RİSK ORANI YÜKSEK VERİ YOĞUNLUĞUNA SAHİP GENİŞ HASTANE AĞLARINDA IEEE 802.1x STANDARDI İLE AĞ GÜVENLİĞİ VE OTOMATİK VLAN YAPILANDIRMALARI

Meriç ÇETİN
Pamukkale Üniversitesi
Bilgisayar Müh. Bölümü
mcetin@pau.edu.tr

Muhittin KARAMAN
Pamukkale Üniversitesi
Hastaneleri Bilgi İşlem Merkezi
mkaraman@pau.edu.tr

Murat AYDOS
Pamukkale Üniversitesi
Bilgisayar Müh. Bölümü
maydos@pau.edu.tr

ÖZET

Dağınık bir yerleşime sahip olan Pamukkale Üniversitesi Hastaneleri, LAN uygulamalarıyla birlikte MAN ağ uygulamalarını da bünyesinde barındırmaktadır. Ancak bir takım problemler nedeniyle ağın güvenli ve etkin bir şekilde kullanılmadığı ve risk oranı yüksek verilerin LAN'da güvenlik tehditleri ile karşı karşıya kaldığı gözlenmiştir.

Yapılan bu çalışmada, karşılaşılan bu problemlerin çözümüne yönelik olarak Otomatik VLAN yapılandırması ve hastane ağına erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmiştir. Uygulama sonucu olarak risk oranı yüksek veriler, gerek internet ortamında gerekse kampüs içinde herhangi bir güvenlik duvarı ile sadece bu ortamlardan gelebilecek saldırılara karşı korunurken, LAN'da gerçek kullanıcıların bulunduğu ortamda yetkili ya da yetkisiz tüm kullanıcılar tarafından aynı erişim hakları ile erişilmektedir. Bu verilere LAN içerisinde sadece yetkili kurum çalışanlarının erişmesiyle yani ağa erişen kullanıcıların kimlik doğrulamasının yapılmasıyla sadece yetkili kullanıcıların kendilerine tanınan erişim hakları ile risk oranı yüksek verilere erişmeleri sağlanmıştır.

Ayrıca uygulamada kullanılan Otomatik VLAN yapılandırmaları sayesinde de sürekli gelişen ağlarda yönetimin kolaylaştırılması ve ağ kaynakları yönetiminin merkezileştirilmesi sağlanmıştır.

ABSTRACT

Pamukkale University Hospital Department buildings are located in seperate geographic areas in the campus. Therefore the Hospital's network system contains not only LAN solutions but also MAN structures and applications. However, due to the some technical problems, it has been observed that the network system is not being used effectively and securely, and the data with high security risk is faced with security treats.

In this work, in order to overcome this defined problems, some methods have been developed. The main approach in these solutions are using Auto VLAN structure and monitoring and controlling the access to the Hospital's networks system by the means of providing authentication for all users. As a result of this work, the data with high security risk is being protected by using a firewall against the treats that may come from internet and inside of the network. At the same time this data is being accessed by all real authenticated users authorized and non-authorized with the same access rights.

In addition to the benefits mentioned above, with the use Auto VLAN structures, rapidly growing network structures can now easily be implemented and network sources management can easily be centralized.

Anahtar Kelimeler: IEEE 802.1x, Otomatik VLAN, Hastane Ağları, Ağ Güvenliği, Kimlik Doğrulama, Risk Oranı Yüksek Veri

1.GİRİŞ

Pamukkale Üniversitesi Hastaneleri, Denizli ili içerisinde dağınık bir yerleşime sahip olmasıyla birlikte Hastane ana yerleşkesi Üniversite kampusü içerisinde yer almaktadır. Hastaneye ait yerleşim alanları; Kınıklı Kampusü, Bayramyeri Hayat Hastanesi, Bayramyeri Göz Merkezi, Kınıklı Güneş Binası, Kınıklı Fizik Tedevi Merkezi ve Kınıklı Ana Deposu şeklindedir. Sahip olduğu bu dağınık yapısı nedeniyle sistem, ağ alt yapısı olarak LAN (Local Area Network) uygulamalarıyla birlikte MAN (Metropolitan Area Network) ağ uygulamalarını da bünyesinde barındırmaktadır.

Hastane ağı içerisinde yer alan sunucular; ORACLE, SQL Veritabanı Sunucuları (HIS, LIS), Active Directory Domain Sunucuları, Proxy Sunucusu, Web Filter Sunucusu, DNS, DHCP Sunucuları, Merkezi Antivirus Sunucusu, Proxy, Windows Güncelleme Servis Sunucusu ve Dosya Sunucusudur. Aktif ürün olarak Omurgada 3COM 7700-8R, katlarda 4400 L2-L4 Switchler kullanılarak; servis önceliklendirmesi

anlamında HIS'te kullanılan ORACLE ve SQL veritabanlarına erişimin öncelikli hale getirilmesi, belirli servislerin kullanım yoğunluğuna göre band genişliğinin arttırılması ya da azaltılmasının gerçekleştirilmesiyle verinin en kısa iletim zamanında taşınması sağlanmıştır.

