KAMPÜS AĞLARINDA ETKİN BANT GENİŞLİĞİ YÖNETİMİ

Enis Karaarslan

Muğla Üniversitesi, Bilgisayar Mühendisliği Bölümü

Vedat Fetah

Ege Üniversitesi, BİTAM Kampüs Network Yönetim Grubu

Gökhan Akın

İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı

Sınmaz Ketenci

İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı

Giriş

- Kurumsal ağ – kampüs ağları
  - Farklı kullanıcı profilleri
  - Farklı ihtiyaçlar
- Hedef: Kısıtlı bant genişliğinin etkin kullanılması

Etkinleştirme Çalışmaları

- Kampüs Ağının Tanımlanması
- Sistem Bilgilerinin Çözümlenmesi
- Kısıtlama/düzenlemelerin uygulanması

Kampüs Ağının Tanımlanması

- Alt ağlar (subnet)
- Bilgisayar Sayısı
- Bant Genişliği (Bandwidth)
- Trafik Profili
- Kullanıcı Profili

Sistem Bilgilerinin Çözümlenmesi

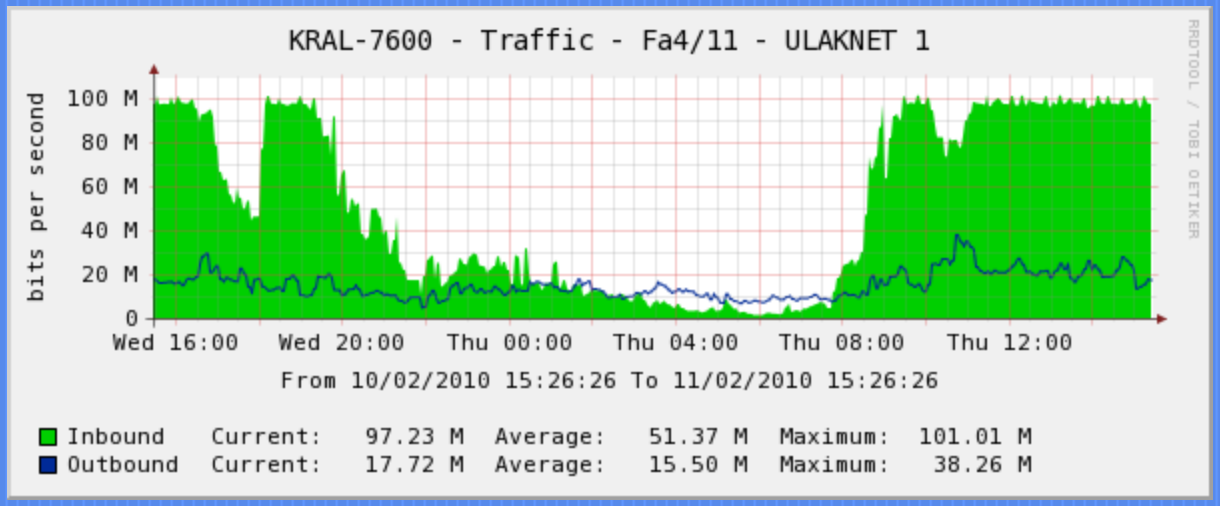
- Bant genişliği ihtiyaçlarının belirlenmesi
- Trafik profili incelenerek kurumun amacına uygun trafik tanımlanmalıdır. Örneğin:
  - YÜKSEK ÖNCELİK: Kurumun asıl öncelikli trafiği
    - Ör: hastane SGK erişimi
  - ORTA DERECE ÖNCELİK:
    - Ör: http web
  - DÜŞÜK ÖNCELİK: İstenmeyen Trafik
    - Ör: P2P

