T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ AĞ STANDARTLARININ KARŞILAŞTIRILMASI VE 802.1x STANDARDI İLE BİR ÜNİVERSİTEDE KABLOSUZ AĞ GÜVENLİĞİ TASARIMI

YÜKSEK LİSANS TEZİ

Mehmet KÖSEM

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Mart, 2016

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ AĞ STANDARTLARININ KARŞILAŞTIRILMASI VE 802.1x STANDARDI İLE BİR ÜNİVERSİTEDE KABLOSUZ AĞ GÜVENLİĞİ TASARIMI

YÜKSEK LİSANS TEZİ

Mehmet KÖSEM
(Y1113.010013)

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ali GÜNEŞ

Mart, 2016

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1113.010013** numaralı öğrencisi **Mehmet KÖSEM**'ın **"KABLOSUZ AĞ STANDARTLARININ KARŞILAŞTIRILMASI VE 802.1 x STANDARDI İLE BİR ÜNİVERSİTEDE KABLOSUZ AĞ GÜVENLİĞİ TASARIMI"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 09.03.2016 tarih ve 2016/07 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul edilmiştir.

Öğretim Üyesi Adı Soyadı **İmzası**

Tez Savunma Tarihi :24.03.2016

1)Tez Danışmanı: Prof. Dr. Ali GÜNEŞ .....

2) Jüri Üyesi : Yrd. Doç. Dr. Evrim KORKMAZ ÖZAY .....

3) Jüri Üyesi : Yrd. Doç. Dr. Ferdi SÖNMEZ .....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "Kablosuz Ağ standartlarının Karşılaştırılması ve 802.1x standardı ile Bir üniversite Kablosuz Ağ güvenliği Tasarımı" adlı çalışmanın tezin projesi safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya 'da gösterilenlerde oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (…/…/2016)

Mehmet KÖSEM

İmza

ÖNSÖZ

İlk olarak tez çalışmamın hazırlanmasında her türlü yardımı esirgemeyen ayrıca değerli görüş ve yorumları, rehberliği ve desteği için değerli danışman hocam sayın Prof. Dr Ali GÜNEŞ'e Teşekkür ederim. Bu tez çalışma süresi boyunca sabrı, anlayışı ve desteği ile bana yardımcı olan eşim ve çocuğuma sonsuz Teşekkür ederim.

Mart 2016 **Mehmet KÖSEM**

İÇİNDEKİLER

SAYFA

KISALTMALAR

AAA	Kimlik doğrulama, yetkilendirme, loglama
ADCS	Dizin Hizmeti Sertifika hizmeti
AD	Dizin hizmeti
Ap	Erişim noktası
EAP	Genişletilmiş Kimlik doğrulama Protokolü
İp	İnternet protokol adresi
Ldap	Hafif dizin erişim protokolü
MSCHAP2	Microsoft Karşılıklı kimlik doğrulama protokolü
Mac	Ortam erişim denetimi
Nps	Ağ ilkesi sunucusu
SSL	Güvenli soket katmanı
Ssıd	Servis seti Tanımlayıcısı
Vlan	Sanal yerel ağ
Web	Kabloluya eş değer Gizlilik
WPA	Wi_Fi Korumalı Erişim
Wlan	Kablosuz Yerel Alan ağı

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

KABLOSUZ AĞ STANDARTLARININ KARŞILAŞTIRILMASI VE 802.1x STANDARDI İLE BİR ÜNİVERSİTEDE KABLOSUZ AĞ GÜVENLİĞİ TASARIMI

ÖZET

Teknolojini günden güne gelişimi ile birlikte teknolojinin kullanımının basite indirgenmesi ve özellikle kullanıcıların taşınabilir cihazları tercih etmesi kablosuz ağlara olan ilgiyi arttırmıştır. Kablosuz cihazların kullanımının artmasıyla beraber bilgi paylaşımı, sistemlerin kullanımı ve birçok farklı uygulama kablosuz ağ üzerinden devreye alınmaya başlamıştır. Fakat kablosuz ağlar havada yayın yapan cihazların ve bu yayını alan cihazların birbiri arasındaki iletişimin gerçekleşmesi ile kullanılan sistemlerdir, bu veri alışverişi esnasından bu yayını takip eden birçok kişi olabilmekte veya bu yayının içerisine dâhil olmuş fakat yetki seviyesi farklı olan kullanıcılarda ağın içerisindeki verilere ulaşabilmektedir. Bu gibi durumlar birçok ağ sisteminde güvenlik açıklarına neden olabilmektedir. Tez çalışması içerisinde kablosuz ağ güvenlik yöntemleri incelenmiş ve güvenlik açıklarından bahsedilmiştir. Kablosuz ağ güvenliği yöntemlerinden kullanımı önerilen özellikle 802.1x standardı üzerinde durulmuştur. Üniversitelerde kablosuz ağ güvenliği ve kullanıcı kimliği tesbiti ve daha güvenilir bir sisteme oluşturabilmek için 802.1x standardı ve sanal ağ mimarisini birlikte kullanımı için tasarılar oluşturulmuştur. Bu tasarıların uygulana bilmesi için çeşitli materyaller kullanılmış ve testlere tabi tutulmuştur. Bu Tez çalışmasında birinci bölümde bilgisayar ağları, ağ protokolleri kablosuz ağ standartlarının gelişim süreçleri hakkında literatürden bilgiler verilmiştir.

İkinci bölümde kablosuz ağlarda güvenliği yöntemlerinden wi-fi korumalı erişim, kabloluya eşdeğer gizlilik, Mac adresi kimlik denetimi, Ssıd yayınını devre dışı bırakma,802.1x standardı gibi kimlik tanıma yöntemleri incelenmiş ve özellikle 802.1x standardı üzerine durulmuştur.

Üçüncü bölümde 802.1x standardının üniversitede kablosuz ağ güvenlik seviyesini arttırılabilmesi için analizler yapılmış analizler neticesinde standardın daha güvenilir bir yapıda kullanımı için sanal ağ mimarisi ile birlikte kullanımı önerilmiş ve bu analizler sonucu tasarılarımlar oluşturulmuş, bu tasarılar için uygun materyaller kurulmuş ve yapılandırılmıştır. Bu tez çalışmada 802.1x standardı EAP kimlik kanıtlama yöntemleri incelenmiş ve bu yöntemlerden Korumalı EAP PEAP ve EAPMSCHAPV2 birlikte kullanılmıştır.

Son bölümde ise 802.1x standardı üniversite kullanımı için çeşitli testler yapılmış ve bu testlerin sonuçlarına yer verilmiştir. Kullanıcıların tanımlamış oldukları kullanıcı adı ve şifresi ile farklı işletim sistemleri ile 802.1x standardıyla kimliği doğrulandıktan sonra sisteme tanımlandığı sanal ağ ile erişim sağlayabilmesi test edilmiştir.

Anahtar Kelimeler: Kablosuz ağ standartları,IEEE802.1x Standardı, Kablosuz ağ Güvenliği, Kimlik kanıtlama yöntemi,

COMPARING WIRELESS LAN STANDARDS AND MODEL PROPOSAL FOR UNIVERSITY WIRELESS NETWORK SECURITY WITH 802.1X

ABSTRACT

The simplification of the use of technology along with the development of technology day by day and especially to users prefer portable devices has increased the interest in wireless networks. information sharing with the increased use of wireless devices, the use of many different applications and systems began to be commissioned over the wireless network. But wireless networks air broadcasting devices and these publications are in the systems used by the realization of communication between each of the devices, during the exchange of data to be many people who follow this post or this publication has been included into the but authorization levels is available to the data within the network, the user is different. Such situations may result in security vulnerabilities in many networks. Wireless network security methods examined in this thesis are discussed and vulnerability. Recommended the use of wireless network security method is especially focused on the 802.1x standard. University wireless network security and user identity identification and design have been created in order to create a more reliable system for use with the 802.1x standard and virtual network architecture. This project used a variety of materials to know to implement and has been subjected to the tests. This thesis computer networks in the first part of the study, network protocols from the literature are given information about the development process of the wireless networking standard.The second part of security methods in wireless networks wi-fi protected access, wired equivalent privacy, MAC address authentication, disable SSID broadcast, examined identification methods such as 802.1x standard and particularly focused on the 802.1x standard.

The third chapter in the 802.1x standard of the university wireless network security level of a more reliable standard analyzes conducted analysis result to increased structure for use with virtual network architecture for use have been proposed and analyzed the results of tasarılarım have been created, set the appropriate materials for this bill is structured. This thesis study examined the 802.1x standard and Protected EAP authentication methods PEAP and EAP EAPMSCHAPV2 of these methods are used together.In the last chapter 802.1x standard for the use of university made several tests and the results of these tests are given. It provides access to virtual network defined by the system after users identify where they have a user name and password with different operating systems with standard 802.1x authenticated by tested

Key Words: Wi-Fi standarts;IEEE 802.1X Standard,Wi-Fi securit

1. GİRİŞ

Kablosuz ağ teknolojilerin kullanım oranları gelişen teknoloji ile sürekli artmaktadır. Kablosuz ağ sistemlerinin kullanımının önemli bir çoğunluğu taşınabilirliktir. Bugün kullanılan donanım cihazları diz üstü bilgisayar, tablet, akıllı telefonlar gibi cihazlar üzerinden kablosuz ağ sistemlerinde büyük bir ağ trafiği ve bilgi paylaşımı gözlemlenmektedir. Paylaşılan bilgi kablosuz ağ sistemlerinde havadaki yayını kullanarak yapılabilmektedir. Bu durum ciddi güvenlik ve bilgilere ikinci kişiler tarafından erişeme açık haline gelmektedir.

Üniversiteler Kablosuz ağ sistemini kullanan kullanıcı sayısı ve yazılımlar itibari ile kablosuz ağ sistemlerinde önemli bir yer almaktadır. Kullanıcı sayıları ortalama 5000 ile 80000 arası değişen kurumlar bulunmaktadır. Bu nedenle sistemlere bağlanan kullanıcıların kimlik tespiti yapılması ve yasal zorunlulukların yerine getirilmesi gerekmekmektedir. Daha önemlisi kullanıcıların ve üniversitenin bilgi güvenliğinin korunması gerekmektedir. Bu sebepten kablosuz ağ sistemlerinde kullanılan kimlik tespit yöntemleri incelenmiş ve üniversitelerin veya büyük kurumlar için 802.1x standardı ile kimlik tespit yöntemi üzerinde durulmuş, tasarılar oluşturulmuş ve güvenlik sisteminin arttırımı için donanım ve yazılım materyallerini kurulum ve yapılandırılma yöntemi önerilmiştir. Standardın uygulanabilmesi için test ortamları oluşturulmuş ve testlere tabi tutulmuş raporlara tezde yer verilmiştir. İşlemlerinin yapılabilmesi için ağ üzerinde kullanılan standartlar, protoklolleri ve ağla ilgili çeşitli litaretürden bilgiler ile tez çalışmasına başlanmıştır.

2. BİLGİSAYAR AĞLARI VE PROTOKELLERİ NELERDİR

2.1 Bilgisayar ağları

Birden fazla bilgisayarın Ethernet kartları aracılığı ile bilgisayarların haberleşmesi ile oluşan yapıya ağ denir. Ağ(network) sitemine bağlı tüm cihazlar(bilgisayar, tablet, akıllı telefonlar vb) kendi aralarında haberleşebilmekte ve kaynakları(belge, klasör, fotokopi cihazı gibi) ortak kullanabilmektedirler. Bir bilgisayarın ağ sistemine erişim sağlayabilmesi için ağ türleri içerisindeki yapılardan herhangi birinde olması gerekmektedir. Ağ türleri üç başlık altında incelenir.

Yerel alan ağı (LAN)

Geniş alan ağı (WAN)

Şehirsel bilgisayar ağı (MAN)

Yerel alan ağı (Lan)

Ofis, bina, yerleşke gibi fiziksel bölge itibari ile sınırlı alanlar içinde kullanılan ağ modelidir. Fiziksel yerleşimlerine göre 3 çeşidi vardır.

Doğrusal yerleşim(Bus topolojisi)

Halka yerleşim(Ring topolojisi)

Yıldız yerleşim(Star topolojisi)

Doğrusal yerleşim (Bus topolojisi)

Doğrusal yerleşim ağ çeşidinde bilgisayarlar bir kablo ile bir birleri arasında veri iletişimi sağlaya bilmektedir. Veri bu kablo boyunca iletilir ve ağ içerisinde ortak veri kanalına yeni terminaller eklenebilir.

Ağ yapılandırılması diğer topolojilere göre daha basit ve maliyeti düşüktür. Bilgisayarlar arasındaki iletimi sağlayan Kablonun iki ucunada özel sonlandırıcı ilave edilir. Tüm ağ sistemine bağlı Donanım cihazları bir kablo üzerinden veri iletişimi gerçekleştirildiği için, kablonun herhangi bir noktasındaki problem tüm ağ iletişimi sonlandırır.

Halka yerleşim (Ring topolojisi)

Halka yerleşim topolojisi Ağ sistemine bağlı Bilgisayarların halka biçiminde bağlantısı oluşturulan kablo sayesinde veri iletimi ve haberleşmesi sağlanır. Halka biçimindeki bağlantısı oluşturulan kablo üzerinde veriler tek taraflı yönde hareket eder ve halka üzerinde daire çizerler. Halka yerleşim topolojisinde oluşturulan yapıların diğer topolojilere göre ağ sistem maliyeti biraz daha pahalıdır. İletişim hızları kablolama sisteminize bağlıdır.

Yıldız yerleşim (Star topolojisi)

Yıldız yerleşim yapısında ise ağ sistemine bağlı tüm bilgisayarlar direk hub ve ya switch'e bağlıdır. Herhangi bir bilgisayarda hata ağ sistemine bağlı bilgisayarlardan her hangi birisinde problem olduğu takdirde tesbiti kolay ve sistemden çıkarılması basittir. Diğer topolojilere kullanılan kablo daha fazladır bu da maliyeti artırmaktadır.

Geniş alan bilgisayar ağı (WAN, Wide area network)

"Geniş alan agları ise yerel ve metropolitan ağların biribirlerine bağlantısı halinde oluşan ağdır. Yani ülkeler arası bilgisayar iletişimini sağlayan ağlardır. Bunu da örnekleyecek olursak; ele aldığımız firmanın yerel ve metropolitan ağını dünyaya açması ve diğer ülkelerdeki bilgisayarlarla kendi ağlarını buluşturma noktasıdır" [Url-1]

Şehirsel bilgisayar ağı (MAN, Metropolitan area network)

"LAN' ın kapsadığı alandan daha geniş, fakat WAN' ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle şehir içi bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur".[Url-2]

2.2 Bilgisayar ağ protokolleri

Ağ sistemleri kullanım oranları artmaya başlaması ile birlikte teknolojik gelişmelerde artmaya başlamıştır, teknoloji firmaları birçok ağ ürünü geliştirmiş, fakat ağ sistemleri arasındaki veri iletişim kurallarında problemler yaşanmaya başlamıştır. Teknoloji firmaları iletişim kurallarını kendilerine özgü tanımlamaya çalışmıştır. Bu sorunlar nedeni ile uluslararası standartlar teşkilatı(İSO) tarafından açık sistemler arabağlatısı(OSI) modeli geliştirilmiş ve tüm üreticeler bu modele göre gelişimlerini sürdürmüş ve ağ sistemleri arasındaki veri iletişimi problemi sorunu çözülmüştür. "internet ağ mimarisi katmanlı yapıdadır. Uygulama katmanı sayılmaz ise temel dört katman vardır. Bilgisayarlar arası iletişim için gerekli bütün iş, bu dört katman tarafından yürütülür. Her katmanda yapılacak görevler protokoller tarafından paylaşılmıştır. TCP ve IP farklı katmanlarda bulunan farklı protokollerdir. Fakat ikisi birlikte TCP/IP olarak kullanıldığında bütün katmanları ve bu katmanlarda bulunan protokollerin tamamını ifade eder. Bu sebeple TCP/IP bir protokol kümesi olarak bilinir."[Url-3]

2.2.1 OSI Modeli

Ağ sistemleri kullanım oranları artmaya başlaması ile birlikte teknolojik gelişmelerde artmaya başlamıştır, teknoloji firmaları birçok ağ ürünü geliştirmiş, fakat ağ sistemleri arasındaki veri iletişim kurallarında problemler yaşanmaya başlamıştır. Teknoloji firmaları iletişim kurallarını kendilerine özgü tanımlamaya çalışmıştır. Bu sorunlar nedeni ile uluslararası standartlar teşkilatı(İSO) tarafından açık sistemler arabağlatısı(OSI) modeli geliştirilmiş ve tüm üreticiler bu modele göre gelişimlerini sürdürmüş ve ağ sistemleri arasındaki veri iletişimi problemi sorunu çözülmüştür.

OSI katmanları

OSI modeli, ağ sistemlerindeki veri iletimi veya ağlar arasındaki haberleşme katmanlar vasıtası ile yapmaktadır. Bu katmanlar uygulama katmanı, sunum katmanı, oturum katmanı, ulaştırma katmanı, ağ katmanı, veri bağlantı katmanı ve fiziksel katman olmak üzere 7 ayrı katmandan oluşmaktadır bu ayırım sayesinde katmanlar üzerindeki işlemler ayrılmış ve daha fonksiyonel bir yapıya ulaşılmıştır.

Herhangi bir katman üzerinde yapılan işlem ne kadar bağımsız olarak çalışsada yapılan işlem hakkında diğer katmanlar bilgisi dâhilinde çalışılmaktadır.

Uygulama katmanı (Aplication layer)

Osi modelinde en üst sırada yer alan uygulama katmanı Katmanların diziliminde kullanıcıya en yakın katmandır. Kullanıcının bilgisayarlarında çalıştıracağı programlar ile ağ sistemi arasındaki ara bir birim görevi üstlenir ve bu programlar ağ sistemi üzerinde çalışması sağlanır. Bu uygulamalardan bazıları email uygulaması,veritabanı uygulamaları,dosya aktarım iletişim kuralı(FTP),Basit ağ yönetim protokolü(SNTP) gibi birçok örnek verilebilmektedir.Kısaca tanımlamak gerekirse Ağ sistemi ile ilgili bir uygulamanın osi modelindeki incelendiği ve işleve alındığı katman uygulama katmanıdır.

Sunum katmanı (Presentatiton layer)

Bu katman gönderilecek verinin, veriyi alacak bilgisayar, tablet, akıllı telefon gibi farklı özellikteki olan yapıların anlaya bilecekleri formata dönüştürüp veriyi istenilen formatta ilgili katmana iletilir. Bu işlem için ihtiyaç duyduğu bilgiyi uygulama katmanından alır ve verinin formatlanması, kodlanması ve sıkıştırılması gibi işlemleri yaparak ilgili katmana sunumu hazır haline getirmekle sorumlu katmandır.

Oturum katmanı (Session layer)

Sunum katmanı ile taşıma katmanı arasındaki iletişimi oturum katman oluşturur, Veriyi ileten ve veriyi alan uygulamalar arasındaki veri transferilerinin başlaması, bitirilmesi ve yönetilmesinden oturum katmanı sorumludur. Ayrıca ağda çalışan uygulamaların bir biri ile haberleşmesini sağlar bu sayede ağ üzerindeki uygulamalar birbirleri ile karışmaz. Örnek verilecek olursa Ahmet kullanıcısı Mehmet kullanıcısının bilgisayarına bağlı paylaşımlı bir yazıcıdan çıktı almak için veri gönderdiği zaman, hasan kullanıcısı da yine Mehmet kullanıcısının bilgisayarından paylaşılmış bir klasörden veri kopyalama isteğinde bulunduğu anda Mehmet kullanıcısının bilgisayarı oturum katmanı yönetimi ve iletişimi sayesinde iki isteğe de cevap verip istekleri yönetilebilir olmasını sağlar.

Ulaştırma katmanı (Transport layer)

“Taşıma katmanı, üst katmanlardan gelen veriyi ağ paketi boyutunda ayrı ayrı parçalara ayırır. Bilgilerin doğruluğunu kontrol eder. Gönderilecek bilginin güvenli bir şekilde ulaştırılmasını sağlar”.[Url-4] “Hata bulma ve hataları düzeltme görevi vardır. Bölünen parçalar veya paketler halinde veri akışında; alan bilgisayarın ulaştırma katmanı mesajı tekrar birleştirmektedir. Hatasız iletim için hata denetimi sürekli olarak gerçekleştirilmektedir.”[1]

Ağ katmanı (Network layer)

“Fiziksel adrese karşı, isimler ve mantıksal Ag adresleri dönüştürmektedir (örnek: bilgisayar ismi MAC adresi). Ağ katmanında, bilgi gönderim aşamasında en iyi yolun bulunması ve bu yoldan bilginin gönderilmesi sağlanmaktadır. Yönlendirici bilgisayarın göndereceği kadar büyük veri çerçevesi gönderemiyorsa, Ağ katmanı küçük ünitelere bölerek dengeleme sağlamaktadır. Network katmanında bulunan IP (internet protocol) ile mantıksal adresleme işlemi gerçekleşir.”[Url-3]

Veri bağı katmanı (Data link layer)

“Veri bağlantısı katmanı fiziksel katmana erişmek ve kullanmak ile ilgili kuralları belirler.Gönderilecek bilginin ağ ortamında nasıl taşınacağını, fiziksel adreslemeyi ve ağ topolojisini tanımlar.”[Url-5]

Media access control (MAC)

MAC alt katmanı, veriyi, hata kontrol kodu (CRC), alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır.Alıcı tarafta da bu işlemleri tersine yapıp veriyi, veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.[Url-5]

Logical link control (LLC)

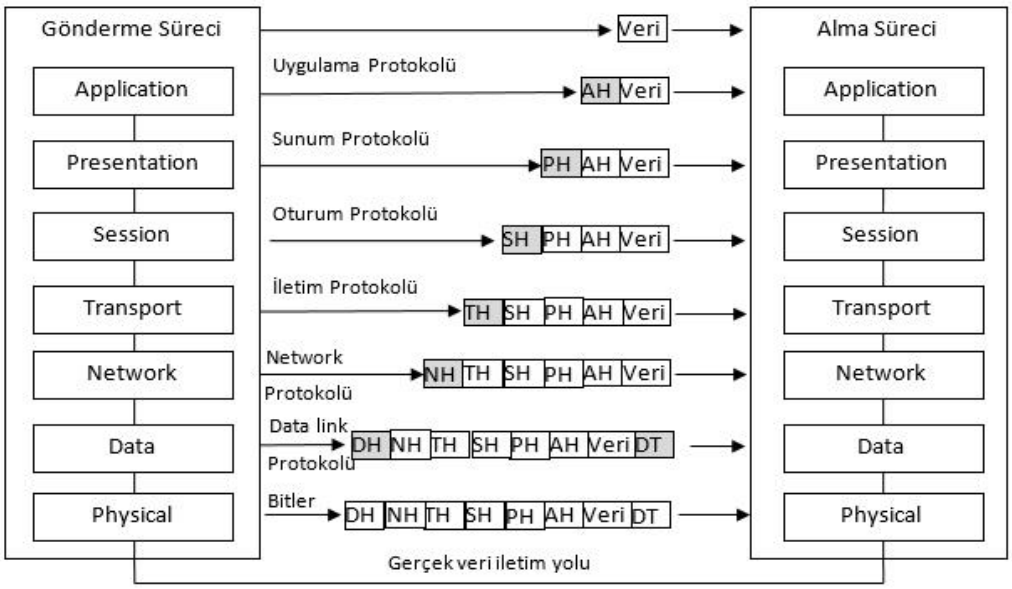
“LLC alt katmanı, bir üst katman olan ağ katmanı için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur (Service Access Points, SAP). Böylece kaynak makinede ve hedef makinede aynı protokoller iletişime geçebilir (örneğin TCP/IP).

LLC ayrıca veri paketlerinden bozuk gidenlerin (veya karşı taraf için alınanların), tekrar gönderilmesinden sorumludur. Flow Control, yani alıcının işleyebileceğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir."[Url-5]

Fiziksel katman (Physical layer)

Bakır tel yâda hava gibi fiziksel bir ortam üzerinde bit iletimi için mekanik ve elektriksel özellikleri tanımlamaktadır[2]. Diğer katmanlar dijital olarak çalışırken fiziksel katman dijital bilgileri dış ortama aktarmak için nasıl elektrik, ışık yâda radyo sinyallerine çevrilip aktarılacağını standartlar aracılığıyla tanımlamaktadır.[3]

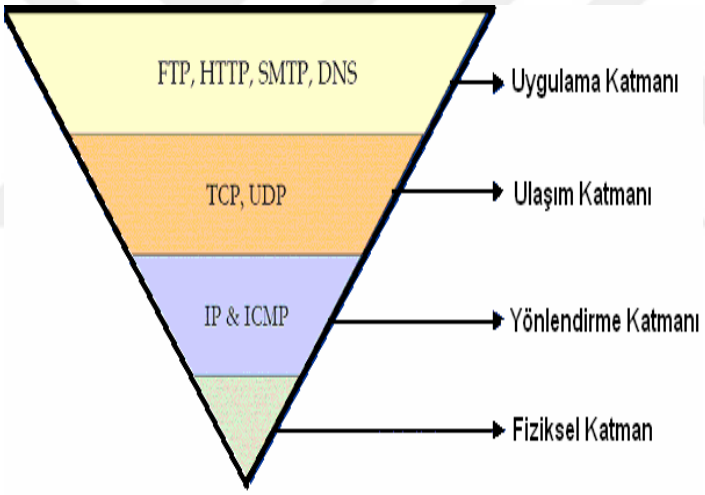
Şekil 2.1.'de bilgilerin katmanlar arasında işleme tabi tutulurken biçimsel olarak almış olduğu değişiklikler görülmektedir. Örneğin Uygulama katmanından sunum katmanına giden bir paketin başına AH(Application Head) geldiği görülmektedir. Data katmanında ise gerektiğinde data link trailer (DT) eklenebilmektedir. Bunun amacı ise data senkronizasyonunu sağlamaktır.[Url-6]



Şekil 2.1: Fiziksel katmanlar

2.2.2 TCP/IP modelleri

İnternet ağ mimarisi katmanlı yapıdadır ve 4 katmandan oluşur Bilgisayarlar arası iletişim için gerekli bütün iş, bu dört katman tarafından yürütülür. Her katmanda yapılacak görevler protokoller tarafından paylaşılmıştır. TCP ve IP farklı katmanlarda bulunan farklı protokollerdir. Fakat ikisi birlikte TCP/IP olarak kullanıldığında bütün katmanları ve bu katmanlarda bulunan protokollerin tamamını ifade eder. Bu sebeple TCP/IP bir protokol kümesi olarak bilinir. TCP/IP (Transmission Control Protocol/Internet Protocol), bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. Bir başka değişle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koyar.[Url-7]



Şekil 2.2: TCP/IP Yapısı

3. KABLOSUZ AĞLAR

Kablosuz teknoloji; Bir veya daha fazla cihazın fiziksel bağlantı olmaksızın haberleşmesi demektir. Kablosuz ağlar; kablolu iletişime alternatif olarak uygulanan, RF (Radyo Frekansı) teknolojisini kullanarak havadan bilgi alışverişi yapan esnek bir iletişim sistemidir.[4]

Kablosuz geniş alan ağları 2G hücreli, Cellular Digital Packet Data (CDPD), Global System For Mobile Communications (GSM) ve Mobitex gibi geniş kapsama alanı teknolojilerini içerir. Kablosuz Yerel Alan Ağları 802. 11, HiperLAN ve diğerlerini, Kablosuz Kişisel Alan Ağları ise Bluetooth ve Infrared (IR) gibi teknolojileri içerir. Bütün bu teknolojiler, bilgiyi elektromanyetik dalgaları kullanarak alırlar ve iletirler. Kablosuz teknolojiler, radyo frekans bandının yukarısında ve IR bandının yukarısındaki dalga boylarını kullanırlar.[4]

Kablosuz iletişim; kullanıcılara taşınabilirlik, esneklik, artan verimlilik ve daha az kurulum maliyeti gibi birçok yarar sunmaktadır. Kablosuz yerel alan ağları; kullanıcılara diz üstü bilgisayarlarıyla ofislerde kablolara gerek kalmadan ve ağ bağlantısı kesilmeden hareket etme olanağını sağlamaktadır. Daha az kablo daha fazla esneklik, verimliliğin artması ve kablolama ücretlerinin azalması anlamına gelmektedir. Ancak riskler, kablosuz ağların ayrılmaz bir parçasıdır. Bu risklerden bazısı kablolu ağlardaki risklerle aynıdır, bazısı da yenidir. Kablosuz ağlarda riskin kaynağı iletim ortamının hava olmasıdır. Yetkili olmayan kullanıcıların sisteme ve bilgilere girmesi, sistem bilgilerinin bozulmasına, ağ bant genişliğinin azalmasına, ağ performansının düşmesine neden olmaktadır.[4]

3.1 Kablosuz yerel ağ standartları

İlk olarak WLAN aygıtları düşük hızları, standart eksikleri ve yüksek maliyetleri ile kullanışlı değildi. Toplam bant genişliğinin 1-2 Mbps gibi bir hızla kısıtlı olması, farklı firmalar tarafından üretilen ağ arayüz kartı (Network Interface Card - NIC) ve erişim

noktalarının (Access Point - AP) birbirleri ile uyumlu çalışamama probleminden dolayı tercih edilmiyordu. Ancak 2000'li yıllardan itibaren, standartlaşmayla birlikte WLAN sistemleri hızla yayılmaktadır. Çünkü standartlaşma sonucunda birçok marka WLAN donanımı aynı kablosuz ağ içinde kullanılabilmektedir. Bugün Wi-Fi (Wireless Fidelity/Kablodan bağımsızlık) kablosuz ağlar için endüstri standarttı olarak yaygın şekilde kullanılmaktadır [5].

3.1.1 IEEE 802.11 Standartları

EEE, OSI (Open System Interconnection) referans modeline göre veri bağlantı katmanını MAC (Media Access Control) ve LLC (Logical Link Control) olarak iki alt katmana ayırmıştır. Bunun nedeni üst katmanların, ağ donanım yapısına ve türüne bakmaksızın aynı arabirimle çalışabilmesini sağlamaktır. 802.11, 1997 yılında standart olmuştur. 802.11 IEEE tarafından kablosuz ağlar için geliştirilmiş bir standarttır. İlk geliştirilen standart olan 802.11; 2.4 GHz frekansında, saniyede 1 Mb veya 2 Mb veri transferine izin verir. Bu standardın fiziksel katmanda, FHSS ve DSSS olmak üzere kullandığı iki farklı modülasyon yöntemi bulunmaktadır. Bu yöntem ile elverişli ortamlarda FHSS ile 2 Mbps, sinyal gürültüsü olan ortamlarda ise DSSS ile 1 Mbps veri iletim hızları sağlamaktadır. Günümüzde kullanılan teknolojiler 802.11a, 802.11b, 802.11g, 802.11n standartlarıdır.[6]

3.1.2 IEEE 802.11a

802.11 standardının gelişen teknoloji ile belirli Özellikleri karşılayamaması ya Başlamış ve 1999 yılında IEEE 802.1a Sürümü yayınlanmıştır. Bu standart temeli 802.11 olmasına karşın yayın bandını 5 gHz frekansında çalıştırmaktadır ve 54 Mbps gibi bir veri iletim hızına ulaşılmış bu standart, açık alanlarda ise 100 metreye kadar kapsama desteğinde bulunmaktadır.[Url-8]

3.1.3 IEEE 802.11b

802.11b standardı 802.11a ile birlikte 1999 yılında yayınlanmıştır. . 802.11b, 802.11 gibi 2.4 gHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına ulaşabilmektedir. İlk Yayına Girdiği sürede sağladığı veri Hızı ve 2.4 GHz de yayın yapabilmesi nedeni ile Kablolu ağ teknolojilerine rakip hale gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır.[Url-8]

3.1.4 IEEE 802.11g

Kablosuz ağ kullanımının yaygınlaşmaya Başlaması ile 2003 yılında IEEE tarafından kablosuz ağ standartlarında geliştirilen 3. nesil teknoloji ve 2.4 gHz frekansında çalışmakta idi.

802.11g standardı, 802.11b standardının temelini almış ve biraz daha geliştirirmiş bir sürümdür fakat veri iletim hızı ve kullanılan bant genişliğinde önemli ölçüde gelişme sağlanmıştır. [Url-8]

3.1.5 IEEE 802.11i

Kablosuz ağların yaygınlaşması nedeni ile birçok güvenlik açıkları oluşmaya Başlamış ve bu güvenlik sorunlarının Çözümü için geliştirirmiş bir standarttır.

3.1.6 IEEE 802.11n

Şu anda taslak aşamasında 802.11n standardı, maksimum veri transfer hızını 540 Mbps çıkarmaya, bunun yanında eş zamanlı olarak çoklu veri iletişimi yapılmasına imkân tanıyan yeni standarttır.

3.2 Kablosuz ağlarda güvenlik

ISO/IEC 27001'e göre güvenlik, bir kurumun bilgi varlıklarının gizliliğinin (bilginin yetkisi olmayan kişi, kurum ya da süreçler için kullanılabilir olmaması ya da ifşa edilmemesini temin etme özelliği), bütünlüğünün (varlıkların doğruluğunun ve eksiksizliğinin teminat altına alınması özelliği) ve kullanılabilirliğinin (yetkili bir kurumun talebi üzerine kullanılabilir olma özelliği) koruması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesinin önlenmesi, kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemleri önceden alması olarak tanımlanmaktadır.[7]

3.2.1 Wi-Fi korumalı erişim (WPA ve WPA2)

Wi-Fi Korumalı Erişim bilgileri şifreler ve ağ güvenlik anahtarının değiştirilmediğinden emin olur. Ayrıca Wi-Fi Korumalı Erişim, yalnızca yetkili

kişilerin ağa erişebilmesini sağlamaya yardımcı olmak için kullanıcıların kimliğini doğrular. İki tür WPA kimlik doğrulaması vardır: WPA ve WPA2. WPA tüm kablosuz ağ bağdaştırıcıları ile çalışmak üzere tasarlanmıştır, WPA2, WPA'ya göre daha güvenlidir. WPA, her kullanıcıya farklı anahtarlar dağıtan 802.1X kimlik doğrulama sunucusuyla kullanılacak şekilde tasarlanmıştır. Bu, WPA-Kuruluş veya WPA2-Kuruluş olarak adlandırılır. Ayrıca, her kullanıcıya aynı parolanın verildiği önceden paylaştırılan anahtar (PSK)modunda da kullanılabilir.[Url-9]

3.2.2 Kabloluya eşdeğer gizlilik (WEP)

Kabloluya Eş değer gizlilik(WEP)teknolojisi geride kalmış fakat günümüzde kullanımına devam edilen Donanım cihazları için kullanılan bir ağ güvenlik yöntemidir. Kabloluya Eşdeğer gizliliği devreye alındığı takdirde, ağ güvenlik anahtarı oluşturulur. Oluşturulan ağ güvenlik Anahtarı, ağdaki bilgisayarların bir biri arasındaki ilettiği bilgileri şifreler, bu sayede şifrelenmiş bir veri iletimi gerçekleştirilip ağ güvenliği sağlanabilmektedir. Fakat kullanılan bu WEP güvenliği yönteminde kullanılan çeşitli yazılımlar ile kolay bir şekilde aradaki şifre kırılabilmektedir bu nedenle günümüzde tercih edilen ağ güvenliği yöntemleri Arasında çok fazla tercih edilmez.

