Journal of the Faculty of Engineering and Architecture of Gazi University 34:1 (2019) 365-380

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

A new SNMP-based algorithm for network traffic balancing in virtual local area networks

Serdar Kırışoğlu[1]*, Resul Kara[2], İbrahim Özçelik[3]

[1]Duzce University, of Information Technologies Department, Presidency, Konuralp, Duzce 81620, Turkey
[2]Duzce University, Faculty of Engineering, Computer Engineering Department, Konuralp, Duzce 81620, Turkey
[3]Sakarya University, Faculty of Computer and Information Sciences, Computer Engineering Department, Serdivan, Sakarya, 54050, Turkey

Highlights:

- VLAN load balancing
- Dynamic VLAN algorithm
- Network software based on SNMP

Keywords:

- Virtual local area networks
- Network traffic load balancing,
- Simple network management protocol

Article Info:

Research Article
Received: 24.06.2017
Accepted: 08.02.2018

DOI:

10.17341/gazimmfd.416499

Acknowledgement:

Correspondence:

Author: Serdar Kırışoğlu
e-mail: serdarkirisoglu@duzce.edu.tr
phone: +90544 804 3263

Graphical/Tabular Abstract

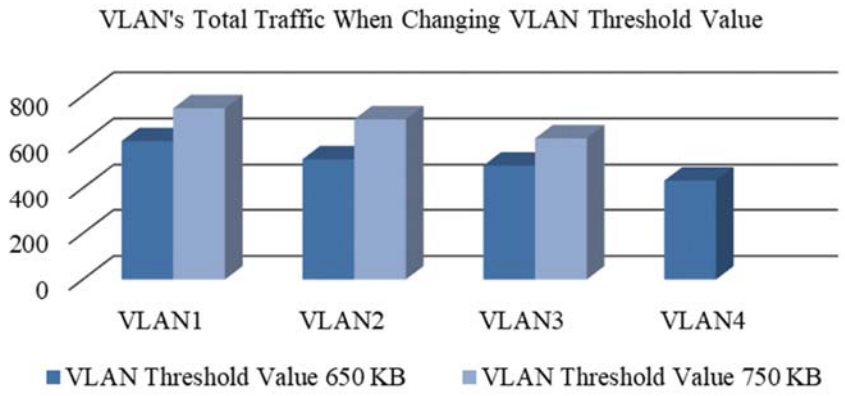


Figure A. When VLAN Threshold Value Changing New VLAN Adding Automatically

Purpose: In this study, an algorithm was developed to adjust the total traffic of each virtual network to be close to each other for use in virtual local area networks. While the total traffic of the virtual local area network is being calculated, the total traffic generated by the nodes belonging to the virtual network is considered. In each algorithm cycle, the memberships of the nodes have been tried to reach the target by changing if necessary. Also system have a threshold value that could be determined by network administrator. If this value exceeded, a new VLAN is involving to system and starts to accept membership of hosts like in the Figure A.

Theory and Methods: A software for the implementation of this algorithm has been developed and used in a real-time network. The software that uses this algorithm is communicated with the end devices on the network using the SNMP protocol. A DHCP server was set up for IP reception according to the virtual local network to which the nodes belong. A database is used to store information about nodes and end devices. In the environment, virtual local networks use a backbone key to communicate with each other when needed. In addition, different VLANs have been created according to the security levels of each node. According to the level of security, the necessary node information is recorded in the database.

Results: As a result, each virtual local area network, in each cycle of the algorithm, has close traffic values. Nodes with different security levels are not able to access resources other than their rights. Nodes that do not have different levels of security have been observed to change VLAN memberships whenever needed, in each cycle of the algorithm.

Conclusion: As a result the work has reached its goal. VLANs dynamically contain different nodes. And each has reached a level of traffic close to each other. There are advantages and disadvantages to the literature in comparison with other similar works. These advantages and disadvantages are detailed in the thesis. It is aimed that this thesis study will be developed in the future with the use of more up-to-date technology in line with the same targets.

Journal of the Faculty of Engineering and Architecture of Gazi University 34:1 (2019) 365-380

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Sanal yerel alan ağlarında ağ trafiği dengeleme için SNMP tabanlı yeni bir algoritma

Serdar Kırışoğlu[1]*, Resul Kara[2], İbrahim Özçelik[3]

[1]Düzce Üniversitesi, Bilgi İşlem Daire Başkanlığı, Rektörlük, Konuralp, Düzce, 81620, Türkiye
[2]Düzce Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Konuralp, Düzce, 81620, Türkiye
[3]Sakarya Üniversitesi Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, Serdivan, SAKARYA, 54050,Türkiye

Ö N E Ç I K A N L A R

- VLAN yük dengeleme
- Dinamik VLAN algoritması
- SNMP'ye dayalı network yazılımı

Makale Bilgileri

Araştırma Makalesi
Geliş: 24.06.2017
Kabul: 08.02.2018

DOI:
10.17341/gazimmfd.416499

Anahtar Kelimeler:
Sanal yerel alan ağı,
ağ trafiği yük dengelemesi,
basit ağ yönetim protokolü

ÖZET

Sanal Yerel Alan Ağları (VLAN), yerel alan ağlarında performansı artırmak, güvenlik yönetimini kolaylaştırmak ve adres yönetimini sağlamak için oluşturulur. Bu çalışmada, VLAN'da yük dengelemesini sağlamak için yeni bir yaklaşım sunulmaktadır. Bu yaklaşım için önerdiğimiz metot, aynı güvenlik düzeyine sahip VLAN'lardaki toplam trafiğe göre, düğümlerin VLAN üyeliklerini dinamik olarak değiştirmektedir. Özel güvenlik düzeyine sahip olan VLAN'lara üye olması gereken düğümler için ağın her noktasından aynı VLAN'a üye olması bu yaklaşımın getirdiği esnekliklerden biridir. Bu metoda göre ağda bulunması gereken VLAN sayısı, parametrik veya sabit öndeğerli olarak ayarlanabilmekte her bir VLAN'da trafik oluşturan üyelerin, yaklaşık eşit şekilde dağıtılması sağlanmaktadır. Bu sayede sanal yerel alan ağlarında eşit ya da birbirine yakın trafik değerleri oluşmaktadır. Bu metodun işlevselliğini test etmek için Basit Ağ Yönetim Protokolü (SNMP) temelli bir yazılım geliştirilmiş ve gerçek ağ ortamında uygulanarak önerilen amaçlara ulaşılmıştır.

A new SNMP-based algorithm for network traffic balancing in virtual local area networks

H I G H L I G H T S

- VLAN load balancing
- Dynamic VLAN algorithm
- Network software based on SNMP

Article Info

Research Article
Received: 24.06.2017
Accepted: 08.02.2018

DOI:
10.17341/gazimmfd.416499

Keywords:
Virtual local area networks,
network traffic load balancing,
simple network management protocol

ABSTRACT

Virtual local area network (VLAN)'s are being created for improve performance, easy to manage security and ensure address on local area networks. This paper introduces a new approach for load balancing on virtual local area networks. The method which is developed for this approach, is dynamically changing the clients ports VLAN membership according to VLAN's total traffic of the same security policy. The clients which have to register to security VLAN, can access their permission level source at all physically location of LAN, this is the flexibility of the method. The VLAN count which have to be on the LAN, can adjust parametrically or default constantly. In the algorithm which developed for this approach, the hosts belong to traffic on the network, ensures as much as possible equal or nearest distributes homogeneous on the VLAN's. In this way the VLAN's have same or nearest traffic value. A software has developed for testing functionality of this method which using SNMP protocol and reached to the aims by testing on the real network.

*Sorumlu Yazar/Corresponding Author: serdarkirisoglu@duzce.edu.tr, resulkara@duzce.edu.tr, ozcelik@sakarya.edu.tr /
Tel: +90 544 804 3263

1. GİRİŞ (INTRODUCTION)

,Sanal Yerel Alan Ağı (VLAN) IEEE (802.3ac) tarafından geliştirilmiş ve yerel alan ağlarında (LAN), ağ kullanıcılarını ve kaynaklarını mantıksal olarak gruplandırarak OSI 2. katman trafiğinin, farklı VLAN'da yer alan anahtar arayüzleri arasında veri akışının engellenmesini sağlayan bir standarttır [1]. LAN'ları VLAN'lara ayırmak kontrol, performans, güvenlik ve ölçeklenebilirlik açısından hem ağ kullanıcılarına hem de ağ kullanıcılarına yansıyacak olan avantajlar sağlamaktadır. VLAN kullanımının avantajları şöyle sıralanabilir;

Kontrol ve performans: LAN'da yayın paketleri tüm uç cihazlara kadar iletilirler. Bu durum gereksiz paket gönderimlerine yol açacağından bant genişliğini azaltmaktadır. VLAN kullanılarak bu durum kontrol altına alınabilir ve gereksiz yayın trafiğine engel olunur. Bir Yerel Alan Ağı'nı (LAN) her bir birim için VLAN'lara ayırmak çok daha iyidir. VLAN'lar LAN'ı yayın bölgelerine (broadcast domain) ayırarak yayın trafiğini azaltır ve ağ performansının artırılmasını sağlar [2].

Güvenlik: LAN'da uç kullanıcılar birbirleriyle haberleşebilir, basit uygulamalar ile ağı dinleyebilir ve saldırı yapabilirler. LAN'ın VLAN'lara bölünmesi birbirlerine ulaşması istenmeyen kullanıcılar gruplara ayırmış olur. Bu sayede her grup sadece kendi grubundaki yayın etki alanına ulaşabileceği için grup bazlı güvenlik sağlanmış olur. Güvenlik bakımından bakılacak olursa, VLAN teknolojisi saldırıların birbirleriyle ilişkili VLAN'lara yayılmasını önlemektedir [3]. Ağda istenmeyen trafik, anahtarların güvenlik özellikleri ve erişim kontrol listeleri (ACL) tarafından engellenir. Aynı şekilde tek bir LAN yerine her bir birim için VLAN kullanmak, sorunların etkisini ve LAN'daki tüm son kullanıcılara yönelik saldırıları azaltmak için etkili bir çözümdür.

