

Sabancı Üniversitesi Kampus Yerel Ağı

İrfan Sağdıncı

Sabancı Üniversitesi, Bilgi Teknolojisi Birimi

Özet

Sabancı Üniversitesi (SU), tüm kullanıcılarının en hızlı şekilde ve sürekli olarak bilgiye ulaşmalarını sağlayabilmek için, hızlı, ölçeklenebilir ve yönetilebilir bir ağ altyapısı oluşturmuştur. Üç aşamada gerçekleştirilen kampus yerel ağ projesinin tamamlanması ile İstanbul-Tuzla'da bulunan kampusta yaklaşık 9500 adet Internet bağlantı noktası her an çalışır duruma getirilmiştir. Bu kablolu ağ erişim altyapısının bir uzantısı olarak, açık alanlardan kablosuz erişim olanağı da sağlanmıştır. Kablolama altyapısı ilerideki büyüme ihtiyaçları da dikkate alınarak tasarlanmıştır. Kampustaki bina ağları, 4Gbps kapasiteli taşıyıcı omurga üzerinde birbirleri ile yüksek hızda haberleşebilmektedirler. Omurga üzerindeki Internet, yurt odalarında, Bilgi Merkezinde (kütüphane), sınıflarda, laboratuvarlarda bulunan tüm uçlardan erişilebilir durumdadır. Dizüstü bilgisayarların yoğun olarak kullanıldığı kampus ağı üzerinde IP (Internet Protocol) adres ayarlarının otomatik olarak gerçekleştirilebilmesi amacıyla LDAP (Light Weight Directory Access Protocol) kayıtlarını kullanan bir otomatik IP atama sistemi kullanılmıştır.

Anahtar Kelimeler; Sabancı Üniversitesi, Yerel Ağ, Kablosuz Ağ, Omurga, DHCP, LDAP

1. Giriş

Bu çalışmanın amacı, Sabancı Üniversitesi kampusunda oluşturulan ağ yapısını tanıtmaktır. Bu tanıtm çalışmasında kampus ağını oluştururken tercih edilen kablolama altyapısı, omurga ve yerel ağın genel yapısı, kullanılan aktif birimler, IP adreslerinin yönetimi ve atanması, kablosuz ağ erişim olanağı ele alınmıştır.

SU-Net olarak adlandırılan kampus yerel ağı, "Gigabit Ethernet" teknolojisi kullanılarak gerçekleştirilen, güçlü bir omurga (backbone) etrafında oluşturulmuştur. Kampus binalarında kurulu bulunan ağlar, omurgayı oluşturan merkezi noktalardan, kendisine en yakın olan, en az iki noktaya bağlanmıştır. Böylece arada taşıyıcı sistem olarak görev yapan omurga üzerinden yüksek hızda haberleşme ve olası arızalarında da sürekliliği sağlayabilmek mümkün olmuştur.

2. Kablolama

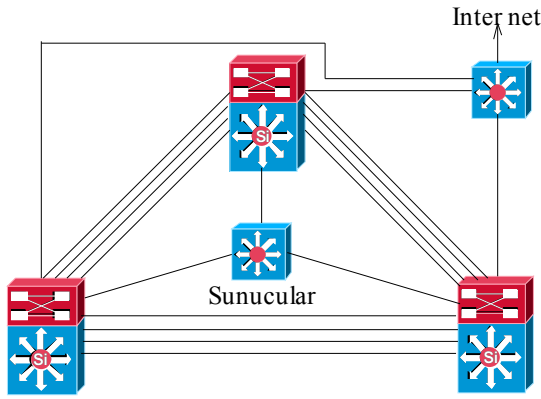
SU-Net'i oluştururken bir tasarım prensibi olarak aktif ağ birimleri arasındaki tüm bağlantılarda fiber optik kablo kullanılmıştır. Bu kapsamda, bina içlerinde ve binaların omurgaya olan bağlantılarında gelecekteki ihtiyaçları da karşılayacak şekilde, en az 12 çiftten oluşan "multi mode" yada "single mode" fiber kablolar kullanılmıştır. Bu yapıyı oluşturmak için kullanılan kablo kanalları ilerideki olası kablo değişimlerine izin verecek şekilde seçilmiştir.

