Uluslararası Teknolojik Bilimler Dergisi
International Journal of Technological Sciences
Elektronik Dergi, e-ISSN: 1309-1220
Cilt/Volume: 11 Sayı/Number: 2 Sayfa/Page: 108-117 Nisan/April 2019

Dinamik VLAN Yapılandırmasının Kablosuz Yerleşke Alan Ağlarında Performans Analizi

Muhammed Fatih TARLACI, Gürcan ÇETİN*, Mahmut TENRUH
*Muğla Sıtkı Koçman Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği, Muğla

(Alınış Tarihi/Received: 24.07.2019, Kabul Tarihi/Accepted: 02.08.2019)
*İlgili yazar/Corresponding Author: gcetin@mu.edu.tr

Anahtar Kelimeler
Ağ performansı
Dinamik VLAN
FreeRadius
LDAP

Özet: Günümüzde kablosuz ağlar son kullanıcıların yanı sıra özel sektör ve kamu kurumlarının ihtiyaç ve beklentileri doğrultusunda şekillenmektedir. Bu beklentilerin en başında yönetilebilir ve güvenli kablosuz ağların oluşturulması gelmektedir. Bu nedenle, kablosuz bir ağa kimin, nereden, nasıl ve hangi yetkilerle bağlanması gerektiği özenli bir planlama gerektirmektedir. Bu çalışmada, Muğla Sıtkı Koçman Üniversitesi (MSKÜ) Eduroam (Education Roaming) ağında dinamik VLAN ataması gerçekleştirilerek öğrenci, personel ve misafirlerin ağa katılımında kural tabanlı bir altyapı oluşturulmuştur. Oluşturulan dinamik VLAN yapısı, tüm kullanıcıların kablosuz ağda tek bir VLAN altında tutulduğu statik VLAN yapılandırılması ile ağda oluşan kullanıcı sayıları, trafik ve genel yayın (broadcast) değerleri açısından karşılaştırılmış ve sonuçlar analiz edilmiştir.

Performance Analysis of Dynamic VLAN Configuration on Wireless Campus Area Networks

Keywords
Network performance
Dynamic VLAN
FreeRadius
LDAP

Abstract: Wireless networks are formed according to the requirements and expectations of the private sector and public institutions, as well as the end users. The most prominent one in these expectations is to form manageable and secure wireless networks. That is why it is necessary to plan wireless networks carefully about whom and where to access, how and with what permissions. In this study, a dynamic VLAN assignment has been established in Muğla Sıtkı Koçman University (MSKU) Eduroam (Education Roaming) network, and a rule-based infrastructure is applied for the students, staff and guests in the network. The dynamic VLAN structure has been compared with respect to the number of users, traffic and broadcast values in the static VLAN configuration where all users were kept under a single VLAN on the wireless network. Then the results were analyzed.

1. Giriş

Günümüz kurumsal ağlarında Ethernet ölçeklenebilirliğini arttırmak ve kullanıcılar için tanımlanacak ağ politikalarını daha esnek hale getirmek için VLAN (Virtual Local Area Network) kullanımı oldukça yaygındır (Minlan vd., 2011). VLAN yapılandırmasında, ağa dâhil olan cihazların sık sık yer değişmediği ortamlarda VLAN ataması elle yapılabilmektedir. Ancak statik VLAN atama yönteminin kullanıcıların çok sık yer değiştirdiği, IEEE 802.11 standardını temel alan WLAN (Wireless Local Area Network) ağlarında kullanılması mümkün değildir. Bu tür ağ altyapılarında kullanıcı hareketliliğini garanti altına almak için dinamik bir atama yönteminin yanında merkezi bir servis yönetiminin de sağlanması gereklidir. Bu bağlamda, dinamik VLAN atamasında IEEE 802.1Q tabanlı VLAN yöntemi, IEEE 802.1x tabanlı kimlik doğrulama işlemi ile birleştirilerek uygulanır. Böylece ağdaki bir kullanıcı bir ağ anahtarına ya da bir AP (Access Point)'ye bağlandığında, kimlik doğrulama sonucuna göre bir

VLAN'a eklenir. Bu sayede kurumda görevli bir kullanıcı ofis ağına erişebilirken, misafir kullanıcı kullanımı sınırlı olan bir ağa katılır (Yamaki vd., 2015).

Literatür incelendiğinde dinamik VLAN yapılandırma performansının değerlendirildiği farklı çalışmalar bulunmaktadır. Jiang ve arkadaşları (2009) çalışmalarında, yerleşke ağlarında IP telefon ve telefonun arkasında bulunan erişim portuna bağlı olarak çalışan bilgisayarın tek bir port üzerinde farklı VLAN'a atanarak ses trafiğinin önceliklendirilmesi üzerinde durmuşlardır. Çalışmada MAC adresi tabanlı VLAN atama işlemi gerçekleştirilmiştir. Çalışma sonucunda iki IP telefon arasında yüksek kaliteli ve kesintisiz ses iletimi sağlanmıştır. Koerner ve Kao (2016) ise çalışmalarında yerleşke ağlarında dinamik VLAN yapılandırmasının önemine vurgu yapmışlardır. Mininet ortamında gerçekleştirilen çalışma, Wireshark ağ yazılımı ile akış tablolarının gözlemlenmesi yoluyla MAC tabanlı dinamik VLAN etiketlemesinin istikrarlı bir şekilde çalıştığını doğrulamıştır. Dinamik VLAN ile yüksek risk oranına sahip hastane verilerinin hastane içinden ve dışından güvenliğini sağlanmak için yapılan bir çalışmada (Çetin, 2006) ise ağa dâhil olacak tüm cihazlar kimlik kontrolünden geçirilmiştir. Çalışmada kullanıcılar ilgili oldukları alan ve bölümlere göre gruplanmış ve VLAN'lara bölünmüştür. Bu sayede sadece yetkili oldukları alanlarda bilgi ve belgelere ulaşmaları sağlanmıştır. Diğer taraftan, Kırışoğlu ve arkadaşları (2019) genel ağ performansını arttırmak için VLAN'larda yük dengelemesi sağlayacak SNMP (Simple Network Management Protocol) tabanlı bir algoritma geliştirmişlerdir. Çalışmada, aynı güvenlik düzeyine sahip VLAN'lardaki toplam trafiğe göre, kullanıcıların VLAN üyelikleri dinamik olarak değiştirilmiştir.

