

İzmir Ekonomi Üniversitesi Kampüs Ağı Yenileme Sürecindeki Çalışmalar ve Dinamik VLAN Yapısına Geçiş

Aydın Mutlu

İzmir Ekonomi Üniversitesi, Bilgi İşlem Müdürlüğü
aydin.mutlu@izmirekonomi.edu.tr

Özet: Bu belge Üniversitemizde öğrenci sayısının hızla artmasına bağlı olarak yeni ek binaların da kampüse dahil olması ile birlikte kampüs ağ omurgasının yenilenmesi ve artan bilgisayar sayısı nedeniyle denetim ve yönetimi zorlaşan statik sanal ağ yapısından dinamik sanal ağ yapısına geçiş sürecindeki çalışmalar hakkında bilgi vermektedir.

Abstract: This paper is about the process of the renovation of the network of our university campus due to the sharp increase in the number of students and accordingly the addition of new buildings within the campus, and the actions performed during the conversion from static VLAN which became difficult to supervise and manage because of the rising number of computers to dynamic VLAN

Anahtar Kelimeler: Kampüs ağı planlama, RADIUS kullanıcı yetkilendirme, OpenLDAP-DHCP-freeRADIUS, Dinamik VLAN.

Giriş

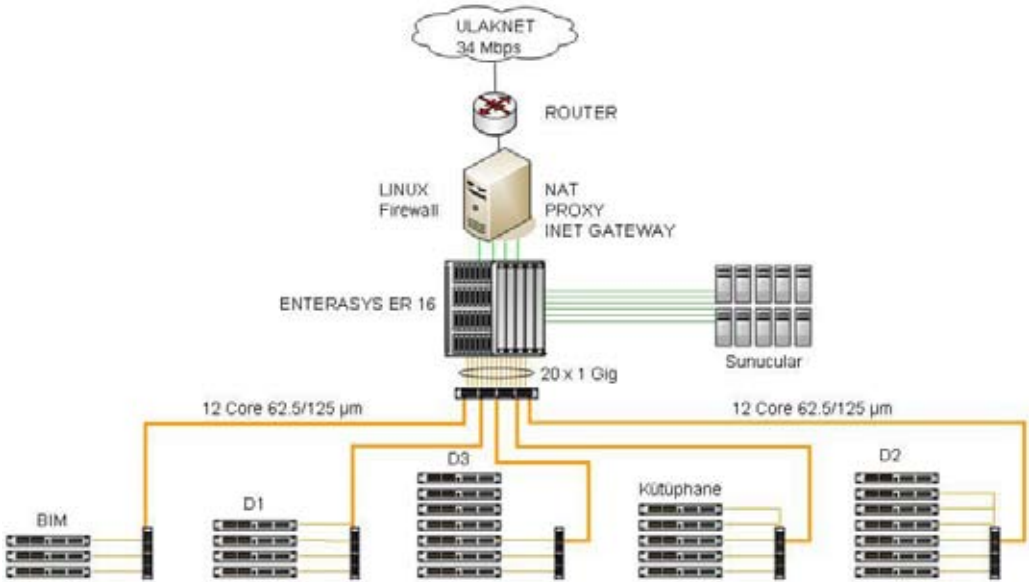
İzmir Ekonomi Üniversitesi; İzmir’de Ege bölgesinin ilk özel üniversitesi olarak 385 öğrenci ve 25 akademik/ıdari personel ile 2001 yılında eğitim ve öğretimine başlamıştır. Ayrıca Üniversitemiz tüm lisans öğrencilerine dizüstü bilgisayar sunan Ege bölgesindeki ilk üniversite olma özelliğini de taşımaktadır.

