

BİLGİSAYAR AĞI GÜVENLİK  
SİSTEMİNİN ÇOK ÖLÇÜTLÜ SEÇİMİ  
ve AHP UYGULAMASI

Kürşat İLHAN

Yüksek Lisans Tezi

Endüstri Mühendisliği Anabilim Dalı

Mayıs - 2009

BİLGİSAYAR AĞI GÜVENLİK  
SİSTEMİNİN ÇOK ÖLÇÜTLÜ SEÇİMİ  
ve AHP UYGULAMASI

Kürşat İLHAN

Dumlupınar Üniversitesi  
Fen Bilimleri Enstitüsü  
Lisansüstü Yönetmeliği Uyarınca  
Endüstri Mühendisliği Anabilim Dalında  
YÜKSEK LİSANS TEZİ  
Olarak Hazırlanmıştır.

Danışman :Yrd. Doç. Dr. Mustafa TÜRENGÜL

Mayıs - 2009

## KABUL ve ONAY SAYFASI

Kürşat İLHAN'nın YÜKSEK LİSANS tezi olarak hazırladığı "BİLGİSAYAR AĞI GÜVENLİK SİSTEMİNİN ÇOK ÖLÇÜTLÜ SEÇİMİ VE AHP UYGULAMASI" başlıklı bu çalışma, jürimizce lisansüstü yönetmeliğin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

20 / 05 /2009

(Sınav tarihi)

Üye : Yrd. Doç. Dr. Mustafa TÜRENGÜL (DANIŞMAN)

Üye : Yrd. Doç. Dr. Özden ÜSTÜN

Üye : Yrd. Doç. Dr. Hasan TEMURTAŞ



Fen Bilimleri Enstitüsün Yönetim Kurulu'nun ...../...../..... gün ve ..... sayılı kararıyla onaylanmıştır.

Prof. Dr. A.KÜÇÜKBURSA  
Fen Bilimleri Enstitüsü Müdürü

**BİLGİSAYAR AĞI GÜVENLİK  
SİSTEMİNİN ÇOK ÖLÇÜTLÜ SEÇİMİ  
ve AHP UYGULAMASI**

Yazar: Kürşat İLHAN

Yüksek Lisans Tezi: Endüstri Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. Mustafa Türengül

Mayıs 2009, 118 Sayfa, 25 Kaynak

**ÖZET**

Bu çalışmada; dağınık bir yerleşime sahip, hizmet işletmerindeki bilgisayar ağları niteliğinde değerlendirilen Dumlupınar Üniversitesi Merkez Kampüsün'de karşılaşılan güvenlik problemlerinin çözümüne yönelik olarak kampüs içindeki kablolu ve kablosuz ağlarında otomatik VLAN yapılandırması ve kampüs ağına erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmiştir. Bu kapsamda; kurumsal ağlardaki performans ve servis kalitesi gibi kriterlerin de önemine değinilmiştir. Bilgi sistemi uygulamalarının yaygınlaşması veri ve bilgi güvenliği açısından bazı problemleri beraberinde getirdiği gibi kişisel ve kurumsal bilgilerin gizlilik ve mahremiyeti açısından da sakınca oluşturmaktadır. Bu çalışmada ayrıca, öğrenci/personel kayıtlarının tutulduğu ana sunucu ve uç bilgisayarların yetkilendirme dahilinde kullandırılması, gizlilik ve mahremiyete aykırı uygulamalara mahal verilmemesi bakımından gerekli tüm tedbirlerin alınması konularında da titizlikle çalışılmıştır. Önerilen çözüm yönteminin Kampüs'ün belirli bölgelerinde uygulamaya konulmasıyla sistemin otomatik olarak tek bir noktadan yönetilebilir hale getirilmesi, otomasyon sisteminin durmaksızın maksimum çalışabilirliği ve kullanılan donanım ve yazılım özellikleri ile birçok uygulamanın senkronize bir şekilde işlerliğini sürdürebilmesi yeteneği öngörülmüştür. Bu sayede ağ kaynaklarına erişimi kontrol etmek, ağa içeriden veya dışarıdan yapılması muhtemel saldırıları engellemek ve önemli bilgilere yalnızca izin verildiği ölçüde, izin verilen yetkili kullanıcıların erişimini sağlamak mümkün kılınmıştır. Son bölümde ise Analitik Hiyerarşi Proses'i (AHP) uygulanarak yapılan çalışma modellenmiştir.

**Anahtar Kelimeler:** Analitik Hiyerarşi Prosesi, IEEE 802.1x, Kimlik Doğrulama, Otomatik VLAN, RADIUS, Servis Kalitesi, Veri ve Ağ Güvenliği.

**MULTI-CRITERIA-SELECTION  
OF COMPUTER NETWORK SECURITY SYSTEM  
and AHP APPLICATION**

Submitted by: Kürşat İLHAN

Master Thesis: Industrial Engineering Department

Submitted to: Asst. Prof. Dr. Mustafa Türengül

May 2009, 118 pages, 25 References

**SUMMARY**

In this study, implementation method of automatic VLAN configuration on wired and wireless networks and identity confirmation processes of all users who will be in access to the campus network were used as a solution for security problems faced at Dumlupınar University main campus, with a dispersed settlement, which is evaluated as computer networks in service enterprises. In this context, importance of criteria such as performance and service quality at institutional networks were mentioned. Spreading of data system applications both brings together some problems concerning data and knowledge and has an unfavourable effect in terms of individual and institutional privacy and confidentiality. In this study, subjects related were taken into consideration diligently to take all necessary precautions in order for the main server and computers within which the student / staff records are kept to be used within authorization and to prevent applications against privacy and confidentiality. With the implementation of the proposed solution method to the specific areas of the campus the ability of system's being automatically managed from one point, maximum non-stop interoperability of automation system and sustainability of synchronize operation of many applications with features of hardware and software used were foreseen. Thanks to this, it was enabled to control the access to network sources, prevent possible attacks to network from inside or outside and provide permitted authorized users with access to important data within permission limit.

In the last chapter the study was modelled by implementing Analytical Hierarchy Process (AHP).

**Keywords:** Analytical Hierarchy Process, Automatic VLAN, Data and Network Security, Identity Confirmation, IEEE 802.1x, RADIUS, Service Quality.

## İÇİNDEKİLER

KABUL ve ONAY SAYFASI.....	iii
ÖZET .....	iv
SUMMARY .....	v
İÇİNDEKİLER .....	vi
ŞEKİLLER DİZİNİ .....	ix
ŞEKİLLER DİZİNİ ( devamı ) .....	x
SİMGELER VE KISALTMALAR DİZİNİ .....	xi
1. GİRİŞ .....	1
1.1 Elektronik Bilgilerin Güvenliği .....	5
2. İNTERNET KİMLİK DOĞRULAMA TEKNOLOJİLERİ .....	8
2.1 Dünyada ve Türkiye’de Bilgi Güvenliği .....	8
2.2 Güvenlik Gereksinimi .....	9
2.2.1 Kimlik doğrulama (authentication) işlemi .....	10
2.2.2 Yetkilendirme (authorization) işlemi .....	10
2.2.3 Hesap oluşturma (accounting) işlemi .....	11
2.3 Ağ Erişim Teknolojileri .....	11
2.4 İnternet Kimlik Doğrulama Hizmeti (IAS) .....	12
2.4.1 IAS'in desteklediği özellikler .....	13
2.5 RADIUS Protokolü .....	15
2.5.1 RADIUS sunucu işlemleri ve ileti türleri .....	16
2.6 IAS'in Çalışma Prensipleri .....	17
2.6.1 IAS'in RADIUS sunucusu olarak kullanılması .....	17
2.6.2 IAS'in RADIUS proxy'si olarak kullanılması .....	19
2.7 RADIUS Altyapı Bileşenleri .....	20
2.8 Active Directory Dizin Hizmeti .....	22
2.8.1 Active Directory için güvenlik bilgileri .....	23
2.8.2 Active Directory'de erişim denetimi .....	23
2.8.3 Dizin erişim protokolü (LDAP) .....	24
2.8.4 Kullanıcı ve bilgisayar hesapları .....	24
2.8.5 Active Directory dizin hizmetinde grup kavramı .....	25
2.8.6 Sertifika dağıtımları .....	26
2.9 IAS ile Kullanılan Kimlik Doğrulama Yöntemleri .....	27
2.9.1 Korunabilir genişletilebilir kimlik doğrulama protokolü (PEAP) .....	28
2.9.1.1 TLS şifrelenmiş kanalı .....	28
2.9.1.2 EAP ile kimliği doğrulanmış iletişim .....	28
2.9.2 Genişletilebilir kimlik doğrulama protokolü (EAP) .....	29
2.9.2.1 EAP altyapısı .....	31
2.9.2.2 EAP-RADIUS .....	32
2.9.3 MS-CHAP .....	32
2.9.4 MS-CHAP v2 .....	33
2.9.5 CHAP .....	33
3. PORT TABANLI KİMLİK DOĞRULAMA .....	34
3.1 Sanal Yerel Alan Ağları (VLAN) .....	34
3.2 Sanal Yerel Alan Ağ Türleri .....	35

3.3 Otomatik VLAN Kavramı .....	35
3.4 Port Tabanlı Kimlik Doğrulama İşlemi .....	37
3.5 IEEE 802.1x Kimlik Doğrulaması.....	38
3.6 802.1x için Kontrollü ve Kontrolsüz Portlar .....	39
3.7 802.1x'in Çalışma Prensibi .....	39
3.8 Servis Kalitesi (QoS) Kavramı .....	41
3.9 Servis Kalitesini Etkileyen Faktörler.....	42
3.9.1 Bant genişliği.....	42
3.9.2 Gecikmeler.....	43
3.9.3 Kayıplar .....	43
3.9.4 İletim öncelikleri.....	43
4. KABLOSUZ AĞLARDA KİMLİK DOĞRULAMA DENETİMİ.....	45
4.1 Kablosuz Haberleşme Sistemleri.....	45
4.2 Kablosuz Teknoloji Bileşenleri .....	45
4.3 Kablosuz Ağlar için Güvenlik Bilgileri.....	46
4.3.1 İstemci güvenlik duvarı .....	46
4.3.2 802.11 kimlik doğrulaması .....	46
4.3.2.1 Açık sistem kimlik doğrulaması .....	46
4.3.2.2 Paylaşılan anahtar kimlik doğrulaması .....	47
4.3.3 802.11 WEP şifrelemesi : .....	48
4.3.4 Wi-Fi korumalı erişim (WPA).....	49
4.3.5 802.1x kimlik doğrulaması .....	49
4.4 802.11 Ağlarında 802.1x'in Çalışma Prensibi .....	50
4.5 802.1x ve IAS .....	52
5. KRİTİK VERİ İÇEREN KAMPÜS AĞLARINDA GÜVENLİK UYGULAMASI. 53	
5.1 DPÜ Kampüs Ağı'nın Uygulama Öncesindeki Mevcut Yapısı .....	53
5.2 Active Directory Yapılandırması.....	58
5.2.1 Active Directory domain yapılandırması.....	59
5.2.2 Otomatik VLAN yapılandırması için Active Directory grup tasarımı .....	60
5.2.3 Merkezi denetim için Active Directory gruplarının tasarımı.....	61
5.2.4 Kullanıcı hesapları için uzak erişim izinlerinin düzenlenmesi .....	61
5.3 IAS Yapılandırması .....	62
5.3.1 Birincil ve ikincil IAS sunucu yapılandırması.....	62
5.3.2 IAS port yapılandırması.....	63
5.3.3 Kat switchlerinin IAS'a RADIUS istemci olarak eklenmesi .....	64
5.4 Kenar Switchlerin Kimlik Doğrulama Switchi Olarak Yapılandırılması.....	65
5.5 Otomatik VLAN için Omurga ve Kenar Switchlerin Yapılandırılması .....	65
5.6 İş İstasyonlarının PEAP MS-CHAPv2 için Yapılandırılması .....	66
5.7 Sertifika Sunucusunun Yapılandırılması .....	67
5.8 Erişim Kurallarının Yazılması .....	68
5.8.1 Uzak erişim politikalarının çalışma şekli .....	68
5.8.2 Uzak erişim politikalarının oluşturulmasında izlenen metot.....	69
5.8.3 Uzak erişim politikalarının oluşturulması.....	70
5.8.4 Kullanıcıların üye oldukları gruba göre yetkilerinin belirlenmesi.....	71
5.9 Servis Kalitesi Analizleri.....	72
5.10 Kablosuz Ağ Tasarımları .....	74
6. AHP uygulaması.....	78

6.1. Analitik Hiyerarşi Prosesi .....	78
6.2. Karar Verme Problemindeki Faktörler .....	78
6.2.1. Performans .....	78
6.2.2. Güvenlik : .....	78
6.2.2.1. İstemci güvenlik duvarı .....	78
6.2.2.2. 802.11 kimlik doğrulaması .....	78
6.2.2.3. 802.11 WEP şifrelemesi .....	79
6.2.2.4. Wi-Fi korumalı erişim (WPA) .....	79
6.2.2.5. 802.1x kimlik doğrulaması .....	79
6.2.3. İş Gücü .....	80
6.2.4. Yenileme Maliyeti .....	80
7. SONUÇ VE ÖNERİLER .....	89
7.1 Sonuçlar .....	89
7.2 Gelecek Çalışmalara İlişkin Öneriler .....	91
8. Literatür Çalışması .....	95
Ek-1 .....	98
3Com SuperStack 3 Switch 4400 ve 7700 Serilerinin Özellikleri .....	98
Ek-2 .....	102
İnternet ve otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi şu şekildedir: .....	102
Yalnızca otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi ise şu şekildedir: .....	103
Erişim listeleri ile VLAN222'den (WLAN) gelen kullanıcıların (notebook), tüm sunuculara ve diğer masaüstü bilgisayarlara ağdan herhangi bir şekilde (TCP/UDP) erişimleri engellenmesi. ....	105



## ŞEKİLLER DİZİNİ

	<b>Sayfa</b>
Şekil 1.1. 1971 yılı internet (Arpanet) bağlantıları .....	8
Şekil 1.2. Günümüz internet haritası .....	9
Şekil 2.1 Ağ erişim teknolojileri mimarisi.....	12
Şekil 2.2 Bir RADIUS paketinin genel yapısı.....	16
Şekil 2.3 RADIUS sunucusu olarak IAS'in kullanılması.....	18
Şekil 2.4 RADIUS Proxy'si olarak IAS'in kullanılması.....	19
Şekil 2.5 RADIUS altyapı bileşenleri.....	21
Şekil 2.7 EAP-RADIUS işlemi.....	32
Şekil 3.1 IEEE 802.1x için kontrollü ve kontrolsüz portlar.....	39
Şekil 3.2 IEEE 802.1x ile kimlik doğrulama işlemi.....	40
Şekil 4.1 Açık sistem kimlik doğrulaması.....	47
Şekil 4.2 Paylaşılan anahtar kimlik doğrulaması.....	48
Şekil 4.3 IEEE 802.1x kimlik doğrulama bileşenleri.....	50
Şekil 5.1 DPÜ Ağ Yapısının uygulama öncesindeki mevcut durumu.....	54
Şekil 5.2 DPÜ VLAN tabanlı güvenlik duvarı yapısı.....	56
Şekil 5.3 DPÜ Active Directory Domain yapısı.....	57
Şekil 5.4 Active Directory Domain yapısından bir kesit.....	59
Şekil 5.5 Otomatik VLAN yapılandırması için Active Directory grup yapısı.....	60
Şekil 5.6 Kampüs ağına erişimin denetlenmesi için oluşturulan genel gruplar.....	61
Şekil 5.7 Kampüs ağının IAS yapılandırmasından bir kesit.....	62
Şekil 5.8 IAS'in Active Directory'e tanıtılması.....	63
Şekil 5.9 RADIUS istemcilerin eklenmesi.....	64
Şekil 5.10 Shared Secret tanımlaması.....	64
Şekil 5.11 Kenar switchler üzerinde RADIUS sunucularının belirlenmesi.....	65
Şekil 5.12 Kullanıcı bilgisayarlarında IEEE 802.1x kimlik doğrulama ayarları.....	67
Şekil 5.13 Sertifika sunucusunun yapılandırılması.....	68
Şekil 5.14 Uzak erişim politikalarının oluşturulmasında izlenen yöntem.....	70
Şekil 5.15 Uzak erişim politikalarının oluşturulması.....	70
Şekil 5.16 Erişim politikasına ait şartların tanımlanması.....	71
Şekil 5.17 Kablosuz ağ örneği.....	74
Şekil 5.18 Kablosuz ağ cihazlarının Kampüs içindeki dağılımı.....	75

**ŞEKİLLER DİZİNİ ( devamı )**

Şekil 5.19	Kablosuz ağ üzerinde PDA'lar ile HIS sisteminin kullanılması.....	76
Şekil 5.21	Kablosuz ağ üzerinden internet erişimi.....	77
Şekil 7.1	DPÜ Ağ Yapısında tasarlanacak olan yedekli yapı topolojisi.....	94

## SİMGELER VE KISALTMALAR DİZİNİ

AAA	Authentication-Authorization-Accounting
CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
DICOM	Digital Imaging and Communications in Medicine
DMZ	DeMilitarized Zone
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunnelled Transport Layer Security
EKG	Elektrokardiyogram
SIS	Öğrenci Bilgi Sistemi
IAS	Internet Authentication Service
IEEE	Institute of Electrical and Electronics Engineers
LAN	Yerel Alan Ağı
LDAP	Basit Dizin Erişimi Protokolü
MAC	Media Access Control
MAN	Metropol Alan Ağı
MD5	Message Digest Algorithm
MR	Manyetik Rezonans Görüntüleme
MS-CHAP v2	Microsoft Challenge Handshake Authentication Protocol version2
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
OBS	Öğretim Elemanı Bilgi Sistemi
PDA	Personel Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PPP	Point to Point Protocol
QoS	Servis Kalitesi
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RF-ID	Radio Frequency Identification
SID	Security Identity
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Sanal Yerel Alan Ağları
VPN	Sanal Özel Ağ
WEP	Wired Equivalent Privacy
WLAN	Kablosuz Yerel Alan Ağları
WPA	Wi-Fi Protected Access
AHP	Analitik Hiyerarşi Prosesi

## 1. GİRİŞ

İletişim araçlarının öneminin çok fazla arttığı günümüzde, bilgiye hızlı bir şekilde ulaşmak toplumların temel ihtiyaçları arasına girmiştir. Bu ihtiyaç doğrultusunda özellikle 1990'lardan sonra bilgisayar ağlarında çok önemli gelişmeler yaşanmıştır. İnternet de, bu çalışmalar neticesinde ortaya çıkan ve yaygın olarak kullanılan bir bilgisayar ağıdır. Yaşanan hızlı teknolojik gelişmelerin ve internetin yaygınlaşmasının bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Bilgi ve iletişim teknolojilerinin yaygınlaşması, sadece etkin ve verimli kullanıma bağlı değildir. Aynı zamanda söz konusu teknolojilerde kullanılan tüm cihaz, donanım ve sistemlerde bilgi ve veri güvenliğinin tam olarak sağlanmasına da bağlıdır. Bu hızlı gelişim sürecinde, bilgi teknolojilerindeki bazı konular için standartların tam olgunlaştırılmadan kullanıma geçirilmesinden dolayı ağ yönetimi ve kontrolü güçleşmiş ve bilgisayar ağlarında birtakım güvenlik sorunları baş göstermiştir. Bu yüzden bilişim sistemlerinde bilginin gizliliği, özgünlüğü ve bütünlüğü gibi özelliklerin sağlanması büyük önem taşımaktadır.

Elektronik ortamlarda kişiler ve kurumların sahip olduğu bilgilerin mahremiyetlerinin korunması, bu ortamların yaygınlaşmasının önünün açılması ve bu ortamlarda herhangi bir kaybın oluşmaması için bu ortamlarda bulunan bilgilerin güvenliğinin sağlanması gereklidir. Bilgi güvenliğini sağlamak toplumda sadece güvenlikle uğraşan kişi ve kuruluşların görevi değil bilgi çağı olarak adlandırılan günümüzde bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle herhangi bir şekilde doğrudan veya dolaylı yönden ilişkisi olan ve bu sistemleri kullanan tüm birey, kurum ve kuruluşların katkıda bulunması ve görev alması gereken önemli bir konu haline almıştır.

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her iki ayda neredeyse iki katına çıkmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen elektronik uygulamaların artması, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir.

Hayatımızı kolaylaştırması iş ve işlemlerin hızlandırılmasına katkılar sağlayan bilgi teknolojileri insan hayatında günden güne daha da önem kazanmakta ve her geçen gün güvenliği üst düzeyde sağlanan güvenilir bilgi sistemlerine duyulan ihtiyaç artmaktadır [1].

Herhangi bir bilgisayar ađında meydana gelen gvenlik ihlali bir anda o ađın bađlı olduđu diđer tm ađları etkileyebilmektedir. Bu kurumsal ađlar zerinden haberleřen, sayıları hızla artarak yaygınlařan ve geniř kitlelerce kullanılan uygulamalar zerinde tutulan bilgilerin deđeri dřnldđnde kurumsal anlamda bilgi gvenliđinin sađlanması nemi daha iyi anlařılacaktır.

Elektronik ortamlarda verilen hizmetlerin (e-ticaret, e-kurum, e-devlet, e-deme, e-đrenme, vb.) sayısı her geen gn artmakta ve bu ortamların kullanımı ise yaygınlařmaktadır. Elektronik ortamlarda kurumlar tarafından verilen hizmetler yaygınlařtıķa, saldırganlar iin bu hizmetlerin verildiđi sistemler cazibe merkezi haline gelmektedir. İerisinde nemli bilgiler (kurumsal ve kiřisel) barındıran bilgi sistemlerinin gvenliđinin sađlanması ve ynetimi nem kazanmıřtır. Bilgi teknolojileriyle birilikte geliřtirilen yeni uygulamalar bir yandan hayatımızı kolaylařtırırken diđer yandan yeni gvenlik tehditlerini beraberinde getirmektedir. Kiřilerin ve kurumların sahip oldukları nemli bilgiler, eřitli sahtekrlikler, bilgi hırsızlıđı, korsan saldırıları, bilgi sızdırma ve kt niyetli kurum alıřanlarınca oluřturulabilecek i saldırılar gibi ok geniř bir yelpazeye sahip kaynaklardan gelen tehdit ve tehlikelerle karřı karřıyadır. Bilgi gvenliđini tehdit eden unsurlar sadece elektronik ortamda yapılan saldırılarla sınırlı deđildir. İnsan hataları, yangın, sel, deprem, terr saldırıları, sabotaj gibi istenmeyen olaylar veya dođal felaketler sonucunda da bilgiler ve bilgi sistemleri tamamen ya da kısmen zarar grmektedir.

Gnmzde elektronik ortamda yapılan gvenlik ihlllerinden hemen hemen her gn bahsedilmektedir. Bu durumdan elektronik ortamda hizmet veren kuruluřlar da hizmet alan kullanıcılar da etkilenmektedir. rneđin internet bankacılıđı yapan kullanıcılar dolandırıldıđı zaman; parasını kaybederken, o hizmeti sađlayan banka ise mřterilerinin gznde gven kaybına uđrayarak ticari itibarını kaybetme tehlikesiyle karřı karřıya kalmaktadır. Bu ve buna benzer tehditlerden etkilenmeyi en aza indirmek iin kurumlara, kuruluřlara ve kullanıcılara dřen nemli grevler vardır. Kullanıcıların bilgi gvenliđi konusunda bilinli olmaları gerekirken, kurumların bilgi gvenliđi konusunda kurumsal nlemler almaları ise mutlaka yapılması gereken grevler arasındadır. Kullanıcılar bilgi gvenliđi hakkında alacakları bilinlendirme ve bilgilendirme eđitimleri sayesinde kendi zerine dřen grevleri bilerek ve uygulayarak gerekli korumayı sađlamıř olacaklardır. Kurumlar ise kurumsal bilgi gvenliđi kavramının temel geređi olan bilgi gvenliđi standartlarına uyumluluk kapsamında altyapılarını uzman kuruluřlardan yardım alarak gzden geirmeli ve gzden geirme sonucunda ortaya ıkan ihtiyalara bađlı olarak alınması gereken nlemleri ve yatırımları zamanında yapmalıdır. Bireyler ve kurumların dıřında devletimize de dřen nemli grevler vardır. Bu grevlerin en bařında bilgi gvenliđinin sađlanmasıyla ilgili yasaların ıkartılarak hukuksal bořlukların

doldurulması ve yeni düzenlemelerin hızlıca yapılması gerekmektedir. Diğer önemli bir konu ise bilgi güvenliği eğitiminin verilebilmesi ve ülke genelinde bilgi güvenliği bilincinin yaygınlaştırılabilmesi amacıyla gerekli olan çalışmaların ve düzenlemelerin yapılmasıdır.

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlikte sağlanamaz.

Ülkemizde son yıllarda sayıları yetersiz de olsa sunulan güvenlik raporlarında kurumsal bilgi güvenliği konusunda kurumlarımızın yeterince duyarlı olmadığı ve gerekli olan önlemleri genellikle bilgisizlik, maddi gerekçeler, personel gibi sebeplerden dolayı alamadıkları tespit edilmiştir. Kurumlar yeni teknolojileri veya kendi uzmanlıkları dışında uzmanlık gerektiren alanları takip etmeyi ve kurumsal altyapılarını buna uyarlama çalışmalarını mevcut kısıtlı kaynaklar nedeniyle başaramamaktadırlar. Kurumların bilgi güvenliği konusunda alanında uzman olan güvenlik profesyonellerine ihtiyaçları vardır. Ancak ülkemizde kurumların kendi bünyesinde bilgi güvenliği alanında yetişmiş eleman sayısı yok denecek kadar azdır. Kurumların bilgi güvenliği alandaki uzmanlık açığını kapatmaları için dış kaynak (Outsource) kullanmaları zorunlu hale gelmiştir. Doğru seçilen dış kaynak kullanımında alınan hizmetin servis kalitesi yüksek olacağından bilgi güvenliği ihlallerinin birçoğu önceden tespit edilecek ve kurumların zararı minimuma inebilecektir.

Alınan birçok önleme geliştirilen birçok yeni donanım ve yazılıma rağmen bilgi teknolojilerine yönelik güvenlik saldırıları her geçen gün hızla artmaktadır. Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak önceden veya zamanında alınacak güvenlik tedbirleriyle kayıpları en aza indirmek mümkündür. Kurumlar tarafından güvenlik tedbirleri alınırken göz önüne alınması gereken önemli noktalar vardır. Öncelikli olarak alınan tedbirlerin çalışanlar tarafından benimsenmesi ve sahiplenilmesi gerekmektedir. İkinci önemli nokta ise korunması gereken bilgi varlıklarının koruma maliyetinin göz önünde tutulmasıdır. Koruma maliyetinin, hasar olasılığı \* hasarın değeri \* hasarın etkisi çarpımlarının toplam değerinden küçük olması dikkate alınmalıdır. Son olarak kullanıcıların tepkileri (performans kaybı, erişim engellemesi, prosedürel yaptırımlar, vb.) ve

yönetimsel zorluklar dikkate alınarak gerekli planlamalar yapılarak arzu edilen güvenlik düzeyinde koruma veya korunma sağlanmalıdır.

Bilgi güvenliği alanında yaşanan güvenlik ihlallerinin giderek artan bir bölümü ağ ve sistemlerden yazılımlara (uygulamalara) doğru kaymaktadır. Kurum bazında veya birey bazında güvenli ortamlarda iş yapma ihtiyaç ve istekleri her geçen gün hızla artmakta, kullanılan yazılımların güvenliği bilgi güvenliğinin sağlanmasında anahtar rol oynamaktadır [2]. Yıllar içerisinde ağ ve sistemlerin güvenliğinin sağlanmasına ilişkin geliştirilen yöntemler kurumlar tarafından başarıyla uygulanmış ve Sınır Ağ Güvenliği (Perimeter Network Security) kavramının önemi çoğu kuruluş tarafından anlaşılmış ve gerekleri yerine getirilmiştir. Ancak benzer durumu yazılım güvenliği için belirtmek zordur. Bilgi güvenliğinin sağlanmasında yazılım güvenliği merkezi ve kritik bir öneme sahiptir [3]. Günümüzde ağ ortamlarında çalışan kişiler ve diğer uygulamalar tarafından erişilebilen uygulama yazılımlarındaki güvenlik zafiyetleri bilgi güvenliği tehditlerinin başında gelmektedir. Özellikle internet ortamında çalışan yazılımlara güvenlik göz ardı edilerek esneklik ve kullanım kolaylığı altında bir sürü eklentiler yapılması ise yangın halinde olan bir binaya benzin dökmekle eş anlamlıdır. Başlıca yazılım güvenliği tehditleri incelendiğinde çevresel değişkenler, bellek taşmaları, enjeksiyonlar, güvensiz ağ ve haberleşme ortamları, varsayılan sistem ayarları, programcı arka kapıları bilinmesi ve önlem alınması gereken önemli zafiyetlerdir [4]. Yazılımlardaki zafiyetlerin artarak güvenlik problemlerinin her geçen gün arttığı US-CERT (The United States Computer Emergency Readiness Team) koordinasyon merkezi tarafından yıllık olarak yayınlanan rapor ve istatistikî veriler incelendiğinde açıkça görülmektedir. US-CERT tarafından açıklanan güvenlik zafiyetleri 2004 yılında 3,780 iken, 2005 yılında 5,990'a ulaşmış 2006 yılında 8,064, 2008 yılının ilk 3 ayında ise 6,058 olarak rapor edilmiştir [5].

Bilgi sistemlerine saldırıların yapılabilmesi için gerekli olan bilgi ve beceri seviyeleri hızla azalırken otomatik araçlar aracılığıyla yeni saldırı yöntemleri geliştirilmekte, bilgi sistemlerine zarar verecek olan saldırgan sayısı her geçen gün artmakta ve koruma teknolojileri saldırı tekniklerinin hep bir adım arkasında kalmaktadır.

İnternet üzerinden gerçekleştirilen iletişim süreçleri geliştikçe, güvenlik sistemlerine olan ihtiyaç giderek daha hayati bir önem kazanmaya başlamıştır. Bilgi ile bu bilgiyi işleyen ve saklayan bilgisayar sistemlerinin saldırılara karşı korunması yaşamsal önem taşımaktadır. Şirket ağlarında doğrudan maliyet ve ticari başarıya yönelik anlam taşıyan ağ sistemlerinin güvenliği, kurumsal ağlarda ulusal güvenlik boyutunda olumsuz etkilere neden olabilecek kritik bilgilerin korunması şeklinde kendini göstermektedir. Teknolojinin her getirdiği yenilik aynı zamanda bir

zayıflık ve saldırı açığı olarak karşımıza çıkabilmektedir. Günümüzde bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır. Bilgisayar sistemlerine ve ağlarına yönelik saldırılar, para, zaman, prestij ve değerli bilgi kayıplarına neden olabilmektedir. Bu saldırıların Kampüs bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilmektedir.

Yerel, geniş ve kablosuz alan ağlarını bünyesinde barındıran ağlar, "Kampüs Ağları" olarak adlandırılır.

Bu çalışmada Dumlupınar Üniversitesi (DPÜ) Ağları da kurumsal bir kampüs ağı niteliğinde olduğu için, bilişim sistemlerinde karşılaşılan güvenlik problemleri ve saldırılarına yönelik olarak bir takım uygulamalar gerçekleştirilmiş ve bu uygulamalar neticesinde veri ve bilgilerin güvenliği tam anlamıyla sağlanarak bu tür güvenlik problemlerine bir çözüm getirilmiştir.

### **1.1 Elektronik Bilgilerin Güvenliği**

Temel işlerin yürütülmesi için bilgi hayati bir kaynaktır. Büyük bir hızla artan bilgi sistemleri ve buna paralel olarak çoğalan ve gelişen ölçü ve görüntüleme yöntemleri, giderek otomatikleşen analiz ve izleme cihazları da büyük bir hızla arttırmaktadır. Daha iyibir hizmet üretebilmek için gerekli bilgi ve verilerin toplanması, kullanılması, paylaşılabilmesi ve bilgi üretiminin standart yöntemlerle gerçekleştirilmesi, üretilen bilgiden en üst düzeyde yararlanmayı sağlar.

Hizmet türlerinin ve rollerinin çeşitliliği nedeniyle eğitim hizmeti sunan kurumlarda, hizmet üretiminin ve üretim yönetiminin planlanmasında ihtiyaç duyulan bilgiye erişim oldukça zor ve karmaşık bir süreç gerektirmektedir. Bu nedenle bilgi üretimi ve bilgiye erişim yöntemleri en baştan iyi bir şekilde tasarlanmalıdır. İdari ve mali kayıtların tutulması ve kullanılmasındaki başarılı uygulamaların öğrenci bilgisi kayıtların tutulması ve kullanılması bakımından da eşdeğer bir başarı çizgisine ulaşması gerekmektedir. Ayrıca bilgi üretimi, ulusal ve uluslararası ölçekte veri ve bilgi paylaşımı, güvenilirlik ve tutarlılık, kaynak ve zaman tasarrufunun sağlanması gibi konular OBS'nin (Sutudent Information System-Öğrenci Bilgi Sistemi) temelini oluşturduğu için Kampüs ağlarının 7 gün 24 saat hizmet veren, sistemin istek ve ihtiyaçlarına cevap verebilen bilgi sistemlerine sahip olmaları da büyük önem taşımaktadır [5].



Üniversitelerdeki bilgi yoğunluğu beraberinde hizmet veren personel sayısı ve çeşitliliğini getirdiği gibi iş yoğunluğunun azaltılması için gerekli olan bilgisayar sayısını da artırmaktadır. DPÜ Kampüs Ağı, diğer tüm Kampüs ağlarında olduğu gibi bünyesinde öğrenci ve Personeli'ne ait gizli ya da özel bilgileri barındırmaktadır. Yüksek risk oranına sahip bu verilerin kampüs içinden veya dışından oluşabilecek saldırılara karşı korunması için bir kampüs ağı kapsamında 7 gün 24 saat temelinde durmaksızın çalışan, yüksek güvenilirlik gerektiren ve sürekli bilgi akışının devam ettiği bir otomasyon sistemine sahip olmak gerekmektedir. Bu teknoloji, stratejik bir önem taşıyan veri yedeklemesinin aktif cihazlar üzerinde yapılabilmesini ve doğabilecek sorunların alt bloklarda izole edilebilmesini sağlar. Bu bilgiler ışığında, verileri toplayan ve depolayan kurum ve kişilere büyük sorumluluklar düştüğü ortadadır. Buradaki sorumluluklar hem etik kurallarca, hem de yasalar tarafından kesin olarak belirlenmektedir [2].

Bu çalışmada; veri ve bilgi güvenliğinin sağlanması amacıyla, DPÜ Kampüs ağı için birer tehlike unsuru oluşturan bir takım güvenlik problemlerinin çözümüne yönelik olarak kampus içinde hem kablolu hem de kablosuz ağlarında, otomatik VLAN (Virtual Local Area Network) yapılandırması ve kampüs ağına erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmiştir. Bununla birlikte, kurumsal kararlılık ve sorumluluk bilinci, altyapı yatırımları ve bilgi teknolojilerinde tecrübeli, iyi yetişmiş teknik personel gibi birçok unsurun bir araya getirilmesiyle de veri güvenliğinin sağlanması hedeflenmiştir.

Çalışmada kullanılan kimlik doğrulama yöntemi ile; ağ üzerindeki bilgilere kolay ulaşım, açık ve güvensiz bir ağ olan internete bağlantı, ağ dışındaki ortamlardan ağa yapılabilecek saldırılar, yerel ağda bulunan yetkisiz kişilerin dış ortama bilgi göndermesi, zararlı/zararsız izinsiz erişimlerin engellenmesi hedeflenmiş ve erişimin sadece yetkili kişilere verilmesi ile risk oranı yüksek verilere sadece yetkili kullanıcıların kendilerine tanınan erişim hakları ile erişmeleri sağlanmıştır. Otomatik VLAN yapılandırmasıyla; internetten de erişilebilen risk oranı yüksek verilerin doğruluğunun ve güvenilirliğinin sağlanması, bu bilgilerin kaybolmasının önlenmesi ve yetkilerine göre gruplandırılan organizasyonel birimlerde muhafaza edilmesi, hasar ve kayıplara karşı korunması (safety), aitliğinin saptanması (ownership), doğru kişilerin erişimine açılması (authorization) ve yetkisiz erişimlere engel olunup bu bilgilerin korunması (protection) sağlanmıştır.

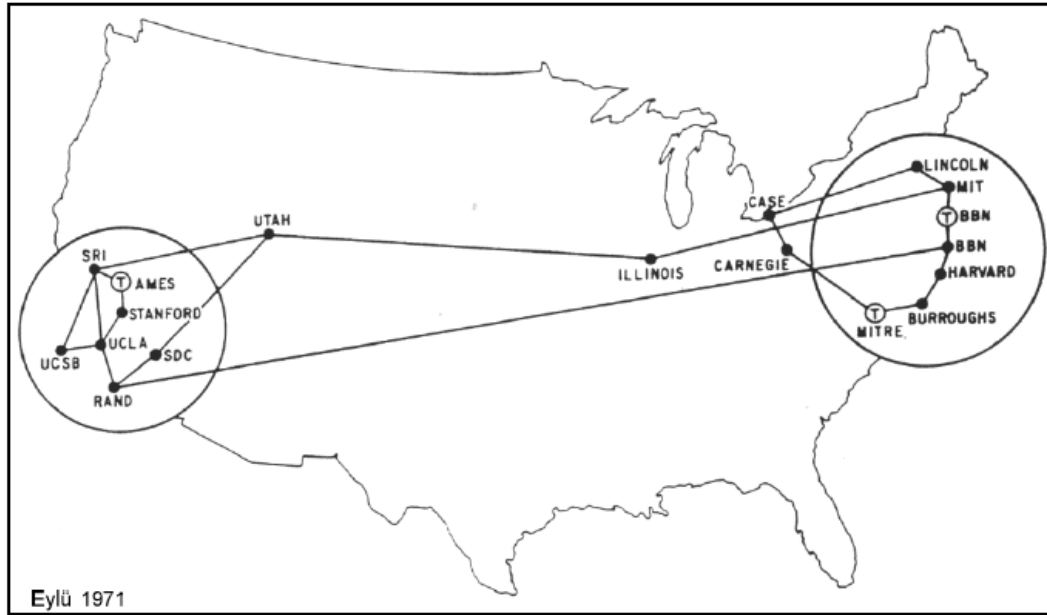
Elektronik bilgilerin mahremiyeti problemine yönelik olarak önerilen çözüm yönteminin yanında kablosuz ağ uygulamaları kapsamında; taşınabilir bilgisayarlara sahip öğrenci, personel ve ziyaretçiler otomasyon sistemine zarar vermeksizin internete erişebilmeleri

ve birimlerde görev yapan personelin eğitim öğretim sırasında OBS sistemine erişerek işlemleri gerçekleştirmeleri öngörülmüştür. Bununla birlikte uygulamada kullanılan Erişim Noktalarıyla (Access Point-AP), Sanal Yerel Alan Ağ (VLAN) desteğinin göz önüne alınması durumunda, istenilen kullanıcıların ya da mobil cihazların (Personel Digital Assistant-PDA) sadece internete erişmelerinden farklı olarak otomasyon sistemine de erişmeleri sağlanmış olacaktır.

## 2. İNTERNET KİMLİK DOĞRULAMA TEKNOLOJİLERİ

### 2.1 Dünyada ve Türkiye’de Bilgi Güvenliği

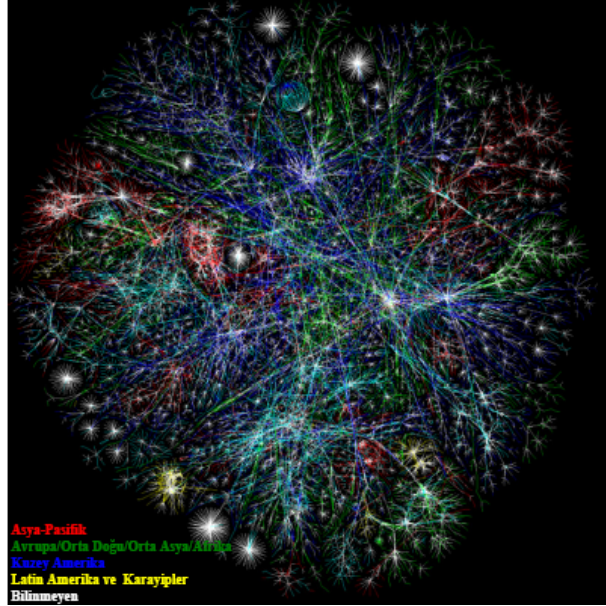
Günümüzde bilgi güvenliği ihlallerinin büyük bölümünün internet üzerinden yapılan saldırılardan kaynaklanmasından dolayı internet ve bilgi güvenliği arasındaki ilişkinin bilinmesinde fayda vardır. Kurulduğu yıllardan günümüze kadar sürekli büyüyerek gelişmekte olan internetin dününün ve bugününün karşılaştırılması büyümenin boyutunun görülmesi açısından önemlidir. Büyümeye paralel olarak güvenlik riskleri ve ihlalleri artmakta ve doğası gereği güvensiz bir ortam olan internet kendisine bağlı olan kurum kuruluş ve bireyleri üst derecede tehdit etmektedir. İnternetin ilk günkü bağlantıları Şekil 2.1’deki harita üzerinde gösterilmiştir.



Şekil 1.1. 1971 yılı internet (Arpanet) bağlantıları

1971 yılında Şekil 2.1’de gösterildiği gibi sadece 18 kurumu bünyesinde barındıran internet her geçen gün hızla büyümekte ve yaygınlaşarak işlevi artmaktadır. İnternetin yaygınlaşmasına ve büyümesine paralel olarak günlük yaşantımızda yaptığımız iş ve işlemlerin bu ortamlara kayması sonucunda güvenlik ihlallerinin etkileri daha fazla hissedilmektedir. İnternetin bugünkü büyüklüğünü Şekil 2.2’de verilen harita görsel bir şekilde özetlemektedir.