İlgili literatür çalışmalarında, dinamik VLAN yapılandırmasının performansını geniş ölçekli kablosuz kurumsal bir ağ üzerinde test eden bir çalışmaya rastlanamamaktadır. Bu açıdan değerlendirildiğinde VLAN yapılandırmalarının geniş ölçekli kurumsal bir ağda karşılaştırmasını sunan bu çalışma literatüre katkı sağlamayı amaçlamaktadır. Çalışmada performans testleri MSKÜ kablosuz Eduroam ağında gerçekleştirilmiştir. Test ağında kullanıcıların kimlik doğrulama, yetkilendirme ve kayıt tutma işlemleri için RADIUS sunucu ve dizin hizmetlerine erişim için OpenLDAP sunucu kullanılmıştır. Ağ ile ilgili istatiksel bilgiler ise SNMP protokolü ve CACTI programı kullanılarak toplanmıştır. Çalışmada ağ performansı değerlendirilirken ağdaki kullanıcı sayısı, kimlik doğrulama yöntemleri, genel yayın paket sayıları ve WLC (Wireless Network Controller) portlarında izlenen toplam trafik göz önünde bulundurulmuştur.

Çalışmanın ilerleyen bölümleri şu şekilde organize edilmiştir; materyal ve yöntem bilgilerine Bölüm 2'de yer verilmiş, çalışmada kullanılan ağ kavramları açıklanmıştır. Test ağ altyapısına ait ayrıntılı içerik Bölüm 3'de sunulurken, Bölüm 4 ve Bölüm 5 ile VLAN yapılandırma testlerinin sonuçları değerlendirilmiştir.

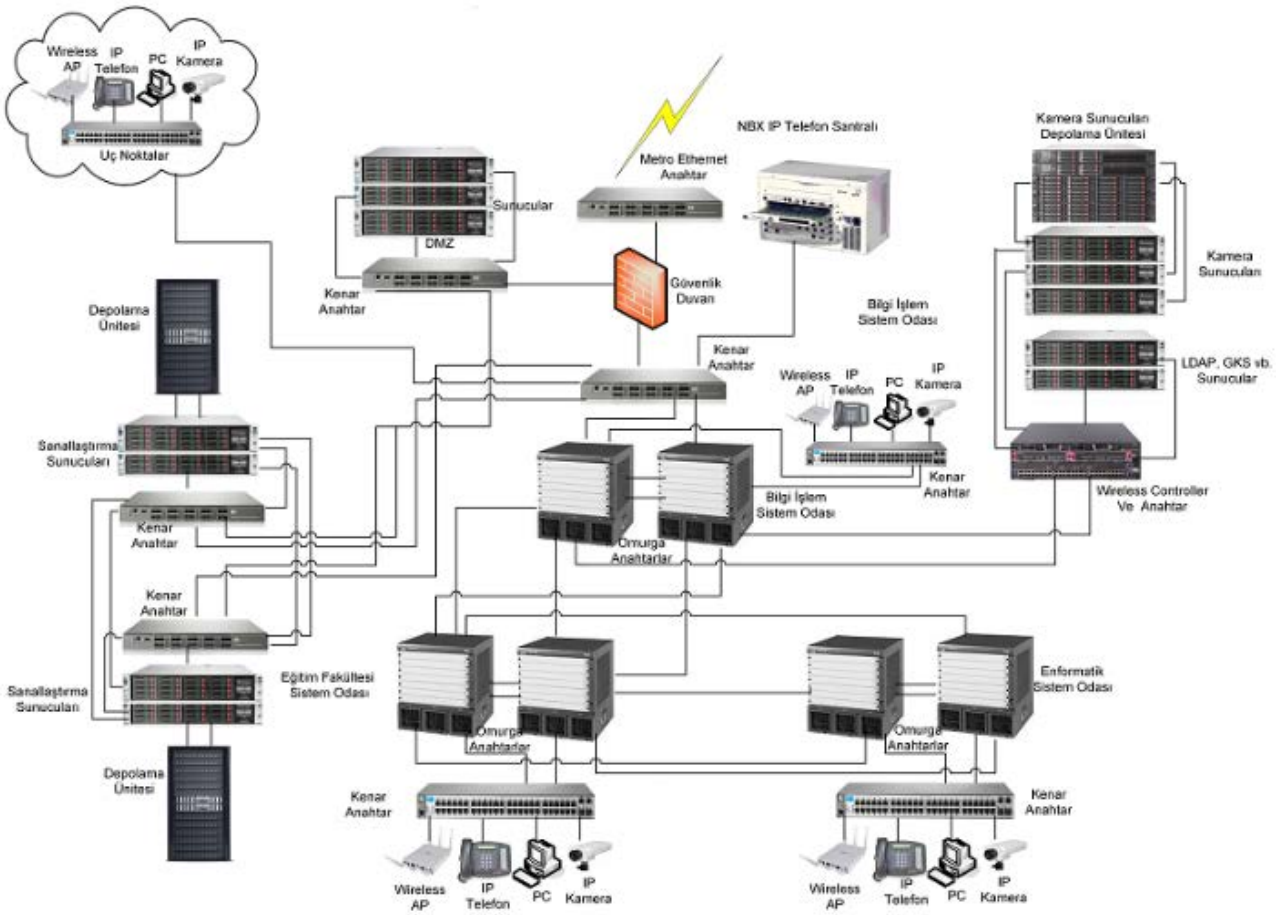
2. Materyal ve Yöntem

2.1. Kablosuz Yerleşke Alan Ağı

Yerleşke Alan Ağları (YAA) genellikle bir veya daha çok yerleşkede birden çok binası bulunan dağıtık yapılardır. YAA'lar da kablosuz hizmetler genellikle mevcut kablolu ağ alt yapısı üzerinden gerçekleştirilir. Örnek bir YAA ağı altyapısı Şekil 1'de verilmiştir. Şekil 1'de görüldüğü gibi YAA çok sayıda aktif cihaz barındırmakta ve TCP/IP protokolü üzerinden çeşitli servisler ağ üzerinde yürütülmektedir. Bu servislerin veri trafiği aynı fiziksel katmanda iletilmektedir. Bir YAA'da IP telefon ile ses trafiği, IP kamera ile video akış trafiği ve bilgisayarların oluşturduğu veri trafiğinin aynı anda çalışması gerekmektedir. Bu amaçla, alt yapının sağlıklı çalışabilmesi için mevcut ağ alt ağlara bölünür ve yönetilir.