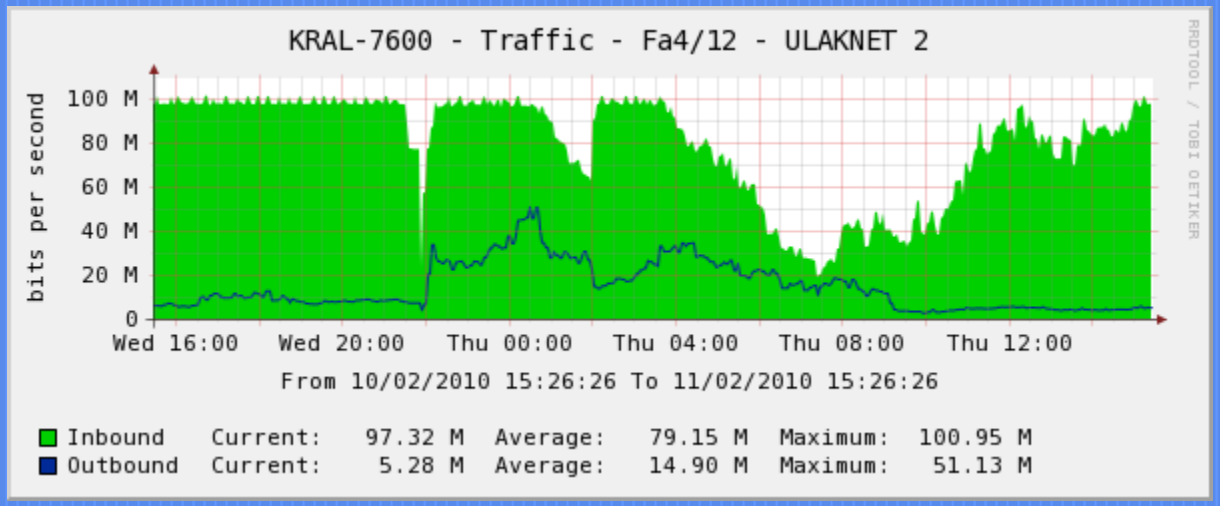
Sistem Bilgilerinin Çözümlenmesi-2

Kısıtlama Düzenleme Zamanının belirlenmesi. Örneğin:

- Hafta içi
  - Mesai içi
  - Mesai dışı
- Hafta Sonu

Sistem Bilgilerinin Çözümlenmesi-3





Kısıtlama/Düzenleme

- Traffic shaping ile uygulama / alt ağ / host bazlı bant genişliğinin ayarlanması
- İhlal yaratan kullanıcıların belirlenmesi ve oluşturulacak bir karantina grubuna alınması - kısıtlanması

Kısıtlama/Düzenleme-2

- P2P vb. protokollerin
  - Tamamen engellenmesi
  - Mesai saatlerinde tamamen engellenmesi
  - Mesai saatlerinde/sonrasında istenilen bant genişliğine sıkıştırılması.

Çözümler

1- Internet Çıkış Noktasında Kullanılabilecek Ürünler
(Açık Kaynak Uygulama İşlenen Örneği: PFSENSE)

2- Proxy Sunucuları

3- Ağ Altyapısı Cihazları ile yapılabilecek Uygulama
(İşlenen Örneği: Cisco cihazları)

PFSENSE Çözümü

Pfsense özelleştirilmiş bir FreeBsd dağıtımıdır.

Esas olarak güvenlik duvarı ve router olarak çalışmak üzere tasarlanmıştır.

IDS, Antivirus Gateway, Squid Proxy, ntop, trafik şekillendirme ve Vpn gibi yazılımlar ekstra modül olarak eklenebilir.

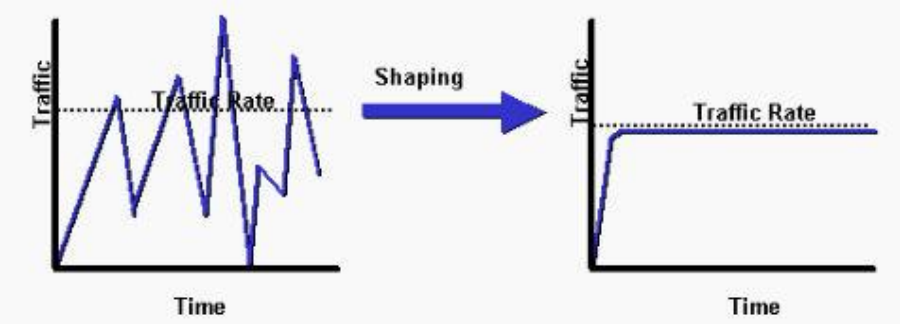
Cisco Cihazlarda Bant Genişliği Yönetimi Teknikleri

