Kampüs Ağlarında Etkin Bant Genişliği Yönetimi Önerileri

Enis Karaarslan[1], Vedat Fetah[2] , Gökhan Akın[3], Sınmaz Ketenci[3],

[1] Muğla Üniversitesi, Bilgisayar Mühendisliği Bölümü, Muğla

[2] Ege Üniversitesi, BİTAM Kampüs Network Yönetim Grubu, İzmir

[3] İstanbul Teknik Üniversitesi, Bilgi İşlem, İstanbul
enis.karaarslan@mu.edu.tr, vedat.fetah@ege.edu.tr, akingok@itu.edu.tr, ketencis@itu.edu.tr

Özet: Kampüs ağı, sınırlı bir coğrafi alan içindeki farklı yerel ağları birbirine bağlayan büyük bir bilgisayar ağıdır. Kampüs ağlarında farklı ihtiyaçlara sahip çok sayıda kullanıcı profili bulunmaktadır. İnternet erişiminin kurumun akademik amaçlarına uygun ve etkin bir şekilde kullanılması sağlanmalıdır. Bunu sağlamak için kurumun ihtiyaçları analiz edilip belirlenmeli ve bant genişliği verimli olarak paylaştırılmalıdır. Bu bildiride bant genişliği kısıtlama ve servis kalitesi (QoS) kavramları ele alınacaktır. Ege Üniversitesi ve İTÜ ağlarında yaşanan deneyimler ve uygulama örnekleri verilecektir.

Anahtar Sözcükler: Ağ yönetimi, kampüs ağları, servis kalitesi, QoS, bant genişliği yönetimi

Efficient Bandwith Management in Campus Networks

Abstract: Campus network is a large computer network which interconnects different local networks in a limited geographical area. Many user profiles with different needs exist in campus networks. It should be assured that internet access is used according to the associations academic purposes and in an efficient way. The needs of the association should be analysed and bandwith must be shared efficiently. Bandwith limitation and quality of service (QOS) concepts will be discussed in this paper. The experience gained in the Ege University and ITU networks and implementation recommendations will be given.

Keywords: Network management, campus networks, quality of service, QOS, bandwith management

1. Giriş

Kampüs ağları, farklı binalara yayılmış farklı yerel ağları (LAN) birleştiren büyük ağlardır. Bu adı, birçok binadan oluşan üniversite kampüslerinden almıştır. Bu bildiride, kurumsal ağlar olarak üniversite ağları ele alınmaktadır. Kampüs ağlarında çok farklı kullanıcı profilleri bulunmakta ve kullanıcıların farklı ihtiyaçları bulunmaktadır.

Kısıtlı olan bant genişliğinin kampüs ağlarında etkin kullanılması için aşağıdaki çalışmaların yapılması gerekecektir:

- Kampüs ağının tanımlanması
- Sistem Bilgilerinin Çözümlenmesi
- Kısıtlama ve/veya düzenlemelerin uygulanması

Bu bildiride uygulama olarak açık kaynak ve ticari ürünlerden örnekler verilecektir. Açık kaynak uygulamalara örnek olarak PFSENSE uygulaması verilecektir. Ağ altyapısında yapılabilecek kısıtlamalara örnek olarak Cisco cihazlarda yapılabilecek ayarlar sunulacaktır.

Bu bildirinin hedefi mümkün olduğunca bu süreci sadeleştirmek ve bu konuda çalışanlara kolaylık sağlamaktır.

2. Kampüs Ağının Tanımlanması

Kampüs ağları, çok sayıda bilgisayar ve çok sayıda iletişim cihazından oluşan kompleks ağlar olduğu için, ağ trafik yönetimi küçük ağlara göre daha zor olmaktadır [1]. Kurumun

ihtiyaçlarına göre, benzer ihtiyaçlara sahip kullanıcılar gruplanmalı ve aynı sanal ağlar (VLAN) içerisinde toplanmalıdır. Her sanal ağ için ayrı bir IP aralığı (subnet) kullanılmaktadır.

Kampüs ağının tanımlanmasının nasıl yapılabileceği ayrıntılı olarak [1]'de incelenmişti. Kampüs ağını tanımlayan bilgilerden bant genişliğinin etkin kullanımı için belirlenmesi gerekenler aşağıdaki gibidir [1]:

• Alt ağlar (subnet): İç ağda kullanılan alt ağlar ve bunların nerede yönlendirildikleri veya yönlendirilecekleri (routing) belirlenmelidir.