2.1.1. Eduroam

Eduroam, uluslararası araştırma ve eğitim topluluğu için geliştirilmiş güvenli, dünya çapında bir internet dolaşım ve erişim hizmetidir. Eduroam üyesi olan kurumlar hem kendi kurumundaki kullanıcıların internete bağlanmasını, hem de diğer Eduroam üyesi kurum kullanıcılarının internete erişimini sağlar (Lopez vd., 2008). Eduroam'un hizmeti hiyerarşik federasyon yapısı ile sağlanır. Her ülkenin veya bölgenin ana RADIUS (Remote Authentication Dial-in User Service) sunucusu bulunur. Domain eki (@domain.edu.tr) ile misafir ağda oturum açmaya çalışan kullanıcının isteği federasyonun üst otoritesi olan ana RADIUS sunucusuna proxy edilir. Ana sunucu isteğin domain ekine göre kullanıcının kendi kurum sunucusuna bu isteği iletir. Yetkilendirmenin başarılı olup olmadığına kullanıcının kendi kurumunun RADIUS sunucusu karar verir. Böylece kullanıcının kimlik ve şifre bilgileri misafir olduğu RADIUS sunucusu tarafından bilinmez.



Şekil 1. Yerleşke Alan Ağı Örneği

2.2. VLAN

Sanal yerel ağ anlamına gelen VLAN, IEEE 802.11Q standardı olarak anılır. Yerel ağ içerisinde çalışma grupları oluşturmak ve yerel ağı mantıksal alt ağlara bölmek için kullanılır (Koerner ve Kao, 2016). Fiziksel olarak aynı ağ içerisinde bulunsalar da farklı VLAN'larda bulunan cihazlar, yönlendirme yapılmaksızın birbirleri ile doğrudan iletişim kuramazlar.

Bir YAA'da bulunan ağ cihazı sayısı binlerce olabilmektedir. Ayrıca aynı ağ anahtarı üzerinde ses, video ve veri trafiği gerçekleştirilebilmektedir. Ses ve video paketleri UDP (User Datagram Protocol) protokolü ile gerçek zamanlı iletilmektedir. Bu servislerin hizmet kalitesinde yaşanacak bir gecikmenin telafisi mümkün olmamaktadır. Bu servisler aynı ağ anahtarı üzerinde gerçekleşse de farklı VLAN yapılandırması ve trafik önceliklendirmesi ile gecikmelerin önüne geçilmeye çalışılmaktadır.

Kullanıcılar ve cihazlar belirli VLAN'lar altında genellikle yerleşim yerine, departmana, güvenlik seviyesine, sunucu ve kaynakların işlevine göre gruplanırlar. Yerleşke ağlarında ağ içerisinde koşan verinin türüne göre, Default VLAN, Data VLAN, Native VLAN, Management VLAN ve Voice VLAN gibi farklı VLAN grupları olabilmektedir.
Statik VLAN atamaları ağ cihazları üzerinde belirli portların gruplanması ile oluşur. Ağ yöneticisi tarafından manuel olarak atanır ve değiştirilmediği sürece aynı kalır. Bu tarz VLAN atamalarına "Port Based VLAN'da denir (Jiang ve Shan, 2008). Özellikle kablolu ağlarda ve ağa dâhil olan cihazların sık sık değişmediği, durağan ağlarda tercih edilir. Yer değiştiren kullanıcılar için yeniden VLAN tanımlaması yapılması gerekmektedir.

2.2.1. Dinamik VLAN

Dinamik VLAN, cihazların ve kullanıcıların sık değiştiği ortamlarda kullanılan VLAN atama yöntemidir. Kablosuz kullanıcının bir YAA içinde hareket ederken aynı VLAN üzerinde kalmasına izin vermek için kullanılır. Dinamik VLAN atamasının ne şekilde yapılacağının belirlenebilmesi için önceden bilgi toplanması gerekir. Başlıca dinamik VLAN atama yöntemleri (Jiang ve Shan, 2008);

MAC Tabanlı VLAN: MAC adresi doğrulamasında ağa dâhil olmak isteyen cihaz ilişkilendirme isteği gönderir. Bir doğrulama sunucusu veya bir MAC listesi aracılığıyla yetkilendirme ve VLAN ataması yapılır.

Protokol Tabanlı VLAN: İlgili port için ayarlanan protokollerin oluşturduğu trafik kabul edilir. Böylece ağda istenmeyen trafik akışının önüne geçilmiş olur.

Kural Tabanlı VLAN: Ağ yöneticisinin belirlediği kurallar çerçevesinde yapılan VLAN atama işlemleridir. VLAN ataması yapılmadan önce kullanıcıların sisteme ne şekilde dâhil olacağı belirlenmiştir. Kullanıcıların profiline, cihaz tipine veya departmanına bağlı kurallar çerçevesinde VLAN ataması yapılabilir. Esnek ve kolay değiştirilebilir bir yapı olmakla birlikte, ilk yapılandırma aşamasında iyi planlama gerektirir.

2.2.1. Dinamik VLAN Gereklilikleri

Kablosuz YAA'lar açısından değerlendirildiğinde dinamik VLAN ataması, ağ yöneticisi tarafından belirlenen kriterler doğrultusunda esnek bir yapı sağlamaktadır. Büyük bir alanda sürekli hareket halinde bulunan kullanıcıların ne zaman ve nereden ağa katılacağını öngörmek güçtür. Çok sayıda kullanıcı tipi ve cihazının bulunduğu bir ortamda tek bir VLAN'da tüm kullanıcıların konumlandırılması birçok sorunu beraberinde getirecektir. Dinamik VLAN kullanımının bu sorunlara getireceği çözümler aşağıda verilmiştir.

