QoS (Quality of Service)

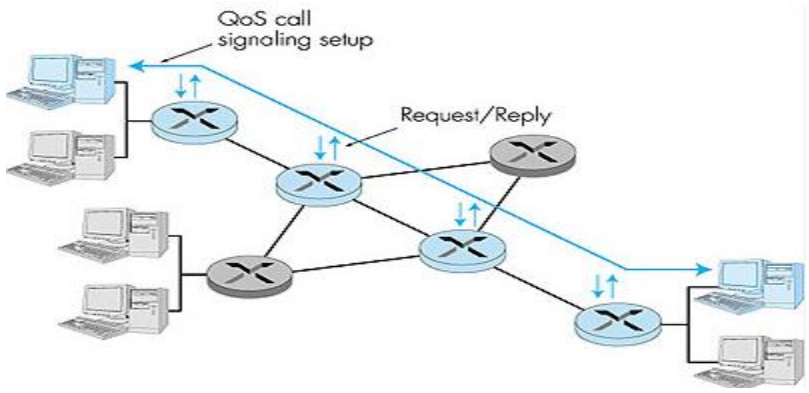
Network haberleşmesinin kalitesini belirleyen unsurlardan biri bant genişliğidir. Bant genişliği sınırlı olan networkler için paket kayıpları, gecikmeler ve Jitter oluşumu gibi sorunlar görülmektedir. Bu sorunlar;

- Packet Loss, networkte sahip olunan bant genişliğinden/ karşılanabilecek paket miktarından daha fazla tragik gönderildiğinde fazlalık trafiğin drop edilmesidir. Bu durumda drop edilen paketlerin tekrar gönderilmesi gerekecek ve internet yavaşlayacaktır.
- Latency, gerçek zamanlı hizmetlerde yaşanan gecikme miktarı olarak tanımlanabilir (Ses haberleşmsinde bu değerin 150 ms'yi geçmemesi istenir). Latency sebeplerine bakıldığında;
    - **Propagation Delay**, verinin kablo üzerinde iletilirken geçirdiği/kaybettiği süredir (Bu süreler çok küçük ve sabit değerlerdir. Örnek olarak bir fiber optic kablo için iletim ışık hızına yakın gerçekleşiyor. İletim mesafesi iki katına çıktığında gecikme süresi de iki katına çıkacaktır).
    - **Serialization Delay**, trafiğin bir network cihazlarına girişi ve çıkışı arasında geçirdiği süredir. Bu gecikme süresi de sabittir (cihadan cihaza farklılık göstermez).
    - **Processing Delay**, Intermediate Device Delay olarak da bilinir. Paketlerin network cihazlarında geçirdiği işlem süresi (Bu süreyi etkileyen parametrelere örnek olarak switchlerde kullanılan anahtarlama teknikleri, Anahtarlama işlemi CPU ile mi yapılıyor ASIC kullanılarak mı yapılıyor gibi durumlar verilebilir).
    - **Delay Variation**, paketlerin gecikme değişimidir (Jitter - Örnek olarak paketler network cihazının Buffer'ında bekletilmesinden kaynaklanabiliyor. Her paket farrklı aralıklarda bekletildiğinde oluşabiliyor).
- Jitter, Latency süresindeki değişim olarak tanımlanabilir (Latency-Jitter arasındaki bağlantı, Hız-Ivme arasındaki bağlantıya benzetilebilir. Delay süresindeki değişimin (yani Jitter) yüksek olması istenmeyen bir durumdur. Ses iletiminde değerin 30ms'yi geçmemesi istenir).

Quality of Service, network üzerinde önem seviyesi daha yüksek olan trafiğe öncelik verilmesini sağlayan teknoloji olarak tanımlanabilir. QoS'a daha çok sınırlı bant genişliğine sahip olunduğunda başvurulduğunu söyleyebliriz. Sınırlı bant genişliği beraberinde paket kayıplarını, gecikme ve Jitter gibi sorunlara neden olacaktır. Networklerde kritik görülen servislerin bu gibi durumlardan etkilenmemesini/aksamamasını için QoS teknolojisi kullanılmaktadır. QoS teknolojisinde ise trafiklere öncelik vermek için birkaç meknizma bulunmaktadır. Bunlara bakıldığında;

- **Best Effort**, QoS mekanizmasının kullanılmadığı (network trafiğinin kendi haline bırakıldığı) modeldir.
- **Integrated Services (IntServ)**, öncelik verilecek trafik için ulaştığı ilk routerdan ihtibaren RSVP (The Resource Reservation Protocol) paketleriyle routerlar arasında haberleşerek trafiğin güzargah boyunca aksamadan iletilebilmesi için belirlenen rota üzerinde bir bant genişliği tahsis edilmesini sağlayan mekanizmadır (Önceliklendirilen trafik için ayrıca bir akış tablosu oluşturuluyor). Bu bant genişliği önceliklendirilen/rezerve edilen trafik akışı olmadığı zamanlarda

boşta bekler (farklı trafikler için kullanılamaz). Yönetiminin zor olması, rezerve edildiği network trafiği dışında kullanılamaması gibi nedenlerden dolayı bu mekanizma tercih edilmemektedir.