• Bilgisayar sayısı: Her sanal ağdaki ve sistemdeki toplam bilgisayar sayısı önemli bir kriterdir. Aslında daha önemlisi birim zamanda aktif olan bilgisayar sayısının belirlenmesidir. Aynı zamanda, ağa eklenebilecek bilgisayarlar sayısı da göz önünde tutulmalıdır.

• Bant genişliği (bandwith): Hattın ne yoğunlukta kullanıldığı ölçülmelidir. SNMP parametreleri tanımlanan her cihazın trafik kullanım istatistiksel değerleri toplanabilir. Bunun için ücretsiz bir yazılım olan Multi Router Traffic Grapher – MRTG (http://oss.oetiker.ch/mrtg/) programı kullanılabilir.

• Trafik Profili: Ağ trafiğini oluşturan trafik sınıflandırılmalıdır.

• Kullanıcı profili: Netflow ve benzeri trafik analiz programları kullanılarak sanal ağ veya IP bazlı olarak kullanıcı profili çıkarılabilir. Böylece belirli bir IP veya IP bloklarının hangi saatler arasında ne tür bir trafik yaptığının belirlenmesi hedeflenmektedir. Kullanıcı tipleri ve kullandıkları ağ tabanlı uygulamalar belirlenmelidir. Kullanıcıların hangi sistemlere, hangi saat dilimlerinde, hangi port'lardan eriştikleri de tespit edilmelidir.

Toplanan bilgilerin nasıl çözümleneceği bir sonraki bölümde ayrıntılı olarak ele alınacaktır.

Bu bilgilerin toplanması ve belgelenmesi kolay bir süreç değildir. Mümkün olduğunca fazla bilgi toplamak, bant genişliğinin daha etkin paylaştırılmasını sağlayacaktır. Bilginin güncel olması için, sürekli olarak bu bilgiler toplanmaya ve belgelenmeye devam edilmelidir.

3. Sistem Bilgilerinin Çözümlenmesi

"Kampüs Ağı Tanımlama", düzenli olarak güncellenmesi gereken bir süreçtir. Bu süreç boyunca toplanan sistem bilgilerinin çözümlenerek bant genişliğinin nasıl paylaştırılacağı belirlenmelidir.

Trafik profili incelenerek kurumun amacına uygun trafik tanımlanmalıdır. Örneğin, kurumda VoIP uygulaması kullanılıyorsa, bu hizmetin aksamaması için gereken bant genişliği tanımlanmalı ve bu hizmetin alabileceği en az bant genişliği garantilenmelidir. Kurumda hastane otomasyonu gibi aksamaması gereken uygulamalar varsa tanımlanmalı ve bant genişliğinin belirli bir miktarı bu uygulamalara ayrılmalıdır.

Kurum için önemli olan ve hiçbir şekilde kısıtlamaya girmemesi ve öncelik verilmesi gereken cihazlar (sunucular ... vb) tanımlanmalıdır. Bu sunucuların bu tür kısıtlamalardan etkilenmemesi sağlanmalıdır.

Kurum ağının bant genişliğini dolduran ve satüre olmasına sebep olan protokollerin neler olduğu belirlenmelidir. Örnek olarak Ege Üniversitesi ağında düzenleme yapılmadan önce şu şekilde bir sıralamadan söz etmek mümkündü:

1- http download
2- ftp download
3- flash video streaming
4- video streaming

Bu sorunun önüne geçebilmek için yapılabilecekler aşağıdaki gibidir:

1. Bant genişliği kısıtlama teknikleri (Trafik şekilleme, trafik denetimi) ile toplam bant

genişliğinin belirlenmesi: Farklı zaman dilimlerinde farklı olacak şekilde alt ağlar için sınırlandırmalar yapılabilir. Örneğin kablosuz ağların kullanacağı bant genişliği sınırlandırılabilir.
2. İhlal yaratan kullanıcıların belirlenmesi ve oluşturulacak bir karantina grubuna alınması. Hattı sömüren kullanıcıların belirli bir bant genişliğinde sınırlandırılmasıdır.
3. P2P vb. protokollerin
    - Mesai saatlerinde tamamen engellenmesi
    - Mesai saatlerinde/sonrasında istenilen bant genişliğine sıkıştırılması.