Üniversite Ağ altyapısı kuruluş aşamasında uzun vadeli teknolojik genişlemeler göz önünde bulundurularak planlanmış ve kuruluş döneminde 85 dizüstü ve 85 PC olmak üzere toplam 170 bilgisayar ile devreye alınmıştır. Öğrenci sayısı bakımında her geçen yıl katlanarak büyüyen Üniversitemiz 2006 yılı itibariyle yaklaşık olarak 5000 öğrenci ve 500 akademik/ıdari personel kapasitesine ulaşmıştır. Artan potansiyele bağlı olarak 2006 yılında Ek-Derslik binaları ve yurt binası yapılarak üniversitemiz genişlemiştir. 5 Yıllık büyüme süreci sonunda 6000 kullanıcıya yaklaşık 5200 bilgisayar ile ağ hizmet sunmaya başlayan Üniversite ağ omurgasının yenilenen teknolojik gelişmelere de bağlı olarak

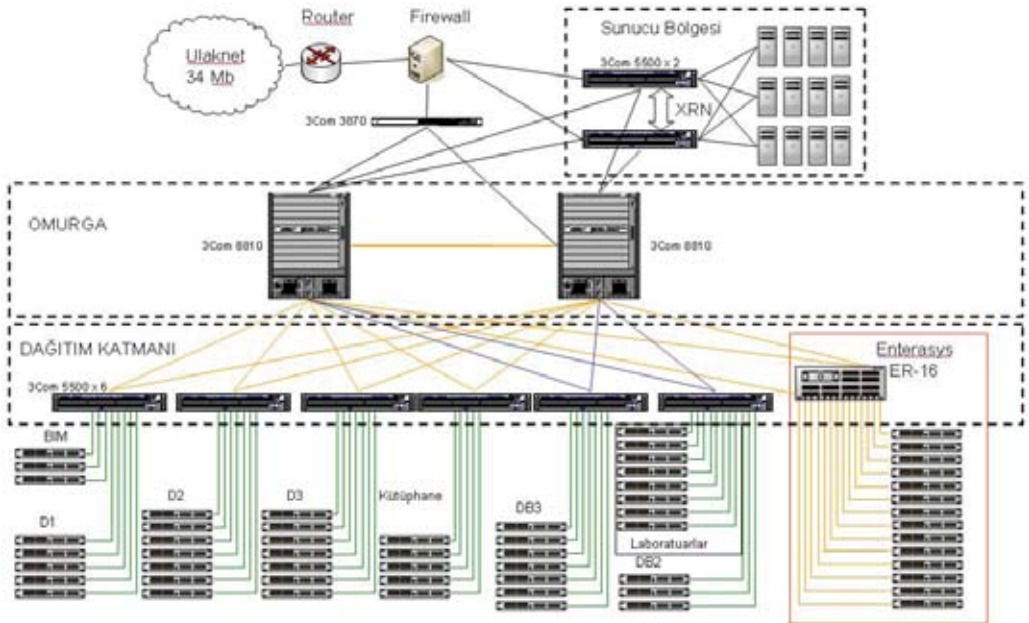
kullanıcılara en iyi hizmeti sağlayabilmek için yeniden yapılanması ihtiyacı doğmuştur.

İEÜ Eski ağ omurgası;

- Merkezde bir omurga anahtar ve her biri F/O linklerle bu merkezi anahtara yıldız topoloji ile bağlanan çok sayıda kenar anahtardan oluşmaktaydı.
- Sistem genelindeki yaklaşık 23 sunucu 10/100 Mb/s Cat5E ile omurga anahtara bağlanarak hizmet vermekteydi.
- Omurga Layer-2 olarak çalışmaktaydı ve sanal ağlar arası tüm yönlendirme (Routing) işlemleri Linux tabanlı sunucuda yapılmaktaydı.
- Ağ Omurgası Akademik, İdari ve Öğrenci olmak üzere 3 kullanıcı sanal ağı (VLAN) ve 5 Sunucu sanal ağı olmak üzere toplam 8 Temel sanal ağ (VLAN) ile hizmet vermekteydi.
- Ağ üzerindeki tüm kullanıcı cihazlarının merkezi DHCP sunucular üzerinde tanıtılarak, kendilerine tahsis edilen IP adresleri ile sisteme girmeleri sağlanmakta ve kontrol edilmekteydi.
- Kenar anahtarlarda portlar üzerinde statik VLAN kullanılmaktaydı.



Şekil-1 : İEÜ Eski Ağ omurgası



Şekil-2 : İEÜ Yeni ağ altyapısı

İEÜ Yeni Ağ Omurgası;

Yeni ağ yapısı planlarken, eski yapıdaki eksiklikler ve yaşanan sıkıntılar da göz önünde bulundurularak aşağıdaki amaçlar hedeflenmiştir.