Ölçeklenebilirlik: VLAN'lar yayın bilgilerine göre ayrılmış ağlardır. İhtiyaç duyulan sayıda VLAN anahtarlama cihazlarında oluşturulup, portları istenilen VLAN'ın üyesi yapılabilir. Bunu VLAN kullanmadan yapmaya çalışmanın karşılığı, fiziksel olarak uç noktadan yönlendirici cihaza kadar fiziksel bağlantı yapmaktır. VLAN oluşturarak sisteme performans ve güvenlik açısından avantajlar sağlansa da kriterleri oluşturulan VLAN'ların farklı VLAN'larla iletişim kurmasında sıkıntılar yaşanmaktadır. Sıkıntıların giderilmesinde üçüncü katmanda çalışan yönlendiricilere ihtiyaç duyulur. Bu durumda farklı VLAN'lar yönlendirici üzerinden haberleşebilir duruma gelir. Ancak farklı birimler arasındaki tüm iletişim, yönlendirici üzerinden geçmek zorunda olduğundan yönlendiricinin yükü artar. Bununla birlikte yönlendiriciye eklenecek erişim listelerindeki kurallarla iletişimin kontrol altına alınması sağlanır [4, 5]. VLAN'lar ağ yöneticisinin ön bilgileri doğrultusunda anahtarlar üzerinde yönetim komutları kullanılarak veya düğümün durumuna göre kendiliğinden olmak üzere sırasıyla statik veya dinamik olmak üzere iki türde kullanılabilir. Oluşturulan bir VLAN'ın statik ya da dinamik olarak anahtar portlarına atanması gerekir. Bir statik VLAN oluşturulurken ağ yöneticisi anahtarın belirli portlarını VLAN'a dahil eder ve portlar ağ yöneticisi tarafından değiştirilene kadar bu VLAN'ın üyesi olarak kalır. Dinamik VLAN oluşturmada ise, ağ yöneticisi sistemin kurulumu aşamasında ağda bulunan tüm cihazların MAC adreslerini bir yazılım aracılığıyla veri tabanına alıp ağdaki adreslerin VLAN'lara üyeliğini gerçekleştirir. Bu yöntemde MAC adresleri kullanılarak hangi cihazın hangi VLAN'a ait olacağı belirlenir [6]. Dinamik VLAN sisteminde merkezi bir yazılım ve ağa bağlanacak düğümlerin MAC adreslerinin bilinmesi zorunludur.

Dinamik VLAN ile ilgili olarak yapılmış çalışmaların çoğu VLAN'ın yük dengelemesinden çok karmaşıklığı azaltma ve tanımlı düğümlerin aynı sanal ağda bulunmasını esas almıştır. Koerner vd. tarafından yapılan çalışmada mobil kullanıcıların ağın herhangi bir noktasından kendi kaynaklarına erişebilmelerine olanak sağlamak için bir yazılım geliştirilmiştir [7]. Bu yaklaşımda anahtarlama donanımlarının OpenFlow protokolünü desteklemeleri şartıyla cihazların MAC adreslerinin merkezi bir yazılımda toplanarak hangi VLAN'da oldukları tanımlanmakta ve buna göre büyük ölçekli ağlarda düğümler nerede olurlarsa olsunlar kendi yerel kaynaklarının bulunduğu VLAN'a erişimleri sağlanmaktadır.

Okayama vd. yaptığı çalışmada büyük bir yerel alan ağında ortak bir noktadan kendi yerel kaynaklarına erişim sağlamak isteyen kullanıcılar için bir yaklaşım sunulmuştur [8]. Sunulan bu yaklaşımda yerel kaynakları farklı bir VLAN'da olan düğümler ortak bir alanda bağlantı sağladıklarında 3 adet sunucu devreye girerek, kimlik doğrulama yapılmakta şayet doğru ise ortak alanın bağlı olduğu anahtar üzerinde geçici oluşturulmuş VLAN kimlik numarası erişmek istedikleri VLAN kimlik numarası ile değiştirilmektedir. Bu işleri yapan VLAN yöneticisi, VLAN kimlik numarası dönüştürücü ve kimlik doğrulayıcı olmak üzere 3 adet sunucu sistemde görev yaparak ağda bulunan tüm anahtarlama cihazlarında geçici VLAN kimlik numarası tanımlanmaktadır.

MAC temelli ve yazılım tabanlı kimlik doğrulama kullanılarak yapılan bir diğer çalışmada kullanıcıların, MAC adresleri ağdaki bir yazılımda toplanmış ve ağa erişmek istedikleri nokta neresi olursa olsun RADIUS sunucu ile kimlik doğrulaması yapılarak bulunması gerektiği VLAN konfigürasyonu gönderilmesinin doğurduğu sonuçlar analiz edilmiştir [6]. Ning Jiang vd. çalışmasında ise [9] Cisco'nun kendine özgü MAC bazlı dinamik VLAN yazılımı olan VLAN Management Policy Server (VMPS) ve ağdaki Internet Protocol (IP) telefonlar ile düğümlerin aynı portta kullanılmasını sağlayan ses VLAN'ı uygulaması ele alınmıştır. Cisco'ya özgü VMPS yazılımı, bir ağ yöneticisi tarafından yazılımın veri tabanında bilgisayarların MAC adresleri bulunulması istenen VLAN ile eşleştirilir. Bu sayede ağın neresinden bağlanılırsa bağlanılsın aynı

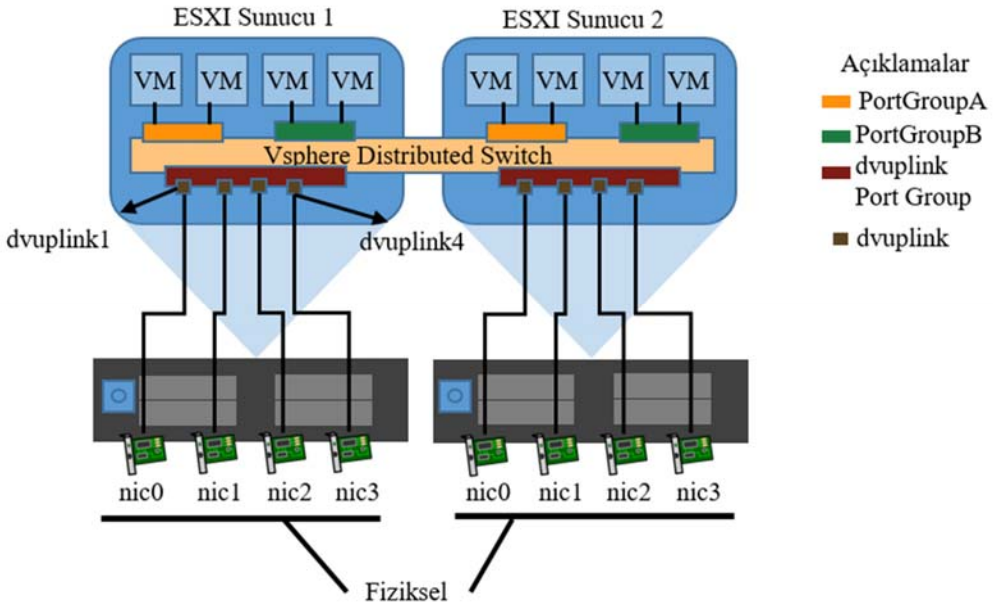
VLAN'da olunmasını sağlayan dinamik VLAN yapısı oluşmaktadır. Bu çalışmada ele alınan ses VLAN'ı ise yine Cisco'ya özgü "Cisco Call Center" santrali ile aralarında olan ve servis kalitesi yüksek sadece ses verisi taşınan bir VLAN'dır.

Vmware sanallaştırma yazılımının kullandığı sanal dağıtık anahtar (vSphere distributed switch-VDS), sanallaştırma ortamlarında yazılım tabanlı ağ (Software Defined Network-SDN) ve sanal olarak dinamik VLAN kullanarak yük dengelemesi yapmaktadır [10]. Bu teknoloji sayesinde sanal ortamdaki sunucular çoğaltılabilmekte, sunucular arası yük dengelemesi ve uygulama yönlendirmeleri sağlanabilmektedir. Şekil 1'de dağıtık anahtar yapısı gösterilmektedir.

Literatürde yer alan dinamik VLAN uygulamalarının çoğunun amacı kullanıcıların ortama eriştiklerinde kendileri için ayrılmış olan VLAN'a, bağlantı portlarının otomatik olarak üye yapılarak erişmelerini sağlamaktır. Ses VLAN'larına otomatik üye yapılmalarının sebebi ise ses verilerinin sadece IP telefonların bağlı bulundukları portlara iletilmelerini Cisco'ya özgü geliştirilmiş bir yazılımla sağlamaktır. Bu çalışmalar dışında bilgisayar ağlarının çeşitli alt alanları ile ilgili literatürde yapılmış çalışmalar da yer almaktadır. Tekerek vd. yaptığı çalışmada Hiper-Metin Transfer Protokolü (Hyper-Text Transfer Protocol-HTTP)'nü çalıştıran sunuculara erişimdeki atakların sınıflandırılmasına dair bir çalışma gerçekleştirilmiştir [11]. Irmak vd. yaptığı çalışmada ise uzaktan erişim sağlanabilen ve yazılımla kullanılabilen bir laboratuvar modellemesi yapılmıştır [12].

Bu çalışmada önerdiğimiz SNMP tabanlı dinamik ağ trafiği dengeleme yönteminde ağda bulunan trafiğin durumuna göre VLAN'larda oluşan yükün dengeli bir şekilde dağılımı için kullanıcıların VLAN'larını gerektiğinde değiştirmek ve buna bağlı olarak trafik yoğunluğu birbirine eşit veya yakın yayın bölgeleri oluşturulması sağlanmaktadır. Bu çalışmada sabit VLAN yapısı oluşturulmuş bir ağda, düğümlerin farklı trafik üretmeleri sonucu, aynı güvenlik politikaları uygulanmış VLAN'ların yük dağılımını, VLAN'lara üye düğümlerin dinamik olarak üyeliklerinin değiştirilmesiyle, VLAN trafiklerinin azaltılarak veya artırılarak dengelenmesi sağlanmıştır. Bu yöntem üreticiden bağımsız olarak endüstri standardı olan SNMP protokolünü destekleyen tüm anahtar cihazlarında uygulanabilmektedir. Bu sayede ağ altyapısındaki anahtarların sadece VLAN ve SNMP destekleyen cihazlar olması şartıyla yeniden bir yatırım yapmak yerine mevcut anahtarlar kullanılarak ek maliyete yol açmayacaktır. Sadece ağ anahtarlarının merkezi bir noktadan yönetimini sağlayacak olan geliştirdiğimiz yazılıma ihtiyaç duyulacaktır. Önerilen yöntemle ağda dinamik olarak VLAN'lar oluşturulabilmekte, portların VLAN'lara üyelikleri dinamik olarak gerçekleştirilebilmektedir. Yönlendirici cihaz kullanma ihtiyacı bulunmadığından mevcut ağ altyapılarında uygulanması ek maliyet getirmemektedir. Ayrıca bu çalışmayla yazılım tabanlı ağların (SDN) ihtiyaç duyduğu özel donanım ve sistemler kullanılmadan, mevcut cihazlar üzerinde dinamik VLAN ile ilgili işlemlerin önerdiğimiz yöntemle gerçekleştirilmesi konusunda literatüre katkı sağlanması hedeflenmiştir.

Bu çalışmanın ikinci bölümünde SNMP'nin çalışması hakkında bilgi verilmiş ve SNMP'de kullanılan nesne tanımlayıcılar (oid) incelenmiştir. 3.bölümde önerdiğimiz VLAN modellemesi ve önerilen yöntemin algoritması üzerinde durulmuş, 4. bölümde ise önerilen yöntemin performans değerlendirmesi yapılmıştır.



Şekil 1. Vmware dağıtık anahtar yapısı görünümün (VMware distributed key structure view)[10]

2. BASİT AĞ YÖNETİM PROTOKOLÜ
(SNMP: SIMPLE NETWORK MANAGEMENT PROTOCOL)

TCP/IP protokol ailesinin bir parçası olan SNMP; ağ yöneticilerinin ağ performansını arttırması, ağ problemlerini bulup çözmesi ve ağlardaki genişleme için planlama yapabilmesine olanak sağlar. SNMP sayesinde ağdaki cihazlar izlenebilir, yönetilebilir ve yapılandırmaları değiştirilebilir.

