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

Gökhan AKIN **Sınmaz Ketenci**

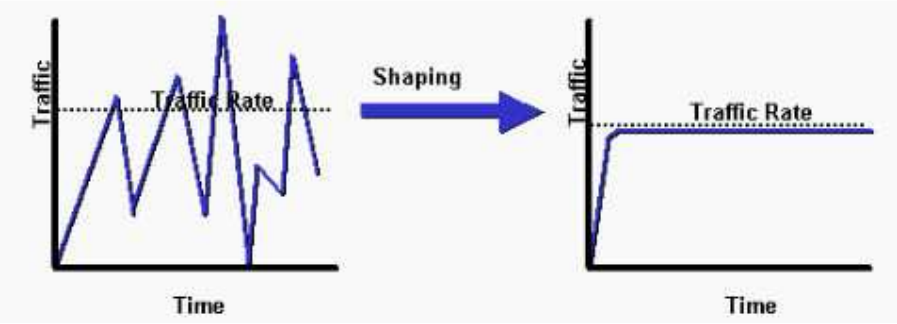
İTÜ Bilgi İşlem Daire Başkanlığı / Ağ Yönetim Grubu

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 gerçekleştirilebilmektedir. Bu iki metodun da 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 sürekli aynı bant genişliğinde kalması sağlanacak şekilde bant genişliğinin akışına izin verilir. Bantgenişliği tüketiminin sabitlenmesinin yanu sıra paket kaybının az olması da sağlanmaktadır.

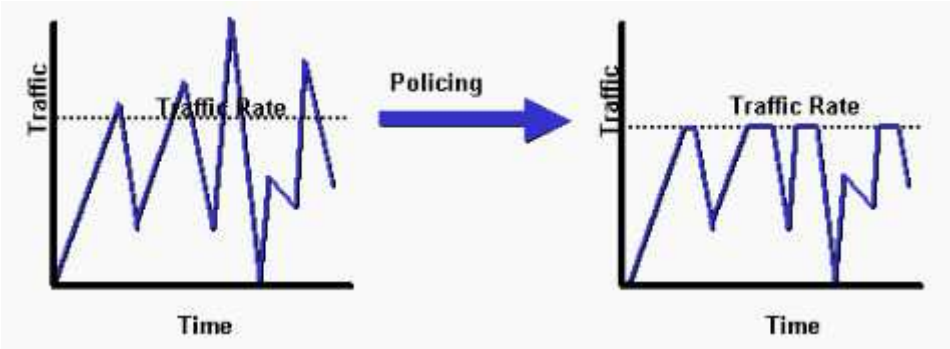


Şekil 1: Traffic Shaping [1]

Ancak 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 linklerinde kullanılmaktadır. Yerel alan ağlarında pek tercih edilen bir bant genişliği yönetim sistemi değildir.

1.2 Traffic Policing(Trafik Sınırlandırılması)

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



Şekil 2 : Traffic Policing [1]

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.

Cisco cihazlarda genel olarak iki farklı “Police” tekniği vardır.

1- Aggregate Policing: VLAN veya fiziksel arayüze uygulanabilen bir tekniktir. Bu teknikte o arayüze bağlı kullanıcılar için bir üst sınır belirlenebilir. Bütün kullanıcılar yerine erişim kontrol listeleri(ACL) kullanılarak o arayüzdeki bazı kaynak veya hedef IP’lere ulaşmak için kullanılabilecek bant genişliği aralığı belirlenebilir.
2- Microflow policing: Bu teknikte bir arayüzden geçen bütün trafiğe değil de o arayüzden akan tek bir trafik akışına (flow) bant genişliği sınırlaması uygulanabilir. Microflow olarak adlandırılan bu teknikteki flow ibaresi kaynak IP, hedef IP, 4.katman protokolu, kaynak ve hedef port numarası gibi önceden referans alınmak üzere konfigurasyonda belirlenmiş parametrelere göre ayrılabilen trafiğe denir.

Aggregate policer arayüzlere giriş ve çıkış yönünde uygulanabilirken microflow policer sadece giriş yönünde uygulanabilir.

