

Doküman Kodu: BGT-6001

KABLOSUZ YEREL ALAN AĞI GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

3 MART 2008

Hazırlayan: Battal ÖZDEMİR

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Fatih KO'a, Burak BAYOĐLU'na ve Mehmet KARA'ya teřekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	6
1.1 Amaç ve Kapsam.....	6
1.2 Hedeflenen Kitle.....	6
1.3 Kısaltmalar.....	6
1.4 Dokümanda Kullanılan Semboller	8
2. KABLOSUZ AĞLAR HAKKINDA GENEL BİLGİ	9
2.1 Kablosuz Haberleşme Teknolojileri	9
2.1.1 Yerel Alan Ağları.....	9
2.1.2 Kişisel Alan Ağları	9
2.1.3 Geniş Alan Ağları	10
2.2 Kablosuz Yerel Alan Ağları Tarihçesi	11
2.3 IEEE 802.11 Kablosuz Yerel Alan Ağları Bileşenleri	11
2.4 IEEE 802.11 Çalışma Modları.....	12
3. KABLOSUZ AĞLARIN TAŞIDIĞI RİSKLER	13
3.1 Kablolu Ağa Sızma.....	13
3.2 Trafik Dinlenip Verinin Çözülmesi.....	13
3.3 Ağ Topolojisinin Ortaya Çıkması.....	13
3.4 İstemcilerin Yetkisiz Erişim Noktalarına Bağlanması	14
3.5 İstenmeyen Yerlere Servis Verme	14
3.6 Servis Dışı Bırakma (DoS).....	14
4. KABLOSUZ AĞ GÜVENLİK STANDARTLARI	15
4.1 IEEE 802.11 Güvenlik Standardı (WEP)	15
4.2 Wi-Fi Protected Access (WPA).....	16
4.3 IEEE 802.11i	19
5. TAVSİYE EDİLEN GÜVENLİK KONFIGÜRASYONLARI	20
5.1 Mimari Topoloji	21
5.2 Gerekli Bileşenler:.....	21

5.3 Etki Alanı Kullanıcı Hesapları ve Grup Ayarları:	22
5.4 IAS Sunumcu Ayarları:	23
5.5 Erişim Noktası Konfigürasyonu:	29
5.6 Kablosuz Ağ (802.11) Grup Politikası Ayarları:	30
5.7 Kablosuz İstemci Ayarları:	35
6. KABLOSUZ AĞLARDA ALINACAK GÜVENLİK ÖNLEMLERİ	38
6.1 Güvenlik Politikası	38
7. EK GÜVENLİK ÖNLEMLERİ.....	39
7.1 Erişim Noktası Fiziksel Güvenliği.....	39
7.2 VPN Uygulaması.....	39
7.3 Saldırı Tespit ve Önleme Sistemleri	39
7.4 Periyodik Testler.....	40
8. TAVSİYELER.....	41

1. GİRİŞ

Bu dokümanda kablosuz yerel alan ağı (802.11b/g) kullanımı durumunda uyulması gereken güvenlik esasları anlatılacaktır.

1.1 Amaç ve Kapsam

Bu dokümanda amaç, kablosuz ağ kurulumunda, yönetilmesinde ve kullanımının denetlenmesinde uyulması gerekli esasları belirlemektir. Esaslar belirlenirken, kablosuz ağ kullanımı durumunda karşılaşılabilecek tehditler incelenmiş, ilgili riskleri düşürecek, standartlaşmış, yaygın olarak kullanılan güvenlik çözümleri araştırılmış ve esas olarak belirlenmiştir. Üçüncü parti çözümler, donanım bağımlılıkları ve belli bir ulusal veya uluslararası standarda dayanılarak geliştirilmemiş olmaları sebepleri ile kapsam dışı tutulmuşlardır. Üçüncü parti çözümler çoğunlukla belli bir marka ve modele dayalı çözümler sunmaktadır.

1.2 Hedeflenen Kitle

Bu doküman kablosuz ağ çözümlerini kuran, yöneten ve denetleyen ya da bu konularda çalışmak isteyen kişiler tarafından kullanılabilir.

1.3 Kısaltmalar

UEKAE	:	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
WLAN	:	Wireless Local Area Network
AES	:	Advanced Encryption Standard
EAP	:	Extensible Authentication Protocol
EAP-TLS	:	EAP Transport Layer Security
MS-CHAP v2	:	Microsoft Challenge Handshake Authentication Protocol version 2
PEAP	:	Protected Extensible Authentication Protocol
SSID	:	Service Set Identifier (SSID)
TKIP	:	Temporal Key Integrity Protocol
WPA2	:	Wifi Protected Access 2

WEP	:	The Wired Equivalent Privacy
IEEE	:	The Institute of Electrical and Electronics Engineers
ISM	:	Industry, Science, Medical
PDA	:	Personal Digital Assistant
PC	:	Personal Computer
Wi-Fi	:	Wireless-Fidelity
LOS	:	Line of Sight
WiMAX	:	Worldwide Interoperability for Microwave Access
VLAN	:	Virtual Local Area Network
EN	:	Erişim Noktası (Access Point)
ESS	:	Extended Service Set
POP3	:	Post Office Protocol 3
SMTP	:	Simple Mail Transfer Protocol
NTLM	:	NT LAN Manager
DoS	:	Denial of Service
PSK	:	Preshared Key
RADIUS	:	Remote Access Dial In Service
TACACS	:	Terminal Access Controller Access-Control System
CRC	:	Cyclic Redundancy Check
IV	:	Initialisation Vector
RSN	:	Robust Security Network
CCMP	:	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CBC- MAC	:	Cipher Block Chaining Message Authentication Code Protocol
VPN	:	Virtual Private Network

CA	:	Certification Authority
IAS	:	Internet Authentication Service
IPSec	:	IP Security
SSL	:	Secure Sockets Layer
HTTPS	:	Hypertext Transfer Protocol over Secure Socket Layer
MMC	:	Microsoft Management Console
KYAA	:	Kablosuz Yerel Alan Ağları
AAA	:	Authentication, Authorization and Accounting
IBSS	:	Independent Basic Service Set

1.4 Dokümanda Kullanılan Format ve Semboller

Sembol	Açıklaması
yabancı terim	Yabancı dildeki terimleri belirtmek içindir.
komut	Kod parçalarını ve betikleri belirtmek içindir.
<u>vurgu</u>	Vurgu yapmak için kullanılır.

2. KABLOSUZ AĞLAR HAKKINDA GENEL BİLGİ

Kablosuz ağlar, kablosuz haberleşme yeteneğine sahip (802.11, bluetooth, infrared, GSM vb.) cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır.

2.1 Kablosuz Haberleşme Teknolojileri

İhtiyaca göre farklılaşmış, farklı frekans bantlarında, değişik standartlara göre çalışan kablosuz haberleşme teknolojileri bulunmaktadır. Kablosuz haberleşme ağlarını 3 sınıfa ayırabiliriz:

2.1.1 Yerel Alan Ağları

IEEE, 802'yi yerel alan ağı standartlarını, 802.11'i kablosuz yerel alan ağlarını, sonda bulunan a, b, g, n gibi harfler ile de özelleşmiş kablosuz ağ standartlarını tanımlamak için kullanmaktadır.

IEEE 802.11 b,g: Türkiye'de 2.4 GHz ISM radyo frekans bandında yüksek hızlı veri transferinin mümkün olduğu (802.1b ile 11Mbps, 802.11g ile 54 Mbps), kapsama alanı 10 ila 100 metre arasında değişen (anten, alıcı kazancı, sinyal gücü, ortam gibi değişkenlere bağlı olarak), dizüstü bilgisayar, masaüstü bilgisayar, PDA vb. cihazların bir erişim noktası üzerinden ya da birbirleriyle kurdukları direk bağlantı ile haberleşmelerini sağlayan kablosuz ağ yapılarıdır. Kablosuz Ethernet ya da Wi-Fi olarak da adlandırılmaktadır.

IEEE 802.11a: Avrupa dışında kullanılan, 802.11b,g standardından farklı olarak 5.0 GHz ISM bandında veri transferine izin veren standarttır. Türkiye'de kullanımına izin verilmemektedir.

IEEE 802.11n: Henüz yaygın olarak kullanılmayan, çoklu antenler ve çeşitli protokoller kullanarak maksimum veri transfer hızını 540 Mbps'a çıkaran standarttır.

2.1.2 Kişisel Alan Ağları

Bluetooth (IEEE 802.15.1): Cihazların düşük hızda bire bir haberleşmeleri için kullanılan, genellikle kısa menzilli (1 ila 20 metre) kablosuz haberleşme sistemleridir. Bluetooth haberleşmesi 802.11b/g ile aynı frekans bandında (2.4 GHz) gerçekleşmektedir, bu sebeple Bluetooth haberleşmeleri 802.11b/g haberleşmeleri üzerinde gürültü olarak olumsuz etki yapabilmektedir. Bluetooth haberleşmesi için cihazlar arasında direk görüş hattı (**Line of Sight - LOS**) olması gerekmemektedir. Bluetooth 1.0 ile 720 Kbps, Bluetooth 2.0 ile 3Mbps maksimum veri hızına ulaşılabilir. Bluetooth haberleşmesine örnek olarak

- Bilgisayarların düşük hızlı kısa mesafeli haberleşmeleri
- Cep telefonları arasında ve PC'ye veri transferi
- Bluetooth kulaklık
- Bluetooth ile yazıcı kullanımı

verilebilir.

2.1.3 Geniş Alan Ağları

GSM: Baz istasyonları üzerinden aktarma yöntemiyle uzun mesafeler arasında cep telefonu ile ses ve veri haberleşmesini sağlayan sistemlerdir.

WiMAX [6]: IEEE 802.16e standardı ile tanımlanmış bir kablosuz geniş bant erişim teknolojisidir. Teorik olarak IEEE 802.16 standardı görüş hattı gerektirmeden 50 km'ye kadar kapsama alanı sağlamak ve maksimum 75 Mbps'lik (yakın mesafelerde) iletim hızını mümkün kılmak üzere tasarlanmıştır. Çeşitli ülkelerde farklılık göstermekle birlikte 2 GHz-11GHz aralığında belirli frekans bantlarının WiMAX Mobil kullanıcılara mekândan bağımsız internet erişimi sunmayı amaçlamakta, ayrıca kablolamanın maliyet ve/veya coğrafi şartlar sebebiyle elverişli olmadığı bölgelerde alternatif bir olarak düşünülmektedir. Türkiye de pilot uygulamalar yapılmaktadır, fakat henüz etkin olarak kullanılmamaktadır.

Bu dokümanda **Kablosuz Yerel Alan Ağları'nda (IEEE 802.11b/g) kullanılan güvenlik mekanizmaları** incelenecektir.

2.2 Kablosuz Yerel Alan Ağları Tarihçesi

KYAA (WLAN) teknolojileri ilk olarak 1990 yılında 900MHz frekans bandında çalışan, 1Mbps veri hızına ulaşan, üreticilerin kendi standartlarını oluşturduğu ürünlerle ortaya çıktı. Bu dönemde kablolu ağların hızı 10 Mbps seviyesindeydi. 1992 yılında 2.4 GHz bandında çalışan ürünler piyasaya çıktı. 1997 yılında IEEE 802.11 kablosuz Ethernet standardını yayınladı, frekans bandı 2.4 GHz ve veri hızı 1 Mbps'ti. 1999 yılında, IEEE daha yüksek veri hızı, farklı frekans bant kullanımı ve güvenlik özellikleri içeren 802.11a (5 GHz, 54 Mbps) ve 802.11b (2.4 Ghz, 11 Mbps) standartlarını yayınladı. 2003 yılında 2.4 GHz bandında çalışan ve 54 Mbps veri hızı sunan, aynı zamanda da 802.11b standardında çalışan cihazlarla haberleşebilmeyi sağlayan IEEE 802.11g standardı yayınladı. IEEE 802.11g'den 10 kat hızlı veri iletişimi sağlaması planlanan 802.11n standardının Draft 2.0 versiyonu Mart 2007'de yayınladı. Standartlaşmamış olmakla birlikte piyasada Ağustos 2007 itibarıyla 70 kadar kablosuz cihaz Draft 2.0 versiyonuna uygunluk sertifikası almış bulunmaktadır [1].