Şekil 1.1 ve Şekil 1.2 kıyaslandığında, internetin baş döndürücü bir hızla büyüdüğü açıkça görülmektedir. İnternetin bu hızda büyümesi ve kullanımının yaygınlaşması, saldırganların iştahını kabartmaktadır. İnternet gelişirken elbette interneti tehdit eden saldırılarda aynı oranda gelişmektedir. İnternet üzerindeki güvenlik olaylarıyla ilgili olarak araştırma yapan önemli kuruluşlar vardır.



Şekil 1.2. Günümüz internet haritası

## 2.2 Güvenlik Gereksinimi

Ağ yapıları üzerindeki yükler yeni uygulamalarla her geçen gün artmaktadır. Bilgilere her lokasyondan ve gerektiğinde ulaşım, standart veri iletimi yanı sıra ses ve görüntü iletimi için aynı hatlardan yararlanma gibi konular performanslı, genişleyebilir, kolay yönetilebilir ve güvenilir ağ altyapılarını gerektirmektedir. Çok fazla kullanıcıya sahip bilgisayar sistemlerin artmasıyla birlikte var olan güvenlik problemi, özellikle açık ağlar üzerinden erişilen ve karmaşık uygulamaların sorunsuz çalışabilmesi için gerekli olan bir unsur haline gelmiştir [6].

Güvenliğin bileşenleri olarak sayılan; Kimlik Doğrulama (Authentication), Yetkilendirme (Authorization) ve Hesap Oluşturma (Accounting) birbirinden ayrılmaz parçalar olarak birlikte ele alınır. Ağ güvenliği de kimlik doğrulama, yetkilendirme ve hesap oluşturma yani "AAA" olmak üzere üç aşamada gerçekleştirilir. Bilgisayar sistemleri için bu işlemlerin her biri ayrı ayrı tanımlanır. Ağ topolojisinde yer alan bir kullanıcının kaynak erişimini kademeli olarak kontrol eden AAA modelinde önce kullanıcıyı tanıma, ardından erişebilecekleri kaynaklar için yetkilendirme ve son olarak erişilen kaynaklar için denetleme aşamasından bahsedilebilir. Bu işlemler genellikle kullanıcının username (kullanıcı ismi) ve password (şifre) bilgileri ile gerçekleştirilir [7]. Bunun yanında akıllı kart, parmak izi ve retina gibi biometrik yöntemlerin kullanıldığı uygulamalar da vardır.

### **2.2.1 Kimlik doğrulama (authentication) işlemi**

Kimlik Doğrulama işlemi sırasında, kimlik doğrulama sunucusunda depolanan username/password çiftlerinin bir listesine karşılık sisteme erişmek isteyen kullanıcı tarafından sunucuya sağlanan username/password çiftini karşılaştırma işlemi gerçekleştirilir. Bu bilgilerin sistemde varlığı ve doğruluğu onaylandıktan sonra sisteme giriş için izin verilir. Sisteme kimlerin erişmesi gerektiği sorusuna cevap verildikten sonra bu kullanıcılar dışında erişimin olmaması için gerekli düzenlemeler yapılır. Ayrıca erişimi olan kullanıcıların da şifrelerinin gerektiği kadar güvenli olduğuna emin olmak için bir şifre politikası izlenmeli ve kullanıcılar buna uymaya zorlanmalıdır. Dikkat edilmesi gereken diğer bir nokta ise, kimlik doğrulama işlemi yapılırken kullanılan ortamın güvenli olup olmadığıdır. Eğer sunucu ile kullanıcı arasındaki haberleşme üçüncü bir kişi tarafından da izleniyorsa ve yapılan haberleşme şifreli değilse kullanıcı bilgileri çok rahatlıkla çalınabilir.

### **2.2.2 Yetkilendirme (authorization) işlemi**

Yetkilendirme işlemi, bilgileri önceden doğrulanan kullanıcının sistem içindeki yetkilerinin ne olduğunun belirtilmesidir. Kullanıcılar gruplandırıldığında bu yetkilendirme daha kolay bir şekilde yapılabilir. Her grubun yetkileri belirlenip daha sonra bu yetkilere sahip olması istenen kullanıcılar bu gruplara eklenebilir. Burada göz önünde bulundurulması gereken nokta, kullanıcıların üyesi buldukları grupların tüm haklarına sahip olmasıdır. Yani iki gruba üye bir kullanıcı, iki grubun haklarının birleşim kümesi olan haklara sahip demektir. Hiçbir kullanıcıya sahip olması gerekenden daha fazla yetki verilmezse istenmeyen durumlardan büyük ölçüde kurtulmuş olunur. Yetkilendirme işlemi ile bir username/password çiftine özgü verilen

özel izinler listesi sağlanır. Aslında yetkilendirme ile kimlik doğrulama işlemi birleştirilebilir. Yetkilendirme, sisteme kendini kimliği ile tanıtmış ve kimlik doğrulaması yapılmış (yani belirttiği kimliğe sahip olan kişi olduğunu ispatlamış) kullanıcılara, sistem kaynaklarına erişim izni verilmesidir. Kullanıcı, kimlik doğrulaması yapıldıktan sonra ağ üzerindeki bir kaynaktaki bir dosyaya erişmek istediğinde, öncelikle bu kullanıcının bu kaynağa erişim yetkisi olup olmadığı sınıranır. Eğer yetkisi varsa, kaynağa erişmesine izin verilir. Yani bir kullanıcı, kimlik doğrulaması yapıldıktan sonra tüm kaynaklara erişme yetkisine sahip olmaz. Erişim yetkisi, kendisine verilen yetki düzeyi ile sınırlıdır.

### **2.2.3 Hesap oluşturma (accounting) işlemi**

Hesap oluşturma işlemi ise; kullanıcı aktivitelerinin izlenmesi gerektiğinde veya bir sorun çıktığında sorunun nereden çıktığının anlaşılması için gerekli bilgiyi sunar. Bu işlem sırasında tüm kullanıcıların erişim saatleri, erişim türü ve yaptıkları işlemlerle ilgili kayıtlar günlük olarak tutulduğu için sorun çıktıktan sonra eğer zarar görmediyse kayıtlar olayın nasıl geliştiğini açıklayabilir. Hesap oluşturma fonksiyonu genellikle kimlik doğrulama ve yetkilendirme fonksiyonundan sonra devreye girer, ancak bu iki fonksiyonla herhangi bir bağı yoktur.

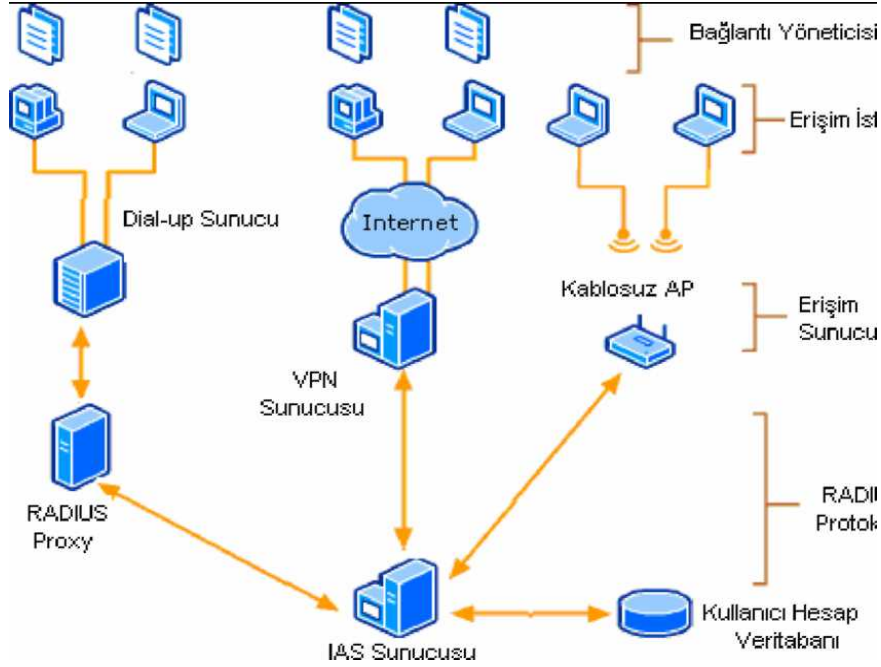
### **2.3 Ağ Erişim Teknolojileri**

Ağ erişimi, her bir bilgisayar sisteminin ağ altyapısı için kritik bir bileşendir. Ağ erişim teknolojileri, bir bilgisayarın daha önceden belirlenmiş politikalara uyumluluğunun onaylanması esasına dayanarak, ağ yöneticilerinin ağ erişimini izlemelerini ve kontrol etmelerini sağlar. Kablosuz yerel alan ağlarına (WLAN-Wireless Local Area Network) ve internet üzerinden intranetlere, uzaktan güvenli erişim, kimlik doğrulama, yetkilendirme ve hesap oluşturma gibi merkezileştirilmiş ağ bağlantısı sağlayan servisler, istemciye (client) dayanan güvenli ağ erişiminin yönetiminde destek sağlamaya yarayan bileşenler ve servisler için çok amaçlı bir ağ erişim çözümü kullanabilir.

Genel olarak bilinen ve bu tez çalışmasında da Internet Kimlik Doğrulama Hizmetinin (IAS-Internet Authentication Service) kullanılacağı ağ erişim teknoloji bileşenleri şu şekilde başlıklandırılabilir:

- 802.11 kablosuz uygulamaları
- Sanal Özel Ağlar-(VPN-Virtual Private Networks)
- Internet Kimlik Doğrulama Hizmeti

■ Bağlantı yöneticisi [8]



Şekil 2.1 Ağ erişim teknolojileri mimarisi

Şekil 2.1'de ağ erişim teknolojisinin altyapı bileşenleri görülmektedir. Buradaki bağlantı yöneticisi istemcinin uzak erişim bağlantısını, dial-up (çevirmeli) veya VPN tabanlı uzak erişim sunucularına bağlar. Uzak erişim sunucuları RADIUS (Remote Authentication Dial-In User Service) istemcileri gibi davranır ve kimlik doğrulama ile yetkilendirme için bir IAS sunucusuna erişim taleplerini gönderir. Benzer şekilde kablosuz erişim noktasından erişen 802.11 kablosuz istemci talepleri bir IAS sunucusuna gönderilir. IAS sunucusu erişim isteklerini alıp işler ve erişim istemci kimlik bilgilerini doğrulamak için bir kullanıcı hesap veri tabanını sorgular.

Bundan sonra incelenecek olan başlık kapsamında bir ağ erişim teknolojisi olan IAS yani Internet Kimlik Doğrulama Hizmetinden bahsedilecektir.

#### 2.4 Internet Kimlik Doğrulama Hizmeti (IAS)

IAS; IETF (Internet Engineering Task Force-Internet Mühendislik Görev Grubu) tarafından tanımlanan RADIUS standardının bir Microsoft uygulamasıdır [9]. IAS bir RADIUS sunucusu olarak, kablolu/kablosuz, kimlik doğrulama anahtarı, dial-up/VPN ve yönlendiriciden

yönlendiriciye bağlantılar gibi birçok ağ erişim türü için merkezileştirilmiş kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemlerini gerçekleştirir. Bir RADIUS Proxy'si olarak da, kimlik doğrulama ve hesap oluşturma iletilerini diğer RADIUS sunucularına iletir. Ayrıca IAS, RFC 2865 ve RFC 2866'da açıklanan RADIUS'a ilişkin IETF standartlarını da destekler. IAS sunucusu Active Directory etki alanının bir üyesi olduğunda IAS, kullanıcı hesabı veritabanı olarak dizin hizmetini kullanır ve çoklu oturum açma çözümünün bir parçası olur. Bu durumda ağ erişim denetimi (kimlik doğrulama ve ağa erişim için yetkilendirme) ve Active Directory etki alanında oturum açma için aynı kimlik bilgileri kullanılır. Kuruluşlar IAS ile kullanıcı kimlik doğrulama, yetkilendirme ve hesap oluşturma üzerindeki denetimini koruyarak, uzaktan erişim altyapısı için bir servis sağlayıcısından dış kaynak sağlayabilirler [6].

Ağ erişimini sağlayan ISS'ler (Internet Servis Sağlayıcısı) ve kuruluşlar, kullanılan ağ erişim donanımının türünden bağımsız olarak, her tür ağ erişimini tek bir yönetim noktasından yönetme konusunda artan bir güçlkle karşılaşmaktadırlar. RADIUS standardı, türdeş ve türdeş olmayan ortamlarda bu işlevi destekler. RADIUS, kimlik doğrulama ve hesap oluşturma isteklerini bir RADIUS sunucusuna göndermek için ağ erişim donanımını etkinleştiren bir istemci/sunucu protokolüdür. RADIUS sunucusunun kullanıcı hesap bilgilerine erişimi vardır ve ağ erişimi kimlik doğrulama bilgilerini denetleyebilir. Kullanıcının kimlik bilgileri doğruysa ve bağlantı girişimine yetki verilirse, RADIUS sunucusu belirlenen koşullara göre kullanıcının erişimine yetki verir ve bir hesap oluşturma günlüğünde, ağ erişimi bağlantısının günlüğünü tutar. RADIUS'un kullanımı, ağ erişimi kullanıcı kimlik doğrulama, yetkilendirme ve hesap oluşturma verilerinin toplanmasına ve her erişim sunucusu yerine merkezi bir konumda tutulmasına olanak verir.

#### 2.4.1 IAS'in desteklediği özellikler

IAS, aşağıdaki özellikleri destekler:

1. **Çeşitli kimlik doğrulama yöntemleri:** Kimlik doğrulama gereksinimlerini karşılayan özel yöntemler eklenmesine olanak vererek çok sayıda kimlik doğrulama protokolünü destekler.
2. **Çeşitli yetkilendirme yöntemleri:** Yetkilendirme gereksinimlerini karşılayan özel yöntemler eklenmesine olanak vererek çok sayıda yetkilendirme yöntemini destekler.
3. **Türdeş olmayan erişim sunucuları:** IAS, RFC 2865 ve 2866'yı destekleyen erişim sunucularına ek olarak şunları da destekler:



- Kablosuz erişim noktaları
- Anahtarların kimliğini doğrulama
- Yönlendirme ve Uzaktan Erişim Hizmeti ile tümleştirme
- RADIUS Proxy'si
- Dış kaynaklı dial-up erişim ve kablosuz ağ erişimi

**4. Merkezi kullanıcı kimliği doğrulama ve yetkilendirme:** Bir bağlantı isteğinin kimliğini doğrulamak için, Active Directory etki alanındaki kullanıcı hesaplarına göre, bağlantı kimlik bilgilerini doğrular. Bir bağlantı isteğini yetkilendirmek için kullanıcı hesabının, bağlantı kimlik bilgilerini ve uzaktan erişim ilkelerine karşılık gelen *dial-in* (içeri arama) özelliklerini kullanır. Uzaktan erişim ilkeleri, uzaktan erişim iznini yönetmek için daha güçlü ve esnek bir yöntem sağlar. Aşağıdakileri içeren çeşitli koşullara göre, ağ erişimi yetkilendirilebilir:

- Bir gruptaki kullanıcı hesabı üyeliği.
- Haftanın günü veya günün saati.
- Kullanıcının, üzerinden bağlantı kurduğu ortamın türü (örneğin, kablosuz ortam, ethernet anahtarı, modem veya VPN).
- Kullanıcının aradığı telefon numarası.
- İsteğin geldiği erişim sunucusu.

**5. Tüm erişim sunucuları için merkezi yönetim:** RADIUS uygulayan her erişim sunucusu için bağlantı parametrelerinin denetlemesine olanak verir.

**6. Merkezi denetim ve kullanım hesapları:** Tüm erişim sunucularının gönderdiği kullanım (hesap) kayıtlarının merkezi bir konumda toplamasına olanak verir. IAS, denetim bilgilerini (örneğin, kimlik doğrulama kabulleri ve redleri) ve kullanım bilgilerini (örneğin, bağlantı ve bağlantı kesilmesi kayıtlarını) günlük dosyalarında depolar. Veriler daha sonra standart bir veri çözümleme uygulaması ile çözümlenir.

**7. Ek bileşen tabanlı yönetim aracı:** Ek bileşen adı verilen bir yönetim aracı sağlar.

**8. Yerel veya uzaktan izleme:** Olay görüntüleyicisi, sistem monitörü ve basit ağ yönetimi protokolü dahil olmak üzere IAS, yerel olarak veya uzak bilgisayardan izlenebilir. Ayrıntılı trafik çözümlemesi ve sorun giderme için RADIUS iletilerini yakalamak üzere ağ izleyicisi de kullanılabilir.

**9. Ölçeklendirilebilirlik:** IAS küçük ağlar için bağımsız sunuculardan, büyük kuruluş ve ISS ağlarına kadar değişen boyutlarda çeşitli ağ yapılandırmalarında kullanılabilir.

**10. Birden çok IAS sunucusu için destek:** Birden çok IAS sunucusunun yapılandırmasının eşitlenmesi, *netsh* komut satırı aracılığı ile gerçekleştirilebilir.

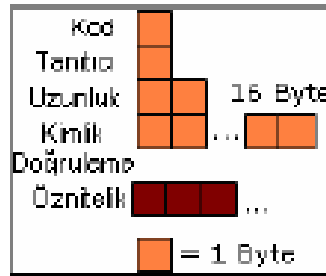
## 2.5 RADIUS Protokolü

Sistem güvenliğinin temeli; kullanıcıların kimliklerinin doğru belirlenmesi ve yetkilendirilmesi işlemine dayanır. Eğer sistemdeki bir kullanıcının kimliği belirlenemiyorsa kişilerin yaptıklarından sorumlu olması mümkün olmayacağından büyük bir karmaşa yaşanır. Bu karmaşayı önlemek için kullanılan teknolojilerden biri olan RADIUS (Uzaktan Kimlik Doğrulama Araması Kullanıcı Hizmeti); RFC 2865 [10] "RADIUS" ve RFC 2866 [11] "RADIUS Hesap Oluşturma" bölümünde açıklanmış olan endüstri standardı bir protokoldür. RADIUS; 3Com, Assend, Cisco gibi ağ teknolojisi sağlayan firmalar tarafından kullanılmıştır ve pek çok uzak erişim aygıtı RADIUS ile birlikte çalışacak şekilde tasarlanmıştır. Bu protokol merkezi kimlik doğrulama, yetkilendirme ve hesap oluşturma (AAA) hizmetlerini sağlamak için kullanılır.

Bir RADIUS istemcisi (genellikle bir dial-up sunucu, VPN sunucusu veya kablosuz erişim noktası), kullanıcı kimlik ve bağlantı parametresi bilgilerini bir RADIUS sunucusuna RADIUS iletisi şeklinde gönderir. RADIUS sunucusu, RADIUS istemci isteğinin kimliğini doğrular, yetkilendirir ve bir RADIUS ileti yanıtı gönderir. Kimlik doğrulama işlemi esnasında kullanıcıların kişisel bilgileri, kimlik doğrulama işlemi yapacak RADIUS sunucusu üzerindeki veri tabanında saklanır. Bu işlem kullanıcıların kimlik bilgilerinin doğruluğundan emin olmak için yapılır. Veri tabanında bulunan kullanıcı bilgileri çeşitli şifreleme metotlarıyla şifrelenir. Ancak bu işlem sunucu üzerinde saklanan bilgilerin tam anlamıyla güvende olduğunu göstermez. Güvenliğin sağlanması için kullanıcı şifrelerinin karmaşık olması ve belirli sürelerde değiştirilmesi ağ güvenliği açısından büyük önem taşır. RADIUS sunucusu üzerinde kullanılan bu teknoloji sayesinde ağ içindeki farklı veri kaynaklarına erişme hakkına sahip kullanıcıların yetkileri tek bir noktadan belirlenebilmekte ve yönetilebilmektedir. Böylelikle, dağıtık yapıdaki kullanıcıların yönetimi kolaylaştırılmaktadır. Bunun yanında RADIUS istemcileri, RADIUS sunucularına RADIUS hesap oluşturma iletileri de gönderir [7].

RADIUS iletileri, UDP (Kullanıcı Datagram Protokolü) iletileri olarak gönderilir. RADIUS, kimlik doğrulama iletileri için 1812 numaralı UDP bağlantı noktasını, hesap oluşturma iletileri için ise 1813 numaralı UDP bağlantı noktasını kullanır. Bazı ağ erişim sunucuları, RADIUS kimlik doğrulama iletileri için 1645 numaralı UDP bağlantı noktasını, RADIUS hesap oluşturma iletileri için ise 1646 numaralı UDP bağlantı noktasını kullanabilir. Varsayılan olarak, IAS her iki UDP bağlantı noktasına ayarlanmış olan RADIUS iletilerinin

alınmasını destekler. Bir RADIUS paketinin UDP bilgilerine yalnızca tek bir RADIUS iletisi eklenir. Aşağıdaki şekil bir RADIUS paketinin genel yapısını göstermektedir.



**Şekil 2.2** Bir RADIUS paketinin genel yapısı

Bu alanları daha kapsamlı bir şekilde inceleyecek olursak;

- **Kod (Code) Alanı:** 1 byte uzunluğunda olup RADIUS paket tipini içerir. Geçersiz bir Kod alanına sahip bir paket kullanılamaz, atılır.
- **Tanıtıcı (Identifier) Alanı:** 1 byte uzunluğundadır ve bir istek ile ona karşı olan cevabı eşleştirmede kullanılır.
- **Uzunluk (Length) Alanı:** 2 octet (sekizli) uzunluğundadır ve RADIUS mesajının tüm uzunluğunu yani Kod, Tanıtıcı, Uzunluk, Kimlik Doğrulama ve RADIUS Özellik alanlarını içerir. İdeal paket uzunluğu 20 byte'dan 4096 byte'a kadar değişir.
- **Kimlik Doğrulama (Authenticator) Alanı:** 16 octet uzunluğundadır ve RADIUS istemci ve sunucusunun her ikisinin de kimlik doğrulamada kullandığı bilgiyi içerir. Bu bir Request (İstek) veya bir Response (Cevap) simgeler.
- **Öznitelik (Attribute) Alanı:** RADIUS paketinin öznitelikler kısmı, RADIUS paketleri için yapılandırma ayrıntılarını, yetkilendirmeyi ve belirli kimlik doğrulama bilgilerini taşıyan bir ya da daha fazla RADIUS özelliği içerir.

### 2.5.1 RADIUS sunucu işlemleri ve ileti türleri

RFC 2865 ve 2866, istemci ve sunucu arasında meydana gelen aşağıdaki RADIUS ileti türlerini tanımlar [10]:

- **Erişim İsteği (Access Request):** RADIUS istemcisi tarafından bir bağlantı girişimi için istek, kimlik doğrulaması ve yetkilendirme amacıyla gönderilir. Bir kullanıcının özel bir

ağ erişim sunucusuna ve diğer herhangi bir özel servise erişimine izin verilip verilmediğini belirler.

- **Erişim Onayı (Access Accept):** Tüm şartlar yerine getirildiğinde bir "Erişim İsteği" iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti RADIUS istemcisine bağlantı girişiminin kimlik doğrulamasının yapıldığını ve yetkilendirildiğini bildirir ve kullanıcı için yapılandırma değerlerinin listesini içerir.
- **Erişim Reddi (Access Reject):** Herhangi bir şart yerine getirilmediğinde bir "Erişim İsteği" iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti RADIUS istemcisine bağlantı girişiminin reddedildiğini bildirir. Kimlik bilgileri özgün değilse veya bağlantı girişimi yetkilendirilmezse, RADIUS sunucusu bu iletiyi gönderir.
- **Erişim İtirazı (Access Challenge):** Bir "Erişim İsteği" iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti, yanıt isteyen RADIUS istemcisine bir itirazdır.
- **Hesap Oluşturma İsteği (Accounting Request):** Kabul edilen bir bağlantının hesap oluşturma bilgilerini belirtmek için RADIUS istemcisi tarafından gönderilir.
- **Hesap Oluşturma Yanıtı (Accounting Response):** "Hesap Oluşturma İsteği" iletisine yanıt olarak RADIUS sunucusu tarafından gönderilir. Bu ileti, "Hesap Oluşturma İsteği" iletisinin başarıyla alındığını ve işlendiğini bildirir.

## 2.6 IAS'in Çalışma Prensipleri

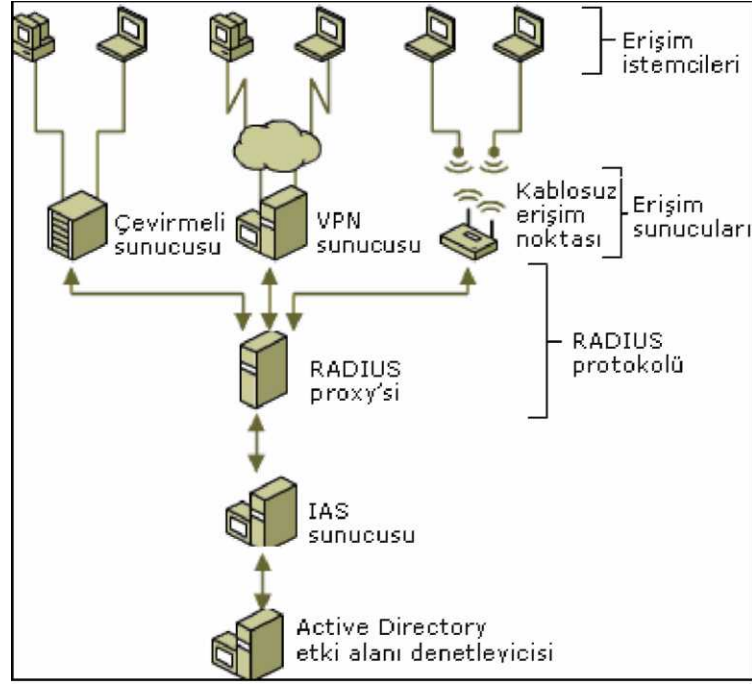
Bu başlık kapsamında RADIUS sunucusu veya RADIUS Proxy'si olarak IAS'in nasıl çalıştığı anlatılacaktır.

### 2.6.1 IAS'in RADIUS sunucusu olarak kullanılması

IAS; RADIUS istemcileri için kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemlerini yapmak üzere bir RADIUS sunucusu olarak kullanılabilir. RADIUS istemcisi, bir erişim sunucusu veya RADIUS Proxy'si olabilir. IAS bir RADIUS sunucusu olarak kullanıldığında, şunları sağlar:

- RADIUS istemcileri tarafından gönderilen tüm erişim istekleri için merkezi bir kimlik doğrulama ve yetkilendirme hizmeti sağlar. Bir bağlantı isteği için kullanıcı kimlik bilgilerini doğrularken, Active Directory etki alanını, bir bağlantıyı yetkilendirmek için ise kullanıcı hesabının arama özelliklerini ve uzaktan erişim ilkelerini kullanır.

- RADIUS istemcileri tarafından gönderilen tüm hesap oluşturma istekleri için merkezi bir hesap kayıt hizmeti sağlar. Hesap oluşturma istekleri, çözümlenmek üzere bir yerel



Şekil 2.3 RADIUS sunucusu olarak IAS'in kullanılması

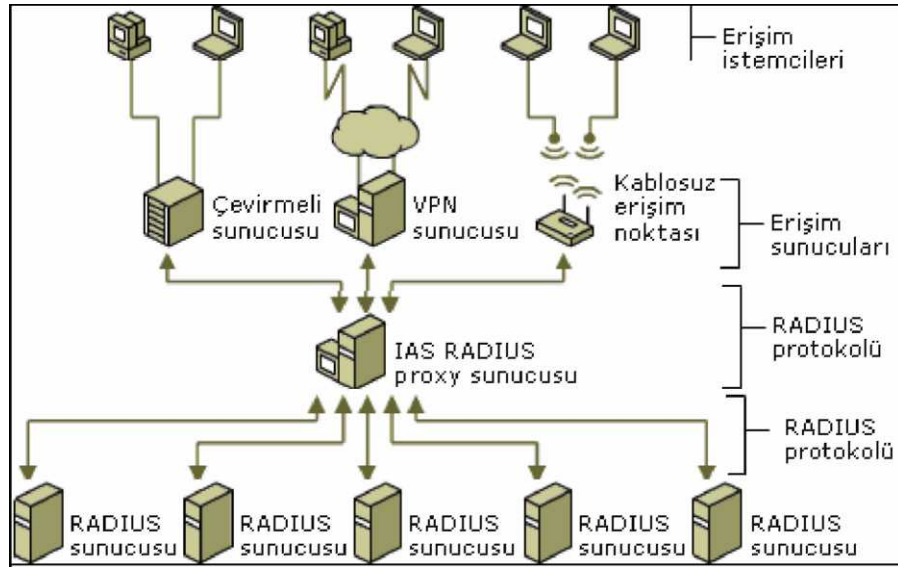
günlüğe depolanır.

Şekil 2.3'te IAS, çeşitli erişim istemcileri ve bir RADIUS Proxy'si için bir RADIUS sunucusu olarak gösterilmektedir. IAS, gelen RADIUS "Erişim-İsteği" iletilerinin kullanıcı kimlik bilgilerinin doğrulanmasında bir Active Directory etki alanı kullanır. IAS bir RADIUS sunucusu olarak kullanıldığında, RADIUS iletileri, ağ erişimi bağlantıları için kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemlerini aşağıdaki şekilde sağlar:

1. Dial-up ağ erişimi sunucuları, VPN sunucuları ve kablosuz erişim noktaları gibi erişim sunucuları, erişim istemcilerinden bağlantı istekleri alırlar.
2. Kimlik doğrulama, yetkilendirme ve hesap oluşturma protokolü olarak RADIUS kullanacak şekilde yapılandırılmış erişim sunucusu bir "Erişim-İsteği" iletisi oluşturur ve bunu IAS sunucusuna gönderir.
3. IAS sunucusu "Erişim-İsteği" iletisini değerlendirir.
4. IAS sunucusu, gerekirse erişim sunucusuna bir "Erişim-İtirazı" iletisi gönderir. Erişim sunucusu itirazı işler ve IAS sunucusuna güncelleştirilmiş bir "Erişim-İsteği" gönderir.

5. Kullanıcı kimlik bilgileri denetlenir ve bir etki alanı denetleyicisine yapılan güvenli bir bağlantı yoluyla kullanıcı hesabının arama özellikleri alınır.
6. Bağlantı girişimi, hem kullanıcı hesabının arama özellikleri ile hem de uzaktan erişim ilkeleri ile yetkilendirilir.
7. Bağlantı girişiminin kimliği doğrulanıp yetkilendirilirse, IAS sunucusu erişim sunucusuna bir "Erişim-Onayı" iletisi gönderir. Bağlantı girişiminin kimliği doğrulanmaz veya yetkilendirilmezse, IAS sunucusu erişim sunucusuna bir "Erişim-Reddi" iletisi gönderir.
8. Erişim sunucusu erişim istemcisi ile ilgili bağlantı sürecini tamamlar ve IAS sunucusuna (ki burada ileti günlüğe kaydedilir) bir "Hesap-İsteği" iletisi gönderir.
9. IAS sunucusu erişim sunucusuna bir "Hesap-Yanıtı" iletisi gönderir.

Erişim sunucusu ayrıca bağlantının kurulduğu süre içinde, erişim istemcisi bağlantısı kapatıldığında, erişim sunucusu başlatıldığında ve durdurulduğunda "Hesap-İsteği" iletileri gönderir.



Şekil 2.4 RADIUS Proxy'si olarak IAS'in kullanılması

### 2.6.2 IAS'in RADIUS proxy'si olarak kullanılması

IAS; RADIUS istemcileri (erişim sunucuları) ile bağlantı girişimi için kullanıcı kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemleri gerçekleştiren RADIUS sunucuları

arasında RADIUS iletilerinin yönlendirilmesini sağlamak için bir RADIUS Proxy'si olarak kullanılabilir.

RADIUS Proxy'si olarak kullanıldığında IAS, RADIUS erişim ve hesap oluşturma iletilerini

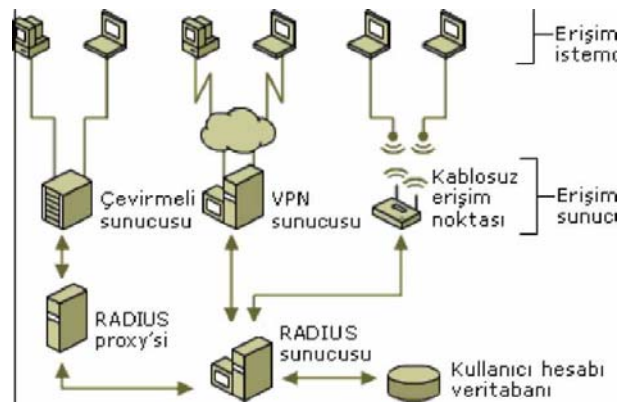
1. IAS RADIUS Proxy'si "Erişim-İsteği" iletilerini alır ve yerel olarak yapılandırılmış bağlantı isteği ilkelerini temel alarak "Erişim-İsteği" iletilerini nereye iletileceğini belirler.
2. IAS RADIUS Proxy'si "Erişim-İsteği" iletilerini uygun RADIUS sunucusuna gönderir.
3. RADIUS sunucusu "Erişim-İsteği" iletilerini değerlendirir.
4. Gerekirse, RADIUS sunucusu IAS RADIUS Proxy'sine bir "Erişim-İtirazı" iletileri gönderir. Erişim sunucusu erişim istemcisi ile ilgili itirazı işler ve IAS RADIUS Proxy'sine güncelleştirilmiş bir "Erişim-İsteği" gönderir.
5. RADIUS sunucusu bağlantı girişiminin kimliğini doğrular ve yetkilendirir.
6. Bağlantı girişiminin kimliği doğrulanıp yetkilendirilirse, RADIUS sunucusu IAS RADIUS Proxy'sine bir "Erişim-Onayı" iletileri gönderir. Bağlantı girişiminin kimliği doğrulanmazsa veya yetkilendirilmezse, RADIUS sunucusu IAS RADIUS Proxy'sine bir "Erişim-Reddi" iletileri gönderir.
7. Erişim sunucusu erişim istemcisi ile ilgili bağlantı sürecini tamamlar ve IAS RADIUS Proxy'sine bir "Hesap-İsteği" iletileri gönderir. IAS RADIUS Proxy'si hesap oluşturma verilerini kaydeder ve iletiyi RADIUS sunucusuna iletir.
8. RADIUS sunucusu IAS RADIUS Proxy'sine bir "Hesap-Yanıtı" gönderir.

## 2.7 RADIUS Altyapı Bileşenleri

Bir RADIUS kimlik doğrulama, yetkilendirme ve hesap oluşturma altyapısı aşağıdaki bileşenlerden oluşur:

- RADIUS Proxy'leri
- RADIUS sunucuları
- Kullanıcı hesabı veritabanları [12].
- Erişim istemcileri Erişim sunucuları (RADIUS istemcileri)

Bu bileşenler Şekil 2.5'de gösterilmiştir.



Şekil 2.5 RADIUS altyapı bileşenleri

**Erişim İstemcileri:** Daha geniş bir ağa bir düzeyde erişim gerektiren bir aygıttır. Erişim istemcilerine örnek olarak, dial-up (çevirmeli) ya da VPN istemcileri, kablosuz istemciler veya bir switch'e bağlı LAN (Local Area Network) istemcileri verilebilir.

**Erişim Sunucuları (RADIUS İstemcileri):** Daha geniş bir ağa bir düzeyde erişim sağlayan bir aygıttır. Bir RADIUS altyapısı kullanan erişim sunucusu aynı zamanda, bağlantı isteklerini ve hesap oluşturma iletilerini bir RADIUS sunucusuna gönderen RADIUS istemcisidir. Erişim sunucularına örnek olarak aşağıdakiler verilebilir:

- Bir kuruluş ağına veya internete uzaktan erişim bağlantısı sağlayan ağ erişim sunucuları, yönlendirme ve uzaktan erişim hizmetini çalıştıran ve bir kuruluş intranetine normal bir dial-up veya VPN uzaktan erişim hizmeti sağlayan bir bilgisayar,
- Bir kuruluş ağına fiziksel düzeyde erişim sağlayan, kablosuz aktarım ve alıcı teknolojileri kullanan kablosuz erişim noktaları,
- Bir kuruluş ağına fiziksel düzeyde erişim sağlayan, ethernet gibi LAN teknolojilerini kullanan switchler.

**RADIUS Proxy'leri:** RADIUS bağlantı isteklerini ve hesap oluşturma iletilerini

RADIUS istemcileri (ve RADIUS Proxy'leri) ile RADIUS sunucuları (veya RADIUS Proxy'leri) arasında ileten veya yönlendiren bir aygıttır. RADIUS Proxy'si, RADIUS iletilerini uygun RADIUS sunucusuna yönlendirmek için RADIUS iletilerindeki bilgileri kullanır. Kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemlerinin farklı kuruluşlardaki birden fazla RADIUS sunucusunda yapılması gerektiğinde, RADIUS Proxy'si; RADIUS iletileri için bir iletilme noktası olarak kullanılabilir.



**RADIUS Sunucuları:** RADIUS istemcileri veya RADIUS Proxy'leri tarafından gönderilen bağlantı isteklerini veya hesap oluşturma iletilerini alan ve işleyen bir aygıttır. Bağlantı istekleri söz konusu olduğunda, RADIUS sunucusu bağlantı isteğindeki RADIUS özniteliklerinin listesini işler. Kullanıcı hesabı veritabanındaki kuralları ve bilgileri temel alarak, RADIUS sunucusu bağlantısının kimliğini doğrular, yetkilendirir ve bir "Erişim-Onayı" ya da bir "Erişim-Reddi" iletisi olarak geri gönderir. "Erişim-Onayı" iletisi, erişim sunucusu tarafından bağlantı süresi ile ilgili olarak uygulanan bağlantı kısıtlamalarını içerebilir.

**Kullanıcı Hesabı Veritabanları:** Kimlik doğrulama, yetkilendirme ve bağlantı parametresi bilgilerini içeren kullanıcı hesabı özelliklerini doğrulamak için, kullanıcı hesaplarının ve bunların bir RADIUS sunucusu tarafından denetlenebilen özelliklerinin bir listesidir. Kimlik doğrulaması yapılacak kullanıcı hesapları farklı türden bir veritabanında ise, IAS, kimlik doğrulama isteğini kullanıcı hesabı veritabanına erişimi olan bir RADIUS sunucusuna iletecek bir RADIUS Proxy'si olarak yapılandırılabilir.

IAS'nin kullanabileceği kullanıcı hesabı veritabanları; yerel güvenlik hesapları yöneticisi, bir Microsoft Windows 2003 Server etki alanı veya Active Directory dizin hizmetidir. Active Directory söz konusu olduğunda IAS, üyesi olduğu bir etki alanında, iki yönlü güven sağlanmış etki alanlarında ve etki alanı denetleyicilerinin bulunduğu güvenilen bölgelerde kullanıcı veya bilgisayar hesapları için kimlik doğrulama ve yetkilendirme sağlayabilir. Bu çalışmada, kullanıcı hesabı veritabanı olarak Active Directory dizin hizmeti kullanılmıştır. Bir sonraki başlık kapsamında Active Directory hakkında genel bilgiler verilecektir.

## 2.8 Active Directory Dizin Hizmeti

Ağdaki nesnelere hakkında bilgi depolayan sıradüzenli yapı, "Dizin" olarak adlandırılır. Veri deposu olarak da bilinen dizin, Active Directory nesnelere hakkında bilgiler içerir. Bu nesnelere genelde; sunucular, birimler, yazıcılar ile ağ kullanıcıları ve bilgisayar hesapları gibi paylaşılan kaynakları içerir. Active Directory gibi bir dizin hizmeti, dizin verilerini depolamayı ve bu verileri ağ kullanıcıları ile yöneticiler için kullanılabilir kılmayı sağlayacak yöntemler sunar ve dizin bilgilerinden mantıksal ve hiyerarşik bir düzen oluşturmak için yapılandırılmış bir veri deposu kullanır. Örneğin, Active Directory, adlar, parolalar, telefon numaraları vb. gibi kullanıcı hesapları hakkında bilgi depolar ve aynı ağ üzerindeki diğer kullanıcılara bu bilgilere erişim olanağı verir. Active Directory; kullanıcı, bilgisayar ve ağ kaynakları hakkında bilgilerin saklandığı, etki alanı içerisindeki kaynaklar ve bu kaynaklara erişim bilgilerinin saklandığı ve erişim denetiminin yapıldığı bir hizmetler bütünü olarak da tanımlanabilir. Ağ kaynakları

yönetiminin merkezileştirilmesi, kaynak yönetiminin ilgili kullanıcılara yetki vererek merkezi yönetimin yetkilerinin dağıtılması, nesnelerin güvenli olarak mantıksal yapıda saklanması ve ağ trafiğinin en iyi şekilde kullanılması Active Directory'nin temel fonksiyonları arasında sayılabilir [2].

### **2.8.1 Active Directory için güvenlik bilgileri**

Active Directory, yerleşik oturum açma kimlik doğrulaması ve kullanıcı yetkilendirmesi kullanan ağlar için güvenli bir dizin ortamı sağlar. Bunlar LSA'nın (Local Security Authority-Yerel Güvenlik Yetkilisi) temel özellikleridir. Oturum açma kimlik doğrulaması ve kullanıcı yetkilendirmesi varsayılan olarak kullanılabilir ve ağ erişimi ile ağ hizmetleri için anında koruma sağlar. Active Directory, ağ erişimine izin vermeden önce kullanıcının kimliğinin onaylanmasını gerektirir; bu işlem "Kimlik Doğrulama" olarak bilinir. Etki alanına (ya da güvenli etki alanlarına) erişim kazanmak için kullanıcıların tek yapması gereken, tek bir oturum sağlamaktır. Active Directory kullanıcının kimliğini onayladığında kimlik doğrulaması yapan etki alanı denetleyicisindeki LSA, kullanıcının ağ kaynaklarına erişim düzeyini belirleyen bir erişim simgesi üretir. Active Directory, oturum açma sırasında kimlik sağlaması için kullanılan birçok güvenli internet standardında protokol ve kimlik doğrulama mekanizması sağlar, bunların arasında SSL (Secure Socket Layer) kullanan Kerberos V5, X.509 v3 sertifikaları, akıllı kartlar, genel anahtar alt yapısı ve basit dizin erişim protokolü (LDAP) sayılabilir.

