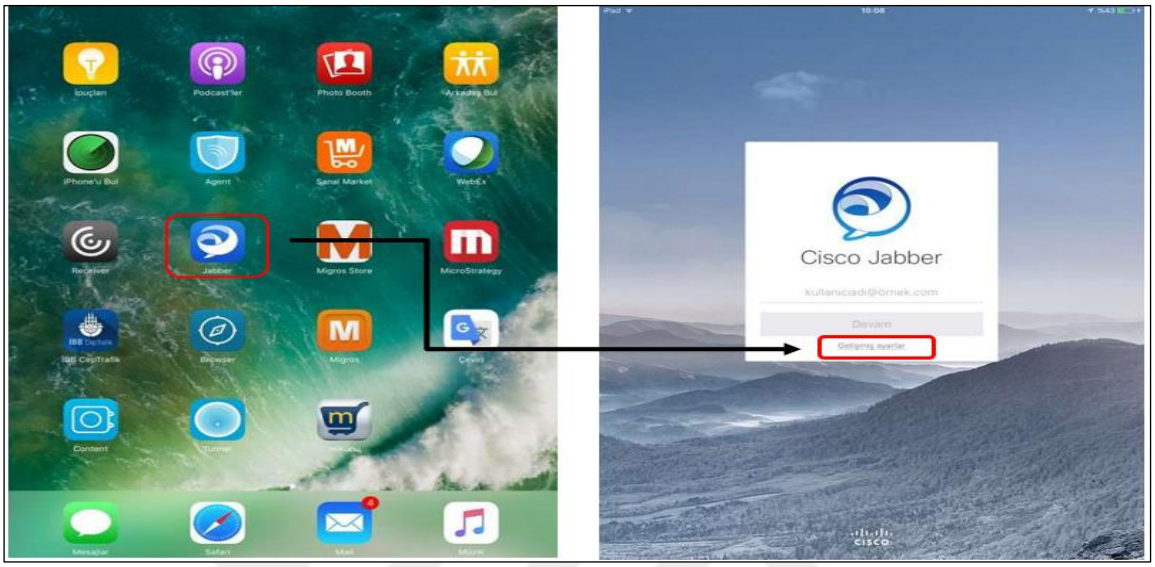
Telefon ana ekranına indirilen uygulama gerekli iç kaynak tanımlarının sağlanması için başlatılır.

a) Uygulama açılır ve ana ekran görünümüne geçilir.
b) Ana ekran görünümü üzerindeki en önemli ölçüt Gelişmiş Ayarlar'ın sağlanmasıdır.
c) Gelişmiş ayarlar alanına giriş yapılarak gerekli sunucu adresi girişi sağlanmalıdır.

Şekil 32 üzerinde gösterildiği gibi Gelişmiş Ayarlar içerisindeki ayarları detaylandıracak olur isek;

d) Gelişmiş Ayarlar'a giriş sağlanır.
e) Gelişmiş Ayarlar içerisinde Otomatik Olarak seçili olan buton pasife alınır.
f) Gelişmiş ayarlar içerisinde hesap türü olarak Cisco IM and Presence Seçilir.
g) Cisco IM and Presence seçildikten sonra Mavi Tik alacaktır.

h) Sunucu Bilgileri kısmına bağlantı sağlanacak ana sunucu bilgileri girilir. Sonraki adımda sağ üstten kaydet seçilerek bağlantı sağlanacak sunucu adresi ve tanımları gerçekleştirilmiş olur.



Şekil 32 - Uygulamanın Ana Ekran Görünümü

Gelişmiş ayarlar tanımı sağlanmadan kurumsal tanımlarda kullanım ve iletişim işlemi gerçekleştirilemez. Bu kısım güvenliği sağladığımız en önemli nokta olmaktadır. Tanımını gerçekleştirdiğimiz sunucu bilgileri tüm cihazlar ile bütünleşmiş çalışmamızı ve iletişimi en hızlı şekilde sağlamamızı gerçekleştirecektir. Güvenlik noktasında kurumsal olarak entegrasyonu sağlamamız her aşamada çok önemlidir.

Sunucu ve CM Admin Ayarların Yapılması

CM admin yapılandırmasının tüm detayları **Ek.1 Cm Admin Ayarları tablosunda** içerisinde verilmiştir. Sunucu gereksinimleri ise **Ek.2 Sunucu Gereksinimleri** Tablosu içerisinde verilmiştir.

Phone Type*: Bu alan zorunlu olarak seçilmektedir. En düşük modelden en yeni modele kadar seçimin yapıldığı alanı ifade eder. Tüm iç cihazlar ve diğer dışarıdan sağlanan cihazlar için tip seçimi yapılmaktadır. **Ek.3 İçerisinde** IOS, Android, Windows ve Mac için sistem ve donanım gereksinimleri tablolar halinde detaylı biçimde verilmiştir. Çalışmamız için seçilecek 2 model bilgisi;

- Cisco Dual Mode For Iphone
- Cisco Dual Mode For Android

Aygıt protokolü ise tüm cihazların birbiri ile bütünleşmiş ve hızlı şekilde VoIP altyapısı ile bağlantı kurabilmesi için SIP olarak ayarlanmaktadır. SIP profilleri, kayıt ve canlı tutma zamanlayıcıları, medya bağlantı noktaları gibi telefon için özel SIP bilgileri sağlar ve denetimi bozmaz. Tipik olarak mobil cihazlar için standart SIP profili bir TCT cihazında kullanılacaktır.

Aygıt Ayarları

Bu alan içerisinde device name ayarları birincil olarak yapılmaktadır. Device name alanının anlaşılır olarak işlenmesi; veri güvenliği, iş takibi, tanımlama kuralları ve diğer sabit yapıların birbirleri ile doğru çalışmasını sağlayacaktır. Bu alan içerisinde device name alanı girilir iken belirli kurallara göre giriş sağlanmaktadır.

Cihaz adı alanındaki cihaz doğruluğu kısmında yeşil tik olması gereklidir. Bu alan cihazın çalışabilir ve tanımlanabilir olduğunu göstermektedir. Cihaz adı girilir iken ilk başına belirli tanımlama isimlerinin girilmesi gereklidir. Tanımlama isimlerinin yoğun olarak kullanılanları Tablo 10'da verilmiştir. Örnek olarak TCTEGUNES kullanılabilir.

Tablo 10 - CUCM Cihaz Kurulumu İçin Gerekli Alan Adları

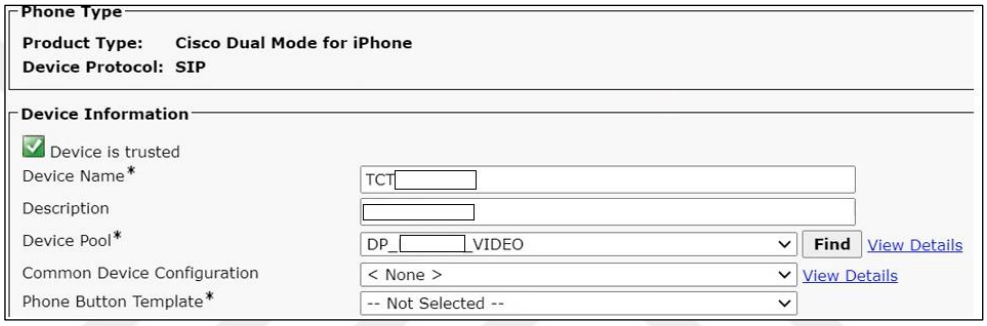
Device Name*	TCT = iphone
	BOT = android
	TAB = tablet
	CSF = windows

Device Pool alanı da zorunlu doldurulması gereken alanlardandır. Cihazın atanmasını istediğimiz cihaz kural alanını seçmemizi sağlar. Aygıt havuzu, aygıtlar için bölge, tarih, saat grubu ve yazılım şablonu gibi ortak özellik kümelerini tanımlar. Bu alan varsayılan olarak yapılandırılamaz. Seçim yapılması gerekli olan alanlardandır. Description alanı ise kullanıcı ismi yazılabilir

.