Hastane Bilgi Teknolojileri kapsamında ana yerleşkede HIS ve LIS uygulamalarının hizmete girmesiyle beraber gerek hastalara ait gizli ya da özel bilgilerin gerekse mali bilgilerin güvenliğinin sağlanması için Hastane ile üniversite ağı arasına güvenlik duvarı yerleştirilmiştir. Hastane içinden veya dışından oluşabilecek saldırılara karşı veri güvenliğini sağlamak için sunucular görevlerine göre farklı **D**e**M**ilitarized **Z**one-DMZ'lere (Güvenlik Bölgelerine) yerleştirilmiştir. Her bir DMZ için güvenlik seviyeleri ayarlanarak sunucular arasında da güvenlik derecelendirmesi uygulamasına gidilmiştir.

Veritabanı sunucuları en yüksek güvenlik bölgesine yerleştirilirken Active Directory Domain sunucuları bir alt seviye DMZ bölgesine yerleşitirilerek 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.

Ağ içindeki broadcast (yayın) domain'lerinin (etki alanı) sayısını arttırmak ve mevcut broadcast domainlerini parçalara ayırmak için Statik VLAN uygulamasına gidilerek kat bazında ikişer adet olmak üzere **V**irtual **L**ocal **A**rea **N**etwork-VLAN'lar (Sanal Yerel Ağlar) yaratılmıştır. Statik VLAN'ların oluşturulması için switch'in belirli portları VLAN'a dahil edilir ve portlar ağ yöneticisi tarafından değiştirilene kadar bu VLAN'ın üyesi olarak kalır [1], [2].

Kullanıcı ve iş istasyonlarının Outside tarafından sonraki en düşük güvenlik bölgesine yerleştirilmesiyle Hastane içinden sunuculara gelebilecek saldırıların da önüne geçilmiştir. Böylece Hastane içindeki kullanıcıların ağa yapabilecekleri muhtemel saldırılardan korunmakla beraber Hastane içindeki iş istasyonları ve kullanıcılar da Outside tarafında yer alan kampus ortamından korunmuş olurlar.

Kullanıcıların etki alanında oturum açması için DMZ dışında yer alan domain sunucularına kimlik doğrulaması yaptırması tercih edilmiştir. Active Directory Domain'i içinde yer alan kullanıcı ve bilgisayarların etki alanı içindeki yetkileri Grup Politikaları ile belirlenmiştir. Tüm Hastane birimlerin organizasyonel birimlere ayrılması ile birime göre farklı Grup Politikaları uygulanabilmiştir. İşletim sistemlerine ait güncellemeler Windows Güncelleme Servis Sunucusu üzerinden Grup Politikası ile güncelleştirilmektedir. Merkezi antivirus yazılımı ile tüm iş istasyonlarının tek bir noktadan antivirus güncellemeleri, virüs tarama gibi işlemleri yapabilmektedir.

Hastanelerdeki hasta yoğunluğu, beraberinde hizmet veren personel sayısı ve çeşitliliğini getirdiği gibi iş yoğunluğunun azaltılması için gerekli olan PC sayısını arttırmaktadır. Yüksek miktarlardaki iş istasyonlarının ve kullanıcıların tek bir noktadan yönetilebilmesi için Active Directory Domain'leri kurularak bölüm ya da görev bazında farklı organizasyonel birimler tanımlanmış, kullanıcı ve bilgisayarlar bu birimlere yerleştirilmiştir. Dağınık bir yerleşime sahip olan Hastanenin her yerleşim yeri için *Child Domain*'ler kurularak tek bir *Forest* (orman) yapısı içerisinde *Domain Tree'* ler (etki alanı ağaçları) oluşturulmuştur. Active Directory Domain'i yapısı sayesinde birimler için ayrı ayrı Grup Politikaları oluşturularak birime özgü haklar ve kurallar belirlenmiştir.

2.MEVCUT SİSTEMDE YAŞANAN SORUNLAR

Aşağıdaki maddelerde mevcut sistemde yaşanan sorunlar ve bu sorunların giderilmesinde kullanılabilecek çözüm önerilerinden 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 Hastane personeli, gerek hasta yakını ve gerekse ilaç firması temsilcilerinin herhangi bir şekilde ağa kişisel bilgisayarları ile erişiminin kontrol ve denetiminin sağlanamaması,
- Hastane içinde kullanılan ve Active Directory Domain'i içinde yer alan bilgisayarlara her türlü yeni gelişmenin kolay uygulanabilmesine karşılık, etki alanına üye olmayan bilgisayarlara yeni gelişmelerin tek bir noktadan ve kısa zamanda uygulanmasında sorunlarla karşılaşılması,
- Hastane 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,
- Hastane içinde çalışmakta olan kullanıcıların ağa erişimlerinin zamanlama sınırlamasının yapılamaması,
- Hastane çalışanlarının kendi çalışma saatlerine bağlı olarak sisteme erişebilecekleri saatlerin kısıtlanamaması,

- Internet 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.

Çözüm Önerileri:

Üniversite Hastanesinde karşılaşılan bu problemlerin çözümünde, Otomatik VLAN yapılandırması ve ağa erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin yapılması yöntemine gidilmiştir.