SNMP, basit tasarımından dolayı ağlara kolayca entegre edilebilme, geniş bir kullanım alanına sahip olma ve dağıtık ve merkezi yönetimi destekleme avantajlarına sahiptir [13]. Günümüzde kullanımda olan üç sürümü vardır. 1. Sürüm 1987 yılında yayınlanmış ve temel bazı komutlar barındırmaktadır. 1. Versiyonda get, set ve trap mekanizmaları vardı. 2. Sürüm ise 1993 yılında yayınlandı ve 1. sürüme ek olarak getbulk, inform ve şifrelenmiş veri trafiği mekanizması eklendi. 3. Sürüm SNMP'ye kullanıcı bazlı güvenlik doğrulama, yönetim bilgisini korumak için DES şifreleme algoritması kullanılması ve buna benzer birçok güvenlik ve esneklik sağlayan özellikler getirmiştir. SNMP, ajan uygulama, yönetici uygulama ve ağ yönetim sistemi (Network Management System-NMS) bileşenlerinden oluşur [14]. Ajan uygulama, SNMP hizmetini ağ cihazı üzerinde çalıştırıp gerekli bilgileri kayıtlı tutarak yönetici birime aktarma veya yönetici birimden gelen değişiklik isteklerini cihaza uygulama görevlerini yerine getirir. Yönetici uygulama, ajan uygulamadan ihtiyaç duyulan bilgileri alıp kullanıcıya görüntüleme ve kullanıcının değiştirmek istediği değerleri ağ cihazına gönderme görevlerini yerine getirir. Ağ yönetim sistemi (NMS), yönetici birimde çalışan ve bir ağa bağlı tüm cihazların izlenmesini ve yönetimini sağlayan uygulamadır.

SNMP bileşenlerinin iletişimi için UDP protokolü kullanılır. UDP'nin karakteristiklerinden dolayı, iletişim verilerinin başlık yükü düşük olup, sıralama, akış kontrolü ve oturum kurma işlemleri gerçekleştirilmez. Bu sayede çok hızlı iletişim gerçekleşir. SNMP'nin üçüncü sürümü ile birlikte şifreli veri iletişimi ve kimlik doğrulama özellikleri sayesinde güvenlik ön plana çıkarılmış ve önceki sürümlerde olan dezavantajlar ortadan kaldırılmıştır [15]. SNMP'nin işleyişinde iki kavramı ön plana çıkarmak gerekir. Bunlar Yönetim Bilgi Tabanı (Management Information Base-MIB) [16] ve Nesne Tanımlayıcısı (Object Identifier-OID)'dır [17]. MIB, her cihazın yerelinde bulunan, cihazdaki ajan uygulama tarafından erişim sağlanan ve cihazla ilgili bilgileri bulunduran bir veri tabanıdır. SNMP'nin çalışma mekanizması istek gönderme ve isteğe cevap alma şeklindedir. İstekler ve cevapları UDP protokolü ile gönderilip alınır. Yönetim sunucusu istekleri herhangi bir portundan ajanın 161. portuna gönderir. İletişimi ajanın başlatması durumunda bildirimler yönetim sunucusunun 162. portuna gönderilir [17]. SNMP sayesinde bir cihazdan bilgi alınabileceği gibi, cihazdaki bilgi değiştirilebilir ve cihazda yeni bir yapılandırma uygulanabilir. Örneğin cihaz yeniden başlatılabilir, cihaza bir yapılandırma dosyası gönderilebilir ya da cihazdan alınabilir. MIB kavramı Şekil 2'deki gibi bir ağaç yapısına benzetilebilir. Ulaşılmak istenen değeri tutan değişken OID'dir [18]. Bu değişkenler ağacın dallarının en uç noktasında olup bir cihazla ilgili tek bir değeri tutabileceği gibi kendisinden sonra gelen bütün alt dalları ifade etmek için de kullanılabilirler. Kökten ağaç dalına uzanan bu hiyerarşi birbirlerinden nokta ile ayrılmış sayı dizileriyle ifade edilir.

Örneğin 1.3.6.1.2.1 ifadesinde yer alan noktayla ayrılmış değerler soldan sağa doğru sırasıyla; 1 : ISO (International Standart Organization), 3 : Org (organization), 6 : Dod (Department of defense), 1 : Internet, 2 : Mgmt (Network management entries), 1: System. Değişkenin başındaki ilk dört değer olan 1.3.6.1 standarttır. Bu noktadan sonra ulaşılmak istenen bilgiye göre alt dallara ilerlenir. Örneğin 1.3.6.1.2.1.1 dalı (sysDescr) sistemle ilgili sistem adı, sistem tanımı, sistemin ayakta olduğu süre gibi değerleri tutar. Bunun alt dalı olan 1.3.6.1.2.1.1 değişkeni bunlardan biridir.

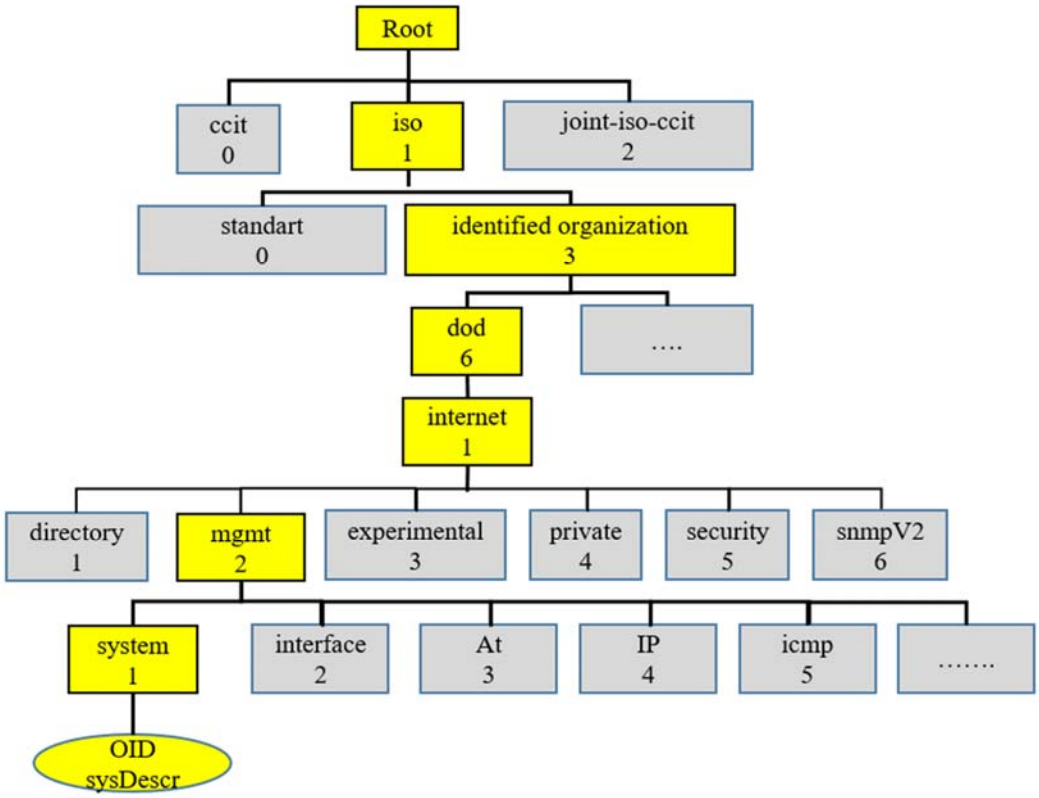
3. SNMP İLE DİNAMİK VLAN MODELLEMESİ
(DYNAMIC VLAN MODELING WITH SNMP)

Bu çalışmada VLAN'lar ile yayın bölgelerine ayrılmış yerel alan ağlarında, düğüm sayısına bakmaksızın her bir VLAN'daki toplam trafiğin birbirine eşit veya yakın yapılması amaçlanmaktadır. LAN'da eşdeğer güvenlik seviyesine sahip VLAN'ların üye düğümlerin ürettikleri trafiklere göre dinamik olarak üyeliklerinin değiştirilmesi ile, VLAN'ların yayın trafiği dengelenmeye, buna bağlı olarak da VLAN'lardaki üye düğümlerin ağa erişimlerinde gecikmelerin azaltılması hedeflenmiştir. Teorik olarak bir ağa ait gecikme süresi ile throughput değerlerinin birbirinden bağımsız olması gerekmektedir. Ancak pratikte bu iki terim arasında bir ilişki vardır. Paket kuyruğu hâlihazırda dolu olan bir yönlendiriciye yeni bir paket geldiğinde, kuyruğun en arka sırasına koyulacak ve önündeki paketlerin iletimi tamamlanıncaya kadar kuyrukta bekletilmesi gerekecektir. Dolayısıyla trafik yoğunluğu olması durumunda paketlerin yola giriş süresi daha uzun olacaktır. Bu bağlamda gecikme süresi oranı Eş. 1'de verilen formülle hesaplanmaktadır.

$$D = \frac{D_0}{(1-U)} \quad (1)$$

Eş. 1'de verilen formülde D efektif gecikme süresi, D_0 ağın kullanılmadığı andaki gecikme süresi ve U ise ölçüm yapıldığı andaki aktif kullanım oranını gösteren 0 ile 1 arasında değişen bir değerdir.

Ağ boş iken U değeri 0 olacak ve efektif gecikme süresi D_0 değerine eşit olacaktır. Ağ aktif kullanım oranı yarı kapasitede olacak şekilde arttırıldığında ise efektif gecikme süresi iki katında çıkacaktır. Trafik ağ kapasitesine yaklaştığında ise (yani U değeri 1 olduğunda) gecikme süresi sonsuza ıraksayacaktır. Bu nedenle ağ yöneticileri ağ aktif kullanım oranını sürekli düşük tutabilmek isterler ve bu amaçla ağ trafiğini devamlı olarak kontrol ederler. Ağın aktif kullanım oranı üst ya da ortalama sınırı aştığında ağ yöneticileri ağı sanal ağlara bölmek suretiyle bu oranı



Şekil 2. MIB ağaç yapısı Oid Numaraları (MIB tree structure Oid Numbers)[18]

düşürmeye çalışmaktadırlar [19]. Bu çalışmada önerdiğimiz yöntemde ağ aktif kullanım oranını dolayısıyla gecikme süresini düşük tutmak amacıyla SNMP'den yararlanılmıştır. VLAN trafiğinin seviyesi ile ilgili olarak tanımlanabilir veya öndeğerli bir eşik değeri kullanılmıştır. Şayet VLAN trafikleri bu eşik değerini aşarsa sistem öntanımlı olarak halihazırda tanımlanmış olan VLAN'ları kullanmaya başlar ve düğümler için bu VLAN'lar aktifleştirilir.