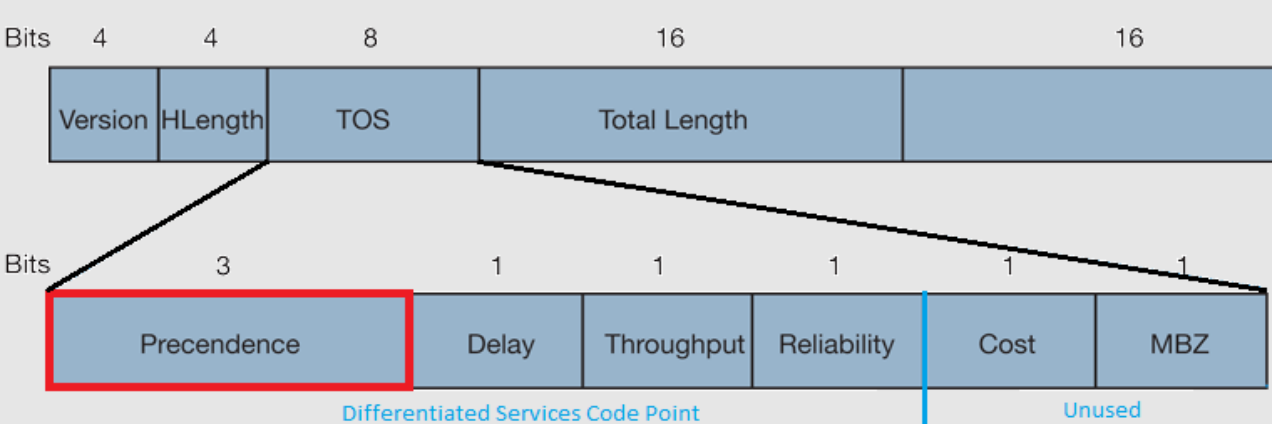
- **Differantiated Services (DiffServ)**, Önceliklendirilmek istenen trafiği işaretleyip (Marking) sınıflandırarak (Classification) iletilmesini sağlayan mekanizmadır. Bu mekanizmada trafik geçerken önceliklendirme mekanizması devreye girdiği için (ayrıca bant genişliği rezerve edilmediği için) Integrated Services modeline kıyasla daha etkili çalışmaktadır ve daha yaygın kullanılmaktadır.
  Network katmanlarında gerçekleştirilebilecek sınıflandırma ve önceliklendirme seçeneklerine bakıldığında;
  - L1, fiziksel arayüzlerden, SubInterface'lerden veya portlardan gelen paketler önceliklendirilebiliyor.
  - L2, MAC adresine bakılarak veya **802.1q-VLAN etiketi/CoS** (Class of Service) alanı kullanılarak paketler önceliklendirilebiliyor.
  - L2.5, **EXP** (MPLS Experimental) bitleri kullanılarak paketler önceliklendirilebiliyor.
  - L3, **DSCP** (Differantiated Services Code Points) veya **IPP** (IP Predence) teknikleriyle bu alana numaralar verip ip başlığındaki **ToS** (Type of Services) alanı kullanılarak veya Hedef/Kaynak ip adresleirne göre paketler önceliklendirilebiliyor.
  - L4, port numaralarına göre paketler önceliklendirilebiliyor.
  - L7, NGFW kullanılarak **NBAR2** (Next Generation Network-Based Application Recognization) gibi mekanizmalarla paketler önceliklendirilebiliyor.

L2 Making İşlemi

L2'de atiketleme işlemi için VLAN etiketi (802.1q) içerisinde 3 bitlik uzunluğundaki CoS/**PCP** (Priority Code Point) alanı kullanılıyordu. Boyutundan da anlaşılabileceği gibi bu alana toplamda 8 farklı değer girilebiliyor (0-> en az öncelikli trafik, 7-> en yüksek öncelikli trafik için kullanılıyor. Genelde, 6 ve 7 kullanılmazken ip telefon trafiği için 5 değeri kulanılır). Bu değerler/işaretleme sayesinde paketlerin hangi öncelik sınıfına dahil olduğu anlaşılıyor ve paketler önceliklendiriliyor.

IP Precedence Decimal	IP Precedence Binary	IP Precedence Name
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-Override
5	101	Critical
6	110	Internetwork Control
7	111	Network Control

L2'de paketlere uygulanan önceliklendirme işlemi paketin karşılaştığı ilk L3 cihazda (router gibi) geçerliliğini kaybedecektir. Bu önceliğin L3 cihazlarda da geçerliliğini sağlamak için L2'de tanımlanan 3 bitlik CoS değerinin ToS (IP Precedence alanına) özelliğine aktarılması sağlanabiliyor. Bu sayede paketin aynı öncelik değeriyle yönlendirilmeye devam etmesi sağlanabiliyor.



|→ Uzun yıllar boyunca ToS alanında saadece 3 bitlik kısım kullanılmıştır (Ip Precedence). Zamanla 3 bitlik alan yeterli gelmediği için 6 bitlik alan kullanılmaya başlanmıştır (Differentiated Services Code Point).