2.3 IEEE 802.11 Kablosuz Yerel Alan Ağları Bileşenleri

IEEE 802.11 Kablosuz yerel alan ağlarında bulunan temel bileşenler aşağıda sıralanmaktadır:

Kablosuz İstemci: En az bir adet 802.11a/b/g kablosuz ağ adaptörüne sahip olan kişisel bilgisayarlar, dizüstü bilgisayarlar, el bilgisayarları, cep telefonları vb.

Erişim Noktası (EN-Access Point): İstemcilerin ağa bağlandıkları noktalardır. Hub gibi davranırlar; gelen paketi havaya basarlar ve tüm istemciler ilgili pakete ulaşabilir. Erişim noktaları SSID (**Service Set ID**)'leri ile ayırt edilirler. EN'ler periyodik olarak beacon paketlerini havaya göndermek suretiyle varlıklarını (SSID bilgilerini) mevcut istemcilere bildirirler.

Kimlik Doğrulama/Yetkilendirme Sunucusu (Opsiyonel bileşen): AAA sunucusu olarak ta bilinmektedir. Kablosuz haberleşmede, tasarlı yapıda (**infrastructure mode**) kablosuz erişim yapmak isteyen kullanıcıların kimlik doğrulama işleminin yapılacağı sunuculardır. Kullanıcı bilgilerinin tutulduğu veritabanını kullanır (Ör: **Active Directory**), tanımlanmış erişim kontrol listesine göre erişim izni verir/dinamik VLAN ataması yapar vb. Yetkilendirme sunucusuna erişim istekleri Erişim Kontrol Cihazı üzerinden gelir. 802.1x kullanılması durumunda erişim noktaları erişim kontrol cihazı görevi yapar.

2.4 IEEE 802.11 Çalışma Modları

IEEE 802.11 kablosuz yerel alan ağlarında iki farklı çalışma modu bulunmaktadır:

Tasarlı (Infrastructure) Mod: Kablosuz istemciler bir veya birden çok EN'ye bağlanmakta ve tüm veri trafiği bu EN'ler üzerinden akmaktadır. Tek EN bulunan ağlar **Basic Service Set** (BSS), çoklu EN bulunan ağlar ise **Extended Service Set** (ESS) olarak isimlendirilmektedirler.

Tasarsız (Ad Hoc) Mod: Kablosuz istemciler herhangi bir EN'ye bağlanmaksızın direk birbirleriyle bağlantı kurmaktadır (Peer-to-Peer bağlantı). Bu tür ağlar aynı zamanda **Independent Basic Service Set** (IBSS) olarak isimlendirilmektedirler.

3. KABLOSUZ AĞLARIN TAŞIDIĞI RİSKLER

3.1 Kablolu Ağa Sızma

Erişim noktaları, uygun güvenlik önlemleri alınmaması durumunda, saldırganlar için kablosuz ve kablolu ağa bağlanmak için açık uç sağlar. Kablolu ağdaki mevcut önlemler saldırganın iç ağa direk erişiminin olmadığı, en azından bir güvenlik duvarı üzerinden geleceği varsayımına dayanmaktadır. EN üzerinden iç ağa erişim, geniş alan ağından gelen saldırganları önlemek için kullanılan güvenlik duvarının atlatılması ve güvenlik açığı bulunması muhtemel birçok servise direk erişim sağlanması riskini taşımaktadır.

3.2 Trafiğin Dinlenip Verinin Çözülmesi

Erişim noktaları bir hub gibi davranırlar, gelen trafiği ortak transmision ortamına, yani havaya gönderirler ve bu trafik ortamdaki diğer bütün kablosuz cihazlar tarafından dinlenebilir ve kaydedilebilir. Kullanılan şifreleme algoritmasının açıklıklarının bulunması durumunda bu veri paketleri olası saldırganlar tarafından çözülebilir. Örneğin yerel ağda gönderilen Telnet / POP3 / SMTP parolaları, NTLM özetleri saldırganlar tarafından elde edilebilir, yazışmalar, e-postalar, internette sörf yapan kişilerin ilgi alanları konusunda bilgiler açığa çıkabilir.

3.3 Ağ Topolojisinin Ortaya Çıkması

Kablolu ağlara yapılan saldırılarda gerçekleştirilen önemli adımlardan biri ağ topolojisinin ortaya çıkarılmasıdır. Kablosuz iletişimde 2. katmanda (Veribağlama katmanı) gönderilen kontrol paketleri şifresiz olarak gönderilmektedir, bu durum kablosuz ağdaki bütün mevcut istemci ve varsa sunumcuların network bilgilerinin ortada olmasına neden olmaktadır. Ayrıca EN'in kablolu ağa bir hub üzerinden bağlanması durumunda kablolu ağın topolojisinin saldırganlar tarafından öğrenilmesi mümkün olabilmektedir. Kablosuz ağdaki şifrelemenin kırılması durumunda iç ağ ile yapılacak trafiğin incelenmesi ile iç ağ topolojisi anahtar (**switch**) cihazı kullanılsa dahi ortaya çıkarılabilir.

3.4 İstemcilerin Yetkisiz Erişim Noktalarına Bağlanması

Saldırganlar ortama sahte erişim noktaları yerleştirebilir, ya da kendi dizüstü bilgisayarlarını basit işlemler sonucunda bir EN'ye dönüştürebilir. Yetkili istemciler uygun şekilde konfigüre edilmezlerse, bu sahte erişim noktaları üzerinden farkında olmadan istenilmeyen bağlantı kurulmasına sebep olunabilir, ya da “*araya girme (man-in-the-middle)*” türü ataklara maruz kalınabilir.

3.5 İstenmeyen Yerlere Servis Verme

Kablosuz haberleşme ortamının hava olması sebebiyle fiziksel erişim kontrolü mümkün değildir. Yetkisiz istemciler güvenli olmayan yetkilendirme ve şifreleme önlemlerini aşarak mevcut kablosuz ağın kaynaklarını kendileri için kullanabilirler.

3.6 Servis Dışı Bırakma (DoS)

Kablosuz ağa bağlı istemcilere gönderilecek sahte **deauthenticate** mesajları ile kablosuz ağa DoS ataklarının yapılması mümkündür. Ayrıca ortamın **jam** edilmesi (frekans bandının gürültü seviyesinin haberleşme yapılamayacak derecede yükseltilmesi), ya da aynı frekansta hizmet veren başka erişim noktalarının ortama konulması suretiyle de DoS atakları yapılabilir.

4. KABLOSUZ AĞ GÜVENLİK STANDARTLARI

4.1 IEEE 802.11 Güvenlik Standardı (WEP)

1999 yılında yayınlanmış olan IEEE 802.11 standardında (WEP – **Wired Equivalent Privacy**) kimlik doğrulama/yetkilendirme, şifreleme ve veri bütünlüğü hususlarında uygulanabilecek güvenlik önlemleri belirlenmiştir. 2000 yılından başlayarak açıklıkları tespit edilmeye başlanmış ve ilgili açıklıkları kullanarak güvenlik önlemlerini etkisiz kılan yazılımlar/kodlar internette yayınlanmıştır. Kullanımı tavsiye edilmemektedir.

İlgili standartta kimlik doğrulama için iki seçenek sunulmaktadır:

Açık Sistem Kimlik Doğrulama (Open System Authentication) : Gerçekte herhangi bir kimlik doğrulama yapılmamakta, erişim noktasına bağlanırken kablosuz ağ bağdaştırıcısının MAC adres bilgisi gönderilmektedir. EN bu bilgiyi kaydederek istemciye kablosuz erişim hakkı verir.

Paylaşılan Anahtar ile Kimlik Doğrulama (Shared Key Authentication) : İstemci ve erişim noktasında ortak bir anahtar tutulmaktadır. İstemci bağlantı kurmak istediğinde EN istemciye rastgele bir mesaj yollar. İstemci bu mesajı ortak anahtarla şifreleyip EN'ye gönderir. EN mesajın ortak anahtarla şifrelendiğini doğrularsa istemciye kablosuz erişim hakkı verir. Ortak anahtarın istemci EN'ye nasıl dağıtılacağı ve sonrasında uygulanacak anahtar güncelleme yöntemi WEP standardında belirtilmemektedir. Ayrıca ortak anahtar aynı zamanda şifreleme amaçlı da kullanılmaktadır. Kimlik doğrulama aşamasında kullanılan açık veri – şifrelenmiş veri trafiği kaydedilip kriptanaliz yöntemleri ile şifrelenmiş bilgilerin kısmen ortaya çıkarılabilmesi mümkündür. Kısacası Kimlik doğrulama için kullanılan anahtar aynı zamanda şifreleme için de kullanıldığı için ek güvenlik sağlamamakta, aksine şifreleme kısmı için güvenlik açığı oluşturmaktadır. Bu sebeple WEP kullanılırken “Açık Sistem Kimlik” Doğrulama seçilmesi daha güvenli kabul edilmektedir.

Şifreleme: Şifreleme için RC4 şifreleme algoritması istemcilerde ve EN üzerinde girilen ortak anahtar ile kullanılmaktadır. Bu yöntemde

- RC4 algoritmasının zayıflıkları,
- Ortak anahtarlar için herhangi bir anahtar yönetim mekanizması bulunmaması,

- 24-bit **Initialization Vector (IV)** kullanımının tekrarlanan şifreleme dizilerinin kullanımına yol açması sebepleriyle şifreleme yeterli gizlilik sağlayamamakta, yeterli veri trafiği saldırganlar tarafından kaydedildiğinde paylaşılan anahtar ele geçirilebilmektedir.

Veri Bütünlüğü: 32 bit CRC (**Cyclic Redundancy Check**)'e dayanan ICV (**Integrity Check Value**) kullanılmaktadır. Bu yöntemde veri paketinin 32-bit CRC'si oluşturulmakta ve WEP anahtarı ile şifrelenerek alıcıya gönderilmektedir. ICV kriptografik veri bütünlüğü sunmamaktadır. Bu sebeple bit değiştirme ve tekrarlama saldırılarına karşı konulamamaktadır. Bit değiştirme saldırısında, şifrelenmiş mesajın belli bitleri değiştirilip şifreli ICV'de de karşılık gelen değişiklik ortak anahtar bilinmeden yapılabilmektedir. Tekrarlama saldırısında ise saldırgan tarafından yakalanmış bir paket farklı bir zamanda EN'ye veya istemciye gönderilebilmektedir. Bu sayede kripto analiz için yapay veri trafiği oluşturulabilmektedir (EN tekrarlanan paketlere yanıt paketleri göndermektedir).

Sonuç olarak WEP standardı kimlik doğrulama, şifreleme ve veri bütünlüğü önlemlerinin hepsinde ciddi açıklıklar bulunmaktadır, bu sebeple kurumsal kablosuz güvenlik standardı olarak kullanımı uygun değildir.

4.2 Wi-Fi Protected Access (WPA)

WEP standardında olan açıklıkların ortaya çıkmasıyla birlikte IEEE yeni bir güvenlik standardı (IEEE 802.11i) oluşturmak amacıyla çalışmalara başlamıştır. Fakat bu standardın çıkmasının gecikmesi sebebiyle ara çözüm olarak **Wi-Fi Alliance** (üretici firmaların oluşturduğu organizasyon) WPA standardını oluşturmuştur.

Kimlik Doğrulama: WPA kimlik doğrulama/yetkilendirme için iki seçenek sunmaktadır.

