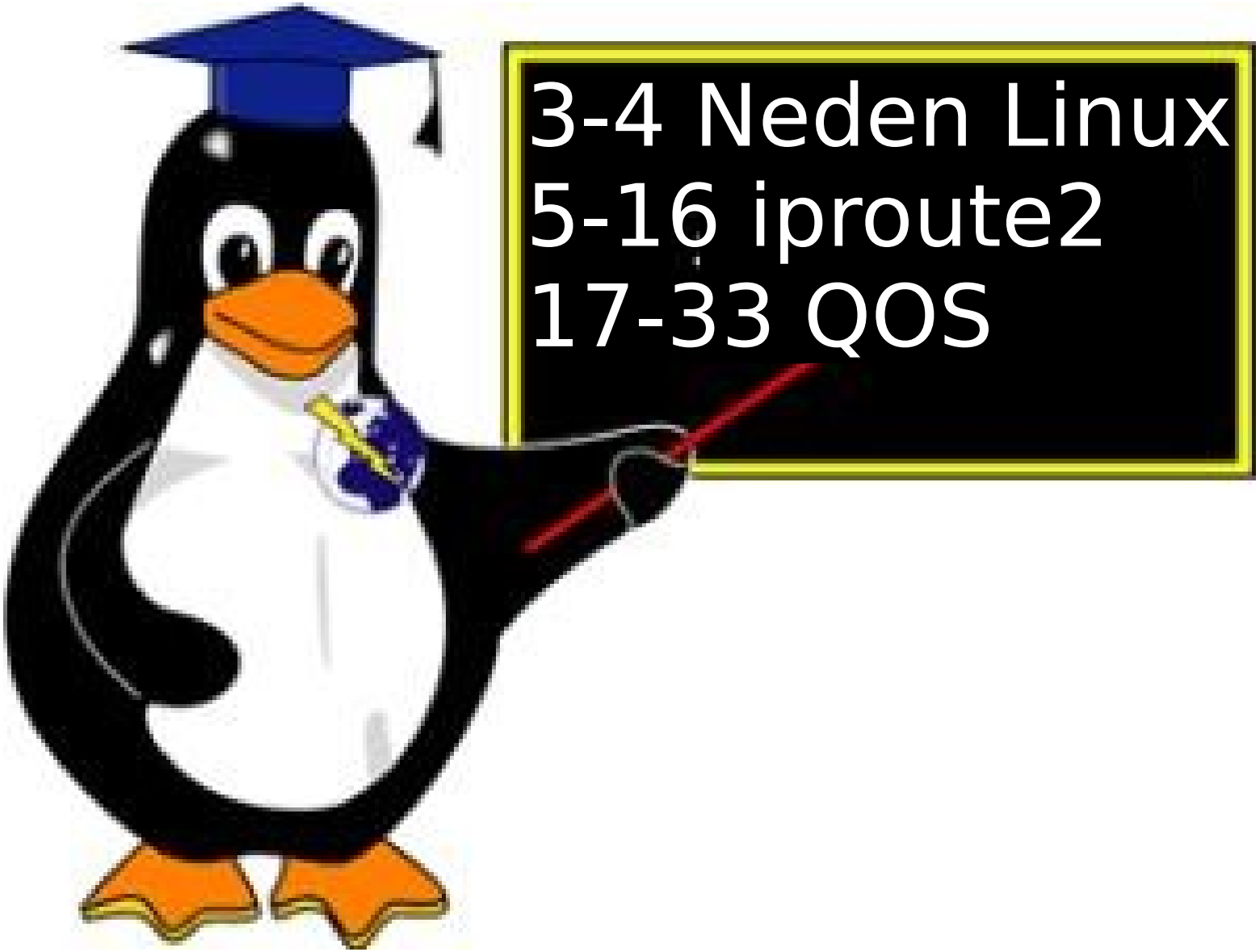
HOŞGELDİNİZ

LINUX'TA ROUTING VE QOS YAPISI

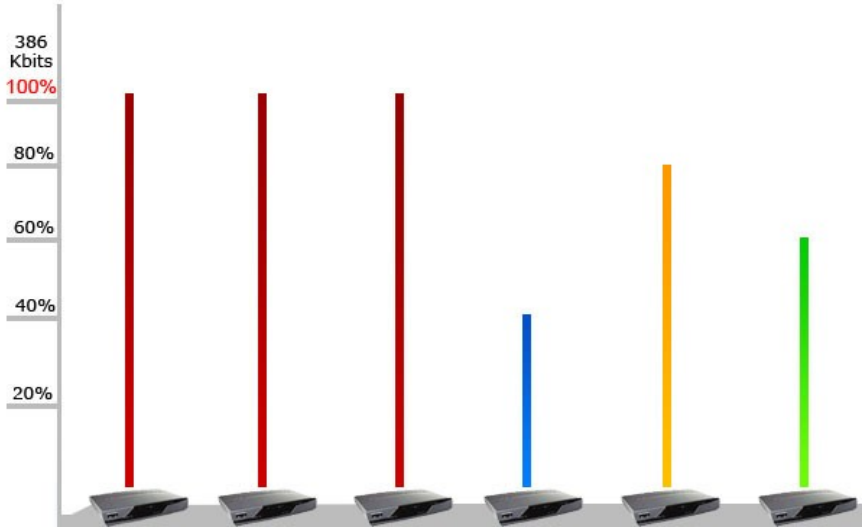
Özgür Yazılım ve Linux Günleri

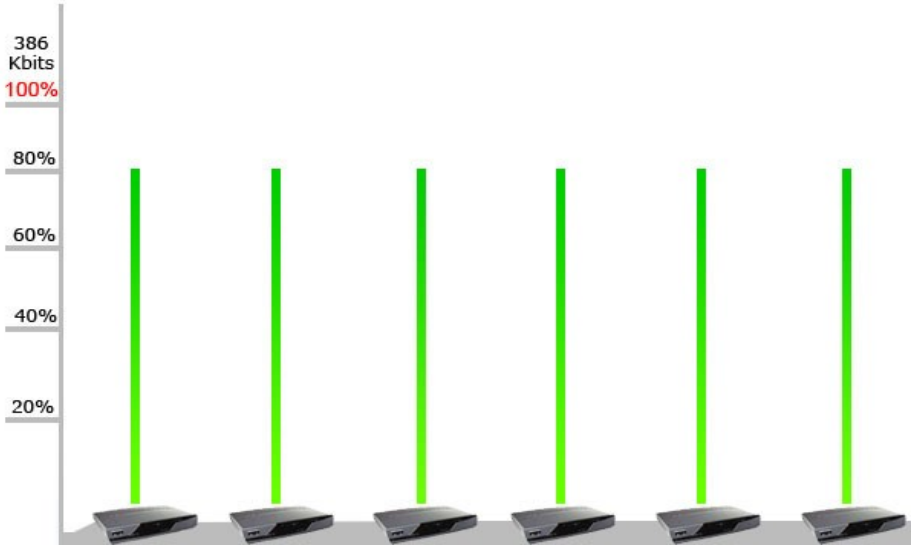
İstanbul Bilgi Üniversitesi
Dolapdere Kampüsü
3 Nisan 2010

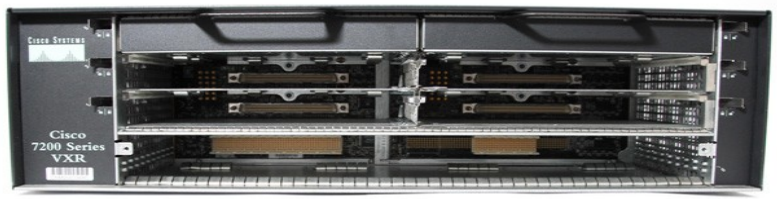
Alper YALÇINER
alper.yalciner@gmail.com


3-4 Neden Linux
5-16 iproute2
17-33 QOS

Cisco > Linux LoadBalancer Upgrade





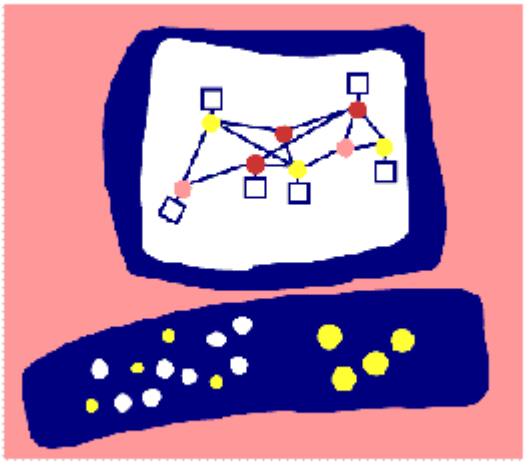


Ücretli firewall'lar ve Linux

Ücretli bir çok firewall'in web arayüzü linux'a göre oldukça yeteneksizdir.

Buna rağmen ücretli firewall'ların bir çoğu linux üstüne kurulmuştur. Örn : Checkpoint , SnapGear ürünleri.

Check Point®
SOFTWARE TECHNOLOGIES LTD.



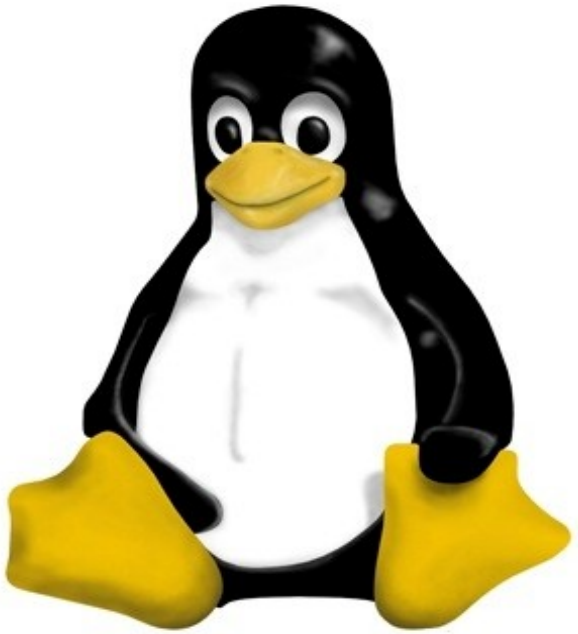
We Secure the Internet.

secure
computing®

Iproute2 nedir ?

Temel olarak iproute2 Kernel 2.2 ve üstü linux sistemlerde temel unix network araçlarının yerini almak için tasarlanmıştır.

- ip addres , ip link = ifconfig
- ip route = route
- ip neigh = arp
- ip tunnel = iptunnel
- ip maddr = ipmaddr
- ss = netstat



Neden yeni bir araç ?

*** İlkel Araçlar**

Değişen ve büyüyen network dünyası , Çoklu Routing katmanları , QOS Loadbalancing ve Tunneling gibi ihtiyaçları doğurarak eski araçları yetersiz ve çağdışı kılmaya başlamıştır.

*** Yetenekli Güncel**

Iproute2, iptables ile beraber linux günüzdeki bir çok paralı router ve firewall dan çok daha yetenekli hale gelmiştir.

Iproute2 Cisco komut satırı referans alınarak dizayn edilmiştir.

Piyasadaki router ve switch'ler %98 Cisco komut satırı uyumludur.

ip route ile statik routing :

ip route add 9.9.9.1/32 via 2.2.2.1

ip route add 0.0.0.0/0 via 1.1.1.1

Ip adresi eklemek

ip link set eth0 up
ip address add 192.168.1.7/24 dev eth0
ip address show eth0
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
link/ether 00:a0:d1:3e:28:43 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.7/24 scope global eth0
inet 192.168.1.8/24 scope global secondary eth0