Cisco yönlendirici ve anahtar cihazlarında bant genişliği yönetimi iki farklı metot ile gerçekleştirilebiliyor:

1- Traffic Shaping (Trafik Şekilleme)

2- Traffic Policing(Trafik Sınırlandırılması)

Traffic Shaping (Trafik Şekilleme)

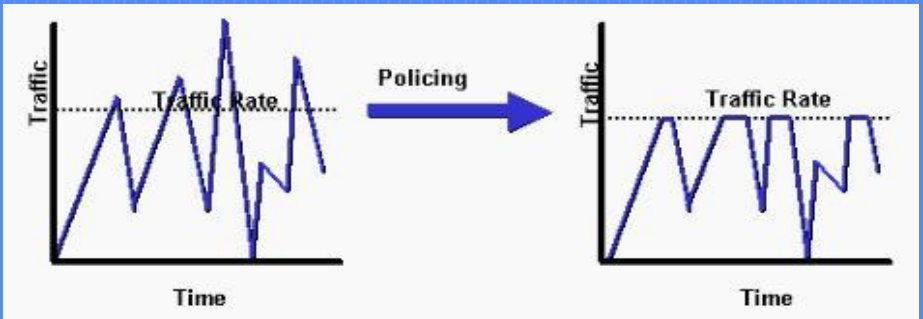


Kaynak: www.cisco.com

"Traffic Shaping" tekniğinde belirlenen limiti aşan trafik yönlendiricin tampon belliğinde tutulur ve akışın sürekli aynı bant genişliğinde kalması sağlanacak şekilde bant genişliğinin akışına izin verilir.

Yaygın olarak Frame-Relay, ATM gibi birbirinden farklı hızlar ile bağlantı sağlanabilen WAN linklerinde kullanılmaktadır.

Traffic Policing (Trafik Sınırlandırılması)



Kaynak: www.cisco.com

"Traffic Policing" metodunda belirlenen bant genişliği miktarının üstündeki trafik ya çöpe atılır (drop) yada bu trafiğin IP başlığında bulunan ToS kısmındaki paket önceliğini belirleyen sayı değerleri değiştirilir.

Traffic Policing Teknikleri

1- Aggregate Policing:

Bu teknik bir grup kullanıcının tamamı için toplam bir üst sınır belirlemekte kullanılır.

2- Microflow Policing:

Bir trafik akışına (flow) bant genişliği sınırlaması uygulanabilir. Doğru bir yapılandırma ile bir kullanıcının anlık erişebileceği bant genişliği üst sınırı belirlenebilir.

Aggregate Policing Türleri

1- Per-interface aggregate policing (arayüz bazlı)

Arayüz bazlı aggregate policer uygulandığı her arayüz için ayrı ayrı sınırlandırma yapar.

2- Named aggregate policing (isimlendirilmiş)

İsimlendirilmiş aggregate policer ise uygulandığı tüm arayüzlerdeki trafiğin toplamına sınırlandırma getirir.

Per-interface Aggregate Policing

Konfigurasyon adımları:
1- Erişim kontrol listeleri ile trafik tarif edilip bir trafik sınıfı oluşturulur. (Class-map)
(örnek: kaynak IP adresi 10.0.0.1 olan gibi)

2- Oluşturulan sınıfa uygulanacak bant genişiliği politikası belirlenir. (Policy-map)
(örnek: kullanıcılar maksimum 10Mb kullanabilsin.)

3- Bu politika ilgili interface'e giren veya çıkan trafiğe uygulanır.