1. Birincisi ev kullanıcıları, küçük işletmeler için tasarlanmış olan WPA-PSK yapısıdır. WPA-PSK'da kimlik doğrulama için istemciler ve erişim noktası üzerinde girilen bir paylaşılan parola (PSK) kullanılmaktadır. Paylaşılmış anahtar istemcilerin işletim sisteminde tutulmakta, bu sebeple PSK anahtarı çalınma/hacker saldırıları ile başkalarının eline geçme riski taşımaktadır (Örnek: WzCook saldırı yazılımı, üzerinde çalıştığı işletim sistemindeki anahtarlarını kullanıcıya bildirmektedir.). Kimlik doğrulama trafiğini kaydeden saldırganların sözlük saldırılarına olanak tanıyan bir yapıdır. Tek ortak anahtar kullanımı kullanıcıların ayırt edilebilmesini/ farklı yetkilendirmelerin yapılmasını/ kullanıcı tabanlı kayıt tutulmasını olanaksız

kılmaktadır. Ayrıca bir istemci bilgisayarının çalınması durumunda ya da yetkisiz bir erişim olduğunda PSK'nın ele geçmesi muhtemeldir. Kurumsal kablosuz ağlarda kullanımı uygun değildir.

2. İkinci seçenek ise 802.1x kullanımudur. IEEE 802.1x, port tabanlı ağ erişim kontrol mekanizmasıdır ve uzaktan erişim, VPN, anahtarlama cihazı vb. uygulama/birimlerin kimlik doğrulama/yetkilendirme yöntemi olarak kablolu ağlarda kullanılmaktadır.
 - a. 802.1x'te PEAP (kullanıcı hesap bilgileri kullanılarak), EAP-TLS (Sertifika tabanlı), EAP-MD5 (şifre kullanılarak) vb. protokoller kullanılarak kimlik doğrulama işlemi gerçekleştirilebilmektedir.
 - b. 802.1x ile çift yönlü kimlik doğrulama mümkündür, istemciler ve RADIUS/TACACS sunumcu karşılıklı olarak kimlik doğrulama işlemi gerçekleştirebilirler, böylece istemcilerde doğru ağa bağlandıklarını kontrol edebilirler.
 - c. 802.1x ile yetkilendirmede erişim politikaları tanımlanabilmekte, ait olduğu etki alanı, kullanıcı grubu, bağlantı türü, bağlantı zamanı, bağlandığı erişim noktası vb. kriterlere göre yetkilendirme yapılabilmektedir.
 - d. 802.1x erişim kontrolünde yer alan bileşenler: istemci (laptop, PDA, cep telefonu, PC vb.), erişim noktası ve RADIUS/TACACS erişim kontrol sunucusudur. İstemciler bağlantı isteklerini erişim noktasına bildirirler, erişim noktası isteği RADIUS/TACAS sunumcuya yöneltir ve kimlik doğrulama/yetkilendirme işlemini RADIUS/TACACS sunumcu gerçekleştirerek sonucu erişim noktası ve istemciye bildirir. Sonuca göre erişim noktası istemciye bağlantı için sanal bir port açar. Bu işlemler sonucunda ek olarak erişim noktası ve istemci arasındaki şifreli haberleşmelerde kullanılacak şifreleme anahtarları oluşturulur.

Sifreleme: 802.1x kimlik doğrulama/yetkilendirme işlemi sonucunda haberleşme için kullanılacak şifreleme anahtarı istemci ve RADIUS/TACACS sunumcu tarafından karşılıklı olarak oluşturulur ve erişim noktasına RADIUS/TACACS sunumcu tarafından iletilir. Şifreleme için **Temporal Key Integrity Protocol (TKIP)** kullanılmaktadır. TKIP yapısında, WEP'te kullanılan şifreleme algoritması RC4 kullanılmakta, fakat WEP'ten farklı olarak her bir pakette şifreleme anahtarını değiştirilmekte (**per packet keying**) ve IV uzunluğu 24 bit yerine 48 bittir. TKIP, WEP'in bilinen zayıflıklarını kapatmak üzere geliştirilmiş bir yapıdır, WEP'ten TKIP'a donanım değişikliği olmadan geçişe imkan verebilmek amacıyla zayıf bir şifreleme algoritması olan RC4 kullanımına devam edilmiştir. Erişim noktaları ve istemci ağ bağdaştırıcılarının yeni nesil şifreleme algoritması olan AES'in donanımsal olarak desteklemediği durumlarda kullanılacak en güvenli şifreleme seçeneğidir. Kurumsal kablosuz ağlarda 802.1x ile birlikte kullanımı gereklidir, WPA-PSK ile kimlik doğrulama yapılması durumunda şifreleme anahtarlarının oluşturulduğu yöntemdeki zayıflık şifreleme yapısının sağladığı gizliliği ortadan kaldırabilir.

Veri bütünlüğü: WPA, WEP yapısından farklı olarak basit CRC hesaplaması yerine kriptografik veri bütünlüğü kontrolü yapılmasına olanak sağlamaktadır. Tekrarlama, bit değiştirme saldırılarına karşı WEP'in taşıdığı zayıflıkları taşımaz. Veri bütünlüğü için Michael olarak adlandırılan, paketlerin veri kısmı özetinin (**hash**) TKIP ile şifrenmesi yöntemi kullanılmaktadır. Veri bütünlüğü için kullanılan anahtar, veri şifreleme anahtarından farklıdır ve 802.1x kimlik doğrulama aşamasında oluşturulmaktadır.

Windows WPA Desteği

Aşağıda belirtilen Windows işletim sistemi sürümlerinde WPA konfigürasyonu desteklenmektedir:

- Windows Vista
- Windows XP SP2
- Windows Server 2003 SP1-SP2
- Windows Server "Longhorn"
- Windows XP SP1 ve Windows Server 2003 (SP1-SP2 yüklenmemiş)'te <http://support.microsoft.com/?kbid=826942> adresinde bulunan güncellemenin yüklenmesi gerekmektedir.

- Windows 2000, Windows XP (SP yüklenmemiş) ve daha eski Windows işletim sistemlerinde WPA konfigürasyonu desteklenmemektedir. Ağ bağdaştırıcısı üretici firmalarının sağlayacağı konfigürasyon yazılımları ile WPA konfigürasyonu yapılabilir.

Ayrıca Windows 2000 Server SP4 ve Windows 2003 Server SP1 etki alanı kontrolcülerini üzerinden grup politikası ile ilgili istemcilerin WPA güvenlik ayarları yapılabilmektedir.

4.3 IEEE 802.11i

IEEE 802.11i çalışma grubu tarafından WEP'in zayıflıklarını tümüyle ortadan kaldırmak amacıyla oluşturulmuş güvenlik standardıdır. WPA2 veya **Robust Security Network (RSN)** olarak da bilinmektedir. **Advanced Encryption Standard (AES)** şifreleme algoritmasının **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** modunda şifreleme ve veri bütünlüğü kontrolü için ve 802.1x'in kimlik doğrulama/yetkilendirme için kullanımını önermektedir.

Kimlik Doğrulama/ Yetkilendirme: WPA ile aynı yapıyı, 802.1x'i kullanmaktadır.

Sifreleme: **Advanced Encryption System (AES)** şifreleme algoritması **Counter Mode** modunda kullanılmaktadır. Bu yöntemle WEP ve TKIP'ta kullanılan IV ve TKIP'te uygulanan **per packet keying** mekanizmasına ihtiyaç kalmaksızın şifreleme anahtarı tekrarını önleyen bir yapı oluşturulmuştur. AES şifreleme algoritması RC4 algoritmasına göre daha güçlü bir şifreleme algoritmasıdır ve bilinen herhangi bir zayıflık içermemektedir. AES kullanımını desteklemeyen donanımlara yönelik uyumluluk için RC4 şifreleme algoritması kullanan TKIP yapısı da IEEE 802.11i standardında bulunmaktadır. Kablosuz ağ'larda kritik bilgi taşıyan kurumlarda 802.11i AES kullanımı tavsiye edilmektedir.

Veri Bütünlüğü: WPA veri bütünlüğü kontrolünden farklı olarak paketlerin veri kısmı özetleri **AES Cipher Block Chaining Message Authentication Code Protocol (CBC-MAC)** ile şifrelenmektedir. WPA veri bütünlüğü şemasına göre daha güçlü bir yapıdır.

Windows 802.11i (WPA2) Desteği

Aşağıda belirtilen Windows işletim sistemi sürümlerinde WPA2 konfigürasyonu desteklenmektedir:

- Windows Vista
- Windows XP SP2, ek olarak <http://support.microsoft.com/?kbid=917021>, adresinde bulunan güncelleme

- Windows Server "Longhorn"

Ayrıca Windows 2003 Server SP2 ve Windows Server Longhorn etki alanı kontrolcülerini üzerinden grup politikası ile ilgili istemcilerin WPA2 güvenlik ayarları yapılabilmektedir.

5. TAVSİYE EDİLEN GÜVENLİK KONFIGÜRASYONLARI

Aşağıda kurumsal kablosuz ağlarda kullanımı önerilen güvenlik standartları(sırasıyla şifreleme ve kimlik doğrulama) güçlüden zayıfa doğru sıralanan şekilde verilmiştir:

- WPA2/AES ve EAP-TLS
- WPA2/AES ve PEAP-MS-CHAP v2
- WPA/TKIP ve EAP-TLS
- WPA/TKIP ve PEAP-MS-CHAP v2

Kullanımı sadece WPA2 veya WPA'ya geçiş aşamasında tavsiye edilen güvenlik standartları (sırasıyla şifreleme ve kimlik doğrulama) güçlüden zayıfa doğru sıralanan şekilde:

- WPA2/AES ve WPA2-PSK
- WPA2/TKIP ve WPA2-PSK
- WPA/TKIP ve WPA2-PSK

Kesinlikle kullanılmaması gereken güvenlik standartları ise:

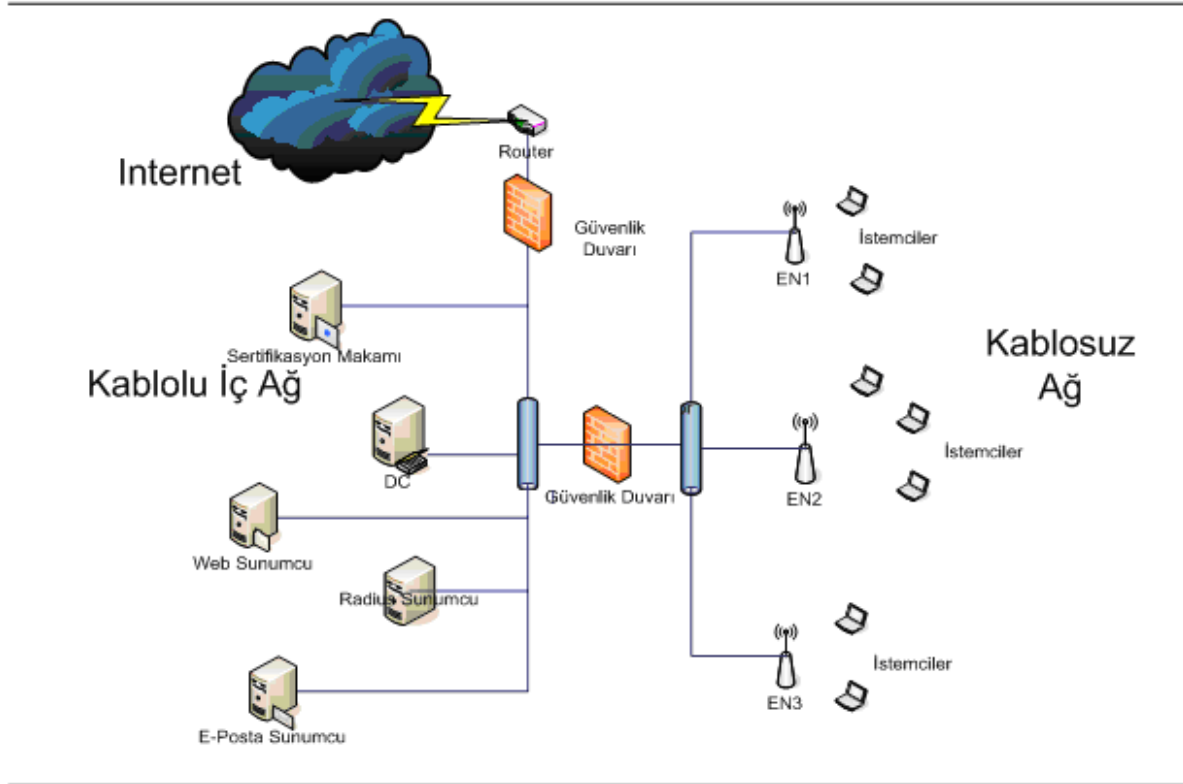
- WPA-PSK
- WEP ve Açık Kimlik Doğrulama
- WEP ve Paylaşılmış Anahtarlı Kimlik Doğrulama
- Hiçbir güvenlik önleminin alınmadığı durum

Aşağıda kablosuz ağ güvenlik konfigürasyonlarının Windows etki alanı bulunan bir yapıda nasıl uygulanacağı örnek bir konfigürasyonla anlatılmaktadır. Bu kısımda kurum ağında Windows 2003 SP2 yüklü bir etki alanı sunucusu olduğu ve kullanıcıların Windows XP SP2 yüklü ve WPA2 güncellemesi yapılmış istemci bilgisayarlarından ilgili etki alanına ait kullanıcı hesapları kullanarak kablosuz ağa bağlanacakları kabul edilmiştir.