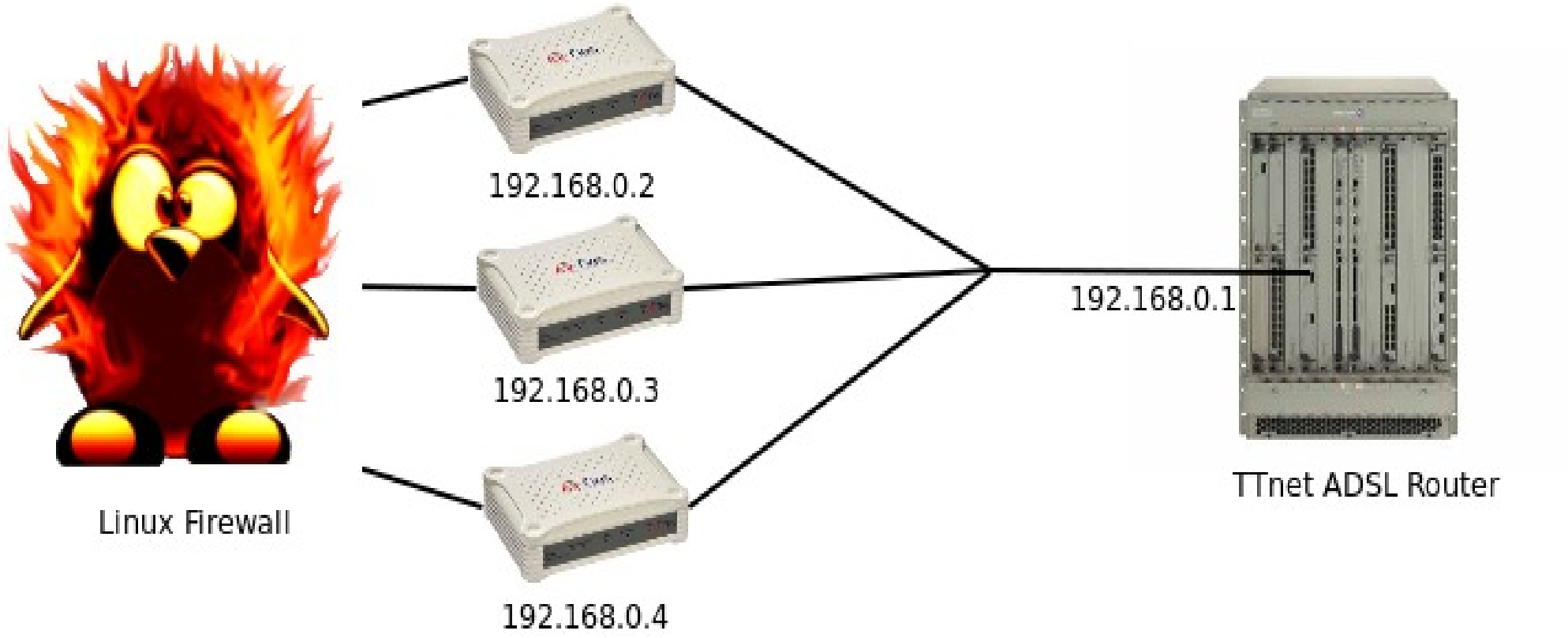
Multiple Routing Tables
(Çoklu Routing Tabloları)

Linux “ip route” ile çoklu routing tablolarını destekler.

Çoklu routing tabloları Main (Ana) Routing tablosu hariç , Sanal tablolar yaratarak normal networkler'de yapılandırılması mümkün olmayan routing işlemlerinin yapılmasına olanak sağlar ve yönetim kolaylığı getirir.

* Diğer işletim sistemleri Çoklu Routing tablosu içermez Sadece FreeBSD “setfib” ile kısıtlı kullanım imkanı sağlar

“ip route” ile Çoklu routing tabloları,aynı ip adresine ait birden çok ağ geçidinin farklı arayüzlerle kullanımını mümkün kılar.



Routing Realms (Routing Alanları, Krallıkları)

Routing Realms bir çok yönden çoklu routing tabloları ile karıştırılsada ana görevleri routing'lerin birbirinden ayrılması değil sınıflandırılmasıdır.

Örneğin : BGP , OSPF , RIP tablolarının sınıflandırılması.

“ip rule” :

“ip rule” routing policie database RPDB (routing “ kural / ilke “ veritabanı) içindir . Iproute2 harici standart Unix/linux araçları muadilini içermez.

“ip rule” kısaca kurala dayalı routing'i (policie routing) içerir ve çoklu routing katmalarına (Multiple Routing Tables) entegre eder.

* “ip rule “ routing kuralları koymaya ve uygulamaya yarar .

“ip neighbour / ip neig” (Komşu):

“ip neigh” arp tablosunu (Mac Adres) görüntülemeye ve yönetmeye yarar.

Kullanılabilecek argumanlar : add, change, replace, delete, flush ve show (list) .

ip neigh add 10.0.0.3 lladdr 00:11:11:44:4e:fa dev wlan0 nud perm

“ip tunnel “ :

“ip tunnel” basitçe iki veya daha fazla nokta arasında tünel oluşturur ve yönetir, **gre** veya **ipip** gibi protokollerde tünel oluşturulabilir.

Gre örneği :

ip tunnel add netb mode gre remote \
195.174.6.140 local 85.8.5.43 ttl 255

ip link set netb up

ip addr add 192.168.2.12/24 dev netb

ss
(Socket Statistics/ Soket İstatistikleri)

“ss” netstat komutuna benzer bir çıktı vererek , linux soket istatistiklerini incelemek için kullanılır . Diğer araçlara göre çok daha fazla TCP ve State “ durum “ hakkında bilgi verir .

Örnekler :

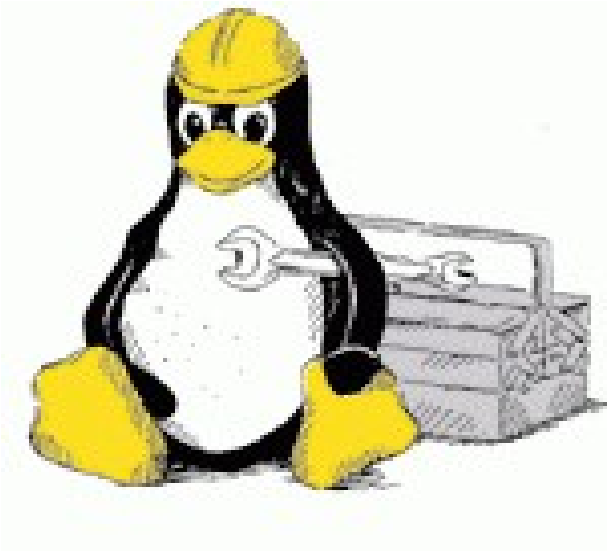
ss -t -a = tüm TCP bağlantılarını görüntüler

ss -x src /tmp/.X11-unix/* = X server e bağlı tüm süreçleri listeler.

ss -o state established '(dport = :ssh or sport = :ssh)' = \
İçeriye veya dışarıya yapılan tüm ssh bağlantıları listeler.