Örneğin mevcut kullanılan VLAN'ların toplam trafiği eşik değerini aşarsa kullanıma açık olmayan fakat IP adres havuzu ve omurga anahtar üzerinde gerekli yönlendirmeleri yapılmış olan VLAN kullanıma alınır. Düğümler bu yeni VLAN'a üye olabilirler. Geliştirilen algoritmada *i* adet VLAN'a ait bilgileri tutmak için *i*x3 boyutlu ve Eş. 2'de verilen *VLAN* adlı matris oluşturulmuştur.

$$VLAN = \begin{bmatrix} \mathrm{id}_1 & \mathrm{tt}_1 & \mathrm{gd}_1 \\ \mathrm{id}_2 & \mathrm{tt}_2 & \mathrm{gd}_2 \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \mathrm{id}_i & \mathrm{tt}_i & \mathrm{gd}_i \end{bmatrix} \quad (2)$$

Eş. 2'deki id_i, VLAN tanımlayıcı numarasını, tt_i, *i.* VLAN'ın toplam trafiğini ve gd_i, VLAN'ın güvenlik düzeyini belirtmektedir. VLAN'lara üye olacak *j* adet düğüme ait bilgileri tutmak için Eş. 3'de verilen *jx6* boyutunda *D* adlı matris oluşturulmuştur.

$$D = \begin{bmatrix} mac_1 & sip_1 & sp_1 & v_1 & tr_1 & gd_1 \\ mac_2 & sip_2 & sp_2 & v_2 & tr_2 & gd_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ macj & sip_j & sp_j & v_j & tr_j & gd_j \end{bmatrix} \quad (3)$$

Eş. 3'deki değerler sırasıyla mac_j, *j*. düğümün mac adresini, sip_j, bulunduğu anahtarın ip adresini, sp_j, anahtardaki port numarasını, v_j, üye olduğu VLAN tanımlayıcı numarasını, tr_j, düğümün ürettiği trafiği, gd_j, üye olduğu VLAN'ın güvenlik düzeyini ifade etmektedir. Burada dikkat edilmesi gereken husus VLAN matrisindeki id_i değişkeni kullanılan VLAN'ın tanımlayıcı numarası D matrisindeki v_j değişkeninin ise düğümlerin üye oldukları VLAN'ın tanımlayıcı bilgisidir.

Algoritmaya göre en yüksek trafik üreten düğümler sırasıyla VLAN'lara dağıtıldıktan sonra, VLAN sayısından fazla olan düğümler son VLAN'dan başlayarak VLAN'lara eklenir (3 adet VLAN varsa 4. Düğüm 3. VLAN'a 5. Düğüm 2. VLAN'a olacak şekilde). Bir düğümün ürettiği trafik şayet ekleneceği VLAN'dan önceki VLAN trafiğinden küçük

veya eşitse o VLAN'a üye olur. Aksi halde bir önceki VLAN'a üye olma aşamasına geçer ve bu kontrol tekrar edilir. k. VLAN'ın toplam trafiği Eş. 4'de verilen ifade ile hesaplanır:

$$\mathrm{tt}_k = \begin{cases} \sum_{k=0}^{i} \mathrm{tr}_n, \mathrm{V}_n = k \\ 0, \mathrm{V}_n \neq k \end{cases} \quad (4)$$

Eş. 4'de verilen V_n, *n*. düğümün VLAN üyeliğini ifade etmektedir.

Düğümlerin VLAN üyeliklerinin belirlenmesi için aşağıdaki ifade kullanılmalıdır:

l. düğümün VLAN üyeliği Eş. 5'de verilen ifade ile elde edilir:

$$\mathrm{V}_l = \begin{cases} k, \mathrm{tt}_k + \mathrm{tr}_l < \mathrm{tt}_{k-1} \\ k-1, \mathrm{tt}_k + \mathrm{tr}_l \geq \mathrm{tt}_{k-1} \end{cases} \quad (5)$$

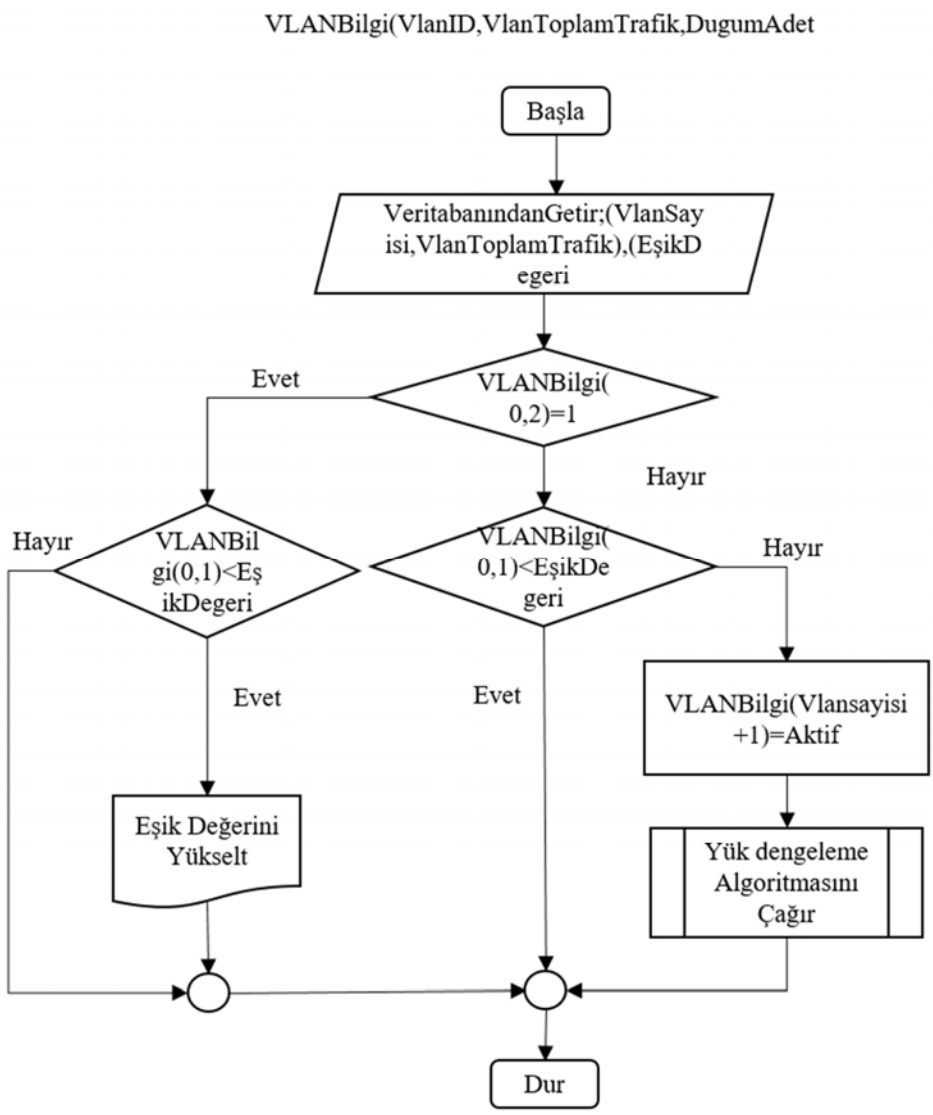
Eş. 5'de *k*: VLAN kimlik numarasını, tt_k: *k*. VLAN'ın toplam trafiğini ve tr_l ise *l*. düğümün ürettiği trafiği temsil etmektedir.

Eş. 4 ve Eş. 5'de verilen ifadeler kullanılarak belirlenen VLAN üyelik işlemlerini kullanan algoritmanın akış diyagramı Şekil 4'de, sözde kodu Şekil 6'da verilmiştir. İlk VLAN ile karşılaştırma yapılana kadar döngü devam eder. Bu süreçte şart sağlanmazsa düğüm ilk VLAN'a üye yapılır. Böylece her bir VLAN'daki ağ trafiği yükü dengeli olarak dağıtılmış olmaktadır. Ağın yoğun kullanımlarında VLAN sayısını dinamik olarak arttırmak için kullanılan algoritmanın akış diyagramı Şekil 3'de sözde kodu Şekil 5'de verilmiştir. VLAN sayısının dinamik olarak arttırılması, kendisine üye olan düğümlerin toplam trafikleri algoritmada belirtilen eşik değerinin üzerine çıktığı zaman, önceden ağda tanımlanmış fakat pasif konumdaki VLAN'ı aktifleştirerek VLAN dağıtım algoritmasının tekrar çağrılmasıyla gerçekleştirilir. Bu işlem için gerçek zamanlı bir ağ kurulmuş olup sonuçları Bölüm 4'de yer alan Senaryo 5'de verilmiştir.

Önerdiğimiz yöntem, iki aşamada işlem gerçekleştirilen algoritmalardan oluşmaktadır. Birinci aşamada ağ için gerekli olan VLAN ekleme işlemini yapan ve Şekil 3'de akış diyagramı, Şekil 5'de sözde kodu verilen algoritma çalışır. İkinci aşamada ağda bulunan VLAN'lara düğüm dağıtımını yapan Şekil 4'de akış diyagramı, Şekil 6'da sözde kodu verilen yük dengeleme algoritması çalışır. Parametrik olarak belirlenen zaman aralıklarında, VLAN ekleme algoritması çağrılır. VLAN'lardan herhangi birinin toplam trafiğinin parametrik olarak belirlenmiş olan VLAN toplam trafik eşik değerini aşması durumunda, ağda önceden tanımlanmış, fakat henüz hiçbir üyesi bulunmayan bir VLAN aktif olarak işaretlenir. Aktif VLAN'lar düğüm üyeliği kabul edebilir VLAN'lardır. Belirlenmiş olan eşik değerinin aşılmaması durumunda herhangi bir işlem yapılmaksızın algoritmanın diğer adımlarına devam edilir. Şekil 6'da sözde kodu verilen algoritmada düğümlerin ürettikleri toplam trafiğe göre, yeni VLAN üyeliklerine karar verme işlemi gerçekleştirilmiştir. Ağdaki anahtar cihazlardan SNMP protokolü vasıtası ile alınan bilgiler bir veritabanında tutulmuş olup karar verme esnasında VLAN'larda hangi düğümlerin en fazla trafiği ürettikleri bilgisi esas alınmıştır. Düğümlerin farklı VLAN'lara üyeliklerinin yapılması ve VLAN sayısı kadar düğüm için bu işlemin gerçekleştirilmesinden sonra geriye kalan düğümler için bu işlemin tekrarlanması ile neticelenir. Örnek olarak 10 tane VLAN bulunan bir ağda 100 tane düğüm var ise bu düğümler ürettikleri trafiğe bakılarak büyükten küçüğe sıralanır. En fazla VLAN sayısı kadar iterasyon gerçekleştirilir (Verilen örnek için en fazla 10 iterasyon). Bir düğümün mevcut VLAN'lardan hangisine üye yapılacağı, sıradaki VLAN'a eklenerek kendinen sonra gelecek VLAN'dan büyük olup olmama durumuna bakılarak karar verilir. Eğer düğümün üyeliği için kontrol edilen VLAN'ın toplam trafiği kendinden sonra gelen VLAN'ın toplam trafiğinden büyük değilse üyelik işlemi gerçekleştirilir. Aksi halde sonraki VLAN'lar için işlem tekrarlanır. Her değişim sonrasında ağdaki cihazlarda port kapama ve açma işlemi gerçekleştirilir. Bunun sebebi düğümlerin değişen VLAN'larına uygun olarak DHCP sunucusundan yeniden IP almaları gerekmesidir. Bu işlemler sonucunda ilk VLAN'da en büyük, sonrakinde ondan daha az olacak şekilde toplam trafikleri birbirine yakın VLAN'lar oluşur. VLAN'lardaki düğüm sayısı ise düğümlerin ürettikleri trafik değerlerine göre değişiklik arz eder. Örneğin ilk VLAN'da iki tane düğüm olabilirken bir sonrakinde on tane düğüm olabilir. Algoritmaya göre ağın başlangıç veya sistem sıfırlama durumunda olması halinde düğümlerin trafik değerlerinin herhangi bir önemi olmadığından düğümler sırasıyla her VLAN'da düğüm adedi yaklaşık eşit olacak şekilde VLAN'lar arasında paylaştırılır. Örneğin beş adet VLAN'a sahip bir ağda sekiz adet düğüm var ise VLAN'larda sırası ile 2-2-2-1-1 olacak şekilde bir paylaşım gerçekleştirilir.