3.2.3 MAC adresi kimlik denetimi

MAC (Media Access Control-Ortam Erişim denetimi) adresi, Kablolu ve kablosuz ağ sisteminde sisteme bağlanmak isteyen Donanım cihazının kendisini tanımlayan 0 ve 9 arası rakamlardan, A ve F arası harflerden oluşan Eşsiz bir Mac adresi ile tanımlanır. Mac adresleri sayesinde Erişim Noktası cihazlarına(accespoint) veya erişim Noktası kontrolür cihazlarına, kullanıcıların ağ sisteme bağlanacakları Donanım cihazlarının Ortam Erişim Denetimi (MAC) adreslerini ağ sistemine kişinin kimlik bilgileri ile eklenmektedir.

Mac adresi kimlik doğrulama yöntemi sayesinde Mac adresi doğru ise veya sisteme ekli ise Kullanıcını ağ sistemine erişimi sağlanmaktadır eğer Mac adresi ağ sistemi cihazlarına dâhil değil ise kullanıcıyı ağa erişimi engellenir bu sayede bir ağda Mac adresi kimlik denetimi güvenlik yönetimi oluşturulmaktadır.

Mac adresi kimlik denetimi geçmiş dönemlerde çok önemli bir kimlik denetimi yöntemi idi fakat günümüzde Kullanıcı sayısı düşük ve sürekli değişken olmayan kurumlarda genel olarak tercih edilen bir yöntem haline gelmiştir. Büyük kurumlarda ise gelişen teknoloji ve sistemlere bağlanan kullanıcı sayısının sürekli artması sebebi ile kimlik kanıtlama yöntemlerinde çok fazla tercih edilmemeye başlanmıştır. Bunun en büyük nedenlerden birtanesi her bir erişim Noktası cihazlarına, erişim Noktası fazla olan kurumlarda erişim Noktası kontrolürü cihazlarına Sürekli Mac adreslerinde Güncelleme yapılması gerekmektedir. Bu işlem ise yönetimi ve deneti güçleştirmektedir. Kullanımın çok fazla tercih edilmemesinin diğer bir nedeni ise mevcut teknolojideki birçok yazılım ve Donanım cihazı ağı dinleyip erişim sağlayan bir kullanıcının ağ sistemine dâhil olduğu Mac adresini tesbit edebilmesidir, mevcut bazı yazılımlar kullanılarak Mac adresleri değiştirilebilmektedir tesbit edilen Mac adresi ilgili yazılımlar ile değiştirilip sanki mevcut bir kullanıcı gibi ağ sistemine erişim sağlana bilmektedir. Kullanıcı sayısı yüksek kurumlarda bu işlemi yapan kişilerin binlerce mac adresi arasından tesbit edilmesi zor bir hale gelmiştir bu nedenlerden dolayı başlangıçda önemli bir kimlik tanıma sistemi olan mac adresi kimlik tanıma yöntemi günümüz teknolojisinde alternatif kimlik kanıtlama yöntemlerine tercihleri artırmıştır.

3.2.4 SSID(Service set identifier-Servis seti tanımlıyıcısı) Yayını devre dışı bırakma

Bir servis seti tanımlıyıcı kablosuz ağ yayınının ismidir. İstemci tarafından kablosuz ağ kartının özelliği ile yayınlanan servis seti tanımlıyıcısının ismi algılanabilmektedir. Kullanıcı bu yayını seçtikten sonra şifre ile sisteme dâhil olabilmektedir, sisteme dâhil olan kullanıcılar dâhil oldukları Ssıd yayınına bağlı olan diğer kullanıcılar ve donanım cihazları ile haberleşebilmekte ayrıca veri paylaşımlarında bulunabilmektedirler.Ssid yayını gerçekleştiren donanım cihazları belirli bir alana yayın yapmaktadır, ilgili alanda farklı kullanıcılılar da sisteme erişim için Ssid yayın ismini görebilmektedir. Bu nedenle servis seti tanımlıyıcı ismini yayınlanan donanım cihazlarında bu isim güvenlik gereği ile Ssid yayınlama özelliği devre dışı bırak seçeneği kullanılarak alandaki diğer kullanıcıların Ssid görmeleri engellenir. Bu sayede Kablosuz ağda güvenlik sağlanabilmektedir.

3.2.5 802.1x kimlik denetimi

802.1x kimlik denetimi 802,11 kablosuz ağlarının ve kablolu ağlarının güvenliğini artırmaya yardımcı port tabanlı bir kimlik tanımlama standardıdır. 802.1x kullanıcıları doğrulamak ve ağ erişimi sağlamak için bir kimlik doğrulama sunucusu kullanır. Kablosuz ağlarda, 802.1x WPA, WPA2 veya WEP anahtarlarıyla çalışabilir. Bu kimlik doğrulama türü genellikle çalışma alanı ağına bağlanırken kullanılır.[16] 802.1x kablosuz ağ sisteminde, erişim noktasında (AP) Bağlantı isteği gönderen bir istemci, Erişim noktasında Genişletilebilir Kimlik Denetimi Protokolü (EAP) başlatma mesajı göndererek kablosuz ağ sistemi üzerindeki tüm cihazlardan kimliği denetimine dâhil olur ve denetimin başarıl olması durumunda sisteme erişim sağlanır başarısız olduğu durumda ise ağ sistemine bağlanmak için kullanacağı port kapalı olduğu için sisteme erişim sağlatmayan bir kimlik denetim standardıdır.

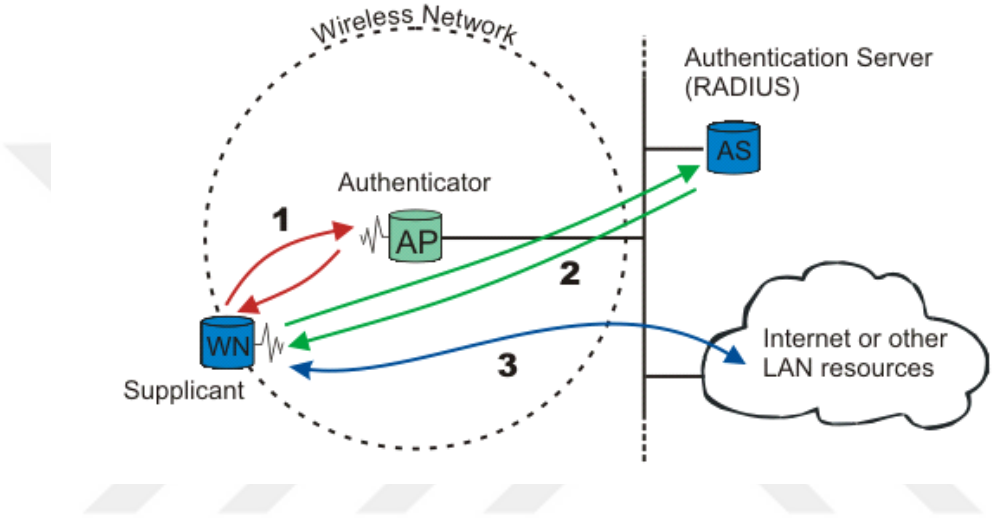
Standartların karşılaştırılması

	WEP	WPA	WPA2
Şifreleme	Şifreleme yapısı kırıldı. RC4 algoritması	WEP in açıklarını kapatıyor. TKIP/RC4	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bitlik anahtar	128 bitlik anahtar	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir.	Anahtarlar her oturum, her paket için değişir.	Anahtar değişikliğine gerek yoktur.
Anahtar yönetimi	Anahtar yönetimi yoktur	802.1x	802.1x
Asıllama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC

Şekil 3.1: Standardların karşılaştırması

4. IEEE 802.1X STANDARDI NEDiR

IEEE 802.1x, port tabanlı ağ erişim kontrolünü sağlayan IEEE standardıdır. Ayrıca 802.1x ağ protokolleri IEEE 802.1 grubunun bir üyesidir. Kablolu ve kablosuz ağ sistemlerinde kimlik doğrulama yöntemlerinden biridir.



Şekil 4.1: 802.1x iletişim

IEEE 802.1X, Kablolu ve kablosuz ağ sisteminde üzerinde Genişletilebilir Kimlik Doğrulama Protokolü (EAP) nü kullanır. 802.1x-2001IEEE 802.3 Kablolu ağ sistemi için geliştirilmiştir, fakat kablosuz ağ sisteminin kullanımının artması ile 802.1x-2004 adı ile Fiber Distributed Data Interface (ISO 9314-2) ve IEEE 802.11 kablosuz ağ gibi diğer IEEE 802 ağ teknolojilerine de uygun hale getirilmiştir. EAP protokolü ayrıca ağ sistemi segmenti üzerinden noktadan noktaya şifreleme ve kimlik tespit hizmetine destek vermek için 802.1x-2010 adı ile Yayınlanan sürümde, IEEE 802.1AR (Secure Device Identity, DevID) ve IEEE 802.1AE (“MACsec”) ile birliktekullanılacak şekilde güncellenmiştir [17]. 802.1x standardı 2.katmanda denetimli kablolu veya kablosuz bir yerel ağa Erişim sağlayabilmek için kullanıcıların kimliklerini doğrulamalarını gerektirir. Ağın dinlenebilir olması ağın herkes tarafından erişilebilir olması durumudur bu durumdan kurtulmak için kimlik kanıtlaması yapılabilir. H

Bilgisayar için belirli bir port tanımlanır. Kullanıcılar da bir porttan ağa dâhil olurlar diğer portlardan da ağ dinlenebilir ancak verilerden anlamlı bir şey çıkartılamaz.

Böylece ağın dışındaki bir bilgisayarın veri göndermesi için kimlik kanıtlaması yapılır. Ağın içindeki ve dışındaki bilgisayar yine de haberleşebilir ancak dışardaki bilgisayarlar ağı dinleyemezler. Kullanıcı doğrulama: MAC adresi, switch port, harici bir yetkilendirme politikası ile sağlanır. Ağa kimin, hangi hakla gireceğinin belirlenmesi, denetlenmesi ve yetkilendirilmesi ağ tabanlı erişim kontrolü olan NAC tarafından belirlenir [Url-10]. Kimlik doğrulama, korumalı ağda güvenlik görevlisi gibi hareket eder. İstek sahibinin kimliği doğrulanana ve yetkilendirilene kadar ağın korumalı tarafına kimlik doğrulama izni verilmez. 802.1x bağlantı tabanlı kimlik doğrulama ile, istek sahibi, kimlik için kullanıcı adı / parola veya dijital sertifika gibi belgeler sağlar ve doğrulama için kimlik doğrulama sunucusuna belgeleri iletir. Eğer ki kimlik doğrulama sunucusu, belgelerin geçerliliğini belirlerse, ağın korumalı tarafında yer alan kaynaklara erişime izin verilir.[Url-10]

4.1. EAP

Genişletilebilir Kimlik Doğrulama Protokolü (EAP) ile rasgele bir kimlik doğrulama mekanizması, bir uzaktan erişim bağlantısının kimliğini doğrular. Kullanılacak tam kimlik doğrulama şeması, uzaktan erişim istemcisi ve kimlik doğrulamasını yapan (uzaktan erişim sunucusu veya Uzaktan Kimlik Doğrulama Araması Kullanıcı Hizmeti [RADIUS] sunucusu) arasında uzlaşmayla belirlenir. Yönlendirme ve Uzaktan Erişim varsayılan olarak, EAP-TLS ve MD5-Çekişme desteği içerir. Başka EAP yöntemleri sunmak için Yönlendirme ve Uzaktan Erişim çalıştıran sunucuya diğer EAP modüllerini takabilirsiniz. EAP, uzaktan erişim istemcisiyle kimlik doğrulamasını yapan arasında açık uçlu bir görüşme yapılmasına olanak verir. Görüşme, kimlik doğrulamasını yapanın kimlik doğrulama bilgilerini istemesinden ve uzaktan erişim istemcisinin ona verdiği yanıtlardan oluşur. Örneğin, EAP, güvenlik token kartlarıyla birlikte kullanıldığında, kimlik doğrulamasını yapan, uzaktan erişim istemcisine bir ad, PIN ve kart token değerini ayrı ayrı sorabilir. Her sorgu sorulup yanıtlandıkça, uzaktan erişim istemcisi, kimlik doğrulamasının bir sonraki düzeyine geçer. Tüm sorular başarılı bir şekilde yanıtlandığında, uzaktan erişim istemcisi kimlik doğrulamasından geçmiş olur. 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.

Windows Server ailesinde, bir EAP altyapısı, iki EAP türü ve EAP iletilerini bir RADIUS sunucusuna (EAP-RADIUS) iletme yeteneği vardır [Url-11]. EAP kimlik kanıtlama sürecinde, kimlik kanıtlama sunucusu ile istemci arasında geçen ve tarafların hangi kimlik kanıtlama yöntemini kullanacaklarını belirler. EAP kimlik kanıtlama yöntemi olarak MD5, TLS, TTLS, PEAP, LEAP kullanır.[Url-12]

EAP-MD5

EAP- MD5, kimlik doğrulama işlemi içim ağa erişecek kullanıcının kullanıcı ismi ve şifresine gereksinim duyar noktadan noktaya bağlantı chap protokolü ile benzerlik gösterir. Kimlik doğrulama işleminde kullanıcının şifresi veri tabanında açık metin olarak kayıt altına alınmaktadır. İstemci, kullanıcı ismi ve şifresi MD5 algoritması ile tekrar şifreleyip kimlik kanıtlama sunucusuna iletir. Kimlik kanıtlama sunucusu kullanıcının kimliğini doğrulamak için veri tabanında açık metin olarak kayıt altına alınmış bilgi ile md5 algoritması ile şifrelenmiş veriyi karşılaştırır Karşılaştırma sonucunda doğrula sağlanır ise kullanıcı kimliği kanıtlanarak sisteme dâhil olur. Md5 algoritması sözlük saldırı gibi yöntemlere zayıftır belirli bir tekrardan sonra alggoritma kırılabilmekte ve kullanıcı verileri başka birinin eline geçebilmektedir. Ayrıca Md5 algortimasında anahtar üretimi mevcut değildir belirli bir süre sistemi analiz eden kullanıclar tarafından sisteme erişimi kanıtlanmıştır.

Hafif EAP (LEAP)

“Kimlik kanıtlama için Kimlik Kanıtlama Sunucusuna (RADIUS) bir kullanıcı adı/parola çifti gönderilir. Leap, Cisco tarafından geliştirilmiş müseccel bir protokoldür ve güvenli olduğu düşünülmez. Cisco LEAP'i PEAP niyetine sunmuştur. Yayınlanmış bir standarta en yakın şey burada bulunabilir. Bu yöntem her iki yönde kimlik kanıtlama sağlar. EAP-TLSRFC2716]'da tanımlanmıştır.”[Url-13]

EAP-TTLS

“Kimlik kanıtlama verisinin emniyetli iletimi için şifreli bir TLS tüneli kurar. TLS tünelinden diğer (herhangi) kimlik kanıtlama yöntemleri faydalanır. Funk Software ve

Meetinghouse tarafından geliştirlmiştir ve şu an bir IETF taslağı halindedir."[Url-13]

Korumalı EAP (PEAP)

"EAP-TTLS gibi şifreli bir TLS tüneli kullanır. Hem EAP-TTLS hem EAP-PEAP için istemci (WN) sertifikaları seçimliktir, ama sunucu (AS) sertifikaları gereklidir. Microsoft, Cisco ve RSA Security tarafından geliştirilmiştir ve şu an bir IETF taslağıdır."[Url-13]

EAP-MSCHAPv2

"Kullanıcı adı/parolaya ihtiyaç duyar ve temel olarak MS-CHAP-v2'nin [RFC2759] EAP kaplamalı olanıdır. Genellikle PEAP şifreli tünelde kullanılır. Microsoft tarafından geliştirilmiştir ve şu an bir IETF taslağıdır."[Url-13]

Çizelge 4.1 Eap yöntemleri karşılaştırılması

	MD5	**TLS**	**TTLS**	**PEAP**	**LEAP**
Standart	Açık	Açık	Açık	Açık	Firma
İstemci Sertifikası	×	✓	×	×	×
Sunucu Sertifikası	×	✓	✓	✓	×
Güvenlik	Yok	Güçlü	Güçlü	Güçlü	Zayıf
Kullanıcı Veritabanı	"Açık Metin" Parola	"Active Directory"	Token Systems, SQL, LDAP	Active Directory, NT Etki Alanı	Active Directory, NT Etki Alanı
Dinamik Anahtar Değişimi	×	✓	✓	✓	✓
Karşılıklı Doğrulama	×	✓	✓	✓	✓

5. IEEE 802.1X STANDARDI KABLOSUZ AĞ GÜVENLİĞİ ÜNİVERSİTE İÇİN GELİŞTİRİLEN TEZ ÇALIŞMASINDA KULLANILAN MATERYALLER

Sanal yerel alan ağı (VLAN)

Hafif dizin erişim protokolü (LDAP)

Dizin hizmeti (Active Directory)

Sertifika (Certificate Services)

Ağ ilkesi sunucusu (Network Policy Services)

Erişim noktası (Access Point)

Servis seti tanımlıyıcısı(Ssid)

Erişim noktası kontrolörü (Access Point Controller)

Switch(Ağ Anahtarı)

Güvenlik duvarı (Firewall)

5.1. Sanal yerel alan ağı

Sanal yerel alan ağı (VLAN), bir kablolu veya kablosuz ağ sistemi üzerinde ağa bağlı kullanıcılıların gruplara bölünerek ağ anahtarı cihazında ya da erişim noktası kontrolür cihazı üzerinde portlara atanması işlemi ile gerçekleştirilir. Sanal ağın oluşturulması ve devreye alınması ile birlikte her sana ağ kendisine ait olan yayını alacağı için yayın trafiği azalacak ve band genişliğ de artacaktır. Sanal ağ yapılandırmaları siteme erişim sağlayan kullanıcıların çalıştığı bölüme, birime hatta erişim sağlayacapı uygulamay göre standart tanımlanabilme imkânı vermektedir.[Url-14]

5.1.1. Yayın kontrol

Yayın her protokol tarafından üretilir. Sanal ağ uygulanmamış bir ağ sisteminde 2. Seviye ağ cihazlarından gelen yayın paketini ağ üzerindeki tüm portlara gönderilir. Kablosuz ağ sistemi üzerinde bağlı olan donanım cihazı sayısının yoğun olduğu bir ortamda yayın tırafiğinin artması ve doğal olarak artan yayın paketlerinin her cihaza

gönderilmesine neden olur. Yayın kontrolü için ağ sistemi tasarılarında mutlaka sanal ağ tasarımını uygulayarak sistemdeki paket alış verişini, band genişliğini ve yayın kontrolünü sanal ağ sistemi sayesinde tasarlayıp daha iyi bir kablosuz ağ sistemi oluşturulmasına imkân sağlamaktadır.[Url-14]

5.1.2. Güvenlik

VLAN sanal Ağ yapısı uygulanmamış bir ağ Tasarısının dezavantajlarından biri de güvenliktir. Sisteme erişim sağlamış tüm Kullanıcılar aynı ağ üzerinde yer alacaktır, aynı ağ üzerinde yer alan Kullanıcılar ağ kartları sayesinde bir birleri ile haberleşebilecek, veri paylaşımında bulunabilecek ve ağdaki donanım cihazları kullanabileceklerdir. Ağ Üzerindeki veri iletimini dinleyip bugün çözen çeşitli yazılım ve Donanım cihazları mevcuttur. Buda tüm Kullanıcıların aynı ağda olmasından doğan güvenlik açığına sebep olmaktadır. Örneğin finans biriminin yer aldığı bir ağda sisteme bağlanan bir misafir kullanıcısıda aynı ağda olacağı için ağı dinleyip veri paketlerini çözebilir bu da finansla ilgili bilgilerin güvenliğini tehlikeye sokmaktadır. Sanal ağ Oluşturulan bir ağ sisteminde birimler ve Bölümler için ayrı sanal ağlar oluşturulmalıdır.

5.1.3. Esneklik

Sanal ağlar oluşturulmuş bir ağda broadcat guruplarında otomatik olarak oluşturulmuş demektir. Kablosuz ağ üzerindeki sisteme erişim sağlayan kullanıcıların ağa erişim yetkileri özel durumlarda artırılabilmesi yani özel bir yetkili ağdaki guruba ve sanal ağa kullanıcının eklenebilmesi kablosuz ağ sistemi içerisinde büyük bir esneklik sağlamaktadır. Diğer bir önemli husus ise ağı büyümesi durumunda ek sanal ağlar oluşturulabilmesidir ve oluşturulan sanal ağa yönlendirme işlemlerinin kolay bir şekilde yapılabilmesidir.

Aynı işlem sanal ağ oluşturulmadan işleme alınmaya kalkıldığında, Yeniden bir ana omurgaya kadar fiziksel kablolama işlemi gerekmekte ayrıca yönlendirme işlemi için ek bir router veya donanım cihazı temin edilmesi gerekmektedir bu da maliyeti ve işlemi artırmaktadır.

5.1.4. Üniversite sanal yerel alan ağ tasarımı

Üniversitenin kablosuz ağ mimarisin içerisinde kullanıcı gruplarının güvenlik seviyelerine göre ayrı sanal alan ağlarından sisteme erişebileceği sanalağlar tasarlanmış ve bu sanal ağların isimleri,tag id(rakamlar) leri , ip adresleri ,netmask, default gateway ve dhcp server belirlenip diğer 802.1x cihazları ile haberleştirilmesi için analizler yapılmıştır ve bu analizler neticesinde tablo oluşturulmuştur.tez çalışmasında

Çizelge 5.1 Sanal ağ tasarımı

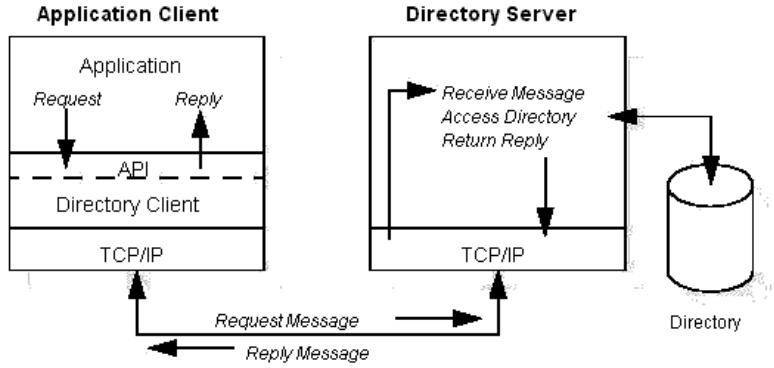
Vlan İsim	**Tag Id**	**Ip Adres**	**Netmask**	**Default Gateway**	**Dhcp Server**
Ogrenci_Test	2000	10.10.0.2	255.255.255.0	10.10.0.1	10.10.0.1
Akademi_Test	2001	10.10.1.2	255.255.255.0	10.10.1.1	10.10.1.1
Bim_Test	2002	10.10.2.2	255.255.255.0	10.10.2.1	10.10.2.1
İdari_Test	2003	10.10.3.2	255.255.255.0	10.10.3.1	10.10.3.1
Server_Test	2004	10.10.4.2	255.255.255.0	10.10.4.1	10.10.4.1

5.2. Hafif dizin erişim protokolü-LDAP (Lightweight Directory Access Protocol)

Hafif Dizin Erişim Protokolü bir dizin servisi standardıdır. Dizin erişim protokolü içerdiği bilgi ve yapı itibari ile veri tabanı olarak isimlendirilir. Dizin erişim protokolü veri tabanı içerisindeki bilgiler bir Sıralama mantığına sahip ve her bir obje hakkında veri barındıran bir liste olarakta tarif edilmektedir.

“Hafif dizin erişim protokolü istemcisi için yazılmış ve istemcisinin içine gömülmüş

API(Application Programming Interface) vasıtasıyla aradığı bilginin formatını oluşturarak TCP/IP vasıtasıyla dizin sunucusuna gönderir. Bu isteği alan dizin sunucusu bu isteği dizini içeren veriyi sorgulayarak gerekli bilgiyi yine ayni yolla istemciye gönderir."[Url-15]

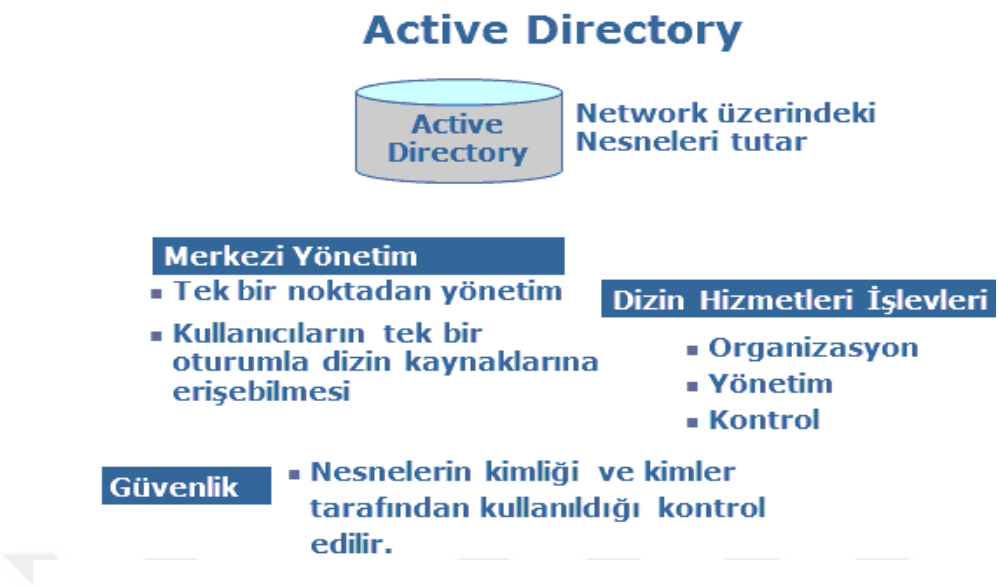


Şekil 5.1 : Haberleşme yapısı

Bir istemci LDAP oturumunu sunucuya bir istekte bulunarak başlatır (varsayılan olarak TCP port 389 üzerinden). İstemci sunucuya bir işlem isteği gönderir ve sunucu da bunu yanıtlar. Dizin hizmeti için 802.1x Standardı Üniversite tasarımında aşağıda belirtilen özellikleri nedeni ile 802.1x tez çalışmasında LDAP işleminde active directory tercih edilmiştir.

5.2.1. Dizin hizmeti (Active directory)

Dizin hizmeti ağ sistemi yönetiminde ağ üzerinde paylaşılan kaynakların,donanım cihazlarının,yazılım programlarının,veya herhangi bir veriye erişim sağlayabilecek kullanıcıların erişim sağlanacak materyallere izinlerinin veya yetkilerini düzenleyebildiğimiz bir ağ yönetim aracıdır.dizin hizmetinin önemli bir diğer özelliği ise kullanıcı ve gurup tanımlamalarıdır tanımlanan kullanıcılar belirli bir kimlik denetiminden sonra dizin hizmetine erişebilmektedirler bu özellik bize dizin hizmeti içerisinde bir kimlik denetimi yapmamıza olanak sağlamaktadır.kimlik denetimine göre kullanıcılara ve guruplara farklı politikalar uygulama imkanı sağlabilmektedir. [Url-16]Örnek olarak ağ üzerinde paylaşılmış bir veriyi aynı dizin hizmetinde olmasına rağmen Mehmet kullanıcısına bu veriye ulaşım yetkisi verilebilmekte fakat fatih kullanıcısına bu veriye ulaşım imkanı kapatılabilmektedir bunun gibi özellikler sayesinde ağ sistemi yöntemlerinde dizin hizmeti önemli bir rol almaktadır.



Şekil 5.2: Dizin hizmeti

Active directory'nin sağladıkları

Ağ sistemini domain (alanlar) şeklinde düzenlememize olanak sağlar.Kullanıcı ve grup listelerini merkezi yönetim yapısı şeklinde verileri depolar ve saklar.Kimlik denetimi (authentication) imkanı verir: Kullanıcılara ve gruplara özel yapılandırma imkanı veriri bu olanka sayesinde gerekli yetkilendirmeler yaparak uygulamalara ve kaynaklara yetki seviyelerindeki izinlere göre ulaşım imkanı verir. "Alanın OU adı verilen alt parçalara bölünmesini sağlar. Daha küçük bu birimler, yönetimin delege edilmesini sağlar. Belli yönetim işlemlerinin yetkilendirilmesi sağlanır."[Url-17]

Active directory özellikleri

Merkezi Veri Depolama: Dizin Hizmetin'de sisteminde yer Alan tüm veriler tek bir veritabanında saklanır. (NTDS.DIT). Merkezi bir veritabanı ile kullanıcılar istedikleri nesneye kolayca erişebilirler.

Ölçeklenebilirlik: Dizin Hizmeti, farklı Ağ sistemlerine göre ölçeklendirilebilir. Domain, organization unit ve ağaç yapıları ile küçük, orta ve büyük ölçekli kurumsal ağ yapılarında uygulanabilir.

Genişletilebilirlik: Dizin hizmeti veri tabanı yapısında artırılıp azaltılabilme

özelliğine sahiptir buda bize genişletilebilme özelliği vermektedir.

Yönetilebilirlik: dizin hizmeti domain'leri sistem yöneticisi tarafından birçok yardımcı yazılımlar ile yönetilebilmektedir.

Domain name system (DNS) ile entegrasyon: Dizin hizmeti, standart bir Internet (TCP/IP) servisi olan domain name sistem ile entegre çalışır.

Politika-tabanlı yönetim: Kullanıcı ve bilgisayarların farklı yapılara göre, domain ya da organization unit içerisindeki işlemlerini kısıtlayan merkezi politikalar düzenlenebilir.

Bilginin kopyalanması (Replication): Dizin hizmeti bilgilerinin sürekliliğini, hataya dayanıklılığını ve yük dengelemesini sağlamak için gelişmiş bir replikasyon teknolojisine sahiptir. Bu sayede domain controller bilgisayarlar arasında domain nesneleri (veriler) kopyalanır.

Güvenlik entegrasyonu: Active Directory, Windows Server 2012 güvenliği ile entegre çalışır. Dizinde yer alan her bir nesne için erişim kontrol edilebilir.

Diğer dizin servisleriyle birlikte çalışabilme: Active Directory LDAP v3 ve NSPI üzerine kuruludur. Bu protokolleri kullanan diğer dizin servisleriyle birlikte çalışabilir. İmzalanmış ve şifrelenmiş LDAP trafiği: Varsayım olarak tüm LDAP trafiği sayısal olarak imzalı (signed) ve şifrelidir (encrypted).

Tek bir noktadan erişim: "Single Sing On". Bir ekran üzerinden ağ sitemine erişimi imkanı ile sistem yöneticilerinin tek bir ekrandan tüm ağ sistemini yönetme imkanı sağlar.Bu imkan sayesinde hata oranı azalmakta ve sisteme hakimiyet oranı artmaktadır.

Delegasyon: Ornanization unit (yapısal birimler) sayesinde sistem yönetimlerinde özelleştirme işlemi yapılabilmektedir sistem biriminde öreneğin bim yapısal birimindeki kullanıcı işlemlerinde yetki devri yapılabilmektedir kullanıcı oluşturma şifre değişiklikleri vb işlemlerde.