Iproute2 Araçları (iproute2 tools):

Iproute2 bir çok araç içersede araçların içeriği hali hazırda ip komutu ile yapılabilen şeylerdir. Araçlar yeni bir özellik kazandırmaktan çok günlük hayatı sadeleştirmek ve kolaylaştırmak için düzenlenmişlerdir.



Araçlardan bazıları :

ctstat Bağlantı durumu

lnstat network istatistikleri (rtstat yerine)

rtacct /proc/net/rt_acct tarafından toplanılan routing bilgileri

rtmon Routing görüntüleme aracı

Bu resimi koyacak yer bulamadım....

Iproute2 – tc
Traffic Controlling Executable
(Trafik Kontrol İdaresi)

tc linux için QOS (Quality Of Service / Sunulan hizmet kalitesi) ve COS (Class of service / Sunulan hizmet sınıflandırması) entegrasyonlarını sağlar.

tc qdisc
tc class
tc estimator
tc filter
tc policy

QOS Nedir ?

Ağ İletişimi Hizmet Kalitesi
(*Quality of Service*)
Kısaca **QoS**, ağ üzerindeki uygulamaları önceliklendirerek, zaman ve kalite kaybını azaltmayı hedefleyen bir ağ servisidir. Bir ağ bağlantısı üzerinden çalışan, bir trafik veya program türüne öncelik veren çeşitli tekniklere karşılık gelir.

QOS Hakkında Bilinen Genel Yanlışlıklar

* QOS Özgürlüğü kısıtlar.
* QOS gelen ve giden (Ingress/Egress) trafiği kontrol edebilir.
* Bant genişliği hız demektir.
* QOS Sadece bant genişliğini sınırlamak içindir.

QOS Gerektiren Hastalık Belirtileri

* Değişken Bant genişliği
* Hizmetlerde Yavaşlama ve/veya Kesinti
* Jitter (Stress)

Neden QOS ?

Sekreter

Patron

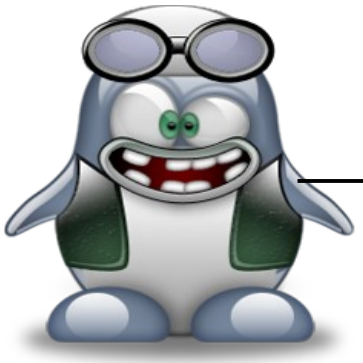
Admin

Gbit/Switch

Sparta

Darboğaz

4Mbit Adsl



User

User

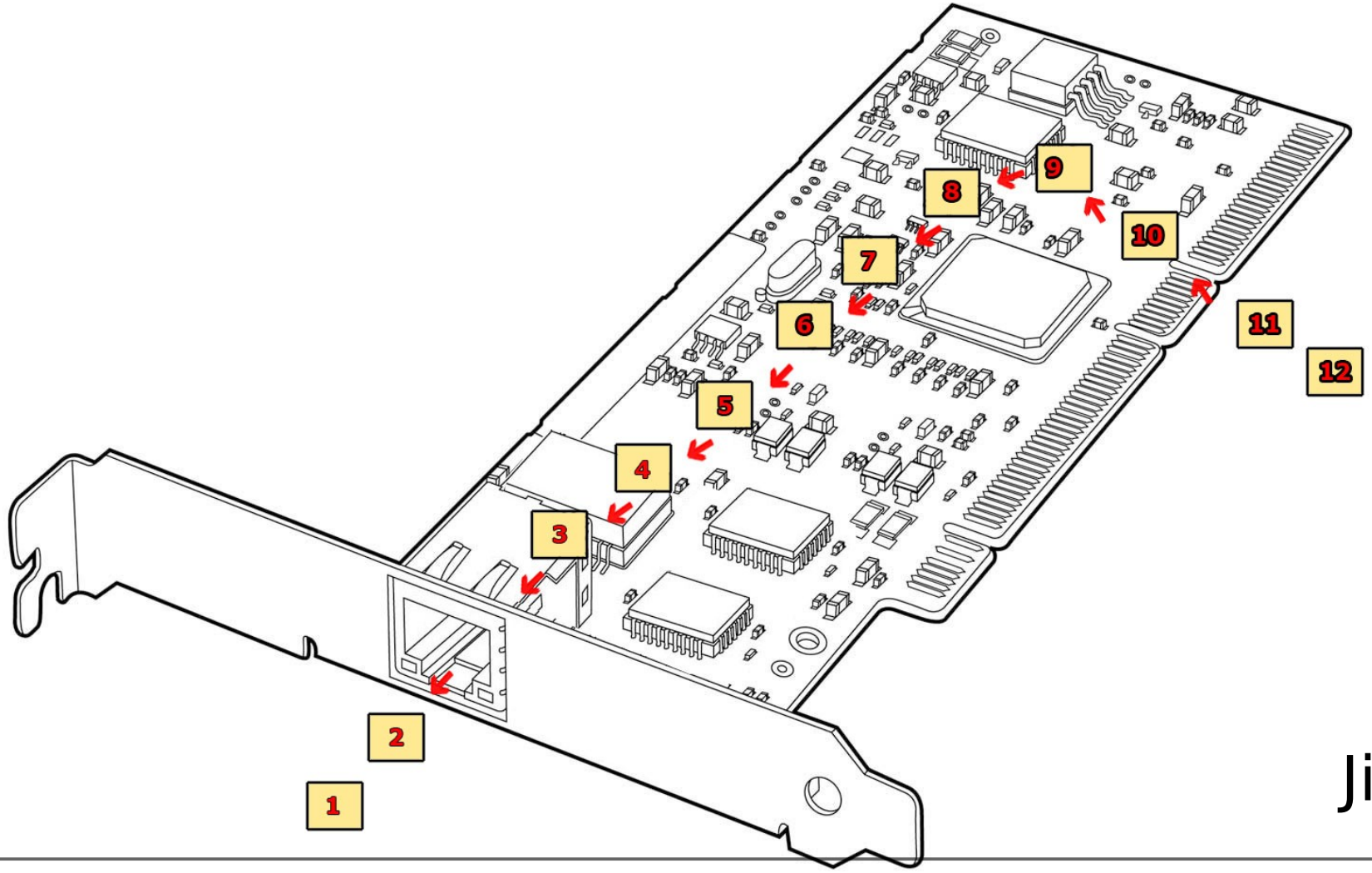
SOHO Network Örneği

Linux ile Çok kullanılan QOS Algoritmaları

* First In First Out (FIFO)
* Priority queue
* Random Early Detection (RED)
* Generalized RED (GRED)
* Stochastic Fair Queuing (SFQ)
* Token Bucket Flow (TBF)
* Class Based Queue (CBQ) Ve Hierarchical Token Bucket (HTB)