4. SNMP'YE DAYALI DİNAMİK AĞ TRAFİĞİ DENGELEME ALGORİTMASI PERFORMANS DEĞERLENDİRMESİ
(SNMP-BASED DYNAMIC NETWORK TRAFFIC BALANCE ALGORITHM PERFORMANCE EVALUATION)

Geliştirilen algoritmanın performans değerlendirmesini yapabilmek için farklı senaryolar üretilmiştir. Senaryolarda farklı sayılarda, birbirine bağlı, toplamda üç adet Enterasys marka B5 model Ethernet anahtar, bir adet Extreme marka X440-24t model Ethernet anahtar, Windows işletim sistemine sahip bilgisayarlar ve geliştirilen yazılımın üzerinde çalıştığı yönetim sunucusu kullanılmıştır. Bu yönetim sunucusu aynı zamanda DHCP sunucusu olarak da kullanılmıştır ve VLAN'lara üye olacak düğümlerin IP havuzları bu sunucu üzerinde tanımlanarak dinamik olarak IP almalarına olanak tanınmıştır. Yönetim sunucusu herhangi bir VLAN'a üye değildir. Anahtarlardan biri omurga anahtarı olarak diğerleri ise kenar anahtarlar olarak çalıştırılmıştır. Sistem üzerinde biri varsayılan, üçü dinamik, biri güvenlik ve diğeri yönetim VLAN'ı olmak üzere toplamda en fazla 6 adet VLAN test için kullanılmıştır. Ağda en çok 10 adet düğüm kullanılarak trafik gözlemlenmiştir. Ağda düğümlerin kullandığı ortak bir ağ yazıcısı kullanılmış



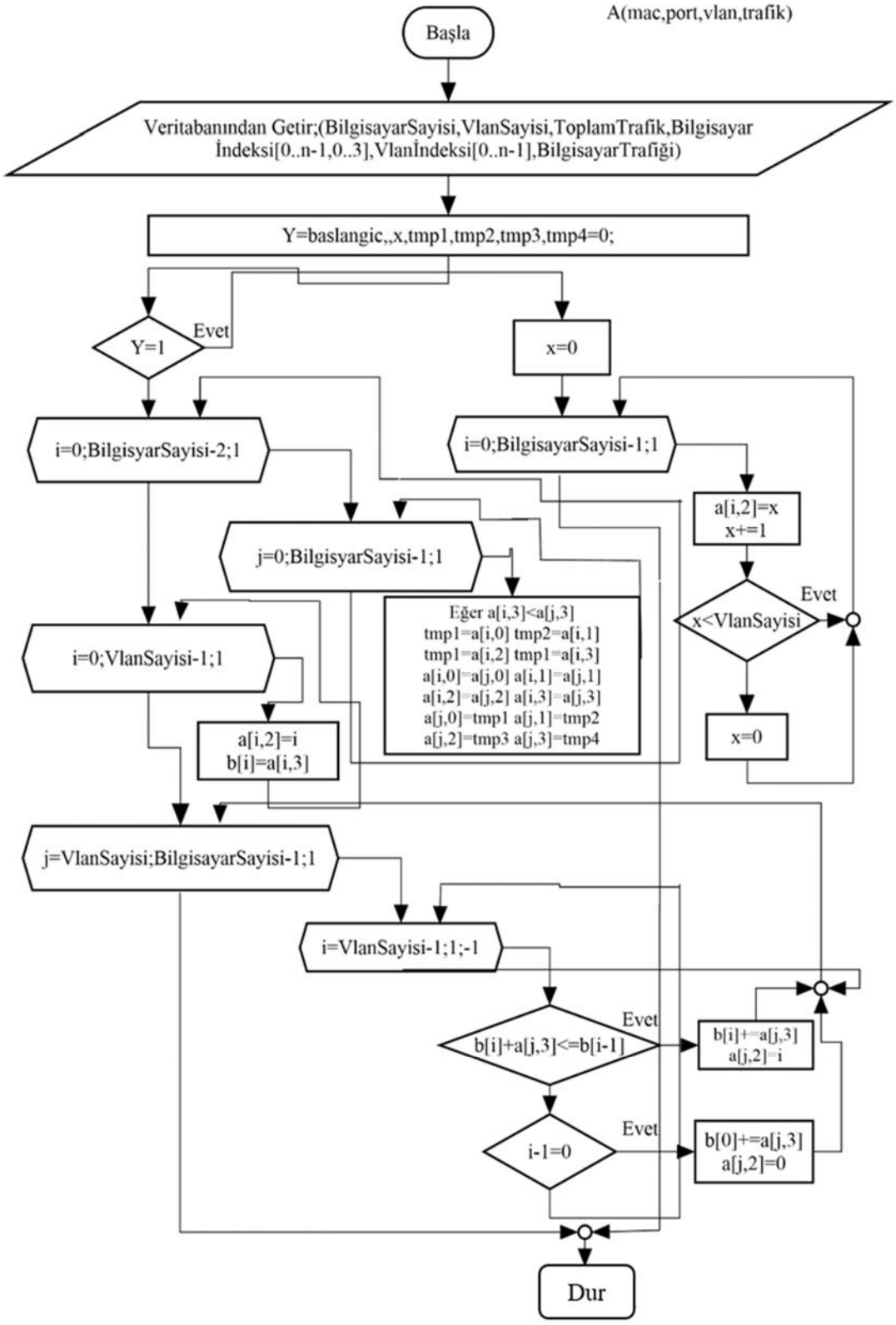
Şekil 3. SNMP'ye dayalı dinamik VLAN ekleme algoritması akış diyagramı
(Dynamic VLAN insertion algorithm based on SNMP flow diagram)

olup bu yazıcının VLAN'ı sabit tutulmuştur. Omurga anahtarda tüm VLAN'lar arası yönlendirme oluşturulmuştur. Böylece yazıcı tüm VLAN'lardaki düğümler tarafından kullanılabilmiştir.

Bu çalışmanın mevcut ağlara ya da yeni kurulacak olan yerel alan ağlarına uygulanmasında başlıca kabuller şunlardır.

- Başlangıçta varsayılan olarak her düğümün üye olacağı, ağdaki bütün anahtarlar ve omurga anahtar üzerinde tanımlanmış bir adet varsayılan VLAN olmalıdır.
- Ağ kaç VLAN'a bölünmek isteniyorsa (Özel güvenlik düzeyine sahip olanlar da dahil) o kadar VLAN omurga üzerinde tanımlanmalıdır.
- Bu VLAN'lar algoritma doğrultusunda geliştirilen yazılımda da tanımlanmalıdır**.**
- Ağda kenar anahtarların SNMPV3 desteklemesi gerekmektedir.
- Özel güvenlik düzeyli VLAN'a üye olacak düğümlerin MAC adresleri bilinmeli ve yazılıma bildirilmelidir. Böylelikle özel güvenlik düzeyine sahip VLAN'lar ve bu VLAN'lara üye düğümler ağın hangi noktasından bağlanırlarsa bağlansınlar aynı VLAN üyeliği ile özel güvenlik düzeyinde ağa erişebileceklerdir.
- MAC adresi bilinmeyen bütün düğümler VLAN'ı değiştirilebilir düğüm olarak kabul göreceklerdir
- Özel güvenlik düzeyine sahip olmayan düğümlerin, ürettikleri trafik değerlerine göre belirlenmiş zaman dilimlerinde, kendilerine uygun VLAN'lar arasında üyelikleri değişebilmektedir. Bu düğümlerin MAC adreslerinin bilinmesine ihtiyaç yoktur.

Ağdaki tüm anahtarların güvenlik ilkeleri gereği SNMPv3 protokolünü desteklemeleri gerekmektedir. Düğümlerin IP adres yapılandırmaları ise otomatik olduğu için yönetim sunucusunun üzerinde bulunan DHCP hizmeti vasıtasıyla



Şekil 4. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması akış diyagramı
(Flow diagram of dynamic VLAN load balancing algorithm based on SNMP)

VLAN'lara atanacak adres havuzları ayarlanmış ve sorunsuz bir şekilde IP adresi almaları sağlanmıştır.

Geliştirilen yazılımda SNMP'nin get, set ve trap mekanizmaları kullanılarak kenar anahtarlardan bilgiler

belirli sürelerde alınıp dinamik VLAN atamasına karar vermek amacıyla kullanılmıştır. Yazılımda kullanılan başlıca oid'ler ise şunlardır;

- 1.3.6.1.2.1.31.1.1.1.x: Bir portun çıkış yönündeki trafiği.
- 1.3.6.1.2.1.31.1.1.1.x: Bir portun giriş yönündeki trafiği.
- 1.3.6.1.2.1.17.7.1.4.3.1.x: Bir VLAN oluşturup porta atama.
- 1.3.6.1.2.1.17.7.1.4.x: Hangi Portun hangi VLAN'a üye olduğu.
- 1.3.6.1.2.1.4.22.1.x: MAC adresi ve IP adresi sorgulama.
- 1.3.6.1.2.1.2.2.1.x: Port açıp kapatma.
- 1.3.6.1.2.1.4.34.1.x: VLAN arayüze IP adresi atama.

Geliştirilen algoritma beş farklı senaryo oluşturularak test edilmiştir. Senaryolar ve elde edilen bulgular aşağıda verilmiştir.

```
//Vlanlar Kontrol ve VlanEkleme Algoritması
//Input: Dizi VLANBilgi[0..n-1,1,1],ilk indis:VLANID;
//ikinci indis: VLAN Toplam Trafik;üçüncü indis
//VLAN'daki düğüm adedi
//Input:VLAN Trafiği için Eşik Değeri
Start
if VLANBilgi[0,2] =1
        if VLANBilgi[0,1]<EşikDeğeri
                goto loop
        else
                print("Eşik Değerini yükseltin")
                goto Loop
        else
                if VLANBilgi[0,1]<EşikDeğeri
                        goto Loop
                else
                        VLANBilgi[VLANSayisi+1] ←aktif
                YükDengelemeAlgoritması()//SNMP'ye
//dayalı dinamik VLAN yük
                        //dengeleme algoritması
Loop
```

Şekil 5. SNMP'ye dayalı dinamik VLAN ekleme algoritması
(Dynamic VLAN insertion algorithm based on SNMP)

Senaryo 1-Sistem başlangıç veya reset durumu: Başlangıçta veri trafiğinin hiç olmadığı durumda 2 anahtar, 3 adet VLAN, 6 adet düğüm ve bir adet yönetim sunucusunun bulunduğu Şekil 7'de verilen ağ topolojisi oluşturulmuştur. Algoritmanın çalışması sonucunda;

- Her bir VLAN'da eşit sayıda düğüm olacak şekilde dağıtılmıştır.
- Algoritmanın çalıştırılması sonucu Tablo 1'de verilen üyelikler gerçekleşmiştir.
- Düğüm sayısı VLAN sayısının tam katı olmadığı durumlarda artan tek düğüm ilk VLAN'a üye yapılır.
- Bu senaryo sistem başlangıç durumu ve sistemin yeniden başlatılması durumu ile aynıdır.