2. Traffic Police Tekniğinin Kullanımı

2.1 Aggregate Police Tekniği

Bu tekniğin kullanımına örnek vermek gerekirse; 30 Mb limitleme ile tanımlamış bir “aggregate policer”, uygulandığı vlan’deki tüm portların toplam trafiği için 30 Mb’lik bir üst sınır uygulamış olacaktır. Bu teknikte 30Mb’lik bant genişliğinin kullanıcılar arasında adil dağılma garantisi yoktur. Tek bir kullanıcı bu 30Mb’lik kaynağı tüketip diğer kullanıcıların hizmet alma olanağını ortadan kaldırabilir.

Bu teknik günümüz kenar ikinci katman anahtarlama cihazlarında da uygulanabilmektedir. Bu sayede bir sunucuya erişilebilecek maksimum hız da belirlenebilir.

2.1.1 Cisco 2950 Kenar Anahtarlarda Konfigürasyon

Catalyst 2950 anahtarlarda bu teknik sayesinde class-map'ler ile eşleşen tüm trafiğin kullanabileceği toplam bant genişliği belirlenebilir. Gigabit arayüzlere uygulanacak policy-map)'lerde bant genişliği sınırlaması 8Mbit ve katları şeklinde, Fast Ethernet arayüzlerde ise 1Mb ve katları şeklinde tanımlanmalıdır. Bu teknik fiziksel arayüzlerde sadece giriş yönünde uygulanabilir. Sırası ile uygulanması gereken adımlar şu şekildedir.

1. Öncelikle class-map'lerde kullanılacak erişim kontrol listeleri (ACL'ler) tanımlanmalıdır.

```
Sw_2950(config)# access-list 101 permit ip any 10.1.1.0 0.0.0.255
Sw_2950(config)# access-list 112 permit ip any 10.1.12.0 0.0.0.255
```

2. Sonraki adımda farklı gruplar için class-map tanımlanmalıdır.

```
Sw_2950(config)# class-map misafir_sınıfı
Sw_2950(config-cmap)# match access-group 101
Sw_2950(config-cmap)# exit

Sw_2950(config)# class-map idari_sınıfı
Sw_2950(config-cmap)# match access-group 112
Sw_2950(config-cmap)# exit
```

3. Bir sonraki adımda policy-map oluşturulur ve her class-map için uygulanacak bant genişliği değerleri belirtilir. "police" sonrasında belirtilen ilk değer bit cinsinden uygulanan bant genişliği sınırlamasını belirtir. Burst diye isimlendirilen ikinci değer ise bant genişliği sınırlandırması yapılmadan iletilebilecek trafiğin byte cinsinden miktarıdır.

```
Sw_2950(config)# policy-map Misafir_Idari
Sw_2950(config-pmap)# class misafir_sinifi
Sw_2950(config-pmap-c)# police 8000000 16384 exceed-action drop
Sw_2950(config-pmap-c)# exit
Sw_2950(config-pmap)# class idari_sinifi
Sw_2950(config-pmap-c)# police 32000000 32768 exceed-action drop
```

4. Policy-map'in anahtarın arayüzüne giriş yönünde uygulanması ile 10.1.1.0/24 ve 10.1.12.0/24 ağlarındaki kullanıcılara iletilecek toplam trafik 8Mb ve 32Mb ile sınırlandırılmış olacaktır.

```
Sw_2950 (config)# interface gigabitEthernet 0/1
Sw_2950 (config-if)# service-policy input Misafir_Idari
```

2.1.2 Cisco 2960 Kenar Anahtarlarda Konfigürasyon

Catalyst 2960 anahtarlarda yukarıda belirtilen komutlar ile bant genişliği kontrolü yapılabilir. 2950 anahtarlardan farklı olarak sadece “mls qos” komutu ile anahtar üzerinde QoS aktif hale getirilmelidir. Tüm arayüzlere uygulanacak policy-map’lerde bant genişliği sınırlaması 1Mb ve katları şeklinde tanımlanmalıdır.