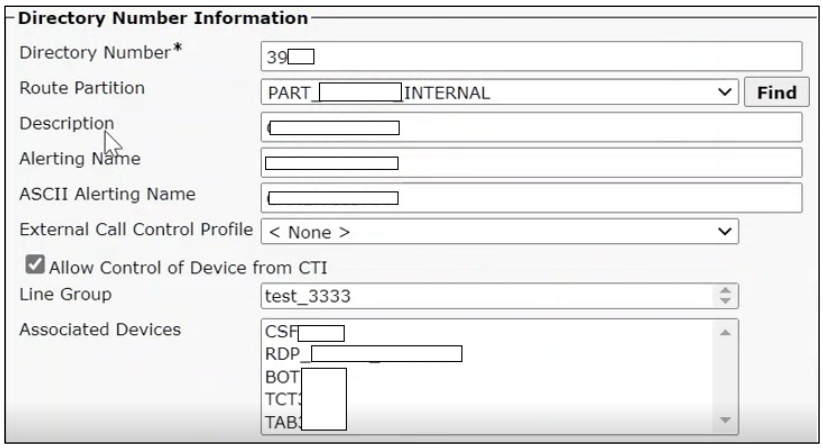
Phone Button Template alanı da zorunlu olarak seçilmelidir. Varsayılan olarak yapılandırılmaz. Şekil 33 üzerinde istediğiniz telefon düğmesinin işlevini seçilir. Programlanabilir satır anahtarı özelliği, satır düğmelerine atanabilecek birden çok özellik sağlar; örneğin, MCID, DND, Call Park, Call Pickup ve daha birçok özellik eklenebilir.

Şablonların oluşturulması ve kullanımı, çok sayıda telefona ortak bir düğme yapılandırması atamanın hızlı bir yolunu sağlar. Örneğin, kurumsal yapıdaki kullanıcılar videolu görüşme özelliğini kullanmıyorsa, bu düğmeyi arama yönlendirme gibi farklı bir özelliği yeniden atayan bir şablon oluşturulabilir.



Şekil 33 - CUCM Aygıt Bilgileri Ayar Ekranı

Directory Number* : Tanımlanacak cihazın dâhili numara bilgilerinin girildiği alandır. Zorunlu olarak seçilmelidir. Yetkilendirme sunucusundaki yapılandırma dosyalarını günceller iken bu alan seçilir. İlişkilendirme Bilgileri alanında, [1] Satırı - Yeni bir DN ekle bağlantısı ile erişim sağlanır. Dizin numarası bilgileri alanında > Dizin numarası detayı girilerek işlem sağlanmaktadır. Şekil 34 üzerinde directory number alanındaki tanımlar kurumsal yapıya göre işlenmiştir. Dizin numarası alanı kullanıcının kısa kodu olarak girilmektedir. Bu kod kullanıcının bulunduğu lokasyon, bölge ve unvan bilgilerine göre yapılandırılabilir. Bu alan girildikten sonra, diğer tüm alanlar bağlantılı olarak eşleşme sağlamaktadır. Associated Device alanı kişiye tanımlı olan tüm cihaz bilgilerini göstermektedir.



Şekil 34 - Dizin Numarası Tanımları ve Eşleştirmeleri

Rota Bölümleri, çağrı yönlendirme hedeflerine atanır. Sesli posta bağlantı noktaları, dizin numaraları (DN), yönlendirme modelleri , çeviri modelleri , birebir konferans numaraları olmak üzere arama yönlendirme tablosunun herhangi bir girişi bir bölüme atanabilir.

Tablo 11 üzerinde rota bölümlerine bir örnek verilmiştir. Cihazlar, Base_CSS gibi bir arama arama alanına otomatik olarak kaydolur. Bu, tüm cihazların hem ağ içi hem de ağ dışı acil numaraları aramasına olanak tanır. LocalPSTN_CSS, UlusalPSTN_CSS, Uluslararası PSTN_CSS olarak yapılan tanımlar ise arama alanlarının genişliğine göre isimlendirilmiştir. Bu rota düzenleri büyük yapılar içerisinde uyumlu olmayı ve kolay bir şekilde kullanıcı tanımlarını gerçekleştirmek için yapılmaktadır.

Çalışmamızda rota bölümlerinin ayarlanması şirket içi ve yurt içi olarak ayarlanmıştır. Bu tanımlar danışma ve müdürlere ait telefonlara verilir iken, kasa ve şarküteri alanlarında ise sadece şirket içi aramalar yapılacak şekilde dizayn edilmiştir. Şirket içi aramalar ücretsiz olarak gerçekleştirilmektedir. Aylık rutinlerde kontrol edilen faturalandırmada ise yurt içi aramaları çok fazla olan kullanıcılar için gerekli aksiyonlar alınmaktadır.

Tablo 11 - Rota Bölüm Alanlarına Ait Bir Örnek (Cisco, 2021)

Arama Alanı	*Rota Bölümü 1*	*Rota Bölümü 2*	*Rota Bölümü 3*	*Yetenekler*
Base_CSS	Base_PT	-	-	Acil Durum
				İnternette
LocalPSTN_CSS	PSTN_Local_PT	-	-	Acil Durum
				İnternette
				Yerel
UlusalPSTN_CSS	PSTN_Local_PT	PSTN_National_PT	-	Acil Durum
				İnternette
				Yerel
				Ulusal
Uluslararası PSTN_CSS	PSTN_Local_PT	PSTN_National_PT	PSTN_Intl_PT	Acil Durum
				İnternette
				Yerel
				Ulusal
				Uluslararası

Kullanıcı Tanımları

Son adım işlemlerinde ise cihazların eşleştirilmesi ve kişiye atanması sağlanmaktadır. Servis ayarları bölümünde, burada uç kullanıcıya bunları kullanmak istediğiniz hizmetleri atayabilirsiniz. Bir kullanıcının Android ve IOS için Jabber'da oturum açabilmesini sağlamak için, hizmet adının yanındaki onay kutusunu işaretleyerek Home Cluster hizmetini etkileştiririz.

Son kullanıcıların anlık mesajlaşma yapısını kullanabilmesi için, Birleşik Anlık İleti ve Durum için Etkinleştir etiketli alanın yanındaki onay kutusunun etkileştirmek gerekir. Daha sonra UC Service Profile menüsünden bir hizmet profili seçerek bir hizmet profili ataması gerçekleştirilir. Hizmet profili, Jabber istemcisine CUCM UC hizmet yapılandırması sağlamak için kullanılır.

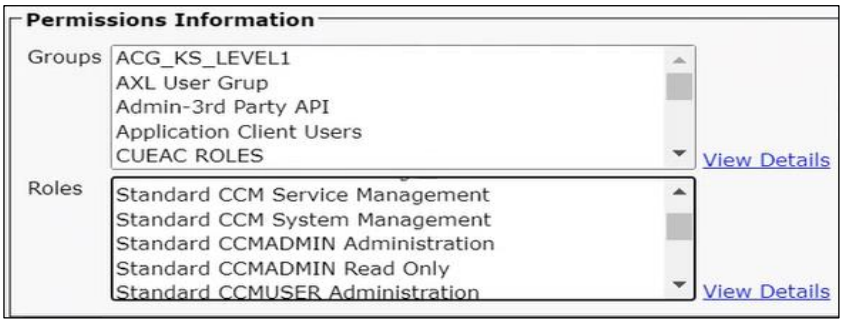
Cihaz eşleştirmesi için Aygıt Bilgileri bölümüne giriş sağlanır. Burada CUCM son kullanıcılar tarafından kontrol edilen tüm cihaz bilgileri görüntülenebilir ve yönetilebilir. Şekil 35 üzerinde çalışmamızın ana hedef noktaları olan Android(BOT) ve

IOS(TCT) cihazlar için olan eşleştirmeleri yapıldığı görülmektedir. Bu eşleştirmeler ile tüm cihazların birbiri ile ilişkilendirilmesi sağlanmaktadır. CUCM, Jabber oturumu açıldığında bu cihaz listesini Android ve IOS için Jabber'a sağlar.