Bir Statik VLAN oluşturulurken ağ yöneticisinin, switch'in belirli portlarını VLAN'a dahil ettiğini belirtmiştik. Bu durumda portlar ağ yöneticisi tarafından değiştirilene kadar bu VLAN'ın üyesi olarak kalırlar. Dinamik VLAN oluşturmada ise ağ yöneticisi sistemin kurulumu aşamasında ağda bulunan tüm cihazların MAC (**M**edia **A**ccess **C**ontrol) adreslerini bir veri tabanına alarak ağdaki adreslerin VLAN'lara üyeliğini gerçekleştirir. Bu yöntemde MAC adresleri kullanılarak hangi cihazın hangi VLAN'a ait olacağı belirlenir. 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 hapsolduğundan sistemin görünür bant genişliği artar ve sistemden daha yüksek hızlarda veri akışı sağlanır [1].

Sanal yerel ağların kullanılmasının önemi; belli işleri yapmak üzere kurumsal bir ağ üzerinde farklılaştırılarak ayrılmış yerel ağların dinamik yapılarındaki değişimlerden etkilenmemeleridir. 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 kısalır.

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 (**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice) protokolünü kullanarak IAS (**I**nternet **A**uthentication **S**ervice) sunucusuna 802.1x bilgilerini gönderir. IAS sunucusu üzerindeki uzak erişim politikaları, kullanıcı hesabının özel bir VLAN grubu 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 [1], [3].

3.UYGULAMA

Otomatik VLAN yapılandırması ve kimlik doğrulama işleminin gerektirdiği işlemler aşağıdaki maddelerde detaylı olarak açıklanmıştır:

1. Active Directory Yapılandırması
2. IAS Yapılandırması
3. Kenar switch olarak adlandırılan switch'lerin Authentication (Kimlik Doğrulama) switch'i olarak yapılandırılması
4. Otomatik VLAN için omurga ve kenar switch'lerin yapılandırılması
5. İş istasyonlarının PEAP MS-CHAPv2 için yapılandırılması
6. Sertifika sunucusunun yapılandırılması
7. Erişim kurallarının yazılması

3.1 Active Directory Yapılandırması

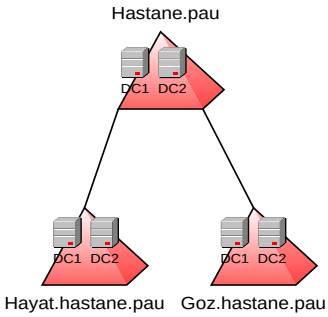
Active Directory yapılandırma işlemi dört aşamadan oluşmaktadır.

3.1.a-Active Directory Domain yapılandırması

Active Directory; kullanıcı, bilgisayar ve ağ kaynakları hakkında bilgilerin saklandığı Windows 2003 ve Windows 2000 ile beraber gelen dağınık 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.

Üniversite Hastaneleri Domain yapısı tek bir forest yapısı (*hastane.pau*) şeklinde tasarlanmıştır. Hastane'ye ait her bir yerleşim yeri aynı forest içerisinde var olan *hastane.pau* etki alanına *child domain* olarak tasarlanmıştır. Burada bulunan kullanıcıların Authentication işlemlerini ana yerleşkede bulunan etki alanı denetleyicilerine yaptırmamak ve aradaki düşük band genişliğinin sadece hasta verileri için kullanılmasıyla, aynı zamanda domaine girmeye çalışan kullanıcıların uzun süre beklemelerini engelleme amacı güdülmüştür.



Şekil 1. Active Directory Domain yapısından bir kesit

Ayrıca mevcut sistemde var olan Windows 2000 etki alanı denetleyicileri Windows 2003'e yükseltilmiştir. Bu işlem gerçekleştirilirken etki alanı içerisinde yükseltme işleminden sonra eski seviyeye geri dönüş yapılamayacağından dolayı Windows 2000 ve öncesi etki alanı denetleyicilerinin olmamasına dikkat edilmiştir.

3.1.b-Dinamik VLAN yapılandırması için Active Directory gruplarının tasarımı

Dinamik VLAN yapılandırması, Statik VLAN yapılandırmasının aksine farklı fiziksel noktalarda bulunan kullanıcı ve bilgisayarların ağ kaynaklarının mantıksal olarak üye oldukları gruplara göre gruplandırılmasını sağlar. Örneğin Hastane içinde farklı katlarda bulunan kullanıcı, bilgisayar ve kaynakların aynı Windows grubuna üye edilmesiyle aynı VLAN içinde dolayısıyla aynı ağ grubunda yer almaları sağlanır.

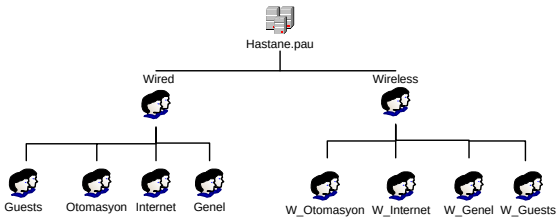
Hastane içinde grup tanımlamaları yapılırken Dinamik VLAN uygulaması için birimlere göre gruplandırma baz alınmıştır. Örneğin Döner Sermaye İşletme Müdürlüğüne bağlı Resmi İşlemler ile yine aynı Müdürlük içindeki Fatura servisi aynı birimde olmasına rağmen farklı gruplara dolayısıyla farklı VLAN'lara üye edilmesi hedeflenmiştir.

Hastane içinde var olan birim ve birime ait alt birimlerin her biri için *Security Global Group*'lar (Genel Güvenlik Grupları) oluşturulmuş, bu birimde çalışan kişiler, ilgili genel güvenlik gruplarına üye edilmiştir.