Senaryo 2: Senaryo 2 Senaryo1'in ağ topolojisi kullanılarak gerçekleştirilmiş fakat farklı bir durum değerlendirilmiştir. Her bir düğüm üzerine kurulmuş olan 3. Parti Ostinato ağ trafik üreticisi kullanılarak [20] Şekil 7'de verilen ağ topolojisinde düğümlere yaklaşık olarak DÜĞÜM1:148KB, DÜĞÜM2:3558KB, DÜĞÜM3:445KB, DÜĞÜM4:296KB, DÜĞÜM5:1779KB, DÜĞÜM6:741KB olacak şekilde trafikler ürettirilmiştir. Trafikler ürettirildikten sonra algoritmanın ağ kontrol mekanizması çalıştırılmıştır. Bu kontrol sonrasında öncelikle ağ trafik değerlerine göre büyükten küçüğe doğru sıralama yapılmış daha sonra her bir düğüm sırasıyla VLAN'lara paylaştırılarak belli bir döngü ve kontrol mekanizması içinde trafiklerin birbirine yakın olacağı şekilde üyeliklerin dağıtıldığı gözlemlenmiştir.

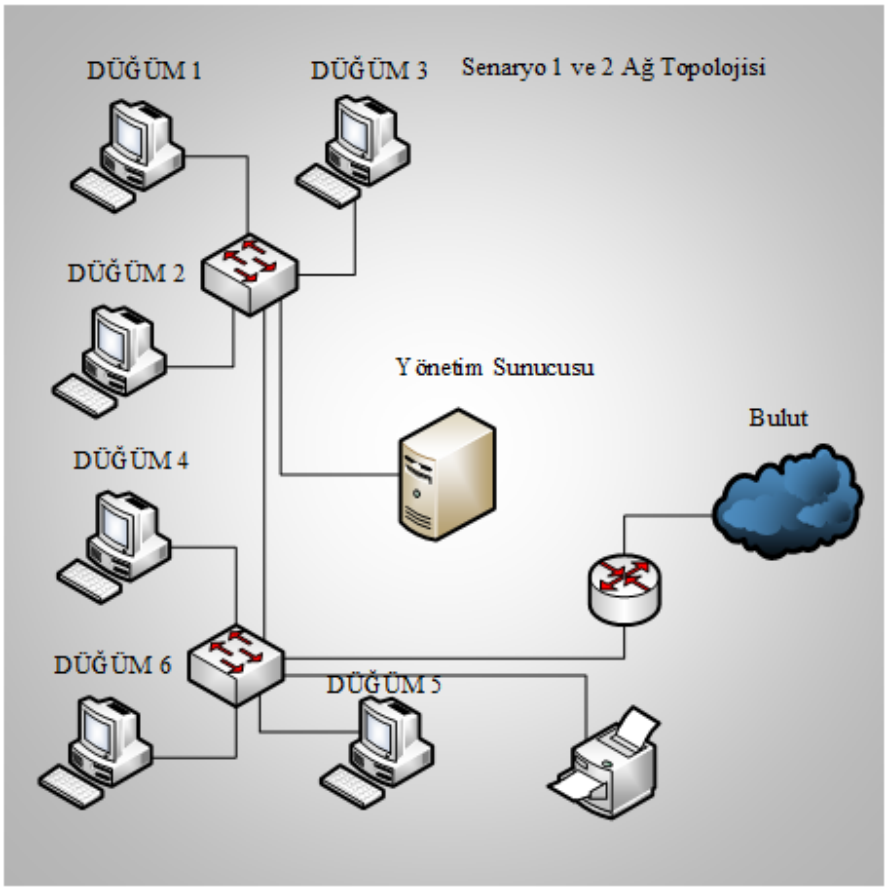
```
//Vlanlar Arası Yük Dengeleme Algoritması
//Input: Dizi A[0..n-1,0..3],ilk indis:BilgisayarSayisi
//ikinci indis:(mac,port,vlan,trafik)
//Input:BilgisayarSayisi,VlanSayisi,ToplamTrafik,BilgisayarTrafigi
//Input:Dizi B[0..n],indis:vlansayisi tuttuğu değer trafik toplamı
//Input: Y sistemin başlangıç durumu
Start
if Y=1
        x←0
        for i ←0 to BilgisayarSayisi-1 do
                a[i,2] ←x
                x←x+1
                        if x<VlanSayisi
                                x←0
else
        for i ←0 to BilgisayarSayisi-2 do
                for j ←0 to BilgisayarSayisi-1 do
                        if a[i,3]<a[j,3]
                                Swap a[i,0] and a[j,0]
                                Swap a[i,1] and a[j,1]
                                Swap a[i,2] and a[j,2]
                                Swap a[i,3] and a[j,3]
        for i ←0 to VlanSayisi-1 do
                a[i,2] ←i
                b[i] ←a[i,3]
        for j←VlanSayisi to BilgisayarSayisi-1 do
                for i←VlanSayisi-1 to 1 step -1 do
                        if b[i]+a[j,3]<=b[i-1]
                                b[i] ←b[i]+a[j,3]
                                a[j,2] ←i
                                break
                        else if i-1=0
                                b[0] ←b[0]+a[j,3]
                                a[j,2] ←0
                                break

Loop
```

Şekil 6. SNMP'ye dayalı dinamik VLAN yük dengeleme algoritması
(Dynamic VLAN load balancing algorithm based on SNMP)

Algoritmanın çalışması sonucunda Tablo 2'de verilen düğümler ve VLAN üyelikleri oluşmuştur. VLAN trafikleri Vlan1:3558KB (DÜĞÜM2); Vlan2:1779KB (DÜĞÜM5); Vlan3:1631KB (DÜĞÜM1 + DÜĞÜM3 + DÜĞÜM4 + DÜĞÜM6) olarak gerçekleşmiştir.

Senaryo 3: Şekil 8'de verilen ağ topolojisine göre ağa özel güvenlik düzeyine sahip bir düğümün dahil olması durumu: Ağ 6 adet düğüm, 1 adet Yönetim Sunucusu, 2 adet anahtar, 3 VLAN ve 1 adet özel güvenlik düzeyli VLAN kullanılarak



Şekil 7. Senaryo 1 ve 2 ağ topolojisi
(Network topology of scenario 1 and 2)

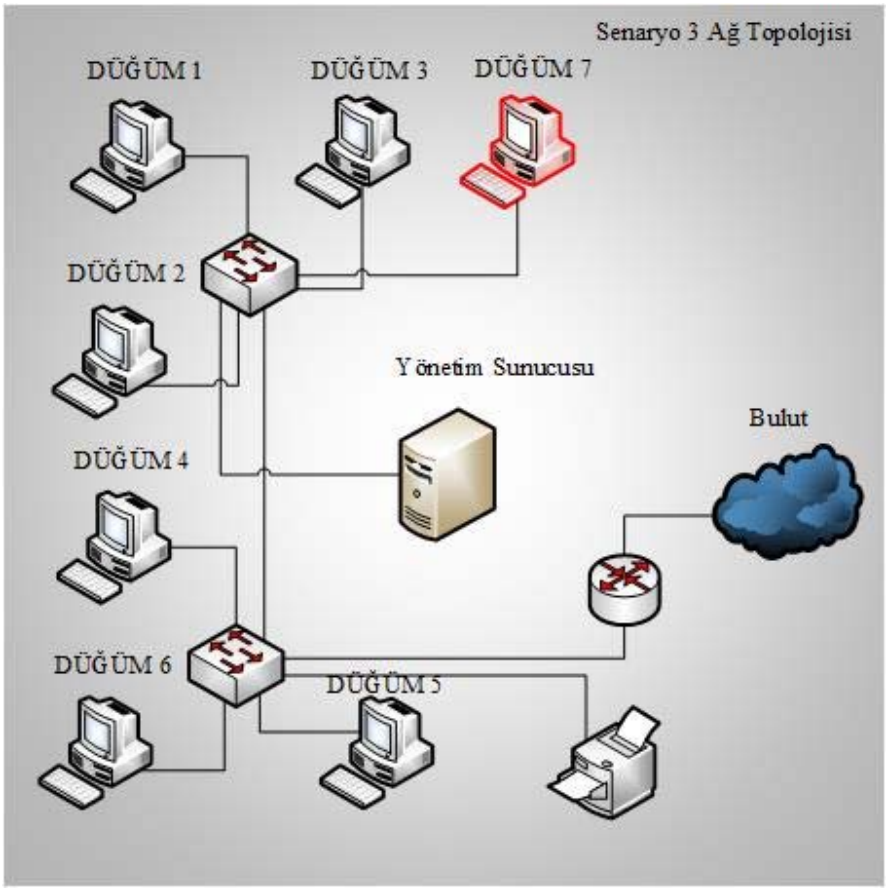
Tablo 1. Başlangıç ve reset durumu VLAN üyelikleri
(Initial and reset status VLAN memberships)

	VLAN1	VLAN2	VLAN3
DÜĞÜM1	✓		
DÜĞÜM2	✓		
DÜĞÜM3		✓	
DÜĞÜM4		✓	
DÜĞÜM5			✓
DÜĞÜM6			✓

Tablo 2. Senaryo 2'de algoritma sonucu VLAN üyelikleri
(Algorithm-ending VLAN memberships in Scenario 2)

	VLAN1	VLAN2	VLAN3
DÜĞÜM1			✓
DÜĞÜM2	✓		
DÜĞÜM3			✓
DÜĞÜM4			✓
DÜĞÜM5		✓	
DÜĞÜM6			✓

oluşturulmuştur. Özel güvenlik düzeyine sahip VLAN'lar ağ yöneticileri, sistem yöneticileri ve gerekli görülen kullanıcılar için farklı güvenlik düzeylerinde tanımlanabilmektedir. Veritabanında yer alan DÜĞÜM7, algoritma tarafından MAC adresi bilgisi kullanılarak özel güvenlik düzeyli VLAN'a üye yapılmıştır.



Şekil 8. Güvenli VLAN senaryosu topolojisi (Secure VLAN scenario topology)

Senaryo 4: Bu senaryoda Şekil 9'daki gibi fiziksel olarak konumlandırılmış ve Ostinato yazılımı ile ürettirilmiş Tablo 3'deki trafik yüklerine sahip 10 adet düğüm içeren, güvenlik düzeyleri eşit üç VLAN bulunan ağa 16 KB trafiğe sahip iki yeni düğüm eklenmesi durumu gerçekleştirilmiştir. Düğümlerin Tablo 3'de verilen trafik yükünü üretmelerinin ardından algoritma tarafından Tablo 4'de gösterildiği gibi 3 adet VLAN'a dağıtımı yapılmıştır. Ağa yeni eklenen düğümlerden birinin VLAN2'ye diğerinin VLAN3'e üyeliği algoritma tarafından gerçekleştirilmiştir. Dinamik dağıtım sonunda Şekil 11'de verilen toplam VLAN trafikleri elde edilmiştir.

