TMMOB ELEKTRİK MÜHENDİSLERİ ODASI ADANA ŞUBESİ

SEMPOZYUM

İTUSEM 2005

İLETİŞİM TEKNOLOJİLERİ ULUSAL SEMPOZYUMU

- YAYINCILIK
- UYGULAMALAR VE SERVİSLER
- İLETİŞİM KURAMI VE TEKNİKLERİ
- İLETİŞİM ALTYAPISI

17-19 KASIM 2005

ÇUKUROVA ÜNİVERSİTESİ
BALCALI KAMPÜSÜ

TÜBİTAK

EMO
ELEKTRİK MÜHENDİSLERİ ODASI
ADANA ŞUBESİ

ÇUKUROVA ÜNİVERSİTESİ
1973

FİLTRE UYGULAMALARI İÇİN DEĞİŞTİRİLMİŞ TOPRAK DÜZLEMLİ YAVAŞ DALGA CPW REZONATÖR
Özlem AKGÜN, Adnan GÖRÜR..... 145 – 149

FREKANS SEÇİCİ KANALLAR İÇİN SOFT-GİRİŞ/SOFT-ÇIKIŞ (SISO) YAPILI BİR TURBO DENKLEŞTİRİCİ
Salim KAHVECİ, İsmail KAYA..... 151 – 153

GEZGİN İLETİŞİM TEKNOLOJİLERİNDE ALAN PROGRAMLANABİLİR KAPI DİZİLERİNİN KULLANILMASI
Özgür TAMER, Ahmet ÖZKURT..... 155 – 158

HARİCİ BÜKME UYGULANAN SİNÜSOİDAL SPİNLİ FİBERLERDE POLARİZASYON MOD DİSPERSİYONU DEĞİŞİMİ
Sait Eser KARLIK, Güneş YILMAZ..... 159 – 163

İLİNTİLİ, ÇOKLU GİRİŞİMCİLİ VE GÜRÜLTÜLÜ ORTAMLARDA, EN İYİ BİRLEŞTİRME SİSTEMLERİNİN KARMAŞIK WİSHART MATRİSLERİ İLE BAŞARIM ANALİZİ
Aysel ŞAFAK, Baran USLU, Sertaç BAHADIR..... 165 – 170

KONVOLUSYONEL ÇARPIM KODLARININ PERFORMANS ANALİZİ
Orhan GAZİ, A. Özgür YILMAZ..... 171 – 176

KURUMSAL BİR AĞDA TRAFİK YOĞUNLUĞU VE CEVAP SÜRESİ OPTİMİZASYON UYGULAMASI
İbrahim ÖZÇELİK, Barış ÇALIŞKAN..... 177 – 180

OFDM SİSTEMLERİNDE ARAKİPLENİM BOZULMALARININ İLERİ BESLEMELİ DOĞRUSALLAŞTIRMA METODU İLE AZALTILMASI
Cebrail ÇİFTLİKLİ, A. Çağrı YAPICI, A. Tuncay ÖZŞAHİN..... 181 – 184

OPTİK ÇOĞUŞMA ANAHTARLAMA ÜZERİNDE JIT İŞARETLEME PROTOKOLÜ
Pınar KIRCI, A. Halim ZAİM..... 185 – 190

OPTİK FİBER İNTERFEROMETRİK SENSÖRLE BASINÇ VE SICAKLIK ÖLÇÜMÜNÜN ANALİZİ
N. Özlem ÜNVERDİ, Öznur TÜRKMEN..... 191 – 194

OPTİK HABERLEŞME SİSTEMLERİNDE GÜVENİLİRLİK ANALİZİ
N. Özlem ÜNVERDİ, N. Aydın ÜNVERDİ..... 195 – 199

OPTİK HABERLEŞME SİSTEMLERİNDE KUPLÖR YARDIMIYLA KAYIP ANALİZİ
N. Özlem ÜNVERDİ, N. Aydın ÜNVERDİ..... 201 – 203

ORTOGONAL FREKANS BÖLMELİ ÇOĞULLAMA SİSTEMLERİNDE TEPE GÜCÜ/ORTALAMA GÜÇ ORANININ DÜŞÜRÜLMESİNİN BİLGİSAYAR SİMÜLASYONLARIYLA İNCELENMESİ
E. Seza ÖRTLEK, Necmi TAŞPINAR..... 205 – 210