Bant genişliği paylaşımı, farklı zaman dilimlerinde farklı yapılacak şekilde tasarlanması etkin olmaktadır. Zaman, aşağıdaki şekilde tanımlanabilir:
- Mesai İçi
- Mesai Dışı
    - Akşam
    - Hafta sonu

4. QOS ve L7 Filtreleme

Ağ İletişimi Hizmet Kalitesi (Quality of Service, kısaca QoS), ağ üzerindeki uygulamaları önceliklendirerek zaman kaybını azaltmayı hedefleyen bir ağ servisidir. Bir ağ bağlantısı üzerinden çalışan bir trafik veya program türüne öncelik veren çeşitli tekniklere karşılık gelir. Ağ üzerinde hareket eden paketler sizin daha önce ağınız üzerinde analiz edip önceliklerini belirttiğiniz sırada bölünerek kuyruğa alınır. Bu sayede iletişimin hızlı olması ve kesintiye uğramaması gereken uygulamaların, daha öncelikli ve belirli bir band genişliğine sahip olarak sorunsuz bir şekilde çalışması sağlanabilir [4].

Kurum ağında, IP ağları üzerinden telefon görüşmesi (VOIP) için QOS tanımlaması yapıldığını farzedelim. Kurum ağında P2P uygulamalarının bant genişliğini aşırı kullanmasında bile, Voip için görüşmelerde herhangi bir kesintiye uğramaksızın gerçekleştirebilmesine olanak sağlar [4].

QoS'un etkin kullanımı için öncelikle çeşitli protokoller ve uygulamalar sınıflandırılmalıdır. Günümüzde uygulamaları ayırt etmek için ağ kapısı (port) numaralarını kullanmak yeterli değildir. Bu yüzden uygulamaların sınıflandırmasını imza veya davranış tabanlı çözümleyen L7 filteleme sistemlerinin kullanılması daha etkin bir çözümdür. Bu sistemler, yüksek başarımla uygulamaları sınıflandırabilmektedir.

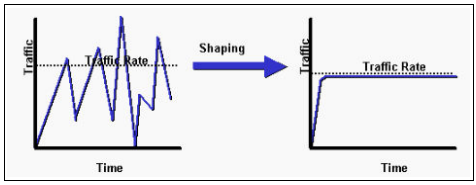
5. Bant Genişliği KısıtlamaTeknikleri

Bant genişliği kısıtlama teknikleri olarak çeşitli yöntemlerden söz etmek mümkündür. Bu bildiride, 2 temel bant genişliği kısıtlama tekniği ele alınacaktır:
- Trafik Şekilleme (Traffic Shaping)
- Trafik Denetimi (Traffic Policing)

Bu iki metodun da avantaj ve dezavantajları ve buna bağlı olarak da farklı kullanım yerleri bulunmaktadır.

5.1. Trafik Şekilleme

Trafik Şekilleme tekniğinde belirlenen limiti aşan trafik, yönlendiricinin tampon belliğinde tutulur ve sürekli aynı band genişliğinde kalması sağlanacak şekilde bant genişliğinin akışına izin verilir. Bant genişliği tüketiminin sabitlenmesinin yanı sıra paket kaybının az olması da sağlanmaktadır. Trafik şekilleme tekniği uygulandığında trafiğin değişimi Şekil 2'de gösterilmiştir [3].



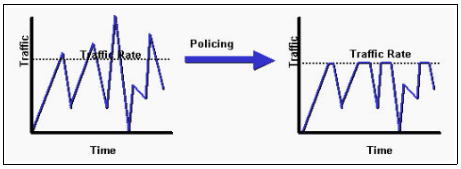
Şekil 1. Trafik Şekilleme

Bu teknikte, verinin tampon bellekte beklemesinden dolayı, verinin hedefe

ulaşmasında gecikme oluşmaktadır. Yaygın olarak Frame-Relay ve ATM gibi uç noktalarının birbirlerine farklı hızlar ile bağlanabildiği WAN bağlantılarında kullanılmaktadır. Yerel alan ağlarında pek tercih edilen bir bant genişliği yönetim sistemi değildir.