5.1 Mimari Topoloji

- Ağda domain yapısı kurulması gereklidir.
- Sunumcuların kablolu ağ bölümünde bulunması gereklidir.
- Erişim noktaları ile kablosuz ağ arasında bir güvenlik duvarı olması gereklidir.
- İnternet açılan güvenlik duvarı ve yönlendirici üzerinde gerekli güvenlik önlemlerinin alınmış olması gerekmektedir.
- Kablolu ağda bulunan sunumcularda ve kablolu kablosuz ağ arasındaki güvenlik duvarında gerekli güvenlik ayarları yapılmalıdır.
- Aşağıda örnek bir ağ şeması verilmiştir.

Kablosuz İnternet Ağı Şeması



Şekil 5.1 – Kablosuz Ağ Topolojisi

5.2 Gerekli Bileşenler:

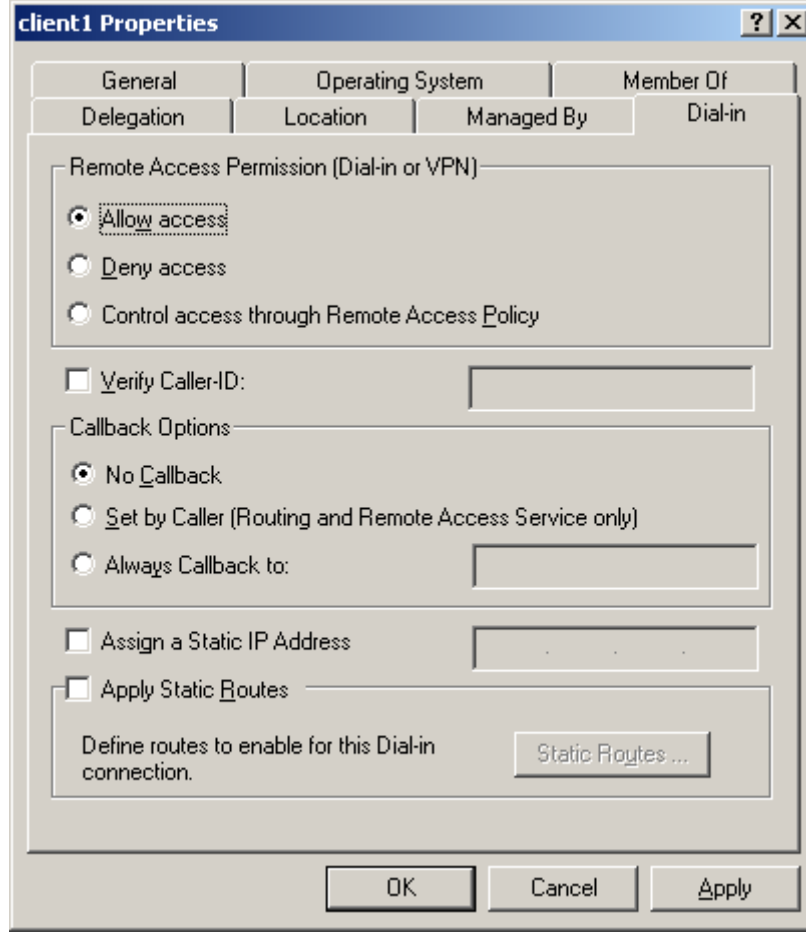
- Etki alanı kontrolcüsü (Windows 2003 SP2) :
- RADIUS Sunumcusu – **Microsoft Internet Authentication Service (IAS)**.
- Sunumcu Sertifikası (Kurum sertifikasyon makamından ya da bir sertifika sağlayıcılardan alınmış)

- İstemci bilgisayarları (Windows XP SP2, WPA2 güncellemesi yapılmış)
- Erişim Noktaları (WPA2 destekleyen)

5.3 Etki Alanı Kullanıcı Hesapları ve Grup Ayarları:

- Windows 2003 etki alanı kontrolcüsü kullanılıyor ise Service Pack 2 yüklenir
- “Kablosuz Kullanıcılar” kullanıcı grubu (**universal** ya da **global group**) yaratılır, gerekli kullanıcılar eklenir.
- Kablosuz Bilgisayarlar bilgisayar grubu(**universal** ya da **global group**) yaratılır, ilgili bilgisayar hesapları eklenir.
- Kablosuz bağlantı yapılacak bilgisayarlar etki alanına üye yapılır.
- İlgili kullanıcı ve bilgisayar hesapları için:

Active Directory Users and Computers snap-in > İlgili Kullanıcı/Bilgisayar Hesabı > **Properties** > **Dial-in tab** > **Remote Access Permission (Dial-in or VPN)**
: **Allow access** veya **Control access through Remote Access Policy** seçilir.

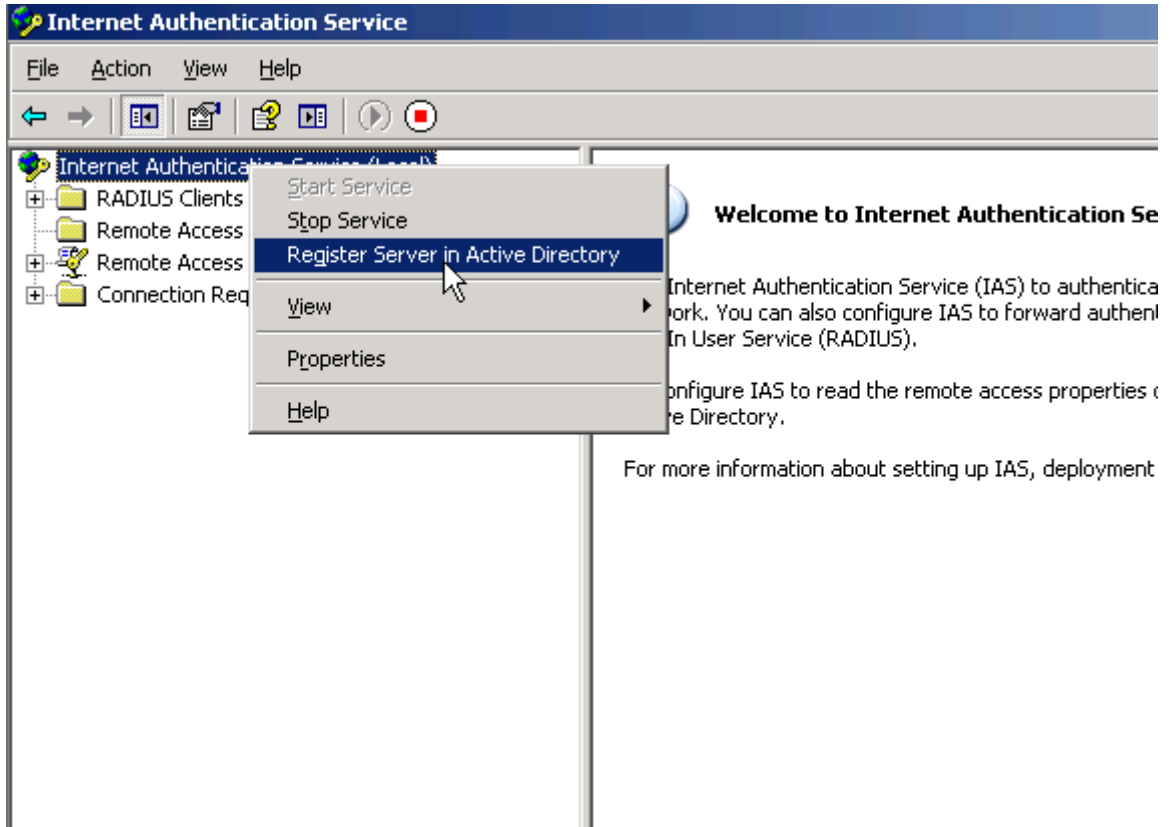


Şekil 5.2 – Oluşturulan Kullanıcı Hesabı Ayarları

5.4 IAS Sunumcu Ayarları:

- Aşağıda belirtilen adımların uygulanması için sunumcuya “**domain administrator**” haklarına sahip bir kullanıcı ile bağlanması gerekmektedir.
- İlk adım olarak IAS sunumcusunun sunumcu sertifikasının yüklenmesi işlemi gerçekleştirilir.
 - Etki alanında kurulu bir CA bulunuyorsa
 - Otomatik (**autoenrollment**) olarak,
 - IAS sunumcusu **Certificates snap-in** üzerinden yeni bilgisayar sertifikası talebinde bulunarak (**Request New Certificate**)
 - CA üzerinde oluşturulmuş sertifika IAS sunumcuya **Certificates snap-in** üzerinden **Import** edilerek.