Güvenlik: YAA'larda öğrenci, akademik personel, idari personel, yönetici, teknik personel gibi çok sayıda kullanıcı tipi bulunmaktadır. Bu kullanıcıların ağa dâhil oldukları zaman hangi yetkilerle bağlanabilecekleri belirlenmek istenir. Günümüzde siber güvenliğin önemi göz önüne alındığında, aynı VLAN'lar da farklı kullanıcı tiplerinin bulunması istenmemektedir. VLAN'lar arası veri trafiği OSI (Open Systems Interconnection) referans modeli 3. katmanda gerçekleşirken, aynı VLAN içerisinde trafik 2. katmanda MAC adresleri kullanılarak gerçekleştirilir. Ağa dâhil olan bir kullanıcı ağ trafiğini dinleyerek ağ paketlerinin çözümlemesini yapabilir. Bu yüzden VLAN yapılandırılmasının dikkatle yapılması gerekmektedir. Farklı VLAN'ların kullanılması sayesinde, ağa yapılacak bir saldırı veya virüs yayılması sadece ilgili VLAN'da kalacak, tüm ağın dinlenmesinin ve zarar görmesinin önüne geçilerek, ağ üzerinden yayılabilen zararlı yazılımların kontrol altına alınması kolaylaşacaktır. Ayrıca VLAN'lar arası bir noktaya konumlandırılacak IPS (Intrusion Prevention Systems), IDS (Intrusion Detection Systems), FW (Firewall) gibi güvenlik cihazları ile ağ daha denetlenebilir hale getirilebilmektedir.

Genel Yayın (Broadcast) Sayısı: Bir alt ağda cihaz sayısı ne kadar artarsa genel yayın sayısı üstel olarak o oranda artmaktadır. Kontrol altına alınmazsa bu durum bir süre sonra genel yayın fırtınası (broadcast storm) oluşmasına neden olur. Doğru yapılandırılmış VLAN atamaları ile genel yayın kontrolü sağlanabilmektedir.

Bant genişliği: YAA'larda alt ağların oluşturduğu çıkış trafiği, genel çıkış hattının toplam bant genişliğini oluşturur. Bu nedenle alt ağların gözlemlenmesi, aşırı trafik üreten kullanıcı ve uygulamaların kontrol edilmesi gerekmektedir.

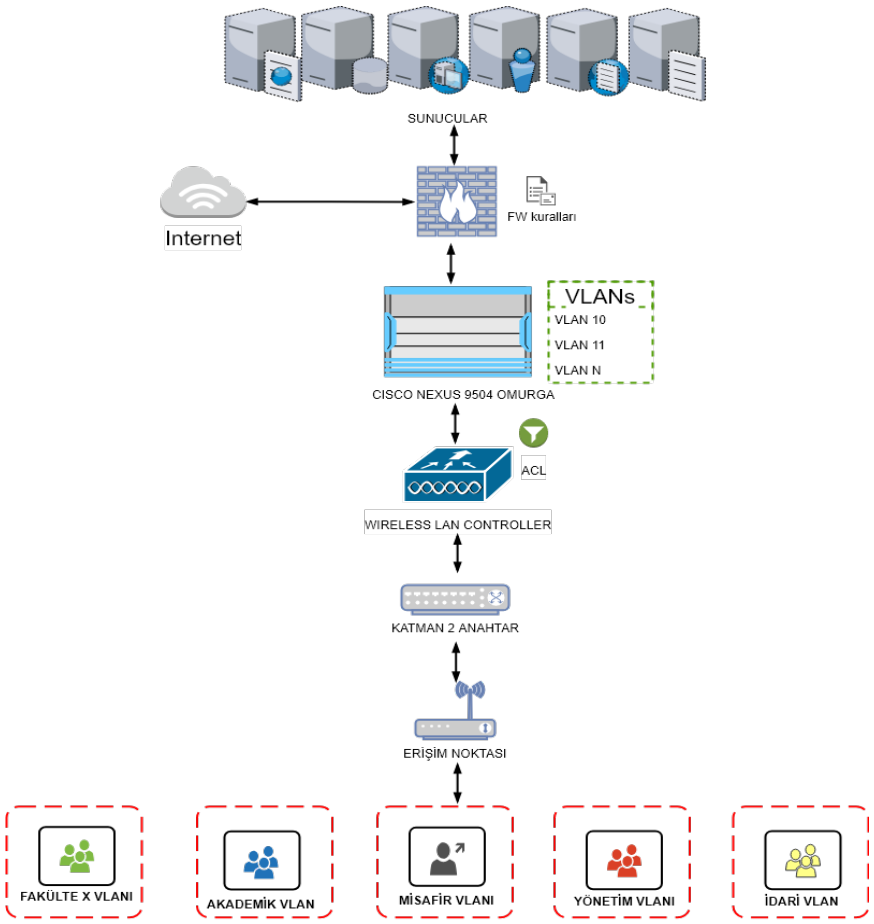
Ağ izleme ve arıza takibi: Kablosuz YAA'nın alt ağlara bölünmesi ağda oluşabilecek sorun ve arızaların ağ izleme yazılımları ile gözlemlenerek tespitini kolaylaştıracaktır.

Esneklik: Kullanıcı nereden ağa dâhil olursa olsun, kendisi için belirlenen VLAN'a ataması yapılacaktır. Kullanıcı profilinde oluşabilecek bir değişiklikte bir VLAN tanımlaması ile kullanıcı ağdaki bağlantısını kesintisiz sürdürebilmektedir.