Şekil 35 - CUCM Cihaz Eşleştirme Alanı

İzin bilgileri alanında ise Iphone ve Android için gerekli olan izinler atanacaktır. İzin ataması sağlamak için Erişim Kontrol Grubuna ekle alanında tüm detaylandırmalar sağlanmaktadır. Eklemek istediğimiz erişim kontrol grubu seçilir ve erişim kontrol grupları eklenir. Şekil 36 üzerinde tanımlanan grup ve rollerin belirli bir listesi sıralanmıştır. Kişinin profiline göre bu liste üzerinde güncelleme sağlanabilmektedir.



Şekil 36 - İzin Bilgileri Gruplar ve Roller Alanı

Servis Keşfi

Cisco Jabber istemcisinin oturum açabilmesi için öncelikle kimlik doğrulama ve yapılandırma alımı için kullanacağı hizmetlerden (CUCM, IM&P veya Expressway) haberdar olması gerekir. Cisco, kesintisiz bir kullanıcı deneyimi ve yönetim kolaylığı sağladığından, Etki Alanı Adı Sistemi (DNS) Hizmet Konumu (SRV) kayıtları kullanılarak otomatik hizmet keşfinin yapılandırılmasını önerir (CiscoJabber, 2020).

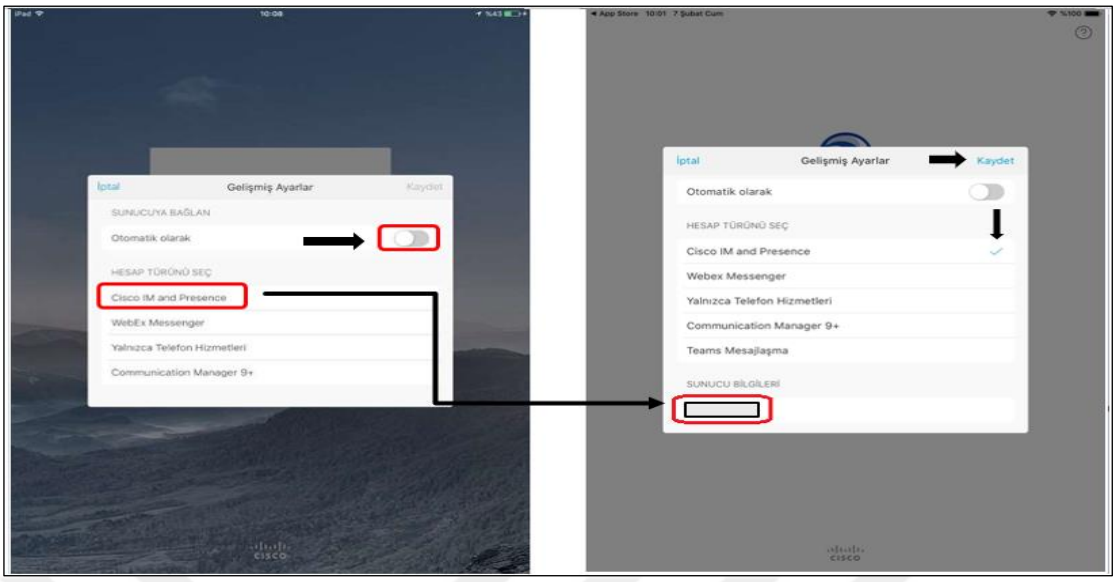
Microsoft DNS Yöneticisi'ne DNS SRV kaydı eklemek için etki erişim sağlanır. TCP klasörüne sağ tıklanır ve Diğer Yeni Kayıtlar seçeneği seçilir. Kaynak kayıt türü alanı altından Hizmet Konumu (SRV) alanı içerisinde kayıt oluşturulur. Jabber' ın ilk UDS ana küme araması için kullanılacak CUCM sunucularının her biri için bir SRV kaydı yapılandırılması sağlanır. Şekil 37 üzerinde _cisco-uds SRV kaydı için yapılandırma örneği verilmiştir. Bu örnek üzerinde _Cisco-uds kaydı bir CUCM kümesi içindeki üç CUCM düğümüne çözümlenmektedir.

```
_cisco-uds._tcp.testlab.com SRV hizmet konumu:
          öncelik = 6
          ağırlık = 30
          bağlantı noktası = 8443
          svr ana bilgisayar adı = cucm3.testlab.com
_cisco-uds._tcp.testlab.com SRV hizmet konumu:
          öncelik = 2
          ağırlık = 20
          bağlantı noktası = 8443
          svr ana bilgisayar adı = cucm2.testlab.com
_cisco-uds._tcp.testlab.com SRV hizmet konumu:
          öncelik = 1
          ağırlık = 5
          bağlantı noktası = 8443
          svr ana bilgisayar adı = cucm1.testlab.com
```

Şekil 37 - Hizmet Konumu (SRV) yapılandırma örneği

Sunucu Tanılama Hatası

Sunucu hatası alınması durumunda ilk kontrol edilecek nokta kurumsal Wi-Fi ağına bağlılığıdır. 3G ve 4G cihaz üzerinden yapılacak tanımlarda ilk eşleşme sağlanamamaktadır. İlk kurulum aşamasında cihazın kurumsal ağa bağlı olması gerekmektedir. Kurumsal ağa bağlanılmadan gerçekleştirilmeye çalışılan tanımlamalarda tanılama vermektedir. Sunucu adresine erişemediği için kurumsal Wi-Fi ağına bağlı olması gerektiği belirtilmiştir. Kurumsal ağa bağlı olduğu durumlarda bu hata alındığında ise tanımların kontrolü gereklidir. Şekil 38'de Gelişmiş ayarlar alanı içerisinden sunucu ayarlarının sağlanması belirtilmiştir.



Şekil 38 - Gelişmiş Ayarlar ve Sunucu Ayarlarının Sağlanması

Bir sonraki adımda uygulamaya giriş için kurumsal mail adresini girmemiz gerekmektedir. Buradaki dikkat edilmesi gereken nokta Cisco IM and Presence alanında giriş sağlanmasıdır. Bu alan tanımlarımızın eşleşeceği alanı ifade etmektedir. Giriş aşamaları Şekil 39 üzerinde belirtilmiştir.

i) Gelişmiş ayarlar aşamasını tamamladıktan sonra karşımıza giriş ekranı açılmaktadır.

j) Giriş ekranında Cisco IM and Presence alanının olması en önemli noktadır.

k) User alanı kullanıcı@şirket.com olarak gözükecektir. Örnek olarak bu alan için emregunes@jabber.xyzfirması.com.tr girilmelidir. @jabber kısmı Telefon ve Dizin hizmetlerinin sabit şekilde çalışması için gerekli tanımın tanımlanması için girilmektedir.

l) Bir sonraki adımda şifre bilgisi girilir, bu kısma LDAP üzerinde tanımlı olan şifremizi girmemiz gerekmektedir. LDAP üzerinden giriş sağlamamız sayesinde güvenlik politikası bir adım daha ileri taşınmış olacaktır.