OTOMATİK VLAN YAPILANDIRMALARINDA IEEE 802.1x STANDARDI KULLANIMININ SİSTEM PERFORMANSINA ETKİSİ
Meriç ÇETİN, Murat AYDOS..... 211 – 214

OTOMATİK VLAN YAPILANDIRMALARINDA IEEE 802.1x STANDARDI KULLANIMININ SİSTEM PERFORMANSINA ETKİSİ

Meriç ÇETİN[1] **Murat AYDOS[2]**

Bilgisayar Mühendisliği Bölümü, Pamukkale Üniversitesi, Kampüs / DENİZLİ

[1]e-posta: mcetin@pamukkale.edu.tr, [2]e-posta: maydos@pamukkale.edu.tr

Tel: 0 258 213 40 30 / Faks: 0 258 212 55 38

Anahtar sözcükler:IEEE 802.1x Standardı, Otomatik VLAN, RADIUS, Kimlik Doğrulama (Authentication).

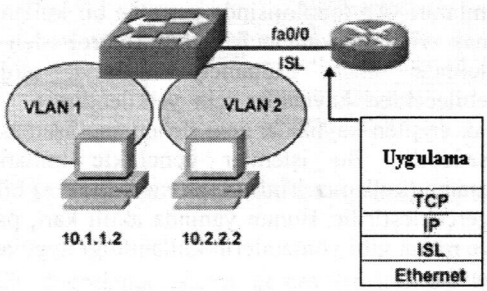
ABSTRACT

In this work, using IEEE 802.1x Standard both wired Ethernet and wireless IEEE 802.11 networks have been accessed by means of authenticated methods and by giving permissions to a server automated VLANs have been created. The effects of creating automated VLANs by this method on the system have been analyzed. When a user wants to access, the server, the server grants access permission in the case of successful authentication. When the encrypted user information matches the user information kept in the database of RADIUS server, authorization and access tasks are accomplished. By this method, keeping the users with no access permission out of the network, the unnecessary traffic behind the server is avoided and general system performance is improved. In addition, data traffic can be controlled according to the rules defined in Access Lists, which determines the IP addresses that can be accessed to the network.

1. SANAL YEREL AĞLAR-(VLAN)

Günümüzde önemli ağ yapılandırma tekniklerinden birisi olarak kabul edilen **V**irtual **L**ocal **A**rea **N**etwork-VLAN (Sanal Yerel Ağlar), bir switch (anahtar) üzerindeki portların gruplandırılmasıyla oluşturulan ağlardır. Fiziksel olarak tek bir ağ gibi görünmesine karşın VLAN uygulaması ile sanal olarak ayrı ağlar yaratılır ve bu VLAN'lar fiziksel olarak ayrı ağların birçok özelliklerini taşırlar. VLAN'lar genellikle kaynakların ve kullanıcıların yerleşimine, işlevine, departmanına, ya da kullanılan uygulama protokolüne göre düzenlenir.

VLAN'lar sayesinde alt ağlar ya da broadcast (yayın) domainleri (etki alanı) yaratılır. Bu sayede broadcast'lar yalnızca bir VLAN içinde gönderilmiş olur. Her VLAN, aynı bir yönlendirici 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. VLAN oluşturarak, sisteme performans ve güvenlik açısından avantajlar sağlansa da, bu, kriterleri oluşturulan VLAN'ların farklı VLAN'larla iletişim kurmasında sıkıntılar yaratmaktadır. Sıkıntıların giderilmesinde üçüncü katmanda çalışan yönlendiricilere (router) ihtiyaç duyulur. Bu durumda Şekil–1'de gösterildiği gibi farklı VLAN'lar yönlendirici üzerinden görüşebilir duruma gelir [1]. 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.