DSCP Per-Hop Behaviour

DSCP mekanizmasında kullanılan 6 bite bakılarak paket değerlendiriliyor. Bu bitlerin anlamlarına bakıldığında;

- **CS (Class Selector)** PHB, ToS alanının sadece son 3 biti kullanılıyorsa (Ip Precedence alanı) bu durumda verilen sınıf numaralarına verilen isimdir (CS0 – CS1 - … - CS7).
  |→ Ek olarak net nalaılması için eklenmiştir; CS yapısı kullanıırken CS tanımıToS alanının son 3 bitine (5,6,7) tanımlanıyor.
- **DF (Defaut Forwarding)** PHB, DSCP mekanizmasında kullanılan 6 bitin de 0 olma durumuna verilen isimdir (DF – CS0 ile aynı durumdur).
- **AF (Assured Forwarding)** PHB, DSCP mekanizmasında kullanılan 6 bitin son 3 bitiyle öncelik durumu belirtilirken ilk 3 bitiyle (*Sadece 2 biti kullanılıyor. Bitlerden biri sürekli sıfır. Aşağıdaki görselde DSCP(bin) kısmındaki son bitlerde görebilirsin*) ikinci bir öncelik durumu daha

belirtiliyor. Bunu bir tür öncelik verme aralığını genişletmek olarak da görebiliriz (AF1 – AF2 – AF3 – AF4). AF değerlerine ek olarak 2 bitlik Drop Probability değerleri de eklenmiştir. **Drop Probability** isminden de anlaşılacağı gibi paketin drop edilme önceliğini belirtmek için kullanılıyor (Paketlerin drop edilmesi gereken durumlarda hangi paketlerin daha öncelikli olduğunu belirlemek için kullanılıyor. Drop Probability değeri büyüdükçe paketin geçiş önceliği azalıyor, drop edilme önceliği yükseliyor). Özetle her AF değeri için 3 farklı 1 değeri bulunuyor. Yani toplamda 12 farklı AF değeri bulunuyor (AF11 en öncelikli ve drop edilme ihtimali en düşük, AF43 en önceliksiz ve drop edilme ihtimali en öncelikli paketler için kullanılıyor).
|→ Ek olarak net nalaılması için eklenmiştir; AF yapısı kullanıırken AF tanımı ToS alanının son 3 bitine (5,6,7), Drop Probability değerleri 2,3,4. bitlerine tanımlanıyor.

- **EF (Expedited Forwarding)** PHB, değeri 5 (**5-7**) ve üstü olan değerlerir. En öncelikli grup olarak değerlendiriliyor ve ciazlarda geçiş üstünlüğünü her zaman bu gruba dahil paketlere verilir (Drop Probability değeri sabittir).

DSCP Class	DSCP (bin)	DSCP (hex)	DSCP (dec)	ToS (dec)	ToS (hex)	ToS (bin)	ToS Prec. (bin)	ToS Prec. (dec)	ToS Delay	ToS Throug	ToS Reliat	TOS String Format
cs0	000000	0x00	0	0	0x00	00000000	000	0	0	0	0	Routine
cs1	001000	0x08	8	32	0x20	00100000	001	1	0	0	0	Priority
af11	001010	0x0a	10	40	0x28	00101000	001	1	0	1	0	Priority
af12	001100	0x0c	12	48	0x30	00110000	001	1	1	0	0	Priority
af13	001110	0x0e	14	56	0x38	00111000	001	1	1	1	0	Priority
cs2	010000	0x10	16	64	0x40	01000000	010	2	0	0	0	Immediate
af21	010010	0x12	18	72	0x48	01001000	010	2	0	1	0	Immediate
af22	010100	0x14	20	80	0x50	01010000	010	2	1	0	0	Immediate
af23	010110	0x16	22	88	0x58	01011000	010	2	1	1	0	Immediate
cs3	011000	0x18	24	96	0x60	01100000	011	3	0	0	0	Flash
af31	011010	0x1a	26	104	0x68	01101000	011	3	0	1	0	Flash
af32	011100	0x1c	28	112	0x70	01110000	011	3	1	0	0	Flash
af33	011110	0x1e	30	120	0x78	01111000	011	3	1	1	0	Flash
cs4	100000	0x20	32	128	0x80	10000000	100	4	0	0	0	FlashOverride
af41	100010	0x22	34	136	0x88	10001000	100	4	0	1	0	FlashOverride
af42	100100	0x24	36	144	0x90	10010000	100	4	1	0	0	FlashOverride
af43	100110	0x26	38	152	0x98	10011000	100	4	1	1	0	FlashOverride
cs5	101000	0x28	40	160	0xa0	10100000	101	5	0	0	0	Critical
ef	101110	0x2e	46	184	0xb8	10111000	101	5	1	1	0	Critical
cs6	110000	0x30	48	192	0xc0	11000000	110	6	0	0	0	Internetwork Control
cs7	111000	0x38	56	224	0xe0	11100000	111	7	0	0	0	Network Control