FIFO

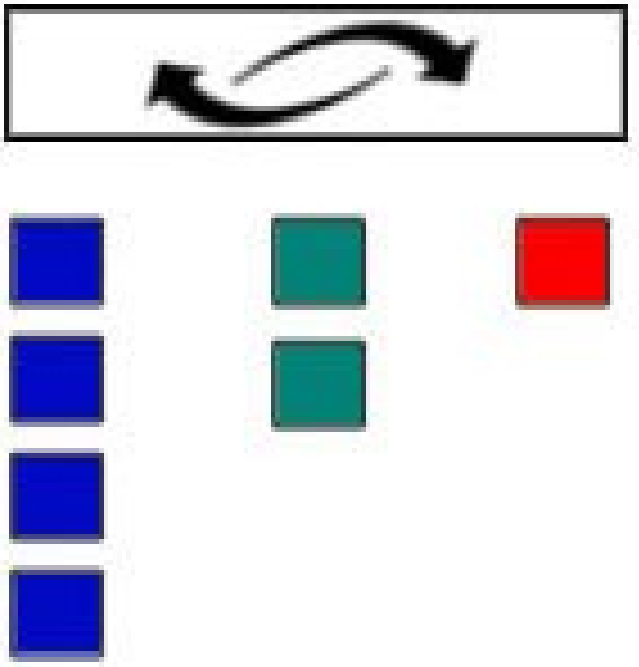
(First In First Out / İlk Giren ilk Çıkar)



Jiffies ?

Stochastic Fair Queuing (SFQ)

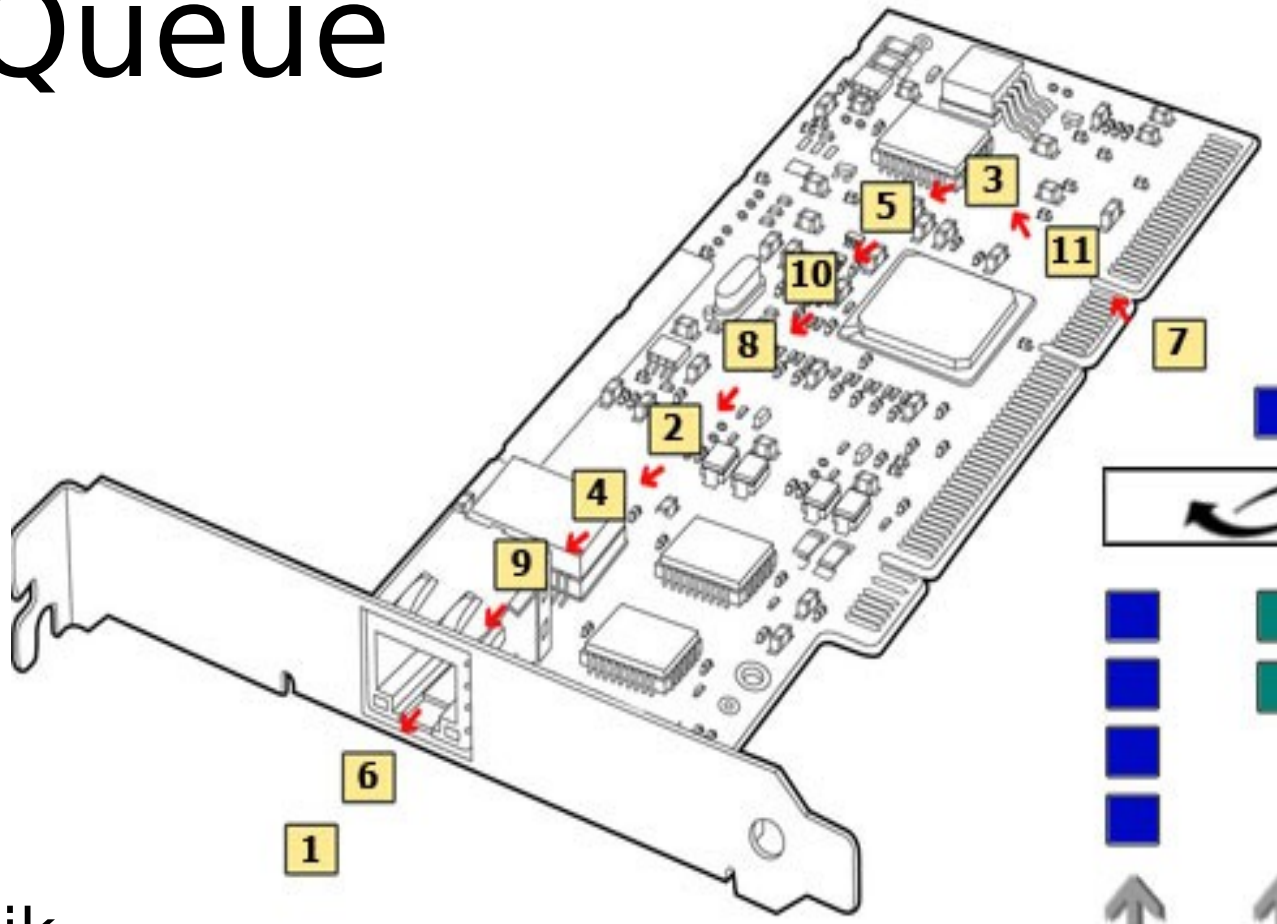
SFQ : Stochastic Fairness Queuing tcp ve udp bağlantıları eşit olarak dağıtmaya çalışarak tek bir bağlantının tüm hattı bloke etmesini önler. “Adil Sıralama “ olarakta bilinir.