5.2.2. Dizin hizmeti (AD) üniversite tasarımı

Organization unit>genel Gurup>Birim Gurup>kullanıcı

a) organization unit

a1) İdari_personel

a1.1) Bilgi_İşlem_DaireBaşkanlığı_gurubu

bidbpersonel1_kullanıcısı

a1.2) Ogrenci_İşleri_DaireBaşkanlığı_Gurubu

oidbpersonel1_kullanıcı

a1.3) Saglık_Kultur_Spor_DaireBaşkanlığı_Gurubu

skspersonel1_kullanıcı

a1.4Strateji_Geliştirme_DaireBaşkanlığı_Gurubu

Sgbpersonel1_kullanıcı

a2) Akademik_Personel

a2.1) Mühendislik Fakültesi-Grubu

a2.1.1Bilgisayar Mühendisliği_Gurubu

a2.1.2Biyomedikal Mühendisliği_Gurubu

a2.2) Edebiyat Fakültesi

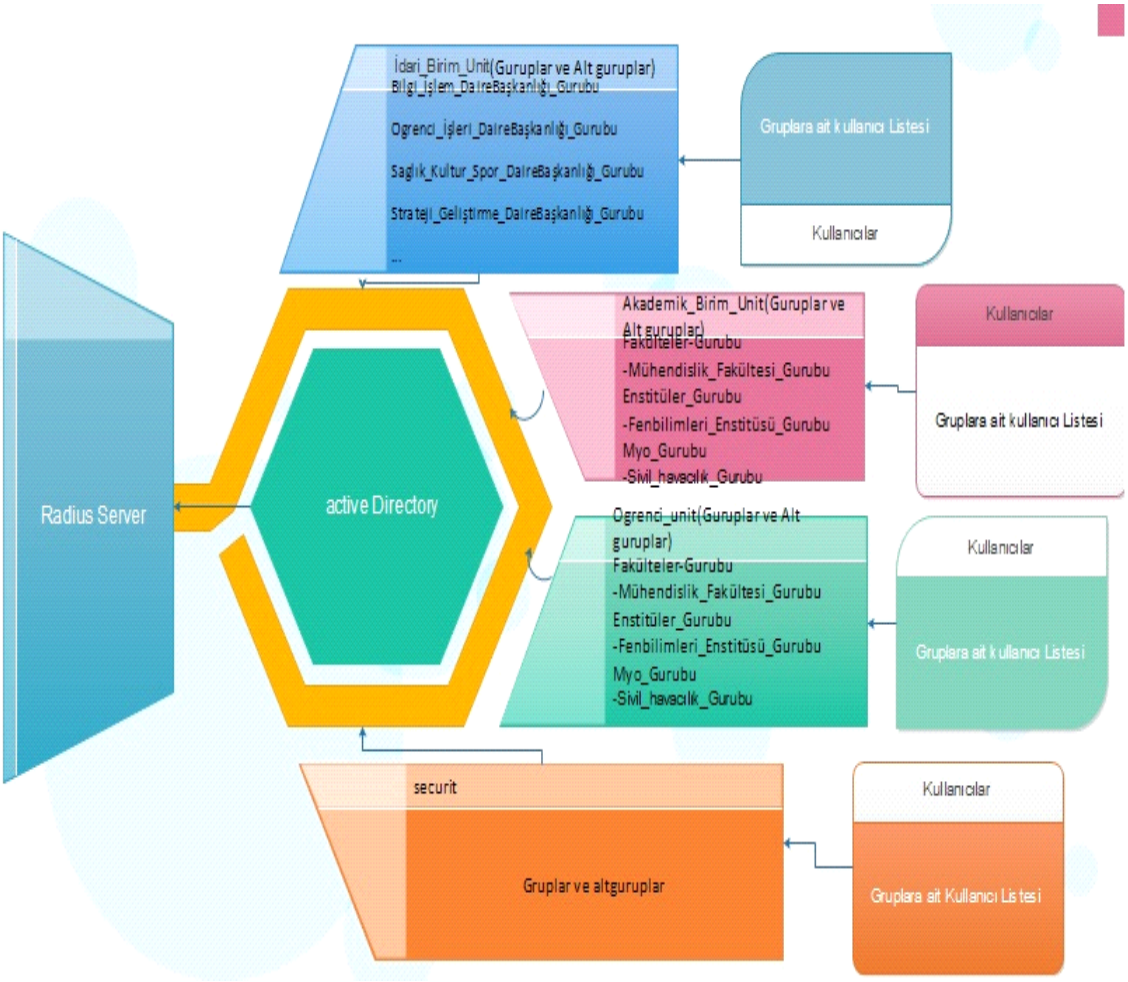
a2.2.1) Edebiyat Bölümü

a2.2.2) Tarih Bölümü

a3) Öğrenci

a4)Bim

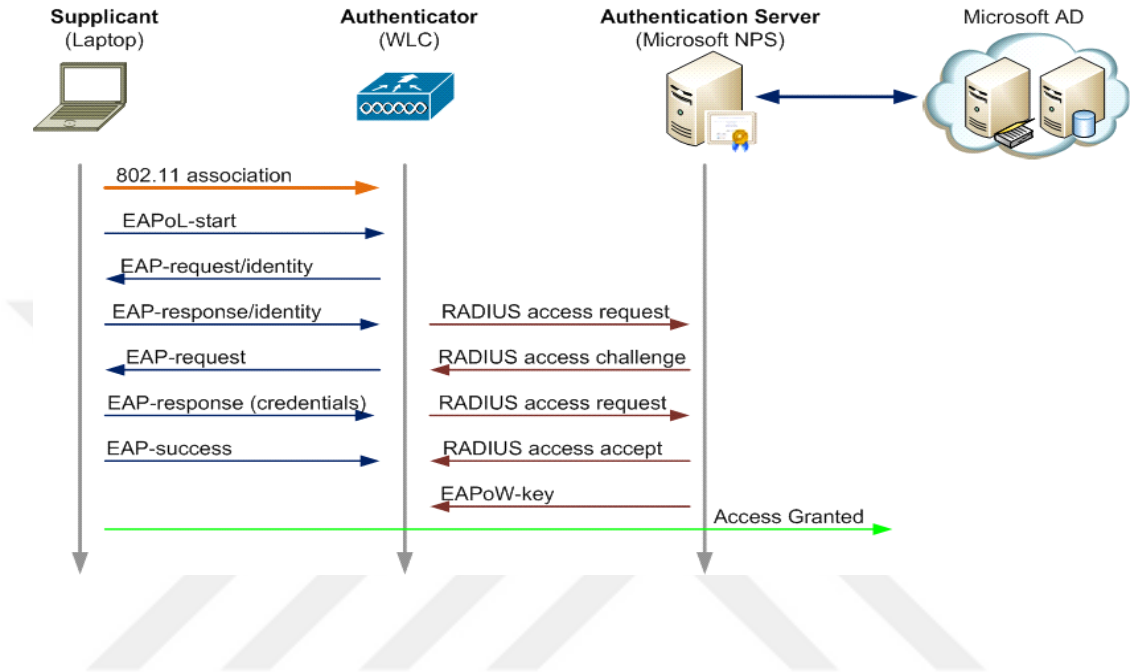
a5)Server



Şekil 5.3: Dizin hizmeti şeması

Active Directory'de kullanıcılar ve guruplar oluşturup her kullanıcının tanımlı olduğu guruba göre yetkilendirme işlemleri gerçekleştirilerek kullanıcıların ağ sistemi üzerinde kendilerine tanınan yetki kadar verilere ulaşım hakkı veya işlem yeteneğine sahip olacaktır.

Dizin hizmeti (ad) üzerinde tanımlanan Grupların kimlik doğrulama ve yetkilendirme sunucusu (NPS)ile haberleşmesi sağlanarak dizin hizmetin de yeralan Kullanıcının dahil olduğu gurubun, NPS sunucusunda Oluşturulan sanal ağlardan dahil olduğu sanal Ağdan ip alması için NPS sunucusun daki vlan tag idleri ile active directory deki tanımlanan grupların eşleştirilmesi gerekmektedir.



Şekil 5.4: dizin hizmeti haberleşme yapısı

5.3. Sertifika hizmeti

Dizin hizmeti sertifika servisi

Dizin hizmeti sertifikası, açık anahtar alt yapısı(public Key Infrastructure-PKI) ile ortak anahtar teknolojilerinden yararlanan ve yazılım güvenliği sistemlerinde kullanılan bir servistir. Dizin hizmeti sertifika servisi(CA)özelleştirilerek açık anahtar altyapısı ile birçok sertifika oluşturmamıza ve oluşturulan sertifikaları yönetmemizi sağlar.

Dizin hizmeti sertifika servis hizmetleri:

Sertifika yetkili servisi (CA)

Sertfika yetkilisi servisi, Sisteme erişim sağlayacak kullanıclara ve erişim sağlayan donanım(bilgisayar, tablet, akıllı telefonlar) chazlarına sertifika taması ve sertfikaları yönetebileceğimiz hizmetleri sağlar.

Çevrimiçi yanıtlıyıcı servisi

Bu servis ise, kullanıcıların talep etmiş oldukları sertifikalar ile ilgili isteklerini kabul etme, iptal etme gibi işlemlerin gerçekleştirilmesinde kullanılır. Sertifikaları değerlendirme süreci sonunda, Online Responder servisi durumu değerlendirir ve istenilen sertifika ile ilgili işlemlerin durum bilgilerini içeren bilgileri imzalayarak geri gönderir.[Url-18]

Ağ aygıtı kayıt hizmeti:

Ağ sistemi içerisinde yer alan yönlendirici ve donanım cihazları ile ilgili sertifika bilgileriniNetwork üzerinde bulunan Routers (Yönlendiriciler) ve cihazlar hakkında ki sertifika bilgilerinin kaydı için kullanılan bir sertifika servis hizmetidir.

Web servisi sertifika ilkesi kayıt hizmeti

Bu servis web servisi içinde sisteme erişim sağlamış kullanıcıların hakkında bilgi veren ve donanım cihazlarının oluşturmuş olduğu sertifika ilkeleri kaydı hakkındaki verilerin incelenmesi için verilen sertifika hizmetidir.

Web hizmeti sertifika kaydı

Sertifika Kaydı Web Hizmeti Sisteme erişim sağlaya kullanıcıların ve donanım cihazlarının(bilgisayar, tablet, akıllıtelefon) HTTPS üzerinden Kimlik kanıtlama protokolü ile sertifikasının kaydının sağlandığı dizin hizmeti hizmet servisidir.

5.4. Kimlik doğrulama ve yetkilendirme sunucusu (RADIUS Server)

RADIUS (Remote Authentication Dial-in User Service) sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama (authentication), raporlama/erişim süresi (accounting) ve yetkilendirme (authorization) işlemlerini yapar. "Livingston Enterprise tarafından geliştirilmiş, daha sonra da IETF RFC 2865 ve RFC 2866 ile standarize edilmiştir. RADIUS client-server modeli tabanlıdır ve mesaj değişimi UDP protokolü ile gerçekleşir. Network Access Server (NAS), RADIUS kullanıcısı olarak davranır ve kullanıcı isteğini RADIUS server'a aktarır. Diğer RADIUS kullanıcıları wireless access point, routerler, ve switchler olabilmektedir."[Url-19]

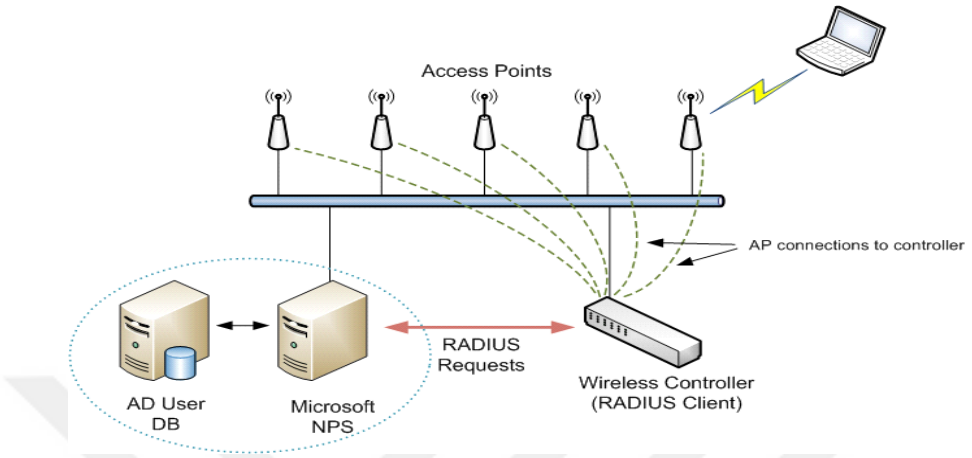
"Kullanıcı ve server arasındaki iletişim private key ile şifrelendirilmiş şekilde gerçekleştirilir, bu sayede şifre asla network üzerinden gönderilmez.Eğer şifreler uyuşmazsa bağlantı sonlandırılır. RADIUS serverlar farklı databaseler'e (örneğin SQL, LDAP) entegre edilebilir authentication methodları kullanır."[Url-19]" RADIUS standartı ilk olarak authentication ve accounting paketleri için UDP 1645 ve 1646 portlarını kullanır. Fakat daha sonra RADIUS standart grubu 1812 ve 1813 portlarını atanmıştır. Tek kullanıcının aynı anda iki bağlantı yapması engellenebilir.Proxy kullanımını destekler"[Url-19]. Radius server olarak Linux tabanlı free Radius server,windows tabanlı network policy server gibi seçenekler mevcuttur.

5.4.1. Ağ ilkesi sunucusu (NPS)Network policy server

Radius server hizmeti üniversite için yapılan tez çalışmasında Windows server Nps hizmeti kullanılmıştır. Ağ İlkesi Sunucusu (NPS), istemci sistem durumu, bağlantı isteği kimlik doğrulama ve bağlantı isteği yetkilendirme işlemleri için üniversite genelinde ağ erişim ilkeleri oluşturulmuştur.Ağ İlkesi Sunucusu, Sisteme erişim Sağlamak isteyen Kullanıcının Uzaktan Kimliğini Doğrulama Hizmeti (RADIUS) sunucusu ve proxy'sinin bir Microsoft uygulamasıdır. Ağ erişimininde, Kablosuz erişim noktaları için 802.1X kimlik doğrulama anahtarlarını içeren değişik ağ erişim sunucularından, merkezi olarak yönetmek için Ağ ilkesi sunucusu kullanılmış ve buna ek olarak, kablosuz bağlantılar için Korumalı genişletilebilir Kimlik Doğrulama

Protokolü (PEAP),MS-CHAP v2 ile güvenli parola doğrulaması dağıtmak için NPS'yi kullanılmıştır.

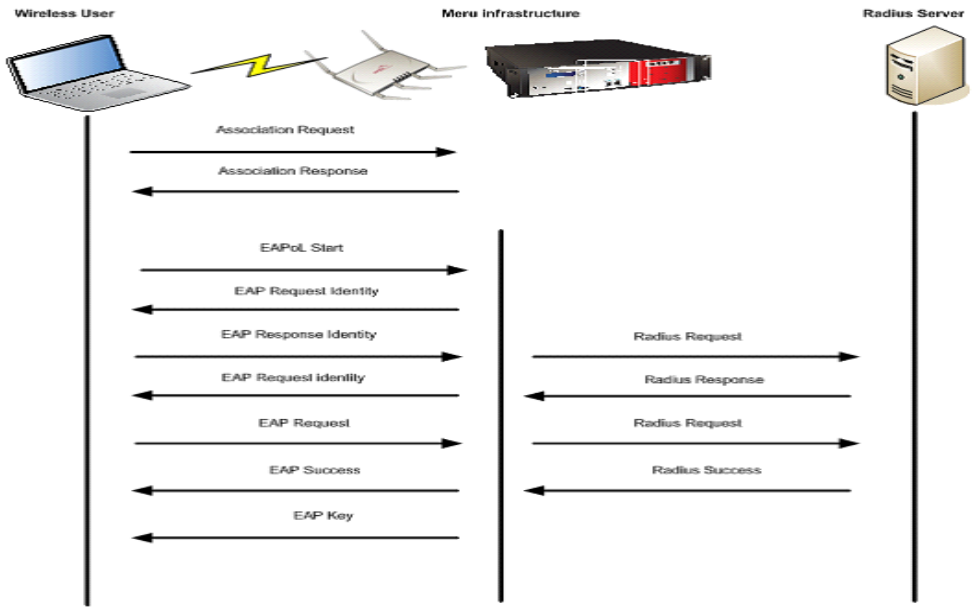
5.5. Erişim noktası kontrolörü



Şekil 5.5: Erişim noktası kontrolörü

Erişim Noktası (accespoint) kablosuz ağ sistemi içerisinde hizmet Takımı tanıtıcısının(Ssid) Yayınlandığı Donanım cihazdır. Erişim Noktası cihazları farklı teknolojide birçok özellik barındırmaktadır günümüzde, bir erişim Noktası cihazına ortalama 40-50 Kullanıcı anlık olarak erişim sağlayabilmektedir. Kullanıcıları kablosuz ağ sistemine dâhil olabilmeleri için erişim Noktası cihazı üzerinde yayınlanan Ssid bilgisayar, tablet, akıllı cihazlar vasıtası ile erişim isteğinde bulunarak kablosuz ağ sistemine dâhil olabilmektedir.

Erişim Noktası kontrolürü, üniversite içerisinde yer alan erişim Noktası cihazlarının tamamını kontrol etmek, yönetmek, raporlamak ve erişim Noktası cihazlarına sisteme Bağlantı isteği iletildiği zaman 802.1x standardın'da kablosuz ağ kapsamı içerisinde hangi Yapılandırmadan etkileneceğini belirttiğimiz donanım cihazdır. Kablosuz ağ sistemi içerisinde üniversite de mevcut olarak kullanılan 250 'nin üzerinde erişim Noktası cihazı bulunmaktadır erişim noktası kontrolü yönetimi sayesinde erişim Noktası kontrolür cihazı üzerindeki yapılan konfigürasyondan tüm erişim Noktası cihazları etkilenmektedir. Bu sayede her bir erişim Noktası cihazı için ayrı ayrı yapılandırma yapılmasına ihtiyaç kalmamaktadır. Diğer önemli bir nokta ise yapılan yeni bir konfigürasyonda veya güncellemede tüm erişim noktası cihazları da güncellenmektedir.



Şekil 5.6: Erişim noktası kontrolorü kullanıcı, erişim noktası ve Nps (Radius sunucu)arasındaki iletişim

Şekil 5.6'da kablosuz ağ sistemine kullanıcı tarafından istek erişim noktası cihazına iletilmektedir Erişim noktası cihazı ise bu iletiyi Erişim Noktası kontrolör cihazına ileterek, Erişim noktası kontrolör cihazı ise Radius sunucu yani ağ hizmeti sunucu ile haberleşerek doğrulam işlemi yapmaktadır. Tabloda kullanıcı, erişim noktası, erişim noktası kontrolör ve Radius sunucu arasında iletişimi göstermektedir.Yapılan çalışmada erişim noktası kontrolörü üzerinde sanal ağ yapısı oluşturulmuş. Sanal ağların Ağ ilkesi sunucusu(Radius sunucu) ve Güvenlik duvar cihazı ile haberleşmesini sağlanmıştır. Authentication (kimlik doğrulama) 1812 portu ve internete erişimi sağlanmış aynı zamanda da 1813 Radius Accounting (Kullanıcının takip edilebilmesi) portundan gelen veriler ile de tanımladığımız kullanıcıların 5651 sayılı kanuna göre kullanıcı yaptığı işlemleri kayıt altına alınması.

Radius profile	(NPS)Radius ip adresi	Radius secret	Radius port
Authentication(kimlik doğrulama)	192.168.240.56	********	1812
Accounting(kullanıcınıntakip edilebilmesi)	192.168.240.56	********	1813

Çizelge 5.2 Erişim noktası kontrolör ’in Radius profile tasarımı

Çizelge 5.2 de erişim noktası kontrolür için Radius profile tasarımı oluşturulmuş Ağ ilkesi sunucunu ile iletişim kurabilmesi için ip adresi ve iletişim esnasında kullanılacak olan şifre ve port numaraları belirlenmiş ve tasarı oluşturulmuştur.

5.5.1. SSID (Service set identifier - Hizmet takımı tanıtıcısı)

Her kablosuz yerel Alan ağı (WLAN), kendini tanımlamak için benzersiz bir ağ adı kullanır. Bu ada SSID (Service Set Identifier - Hizmet Takımı Tanıtıcısı) de denir. WiFi bağdaştırıcınızı kurduğunuzda SSID değerini belirtmeniz gerekir. Varolan bir WLAN'a bağlandığınızda, bu ağın adını kullanmak zorundasınız. Kendi WLAN ağınızı kuruyorsanız, kendinize göre bir ad belirleyip her bilgisayarda bu adı kullanmanız gerekir. Ad için, harflerden ve sayılardan oluşan en çok 32 karakter kullanabilirsiniz. SSID ya da ağ adı, erişim noktasında ya da kablosuz yönlendiricide atanır.

Üniversite’de öğrencilerin,personellerin ve misafirlerin kablosuz ağa bağlanması için erişim noktası kontrolörü cihazından fsmk adı ile bir Ssıd yayınlanmış ve yayınlanan Ssıd den ağa erişmek isteyen kullanıcıların ,802.1x standardına göre kullanıcı adı ve şifresi doğrulandıktan sonra farklı sanal ağlara atanması ve kullanıcıların güvenliği ,üniversitenin kablosuz ağ güvenlik politikalarına göre sisteme erişim sağlanmıştır.

5.5.2. Erişim kontrolü üzerinde 802.1x Standardı için sanal ağ tasarımı

Üniversitenin kablosuz ağ içerisinde kullanıcı gruplarının güvenlik seviyelerine göre ayrı sanal ağlar oluşturmak ve bu sanal ağlardan sisteme erişebilmesi için her ağın içerisinde tanımlanması gereken bazı yapılandırmalar yapılması gereklidir.Öncelikle ağ sistemleri içerisinde her sanal ağın bir sanal ağ ismi (vlan ismi) ve sanal ağ numarası (tagid) tanımlanmalıdır, tanımlanan bu isimleri ağ sistemi içerisinde iletişim sağlandıktan sonra sanal ağ ile yapılacak işlemleri vlan numarası yani tag idler üzerinden dizin hizmeti (ad), güvenlik duvarı (firewall) ve erişim noktası kontrolürü(acces point controller) ayrı ayrı ağlar olduğu belirlenmiş olur.

Kullanıcının kablosuz ağ sistemine istek gönderdikten sonra sanal ağ üzerine bir ip adresi alarak kablosuz ağa dahil olacaktır bu ip adresin sınıfı (netmask) geçici ağ (default gateway) ve ip adreslerinin başlangıç noktaları itibariile dağıtımı için dhcp server tanımlanması gerekmektedir. vlan isimleri,tag id leri, ip adresleri, net mask, default gateway ve dhcp sunucu belirlenip diğer 802.1x standardı kapsamında yapılandırılan yazılım ve donanım cihazları ile haberleştirilmesi için analizler yapılmış ve bu analizler neticesinde Tasarı oluşturulmuştur.

Çizelge 5.3 Sanal ağ tasarımı

Vlan isim	Tag id	Ip adres	netmask	Default gateway	Dhcp server
Ogrenci_test	2000	10.10.0.2	255.255.255.0	10.10.0.1	10.10.0.1
Akademi_Test	2001	10.10.1.2	255.255.255.0	10.10.1.1	10.10.1.1
Bim_Test	2002	10.10.2.2	255.255.255.0	10.10.2.1	10.10.2.1
İdari_Test	2003	10.10.3.2	255.255.255.0	10.10.3.1	10.10.3.1
Server_test	2004	10.10.4.2	255.255.255.0	10.10.4.1	10.10.4.1

5.5.3. Security profile

Çizelge 5.4 Güvenlik profil tasarımı

Secret profile ismi	Model	Data Encript	Radius profil ismi
FSMK_Güvenlik_Profili	802.1x	********	Authentication(Kimlik Doğrulama

Figür 5.4 Erişim noktası kontrolör Güvenli profil kısmında oluşturacağımız güvenlik profilinin ismi, uygulayacağımız güvenlik methodunu, veri şifreleme metodolojisini, tasarımı oluşturulmuştur.

5.5.4. ESS profile

SSID (Service set identifier - hizmet takımı tanıtıcısı)

Üniversite kablosuz ağ kullanıclıların 802.1x standardı ile sisteme erişim sağlayabilmeleri için oluşturacağımız kablosuz yayının ismi ve bu isimden sisteme bağlanan kullanıcıların 802.1x standardı kapsamında etkileneceği özellikleri için oluşturulan hizmet tanıtıcısı tasarımı;

Çizelge 5.5: Hizmet takımı tanıtıcısı tasarımı

ESS Profil ismi	Aktif olma bilgisi	Hizmet takımı tanıtıcı ismi	Güvenlik görüntü ismi	Broadcast	Bağlantı bölge tipi	Veri bağlantı	Yönetici
FSMK	Enable	FSMK	FSMK_Güvenlik profile	On	Radius vlan only	Tunnel	controlur

6. IEEE 802.1X STANDARDININ TEZ ÇALIMASINDA KULLANILAN MATERYELLERIN KURUMU VE YAPILANDIRILMASI

6.1. IEEE 802.1X Standardının dizin hizmeti (Active directory) kurulumu

Windows Server işletim sistemi üzerinde, dizin hizmeti kurulumunu iki şekilde yapılabilmektedir birinci yöntem server manager yönetim aracılığı ile kurulum, Diğer bir yöntem ise PowerShell komut alanı ile kurulumlar gerçekleştirilebilmektedir.

C:\>Get-Windowsfeature |Where Installed -Eq True

Dizin hizmeti kurulumuna ilk önce dizin hizmeti özelliklerin kurulumu ile başlanmış ve bu işlem için windows powershell komut satırı ekranı üzerinde iken,

Add-windowsfeature ad-domain-services komutunu çalıştırarak dizin hizmeti domain servisi ile ilgili özellikler'in kurulumunu gerçekleştirildi.

C:\>Add-Windowsfeature AD-Domain-Services.

Dizin hizmeti kurulumu için ön hazırlıkları tamamlamış ve dizin hizmeti domain yapısını kurmak için windows powershell ekranı üzerinde aşağıdaki komut devreye alınıştır.

C:\> Install-Addsforest

-Creatednsdelegation: $False `

-Databasepath "C:\Windows\NTDS" `

-Domainmode "Win2012" `

-Domainname "FSMK.Local" `

-Domainnetbiosname "FSMK" `

-Forestmode "Win2012" `

-Installdns: $True `

-Logpath "C:\Windows\NTDS" `

-Norebootoncompletion: $False `

-Sysvolpath "C:\Windows\SYSVOL" `

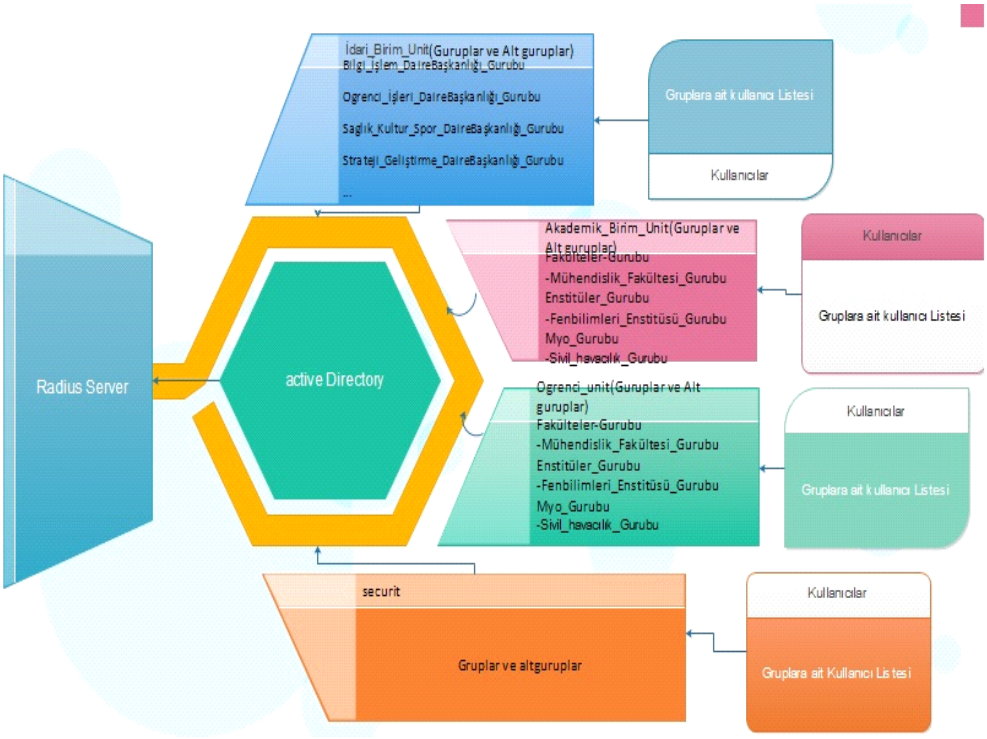
-Force: $True

Komutun çalıştırılmasının ardından user name ve password bilgilerini girimiş ve kurulum tamamlandıktan sonra sistem yeniden başlatılmıştır.

Dizin hizmeti üniversite kablosuz ağ çalışması yapılandırılması

Üniversitenin genel yapısı itibari ile analizler yapılmış ve 5.2.3 konusunda tasarımı ve şeması oluşturulan 802.1x standardı için üniversite genel yapıda oluşturulması planlanan dizin hizmeti yapısı aşağıdaki şekilde tez çalışmasında oluşturulmuştur.

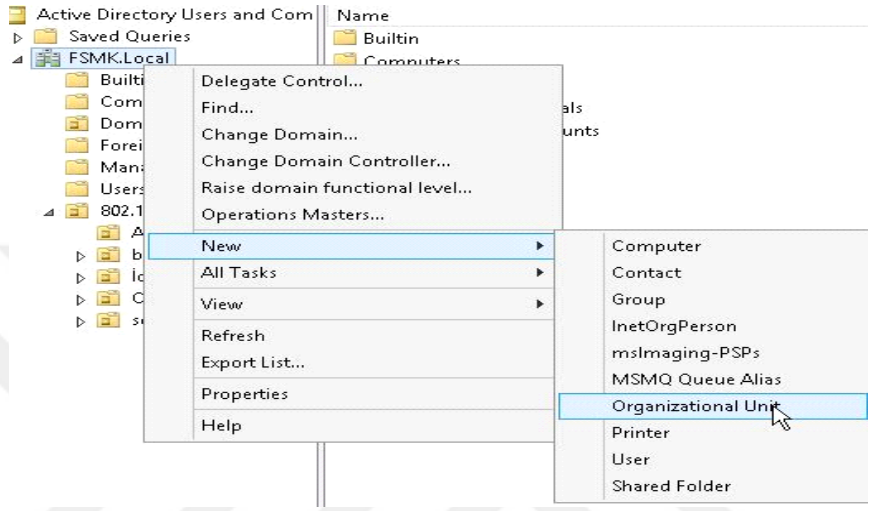
Çizelge 6.1 Dizin hizmeti tasarımı



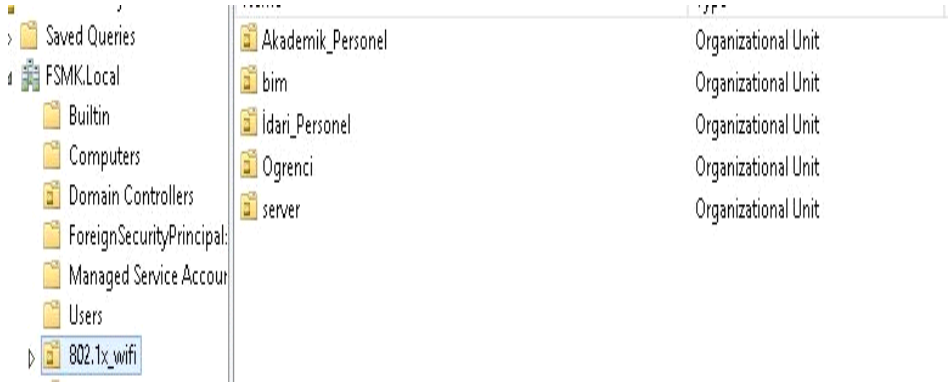
Dizin hizmeti üzerinde organization unit oluşturma

Bu bölümde analizde tespit edilen organization unitleri oluşturulmuştur.

İşlem fsmk. local üzerinde sağ click >new>organization unit>Name



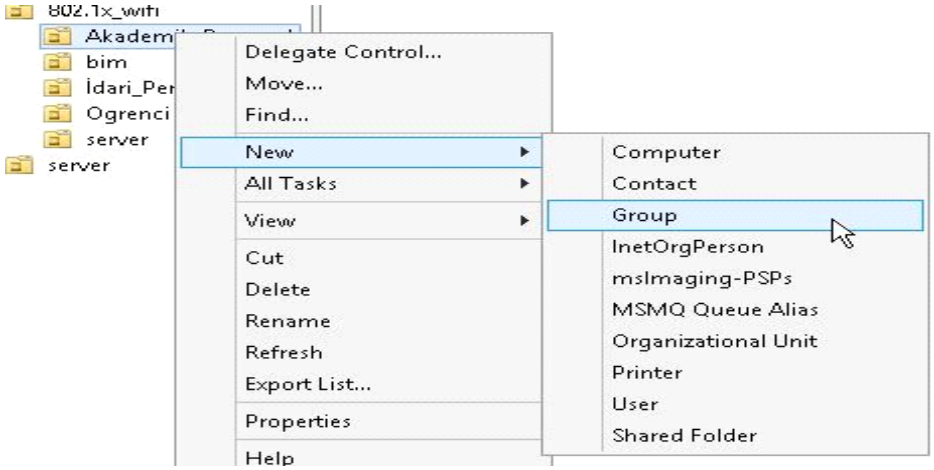
Şekil 6.1: Dizin hizmeti organization yeni organizational unit oluşturma ekranı



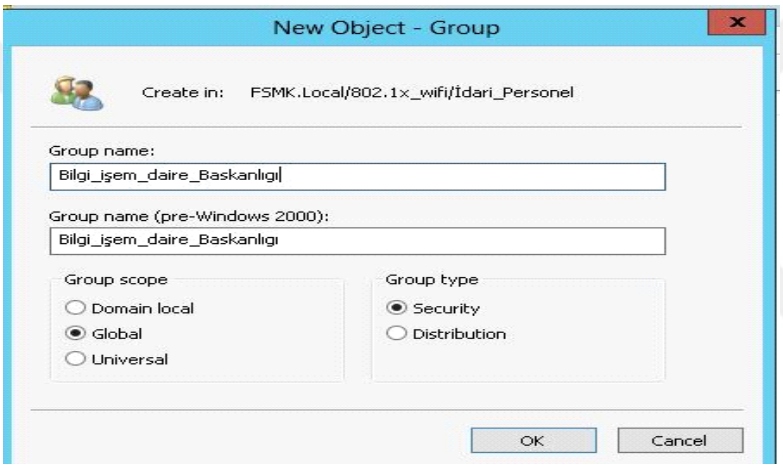
Şekil 6.2: Dizin hizmeti üzerinde oluşturulan organization unit listesi

Dizin hizmeti (AD) de grup oluşturma

Organization unit sağ click>new>grup>name

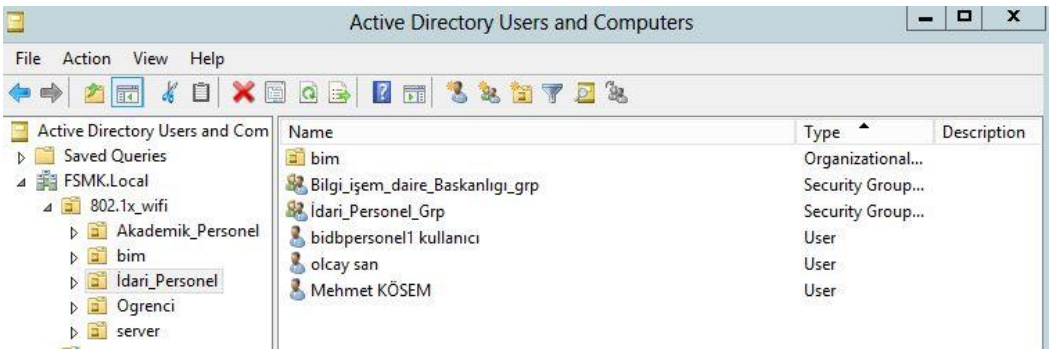


Şekil 6.3: Dizin hizmeti yapılandırma yeni gurup ekranı1



Şekil 6.4: Dizin hizmeti yapılandırma yeni gurup oluşturma ekranı 2

Şekil 6.4 Dizin hizmeti üzerinde bilgi işlem daire başkanlığı grup oluşturulmuş bu grubun kapsamı global ve group türünün güvenlikli olduğu belirtilmiştir.

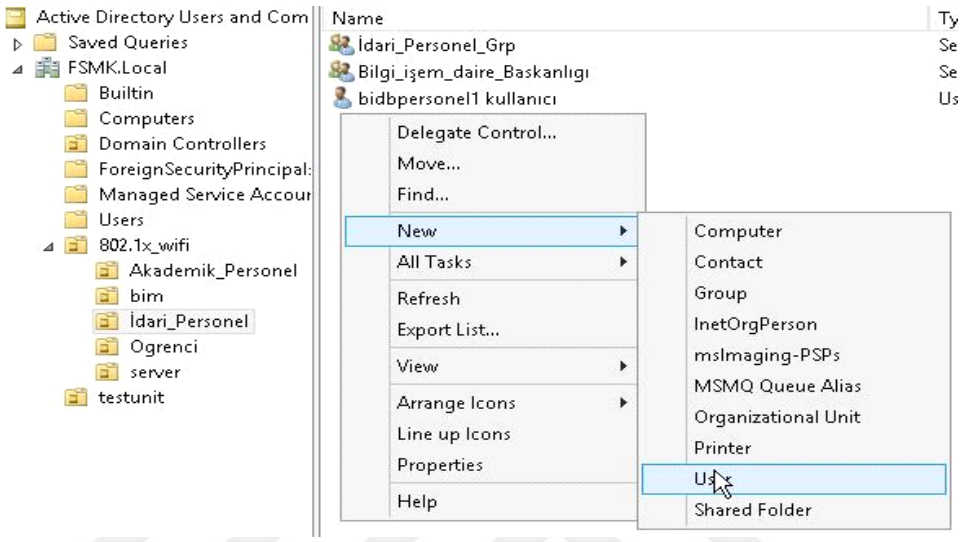


Şekil 6.5: Dizin hizimeti üzerinde oluşturulan grup listesi ekranı

Şekil 6.5 de dizin hizmeti gurup listesinde oluşturduğumuz Bilgi_işlem_daire_ başkanlığı gurubunun listede yer aldığı görülmektedir.