Kimlik doğrulama ile güvenli ağ erişimine ek olarak, Active Directory kullanıcı yetkilendirmesi basitleştirilerek paylaşılan kaynakları korumaya yardım edilir. Kullanıcı oturumu Active Directory tarafından kimlik doğrulamasından geçtiğinde, bu kullanıcıya güvenlik grupları yoluyla atanan kullanıcı hakları ve paylaşılan kaynaklar için atanan izinler, kullanıcının bu kaynağa erişmek için yetkili olup olmadığını belirler. Bu yetkilendirme işlemi, paylaşılan kaynakları yetkisiz erişime karşı korur ve yalnızca yetkili kullanıcı ve grupların erişimine izin verir.

### **2.8.2 Active Directory'de erişim denetimi**

Güvenlik nedeniyle yöneticiler, paylaşılan kaynaklara kullanıcı erişimini yönetmek için erişim denetimini kullanabilir. Active Directory'de erişim denetimi, farklı erişim düzeyleri veya nesnelere "Tam Denetim", "Yazma", "Okuma" veya "Erişim Yok" gibi izinler ayarlayarak, nesne düzeyinde yönetilir. Active Directory içinde erişim denetimi, farklı kullanıcıların Active Directory nesnelere kullanma şeklini tanımlar. Varsayılan olarak, Active Directory içindeki

nesnelerle ilgili izinler için en güvenli ayarlar belirlenir. Active Directory nesnelerinde erişim denetimini tanımlayan öğeler, güvenlik tanımlayıcılarını, nesne devralmalarını ve kullanıcı kimlik doğrulamasını içerir.

### 2.8.3 Dizin erişim protokolü (LDAP)

Active Directory istemcileri, ağda oturum açarken ve paylaşılmış kaynakları ararken etki alanı denetleyicileri ile iletişim kurmalıdır. Etki alanı denetleyicilerine ve genel kataloglara erişim, Basit Dizin Erişimi Protokolü (LDAP) kullanılarak gerçekleştirilir. Adından da anlaşıldığı üzere LDAP, diğer karmaşık dizin erişim iletişim kurallarına gerek kalmadan, dizin hizmetlerine erişim için verimli bir yöntem olarak TCP/IP ağlarında kullanılmak üzere tasarlanmış bir iletişim kuralıdır. Bir dizindeki bilgileri sorgulamak ve değiştirmek için hangi işlemlerin yapılabileceğini ve dizindeki bilgilere nasıl güvenli bir biçimde erişilebileceğini tanımladığından, dizin nesnelerini bulmak veya sıralamak ve Active Directory'yi sorgulamak veya yönetmek için LDAP hizmeti kullanılabilir.

### 2.8.4 Kullanıcı ve bilgisayar hesapları

Active Directory kullanıcı ve bilgisayar hesapları (ve gruplar), bilgisayar veya kişi gibi fiziksel bir varlığı temsil eder ve güvenlik ilkeleri olarak da adlandırılabilir. Güvenlik ilkeleri, etki alanı kaynaklarına erişimde kullanılabilen, otomatik olarak atanan güvenlik kimlikleri (SID-Security Identity) olan dizin nesnelere aittir.

**Kullanıcı Hesapları:** Active Directory; "Yönetici" (Administrator), "Konuk" (Guest) ve "Yardımcı Asistan" (HelpAssistant) olmak üzere üç yerleşik kullanıcı hesabını barındırır. Bir etki alanı oluşturulduğunda, bu yerleşik kullanıcı hesapları otomatik olarak oluşturulur. Her yerleşik hesabın farklı hak ve izin birleşimi vardır. Etki alanındaki en kapsamlı haklar ve izinler yönetici hesabına aittir; konuk hesabının hakları ve izinleri ise sınırlıdır. Kullanıcı kimlik doğrulaması veya yetkilendirilmesi için güvenliğin temininde, ağa Active Directory kullanıcıları ve bilgisayarlarını kullanarak katılacak her kullanıcı için bireysel bir kullanıcı hesabı oluşturulmalıdır. Her kullanıcı hesabı, bu hesaba atanan hakları ve izinleri denetlemek üzere bir gruba eklenebilir. Ağ için uygun hesapların ve grupların kullanılması, bir ağa oturum açan kullanıcıların belirlenebilmesini ve yalnızca izin verilen kaynaklara erişilebilmesini sağlar. Güçlü parolalar gerektirerek ve bir hesap kilitleme ilkesi uygulanarak, etki alanı saldırganlara karşı savunulabilir.

**Bilgisayar Hesapları:** Her bilgisayarın ya da bir etki alanına katılan her sunucunun bir bilgisayar hesabı vardır. Kullanıcı hesaplarına benzer bir şekilde, bilgisayar hesapları, bilgisayarların ağı ve etki alanı kaynaklarına erişimi için kimlik doğrulama ve denetim araçları sağlar. Dolayısıyla her bilgisayar adı benzersiz olmalıdır. Kullanıcı ve bilgisayar hesapları, Active Directory kullanıcıları ve bilgisayarları kullanılarak eklenebilir, devre dışı bırakılabilir, sıfırlanabilir veya silinebilir. Bilgisayar hesabı, bir bilgisayar bir etki alanına eklenirken de oluşturulabilir. Bir kullanıcı veya bilgisayar hesabı aşağıdaki işlemlerde kullanılabilir:

- **Bir kullanıcının veya bilgisayarın kimliğini doğrulamak:** Kullanıcı hesabı, kullanıcının bilgisayarlara ve etki alanlarına, etki alanı tarafından doğrulanabilen bir kimlikle oturum açmasını sağlar. Ağa oturum açan her kullanıcının benzersiz bir kullanıcı hesabı ve parolası olmalıdır.
- **Etki alanı kaynaklarına erişim izni vermek veya reddetmek:** Kullanıcının kimliği doğrulandıktan sonra, kaynakta o kullanıcı için atanan açık izinlere bağlı olarak, kullanıcıya etki alanı kaynaklarına erişim yetkisi verilir veya bu kaynaklara erişimi engellenir.
- **Diğer güvenlik ilkelerini yönetmek:** Güvenilen dış etki alanındaki her güvenlik ilkesi için yerel etki alanında yabancı bir güvenlik ilkesi oluşturulur.
- Kullanıcı veya bilgisayar hesabı kullanarak gerçekleştirilen işlemleri denetlemek amacıyla kullanılabilir.

### 2.8.5 Active Directory dizin hizmetinde grup kavramı

Grup; tek bir birim olarak yönetilebilen, kullanıcı ve bilgisayar hesapları, kişiler ve diğer gruplardan oluşan bir topluluktur. Belirli bir gruba ait kullanıcılar ve bilgisayarlara grup üyeleri olarak başvurulur. Grupları kullanarak, izinleri ve hakları tek tek hesaplara atamak yerine bir kerede bir izin ve haklar kümesi birçok hesaba atanabilir ve böylece yönetim basitleştirilebilir. Active Directory grupları aşağıdakilerin yapılmasına olanak sağlar:

- Paylaşılan bir kaynak için kullanıcılar yerine gruba izin atanarak yönetim basitleştirilir. Böylece kaynak üzerindeki erişim, grubun tüm üyelerine atanır.
- Önce Grup İlkesi (Group Policy) üzerinden bir gruba kullanıcı hakları atanarak yönetim temsil edilir, daha sonra gereken üyeler aynı haklarına sahip olması istenen gruba eklenir.

Grupların (güvenlik grubu veya dağıtım grubu) etki alanı ağacı veya bölgesinde grubun hangi çapta uygulandığını tanımlayan evrensel, genel ve yerel etki alanı olmak üzere üç farklı bir kapsamı vardır.

Yerel etki alanı kapsamlı gruplar, tek bir etki alanındaki kaynaklara erişimi tanımlama ve yönetmeye yardımcı olur. Genel, evrensel, yerel etki alanı kapsamlı gruplar veya hesaplar bu grubun üyeleri olabilir. Örneğin, belli bir yazıcıya beş kullanıcı erişimi vermek için, beş kullanıcı hesabı da yazıcının izinler listesine eklenebilir. Ancak, daha sonra bu beş kullanıcıya yeni bir yazıcı için erişim vermek istenirse, yeni yazıcının izinler listesinde beş hesabın tümünün yeniden belirtilmesi gerekir. Küçük bir planlamayla, her zaman yapılan bu yönetim görevi, yerel etki alanı kapsamlı bir grup oluşturularak ve bu grup için yazıcıya erişim izni atanarak basitleştirilebilir. Beş kullanıcı hesabı genel kapsamlı bir grubun içine konur ve bu grup, yerel etki alanı kapsamlı gruba eklenir. Beş kullanıcıya yeni bir yazıcı için erişim vermek istendiğinde, yerel etki alanı kapsamlı grup için yeni yazıcının erişim izni atanır. Böylece genel kapsamlı grubun tüm üyeleri, otomatik olarak yeni yazıcıya erişim hakkı kazanmış olur.

Genel kapsamlı gruplar, kullanıcı ve bilgisayar hesapları gibi günlük bakım gerektiren dizin nesnelerini yönetmek için kullanılır. Kendi etki alanları dışında yinelenmedikleri için genel kapsamlı bir grup içindeki hesaplar, genel kataloğa ek yineleme işlemi getirilmeden sık sık değiştirilebilir. Her ne kadar hak ve izin atamaları yalnızca atanmış oldukları etki alanında geçerli olsa da, genel kapsamlı gruplar uygun etki alanları boyunca uygulanarak, aynı amaçlı hesaplara başvurular bir araya toplanabilir. Böylece, etki alanları boyunca grup yönetimi daha basitleşir ve verimli hale gelir. Örneğin, Avrupa ve ABD olmak üzere iki etki alanlı bir ağda, ABD etki alanında Muhasebe adlı genel kapsamlı bir grup varsa, (Avrupa etki alanında muhasebe işlevi olmadığı sürece) Avrupa etki alanında da Muhasebe adlı bir grup olmalıdır.

Evrensel kapsamlı gruplar, etki alanlarına yayılmış grupları birleştirmek için kullanılır. Bunu yapmak için hesaplar genel kapsamlı gruplara eklenir ve bu gruplar evrensel kapsamlı grupların içine yerleştirilir. Bu stratejinin kullanılmasıyla, genel kapsama sahip gruplardaki herhangi bir üye değişikliğinin, evrensel kapsamlı grupları etkilememesi sağlanır.

### **2.8.6 Sertifika dağıtımları**

Bazı kimlik doğrulama yöntemleri bilgisayarların ve kullanıcıların kimliklerini doğrulamak için sertifika kullanabilir. Kimlik doğrulama yapmak için sertifika kullanacak şekilde yapılandırılmış bir bilgisayar bir sertifikayı kaydedemiyorsa, kimlik doğrulaması başarısız olur. Örneğin, IAS çalıştıran yeni bir bilgisayar yerel bir etki alanı denetleyicisi

tarafından etki alanına eklenirse, IAS sunucusu yeniden başlatılır ve grup ilkesi uygulanır. Grup ilkesi uygulandıktan ve sertifika kaydı yapılandırıldıktan sonra, IAS sunucusu sertifikayı bir CA (Certificate Authority-Sertifika Yetkilisi) ile kaydetmeyi dener. CA, sertifikayı kaydetmek için gerekli olan güvenlik izinlerine IAS sunucusunun sahip olup olmadığını anlamak için Active Directory'i sorgular. IAS sunucusunu etki alanına ekleyen etki alanı denetleyicisi IAS sunucusunun etki alanı üyeliği bilgilerini tüm etki alanına çoğaltmışsa, CA, IAS sunucusunun bir sertifika alıp almaması gerektiğini doğrulayabilir. Sonra CA, IAS sunucusuna bir sertifika kaydeder. Etki alanına oturum açarak veya "*gpupdate*" komutu çalıştırılarak grup ilkesi el ile yenilenebilir.

IAS sunucusunun etki alanı üyeliği ile ilgili bilgiler diğer etki alanı denetleyicilerine kopyalanmadığında, CA henüz IAS sunucusu hakkındaki bilgilere sahip olmayan bir etki alanı denetleyicisini sorgularsa; CA, IAS sunucusunun etki alanının üyesi olan bir bilgisayarda çalışıp çalışmadığını doğrulayamaz. CA, IAS sunucusunun sertifika kaydetmek için gereken güvenlik izinlerine sahip olup olmadığını doğrulayamadığından, IAS sunucusu için bir sertifika kaydedemez. Sonuç olarak, kimlik doğrulama başarısız olur ve sunucu ağa oturum açamaz.

## **2.9 IAS ile Kullanılan Kimlik Doğrulama Yöntemleri**

Erişim istemcilerinin kimliklerini doğrulama işlemi önemli bir güvenlik konusudur. Kimlik doğrulama yöntemlerinde genellikle bağlantı kurma işlemi sırasında karar verilen bir kimlik doğrulama iletişim kuralı kullanılır. Bunun yanında IAS, kimliği doğrulanmamış bağlantıları da destekler. Her kimlik doğrulama yönteminin güvenlik, kullanılabilirlik ve destek kapsamı açısından olumlu ve olumsuz yanları vardır. Kullanılan kimlik doğrulama yöntemini hem erişim sunucusunun, hem de istemcinin yapılandırması belirler.

IAS birden fazla kimlik doğrulama yöntemi kabul edecek şekilde yapılandırılabilir. Erişim sunucuları da bağlantıyı, ilk olarak en güvenli protokolü kullanarak, daha sonra ikinci derecede güvenli olanı ve sırasıyla diğerlerini kullanarak görüşmeye çalışacak şekilde yapılandırılabilir. Örneğin yönlendirme ve uzaktan erişim hizmeti, bir bağlantıyı görüşmek için önce EAP'ı kullanır sonra MS-CHAP v2, MS-CHAP ve en sonunda da CHAP'ı kullanır. Kimlik doğrulama yöntemi olarak EAP seçilirse erişim istemcisi ve IAS sunucusu arasında EAP türünde bir görüşme olur. Kimliği doğrulanmakta olan istemcinin türüne bağlı olarak, çeşitli kimlik doğrulama yöntemleri için uzaktan erişim ilkeleri kullanılabilir. Örneğin; biri VPN istemcileri, diğeri kablosuz istemciler için olmak üzere, her biri farklı kimlik doğrulama yöntemi kullanan iki uzaktan erişim ilkesi oluşturulabilir. VPN istemcileri için uzaktan erişim ilkesi, kimlik doğrulama yöntemi olarak akıllı kartlar veya sertifikalarla birlikte EAP-TLS

kullanacak şekilde, kablosuz istemciler için uzaktan erişim ilkesi ise, güvenli parola kimlik doğrulaması sağlayan PEAP-EAP-MS-CHAP v2 kullanacak şekilde yapılandırılabilir [13].

### **2.9.1 Korumalı genişletilebilir kimlik doğrulama protokolü (PEAP)**

PEAP (Protected Extensible Authentication Protocol-Korumalı Genişletilebilir Kimlik Doğrulama Protokolü), EAP (Extensible Authentication Protocol-Genişletilebilir Kimlik Doğrulama Protokolü) protokolleri ailesinin yeni bir üyesidir. Kablosuz bilgisayar gibi kimlik doğrulayan PEAP istemcisi ile IAS veya RADIUS sunucusu gibi bir PEAP kimlik doğrulayıcısı arasında şifrelenmiş kanal oluşturmak için TLS'i (Transport Layer Security-Aktarım Düzeyi Güvenliği) kullanır. PEAP bir kimlik doğrulama yöntemi belirtmez, ancak diğer EAP kimlik doğrulama protokolleri için ek güvenlik sağlar. 802.11 kablosuz istemci bilgisayarları için bir kimlik doğrulama yöntemi olarak kullanılır, ancak VPN veya diğer uzaktan erişim istemcileri için desteklenmez. PEAP istemcisi ile kimlik doğrulayıcı arasındaki PEAP kimlik doğrulama işlemi iki aşamalıdır. İlk aşamada, PEAP istemcisi ile kimlik doğrulayan sunucu arasında güvenli bir kanal oluşturulur. İkinci aşamada ise, EAP istemcisi ile kimlik doğrulayıcı arasında EAP kimlik doğrulaması sağlanır [12].

#### **2.9.1.1 TLS şifrelenmiş kanalı**

Kablosuz istemci bir kablosuz erişim noktası ile ilişkilidir. IEEE 802.11'e dayalı bir ilişkilendirme, istemci ile erişim noktası arasında güvenli bir ilişki oluşturulmadan önce "Açık Sistem" veya "Paylaşılan Anahtar" kimlik doğrulaması sağlar. İstemci ile erişim noktası arasında IEEE 802.11'e dayalı ilişkilendirme başarılı bir şekilde kurulduktan sonra, erişim noktası ile TLS oturumu görüşülür. Kablosuz istemci ile sunucu (IAS sunucusu) arasında kimlik doğrulama başarılı bir şekilde yapıldıktan sonra, bunların arasında TLS oturumu görüşülür. Bu görüşmede elde edilen anahtar bundan sonraki iletişimin tümünü şifrelemede kullanılır.

#### **2.9.1.2 EAP ile kimliği doğrulanmış iletişim**

EAP görüşmesi dahil, tüm EAP iletişimi TLS kanalı ile yapılır. IAS sunucusu, kullanıcının ve istemci bilgisayarın kimliğini EAP türünün belirlediği ve PEAP içinde kullanılmak üzere seçilen yöntemle doğrular (EAP-TLS veya EAP-MS-CHAPv2). Erişim noktası, iletileri yalnızca kablosuz istemci ile RADIUS sunucusu arasında iletir.

PEAP ile kullanmak üzere EAP-MS-CHAPv2 veya EAP-TLS şeklinde olan iki EAP türünden biri seçilebilir.

**EAP-MS-CHAPv2 ile PEAP:** EAP-MS-CHAPv2 ile PEAP'ın dağıtımı EAP-TLS'den daha kolaydır. Çünkü kullanıcı kimlik doğrulaması, sertifika veya akıllı kart yerine, parolaya dayalı kimlik bilgileriyle (kullanıcı adı ve parolası) yapılır. Yalnızca IAS veya RADIUS sunucusunun bir sertifikası olması gerekir. Ayrıca, sunucu sertifikası, istemci bilgisayarın güvendiği bir ortak sertifika yetkilisi tarafından verilebilir. PEAP-EAP-MS-CHAPv2, karşılıklı kimlik doğrulama yöntemini kullanarak MS-CHAPv2 üzerinde gelişmiş güvenlik sağlarken, izinsiz bir sunucunun en az güvenli kimlik doğrulama yöntemini görüşmesini önler ve TLS ile anahtar oluşturulmasını sağlar. PEAP-EAP-MS-CHAPv2, istemcinin sunucu tarafından sağlanan sertifikalara güvenmesini gerektirir.

**EAP-TLS ile PEAP:** Ortak anahtar sertifikaları, parolaya dayalı kimlik bilgileri kullananlardan çok daha sağlam bir kimlik doğrulama yöntemi sağlar. EAP-TLS ile PEAP, sunucu kimlik doğrulaması için sertifikaları, kullanıcı ve istemci bilgisayarı kimlik doğrulaması için ise sertifika veya akıllı kart kullanır. PEAP-EAP-TLS'yi kullanmak için, bir ortak anahtar altyapısı (PKI-Public Key Infrastructure) dağıtılması gerekir.

### 2.9.2 Genişletilebilir kimlik doğrulama protokolü (EAP)

Genişletilebilir Kimlik Doğrulama Protokolü EAP ile rasgele bir kimlik doğrulama mekanizması, bir uzaktan erişim bağlantısının kimliğini doğrular [14]. Kullanılacak tam kimlik doğrulama şeması, uzaktan erişim istemcisi ve kimlik doğrulamasını yapan arasında uzlaşmayla belirlenir. EAP, kullanıcının LAN'a erişimini garantilemeden önce bir kimlik doğrulayıcı ve kullanıcı arasındaki standart mesaj değişimini tanımlar. Her iki kısım tarafından da anlaşılması sağlanan bir kimlik doğrulama protokolüne dayanan istemci kimliğini tanımlamak için kimlik doğrulama sunucusuna izin verir. EAP protokolü cihazlar arasındaki mesajları taşımak için IP protokolü gerektirmez. İstemciler geçerli bir IP adresine gerek duymadan erişim noktaları ile iletişim kurabilirler ve mesajları iletmek için EAPoL (EAP over LAN) protokolünü kullanırlar. EAPoL, üzerinde kimlik doğrulama meydana gelebilecek kimlik doğrulayıcı ve kullanıcı arasında bir iletişim yolu sağlar ve EAP paketlerinin Ethernet, Token Ring veya FDDI yapıları içinde nasıl iletildiğini tarif eder. Bir ağa bir istemcinin kimliğini tanımlamak için EAP standart bir mesaj yapısı yaratır. Kimlik doğrulama protokolüne bağlı olarak bir istemci tarafından anlaşma sağlanır ve sunucu mesaj değişimindeki ayrıntıları değiştirebilir. Şekil 2.6 EAP istemcisi, kimlik doğrulayıcı ve kimlik doğrulama sunucusu arasında meydana gelen genel mesaj akışını gösterir.

EAP mesaj değişimini oluşturan adımlar aşağıdaki maddelerde verilmiştir:



- EAP istemcisi ağına bağlanır ve ağ üzerindeki erişim bilgisi için girişimde bulunur. İletişim EAPoL protokolü kullanılarak gerçekleştirilir.
- Kimlik doğrulayıcı, kullanıcıya bir EAP-Request/Identity mesajı gönderip onun kimlik bilgilerini sorarak istemciye cevap verir.
- İstemci EAPoL protokolünü kullanarak kimlik bilgisini bir EAP-Response/Identity mesajını ile birlikte kimlik doğrulayıcıya gönderir.
- Kimlik doğrulayıcı bu bilgileri kimlik doğrulama sunucusuna iletir.
- Kimlik doğrulama sunucusu bir parola sınaması içeren EAP-Request paketi ile kimlik doğrulayıcıya cevap verir ve kimlik doğrulama sunucusu tarafından desteklenen EAP kimlik doğrulama türünü belirler. Bu mesaj RADIUS protokolü üzerinden kimlik doğrulayıcıya geri iletir.
- Kimlik doğrulayıcı, EAPoL kullanarak kimlik doğrulama sunucusu tarafından istenen kimlik doğrulama türüyle sınamayı istemciye geri iletir.
- İstemci sınamayı gözden geçirir ve istenen EAP kimlik doğrulama protokolünü desteklerse, EAPoL'ü kullanarak onun kimlik bilgisi ile cevap verir.
- Kimlik doğrulayıcı, RADIUS protokolünü kullanarak kimlik doğrulama sunucusuna istemci kimlik bilgilerini gönderir.
- Eğer istemcinin kimlik bilgileri geçerliyse kimlik doğrulama sunucusu kimlik doğrulamasını ve istemci yetkilendirmesini yapar. Aksi takdirde, istemci reddedilir ve RADIUS protokolü kullanılarak uygun RADIUS Access-Accept veya Access-Reject mesajı kimlik doğrulayıcıya geri gönderilir.
- Kimlik doğrulayıcı RADIUS Access-Accept veya Access-Reject mesajını alır ve ağ erişimini buna göre yapılandırır.
- RADIUS Accept paketinin alınması üzerine kimlik doğrulayıcı, istemci portunu yetkili bir duruma geçirir ve ağ trafiği iletir.

EAP, uzaktan erişim istemcisiyle kimlik doğrulamasını yapan arasında açık uçlu bir görüşme yapılmasına olanak sağlar. Görüşme, kimlik doğrulamasını yapanın kimlik doğrulama bilgilerini istemesinden ve uzaktan erişim istemcisinin ona verdiği yanıtlardan oluşur. Yönlendirme ve uzaktan erişim varsayılan olarak, EAP-TLS ve MD5-Sınama (Message Digest 5 Challenge) desteği içerir. Belirli bir EAP kimlik doğrulama şeması, bir EAP türü olarak adlandırılır. Kimlik doğrulama işleminin başarıyla sonuçlandırılabilmesi için uzaktan erişim istemcisiyle kimlik doğrulayıcının aynı EAP türünü destekliyor olması gerekir.

### **2.9.2.1 EAP altyapısı**

EAP, herhangi bir EAP türü için bir eklenti parçası gibi mimari destek sunan bir dizi iç bileşendir. Başarılı kimlik doğrulaması için uzaktan erişim istemcisinde ve kimlik doğrulamasını yapanda aynı EAP kimlik doğrulama modülünün yüklü olması gerekir. İki EAP türü vardır: MD5-Sinama ve EAP-TLS. Bir EAP türüne ilişkin bileşenlerin her uzaktan erişim istemcisine ve her kimlik doğrulayıcısına yüklenmesi gerekir [15].

**MD5-Sinama:** PPP tabanlı CHAP ile aynı el sıkışma protokolünü kullanan gerekli bir EAP türüdür ancak istekler ve cevapları EAP iletileri olarak gönderilir. MD5-S inamanın en yaygın kullanımı kullanıcı adı ve parola güvenlik sistemlerini kullanarak, uzaktan erişim istemcilerinin kimlik bilgilerine kimlik doğrulama uygulamaktır.

**EAP-TLS:** Sertifika tabanlı güvenlik ortamlarında kullanılan bir EAP türüdür [16]. Uzaktan erişim kimlik doğrulaması için akıllı kart kullanılıyorsa, EAP-TLS kimlik doğrulama yöntemi kullanılmalıdır. EAP-TLS uzaktan erişim istemcisiyle kimlik doğrulayıcı arasında karşılıklı kimlik doğrulama, şifreleme yöntemi üzerinde anlaşma ve şifrelenmiş anahtar belirlemeyi sağlayarak en sağlam kimlik doğrulama ve anahtar belirleme yöntemini sunar. Yönlendirme ve uzaktan erişim çalıştıran, Windows kimlik doğrulaması veya RADIUS kullanacak şekilde yapılandırılmış olan ve bir etki alanının üyesi olan sunucularda desteklenir. Tek başına bir sunucu veya bir çalışma grubunun üyesi olarak çalışan bir uzaktan erişim sunucusu EAP-TLS'yi desteklemez. EAP-TLS'in temel sakıncası, her kullanıcının bir PKI sertifikasına sahip olmasını gerektirmesidir. Kullanıcı sertifikalarını yönetmek, iptal etmek ve dağıtmak için bir sertifika otoritesi işletiminde çok sağlam yönetsel bir yükü zorla kabul ettirir.

EAP kimlik tanımlama metotlarından olan EAP-TTLS (EAP-Tunneled Transport Layer Security) ve PEAP olarak isimlendirilen protokoller, EAP-TLS içindeki PKI engeline olan cevapta geliştirilir. Her ikisi de sunucunun kimlik doğrulamasını yapmak için TLS'i kullanır ve istemcinin kimlik doğrulamasını yapmak için CHAP, MD5 gibi diğer kimlik doğrulama metotlarının tünellemesini önerir. Böylece TLS'in güçlü kriptografik temeli korunmuş olur. EAP-TTLS, EAP-TLS'i kapsayan bir EAP protokolüdür ve sağlam şifreleme temeli oluşturduğu için taşıma katmanı güvenliğini kullanır [17]. Sertifikalara sahip olma gerekliliğinden dolayı kullanıcılarda değil sadece RADIUS sunucularında farklılık gösterir. Alışılmış kullanıcı isimleri ve parola bilgileri TLS içindeki güvenlik sınırında çevrelenip kullanıcının ağa kimlik doğrulaması yapılır. Bu yüzden EAP-TTLS'de TLS anlaşması karşılıklı veya tek yönlü olabilir (sadece sunucu, istemciye kimliklendirilir). Anlaşmayla kurulan güvenli bağlantı, var olan geniş yayımlı kimlik doğrulama altyapılarını kullanarak (RADIUS gibi) istemcinin kimlik

doğrularmasını yapmak için sunucuya izin verebilir. İstemcinin kimlik doğrularması bizzat EAP veya diğerk kimlik tanımlama protokolü olabilir.

### **2.9.2.2 EAP-RADIUS**

EAP-RADIUS bir EAP türü değıl, tüm EAP türlerindeki EAP iletilerinin bir kimlik doğrularayıcı tarafından kimlik doğrularması yapılmak üzere bir RADIUS sunucusuna geçirilmesidir. Kimlik doğrularayıcı olarak RADIUS kullanılan ortamlarda, EAP-RADIUS kullanılır. Bunun avantajı, EAP türlerinin her bir uzaktan erişim sunucusuna yüklenmesinin gerekmemesi, yalnızca RADIUS sunucusuna yüklenmesinin yeterli olmasıdır. En yaygın EAP-RADIUS kullanımlarından birinde, yönlendirme ve uzaktan erişimi çalıştıran bir sunucu, EAP kullanacak ve kimlik doğrularmasında IAS sunucusunu kullanacak şekilde yapılandırılır. Bir bağlantı yapıldığında, uzaktan erişim istemcisi, EAP kullanımı konusunda uzaktan erişim sunucusuyla uzlaşır. İstemci uzaktan erişim sunucusuna bir EAP iletisi gönderdiğinde, uzaktan erişim sunucusu EAP iletisini bir RADIUS iletisi olarak saklar ve iletiyi kendi yapılandırılmış IAS sunucusuna gönderir. IAS sunucusu EAP iletisini işler ve uzaktan erişim sunucusuna bir RADIUS saklı EAP iletisi gönderir (Şekil 2.7).



**Şekil 2.7** EAP-RADIUS işlemi

Daha sonraki adımda uzaktan erişim sunucusu EAP iletisini uzaktan erişim istemcisine iletir. Bu yapılandırmada, uzaktan erişim sunucusu yalnızca bir geçiş aygıtıdır. EAP iletilerine uygulanan tüm işlemler, uzaktan erişim istemcisinde ve IAS sunucusunda gerçekleşir [8]. Bundan sonra anlatılacak kimlik doğrularma protokolleri, IEEE 802.11i protokolü ile gerçekleştirilen ve RADIUS protokolü ile desteklenen protokollerdir.

### **2.9.3 MS-CHAP**

Microsoft, LAN tabanlı kullanıcıların alışık oldukları fonksiyonları Windows ağlarında kullanılan karma algoritmalarla bütünleştirerek, uzak Windows tabanlı iş istasyonlarının kimliğini doğrulamak için MS-CHAP'yi (Microsoft Challenge Handshake Authentication Protocol-Microsoft Karşılıklı Kimlik Doğrularma) oluşturmuştur. MS-CHAP parola göndermeden bağlantıların kimliğini doğrulamak için bir sınaama-yanıtlama mekanizması

kullanır. Bunu oluşturmak için, MD4 (Message Digest 4 - İleti Özeti-4) ve DES (Data Encryption Standard) şifreleme algoritması kullanır. Bağlantı hatalarını raporlamak ve kullanıcı parolasını değiştirmek için mekanizmalar sağlayan MS-CHAP, CHAP'tan farklı olarak, kullanıcı parolasının geri döndürülebilir olarak şifrelendirilmiş biçimde depolanmasını gerektirmez.

#### **2.9.4 MS-CHAP v2**

Karşılıklı kimlik doğrulama, Microsoft noktadan noktaya şifreleme için daha güçlü başlangıç verisi şifreleme anahtarları üretimi ve gönderilen/alınan veriler için farklı şifreleme anahtarları sağlamada MS-CHAP v2 kullanılır. Parola değiştirme sırasında parola güvenliğini tehlikeye atma riskini en aza indirmek için bu sürüm kullanılır. MS-CHAP v2, MS-CHAP'ye göre daha güvenli olduğundan, tüm bağlantılarda (etkinleştirilmişse) MS-CHAP'den önce sunulur. MS-CHAP v2, hem sunucu hem de istemcinin kullanıcı parolası hakkında bilgi sahibi olduğunu kanıtladığı, karşılıklı kimlik doğrulama iletişim kuralıdır. Bu iletişim kuralında ilk olarak, uzaktan erişim sunucusu uzaktan erişim istemcisine kimlik sorma talebi göndererek kanıt ister. Ardından, uzaktan erişim istemcisi uzaktan erişim sunucusuna kimlik sorma talebi göndererek kanıt ister. Sunucu, istemciden gelen kimlik sorma talebine doğru cevap vererek kullanıcı parolası hakkında bilgi sahibi olduğunu kanıtlayamazsa, istemci bağlantıyı sonlandırır. Karşılıklı kimlik doğrulaması olmadan, uzaktan erişim istemcisi, yetkili olmayan uzaktan erişim sunucusuyla bağlantı kuramaz.

#### **2.9.5 CHAP**

CHAP (Challenge Handshake Authentication Protocol-Karşılıklı Kimlik Doğrulama Protokolü), kimlik doğrulama işlemi sırasında kullanıcı parolasının kendisinin değil, parola gösteriminin gönderildiği, geniş çapta desteklenen bir kimlik doğrulama yöntemidir. CHAP ile uzaktan erişim sunucusu uzaktan erişim istemcisine bir kimlik sorma dizesi gönderir. Uzaktan erişim istemcisi bir karma algoritma kullanarak, kimlik sorma isteğini temel alan bir MD5 karma sonucu ve kullanıcının parolasından hesaplanan bir karma sonucu hesaplar. Uzaktan erişim istemcisi MD5 karma sonucunu uzaktan erişim sunucusuna gönderir. Kullanıcı parolasının karma sonucuna da erişimi olan uzaktan erişim sunucusu, karma algoritmasını kullanarak aynı hesaplamayı yapar ve sonucunu istemci tarafından gönderilen sonuçla karşılaştırır. Sonuçlar eşleşirse, uzaktan erişim istemcisinin kimlik bilgileri gerçek kabul edilir. Karma algoritması tek yönlü şifreleme sağlar ve buna göre, bir veri bloğu için karma sonucunu

hesaplamak kolaydır, ancak özgün veri bloğunu karma sonucundan hesaplamak matematiksel olarak mümkün değildir.

### 3. PORT TABANLI KİMLİK DOĞRULAMA

Bu tez çalışması kapsamında, DPÜ Kampüs ağında karşılaşılan problemlerin çözümüne yönelik olarak otomatik VLAN yapılandırması ve ağa erişim yapacak tüm kullanıcıların IEEE 802.1x standardı ile kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmiştir. Bu bölümde, uygulamanın gerektirdiği materyaller olarak kullanılan otomatik VLAN yapılandırmaları ile IEEE 802.1x kimlik doğrulama işlemleri tanıtılacak ve bu işlemlerin gerekliliğinden bahsedilecektir.

#### 3.1 Sanal Yerel Alan Ağları (VLAN)

Günümüzde önemli ağ yapılandırma tekniklerinden birisi olarak kabul edilen VLAN'lar, hedef ve kaynak MAC (Media Access Control) adreslerini kullanarak anahtarlama işlemini gerçekleştiren bir switch üzerindeki portların mantıksal gruplandırılmasıyla oluşturulan ağlardır. Fiziksel olarak tek bir ağ gibi görünmesine karşın VLAN uygulaması ile sanal ağlar yaratılır ve bu sanal ağlar diğer ağların birçok özelliğini taşır. VLAN'lar genellikle kaynakların ve kullanıcıların yerleşimine, işlevine, departmanına, ya da kullanılan uygulama protokolüne göre düzenlenir.

İyi bir sanal ağ çözümü, yerel ve geniş alan ağlarını içeren bir kurum ağı olabileceği gibi bir kampüs veya bir şehir ağı da olabilir. Bu sayede yönlendirme ihtiyacı düşer ve veri iletim hızı artar. Geniş alan ağlarını da kapsayan kurumsal ağlarda birçok kullanıcının sık sık yer değiştirdiği, ağa yeni kullanıcıların eklendiği veya ağdan mevcut kullanıcıların silindiği göz önüne alınırsa, ağ adresi değiştirme işlemi çok zaman alacağından bu konular ağ ortamında problemlere neden olabilecektir. Ayrıca değişim tamamlanana kadar kullanıcılar ağa erişemeyecektir. Gelişmiş sanal ağ desteği sağlayan switchler kullanılarak bu sorunlar kolaylıkla çözülebilir. Bu sayede, kullanıcı ağın neresinden bağlanırsa bağlansın, sistem tarafından otomatik tanınarak aynı sanal ağ içinde yer almaya devam edecektir.

VLAN'lar sayesinde alt ağlar ya da broadcast (yayın) domainleri (etki alanı) oluşturularak broadcast'lar yalnızca bir VLAN içinde gönderilir. Her VLAN, ayrı bir yönlendirici (router) ile bölünmüş ağlar gibi ayrı bir ağ kimliğine sahip olmalıdır. Böylece sistemdeki bir bilgisayar, ağa bir broadcast gönderdiğinde bu broadcast sadece o bilgisayar ile aynı ağda olan bilgisayarlarca alınır, yani farklı bir ağda yer alan diğer bilgisayarlar bu broadcastten etkilenmezler. Bildirdiği gibi VLAN oluşturarak sisteme performans ve güvenlik

açısından avantajlar sağlansa da, kriterleri oluşturulan VLAN'ların farklı VLAN'larla iletişim kurmasında sıkıntılar yaşanmaktadır [18]. Sıkıntılıların giderilmesinde üçüncü katmanda çalışan yönlendiricilere ihtiyaç duyulur. Bu durumda farklı VLAN'lar yönlendirici üzerinden görüşebilir duruma gelir. Ancak farklı birimler arasındaki tüm iletişim, yönlendirici üzerinden geçmek zorunda olduğundan yönlendiricinin yükü artar. Bununla birlikte yönlendiriciye eklenecek erişim listelerindeki kurallarla iletişimin kontrol altına alınması sağlanır[3] [19].

### 3.2 Sanal Yerel Alan Ağ Türleri

Sanal ağlar oluşturabilmek için çeşitli yöntemler mevcuttur. Bazı switchler temel birtakım yeteneklere sahipken, diğerleri çok daha güçlü özellikler içerdiği için üreticiler kendi switch mimarilerine uygun metotlar geliştirmişlerdir. Bu yöntemler aşağıdaki maddelerde verilmiştir:

- **Port tabanlı sanal ağlar:** Sanal ağ oluşturmanın en basit yolu olup switch portlarının gruplandırılmasıyla oluşturulur. Gruplama işlemi bir switch üzerinde olabileceği gibi, birden çok switch üzerindeki portlardan da oluşabilir. Port tabanlı sanal ağ tanımları yapıldığında, bir port birden çok sanal ağa üye olamaz. Ayrıca cihazlar yer değiştirdiğinde, yer değiştiren kullanıcı için yeniden yapılandırma işlemi gerekir.
- **MAC tabanlı sanal ağlar:** MAC kaynak adreslerine göre cihazları sanal ağlara atamak mümkündür. Bu durumda her sanal ağ, bir MAC adres listesidir. MAC tabanlı sanal ağlarda cihaz, bina veya kampüs içinde yer değiştirirse bile aynı sanal ağda çalışmaya devam eder.
- **Protokol tabanlı sanal ağlar:** Az kullanılan protokol türlerini toparlamak için kullanılan bir yöntemdir. Ancak yaygın olarak kullanılan protokoller için broadcast desteği yetersizdir.
- **Kural tabanlı sanal ağlar:** En esnek sanal ağ yöntemidir. Kullanıcılar, ağ yöneticisi tarafından belirlenen kurallara göre tanımlanan sanal ağlara bir kez atandıktan sonra, fiziksel yerlerinden bağımsız olarak çalışmalarını sürdürebilmektedir.

### 3.3 Otomatik VLAN Kavramı

VLAN'ların kullanılmasının önemi; belli işleri yapmak üzere kurumsal bir ağda farklılaştırılarak ayrılmış yerel ağların dinamik yapılarındaki değişimlerden etkilenmemeleri ve kısmi de olsa bir gizlilik sağlamasından gelmektedir. VLAN'lar fiziksel yapıdan bağımsız olduğu için, ağ üzerindeki sunucuların başka bir noktaya taşınması veya yenilerinin eklenmesi

işlemi kolaylaşmış olur. Böylece sistemdeki iş yükü azalır, maliyet düşer ve isteklere verilen yanıt süresi kısalmır.

Oluşturulan bir VLAN'ın statik ya da dinamik olarak switch portlarına atanması gerekir. Bir statik VLAN oluşturulurken ağ yöneticisi switchin belirli portlarını VLAN'a dahil eder ve portlar ağ yöneticisi tarafından değiştirilene kadar bu VLAN'ın üyesi olarak kalır. Dinamik VLAN oluşturmada ise, ağ yöneticisi sistemin kurulumu aşamasında ağda bulunan tüm cihazların MAC adreslerini bir yazılım aracılığıyla veri tabanına alıp ağdaki adreslerin VLAN'lara üyeliğini gerçekleştirir. Bu yöntemde MAC adresleri kullanılarak hangi cihazın hangi VLAN'a ait olacağı belirlenir [20].

Dinamik VLAN teknolojisi sayesinde ağ üzerinde bulunan bir son kullanıcının yeri değiştiğinde, yeni gittiği yerdeki switch, merkezi MAC veritabanından kullanıcının hangi VLAN'a üye olduğunu bulur ve portu o VLAN'a üye yapar. Böylece merkezi bir bağlantı panosu üzerindeki fiziksel bağlantının yeniden düzenlenmesine gerek kalmadan, değişikliklerin ağ yönetimi denetim terminali üzerinden kolay bir şekilde yapılmasıyla esnek, alternatif bir çözüm sunulmuş olur. Ayrıca switch portlarının ayrı VLAN'lara atanmasıyla her VLAN'a ait porttan yapılan broadcast sadece o VLAN'a ait diğer portlara iletilir. Bu özellik, ağ performansını arttırmanın yanı sıra ağ yönetimi ve güvenliğini de kolaylaştırır. Broadcast trafiği VLAN içerisine hapsediğundan sistemin görünür bant genişliği artar ve sistemden daha yüksek hızlarda veri akışı sağlanır [3] [4]. Bunun yanında, ağ yöneticileri "Erişim Listeleri" (Access Lists) yaratarak, hangi adreslerin ağa erişeceğini belirler, böylece veri trafiği denetim altında tutulmuş olur.