5.2. Trafik Denetimi

Trafik denetimi (Traffic Policing) tekniğinde, belirlenen bant genişliği miktarının üstündeki trafik ya çöpe atılır (drop) ya da bu trafiğin IP paket başlığında bulunan ToS kısmındaki paket önceliğini belirleyen sayı değerleri değiştirilir. Trafik sınırlandırılması tekniği uygulandığında trafiğin değişimi Şekil 2'de gösterilmiştir [3].



Şekil 2. Trafik Denetimi

Bu sayede düşük öncelikli olarak belirlenmiş bu trafik, çıkış yönlendiricisi tarafından bant genişliği yönetimi amaçlı bir işleme tabi tutulabilir. Bu teknikte tampon bellek kullanılmadığı için paket kaybı daha fazladır. Ancak gecikme ve hafıza ihtiyacı daha azdır.

6. Uygulamalar

Uygulamalar, eğer kurumun altyapısı destekliyorsa ana omurga cihazlarında yapılabileceği gibi, bu işi yapmak için bir güvenlik duvarı gibi ayrı bir cihaz üzerinde de gerçekleştirilebilir. Bu bildiride aşağıdaki uygulamalardan örnekler verilmiştir:

- Açık kaynak yazılım - PFSENSE uygulaması
- Cisco L3 cihazlarda (yönlendirici yeteneğindeki) uygulama örnekleri

6.1. PFSENSE Uygulaması

PFSENSE, arayüzü oldukça basit tasarlanmış ve kullanımı kolay bir dağıtımdır. Bu dağıtımın 2.0 Alpha Alpha versiyonu ile birlikte L7 seviyesinde Qos ve paket filtreleme yapılabilmektedir. Önceki sürümlerinde sadece snort ve squid kullanılarak bandgenişliği kontrolü sağlanırken, yeni sürümü ile birlikte trafik şekillendirme özelliği güçlendirilmiştir. Uygulama seviyesinde bir çok uygulamanın imzası kendi içerisinde olduğu için ekstra bir çabaya gerek yoktur. Bunun yanı sıra, var olan imzalar dışında herhangi bir uygulama için de paket yüklenmesi ve imzanın tanıtılması mümkündür. Pfsense kurulumunuzu bitirdikten sonra birçok değişikliği web arayüzünden yapabilirsiniz.

L7 seviyesinde firewall olarak çalışan birkaç dağıtım daha vardır. Bunları sayacak olursak IPCop Firewall, OpenBSD PF, ebtables ve Bandwidth Arbitary gibi yazılımlar listelenebilir. Pfsense dağıtımının bu dağıtımlar arasından ön plana çıkaran temel özellikleri aşağıdaki gibidir:

1. L7 filtrelemede uygulama imzası girebilir ve bu sayede dağıtımın desteklemediği uygulamalar için de paket filtreleme özelliğini kullanır.
2. Grafik arayüzünün basitliği sayesinde kullanıcı isterse ekstra modüller kurabilir. Kurulabilecek modüller arasında IDS, Antivirus Gateway, Squid Proxy, ntop, traffic shaping ve Vpn gibi açık kaynak yazılımları sayılabilir.
3. Kurulan modüller web arayüzünden aktive ya da deaktive edilebilir,
4. Yüksek boyutlu disklere kurulumu sırasında diski görmeme gibi sorunlar yaşanmaz,
5. Diğer Linux dağıtımlarındaki gibi kurulum sırasında grafik kartının tanınmaması gibi bir sorun ile uğraşmak zorunda kalınmaz,
6. Vlan desteği vardır.
7. Birden fazla Wan ve Lan arayüzünü

destekler.

8. NAT, CARP, Load Balance, Packet Capture ve Bogon networkleri tanıma özellikleri ayrıca bulunmaktadır.

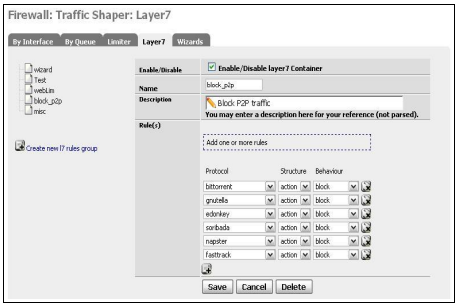
Pfsense özelleştirilmiş bir FreeBsd dağıtımıdır. Ana özellikler firewall ve router olarak çalışmak üzere tasarlanmıştır. Pfsense, yüksek throughput senaryoları düşünülerek (500 Mbps) tasarlanmış bir dağıtımdır. Bu hızlarda çalışabilmesi için kullanacağınız yüksek kapasiteli bir donanım mimarisi kullanmanız gerekmektedir.