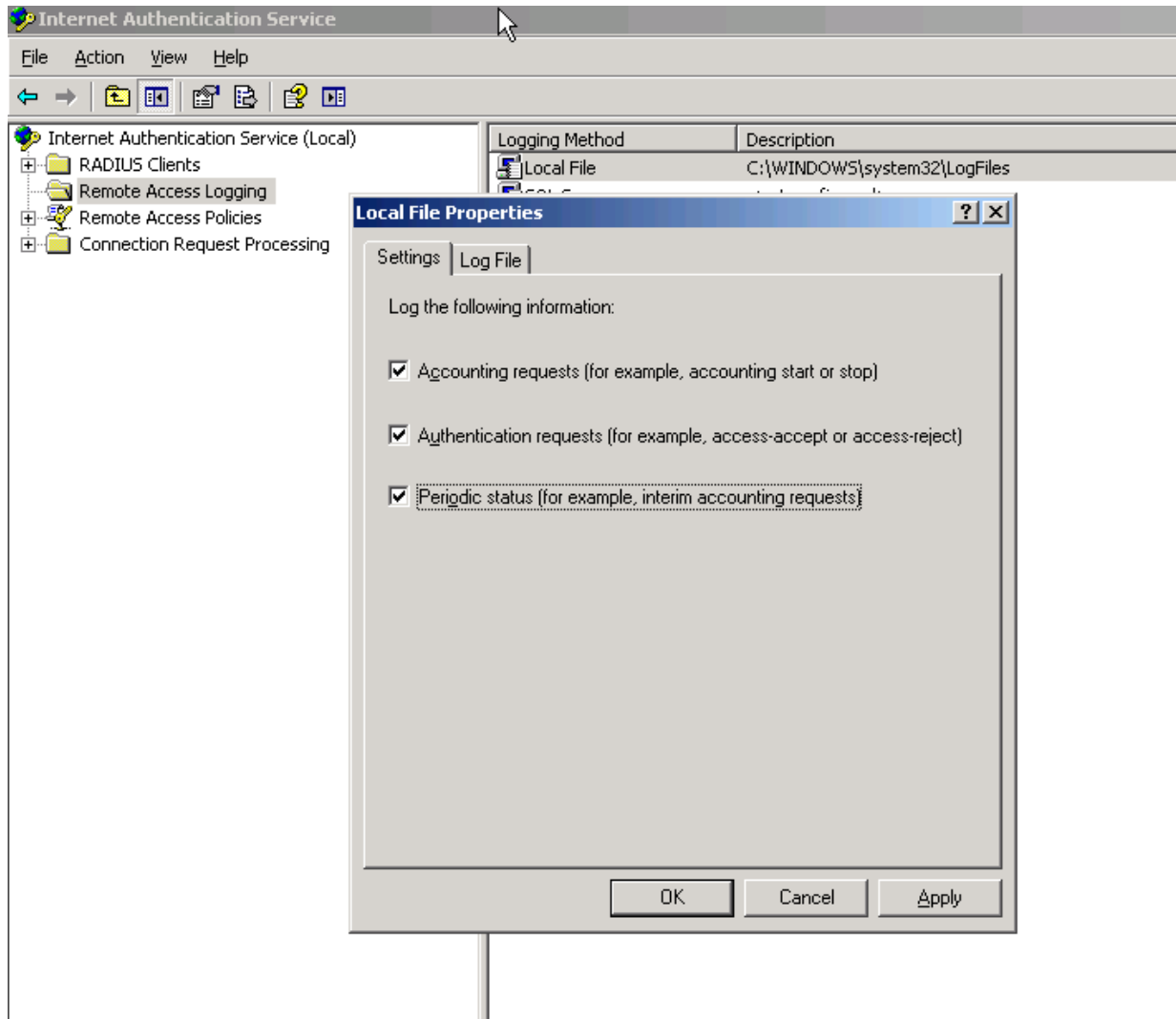
- Ticari sertifika (Verisign vb.) kullanımı durumunda alınmış sertifika IAS sunumcu **Certificates snap-in** üzerinden **Import** edilir.
- IAS servisi kurulur.
Add Remove Programs > Windows Components > Optional Networking Components > Internet Authentication Service
- IAS servisi etki alanı kontrolcüsü üzerine kurulmadı ise, IAS servisinin etki alanındaki kullanıcı ve bilgisayar hesapları bilgilerine erişim izni verilmesi gerekmektedir.
 - **Start > Administrative Tools > Internet Authentication Service snap-in > Internet Authentication Service(Local) > “Register Server in Active Directory”** seçilir.
 - **“Register Internet Authentication Service in Active Directory”** penceresinde **“OK”** tıklanır.



Şekil 5.3 – IAS Yapılandırması

- Analiz ve olay sonrası güvenlik incelemeleri için bağlantı istekleri hakkında kayıt tutulması:

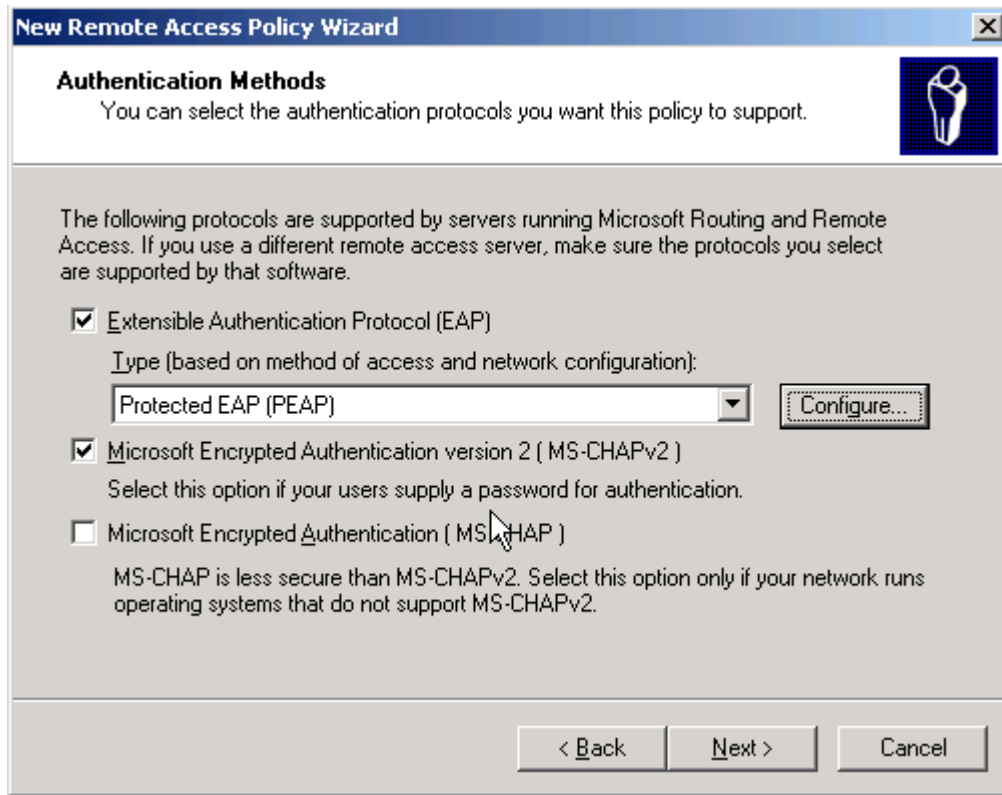
- **Internet Authentication Service snap-in > Internet Authentication Service(Local) > Properties > General** sekmesi altında:
“Rejected Authentication Requests” ve **”Successful Authentication Requests”** seçenekleri seçili konumda olmalıdır.
- **Internet Authentication Service snap-in > Remote Access Logging** altında istenilen (Local File veya SQL veritabanı) kayıt saklama yöntemi seçilir ve konfigüre edilir. Örneğin **Local File**'a tıklanır, **Settings** sekmesi altında ve **“Accounting Requests, Authentication requests, Periodic Status”** seçenekleri seçilir.



Şekil 5.4 – IAS Yapılandırması II

- **Log File** sekmesi altında kayıt dosyalarının tutulacağı yer, yeni kayıt dosyası yaratma sıklığı ve sabit diskin dolması durumunda yapılacak işlem ayarları yapılabilmektedir.
- Bir sonraki aşamada “**RADIUS Clients**” altında IAS tarafından isteklerine cevap verilecek erişim noktaları ile ilgili ayarlar yapılacaktır. Her bir erişim noktası için aşağıda belirtilen ayarlar yapılmalıdır.
 - **RADIUS Clients > New RADIUS Client** seçilir
 - Erişim noktasını tanımlayıcı bir isim (SSID olabilir), IP ve Erişim noktası ile IAS sunumcunun birbirini doğrulamak ve trafiği şifrelemek için kullanacağı şifre “**Shared Secret**” bilgileri girilir. Şifre büyük, küçük harf, sayı ve diğer karakterlerden oluşmalı, en az 22 karakter uzunluğunda olmalıdır. **Client-Vendor** kısmına biliniyorsa ve listede varsa EN üreticisinin ismi girilir, bilinmiyorsa RADIUS Standard olarak bırakılır. Ayrıca eğer EN, **Message Authentication Code** özelliğini desteklemiyor ya da bilinmiyorsa **Request must contain Message Authentication Code** seçeneği seçilmemiş olmalıdır. IAS ve EN’ler arasındaki RADIUS mesaj trafiğinin gizliliği, bütünlüğü ve kimlik kontrolü için IPsec kullanımı tavsiye edilmektedir.
- EN’lerden gelecek kimlik doğrulama/yetkilendirme isteklerinin hangi kriterlere göre değerlendireceğini **Remote Access Policy**’ler belirlemektedir. IAS kurulumu ile 2 adet politika gelmektedir. Bu politikalar tüm istekleri reddedecek şekilde ayarlanmıştır. Politikalar listedeki sıralarına göre uygulanırlar, en üstteki ilk uygulanan politikadır. Bir istek politikada belirtilen kriterlere uyuyorsa diğer tanımlanmış politikalar o istek için uygulanmaz. Yeni bir politika yaratmak için:
 - **Internet Authentication Service snap-in > Remote Access Policies > New Remote Access Policy > New Remote Access Policy Wizard**
 - Politika ismi girilir, **Next**’e tıklanır.
 - **Access Method** olarak **Wireless** seçilir.
 - **User or Group Access** kısmında **Group** seçilir ve *Kablosuz Kullanıcılar* grubu eklenir.

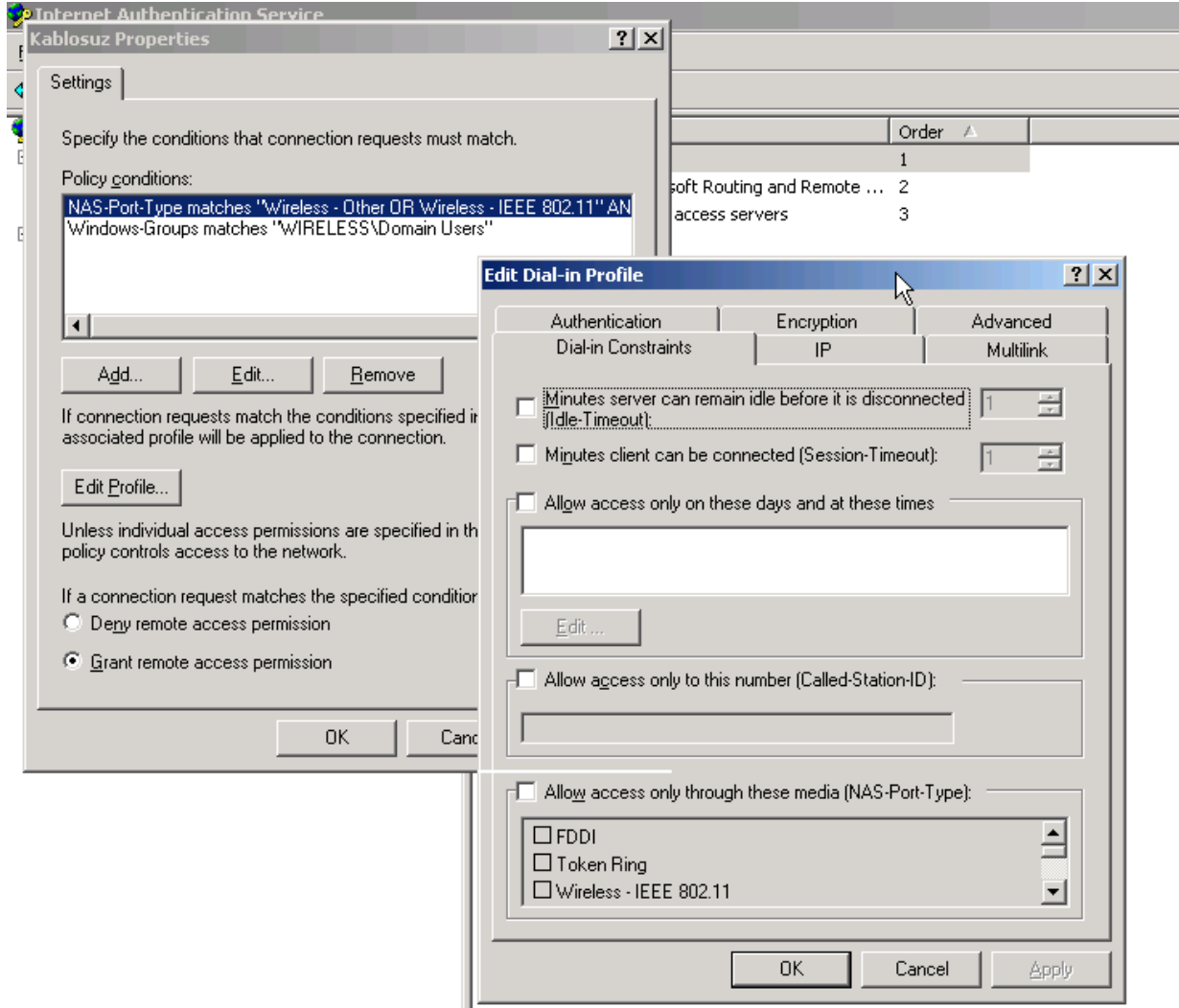
- **Authentication Methods** kısmında **Extensible Authentication Protocol**'e tıklanır ve **Type** listesinden **Protected EAP (PEAP)** seçilir. Type olarak seçilebilecek bir başka seçenek **Smart Card and other certificates (EAP-TLS)**'tir. Fakat o durumda tüm kablosuz olarak bağlanacak tüm bilgisayarlara sertifika dağıtma gereksinimi vardır. Eğer etki alanında bir Sertifikasyon Makamı kurulmuş ise ve kurum politikası olarak sadece sertifika yüklenmiş, kuruma ait bilgisayarların kablosuz ağ bağlantısı yapması isteniyorsa **Type** olarak **Smart Card and other certificates** seçilir ve tüm istemcilere sertifika yüklenmesi sağlanır. Örneğimize PEAP seçilmiş olarak devam ediyoruz. **MS-CHAPv2** seçili olarak kalır ve **Next**'e tıklanır.