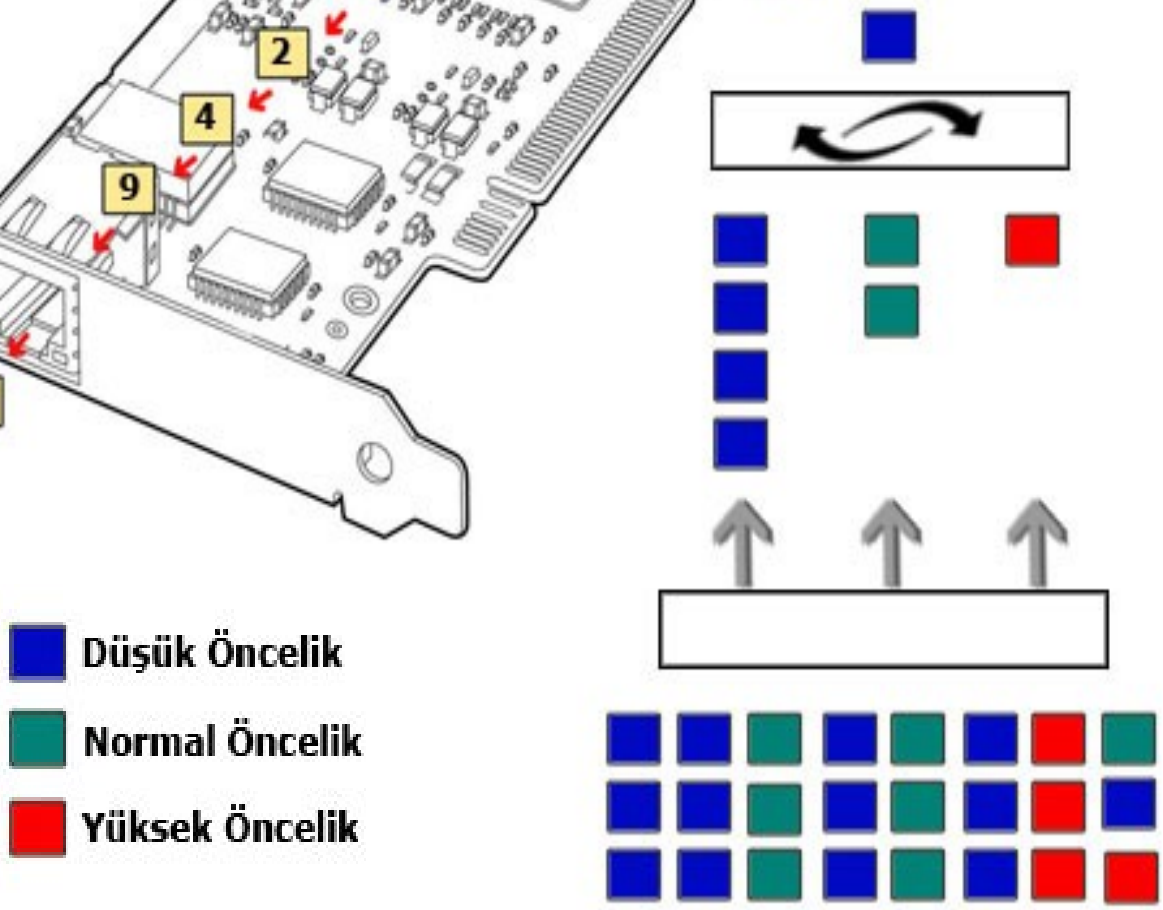
tc qdisc add dev wlan0 root sfq perturb 10

tc, wlan0 device i için qdisc ekle sfq için root olsun dağıtımı 10 saniyede bir yeniden düzenle.