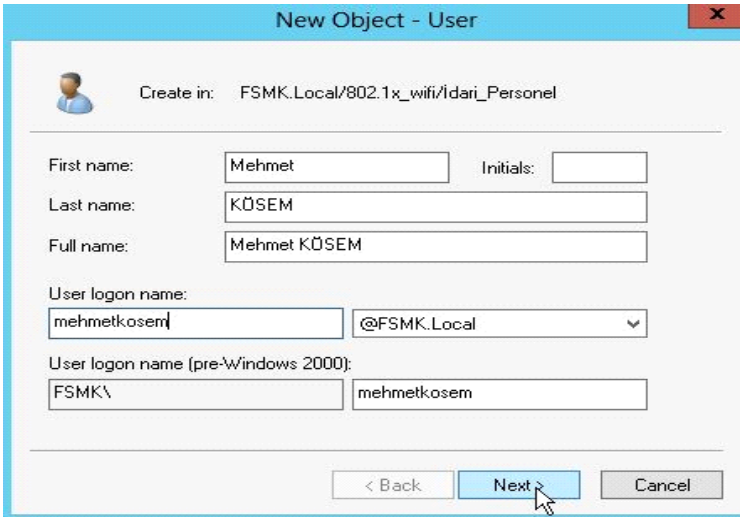
Dizin hizmetin (AD)'de kullanıcı oluşturma

Organization unit sağ click>new>user>name



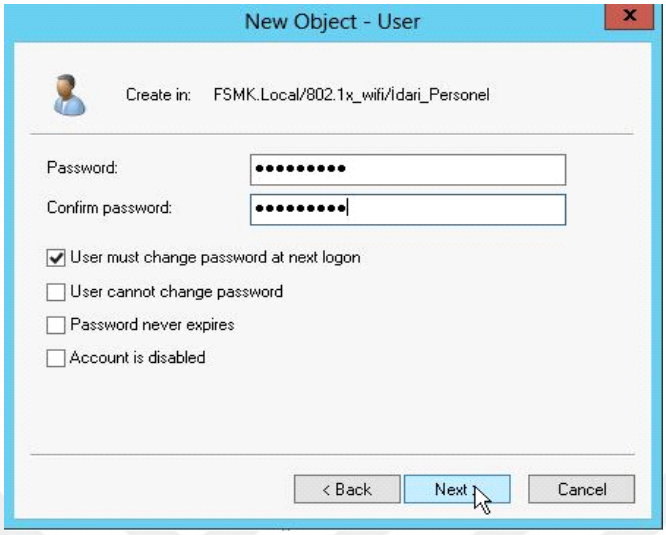
Şekil 6.6: Dizin hizmeti yapılandırılması yeni kullanıcı oluşturma ekranı-1

Şekil 6.6'da Dizin hizmeti yapılandırılması yeni kullanıcı ekranında oluşturulmak istenen kullanıcı organization unit üzerine gelip fare ile sağtuş yeni seçeneği seçilmiş buradanda oluşturulacak olan yeni işlem listesinde kullanıcı seçilmiştir.



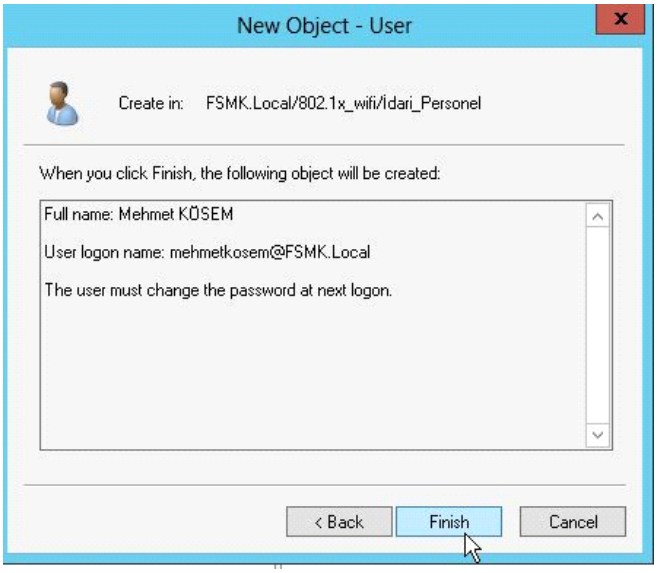
Şekil 6.7: Dizin hizmeti yeni kullanıcı bilgilerinin oluşturma ekranı

Şekil 6.7 de Dizin hizmeti yapılandırılmasında yeni kullanıcı ekranından oluşturulan kullanıcının isim, orta ismi, soy ismi, tüm adı, sisteme bağlanacığı isim ve hangi domain adresinden bağlanacağı kulanıcı bilgileri oluşturulmuştur.



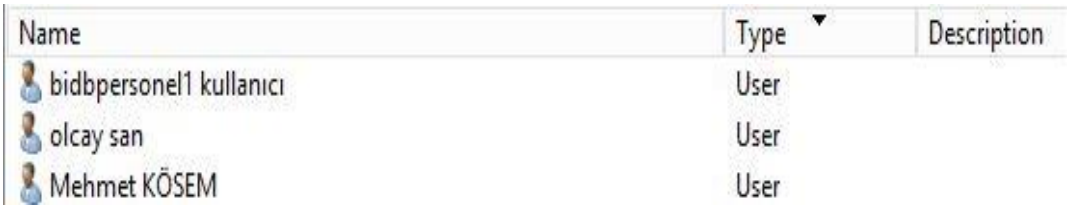
Şekil 6.8: Dizin hizmeti yapılandırma yeni kullanıcı şifre oluşturma ekranı

Şekil 6.8 de oluşturulan kullanıcının sisteme bağlanırken kullanacağı geçişi şifresi oluştulmuştur.



Şekil 6.9: Dizin hizmeti yapılandırma yeni kullanıcı oluşturma kontrol ekranı

Şekil 6.9 da oluşturulan kullanıcının sisteme bağlanacağı alanın, tüm isminin ve kullanıcını sisteme bağlandıktan sonra zorunlu olarak şifresini değiştirileceği bilgilerin kontrolü sağlanmıştır.



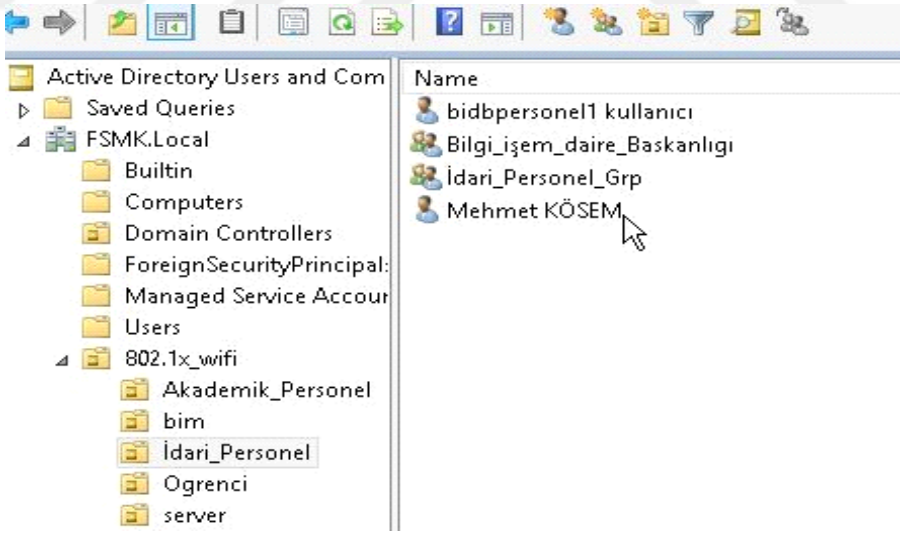
Şekil 6.10: Oluşturulan kullanıcı listesi

Şekil 6.10 da Dizin hizmetinde oluşturulan kullanıcı, kullanıcı liste ekranında Mehmet KÖSEM listede yer almaktadır.

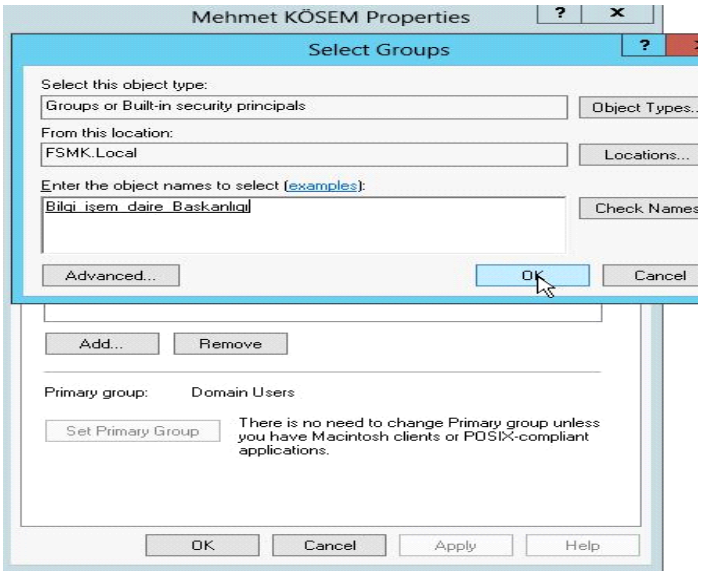
Dizin hizmetinde kullanıcıyı ilgili gruba atama işlemi

Kullanıcıyı ilgili gruba atama işlemi

Kullanıcı üzerinde enter>member of tabı seçilip >add>select grup>ok



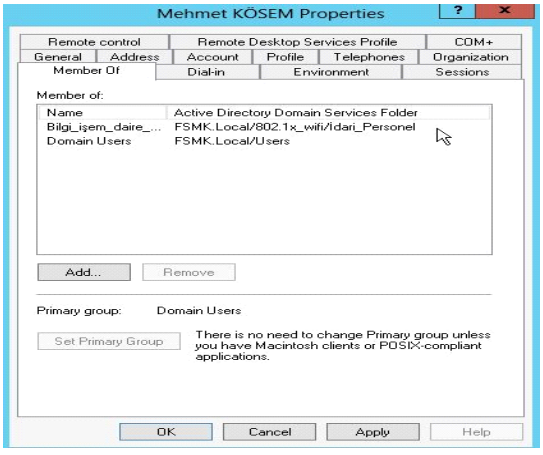
Şekil 6.11: Dizin hizmeti yapılandırma kullanıcı liste ekran



Şekil 6.12: Dizin hizmeti yapılandırma kullanıcının ekleneceği gurup listesi ekranı

Şekil 6.12 de seçilen kullanıcının hangi guruba dağil edileceğini belirlendiği ve 802.1x satandardı üniversite tasarımında en önemli işlemdir.

Kullanıcıların sisteme bağlandıktan sonra tüm işlemin guruplar üzerinde devam edildiği bir yapıda kullanıcının yanlış bir guruba dağil edilmesi dahil edildiği gurubun tüm yetkilerine sahip olması anlamına gelmektedir .mehmet kösem kullanıcısının bilgi işlem daire başkanlığı gurubuna eklenmiştir.

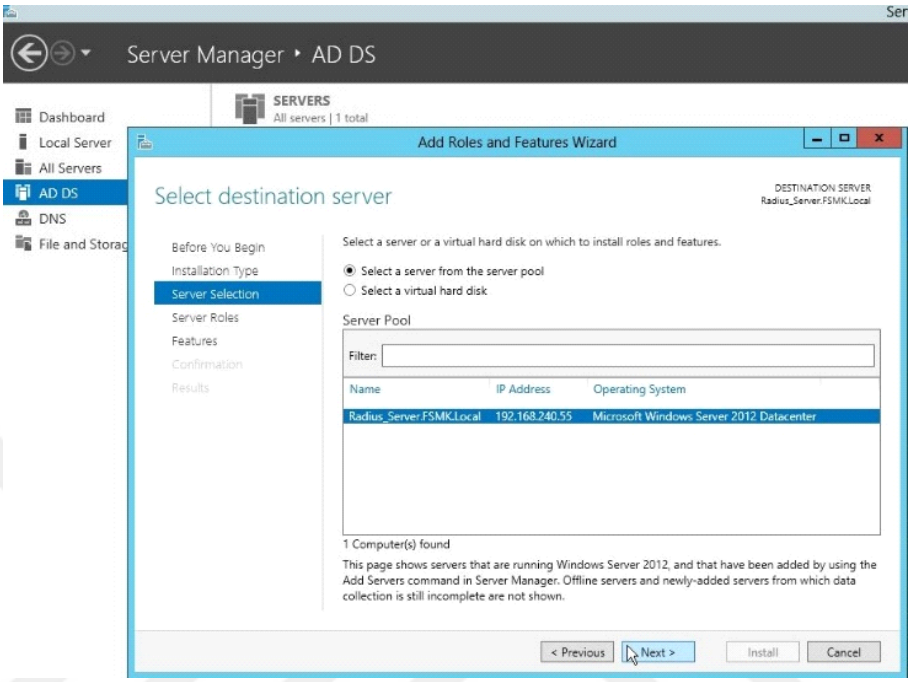


Şekil 6.13: Dizin hizmeti yapılandırma kullanıcının dahil olduğu gurup ekranı

Şekil 6.13 de işleme alınan kullanıcının dizin hizmeti üzerindeki özelliklerini ve bu özelliklerini değiştirebileceğimiz gurup ekranı yer almaktadır.

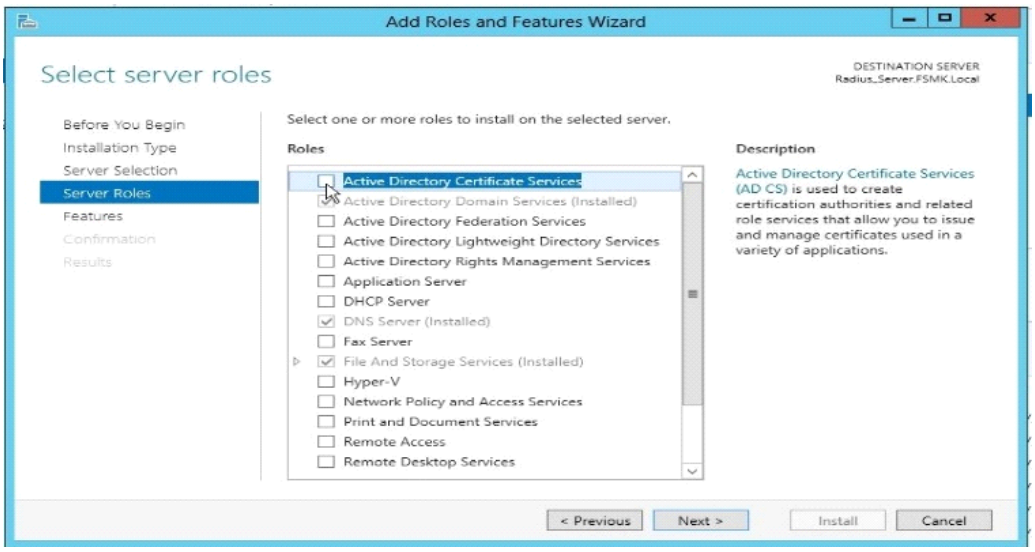
6.2. Sertifika (AD CS) kurulumu

Windows Server işletim sistemi üzerinde dizin hizmeti sertifika servisi kurulumu sunucu yöneticisi yönetim konsolunu ile gerçekleştirilmiştir.



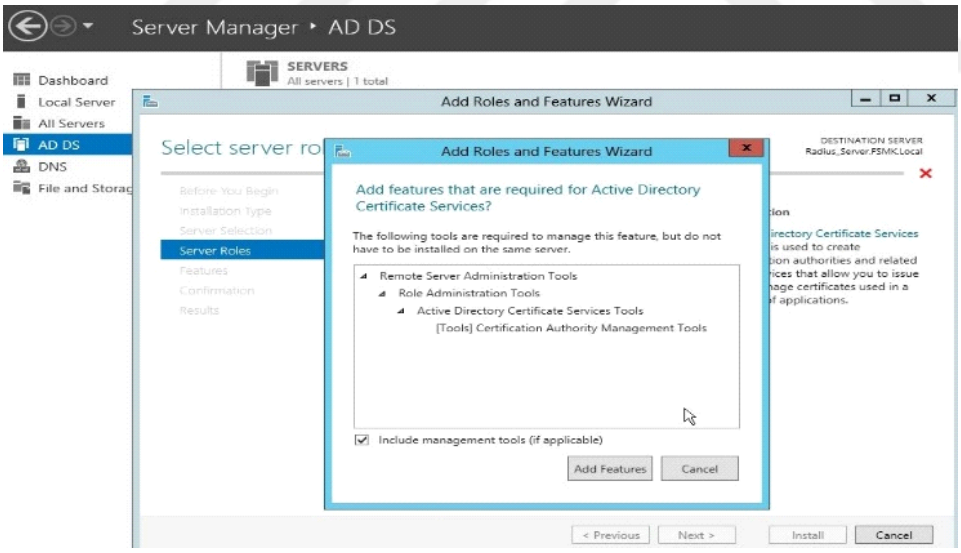
Şekil 6.14: Kurulacak sertifikanın yükleneceği sunucunu belirleme ekranı

Şekil 6,14 de Kurulumu mevcut Radius (Ağ ilkesi) sunucusunun üzerinde gerçekleştirdiğim için seçenekler arasından Sunucu havuzundan bir sunucu seçin seçeneğini seçilmiştir, listelenen sunucu ekranından kurmuş olduğumuz ağ ilkesi sunucusu üzerine kurulum yapacağımızı belirtmiş ve bir sonraki işleme geçilmiştir.



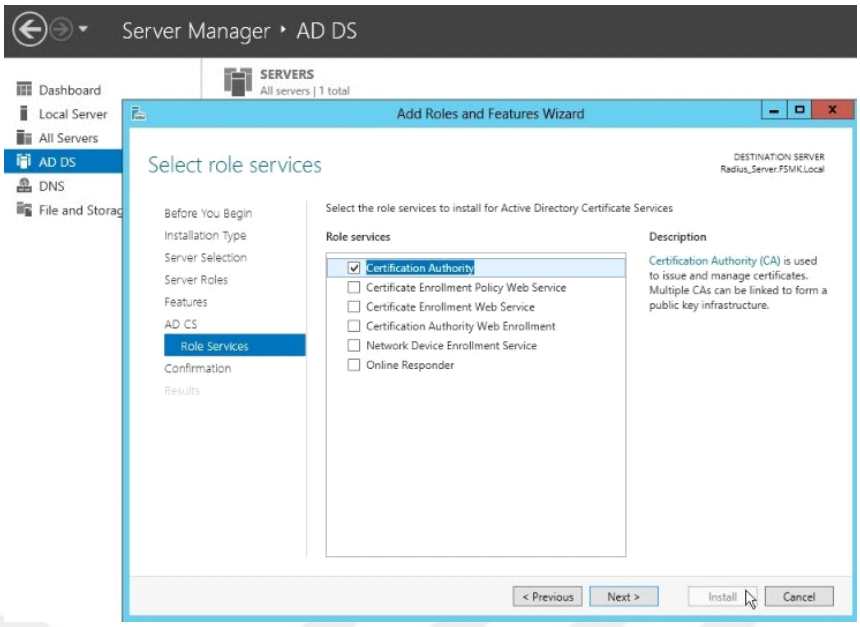
Şekil 6.15: Dizin hizmeti sertifika servisi kurulum başlangıç ekranı

Şekil 6.15 de Dizin hizmeti sertifika servisinin kurulumunu gerçekleştireceğimiz için ilgili seçeneği seçilmiştir.



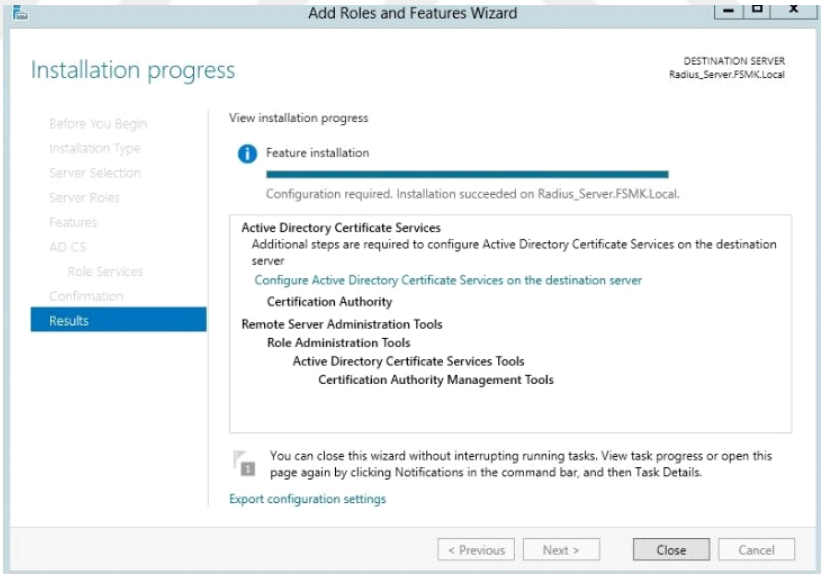
Şekil 6.16: Sertifika özellikleri ekleme ekranı

Şekil 6.16 ‘da dizin hizmeti sertifika servisinin yüklenecek özellikleri listelenmektedir özellikleri ekle seçeneği seçilmiş ve işleme devam edilmiştir.



Şekil 6.17: Sertifika yetkilisi ekleme ekranı

Şekil 6.17'de Dizin hizmeti sertifikası ile sertifika yetkilisi rolünü beraber kurulumunu yapılmıştır. Sertifica yöneticisi servisini seçilmiş ve işleme devam edilmiştir.

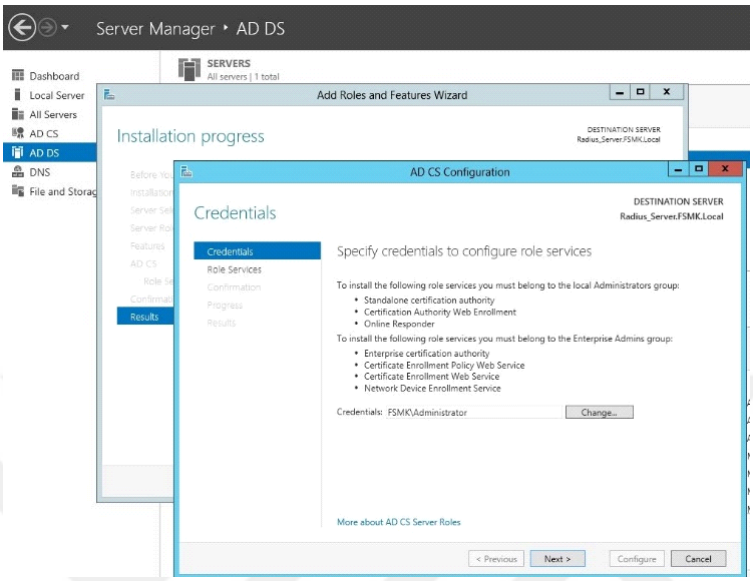


Şekil 6.18: Sertifika kurulumu bitiş ekranı

Şekil 6.18'de Sertifika sunucusu için gerekli özellikler belirlendikten sonra yükle seçeneği seçilmiş ve kurulum işlemi bitirilmiştir.

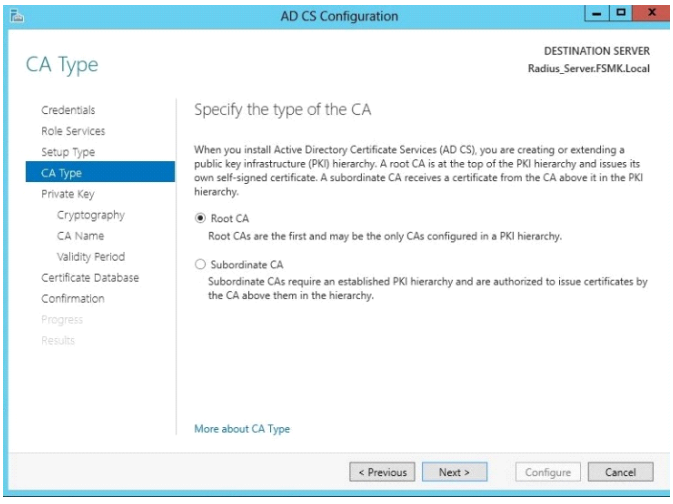
6.2.1. Sertifika (AD CS) yapılandırma

Serfika servis yapılandırma işlemine için sunucu yönetici ekranından Configure Active Directory Certificate Services on the destination server ‘a seçilmiştir.



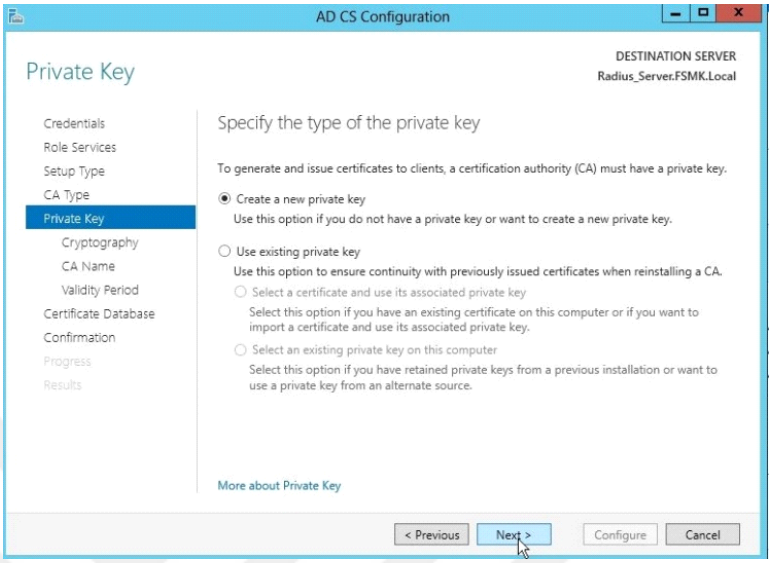
Şekil 6.19: Sertifika üyelik işlemleri ekranı

Şekil 6.19’da sertifika üyelik işlemleri yapılandırma işleminde, kurulumunu yapmak istediğimiz rol ve servislerin Yerel yönetici grup ve kuruluş yönetici gruplarına üye yapılması gerektiğine dair bize bilgi verilmekte. Bu üyeliklerin kimliğini FSMK\Administrator olarak belirlenip üyelik işlemlerini gerçekleştirilmiştir.



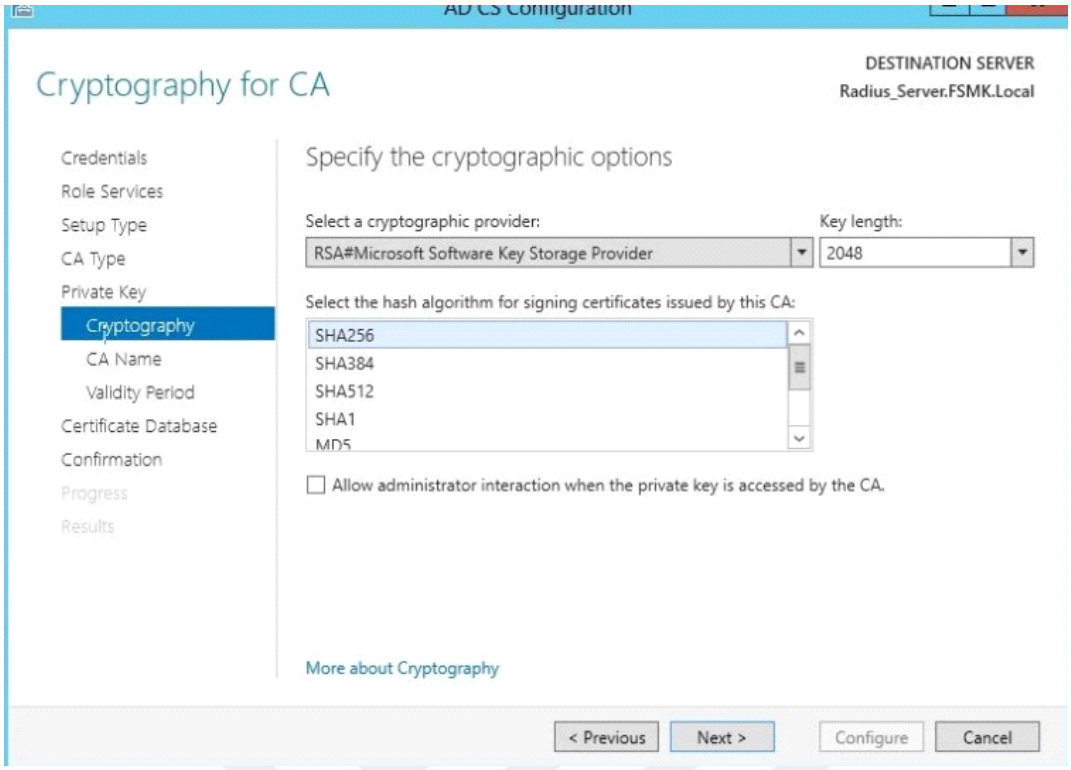
Şekil 6.20: Kök sertifika oluşturma ekranı

Şekil 6.20'de Sertifika servisin kurulum türünü belirlendiği bu alanda iki tip sertifika servis seçeneği mevcuttur. İlkez sertifika kurulumu gerçekleştireği için kök sertifika servis seçilmiş ve yapılandırmaya devam edilmiştir.



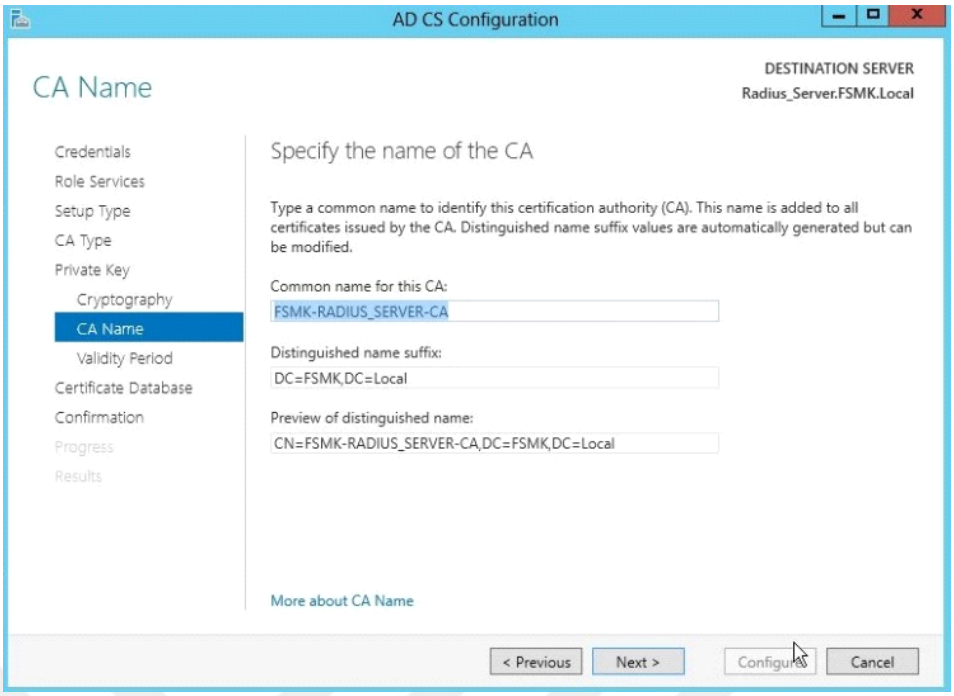
Şekil 6.21: Sertifika yeni özel anahtar olşuturma ekranı

Şekil 6.21'de Özel anahtarın türünü belirtilen bu alanda iki seçenkek karşımıza çıkmaktadır, sertifika servis sunucusundan sertifika talebinde bulunan Kullanıcı donanım cihazları (Bilgisayar,tablet,akıllı telefon gibi cihazlar) için daha önceden oluşturulmuş özel anahtarı olmadığı için Yeni özel anahtar oluştur seçeneği seçilerek işleme devam edilmiştir.



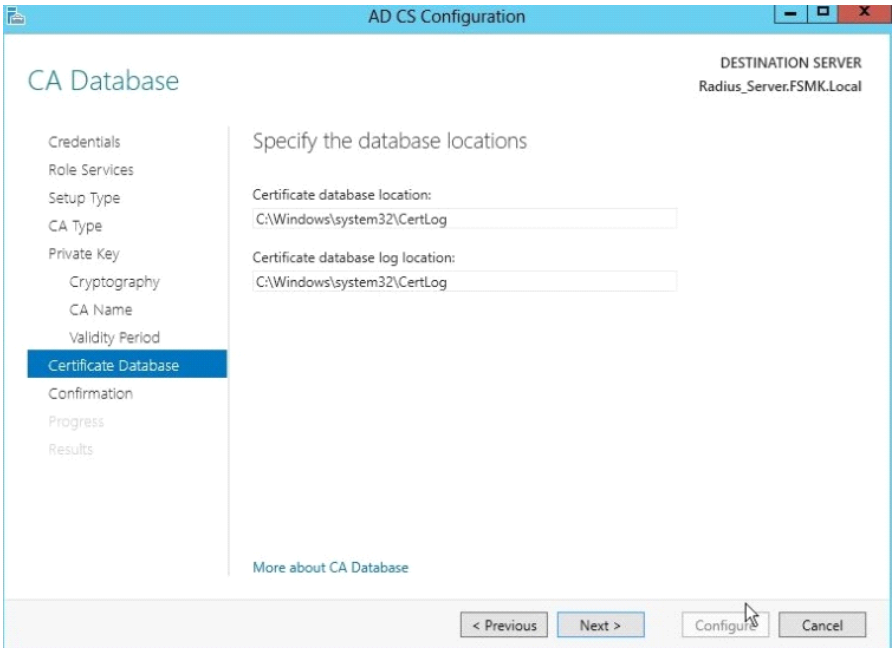
Şekil 6.22: Sertifika şifreleme protolü ekranı

Şekil 6.22'de Kriptografik seçeneklerin belirlendiği bu alanda, oluşturulacak olan özel anahtar için şifreleme protokolünü belirlenmiş. Oluşturulacak olan özelanahtarın, default olarak SHA256 algoritması ile şifreleneceği, anahtar uzunluğunun 2048 olacağı ve kripto sağlayıcısının RSA olarak belirlenmiş ve işleme devam edilmiştir.