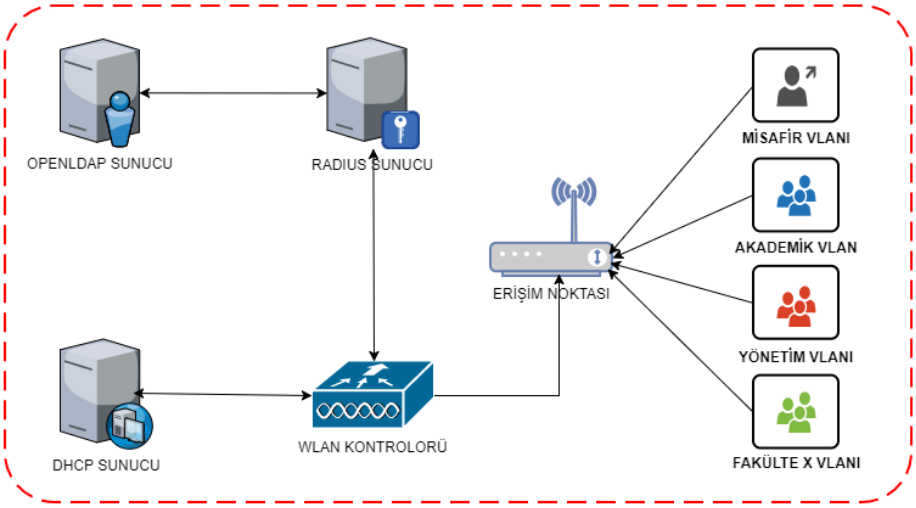
3. Test Ağı Altyapısı

Bu çalışmada, testlerin gerçekleştirdiği MSKÜ kablosuz YAA büyük oranda Eduroam alt yapısını kullanmaktadır. Bu ağda kullanıcılar akademik personel, idari personel, öğrenci ve misafir olmak üzere 4 farklı gruba ayrılmışlardır. Test ağının mevcut yapısında tüm kullanıcılar birbirlerinden izole edilmeden tek bir VLAN içerisinde konumlandırılmaktadırlar. Bu nedenle ağ ile ilgili gerçekleştirilen güvenlik kuralları ya da ortaya çıkan sorunlar tüm kullanıcıları etkilemektedir**.**

Şekil 2'de verilen, çalışma kapsamında tasarlanan dinamik VLAN atama yönteminde ise, kullanıcılar kural tabanlı gruplandırılarak ilgili VLAN üzerinde ağa dâhil olmaları sağlanmıştır. Tüm kullanıcılar için toplamda 45 VLAN oluşturulmuştur. Kullanıcıların AP'den WLC'ye kadar olan trafiği kapsüllenerek getirilmiştir ve böylece kullanıcıların başka bir VLAN'a ulaşmasının önüne geçilmiştir. Bunların yanı sıra WLC'de ve FW'da alt ağlara yönelik detaylı kurallar yazılabilmektedir. VLAN grupları arasından hem iç sunuculara hem de internet yönüne denetim ve yetkilendirme imkânı artırılmıştır.



Şekil 2. Dinamik VLAN ile tasarlanan yapı



Şekil 3. Ağ sunucu alt yapısı

Şekil 2'de verilen ağ alt yapısındaki sunucuların oluşturdukları genel yapı ise Şekil 3'te gösterildiği gibi tasarlanmıştır. Test ağında OpenLDAP, RADIUS, Sanal ve DHCP sunucuları kullanılmıştır.

3.1. OpenLDAP Sunucu

Haziran 2006'da OpenLDAP Foundation tarafından geliştirilen açık erişimli LDAP (Lightweight Directory Access Protocol) protokolüdür. IETF RFC 4510 açık standardı ile özellikle X.500 tabanlı dizin hizmetlerine erişim için kullanılır (OpenLDAP Software, 2019).

3.2. RADIUS / FreeRadius Sunucu

RADIUS, kablolu ve kablosuz ağlarda 802.1x ile kimlik doğrulama, yetkilendirme ve kayıt tutma gibi işlemlerde yaygın olarak kullanılan bir servistir. Radius sunucu/istemci tabanlı çalışır. İstemcilerin istekleri NAS (Network Access Server) adı verilen cihaz üzerinden RADIUS sunucuya iletilir (Rehman vd., 2010). RADIUS sunucu gelen kimlik doğrulama isteklerini belirlenen yapılandırmaya göre doğrulamaya çalışır ve sonucu NAS'a geri bildirir.

Freeradius, RADIUS protokolünü kullanarak kimlik doğrulaması gerçekleştiren en çok bilinen ve kullanılan yazılımdır (FreeRADIUS, 2019). Az kullanıcı içeren sistemlerde Freeradius kimlik doğrulamasını metin dosyası içerisine tanımlanan kullanıcı bilgilerine göre gerçekleştirebilirken, çok kullanıcılı sistemlerde LDAP (Lightweight Directory Access Protocol) dizin servisleri ve SQL (Structured Query Language) veri tabanının kullanılması gerekmektedir.

Testlerin yapıldığı MSKU Eduroam ağında kimlik doğrulama sunucusu olarak Freeradius 3.0.16 kullanılmıştır. MSKU'da kimlik doğrulama yöntemi olarak Eduroam Fedarasyonu'nun tercih ettiği EAP-TTLS/PAP kimlik doğrulama yöntemi seçilmiştir.

3.3. Sanal Sunucu

Sanal sunucu kavramı, ağ üzerinde farklı politikalara ihtiyaç duyulması halinde tek bir RADIUS sunucu ile bu ihtiyaçların karşılanabilmesini sağlamak amacıyla geliştirilmiştir. Örneğin ağdaki bir bölgede TTLS-PAP ile kimlik doğrularken başka bir bölgede PEAP-MSCHAPv2 kimlik doğrulaması gerekebilir. Sanal sunucular bu gibi durumlarda oldukça esnek bir yapı sağlayarak, istenilen şekilde yapılandırılabilirler.

3.3. Kablosuz Ağ Kontrolörü

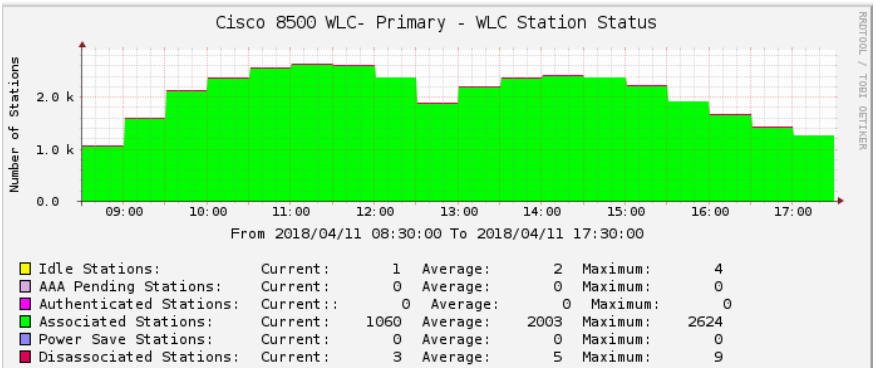
Kablosuz ağların geniş ölçekli alan ve yerleşkelerde kullanılmaya başlanması ile birlikte ağda konumlandırılan AP sayısı önemli ölçüde artmıştır. Bu sayı ortalama bir YAA'da yüzlerce AP'ye karşılık gelmektedir. Her bir AP'nin yönetimini ayrı ayrı yapmak oldukça güç ve zaman gerektirmektedir. Birçok üretici ağdaki tüm AP'lerin merkezi bir cihaz üzerinden yönetilmesi amacıyla, donanım ya da sanallaştırılmış yazılım tabanlı WLC çözümü sunmaktadır (What is WLAN Controller? WLC – Cisco, 2019). Bir WLC'ye kayıtlı tüm AP'lerin, kimlik doğrulama yöntemi ve yazılım güncellemeleri gibi pek çok yapılandırma WLC üzerinden yapılabilir. Test ağında Cisco 8540 WLC kullanılmıştır.