- Mevcut 2 katmanlı ağ yapısından 3 katmanlı ağ yapısına geçerek performans artırımına ulaşmak,
- Esnek yapıda genişleyebilen VLAN yapısına ulaşmak,
- Modüler ve gelişime açık ağ altyapısı oluşturmak,
- Yüksek bant genişliği gerektiren uygulamaları kullanabilecek esnek bir yapı oluşturmak,
- Maksimum sistem "Uptime" 'ı yakalayabilmek,
- Omurga seviyesinde tam yedekliliğe ulaşmak,
- Arızaların lokalize edilerek kolay denetlenebilir yapıya ulaşmak,

Planlanan hedefler doğrultusunda kapsamlı bir planlama sonucunda Şekil-2'de gösterilen yeni ağ yapısı devreye alınmıştır.

Eski ağ omurgası tamamen L2 olarak çalışmaktaydı. Sanal ağlar (VLAN) arasındaki tüm trafik yönlendirmeleri Linux tabanlı bir sunucu üzerinden yapılmaktaydı. Bu sunucu Firewall, NAT ve varsayılan ağ geçidi gibi önemli görevleri de yürütmekte olduğundan sunucu üzerinde meydana gelen teknik arızalar tüm sistemin devre dışı kalmasına neden olmaktaydı. Ayrıca yukarıda bahsedilen görevlerin sunucu tabanlı tek bir merkezde yapılıyor olması ağ genelinde darboğazlara da neden olmakta ve ağ performansını önemli ölçüde etkilemekteydi.

Oluşturulan yeni yapıda tam yedeklilik ve sistem sürekliliğini sağlamak amacıyla omurga katmanında iki adet yüksek performanslı şase tipi anahtarlar kullanılmıştır. Yeni yapıda ihtiyaçlar ile doğru orantılı olarak artan sanal ağlar arasındaki tüm trafik yönlendirmeleri omurga anahtarlar üzerine alınmış ve yüksek yönlendirme performansı elde edilmiştir. Bu katmanda ağ geçidi (Gateway) yedekliliği ve yük paylaşımı sağlamak amacıyla VRRP teknolojisi kullanılmıştır. VRRP teknolojisi varsayılan ağ geçidini

yedeklemek için kullanılan bir protokoldür. Ağ geçidinde bir sorun olursa kullanıcı diğer ağlara ulaşamayacaktır. VRRP teknolojisi bu sorunu ortadan kaldırmak için kullanıcı tarafında herhangi bir adres değişikliği yapmadan varsayılan ağ geçidini yedeklemeyi sağlar. VRRP teknolojisini kullanarak ağ yedekliliğini sağlamak için sistemimizde kullanılan iki omurga anahtardan biri ana ağ geçidi diğeri de yedek ağ geçidi olarak konfigüre edilerek tam yedeklilik ve yük paylaşımı sağlanmıştır.

Dağıtım katmanında yüksek performanslı Gigabit anahtarlar kullanılmıştır. Yeni yapıda bu katmanın kullanım amacı ağ performansını yükseltmek, olası ağ sorunlarını (Worm, Virüs, Ethernet Arızası vb.) lokalize etmek ve yönetim kolaylığı sağlamaktır. Dağıtım anahtarları Kampüs genelindeki ara toplama bölgelerinde konumlandırılmıştır. Her bir dağıtım anahtarı her bir omurga anahtara tam yedekli yapıyı sağlayacak şekilde 2'şer adet Gigabit F/O linkler halinde bağlanmıştır. Bu sayede her bir dağıtım anahtarı ana omurgaya toplamda 4 Gigabit F/O linkle bağlanmıştır, böylece eski yapı performansı 4 kat arttırılmıştır.

Dağıtım anahtarları ve omurga anahtarları arasında MSTP teknolojisi kullanılarak bu katmanlar arasında da yedeklilik ve yük paylaşımı sağlanmıştır. MSTP teknolojisi STP ve RSTP teknolojilerinin geliştirilmesi ile ortaya çıkmıştır. Kısaca MSTP önceden tanımlanmış VLAN guruplarını belirli bir algoritma dahilinde yönlendirerek omurgaya giden tüm linklerin aktif olarak kullanılmasını sağlamaktadır.