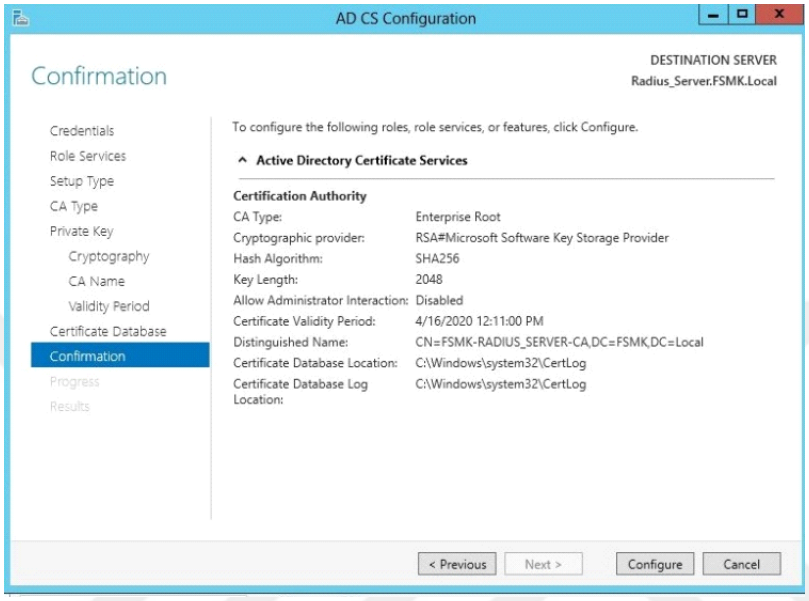
Şekil 6.23: Sertifika ismi belirleme ekranı

Şekil 6.23'deSertifika isminin belirlendiği bu alanda, sertifika servis sunucusuna erişim sağlayacak olan kullanıcıların donanım cihazlarında kullanacakları sertifika için FSMK-Radius ismi tanımlanmış ve sertifika süresinin 5 yıl olarak belirlenmiştir.



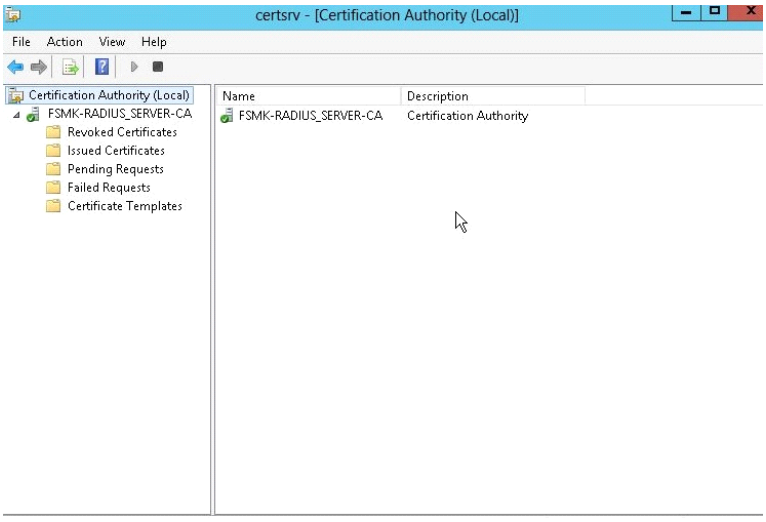
Şekil 6.24: Sertifika veritabanının tutulduğu alan bilgileri ekranı

Şekil 6.24'de Veritabanı yerlerinin belirlendiği bu alanda, veritabanı dosyalarının depolandığı Alan bilgileri yer almaktadır. İstenildiği takdirde veri tabanının tutulacağı alan ve veri tabanı log kayıtlarının tutulacağı alan kurulum esnasında değiştirilebilmektedir yapılan çalışmada değişikğe gerekduyulmadığı için yapılandır seçeneği seçilerek işleme devam ettirilmiştir.



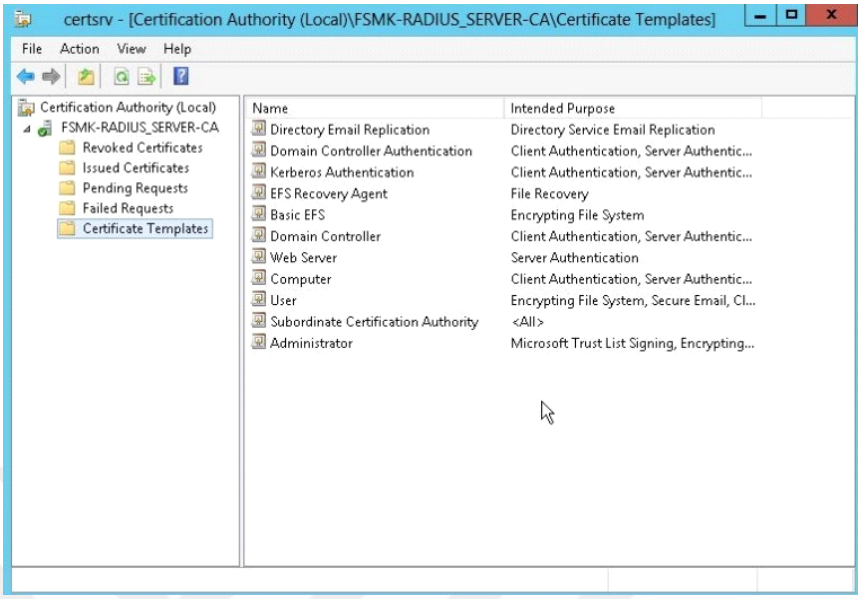
Şekil 6.25: Sertifika özet bilgileri ekranı

Şekil 6.25'de Yapılandırma ekranında, oluşturulacak olan sertifikaya ilişkin özet bilgiler yeralmaktadır bu bilgiler incelendikten sonra herhangi bir eksiklik görülmemiş ve. Yapılandır seçeneği ile işleme devam edilmiştir.



Şekil 6.26: Sertifika yönetim konsolu ekranı

Şekil 6.26 da Kurmuş olduğumuz Sertifika sunucumuza ait yönetim konsolu ve oluşturulan fsmk sertifikası listelenmektedir.



Şekil 6.27: sertifika tipleri ekranı

Revoked certificates

İptal edilen sertifikaların listesi yer alır.

Issued certificates

Onaylanmış ve dağıtılmış sertifikaların listesinin bulunduğu alan

Pending requests

Onaylanmak için bekleyen sertifikaların listesinin bulunduğu alan

Failed requests

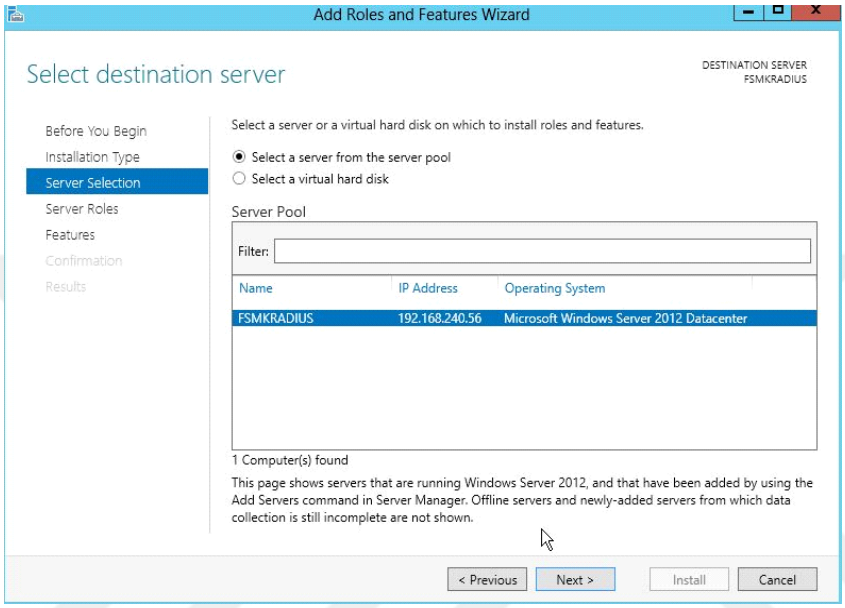
Başarısız taleplerin listesini bulunduğu alan

Certificate templates

Dağıtabileceğimiz sertifikaların listesinin bulunduğu alan

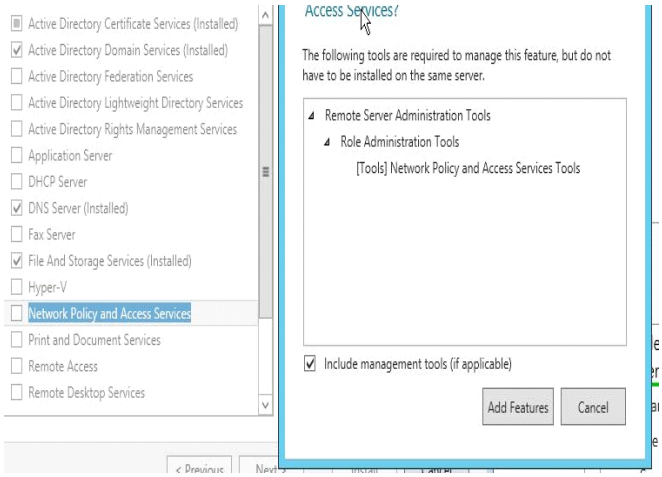
6.3. Kimlik doğrulama ve yetkilendirme sunucusu (Radius) Kurulumu

Kimlik doğrulama ve yetkilendirme sunucusu olarak 802.1x standardı üniversite kablosuz ağ çalışmasında Windows Network policy and Access services NPS kullanılmıştır. Ağ ilkesi sunucusu (NPS) kurulumu ve yapılandırılması adım adım yapılmıştır.



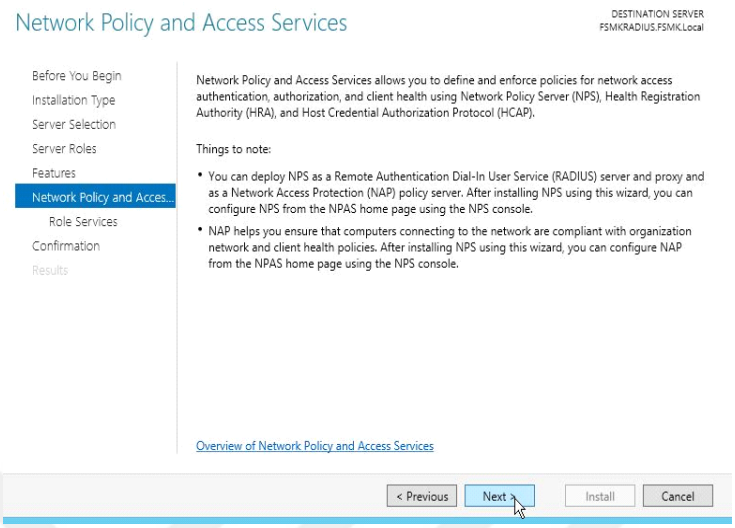
Şekil 6.28 Radius server (Ağ ilkesi sunucusu)kurulumu ekranı

Şekil 6.28'de Mevcut sunucumuzun üzerine ağ ilkesi sunucusunu kuracağımız belirtip sunuc seçilmiştir.



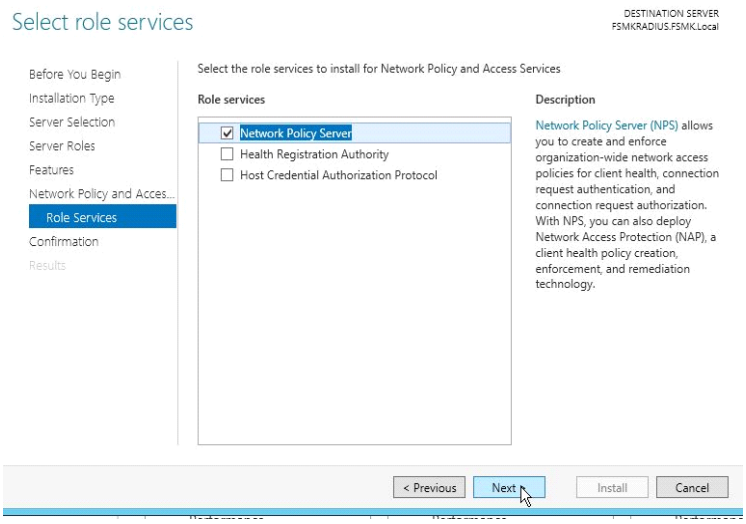
Şekil 6.29: Ağ ilkesi sunucusu kurulum ekranı 1

Şekil 6.28 de Kurulacak özellikler içinden Ağ ilkesi ve erişim hizmetleri seçeneği seçilmiş ve ağ ilkesi sunucusu için gerekli olan ek özellikler kuruluma dahil edilmiştir.



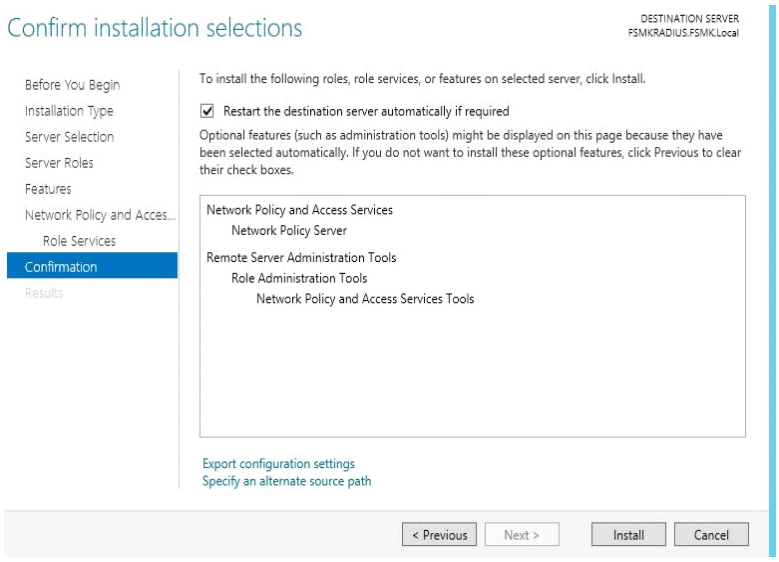
Şekil 6.30: Ağ ilkesi sunucusu kurulum ekranı 2

Şekil 6.30'da Ağ ilkesi sunucusu hakkında bilgilendirme ekranı yer alamaktadır ileri seçeneği seçilmiş ve işleme devam edilmiştir.



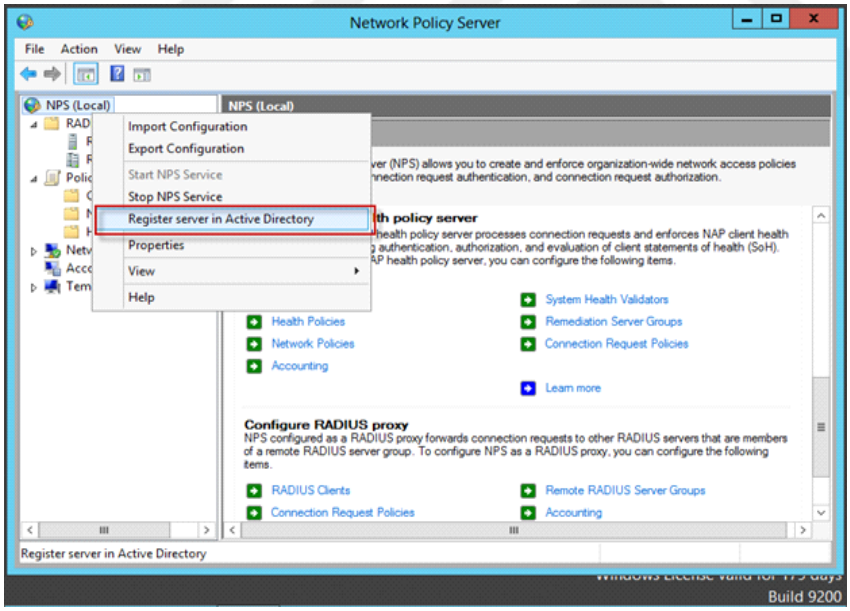
Şekil 6.31: Ağ ilkesi sunucusu kurulum ekranı 3

Şekil 6.31'de Ağ ilkesi sunucusu için rol hizmetlerinden Ağ politika sunucu seçilmiş işleme devam edilmiştir.



Şekil 6.32: Ağ ilkesi suncusu kurulum ekranı 4

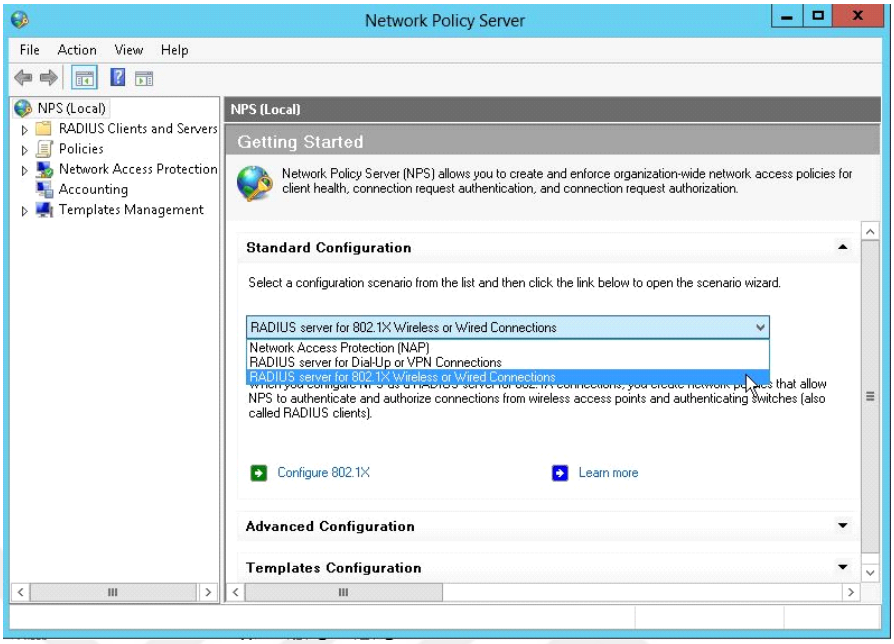
Şekil 6.32'de Ağ ilkesi sunucusu için seçilen ve yüklenecek olan özellikler listelenmektedir. İlgili özellikler incelenmiş ve işleme devam edilmiştir.



Şekil 6.33: Ağ ilkesi sunucusu yapılandırma ekranı

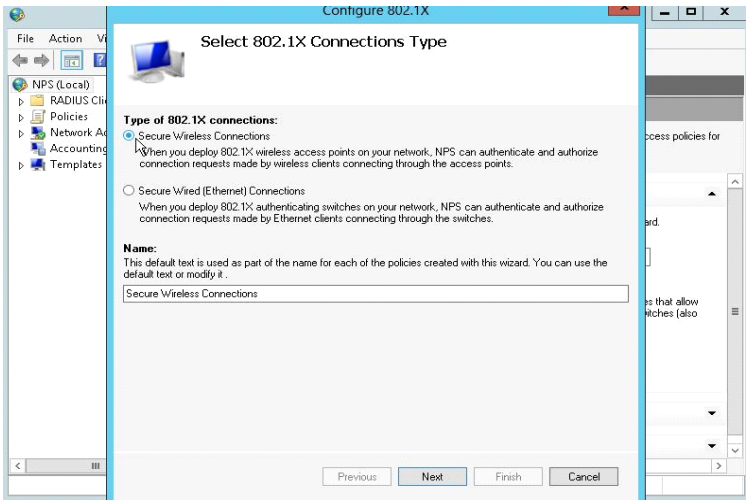
Şekil 6.33'de ağ ilkesi sunucusu yapılandırma ekranında Ağ ilkesi sunucusu kurulum bitmiş ve yapılandırma işlemine başlanmıştır. Daha önce 802.1x standardı için kurulan Dizin hizmeti(Ad) ile Ağ ilkesi sunucusu (Radius server) arasındaki iletişim için Ağ ilkesi sunucusunu dizin hizmetine kaydı yapılmış ve işleme devam edilmiştir.

6.3.1. Ağ ilkesi sunucusu (Radius server) için 802.1x standardı kablosuz ağ yapılandırması



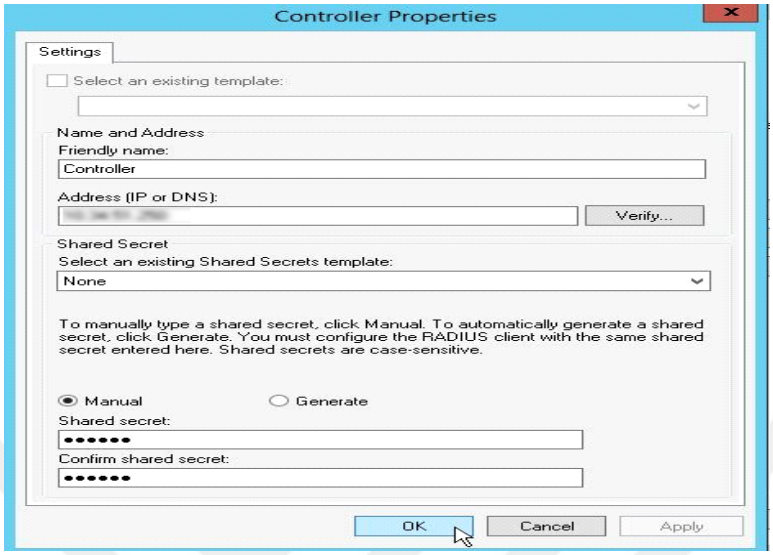
Şekil 6.34: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 1

Şekil 6.34'de Kurulan Ağ ilkesi sunucusu hangi durum için kullanılacağını belirlenen alan yer almaktadır. Ağ ilkesi sunucusunun 802.1x standardı'nın ağ sitemininde kablolu veya kablosuz alanından radius server olarak kullanılacağı seçilmiş ve Ağ ilkesisunucusu kimlik doğrulama ve yetkilendirme sunucusu (radius server) olarak kullanıcağı belirtilmiştir.



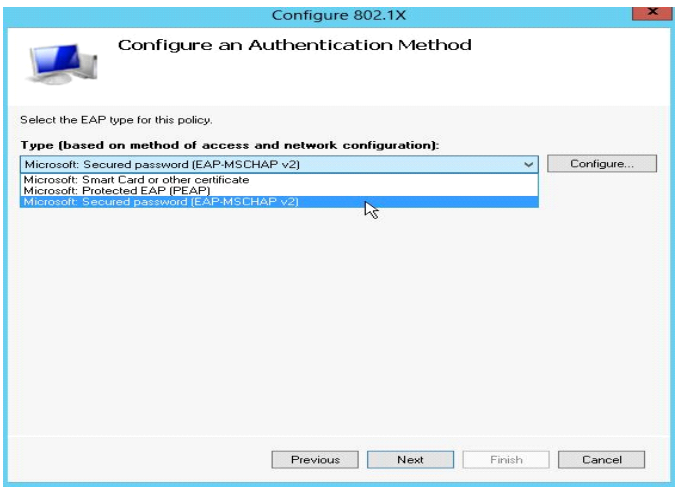
Şekil 6.35: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 2

Şekil 6.35'de 802.1x bağlantı türü seçim alanında, Ağ ilkesi sunucusunun Kablosuz ağ siteminde 802.1x standardının uygulanacağı belirlenmiş ve işleme devam edilmiştir.



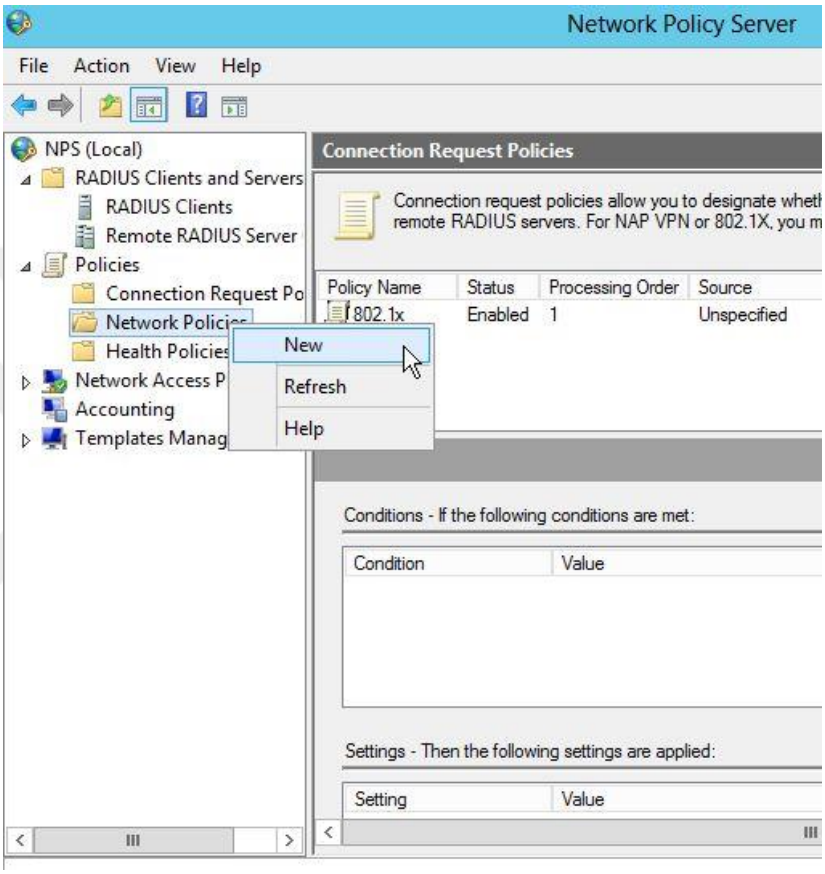
Şekil 6.36: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 3

Şekil 6.40'da 802.1x standardını daha önceki şekillerde ağ ilkesi sunucusunun ağ sistemlerinden kablosuz ağ alanında uygulanacağı belirlenmiştir.kablosuz ağda kullanıcılar erişim noktası cihazları üzerinde sisteme erişim sağlamaktadır.Erişim noktası cihazların tamamının kontrol edebildiğimiz erişim noktası kontrolörünü Ağ ilkesi sunucusu ile haberleşmesi için Bu alanda erişim noktası kontrolörünün ip adresini ve arada kullanılacak olan ortak gizli bir şifre belirlenmiştir.



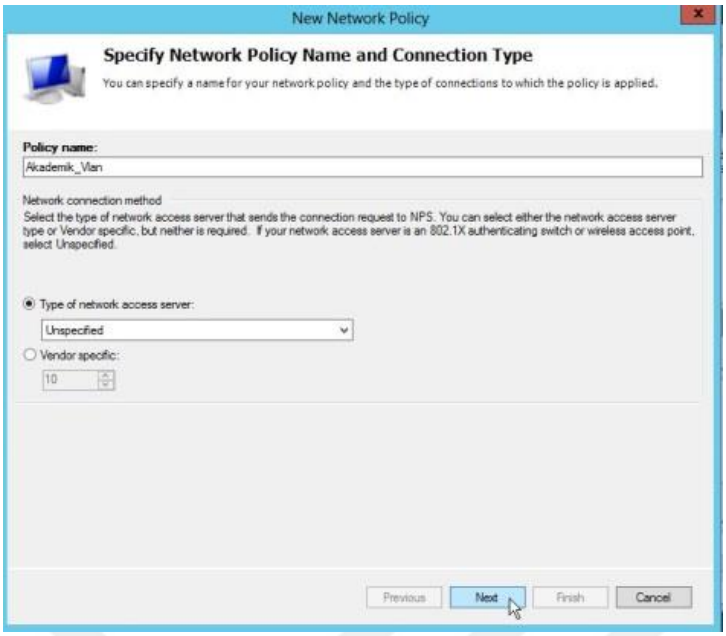
Şekil 6.37: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 4

Şekil 6.37'de Kimlik doğrulama methodlarının belirlendiği alanda Ağ ilkesi sunucusun da 802.1x standardının kullandığı Eap kimlik tanıma yöntemlerinden Eap(Peap) ,Eap-Mschap2 birlikte kullanımı için her ikiside sisteme ilave edilmiştir. Bu aşama itibari ile 802.1x standardı ağ ilkesi sunucusu için genel yapılandırma işlemleri oluşturulmuştur tez çalışması 802.1x standırdı için oluşturulan sanal ağlar için politikalar oluşturma işlemine geçilmiştir.



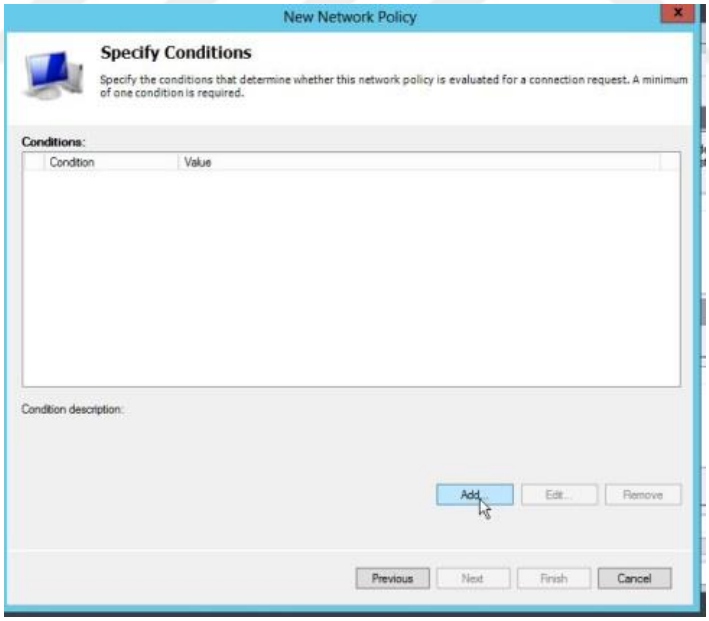
Şekil 6.38: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırmaekranı 5

Şekil 6.38'de ağ ilkesi sunucusu üzerinde sanal ağ ve guruplar için kural oluşturma (policiy) işlemine geçilmiştir.Yapılan işlemde ağ ilkesi sunucusu yönetim konsolunda kurallar (policies) fare sağ tuş yeni seçeneği seçilmiş ve yeni bir kural oluşturulmaya başlanmıştır.



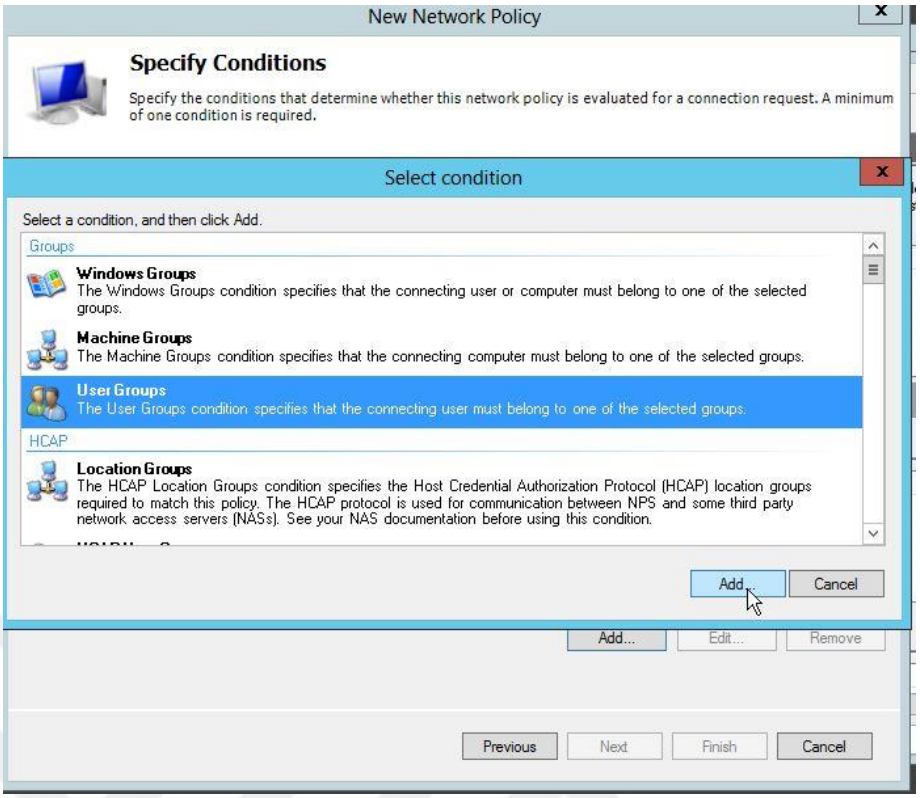
Şekil 6.39: Ağ ilkesi sunucusu 802.1x Kablosuz ağ yapılandırma ekranı 6

Şekil 6.39'da O ağ ilkesi sunucusu üzerinde yeni oluşturulan kuralın, kural ismini akademik_vlan olarak tanımlanmıştır.



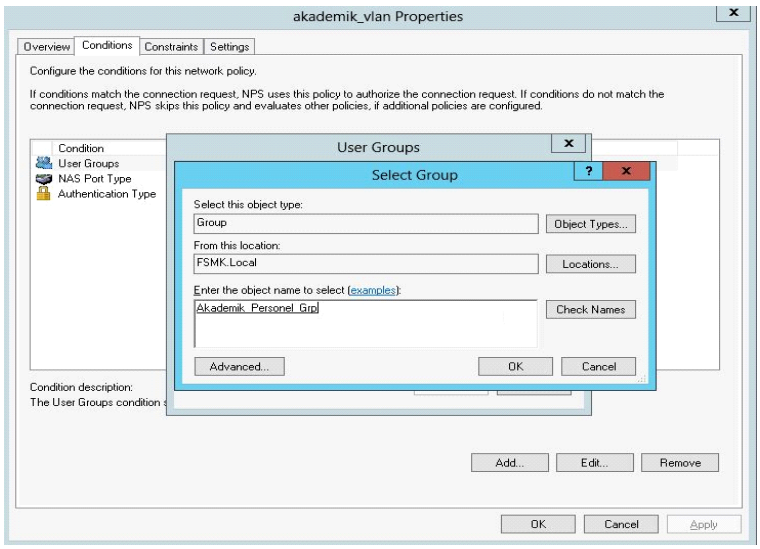
Şekil 6.40: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 7

Şekil 6.40'da akademik_vlan kuralının bağlatı koşulunu belirlmek içi ekle işlemi seçilmiştir.