Sayısı 9500'ü bulan kullanıcı bağlantı uçları, CAT-6 standardındaki UTP bakır kablolar ile sağlanmaktadır. Şu an itibariyle kullanıcı uçlarından 100Mbps'lık kapasite sağlanmaktadır. Ancak CAT-6 standardındaki kablolar ile her bir kullanıcı bilgisayarına gelecekte 1000Mbps kapasite

sağlanabilecektir. Bunu gerçekleştirebilmek için aktif ağ birimlerinde yapılacak değişiklikler yeterli olacaktır.

3. SU-Net Omurgası ve Ağ Yapısı

SU-Net omurgası birbirlerine 4 Gbps kapasite ile bağlı, aynı anda anahtarlama ve yönlendirme yapabilen (multi layer switch-router) üç adet aktif birimden oluşur (Şekil-1).“Gigabit Ethernet” teknolojisinin tercih edildiği omurga üzerinden kampus binaları arasındaki yüksek hızdaki haberleşme gerçekleştirilmekte, İnternet ve Üniversite sunucularına erişim sağlanmaktadır.



Şekil-1, SU-Net Omurgası

Omurgayı oluşturan her bir aktif birim sunucu sistemlerinin bağlı olduğu yönlendiriciye ve İnternet erişim yönlendiricisine bağlıdır. Böylece, omurgaya bağlı ağ bölgelerinden sunucu sistemlerine ve İnternet'e yedekli bağlantı elde edilmiştir.

Kampusta yer alan tüm bina ağları, üçüncü seviye (L3) çalışan aktif birimler ile kendilerine en yakın iki farklı omurga noktasına bağlıdır. Bu çoklu bağlantılar ile bağlantılarda süreklilik sağladığı gibi hatlar üzerinde yük dağılımı da yapılmaktadır.

Omurga üzerinde ve omurgaya yapılan bağlantılarda, yerel ağ uygulamalarında çok sayıda avantaj sağlayan EIGRP (Enhanced Interior Gateway Routing Protocol) yönlendirme protokolünü kullanarak, farklı ağ bölgeleri arasında yön bulma işlemleri gerçekleştirilmektedir. EIGRP yönlendirme

protokolü, haberleşme kurulacak iki nokta arasında en kısa yolun, en yüksek kapasiteli hat üzerinden tercih edilmesini sağlar. Buna ek olarak, hızlı güncelleme yapan bir yönlendirme protokolü olması nedeni ile, kampus ağına eklenen veya çıkartılan aktif birim veya ağ parçalarına ait bilgilerin hızlı bir şekilde yayılması sağlanmaktadır.

SU-Net, sayısı 60'ı geçen VLAN (Virtual Lan) ile farklı ağ gölgelerine ayrılmıştır. VLAN kullanımı ile “broadcast” alanları sınırlandırılmak suretiyle performans artırılmış ve gerekli durumlarda VLAN'lar arasında güvenlik ilişkileri tanımlanabilmiştir.

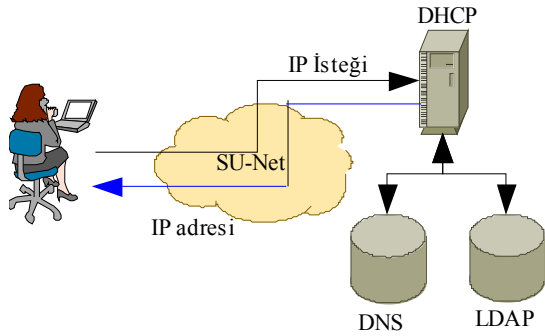
SU-Net'i oluşturan ve sayısı 130'u bulan tüm aktif ağ birimleri uzaktan yönetilebilir özelliklerine sahiptir. Yönetim amaçlı olarak kullanılan çeşitli yazılım ve donanımlarla, tüm ağ görsel olarak tek merkezden izlenmekte, yazılım güncellemeleri yapılmakta ve paket kaybı ve yönlendirme ile ilgili sorunlarda hata analizleri yapılabilmektedir.