L7 filtreleme yapabilmek için öncelikli olarak uygulama olarak **ipfw-classifyd** konusunda bilgi vermemiz gerekmektedir. Bu uygulamanın neler yapabileceğine göz atacak olursak:

(i) gelen trafik için bloklama kuralı oluşturabilir,

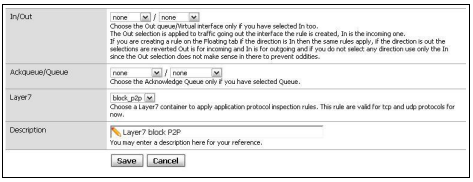
(ii) Gelen ip paketleri veya belirlenen akışlar traffic shaper sayesinde AltQ kuyruğuna atılır.

Bir L7 kuralı oluşturulduğu zaman bu işlemin sonunda pf otomatik olarak ipfw-classifyd ile arka planda kuyruğa atma işlemi için gerekli kuralları oluşturur. Burada dikkat edilmesi gereken husus, ipfw-classifyd uygulamasının sadece TCP ve UDP packetleri desteklemesidir. Bu yüzden işlemlerin yapılacağı paketlerin protokolleri çok önemlidir. Pfsense kutusunda bu kuralların nasıl kolaylıkla yazıldığı Resim 1'de gösterilmiştir.



Resim 1. Traffic Shaper: L7 Kural Yazma Alanı

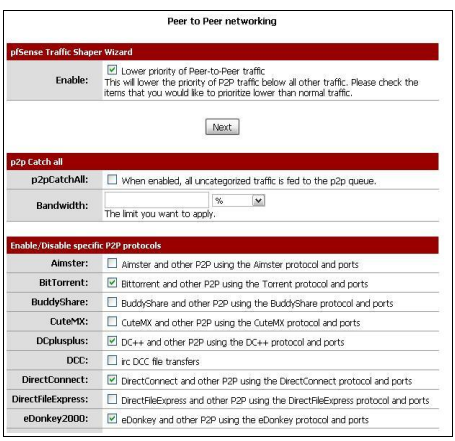
Belirlenen protokollere göre yapılacak işlemlerde protokolün bloklanması dışında "Limiter" sekmesinde belirli bir limit dahilinde çalışması sağlanabilir. Yani "video streaming" işlemi için verilecek değerin üzerine çıkılması durumunda işlemin kuyruğa atılması özelliği de kullanılabilir. Bu işlemleri tanımladıktan sonra firewall tablosunda kural yazabileceğimiz alanda nasıl özellikler kullanabileceğimizi Resim2 'de daha net görebiliriz.



Resim 2. Firewall kural yazım alanı

Resim 2'de görülebileceği üzere güvenlik duvarında yazılması gereken kurala atayabileceğiniz L7 kuralı ve kuyruk işlemleri görülmektedir. Bloklama işlemi yapılabildiği gibi kuyruğa atma işlemi de gerçekleşebilmektedir.

Yukarıda belirlenen şekilde protokoller hakkında işlem yapılacağı gibi pfsense'in kendi üzerinde bulunan sihirbazlar sayesinde belirli bazı protokol gruplar için de özel yaptırımlar uygulanabilir. Resim 3'de trafik şekillendirme sihirbazı gösterilmiştir.



Resim 3. Trafik şekillendirme sihirbazı uygulaması

Bu sihirbaz kullanılarak, p2p uygulamalar için atanacak bant genişliği belirlenebilir, bazı p2p uygulamalarını bu gruptan çıkarılabilir veya hepsi için bütün bu kurallar uygulanabilir. Bu uygulamalar sadece p2p uygulamaları için geçerli değildir. Aynı zamanda oyun ağları için de aynı özelliklerin kullanabilmesi mümkündür. Pfsense ile yapılabileceklerin ayrıntılı yazıldığı belge için bakınız [5].