3.1.c-Merkezi denetim için Active Directory gruplarının tasarımı

Hastane içinde gerek hasta 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 gerekir.

Yapılan uygulamada Hastane içinde yer alan kullanıcılar, sadece otomasyon kullananlar (*Otomasyon Grubu*), sadece internet kullananlar (*Internet*), hem internet hem de otomasyon kullananlar (*Genel*), ağa hiçbir şekilde kimlik doğrulama yaptırmayanlar (*Guest-Misafir*) şeklinde farklı Genel Gruplara (Universal Group) ayrılmıştır. Ayrıca bu grupları 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 ayırmak da mümkündür.



Şekil 2. Ağa erişimin denetlenmesi için oluşturulan Universal Gruplar

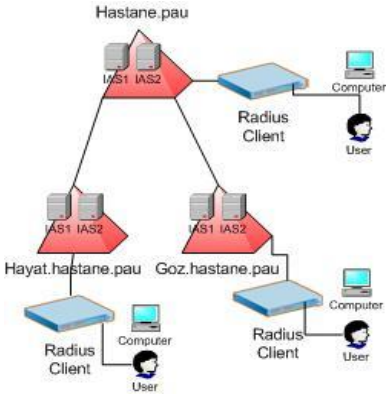
Dinamik VLAN yapılandırması için oluşturulan Genel Güvenlik Grupları yetkilerine göre ilgili Genel Gruplara üye edilerek ilgili haklardan yararlandırılabilir.

3.1.d-Kullanıcı Hesapları için Remote Access Permission (Uzak Erişim İzinlerinin) Düzenlemesi

Etki alanı içerisinde yer alan kullanıcılar için verilebilecek olan uzak erişim izinleri; ***Allow Access, Deny Access, Control Access Through Remote Access Policy***'dir. Belirtilmiş olan seçenekler kullanıcının yetkilendirilmesi için kullanılır. Hastane etki alanı Windows 2003 seviyesine yükseltildiği için ***Control Access through Remote Access Policy*** seçeneği seçilerek kullanıcıların yetkilendirilmesi işlemlerinin politikalarla belirlenmesi yöntemi tercih edilmiştir.

3.2 IAS Yapılandırması

Hastane ağında tüm etki alanlarında birden fazla etki alanı denetleyicisi olmasından dolayı IAS, etki alanı denetleyicileri üzerine kurulmuştur. Her etki alanı kendi IAS sunucusunu kendi içinde barındırmakta olup, her bir etki alanı için Authentication (Kimlik Doğrulama) ve Accounting (Hesap Oluşturma) işlemleri bu sunucular üzerinden geçekleştirilmektedir. Böylelikle ayrı etki alanlarının bulunduğu uzak noktalar arasında ekstra Radius trafiğinin oluşumu engellenmiş olur. Uygulamada, etki alanı içinde IAS sunucular kurulurken her bir etki alanında Primary (Birincil) ve Secondary (İkincil) olmak üzere ikişer adet Radius sunucusu oluşturulmuştur [4].



Şekil 3. Genel Hastane ağından bir kesit

IAS yapılandırma işlemi aşağıda belirtilen dört aşamadan oluşmaktadır:

3.2.a-Birincil IAS sunucu yapılandırması

IAS Sunucuları Native 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 kapsaması sağlanabilir. Ayrıca kullanıcı hesabına özel, statik yönlendirme tanımlaması yapılması sağlanır. IAS'in, Active Directory'de saklanan kullanıcı hesapları Dial-in özelliklerine erişebilmesi için RAS and IAS Sunucu Güvenlik Grubuna üye olması gerekmektedir.

Birincil IAS sunucusu, etki alanı içerisinde yer alan hesap bilgilerine erişebilmelidir. 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 Administrator haklarına sahip bir hesapla oturum açılır.

Şekil 4. IAS'in Active Directory'ye tanıtılması

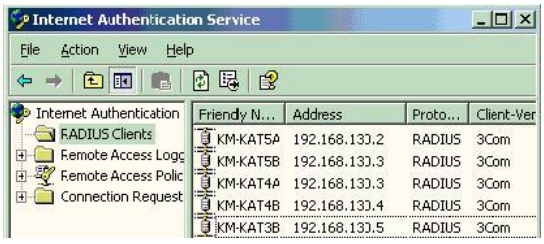
IAS diğer etki alanlarındaki kullanıcılar için kimlik doğrulama ve yetkilendirme işlemi gerçekleştiricekse, IAS'ın bulunduğu etki alanı ile kullanıcıların bulunduğu etki alanları arasında çift yönlü güven ilişkisi kurulmuş olmalıdır. IAS'ın yine kendi etki alanı dışındaki kullanıcı hesap bilgilerine erişebilmesi için ilgili etki alanı içerisindeki **RAS and IAS Servers** grubuna üye edilmesi gerekir.

3.2.b-IAS port yapılandırması

RADIUS, Authentication 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 Authentication ve Authorization (Yetkilendirme) işlemlerinin gerçekleşebilmesi için DMZ güvenli bölgelerinde 1812, 1645 ve 1813, 1646 portlarından IAS sunusuna erişim izninin verilmesi gerekir.