Ayrıca farklı olarak aggregate policer (ortak sınırlandırıcı) tanımlanıp bir policy-map’deki class-map (sınıf haritalar) tarafından bu sınırlandırıcıyı ortak olarak kullanmaları sağlanabilir. Aggregate policer aşağıdaki gibi yapılandırılabilir.

1. QoS switch'te aktive edilir.
   Sw_2960(config)# mls qos

2. Aggregate policer tanımlanır.
   Sw_2960(config)# mls qos aggregate-policer ortak_8Mb 8000000 16000 exceed-action drop

3. Policy-map’de kullanılan class-map’ler için aggregate policer kullanılır.
   Sw_2960(config)# policy-map Misafir_Idari
   Sw_2960(config-pmap)# class misafir_sinifi
   Sw_2960(config-pmap-c)# police aggregate ortak_8Mb
   Sw_2960(config-pmap-c)# exit

   Sw_2960(config-pmap)# class idari_sinifi
   Sw_2960(config-pmap-c)# police aggregate ortak_8Mb
   Sw_2960(config-pmap-c)# exit

4. Policy-map’in anahtarın arayüzüne giriş yönünde uygulanması ile 10.1.1.0/24 ve 10.1.12.0/24 ağlarındaki kullanıcılara iletilecek toplam trafik 8Mb ile sınırlandırılmış olacaktır.

   Sw_2960 (config)# interface gigabitEthernet 0/1
   Sw_2960 (config-if)# service-policy input Misafir_Idari

2.1.3 Cisco Yönlendiriciler ve 6500 Serisi Anahtarlama Cihazlarında Konfigurasyon [2]

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 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
```

Not: Bu konfigurasyon ile tanımlanan class-map ile eşleşen trafik için Gigabit 2/1 ve Gigabit 2/2 interface'lerine girebilecek bant genişliği toplam 10Mb ile sınırlandırılmıştır.

2.2 Microflow Policy Tekniği:

Bu teknik ile örnek olarak bir arayüzden erişim sağlayan bütün IP adresleri için ayrı ayrı bant genişliği yönetimi yapılabilir. Örneğin her kullanıcı aynı anda maksimum 1024Kbit erişim yapabilir diye bir sınırlama konabilir. Bu sayede tek bir kullanıcının bütün bantgenişliğini kullanması engellenmiş olur. Ayrıca aynı arayüzde farklı kullanıcı profillerine göre tanımlanmış class-map ile farklı bant genişliği değerlerinin belirlenmesi de mümkün olmaktadır.

Microflow policy'de akış (flow) tanımlanması aşamasında sadece kaynak IP adresi(src-only), sadece hedef IP adresi(dest-only) ya da kaynak ve hedef IP ile birlikte kaynak ve hedef port numaraları(full-flow) seçilebilir. Eğer kullanıcı bazlı bir bant genişliği sınırlandırılması isteniyorsa src-only ya da dest-only seçeneği kullanılmalıdır. Full-flow seçilmesi durumunda bir kullanıcının kurduğu her bağlantı ayrı bir flow olarak tanımlanacağından herhangi bir kullanıcının kullanabileceği bant genişliği üst sınırını tanımlama imkanı olmaz. Bu şekilde sadece tek bir session(oturum) için sınırlandırma konulmuş olur.

Bunların yanı sıra istenirse aggregate ve microflow policy aynı anda kullanılabilir. Örnek olarak misafirlere kullanıcı bazında 512 Kb'lik sınırlandırma yapılmasının yanı sıra bütün misafirlerin toplamda da 50Mb'lik bant genişliğini aşmaları engellenebilir.

2.2.1 Microflow Policing Konfigürasyonu:

Bu teknik şu anda sadece supervisor 720'ye sahip Cisco 6500/7600 serisi cihazlarda uygulanabilmektedir. Öncelikle trafik tiplerinin gruplanması için kullanılacak class-map'ler oluşturulur. Class-Map'lerde trafiğin tanımlanması için erişim kontrol listeleri(ACL) kullanılır. Policy-map'ler ile farklı class-map'ler için farklı bant genişliği sınırlandırılması yapılabilir. Aşağıda örnek yapılandırma açıklamaları ile verilmiştir.

1. Farklı class-map'lerde kullanılacak erişim kontrol listeleri tanımlanır.
   Router(config)# access-list 101 permit ip any 10.0.0.0 0.0.0.255
   Router(config)# access-list 102 permit ip any 20.0.0.0 0.0.0.255

2. Class-map'ler tanımlanmalıdır.
   ! Personel sınıfının tanımlanması
   6500(config)# class-map personel_sinifi