Sistem güvenliği temelinin kullanıcıların kimliklerinin doğru belirlenmesi ve yetkilendirmesi işlemine dayandığını önceki bölümlerde belirtmiştik. Eğer sistemdeki bir kullanıcının kimliği belirlenemiyorsa kişilerin yaptıklarından sorumlu olması mümkün olmayacağından büyük bir karmaşa yaşanır. Bu karmaşayı önlemek için RADIUS sunucunda, kullanıcı kimlikleri belirlenir [7]. Kimlik doğrulama işlemi esnasında kullanıcıların kişisel bilgileri, kimlik doğrulama işlemi yapacak RADIUS sunucusu üzerindeki veri tabanında saklanır. Bu işlem kullanıcıların kimlik bilgilerinin doğrulandan emin olmak için yapılır. RADIUS sunucusu üzerinde kullanılan bu teknoloji sayesinde ağ içindeki farklı veri kaynaklarına erişme hakkına sahip kullanıcıların yetkileri tek bir noktadan belirlenebilmekte ve yönetilebilmektedir. Böylelikle, dağıtık yapıdaki kullanıcıların yönetimi kolaylaştırılmaktadır.

Ağ içerisinde ve dışında yer alan kullanıcılara kritik sistem verilerine erişim hakkının verilmesi, iş akışını hızlandırmak ya da daha iyi servis vermek gibi avantajlar sağlasa da,

güvenlik açısından dikkat edilmesi gereken durumlar yaratabilir. Kullanıcıların kritik verilere doğrudan erişimini sağlayan, sunucu merkezindeki kayıtların tutulduğu veritabanına erişim kullanıcı bazında ayarlanmalıdır. Kullanıcılar veritabanına nasıl erişirlerse erişsinler bir veritabanında sadece kendilerinin görmelerine izin verilmiş olan kayıtlara ulaşırlar. Bu filtreleme işlemi ağ yöneticisi tarafından veritabanı düzeyinde tanımlanmaktadır. Böylece daha önce olduğu gibi güvenliğin, veriye ulaşan tüm uygulamalarda ayrı ayrı kodlanması gerekliliği ortadan kalkar [7]. Bu da otomatik VLAN kavramını doğurur.

Otomatik VLAN ataması olarak adlandırılan özellik; 802.1x port kimlik doğrulamasıyla gerçekleştirilir. Otomatik VLAN ataması, bir kullanıcı hesabına belirli bir VLAN' ı atamak için ağ yöneticisine izin verir. Kullanıcı 802.1x port kimlik doğrulamasını kullanarak başarılı bir şekilde ağa kendini tanıttığında otomatik olarak kendi VLAN' ına yerleştirilir. Kullanıcı RADIUS protokolünü kullanarak IAS sunucusuna 802.1x bilgilerini gönderir. IAS sunucusu üzerindeki uzak erişim politikaları, kullanıcı hesabının özel bir VLAN grubunun üyesi olup olmadığına karar vermek için kullanılır. Eğer kullanıcı hesabı bir VLAN grubunun parçası ise ve kimlik doğrulaması başarılı bir şekilde gerçekleşmişse VLAN grubu ile ilişkilendirilen kullanıcı bilgileri RADIUS özelliği kullanılarak kimlik doğrulayıcıya geri gönderilir. Kimlik doğrulayıcı üzerindeki kullanıcı portu dinamik olarak VLAN bilgisi eşleşmesiyle VLAN'a atanır ve kullanıcı port tabanlı VLAN' ın bir üyesi haline gelir. Bu özellik sadece port-tabanlı VLAN'larda desteklenir [21].

### 3.4 Port Tabanlı Kimlik Doğrulama İşlemi

Hem kablolu hem de kablosuz ağları kapsayan IEEE 802 standartlarından IEEE 802.11 standardı, çoğunlukla kablosuz yerel ağları oluşturan cihazların kullanıma uygun olarak tasarlanmıştır. IEEE 802.11 çalışma grubu tarafından geliştirilen IEEE 802.11i protokolü; kimlik doğrulama, şifreleme (encryption), yetkilendirme ve anahtar yönetimi (key management) işlemlerini gerçekleştirebilmektedir. Gizlilik ve mesaj bütünlüğünün sağlanması için güçlü bir şifreleme algoritmasının kullanıldığı IEEE 802.11i protokolünün yardımıyla servis kalitesi gelişmelerine uyum sağlama yoluna da gidilmiştir [22]. IEEE 802.11i standardının sağladığı pek çok faydadan birkaçı da şu şekilde özetlenebilir:

- WEP'de (Wired Equivalent Privacy - Kablolu Eşdeğer Gizlilik) olmayan anahtar yönetimini hiyerarşik bir şekilde sağlamaktadır.
- Karşılıklı kimlik doğrulama (mutual authentication) mevcuttur.



- Kimlik doğrulama için kullanılan IEEE 802.1x protokolü, üst katman kimlik doğrulama protokollerini de destekler.
- Güçlü bir şifreleme algoritması olan AES'i (Advanced Encryption Standard) kullanmaktadır.

İki katmandan oluşan IEEE 802.11i'nin alt katmanında gelişmiş kriptolama algoritmaları, üst katmanında ise kimlik doğrulama ve anahtar dağıtımı için gerekli 802.1x bulunmaktadır [6]. Kullanıcılar ağ kaynaklarına erişmeden önce kimlikleri doğrulanmakta, bu işlemden sonra üretilen oturum anahtarları dağıtılmakta ve bu anahtarlar kullanılarak üretilcek yeni anahtarlar ile güvenli veri transferi yapılmaktadır.

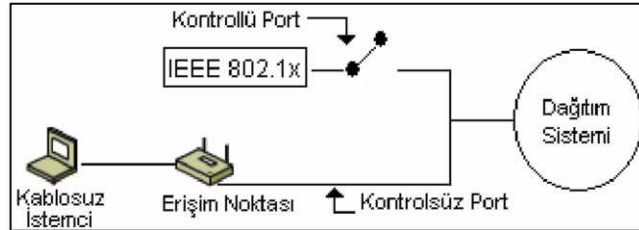
### 3.5 IEEE 802.1x Kimlik Doğrulaması

Kablolu ethernet ağlarına ve kablosuz 802.11 ağlarına kimliği doğrulanmış ağ erişimi sağlamak ve port tabanlı ağ erişim kontrolünü gerçekleştirmek için IEEE 802.1x standardı kullanılır [23]. 802.1x her ne kadar bir kimlik doğrulama ve yetkilendirmeye ait çalışma ortamı sağlamak anlamına gelse de, bir Noktadan Noktaya Topolojisi (Point to Point Protocol-PPP) ile her IEEE 802 tabanlı yerel alan ağı için çok elverişlidir ve özellikle güvenlik saldırılarına karşı çok daha hassastır. IEEE 802.11i standardı, karşılıklı kimlik doğrulama için 802.1x EAP tabanlı kimlik doğrulamayı uygulamaktadır. EAP, çoklu kimlik doğrulama metotlarını destekleyen bir kimlik doğrulama ortamıdır ve bu protokol ile LAN ortamına bağlanılır.

802.1x kablolu ağlar için geliştirilmesine karşın kablosuz ağlar için de kullanılmaktadır. Bu standart, istemci ile erişim noktası arasında bir kimlik doğrulama sunucusu (genellikle RADIUS) kullanarak kimlik doğrulama ve port tabanlı erişim kontrolü sağlamaktadır. 802.1x; İstemci (Supplicant), Kimlik Doğrulama Sunucusu (Authentication Server) ve Kimlik Doğrulayıcı (Authenticator) olmak üzere temelde 3 kısımdan oluşmaktadır. İstemci; kimlik doğrulama isteğinde bulduktan sonra kimlik doğrulayıcıya username/password bilgisini gönderir ve bu iletişim için EAP'yi kullanır. Kimlik doğrulama sunucusu; RADIUS gibi kimlik doğrulama işlemini gerçekleştiren bir sunucudur. İstemciden gelen username/password bilgisini doğrular ve onun erişime yetkisi olup olmadığını belirler. Kimlik doğrulayıcı; istemci ile kimlik doğrulama sunucusu arasında yer alan, 802.1x port güvenliğini sağlayan ve ağa erişimi kontrol eden bir erişim noktasıdır. Kullanıcıdan username/password bilgisini alır, RADIUS'a geçirir ve gerekli filtrelemeyi gerçekleştirir ya da RADIUS'tan gelen sonuçlara dayalı eyleme izin verir [7]. Dördüncü bölümde bu bileşenlere ek olarak kablosuz LAN için IEEE 802.1x standardının kapsadığı Ağ Erişim Portu (Network Access Port) ve Port Erişim Elemanı (Port Access Entity) gibi kimlik doğrulama bileşenlerinden de bahsedilecektir.

### 3.6 802.1x için Kontrollü ve Kontrolsüz Portlar

Kimlik doğrulayıcının port tabanlı erişim kontrolü, Şekil 3.1'de gösterildiği gibi tek bir fiziksel LAN portu aracılığıyla kablolu LAN'a erişim için farklı lojik port türlerini tanımlar.

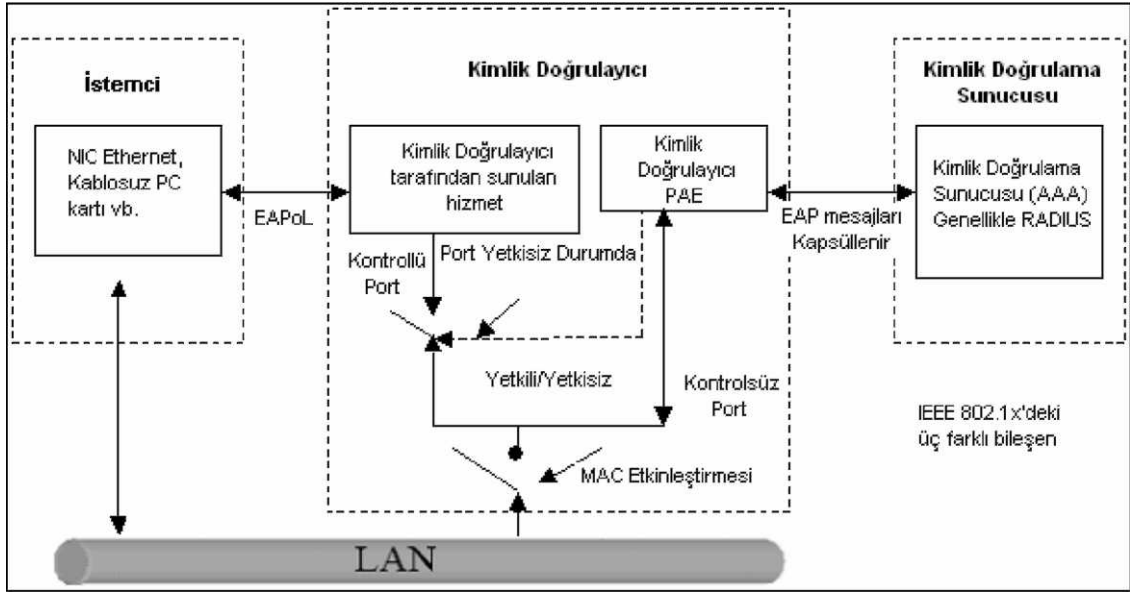


Şekil 3.1 IEEE 802.1x için kontrollü ve kontrolsüz portlar

"Kontrolsüz Port" olarak etiketlenirilmiş birinci lojik erişim noktası, sistemin yetki durumuna bakmaksızın kimlik doğrulayıcı ve LAN üzerindeki diğer sistemler arasında kontrolsüz değişime izin verir [24]. Kablosuz istemci tarafından gönderilen yapılar asla kontrolsüz port kullanarak gönderilmez. Kontrolsüz portun bir diğer özelliği de kimlik doğrulayıcı ve kullanıcı arasındaki değişiklikler için bir yol sağlamasıdır. "Kontrollü Port" olarak etiketlenirilmiş ikinci lojik erişim noktası ise sadece kablosuz istemci 802.1x tarafından yetkilendirildiğinde, kablolu ağ ve kablosuz istemci arasındaki değişime izin verir. Kimlik doğrulama işleminden önce switch "açık" durumdadır ve kablosuz istemci ile kablolu ağ arasında hiçbir yapı gönderilmez. Burada yetkisiz bir durum söz konusudur. Kablosuz istemcinin IEEE 802.1x kullanılarak başarılı bir şekilde kimlik doğrulamasının yapılması halinde switch "kapalı" konuma geçer ve yapılar kablosuz istemci ile kablolu ağ üzerinde bulunan bir nokta arasında gönderilebilir duruma gelir. Kullanıcının yetkilendirilmesi üzerine de yetkili duruma geçiş yapılmış olur.

### 3.7 802.1x'in Çalışma Prensipleri

IEEE 802.1x standardının farklı bileşenleri ile bu bileşenler arasındaki işlem prensibi Şekil 3.2'de gösterilmiştir.



**Şekil 3.2** IEEE 802.1x ile kimlik doğrulama işlemi

Kimlik doğrulayıcı ilk olarak kimlik doğrulama işlemini tamamlamak için gerekenler hariç, istemcinin oluşturduğu giriş ve çıkış yapan tüm dış trafiği filtreler. Böylece kimlik doğrulayıcı EAPoL protokolü veri birimleri aracılığıyla istemci ile iletişim kurar. İstemci, kimlik doğrulayıcıya bağlantı isteğinde bulunur. Kimlik doğrulayıcı, bağlantı isteğini alınca tüm portları kapalı tutarak sadece istemci ile arasında bir port açar. Kimlik doğrulayıcı, istemciden kimliğini (username/password) istedikten sonra istemci kimliğini gönderir. Kimlik doğrulayıcı kimlik bilgisini bir RADIUS sunucusuna gönderir. RADIUS sunucusu, veritabanında tuttuğu bilgilerle kimliği eşleştirerek istemcinin kimliğini sorgular. Kimlik doğrulama işlemi gerçekleştiğinde sunucu, "Kabul" (Accept) mesajını kimlik doğrulayıcıya gönderir. Bu işlemlerden sonra kimlik doğrulayıcı, istemcinin portunu yetkilendirilmiş port durumuna getirir. Böylece istemcinin erişimi garantilenmiş olur [23]. LAN'a olan tüm erişimler, ilaveten bir port aracılığıyla ilişkilendirilen MAC'ın yönetimsel durumuna bağlı olabilir. Örneğin port yönetimsel olarak pasifleştirilmişse port içinden hiçbir trafiğe izin verilmez.

IEEE 802.1x protokolü tüm bu işlemlerin yanında anahtar yönetimi işlemini de gerçekleştirir. İstemci ve kimlik doğrulama sunucusunun ana anahtarı vardır. Bu anahtar kullanılarak, grup anahtar ve oturum anahtar kümesi olarak adlandırılan diğer anahtarlar üretilir. Grup anahtar kümesi, erişim noktası ve ona erişen istemciler arasındaki çoğullama işleminde kullanılır. Oturum anahtarları ise erişim noktası ile istemci arasındaki bağlantı sırasında oluşturulur. Anahtar yönetimi özelliği ile birlikte kimlik doğrulama işlemi gerçekleştirildikten sonra üretilen oturum anahtarları ile veri transferi başlamaktadır.

### 3.8 Servis Kalitesi (QoS) Kavramı

Servis kalitesi, bir ağ bileşenin belirlenmiş düzeydeki ağ trafiğini ve ağ servis gereksinimlerini yerine getirebilmesi özelliğidir. Gerçek zamanlı programların ağ bant genişliğini en etkin biçimde kullanmasına olanak sağlar ve ağ kaynaklarının yeterliliğini belirli bir düzeyde garanti ettiği için, paylaşılan bir ağa, ayrılmış bir ağın sahip olduğuna benzer bir düzeyde hizmet verir. Servis kalitesi garantisi, bir programın belirlenen bir hız ve sürede veriyi iletmesine olanak tanıyan bir hizmet düzeyini gösterir. Ek bant genişliği sağlamaz, ağ kapasitesini arttırmaz, trafik kısıtlaması yapmaz (ses, görüntü, HTTP v.s.) ve ağ yönetimini basitleştirmez. Ancak, kilit uygulamalar ve kullanıcılara garanti edilmiş kaynaklar sağlar. Ağdaki trafik akışının ölçeklenmesini ve yönetilmesini temin ederek ileriye dönük ağ planlanmasına yardımcı olur. Daha hızlı ağ ortamlarına gerekliliği azaltır ve var olan ağ yapısının daha etkin kullanılabilmesini sağlar.

Günümüzde çoğu ağ trafiği IP tabanlı olup, her trafik türünün kendine özgü bant genişliği, gecikme, kayıp ve kesintisiz çalışma özellikleri mevcuttur. Geçmişte IP protokolü tasarlanırken bir paketin varış noktasına güvenle ulaşmasını sağlama amacı güdülmüş ancak o noktaya giderken geçen zaman göz önüne alınmamıştır. Şimdiki IP ağları farklı türlerde uygulamaları da desteklemek zorundadır. Bu uygulamaların büyük çoğunluğu ise düşük gecikme gerektirir. Aksi takdirde, uç kullanıcı ciddi ölçüde etkilenebilir ya da uygulama tamamen çalışmaz duruma gelir. Ağ performansındaki problemlerle mücadele etmek için etkin trafik kurallarının hayata geçirilmesi ve ciddi bir ağ yönetimine ihtiyaç vardır. Bu sayede çoklu uygulamaların IP paketleri üzerinden taşındığı, zamana dayanan uygulamalarda gecikme ve sorunlar yaşanmamış olacaktır.

Servis kalitesi, farklı trafik türleri arasında kaynak paylaşımı yapabilme kabiliyetine sahiptir. Bu paylaşımı düzenlerken bant genişliği, gecikme ve paket kaybı gibi ölçüleri kullanır. Bu durum, bir kavşaktaki trafik akışına benzetilebilir. Bir anda sadece bir aracın geçişine izin verilir. Normal şartlarda bu ilk gelen ilk hizmeti alır prensibine göre en iyi çözümdür. Servis kalitesi, böyle bir kavşaktaki trafik polisine benzetilebilir. Trafik polisi olduğunda da ilk gelen ilk hizmet alır prensibi geçerlidir. Ancak bir istisna olması durumunda trafik polisi bütün arabaları durdurur ve bu istisnai durumun ortadan kalkmasını sağlar (örneğin bir ambulans). Verilen örnek, bilgisayar ağlarına adapte edildiğinde servis kalitesinin yaptığının; öncelik hakkına sahip olan verilerin daima daha az öncelik değerine sahip verilerden önce iletilmesi işini gerçekleştirmek olduğu söylenebilir.

Bir bilgisayar ağı, aynı zamanda hem verinin kaynağı hem de verinin ulaşacağı hedef olamaz. Ağ, sadece kaynak ile hedef arasındaki veriyi taşıyan bir iletim kanalıdır. Eğer hedefteki bilgisayar çok yavaş ise kanal ne kadar geniş olursa olsun ağ trafiğinin oluşması engellenemez. Çünkü, hedef bilgisayar kabul edebileceğinden çok daha fazla veri ile karşı karşıya kalır. Aynı yaklaşımla düşünüldüğünde servis kalitesi de, bilgisayar ağının temel prensibini asla değiştirmeyecektir. Servis kalitesinin yaptığı işlem, verilen ölçütlere göre gecikmeden az etkilenen paketleri gerekirse geciktirmek, ancak gecikmeden çok etkilenen paketleri daha az gecikecek şekilde ağ üzerinde aktarmaktır. IP tabanlı ağlar bu türden veri dağıtımını destekler ve verileri hedefe belli bir sürede ulaştırmak için çaba sarf eder. Bunu başaramazsa veri paketini ya bekletir ya da tamamen ağdan atılmasını sağlar.

### **3.9 Servis Kalitesini Etkileyen Faktörler**

Ağ tabanlı bütünsel servisler tarafından verilen servis kalitesi hizmetinden etkilenen uygulamalarda karşılaşılan husus, her bir uygulamanın kendine göre özel sayılabilecek farklı nitelik ve ölçülerde hizmete gereksinim duymasındır. Servis kalitesi bir performans ölçütü olup, bunu etkileyen her faktör, sistem performansını da doğrudan etkilemektedir. Belirli bir servis kalitesi değerinin tutturulabilmesi için ek bir maliyet gerekebileceğinden, servis kalitesini etkileyen unsurların iyi analiz edilmesi gerekir. Servis kalitesinde etkili olan faktörler, aşağıdaki başlıklar halinde sıralanabilir:

#### **3.9.1 Bant genişliği**

Servis kalitesi uygulamasının çok karmaşık olduğu düşünülen bazı çevrelerce, bant genişliğini arttırmanın tüm uygulamalar için gerekli servis kalitesini sağlayacağına inanılır. Ancak servis kalitesi ile çözümlenen sorunlara bakıldığında, bant genişliği ilavesinin bu sorunlara çözüm getirip getirmediği değerlendirilmelidir. Servis kalitesi bant genişliğini arttırmaz ancak mevcut bant genişliğinin çok etkin ve verimli bir şekilde kullanılmasına yardım eder.

İki şekilde dağıtım yapılan bant genişliğinin, kullanıcılara mevcuttan fazla sunulması, bir kullanıcı için tanımlanan bant genişliğinin her zaman kullanımına açık olamaması demektir. Bu durum kullanıcıların mevcut bant genişliği için birbirleriyle yarışmaları sonucunu doğurur. Kullanıcılar, herhangi bir zaman diliminde diğer kullanıcıların bant genişliği kullanımına bağlı olarak daha az veya daha çok bant genişliği kullanırlar. Servis sağlayıcılar garanti edilmiş bant genişliği hizmetine kayıt oldukları takdirde abonelerine, VLAN gibi fiziksel ya da mantıksal ağlar üzerinde, mevcut bant genişliği hizmetine kıyasla daha ayrıcalıklı bir hizmet verirler. Bazı

durumlarda da garanti edilmiş bant genişliği hizmetine ait veri trafiği, mevcut bant genişliği hizmeti veri trafiğinin kullandığı ağın altyapısını kullanabilmektedir. Bu, genellikle ağ bağlantılarının maliyetinin daha yüksek olduğu ya da bant genişliğinin bir başka hizmet sunucusundan kiralanmış olduğu durumlarda söz konusu olur.

### 3.9.2 Gecikmeler

Ağ üzerindeki gecikme, bir uygulamanın iletim sürecinde ağın giriş ve çıkış noktaları arasında hareket ettiği zaman dilimidir. Gecikme, ses ve görüntü iletimleri gibi normalin dışındaki gecikmelerde zaman aşımına uğrayıp, iptal olan uygulamalar üzerinde önemli servis kalitesi sorunları yaratmaktadır. Bazı uygulamalar az miktarlardaki gecikmeleri tolere edebilmektedir. Ancak belirli bir süre aşıldıktan sonra servis kalitesi sorunu kaçınılmaz hale gelmektedir. Gecikme değişikliğinin çoklu uygulamalar gibi gerçek zamanlı ve gecikmeye duyarlı uygulamalar üzerinde önemli etkileri olabilir. Bu uygulamalar paketleri sabit bir hızda ve aralarında sabit süreler olduğu halde almak isterler. Varış hızı değişkenlik gösterdikçe uygulamanın performansı etkilenir. Gecikme değişiklikleri minimum seviyede olduğunda, sorun yaşanmayabilir; ancak gecikme arttıkça uygulama kullanılamaz hale gelecektir.

### 3.9.3 Kayıplar

Fiziksel iletim ortamında hatalar oluşması ile kayıplar meydana gelebilir. Karasal hatların büyük çoğunluğunda kayıp oranı oldukça azdır. Ancak; uydu, mobil ya da sabit kablosuz bağlantılarda kayıp oranı, çevresel faktörler ile sis, yağmur, RF karışması gibi olumsuzluklara, ağaçlar, binalar ve dağlar gibi fiziksel engeller eklenmesi halinde değişiklik gösterebilir.

### 3.9.4 İletim öncelikleri

İletim önceliği ağdan çıkmakta olan trafiğin hangi sırada iletileceğini belirler. İletim önceliği olan trafik, iletim önceliği olmayandan daha önce iletilir. İletim öncelikleri, ağ kuyruklama mekanizmalarının trafiğe getireceği gecikme miktarlarını da belirlemektedir. Örneğin, e-posta gibi gecikmeyi tolere edebilecek olan uygulamalar, ses ve video gibi gecikmeye hassas olan gerçek-zamanlı uygulamalardan daha düşük iletim önceliğine sahiptirler. Gecikmeye hassas olmayan bu uygulamalar, gecikmeye hassas uygulamalar iletimde iken kuyrukta bekletilebilirler. Bu yaklaşımın en zayıf yönü, bant genişliği sınırlaması olmayan

ortamda yüksek öncelikli iletimin gönderilerek, düşük öncelikli iletimlerin hiçbir zaman gönderilememe riskinin olmasıdır. Atılım öncelikleri ise, hangi iletimin devre dışı bırakılacağını belirlemektedir. Trafik, ağdaki tıkanıklık ya da trafiğin belirlenmiş olan profiline dışına çıkması durumlarında (trafiğin belirlenmiş olan bant genişliğini belirli bir süre için aşması gibi) devre dışı bırakılır. Tıkanıklık durumunda, yüksek atılım önceliği olan trafik, düşük atılım önceliği olandan daha önce devre dışı bırakılır.

## 4. KABLOSUZ AĞLARDA KİMLİK DOĞRULAMA DENETİMİ

### 4.1 Kablosuz Haberleşme Sistemleri

Bir iletişim sisteminin amacı, bilgiyi bir yerden başka bir yere iletmektir. Sistemin randımanı, iletim sırasında kaçınılmaz olarak meydana gelen bilgi kaybının miktarı ile ölçülür. Eğer iletişim sistemi kablosuz ise bilgi, daha yüksek frekanslı bir taşıyıcı üzerine bindirilir. Kablosuz iletişim teknolojisi, en basit tanımıyla, noktadan noktaya veya bir ağ yapısı şeklinde bağlantı sağlayan, bir teknolojidir. WLAN'lar iki yönlü geniş bant veri iletişimi sağlayan, iletim ortamı olarak fiber optik veya bakır kablo yerine radyo frekansı veya kızılötesi ışınları kullanan ve salon, bina veya kampüs gibi sınırlı bir alanda çalışan iletişim ağlarıdır. WLAN sistemleri hareketli kullanıcılar, küçük ve orta ölçekli işletmeler ve bireysel kullanıcılar gibi büyük bir kesime internet ve üyesi oldukları kurumsal ağa mobil olarak bağlanma imkanı sağlamaktadır.

WLAN kullanıcısı, pahalı bir kablolu alt yapısı yerine özünde küçük bir radyo vericisi olan erişim noktası ile iletişim ortamı sağlayabilmekte ve yerel alan ağı oluşturabilmektedir. Temel olarak WLAN sistemi iki ana unsurdan oluşmaktadır; birincisi erişim noktası, ikincisi ise kablosuz cihazlardır. Kablosuz cihazlar genellikle bir dizüstü bilgisayar, kişisel bilgisayar, cep bilgisayarı (PDA) veya kablosuz ağ ünitesi ile donatılmış benzer bir cihaz olabilir. Erişim noktaları ihtiyaca göre bir eve, iş yerine, toplantı salonuna veya bir binaya kurulabilir. Halka açık kullanımı sağlamak üzere ise şehir merkezlerine, büyük alışveriş merkezlerine, hava alanı, tren istasyonu, otobüs terminali veya restoran gibi kamuya açık alanlara da kurulabilir.

### 4.2 Kablosuz Teknoloji Bileşenleri

WLAN teknolojisi kapsamında; WLAN ağ bileşenleri, IEEE 802.11, 802.11 kimlik doğrulaması, WEP ve IEEE 802.1x konuları yer almaktadır. Kablosuz yerel alan ağı, kablosuz istemci ve erişim noktası olarak adlandırılan bileşenlerden oluşmaktadır. İstemci, kablosuz bir ağ çeviricisi ile donatılan bir hesaplama cihazıdır. Kablosuz bir ağ çeviricisi ile donatılan kişisel bir bilgisayar, kablosuz bir istemci olarak kabul edilebilir. Kablosuz istemciler doğrudan birbirleri ile veya bir erişim noktası boyunca iletişim kurabilirler ve taşınabilirler. Erişim noktası ise, istemciler ve kablolu ağ arasında bir köprü gibi davranan kablosuz ağ bağdaştırıcısı ile donatılmış bir ağ cihazıdır. Taşınabilir değildir ve kablolu bir ağı genişletmek için çevresel köprü cihazı gibi davranırlar.



### 4.3 Kablosuz Ağlar için Güvenlik Bilgileri

Kablosuz ağ teknolojileri kolaylık ve esneklik sağlamanın yanında mevcut ağ için bir takım güvenlik risklerine de sahiptir. Örneğin, kimlik doğrulama ve yetkilendirme mekanizmaları uygulanmazsa, uyumlu kablosuz ağ bağdaştırıcısı olan herhangi bir cihaz ağa erişebilir. Şifreleme olmadan kablosuz veriler düz metin olarak gönderilir, bu yüzden kablosuz erişim noktasından yeterli uzaklıkta bulunan biri kablosuz erişim noktasına gönderilen ve kablosuz erişim noktasından gönderilen tüm verileri algılar ve alır. Aşağıdaki güvenlik mekanizması kablosuz ağlar üzerindeki güvenliği geliştirir:

1. İstemci Güvenlik Duvarı
2. 802.11 Kimlik Doğrulaması
3. 802.11 WEP Şifrelemesi
4. Wi-Fi Korumalı Erişim (WPA)
5. 802.1x Kimlik Doğrulaması

#### 4.3.1 İstemci güvenlik duvarı

İstemci güvenlik duvarı istemci ve sunucuların her birinde çalışır. Çevre ağlardan geçen veya kuruluşun kendi içinden kaynaklanan Truva Atı saldırısı, bağlantı noktası tarama saldırısı veya solucanlar gibi ağ saldırılarına karşı koruma sağlar. Birçok güvenlik duvarı teknolojisi gibi, istemci güvenlik duvarı da durum bilgisi olan bir güvenlik duvarıdır. Bilgisayardan bir isteğe yanıt olarak gönderilmemişse veya izin verilir olarak belirtilmemişse tüm gelen trafiği bırakır. İstemci güvenlik duvarı, bazı ICMP (İnternet Denetim İletisi Protokolü) iletileri dışında tüm giden trafiğe izin verir.

#### 4.3.2 802.11 kimlik doğrulaması

Kimlik doğrulamak için IEEE 802.11, açık sistem ve paylaşılan anahtar kimlik doğrulama alt türlerini tanımlar [12].

##### 4.3.2.1 Açık sistem kimlik doğrulaması

Açık sistem kimlik doğrulaması gerçekte kimlik doğrulama sağlamaz; yalnızca kablosuz ağ bağdaştırıcısının MAC adresini kullanarak kablosuz istemci ve kablosuz erişim noktası arasında ileti değişimiyle kimliğin belirlenmesini sağlar. Açık sistem kimlik doğrulamasıyla hatta bulunan bir istemci, kimlik tanımlamasını ve bir erişim noktası ile

ilişkisini tamamlayabilir. İstemci doğru WEP anahtarına sahip olmadıkça WEP'in kullanımı istemcinin erişim noktasından veri almasına ve veri göndermesine engel olur. Bu kimlik doğrulama yönteminde; kimlik doğrulamayı başlatan kablosuz istemci kendi kimliğini içeren bir IEEE 802.11 kimlik doğrulama yönetim yapısını gönderir. Daha sonra kablosuz erişim noktası, istemcinin kimliğini kontrol eder ve bir kimlik doğrulama yapısını geri gönderir (Şekil 4.1).



**Şekil 4.1** Açık sistem kimlik doğrulaması

Bazı erişim noktaları ile MAC filtreleme kullanılarak izin verilen kablosuz istemcilerin MAC adresleri yapılandırılabilir. Bir kablosuz ağ kurarken ağa izinsiz erişimleri önlemek için başvurulmuş en basit yollardan birisi ağa, erişimine izin verilen bilgisayarların MAC adreslerini tanıtmaktır. Bu sayede ağa erişmek isteyen bilgisayarlar bir MAC filtresinden geçecek ve MAC adresi sunucuda tanımlı olmayan bilgisayar ağa erişemeyecektir. MAC filtrelemenin en büyük dezavantajı büyük ağlarda ortaya çıkmaktadır. Çok sayıda kullanıcısı olan büyük yerel ağlarda çok fazla sayıda bilgisayar olduğundan bütün MAC adreslerini sunucuya kayıt etmek zor bir işlemdir. Ayrıca değişen bir bilgisayar için yeniden tanımlama yapılması ihtiyacı da büyük ağlara oldukça fazla bir yük getirir. Dolayısıyla basit olmasının yanında MAC filtrelemenin güvenli olmadığı söylenebilir.

#### **4.3.2.2 Paylaşılan anahtar kimlik doğrulaması**

Paylaşılan anahtar kimlik doğrulaması, kablosuz istemcinin paylaşılan gizliliği bildiğini doğrulayarak kimlik doğrulaması sağlar. 802.11 standardında, paylaşılan gizliliğin 802.11'den bağımsız, güvenli bir kanal üzerinden kablosuz erişim noktasına gönderildiği varsayılır. Paylaşılan anahtar kimlik doğrulaması, tüm kablosuz erişim noktaları ve istemcileri tarafından paylaşılan gizli bir anahtarın değişimini gerektirmesi nedeniyle bilinen metin saldırılarına karşı daha zayıf olduğundan açık sistem kimlik doğrulamasına göre daha az güvenlidir. Ayrıca birden çok kablosuz erişim noktası olan bir kablosuz ağ için paylaşılan anahtar kimlik doğrulaması kullanılıyorsa bir kablosuz erişim noktasından bir başka kablosuz erişim noktasına gidildiğinde ağ anahtarı tüm kablosuz erişim noktaları tarafından kullanılan paylaşılan anahtarla eşleşmeyeceğinden ağ bağlantısı kaybedilebilir.



**Şekil 4.2** Paylaşılan anahtar kimlik doğrulaması

Şekil 4.2'de görülen paylaşılan anahtar kimlik doğrulaması aşağıdaki işlemleri kullanır:

- Kimlik doğrulamayı başlatan kablosuz istemci kimlik doğrulama için bir isteği ve bir kimlik bildirimini içeren yapıyı gönderir.
- Kimlik doğrulama yapan kablosuz düğüm bir sınama metni ile kimlik doğrulamayı başlatan kablosuz düğüme cevap gönderir.
- Bir sınama metni ile kimlik doğrulama yapan kablosuz düğüme yanıt veren kimlik doğrulamayı başlatan kablosuz düğüm, WEP ve paylaşılan anahtar kimlik doğrulamasından türetilen bir şifreleme anahtarı kullanarak şifrelenir.
- Eğer istemci yanlış anahtara sahip olursa veya anahtara sahip olmazsa kimlik doğrulama başarısız olur ve istemcinin erişim noktası ile ilişki kurmasına izin verilmez. Kimlik doğrulama yapan kablosuz düğüm kimlik doğrulama sonucunu gönderir.

#### 4.3.3 802.11 WEP şifrelemesi :

IEEE 802.11'in kablosuz yerel alan ağ ortamında hızlı gelişimi denenirken, kablosuz ağlar için birçok güvenlik tehdidi de ortaya çıkmıştır. IEEE 802.11 kablosuz LAN standardı, kablosuz istemcilerle kablosuz erişim noktaları arasında gönderilen verileri şifreleyerek verinin gizli kalmasını sağlayan WEP algoritmasına dayanan kimlik denetimi ve şifreleme servisleri tanımlar. WEP ile kablolu ağlarda sağlanan seviyede bir güvenlik hedeflenmiştir. Bunun yanında, kablosuz bir LAN'ın gizli dinlenmesinden yetkili kullanıcıları korumak için, şifreleme servislerini ve kablolu bir ortama benzer fiziksel güvenlik özelliklerini destekleyen, şifreleme ve şifre çözme işlemleri için aynı anahtar kullanılan simetrik bir algoritma olan WEP'in IEEE 802.11 çalışma grubu tarafından da kabul edilen pek çok zayıf yönü vardır. WEP'in bu zayıflıkları, saldırganların aktif veya pasif saldırılar düzenlemesine yardımcı olur. Her bir saldırı, frekans bandını dinledikten sonra elde edilen bilgilere göre yapılır [25].

#### 4.3.4 Wi-Fi korumalı erişim (WPA)

WPA (Wi-Fi Protected Access), Wi-Fi Alliance tarafından geliştirilen yeni bir kablosuz güvenlik teknolojisidir. Wi-Fi korumalı erişim, WEP'de var olan şifreleme zayıflıklarını güçlendirir ve şifreleme anahtarlarını otomatik olarak üretmek ve dağıtmak için bir yöntem sunar. Bu çözüm ayrıca, iletişimde alınıp verilen bilgi paketlerinin saldırganlar tarafından değiştirilememesi için veriler üzerinde bütünlük denetimi de sunar. Wi-Fi korumalı erişim ağdaki her kullanıcının kimliğini doğrular ve bu kullanıcıların aldatici ağlara katılmalarını engeller. WPA var olan teknolojileri temel alıp, 802.11i ile ileri doğru ve var olan 802.11 çözümleriyle de geriye doğru uyumluluk sunarak, WEP ile ilgili zayıflıklara pratik bir çözüm sağlar. WPA, donanım değişikliğine gidilmeden WEP'e göre daha güçlü şifreleme (TKIP-Temporal Key Integrity Protocol-Geçici Anahtar Bütünlüğü Protokolü) ve kimlik doğrulama (802.1x) yapısına sahiptir. WPA'da veri miktarı veya zamana bağlı olarak değişen güvenlik anahtarı kullanılmaktadır. WEP ile kıyaslandığında WPA güvenlik şifresini elde etmek daha zordur ve daha fazla zaman harcamak gerekmektedir.

#### 4.3.5 802.1x kimlik doğrulaması

Açık sistem veya paylaşılan anahtar kimlik doğrulaması, statik WEP anahtarları veya MAC kimlik doğrulamasına dayanan geleneksel WLAN güvenlik yöntemleri yeterince güvenli değildir. 802.1x, kablolu ethernet ağlarına ve kablosuz 802.11 ağlarına kimliği doğrulanmış ağ erişimi sağlamak ve port tabanlı ağ erişim kontrolünü gerçekleştirmek için kullanılan bir IEEE standardıdır [23]. Merkezi kimlik doğrulama, dinamik anahtar yönetimi ve hesap oluşturma desteği sağlar. 802.1x standardı, bilgisayar ve ağın birbirlerinin kimliğini doğrulamalarına izin vererek, kablosuz bağlantılar üzerinden veri şifreleme için kullanıcı veya oturum bazında anahtarlar oluşturarak ve anahtarları dinamik olarak değiştirmeye olanak vererek güvenliği geliştirir.

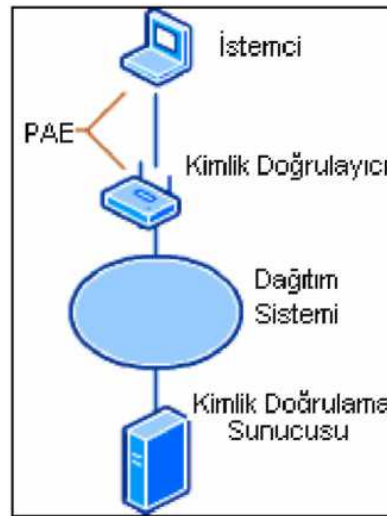
802.1x, port tabanlı ağ erişim denetimini uygular. Bu denetim, LAN bağlantı noktasına bağlanmış bilgisayarın kimliğini doğrulamak ve kimlik doğrulama işlemi başarısız olduğunda ilgili bağlantı noktasına erişimi engellemek için anahtarlı LAN altyapısının fiziksel özelliklerini kullanır. Port tabanlı ağ erişim denetimi etkileşimi sırasında, LAN bağlantı noktası kimlik doğrulayıcı veya istemci rollerinden birini üstlenir. LAN bağlantı noktası kimlik doğrulayıcı rolünü üstlendiğinde, kullanıcıların bu bağlantı noktası üzerinden erişilebilen hizmetlere erişmelerine izin vermeden önce kimlik doğrulaması yapılmasını gerektirir. LAN bağlantı noktası istemci rolünü üstlendiğinde, kimlik doğrulayıcısının bağlantı noktası üzerinden

erişilebilen hizmetlere erişimini gerektirir. Aynı bir varlık olabileceği gibi kimlik doğrulayıcı ile aynı yerde de bulunabilen kimlik doğrulama sunucusu, kimlik doğrulayıcısının adına istemcinin kimlik bilgilerini denetler. Böylece kimlik doğrulama sunucusu, kimlik doğrulayıcısına istemcinin kimlik doğrulayıcısının hizmetlerine erişmek için yetkili olup olmadığını belirten bir yanıt verir.

Kimlik doğrulayıcısının port tabanlı ağ erişim denetimi, bir fiziksel LAN bağlantı noktası üzerinden LAN'a giden iki mantıksal veri yolu tanımlar. İlk veri yolu olan denetlenmeyen bağlantı noktası, kimlik doğrulayıcısı ve LAN'da bulunan bilgisayar aygıtları arasında aygıtın kimlik doğrulama durumuna bakmadan veri geçişine izin verir. Bu, EAPoL iletilerinin alacağı yoldur. İkinci veri yolu olan denetlenmiş bağlantı noktası, kimliği doğrulanmış bir LAN kullanıcısıyla kimlik doğrulayıcısı arasında veri geçişine izin verir. Bu, bilgisayar aygıtının kimliği doğrulandıktan sonra, diğer tüm ağ trafiğinin geçeceği yoldur.