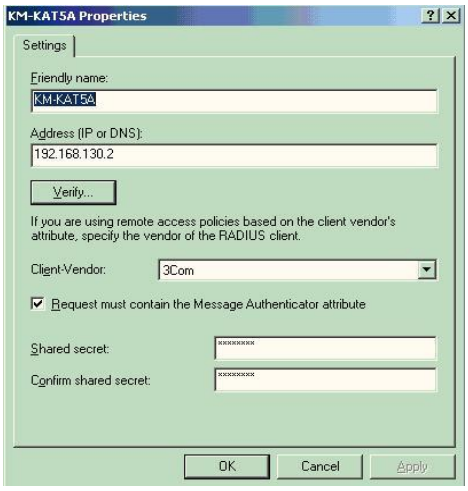
3.2.c-3COM 4400 kat switchlerinin IAS'a Radius client olarak eklenmesi



Şekil 5. RADIUS Client'lerin eklenmesi

Radius Client (istemci) ekleme işleminde her katta bulunan aktif cihazlar için ayrı ayrı client ekleme işlemi yapılır. Client IP adresi switch'in yönetim IP adresidir. Ağda yer alan kenar switchler 3COM olduğu için Client Vendor kısmında bu switchlerin 3COM olduğu seçilerek belirtilmelidir. Daha sonra kimlik doğrulama switch'i ile IAS arasında bir Shared Secret (Paylaşımlı Sözcük) belirlenir. Shared Secret birbirinden farklı büyük küçük harf ve rakamların diziliminden meydana gelmeli ve en az 22 karekterden oluşmalıdır. Her bir kimlik doğrulama switch'i için ayrı Shared Secret belirlenmesi güvenlik anlamında önemlidir. Kimlik doğrulama switch'i ile IAS

sunucusu arasında Radius trafiğinin korunması için IPSec ESP kullanmalı, mümkünse en az 3DES şifreleme yapılmalıdır.



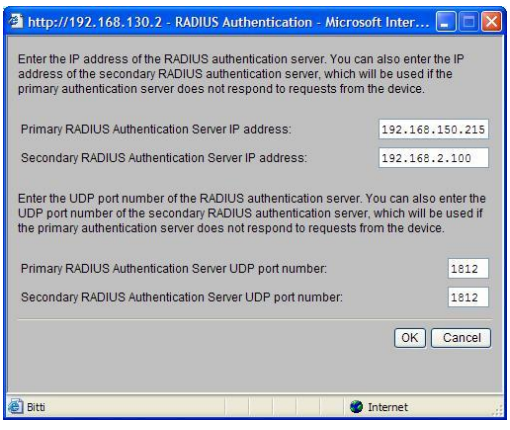
Şekil 6. Shared Secret tanımlaması

3.2.d-İkincil IAS Sunucu yapılandırması

İkincil IAS sunucusu yapılandırması birincil sunucu yapılandırması ile aynıdır.

3.3 Kenar switch olarak adlandırılan switch'lerin Kimlik Doğrulama switch'i olarak yapılandırılması

3Com 4400 switch'lerdeki güvenlik ayarları web ya da telnet üzerinden yapılandırılır. Web arayüzünde Authentication için; *Security-Radius-Authenticaiton-Modify* menulerinden Birincil ve İkincil Radius sunucularına ait IP adresleri ve Radius sunucusu port bilgileri girilir.



Şekil 7. Kenar switch'ler üzerinde Birincil ve İkincil Radius sunucuların belirlenmesi

Accounting için; *Security-Radius-Accounting-Modify* menulerinden Birincil ve İkincil Radius sunucularına ait IP adresleri ve Radius sunucusu port bilgileri girilir. IAS sunucusu ile Kimlik Doğrulama switch'i arasında belirlenen en az 22 karakterlik Shared Secret, **Security-Radius-Authenticaiton-Shared Secret** menusunden girilir.

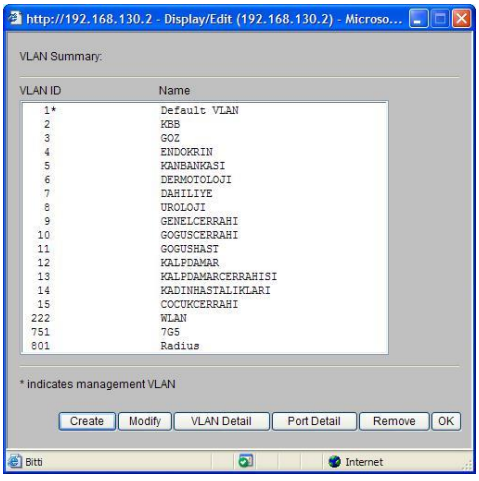
Switch üzerindeki tüm portlarda, kullanıcıların yetkilendirildiği takdirde erişebilmelerini sağlayan **Network Login** güvenlik ayarı yapılır. Kullanıcının yetkilendirilmemesi durumunda portun hala etkin olması için **Do not disable the port** seçeneği seçilmelidir. Otomatik VLAN yapılandırması kapsamında kullanıcının, uzak erişim politikasında üye olduğu VLAN'a etkin portun üye olması için **Source of port VLAN membership and QoS profile: RADIUS** seçilir.