4. Performans Testleri

Çalışmada statik ve dinamik VLAN performanslarını test etmek için iki farklı senaryo hazırlanmıştır. Kablosuz YAA'ya dâhil olan tüm kullanıcılar kendileri için oluşturulan VLAN gruplarına dâhil olurlarken ağ ile ilgili istatiksel bilgiler SNMP protokolü ve CACTI programı kullanılarak toplanmıştır. Testler sırasında ağ performanslarını değerlendirmek için ağdan toplanan bilgiler ağdaki kullanıcı sayıları, kimlik doğrulama yöntemleri, genel yayın paket sayıları ve WLC portlarında izlenen toplam trafiktir. WLC 2 adet 10 Gbit/s'lık portlar üzerinden Cisco Nexus 9504 omurga anahtara bağlanmıştır. Port channel ile toplamda 20 Gbit/s'lık bir hat elde edilmiştir. Tüm ağ istatistikleri ve raporlar bu portlar üzerinden ağın en yoğun kullanıldığı hafta içi sabah 08:30 ile akşam 17:30 arasında alınmıştır.

4.1. Statik VLAN Testleri (Senaryo 1)

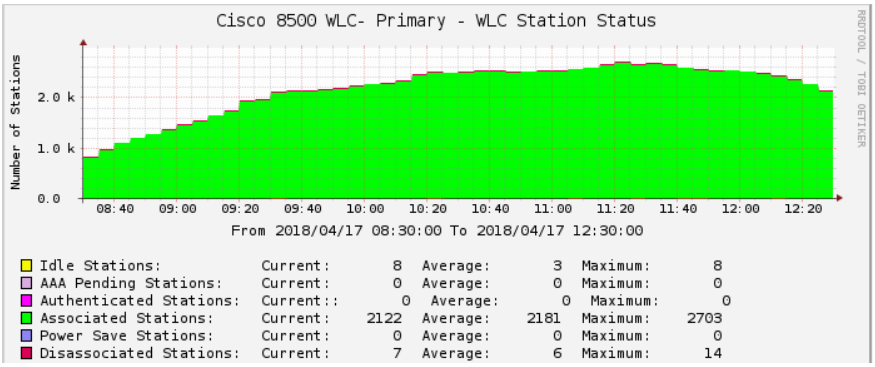
Bu senaryoda ağdaki tüm kullanıcılar WLC'de statik olarak tek bir VLAN içerisine alınmıştır. Testler sırasında ağa 1773 ile 2624 arasında kullanıcı dâhil olmuştur. 3. günde maksimum 2624 bağlantı ile ağda başarılı bir şekilde oturum açan kullanıcıların sayısı saat aralıklarına göre Şekil 4'te verilmiştir. Şekil 4'e göre gün içerisinde sabah 10:00-12:00 ve öğleden sonra 13:00-15:00 arasında kullanıcı sayısında artış yaşandığı görülmektedir.



Şekil 4. Ağ kullanıcı sayıları (Senaryo-1)

4.2. Dinamik VLAN Testleri (Senaryo 2)

Bu test senaryosunda ağda 45 adet VLAN grubu oluşturulmuş ve ağdaki kullanıcılar çalıştıkları bölüme ya da kayıtlı oldukları fakültelere göre gruplandırılarak ağa dâhil edilmişlerdir. Testler sırasında ağa en az 1774 ve en fazla 2678 kullanıcı başarılı bir şekilde giriş yapmıştır. Günlük olarak WLC'nin portlarında saniyede oluşan genel yayın sayısı ve giriş-çıkış trafikleri ölçülmüş ve Şekil 5'te verildiği gibi kaydedilmiştir.



Şekil 5. Ağ kullanıcı sayıları (Senaryo-2)

5. Değerlendirme

Senaryo 1 ve Senaryo 2'de ağa dâhil olan kullanıcı sayıları, 10G portlarında oluşan genel yayın ve trafik değerleri ölçülerek, en yüksek ve ortalama değerler cinsinden sırası ile Tablo 1 ve Tablo 2'de verilmiştir.

Tablo 1. Senaryo 1 kullanıcı ve broadcast sayıları

Parametreler	Birim	1.gün	2.gün	3.gün	4.gün	5.gün
Kullanıcı Sayısı (max)	Kişi	2364	2615	2624	2278	1773
Kullanıcı Sayısı (ort)	Kişi	1995	2027	2003	1806	1410
Genel yayın Sayısı Maximum	pkt/s	**39.91**	**60.43**	**38.66**	**50.52**	**35.88**
Genel yayın Paketi Ortalama	pkt/s	**31.64**	**23.79**	**18.75**	**20.68**	**16.21**
Outbound Ortalama Toplamı	Mbit/s	315.92	286.78	284.17	283.12	198.13
Inbound Ortalama Toplamı	Mbit/s	303.72	276.05	273.7	271.65	190.62
In/out Ortalama Toplamı	Mbit/s	619.64	562.83	557.87	554.77	388.75
Ort Kullanıcı Başına Ort Outbound Trafiği	Mbit/s	**0.158**	**0.141**	**0.141**	**0.155**	**0.140**
Ort Kullanıcı Başına Ort Inbound Trafiği	Mbit/s	**0.152**	**0.136**	**0.136**	**0.150**	**0.135**
Ort Kullanıcı Başına Ort In/Out Toplamı Trafiği	Mbit/s	**0.310**	**0.277**	**0.278**	**0.307**	**0.275**