Assure Forwarding and WRED

AF değerlerinne bakıldığında bir mekanizmanın bu değerlere bakarak önceliklerini değerlendirdiğini anlayabiliriz. Bu işlem **WRED** (Weighted Random Early Detection) ve **CBWFQ** (Class-Based Weighted Fair Queueing) teknikleriyle sağlanıyor.

|→ WRED tekniği, cihaz Buffer'ı dolmasına yakın paketlerin AF (Drop Probability) değerlerini kontrol ederek drop etmeye başlayan mekanizmadır (Yani Buffer'ın dolmasına yakın önlem olarak paketleri drop etmeye başlıyor).

|→ CBWFQ tekniği, birçok kuyruk/class oluşturulur ve ACL'ler kullanılarak bu kuyruklara eklenecek paket tipleri belirtilir. Oluşturulan kuyruklara ise belirli bant genişliği atanarak kuyruklara (önem seviyesine bağlı olarak) eklenen paketlere öncelik verilmesi sağlanır. Günümüzde yaygın kullanılan kuyruklama stratejisidir (**Kuyruklama stratejileri hakkında detaylı bilgi için CCNA - 3.07 – QoS notlarını inceleyebilirsin**).

Scavenger Class

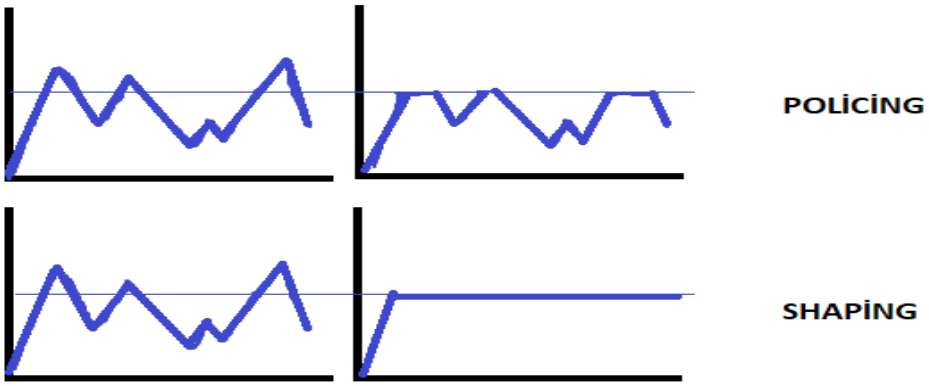
Network trafiğinde paketler öncelikli ve normal (önceliksiz) olarak sınıflandırılırken normal (önceliksiz) trafiklerden daha az önceliğe sahip oluması istenen trafikler için Scaveger Class oluşturulmuştur. Scavenger Class, P2P (Torrent …), oyun uygulamaları (Minecraft, Valorant, Fortnite …) veya eylence amaçlı kullanılan video uygulamaları (Youtube, Netflix …) gibi network trafikleri sınıflandırılarak önceliğini normal (önceliksiz) trafiğin de altında tanımlanabilmesi sağlanmıştır (*Scavenger Class trafikleri CS1 değeriyle işaretlenmektedir*).

Trust Boundary

Kullanıcıların paketlerine öncelik değerleri tanımlayarak networke bırakılmasının önüne geçmek için kullanılan bir özelliktir. Bu özellik sayesinde pakete hangi öncelik değeri tanımlanırsa tanımlansın port üzerinde trafik güvenli kabul edilmediği sürece öncelik verilmiyor (Varsayınalda Trust Boundary özelliği kapalı geliyor. Kullanılmak istendiğinde ayrıca devreye alınması gerekiyor).

Policing and Shaping

Network trafiğini sınırlandırma, engelleme gibi işlemlerde için Policing ve Shaping teknikleri kullanılıyor. **Policing**, sahip olunan/belirlenen bant genişliğinden daha yüksek boyutlarda trafik geldiğinde bu trafiğin doğrudan drop edilmesini sağlayan tekniktir. Günümüzde Shaping tekniğine kıyasla daha çok tercih edimlektedir. **Shaping**, sahip olunan/belirlenen bant genişliğinden daha yüksek bant genişliğinde trafik gönderildiğinde bu trafiği bir Buffer kullanarak depolanmasını ve zaman içerisinde (zaman dilimine yayarak) iletilmesini sağlayan tekniktir (paket kaybı olmuyor).