6.2. Cisco Cihazlarda Uygulama Örnekleri

Bu bölümde Cisco l3 cihazlarda yapılabilecek uygulamalara örnekler verilecektir. Kurumun kampüs ağının ana omurgasında 6500 serisi bir L3 anahtar olması durumunda aşağıda verilen örnekler gibi uygulamalar yapılabilmesi mümkün olacaktır.

Cisco 6500 serisi anahtarlar, iki çeşit aggregate policer (toplam sınırlandırıcı) destekler. Bunlar per-interface (arayüz bazlı) ve named (isimlendirilmiş) aggregate policer'lardır. Per-interface aggregate policer uygulandığı her arayüz için giriş yönünde ayrı ayrı sınırlandırma yapar. Per-interface sınırlandırıcı "policy-map" yapılandırması ile tanımlanır. İsimlendirilmiş aggregate policer ise uygulandığı tüm arayüzlerdeki trafiğin toplamına sınırlandırma getirir. İsimlendirilmiş aggregate policer Cisco yönlendiriciler tarafından desteklenmemektedir.

Per-interface aggregate policer ile toplam bant genişliği sınırının belirlenmesi aşağıdaki şekilde yapılır. Bu örnekte gigabit 2/1 arayüzüne gelen trafiğin toplam 60Mb ile sınırlanmasını sağlayan yapılandırma gösterilmiştir.

```
6500(config)# mls qos
6500(config)# access-list 160 permit ip any
10.0.0.0 0.0.0.255
6500(config)# class-map 60Mb_Sinifi
6500(config-cmap)# match access-group 160
6500(config-cmap)# exit
6500(config)# policy-map 60Mb_toplam
6500(config-pmap)# class 60Mb_Sinifi
6500(config-pmap-c)# police 60000000
6500(config-pmap-c)# exit
6500(config-pmap)# exit
6500(config)# int gi2/1
6500(config-if)# service-policy input 60Mb_toplam
```

İsimlendirilmiş aggregate policer ile toplam bant genişliği sınırının belirlenmesi ise şu şekilde yapılır. Bu örnekte gi2/1 ve gi2/2 arayüzüne gelen tcp 445 hedefli trafiğin toplam 10Mb ile sınırlanmasını sağlayan yapılandırma gösterilmiştir. Tanımlanan named aggregate policer farklı policy-map'lerde de kullanılabilir. Bu durumda named aggregate policer'da tanımlanan bant genişliği uygulandığı policy-map'ler tarafından ortak olarak paylaşılır.

```
! QoS aktif hale getirildi.
6500(config)# mls qos
! İsimlendirilmiş aggregate policer tanımlandı.
6500(config)# mls qos aggregate-policer smb_10Mb
10000000 312000 312000 conform-action transmit
exceed-action drop
6500(config)# access-list 110 permit tcp any any
eq 445
6500(config)# class-map smb
6500(config-cmap)# match access-group 110
6500(config-cmap)# exit
6500(config)# policy-map 10Mb
6500(config-pmap)# class smb
6500(config-pmap-c)# police aggregate smb_10Mb
6500(config-pmap-c)# exit
6500(config-pmap)# exit
6500(config)# int gi2/1
6500(config-if)# service-policy input 10Mb
6500(config)# int gi2/2
6500(config-if)# service-policy input 10Mb
```

Cisco cihazlarda kullanıcı grupları tanımlanarak bu gruplardaki her kullanıcı için bant genişliğinin sınırlandırması da mümkündür. Bu işlem için öncelikle trafik tiplerinin gruplanması için kullanılacak sınıf haritaları (class-map) oluşturulur. Sınıf haritalarında trafiğin tanımlanması için erişim

kontrol listeleri (ACL) kullanılması yapılacak sınırlandırmanın zaman bazlı uygulanabilmesi seçeneğini de beraberinde getirecektir. Tanımlanmış olan farklı sınıf haritaları için tek bir politika haritası (policy-map) altında farklı bant genişliği sınırlandırılması yapılabilir. Aşağıda örnek yapılandırma açıklamaları ile verilmiştir.