Tablo 2. Senaryo 2 kullanıcı ve genel yayın sayıları

Parametreler	Birim	1.gün	2.gün	3.gün	4.gün	5.gün
Kullanıcı Sayısı (max)	Kişi	2393	2678	2673	2493	1811
Kullanıcı Sayısı (ort)	Kişi	1890	2084	2066	1915	1411
Genel yayın Sayısı Maximum	pkt/s	**38.14**	**46.61**	**24.36**	**42.06**	**22.63**
Genel yayın Paketi Ortalama	pkt/s	**16.45**	**10.84**	**17.11**	**18.2**	**11.84**
Outbound Ortalama Toplamı	Mbit/s	287	312.81	325.32	297.66	228.58
Inbound Ortalama Toplamı	Mbit/s	276.93	300.93	312.57	286.06	219.95
In/out Ortalama Toplamı	Mbit/s	563.93	613.74	637.89	583.72	448.53
Ort Kullanıcı Başına Ort Outbound Trafiği	Mbit/s	**0.151**	**0.150**	**0.157**	**0.155**	**0.161**
Ort Kullanıcı Başına Ort Inbound Trafiği	Mbit/s	**0.146**	**0.144**	**0.151**	**0.149**	**0.155**
Ort Kullanıcı Başına Ort In/Out Toplamı Trafiği	Mbit/s	**0.298**	**0.294**	**0.308**	**0.304**	**0.317**

Belirlenen saatler arasında TenGigabit portlarının oluşturduğu In/out Ortalama Toplam Trafiğin, ortalama kullanıcı sayısına bölümü ile ortalama kullanıcı başına düşen trafik değeri elde edilmiştir. Değerlerin karşılaştırmaları mesai günleri olan Pazartesi-Cuma günleri birebir olarak gerçekleştirilmiştir. Ağ performanslarının ölçülmesinde kullanılan parametreler ve sonuç değerlendirmeleri aşağıda verilmiştir.

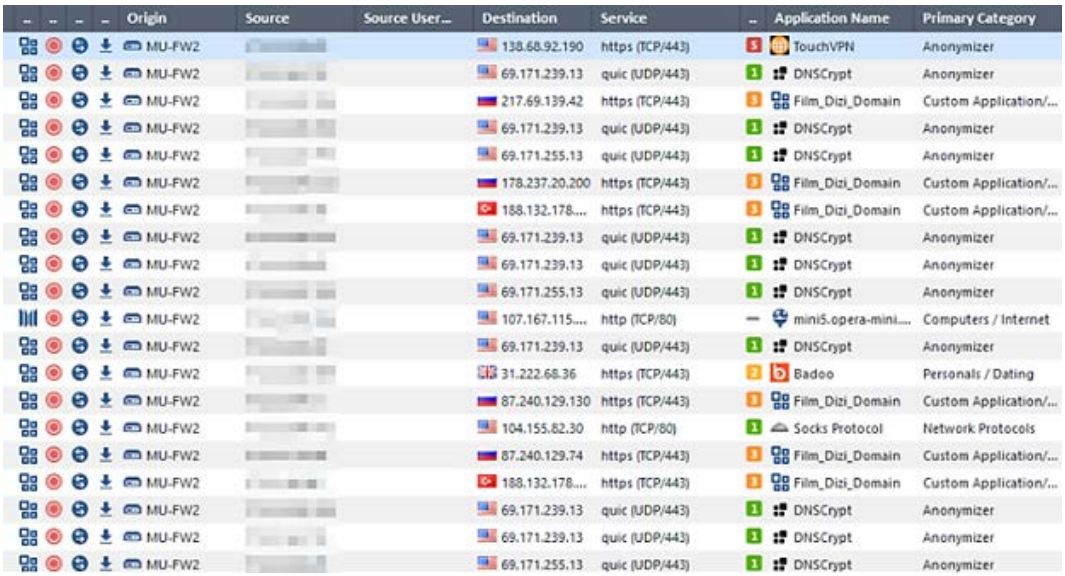
Genel Yayın Paket Sayıları: Kullanıcıların tek bir VLAN altında toplandığı Senaryo 1'de oluşan genel yayın sayısının, tüm gün karşılaştırmalarında Senaryo 2'ye göre daha fazla çıktığı gözlemlenmiştir. Kullanıcıların alt ağlara bölünerek, tasnif edilmesi ile oluşan genel yayın sayılarında önemli ölçüde azalma görülmüştür. Günlük genel yayın paketi ortalamasının 5 günlük ortalaması 1. senaryoda 22.21 olurken, dinamik VLAN yapılandırmasının yapıldığı 2. Senaryoya göre bu değer 14.88 olmuştur. Böylece ortalama genel yayın paket sayısında %33'lük bir iyileşme sağlanmıştır. Ayrıca, bu durumun ağa dâhil olan kullanıcı sayısının daha fazla ya da daha az olmasından bağımsız olduğu tespit edilmiştir.

Kullanıcı Başına Düşen Toplam Ortalama Trafik: Tablo 1 ve Tablo 2 incelendiğinde ölçümlerin yapıldığı ilk gün haricindeki diğer tüm günlerde Senaryo 2'de oluşan kullanıcı başına düşen toplam ortalama trafik, Senaryo 1'e göre daha fazla oluşmuştur. Senaryo 1'de yalnızca 1.gün kullanıcı başına düşen toplam trafik 0.158 Mbit/s ile dinamik VLAN senaryosundaki 0.151 Mbit/s'yi geçmiştir.

Kullanıcı Başına Düşen Ortalama Trafik: Senaryo 1 ve Senaryo 2 test sonuç tabloları incelendiğinde, kullanıcı başına düşen ortalama trafik değerleri noktasında önemli bir performans artışı görülmemiştir. Örnek olarak testlerin 4. gününde Senaryo 1'de kullanıcı başına 0.307 Mbit/s, Senaryo 2'de ise kullanıcı başına 0.304 Mbit/s'lik oluşmuştur. Bu iki değer arasında kullanıcı başına 0.002 Mbit/s'lik bir fark söz konusu olmuştur. Bu değere göre söylenebilir ki; Dinamik VLAN ve Statik VLAN yapılandırmalarında kullanıcı başına düşen ortalama trafik sayıları birbirlerine oldukça yakındır.