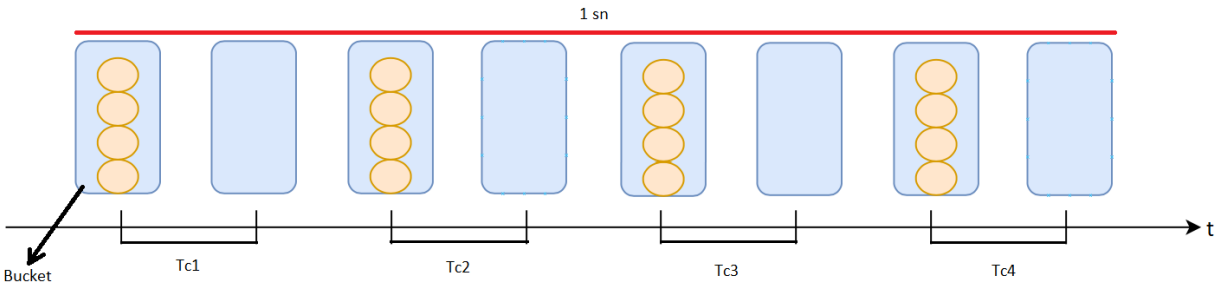
Token Bucket Algoithm

Network traiğini sınırlamak için kullanılan algoritmadır. Algoritmanın çalışma yöntemini açıklamadan önce bilinmesi gereken birkaç terime bakıldığında;

- CIR (Committed Information Rate), izin verilen network trafiğinde saniyede sağlanacak bant genişliğidir.

- Bc (Commited Brust size), algoritmada Bucket (kova) olarak tanımlanan kullanıcıya birim zamanda sağlanacak bant genişliği miktarınıdır.
- Tc (Commited Brust Size), kovanın ne kadar sürede bir yenileneceğini (birim zaman süresi) temsil eden semboldür (Periyot).
    - Bc = CIR x (Tc / 1000)
    - Tc = Bc / CIR
- Token, 1 bayttır (8 bittir). Bucket içerisine atılan Token (veriyi temsil ediyor) olarak tasfir ediliyor (Bucket dolduktan sonraki verilerin drop edilmesini temsil ediyor).

Token Bucket algoritması, bir saniyelik zaman birimini daha küçük zaman dilimlerine bölerek (Tc) çalışıyor. Her zaman diliminde veri iletimine izin verilen bir süre bulunuyor. Bu süre içerisinde Bucket (kova) adı verilen belirli bir bant genişliği sınırı konuluyor. Kullanıcı kendisine bant genişliğini kullanması için ayrılan zaman diliminde kendisine ayrılan bant genişliğinin tamamını kullandıktan sonra içerisinde olduğu zaman diliminin sonuna kadar trafiği doğrudan drop edilebilir, Buffer'a koyulabilir veya önceliklendirilebilir (yöneticinin kararına bağlı). Bir örnek üzerinden açıklamak gerekirse;

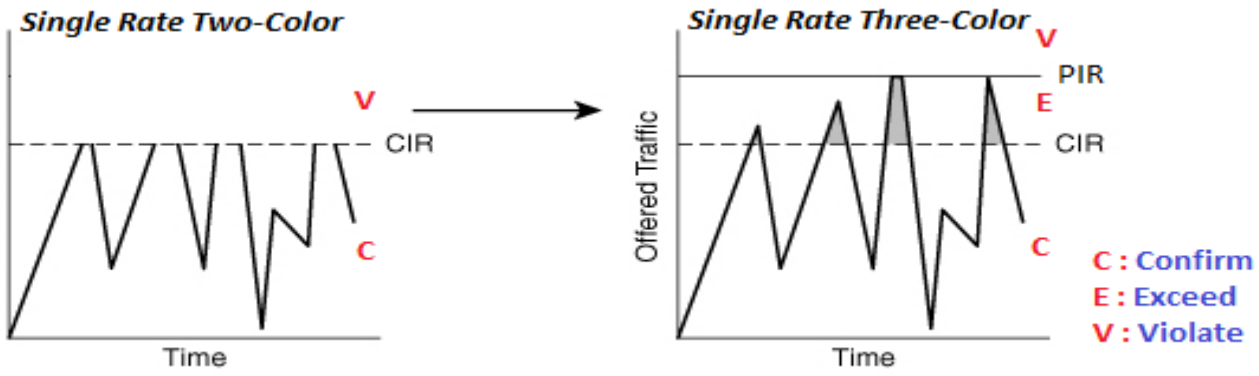


|→Örnek olarak 128 Kbps bant genişliğine sahip olan bir kurumun bant genişliği 64 Kbps ile sınırlandırılmak istendiğinde; Yukarıdaki görsel için 1 saniye 4 periyoda bölünmüş (Tc = Bc / CIR ➔ 16000 / 64000 =0.25 (her periyot 250ms)). Bu durumda 64 Kbit bant genişliği sağlayabilmek için her periyotta 16 Kbitlik Bucket (kovalar) kullanılır (64000/4 = 16000 bit). Her periyotta sadece 125 ms boyunca 16 Kbitlik trafik oluşturulabilirken, sonraki 125 ms'de gelen trafiğin tamamı drop ediliyor. Bu sayede bant genişliği istenen değerlerde sınırlandırılabiliyor.