Kenar anahtar katmanında yüksek performanslı 48 portlu yönetilebilir anahtarlar kullanılmıştır. Kenar anahtarların ihtiyaçlar çerçevesinde zaman zaman konum değiştiriyor olmaları nedeniyle, bu noktada bakır kablolanmanın esnekliğinden ve performansından faydalanılmıştır. Her bir kenar anahtar konumlandırıldığı fiziksel dağıtım noktasındaki dağıtım anahtarına 2Gigabit Cat5E'ile bağlanmaktadır böylece performans artışı sağlanmıştır.

Eski yapıda tüm sunucuların merkezdeki tek bir omurga anahtar üzerinde toplanması ve omurgaya 10/100 Mb/s gibi düşük kapasite ile bağlanması yerel ağ servislerinde darboğazlar yaratmaktaydı. Aynı zamanda omurga anahtar üzerindeki herhangi bir sistem arızasında sunucular da devre dışı kalmaktaydı.

Yeni yapıda sunucular iki adet yüksek performanslı gigabit anahtar ile oluşturulan ayrı bir sunucu bölgesinde toplanmıştır. Bu yapıda tam yedekliliğin sağlanması için XRN yığılma teknolojisi kullanılmıştır. Yığın içerisinde farklı üniteler üzerinde bulunan portlarda link-aggregation tanımlanarak sunucuların yüksek performansla (2Gigabit) omurgaya bağlantı yedekliliği sağlanmıştır. Böylece bir sunucu bölgesi anahtarı tamamen devre dışı kalsa bile sistem ikinci anahtar üzerinden hizmetine kesintisiz olarak devam edebilmektedir.

Eski yapıda her bir VLAN farklı ağ güvenlik politikaları uygulanmaktaydı. Statik VLAN yapısı kullanılıyor olması nedeniyle kenar anahtarlarda her bir port için tek tek manuel olarak VLAN ataması yapılması gerekirdi bu da çok fazla iş yükü gerektirmekteydi.

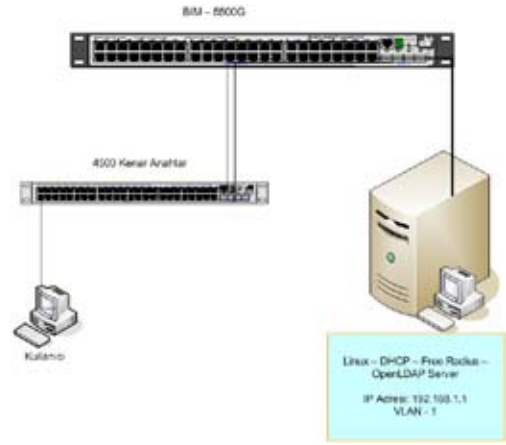
Kullanıcılar için tanımlanabilen ağ sayısının kısıtlı olması nedeniyle çok sayıda kullanıcı tek bir VLAN üzerinde toplanmaktaydı. Bu durum VLAN'lerde çok sayıda broadcast trafiği yaratmakta ve ağ performansını olumsuz olarak etkilemekteydi aynı zamanda solucan ve virüs saldırılarında güvenlik açısından ciddi tehditler oluşturmaktaydı.

Ağ genelinde statik VLAN yapısı kullanılıyor olması nedeniyle bazı kullanıcılar bilgisayarlarına statik IP set etmek suretiyle kontrolsüz olarak ağa giriş yapabilmekteydi bu durum denetim ve güvenlik sorunları yaratmaya başlamıştı.

Yeni ağ yapısında statik VLAN yapısını getirdiği ağ yönetim zorluklarının önüne geçilebilmek için Dinamik VLAN yapısına geçiş yapılmıştır. Dinamik VLAN yapısında MAC

adresini bazında VLAN ataması yapılmaktadır böylece her port için ayrı ayrı VLAN tanımlaması yapılmasına gerek kalmaksızın merkezi bir RADIUS server üzerinden kullanıcı VLAN ataması ve erişim kontrolü yapılmaktadır.