Şekil 39 - User Ve Şifrenin Uygulama Tanım Ayarlarına Göre Girilmesi

Kurumsal yapılarda uygulama veya uygulama gruplarında çeşitli sertifikasyonlar bulunmaktadır. Bu sertifikasyonlar güvenlik, erişim ve kişi bilgilerini barındırabilir.

m) Oturum açtıktan sonra bize atanan sertifika veya güncellemeleri onaylamak gereklidir.

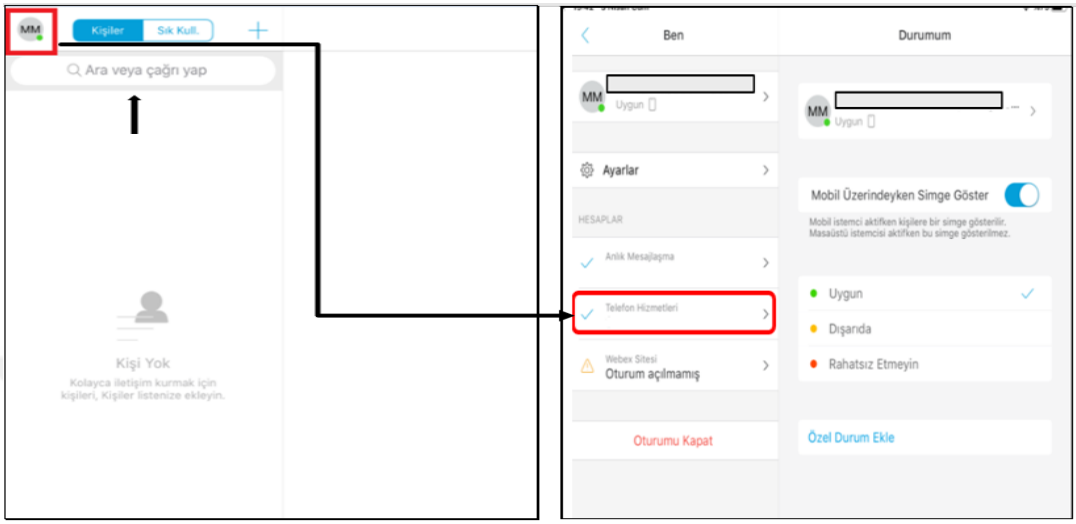
n) Onay işleminden sonra ana ekran hattı karşımıza çıkacaktır. Şekil x.x. üzerinde gösterildiği şekilde sağ üstten uygulamanın Telefon ve Anlık Mesajlaşma hizmet tanımlarının doğru ve çalışır olduğu kontrol edilir.

o) Bu kontroller mavi tik'e sahip olduğuna bakılarak anlaşılır. Şekil 40'da detaylı olarak gösterilmiştir.

p) Tüm kurulumlar tamamlandıktan sonra Kişi arama veya Çağrı yapma ekranından VoIP tabanlı olarak iletişim kurulabilmektedir. Bu alandan kişi tanım kurallarına göre şirket içi, yurt içi ve yurt dışı olarak geniş kapsama giden aramalara göre yetkilendirmeler sağlanabilmektedir.

Güvenliğin üst düzeyde olduğu ve kurumsal içyapıda gerçekleştirilen bu eylem iletişim kalitesini üst düzeyde tutmaktadır. Anlık mesajlaşma özelliği de artı bir değer olarak gözükmektedir. Perakendenin 7/24 aktif olduğu ülkemizde iletişimin de kesintisiz sağlanması gereklidir. Özellikle yoğun dönemlerde bayram, yılbaşı, özel ve dini günler gibi zamanlarda personellerin birbiri ile kesintisiz ve en hızlı şekilde

iletişimi diğer tüm operasyonları (pazarlama, satış, bilgi teknolojileri, saha çalışanları gibi) etkilemektedir. VoIP tabanlı iletişim kesintisiz ve maliyetsiz iletişimin temelidir. Ayrıca raporlanabilir olması da ayrıca bir artı değeridir.



Şekil 40 - Telefon ve Anlık Mesajlaşma Hizmetlerinin Doğrulanması

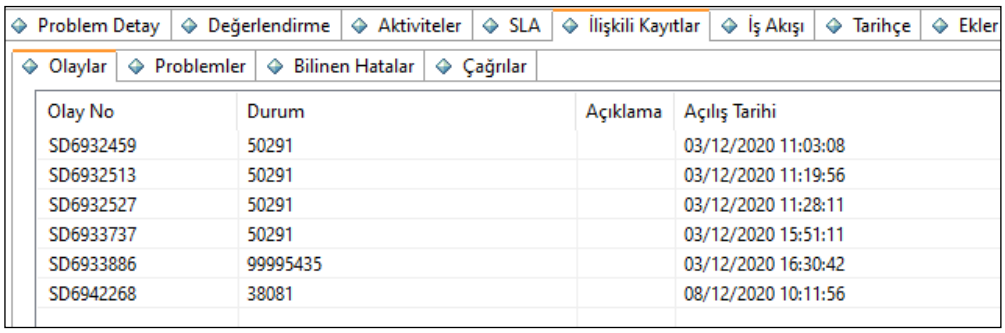
Problemi Tespit Kaydetme ve Sınıflandırma, Problemi Önceliklendirme ve Planlama, Problemi İnceleme ve Teşhis aşamalarından sonra çözümün uygulanacağı ve canlı bir yapıya dönüşeceği Problem Çözüm aşamasın da gerçekleştirilir. Bu aşamada teşhis, inceleme ve gerekli materyaller sağlandıktan sonra canlıya alma aşamasıdır. Çözüm aşamasına ulaşmak için ilk 3 maddede en ince ayrıntıya kadar incelemeler sağlanmıştır. Problem çözüm aşamasında BYOD (kendi cihazını getir) hizmetinin kullanımı ve gerekli tanımları uygulanmıştır. Güvenli ağ protokollerinin uygulamasından başlayarak örnek uygulama tanımlarının en son aşamasına kadar tüm tanımlar ayrıntılı olarak gösterilmiştir. Kurumsal protokoller ve KVKK süreçleri göz önüne alınarak tanım ve kullanım gerçekleştirilmiştir. Sırası ile uygulamanın kurumsal VoIP mimarisi tanımları, kurumsal sertifikaya uygun güvenli ağ tanımları, VoIP sertifikalarının cihaz üzerinde onaylanması ve LDAP eşleştirmelerinin sağlanması gerçekleştirilmiştir. Erişimlerin takip edilebilir ve kurum içinde erişilebilir olması en önemli ölçüttür.

Kapama ve İzleme

I. Problemi Tespit Kaydetme ve Sınıflandırma
II. Problemi Önceliklendirme ve Planlama
III. Problemi İnceleme ve Teşhis

Adımlarından sonra son aşama olan Problemi Kapama ve İzleme adımı gelmektedir. Bu adımda 3. Madde olan Problemi İnceleme ve Teşhis sağlandıktan sonra gerekli altyapı ve materyaller oluşturulmuştur. Kazançları başlık olarak sıralayacak olur isek; Erişilebilirliği arttırmak, maliyetleri düşürmek, iş gücünü arttırmak, kaynakların verimli kullanılmasını sağlamak, ölçüle bilirliği artırmak, kapasiteyi ayarlamak. BT ve yönetsel kaliteyi üst düzeyde tutmak olarak değerlendirebiliriz. Problemin kapanması ve izlenmesi tüm süreçlerin bir arada olumlu bir yol çizmesi ile gerçekleşmektedir.