3.4 Otomatik VLAN için omurga ve kenar switch'lerin yapılandırılması

Hastane ağı içerisinde Otomatik VLAN yapılandırması için;

Omurga Switch üzerinde; tüm VLAN'lar tanımlanır, mantıksal olarak VLAN'lar için VLAN interface'leri (arayüz) yaratılır ve mantıksal VLAN arayüzlerine IP adresi atanır. Omurga Switch üzerinde kat switchlerin bağlı olduğu tüm portların link tipi **Trunk** olarak ayarlanır. Böylelikle birden fazla VLAN o port üzerinde tanımlanabilir hale gelir. Tüm VLAN'ların ilgili interface üzerinden iletimine izin verilir.

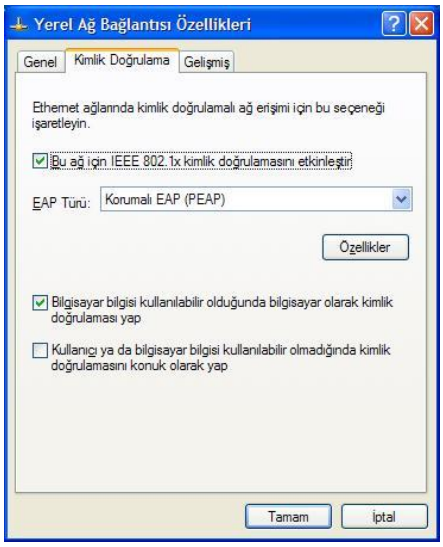
Kenar Switchler üzerinde; kullanıcıların Hastane içindeki herhangi bir odadan ağa bağlantı kurmak istemeleri göz önüne alınarak tüm kenar switch'lerde ağda tanımlı olan VLAN'lar oluşturulur. Switch üzerindeki hiçbir port bu VLAN'lara gerek *Tagged* gerekse U*ntagged* olarak üye yapılmaz. Ancak kenar switch'i omurgaya bağlayan Gigabit port, Management VLAN'a Untagged olarak üye olurken, diğer VLAN'lara Tagged olarak üye yapılmalıdır.



Şekil 8. Ağdaki tüm VLAN'ların kenar switch üzerinde tanımlanması

3.5 İş istasyonlarının PEAP MS-CHAPv2 için yapılandırılması

Ağ içinde yer alan iş istasyonlarında kullanılan işletim sistemi Windows 2000 Professional, diğer bilgisayarda Windows XP Professional'dır. Windows güncelleme servisi ile tüm bilgisayarların periyodik olarak tek bir noktadan işletim sistemi güncellemeleri gerçekleştirilmektedir. PEAP MS-CHAPv2'nin etkinleştirilebilmesi için bilgisayarlar üzerinde, Windows XP SP2, Windows XP SP1 ya da Windows 2000 SP4 olmalıdır. Şekil-10'da görüldüğü gibi ağ bağlantısı özelliğinin **Kimlik Doğrulama** sekmesinde "**Bu ağ için IEEE 802.1x kimlik doğrulamasını etkinleştir**" ve EAP türü kısmında "**Korumalı EAP (PEAP)**" seçilir ve "**Bilgisayar bilgisi kullanılabilir olduğunda bilgisayar olarak kimlik doğrulaması yap"** seçeneği aktif hale getirilir [5], [6].



Şekil 9. Kullanıcı bilgisayarlarında IEEE 802.1x kimlik doğrulama ayarları

PEAP özelliklerine ilişkin olarak "**Sunucu sertifikasını doğrula**" seçeneği etkinleştirilmeli ve "**Bu sunuculara bağlan**" kısmında Authentication sunucusunun adı verilmelidir (**radius.hastane.pau**). Kimlik doğrulama yöntemi olarak Güvenli Parola (EAP-MSCHAPv2) seçilmelidir. Varsayılan olarak PEAP MS-CHAPv2 Authentication için Windows oturum açma kimlik bilgilerini kullanır. Kullanıcıların etki alanına bağlanmaları için kullandıkları oturum açma bilgilerinin aynı zamanda Authentication 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 Authentication için kullanılmayacak ve kısa bir süre sonra kullanıcıdan Authentication bilgisini girmesi istenecektir. Bu durum kullanıcılar için yapılacak işlem sayısını arttırması ve ağa bağlantı kuracak bilgisayarların mutlaka etki altına alınması durumunu ortadan kaldıracağı için istenmeyen bir durumdur. Etki alanında olmayan bilgisayarlar da etki alanına alınarak PEAP MS-CHAPv2'nin yapılandırması Grup Politikaları ile tüm bilgisayarlara uygulanmıştır.

3.6Sertifika 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.

Hastane ağında 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. Etki alanı içinde yer alan bilgisayarların otomatik olarak bilgisayar sertifikasını kayıt ettirmesi için Grup Politikaları yazılmıştır.

3.7 Erişim kurallarının yazılması (Remote Access Policy)

Kullanıcı hesapları veritabanı olarak Active Directory kullanıldığında gerçekleşen ağ erişimlerindeki Authentication ve Authorization işlemleri, Active Directory'deki kullanıcı hesapları Dial-in özellikleri ile IAS'ta ayarlanan uzak erişim politikalarına göre yapılır.

Authentication sadece kimlik doğrulama işlemi iken, Authorization ağa bağlanmakta olan kullanıcı ya da cihazın bunu gerçekleştirmeye yetkisinin olup olmadığının denetiminin yapılması işlemidir. 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.