#### 4.4 802.11 Ağlarında 802.1x'in Çalışma Prensibi

IEEE 802.1x standardı için port tabanlı ağ erişim kontrolünde bir LAN portuna iliştirilen kimlik doğrulama cihazları için anahtarlanan LAN altyapısının fiziksel karakteristikleri kullanılır. Kimlik doğrulama işlemi başarısız ise porta erişim engellenebilir. Kablolü ethernet ağları içinde kullanılmasının yanında bu standart, 802.11 kablosuz LAN'lara da uyarlanmıştır. Şekil 4.3'de kablosuz LAN için IEEE 802.1x standardının kapsadığı Kimlik Doğrulayıcı, İstemci, Kimlik Doğrulama Sunucusu ve Port Erişim Elemanı gibi kimlik doğrulama bileşenleri görülmektedir [24].



Şekil 4.3 IEEE 802.1x kimlik doğrulama bileşenleri

**Kimlik Doğrulayıcı:** LAN servislerine erişilebilir bir port aracılığıyla erişim izni verilmeden önce onun kontrollü portuna iştirilen bir cihazın kimlik tanımlamasını yapmaya zorlamakla sorumludur. Kablosuz bağlantılar için kimlik doğrulayıcı, kablosuz erişim noktası üzerindeki bir lojik LAN portudur. Bu port sayesinde altyapı modundaki kablosuz istemciler, diğer kablosuz istemci ve kablolu ağlara erişim hakkı kazanırlar.

**İstemci:** Bir kimlik belirleyici portu aracılığıyla kullanılabilir servislere isteklerin erişimini yapan kablosuz LAN ağ bağdaştırıcısı üzerinde bulunan bir lojik LAN portudur. Bu port sayesinde bir kimlik doğrulayıcı ile işbirliği yapıp daha sonra o kimlik doğrulayıcının kimliği doğrulanarak diğer kablosuz istemci ve kablolu ağlara isteklerin erişimi gerçekleştirilir. İstemci, kimlik doğrulayıcıdan gelen isteğe gönderilecek cevabında kimlik bilgilerini kimlik doğrulayıcıya iletmekle sorumludur.

**Kimlik Doğrulama Sunucusu:** Uç noktalara sağlanan kimlik tanımlama servislerinin asıl kaynağıdır. Kimlik doğrulayıcı adına istemcinin kimlik bilgilerini kontrol etme işlemini gerçekleştirir ve onun LAN servislerine erişim için yetkilendirilip yetkilendirilmediğini gösterir. Kimlik doğrulama sunucusu için aşağıdaki durumlardan birisi söz konusu olabilir:

- Erişim noktasının bir bileşeni olduğu durumda, erişim noktası bağlantı girişiminde bulunan kablosuz istemcilere ait kullanıcı kimlik bilgileri ile yapılandırılmalıdır. Kablosuz erişim noktaları için genelde bu özellik uygulanmaz.
- Ayrı bir eleman olduğu durumda, erişim noktası kablosuz bağlantı girişiminin bilgilerini ayrı bir sunucuya iletir. Tipik olarak kablosuz erişim noktası bir RADIUS sunucusuna bağlantı girişimi parametrelerini göndermek için RADIUS protokolünü kullanır.

**Ağ Erişim Portu:** Ağ erişim portu cihazın ağa ilişkilendirilen noktasıdır. Kablosuz istemciler fiziksel ağ bağlantılarına sahip olmadığı için bir kablosuz istemci ve bir erişim noktası arasındaki ilişki bir ağ erişim portu olarak düşünülebilir.

**Ağ Erişim Elemanı (PAE):** PAE, IEEE 802.1x'i destekleyen bir port ile işbirliği yapan lojik bir elemandır. Erişim kontrol etkileşiminde bulunan, rolleri kimlik tanımlama işlemi içinde olan PAE, istemci, kimlik doğrulayıcı veya her iki role de bürünebilir.

#### 4.5 802.1x ve IAS

Kablosuz ağ bağlantılarında kimlik doğrulamayı, yetkilendirmeyi ve hesap oluşturmaya desteklemek için, IAS ile 802.1x kullanılabilir. IAS, RADIUS ve Proxy sunucusunun Microsoft uygulamasıdır. RADIUS istemcileri olarak yapılandırılan kablosuz erişim noktaları, bağlantı isteklerini ve hesap iletilerini merkezi RADIUS sunucusuna göndermek için RADIUS protokolünü kullanır. RADIUS sunucusu bir kullanıcı hesabı veritabanına yetki verme kurallar kümesine erişir ve kablosuz erişim noktası bağlantı isteklerini işler, ardından bağlantı isteğini kabul eder veya reddeder. RADIUS uygulandığında, kablosuz bir erişim noktası, verilerin geçerli bir kimlik doğrulaması anahtarı olmadan kablolu bir ağa veya başka bir kablosuz istemciye aktarılmasını önler. Geçerli bir kimlik doğrulama anahtarı alma işlemi şu şekilde olur:

1. Kablosuz istemci bir kablosuz erişim noktası aralığına geldiğinde, kablosuz erişim noktası istemciyi sınar.
2. Kablosuz istemci kimliğini kablosuz erişim noktasına gönderir; kablosuz erişim noktası bu bilgiyi RADIUS sunucusuna iletir.
3. RADIUS sunucusu, kablosuz istemcinin kimliğini doğrulamak için istemcinin kimlik bilgilerini ister. Bu isteğin bir parçası olarak, RADIUS sunucusu gereken kimlik bilgileri türünü belirtir.
4. Kablosuz istemci kimlik bilgilerini RADIUS sunucusuna gönderir.
5. RADIUS sunucusu kablosuz istemcinin kimlik bilgilerini doğrular. Kimlik bilgileri geçerliyse, RADIUS sunucusu, kablosuz erişim noktasına şifreli bir kimlik doğrulama anahtarı gönderir.

## 5. KRİTİK VERİ İÇEREN KAMPÜS AĞLARINDA GÜVENLİK UYGULAMASI

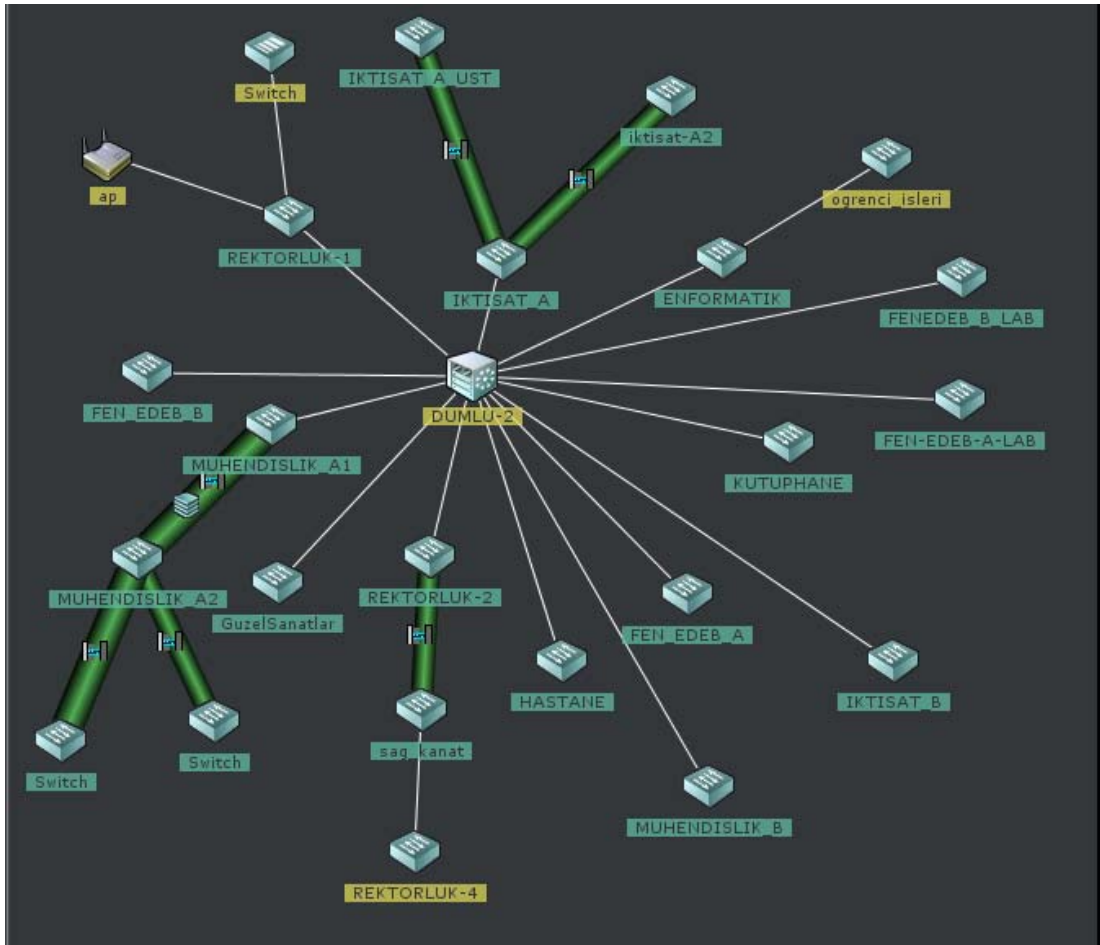
Elektronik ortamlarda yapılan işlem sayısının ve çeşitliliğinin günden güne artış göstermesi, kişisel verilerin korunması ve gizliliğinin sağlanması konusunda yeni önlemler alınması ve düzenlemeler yapılmasını zorunlu hale getirmiştir. Kişisel verilerin işlenmesinin yaygınlaşmasıyla bu verilerin elektronik ortamlarda kullanılması zorunlu hale gelirken, diğer yandan da hakkında veri toplanan kişinin kişilik haklarının korunması gerekli olmaktadır. Bu nedenle; günümüzün gelişen teknolojisi dikkate alındığında kişisel verilerin eskisine oranla daha büyük bir hızda ve oranda gizliliğinin, mahremiyetinin ve bütünlüğünün riske girdiği açıktır. Bu bilgiler ışığında, verileri toplayan ve depolayan kurum ve kişilere büyük sorumluluklar düşmektedir. Bu bilgilerin kaybolmasının önlenmesi, erişimin sadece yetkili kişilere verilmesi, zararlı/zararsız izinsiz erişimlerin mutlaka engellenmesi gerekmektedir.

Kampüs ağlarında karşılaşılan bir takım güvenlik problemlerine maruz kalan yüksek risk oranına sahip Kampüs verilerinin, Kampüs içinden veya dışından gelebilecek saldırılara karşı korunması için önerilen çözümü anlatmaya geçmeden önce, belirli katlarında demo uygulamaları gerçekleştirilen DPÜ Kampüs Ağı'nın uygulama öncesindeki mevcut yapısı tanıtılacak ve karşılaşılan problemlerden bahsedilecektir. Ardından bu problemlerin çözümüne yönelik olarak kullanılacak materyal ve yöntemler anlatılacaktır.

### 5.1 DPÜ Kampüs Ağı'nın Uygulama Öncesindeki Mevcut Yapısı

DPÜ Kampüsleri, Kütahya ili içerisinde iki ayrı noktada yerleşime sahip olmasıyla birlikte Kampüs ana yerleşkesi üniversite kampüsü içerisinde yer almaktadır. Kampüsyeye ait yerleşim alanları; Merkez Kampüsü ve Germiyan Kampüsü şeklindedir. Sahip olduğu bu iki kampüs yapısı nedeniyle sistem, ağ alt yapısı olarak LAN uygulamalarıyla birlikte MAN (Metropolitan Area Network) ağ uygulamalarını da bünyesinde barındırmaktadır (Şekil 5.1). Bu özelliği ile bir kampüs ağı niteliğindedir.





Şekil 5.1 DPÜ Kampüs Ağı'nın uygulama öncesindeki mevcut yapısı

Üniversite Kampüs LAN yapısında; yapısal kablolama anlamında katlara kadar çok modlu fiber optik kablo, kat içlerinde CAT5 UTP kablo kullanılmıştır. Aktif ürün olarak katlarda 3Com 4400 (Bkz. Ek-1) L2-L4, omurgada 3Com 7700-8R (Bkz. Ek-1) switchler kullanılarak; servis önceliklendirmesi anlamında SIS'te kullanılan ORACLE ve SQL veritabanlarına erişimin öncelikli hale getirilmesi, belirli servislerin kullanım yoğunluğuna göre bant genişliğinin artırılması ya da azaltılmasının gerçekleştirilmesiyle de verinin en kısa iletim zamanında taşınması sağlanmıştır. Ayrıca ağ içindeki broadcast domainlerinin sayısını arttırmak ve mevcut broadcast domain'lerini parçalara ayırmak için statik VLAN uygulamasına gidilerek kat bazında ikişer adet olmak üzere VLAN'lar yaratılmıştır.

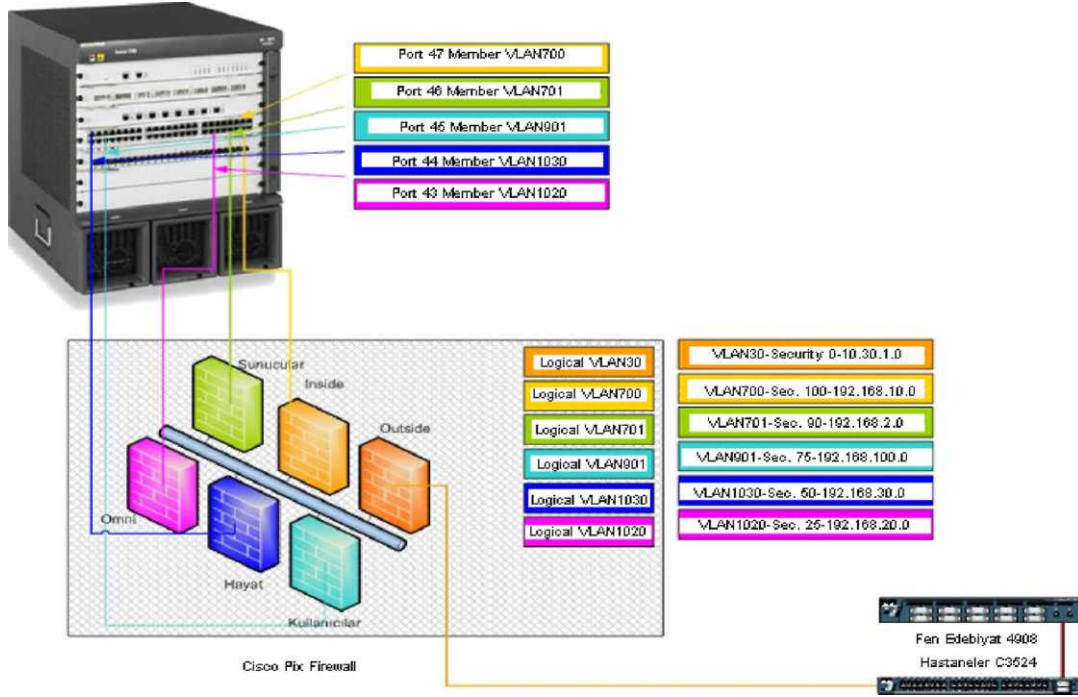
Kampüs ağı içerisinde yer alan sunucular; ORACLE (192.168.10.3), SQL (192.168.10.4) Veritabanı Sunucuları (HIS, LIS-Laboratory Information System), Active Directory Domain Sunucuları, Proxy Sunucusu, Web Filter Sunucusu, DNS, DHCP Sunucuları

(192.168.2.6), Merkezi Antivirus Sunucusu (192.168.150.217), Windows Güncelleme Servis Sunucusu ve Dosya Sunucusudur (192.168.100.30).

Sunucu işletim sistemleri olarak; domain sunucuları için Windows Server 2003 Enterprise Edition, veritabanı sunucuları için Windows Server 2000 Advanced Edition, Proxy için Redhad Linux kullanılmaktadır. İş istasyonlarında ise işletim sistemi olarak; SIS ve OBS uygulamalarını kullananlar için Windows XP Professional Edition tercih edilmiştir. İşletim sistemlerine ait güncellemeler Windows güncelleme servis sunucusu üzerinden grup ilkeleri ile gerçekleştirilmektedir. Merkezi antivirüs yazılımı ile de tüm iş istasyonlarının tek bir noktadan antivirüs güncellemeleri ve virüs tarama vb. işlemleri yapılmaktadır. Kampüs içerisinde çalışan sayısı yaklaşık olarak 1000 kişi olup, aktif olarak veritabanını kullanan personel sayısı 750, işi gereği olsun ya da olmasın sistemde tanımlı olan hesap sayısı ise 800'dür. Kampüs içinde SIS, OBS ve diğer işler için kullanılan iş istasyonu sayısı da 600'dür.

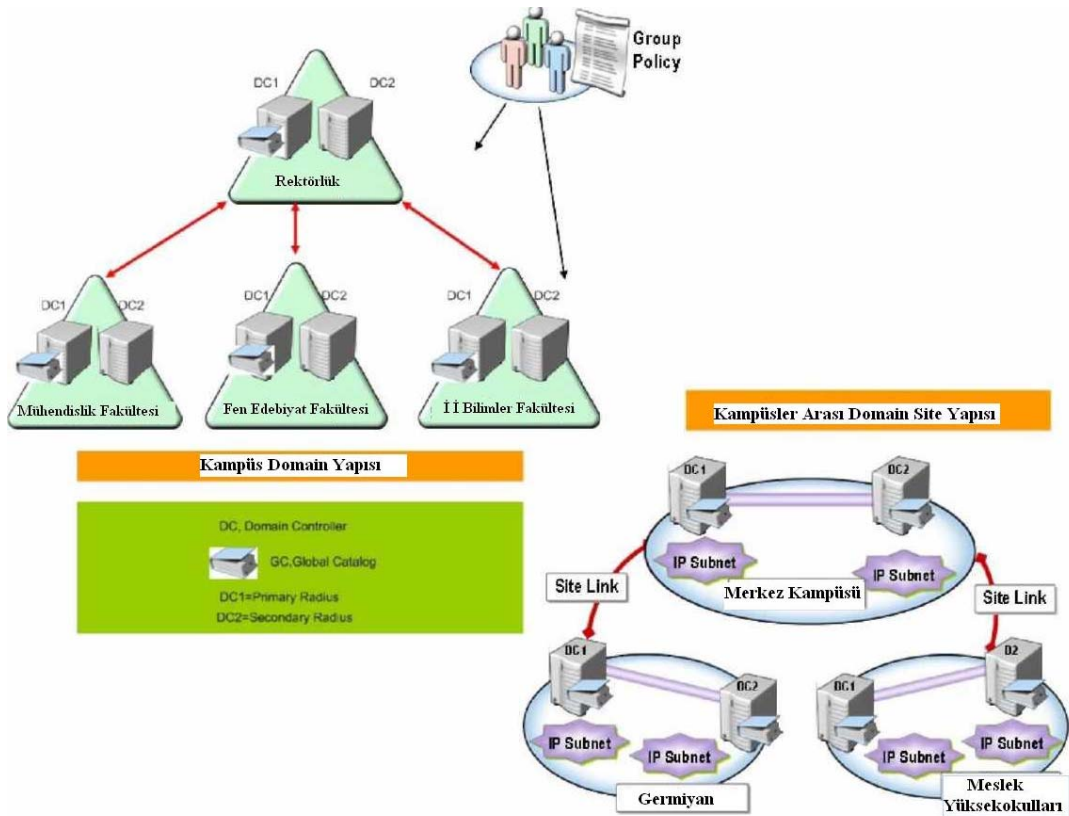
Kampüs ağı kapsamında ana yerleşkede veritabanı sunucu uygulamalarının hizmete girmesiyle beraber gerek özel bilgiler gerekse gizli bilgiler gibi risk oranı yüksek verilerin güvenliğinin sağlanması için Kampüs ile WAN ağı arasına güvenlik duvarı yerleştirilmiştir. Çalışmada önerilen çözüm için Kampüs içinden veya dışından oluşabilecek saldırılara karşı veri güvenliğini sağlamak amacıyla sunucular görevlerine göre farklı DeMilitarized Zone-DMZ'lere (Güvenlik Bölgelerine) yerleştirilmiştir. Her bir DMZ için güvenlik seviyeleri ayarlanarak sunucular arasında da güvenlik derecelendirmesi uygulamasına gidilmiştir (Şekil 5.2).

Bu kapsamda; veritabanı sunucuları en yüksek güvenlik bölgesine ("100") yerleştirilirken Active Directory Domain sunucuları bir alt seviye DMZ bölgesine ("50") yerleştirilerek sadece kullanıcılarla aynı bölgede yer alan sunucu ile "*Replication*" (var olan kayıtların kopyalanması-çoğaltılması) yapması için gerekli olan izinler tanımlanmıştır. Daha düşük bölgelerden erişimlerde sadece SQLNET'in 1521, 1433 nolu portlarına erişim izni verilmiştir. Kullanıcı ve iş istasyonlarının outside (dış ağ) tarafından sonraki en düşük güvenlik bölgesine yerleştirilmesiyle Kampüs içinden sunuculara gelebilecek saldırıların da önüne geçilmiştir. Böylece Kampüs içindeki kullanıcıların ağa yapabilecekleri muhtemel saldırılardan korunmakla beraber Kampüs içindeki iş istasyonları ve kullanıcılar da outside tarafında yer alan kampüs ortamından korunmuş olurlar.



Şekil 5.2 DPÜ Kampüsleri VLAN tabanlı güvenlik duvarı yapısı

Uygulamada, kullanıcıların etki alanında oturum açması için DMZ dışında yer alan etki alanı sunucularına kimlik doğrulama yaptırması tercih edilmiştir. Active Directory etki alanı içinde yer alan kullanıcı ve bilgisayarların etki alanı içindeki yetkileri grup ilkeleri ile belirlenmiştir. Tüm Kampüs birimlerinin organizasyonel birimlere ayrılması ile birime göre farklı grup ilkeleri uygulanabilmektedir. Sistemdeki iş istasyonlarının ve kullanıcıların tek bir noktadan yönetilebilmesi için Active Directory Domain'leri kurularak bölüm ya da görev bazında farklı birimler tanımlanmış, kullanıcı ve bilgisayarlar bu birimlere yerleştirilmiştir. Dağınık bir yerleşime sahip olan Kampüsün her yerleşim yeri için şekil 5.3'de görüldüğü gibi Child (Alt) Domain'ler kurularak tek bir Forest (orman) yapısı içerisinde Domain Tree'ler (etki alanı ağaçları) oluşturulmuştur. Active Directory Domain yapısı sayesinde birimler için ayrı ayrı grup ilkeleri oluşturularak birime özgü haklar ve kurallar belirlenmiştir.



**Şekil 5.3** DPÜ Kampüsleri Active Directory Domain yapısı

DPÜ Kampüsleri Öğrenci Bilgi Sistemi (SIS) içerisinde, sistemin tümünde iş istasyonları olarak masaüstü bilgisayarlar kullanılmaktadır. Tüm bilgisayarlar virüslere karşı korumak amacıyla merkezi antivirüs sistemi ile virüs kontrolünden geçirilmektedir. Virüs sisteminin sağlıklı bir şekilde gerçekleştirilebilmesi için bilgisayarların Active Directory etki alanı içerisinde olmaları yönetim kolaylığı anlamında bir gerekliliktir. Ayrıca Kampüs ağında masaüstü bilgisayarların aksine, Kampüs ağına ait taşınabilir bilgisayarların gerek Kampüs otomasyonuna gerekse internete erişim izinleri, karşılaşılan güvenlik problemleri nedeniyle verilmemiştir.

Dağınık bir yerleşime sahip olan DPÜ Kampüslerinin karşılaşılan bir takım problemler nedeniyle güvenli ve etkin bir şekilde kullanılmadığı ve risk oranı yüksek verilerin LAN'da güvenlik tehditleri ile karşı karşıya kaldığı gözlenmiştir. Aşağıdaki maddelerde mevcut sistemde yaşanan sorunlardan bahsedilmiştir.

- Ağ yapısı genişledikçe ve yeni switchler eklendikçe yapılandırma sırasında istemeyerek de olsa portların yanlış VLAN'lara üye edilmesi,
- Statik VLAN yapılandırma işlemlerinin uzun zaman alması, büyük dikkat istemesi ve bunun kullanılmakta olan Statik VLAN yapılandırması uygulanabilirliğini zorlaştırması,

- Gerek Kampüs personeli, gerek öğrenci, gerekse misafir kullanıcıların herhangi bir şekilde ağa kişisel bilgisayarları ile erişiminin kontrol ve denetiminin sağlanamaması,
- Kampüs içinde kullanılan bilgisayarlara her türlü yeni gelişmenin kolay uygulanabilmesine karşılık, etki alanına üye olmayan bilgisayarlara yeni gelişmelerin tek bir noktadan ve kısa zamanda uygulanmasında sorunlarla karşılaşılması,
- Kampüs içinde herhangi bir kişinin kablolu ya da kablosuz bağlantı ile herhangi bir veri bağlantısının olduğu noktadan çok kolay bir şekilde kullanıcı bilgisayarlarına ve güvenlik duvarı üzerinden izin verilen portlardan da sunuculara erişebilmesi,
- Kampüs içinde çalışmakta olan kullanıcıların ağa erişimlerinde zamanlama sınırlamasının yapılamaması,
- Kampüs çalışanlarının kendi çalışma saatlerine bağlı olarak sisteme erişebilecekleri saatlerin kısıtlanamaması,
- İnternet erişimi olmayan kullanıcılara öğle saatlerinde ve mesai sonrasında internet erişimi verilmesi isteği,
- Herhangi bir şekilde işten ayrılmış ya da istenmeyen kullanıcıların ağa erişimlerinin yerel olarak engellenememesi.

Çalışmanın bundan sonraki kısmında, karşılaşılan problemlerin çözümüne yönelik olarak kullanılacak otomatik VLAN yapılandırması ve kimlik doğrulama işleminin gerektirdiği işlemler ile kablosuz ağ tasarımı tarafında yapılacaklar detaylı bir şekilde açıklanmıştır. Otomatik VLAN yapılandırması ve kimlik doğrulama işlemlerinin gerektirdiği maddeler aşağıdaki yedi ana başlık altında incelenmiştir.

1. Active Directory Yapılandırması
2. IAS Yapılandırması
3. Kenar switch olarak adlandırılan switchlerin kimlik doğrulama switchi olarak yapılandırılması
4. Otomatik VLAN için omurga ve kenar switchlerin yapılandırılması
5. İş istasyonlarının PEAP MS-CHAPv2 için yapılandırılması
6. Sertifika sunucusunun yapılandırılması
7. Erişim kurallarının yazılması

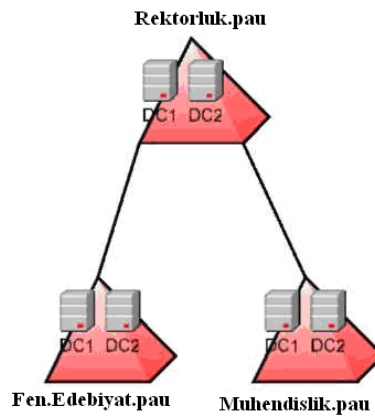
## **5.2 Active Directory Yapılandırması**

Active Directory; kullanıcı, bilgisayar ve ağ kaynakları hakkında bilgilerin saklandığı Windows 2003 ve Windows 2000 Server ile birlikte gelen dağıtık dizin hizmetlerinin bir

entegrasyonu olup etki alanı içerisindeki kaynaklar ve bu kaynaklara erişim bilgilerinin saklandığı ve erişim denetiminin yapıldığı bir hizmetler bütünüdür. Ağ kaynakları yönetiminin merkezileştirilmesi, kaynak yönetiminin ilgili kullanıcılara yetki vererek merkezi yönetimin yetkilerinin dağıtılması, nesnelerin güvenli olarak mantıksal yapıda saklanması ve ağ trafiğinin en iyi şekilde kullanılması Active Directory'nin temel fonksiyonlarıdır. Active Directory ayrıca ağ üzerinde yer alan kaynaklara ilişkin tutarlı ad, açıklama, yer, erişim ve güvenlik bilgilerini de sağlar. Otomatik VLAN ve kimlik doğrulama işlemlerinin gerçekleşmesi için bu çalışmada da kullanılan dört aşamalı bir Active Directory yapılandırmasına ihtiyaç vardır:

### 5.2.1 Active Directory domain yapılandırması

Mevcut yapıda Üniversite Kampüsleri domain yapısı tek bir forest yapısı (*Kampüs.pau*) şeklinde ve Kampüse ait her bir yerleşim yeri aynı forest içerisinde var olan *Kampüs.pau* etki alanına Child Domain olarak tasarlanmıştır (Şekil 5.3 ve Şekil 5.4). Burada bulunan kullanıcıların kimlik doğrulama işlemlerini ana yerleşkede bulunan etki alanı denetleyicilerine yaptırmamak suretiyle ve aradaki düşük bant genişliğinin sadece öğrenci verileri için kullanılmasıyla, uygulamada aynı zamanda etki alanına girmeye çalışan kullanıcıların uzun süre beklemelerini engellenme amacı güdülmüştür. Active Directory Domain yapılandırması işlemi kapsamında mevcut sistemde var olan Windows 2000 etki alanı denetleyicileri Windows 2003 olacak şekilde güncellenmiştir.

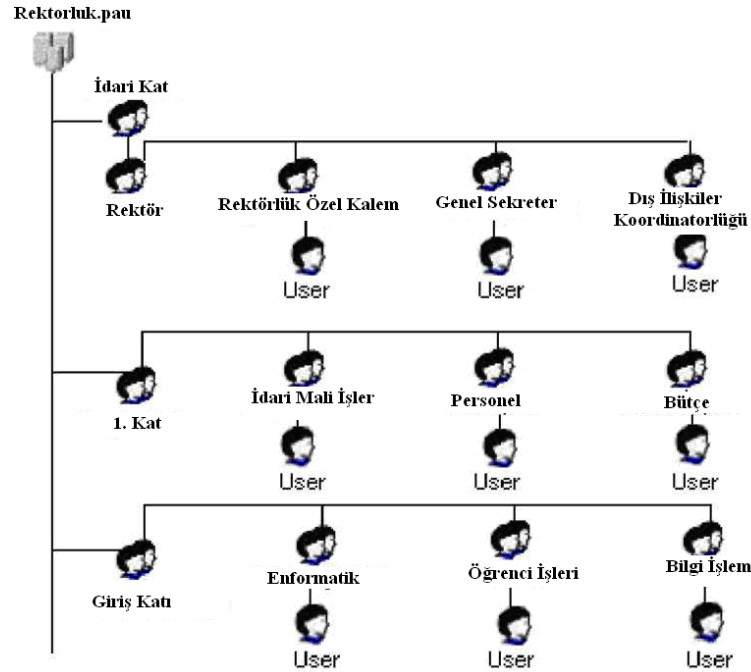


Şekil 5.4 Active Directory Domain yapısından bir kesit

### 5.2.2 Otomatik VLAN yapılandırması için Active Directory grup tasarımı

Otomatik VLAN yapılandırması, statik VLAN yapılandırmasının aksine farklı fiziksel noktalarda bulunan kullanıcı ve bilgisayarların ağ kaynaklarının mantıksal olarak üye oldukları gruplara göre gruplandırılmasını sağlar. Kampüs içinde farklı katlarda bulunan kullanıcı, bilgisayar ve kaynakların aynı Windows grubuna üye edilmesiyle aynı VLAN içinde dolayısıyla aynı ağ grubunda yer almaları sağlanır. Örneğin Kampüs içindeki Fen Edebiyat Fakültesi içerisinde Öğrenci Bilgisayar Laboratuvarı ile Mühendislik Fakültesi içerisinde Öğrenci Bilgisayar Laboratuvarı ayrı binalarda olmasına rağmen aynı Windows grubuna üye edilmesi ile birimlerin aynı VLAN içinde yer almaları sağlanmıştır.

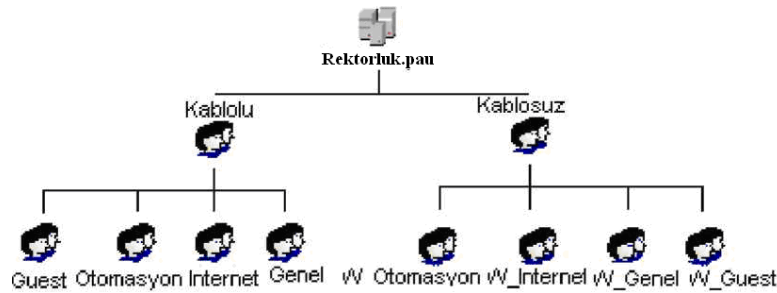
Kampüs içinde grup tanımlamaları yapılırken otomatik VLAN uygulaması için birimlere göre gruplandırma baz alınmıştır. Örneğin İdari Kata Bağlı " Genel Sekreterlik " ile yine aynı kat içindeki "Dış İlişkiler Koordinatörlüğü" aynı katta olmasına rağmen farklı gruplara, dolayısıyla farklı VLAN'lara üye edilmesi hedeflenmiştir (Şekil 5.5). Bunun için Kampüs içinde var olan birim ve birime ait alt birimlerin her biri için Genel Güvenlik Grupları (Security Global Group) oluşturulmuş, bu birimlerde çalışan kişiler de ilgili Genel Güvenlik Gruplarına üye edilmiştir. Bu sayede otomatik VLAN yapılandırması için Active Directory grup tasarımları tamamlanmıştır.



Şekil 5.5 Otomatik VLAN yapılandırması için Active Directory grup yapısı

### 5.2.3 Merkezi denetim için Active Directory gruplarının tasarımı

Kampüs içinde gerek öğrenci, gerekse çalışan ve ziyaretçi sayılarının çok olmasından dolayı ağa erişimin kontrol altına alınması için sistemde tanımlı olmayan kullanıcıların ağdaki herhangi bir kaynağa erişiminin engellenmesi ve erişime izni olan kullanıcıların da yetkilerine göre ağ içinde hareket etmelerinin sağlanması gerekmektedir. Yapılan uygulamada Kampüs içinde yer alan kullanıcılar, sadece otomasyon kullananlar (*Otomasyon*), sadece internet kullananlar (*Internet*), hem internet hem de otomasyon kullananlar (*Genel*), ağa hiçbir şekilde kimlik doğrulama yaptırmayanlar (*Guest-Konuk*) şeklinde farklı Genel Gruplara (Universal Group) ayrılmıştır (Şekil 5.6).



Şekil 5.6 Kampüs ağına erişimin denetlenmesi için oluşturulan genel gruplar

Bu gruplar "sadece otomasyon kullanıp tam zamanlı olarak erişebilenler", "sadece otomasyon kullanıp sadece mesai saatleri içinde erişebilenler" ya da "sadece otomasyon kullanıp sadece mesai saatleri dışında erişebilenler" şeklinde detaylara ayrılabilir. Otomatik VLAN yapılandırması için oluşturulan Genel Güvenlik Grupları, yetkilerine göre ilgili genel gruplara üye edilerek ilgili haklardan yararlandırılabilir.

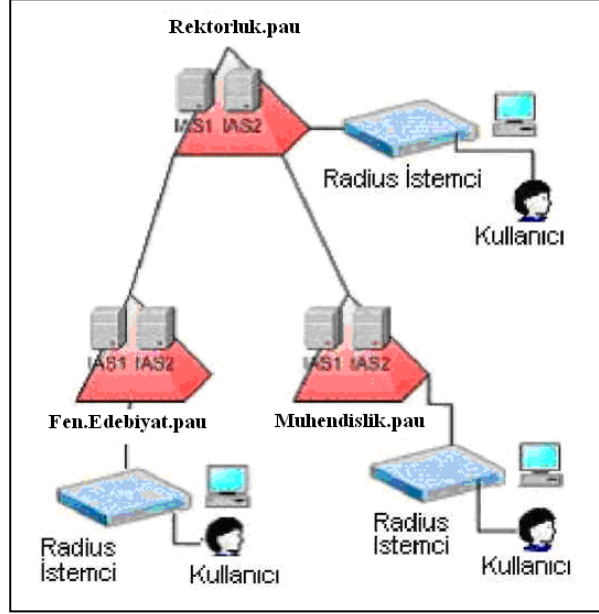
### 5.2.4 Kullanıcı hesapları için uzak erişim izinlerinin düzenlenmesi

Etki alanı içerisinde yer alan kullanıcılar için verilebilecek olan Uzak Erişim İzinleri (Remote Access Permission); "*Allow Access*", "*Deny Access*", "*Control Access Through Remote Access Policy*" şeklindedir ve bu seçenekler kullanıcının yetkilendirilmesi için kullanılır. Kampüs etki alanı Windows 2003 seviyesine yükseltildiği için "*Control Access Through Remote Access Policy*" seçeneği seçilerek kullanıcıların yetkilendirme işlemlerinin politikalarla belirlenmesi yöntemi tercih edilmiştir.



### 5.3 IAS Yapılandırması

Kampüs ağındaki tüm etki alanlarında birden fazla etki alanı denetleyicisi olmasından dolayı IAS, etki alanı denetleyicileri üzerine kurulmuştur (Şekil 5.7).



Şekil 5.7 Kampüs ağının IAS yapılandırmasından bir kesit

Her etki alanı kendi IAS sunucusunu kendi içinde barındırmakta olup, her bir etki alanı için kimlik doğrulama ve hesap oluşturma işlemleri bu sunucular üzerinden gerçekleştirilmektedir. Böylelikle ayrı etki alanlarının bulunduğu uzak noktalar arasında ekstra RADIUS trafiğinin oluşumu engellenmiştir. Etki alanı içinde IAS sunucuları kurulurken her bir etki alanında Birincil (Primary) ve İkincil (Secondary) olmak üzere ikişer adet RADIUS sunucusu oluşturulmuştur. Bu sayede tek bir IAS sunucusunun kimlik doğrulama, yetkilendirme ve hesap oluşturma işlemlerinde tek hata noktası olması önlenir ve hataya dayanıklılık sağlanmış olur. Sunuculardan birinin birincil diğerinin ise yedek olarak kullanılmasıyla aynı zamanda çok miktardaki kimlik doğrulama ve hesap isteklerinin yükü dengelenir. Uygulamada gerçekleştirilen IAS yapılandırma işlemi aşağıda belirtilen üç aşamadan oluşmaktadır:

#### 5.3.1 Birincil ve ikincil IAS sunucu yapılandırması

IAS Sunucuları *native mod* (yerel mod) etki alanı içinde yer aldıklarında gruplar üzerinden uzak erişim denetiminde büyük kolaylık sağlanmış olur. Oluşturulacak bir genel gruba etki alanı dışından kullanıcılar üye edilerek ilgili grup için yazılan uzak erişim

politikasının farklı etki alanındaki kullanıcıları da kapsamı sağlanabilir. Ayrıca kullanıcı hesabına özel, statik yönlendirme tanımlaması yapılmasını da sağlamaktadır. IAS'in, Active Directory'de saklanan kullanıcı hesapları dial-in özelliklerine erişebilmesi için RAS (Remote Access Server - Uzak Erişim Sunucusu) ve IAS Sunucu Güvenlik Grubu'na üye olması gerekmektedir. Birincil IAS sunucusu, etki alanı içerisinde yer alan hesap bilgilerine erişebilmelidir (uygulamada kullanılan birincil IAS sunucusunun IP adresi: 192.168.2.6 ve ikincil IAS sunucusunun IP adresi: 192.168.100.30'dur). IAS'ın etki alanı içinde yer alan herhangi bir etki alanı denetleyicisi üzerine kurulması durumunda hesap bilgilerine doğrudan erişimi sağlanmış olur. IAS'in, etki alanı denetleyicisi olmayan başka bir sunucu üzerine kurulması durumunda hesap bilgilerine erişmek için IAS sunucusuna domain yöneticisi haklarına sahip bir hesapla oturum açılmalıdır. IAS diğer etki alanlarındaki kullanıcılar için kimlik doğrulama ve yetkilendirme işlemi gerçekleştirecekse, IAS'ın bulunduğu etki alanı ile kullanıcıların bulunduğu etki alanları arasında çift yönlü güven ilişkisi kurulmuş olmalıdır. IAS'ın yine kendi etki alanı dışındaki kullanıcı hesap bilgilerine erişebilmesi için ilgili etki alanı içerisindeki *RAS ve IAS Sunucuları* grubuna üye edilmesi gerekir (Şekil 5.8). İkincil IAS sunucusu yapılandırması da birincil IAS sunucu yapılandırması ile aynıdır.



Şekil 5.8 IAS'in Active Directory'e tanıtılması

### 5.3.2 IAS port yapılandırması

RADIUS, kimlik doğrulama için UDP 1812 ve 1645 nolu portları kullanırken Accounting için UDP 1813 ve 1646'nolu portları kullanmaktadır. IAS sunucularının güvenlik duvarının DMZ güvenli bölgelerinde yer alması durumunda, kullanıcıların kimlik doğrulama ve yetkilendirme işlemlerinin gerçekleşebilmesi için DMZ güvenli bölgelerinde 1812, 1645 ve 1813, 1646 portlarından IAS sunusuna erişim izninin verilmesi gerekir.

### 5.3.3 Kat switchlerinin IAS'a RADIUS istemci olarak eklenmesi

Kampüs ağı içinde yer alan switch gibi aktif ürünleri yönetim portu, varsayılan olarak VLAN1 içinde yer almaktadır. Şekil 5.9'da görüldüğü gibi yönetim VLAN'ında 192.168.130.0/24 IP bloğu kullanılmış ve statik olarak tüm aktif ürünlere bu IP bloğundan IP adresi verilmiştir.