Şekil–1. Katman 3 Düzeyinde Farklı VLAN' ların Birbiri İle İletişimi

Oluşturulan bir VLAN'ın statik ya da dinamik olarak switch portlarına atanması gerekir. Bir statik VLAN oluşturulurken ağ yöneticisi switch'in belirli portlarını VLAN'a dahil eder. 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 üyeliği gerçekleştirilir. 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.

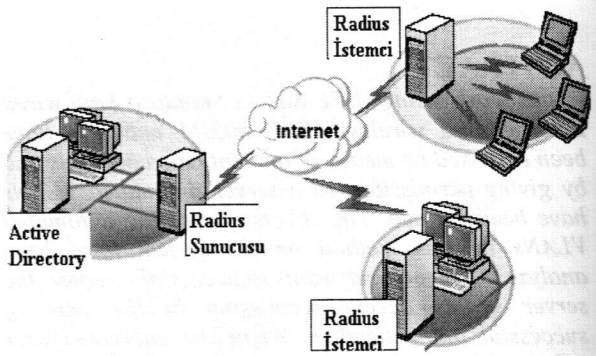
Sanal yerel ağların kullanılmasının önemi; belli işleri yapmak üzere kurumsal bir ağ üzerinde farklılaştırılarak ayrılmış yerel ağların dinamik yapılarındaki değişimlerden etkilenmemeleridir. VLAN'lar fiziksel yapıdan bağımsız olduğu için, ağ üzerindeki sunucuların başka bir noktaya taşınması veya yenilerinin eklenmesi işlemi kolaylaşmış olur. Böylece sistemdeki iş yükü azalır, maliyet düşer ve isteklere verilen yanıt süresi kısalır.

2. AAA & RADIUS İLE AĞ GÜVENLİĞİ

Ağ güvenliği; Kimlik Doğrulama (Authentication), Yetkilendirme (Authorization) ve Denetleme (Accounting) yani AAA olmak üzere üç aşamada gerçekleştirilir. 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 bahsedebilir. Bu işlemler genellikle kullanıcının username (kullanıcı ismi) ve password (şifre) bilgileri ile gerçekleştirilir. Bunun yanında akıllı kart, parmak izi ve retina gibi yöntemlerin kullanıldığı uygulamalar da vardır.

Kimlik doğrulama; sunucuda depolanan username/password çiftlerinin bir listesine karşı kullanıcı tarafından sunucuya sağlanan username/password çiftini karşılaştırma işlemini gerçekleştirir. Yetkilendirme; bir username/password çiftine özgü verilen özel izinler listesini sağlar. 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 sınanır. 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. Denetleme ise kullanıcı oturumlarının süresi, türü ve numarası gibi bilgileri günlük olarak tutar.

Sistem güvenliğinin temeli; kullanıcıların kimliklerinin doğru belirlenmesi ve yetkilendirmesi 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 (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) sunucunda, kullanıcı kimlikleri belirlenir. Bu durum Şekil–2'de gösterilmiştir [2,3,4].



Şekil–2. Ağ İçerisine RADIUS Sunucu ve Kullanıcılarının Yerleştirilmesi.

Kimlik doğrulama işlemi esnasında kullanıcıların kişisel bilgileri, kimlik doğrulama işlemini yapacak RADIUS sunucusu üzerindeki veri tabanında saklanır. Bu işlem kullanıcıların kimlik bilgilerinin doğrulundan 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.

Ağ içerisinde ve dışında yer alan kullanıcılara kritik sistem verilerine erişim hakkının verilmesi, iş akışını hızlandırmak, daha iyi servis vermek gibi avantajlara sahip olmakla birlikte, güvenlik açısından dikkat edilmesi gereken bir açık kapı olabilir. 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 [5,6,7]. Bu da otomatik VLAN kavramını doğurur.

3.IEEE802.1x KİMLİK DOĞRULAMASI

Hem kablolu hem de kablosuz ağları kapsayan IEEE 802 standartlarından IEEE 802.11 standartı, çoğunlukla kablosuz yerel ağları oluşturan cihazların kullanıma uygun olarak tasarlanmıştır. IEEE 802.11 standartlarına göre oluşturulan cihazlar farklı üreticiler tarafından yapılmış olsalar da birbirleri ile uyumlu bir şekilde haberleşebilirler ve rahatlıkla kablosuz yerel alan ağ oluşturabilirler.