Tablo 3. Düğümler tarafından üretilen trafik değerleri
(Traffic values generated by nodes)

	Ürettiği Toplam Trafik(KB)
DÜĞÜM1	120
DÜĞÜM2	51
DÜĞÜM3	158
DÜĞÜM4	197
DÜĞÜM5	185
DÜĞÜM6	174
DÜĞÜM7	106
DÜĞÜM8	120
DÜĞÜM9	102
DÜĞÜM10	152

DÜĞÜM1-DÜĞÜM10'a ait üretilen trafik miktarları Tablo 3'de verilmiştir. Ağa ilk VLAN belirleme işleminden sonra Tablo 4'de ürettikleri trafik değerleri gösterilen DÜĞÜM11 ve DÜĞÜM12 dahil edilmiştir.

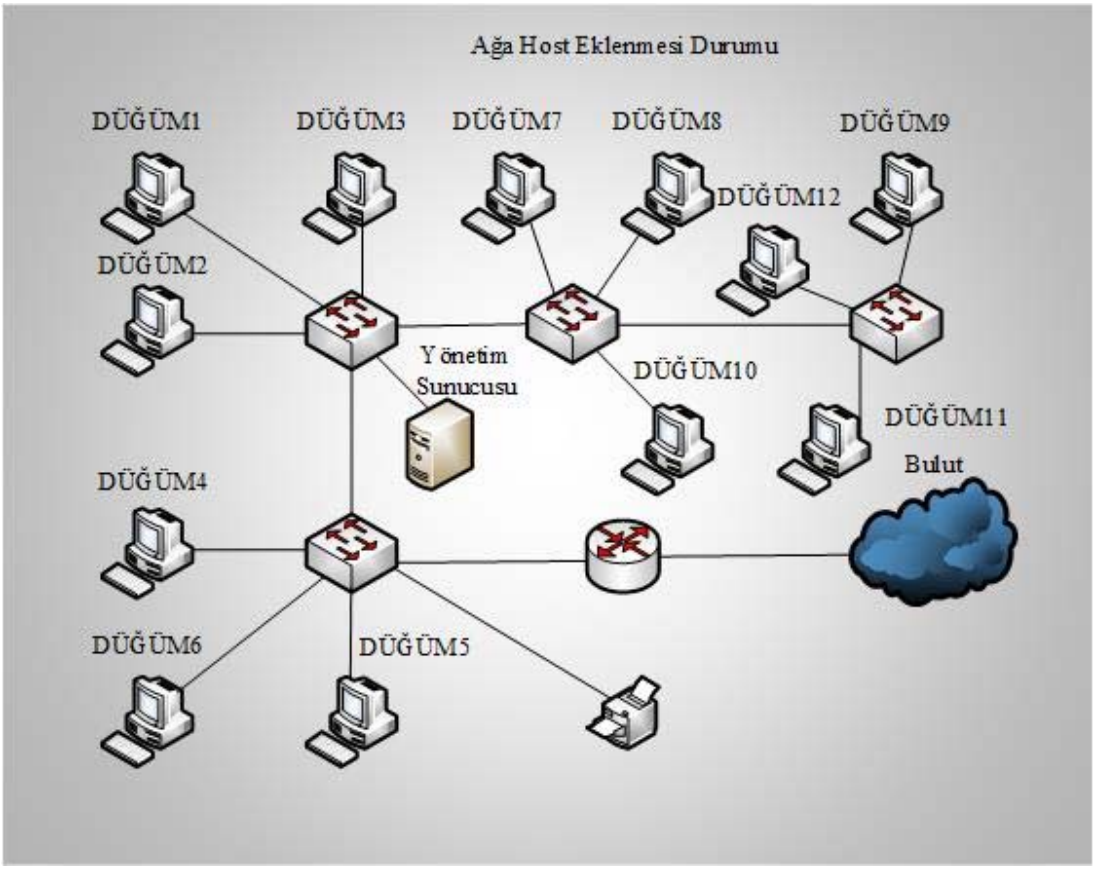
Tablo 4. Ağa sonradan dahil olan düğümler ve trafikleri
(Nodes and traffics that are later included in the network)

	Ürettiği Toplam Trafik(KB)
DÜĞÜM11	16
DÜĞÜM12	16

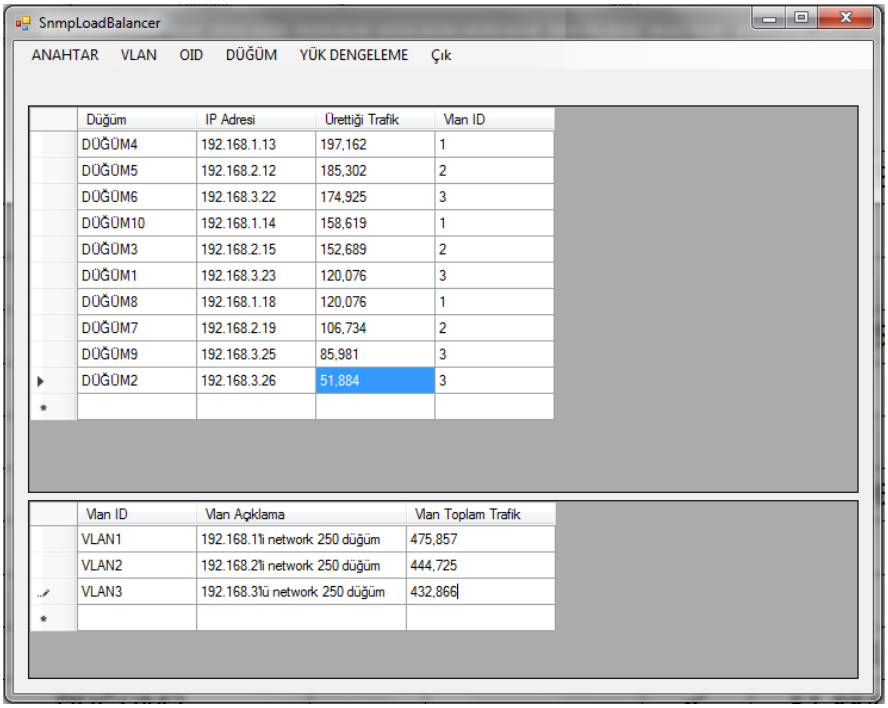
Tablo 4'de DÜĞÜM11 ve DÜĞÜM12'nin ürettikleri trafik gösterilmiş olup, bu iki düğümün ağa katılmasından önce algoritmanın çalışması sonucunda ağa ilk dahil olan Düğüm1-Düğüm10 aralığındaki düğümlerin üyelikleri Şekil 10'da verilmiştir.

Algoritmaya göre ağa sırasıyla dahil olan DÜĞÜM11'in VLAN2'ye, DÜĞÜM12'nin VLAN3'e üyelikleri yapılmıştır. Şekil 11'de senaryonun birinci aşamasında dahil olan düğümlerin ve ikinci aşamasında dahil olan düğümlerin oluşturduğu trafiğin VLAN'lara göre dağılımı verilmiştir.

Şekil 11'de verilen değerlerden anlaşılacağı üzere ağdaki tüm düğümlerin VLAN'lara dağılımı sonrasında her üç VLAN birbirlerine yakın trafik değerlerine ulaşmıştır.



Şekil 9. Ağa düğüm eklenmesi durumu (Node attachment to the network)

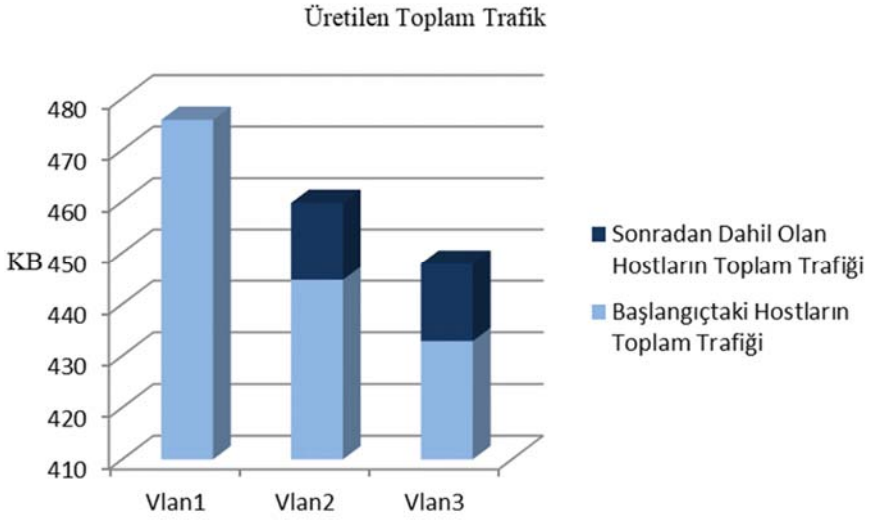


Şekil 10. Senaryo 4 başlangıç düğümlerinin VLAN'lara dağılımı (Scenario 4 allocation of start nodes to VLAN's)

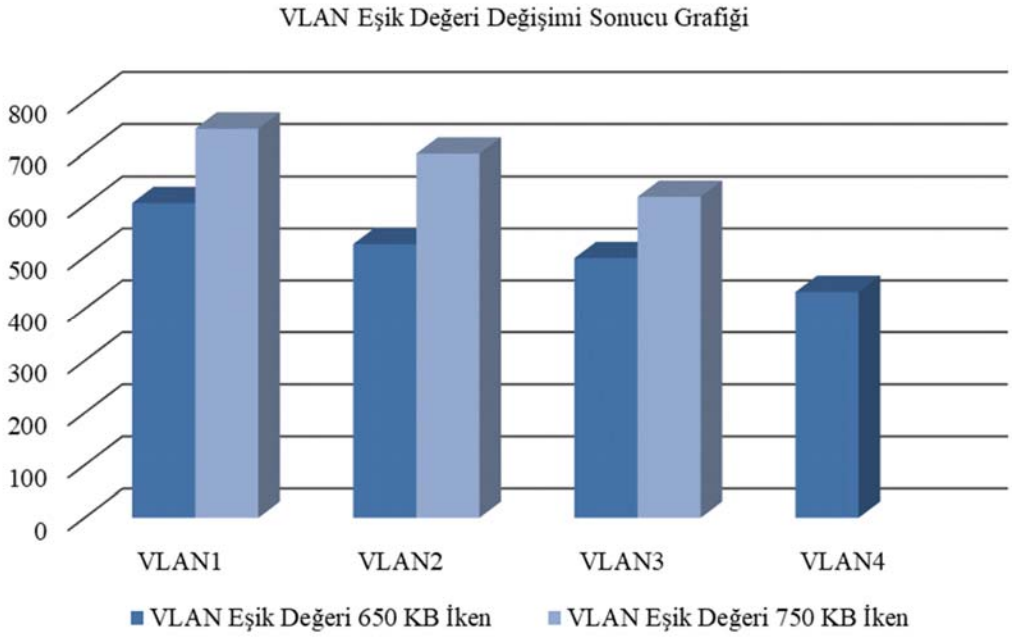
Senaryo 5: Bu senaryoda Senaryo 4 için oluşturulmuş ağ topolojisi kullanılmış fakat farklı bir durum olan VLAN eşik değerinin nasıl bir sonuç ortaya koyduğu gözlemlenmiştir. Bu senaryo için Tablo 5'de verilen düğüm trafikleri ürettirilmiş olup

Başlangıçta VLAN eşik değeri 750 KB olarak belirlenmiş senaryonun başlangıcında belirtilen ve Şekil 12'de gösterilen dağılım sonucu elde edilmiştir. VLAN eşik değerini 650 KB'a çektiğimiz zaman ağımızda VLAN4 aktif olarak kullanılmaya başlanmış olup ve Şekil 12'de gösterilen VLAN dağılımı elde edilmiştir. Şekil 12'de başlangıçta 750 KB olarak belirlenen eşik değeri bir sonraki aşamada trafikler aynı tutularak 650 KB'a çekilmiştir. Bunun sonucunda algoritma VLAN4'ü aktif hale getirmiş ve düğümlerin üyelikleri değişerek VLAN dağılımları sonucu eşik değerini geçmeyen VLAN trafikleri oluştuğu gözlemlenmiştir.