Friendly N...	Address	Proto...	Client-Ver
KM-KAT5A	192.168.130.2	RADIUS	3Com
KM-KAT5B	192.168.130.3	RADIUS	3Com
KM-KAT4A	192.168.130.3	RADIUS	3Com
KM-KAT4B	192.168.130.4	RADIUS	3Com
KM-KAT3B	192.168.130.5	RADIUS	3Com

Şekil 5.9 RADIUS istemcilerin eklenmesi

RADIUS istemci ekleme işleminde her katta bulunan aktif cihazlar için ayrı ayrı istemci ekleme işlemi yapılır. İstemci IP adresi, switchin yönetim IP adresidir. Ağda yer alan kenar switchler için 3Com marka olduğu için "Client Vendor" kısmında bu switchlerin hangi sağlayıcı tarafından üretildiği belirtilir. Ayrıca kimlik doğrulama switchi ile IAS arasında birbirinden farklı büyük küçük harf ve rakamların diziliminden meydana gelen ve en az 22 karakterden oluşacak bir Shared Secret (Paylaşımlı Sözcük) belirlenmelidir (Şekil 5.10). Her bir kimlik doğrulama switchi için ayrı Shared Secret belirlenmesi güvenlik anlamında önemlidir. Kimlik doğrulama switchi ile IAS sunucusu arasında RADIUS trafiğinin korunması için IPsec ESP (Encapsulating Security Payload) kullanılmalı, mümkünse en az 3DES şifreleme yapılmalıdır.

Settings

Friendly name: KM-KAT5A

Address (IP or DNS): 192.168.130.2

Client-Vendor: 3Com

Request must contain the Message Authenticator attribute

Shared secret: [Empty]

Confirm shared secret: [Empty]

OK Cancel Apply

Şekil 5.10 Shared Secret tanımlaması

#### 5.4 Kenar Switchlerin Kimlik Doğrulama Switchi Olarak Yapılandırılması

Kenar switchlerdeki güvenlik ayarları web ya da telnet üzerinden yapılandırılır. Web arayüzünde kimlik doğrulama için; Authentication düzenleme menüsünde Birincil ve İkincil RADIUS sunucularına ait IP adresleri ve RADIUS sunucu port bilgileri girilir. Hesap oluşturma için ise; Accounting düzenleme menüsünde Birincil ve İkincil RADIUS sunucularına ait IP adresleri ve RADIUS sunucu port bilgileri girilir (Şekil 5.11). IAS sunucusu ile kimlik doğrulama switchi arasında belirlenen en az 22 karakterlik Shared Secret da bu işlemler yapılırken girilmelidir. Ayrıca switch üzerindeki tüm portlarda, kullanıcıların yetkilendirildiği takdirde erişebilmelerini sağlayacak güvenlik ayarları yapılır. Bunun yanında kullanıcının yetkilendirilmemesi durumunda portun hala etkin olmasını sağlayan ayarlar da yapılmalıdır.

Şekil 5.11 Kenar switchler üzerinde RADIUS sunucularının belirlenmesi

#### 5.5 Otomatik VLAN için Omurga ve Kenar Switchlerin Yapılandırılması

Kampüs ağı içerisinde otomatik VLAN yapılandırması için omurga switch üzerinde;

- Öncelikle tüm VLAN'lar tanımlanır.
  - `[SW7700] vlan 2`
  - `[SW7700] vlan 3`
- Daha sonra mantıksal olarak VLAN'lar için VLAN ara yüzleri yaratılır,
  - `[SW7700] interface vlan-interface 2`
  - `[SW7700] interface vlan-interface 3`
- Mantıksal VLAN ara yüzlerine IP adresi atanır.
  - `[SW7700-vlan-interface2] ip address 192.168.2.1 255.255.255.0`

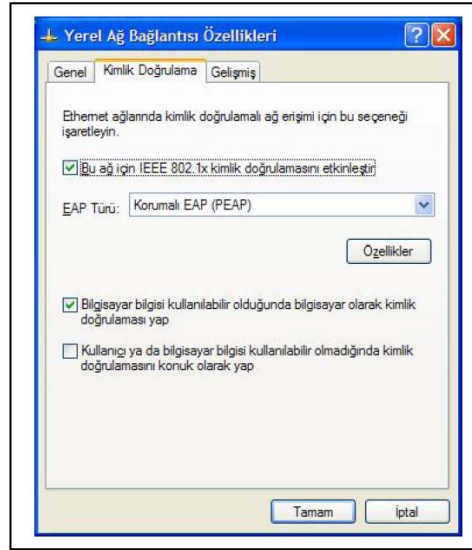
- Omurga switch üzerinde kat switchlerin bağlı olduğu tüm portların iletişim tipi birden fazla VLAN'ı kapsama özelliğinden dolayı "*Trunk*" olarak ayarlanır. Sadece kendi VLAN'ına ait bilgisayarların kendi aralarında iletişimini sağlamak için VLAN'lar oluşturulup switchler birbirine bağlanıyorsa, gelen isteklerin hangi VLAN'a ait bilgisayardan geldiğini ve kiminle irtibata geçeceğini bildiren ve switch'ler arasında bir çeşit köprü görevi gören özel bağlantı kanalları devreye girmektedir. Bu hatlara "*Trunk Hatları*" denilmektedir. Bu hatlar sayesinde birden fazla VLAN o port üzerinde tanımlanabilir hale gelir ve tüm VLAN'ların ilgili ara yüz üzerinden iletimine izin verilir. Aşağıdaki maddelerde bu tanımlamaların nasıl yapıldığı gösterilmektedir.

- *[SW7700-Ethernet 1/0/1] port link type trunk*
- *[SW7700] interface Ethernet 1/0/1*
- *[SW7700-Ethernet 1/0/1] port trunk permit vlan 2 to 100*

Kampüs ağı içerisinde otomatik VLAN yapılandırması için kenar switchler üzerinde, kullanıcıların Kampüs içindeki herhangi bir odadan ağa bağlantı kurmak istemeleri göz önüne alınarak ağda tanımlı olan VLAN'lar oluşturulur. Trunk hattı üzerinden geçen paketlerin hangi VLAN'a ait olduğunu bildirmek için paketlere etiket eklenmesine *Tagging* (Etiketleme) denir. Tagging yönteminde paketin geldiği switch, paketin VLAN ID'sini (VLAN numarasını) tanıyarak filtre tablosundan pakete ne yapılması gerektiğini bulur. Switch üzerindeki hiçbir port kenar switchlerde oluşturulan VLAN'lara gerek *tagged* (etiketli) gerekse *untagged* (etiketsiz) olarak üye yapılmaz. Bunun yanında kenar switchi omurgaya bağlayan Gigabit port, yönetim VLAN'ına *untagged* olarak üye olurken, diğer VLAN'lara *tagged* olarak üye yapılır.

### **5.6 İş İstasyonlarının PEAP MS-CHAPv2 için Yapılandırılması**

Ağ içinde yer alan iş istasyonlarında kullanılan işletim sistemi Windows 2000 Professional, diğer bilgisayarlarda ise Windows XP Professional'dır. Windows Güncelleme Servisi ile tüm bilgisayarların periyodik olarak tek bir noktadan işletim sistemi güncellemeleri gerçekleştirilmektedir. PEAP MS-CHAPv2 özelliğinin etkinleştirilebilmesi için bilgisayarlar üzerinde, Windows XP SP2, Windows XP SP1 ya da Windows 2000 SP4 olmalıdır. İş istasyonlarının bu özellik için yapılandırılması işlemi Şekil 5.13'de görüldüğü gibi bilgisayarların yerel ağ bağlantıları üzerindeki kimlik doğrulama sekmesinde yapılır.



**Şekil 5.12** Kullanıcı bilgisayarlarında IEEE 802.1x kimlik doğrulama ayarları

Şekilden de görüldüğü üzere yerel ağ bağlantısı özelliklerinde, IEEE 802.1x kimlik doğrulaması etkinleştirilir ve EAP türü kısmında "Korumalı EAP (PEAP)" seçilerek PEAP özelliklerine ilişkin sunucu sertifikasının doğrulanması kısmında kimlik doğrulama sunucusuna "*radius.Kampüs.pauW*" adı verilir. Kimlik doğrulama yöntemi olarak güvenli parola (EAP-MSCHAPv2) yöntemi seçilmelidir. Varsayılan olarak PEAP-MS-CHAPv2, kimlik doğrulama için Windows oturum açma kimlik bilgilerini kullanır. Kullanıcıların etki alanına bağlanmaları için kullandıkları oturum açma bilgilerinin aynı zamanda kimlik doğrulama bilgisi olarak kullanılması için "*Otomatik olarak Windows oturum açma adımı ve parolamı (varsa etki alanımı) kullan*" seçeneği seçilir. Bu seçeneğin iptal olması durumunda Windows oturum açma bilgileri kimlik doğrulama için kullanılmayacak ve kısa bir süre sonra kullanıcıya kimlik doğrulama bilgisini girmesi istenecektir. Bu durum, kullanıcılar için yapılacak işlem sayısını arttırması ve ağa girecek bilgisayarların mutlaka etki altına alınması durumunu ortadan kaldıracağından istenmeyen bir haldir. Etki alanında olmayan bilgisayarlar da etki alanına alınarak PEAP-MS-CHAPv2'nin yapılandırması grup ilkeleri ile tüm bilgisayarlara uygulanmıştır. Böylece kullanıcıların tek bir işlemde hem Active Directory etki alanına hem de Kampüs ağına dahil olması sağlanmıştır.

### 5.7 Sertifika Sunucusunun Yapılandırılması

PEAP MS-CHAPv2 tipi kimlik doğrulamada, IAS sunucusu üzerindeki bilgisayar sertifikasının ve istemciler tarafındaki IAS sunucusu bilgisayar sertifikasının dağıtımı için *root CA* sertifikalarına ihtiyaç vardır. Bu çalışmada, Kampüs ağına IAS'in etki alanı

denetleyicisinin üzerine kurulu olması ve hali hazırda sertifika sunucusu etki alanı denetleyicisi üzerinde var olmasından dolayı sertifika sunucusu kurulumu ile ilgili herhangi bir işlem yapılmamıştır. Bunun yanında, etki alanı içinde yer alan bilgisayarların otomatik olarak bilgisayar sertifikalarını kayıt ettirmesi için grup ilkeleri yazılmıştır. Bilgisayar sertifikası için *Otomatik Sertifika İsteği* ayarlama kısmında sertifika şablonları içindeki "*bilgisayar*" sertifikası seçilir. Otomatik kaydetme ayarları bölümünde sertifikaları otomatik kaydetme, süresi biten sertifikaları yenileme, beklemede olan sertifikaları güncelleme ve iptal edilen sertifikaları ortadan kaldırmak için kullanılan sertifikaları güncelleme işlemi seçilerek kullanıcı sertifikasının otomatik olarak yüklenmesi etkinleştirilir (Şekil 5.13).



Şekil 5.13 Sertifika sunucusunun yapılandırılması

## 5.8 Erişim Kurallarının Yazılması

Kullanıcı hesapları veritabanı olarak Active Directory kullanıldığında gerçekleşen ağ erişimlerindeki kimlik doğrulama ve yetkilendirme işlemleri, Active Directory'deki "*Kullanıcı Hesapları Dial-in*" özellikleri ile IAS'te ayarlanan uzak erişim politikalarına (Remote Access Policy) göre yapılır. Burada Authentication, sadece kimlik doğrulama işlemi anlamında iken Authorization, ağa bağlanmakta olan kullanıcı ya da cihazın bunu gerçekleştirmeye yetkisinin olup olmadığının denetiminin yapılması işlemi anlamındadır. Uzak erişim politikaları da gerçekleştirilen ağ bağlantısına izin verilip verilmeyeceğinin belirlendiği, içinde birden fazla koşulun belirtildiği sıralı kurallardır. Her bir uzak erişim politikası için bir ya da birden fazla koşulun sağlanması durumunda erişim izni verilip verilmeyeceği ("*Grant*", "*Deny Remote Access Permission*"), şayet izin verilecekse gerçekleşen bu bağlantının içeride hangi özelliklere ya da profile sahip olacağı (hangi VLAN'da yer alacak, oturum süresi vb.) belirlenir.

### 5.8.1 Uzak erişim politikalarının çalışma şekli

Bir bağlantının yapılması durumunda bu bağlantının kabul edilip edilmeyeceğine aşağıdaki maddelerde sıralanan biçimde karar verilmektedir:

1. Var olan kurallar içindeki ilk kural kontrol edilir. Eğer hiçbir kural tanımlanmamışsa bağlantı reddedilir.
2. Kural içindeki şartların tümü sağlanmazsa, bir sonraki kural kontrol edilir. Eğer başka kural yoksa bağlantı reddedilir.
3. Kurala ait tüm şartların sağlanması durumunda, uzak erişim izinlerine bakılır;
  - Deny Access seçilmişse, bağlantı reddedilir.
  - Allow Access seçilmişse;
    - ° Yapılan bağlantının, kullanıcı hesap özellikleri ve profil özellikleri ile uyuşmaması durumunda bağlantı reddedilir.
    - ° Yapılan bağlantının kullanıcı hesap özellikleri ve profil özellikleri ile uyuşması durumunda bağlantı kabul edilir.
  - Control Access Through Remote Access Policy seçilirse, uzak erişim izin ayarlarına bakılır;
    - ° Deny Remote Access Permission seçilirse, bağlantı reddedilir.
    - ° Grant Remote Access Permission seçilirse, kullanıcı hesap özellikleri ve profil özellikleri uygulanır. Eğer yapılan bağlantı profil özelliklerine uyarsa bağlantı kabul edilir, aksi durumda ise reddedilir.

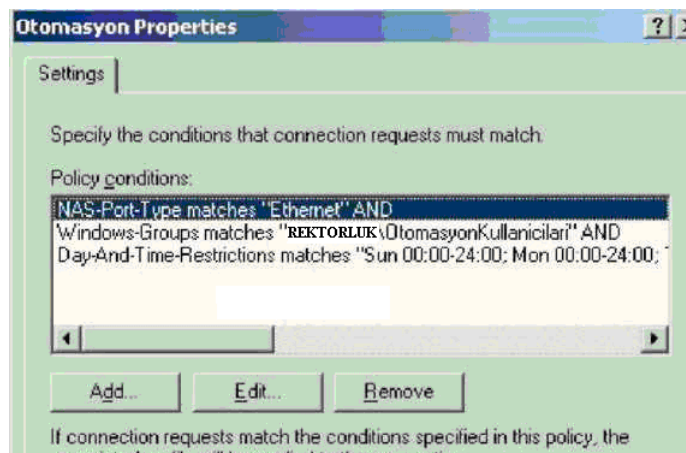
### 5.8.2 Uzak erişim politikalarının oluşturulmasında izlenen metot

IAS üzerinde yazılan uzak erişim politikaları yukarıdan aşağıya doğru uygulama önceliğine sahiptirler. Bu özellik göz önünde bulundurularak çalışmada, en belirgin ya da dar bir kısmı kapsayan koşullar en üste, geneli kapsayacak kurallar daha alt kısımlara yerleştirilmiştir. Böylelikle yukarıdan aşağı işletme önceliğine göre üstte olan kural ilk işletileceğinden, ilk önce genelin işletilerek daha sonra özele geçilmesi engellenmiştir. Uygulamadan örnek verilecek olursa, Döner Sermaye İşletme Müdürlüğü'ne ait global bir grubun internete erişmesi istenirken, yine Döner Sermaye İşletme Müdürlüğü'ne bağlı Resmi İşlemler global grubunun internete erişmemesi istenmektedir. Bu durumda Resmi İşlemler global grubunun internete erişmemesi için oluşturulacak kuralın diğer kurala göre önceliğe sahip olması nedeniyle daha yukarıya yazılması gerekmektedir (Şekil 5.15). Oluşturulan kurallarda; sadece bir kullanıcı için kural oluşturmak yerine güvenlik grubu temeline dayalı kural oluşturup, kullanıcıları ilgili gruba üye yapma yöntemi tercih edilmiştir.





Uzak erişim kuralları oluşturulmadan önce varsayılan kurallar kaldırılır. Yeni bir uzak erişim kuralı oluşturmak için *Yeni Uzak Erişim Politika Sihirbazı* seçilir (Şekil 5.15 ve Şekil 5.16). Daha sonra sırasıyla kural adı, erişim tipi (örneğin *ethernet*), kuralın etkileyeceği Windows Genel Güvenlik Grubu (örneğin *Enformatik*) belirlenir. Kimlik doğrulama metodu kısmında PEAP seçilir. Sihirbazın tamamlanmasından sonra ilave bileşenlerin ayarlanması için kural tekrar açılır ve yeni şartlar eklenir (*Day-And-Time-Restrictions*).



Şekil 5.16 Erişim politikasına ait şartların tanımlanması

Bu uygulamada ilgili gruba üye olan kullanıcıların üye olacakları VLAN için *Service-Type*, *Tunnel-Medium-Type*, *Tunnel-Pvt-Group-ID*, *Tunnel-Type* parametreleri aşağıdaki gibi ayarlanmıştır.

- Service-Type: Framed
- Tunnel-Medium-Type: 802
- Tunnel-Pvt-Group-ID: İlgili grubun üye olacağı VLAN numarası
- Tunnel-Type: VLAN

#### 5.8.4 Kullanıcıların üye oldukları gruba göre yetkilerinin belirlenmesi

Uygulamada, tüm kullanıcılar ve birimleri belirlenerek Kampüs organizasyon şeması çıkartılmış, bu şema içinde hangi birimin hangi VLAN'a üye olacağı belirlenmiştir. Otomatik VLAN yapılandırması sonucu kullanıcı hesaplarının üye olduğu gruba göre belirli VLAN'lara yerleşen kullanıcılar, omurga switch üzerinde yazılan erişim listeleriyle ya otomasyon, ya

internet ya da her ikisini birden kullanabilir duruma gelmiştir. İnternet ve otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi Ek-2’de verilmiştir.

Yazılan bu erişim kuralları ile kablolu ağlarda işlem yapan kullanıcılar için, internete çıkış VLAN'ına (192.168.3.0) ve otomasyon sistemini kullanan veritabanı sunucularına (192.168.10.0) erişim yetkisi verilmiştir. Veritabanı sunucularının yalnızca 1433 ve 1521 numaralı portlarından erişim izni verilmiştir. Otomasyon ve internet uygulamalarının dışındaki uygulamalar ise bu kullanıcılara engellenmiştir. Bir sonraki adımda, hem internet hem de otomasyon sistemini kullanan kablolu ağ kullanıcılarının yerleştirildiği VLAN80 ve bu VLAN'ın ara yüzleri tanımlanmıştır. Port türünün "*Trunk*" olarak seçilmesiyle birden fazla VLAN trafiğinin bu iletim kanalı içinden geçmesi sağlanmıştır. En son adımda da, servis kalitesi faktörü "packet filter - paket filtreleme" özelliği ile tüm kurallara atanmıştır. Yalnızca otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi Ek-2’de verilmiştir.

Burada yazılan erişim kuralları, kablolu ağlarda yalnızca otomasyon uygulamalarını kullanan kullanıcılara erişim yetkisi vermektedir. Bu sebeple erişim kurallarında, yalnızca veritabanı sunucularına erişim izni verilmiştir. Otomasyon sistemi uygulamalarının dışındaki uygulamaların tamamı ve diğer VLAN'lara erişim tamamen engellenmiştir. Daha sonraki adımlarda, otomasyon sistemini kullanan kablolu ağ kullanıcılarının yerleştirildiği VLAN70 tanımlanmış, bu VLAN' ın ara yüzleri yaratılmış ve servis kalitesi faktörü paket filtreleme özelliği ile tüm kurallara atanmıştır.

Kenar switchler üzerinde servis kalitesi desteği olmasından dolayı, bir takım trafik yetkilendirme işlemleri kenar switchlerde yapılabilecek olmasına rağmen, bu işlemlerin kenar switchler üzerinde yapılması tercih edilmemiştir. Kenar switchler üzerinde kullanıcıların hangi VLAN'a bağlanacağı sabit olmadığından, herhangi bir servis kalitesi ifadesinin uygulandığı porttan, portu kullanan bütün kullanıcıların etkilenmesi, uygulamanın "merkezden gruba göre değişken yapı" felsefesine ters düşecektir.

### **5.9 Servis Kalitesi Analizleri**

Ses ve görüntü tabanlı çoklu uygulamaların kullanıldığı risk oranı yüksek veri yoğunluğuna sahip Kampüs ağlarında, servis kalitesi uygulamaları büyük önem taşımaktadır. Bu ağlarda büyük boyutlarda ve fazla miktarlarda veri taşındığı göz önüne alındığında konunun sistem performansını etkilemesi açısından önemi daha da artmaktadır. Farklı trafik türleri arasında servis kalitesi faktörü bünyesinde olan uygulamalarla, sistemde öncelik hakkına sahip olan verilerin daha az önceliğe sahip verilerden önce taşınması işlemi gerçekleştirilmektedir.

Servis kalitesi analizleri kapsamında; önceliklendirme konusunda yapılan çalışmada veritabanı sunucuları, mail ve web sunucuları en yüksek önceliğe sahip güvenlik bölgesine (1.seviye öncelik bölgesi) yerleştirilirken, Active Directory domain sunucuları ile internet hizmetleri bir alt seviye güvenlik bölgesine (2.seviye öncelik bölgesi) yerleştirilmiştir. Kullanıcı ve iş istasyonları tarafında, ağa yapılabilecek muhtemel saldırıları engellemek için 3.seviye önceliklendirme yoluna gidilmiştir. Böylece sistemdeki veri trafiği akışı düzenlenerek performans artırımı öngörülmüş, güvenlik derecelendirmesi ile de risk oranı yüksek verilerin Kampüs içinden veya dışından oluşabilecek saldırılara karşı güvenliği temin edilmiştir.

Uygulamada, sistem performansının artırılması için rol tabanlı yetkilendirme kullanılarak servis kalitesi faktörünün de etkin bir şekilde gerçekleşmesi sağlanmıştır. Bu amaçla; Active Directory etki alanı içinde yer alan kullanıcı ve bilgisayarların etki alanı içindeki yetkileri grup ilkeleri ile belirlenmiş, tüm Kampüs birimlerinin organizasyonel gruplara ayrılması ile de birime göre farklı grup ilkeleri uygulanabilmiştir. Kampüsün farklı katlarında bulunan kullanıcı, bilgisayar ve kaynakların aynı gruplara üye edilmesiyle aynı VLAN içinde, dolayısıyla aynı ağ grubunda yer almaları sağlanmıştır. Böylece otomatik VLAN uygulaması için birimlere göre gruplandırma temel alınarak, Kampüs içinde var olan birim ve alt birimlerin her birinde çalışan kişilerin ilgili genel güvenlik grubuna üye edilmesi gerçekleştirilmiştir.

Gerek öğrenci, gerekse çalışan ve ziyaretçi sayısının çok olması nedeniyle Kampüs ağına erişimin kontrol altına alınması için sistemde tanımlı olmayan kullanıcıların ağdaki herhangi bir kaynağa erişiminin engellenmesi ve erişime izni olan kullanıcıların da yetkilerine göre ağ içinde hareket etmelerinin sağlanması gerekmektedir. Rol tabanlı yetkilendirme işlemi kapsamında, yapılan işe göre; Kampüs içinde yer alan kullanıcılar, "*Otomasyon*" (sadece otomasyon kullananlar), "*İnternet*" (sadece internet kullananlar), "*Genel*" (hem internet hem de otomasyon kullananlar) ve "*Guest-Konuk*" (ağa hiçbir şekilde kimlik doğrulama yaptırmayanlar) şeklinde farklı genel gruplara ayrılmıştır. Bu grupların tümü yine kendi içlerinde "*sadece otomasyon kullanıp tam zamanlı olarak erişebilenler*", "*sadece otomasyon kullanıp sadece mesai saatleri içinde erişebilenler*" ya da "*sadece otomasyon kullanıp sadece mesai saatleri dışında erişebilenler*" şeklinde detaylı gruplara da ayrılabilir.

Servis kalitesini etkileyen zamanlama ile ilgili bu kurallar, erişim listelerine "*time range*" (zaman aralığı) parametresi ile eklenebilmektedir. Örneğin yazılan bir erişim listesi ile 10.1.1.1 kaynak IP adresine sahip bir kullanıcının günlük olarak saat 08.00 ve 18.00 arasında paket filtreleme işlemi yapması istenirse, bu istek *time range* özelliği kullanılarak aşağıdaki şekilde gerçekleştirilebilir:

```

time-range 3com 8:00 to 18:00 daily
acl mode ip-based
acl name traffic-of-host basic
rule 1deny ip source 10.1.1.0 time-range 3com
qos packet-filter inbound ip-group traffic-of-host

```

Genel grupların servis kalitesi analizleri ile ilişkileri incelendiğinde, bu gruplara görevlerine göre öncelik verilmesi konusunun önem kazandığı görülmüştür. Uygulamada gerçekleştirilen öncelik derecelendirmesi kapsamında, Kampüs otomasyon sistemini kullanan kullanıcılar ("*Otomasyon*" genel grubu) için e-posta ve web uygulamalarına düşük öncelik (LowP-Low Priority), otomasyon uygulamalarına ise yüksek öncelik (HighP-High Priority) verilmiştir. Yani bu grup için e-posta gibi gecikmeyi tolere edebilecek olan uygulamalar, otomasyon uygulamaları gibi gecikmeye hassas olan gerçek-zamanlı uygulamalardan daha düşük iletim önceliğine sahiptir. Otomasyon uygulamalarını kullanmayıp interneti kullanan kullanıcılar ("*İnternet*" genel grubu) için internet uygulamalarına yüksek öncelik verilmiştir. Hem interneti hem de otomasyonu kullanan "*Genel*" grubu için yazılan uzak erişim izinleri öncelikleri belirlerken, "*Guest*" genel grubu için sadece internet uygulamaları aktiftir ve bu uygulamalara yüksek öncelik verilmiştir.

### 5.10 Kablosuz Ağ Tasarımları

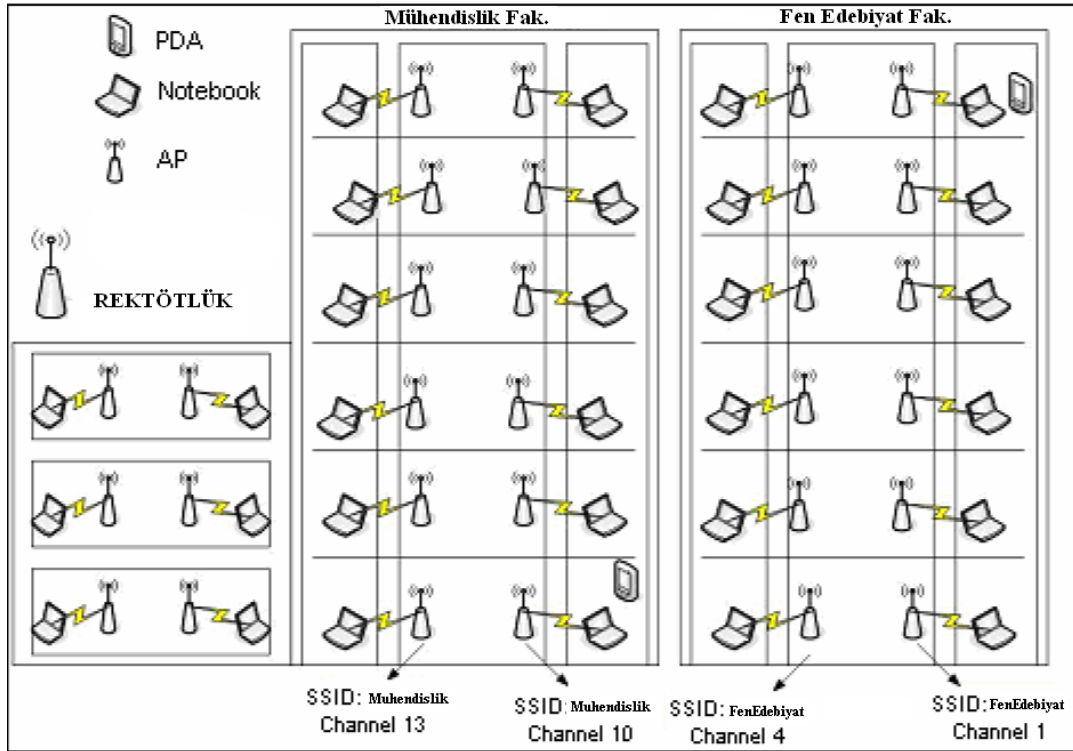
Kablosuz yerel alan ağları kullanıcı ve alıcı arasında radyo frekansları ile kablosuz ortamlarda, kabloya gerek kalmadan veriyi alır ve iletir ayrıca bir gezici kullanıcının herhangi bir fiziksel bağlantı olmadan ağa bağlı kalmasını sağlar. Mobil kullanıcılar da kablosuz bağlantı sayesinde çeşitli internet hizmetlerinden herhangi bir yapısal kablo ihtiyacı olmaksızın yararlanabilmektedir (Şekil 5.17).



Şekil 5.17 Kablosuz ağ örneği

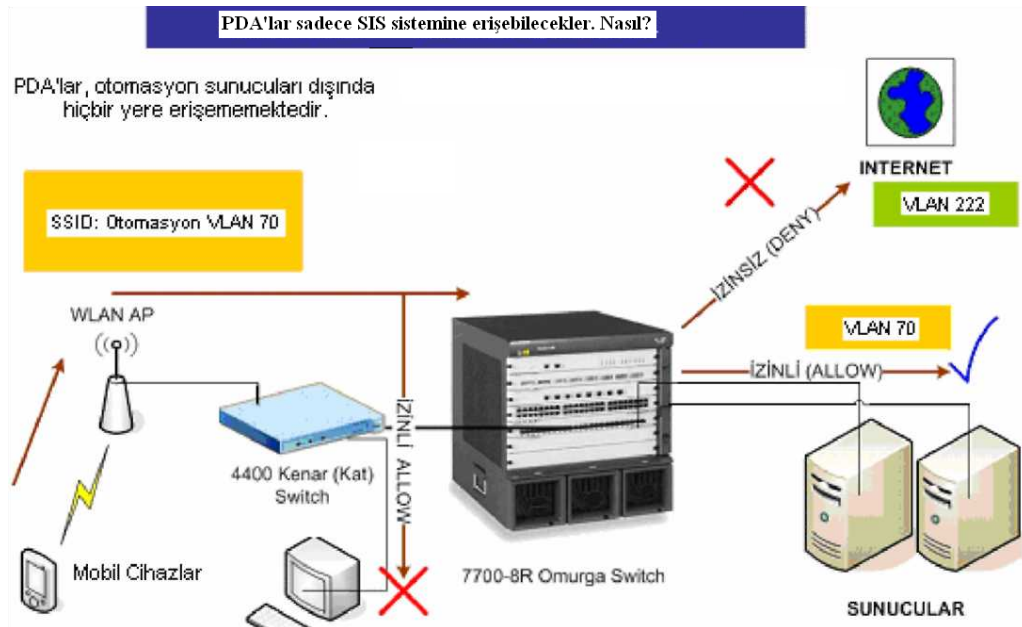
Uygulama kapsamındaki WLAN ağı öncelikli olarak öğretim üyesi ofislerinin de bulunduğu rektörlük Binası, Fen Edebiyat Fakültesi ve Mühendislik Fakültesin'de kullanılmak üzere tasarlanmıştır. Yapının daha sonra kliniklerin bulunduğu katları da içine alacak şekilde tüm DPÜ Kampüslerini içine alan bir yapıda genişlemesi mümkün olabilecektir.

WLAN ağ kurulumunda genellikle merkezi hub olarak erişim noktaları yerleştirilir. Erişim noktaları yapısal kablolu ile internet erişim noktasına ya da kablolu ağa bağlanırlar. Uygulamada her kata yerleştirilecek olan erişim noktasının sayısı en az ikidir ve kullanılan erişim noktalarına ait Channel (kanal) koridorlar arasında en az +3/3 fark olacak şekilde tasarlanmıştır. Kablosuz istemci cihazlarının erişim noktalarıyla haberleşmek için kullanacağı SSID (Service Set Identifier) internet olup, tüm erişim noktaları aynı SSID'ye sahip olacaktır. Bu işlemle kullanıcının, bilgisayarını katlar arasında taşıdığına tekrar yapılandırma yapmasını ortadan kaldırma amacı güdülmüştür. Ayrıca erişim noktalarında, SSID broadcast'ine izin verilerek kullanıcıların otomatik olarak sisteme bağlanması sağlanmıştır. Oluşturulan kablosuz ağ mimarisinde tüm erişim noktaları üzerinde açılan SSID'ler; *Internet* ve *Otomasyon* (HIS için) SSID'leridir. Ortamda kablosuz istemciler tarafından tarama yapılması durumunda, sadece *Internet* SSID'sinin görülmesi istendiğinden, broadcast SSID sadece internet için izin verir. Diğer SSID'nin kablosuz istemciler tarafından görülmesi istenmediğinden bunlar yayınlanmaz. *Internet* SSID'sinin yayınlanmaması durumunda bu hizmetten yararlanacak olan kişiler Bilgi İşlem Merkezi ile bağlantıya geçmek zorunda kalabilir. Bu durumu ortadan kaldırmak için erişim noktası üzerinde *Internet* SSID'si için her hangi bir güvenlik ayarı yapılmaz ve *Otomasyon* SSID'sinin broadcast durumunda olmayıp gizli olarak durması yöntemi tercih edilir.



Şekil 5.18 Kablosuz ağ cihazlarının Kampüs içindeki dağılımı

Şekil 5.18'de kablosuz ağ cihazlarının DPÜ Kampüsü içindeki dağılımları görülmektedir.



WLAN uygulamasında kullanılan erişim noktalarının üzerindeki VLAN etkinleştirilerek istenilen kullanıcıların sadece internete erişimleri dışında otomasyona da erişimleri mümkün olur (Şekil 5.19). Bunun için kablosuz cihazların (sunucu/istemci) VLAN'ı desteklemesi gerekmektedir.

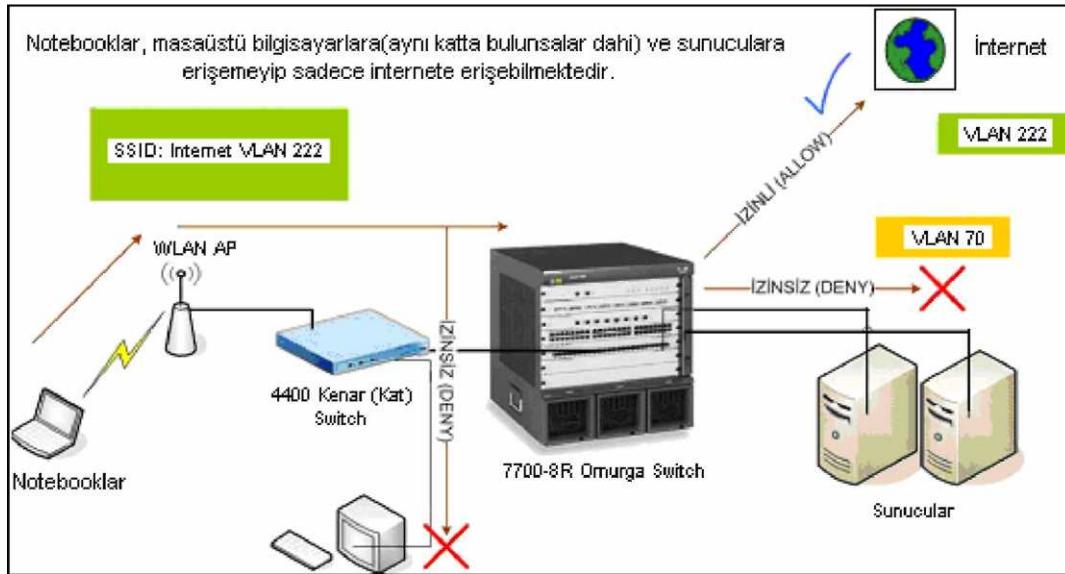
VLAN desteği sayesinde omurga switch üzerinde oluşturulmuş olan VLAN'lar erişim cihazlarına eklenerek, her bir SSID'nin ayrı VLAN'larda olması sağlanmıştır. Buna paralel olarak *Internet* SSID'sine bağlanarak internete erişmek isteyen kullanıcılar, VLAN222'ye üye olup, 192.168.222.\* IP numarasına sahip olur. Yine otomasyon SSID'sine bağlanarak otomasyona erişmek isteyen kullanıcılar VLAN70'e üye olup, 192.168.70.\* IP numarasına sahip olur (Şekil 5.19 ve Şekil 5.20).

WLAN uygulamasında güvenlik anlamında;

- İnternete bağlanmak isteyen kullanıcılar için kablosuz ağ erişim cihazlarında açık mod kimlik doğrulama ve WEP şifrelemesi devre dışı olur. Ayrıca HIS için kullanılan terminallerden internete erişimin kısıtlanması için de, HIS kablosuz

terminallerinin bu ortama erişmesi için "*deny MAC filter*" (MAC filtrelemeyi yasaklama) kuralları yazılır.

- Otomasyona bağlanmak isteyen kullanıcılar için kablosuz ağ erişim cihazları üzerinde MAC Filter, WEP ya da WPA şifreleme etkin olup, son aşamada kimlik doğrulama da etkinleştirilerek 3 aşamalı güvenlik sağlanır.



Şekil 5.20 Kablosuz ağ üzerinden internet erişimi

Bu güvenlik politikaları altında kablosuz erişim cihazları üzerinden gerek internet, gerekse HIS için ana omurgaya erişecek olan kullanıcıların birbirine zarar vermemesi, dolayısıyla internet ortamından oluşabilecek saldırıların engellenmesi için VLAN tabanlı erişim listeleri yazılmıştır. Ek-2'de örneği görülen erişim listeleri ile VLAN222'den (WLAN) gelen kullanıcıların (notebook), tüm sunuculara ve diğer masaüstü bilgisayarlara ağdan herhangi bir şekilde (TCP/UDP) erişimleri engellenmiş olur.

Yazılan bu erişim kuralları ile kablosuz ağlardaki kullanıcılara sadece internete çıkış için erişim yetkisi verilmiş, internet uygulamaları dışındaki uygulamalar ise engellenmiştir. Diğer adımlarda internet uygulamalarını kullanan kablosuz ağ kullanıcılarının yerleştirildiği VLAN222 tanımlanmış ve bu VLAN'ın arayüzü yaratılmıştır. Son adımda da, servis kalitesi faktörü paket filtreleme özelliği ile tüm kurallara atanmıştır.



## 6. AHP UYGULAMASI

### 6.1. Analitik Hiyerarşi Prosesi

Analitik Hiyerarşi Proses (AHP), ilk olarak 1968 yılında Myers ve Alpert ikilisi tarafından ortaya atılmış ve 1977 de ise Saaty tarafından bir model olarak geliştirilerek karar verme problemlerinin çözümünde kullanılabilir hale getirilmiştir. AHP, karar hiyerarşisinin tanımlanabilmesi durumunda kullanılan, kararı etkileyen faktörler açısından karar noktalarının yüzde dağılımlarını veren bir karar verme ve tahminleme yöntemi olarak açıklanabilir. AHP bir karar hiyerarşisi üzerinde, önceden tanımlanmış bir karşılaştırma skalası kullanılarak, gerek kararı etkileyen faktörler ve gerekse bu faktörler açısından karar noktalarının önem değerleri açısından, birebir karşılaştırmalara dayanmaktadır. Sonuçta önem farklılıkları, karar noktaları üzerinde yüzde dağılıma dönüşmektedir.

### 6.2. Karar Verme Problemindeki Faktörler

#### 6.2.1. Performans

Tercih edilecek ağ güvenlik sisteminin bant genişliği, gecikmeler ve kayıplarının incelenip mevcut durum ve tercih edilecek alternatifleri belirlemek.

#### 6.2.2. Güvenlik :

##### 6.2.2.1. İstemci güvenlik duvarı

İstemci güvenlik duvarı istemci ve sunucuların her birinde çalışır. Çevre ağlardan geçen veya kuruluşun kendi içinden kaynaklanan Truva Atı saldırısı, bağlantı noktası tarama saldırısı veya solucanlar gibi ağ saldırılarına karşı koruma sağlar. Birçok güvenlik duvarı teknolojisi gibi, istemci güvenlik duvarı da durum bilgisi olan bir güvenlik duvarıdır. Bilgisayardan bir isteğe yanıt olarak gönderilmemişse veya izin verilir olarak belirtilmemişse tüm gelen trafiği bırakır. İstemci güvenlik duvarı, bazı ICMP (Internet Denetim İletisi Protokolü) iletileri dışında tüm giden trafiğe izin verir.

##### 6.2.2.2. 802.11 kimlik doğrulaması

Kimlik doğrulamak için IEEE 802.11, açık sistem ve paylaşılan anahtar kimlik doğrulama alt türlerini tanımlar.

### **6.2.2.3. 802.11 WEP şifrelemesi**

IEEE 802.11'in kablosuz yerel alan ağ ortamında hızlı gelişimi denenirken, kablosuz ağlar için birçok güvenlik tehdidi de ortaya çıkmıştır. IEEE 802.11 kablosuz LAN standardı, kablosuz istemcilerle kablosuz erişim noktaları arasında gönderilen verileri şifreleyerek verinin gizli kalmasını sağlayan WEP algoritmasına dayanan kimlik denetimi ve şifreleme servisleri tanımlar. WEP ile kablolu ağlarda sağlanan seviyede bir güvenlik hedeflenmiştir. Bunun yanında, kablosuz bir LAN'ın gizli dinlenmesinden yetkili kullanıcıları korumak için, şifreleme servislerini ve kablolu bir ortama benzer fiziksel güvenlik özelliklerini destekleyen, şifreleme ve şifre çözme işlemleri için aynı anahtar kullanılan simetrik bir algoritma olan WEP'in IEEE 802.11 çalışma grubu tarafından da kabul edilen pek çok zayıf yönü vardır. WEP'in bu zayıflıkları, saldırganların aktif veya pasif saldırılar düzenlemesine yardımcı olur. Her bir saldırı, frekans bandını dinledikten sonra elde edilen bilgilere göre yapılır.