Şekil 41 üzerinde bu olumlu sürecin analizi test mağazalarından sağlanan çok düşük düzeydeki geri dönüşler ile gözlemlenmiştir. 70 mağaza, 2 dağıtım merkezi ve BT birimi üzerinde gerçekleştirilen yayılımda problem geri dönüşü 6 adet olarak gerçekleştirilmiştir. IPT (Internet Protokol Telefonu) cihazların mali değerlendirilmesi başlığında vurguladığımız 1800 cihaz üzerinden orantılandığımızda 25,7 kat daha fazla kullanıcının sürece dâhil edilmesi sağlanacaktır.



Olay No	Durum	Açıklama	Açılış Tarihi
SD6932459	50291		03/12/2020 11:03:08
SD6932513	50291		03/12/2020 11:19:56
SD6932527	50291		03/12/2020 11:28:11
SD6933737	50291		03/12/2020 15:51:11
SD6933886	99995435		03/12/2020 16:30:42
SD6942268	38081		08/12/2020 10:11:56

Şekil 41 - Test Mağazaları Problem Geri Dönüş Kayıtları

BÖLÜM 4. SONUÇ

Özet

Bu tezin 1. bölümünde tez hakkında bilgiler verilmiş ve amacı açıklanmıştır. 2. bölümde kablolu ağ teknolojileri, Kablosuz ağ teknolojileri standartlarına, büyüklüklerine, avantajlarına ve dezavantajlarına göre incelenmiştir ve literatürdeki araştırmaların özetleri verilmiştir. 3. bölümde ise kablosuz ağ güvenliği ve kimlik doğrulama yöntemlerine yer verilmiştir. CIA ve AAA metotları incelenmiştir. Açık sistem ve 802.1x kimlik doğrulama yöntemlerine yer verilmiştir. 4. bölümde ise internet protokolü üzerinden ses haberleşmesine ait protokoller incelenmiş ve dezavantajları/avantajlarına yer verilmiştir. Bir uygulama üzerinden çözüm önerisi gerçekleştirilmiştir ve orantısal olarak sonuçları verilmiştir. 5. bölümde ise çalışmaya ait nihai sonuç ifade edilerek daha sonraki çalışmalar için de değerlendirmeler verilmiştir

Yargı

Tez çalışmamızda kablolu ağ yapılarından kablosuz ağ yapılarına evirilen bir düzene gidildiği görülmektedir. Kablosuz ağ yapılarının hayatımızın her anında olması iletişimimizi kuvvetlendiren yegâne nedendir. Bu yapıların kendi kendine yönetebilmesi sayesinde insan gücünün daha az ön planda olduğu dijital dünyada, IP tabanlı erişim önem kazanmıştır. IP tabanlı erişimin önem kazanması ile geliştirilen teknolojiler sayesinde maliyetler düşürülmüş ve dijital iletişim hegemonyası artmıştır. İnternet Protokolü Üzerinden Ses (VoIP) tabanlı iletişim kablolu ve kablosuz ağlar üzerinden sağlanabilecek en ucuz ve hızlı iletişim olmuştur. Ağlar üzerinden IP tabanlı ses erişimi (VOIP-Voice Over İnternet Protocol) geçmişten günümüze etkinliğini arttırmıştır. PSTN (Public Switched Telephone Network – Genel Aktarmalı Telefon Şebekesi) tabanlı iletişim altyapısının yerini verim ve maliyet avantajları sebebiyle IP tabanlı sistemler almaya başlamıştır. Günümüzde ses verilerini iletmek için kullanılan IP üzerinden ses teknolojisi; çevrimiçi eğitim, konferans hizmetleri, kurum içi görüşme hizmetleri verebilen kablosuz IP tabanlı araçların üretilmesiyle yaygın olarak kullanılan kablosuz ağlara bütünleşmiş

bir şekilde çalışmaya başlamıştır. IP tabanlı sistemlerin kullanımının artmasıyla birlikte VoIP iletişim sistemleri ve VoIP oturumunun organize edilmesini sağlayan SIP protokolü oldukça geniş bir alanda kullanılmaya başlanmıştır. Birçok kurum ve kuruluş IP tabanlı yazılım ürünlerini taşınabilir cihazlar üzerinden kullanıcılarına kablosuz erişim altyapıları ses ve görüntü hizmeti sağlamaktadır. VoIP tabanlı hizmetlerin verimliliği ve devamlılığı ağ güvenliği ile doğru orantılı olduğu görülmüştür. 2020 yılında Covid-19 sürecinin başlaması kablosuz cihaz erişimlerinin artmasını da beraberinde getirmiştir. Çalışmamızda 2020 yılındaki VoIP etkileşiminin 2019 yılına oranla ne kadar arttığı gerçek rakamlarla verilmiştir. 2020 Nisan ayındaki VoIP tabanlı görüşme oranı 2019 yılındaki VoIP tabanlı görüşmeye oranla %486,95 artış göstermiştir. Bu süreç içerisinde yaşanan iletişim eksikliğini gidermek için ise sahadaki kullanıcılarının ne kadar önemli olduğu ön plana çıkmıştır. Tüm kurum içerisindeki iletişim problemi bir uygulama üzerinden çözülmüş ve maliyet olarak en alt seviyede kalınmıştır. VoIP tabanlı uygulamaların bu dönemde eğitim ve iş tabanlı uygulamalarda kullanılması sebebiyle kişi etkileşimi artmıştır. Çalışmamızda bu etkileşim süreçlerindeki problemi iş tabanlı VoIP uygulaması üzerinden nasıl çözüme kavuşturulduğu ele alınmıştır. Geleceğe yönelik dijitalleşme adımlarında VoIP tabanlı yazılım ve uygulamaların her zaman hayatımızın bir parçası olacağını öngörmekteyim. Perakende firmalarının her daim müşteri ile iletişimde olması sebebiyle esnek iletişim yapılarını kullanması gerekmektedir. Müşteri memnuniyeti ve büyük pazar payından faydalanmak isteyen kurumlar günümüzdeki ve gelecekteki teknolojilerin özelliklerine göre yatırım yapmaları gerekmektedir.

Öneriler

Bu çalışmada problemin incelenmesi ve teşhisi adımında 2019 ve 2020 yılları arasındaki VoIP tabanlı görüşmeleri ve bunlar arasındaki farklar detaylı biçimde incelenerek problemin çözümü örnek bir perakende kurumu üzerinde gerçekleştirilmiştir. Bu çözüm diğer sektör ve benzer kurumlarda uygulanabilir ya da VoIP tabanlı başka bir uygulama üzerinden de benzer sorunlara çözümler geliştirilebilir. Farklı VoIP tabanlı uygulama ve kablolu/kablosuz altyapılar ile VoIP tabanlı iletişim genişletilebilir. Bu yapıların genişletilmesinde yazılım tabanlı network altyapıları kullanılarak insan hatası mümkün olan en az seviyeye indirgenebilir. Güvenlik altyapılarının da göz ardı edilmeyeceği düzenler ile daha kusursuz bütünleşik bilgi sistemleri ortaya çıkarılabilir.