Öncelikle sınıf haritalarında kullanıcı gruplarını tanımlayacak erişim kontrol listeleri oluşturulmalıdır. Uygulanacak sınırlandırmanın zaman bazlı olması isteniyorsa zaman aralıkları tanımlanmalı ve erişim kontrol listeleri satırlarında kullanılmalıdır. Zaman aralığının tanımlanması aşağıdaki gibidir:

```
Router(config)#time-range gunduz
Router(config-time-range)#periodic weekdays 09:00
to 18:00
```

Farklı sınıf haritalarında kullanılacak erişim kontrol listelerinin tanımlanması aşağıdaki gibidir:

```
Router(config)#access-list 101 permit ip any
160.75.1.0 0.0.0.255 time-range gunduz
Router(config)#access-list 102 permit ip any
160.75.11.0 0.0.0.255 time-range gunduz
```

Sonraki adımda sınıf haritaları tanımlanmalıdır. Örneğin, personel ve misafir sınıfının tanımlanması aşağıda verilmiştir:

```
Router(config)#class-map personel_sinifi
Router(config-cmap)#match access-group 101
Router(config-cmap)#exit
Router(config)#class-map misafir_sinifi
Router(config-cmap)#match access-group 102
```

Son adımda ise hizmet haritası oluşturulup cihazın uygun arayüzüne uygulanmalıdır. Hizmet haritası oluşturulur ve her sınıf haritası için uygulanacak bant genişliği değerleri belirtilir. “police flow” sonrasında belirtilen ilk değer saniyedeki bit sayısını belirtir. İkinci değer ise her kullanıcı için bant genişliği sınırlandırması yapılmadan yaratabileceği trafiğin byte cinsinden miktarıdır.

```
Router(config)#policy-map gunduz_sinirla
Router(config-pmap)#class personel_sinifi
Router(config-pmap-c)#police flow 1024000 256000
conform-action transmit exceed-action drop
Router(config-pmap-c)#exit
Router(config-pmap)#class misafir_sinifi
Router(config-pmap-c)#police flow 512000 128000
conform-action transmit exceed-action drop
```

Hizmet haritasının cihazın dış ağa bakan arayüzüne giriş yönünde uygulanması ile kullanıcıların dış ağdan gelen trafiğine sınırlandırma getirilmiş olacaktır. Bu sayede 101 nolu ACL’ye uyan kullanıcılar anlık 1Mb kullanabilirler. 102 nolu ACL’ye uyan misafir grubu ise anlık 512Kbit’lık erişim yapabilirler.

```
Router(config)# interface gigabitEthernet 1/1
Router(config-if)#service-policy input
gunduz_sinirla
```

Cisco uygulamaların ayrıntılı anlatıldığı belge için bakınız [6].

6. Sonuç ve Öneriler

Bu bildiride, kurumların kısıtlı olan bant genişliklerini daha etkin kullanmaları için yapabileceklere öneriler verilmiştir.

Bildiride PFSENSE ve CISCO ortamındaki uygulamaların bir kısmına yer verilmiştir. Daha ayrıntılı içeriğe ULAK-CSIRT belgeler (http://csirt.ulakbim.gov.tr/dokumanlar/) sayfasından ve referanslardan ulaşılabilir.

7. Kaynaklar

[1] 2005, Karaarslan Enis, ”Kampüs Ağ Yönetimi”, Akademik Bilişim 2005, http://www.karaarslan.net/bildiri

[2] 2005, Soysal M., Fetah V., Akın G., Karaarslan Enis, ”P2P ile Yaşamak”, Akademik Bilişim 2005, http://www.karaarslan.net/bildiri

[3] Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting, Cisco, 2005, http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

[4] Yalçıner A., QOS Quality of Service, 2009, http://alper.web.tr/2009/03/16/qos-quality-of-service/

[5] Fetah V., Pfsense ile Uygulama Seviyesinde Bant Genişliği Yönetimi, 2010 http://csirt.ulakbim.gov.tr/dokumanlar/2010_pfSensePlatform_L7FiltrelemeQoSUygulamalariv2.pdf

[6] Akın G., Ketenci S., Kampüs Ağlarında Cisco Yönlendirici ve Anahtar Cihazları ile Bant Genişliği Yönetimi Teknikleri, 2010 http://csirt.ulakbim.gov.tr/dokumanlar/2010-Cisco-BantGenisligiYonetimi.pdf