5.1. Dinamik VLAN Güvenlik Değerlendirmesi

MSKÜ Eduroam ağına gelen misafir kullanıcılar Freeradius sanal sunucusu aracılığıyla misafir VLAN'ına atanırlar. Freeradius sanal sunucusunda yazılan kurallara göre engellenen uygulama ve trafik istekleri satır satır Şekil 6'da verilmiştir. Ayrıca FW ve IPS tarafında yazılan kurallar ile VLAN temelli erişim yetkileri tanımlanmıştır. Buna göre; dinamik VLAN ile yapılandırılan YAA içerisinde konumlandırılan DNS sunucuları dışında harici DNS sorgulamaları ve VPN (Virtual Private Network) ile proxy edilen trafikler engellenmiştir. Şekil 7'de ise tanımlanan kurallara göre BotNet ağına doğru yapılan trafiklerin engellendiği görüntülenmektedir.



Origin	Source	Source User...	Destination	Service	Application Name	Primary Category
MU-FW2			138.68.92.190	https (TCP/443)	TouchVPN	Anonymizer
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			217.69.139.42	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			69.171.255.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			178.237.20.200	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			188.132.178....	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			69.171.255.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			107.167.115....	http (TCP/80)	mini5.opera-mini....	Computers / Internet
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			31.222.68.36	https (TCP/443)	Badoo	Personals / Dating
MU-FW2			87.240.129.130	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			104.155.82.30	http (TCP/80)	Socks Protocol	Network Protocols
MU-FW2			87.240.129.74	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			188.132.178....	https (TCP/443)	Film_Dizi_Domain	Custom Application/...
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			69.171.239.13	quic (UDP/443)	DNSCrypt	Anonymizer
MU-FW2			69.171.255.13	quic (UDP/443)	DNSCrypt	Anonymizer

Şekil 6. Ağ yapılandırmasında FW'de engellenen uygulamalar

Origin	Source	Source User...	Destination	Service
MU-FW2			static.183.75.63.178.clients.your-server.de (178.63.75.183)	https (TCP/443)
MU-FW2			static.183.75.63.178.clients.your-server.de (178.63.75.183)	https (TCP/443)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			BotNet-17 (141.8.224.169)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			static.248.71.63.178.clients.your-server.de (178.63.71.248)	http (TCP/80)
MU-FW2			de717.cxense.com (178.63.13.144)	https (TCP/443)
MU-FW2			de717.cxense.com (178.63.13.144)	https (TCP/443)
MU-FW2			de717.cxense.com (178.63.13.144)	https (TCP/443)
MU-FW2			de717.cxense.com (178.63.13.144)	https (TCP/443)
MU-FW2			de717.cxense.com (178.63.13.144)	https (TCP/443)

Şekil 7. Ağ yapılandırmasında FW'de engellenen trafik istekleri

6. Sonuçlar

Çalışmada kurumsal geniş ölçekli bir kablosuz yerleşke alan ağında dinamik ve statik VLAN yapılandırmaları yapılarak performans karşılaştırmaları analiz edilmiştir. Kullanıcıların kural tabanlı VLAN gruplarına bölünerek ağa dâhil olmaları ile oluşan genel yayın sayılarında %33'lük düşüş görülmüştür. Diğer taraftan toplam ve ortalama kullanıcı başına düşen trafikte ise çoğunlukla artış olduğu gözlemlenmiştir. VLAN yapısının esneklikleri sayesinde kullanıcılar güvenlik seviyesine göre ait oldukları ağda yaşamına devam etmesi sağlanarak, ACL, FW, IPS ve IDS kuralları vasıtasıyla ağın daha denetlenebilir hale gelmesi sağlanmıştır. Gelecek çalışmalarda mevcut dinamik VLAN yapısının SDN (Software Defined Network) ile bütünleştirilerek çok daha esnek ve daha yönetilebilir bir altyapıya kavuşturulması planlanmaktadır.

Kaynaklar

Çetin, M., 2006, Kurumsal Kampüs Ağlarında Otomatik Sanal Yerel Alan Ağ Tasarımları Ve Servis Kalitesi Analizleri, Yüksek Lisans Tezi, Pamukkale Üniversitesi, Fen Bilimleri Enstitüsü, Denizli.

FreeRADIUS, 2019. Erişim Tarihi: 07.07.2019. https://freeradius.org.

Jiang, N., Shan, L., 2008. Application of MAC-based VLANs for Mobile Office in Campus Area Network, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 1030-1032.

Jiang, N., Shan, L., Zhao, J., 2009. Application of Dynamic Port VLAN Membership with Auxiliary VLAN Campus Area Network, International Conference on Hybrid Intelligent Systems, 279-282.

Kırışoğlu, S., Kara, R., Özçelik, İ., 2019, A new SNMP-based algorithm for network traffic balancing in virtual local area networks, Journal of the Faculty of Engineering and Architecture of Gazi University 34(1), 365-380.

Koerner, M., Kao, O., 2016. MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks, International Workshop on Applications of Software-Defined Networking in Cloud Computing, 94, 497-501.

Lopez, G., Canovas, O., Gomez-Skarmeta, A.F., Sanchez, G., 2008. A proposal for extending the eduroam infrastructure with authorization mechanisms, Computer Standards & Interfaces, 30(6), 418-423.

Minlan, Y., Rexford, J., Sun, X., Rao, S., Feamster, N., 2011. A Survey of Virtual LAN Usage in Campus Networks, IEEE Communications Magazine, 49(7), 98-103.

Rehman, H., Govardhan, A., Rao, V.N., 2010. Design and Implementation of RADIUS – An Network Security Protocol, Global Journal of Computer Science and Technology, 10(7), 48-54.

OpenLDAP Software, 2019. Erişim Tarihi: 07.07.2019. https://www.openldap.org/doc/admin24.

What is WLAN Controller? WLC – Cisco, 2019. Erişim Tarihi: 08.07.2019. https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/wh at-is-wlan-controller.html.

Yamaki, H., Yamada, Y., Kato, Y., Kobayashi, E., Saotome, Y., Matsumoto, D., 2015. Integration of Wifi Services Based on the IEEE 802.11u Standard, International Conference on Computer Application Techniques, 132-137.