IoS Quality of Service : Some IoS tips for Internet Service Providers (ISP) or Access Points (AP) *

Mehmet Süzen
E-mail: mehmet dot suzen at physics dot org
Memo's Island
(Dated: January, 2005)

The document explains some Cisco's IoS configuration tricks and tips for an improved quality of traffic handling on the interfaces. Possible set-up configuration for IoS firewall features agains Denial of Service attacks also discussed.

* The document initially has written while I was working in Kibris.Net Internet Services, Nicosia, Cyprus as Freelance Systems and Software Engineer, it is updated and expanded in January 2008 for passing my experience to community and for archive purposes. This document is in no way affiliated with Cisco Systems, IoS is the property of Cisco Systems and other mensioned products or algorithms are property of respected copyright owners.

Arguably, the most important part of a service provider's network infrastructure is the border router. Hence, having an appropriate settings on those devices is quite curicial for the quality of service considerations, as well as, security. The most popular device used on those points, like border routers, are Cisco products, and its operationg system IoS.

I. CONGESTION AVOIDANCE AND QUEUING STRATEGY

It is important to assign appropriate queing strategy on the up or down stream interfaces. One of the best strategy for congestion avoidance is an algorithm called Random Early Detection (RED). You may want to apply following IoS config for all interfaces for which traffic is congested (parameters must be adjusted accordingly).

```
random-detect
random-detect flow
random-detect flow count 16
random-detect flow average-depth-factor 8
```

More information on how to apply $random-detect$ can be consulted from Cisco document on congestion avoidance.

II. PREVENTING FLOOD AND DDOS TYPE ATTACKS: REDUCING THEIR IMPACT

Another important issue is flooding. Some people can cause your traffic being flooded (denial of service: DOS) by exessive traffic with bad intentions or without any intention but by means of misuse. So IoS has some protection against this type of flood traffic. Example command set would be;

```
ip inspect max-incomplete high 400
ip inspect one-minute high 400
ip inspect udp idle-time 20
ip inspect dns-timeout 60
ip inspect tcp idle-time 50
ip inspect tcp finwait-time 50
ip inspect tcp synwait-time 15
```

Parameters should be adjusted according to your network state. Consult with Cisco documentation for firewalling.

III. MORE TIPS FOR ISP'S

You may want to apply following command set for your important interfaces;

```
no ip redirects
no ip unreachables
no ip proxy-arp
ip route-cache policy
ip route-cache flow
no ip mroute-cache
```

More detailed descriprions can be found on documentations.

IV. OUTLOOK

General hints you must consider;

- ARP packets should not be allowed to reach other interfaces, unless it is necessary.
- Packet re-writing should be prevented.
- Route caches must be set and used efficiently.
- Ingress filtering must be set. That means packets of origin show different then your inbound traffic must not be allowed to pass border, and vice versa.

There is a saying, Quality of Service (QoS) and Security has no absolute solution in general, it is a way of life.