3.7.a Uzak Erişim Politikalarının Çalışma Şekli

Bir bağlantının yapılması durumunda bu bağlantının kabul edilip edilmeyeceğine şu şekilde karar verilir:

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: Eger yapılan bağlantı profil özelliklerine uyarsa bağlantı kabul edilir aksi durumda reddedilir.

3.7.b Politikaların Oluşturulmasında İzlenen Metod

IAS üzerinde yazılan uzak erişim politikaları yukarıdan aşağıya doğru uygulama önceliğine sahiptirler. Dolayısıyla en belirgin ya da dar bir kısmı kapsayan koşullar en üste, geneli kapsayacak kurallar daha alt kısımlara yerleştirilir. Böylelikle yukarıdan aşağı işletme önceliğine göre üstte olan kural ilk işletileceğinden, ilk önce genelin işletilerek daha sonra özele geçilmesi engellenmiş olur.

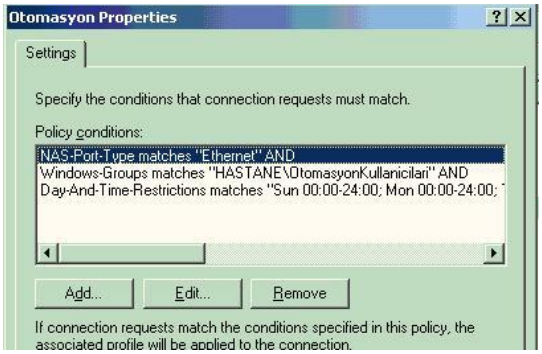
Oluşturulan kurallarda; sadece bir kullanıcı için kural oluşturmak yerine Güvenlik Grubu temeline dayalı kural oluşturup, kullanıcıları ilgili gruba üye yapma yöntemi tercih edilmiştir.

3.7.c Uzak Erişim Politikalarının Oluşturulması

IAS sunucusu üzerindeki yapılandırma işlemlerinde IAS sunucusu, kimlik doğrulama switch'inden gelen kimlik doğrulama isteğini ya kendisi gerçekleştirir (Radius Sunucusu) ya da bu isteği bir Radius Proxy gibi davranarak başka bir bilgisayara iletir. Kimlik doğrulama işleminin yerel mi yoksa uzaktan mı gerçekleştirileceği bağlantı isteği politikasında varsayılan politika üzerinde belirtilir.

Şekil 10. Uzak Erişim Politikalarının Oluşturulması

Uzak erişim kuralları oluşturulmadan önce varsayılan kurallar kaldırılmalıdır. Yeni bir uzak erişim kuralı oluşturmak için **New Remote Access Policy Wizard** seçilir. Daha sonra sırasıyla kural adı, erişim tipi (Ethernet), kuralın etkileyeceği Windows Genel Güvenlik Grubu belirlenir. **Authentication Methods** kısmında PEAP seçilir. Sihirbazın tamamlanmasından sonra ilave bileşenlerin ayarlanması için kural tekrar açılır ve yeni şartlar eklenir (**Day-And-Time-Restrictions**).



Şekil 11. Erişim Politikasına ait şartların tanımlanması

Belirtilen şartların sağlanması durumunda erişime izin verilmesi için **Grant Remote Access Permission** seçeneği seçilir. 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 [7].

- **Service-Type:** Framed
- **Tunnel-Medium-Type:** 802 (Includes all 802 media plus Ethernet canonical format)**.**
- **Tunnel-Pvt-Group-ID:** ilgili grubun üye olacağı VLAN numarası
- **Tunnel-Type:** VLAN

3.7.d Kullanıcıların üye oldukları gruba göre internet ve otomasyon grubu kullanım yetkilerinin belirlenmesi

Tüm kullanıcılar ve birimleri belirlenerek Hastane organizasyon şeması çıkartılmış, bu şema içinde hangi birimin hangi VLAN'a üye olacağı belirlenmiştir. Dinamik VLAN yapılandırması sonucu kullanıcı hesaplarının üye olduğu gruba göre belirli VLAN'lara

yerleşen kullanıcılar, Omurga switch üzerinde yazılan Access List'ler (Erişim Listeleri) ile ya otomasyon, ya internet ya da her ikisini kullanabilir duruma gelmiştir.

Access-List örneği:

acl name database advanced
rule 1 permit tcp source-port eq 1521
rule 2 permit tcp source-port eq 1433
rule 3 permit tcp source-port eq 4899 destination 192.168.150.0 0.0.0.255
rule 4 permit tcp source-port eq telnet
rule 5 permit tcp destination-port eq telnet
rule 6 deny tcp
rule 7 deny udp

Kenar switch'ler üzerinde QoS desteği olmasından dolayı bir takım trafik yetkilendirme işlemi kenar switch'lerde yapılabilecek olmasına rağmen bu işlemin kenar switch'ler üzerinde yapılması tercih edilmemiştir. Kenar switch'ler üzerinde kullanıcıların hangi VLAN'a bağlanacağı sabit olmadığından herhangi bir QoS'in uygulandığı porttan, portu kullanan bütün kullanıcıların etkilenmesi uygulamanın "*merkezden gruba göre değişken yapı*" felsefesine ters düşecektir.