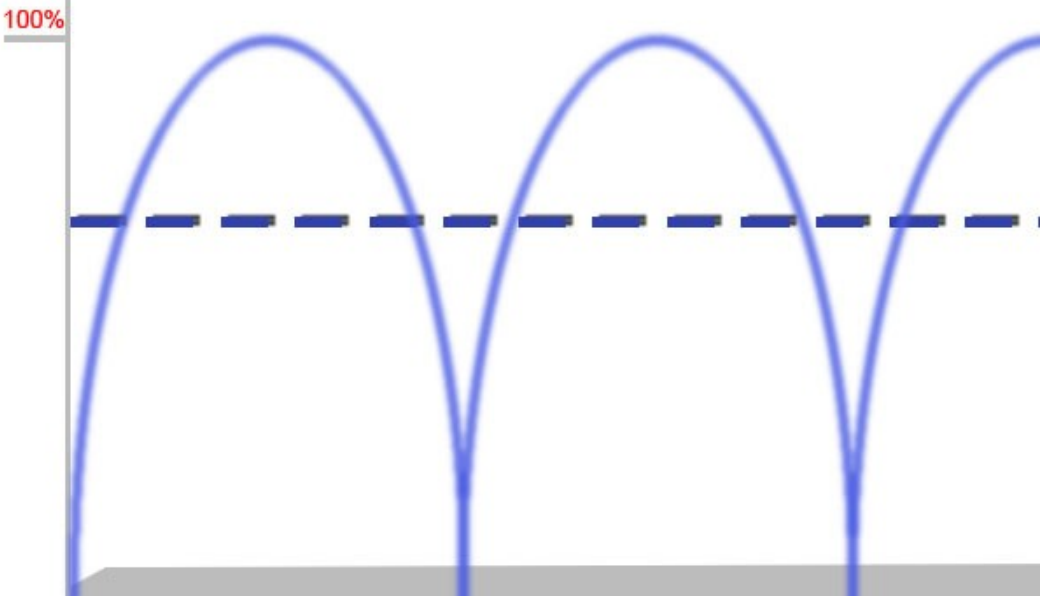
Priority Queue

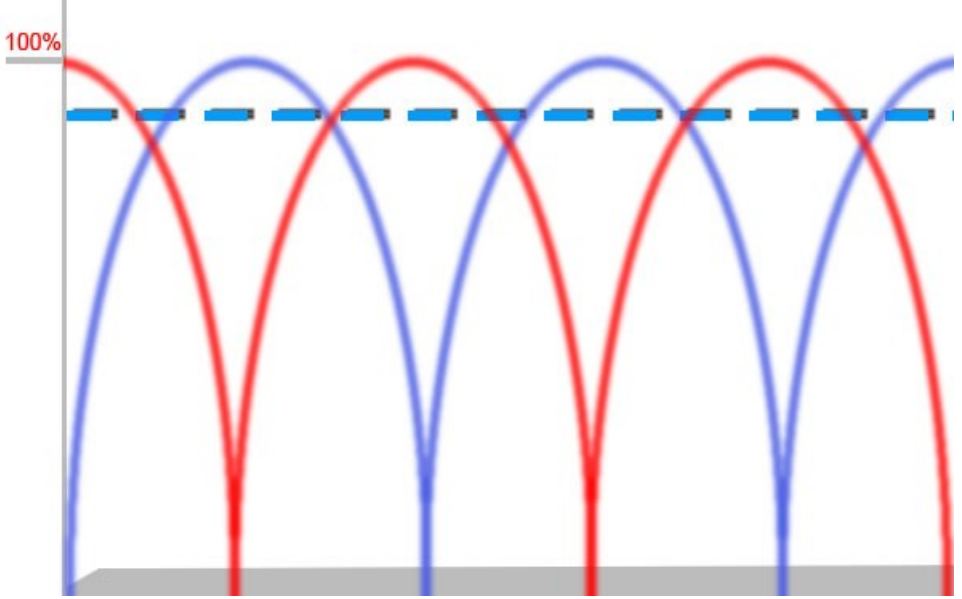


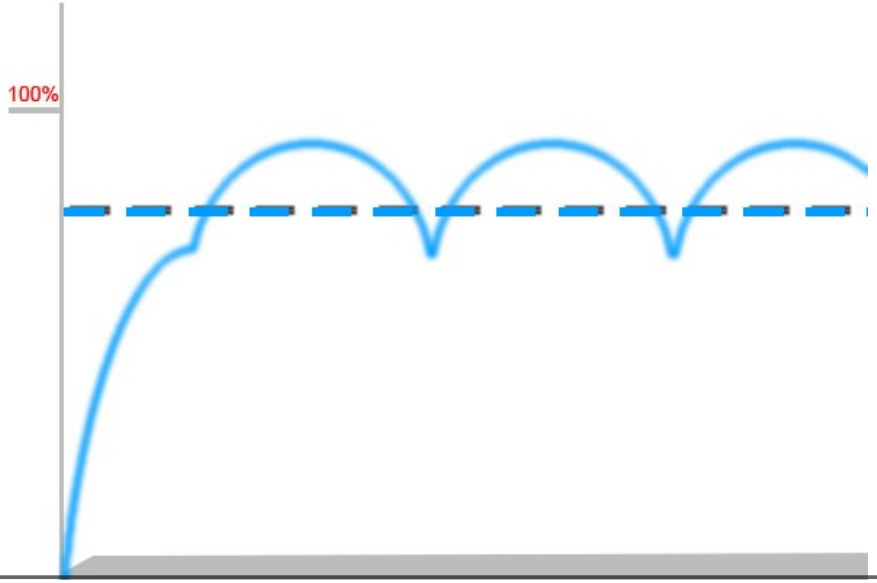
Paketlere öncelik vererek istenilen paketlerde gecikmeyi minumum a indirmeyi hedefler.



RED (RANDOM EARLY DEDECTION)







Aşırı yükte network üzerinde oluşacak kuyrukta paketlerin düşürülmesinin önceden kontrolünü sağlar.

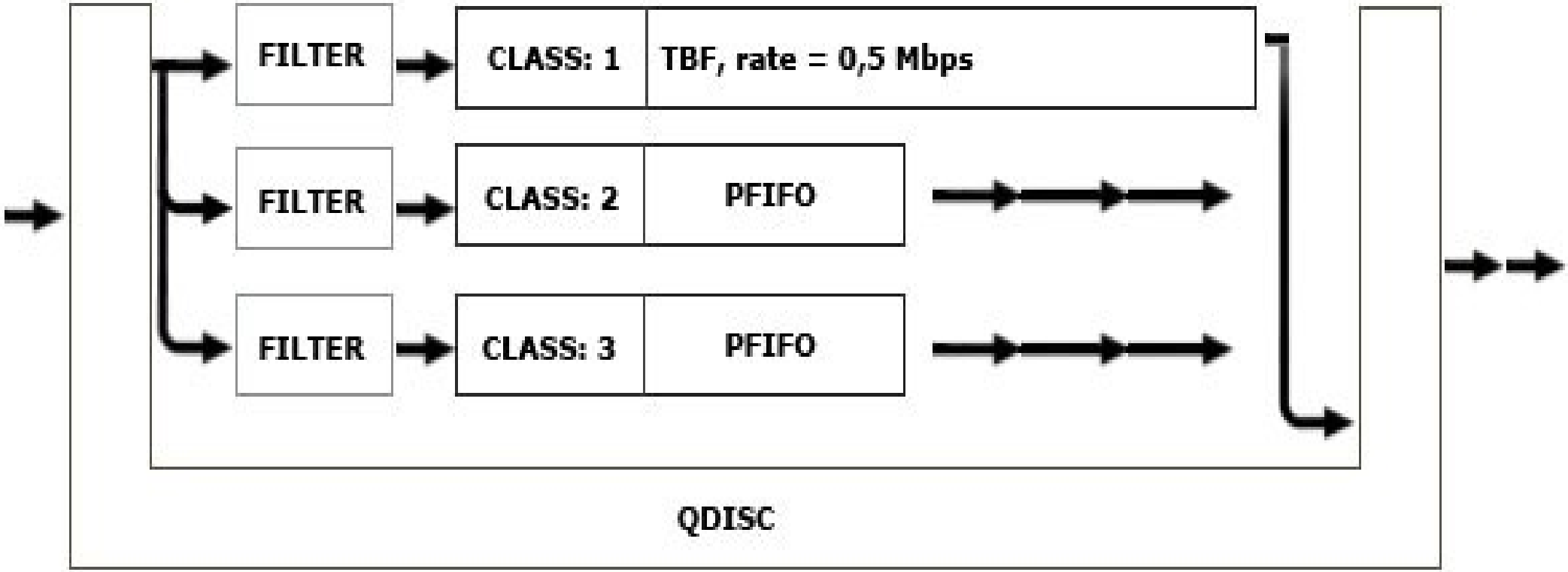
Generalized RED (GRED)

RED algoritmasının değişik threshold (Eşik değerleri), Atanabilen şeklidir. Cisco WRED (Weighted RED)'e tekamül eder.