Şekil 6.41: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 8

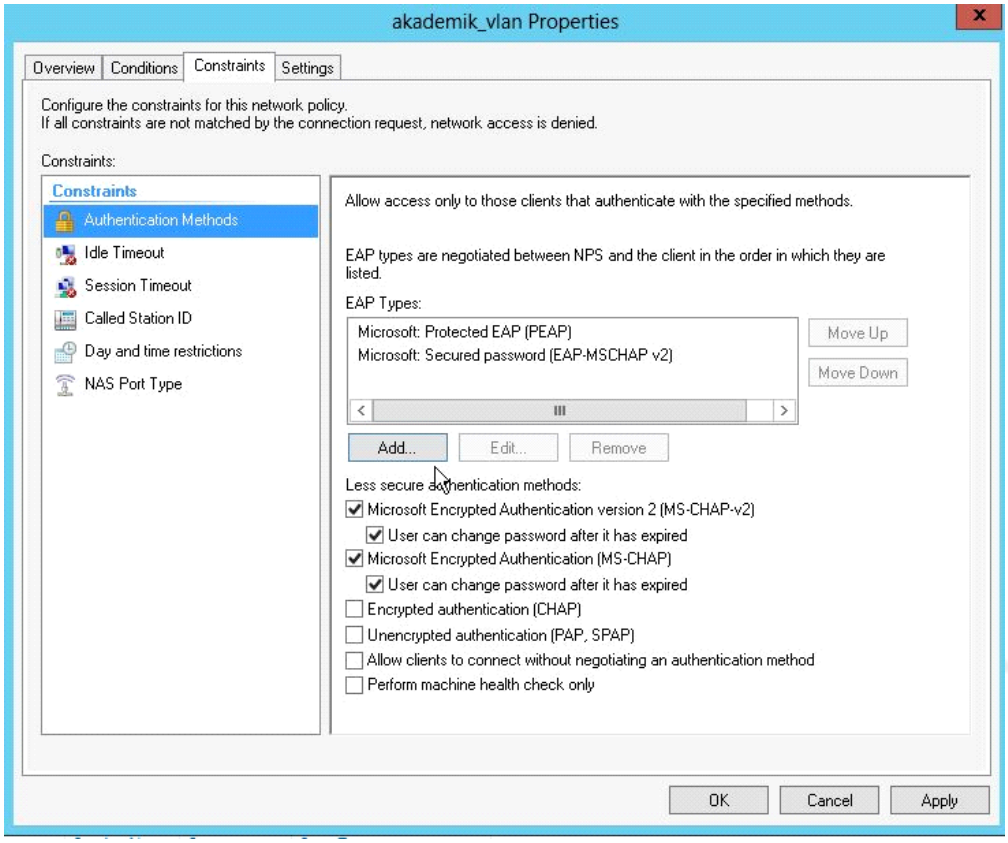
Şekil 6.41'de Ağ ilkesi sunucu üzerinden 802.1x standardı kablosuz ağ bağlantısında akademik_vlan içerisindeki kurallara dahil olacak türün kullanıcı gurubu olarak belirlenmiştir.



Şekil 6.42: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 9

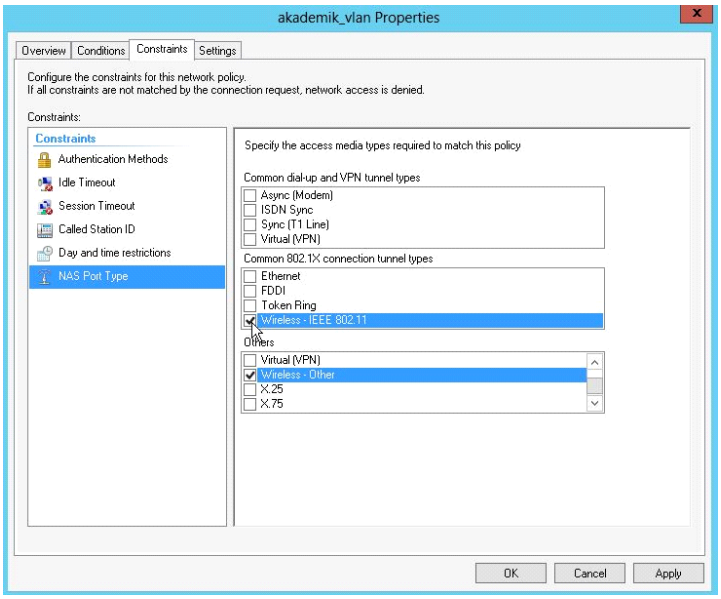
Şekil6.42'de Ağ ilkesi sunucusu (Radius server) akademik_vlan içerisinde dahil

edilecek ve dizin hizmeti (AD) ile ağ ilkesi sunucusu (radius server) iletişime geçtiği zaman dizin hizmetinde tanımlanan guruplardan,ağ ilkesi sunucusunda tanımlana sanal ağlardan , tanımlanan kuralardan etkileceğini belirtiğimiz gurupların eklendiği alandır.Bu alanda akademik_vlana dizin hizmetinden akadamik_Personel_Grp dahil edilmiştir.



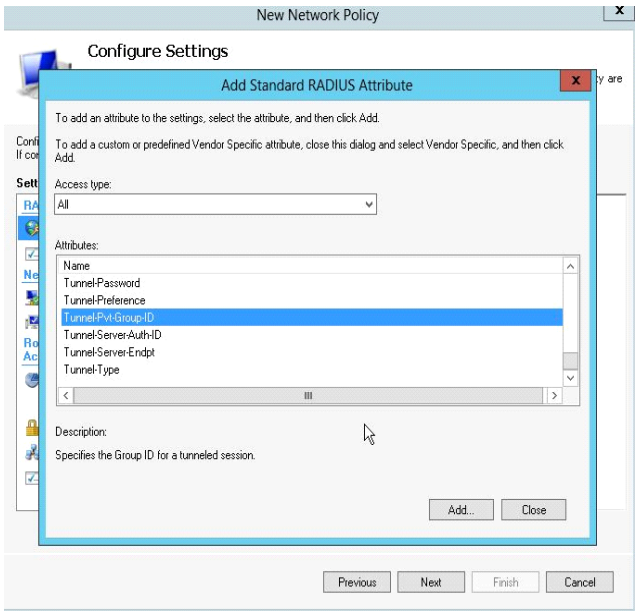
Şekil 6.43: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 10

Şekil 6.43'de Ağ ilkesi sunucusunun 802.1x standardından EAP güvenlik kimlik kanıtlama yöntemlerinden akademik_vlan içerisindeki guruplara dahil olan kullanıcıların kimlik doğrula esnasında Eap türlerinden EAP(PEAP),ve EAP-MSCHAPv2 uygulanacağı belirtilmiş ve yapılandırmaya devam edilmiştir.



Şekil 6.44: Ağ ilkesi sunucusu 802.1x Kablosuz ağ yapılandırma ekranı 11

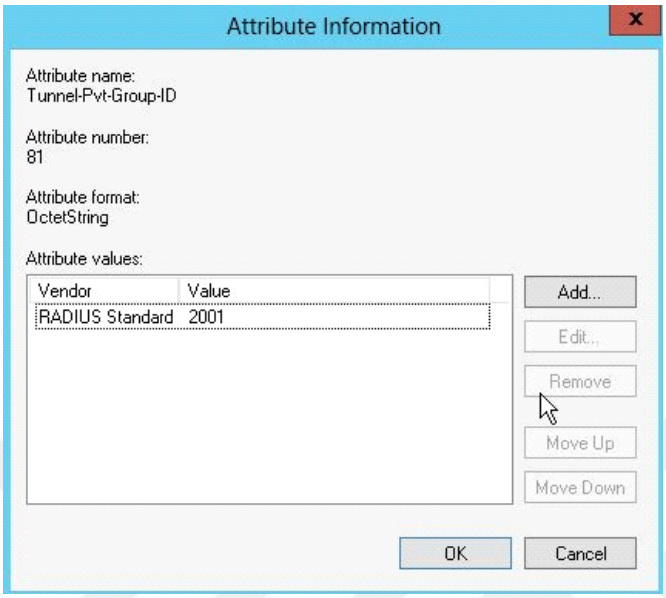
Şekil 6.44'de Ağ ilkesi sunucusundan kablosuz ağ üzerinden akademik_vlana dahil olan gurupların İEEE 802.11 ve diğer standartlardan 802.1x bağlatısına izin verilmiş ve vpn gibi diğer işlemlere yetki verilmemiştir. Diğer bağlatı istekleri için farklı guruplar tanımlanmıştır.



Şekil 6.45: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 12

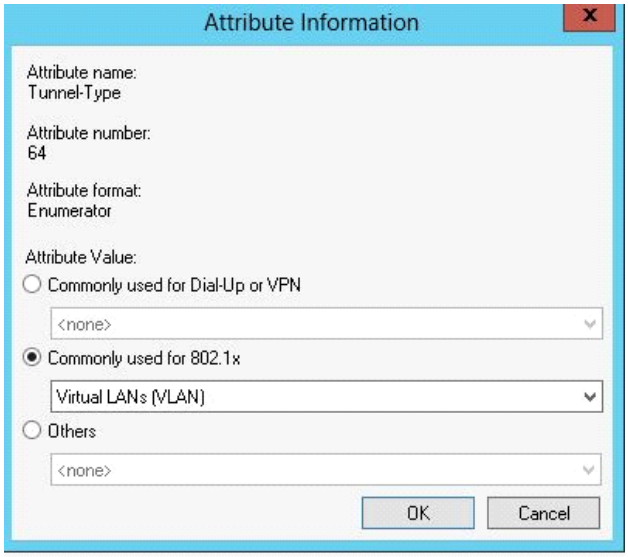
Şekil 6.45'de Ağ ilkesi sunucusu üzerinde tanımlanan vlanların erişim noktası kontroluru üzerinde vlan isimlerinin bir önemi yoktur.

Bu iletişim vlan tag id leri ile gerçekleştirilir bu nedenle şu ana kadar tanımlanan vlanların 802.1x standardı Radius özelliklerinden tunnel Pvt-Group-İD (Gurup üyelerinin atanacağı sanal ağ numarası) ile tanımlanması gerekmektedir. Akademik_vlan için tasarlanan vlan tag id (sanal ağ numarası) 2001.



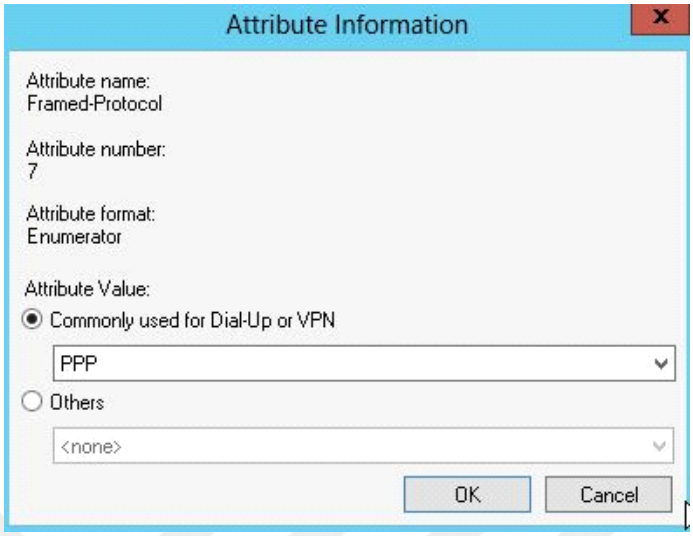
Şekil 6.46: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 13

Şekil 6.46'da Ağ ilkesi sunucusun'da radius standart Tunnel_Pvt_group_id 2001 akademik_vlan için tanımlanmıştır.



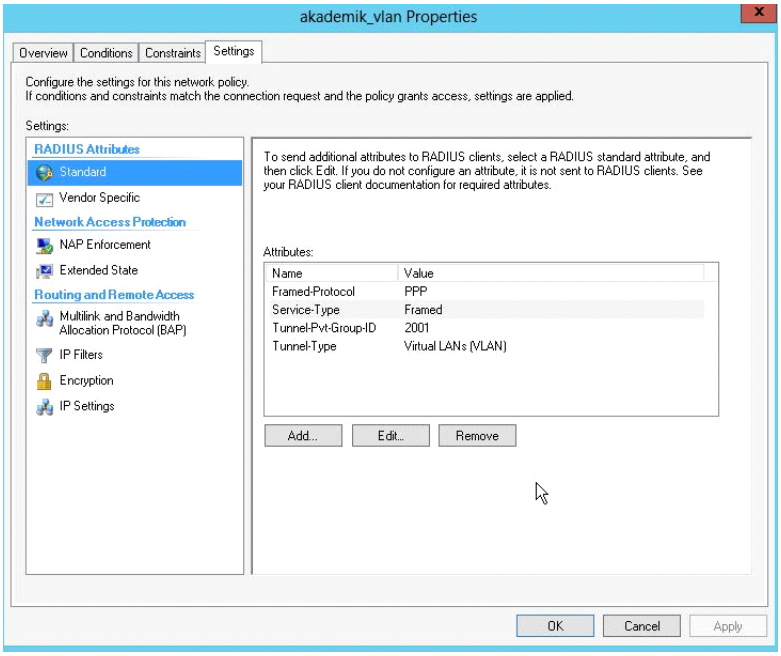
Şekil 6.47: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 14

Şekil 6.47'de Ağ ilkesi sunucusu üzerinde 802.1x özelliklerinden Tunnel_Type ile sağlanacak bağlantı isteğinin vlan (sanal ağ) olduğunu tanımlanmıştır.



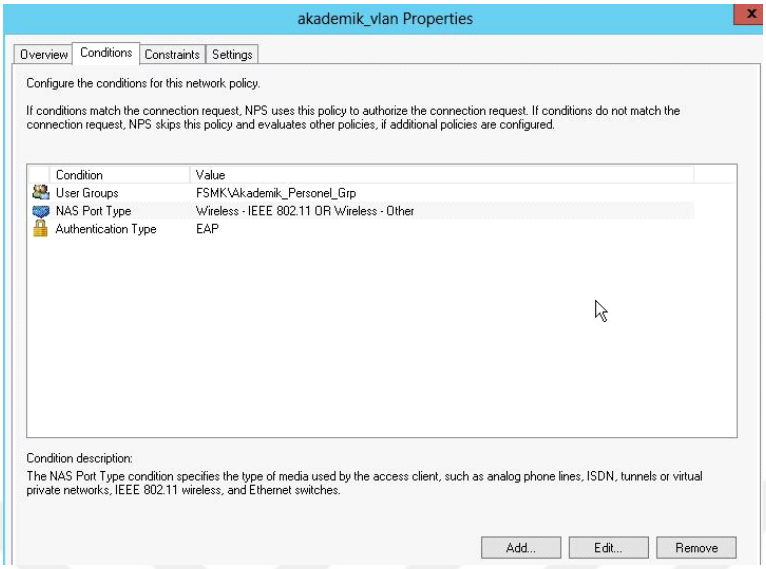
Şekil 6.48: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 15

Şekil 6.48'de Ağ ilkesi sunucusu ile arada bağlantı kuracak olan cihazların framed-Protocol'ün ppp(noktadan noktaya) ağların birbiri arasında doğrudan bağlantı kurmasını sağlayan veri köprüleme protokolünün kullanılacağı tanımlanmıştır.



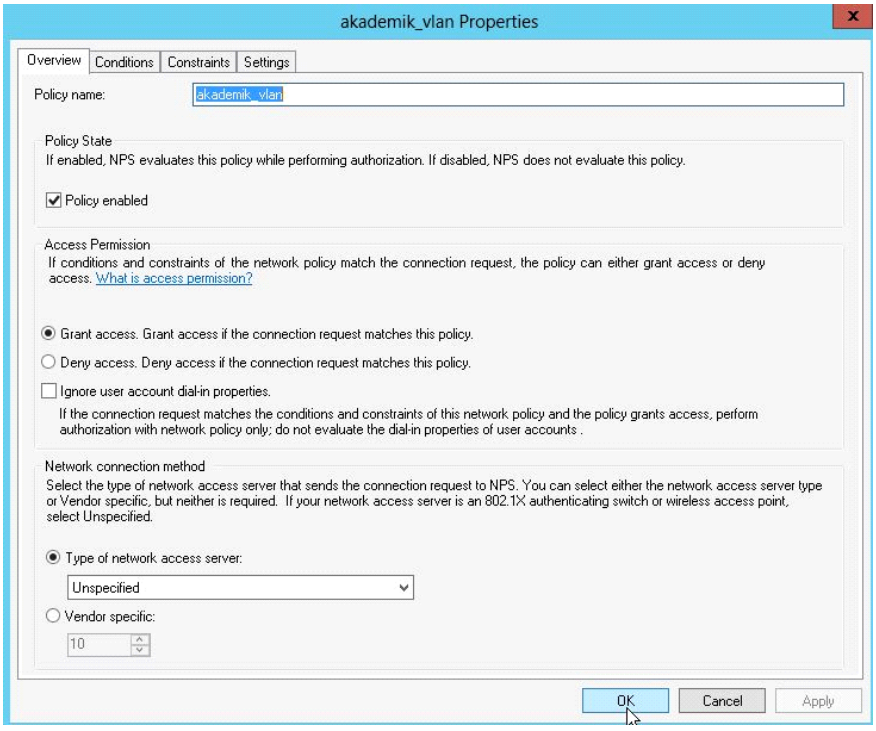
Şekil 6.49: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 16

Şekil 6.49'da Ağ ilkesi sunucusunda akademik_vlan için tanımlanan özellikler listelenmiştir.



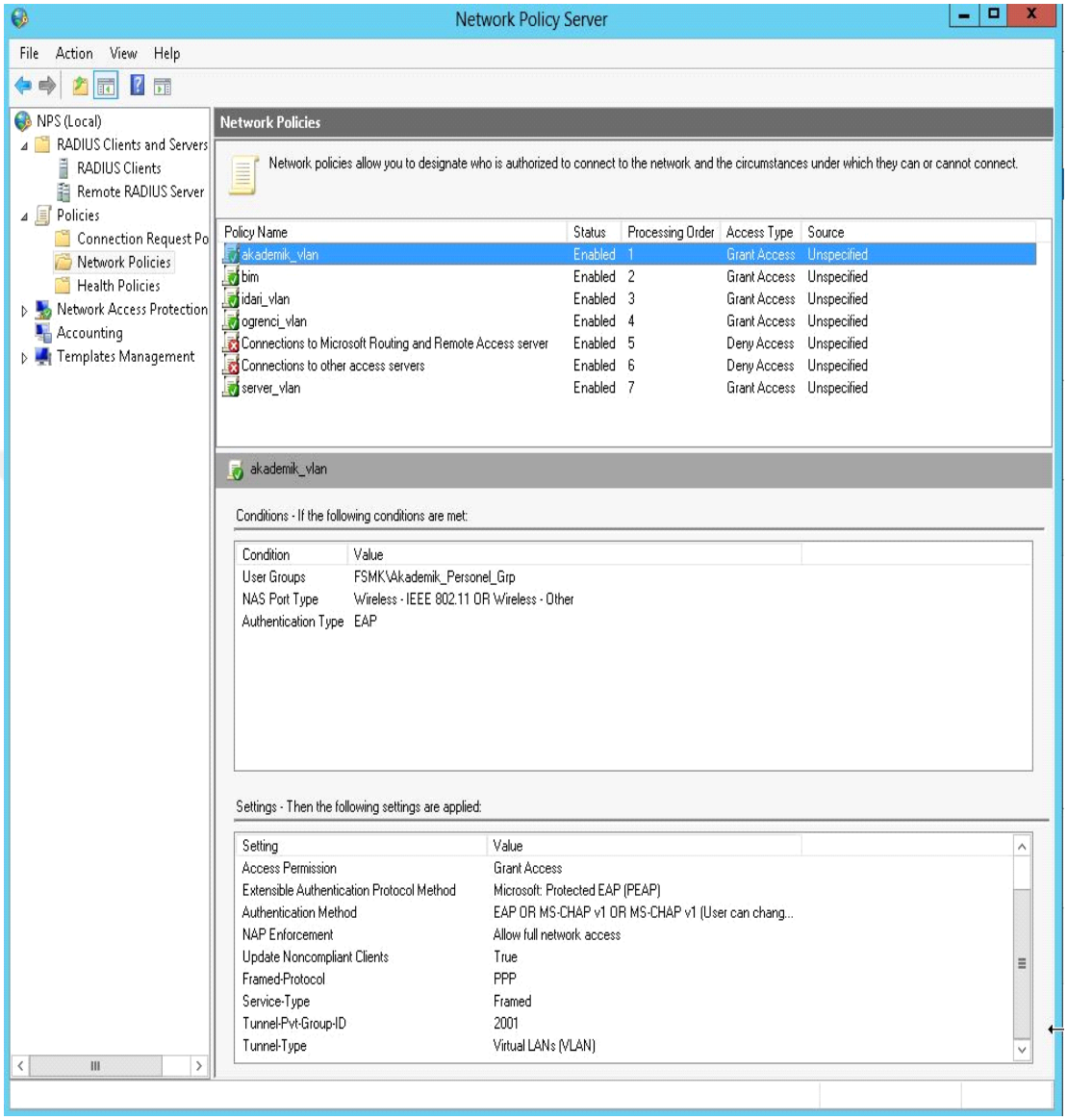
Şekil 6.50: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 17

Şekil 6.50'deAğ ilkesi sunucusu Akademik_Vlanın üzerinden bağlantı kurulabilecek koşullar listelenmiştir.



Şekil 6.51 :Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 18

Şekil 6.51'de Ağ ilkesi sunucusu üzerinde Akademik sanal ağ ile ilgili kuralların devreye alındığı belirtilmiştir.

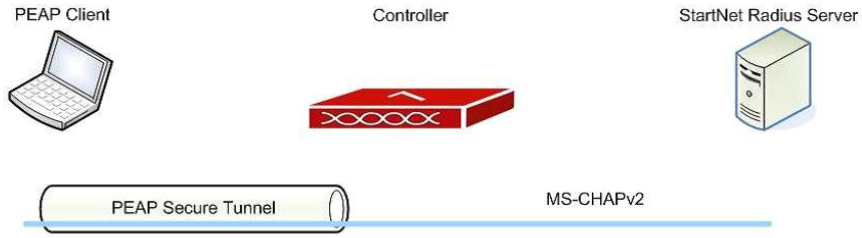


Şekil 6.52: Ağ ilkesi sunucusu 802.1x kablosuz ağ yapılandırma ekranı 19

Şekil 6.52'de Ağ ilkesi sunucusu üzerinde tanımlanan sanal ağların listesi, uygulanacağı koşullar ve sınırlamalar listelenmiştir. Tez çalışması içerisinde tüm sanal ağlar, guruplar ve kullanıcılar için kurallar oluşturulmuş ve devreye alınmıştır.

6.4. Erişim noktası kontrolürü (Acces point controller) yapılandırılması

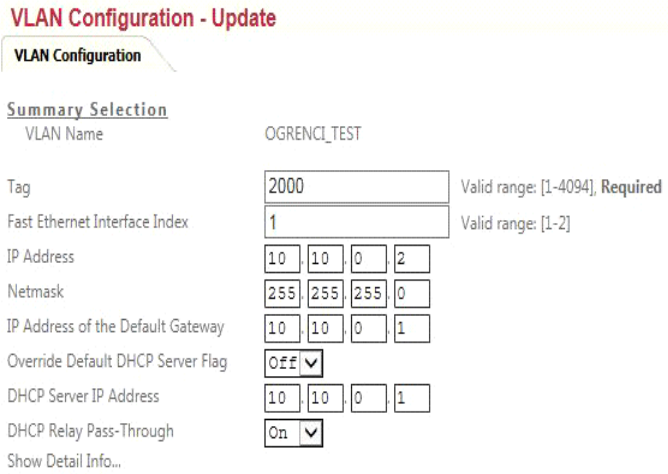
802.1x standardının uygulamasında donanım cihazları olarak farklı markalarda Erişim noktası kontrollörleri 802.1x standardını desteklemektedir. Üniversite bünyesinde erişim noktası kontrolleri olarak Meru MC3000 kullanılmaktadır. Yapılan sanal ağ tasarımlarının uygulanmasının sistemde bulunan kimlik Ağ ilkesi sunucusu, dizin hizmeti, güvenlik duvarı ile haberleşebilmesi için tasarımın erişim noktası kontrollerinda da tanımlanması gerekmektedir



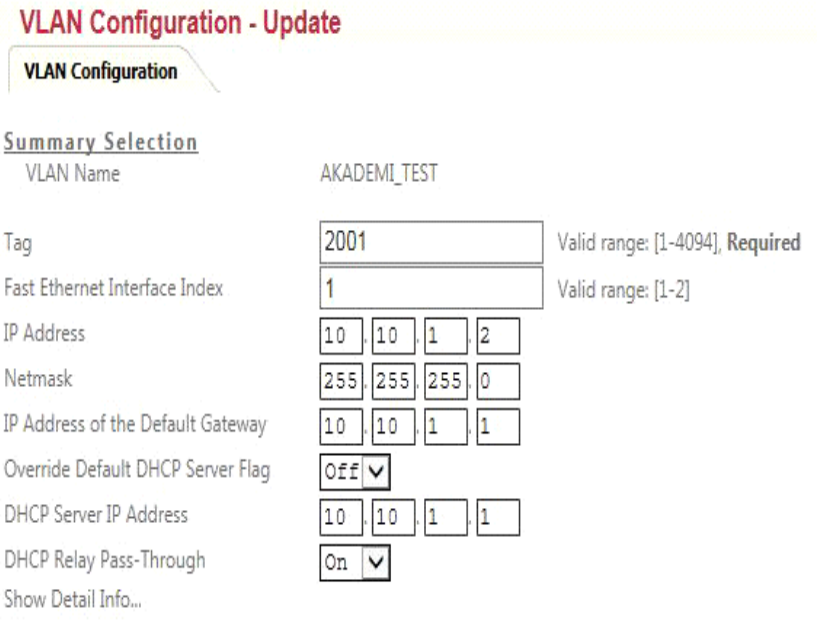
Şekil 6-53: Erişim Noktası Kontrolörı ağ ilkesi sunucu haberleşmesi

Şekil 6.53 de 802.1x standardı ile sisteme bağlanacak bir kullanıcının kullanıcı, kontrolör, ağ ilkesi sunucusu arasındaki haberleşmesi şekilsel olarak gösterilmiştir.

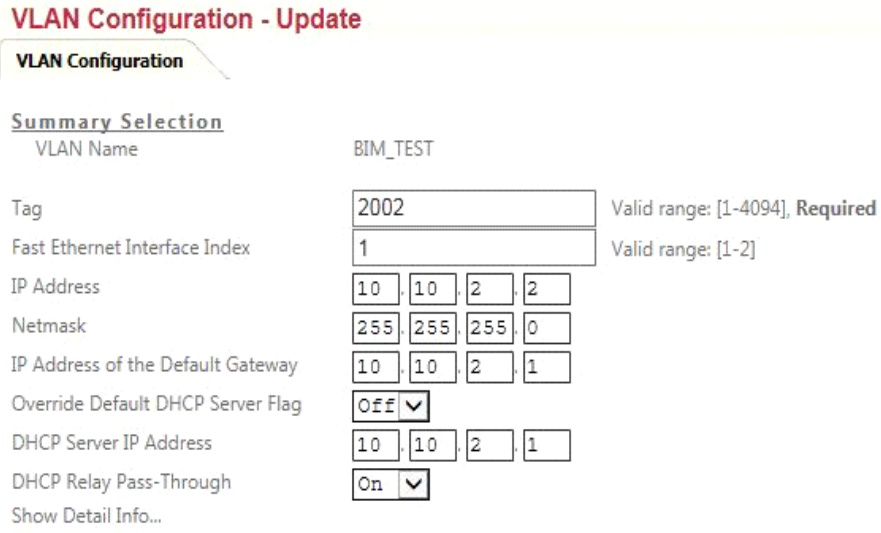
Erişim noktası kontrolürü üzerinde sanal ağ yapılandırması



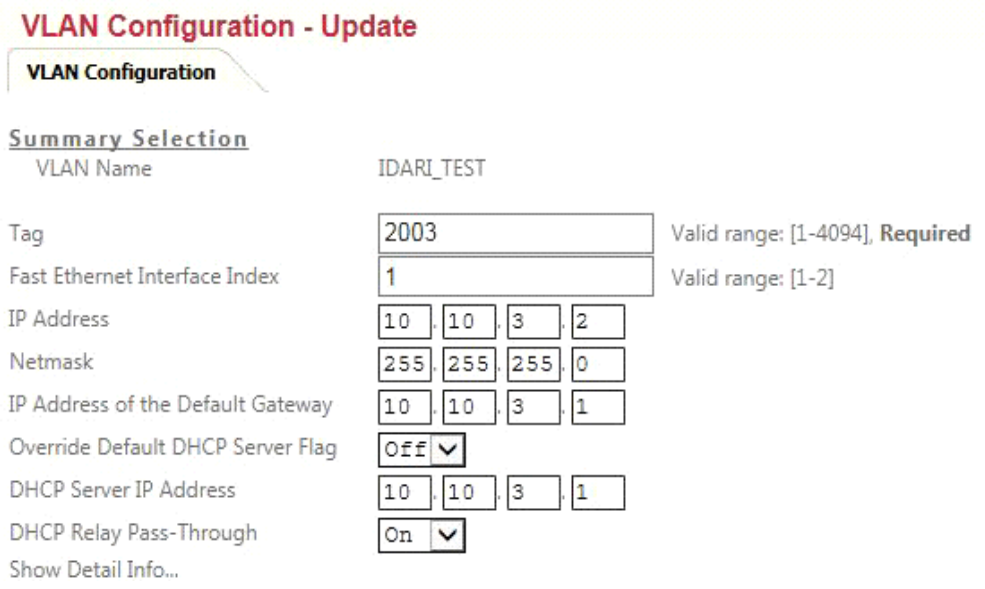
Şekil 6.54: Erişim noktası kontrolürü üzerinde öğrenci sanal ağ yapılandırması



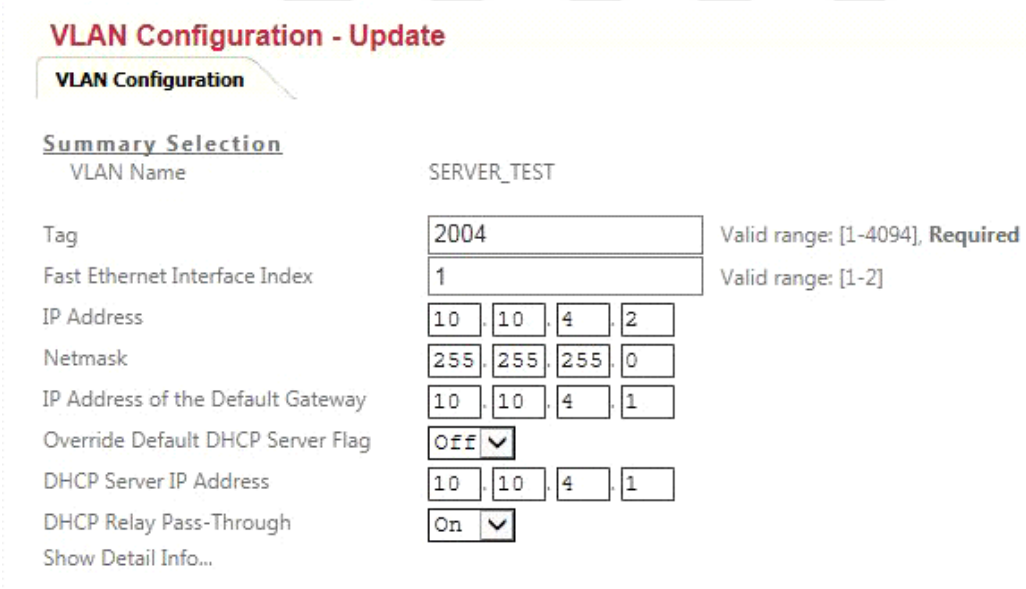
Şekil 6.55: Erişim noktası kontrolörü üzerinde Akademi sanal ağ yapılandırıması



Şekil 6.56: Erişim noktası kontrolörü üzerinde Bim sanal ağ yapılandırması



Şekil 6.57: Erişim noktası kontrolırı üzerinde İdari sanal ağ yapılandırması

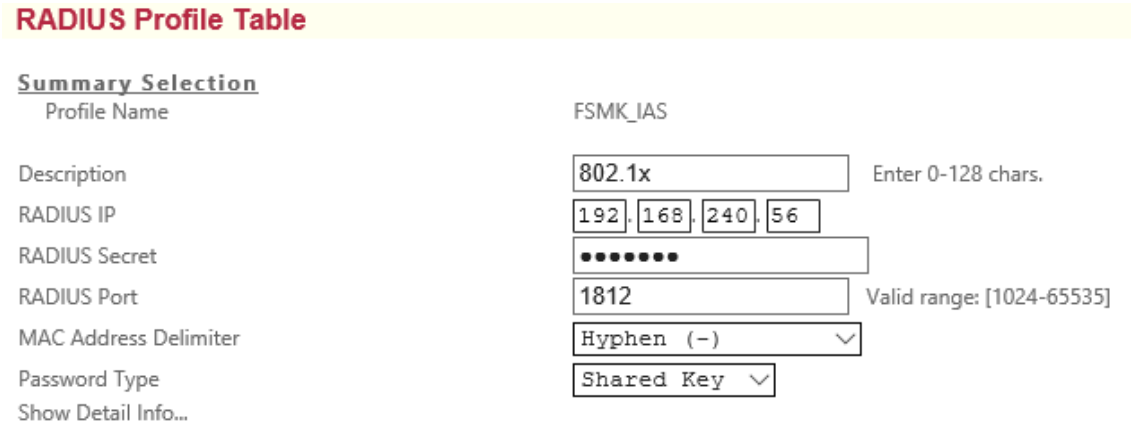


Şekil 6.58: Erişim noktası kontrolırı üzerinde server sanal ağ yapılandırması

Şekil 6.59: Erişim noktası kontrolörü üzerinde oluşrurulmuş sanal ağ listesi

Erişim noktası kontrolürü üzerinde radius profile tasarımın uygulanması

Radius Authentication tanımı. Meru Radius Secret'in kurmuş olduğumuz Microsoft Windows 2012 Server'daki Ağ hizmeti sunucusunda Radius client shared secret ile aynı olmasına gerekmektedir.