|→ 1 saniyeyi alt periyotlara bölerek kullanıcıya internet kesintisini hissttirmeden bant genişliğinin sınırlanabilmesi sağlanıyor (Yani 1 saniyenin yarısında veri aktarımına izin verilirken diğer yarısında limitlemek, kesintilerin çok uzun sürmesine neden olacaktır. Yani internet kesintisi etkisi oluşturacaktır).

|→ *Tek kova kullanılarak gerçekleştirilen mekanizmada (**Single Rate Two-Color Makers/Policers**) trafik oluşturmaya izin verilen 125 ms'de 16 Kbitin tamamı kullanılmadığı durumda bu miktar trafik oluşturulmasına izin verilmeyen zaman biriminde kullanılamıyor (Burada iki renk ile drop edilen ve geçirilen trafik temsil ediliyor)*.

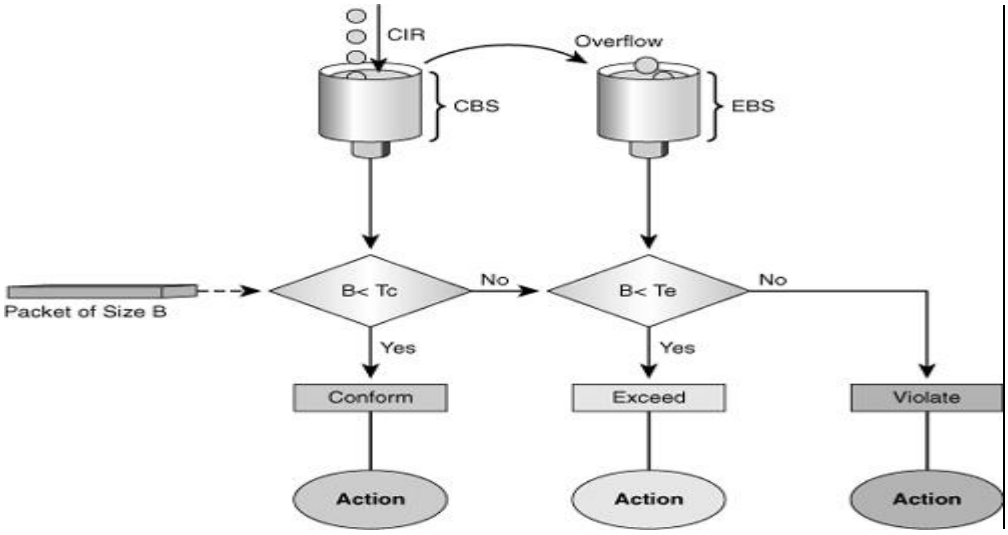
|→ *Çift kova kullanılarak gerçekleştirilen mekanizmada (**Single Rate Three-Color Makers/Policers**) trafik oluşturmaya izin verilen 125 ms'de 16 Kbitin tamamı kullanılmadığı durumda kullanılmayan trafik miktarını tutmak için ikinci bir kova (Be) tanımı yapılıyor. İlk kova sınırına ulaşıldıktan sonra ikinci kovada tutulan miktarkadar bant genişliği kullanılmasına izin veriliyor. Bu durumda da 1 saniyede toplam kullanılacak bant genişliği aşılmıyor (Burada üç renk ile drop edilen, geçirilen ve arta kalan/depolanan miktar temsil ediliyor) (Confirm – Geçirilen trafik, Exceed – Depolanan trafik, Violate – Drop edilen trafik).*



|→ Trafik oluşturmasına izin verilen 125 ms'den önce kova değeri doldurulursa bu durumda kullanıcı bir sonraki trafik oluşturulmasına izin verilen periyota kadar bekletilecektir. Yani kullanıcı için internet kesintisi etkisi yaratacaktır. Bunun gibi durumların yaşanmaması için kova boyutunun dikkatli seçilmesi gerekiyor.

|→ Konfigürasyonunda Bucket boyutu belirtilmediği taktirde varsayılanda Tc değeri 125 ms olarak alınıyor. Bucket boyutu Bc = CIR x (Tc / 1000) formülüyle otomatik olarak hesaplanıyor.

|→ Konfigürasyonda değiştirilebilecek değerler; Committed Information Rate (**CIR**), Committed Brust Size (**Bc**), Excess Brust Size (**Be**), Peak Information Rate (**PIR**), Bc Bucket Token Count (**Tc**), Be Bucket Token Count (**Te**), Incoming Packet Length (**B**). Özetle;