Servis	Paylaşım	Gecikme (MS)	Paket Uznlğ.	Düşürme İht.
VoIP	%3	20	128	N/A
DNS	%2	50	256	N/A
SQL	%20	100	1024	%1
WWW	%40	100	512	%4
FTP	%20	100	1024	%4
UDP (Diğer)	%10	50	1024	N/A
Diğer	%5	100	1024	%4

Token Bucket Flow (TBF)

TBF basitce bir internet bağlantısını yavaşlatmak istiyorsak seçebileceğimiz en iyi yoldur. TBF nin diğer queue lere göre en büyük avantajı cpu ve ram dostu olmasıdır.

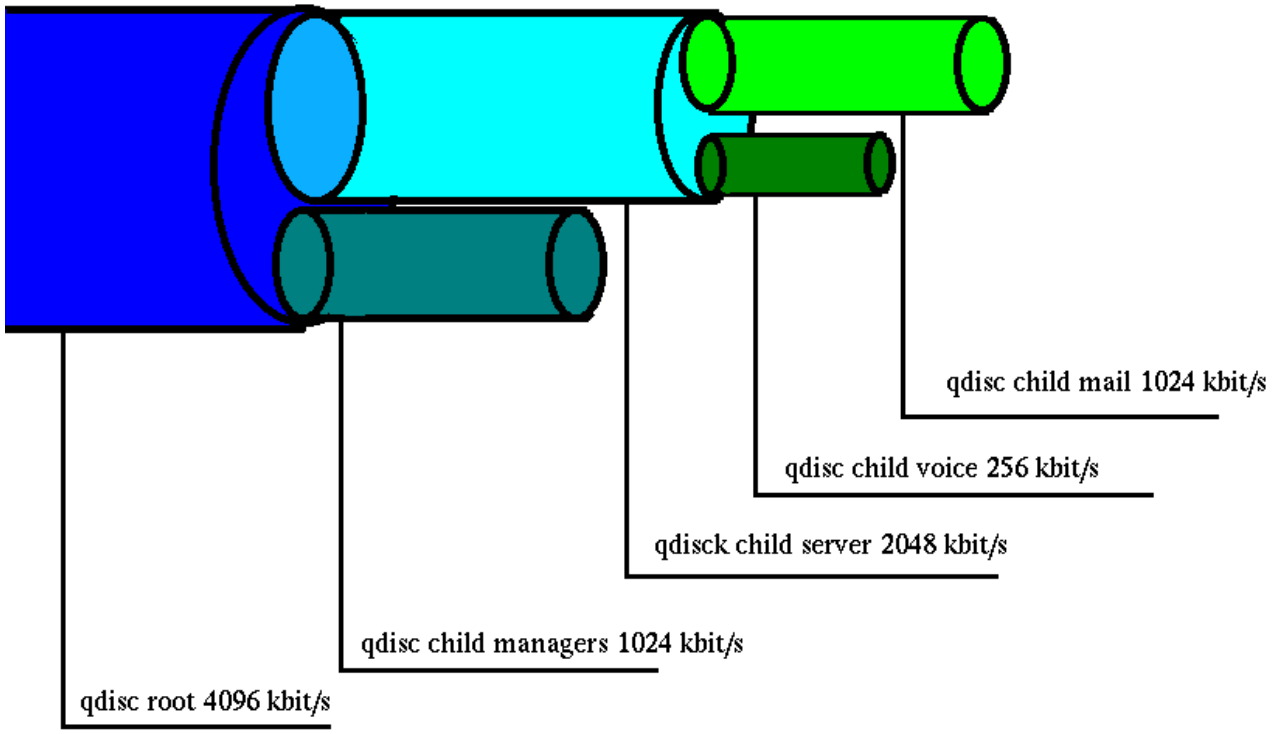


ECN Nedir ?

Explicit Congestion Notification (ECN – Kesin Tıkanıklık duyurusu) RED ile paketleri düşürmek yerine bir sonraki noktaya (Router / Firewall) haber vermek için kullanılır.

Class Based Queue (CBQ) & Hierarchical Token Bucket (HTB)

HTB ve CBQ bize link sharing yani bant genişliği yönetimi yapmamızı sağlayan bir queuing disiplinidir. kısaca interetimizi servislerimiz veya istemcilerimiz arasında bant genişliği olarak paylaştırmamızı sağlar.



Tüm linux dökümanları (Hatta CBQ kodunu yazan Alexey N. Kuznetsov) , HTB nin linux da daha iyi çalıştığını belirtmişlerdir. Ama bazı uygulama ve benchmark'larda CBQ daha iyi sonuç verebilmektedir.

İptables , Network cihazları iproute2

Iproute2 ile diğer network araçları arasında haberleşmeyi sağlamak için en çok kullanılan yöntemler.

1 . iptables fwmark,mark target
2 . iptables Classify target
3 . TOS ve DSfield

Linux Versus *BSD

Linux	BSD
Daha fazla Sistem kaynağı tüketir.	Çok az sistem kaynağı ile kararlı çalışır
Çoklu routing tabloları destekler.	Çoklu routing tabloları gelişme aşamasında
Aşırı yetenekli	Gerektiğince yetenekli
Bir çok paralı üründe kullanılır	Paralı ürünlerde rastlanmaz veya nadir rastlanır
Yapılandırması ve yönetilmesi zordur	Son derece basit ve tek yerden yönetim.

TEŞEKKÜRLER

Özgür Yazılım ve Linux Günleri

İstanbul Bilgi Üniversitesi
Dolapdere Kampüsü
3 Nisan 2010

Alper YALÇINER
alper.yalciner@gmail.com