Per-interface Aggregate Policing

Erişim Kontrol Listeleri ile Trafiğin Tarifi

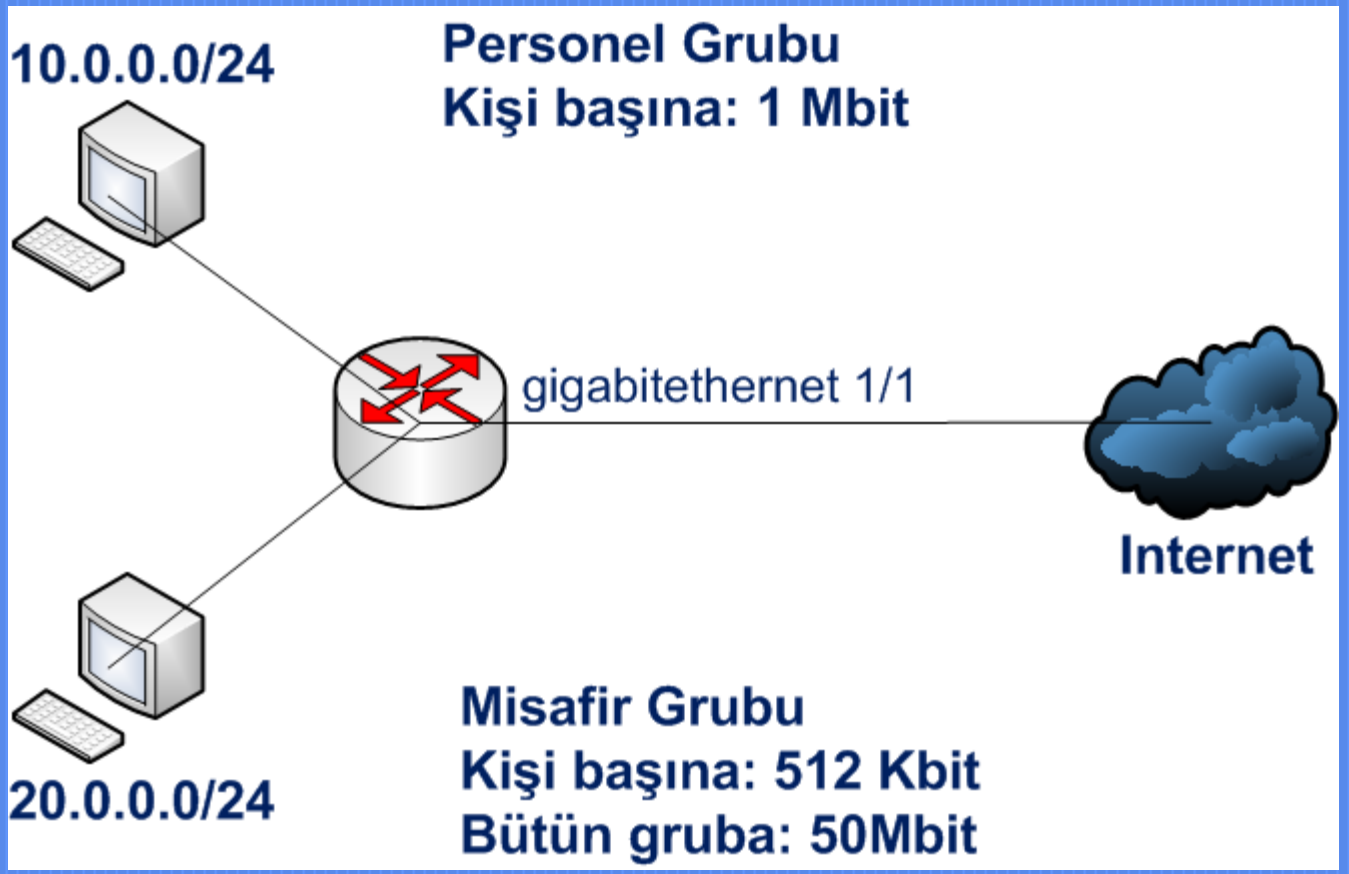
```
6500(config)#mls qos
6500(config)#access-list 160 permit ip any 10.0.0.0
    0.0.0.255

6500(config)#class-map 60Mb_Sinifi
6500(config-cmap)#match access-group 160
6500(config-cmap)#exit
```

Politikanın Belirlenmesi ve Uygulanması

```
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)# interface gigabit 2/1
6500(config-if)# service-policy input 60Mb_toplam
```

Not: L3 Interface'ine giren ve çıkan trafiğe (Input ve Output) uygulanabilir.