### **6.2.2.4. Wi-Fi korumalı erişim (WPA)**

WPA (Wi-Fi Protected Access), Wi-Fi Alliance tarafından geliştirilen yeni bir kablosuz güvenlik teknolojisidir. Wi-Fi korumalı erişim, WEP'de var olan şifreleme zayıflıklarını güçlendirir ve şifreleme anahtarlarını otomatik olarak üretmek ve dağıtmak için bir yöntem sunar. Bu çözüm ayrıca, iletişimde alınıp verilen bilgi paketlerinin saldırganlar tarafından değiştirilememesi için veriler üzerinde bütünlük denetimi de sunar. Wi-Fi korumalı erişim ağdaki her kullanıcının kimliğini doğrular ve bu kullanıcıların aldatıcı ağlara katılmalarını engeller. WPA var olan teknolojileri temel alıp, 802.11i ile ileri doğru ve var olan 802.11 çözümleriyle de geriye doğru uyumluluk sunarak, WEP ile ilgili zayıflıklara pratik bir çözüm sağlar. WPA, donanım değişikliğine gidilmeden WEP'e göre daha güçlü şifreleme (TKIP-Temporal Key Integrity Protocol-Geçici Anahtar Bütünlüğü Protokolü) ve kimlik doğrulama (802.1x) yapısına sahiptir. WPA'da veri miktarı veya zamana bağlı olarak değişen güvenlik anahtarı kullanılmaktadır. WEP ile kıyaslandığında WPA güvenlik şifresini elde etmek daha zordur ve daha fazla zaman harcamak gerekmektedir.

### **6.2.2.5. 802.1x kimlik doğrulaması**

Açık sistem veya paylaşılan anahtar kimlik doğrulaması, statik WEP anahtarları veya MAC kimlik doğrulamasına dayanan geleneksel WLAN güvenlik yöntemleri yeterince güvenli değildir. 802.1x, kablolu ethernet ağlarına ve kablosuz 802.11 ağlarına kimliği doğrulanmış ağ erişimi sağlamak ve port tabanlı ağ erişim kontrolünü gerçekleştirmek için kullanılan bir IEEE

standardıdır [23]. Merkezi kimlik doğrulama, dinamik anahtar yönetimi ve hesap oluşturma desteği sağlar. 802.1x standardı, bilgisayar ve ağın birbirlerinin kimliğini doğrulamalarına izin vererek, kablosuz bağlantılar üzerinden veri şifreleme için kullanıcı veya oturum bazında anahtarlar oluşturarak ve anahtarları dinamik olarak değiştirmeye olanak vererek güvenliği geliştirir.

802.1x, port tabanlı ağ erişim denetimini uygular. Bu denetim, LAN bağlantı noktasına bağlanmış bilgisayarın kimliğini doğrulamak ve kimlik doğrulama işlemi başarısız olduğunda ilgili bağlantı noktasına erişimi engellemek için anahtarlı LAN altyapısının fiziksel özelliklerini kullanır. Port tabanlı ağ erişim denetimi etkileşimi sırasında, LAN bağlantı noktası kimlik doğrulayıcı veya istemci rollerinden birini üstlenir. LAN bağlantı noktası kimlik doğrulayıcı rolünü üstlendiğinde, kullanıcıların bu bağlantı noktası üzerinden erişilebilen hizmetlere erişmelerine izin vermeden önce kimlik doğrulaması yapılmasını gerektirir. LAN bağlantı noktası istemci rolünü üstlendiğinde, kimlik doğrulayıcısının bağlantı noktası üzerinden erişilebilen hizmetlere erişimini gerektirir. Aynı bir varlık olabileceği gibi kimlik doğrulayıcı ile aynı yerde de bulunabilen kimlik doğrulama sunucusu, kimlik doğrulayıcısının adına istemcinin kimlik bilgilerini denetler. Böylece kimlik doğrulama sunucusu, kimlik doğrulayıcısına istemcinin kimlik doğrulayıcısının hizmetlerine erişmek için yetkili olup olmadığını belirten bir yanıt verir.

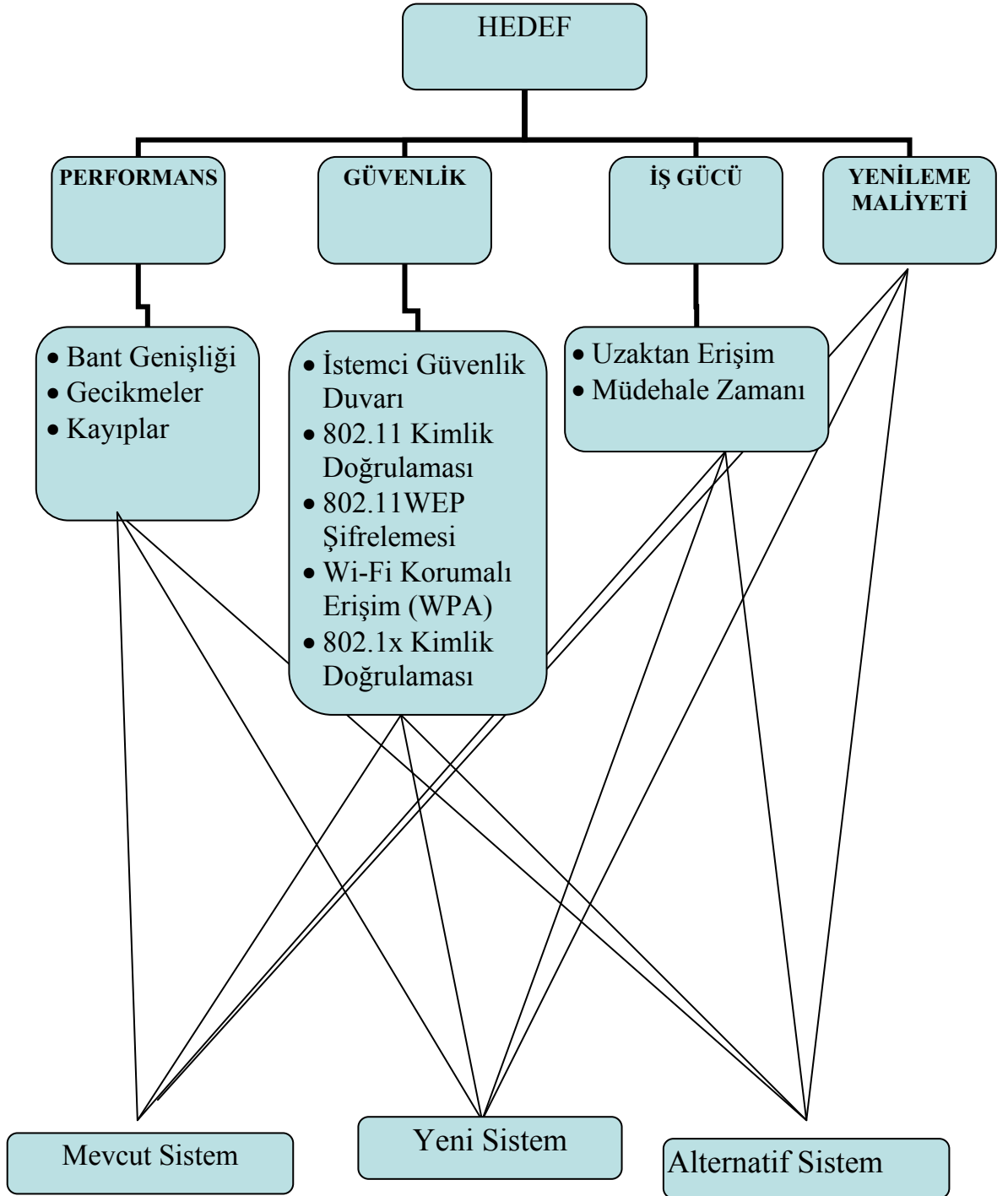
Kimlik doğrulayıcısının port tabanlı ağ erişim denetimi, bir fiziksel LAN bağlantı noktası üzerinden LAN'a giden iki mantıksal veri yolu tanımlar. İlk veri yolu olan denetlenmeyen bağlantı noktası, kimlik doğrulayıcısı ve LAN'da bulunan bilgisayar aygıtları arasında aygıtın kimlik doğrulama durumuna bakmadan veri geçişine izin verir. Bu, EAPoL iletilerinin alacağı yoldur. İkinci veri yolu olan denetlenmiş bağlantı noktası, kimliği doğrulanmış bir LAN kullanıcısıyla kimlik doğrulayıcısı arasında veri geçişine izin verir. Bu, bilgisayar aygıtının kimliği doğrulandıktan sonra, diğer tüm ağ trafiğinin geçeceği yoldur.

### **6.2.3. İş Gücü**

Ağ güvenlik sistemine müdahaleleri daha hızlı ve anında yapabilmek için mevcut sistem ve alternatif sistem arasında karşılaştırmalar yapılmıştır.

### **6.2.4. Yenileme Maliyeti**

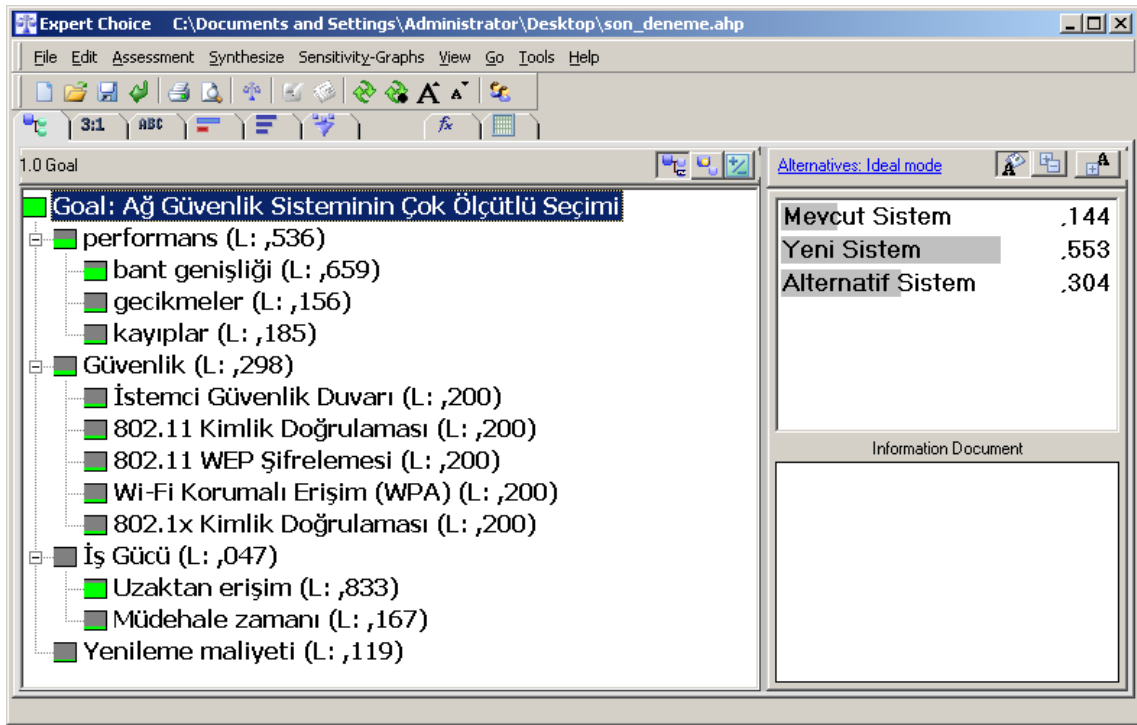
Karar verilecek yeni sistemin alternatiflerini belirlerken kullanılacak malzemeler, switchler, güvenlik yazılımları ve bunları yönetecek personelin eğitimi dahil maliyetler göz önüne alınmıştır.



#### Adım 1 : Karar Verme Problemi Tanımlanır

Karar verme probleminin tanımlanması, iki aşamadan oluşturulur. Birinci aşamada karar noktaları saptanır. Diğer bir deyişle karar kaç sonuç üzerinden değerlendirilecektir sorusuna cevap aranır. İkinci aşamada ise karar noktalarını etkileyen faktörler saptanır. Bu

çalışmada karar noktalarının sayısı  $m$ , karar noktalarını etkileyen faktör sayısı ise  $n$  ile sembolize edilmiştir. Özellikle sonucu etkileyecek faktörlerin sayısının doğru belirlenmesi ve her bir faktörün detaylı tanımlarının yapılması, ikili karşılaştırmaların tutarlı ve mantıklı yapılabilmesi açısından önemlidir.



Adım 2 : Faktörler Arası Karşılaştırma Matrisi Oluşturulur

Tablo 2.1 Önem Skalası

Önem Değerleri	Değer Tanımları
1	Her iki faktörün eşit öneme sahip olması durumu
3	1. Faktörün 2. faktörden daha önemli olması durumu
5	1. Faktörün 2. faktörden çok önemli olması durumu
7	1. Faktörün 2. faktöre nazaran çok güçlü bir öneme sahip olması durumu
9	1. Faktörün 2. faktöre nazaran mutlak üstün bir öneme sahip olması durumu
2,4,6,8	Ara değerler

Expert Choice C:\Documents and Settings\Administrator\Desktop\son\_deneme.ahp

File Edit Assessment Inconsistency Go Tools Help

3:1 ABC

Compare the relative importance with respect to: performans

bant genişliği

gecikmeler

Extreme  
Very Strong  
Strong  
Moderate  
Equal  
Moderate  
Strong  
Very Strong  
Extreme

	bant genişliği	gecikmeler	kayıplar
bant genişliği		5,0	3,0
gecikmeler			1,0
kayıplar			
	Incon: 0,03		

Expert Choice C:\Documents and Settings\Administrator\Desktop\son\_deneme.ahp

File Edit Assessment Inconsistency Go Tools Help

3:1 ABC

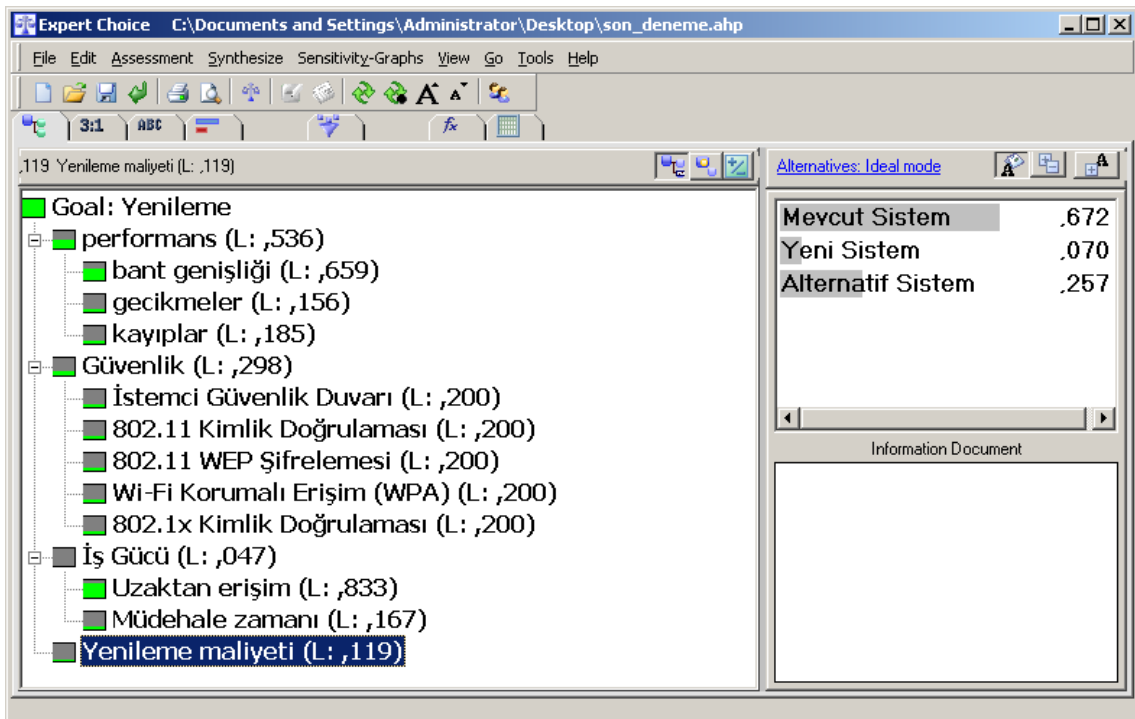
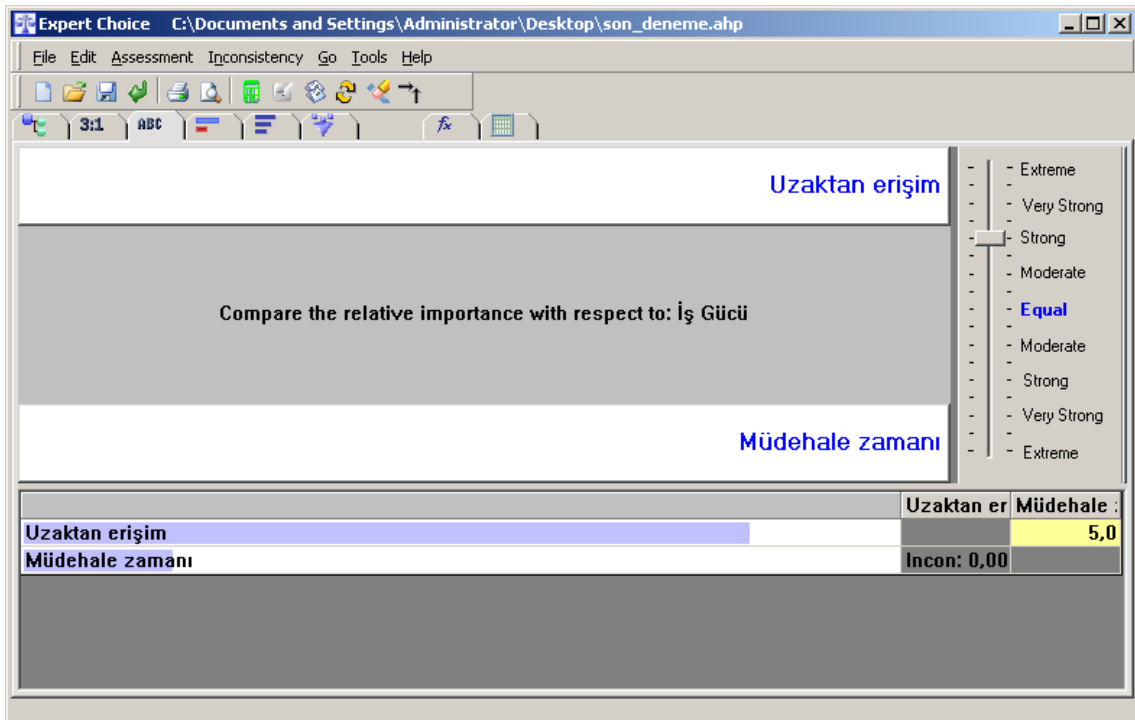
Compare the relative importance with respect to: Güvenlik

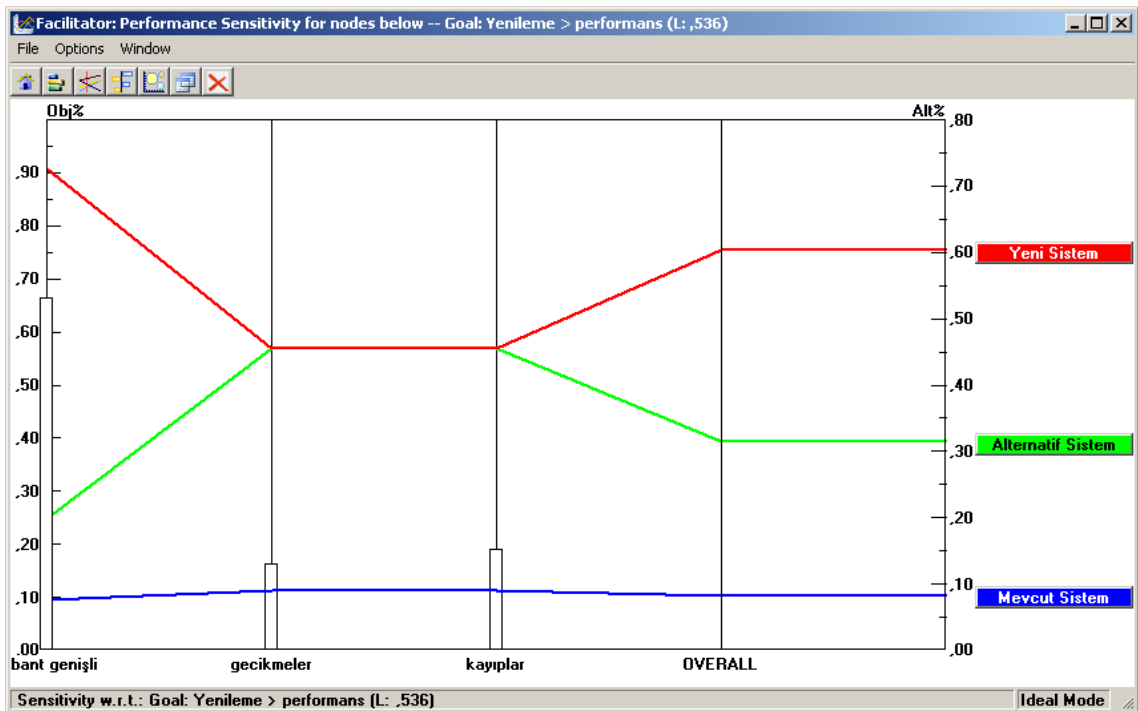
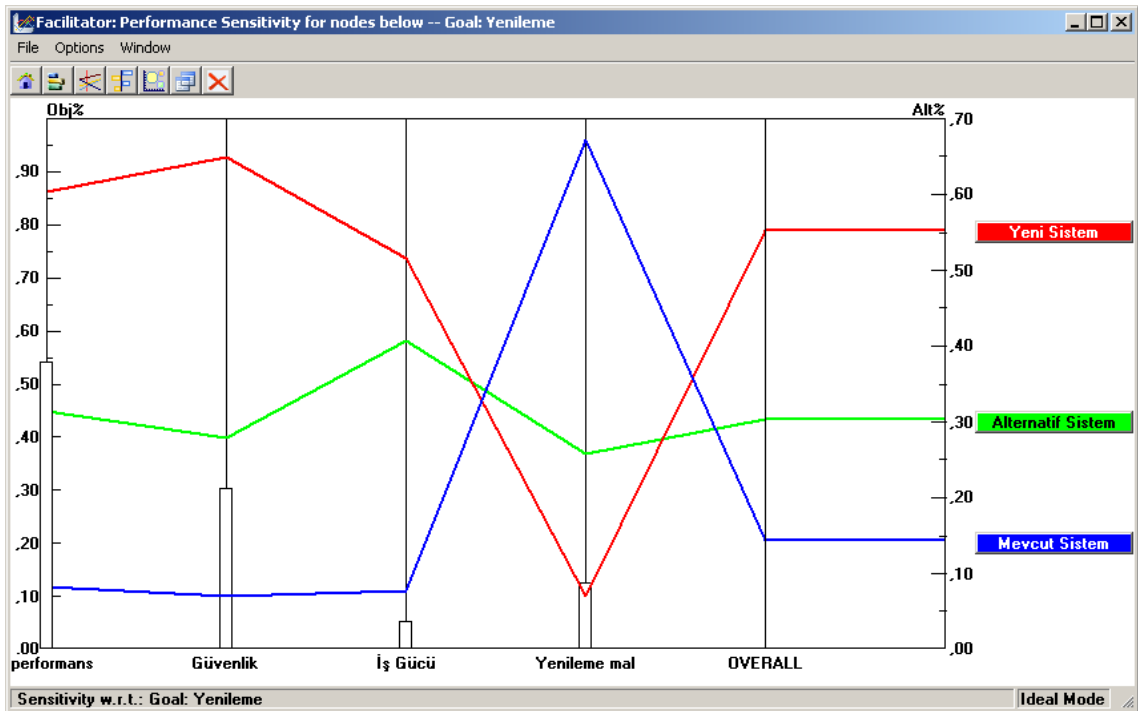
İstemci Güvenlik Duvarı

802.11 Kimlik Doğrulaması

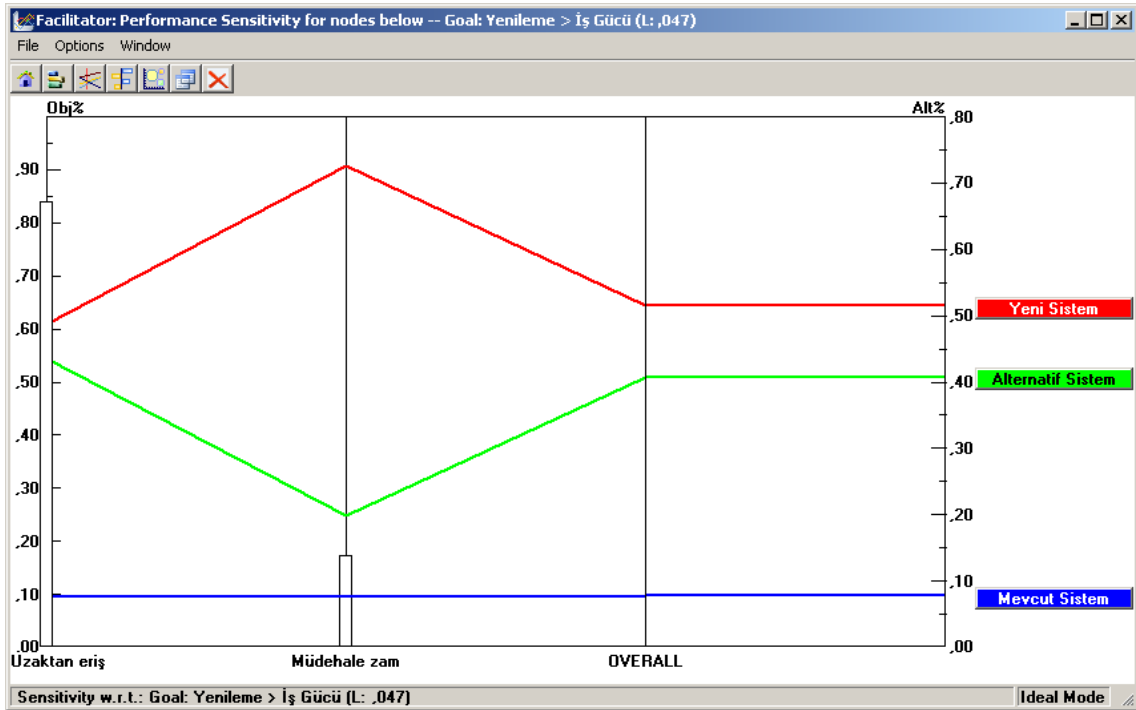
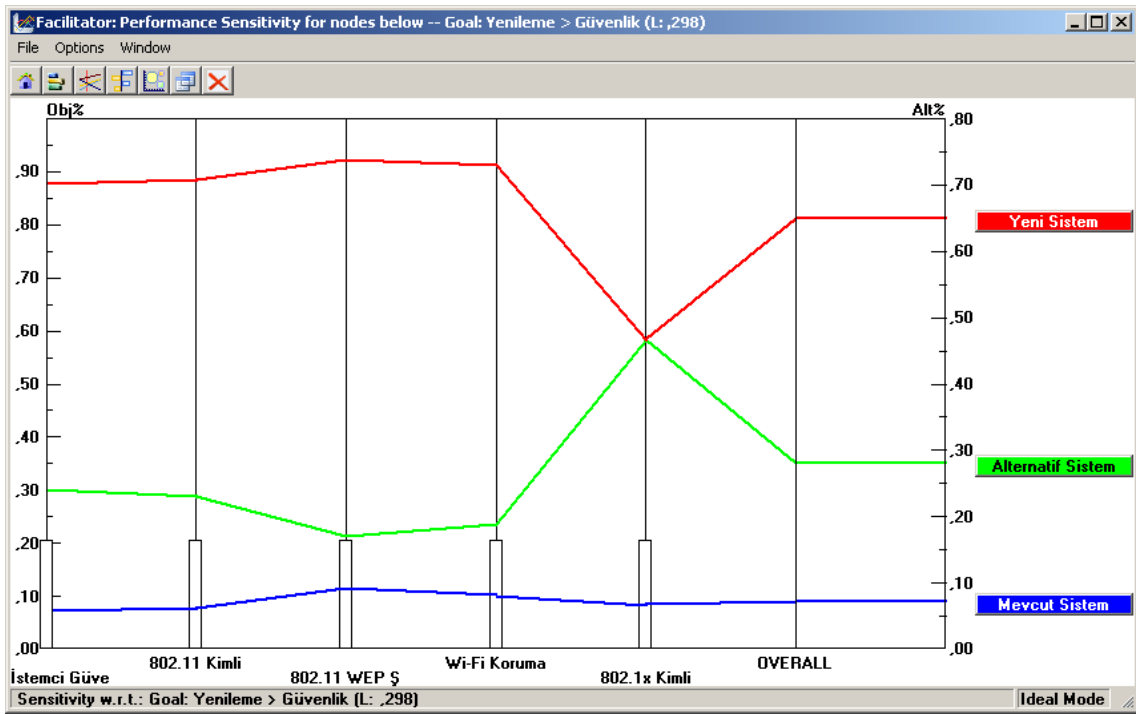
Extreme  
Very Strong  
Strong  
Moderate  
Equal  
Moderate  
Strong  
Very Strong  
Extreme

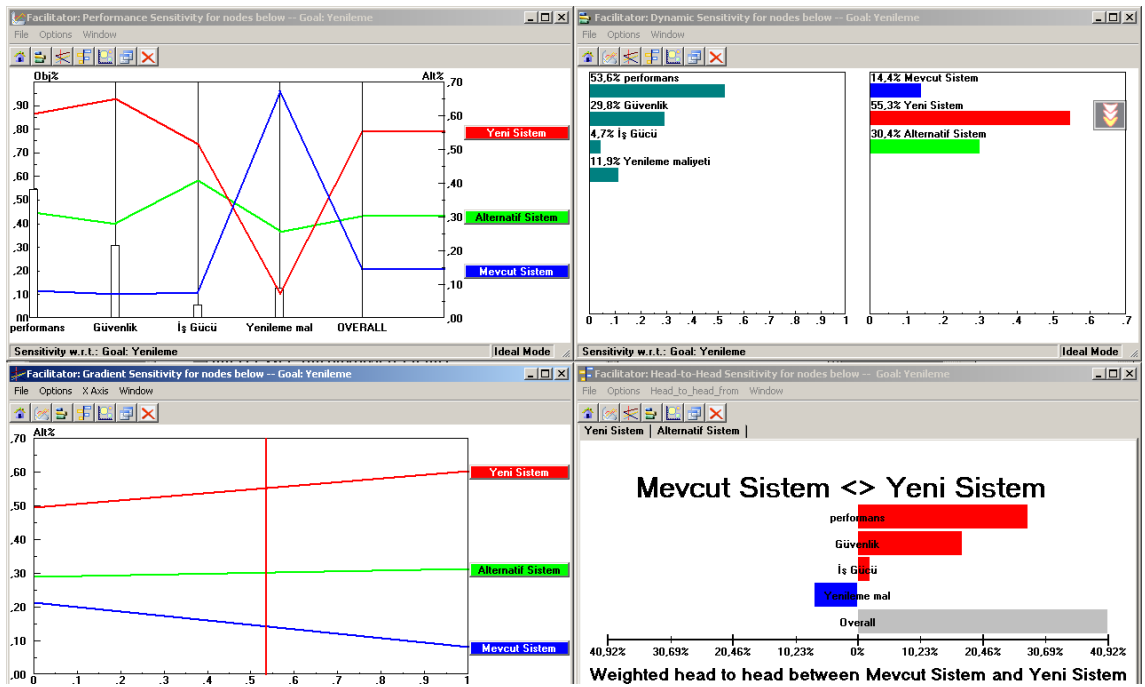
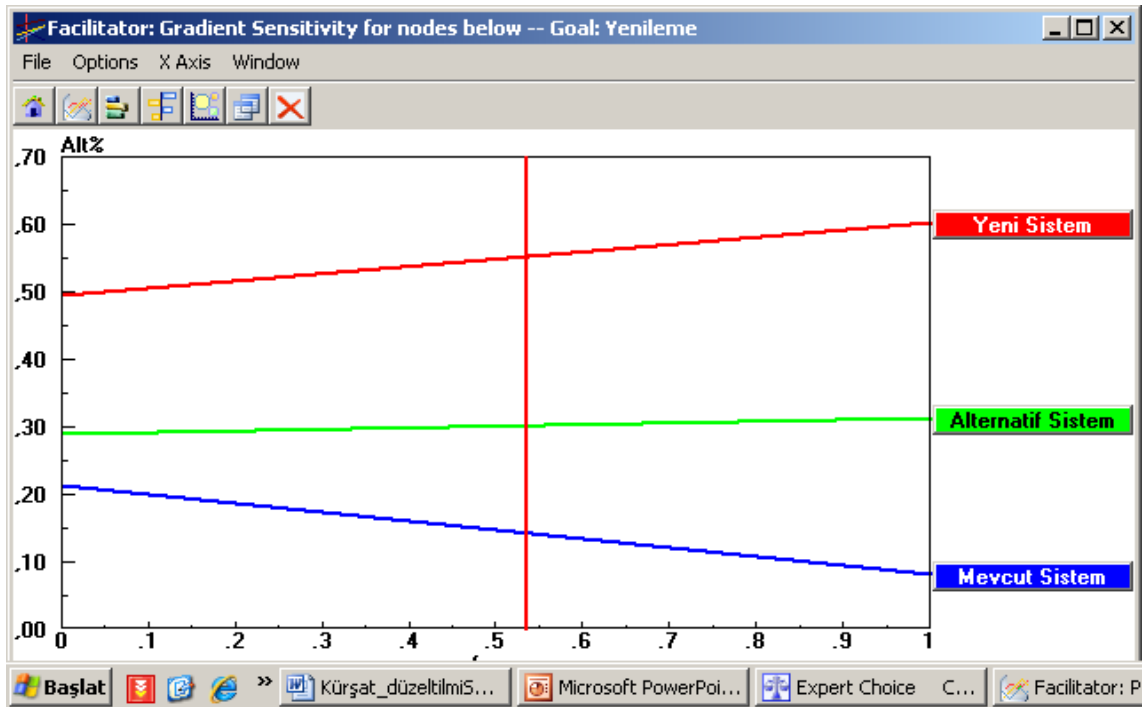
	İstemci Gü	802.11 Kim	802.11 WE	Wi-Fi Korum	802.1x Kim
İstemci Güvenlik Duvarı		1,0	1,0	1,0	1,0
802.11 Kimlik Doğrulaması			1,0	1,0	1,0
802.11 WEP Şifrelemesi				1,0	1,0
Wi-Fi Korumalı Erişim (WPA)					1,0
802.1x Kimlik Doğrulaması	Incon: 0,00				

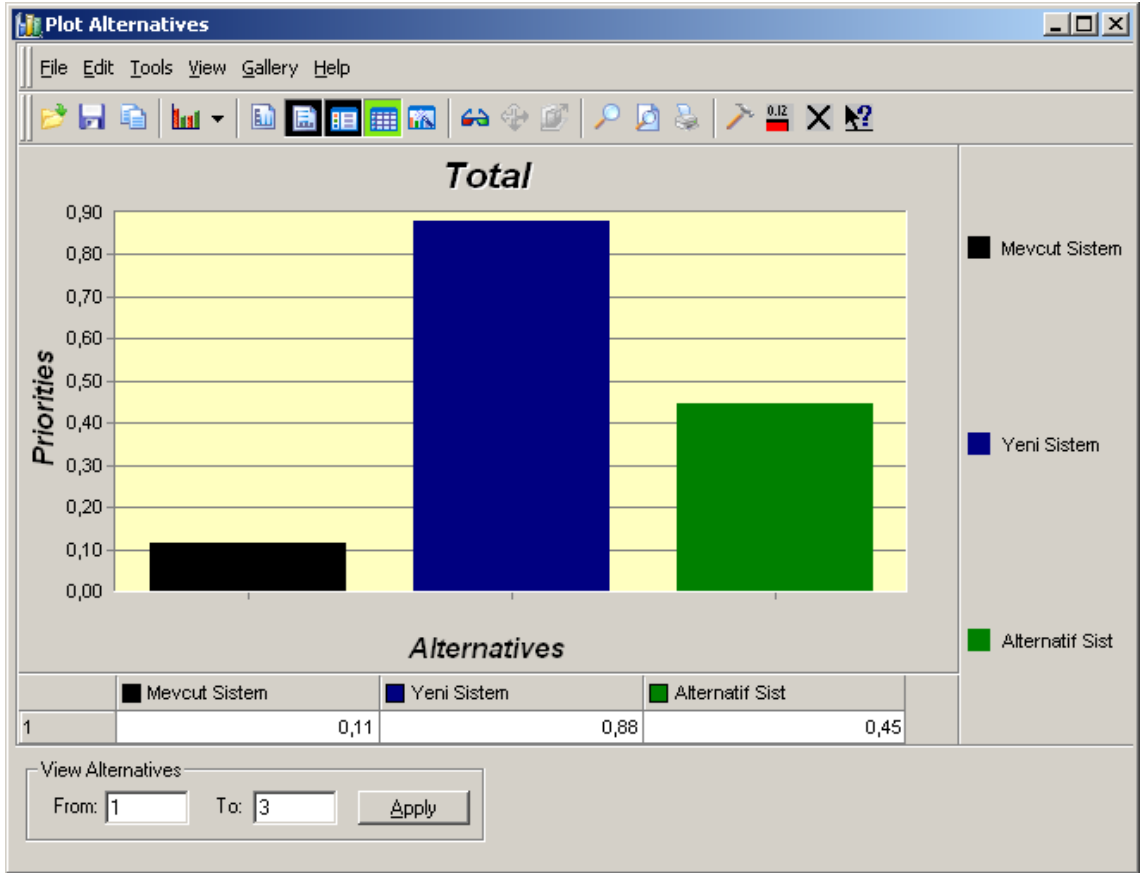












Görüldüğü üzere yapılan tercihin Yeni Sistem olması gerektiği sonucuna varılmıştır.

## 7. SONUÇ VE ÖNERİLER

Bu bölümde yapılan çalışmanın sonuçları ve devamında ileride yapılabilecek çalışmalar irdelenmiştir.

### 7.1 Sonuçlar

Bu çalışmada; yüksek risk oranına sahip Kampüs verilerinin, Kampüs içinden veya dışından oluşabilecek saldırılara karşı korunması amaçlanmış, bu ağlarda karşılaşılan bazı güvenlik problemlerinin çözümüne yönelik olarak bir Kampüsün hem kablolu, hem de kablosuz ağlarında otomatik VLAN yapılandırması ve ağa erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesine gidilerek bu kapsamda bir çözüm önerisi sunulmuştur. Uygulama ile LAN içerisinde risk oranı yüksek verilere sadece yetkili kullanıcıların kendilerine tanınan erişim hakları ile erişimleri sağlanmıştır. Sürekli olarak büyüyen Kampüs ağlarında açılacak olan her bir bilgi servisi, bilişim alt yapı yatırımlarını da beraberinde getirmektedir. Ağ ortamına eklenecek her bir cihazda otomatik VLAN yapılandırmasının etkin hale getirilmesiyle kullanıcı hataları ortadan kaldırılıp sistemin gün boyunca çalışmasındaki kesintiler vb. olayların yaşanması engellenebilecektir.

Yapılan çalışmanın kablosuz ağ uygulamaları kapsamında internet tarafında; hali hazırda kullanılmakta olan ve Kampüs çalışanlarına ait taşınabilir (notebook) bilgisayarların Kampüs otomasyon sistemine zarar vermeksizin, internet ortamına erişebilmeleri, öğrenci, personel ve misafir kullanıcıların şahsi mobil cihazları ya da taşınabilir bilgisayarları ile internete erişebilmeleri, dolayısıyla Kampüste kaldıkları sürece işlerini internet üzerinden takip edebilmeleri, mobil cihaz ve taşınabilir bilgisayara sahip olma oranı %80'lere varan ilaç firması temsilcilerinin Kampüs içerisindeki herhangi bir noktadan internetle ilgili tüm işlemlerini gerçekleştirebilmeleri öngörülmüştür. Kullanılan erişim noktalarının tespiti sırasında VLAN desteği göz önüne alınırsa, istenilen kullanıcıların ya da mobil cihazların (PDA) sadece internete erişmelerinden farklı olarak otomasyon sistemine erişimleri de mümkün olabilecektir.

Mevcut Kampüs ağ yapısında öğrenci ve personel internet hizmetinden yararlanabilmek için odalarına ve internet merkezlerine gitmek zorunda kaldıkları göz önüne alındığında, bu tür sorunların ortadan kaldırılması için çalışmada önerilen çözümün kablosuz teknolojilere uyarlanmasıyla, personel ve öğrenciler kablosuz cihazlarla SIS ve OBS sistemlerine erişimleri mümkün olabilecektir.

Tez çalışmasının tamamlandığı sıralarda uygulamanın omurga ve kenar ahatarların değişimi uygulamaya geçmiştir. DPÜ Kampüs Ağları'nın belirli katlarında demoları gerçekleştirilen uygulamanın getirdiği ve getirmesi beklenen katkılar şu şekilde sıralanabilir.

### **Güvenlik Anlamında;**

- DPÜ Kampüsleri ile Üniversite arasına güvenlik duvarı yerleştirilip IP ve port bazında sınırlamalar yapılarak kampüs ortamından gelen saldırılara karşı Kampüs ağının korunması,
- Güvenlik duvarının VLAN tabanlı yapılandırılmasıyla doğrudan güvenlik duvarına bağlı olmayan farklı VLAN'lar arasında güvenliğin sağlanması,
- Tüm kampüs birimlerinin ayrı DMZ'lere yerleştirilip merkezin dışında olan ve merkeze veri amaçlı erişen bölgelerin güvenlik seviyesi merkezden daha düşük tutularak, bu bölgelerden gelen trafikte belli portlara izin verilmesiyle geniş alan ağından merkeze yapılabilecek saldırıların engellenmesi,
- Kampüs'deki SIS ve OBS sunucularına sadece SQL ve ORACLE gibi belli portlardan erişim izni verilerek, bu sunuculara açık portlardan erişimin engellenmesi dolayısıyla güvenliğin sağlanması,
- Rol tabanlı yetkilendirmenin kullanıldığı servis kalitesi analizleri ile sistemdeki veri trafiği akışının düzenlenip performansın artırılması, güvenlik derecelendirmesi yoluna gidilmesi ile de risk oranı yüksek verilerin Kampüs içinden veya dışından oluşabilecek saldırılara karşı güvenliğinin temin edilmesi öngörülmüştür.