4.SONUÇ

Yapılan bu çalışmada, Üniversite Hastanesinde karşılaşılan problemlerin çözümünde Otomatik VLAN yapılandırması ve ağa erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmesiyle aşağıda maddeler halinde sunulan sonuçlar elde edilmiştir:

- Hasta ve yakınlarının internete erişememelerine karşın Hastane içinde tüm aktif cihazlar üzerinde kimlik doğrulaması etkin hale getirildiğinden internete erişmek isteyen yatan hastalar için, hastanın yatış işlemlerinin yapıldığı sırada kullanıcı hesabı ve şifresi tanımlanıp, hastanın çıkışı sırasında ilgili hesabın iptal edilmesi yöntemine gidilmiştir. Dolayısıyla hastalar için oluşturulan VLAN, yazılan erişim listeleri ile sadece internete erişebilir hale getirilmiştir.

- Hastaneleri çok yoğun bir şekilde ziyaret eden ilaç firması temsilcilerinin kablosuz ağ üzerinden internete eriştirilmesi, tüm kablosuz ağ cihazlarının aynı VLAN içerisine alınması ve yazılan erişim listeleri ile sadece internete erişebilir hale getirilmesi gerekir.

- Forest root domaini (Birincil Domain) içinde en az iki tane etki alanı denetleyicisi IAS sunucusu olarak tasarlanmalıdır. Birincil IAS üzerinde herhangi bir sorun olması durumunda İkincil 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.

- IAS sunucuları her domainde Birincil ve İkincil olmak üzere yine iki adet tasarlanmalıdır. Eğer bunun için yeterli maddi kaynak yoksa var olan etki alanı denetleyicilerinden biri o etki alanı için Birincil IAS olarak belirlenirken, İkincil IAS olarak Forest root etki alanındaki IAS sunucusu belirlenmelidir.

- Etki alanı denetleyicileri üzerindeki *netlogon.log* dosyasının boyutu (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\LogFileMaxSize) arttırılmalıdır. Aksi takdirde kimlik doğrulama sırasında sorunlar yaşanabilir.

- Uygulamaya geçmeden önce tüm Hastanedeki 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 zamanları göz önüne alınmalıdır.

- Kimlik doğrulama uygulamasına geçilmeden önce elektronik ya da yazılı olarak kullanıcıların çok iyi bir şekilde bilinçlendirilmesi gerekir.

- Uygulama ile ilgili olarak kullanıcıları bilgilendirecek yardım kitapları basılmalıdır.

- Uygulamaya geçmeden önce bütün kullanıcılar gruplar halinde eğitime alınmalıdır.

- Uygulamaya geçmeden önce belirli noktalarda belirli kullanıcılar tarafından sistemin test edilmesi gerekir.

- Uygulamaya aynı anda Hastanenin tamamında değil, kat kat ya da parça parça geçilmelidir.

- Destek anlamında tüm Bilgi İşlem personelinin çok iyi bir şekilde bilinçlendirilmesi, oluşan sorunların kısa sürede çözümü için gereklidir.

Sonuç olarak yapılan bu çalışmada, karşılaşılan problemlerin çözümüne yönelik olarak Otomatik VLAN yapılandırması ve hastane ağına erişim yapacak tüm kullanıcıların kimlik doğrulama işlemlerinin gerçekleştirilmesi yöntemine gidilmiştir.

Uygulama sonucu olarak risk oranı yüksek veriler, gerek internet ortamında gerekse kampüs içinde herhangi bir güvenlik duvarı ile sadece bu ortamlardan

gelebilecek saldırılara karşı korunurken, LAN'da gerçek kullanıcıların bulunduğu ortamda yetkili ya da yetkisiz tüm kullanıcılar tarafından aynı erişim hakları ile erişilmektedir. Risk oranı yüksek verilere LAN içerisinde sadece yetkili kurum çalışanlarının erişmesiyle yani ağa erişen kullanıcıların kimlik doğrulamasının yapılmasıyla sadece yetkili kullanıcıların kendilerine tanınan erişim hakları ile risk oranı yüksek verilere erişmeleri sağlanmıştır.

Ayrıca uygulamada kullanılan Otomatik VLAN yapılandırmaları sayesinde de sürekli gelişen ağlarda yönetimin kolaylaştırılması ve ağ kaynakları yönetiminin merkezileştirilmesi sağlanmıştır.

KAYNAKLAR

[1] Çetin, M. ve Aydos, M., "Otomatik VLAN Yapılandırmalarında IEEE 802.1x Standardı Kullanımının Sistem Performansına Etkisi", İletişim Teknolojileri Ulusal Sempozyumu, 17-19 Kasım 2005, Adana

[2] Deploying Windows Server 2003 Internet Authentication Service IAS with Virtual Local Area Networks (VLANs), Microsoft Corporation, June 2004

[3] Deployment of IEEE 802.1x for Wired Networks using Microsoft Windows, Microsoft Corporation, October 2003

[4] http://www.microsoft.com/windowsserver2003/technologies/ias/default.mspx

[5] http://www.microsoft.com/technet/community/columns/cableguy/cg0402.mspx

[6] http://www.microsoft.com/technet/community/columns/cableguy/cg0702.mspx

[7] http://www.microsoft.com/whdc/device/network/802x/AccessPts.mspx