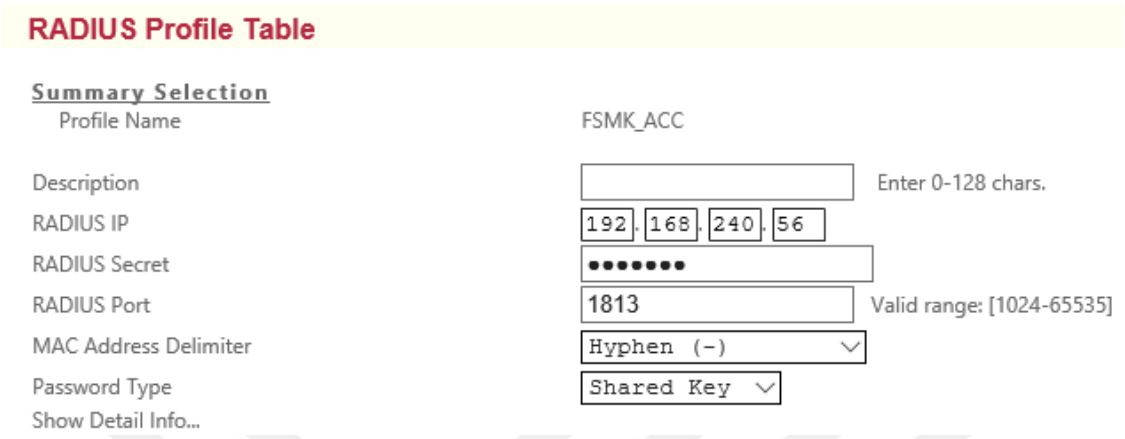
Şekil 6.60: Erişim noktası kontrolör yapılandırma Radius profile

Radius profile Accounting

Erişim noktası controller sistemine erişip

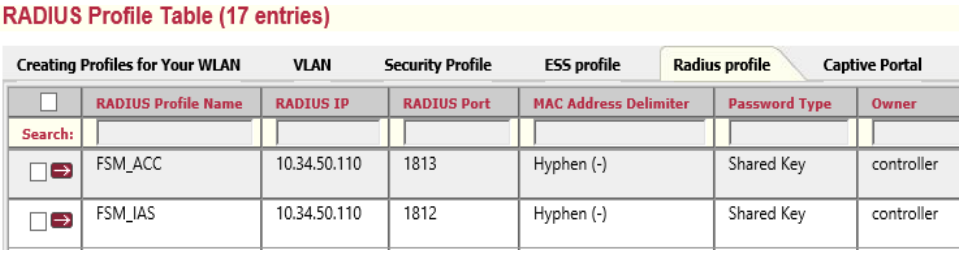
Wlan managemet-Configuration-Security-Radius

Radius Acconting tanımı. Meru Radius Secret'in kurmuş olduğumuz Microsoft Windows 2012 Server'daki Ağ ilkesi sunucusunda Radius client shared secret ile aynı olmasına gerekmektedir.



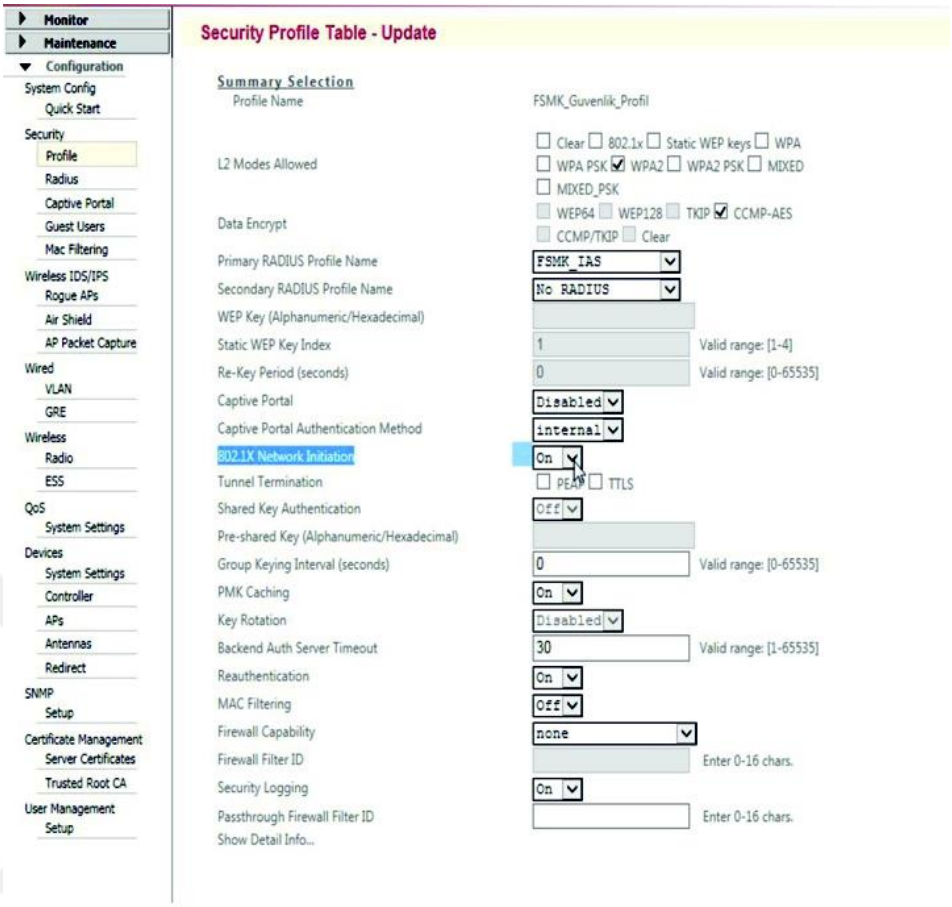
Şekil 6.61: Erişim noktası kontrolörü Radius profile 2

Erişim noktası kontrolörü şu an Ağ ilkesi sunucusu (Radius server) ile 1812, 1813 portlarını kullanarak haberleşme işlemi sağlandı.

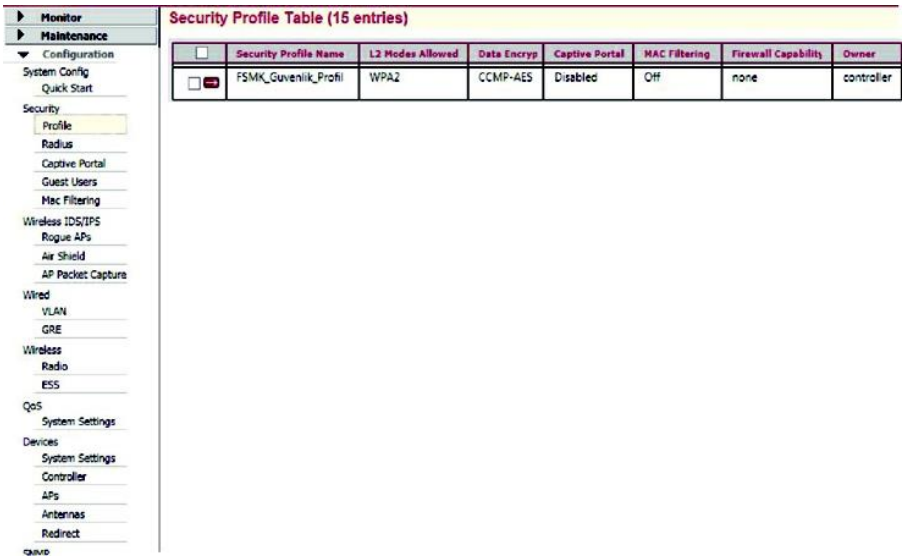


Şekil 6.62: Erişim noktası kontrolör Radius profil listesi

Erişim noktası kontrolür için güvenlik profilinin tasarımının uygulanması



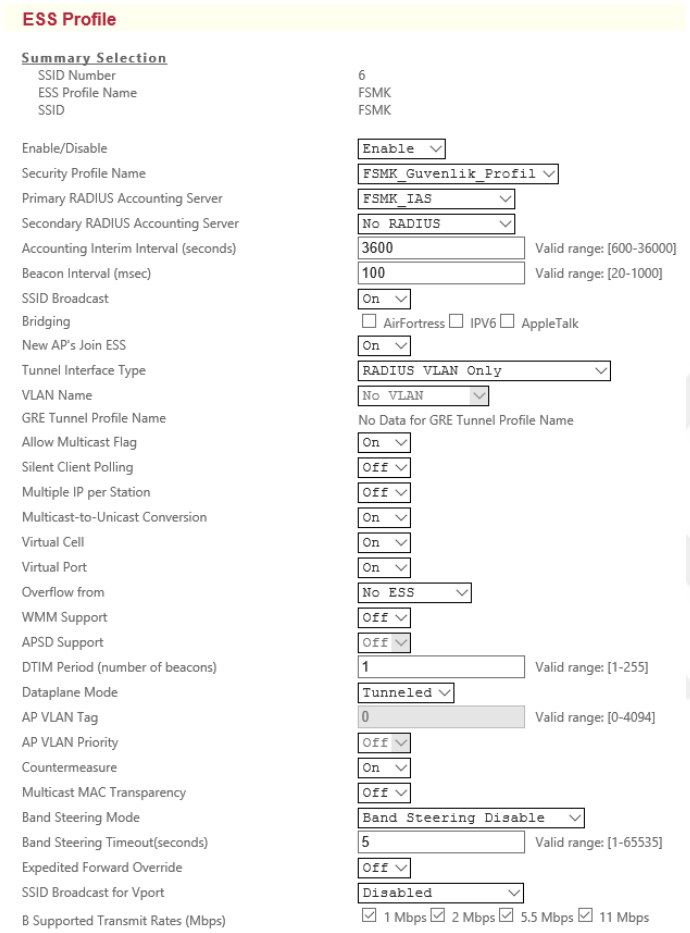
Şekil 6.63: Erişim noktası kontrolör Güvenlik profili yapılandırılması



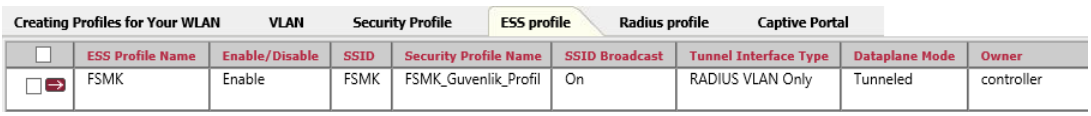
Şekil 6-64: Erişim noktası kontrolör Security profile

Erişim noktası kontrolür için SSID tasarımının uygulanması

Ess profile



Şekil 6-65: Erişim noktası kontrolırı SSID yapılandırılması



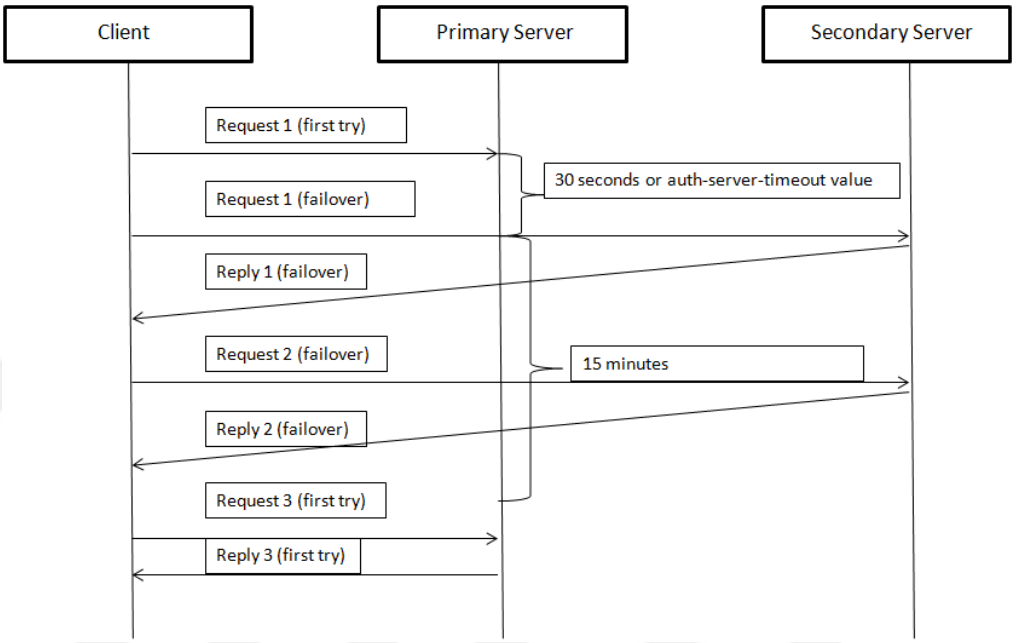
Şekil 6.66: SSID (Hizmet Takımı Tanıtıcısı) listesi

Radius failover

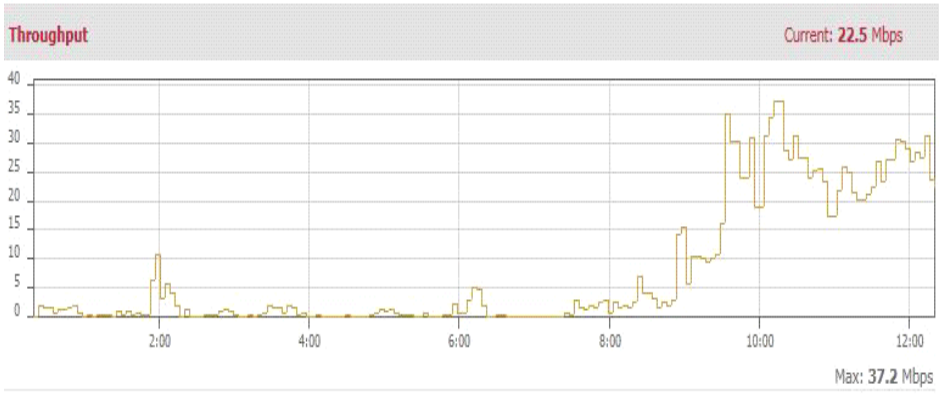
RADIUS kimlik doğrulama özelliği zorunlu kılan bir Meru denetleyicisi dahili modülleri veya hizmetler bulunmaktadır. Kullanıcı kimlik doğrulaması türüne göre tanımlanan başarısızlık yöntemi, standart 802.1x veya kurumsal WPA / WPA2 kimlik

türüne göre:

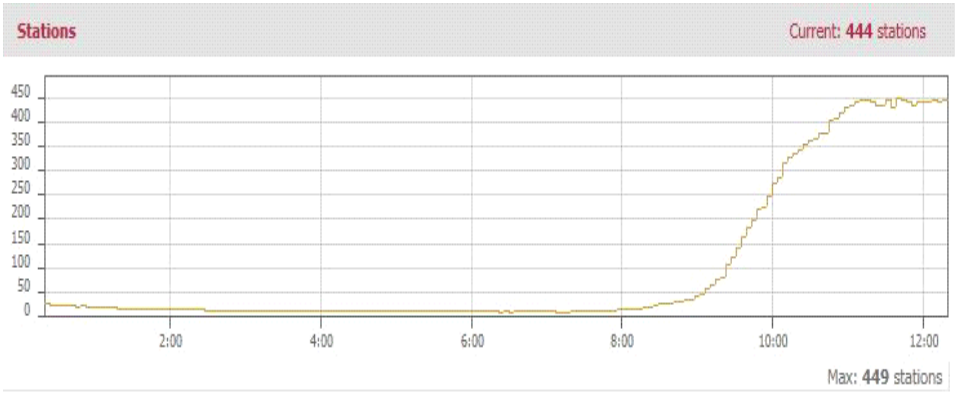
Authentication failover (802.1x)



Şekil 6.67: Bağlantı hatası işlem ekranı



Şekil 6.68: Erişim cihazı üzerindeki internet tırafiği

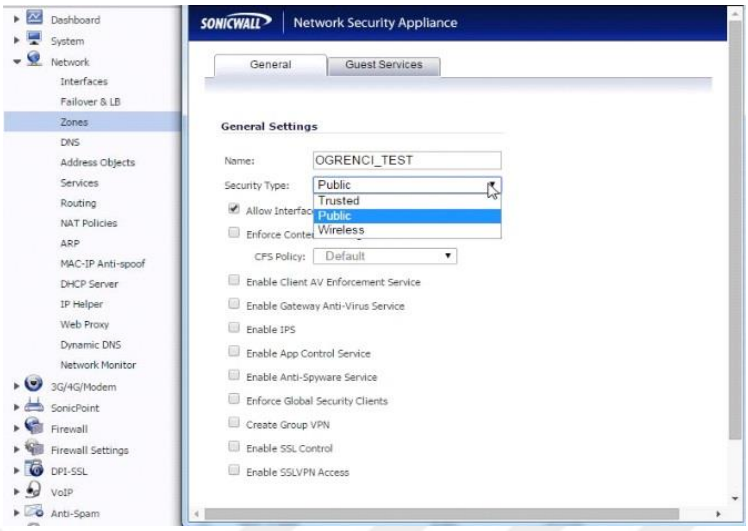


Şekil 6.69: Erişim noktası kontrolür üzerindeki bağlana kullanıcı sayısı

Controller				Alarms		Rogues		AP Status		APs with Alarms		Stations		ESSIDs	
Model	MC3000	#VLANs	12	Critical	1	APs	7	Online	38	Critical	1	Data	454	Clear	1
SW Version	5.1-90	Stats Polling	60	Major	12	Stations	3	Offline	1	Major	0	Phones	0	Secured	7
Auto Ap Upgr	on	DHCP Relay	on	Minor	37	Unknown	0	Total:	39	Minor	0	Total:	454	Captive Portal	0

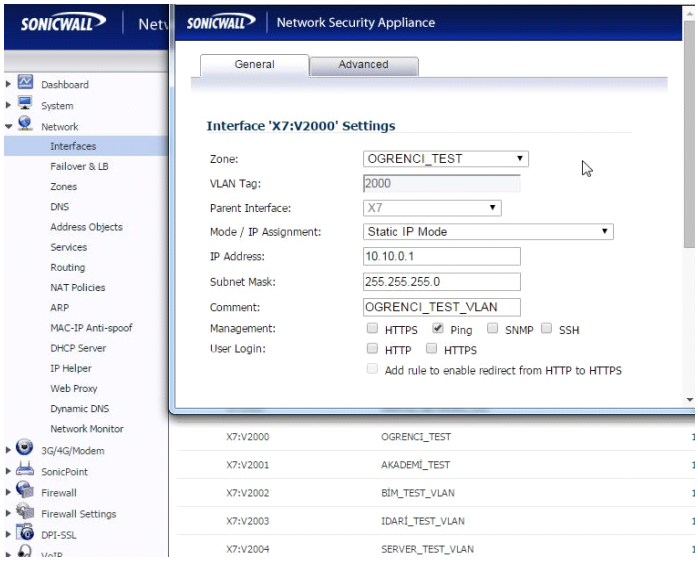
Şekil 6.70: Erişim noktası kontroler cihazı üzerindeki raporlar

6.5. Güvenlik duvarı (Firewall) Yapılandırılması



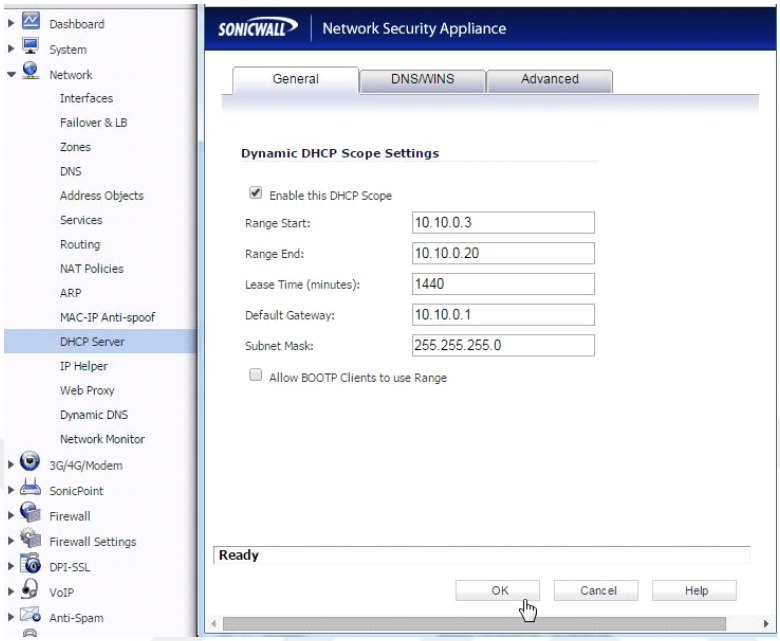
Şekil 6.71: Firewall yapılandırma ekranı 1

Şekil 6.71 de 802.1x standardının güvenlik duvarı işleminde tasarlanan her sanal ağ için Güvenlik duvarı üzerinde zones (bölge)oluşturulması gerekmektedir. Oluşturulan bu bölgeler üzerinde sanal ağ isimleri ve güvenlik seviyelerinin genel bir kullanıcı olduğu belirtilmelidir. Bu işleme göre öğrenci sanal ağın ismi ve güvenilirlik tipi genel kullanıcı seçilerek güvenlik duvarı üzerinde bölge olarak tanımlanmıştır.



Şekil 6.72: Firewall yapılandırma ekranı 2

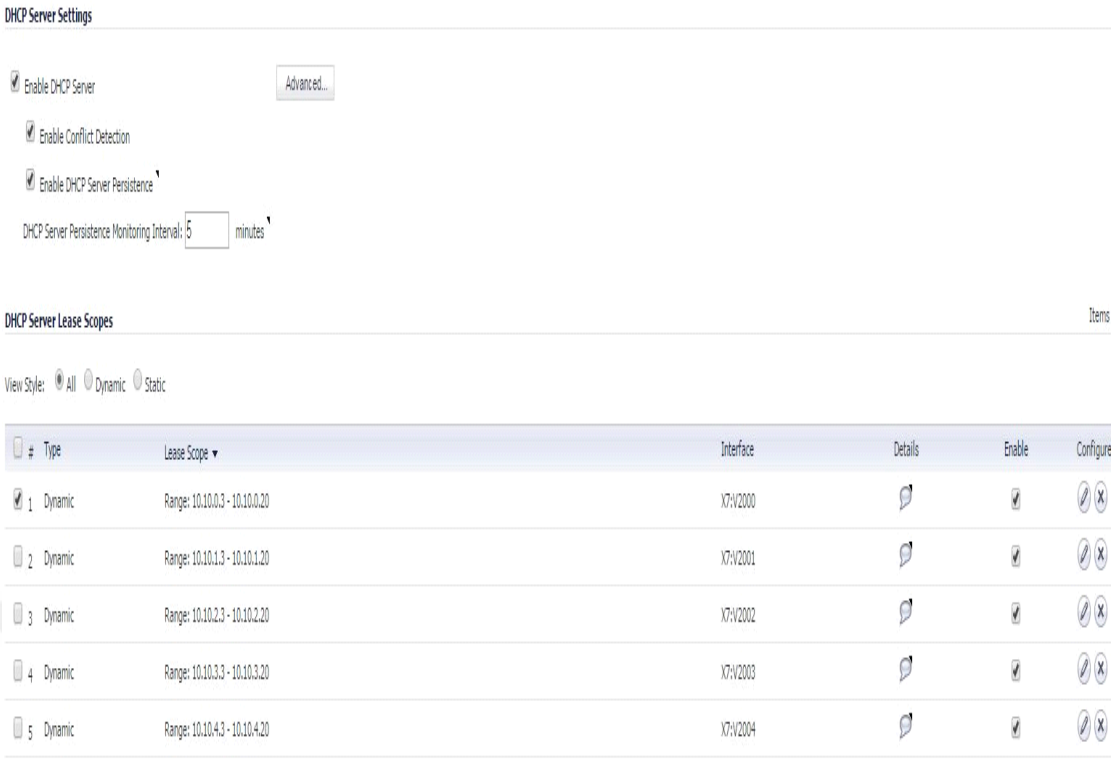
Şekil 6.72'de Güvenlik duvarı üzerinde şekil 6.71 de oluşturulan bölgelerin interface(arayüz) üzerinden hangi sanal ağ numarası ile internete çıkacağı ve bu sanal ağın ip adresi ve ağ üzerinde yapabileceği işlemlerin tanımlaması gerekmektedir.



Şekil 6.73: Firewall yapılandırılması ekranı 3

Şekil 6.73'de Güvenlik duvarı üzerinde tanımlanmış olan bölgelere ve internete hangi vlan üzerinden çıkacağı şekil 6.71 ve şekil 6.72 de oluşturulmuştur. Firewall üzerinde internete erişim sağlamak veya kablosuz ağa dâhil olabilmek için 802.1x Standardı ile Ağ ilkesi sunucusu, dizin hizmeti, erişim noktası kontrolürü üzerindeki tüm kurallardan kullanıcı bilgileri denetlenip kullanıcının kimliği doğrulandıktan sonra sanal ağı gurubuna göre belirlenir.

Fakat sisteme dâhil olabilmesi için kullanıcı bulunduğu sanal ağa göre ip adresi alması gerekmektedir. Şekil 6.73' de öğrenci sanal ağındaki kullanıcıların sisteme dâhil olurken alabileceği ip aralığı tasarıya göre tanımlanmıştır.



Şekil 6.74: Firewall yapılandırma ekranı 4

Şekil 6.74'de Güvenlik duvar dhcp server üzerinde akadamik, öğrenci, idari, bim, server tanımlanan ip aralıkları listelenmiştir.

6.6. Ağ anahtarı

Kablosuz ağ sitemi içerisinde veri heberleşme ve yönlendirme işlemlerinin önemli bir parçasınıda ağ anahtarı oluşturmaktadır. Kablosuz ağ yayını havadan yapılsa dahi oluşturulan yapılandırmayı ağ anahtarı üzerindede oluşturmamız gerekmektedir. Çünkü erişim noktası cihazaları, erişim noktaları, güvenlik duvarı, ağ ilkesi sunucusu gibi cihazlar bir ağ anahtarlama cihazından gelen bir uca yani Ethernetportuna veya fiberbağlantı vasıtası ile haberleşirler. 802.1x standardında sanal ağ teknolojisinde de üniversitenin güvenlik seviyesini artırmak için ek olarak bu tez çalışmasında kullanılmıştır. Oluşturduğumuz sanal ağları, ağ anahtarı cihazı üzerinde'de oluşturmamız gereklidir oluşturmak için izleneceke yol kodları ve uygulaması ile tez çalışmasında gösterilmiştir.

Yapılandırma

ssh@core_switch>en

password:

ssh@core_switch># config term

ssh@core_switch(config)#vlan 2002 name BIM_TEST_Vlan

ssh@core_switch(config-vlan-2002)#tagget Ethernet

ssh@core_switch(config-vlan-2002)#tagget Ethernet 1/2/1/

Yukarıdaki yapılmış olan yapılandırma ana ağ anahtarlama cihazı üzerinde yapılmıştır ayrıca kurum içerisinde ana anahtar cihazına bağlı blok dağıtım cihazları ve blok dağıtım cihazlarına bağlı kenar dağıtım cihazları mevcuttur aynı yapılandırmalar bu ağ cihazları üzerindede yapılmıştır. Yapılan konfigirasyon neticesinde tanımlanan sanal ağlarda ağ anahtarlama cihazları sayesinde bütün ağ cihazları ile haberleşmesi sağlanmıştır.

Şekil 6.75: Ana ağ anahtar cihazı üzerinde yapılan sanal ağ tanımı

Şekil 6.75 de omurga ağ anahtarıcı cihazı üzerinde sanal ağlar tanımlanmış ve bu sanal ağlarının dağıtım ağ cihazı ile haberleşmesi için dağtım cihazı ile ana omurga cihazına bağlı portlar bir biri ile tagget fonksiyonu ile haberleştirilmiştir.

```
SSH@      -Dagitim(config)#vlan 2000 name OGRENC_TEST_VLAN
SSH@      -Dagitim(config-vlan-2000)#vlan 2001
SSH@      -Dagitim(config-vlan-2001)#vlan 2001 na
  name      VLAN name
SSH@      -Dagitim(config-vlan-2001)#vlan 2001 name AKADEMI_TEST_VLAN
SSH@      -Dagitim(config-vlan-2001)#vlan 2002 na
  name      VLAN name
SSH@      -Dagitim(config-vlan-2001)#vlan 2002 name BIM_TEST_VLAN
SSH@      -Dagitim(config-vlan-2002)#vlan 2003 n
  name      VLAN name
SSH@      -Dagitim(config-vlan-2002)#vlan 2003 name IDARI_TEST_VLAN
SSH@      -Dagitim(config-vlan-2003)#vlan 2004 name SERVER_TEST_VLAN
SSH@      -Dagitim(config-vlan-2004)#
SSH@      -Dagitim(config-vlan-2004)#
```

Şekil 6-76: Dağıtım ağ anahtarlama cihazı yapılandırması

Şekil 6.76 da dağıtım anahtarlama cihazı üzerinde sanal ağlar oluşturulmuştur ve tagget fonksiyonu ile kenar ağ anahtarlama cihazlarına haberleşmesi sağlanmıştır

```
PORT-VLAN 2004, Name SERVER_TEST_VLAN, Priority level0, Spanning tree O
 Untagged Ports: None
   Tagged Ports: (U1/M1)   1   2   3   4
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
SSH@      -Kenar  (config-vlan-2004)#show vlan 2003
Total PORT-VLAN entries: 32
Maximum PORT-VLAN entries: 256

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 2003, Name IDARI_TEST_VLAN, Priority level0, Spanning tree O
 Untagged Ports: None
   Tagged Ports: (U1/M1)   1   2   3   4
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
SSH@      -Kenar  (config-vlan-2004)#show vlan 2002
Total PORT-VLAN entries: 32
Maximum PORT-VLAN entries: 256

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 2002, Name BIM_TEST_VLAN, Priority level0, Spanning tree On
 Untagged Ports: None
   Tagged Ports: (U1/M1)   1   2   3   4
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
SSH@      -Kenar  (config-vlan-2004)#show vlan 2001
Total PORT-VLAN entries: 32
Maximum PORT-VLAN entries: 256

Legend: [Stk=Stack-Id, S=Slot]

PORT-VLAN 2001, Name AKADEMI_TEST_VLAN, Priority level0, Spanning tree On
 Untagged Ports: None
   Tagged Ports: (U1/M1)   1   2   3   4
   Uplink Ports: None
 DualMode Ports: None
 Mac-Vlan Ports: None
     Monitoring: Disabled
SSH@      -Kenar  (config-vlan-2004)#
```

Şekil 6-77 Kenar ağ anahtarlama cihazı yapılandırması

Şekil 6.77' de kenar ağ cihazı sanal ağ tanımları yapılmış ve tagget fonksiyonu ile diğer ağ cihazlarına bağlı portların tanımları yapılmıştır.

7. 802.1X STANDARDI TEZ ÇALIŞMASI KIMLIK DOĞRULAMA, SANAL AĞ VE İNTERNET BAĞLANTISI TESTI

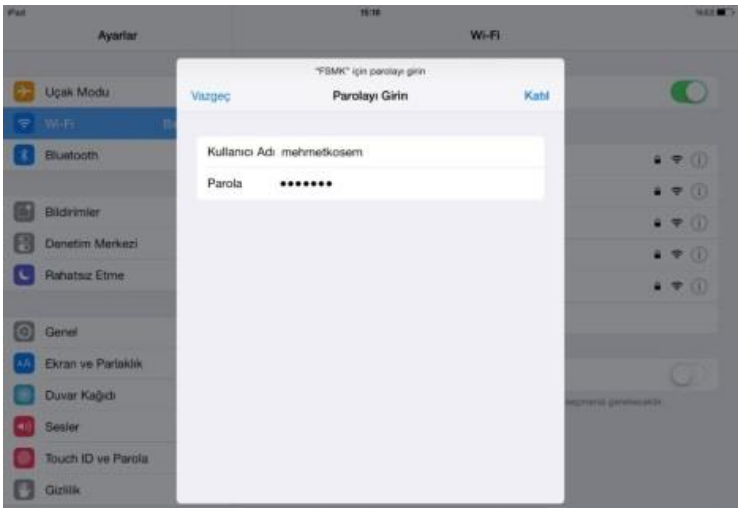
Tezin çalışmasında yapılan çeşitli analizlerle oluşturalan tasarımın 802.1x standardının güvenlik yapısı sanal ağ mimarisi ile bir ünüversitede kablosuz ağ güvenliğinin geliştirilmesi ve farklı işletim sistemlerin de işlevselliği test edilmiştir. Üniversitede fsmk adında bir Ssıd yayınlanmış ve kullanıcıların bu Ssıd üzerinden üniversite tarafından kendilerine verilen kullanıcı adı ve şifresi ile 802.1x standart kapsamında güvenlikli bir bağlatı hedeflenmiştir.

Tezin uygulama testinde Mehmet kösem adlı kullanıcının fsmk ssid ile bağlatı isteğinde bulunup sistem içerisinde idari personel gurubunda yer almaktadır.802.1x standardına göre kimliği doğrulandıktan sonra idari_test sanal ağından 10.10.3.x li bir ip adresi alması ve default gateway (ip yöneticisinin)10.10.3.1 olması hedeflenmekte ayrıca standardın ios işletim sisteminde çalışabilirliği test edilmektedir.

Çizelge 5.3:Sanal ağ tasarımı

Vlan isim	Tag id	Ip adres	netmask	Default gateway	Dhcp server
Ogrenci_test	2000	10.10.0.2	255.255.255.0	10.10.0.1	10.10.0.1
Akademi_Test	2001	10.10.1.2	255.255.255.0	10.10.1.1	10.10.1.1
Bim_Test	2002	10.10.2.2	255.255.255.0	10.10.2.1	10.10.2.1
İdari_Test	2003	10.10.3.2	255.255.255.0	10.10.3.1	10.10.3.1
Server_test	2004	10.10.4.2	255.255.255.0	10.10.4.1	10.10.4.1

İos işletim sisteminde 802.1x standardı işlevselliği test süreci

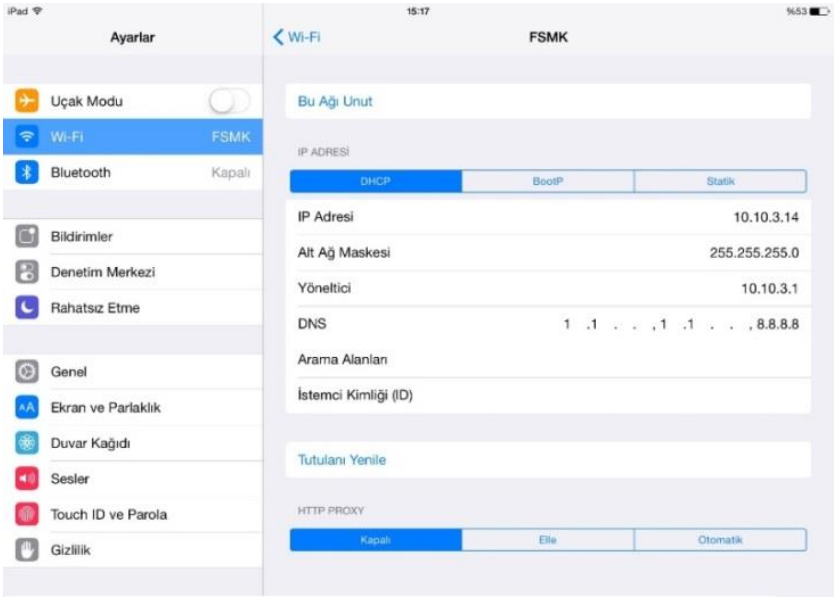


Şekil 7.1: İos kullanıcı adı ve şifre ekranı

Şekil 7.1'de ios işletim sistemi üzerinden kullanıcı adı ve şifresini girerek Mehmet kösem 802.1x standardı kimlik kanıtlama yöntemi ile istekte bulunmuştur.