Şekil 5.5 – “Remote Access” Politika Sihirbazı

- **Policy Encryption Level** EN ile ISA sunumcunun **RADIUS** mesajlaşma trafiğinin güvenliğini sağlamak için kullandıkları şifrelemenin gücünü belirtir. EN'lerin bunlardan hangilerini desteklediğini bilmiyorsak hepsi seçili olarak bırakılır ve **Finish**'e tıklanır. Eğer destekleniyorsa **Strongest Encryption** seçeneği seçilir.

- Politika tanımlama işlemi tamamlandıktan sonra **Remote Access Policies** altında **Wireless** politikasının birinci sırada yer aldığı görülür, yani ilk uygulanacak politikadır, mevcut tüm istekleri reddeden politikalar **Wireless** politikasına uyan istekler için uygulanmayacaktır. **Wireless** politikasında **Remote Access Policy Wizard**'la yaptığımız ayarlara ek ayarlar yapılabilmektedir. Politika üzerine çift tıklanarak yapılabilecek ayarlar görülebilir. **Edit Profile**'a tıklanarak birçok detaylı ayar yapılabilir.



Şekil 5.6 – “Remote Access” Politika Yapılandırması

- **Connection Request Processing** kısmında **Proxy IAS** sunumcular kullanılması durumunda yapılması gereken ayarlar bulunmaktadır. Varsayılan politika gelen isteklerin mevcut IAS sunumcu tarafından değerlendirilmesidir, bu ayar değiştirilmeyecektir.

5.5 Erişim Noktası Konfigürasyonu:

Erişim noktalarının konfigürasyonu üretici firmalara ve EN'nin modeline göre farklılıklar gösterebilmektedir. Genel olarak yapılacak işlemler şunlardır:

- Erişim noktası SSID (**Service Set ID**, kablosuz istemcilerin kablosuz ağ ayarlarında bağlanmak istedikleri EN'yi belirtmek için girdikleri isim) girilir. **Disable Broadcast SSID** seçeneği seçilerek Güvenlik için SSID bilgisinin EN **Beacon** paketlerinde yayınlanması engellenir. SSID yönetim kolaylığı açısından sistem yöneticilerine EN'nin konumu hakkında bilgi veren bir isim olabilir, fakat saldırganların dikkatini çekecek, kurum adı vb. bilgiler içeren isimlerden kaçınılmalıdır.
- Şifreleme için **WPA2/AES** seçilir. **WPA2/AES** desteklenmiyorsa, **TKIP** seçilir.
- Kimlik doğrulama için **WPA/802.1x** seçilir, **RADIUS/IAS** sunumcunun IP, Port (varsayılan değerler kabul edilir, UDP 1812, 1645), **Shared Secret** bilgileri girilir.
- Erişim noktalarının yönetimi sadece konsol ya da kablolu ağ üzerinden yapılabilmesi, kablosuz arayüzden yönetim için erişim engellenmelidir.
- Erişim noktalarının yönetiminde **ssh**, **https** gibi şifreli haberleşme protokolleri kullanılmalıdır.
- Erişim noktalarına yönetim için kullanılan kullanıcı ismi ve şifresi varsayılan değerinden farklı olmalı, şifre karmaşık olmalıdır.

Bu örnek senaryoda bir adet Cisco EN'ye sahip olduğumuzu kabul edeceğiz:

- **Express Setup** seçilir.
- **Server Manager** kısmına girilir.
 - **Corporate Servers** bölümünde IAS sunumcunun IP adresi girilir.
 - **Shared Secret** olarak IAS üzerinde girilen en az 22 karakter uzunluğundaki şifre girilir. **Apply**'a basılarak
- **SSID Manager** kısmına girilir.
 - **Radio Service Set ID** (SSID) kısmına kablosuz istemcilerin göreceği EN ismi girilir.
 - VLAN değeri "1" girilir.

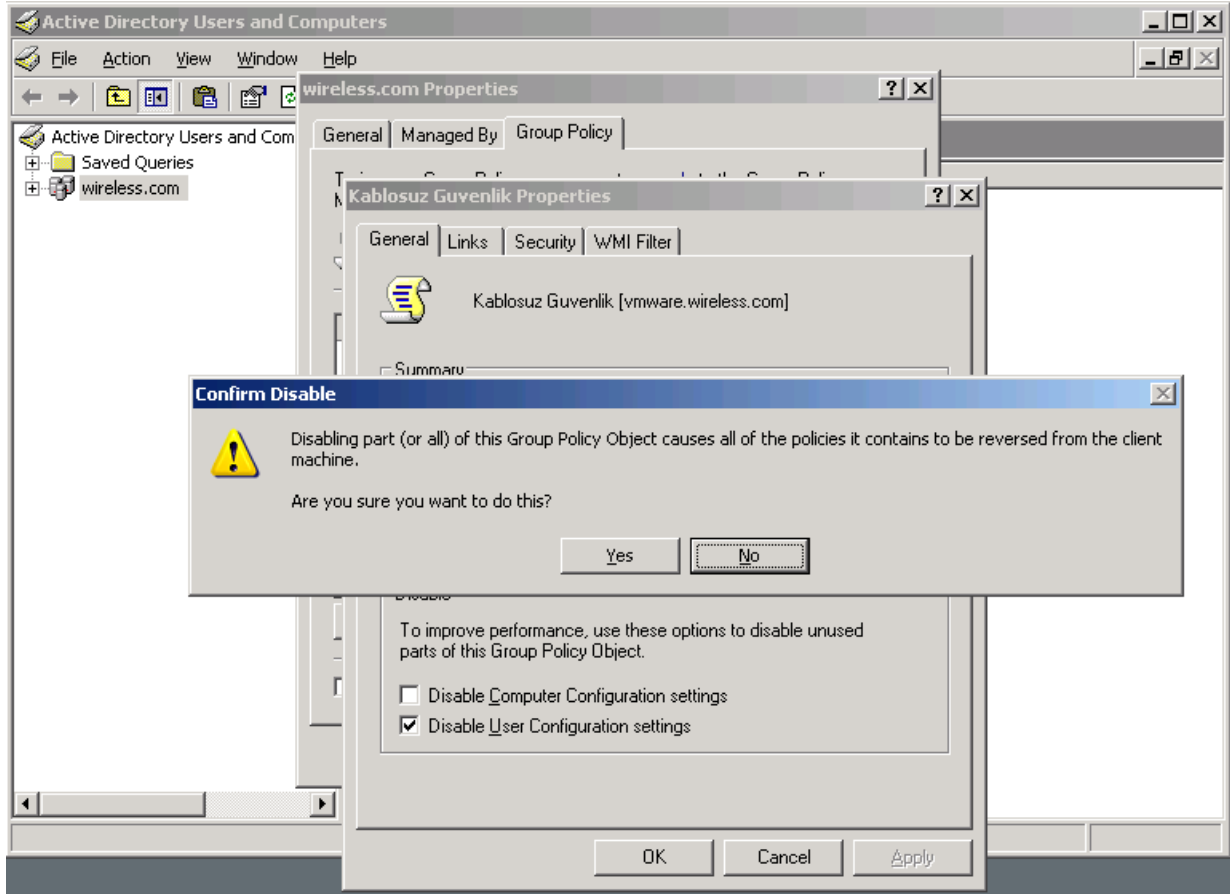
- **Authentication Key Management** altında, "**Key Management**" değeri "**Mandatory**" olarak seçilir ve **WPA**'e tıklanır. **Apply**'a basılır.

- **Encryption Manager** kısmında **Cipher** ve **TKIP** seçilir. **Apply**'a basılır.

5.6 Kablosuz Ağ (802.11) Grup Politikası Ayarları:

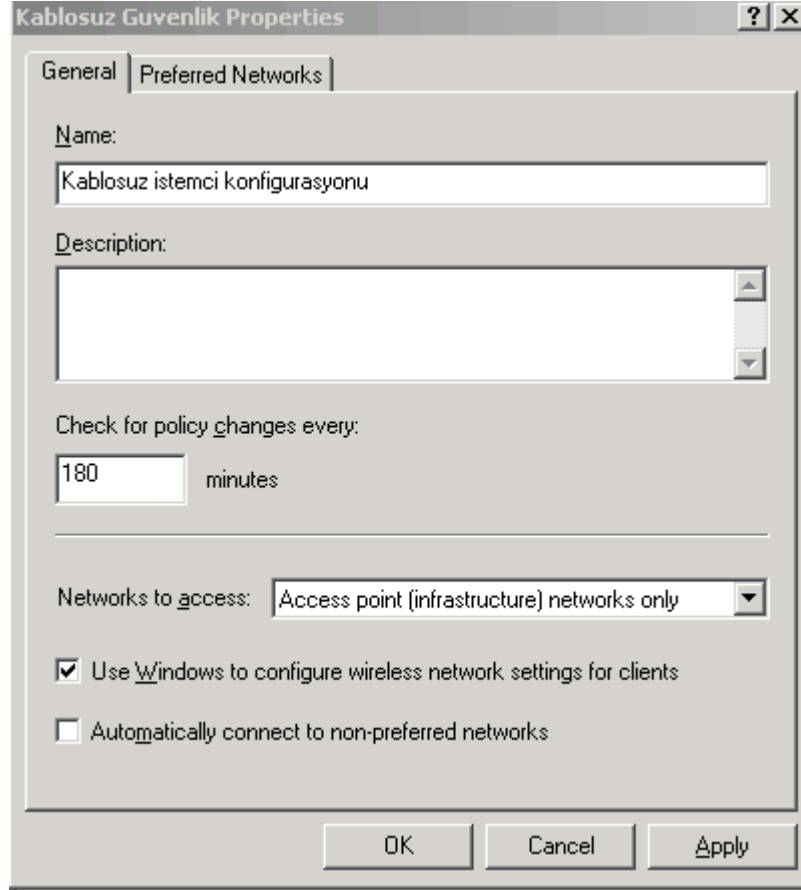
Çok sayıda kablosuz ağ kullanıcısının olduğu durumlarda, kullanıcı bilgisayarlarında kablosuz ağ bağlantı ve güvenlik ayarlarının her bir bilgisayar için elle yapılması mümkün olmayabilir. Daha da önemlisi kablosuz ağ güvenlik ayarlarının kullanıcılar tarafından değiştirilebiliyor olması tüm ağ için büyük risk doğurmaktadır. Kullanıcıların yapılan güvenlik ayarlarını zayıflatmasını engellemek ve tüm kablosuz bilgisayarlarda standart ayarları merkezi olarak yapabilmek için Windows etki alanı grup politikaları kullanılabilir. Etki alanına üye olmayan bilgisayarların ayarları ise elle yapılacaktır.