### **Kimlik Denetimi Anlamında;**

- Çalışanların sözleşmeli/kadrolu olmasına göre ya da vardiya/nöbet sistemi göz önüne alınarak hangi saatlerde internete, hangi saatlerde Kampüs otomasyonuna erişeceği belirlenmiştir. Belirlenen saatlerin dışında sisteme erişilemeyecektir.
- Personelin iş tanımına göre Kampüs içinde erişebileceği hizmetler belirlenerek yetki dahilinde olmayan elektronik hizmetlere erişim engellenmiştir.
- Kurum içi yazışma evrakları, elektronik yazışma evraklarının, yazan kişinin bilgisayarında değil, merkezde güvenli bir ortamda tutulması, sadece yetkili kişi/kişiler tarafından erişilebilmesi ve yine merkezde yedeklerinin tutulması sağlanarak kurum bilgilerinin gizliliğinin ve güvenliğinin arttırılması yoluna gidilmiştir.

- Kampüs içinde ağa bağlanacak kullanıcıların ve bilgisayarların kimlik denetiminden geçirilmesi ile Kampüs ve çalışanlara ait olmayan bilgisayarların ağa bağlanması, SIS ve OBS sistemine erişim denetiminin yapılabilmesi gerçekleştirilmiştir.
- Kampüs çalışanlarına verilen tek kullanıcı hesabı ile tek bir noktadan kullanıcıların tüm yetkileri tanımlanabilmiştir. Böylece kullanıcıların hangi VLAN'a üye olacağı yine merkezden belirlenmiştir.
- Mevcut yapıda ORACLE ve SQL trafiğinin öncelikli hale getirilmesi için servis kalitesi yapılandırılmasının yanında, otomatik VLAN yapılandırması ile kullanıcı tabanlı trafik önceliklendirmesi ve yetkilendirmesinin (hangi kullanıcıların Telnet yapabileceği vb.) gerçekleştirilmesi beklenmektedir.

### **Kablosuz Ağ Tarafında;**

- Güvenlik nedeniyle internete erişimi izin verilmeyen taşınabilir bilgisayarların kablosuz ağ üzerinden güvenli bir şekilde internete erişmeleri sağlanmıştır.
- Oluşturulan kablosuz ağ aracılığıyla, tablet bilgisayarlar veya PDA'lar ile kablosuz ağ üzerinden SIS ile ilgili işlemleri yapabilmeleri sağlanmıştır.

### **7.2 Gelecek Çalışmalara İlişkin Öneriler**

Bu çalışma ile ilgili verilebilecek öneriler şu şekilde sıralanabilir:

- En az iki tane etki alanı denetleyicisi, IAS sunucusu olarak tasarlanmalıdır. Birincil IAS üzerinde herhangi bir sorun olması durumunda ikincil IAS üzerinden kimlik doğrulama işlemlerinin kesintisiz olarak devam ettirilmesi gerekir. IAS sunucusu var olan etki alanı denetleyicileri üzerine kurulabileceği gibi maliyetlerin göz önüne alınması durumunda tamamen bu iş için adanmış sunucular üzerine de kurulabilir.
- Bu tür bir uygulamaya geçmeden önce, Kampüsdeki tüm bilgisayarlar, çalışanların görev ve yetkileri çok iyi bir şekilde analiz edilmeli, detaylı inceleme sonucu ihtiyaçlara göre gruplar belirlenmelidir. Gruplandırma işlemlerinde, kullanıcıların görev yaptığı birimler, kişinin pozisyonu ve kişinin çalışma saatleri göz önünde bulundurulmalıdır.
- Kimlik doğrulama uygulamasına geçilmeden önce elektronik ya da yazılı olarak kullanıcıların çok iyi bir şekilde bilinçlendirilmesi, gerekirse tüm kullanıcıların gruplar halinde eğitime alınması gerekmektedir.

- Uygulamaya geçmeden önce belirli noktalarda belirli kullanıcılar tarafından sistemin test edilmesi gerekir. Uygulamaya aynı anda Kampüsün tamamında değil, kat kat ya da parça parça geçilmelidir.
- Destek anlamında tüm bilgi işlem personelinin çok iyi bir şekilde bilinçlendirilmesi, oluşan sorunların kısa sürede çözümü için gereklidir.

Günümüz bilgi teknolojilerinde, veri iletişimini sağlayan cihazların yanı sıra bilgisayar destekli çalışan ve işe özgü çözüm üreten yazıcı, tarayıcı ve faks vb. cihazların ağa bağlanmaya başlamasıyla bu tür cihazların da zamanla hedef haline gelebileceği ihtimali ortaya çıkmıştır. Sınav sonuçlarının OBS bünyesinde yer alan yazılımlar ile veri merkezine aktarılması gerekmektedir. Kullanıcıların ağda mantıksal anlamda farklı VLAN'larda bulunmaları sağlansa da, mutlak şekilde ethernet üzerinden ağa bağlandıkları düşünüldüğünde, mevcut sistemde var olan sıradan bir SIS istasyonunun bir bilgisayar gibi tüm saldırılara açık hale gelmesi kaçınılmaz olacaktır. Böyle bir senaryonun gerçekleşmesi durumunda, bu cihazların bilgisayar destekli bölümlerinin arızalanması, cihazların tamirinde yaşanacak zaman ve maddi kayıplar ciddi boyutlara ulaşacaktır.

DPÜ Kampüslerinde kullanılan Java tabanlı öğrenci otomasyonları göz önüne alındığında, sürekli olarak sisteme giriş yapmaya çalışan personel, sistemde var olan virüs ya da solucanlar nedeniyle, bu verilere erişememe veya erişmede yavaşlıklar gibi bir takım problemlerle karşı karşıya kalmaktadırlar. Bu problemler işlerin yavaşlamasına ve uzamasına, öğrenci memnuniyetsizliğine ve çalışanların motivasyon bozukluğuna yol açmaktadır. Çalışmada önerilen çözüm ile birlikte uygulamanın gelecek çalışmalar kapsamında tasarlanabilecek olan "*Intelligent Network*" (Akıllı Ağ) uygulaması ile bu tür sorunların önüne geçilmiş olacaktır. [24],[25] Kampüs ağ yapısının büyüklüğü dikkate alındığında sınırlı sayıdaki personel sayısı, kontrol edilmesi gereken cihaz fazlalığı, günlük saldırı tespitleri gibi olayları aşmak için ağa bir saldırı yapıldığı anda sistemdeki saldırıyı tespit edecek, doğrudan kullanıcı portunu (hangi switche bağlıysa o portu) kapatacak ve yazılan erişim kurallarıyla sistemin bu işlemleri otomatik olarak yapmasını sağlayacak bir "Akıllı Network" tasarlanacaktır. Bu sayede;

- Farklı güvenlik seviyelerindeki kaynaklarda oluşabilecek solucan, virüs, saldırı gibi ağın yavaşlamasına ve hatta durmasına sebep olan faktörler engellenmiş olacak, otomasyon sisteminin maksimum çalışır halde kalması sağlanabilecektir.
- Bu güvenlik sistemi ile sadece kullanıcı bilgisayarları, sunucular ya da veri tabanları değil aynı zamanda bilgisayar destekli çalışan cihazlar da korunuyor olacaktır.

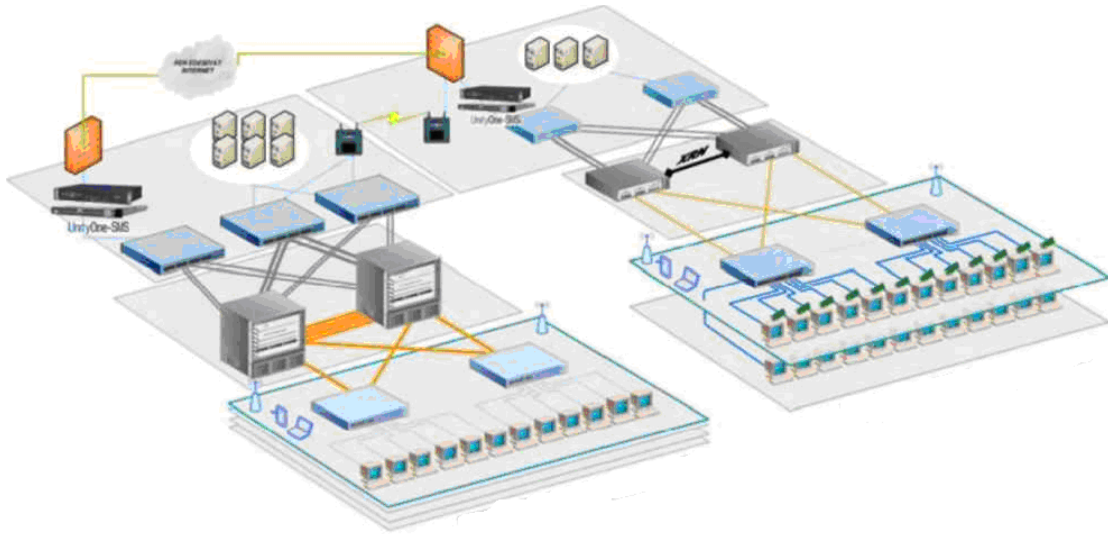
- Kullanıcı bilgisayarları, PDA'ler ağa girmeye çalıştığında bu bilgisayarlarda bulunan ve yayılmaya çalışan virüsler veya kullanıcıların farkında olmadığı saldırılar kenar switch bazında engellenebilecek, böylelikle bu tip saldırıların ağda yayılması engellenmiş olacaktır.
- Sisteme yapılabilecek olan saldırılar sadece port tabanlı değil aynı zamanda içerik tabanlı olarak tespit edilip kesilebilecektir.

Oluşturulan kablosuz ağ sistemleri yapısında ileride yapılması planlanan RF-ID (Radio Frequency Identification) özelliğinin kullanılmasıyla, Kampüs içinde; istenilen personelin ya da öğrencinin nerede olduğu gibi konum takip sistemleri için alt yapı oluşturulmuş olacaktır.

RF-ID konum belirleme ve takip özelliği sayesinde tipik bir Kampüste bu tür ihtiyaçların karşılanmasıyla kayıplar engellenebilecek, emek ve zaman kazancı sağlanarak ciddi oranlarda büyük tasarruflar elde edilebilecektir.

Gelecekte yapılması planlanan bir diğer konu da; Kampüs içinde kullanılmakta olan SIS ve OBS sistemlerinin 7 gün 24 saat devamlılığının sağlanabilmesi için, tam yedekli bir yapıya geçilecek olmasıdır (Şekil 7.2). Bu sunuculara Gigabit ethernet ilavesiyle erişim kapasitesi artırılacaktır. Omurga switch sayısı gibi ikiye çıkartılarak switchlerden birinde sorun olması durumunda tüm sistemin diğer omurga switch üzerinden devamlılığı sağlanabilecektir. Çalışma sırasında omurga switchler arasında yük paylaşımı yapılarak sistemin daha hızlı çalışmasına yardım edilecektir. Her bir binaya giden fiber optik kablo bağlantı sayısı ikiye çıkartılıp ana omurgada ayrı omurga switchlerine takılarak fiber optik kablo bağlantılarından birinde problem olması durumunda, diğeri üzerinden sisteme erişimin devam ettirilmesi sağlanacaktır. Ayrıca, güvenlik duvarının bağlı olduğu ve internet çıkışı olarak nitelendirilen switch, yine yedekli olarak her iki omurga switchine bağlanacaktır. Bu sayede, omurga switchlerden birinde problem olması durumunda, internet trafiği aksamadan diğeri üzerinden devam edebilecektir.





**Şekil 7.1** DPÜ Kampüs Ağları'nda tasarlanacak olan yedekli yapı topolojisi

Planlanan bu konularla birlikte, uygulama planının bir parçası ve ona paralel olarak idari, hukuki, teknik ve mali riskler tespit edilerek bir risk yönetim planı hazırlanmalıdır. Bu planda muhtemel riskler, ortaya çıkma olasılıkları, riskin ortaya çıkmasının projede yaratacağı etkiler, riski ortadan kaldırmak veya etkisini azaltmak için neler yapılabileceği ve riskin ortaya çıkması durumunda projenin ilerleyebilmesi için alternatif seçeneklerin neler olabileceği düşünülmüş olmalıdır. Kurumların, kurumsal güvenlik risklerini gerçekçi olarak değerlendirebilmek için diğer uzman kurumlardan ve bağımsız uzmanlardan destek almaları önerilmektedir.

## **8. LİTERATÜR ÇALIŞMASI**

Yapılan Çalışma Yurt içinde başka bir çalışma ile benzerlik sağlamamaktadır. Uluslar arası geçerliliğe sahip olan sciencedirect network security AHP olarak artılmış fakat hiçbir sonuca rastlanmamıştır. Google arama motorunda yapılan tarama sonucunda benzer bir çalışma olarak virginia polytechnic institute Edward D. Wagner'a ait mastır tezine rastlanmıştır.

## KAYNAKLAR

- [1] Schmidt, A. H., (2004) "Building a mosaic of security for a better world", Security Matters, Aspatore Books, U.S.A., 24-26.
- [2] Stytz, M. R., (2006) Banks, S.B., "Dynamic software security testing", Security & Privacy Magazine IEEE , 4(3):77.
- [3] McGraw, G., (2004) "Software security", Security & Privacy Magazine IEEE, 2(2): 80 – 81.
- [4] Gilliam, D.P., Wolfe, T. L., Sherif, J. S.; Bishop, M., (2003) "Software security checklist for the software life cycle", Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Linz, 243-248.
- [5] İnternet: CERT "CERT/CC Statistics 1988-2006" <http://www.cert.org/stats/> (04.03.2007).
- [6] Stalling, W. (2001) "High Speed Networks and Internets", Prentice Hall, New Jersey, 715s
- [7] Çetin, M., Aydos, M. (2005) "Otomatik Vlan Yapılandırmalarında IEEE 802.1x Standardı Kullanımının Sistem Performansına Etkisi" 2. İletişim Teknolojileri Ulusal Sempozyumu, Adana, s.211-214
- [8] Microsoft (2000) "Internet Authentication Service for Windows 2000", 154s., [http ://  
download.microsoft.com/download/b/6/4/b64bcb2e-867c-4458-ae8-589d750e68a8  
/IAS.doc](http://download.microsoft.com/download/b/6/4/b64bcb2e-867c-4458-ae8-589d750e68a8/IAS.doc) (12.09.2005)
- [9] Rigney, C., Rubens, A., Simpson, W., and Willens, S., (1997) "Remote Authentication Dial In User Service (RADIUS)", RFC 2138. [http://www.ietf.org/rfc/  
rfc2138.txt?number=2138](http://www.ietf.org/rfc/rfc2138.txt?number=2138) (13.10.2005)
- [10] Rigney, C., Willens, S., Rubens, A. and Simpson, W., (2000) "Remote Authentication Dial In User Service (RADIUS)", RFC 2865. <http://www.ietf.org/rfc/rfc2865.txt?number=2865> (13.10.2005)
- [11] Rigney, C., (2000) "RADIUS Accounting", RFC 2866. <http://www.ietf.org/rfc/rfc2866.txt?number=2866> (13.10.2005)
- [12] Bulusu, N., (2003) "Implementation and Performance Analysis of The Protected Extensible Authentication Protocol", Master Thesis, Faculty of Graduate School of the University of Colorado at Colorado Springs, 169s
- [13] Microsoft (2003) "Deployment of IEEE 802.1x for Wired Networks Using Microsoft Windows", 41s. [http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-  
020818f57234/Wired\\_depl.doc](http://download.microsoft.com/download/b/0/e/b0e2a363-0044-4327-8f17-020818f57234/Wired_depl.doc) (13.12.2005)

### KAYNAKLAR ( devamı )

- [14] Blunk, L. and Vollbrecht, J., (1998) "PPP Extensible Authentication Protocol (EAP)", RFC 2284. <http://www.ietf.org/rfc/rfc2284.txt?number=2284> (13.10.2005)
- [15] Moen, R., (2004) "802.1x Port-Based Authentication How To". <http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/8021X-HOWTO.pdf> (27.12.2005)
- [16] Aboba, B. and Simon, D. (1999) "PPP EAP TLS Authentication Protocol", RFC 2716. <http://www.ietf.org/rfc/rfc2716.txt?number=2716> (13.10.2005)
- [17] Funk, P., and Wilson, S. B., (2005) "EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0)", <http://www.watersprings.org/pub/id/draft-funk-eap-ttls-v0-00.txt> (13.10.2005)
- [18] Cambazoğlu, T., (2003) "Internet ve Güvenlik", 78s. **Hata! Köprü başvurusu geçerli değil.** (18.9.2005)
- [19] WEB\_1. (2006). Microsoft TechNet Windows Server 2003 Active Directory. <http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx> (07.01.2006).
- [20] Aboba, B., (2003) "IEEE P802.11 Wireless LANs", s.8-10 <http://www.drizzle.com/~aboba/IEEE/11-03-154r1-I-Virtual-Access-Points.doc> (11.02.2006)
- [21] Çetin, M., Karaman, M. ve Aydos, M., (2006) "Risk Oranı Yüksek Veri Yoğunluğuna Sahip Kampüs Ağlarında IEEE 802.1x Standardı ile Ağ Güvenliği ve Otomatik VLAN Yapılandırmaları", Bilgi Teknolojileri Kongresi IV-Akademik Bilişim 2006, Denizli, s.408-413
- [22] Stallings, W. (2000) "Data & Computer Communications", 6th Ed., Prentice Hall, International, 810s.
- [23] IEEE Std 802.1X (2001) "IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control", IEEE
- [24] Fout, T., and Barkley, W., (2001) "Wireless 802.11 Security with Windows XP", 14s. <http://cnscenter.future.co.kr/resource/rsc-center/vendor-wp/microsoft/XP80211Security.doc> (20.01.2006)
- [25] Ayyagari, A. and Fout, T., (2001) "Making IEEE 802.11 Networks Enterprise-Ready", 56s. <http://www.microsoft.com/windows2000/docs/wirelessec.doc> (20.01.2006)

## EKLER

### Ek-1

### 3Com SuperStack 3 Switch 4400 ve 7700 Serilerinin Özellikleri

#### 3Com SuperStack 3 Switch 4400 Serisinin Özellikleri

Ürün Özellikleri	3Com SuperStack 3 Switch 4400 24-port	3Com SuperStack 3 Switch 4400 48-port	3Com SuperStack 3 Switch 4400-PWR	3Com SuperStack 3 Switch 4400-FX
Port Sayıları	24 x 10/100 + 2 Genişleme Yuvası	48 x 10/100 + 2 Genişleme Yuvası	24 x 10/100 (PoE) + 2 Genişleme Yuvası	24 x 100Base-FX + 2 genişleme yuvası
Anahtarlama Kapasitesi	8.8 Gbps	13.6 Gbps	8.8 Gbps	8.8 Gbps
İletim Oranı	6.6 Mpps	10.1 Mpps	6.6 Mpps	6.6 Mpps
İletim Metodu	Sakla-veilet, gecikme < 2.6 µs (Store-and-Forward)			
MAC Adres Kapasitesi	8000 MAC Adresi, 256 Güvenli MAC Adresi			
VLAN	64 (IEEE 802.1q)			
Hat Toplama (Link Aggregation)	IEEE 803.2ad LACP, 4 kanal grubu (her bir kanalda 4 port), Farklı istiflerdeki portları gruplayabilme			
Hız ve Çift-Yön (Duplex) Otomatik-Görüşme (Auto-Negotiation)	Otomatik MDI/MDIX, hız ve çift yön modu (tüm portlarda)			
Trafik Kontrolü	IEEE 802.3x tam çift yön (full-duplex) akış kontrolü, yarı çift yön (half-duplex) için geri baskı ve yayın fırtınası kontrolünü (3,000 pps eşik değeri) destekler.			
Kapsayan Ağaç Protokolü (Spanning Tree Protocol) Kontrolü	IEEE 802.1D STP, IEEE 802.1w RSTP, STP ile geriye-uyumluluk, STP hızlı-başla (fast-start) modu, port başına STP etkinleştirme/devre dışı bırakma			
İstifleme	384 porta kadar istifleyebilme, İstif yönetimi için tek bir IP adresi, Esnek döngü dönüşü, Çalışırken takılıp/çıkanlabilen (hot-swappable) istif			
Çoklu Gönderim (Multicast)	128 multicast grup için filtreleme, 2. Katman arayüzü üzerinde IGMP araştırma (IGMP snooping), IGMPv1 ve IGMPv2, IGMP Sorgulayıcı			
Öncelik Kuyrukları	Her port için 4 öncelik kuyruğu, WRR kuyruklama, Katı öncelik kuyruklaması			
Trafik Önceliklendirme	IEEE 802.1p Servis Sınıfı (Class-of-Service - CoS ) İşaretleme/Yeniden İşaretleme, kaynak / hedef TCP/UDP port numarasına, IP adresine/protokole göre, CoS - Ayrılmış Servisler Kod Noktası (Differentiated Services Code Point - DSCP) dönüştürme, varsayılan port önceliği ve 3Com NBX telefon			

	trafiğinin otomatik sınıflandırılmasına göre önceliklendirmeyi destekler.
Bant Genişliği Yönetimi	Port-tabanlı bant genişliği yönetimi, 1 Mbps artırımlar ile (10/100 portlar için), 8 Mbps artırımlar ile (Gigabit portlar için), uygulama / protokol bloklama
Esneklik	3Com Gelişmiş Fazla Güç Kaynağı (Advanced Redundant Power Supply) ile anahtara yedek güç, Anahtar konfigürasyonun yedekleme ve geri devreye alınması.
Ağ Erişimi	IEEE 802.1x kullanıcı kimlik doğrulama, RADIUS kimlik doğrulama, Port başına birçok kullanıcının MAC adreslerini kilitleyebilme, Porta bağlı kullanıcıya göre otomatik VLAN ve QoS profili atayabilme, Misafir VLAN opsiyonu, Radius Kimlik Doğrulanmış Cihaz Erişimi (RADA), RADIUS sunucusunda MAC adresine göre otomatik kimlik doğrulama, Port başına birçok cihazın kimlik doğrulanması, Belirlenmiş portlara bağlanan cihazlara otomatik VLAN ve QoS profili atayabilme,
	Kullanıcı-cihaz ikilisine göre IEEE 802.1x kimlik doğrulama, Bilinmeyen Cihazın Bağlantısını Kes (DUD) özelliği, RADIUS sunucusu kullanılmadığı durumlarda varsayılan VLAN üyeliği
Anahtar Yönetimi	Anahtar şifrelerinin yerel veya RADIUS yönetimi, Güvenilir IP yönetim adresleri, Telnet, Syslog, SSHv1 (56-bit DES), SSHv2 (168bit DES)
Uzak Yönetim	SNMPv1, kullanıcı tanımlı yönetim VLAN'ı tarafından
Yazılım	Yedekleme ve geri yükleme, TFTP konfigürasyon ve yükleme, TFTP ajanı
Konfigürasyon	Komut satırı arabirimi, Konsol (Seri port), Telnet, SNMP, Web-tabanlı
Ayna Portu (Mirror Port) / RAP (Roving Analysis Port - Tarayan Analiz Portu)	Bire bir
IP Adres tahsisi	E1 ile, DHCP, Otomatik IP, BOOTP
Ağ Zamanı	Syslog tarafından yakalanmış olaylara zaman damgası atamak için Basit Ağ Zaman Protokolü (SNTP)
RMON grupları	4 grup:Tarihçe, olaylar, alarmlar, istatistikler

### 3Com SuperStack 3 Switch 7700 Serisinin Özellikleri

<b>Ürün Özellikleri</b>	<b>3Com Switch 7700 4-slot, 7-slot, 8-slot</b>
Performans	
Anahtarlama Kapasitesi	7-slot ve 8-slot için 96 Gbps, 4-slot için 48 Gbps
İletim Oranı	7-slot ve 8-slot için 177 Mpps, 4-slot için 95 Mpps
Azami Bant Genişliği	7-slot ve 8-slot için 240 Gbps, 4-slot için 120 Gbps
<b>2. Katman Anahtarlama Özellikleri</b>	
MAC Adres Kapasitesi	32000 MAC Adresi, 10K Statik MAC Adresi,

	Modül iletimi (gecikme <10µs), 9K Jumbo Çerçeve desteği
VLAN	4096 (IEEE 802.1q), Port-tabanlı (IEEE 802.1q) ve protokol-tabanlı (IEEE 802.1v), Protokol tabanlı VLAN kullanarak IPv6 tünelleme, GVRP (GARP VLAN Registration Protocol) desteği
Hat Toplama (Link Aggregation)	E1 ile veya IEEE 803.2ad LACP, Azami 64 kanal grubunu destekler.
Hız ve Çift-Yön (Duplex) kOtomatik-Görüşme (Auto-Negotiation)	Otomatik MDI/MDIX, Hız ve çift yön modu (tüm portlarda)
Trafik Kontrolü	IEEE 802.3x tam çift yön (full-duplex) akış kontrolü Yarı çift yön (half-duplex) için geri baskı ve VLAN başına yayın fırtınası kontrolünü destekler.
Kapsayan Ağaç Protokolü (Spanning Tree Protocol) Kontrolü	IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s Çoklu Kapsayan Ağaç Protokol (MSTP) örneği, Tek STP örneği, BPDU (Köprü Protokol Data Birimi - Bridge Protocol Data Unit) koruması
<b>3. Katman Anahtarlama Özellikleri</b>	
Rotalar	Donanım-tabanlı yönlendirme, 64000 IP rota, 64000 statik rota, 64000 dinamik/statik ARP girdisi, 64 IP arayüzü
IP Yönlendirme	RIPv1, RIPv2, OSPF (50 bölge), BGPv4 IS-IS desteği
Çoklu Gönderim (Multicast)	Donanım-tabanlı tel-hızında çoklu gönderim yönlendirme, 1K çoklu gönderim rotası, 2. Katman arayüzü üzerinde IGMP araştırma (IGMP snooping), IGMPv1 ve IGMPv2, IGMP Sorgulayıcı, GMRP (GARP Multicast Registration Protocol), PIM-DM, PIM-SM
Ağ Protokolleri	DHCP Relay, TCP/IP Protokol Yığılı, ARP
Esneklik	VRRP (Sanal Yönlendirici Fazlalık Protokolü), Anahtar başına 14 sanal yönlendirici, Her bir sanal yönlendirici 16 adet IP adresini destekler.
<b>Yakınsama Özellikleri</b>	
Öncelik Kuyrukları	Her port için 8 öncelik kuyruğu
Trafik Önceliklendirme	Akış tabanlı QoS profilleri, Giriş kuyruğu ve çıkış kuyruğunda, IEEE 802.1p Servis Sınıfı (Class-of-Service - CoS ), Kaynak/ hedef TCP/UDP port numarasına, Kaynak/hedef IP adresine göre, Ayrılmış Servisler Kod Noktasına (Differentiated Services Code Point - DSCP), Seçilebilen port önceliği, 3Com NBX telefon trafiğinin otomatik sınıflandırılması, Ethertype numarasına göre önceliklendirmeyi destekler.
Bant Genişliği Yönetimi	Akış tabanlı bant genişliği yönetimi, Akışlar erişim kontrol listeleri ile tanımlanabilir,

	Asgari ve azami eşik değerleri: 64 Kbps artırımlar ile port başına 128 trafik sınıfı, sınıf başına 512 akış.
Kuyruk İşleme	Rasgele Erken Tespit (Random Early Detection - RED), Katı Öncelik Kuyruklama, Bant genişliği yönetimi ile ilişkilendirilmiş WRR kuyruklama algoritmalarını destekler.
Güvenlik Özellikleri	
Ağ Erişimi	IEEE 802.1x kullanıcı kimlik doğrulama, Yerel kimlik doğrulama ve RADIUS kimlik doğrulama
Paket Filtreleme	Donanım içerisinde tel-hızında paket filtreleme, Azami 1536 ACL(Erişim Kontrol Listesi) listesini destekler. 2. 3. ve 4. katmanda ACL filtreleme: fiziksel port, kaynak/hedef MAC adresi, VLAN bilgisi, Ethernet tipi (Ethertype), 3. Katman protokol kaynak/hedef IP adresi, DSCP, veri paketi tipi, IP 4. Katman protokol ve IP 4.Katman portlarına göre paket filtreleme yapabilmektedir.
Anahtar Protokol Güvenliği	RIPv1, RIPv2, OSPFv2 ve SNMPv3 trafiği için MD-5 gizli-yazı ve temiz-yazı kimlik doğrulaması
Anahtar Yönetimi	Anahtar Telnet oturumları üzerinde IEEE 802.1x kullanıcı kimlik doğrulama, Yönetim arayüzü için hiyerarşik yönetim ve şifre koruması
Yönetim Özellikleri	
Sistem Konfigürasyonu ve Yönetimi	Komut Satırı Arayüzü (CLI) konfigürasyon modu, Konsol portu ile konfigürasyon, Telnet ile yerel veya uzaktan konfigürasyon, Çevirmeli modem ile uzaktan konfigürasyon, SNMP v1,v2 ve v3 ile sistem konfigürasyonu, Ayrıntılı istatistikler, RMON grupları: tarihçe, istatistikler, alarmlar ve olaylar, ACL/QoS istatistikleri, IP arayüzü istatistikleri, Sistem logları, Syslog sunucu desteği
Sistem Bakımı	Detaylı alarm/hata ayıklama bilgisi, Hiyerarşik alarmlar, Alarm üretimi, Alarm filtreleme, İstatistikler, Ping ve Traceroute komutlarını destekler, Konfigürasyon yedekleme ve geri yükleme
Sistem Dosya Transfer Mekanizmaları	XModem, FTP ve TFTP



**Ek-2****İnternet ve otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi şu şekildedir:**

*Hem internet hem de otomasyon sistemini kullanan kablolu ağlar için erişim kontrol listesi acl name otomasyoninternet advanced*

*rule 1 permit tcp source 192.168.80.0 0.0.0.255 destination 192.168.10.2 0.0.0.255 eq 1433*

*rule 2 permit tcp source 192.168.80.0 0.0.0.255 destination 192.168.10.3 0.0.0.255 eq 1521*

*rule 3 permit tcp source 192.168.80.0 0.0.0.255 destination 192.168.10.4 0.0.0.255 eq 1521*

*rule 4 permit ip source 192.168.80.0 0.0.0.255 destination 192.168.3.0 0.0.0.255*

*rule 5 permit tcp source-port eq 4899 destination 192.168.150.0 0.0.0.255*

*rule 6 permit tcp source-port eq telnet*

*rule 7 permit tcp destination-port eq telnet*

*rule 8 deny tcp*

*rule 9 deny udp*

*#*

*Hem internet hem de otomasyon sistemini kullanan kablolu ağlar için VLAN 80 oluşturulması vlan 80 description otomasyon & internet VLAN 80*

*interface oluşturulması interface Vlan-*

*interface 80 ip address 192.168.80.1*

*255.255.255.0 dhcp-server 1*

*Erişim kontrol listesinin Omurga Switch portuna atanması*

*interface GigabitEthernet2/0/1 port link-type trunk*

*port trunk permit vlan 70 80 200 201 222 702 711 712 721 722 731 732 741 742 751 752 801*

*802 811 812 821 822 831 832 841 842 851 852 901 1020 1030*

*qos*

*packet-filter inbound ip-group otomasyoninternet rule 1 system-index 1 packet-*

*filter inbound ip-group otomasyoninternet rule 2 system-index 2 packet-filter*

*inbound ip-group otomasyoninternet rule 3 system-index 3 packet-filter inbound*

*ip-group otomasyoninternet rule 4 system-index 4 packet-filter inbound ip-group*

*otomasyoninternet rule 5 system-index 5 packet-filter inbound ip-group*

*otomasyoninternet rule 6 system-index 6 packet-filter inbound ip-group*

*otomasyoninternet rule 7 system-index 7 packet-filter inbound ip-group*

*otomasyoninternet rule 8 system-index 8 packet-filter inbound ip-group*

*otomasyoninternet rule 9 system-index 9*

**Yalnızca otomasyon sistemine erişim yetkisi verilen kullanıcılar için yazılmış olan erişim listesi ise şu şekildedir:**

*Otomasyon sistemini kullanan kablolu ağlar için erişim kontrol listesi acl name otomasyon advanced*

*rule 1 permit ip source 192.168.70.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 rule 2 permit*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.10.0 0.0.0.255 rule 3 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.2.7 0.0.0.255 rule 4 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.2.8 0.0.0.255 rule 5 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.2.13 0.0.0.255 rule 6 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.7.5 0.0.0.255 rule 7 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.7.7 0.0.0.255 rule 8 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.10.3 0.0.0.255 rule 9 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.10.4 0.0.0.255 rule 10 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.10.7 0.0.0.255 rule 11 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.10.8 0.0.0.255 rule 12 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.100.30 0.0.0.255 rule 13 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.201.0 0.0.0.255 rule 14 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.200.0 0.0.0.255 rule 15 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.150.0 0.0.0.255 rule 16 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.151.0 0.0.0.255 rule 17 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.152.0 0.0.0.255 rule 18 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.153.0 0.0.0.255 rule 19 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.154.0 0.0.0.255 rule 20 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.155.0 0.0.0.255 rule 21 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.156.0 0.0.0.255 rule 22 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.157.0 0.0.0.255 rule 23 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.158.0 0.0.0.255 rule 24 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.159.0 0.0.0.255 rule 25 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.160.0 0.0.0.255 rule 26 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.161.0 0.0.0.255 rule 27 deny*

*ip source 192.168.70.0 0.0.0.255 destination 192.168.162.0 0.0.0.255 rule 28 deny*

```

ip source 192.168.70.0 0.0.0.255 destination 192.168.163.0 0.0.0.255 rule 29 deny
ip source 192.168.70.0 0.0.0.255 destination 192.168.164.0 0.0.0.255 rule 30 deny
ip source 192.168.70.0 0.0.0.255 destination 192.168.100.0 0.0.3.255
#

```

*Otomasyon sistemini kullanan kablolu ağlar için VLAN 70 oluşturulması*

*vlan 70*

*description otomasyon*

*VLAN 70 interface oluşturulması*

*interface Vlan-interface70*

*ip address 192.168.70.1 255.255.255.0*

*dhcp-server 1*

*Erişim kontrol listesinin Omurga Switch portuna atanması*

*interface GigabitEthernet2/0/1 port link-type trunk*

*port trunk permit vlan 70 200 201 222 702 711 712 721 722 731 732 741 742 751 752 801*

*802 811 812 821 822 831 832 841 842 851 852 901 1020 1030*

*qos packet-filter inbound ip-group otomasyon rule 1*

*system-index 1 packet-filter inbound ip-group otomasyon rule 2*

*system-index 2 packet-filter inbound ip-group otomasyon rule 3*

*system-index 3 packet-filter inbound ip-group otomasyon rule 4*

*system-index 4 packet-filter inbound ip-group otomasyon rule 5*

*system-index 5 packet-filter inbound ip-group otomasyon rule 6*

*system-index 6 packet-filter inbound ip-group otomasyon rule 7*

*system-index 7 packet-filter inbound ip-group otomasyon rule 8*

*system-index 8 packet-filter inbound ip-group otomasyon rule 9*

*system-index 9 packet-filter inbound ip-group otomasyon rule 10*

*system-index 10 packet-filter inbound ip-group otomasyon rule 11*

*system-index 11 packet-filter inbound ip-group otomasyon rule 12*

*system-index 12 packet-filter inbound ip-group otomasyon rule 13*

*system-index 13 packet-filter inbound ip-group otomasyon rule 14*

*system-index 14 packet-filter inbound ip-group otomasyon rule 15*

*system-index 15 packet-filter inbound ip-group otomasyon rule 16*

*system-index 16 packet-filter inbound ip-group otomasyon rule 17*

*system-index 17 packet-filter inbound ip-group otomasyon rule 18*

*system-index 18 packet-filter inbound ip-group otomasyon rule 19*

*system-index 19 packet-filter inbound ip-group otomasyon rule 20*

*system-index 20 packet-filter inbound ip-group otomasyon rule 21*  
*system-index 21 packet-filter inbound ip-group otomasyon rule 22*  
*system-index 22 packet-filter inbound ip-group otomasyon rule 23*  
*system-index 23 packet-filter inbound ip-group otomasyon rule 24*  
*system-index 24 packet-filter inbound ip-group otomasyon rule 25*  
*system-index 25 packet-filter inbound ip-group otomasyon rule 26*  
*system-index 26 packet-filter inbound ip-group otomasyon rule 27*  
*system-index 27 packet-filter inbound ip-group otomasyon rule 28*  
*system-index 28 packet-filter inbound ip-group otomasyon rule 29*  
*system-index 29 packet-filter inbound ip-group otomasyon rule 30*  
*system-index 30*

**Erişim listeleri ile VLAN222'den (WLAN) gelen kullanıcıların (notebook), tüm sunuculara ve diğer masaüstü bilgisayarlara ağdan herhangi bir şekilde (TCP/UDP) erişimleri engellenmesi.**

*Sadece interneti kullanan kablosuz ağ kullanıcıları için erişim kontrol listesi acl name*  
*wlaninternetonly advanced*  
*rule 1*  
*permit ip source 192.168.222.0 0.0.0.255 destination 192.168.2.6 0.0.0.255 rule 2 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.10.0 0.0.0.255 rule 3 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.2.7 0.0.0.255 rule 4 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.2.8 0.0.0.255 rule 5 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.2.13 0.0.0.255 rule 6 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.7.5 0.0.0.255 rule 7 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.7.7 0.0.0.255 rule 8 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.10.3 0.0.0.255 rule 9 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.10.4 0.0.0.255 rule 10 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.10.7 0.0.0.255 rule 11 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.10.8 0.0.0.255 rule 12 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.100.30 0.0.0.255 rule 13 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.201.0 0.0.0.255 rule 14 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.200.0 0.0.0.255 rule 15 deny*  
*ip source 192.168.222.0 0.0.0.255 destination 192.168.150.0 0.0.0.255 rule 16 deny*

```

ip source 192.168.222.0 0.0.0.255 destination 192.168.151.0 0.0.0.255 rule 17 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.152.0 0.0.0.255 rule 18 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.153.0 0.0.0.255 rule 19 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.154.0 0.0.0.255 rule 20 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.155.0 0.0.0.255 rule 21 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.156.0 0.0.0.255 rule 22 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.157.0 0.0.0.255 rule 23 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.158.0 0.0.0.255 rule 24 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.159.0 0.0.0.255 rule 25 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.160.0 0.0.0.255 rule 26 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.161.0 0.0.0.255 rule 27 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.162.0 0.0.0.255 rule 28 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.163.0 0.0.0.255 rule 29 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.164.0 0.0.0.255 rule 30 deny
ip source 192.168.222.0 0.0.0.255 destination 192.168.100.0 0.0.3.255
#

```

*WLAN için VLAN 222 oluşturulması*

```

vlan 222
description WLAN_Only_Internet_VLAN_222
interface oluşturulması
interface Vlan-interface222
ip address 192.168.222.1 255.255.255.0
dhcp-server 1

```

*Erişim kontrol listesinin Omurga Switch portuna atanması*

```

interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 70 200 201 222 702 711 712 721 722 731 732 741 742 751 752 801
802 811 812 821 822 831 832 841 842 851 852 901 1020 1030 qos
packet-filter inbound ip-group
wlaninternetonly rule 1 system-index 1 packet-filter inbound ip-group
wlaninternetonly rule 2 system-index 2 packet-filter inbound ip-group
wlaninternetonly rule 3 system-index 3 packet-filter inbound ip-group
wlaninternetonly rule 4 system-index 4 packet-filter inbound ip-group
wlaninternetonly rule 5 system-index 5 packet-filter inbound ip-group

```

wlaninternetonly rule 6 system-index 6 packet-filter inbound ip-group  
wlaninternetonly rule 7 system-index 7 packet-filter inbound ip-group  
wlaninternetonly rule 8 system-index 8 packet-filter inbound ip-group  
wlaninternetonly rule 9 system-index 9 packet-filter inbound ip-group  
wlaninternetonly rule 10 system-index 10 packet-filter inbound ip-group  
wlaninternetonly rule 11 system-index 11 packet-filter inbound ip-group  
wlaninternetonly rule 12 system-index 12 packet-filter inbound ip-group  
wlaninternetonly rule 13 system-index 13 packet-filter inbound ip-group  
wlaninternetonly rule 14 system-index 14 packet-filter inbound ip-group  
wlaninternetonly rule 15 system-index 15 packet-filter inbound ip-group  
wlaninternetonly rule 16 system-index 16 packet-filter inbound ip-group  
wlaninternetonly rule 17 system-index 17 packet-filter inbound ip-group  
wlaninternetonly rule 18 system-index 18 packet-filter inbound ip-group  
wlaninternetonly rule 19 system-index 19 packet-filter inbound ip-group  
wlaninternetonly rule 20 system-index 20 packet-filter inbound ip-group  
wlaninternetonly rule 21 system-index 21 packet-filter inbound ip-group  
wlaninternetonly rule 22 system-index 22 packet-filter inbound ip-group  
wlaninternetonly rule 23 system-index 23 packet-filter inbound ip-group  
wlaninternetonly rule 24 system-index 24 packet-filter inbound ip-group  
wlaninternetonly rule 25 system-index 25 packet-filter inbound ip-group  
wlaninternetonly rule 26 system-index 26 packet-filter inbound ip-group  
wlaninternetonly rule 27 system-index 27 packet-filter inbound ip-group  
wlaninternetonly rule 28 system-index 28 packet-filter inbound ip-group  
wlaninternetonly rule 29 system-index 29 packet-filter inbound ip-group  
wlaninternetonly rule 30 system-index 30