```
6500(config-cmap)# match access-group 101
6500(config-cmap)# exit

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

3. Bu adımda policy-map oluşturulup cihazın uygun arayüzüne uygulanmalıdır. Policy-map ile her class-map 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(burst bytes).

```
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
exit
```

4. Son adımda policy-map’in cihazın dış ağa bakan interface’ine giriş yönünde uygulanması ile kullanıcıların dış ağdan indirebilecekleri trafiğe 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 ve bütün misafirlerin toplam trafiği de 50Mb ile kısıtlanmıştır.

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

3. Zamana Bağlı Bant Genişliği Yönetimi

Class-map’lerde trafiğin tanımlanması için erişim kontrol listeleri(ACL) kullanılması, yapılacak sınırlandırmanın zaman bazlı uygulanabilmesi seçeneğini de beraberinde getirmektedir. Bunun için öncelikle istenen zaman aralıkları tanımlanmalıdır.

Kesin bir tarih aralığı için kullanılacak konfigürasyon aşağıdaki gibidir.

```
Router(config)# time-range time_range_ismi
Router(config-time)# absolute start [Başlangıç saat-dakika-saniye-gün- ay-yıl] end
[bitiş saat-dakika-saniye-gün- ay-yıl]
```

Periyodik olarak tekrarlanması isteniyor ise konfigürasyon şu şekilde yapılmalıdır.

Router(config)# time-range time_range_ismi
Router(config-time)# periodic [istenen günler] [hh:mm] to [hh:mm]

Gün tanımı aşağıda sıralanmış İngilizce haftanın günlerinin belirtilmesi ile gerçekleştirilebilir.

- monday
- tuesday
- wednesday
- thursday
- friday
- saturday
- sunday
- daily (hergün)
- weekdays (Pazartesiden Cumaya)
- weekend (hafta sonu)

Aşağıdaki şekilde zaman aralığı tanımlanır. Bu zaman aralığı erişim kontrol listesine eklenmesi ile hafta içi saat 9 ile 18 saatleri arasında istenen bant genişliği kurallarının uygulanması sağlanabilmektedir.

```
!Zaman aralığının tanımlanması:
Router(config)# time-range mesai
Router(config-time-range)# periodic weekdays 09:00 to 18:00
Router(config-time-range)# exit
!Erişim kontrol listesinde zaman aralığının uygulanması:
Router(config)# access-list 101 permit ip any 10.0.1.0 0.0.0.255 time-range
mesai
```

4. Sonuç

Cisco yönlendiricilerde, ikinci katman kenar anahtarlarda ve üçüncü katman anahtarlarda Traffic Policing(Trafik Sınırlandırılması) konfigürasyonu ile bant genişliği yönetimi yapılabilmektedir. Aggregate policing ile bir grup bilgisayarın toplam kullanabilecekleri bant genişliği üst sınırı belirlenebilmektedir. Microflow policing ise IP bazında kullanıcıların maksimum indirebilecekleri (download) ve yollayabilecekleri (upload) trafik kontrol altına alınmasında kullanılabilir. Bu teknik ile adil bir şekilde bant genişliği yönetimini sağlanabilir.

5. Kaynaklar

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

[2] QoS Policing on Catalyst 6500/6000 Series Switches, http://www.cisco.com/en/US/products/hw/switches/ps700/products_tech_note09186a00801c8c4b.shtml, Cisco Corp.

[3] P2P Trafiği Tespiti için Cisco NBAR Kullanımı, P2P Trafiği Tespiti için Cisco NBAR Kullanımı, Gökhan AKIN, Akademik Bilişim 2006