- Windows 2003 Server etki alanı kontrolcüsü üzerinde **Active Directory Users and Computers MMC snap-in**'i açılır.
- Etki alanına üzerine sağ tıklanıp **Properties** seçilir ve Grup politikası sekmesi açılır. **New**'e tıklanarak Kablosuz Ağ Politikası ismiyle yeni bir grup politikası yaratılır.
- **Kablosuz Ağ Politikası > Properties**'e tıklanır, General sekmesinde **Disable User Configuration Settings** seçilir ve uyarı mesajında **YES** tıklanır.



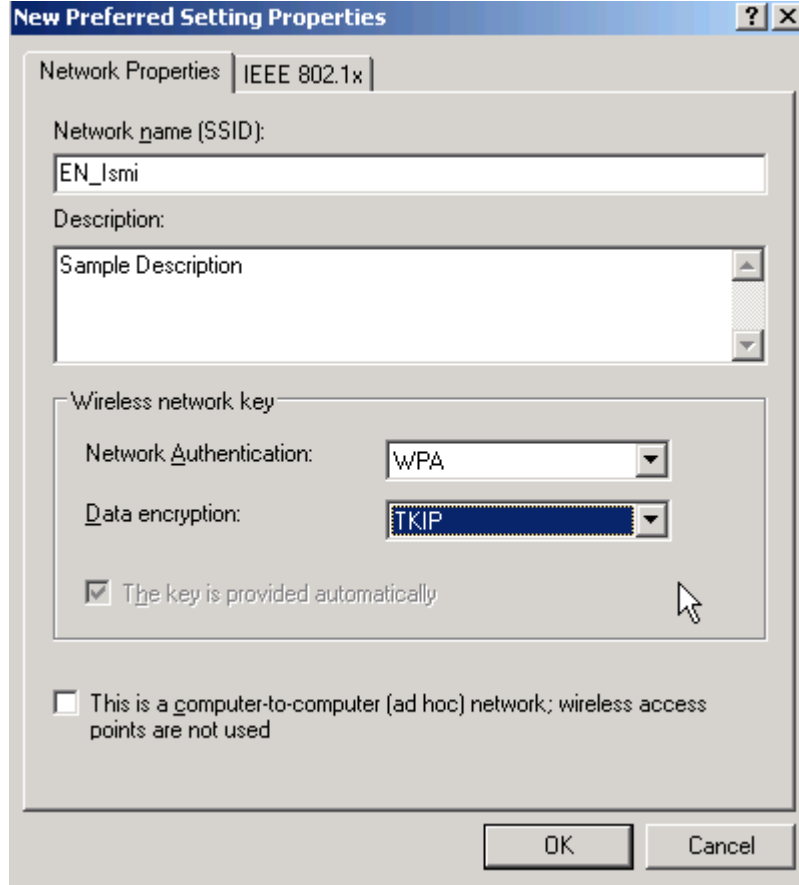
Şekil 5.7 – “Active Directory” Grup Politikası Yapılandırması

- Kablosuz Ağ Politikası > **Edit**'e tıklanır ve **|Computer Configuration\Windows Settings\Security Settings\Wireless Network (IEEE 802.11) Policies** açılır.
- **Action** menüsünden **Create Wireless Network Policy** seçilir. “Kablosuz istemci konfigürasyonu” ismi verilir ve **Finish**'e tıklanır.
- “Kablosuz istemci konfigürasyonu”na çift tıklanır. Açılan pencerede **Networks to Access** kısmında **Access Point (infrastructure) Networks only** seçilir.



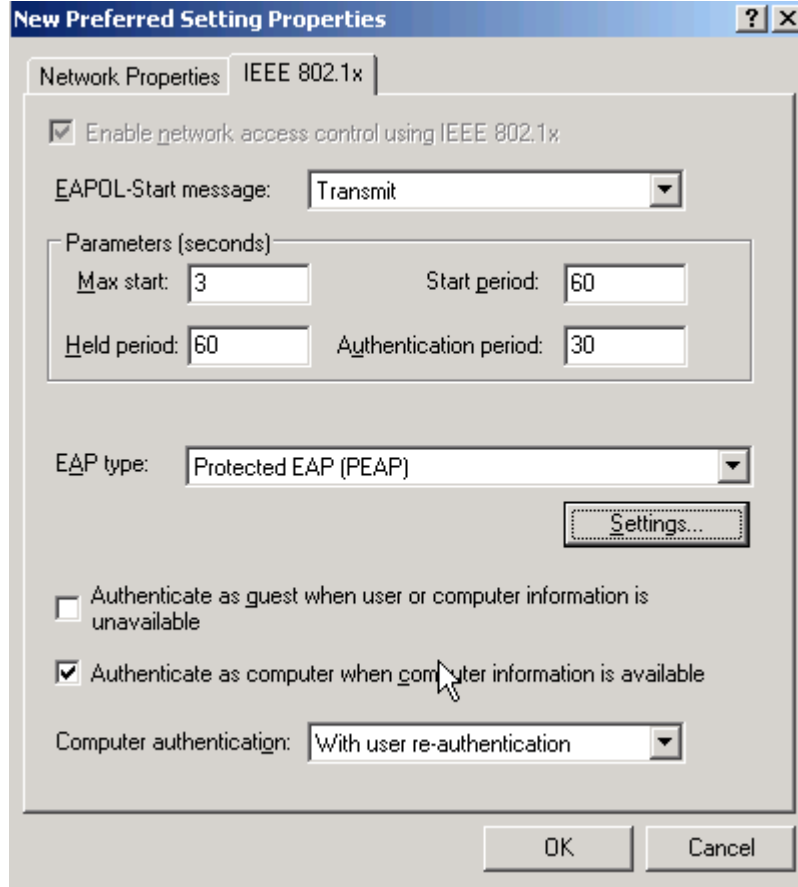
Şekil 5.8 – Grup Politikası ile Kablosuz İstemci Konfigürasyonu (Genel)

- **Preferred Networks** sekmesinde **Add**'e tıklanarak bağlanılması istenen erişim noktası SSID ve güvenlik ayarları girilir.
 - **Network Properties** sekmesinde **ssid** bilgisi girilir. **Network Authentication** için **WPA2**, **Data Encryption** için **AES** seçilir.



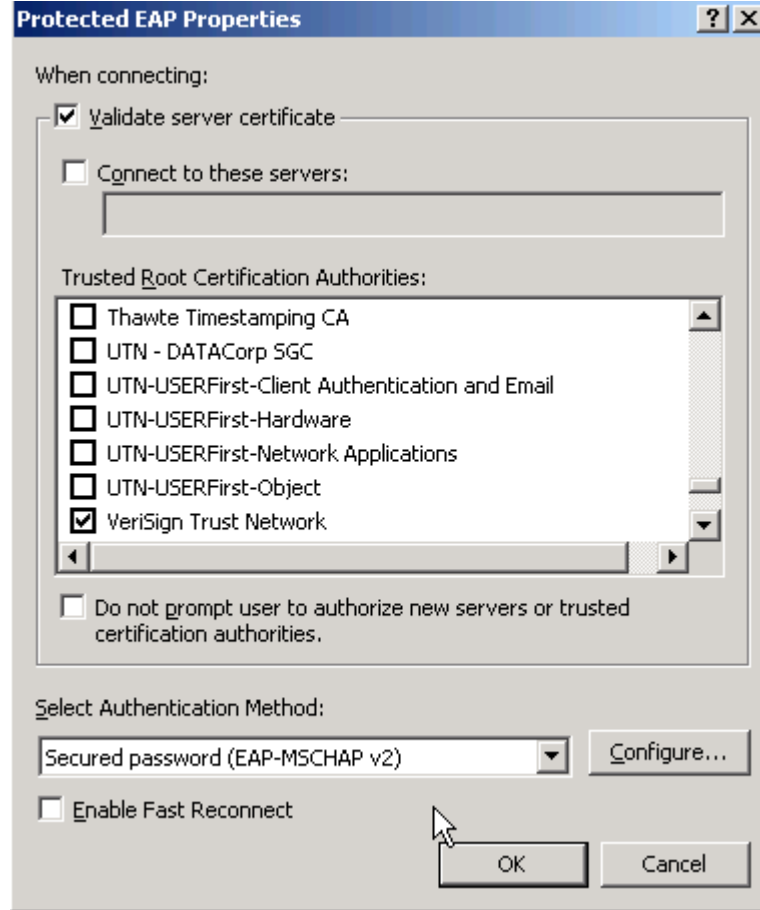
Şekil 5.9 – Grup Politikası ile Kablosuz İstemci Konfigürasyonu (Kimlik Doğrulama, Şifreleme)

- o **IEEE 802.1X** sekmesinde **Protected EAP** seçilir, **settings**'e tıklanır.



Şekil 5.10 – Grup Politikası ile Kablosuz İstemci Konfigürasyonu (802.1x)

- **Trusted Root Certificate Authorities** kısmında IAS sunumcu sertifikasını düzenleyen CA seçilir. **Finish**'e tıklanır.

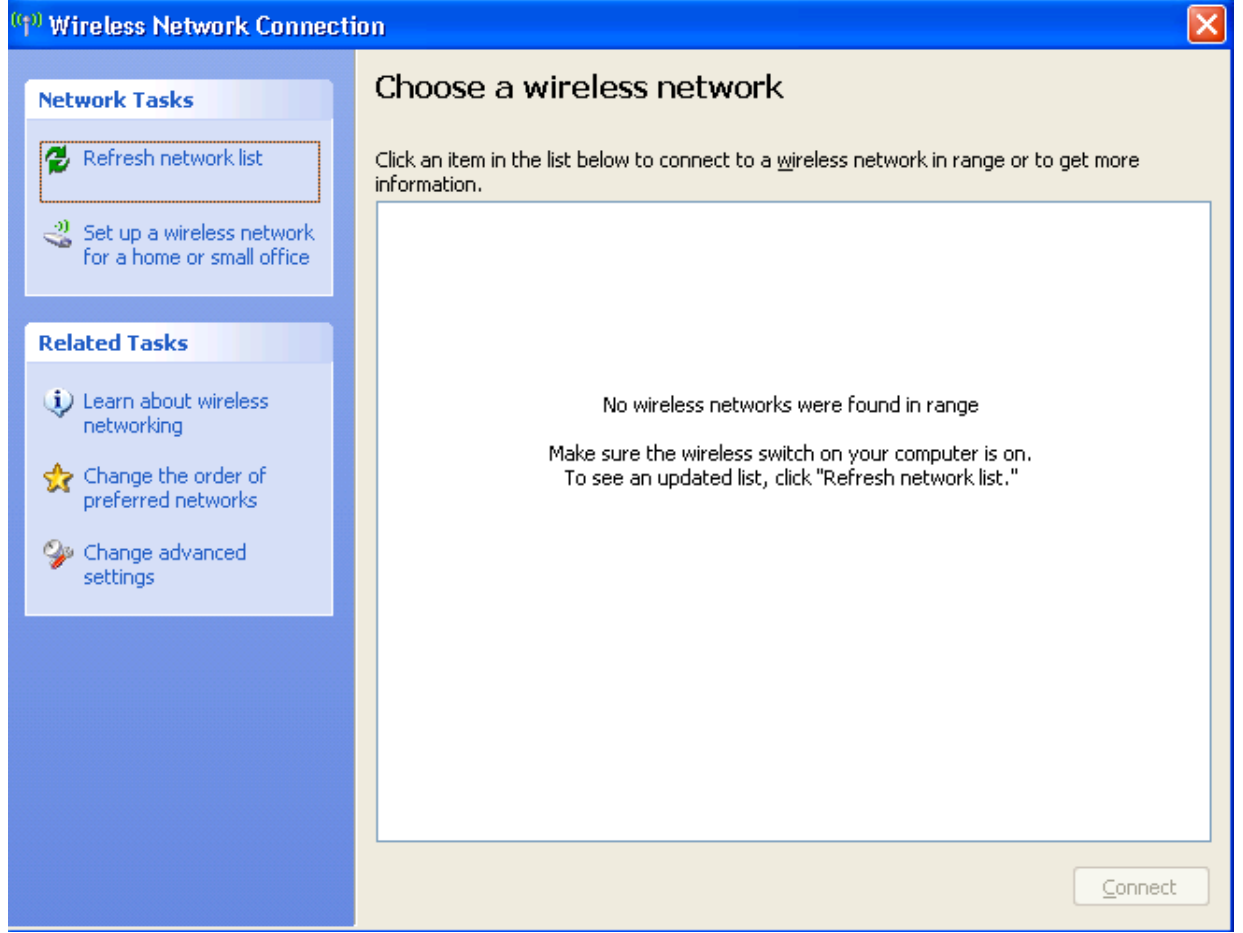


Şekil 5.11 – Grup Politikası ile Kablosuz İstemci Konfigürasyonu (PEAP Yapılandırması)