EK'LER

CM Admin Ayarları EK. 1

	CM ADMİN AYARLARI			
1	Add a New Phone	Phone Template	Device Protokol*	SIP
			Phone Type*	Cisco Dual Mode For Iphone
				Cisco Dual Mode For Android
2	Phone Configuration	Device Information	Device Name*	TCT = iphone BOT = android TAB = tablet CSF = windows / and "NAME"
			Description	User Name
			Device Pool*	Device pool find : "Search authority"
			Phone Button Template*	Cisco Dual Mode For Iphone
				Cisco Dual Mode For Android
			Owner User ID	Find User Where : "User ID" begins with "User"
		Protocol Specific Information	Device Security Profile	Phone Type + Standart SIP Non-Scure Profile
			SIP Profile	Standart SIP Profile
3	Directory Number Configuration	Directory Number Information	Directory Number*	User Number
			Route Partitions	Find User Where : "Name" + "contains" + part company name internal
		Directory Number Settings	Calling Serach Space	CSS_CompanyName
		Line 1 on Device Name(TCT,BOT, TAB,CSF)	Display (Caller ID)	Caller ID User Name
		Device Name*	TCT = iphone	
			BOT = android	
			TAB = tablet	
			CSF = windows	

Sunucu Gereksinimleri (12.9 sürüm için) Ek 2.

Hizmet	Yazılım Gereksinimi	Desteklenen Sürüm
IM ve İletişim Durumu Telefon	Cisco Birleşik İletişim Yöneticisi IM ve İletişim Durumu Hizmeti Cisco Webex Messenger	10.5(2) ve sonrası (Minimum) 11.5(1) SU2 veya üstü (Önerilen)
	Cisco Birleşik İletişim Yöneticisi	10.5(2) ve sonrası (Minimum) 11.5(1) SU3 veya üstü (Önerilen)
Telefon Aramayla İlgili Kişi Sesli	Cisco Birleşik Kurtarılabilir Uzak Site Telefonu	Birleşik SIP SRST 12.8 ve sonrası
	LDAP dizini	Microsoft Active directory 2008 R2 ve Open LDAP 2.4 veya sonraki bir tür gibi LDAP v3 uyumlu dizin
	Cisco Unity Bağlantısı	10.5 ve sonrası
Çok satırlı	Cisco Birleşik İletişim Merkezi Express	11.6
Konferans	Cisco Toplantı Sunucusu	2.2 ve sonrası
Çok satırlı	Cisco TelePresence Sunucusu	3.1 ve sonrası
Konferans Uzaktan Erişim	Cisco TelePresence MCU	4.3 ve sonrası
	Cisco ISR PVDM3	Cisco Birleşik İletişim Yöneticisi 9.x ve sonrası
	Bulut CMR	Cisco Webex Toplantıları İşbirliği Toplantı Odası olan sunucu
	Cisco Webex Toplantıları Sunucu	2.8 MR1 ve sonrası
	Cisco Webex Toplantıları Merkezi	ÇÇY33 ve sonrası

	Cisco Uyarlanabilir Güvenlik Gereci Yalnızca Android için Cisco Jabber için geçerlidir.	8.4(1) ve sonrası
	Cisco AnyConnect Güvenli Mobilite İstemcisi Yalnızca Android için Cisco Jabber ve iPhone ve iPad istemcileri için Cisco Jabber.	Platforma bağımlı
Uzaktan Erişim Hizmet IM ve İletişim Durumu Telefon	Cisco Expressway C	X8.10.1 ve sonrası X8.10.1 ve sonrası.
	Cisco Expressway E	
	Yazılım Gereksinimi	Desteklenen Sürüm
	Cisco Birleşik İletişim Yöneticisi IM ve İletişim Durumu Hizmeti	10.5(2) ve sonrası (Minimum) 11.5(1) SU2 veya üstü (Önerilen)
	Cisco Webex M**essenger**	
	Cisco Birleşik İletişim Yöneticisi	10.5(2) ve sonrası (Minimum) 11.5(1) SU3 veya üstü (Önerilen)

(CiscoJabber, 2020)

Windows, Mac, iOS ve Android İçin Sistem ve Donanım Gereksinimleri Ek.3

Cisco Jabber Gereksinimleri Windows ve Mac İçin (12.9 sürüm için)

Gereksinim	**Windows için Cisco Jabber**	**Mac için Cisco Jabber**
Yüklü RAM	2 GB RAM	2 GB RAM
Boş fiziksel bellek	128mb	1gb
Boş disk alanı	256mb	300 MB
CPU hızı ve türü	AMD Mobil Sempron İşlemci 3600+ 2 GHz Intel Core 2 Duo İşlemci T7400 @ 2. 16 GHz	Aşağıdaki Apple donanımlarından herhangi birinde Intel Core 2 Duo veya sonraki işlemciler: iMac Pro, MacBook Pro (Retina Ekran modeli dahil), Macbook, MacBook Air, Imac, Mac Mini
I/O bağlantı noktaları	USB kamera ve ses aygıtları için USB 2.0.	USB kamera ve ses aygıtları için USB 2.0

(CiscoJabber, 2020)

İphone ve İpad için Cisco Jabber Donanım Gereksinimleri

Apple Aygıtı	**Sürüm**
Ipad	5. ve 6.
iPad Air	Air 1, Air 2 ve Air 3
iPad Pro	9,7 ve 10,5 inç 12.9 inç, 1.
iPad mini	Mini 2, mini 3, mini 4 ve mini 5
Iphone	5s, 6, 6 Plus, 6s, 6s Plus, 7, 7 Plus, 8, 8 Plus, X, Xs, Xs Max, XR ve SE

Apple Aygıtı	Sürüm
iPod touch	6. nesil
Apple Watch	Apple Watch ve Apple Watch 2, 3 ve 4'te çalışan WatchOS 5.

Not. Cisco, iPhone ve iPad için Cisco Jabber'ın yalnızca geçerli App Store sürümünü destekler. Herhangi bir Cisco Jabber for iPhone ve iPad sürümünde bulunan kusurlar geçerli sürümlere göre değerlendirilir. (CiscoJabber, 2020)

Aygıt	Modeli	Minimum Android işletim sistemi sürümü	Notlar
Blackberry	Priv	6.0.1	Jabber'ı son görüntülenen uygulamalar listesinden kaldırırsanız ve cihazı bir süre boşta tutarsanız Jabber etkin olmaz.
Fujitsu	Oklar M357	6.0.1	
Google	Nexus 5	6.0	
	Nexus 5X	6.0	
	Nexus 6	6.0	
	Nexus 6P	6.0	Android işletim sistemi sürüm 6.x veya 7.0'a sahip Google Nexus 6P için yöneticinizin Jabber telefon hizmetinizi güvenli bir telefon hizmeti olarak ayarlaması gerekir. Aksi takdirde, cihazınız yanıt vermeyebilir. Android işletim sistemi sürüm 7.1 veya üstü için herhangi bir işlem yapılması gerekmez.
	Nexus 7	6.0	
	Nexus 9	6.0	

	Piksel	7.0	
	Piksel C	6.0	
	Piksel XL	7.0	
	Piksel 2	8.0	Jabber araması sırasında, kullanıcı sesi mobil cihazdan kulaklığa geçirirse anlık ses sorunları mümkündür.
	Piksel 2 XL	8.0	Jabber araması sırasında, kullanıcı sesi mobil cihazdan kulaklığa geçirirse anlık ses sorunları mümkündür.
	Piksel 3	8.0	Takılı kulaklığı telefonla kullanıyorsanız, ses ile ilgili birkaç saniyeliğine bazı sorunlar olabilir.
	Piksel 3 XL	8.0	Takılı kulaklığı telefonla kullanıyorsanız, ses ile ilgili birkaç saniyeliğine bazı sorunlar olabilir.
Honeywell	CT50	6.0	
	CT40	7.1.1	
	CT60	7.1.1 ve 8.1	CT60'ı yalnızca Android OS 7.1.1 ve 8.1 ile destekliyoruz.
Htc	10	6.0	
	A9	6.0	
	M8	6.0	
	M9	6.0	
	X9	6.0	
Huawei	Onur 7	6.0	
	Montaj ilişkisi 8	6.0	
	Montaj ilişkisi 9	6.0	