Yukarıda bahsedilen yapı Linux tabanlı sunucular üzerinde tarafımızdan geliştirilen uygulama ve yöntemlerle OpenLDAP, FreeRADIUS ve DHCP gibi açık kaynaklı yazılımlar kullanılarak devreye alınmıştır.



Şekil-3: RADIUS ve LDAP ile kullanıcı doğrulama

Geliştirilen bu uygulama sayesinde her kullanıcı ağa bağlanmak istediğinde MAC adresi kenar anahtar tarafından alınıp üzerinde tanımlı olan RADIUS sunucuda denetleniyor. RADIUS sunucusu bu isteği entegre olarak çalıştığı LDAP'a soruyor ve tanımlı bir kullanıcı ise MAC adresine bakılarak bağlı olduğu porta kullanıcının tanımlı olduğu VLAN atanıyor. VLAN atama işleminden sonra ilgili LDAP ile entegre çalışan DHCP sunucusu kullanıcının kendi MAC adresi için ayrılmış olan IP adresini atıyor. RADIUS sunucusu LDAP'ta tanımlanmamış bir kullanıcı olduğunu tespit ederse, port üzerindeki tanımsız kullanıcıyı kısıtlı yetkilere sahip bir VLAN'a yönlendiriyor. Bu şekilde yetkisiz erişimlerin önüne geçilebildiği gibi kullanıcının Kampüs içerisinde özgür bir şekilde dolaşmasına ve Kampüs dahilindeki her porttan kendi VLAN'inden ve kendi IP adresi ile dolaşması sağlanmaktadır.(Şekil-3)

Dinamik VLAN yapısı ile birlikte kullanılmaya başlanan bu denetleme mekanizması sayesinde izinsiz kullanıcıların, statik IP set etseler bile sisteme kontrolsüz girişleri engellenmiştir.

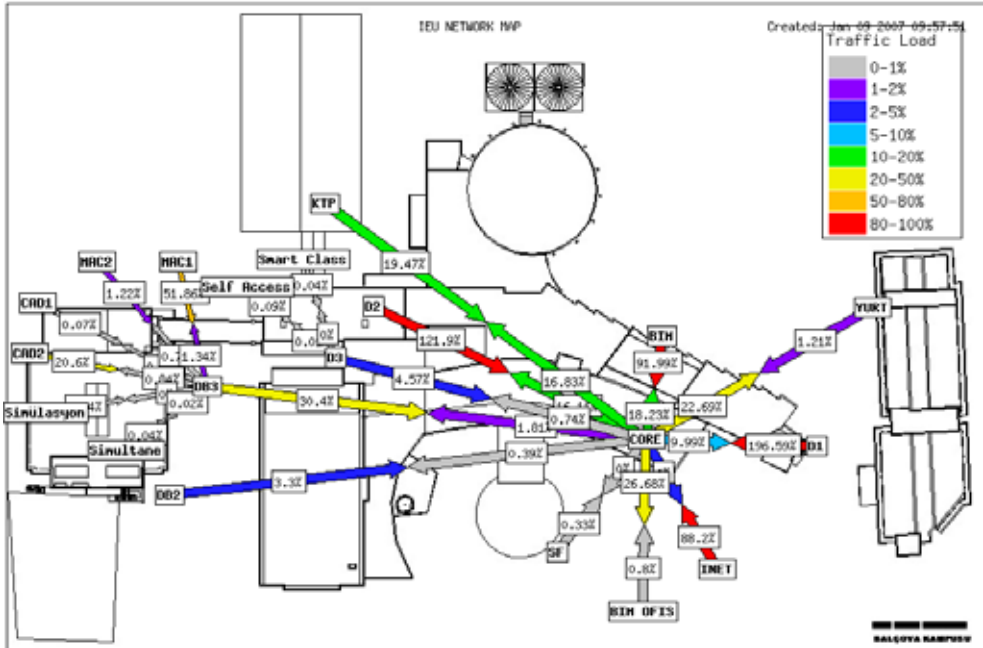
Esnek yapıda sanal ağ oluşturulması ve merkezi olarak denetlenmesini sağlayan bu dinamik yapı ile birlikte kullanıcılar Fakülte ve Departman bazında sanal ağlara bölünmüştür. Çok sayıda kullanıcıyı tek bir ağ üzerinde yığılması engellenmiş ve solucan, virüs gibi olumsuz etkenler kontrol altına alınarak yüksek performanslı esnek bir ağ yapısına ulaşılmıştır.