5.7 Kablosuz İstemci Ayarları:

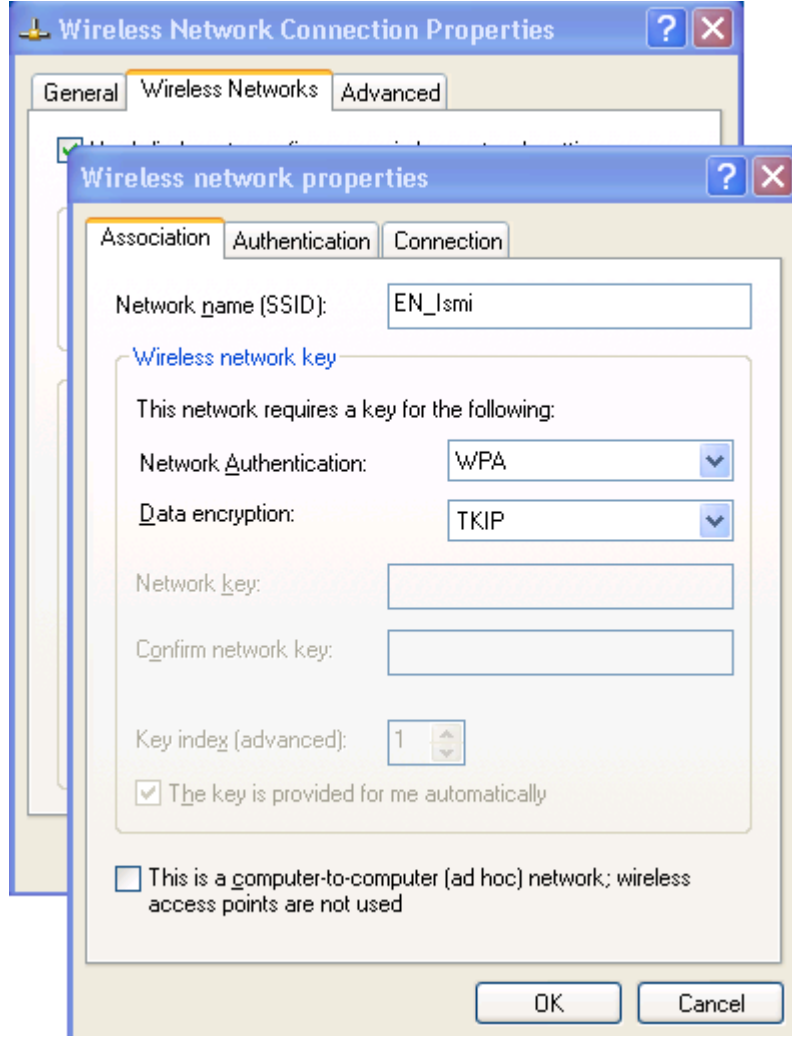
Etki alanı üyesi olmayan fakat kablosuz ağa bağlanacak bilgisayarlarda şu ayarlar yapılır:

- Windows kablosuz bağlantı ayarları açılıp, **Change Advanced Settings**'e tıklanır.



Şekil 5.12 – Kablosuz İstemci Konfigürasyonu

- Açılan **Wireless Network Connection Properties** penceresinde **Wireless Networks** sekmesine tıklanır ve **Add**'e basılır. **SSID** ismi, **Network Authentication** için **WPA** ve **Data Encryption** için **TKIP** seçilir.



Şekil 5.13 – Kablosuz İstemci Konfigürasyonu (Kimlik Doğrulama - Şifreleme)

- **Authentication** sekmesinde **Protected EAP** seçilir, **Properties**'e tıklanır. **Trusted Root Certificate Authorities** kısmında IAS sunumcu sertifikasını düzenleyen **CA** seçilir. **Finish**'e tıklanır.
- Kablosuz ağa bağlanacak kullanıcı bilgisayarlarında aşağıda belirtilen şartların sağlanması gerekmektedir:
 - İşletim sistemi yamalarının güncel olması,
 - Antivirüs yazılımının güncel virüs tanımları yüklü olarak çalışıyor konumda olması,
 - Güvenlik duvarının aktif olması

6. KABLOSUZ AĞLARDA ALINACAK GÜVENLİK ÖNLEMLERİ

6.1 Güvenlik Politikası

- Kullanıcıların kullanılan güvenlik önlemleri konusunda bilgilendirilerek belli güvenlik önlemlerini yanlışlıkla kapatmaları önlenmelidir.
- Kullanıcı bilgisayarlarında; kablosuz bağlantı sırasında, ethernet ara yüzünden kablolu ağa bağlanılmamalıdır. Aksi takdirde kullanıcı bilgisayarını kablosuz ağ ile kablolu ağ arasında köprü (**bridge**) işlevi görebilir.
- Erişim noktaları, kablosuz köprü cihazları çalıntı veya müdahaleye olanak tanımayacak şekilde yerleştirilmelidir.
- Kayıp veya çalınmış dizüstü bilgisayarlar ve kablosuz ağ adaptörleri en kısa zamanda bildirilmelidir.
- Bina yakınlarında güçlü antenler kullanılarak kablosuz ağın dinlenilmesi mümkün olabilir, bu sebeple tesis güvenliğinden sorumlu personelin bu hususta bilgilendirilmesi gereklidir.
- Kullanıcıların bilgisayarlarına donanım eklemeleri ya da yazılım yüklemeleri engellenmelidir.
- Kullanıcıların ağ ayarlarını değiştirmemelidir
- Kablosuz **Ad-Hoc** bağlantıya izin verilmemelidir.

7. EK GÜVENLİK ÖNLEMLERİ

7.1 Erişim Noktası Fiziksel Güvenliği

Birçok erişim noktası üzerinde olası kurtarma / geri alma eylemleri için yönetim konsol bağlantı arayüzü bulunmaktadır. Bu tür bağlantı bulunmayan erişim noktalarında ise **reset** düğmesi bulunmaktadır. Bunların her ikisine de yetkisiz erişim sonucu kötü niyetli eylemler gerçekleştirilebilir. Bu sebeple erişim noktasının konumlandırılacağı yerin kararı verilirken bu durum değerlendirilmelidir. Erişim noktasını güvenlik kameralarının görüş alanına yerleştirmek, erişim noktasının antenini harici olarak kullanarak erişim noktasının görünür bölgeden uzaklaştırılması (alçaltılmış tavanda bulundurulması) alınabilecek önlemler arasında sayılabilir.

7.2 VPN Uygulaması

Her ne kadar AES-CCMP güvenlik çözümünün uygulanması WEP ve TKIP'a oranla yüksek seviyede güvenlik sağlıyorsa da, AES-CCMP'nin kullanımında ortaya çıkabilecek olası aksamalara (kablosuz ağ bağdaştırıcısı ya da erişim noktası donanımın AES şifrelemeyi desteklememesi, işletim sisteminde ayar yapılamaması, etki alanı seviyesinin grup ilkeleri ile güvenlik ayarı yapmaya elverişli olmaması vb.) karşı önlem olarak VPN ile ikinci bir güvenlik katmanının gerçekleştirilmesi tavsiye edilmektedir. VPN uygulaması, istemciler ile erişim noktalarının arkasında bulunacak bir VPN konsantratör arasında olacaktır.

7.3 Saldırı Tespit ve Önleme Sistemleri

Şifreleme, yetkilendirme, protokol filtreleme vb. güvenlik tedbirleri önleyici faaliyetler olmakla birlikte uygulanan güvenlik tedbirlerinde çıkabilecek yeni güvenlik açıklıklarının kötüye kullanılması suretiyle sisteme saldırılar mümkün olabilmekte, güvenlik önlemlerinin yanlışlıkla ya da bilinçli olarak devreden çıkarılabilmektedir. Ayrıca alınan güvenlik tedbirleri kuruma ait olmayan erişim noktalarının ortamda bulunmasını önlememektedir. Bu tür tehditlerin fark edilmesi ve zamanında müdahale edilmesi, kablosuz erişimin gerçekleştiği ortamı sürekli monitör eden, bilinen saldırı çeşitlerinin gerçekleşmesi durumunda alarm veren, yetkisiz erişim noktalarını ve istemcileri tespit eden bir gerçek zamanlı saldırı tespit sisteminin bulunmasını gerektirmektedir.

Ayrıca kablosuz ağı yapılan yetkisiz erişimleri tespit edip, kurulan bağlantıları koparma (**de-authentication**) veya buna benzer işlemleri gerçekleştirebilecek bir saldırı önleme sistemi kullanılmalıdır.

7.4 Periyodik Testler

Sistem kullanılmaya başlanmadan önce sinyal güç analizini kapsama alanı analizi ve güvenlik testleri mümkünse **bağımsız uzman kuruluş/kişilere** yaptırılmalıdır. İlgili testlerin **periyodik hale getirilmesi tavsiye edilmektedir.**

8. TAVSİYELER

Bu raporda belirtilen güvenlik önlemleri belirtilen güvenlik protokollerinde ilerleyen dönemlerde ortaya çıkabilecek yeni açıklıklarla risklerin karşılanmasında yetersiz kalabilir, bu yeni çıkan açıklıkların takibi ve kurulacak sistemin periyodik testlerle denetlenmesi tavsiye edilmektedir. Ayrıca burada kullanılacak ürünler ve yazılımlar konusunda herhangi bir tavsiyede bulunulmamaktadır, ilgili ürünlerin olası güvenlik açıklıkları dikkate alınmalıdır.

KAYNAKÇA

- [1] IEEE P802.11 - task group n - meeting update :
<http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm>
- [2] Mark Levitt and Brian E. Burke, *Choosing the Best Technology To Fight Spam*, IDC, April 2004
<http://www.commtouch.com/documents/040429_IDC_Choosing%20_the%20_Best%20_AS_Technology.pdf>
- [3] <http://www.broadbandreports.com/shownews/38004>
- [4] Kurt, A., *Genişbant Telsiz Erişim Hizmeti Yetkilendirmesi Çalışmaları ve WiMAX Teknolojisi, Bilgi Notu*, Telekomünikasyon Kurumu, Ankara. 2006
- [5] IEEE 802.16 Standard— Local and Metropolitan Area Networks — Part 16, IEEE Std 802.16a-2003, 2003