Microflow Policing



Erişim Kontrol Listeleri ile Trafiğin Tarifi

6500(config)# access-list 101 permit ip any 10.0.0.0 0.0.0.255

```
! Personel sınıfının tanımlanması
6500(config)# class-map personel_sinifi
6500(config-cmap)# match access-group 101
6500(config-cmap)# exit
```

Erişim Kontrol Listeleri ile Trafiğin Tarifi - 2

6500(config)# access-list 102 permit ip any 20.0.0.0 0.0.0.255

```
! Misafir sınıfının tanımlanması
6500(config)# class-map misafir_sinifi
6500(config-cmap)# match access-group 102
6500(config-cmap)# exit
```

Politikanın Belirlenmesi ve Uygulanması

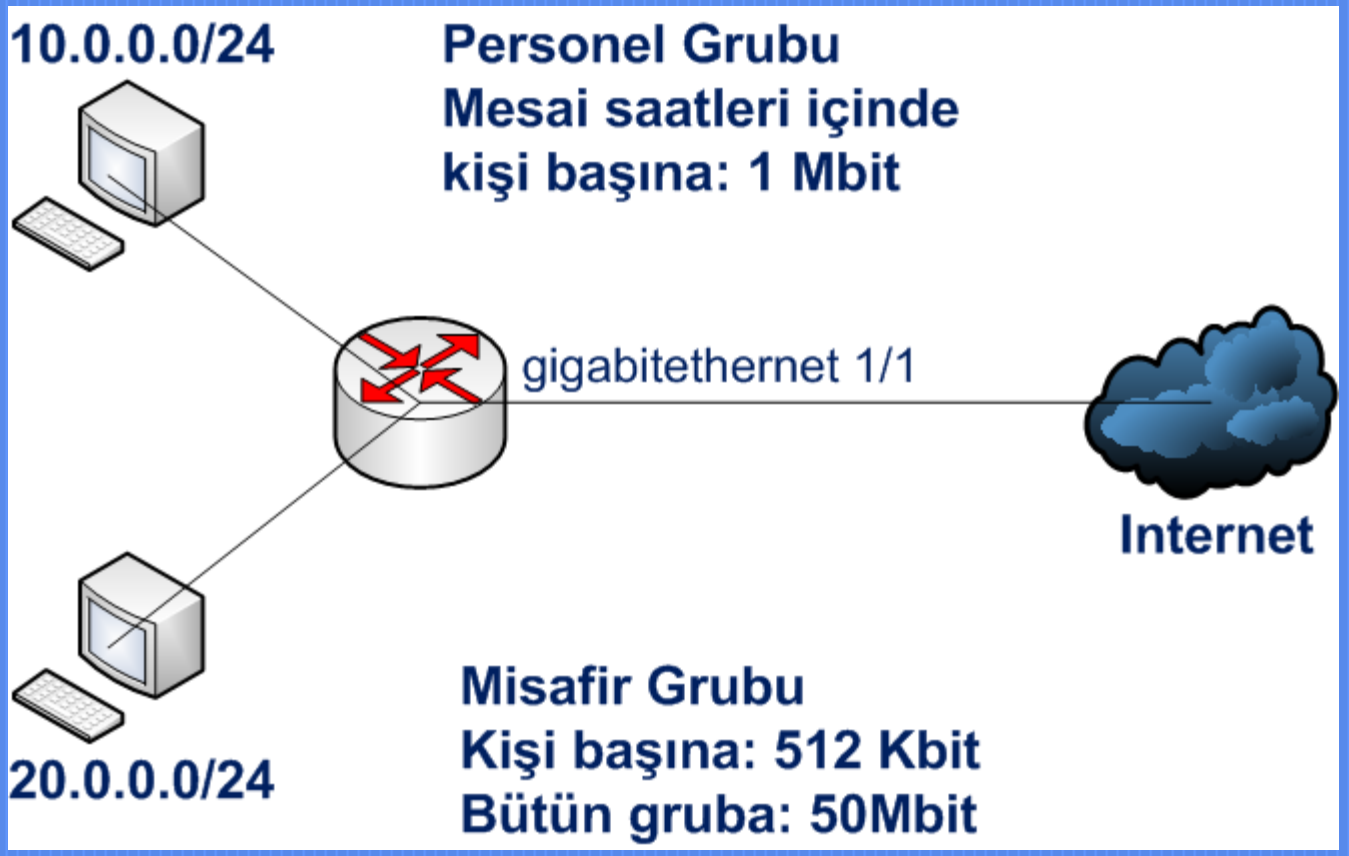
```
6500(config)# policy-map Personel_Misafir_sinirla
6500(config-pmap)# class personel_sinifi
6500(config-pmap-c)# police flow mask dest-only 1024000
256000 conform-action transmit exceed-action drop
6500(config-pmap-c)# exit

6500(config-pmap)# class misafir_sinifi
6500(config-pmap-c)# police flow mask dest-only 512000
128000 conform-action transmit exceed-action drop
6500(config-pmap-c)# police 50000000
6500(config-pmap-c)# exit
```