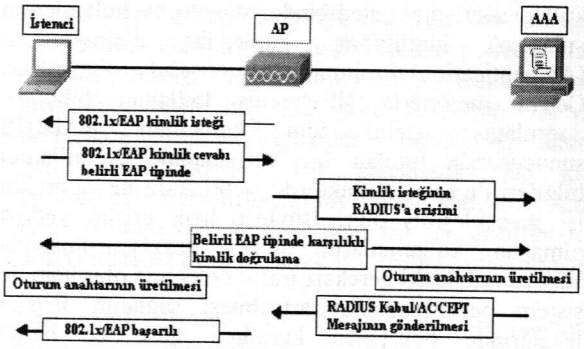
IEEE 802.11 çalışma grubu tarafından geliştirilen yeni bir protokol olan IEEE 802.11i protokolü kimlik doğrulama, şifreleme, yetkilendirme ve anahtar (key) yönetimi işlemlerini gerçekleştirebilmektedir. İki katmandan oluşan IEEE 802.11i'nin alt katmanında gelişmiş kriptolama algoritmaları, üst katmanında ise kimlik doğrulama ve anahtar dağıtımı için gerekli 802.1x bulunmaktadır. Kullanıcılar ağ kaynaklarına erişmeden önce kimlikleri doğrulanmakta, bu işlemden sonra üretilen oturum anahtarları dağıtılmakta ve bu anahtarlar kullanılarak üretilecek yeni anahtarlar ile güvenli veri transferi yapılmaktadır [8,9].

IEEE 802.11i standartı, karşılıklı kimlik doğrulama için 802.1x EAP (**E**xtensible **A**uthentication **P**rotocol) tabanlı kimlik doğrulamayı uygulamaktadır. EAP, çoklu kimlik doğrulama metotlarını destekleyen bir kimlik doğrulama ortamıdır. Tipik olarak, IP gereksinimi olmaksızın Point-to-Point Protocol (PPP) veya IEEE 802 gibi veri hattı katmanlarını doğrudan gözden geçirir[10]. 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; kullanıcı (supplicant), kimlik doğrulama sunucusu (authentication server) ve kimlik doğrulayıcı (authenticator) olmak üzere 3 kısımdan oluşmaktadır.

Kullanıcı; kimlik doğrulama isteğinde bulunur. Kimlik doğrulayıcıya username/password bilgisini sağlar. Kullanıcı kimlik doğrulayıcı ile iletişim için EAP'yi kullanır. Kimlik doğrulama sunucusu; RADIUS gibi kimlik doğrulama işlemini gerçekleştiren bir sunucudur ve genellikle RADIUS'tur. Kullanıcıdan gelen username/password bilgisini doğrular ve erişime yetkisi olup olmadığını belirler. Kimlik doğrulayıcı; kullanıcı ile kimlik doğrulama sunucusu arasında yer alan, 802.1x port güvenliğini sağlayan ve ağa erişimi kontrol eden bir erişim noktasıdır (Access Point-AP). Kullanıcıdan username/password bilgisini alır, RADIUS'a geçirir ve gerekli tıkamayı gerçekleştirir ya da RADIUS'tan gelen sonuçlara dayalı eyleme izin verir.

IEEE 802.1x standardı ile kimlik doğrulama işlemi Şekil–3'de gösterilen adımlardan oluşmaktadır.