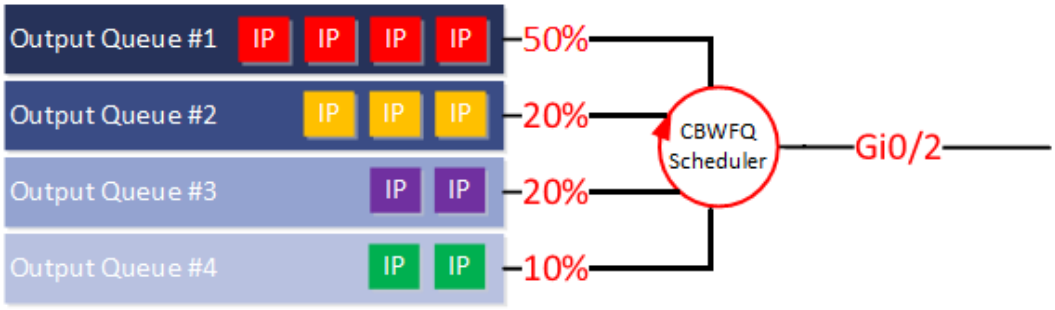
Single Rate Three-Color Makers/Policers Konfigürasyonu

-

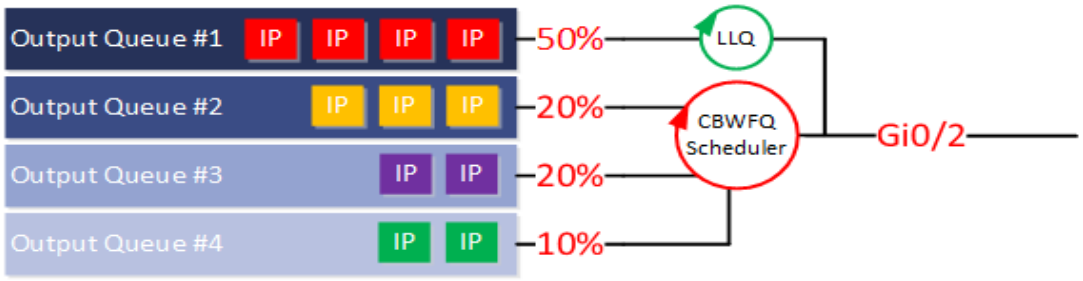
Congestion Management and Avoidance

Network cihazlarında trafğin giriş yaptığı portların bant geniliğinin toplamının çıkış yaptığı bant genişliğinden düşük veya eşit olması gerekir. Aksi durumda **Congestion (Tıkanıklık)** oluşacaktır. Congestion oluştuğunda uygulanan ilk çözüm Queuing (kuyruklama) mekanizmasıyla trafiğin bir Buffer'a depolanmasıdır. Trafiği Buffer'a eklemek için (Queuing) farklı mekanizmaları kullanılabilmektedir. Bunlar; **FIFO** (First In First Out), **WRR** (Weighted RoudRobin), **PQ** (Priority Queuing), **RoudRobin**, **CQ** (Custom Queuing), **WFQ** (Weighted Fair Queuing), **CBWFQ** (Class-Based Weighted Fair Queuing) ve **LLQ** (Low-Latency Queuing) tekniklerdir. **CBWFQ** (Class-Based Weighted Fair Queuing) ve **LLQ** (Low-Latency Queuing) dışındaki teknikler günümüzde kullanılmamaktadır.

|→ CBWFQ (Class Based Weighed Fair Queuing), birçok kuyruk/class oluşturulur (256 taneye kadar kuyruk oluşturulabiliyor) ve ACL'ler kullanılarak bu kuyruklara eklenecek paket tipleri belirtilir. Oluşturulan kuyruklara ise belirli bant genişliği atanarak kuyruklara (önem seviyesine bağlı olarak) eklenen paketlere öncelik verilmesi sağlanır. Günümüzde yaygın kullanılan kuyruklama stratejisidir.



|→ LLQ (Low Latency Queuing), CBWFQ mekanizmasının ses trafiğine öncelik verilen versiyonudur. Ses trafiğine LLQ adı verilen ayrı bir kuyruk yapısı kullanarak gerçekleştiriyor (**bu kuyruğa ses dışında farklı trafiklerin koyulması da sağlanabiliyor**). Eğer ki ses paketlerinin bulunduğu kuyrukta bekleyen paket varsa diğer kuyruklar bekletileerek ses paketlerine öncelik verilmesi sağlanıyor. Ses paketlerinin bulunduğu kuyrukta paket yoksa diğer kuyruktaki paketler kendilerine ayrılan bant genişliğince paketleri iletmeye devam ediyor. Yani LLQ kuyruğuna gelen paketler bekletilmeden doğrudan işleme alınıyor. Bu durumda LLQ kuyruğuna yüksek yüzdelik dilim verilirse LLQ kuyruğunda trafiğin yoğun olması durumunda diğer kuyrukları çalışamaz hale getirecektir.