Politikanın Belirlenmesi ve Uygulanması

6500(config)# interface gigabitEthernet 1/1
6500(config-if)# service-policy input Personel_Misafir_sinirla

Not: Sadece interface'e giren trafiğe (input) uygulanabilir.

Zamana Bağlı Bant Genişliği Yönetimi



Zaman Aralığı Belirtilmesi

1- Periyodik tekrar eden zaman aralığı tarifi:

Router(config)# time-range time_range_name
Router(config-time)# periodic [istenen günler] [hh:mm] to [hh:mm]
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday ,
Sunday, Daily (hergün), Weekdays (haftaiçi), Weekend (hafta sonu)

2- Sadece belirli tarih için:

Router(config)# time-range time_range_name
Router(config-time)# absolute [Başlangıç saat-dakika-saniye-gün-ay-yıl] [bitiş saat-dakika-saniye-gün- ay-yıl]

Erişim kural listesine zaman aralığının tanımlanması

Mesai saatleri aralığının tarifi:

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

Router(config)# access-list 101 permit ip any 10.0.0.0 0.0.0.255 time-range mesai
```

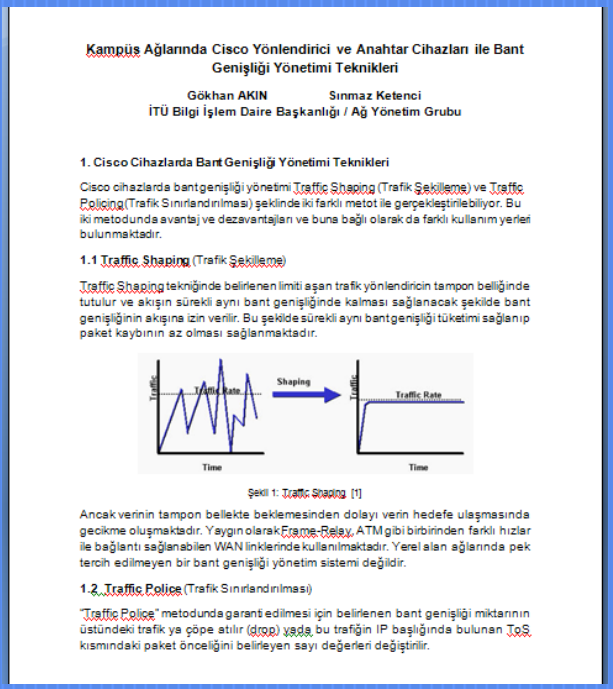
Uygulamanın Belirtilmesi

1- Port numarası belirterek:
Router(config)# access-list 101 permit tcp 10.0.0.0 0.0.0.255 eq 80 any time-range mesai

2- Protokol analizi yaparak: Yönlendiricilerde NBAR özelliği ile gerçekleştirilebilir.
Router(config)# class-map match-any WEB_TRAFIGI
Router (config-cmap)#match protocol http

Detay : P2P Engellemek için QoS ile Cisco NBAR Kullanılması
http://www2.itu.edu.tr/~akingok/etkinlikler.php
(Akademik Bilişim 2006)

Sorular



Kampüs Ağlarında Cisco Yönlendirici ve Anahtar Cihazları ile Bant Genişliği Yönetimi Teknikleri