- Kullanıcı, kimlik doğrulayıcıya bağlantı isteğinde bulunur. Kimlik doğrulayıcı, bağlantı isteğini alınca, tüm portları kapalı tutar ama kullanıcı ile arasında bir port açar.
- Kimlik doğrulayıcı, kullanıcıdan kimliğini (username/password) ister.
- Kullanıcı kimliğini gönderir. Kimlik doğrulayıcı kimlik bilgisini bir RADIUS sunucuna gönderir.
- RADIUS sunucusu, veritabanında tuttuğu bilgilerle kimliği eşleştirerek kullanıcının kimliğini doğrular. Kimlik doğrulama işlemi gerçekleştiğinde, *Kabul(ACCEPT)* mesajını kimlik doğrulayıcıya gönderir. Kimlik doğrulayıcı, kullanıcının portunu yetkilendirilmiş port durumuna getirir.
- Kullanıcı, RADIUS sunucusundan, sunucunun kimliğini ister. RADIUS sunucusu kimlik bilgisini kullanıcıya gönderir.
- Kullanıcı RADIUS sunucusunun kimliğini doğruladığında veri trafiğine başlanır.



Şekil–3. IEEE 802.1x ile Kimlik Doğrulama İşlemi.

Kimlik doğrulama işlemi gerçekleştirildikten sonra üretilen oturum anahtarları ile veri transferi başlamaktadır. IEEE 802.1x protokolü tüm bu işlemlerin yanında anahtar yönetimi işlemini de gerçekleştirmektedir.

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 (**I**nternet **A**uthentication **S**ervice) 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.

4. SONUÇ

Bir switch üzerindeki portların gruplandırılmasıyla oluşturulan VLAN'ların; belli işleri yapmak üzere kurumsal bir ağ üzerinde farklılaştırılarak ayrılmış yerel ağların dinamik yapılarındaki değişimlerden etkilenmeme özellikleri, onların ağ üzerinde kullanılmasının önemini göstermektedir. VLAN'lar fiziksel yapıdan bağımsız olduğu için, ağ üzerindeki sunucuların veya kullanıcıların başka bir noktaya taşınması veya yenilerinin eklenmesi işlemi kolaylaşmış olur. Böylece sistemdeki iş yükü azalır, maliyet düşer ve isteklere verilen yanıt süresi kısalır.

Bu çalışmada; IEEE 802.1x standardı kullanılarak, hem kablolu Ethernet hem de kablosuz IEEE 802.11 ağlarına kimlik doğrulamalı erişim sağlanmasıyla, bir sunucuya izin atanarak sistem üzerinde otomatik VLAN'lar oluşturmanın sistem performansına etkisi araştırılmıştır. Bu özelliklere sahip bir VLAN'a bir kullanıcı erişmek istediğinde, sunucu bu kullanıcının yalnızca kimliğinin başarıyla doğrulanması (Authentication) durumunda ağa erişebilmesini sağlar. Çeşitli metotlarla şifrelenmiş kullanıcı bilgileri, doğrulama işlemi için kullanılan RADIUS sunucusunda tutulan bir veritabanındaki kullanıcı bilgileri ile eşleştiği takdirde, yetkilendirme ve erişim işi gerçekleşmiş olur. Böylece hem erişim yetkisi olmayan kullanıcıların ağdan uzaklaştırılmasıyla sunucu ardındaki gereksiz trafik önlenmiş olur hem de sistem performansının artırılması sağlanır. Erişim listelerinde belirlenen kurallara göre de hangi adreslerin ağa erişeceği belirlenerek veri trafiği denetim altına alınmış olur.

5. KAYNAKLAR

[1] http://www.sistemuzmani.com/Makaleler/

[2] Remote Authentication Dial in User Service (RADIUS), IETF RFC 2865.

[3] Remote Authentication Dial in User Service Accounting, IETF RFC 2866.

[4] Microsoft Training and Certification Modul 10:RADIUS as a Solution for Remote Access.

[5] Bilişim Güvenliği, Pro-G ve Oracle, Seminer Notu

[6] www.oracle.com.tr

[7] www.pro-g.com.tr

[8] Mishra and W. Arbaughm, "*An Initial Security Analysis of the IEEE 802.1X Standard*", Technical Report CS-TR–4328, Department of Computer Science, University of Maryland, Feb. 2002.

[9] Bernard Aboba, Tim Moore, et.al., IEEE 802.1x For Wireless LANs, IEEE Plenary, März 2000, 25 September 2002.

[10] Extensible Authentication Protocol (EAP), IETF RFC 3748