Şekil 7.2: Sertifika doğrulama ekranı

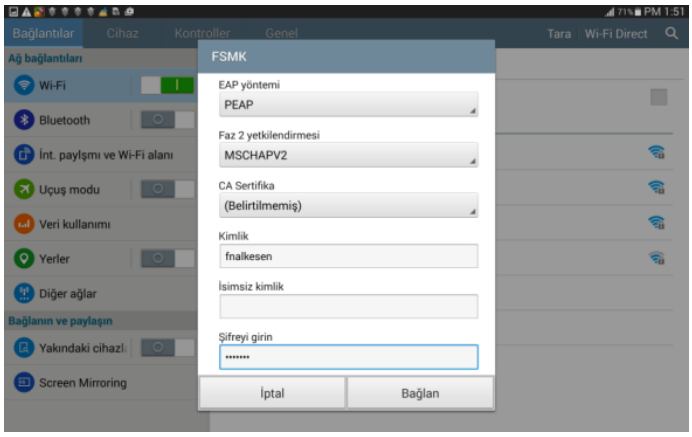
Şekil 7.2'da 802.1x standardı için kimlik doğrulaması gerçekleşmiş ve arada güvenli bağlantı için sisteme daha önce kurmuş olduğumuz sertifika servisi devreye girmiştir.



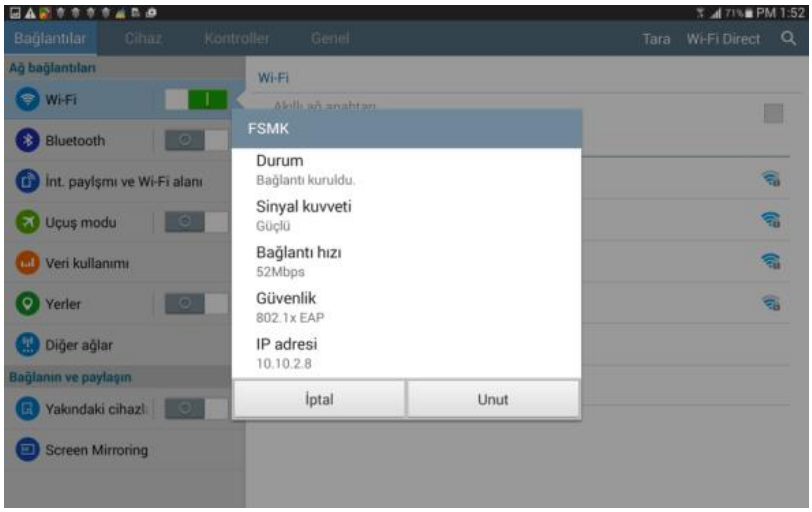
Şekil 7.3: 802.1x denetiminden sonra ağ bilgileri

Şekil 7.3' de 802.1x standardının üniversite test uygulamasında Mehmet kosem adlı kullanıcı. Tez çalışamasın içerisinde kullanılan kablosuz ağ sistemlerin tümünden başarılı bir şekilde geçtikten sonra güvenlik duvarı kullanıcının bağlı olduğu sanal ağ numarasına göre İdari_test için belirlenen ip aralığın'dan 10.10.3.14 ip adresini atamış, default gateway 10.10.3.1 ve kullanıcı ios işletim sistemi ile siteme erişim sağlamıştır.

Android işletim sisteminde 802.1x standardı tez çalışasının işlevselliği test süreci



Şekil 7.4 : Android işletim sistemi kullanıcı adı ve şifre bilgi ekranı

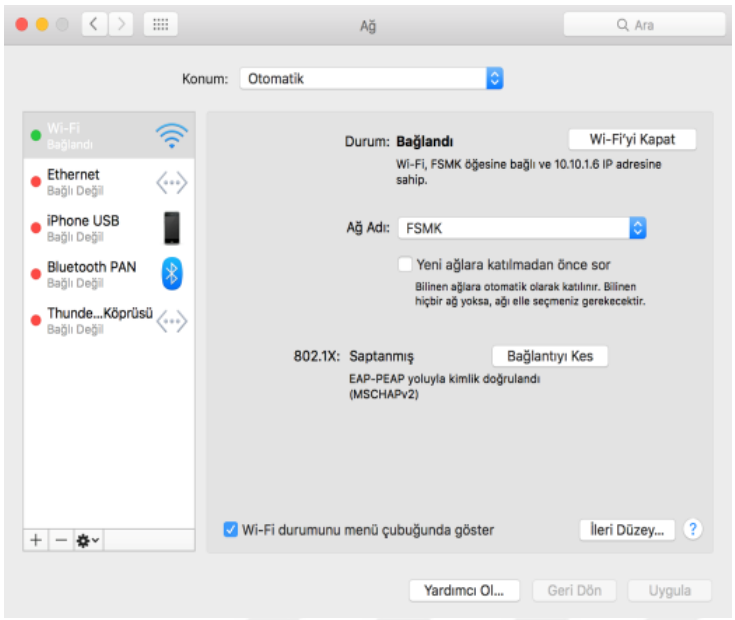


Şekil 7.5: Android işletimi ağ bilgi ekranı

Şekil 7.5'de 802.1x standardının üniversite test uygulamasında Fatih Nalkesen adlı kullaıcı tez çalışmasındaki kullanılan sistemlerin hepsinden başarılı bir şekilde geçtikten sonra güvenlik duvarı kullanıcının bağlı olduğu sanal ağ numarasına göre BİM_test için belirlenen ip Aralığından 10.10.2.8 ip adresini almış, default gateway 10.10.2.1 ve kullanıcı Android işletim sistemi ile siteme bağlanmıştır.

Mac Os işletim sisteminde 802.1x standardı tez çalışmasının işlevselliği test süreci.

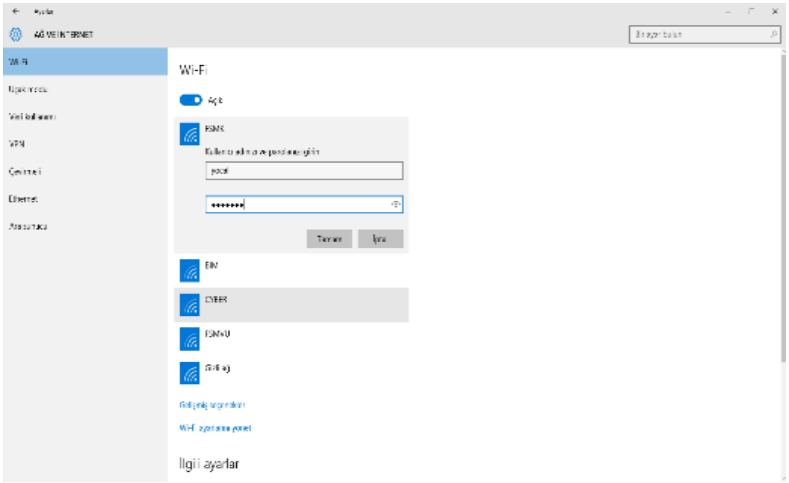
Şekil 7.6: Mac Os Kullanıcı bilgi ve şifre giriş ekranı



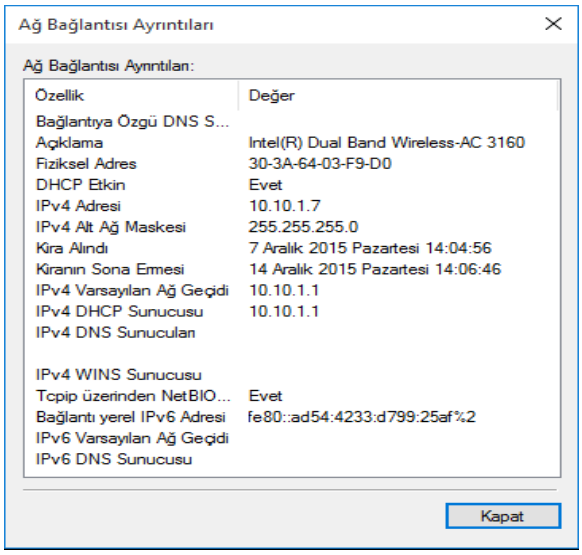
Şekil 7.7: Mac Os ağ bilgi ekranı

Şekil 7.7'te 802.1x standardının üniversite test uygulamasında Emre Ak adlı kullaıcı Tez çalışmasında kullanılan sistemlerin hepsinden başarılı bir şekilde geçtikten sonra güvenlik duvarı kullanıcının bağlı olduğu sanal ağ numarasına göre Akademik_test için belirlenen ip aralığından 10.10.1.6 ip adresini almış , default gateway 10.10.1.1 ve kullanıcı Mac OS işletim sistemi ile siteme başarılı ve güvenli bir şekilde erişmiştir.

Windows işletim sisteminde 802.1x standardı tez çalışasının işlevselliği test süreci



Şekil 7.8: Windows kullanıcı ve şifre giriş ekranı



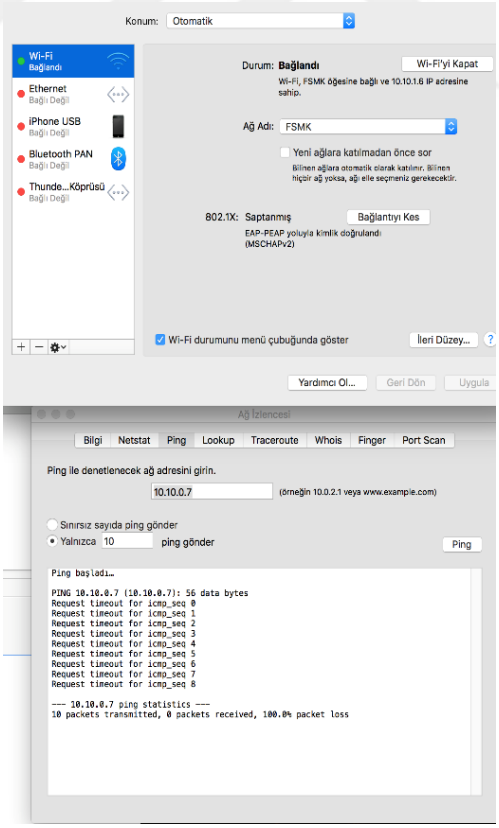
Şekil 7.9: Windows ağ bilgi ekranı

Şekil 7.9'da 802.1x standardının üniversite test uygulamasında Yakup öcal adlı kullanıcı Tez Çalışmasında kullanılan sistemlerin hepsinden başarılı bir şekilde geçtikten sonra güvenlik duvarı kullanıcının bağlı olduğu sanal ağ numarasına göre Akademi_test için belirlenen ip aralığından 10.10.1.7 ip adresini almış, default gateway 10.10.1.1 ve kullanıcı Windows işletim sistemi ile kablosuz ağ sistemine erişim sağlamıştır.

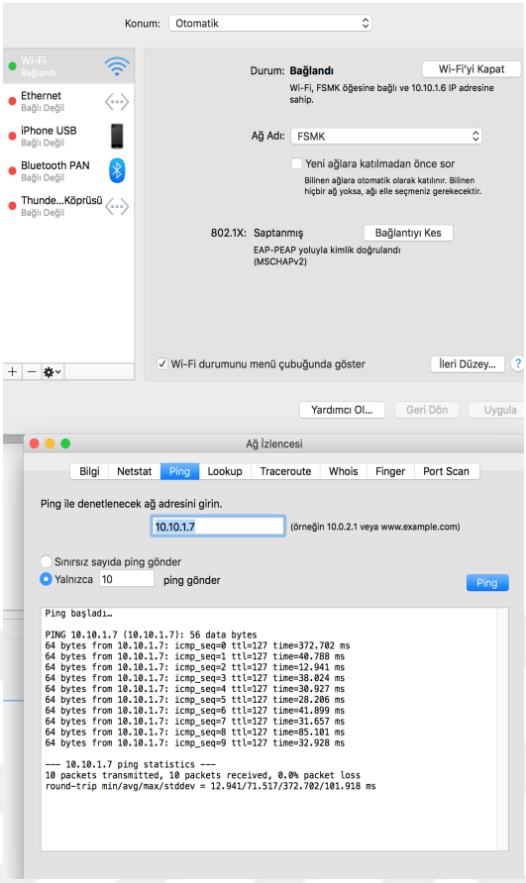
7.1 802.1x standardı tez çalışmasının sanal ağ haberleşme ve internet erişimi testi

Kullanıcılar 802.1x standardı ile farklı işletim sistemileri ile kullanıcıların farklı sanal ağlara bağlantısı test edilmiş ve standardın tez çalışasında üniverisitede test ortamında uygulanmıştır. Hedeflenen 802.1x standardında sanal ağ mimarisi ile sistemin daha güvenilir bir şekilde üniversitede kullanıcıların bağlı bulundukları sanal ağların yetki seviyelerine göre sanal ağların birbiri ile haberleşmesinin kısıtlanması veya sanal ağlarını tamamı ile birbiri ile haberleşmesinin önüne geçilmesidir bu sayede üniversite içerisinde örnek olarak öğrenci ağındaki bir kullanıcının akademik ağdaki bir kullanıcıya erişimi kapatılarak akademik ağ içerisinde paylaşılan bir bilginin güvenliğini ve akademik ağın güvenliğini arttırmaktır

Test: Eak kullanıcısı 802.1x standardı ile kimliği doğrulandıktan sona akademik sanal ağ üzerinden sisteme erişmiş ve bir ip almıştır hedeflenen testte akademik ağ içerisinde olduğu için akademik ağ ile haberleşebilmesi fakat ogrenci ağı ile haberleşememesi;

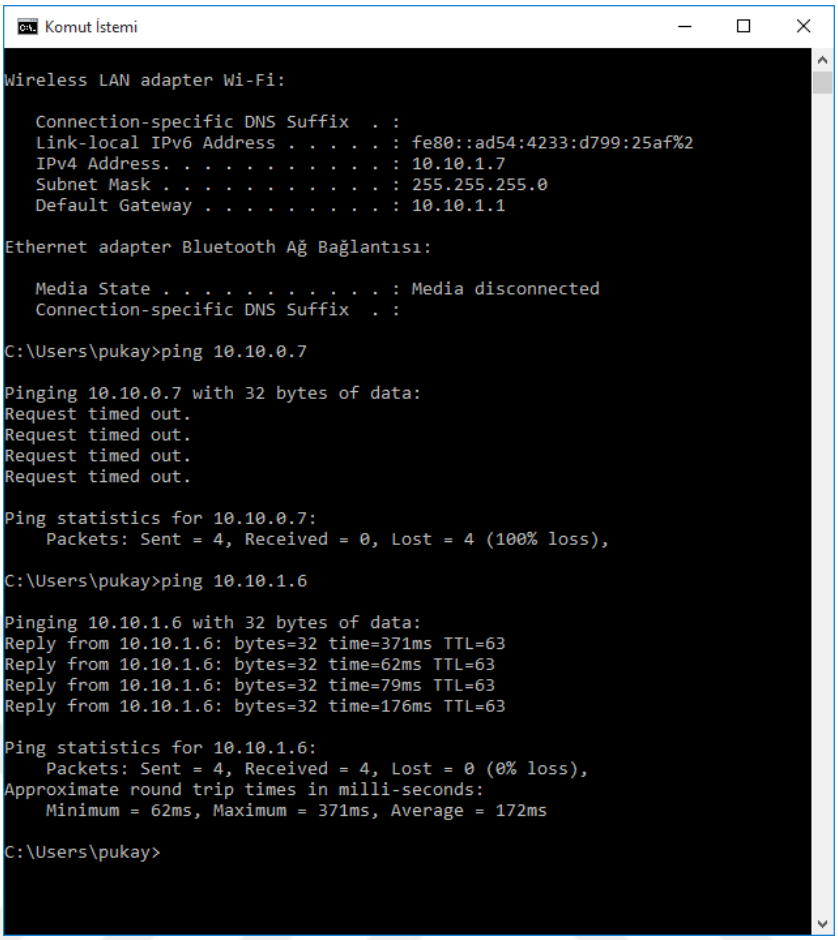


Şekil 7.10: Komut sistemi ekranı 1

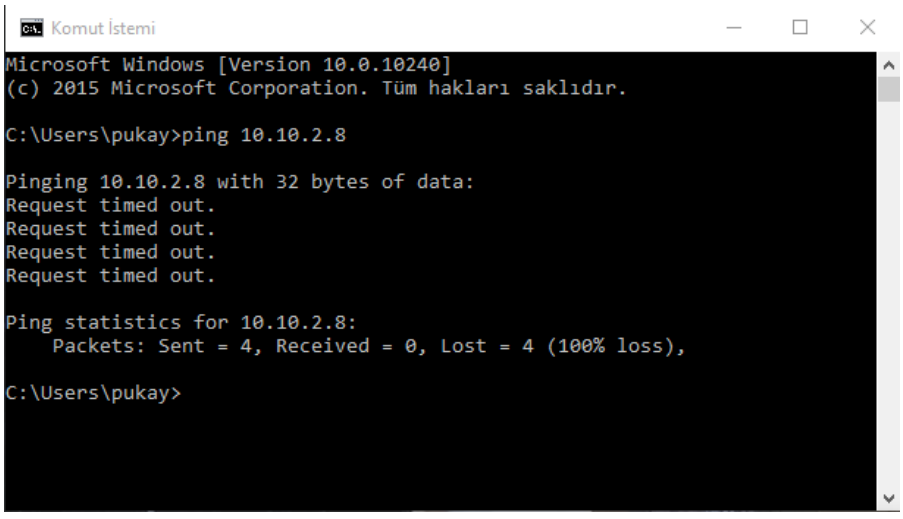


Şekil 7.11 Komut sistemi ekranı 2

Test sonucu şeki 7.11'de ogrenci sanal ağı ile erişimi kapatılmış akademik ağ ile erişimi mevcuttur. Yocal kullanıcısı 802.1x standardı ile sisteme erişim sağlanmış ve Akademik sanal ağdan ip almıştır teste birden fazla sanal ağa erişim kapatılması test edilmiştir.



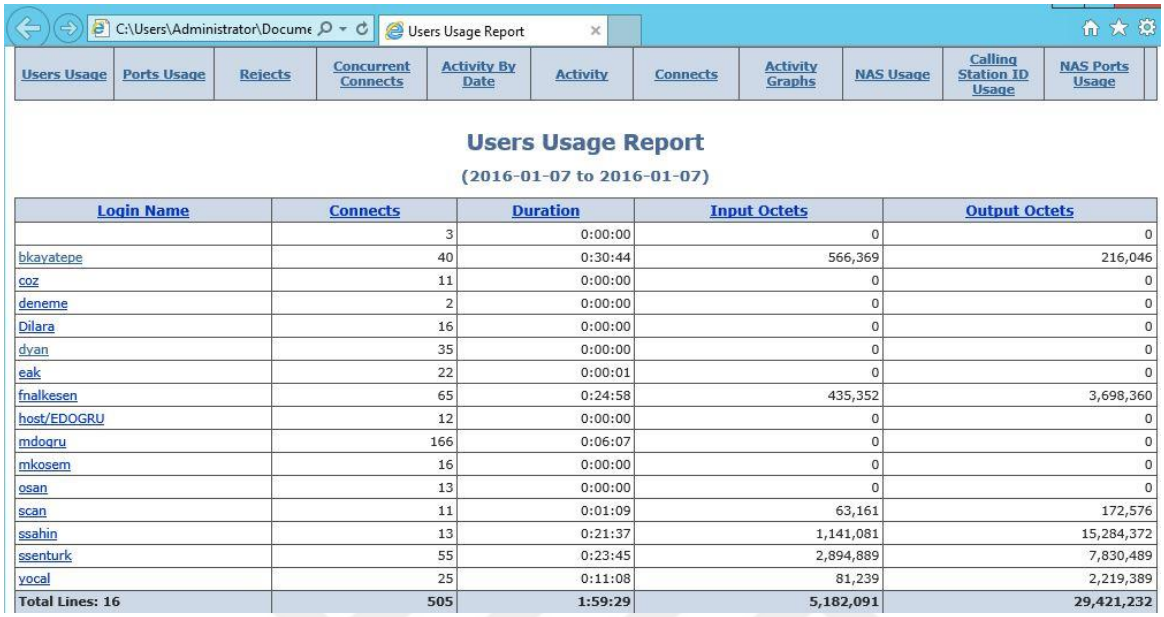
Şekil 7.12: Komut sistemi ekranı 1



Şekil 7.13: Komut sistemi ekranı 2

Test sonucu kullanıcı akademik sanal ağ içerisinde erişimi mevcut fakat ogrenci sanal ağı ve idari sanal ağına erişimi mevcut değildir.

7.2 Kullanıcı log raporları



C:\Users\Administrator\Docume Users Usage Report

Users Usage | Ports Usage | Rejects | Concurrent Connects | Activity By Date | Activity | Connects | Activity Graphs | NAS Usage | Calling Station ID Usage | NAS Ports Usage

Users Usage Report

(2016-01-07 to 2016-01-07)

Login Name	Connects	Duration	Input Octets	Output Octets
	3	0:00:00	0	0
bkayatepe	40	0:30:44	566,369	216,046
coz	11	0:00:00	0	0
deneme	2	0:00:00	0	0
Dilara	16	0:00:00	0	0
dyan	35	0:00:00	0	0
eak	22	0:00:01	0	0
fnalkesen	65	0:24:58	435,352	3,698,360
host/EDOGRU	12	0:00:00	0	0
mdogru	166	0:06:07	0	0
mkosem	16	0:00:00	0	0
osan	13	0:00:00	0	0
scan	11	0:01:09	63,161	172,576
ssahin	13	0:21:37	1,141,081	15,284,372
ssenturk	55	0:23:45	2,894,889	7,830,489
vocal	25	0:11:08	81,239	2,219,389
Total Lines: 16	**505**	**1:59:29**	**5,182,091**	**29,421,232**

Şekil 7.14: Kullanıcı raporları 1

Şekil 7.14'de Tez çalışmasında üniversite kullanımı için yapılan tasarıların, kullanılan materyallerin kurum ve yapılandırma işlemleri sonucunda 802.1x standardı ile kimlik doğrulandıktan sonra ağ mimarisi ile birlikte sisteme erişim sağlamış kullanıcı listesi.

Şekil 7.15: 802.1x standardı ile sisteme erişim sağlamış kullanıcı özellikleri

Şekil 7.15'de suat sahin kullanıcısını 802.1x standardı ile kimlik tesbitinden sonra sisteme bağladığı özleliklerin log programındaki listesi yer almaktadır. Kullanıcının erişiminden sonra aldığı ip adresi, bağlandığı policyle, sisteme erişim zamanı, nas port id gibi özelliklerin listelendiği alandır.

Start Date Time	User Name	Stop Date Time	Duration	User IP	Output Octets	Input Octets	Connect Request	Connect Re...
01/07/2016 15:06:57	ssahin	01/07/2016 15:26:21	00:19:24	10.10.3.3	14,422,783	1,120,913	IAS_SUCCESS	Finished
01/07/2016 15:17:17	fnalkesen	01/07/2016 15:20:43	00:03:26	10.10.2.4	73,100	35,511	IAS_SUCCESS	Finished
01/07/2016 14:53:29	fnalkesen	01/07/2016 15:09:09	00:15:40	10.10.2.3	3,625,260	399,841	IAS_SUCCESS	Finished
01/07/2016 15:25:33	scan	01/07/2016 15:26:42	00:01:09	10.10.0.5	172,576	63,161	IAS_SUCCESS	Finished
01/07/2016 15:09:54	ssenturk	01/07/2016 15:16:34	00:06:40	10.10.0.4	1,625,967	1,072,463	IAS_SUCCESS	Finished
01/07/2016 15:27:29	ssenturk	01/07/2016 15:29:16	00:01:47	10.10.0.4	2,224,482	623,113	IAS_SUCCESS	Finished
01/07/2016 15:29:22	ssenturk	01/07/2016 15:29:33	00:00:11	10.10.0.4	0	0	IAS_SUCCESS	Finished
01/07/2016 15:29:51	ssenturk	01/07/2016 15:33:49	00:03:58	10.10.0.4	0	0	IAS_SUCCESS	Finished
01/07/2016 15:09:28	bkayatepe	01/07/2016 15:43:13	00:33:45	10.10.0.3	33,589,101	2,284,285	IAS_SUCCESS	Finished

Şekil 7.16: Sisteme erişim sağlamış kullanıcıların kısa bilgileri

Şekil 7.16'da sisteme erişim sağlamış kullanıcılar sistem üzerinde oluşturmuş olduğu tırafiğin izlene bildiği log ekranı;

Ports Usage Report

(2016-01-07 to 2016-01-07)

Port	Connects	Duration	Input Octets	Output Octets
0	2	0:02:13	20,168	861,589
12,289	94	0:43:00	710,769	2,608,011
12,290	108	0:19:24	1,120,913	14,422,783
12,291	31	0:00:01	0	0
12,292	31	0:15:40	399,841	3,625,260
12,293	107	0:00:00	0	0
12,294	55	0:23:45	2,894,889	7,830,489
12,295	51	0:15:17	35,511	73,100
12,296	26	0:00:09	0	0
Total Lines: 9	505	1:59:29	5,182,091	29,421,232

Şekil 7.17: Port erişim rapor ekranı

Şekil 7.17' de Sisteme 802.1x standardı ile erişim sağlamış kullıcılara atanan port ekranı;

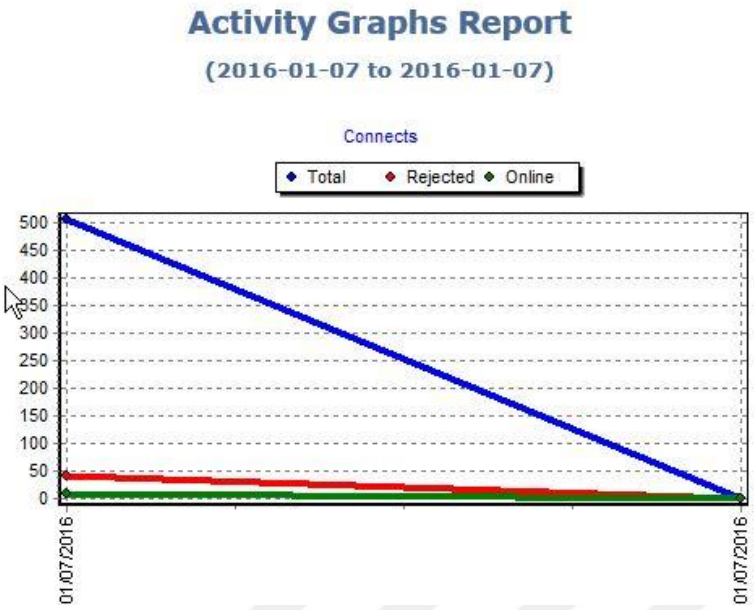
Rejects Report

(2016-01-07 to 2016-01-07)

Start DateTime	User Name	Terminate Cause
01/07/2016 14:40:36	fnalkesen	The certificate that the user or client computer provided to NPS as proof of identity chains to an enterprise root certification authority that is not trusted by the NPS server.
01/07/2016 14:40:45	deneme	The client could not be authenticated because the EAP type cannot be processed by the server.

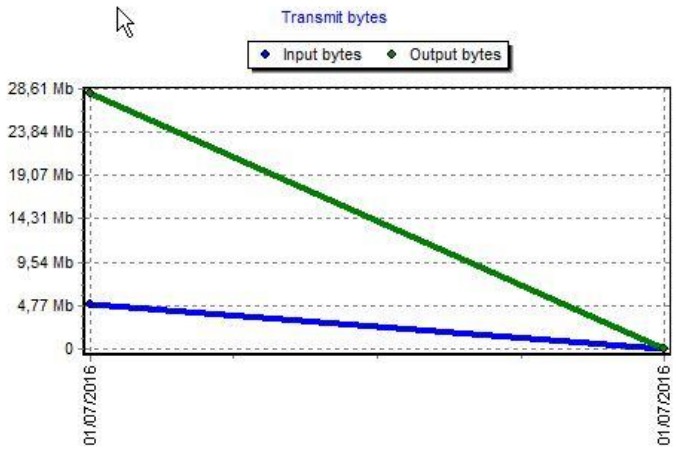
Şekil 7.18: Erişim sağlayamamış kullınıcı raporu

Şekil 7.18'de sisteme 802.1x satandardı kapsamında erişim sağlayamamış kullanıcıların log ekranı yer almaktadır.



Şekil 7.19: Kullanıcı bağlatı sayısı

Şekil 7.19'da sisteme erişim sağlamış kullınıcınların grafiksel görüntüsü yer almaktadır.



Şekil 7.20: Kullanıcıların sistem üzerindeki kullanılan veriboyutu

Şekil 7.20'de sistem içerisinde kullanılan veri logu yer almaktad

8 SONUÇ VE ÖNERİLER

Teknolojinin gelişimi ile birlikte Kablosuz ağların kullanımı her geçen gün artmaktadır. Kullanım oranının artması ile birlikte kimlik doğrulama ve kablosuz ağ güvenliği ile ilgli birçok çalışma yapılmaktadır.

Bu tez çalışmasında Kablosuz ağ güvenlik yöntemleri üzerinde çalışılmış ve Kablosuz ağ sisteminde kimlik doğrulama ve erişim konrolü için 802.1x standardı önerilmiştir.

Çalışmada gerçekleştirilen testler ve uygulamalar neticesinde 802.1x standardının üniversite kablosuz ağ güvenliğinde kullanımı için analizler neticesinde donanım ve yazılım materyalleri bağımsız tasarılar önerilmiştir.

Çalışmada 802.1x sıtandardının kablosuz ağ güvenliğinde Kimlik doğrulandıktan sonra Ağ sistemi güvenliğini arttırmak için sanal ağ teknolojisi ile birlikte kullanımı önerilmiştir.

Çalışmada 802.1x standardı Eap Yöntemleri incelenmiş Eap (PEAP) ve EAP MSCHAPV2 Birlik te kullanıldığında veri iletişimindeki şifreleme ve verinin dinlenmesi veya dinlenen verininin anlamlı sonuçlara ulaşabilmesinin henüz çözülemediği için birlikte kullanımı önerilmiştir.

Bu tez çalışmasında kablosuz ağ güvenliğinde kimlik doruğlama sunucusu, Serifika sunucusu, Dizin hizmeti sunucusu, Erişim Noktası kontrolülürü, Ağ anahtarlama cihazı, Güvenlik duvarı cihazlarının test ortamı oluşturulmuş ve Üniversitede 802.1x standardı için yapılandırma işlemleri gerçekleştirilmiştir. Test sonuçlarında sonra raporları alınmış ve üniversiteler için yöntem önerilmiştir

KAYNAKLAR

[1] Marsic I. , 2010, ”Computer Networks” , Rutgers University, New Jersey

[2] TCP/IP Overview, Document ID:13769, Cisco System Inc., 2005

[3] Da˜nobeitia-Paul B., Ferrer-Gomila J. L., Femenias G., 2008, ” Cross-layer architecture design in wireless networks”, Mobile Communication Group

[4] Merve KINAY,Kablosuz Ağlar (Wıreless Networks) Ve Kablosuz Ağlarda Güvenlik,Yüksek Lisans Tezi 2005

[5] Lehr, W., Chapin, J., “On The Convergence of Wired and Wireless Access Network Architectures”, Information Economics and Policy, 22(1), 33-41, 2010.

[6] Hung, K., Bensaou, B., “Throughput Analysis and Bandwidth Allocation for IEEE 802.11 WLAN with Hidden Terminals”, Journal of Parallel and Distributed Computing, 71(9) , 1201-1214, 2010.

[7] Calder, A., “Nine Steps to Success: An ISO 27001 Implementation Overview”, IT Governence Institute Conference, (2006)

İnternet kaynakları:

Url-1<http://www.msxlabs.org/forum/bilgisayar/51750-bilgisayar-agi-network-nedir.html>
Url-2<www.hasanbalik.com/dersler/trakya/10-11Bahar/Eser%20Sert/Kablosuz%20A%C4%9F%20Protokolleri.docx>
Url-3<http://slideplayer.biz.tr/slide/1905527/>
Url-4< www. lerningnetwork.cisco.com, OSI Model Concepts>
Url-5<http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/55.html>
Url-6<www.beyaz.net/tr/dokumanlar/katman-katman-katmerli-osi-modeli.html>
Url-7<http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/55.html>
Url-8<bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/tcp-ip-protokol%C3%BC>
Url-9<http://windows.microsoft.com/tr-tr/windows/what-are-wireless-network-security-methods#1TC=windows-7>
Url-10< tr.wikipedia.org/wiki/IEEE_802.1X>
Url-11<https://technet.microsoft.com/tr-tr/library/Cc782851(v=WS.10).aspx>
Url-12<http://csirt.ulakbim.gov.tr/dokumanlar/Ag_Kimlik_Denetimi.pdf>
Url-13<http://docs.comu.edu.tr/howto/8021x-howto-intro.html>
Url-14< http://mburakakkoc.blogspot.com.tr/>
Url-15<http://docs.comu.edu.tr/howto/ldap-howto-intro.html>
Url-16<http://www.mertnekarman.com/?tag=active-directory-nedir>
Url-17< http://www.yavuztasci.com/>
Url-18< http://www.mshowto.org/radius-nedir.html>
Url-19<yunus.hacettepe.edu.tr/~b0145561/bilg_aglar.html>

ÖZGEÇMİŞ

MEHMET KÖSEM

İletişim Bilgileri

E-Posta: mehmetkosemm@gmail.com
Adres Bilgileri: Türkiye - İstanbul(Asya) - Üsküdar - bulgurlu

Kişisel Bilgiler

Toplam Tecrübe: 11 Yıl
Eğitim Durumu: Yüksek Lisans
Medeni Durumu: Evli
Uyruk: Türkiye Cumhuriyeti
Doğum Yeri: Türkiye - Manisa

Eğitim Bilgileri

Üniversite(Yüksek Lisans)2016
İstanbul Aydın Üniversitesi
Fen Bilimler Enstitüsü, Bilgisayar Mühendisliği -*Destek Bursu (%50)*
Üniversite (Lisans)2010
Near East Universty - (Örgün Öğretim)-Destek Bursu(%25)
Mühendislik Fakültesi, Bilgisayar Mühendisliği(*İngilizce*)
Üniversite (Ön Lisans)2003
Yüzüncü Yıl Üniversitesi - *(Örgün Öğretim)*
Bilgisayar Bilimleri Fakültesi, Bilgisayar programcılığı (*Türkçe*)
Lise,1998
İzmir Namık Kemal Lisesi(Fen bilimleri bölümü)

İş Deneyimleri
Daire Başkanı
Fatih Sultan Mehmet Vakıf Üniversitesi
07.2010-... (6 yıl) İstanbul(Avr.) Tam Zamanlı
Bilgisayar Öğretmeni
Özel İzmir Atılım Bilgisayar Ve Yabancı Dil Kursu
06.2005-10.2006 (1 yıl, 4 ay) İzmir Tam Zamanlı

Bilgisayar Öğretmeni
MESLEKİ TEKNİK EĞİTİM LİSESİ
03.2003-06.2005 (2 yıl, 3 ay) Manisa Tam Zamanlı