Gökhan AKIN Sınmaz Ketenci
İTÜ Bilgi İşlem Daire Başkanlığı / Ağ Yönetim Grubu

1. Cisco Cihazlarda Bant Genişliği Yönetimi Teknikleri

Cisco cihazlarda bant genişliği yönetimi Traffic Shaping (Trafik Şekilleme) ve Traffic Policing (Trafik Sınırlandırılması) şeklinde iki farklı metot ile gerçekleştirilebiliyor. Bu iki metodunda avantaj ve dezavantajları ve buna bağlı olarak da farklı kullanım yerleri bulunmaktadır.

1.1 Traffic Shaping (Trafik Şekilleme)

Traffic Shaping tekniğinde belirlenen limiti aşan trafik yönlendiricin tampon belliğinde tutulur ve akışın sürekli aynı bant genişliğinde kalması sağlanacak şekilde bant genişliğinin akışına izin verilir. Bu şekilde sürekli aynı bant genişliği tüketimi sağlanıp paket kaybının az olması sağlanmaktadır.

Şekil 1: Traffic Shaping [1]

Ancak verinin tampon bellekte beklemesinden dolayı verin hedefe ulaşmasında gecikme oluşmaktadır. Yaygın olarak Frame-Relay, ATM gibi birbirinden farklı hızlar ile bağlantı sağlanabilen WAN linklerinde kullanılmaktadır. Yerel alan ağlarında pek tercih edilmeyen bir bant genişliği yönetim sistemi değildir.

1.2 Traffic Police (Trafik Sınırlandırılması)

"Traffic Police" metodunda garanti edilmesi için belirlenen bant genişliği miktarının üstündeki trafik ya çöpe atılır (drop) yada bu trafiğin IP başlığında bulunan ToS kısmındaki paket önceliğini belirleyen sayı değerleri değiştirilir.

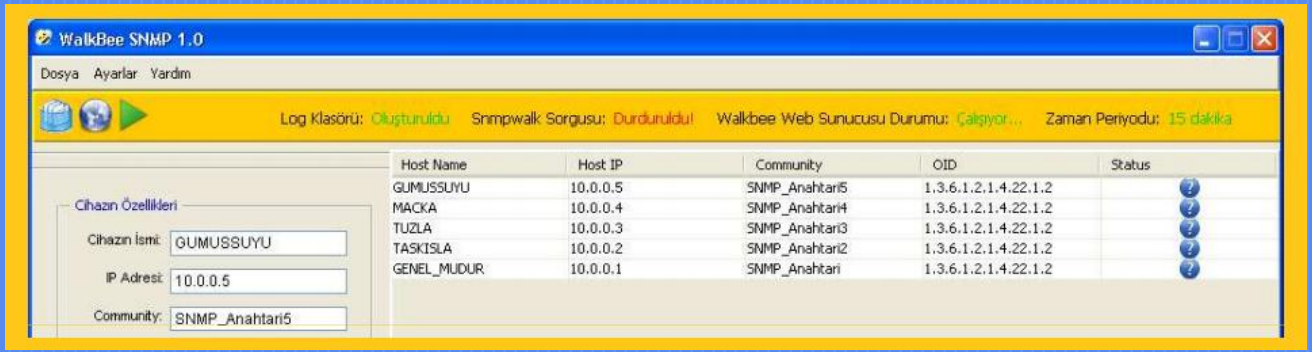
Teşekkürler.

Dökümanlar için:

http://web.itu.edu.tr/akingok

(http://www.gokhanakin.net)

http://csirt.ulakbim.gov.tr/dokumanlar



http://www.walkbee.net