4. IP Adres Yönetimi

Dizüstü bilgisayarların yoğun olarak kullanıldığı kampusta her alana yayılmış durumda olan bağlantı uçlarının, herhangi bir ayarlamaya gerek kalmadan kolay kullanımını sağlamak amacıyla DHCP (Dynamic Host Configuration Protocol) kullanılmıştır. Bilinen DHCP uygulamalarından farklı olarak, istekte bulunan kullanıcı bilgisayarlarına IP adresi verilirken, LDAP veritabanındaki kullanıcı bilgileri kullanılır.

Bir IP isteği geldiğinde, DHCP sunucusu istekte bulunan bilgisayarının MAC adresini LDAP sunucusundan sorgular. Uygun bir karşılık bulduğunda, ilgili kullanıcının bilgilerini kullanarak otomatik olarak DNS kayıt işlemi gerçekleştirilir (Şekil-2). Sorgulama sonucunda, uygun bir karşılık

bulunamaması durumunda, istekte bulunan bilgisayara IP adresi verilmez.



Şekil-2 IP Adres Yönetimi

Otomatik olarak gerçekleştirilen bu DNS kayıtları tüm sistemler üzerinde, kullanıcı adı ve şifrelere ek olarak tanımlayıcı bilgi olarak kullanılır. MAC adresi önceden kayıt edilmemiş bilgisayarların SU-Net'e bağlantısına izin verilmez. Böylece, kayıtsız bilgisayarların yaygın ağ uçlarından izinsiz faydalanması engellenmiş olmakla birlikte, ağdan faydalanan bilgisayarların sayısı bilinmekte ve gerekli kaynakların planlanması kolaylaşmaktadır.

5. Kablosuz Ağ

Yaygın kablolu ağın bir uzantısı olarak, kablolu ağın kullanımının mümkün olmadığı açık alanlardan da SU-Net'e kablosuz erişim sağlanabilmektedir. Kablosuz ağı oluşturan erişim noktaları IEEE-802.11b standardını desteklemektedir. Bu standart ile bilindiği gibi her bir erişim noktasının kapsama alanı içerisinde 11Mbps'lik kapasite sağlanabilmektedir. Tasarım prensibi olarak, 60-70 m²'lik alana bir erişim noktası yerleştirilmiştir. Bina dışı açık alanlarda doğrusal ve dairesel düzlemlerde erişim sağlayabilme özellikleri sağlayan dış anten ve aksesuarları kullanılmıştır.

Kablolu ağda olduğu gibi, kablosuz ağ üzerinde SU-Net'e bağlanacak kullanıcı bilgisayarlarının MAC adresleri önceden kayıtlı olmalıdır.

Kablosuz ağlarda, kullanılan radyo frekans ortamından dolayı haberleşmenin güvenli olarak gerçekleştirilmesi güçleşmektedir.

SU-Net'e kablosuz erişimde güvenliği sağlamak için, bilinen en güvenli ağ erişim yöntemlerinden olan sertifika tabanlı VPN (Virtual Private Network) kullanılmaktadır.

VPN sunucusu için açık kaynak kodlu ve mevcut standartları destekleyen Free/Swan kullanılmıştır. Böylece kullanıcı bilgisayarlarında çeşitli firmalar tarafından geliştirilen ve özel standartları olan yazılımları kullanmaya gerek kalmadan, tüm işletim sistemleri tarafından içerisinde sağlanan VPN istemci yazılımları kolaylıkla kullanılabilir.

VPN kullanımı ile, kullanıcı bilgisayarları ile kullanıcı adına işlem yapan vekil sunucu gibi davranan VPN sunucusu arasında kriptolu bir hat oluşturulmakta ve açık havada dolaşan bilgi şifrelenerek korunmaktadır. Böylece, açık havada ilerleyen bilgi üçüncü parti bilgisayarlar tarafından dinlenebilse bile anlaşılamayacaktır. VPN kullanılmadan yapılarak erişimlerde sadece Üniversitenin Internet'e açık servislerine erişime izin verilmiştir. Bazı iç servislerden faydalanmak için VPN kullanımı zorunludur.

VPN sertifikalarının hazırlanması, saklanması ve kullanıcılara ulaştırılması, kablosuz ağ erişim istek/kayıt formları ile Web üzerinden gerçekleştirilmektedir.