	Nova	7.0	
	Montaj ilişkisi 10	8.0	
	Mate 10 Pro	8.0	
	P8	6.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	
Lg	G3	6.0	
	G4	6.0	
	G5	6.0	
	G6	7.0	
	V10	6.0	
	V30	8.0	
Motorola	Moto G4	6.0	
	Moto G5	7.0	
	Moto G6	8.0	
	Moto Z Droid	6.0	

Nokia	6.1	8.0	
	8.1	8.1	
OnePlus	One	6.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
	7T	10.0	
Samsung	All	6.0	Android işletim sistemi 6.x veya sonraki bir sürümüne yükseltilen cihazlar artık desteklenmez. Jabber için otomatik çalıştırma seçeneğini etkinleştirin. Android OS 6.x ve sonraki sürümü için, otomatik çalıştırma seçeneğini App Smart Manageraltında bulabilirsiniz. Jabber, Kanada için Samsung Galaxy Tab Pro 8.4'te (Model T320UEU1AOC1) gelen çağrı bildirimi açılır menüsünün gecikmesini geciktirir. Jabber, Wi-Fi bağlantısını kaybettiğinde Samsung Xcover 3'te ağa yeniden bağlanmayı geciktirir. Samsung, Galaxy Note cihazlarını telefon olarak değil tablet olarak görüyor. Birleşik CM'de, bu aygıtları "BOT Aygıtı" olarak değil, "SEKME Aygıtı" olarak yapılandırın. Yonga seti Exynos 7580 olan Samsung cihazlarında ses kalitesi sorunu var. Cihaz ekranı kapalıyken ses belirsizleşir. cihaz listesi aşağıdadır:

			Samsung Galaxy A3 2016 Samsung Galaxy A5 2016 Samsung Galaxy A7 2016 Samsung Galaxy S5 Neo Samsung Galaxy J7 Samsung Galaxy Görünümü
Seuic	Seyir 1	9.0	
Sonim	XP8	7.1.1	
Sony Xperia	Xz	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z2	6.0	
	Z2 tablet	6.0	
	Z3	6.0	Android işletim sistemi 5.0.2 ile Sony Xperia Z3 (Model SO-01G) Jabber çağrılarında zayıf sese sahiptir.
	Z3 Tablet Kompakt	6.0	
	Z3+/Z4	6.0	Sony Z3+/Z4'te görüntülü arama kararsız. Görüntülü arama için kendi videonuzu devre dışı bırakmayı deneyin. Aksi takdirde, yalnızca sesli arama yapın.
	Z4 SEKMESI	6.0	
	Z5 Premium ve Z5	6.0	

Xiaomi	4C	6.0	Bu cihazlarda yalnızca 32 bit sürüm çalışır.
	Max	6.0	
	Mi 4	6.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Mi 10	10.0	
	Pocophone	8.0	
	Mi Notu	6.0	Bu cihazlarda yalnızca 32 bit sürüm çalışır.
	Mi Not 2	7.0	
	Mi MIX 2	8.0	
	Mi A1	8.0	
	Redmi Note 3	6.0	
	Redmi Note 4X	6.0.1	
	Redmi Note 5	8.0	
	Redmi Note 6 Pro	8.1	
Zebra	TC75X	6.0	
	TC51	6.0	

(CiscoJabber, 2020)

KAYNAKÇA

Ahvanooey, M. T., Li, Q., Hou, J., Mazraeh, H. D., & Zhang, J. (2018). AITSteg: An innovative text steganography technique for hidden transmission of text message via social media. *IEEE Access , 6*, 65981-65995.

Bıktım, E. (2016, Aralık 5). *Donanım Günlüğü*. Nisan 25, 2020 tarihinde https://donanimgunlugu.com/beamforming-teknolojisi-nedir-121552 adresinden alındı

Boris, B. (2016). IEEE 802.11 ax: High-efficiency WLANs. *IEEE Wireless Communications, 23(1)*, 38-46.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2012). *YOD: A Global Perspective.* Cisco.

Cisco. (2006, Mart 7). *https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/69267-callstates-sccp-endpoints.html*. Mart 14, 2020 tarihinde Cisco unified communications manager: https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/69267-callstates-sccp-endpoints.html adresinden alındı

Cisco. (2008, Mart 11). *Cisco : Authentication Types for Wireless Devices*. Ekim 24, 2020 tarihinde https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html#wp1035025 adresinden alındı

Cisco. (2014, Temmuz 2). *Cisco IP Telephony for 802.1X Design Guide*. Ocak 21, 2021 tarihinde https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/IP_Tele/IP_Telephony_DIG.html adresinden alındı

Cisco. (2018). *802.11ac: The Fifth Generation of Wi-Fi.* Cisco. Nisan 2020 tarihinde https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf adresinden alındı

Cisco. (2019, Şubat 22). *EAP-FAST Authentication with Wireless LAN Controllers and Identity Services Engine*. (R. Mancur, Editör) Ekim 27, 2020 tarihinde Cisco: https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99791-eapfast-wlc-rad-config.html#anc0 adresinden alındı

Cisco. (2020). *Cisco.* Ekim 27, 2020 tarihinde Leap Nedir. adresinden alındı

Cisco. (2021). *System Configuration Guide for Cisco Unified Communications Manager, Release 12.0(1).* Aralık 21, 2020 tarihinde https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201/cucm_b_system-configuration-guide-1201_chapter_010010.html adresinden alındı

CiscoJabber. (2020, Kasım 13). *Cisco Jabber for iPhone - Quick Start Guide.* Ocak 4, 2021 tarihinde https://www.cisco.com/c/en/us/support/docs/unified-communications/jabber-iphone/213950-jabber-for-iphone-quick-start-guide.html#:~:text=Jabber%20for%20iPhone%20provides%20a,and%20navigate%20to%20Device%20%3E%20Phone adresinden alındı

CiscoJabber. (2020, Ağustos 6). *Planning Guide for Cisco Jabber 12.9.* Ocak 25, 2020 tarihinde Planning Guide for Cisco Jabber 12.9: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_9/cjab_b_planning-guide-cisco-jabber-129/cjab_b_planning-guide-cisco-jabber-129_chapter_01.html adresinden alındı

Computer Controls. (2020). Nisan 27, 2020 tarihinde Computer Controls: https://www.ccontrols.net/en/applications/internet-of-things-iot/wireless-networks/ adresinden alındı

Güneş, E., Sahinaslan, O., & Sahinaslan, E. (2020). A Research on New Generation Technologies to be Used in the Retail Industry After COVID-19. M. University (Dü.), *International Conference of Mathematical Sciences (ICMS 2020)* içinde, (s. 92).