Random Early Detction (RED)

Kuyruklama mekanizmasında Buffer dolduktan sonra paketlerin önceliği farkletmeksizin gelen bütün paketler drop edilir. He paketin drop edilmesi bir süre sonunda internet kesintileri oluşturacaktır. Bunun önüne geçebilmek için RED mekanizması kullanılıyor. Red mekanizması kullanılarak Buffer'ın

dolmasına yakın Buffer üzerinde tutula paketlerden rastgele seçim yaparak paketleri drop ediyor. Bu sayede trafiğin tamamı kaybedilmemiş oluyor. Örnek olarak bir TCP bağlantısında bağlantıyı yeniden kurmak yerine sadece arada drop edilen paketlerin telafisi sağlanacaktır (Aynı zamanda TCP Flow Control özelliğiyle trafik hızının yavaşlatılması sağlanıyor).

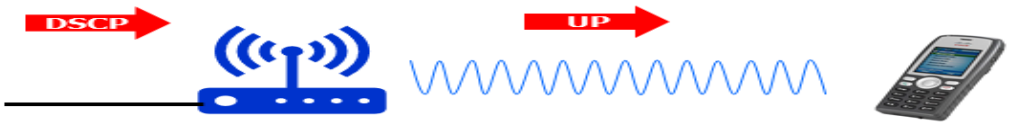
Weighted Random Early Detction (WRED)

RED mekanizmasında Buffer dolmasına yakın paketlerin rastgele seçilerek drop ediliyordu. WRED mekanizmasında ise Buffer'ın doluluk oranıyla paketlerin öncelik değerleri doğrultusunda paketlerin drop edilmesi sağlanıyor. Örnek olarak Buffer'ın %50'si dolu olduğunda AF13 etiketine sahip paketler, Buffer'ın %60'ı dolu olduğunda AF12 etiketine sahip, Buffer'ın %80'ı dolu olduğunda AF11 etiketine sahip paketler arasında rastgele paketler seçerek drop etmeye başlanması sağlanabiliyor.

KONFİGÜRASYONLAR YAKINDA EKLENECEK

NOT

- Gecikmeleri ve paket kayıplarını önüne geçebilmek için;
    - Bant genişliği arttırılabilir
    - Sıkışıklığı önleyecek/azaltacak algoritmalar/mekanizmalar kullanılabilir
    - Paketlere öncelik değerleri tanımlanarak düşük öncelikli paketlerin drop edilmesi, yüksek öncelikli paketlere öncelik verilmesi sağlanabilir (Traffic Policing, Traffic Shaping)
- Günümüzde sınırlı bant genişliğine sahip kurumlar bant genişliğini daha verimli kullanabilmek adına Video Stream sitelerinin trafiğini kısıtlayabiliyor veya engelleyebiliyor. Bunu trafiğin içeriğini baz alarak özel kısıtlamalar tanımlanabilen NGFW ile gerçekeştiriyorlar. Bu tanımlamalara örnek olarak;
    - Video Stream için total bant genişliğinin (örnek olarak 15 Mb gibi) belirli bir kısmı ayrılabiliyor. Bu sayede Video Stream sitelere erişim sağlanabilse de Video Stram trafiği için bant genişliğini gereksiz yere harcamasının önüne geçiliyor.
    - İstenmeyen domain veya ip adresleri için engellemeler yapılabiliyor.
- Normalde 802.1Q etiketinde bulunan **CFI** (Canonical Format Indicator) alanı Token Ring teknolojisini ayırt edebilmek için kullanıyordu. Günümüzde ise bu kısım revize edilerek **DEI** (Drop Eligible Indicator) ismini almıştır. Bu alan kullanılarak paketlerin drop edilmesi sağlanabliyor.
- Wireless için de paketlere öncelik verilebiliyor. Bu işlem Wireless'a gelen trafiği kablolu ortma aktarılırken etiket bilgisi eklenerek gerçekleştiriliyor. Bunun için farklı bir SSID yayını yapılması gerekiyor. Yani tek bir SSID kullanılarak trafikler önceliklendirilemiyor. Oluşturlan yeni SSID'den gelen paketler işaretlenerek kablolu ortama bırakılıyor (**Kablo üzerinden gelen trafiği kablosuz ortama geçerken de (Hava otamında) önceliklendirme işlemi yapılabiliyor – EDCF – Detaylar için https[:]//web.itu.edu.tr/akingok/ab08/KABLOSUZ%20AGLARDA%20SERVIS%20KALITESI.pdf inceleyebilirsin**).



IETF Traffic Class	PHB
Network Control	CS6
Voice (46), Voice-Admit(44)	EF,VA
Signaling	CS5
Multimedia Conferencing	AF4x
Real-time Interactive	CS4
Multimedia Streaming	AF3x
Broadcast Video	CS3
Low Latency Data	AF2x
OAM	CS2
High Throughput Data	AF1x
Standard (Best Effort)	DF
Low Priority Data	CS1

AC	UP
AC_VO	7
AC_VO	6
AC_VI	5
AC_VI	4
AC_VI	4
AC_VI	4
AC_VI	4
AC_BE	3
AC_BE	0
AC_BE	0
AC_BE	0
AC_BK	1