Ağ Yönetimi

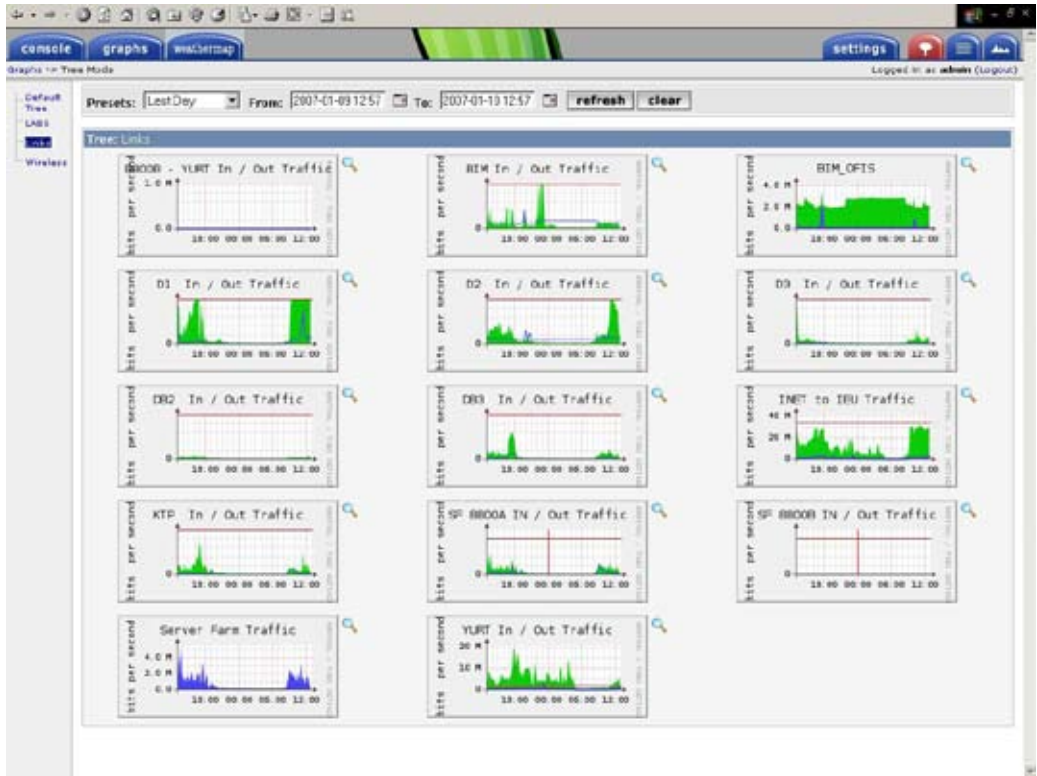
Yeni yapı ile birlikte ağdaki tüm aktif cihazlar tek bir merkezden yönetilebilir hale getiril-

miştir. Ağ yönetim merkezinden ağ üzerindeki herhangi bir cihaz IP veya MAC adresine göre sorgulanarak yer tespiti yapılabilmektedir. Ağ dahilindeki tüm aktif cihazların yapısal haritası çıkartılabilmekte ve oluşan sorunlar sistem tarafından otomatik olarak ağ yöneticilerine bildirilmektedir.

Sistemde kullanılan SNMP tabanlı açık kaynak yazılımları olan CACTI ve WeatherMap ile ağ genelindeki tüm aktif cihazların ağ performansları gerçek zamanlı olarak izlenmekte ve geriye dönük detaylı bilgi alınabilmektedir. Bu denetleme ve gözetleme mekanizması sayesinde Ağ genelinde oluşabilecek sorunlar ve oluşabilecek istenmeyen trafik kontrol altına alınmıştır. (Şekil-4, Şekil-5)



Şekil-4



Şekil-5