Handley, M., Schulzrinne, H., Schooler, E., & Rosenberg, J. (1999, Mart). SIP: Session Initiation Protocol. Kasım 11, 2020 tarihinde https://tools.ietf.org/html/rfc2543#page-7 adresinden alındı

Henry, J. (2011, Kasım). *802.11s Mesh Networkin.* (M. Burton, Dü.) Nisan 27, 2020 tarihinde cwnp web sitesi: https://www.cwnp.com/uploads/802-11s_mesh_networking_v1-0.pdf adresinden alındı

Huawei. (2020). *Huawei WPA2*. Ekim 24, 2020 tarihinde Huawei Support Web Sitesi: https://support.huawei.com/enterprise/br/doc/EDOC1100035626/4c917c4/example-for-configuring-a-wpa2-psk-aes-security-policy adresinden alındı

Huawei. (2020). *What Is 802.11ax (Wi-Fi 6).* Huawei. Ağustos 31, 2020 tarihinde https://support.huawei.com/enterprise/en/doc/EDOC1100102755 adresinden alındı

IETF. (2002, Haziran). *tools.ietf.org*. SIP: Session Initiation Protocol: https://tools.ietf.org/html/rfc3261#page-36 adresinden alındı

İletişim3xc. (2020). H232 Nedir. *H232 Nedir*. Kasım 2020 tarihinde https://www.3cx.com.tr/voip-sip/h323/ adresinden alındı

Ipropertymanagement. (2019). *ipropertymanagement*. Nisan 21, 2020 tarihinde ipropertymanagement.com: https://ipropertymanagement.com/research/iot-statistics adresinden alındı

ITU. (2001). *ITU.INT.* ARALIK 12, 2020 tarihinde H.323 : Visual telephone systems and equipment for local area networks which provide a non-guaranteed quality of service: https://www.itu.int/rec/T-REC-H.323-199611-S/en/ adresinden alındı

İTÜBİDB. (2013). *https://bidb.itu.edu.tr/*. Nisan 30, 2020 tarihinde PAN, LAN, MAN, WAN karşılaştırması: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/pan-lan-man-wan-kar%C5%9F%C4%B1la%C5%9Ft%C4%B1rmas%C4%B1 adresinden alındı

Juniper. (2020). *What is SD-WAN?* Mayıs 1, 2020 tarihinde Juniper Web Sitesi: https://www.juniper.net/us/en/products-services/what-is/sd-wan/ adresinden alındı

Klein, A. (2008, March 24). Attacks on the RC4 stream cipher. . *Attacks on the RC4 stream cipher. Designs, codes and cryptography*, 269-286.

Kösem, M. (2016, Mart). Kablosuz Ağ Standartlarının Karşılaştırılması ve 802.1 X Standardı İle Bir Üniversitede Kablosuz Ağ Güvenliği Tasarımı. İstanbul: İstanbul Aydın Üniversitesi.

Kurt, Ç. (2013, OCAK). Kablosuz Ağlarda EAP Tabanlı Bir Kimlik Doğrulama Protokolü. *Gazi Üniversitesi Bilişim Enstitüsü Yüksek Lisans Tezi*. Ankara.

Mathy, V., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Securit*, (s. 1313-1328).

NetworkKampus. (2018, Nisan 27). *802.1x Şifreleme Yöntemleri*. Ekim 27, 2020 tarihinde Network Kampus Web Sitesi: https://networkkampus.com/3-802-1x-sifreleme-yontemleri/ adresinden alındı

NetworkLessons. (2020). *Network Lessons*. Nisan 27, 2020 tarihinde Network Lessons Cisco CCNA Web Sitesi: https://networklessons.com/cisco/ccna-200-301/wireless-lan-802-11-service-sets adresinden alındı

Özbilgin, S. (2017, Şubat). Bilgi Teknolojileri Servis Yönetiminin ITIL Çerçevesinde Perakende Firması İçin İncelenmesi ve ITIL Uygulaması Önerisi. İstanbul, Maltepe.

Perahia, E. (2008). IEEE 802.11 n development: History, process, and technology. *EEE Communications Magazine*, 48-55.

Rivest, R. (1992). The MD5 Message-Digest Algorithm. *RFC1321*. Ekim 27, 2020 tarihinde https://tools.ietf.org/html/rfc1321 adresinden alındı

Rohde-Schwarz. (2017, Kasım). *802.11ad - WLAN at 60 GHz A Technology Introduction.* Nisan 2020 tarihinde scdn.rohde-schwarz.com: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma220/1MA220_3e_WLAN_11ad_WP.pdf adresinden alındı

RouterSwitch. (2021, Ocak). *Router Switch*. Ocak 17, 2021 tarihinde Cisco IP Phones VOIP: https://www.router-switch.com/cp-8821-k9-bun.html adresinden alındı

Sahinaslan, E. (2019, 04 02). On the internet of things: Security, threat and control. *AIP Conference Proceedings 2086, Volume 2086*(10.1063/1.5095120), 030035-1- 4. doi:https://doi.org/10.1063/1.5095120

Saraç, M. (2014). *http://mustafasarac.blogspot.com/2014/11/bt-talep-yonetimi.html*. Aralık 21, 2020 tarihinde http://mustafasarac.blogspot.com/2014/11/bt-talep-yonetimi.html: http://mustafasarac.blogspot.com/2014/11/bt-talep-yonetimi.html adresinden alındı

Schulzrinne, H. (1996, Şubat 22). Simple conference invitation protocol, draft-ietf-mmusic-scip-00. txt. Kasım 25, 2020 tarihinde Simple conference invitation protocol. draft-ietf-mmusic-scip-00. txt. adresinden alındı

Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. (1996, Temmuz). RTP: A transport protocol for real-time applications. https://tools.ietf.org/html/rfc3550 adresinden alındı

Soy, H., Özdemir, Ö., & Bayrak, M. (2013). Kablosuz Yerel Alan Ağlarında Güncel Gelişmeler: IEEE 802.11ac ile Yeni Nesil Gigabit Wi-Fi. *Akademik Bilişim 2013 – XV*. Antalya. https://ab.org.tr/ab13/kitap/soy_ozdemir_AB13.pdf adresinden alındı

Şahinaslan, E. (2010). Standartlara Dayalı Bilgi Güvenliği Risk Analiz Ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi Ve Uygulama Yazılımının Geliştirilmesi. Edirne: Trakya Üniversitesi.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *Akademik Bilişim*, (s. 1). Şanlıurfa.

Şahinaslan, Ö., Şahinaslan, E., & Kantürk, A. (2010). Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık. *Ağ ve Bilgi Güvenliği Sempozyumu* (s. 6). Ankara: EMO.

Tarlacı, M. F. (2018, Temmuz). Kablosuz Kampüs Ağlarında Dinamik Vlan Yapılandırmasının Ağ Performans Parametreleri Üzerindeki Etkisi. 11. Muğla.

Tech. (2020). *Phone Lines VoIP / SIP*. Kasım 10, 2020 tarihinde southpointcommunications.tech sitesi: https://southpointcommunications.tech/phone-lines-voip-sip/ adresinden alındı

Techtarget. (2020, Kasım). *searchnetworking.techtarget.com*. (A. Irrei, Editör) Aralık 21, 2020 tarihinde What is the difference between IP telephony and VoIP?: https://searchnetworking.techtarget.com/answer/What-is-the-difference-between-IP-telephony-and-voice-over-IP-VoIP adresinden alındı

TS ISO/IEC 17799. (2002, Kasım). Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri. Ankara: TSE.

Van Nee, R. J. (2006). The 802.11 n MIMO-OFDM standard for wireless LAN and beyond. *Wireless Personal Communications, 37(3)*, 445-453.

Wi-Fi Alliance. (2005). *Deploying Wi-Fi Protected Access (WPAtm) and WPA2tm in the Enterprise.*

Wikipedia. (2019). *tr.wikipedia.org*. Aralık 25, 2020 tarihinde Wikipedia Microsoft Teams: https://tr.wikipedia.org/wiki/Microsoft_Teams adresinden alındı

Wikipedia. (2020). *Wikipedia IEEE 802 1x*. Nisan 2020 tarihinde IEEE 802 1x: https://tr.wikipedia.org/wiki/IEEE_802.1X adresinden alındı

Worldometers. (2021). *https://www.worldometers.info/coronavirus/country/turkey/*. Ocak 10, 2021 tarihinde Coronavirus Cases: https://www.worldometers.info/coronavirus/country/turkey/ adresinden alındı

Yao, Y., Chong, J., & Xingwei, W. (2010). Enhancing RC4 algorithm for WLAN WEP protocol. *Chinese Control and Decision Conference* (s. 3623-3627). Çin: IEEE. doi:10.1109/CCDC.2010.5498536