Senaryo 5'için kullandığımız ve algoritmamız doğrultusunda geliştirilmiş yazılım arayüzü Şekil 13'de verilmiştir.



Şekil 11. Senaryo 4 tüm düğümlerin oluşturduğu trafiğin VLAN'lara dağılımı
(Scenario 4 distribution of traffic generated by all nodes to VLAN's)

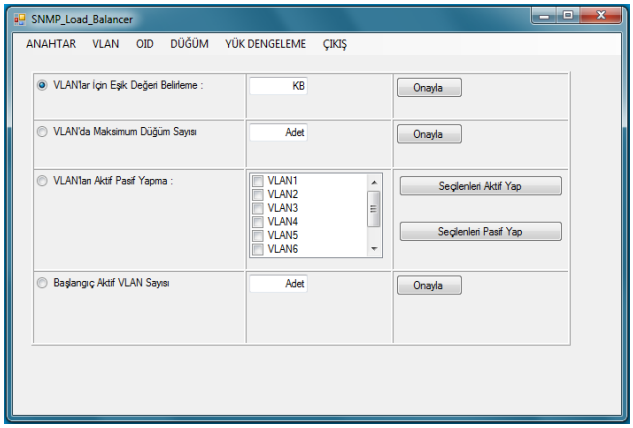


Şekil 12. VLAN eşik değeri değişimi sonucu VLAN trafik dağılımları
(VLAN traffic distributions after VLAN threshold value change)

Tablo 5. Senaryo 5, VLAN ekleme algoritması için düğüm trafikleri
(Scenario 5 Node traffics for VLAN insertion algorithm)

	Ürettiği Toplam Trafik(KB)
DÜĞÜM1	171
DÜĞÜM2	102
DÜĞÜM3	209
DÜĞÜM4	248
DÜĞÜM5	236
DÜĞÜM6	225
DÜĞÜM7	157
DÜĞÜM8	171
DÜĞÜM9	153
DÜĞÜM10	203
DÜĞÜM11	67
DÜĞÜM12	118

Şekil 13'de yazılımın ağda bulunan VLAN'lar için temel bazı ayarlar yapabileceğimiz görülmektedir. Bu ayarlar sonrasında sistem, düğümlerin VLAN'lar arasında dağılımını tekrardan otomatik olarak yapmaktadır. Böylelikle yapılan her değişiklik o esnada gerçek zamanlı olarak ağa uygulanmaktadır.



Şekil 13. VLAN'lar için eşik değeri belirleyebileceğimiz yazılım arayüzü
(Software interface on which we can set the threshold value for VLAN's)

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada, VLAN'da yük dengelemesini sağlamak için yeni bir yaklaşım sunulmuştur. Bu yaklaşım için geliştirilen algoritma, VLAN'daki toplam trafiğe göre VLAN'a dahil olan bilgisayarların üyeliklerini dinamik olarak değiştirmektedir. Bu metoda göre ağda bulunması gereken VLAN sayısı, parametrik veya sabit ön değerli olarak ayarlanabilmekte ve her bir VLAN'da trafik oluşturan üyelerin, yaklaşık eşit şekilde dağıtılması sağlanmaktadır. Önerilen yönteme göre ağdaki VLAN'ların her birinde eşit ya da birbirine yakın trafik değerleri oluşmaktadır. Bu metodun işlevselliğini test etmek için SNMP temelli bir yazılım geliştirilerek farklı senaryolarda gerçek ağ ortamında VLAN ve trafik dağıtımı açısından performans değerlendirmesine tabi tutulmuştur. Yapılan deneysel çalışmalar sonucunda ağa dâhil olan düğümlerin ön değerli veya oluşturdukları ağ trafiğine göre VLAN'lara dağıtıldıkları görülmüştür. Literatürde yer alan çalışmalarda düğümlerin MAC adresleri kullanılarak hep aynı VLAN'a üye yapıldığından dolayı önerdiğimiz yöntem hem yük dengeleme hem de VLAN'lara dağıtım açısından benzer yaklaşımlar içermediğinden doğrudan karşılaştırılabilir değildir. Ayrıca önerilen yöntem Ethernet anahtarların markasından bağımsız olarak SNMP desteğine sahip anahtarlardan oluşan tüm ağlarda uygulanabilir olması açısından literatürde yer alan yöntemlere göre üstünlüğe sahiptir.

Bu çalışma ile ağ altyapısında SNMP destekleyen mevcut cihazların daha etkin kullanılabilmesi, ağ yöneticilerine yük dengelemesinde yönetim kolaylığı sağlanabilmesi, dinamik VLAN oluşturularak SDN'e gerek kalmaksızın ağ trafik yük dengelemesi yapılabilmesi, düğümlerin trafiklerinin merkezi bir noktadan izlenebilmesi, sabit ya da ön değerli olarak toplam trafik değerlerine göre dinamik VLAN tanımlama yapılabilmesi noktasında katkılar sağlanmıştır. Bütün bunlara bağlı olarak yapılan bu çalışma ile SDN'in uygulanması için ihtiyaç duyulan özel donanım ve sistemler olmaksızın, dinamik VLAN oluşturma konusunda literatüre yeni bir yöntem eklenmiştir.

KAYNAKLAR (REFERENCES)

1. Shen Guo Z., Zhuang Y., Improving network performance by traffic reduction, Information, Communications and Signal Processing Theme: Trends in Information Systems Engineering and Wireless Multimedia Communications, 1226-1230 , 2, Singapur, 12-12 Eylül, 1997.
2. Rajaravivarma V., Virtual local area network technology and applications, The Twenty-Ninth Southeastern Symposium on System Theory, Cookeville, Tennessee, 49-52, 9-11 Mart,1997
3. Aktaş A., VLAN teknolojisi ile kampüs ağında aşırı istenmeyen paket trafiğin önlenmesi, Yüksek Lisans Tezi, Gaziantep Üniversitesi, Fen Bilimleri Enstitüsü, Gaziantep, 2016
4. Cambazoğlu T., "Internet ve Güvenlik", 78s. http:// www.ssm.gov.tr/ library/ docs/tr/teskilat /dosyalar/bim /int_guv.pdf, Eylül 2005.
5. http://www. dienekis.gr /resource/ papers/ extreme011. pdf
6. Metin Ç., Kurumsal Kampüs Ağlarında Otomatik Sanal Yerel Alan Ağ Tasarımları Ve Servis Kalitesi Analizleri, Yüksek Lisans Tezi, Pamukkale Üniversitesi, Fen Bilimleri Enstitüsü, Denizli, 2006.
7. Koerner M., Kao O. MAC Based Dynamic VLAN Tagging with OpenFlow for WLAN Access Networks, Procedia Computer Science, 94, 497–501,2016
8. Okayama K., Yamai N., Miyashita T., Kawano K., Okamoto T., A Method of Dynamic Interconnection of

VLANs for Large Scale VLAN Environment, 6th Asia-Pacific Symposium on Information and Telecommunication Technologies, Yangon-Myanmar, 427-432, 11 Eylül-11 Ekim,2005.

9. Shan L., Jiang N., Zhao J., Application of Dynamic Port VLAN Membership with Auxiliary VLAN in Campus Area Network, Hybrid Intelligent Systems, 2009. HIS '09. Ninth International Conference, Shenyang-China, 279-282,12-14 Ağustos,2009.

10. VMWARE, Vsphere Distributed Switch http://www.vmware.com/content/ dam/digitalmarketing/ vmware/ en/pdf/techpaper/ vsphere-distributed-switch-best-practices-white-paper.pdf, 2017.

11. Tekerek A., Gemci C., Faruk Bay Ö., Design and implementation of a web-based intrusion prevention system: a new hybrid model, Journal of the Faculty of Engineering and Architecture of Gazi University, 31 (3),645-653, 2016.

12. Irmak E., Calpbinici A., A Novel design for E-laboratories : Simultaneously accessible experimental application platform, Journal of the Faculty of Engineering and Architecture of Gazi University, 32 (2), 363-375, 2017.

13. Balta M., Özçelik İ., The Discovery of Enterprise Network Topology Created in a Virtual Environment with SNMPv3. The Online Journal of Science and Technology (TOJSAT), 2 (2), 64-70, 2012.

14. Affandi A. Riyanto R, Pratomo I, Design and implementation fast response system monitoring server using Simple Network Management Protocol (SNMP), International Seminar on Intelligent Technology and Its Applications, 2015 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 385-390, ,20-21 Mayıs, 2015.

15. Iqbal A., Pattinson C., Kor A., Managing Energy Efficiency in the Cloud Computing Environment Using SNMPv3: A Quantitative Analysis of Processing and Power Usage, Auckland,New Zealand 239-244, 8-10 Ağustos, 2016.

16. Jianxin Li, Leon B.J., A formal approach to model SNMP network management systems, Fourth International Conference on Computer Communications and Networks, Las Vegas, Nevada, 284 - 287, 20-23 Eylül,1995.

17. Koth A.M., El-Sherbini A., and Kamel T., A new interoperable management model for IP and OSI architectures, IEEE AFRICON 4th Africon Conference, Kuzey Afrika ,944-949 vol.2., 25-27 Eylül, 1996.

18. http://www.loriotpro.com/Products/On-line_ DocumentationV3/LoriotProV3Doc/C3- Introduction _to_Network_Supervision/C3-D4_SNMP_Object.htm

19. E. Comer D., Bilgisayar Ağları Ve İnternet - Computer Networks and Internets, Rüya Şamlı , Zeynep Gürkaş Aydın, Nobel Akademik Yayıncılık, Ankara, Türkiye, 2016.

20. Ostinato, Bilgisayar Programı. Ağ trafik üretici ve analiz edici program. https://ostinato.org/. Yayın tarihi Ekim 11 2016. Erişim tarihi Şubat 8, 2018.