Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Spring Term 2016
Prof. Adrian Perrig

Operating Systems and Networks
Assignment 11

Assigned on: **June 3, 2016**

1 Congestion 1

RFC 791 `http://tools.ietf.org/html/rfc791` defines a TCP header field known as *Type of Service* (TOS). TOS was originally designed to allow senders of TCP traffic (i.e., applications) to specify whether traffic they create should be treated with priority, preference for high reliability or preference for low delay.

Explain why it is a bad idea to allow routers to read this field and make congestion control decisions based on it.

2 Congestion 2

Consider the arrangement of hosts `H1` to `H8` and routers `R1` to `R7` in Figure 1.

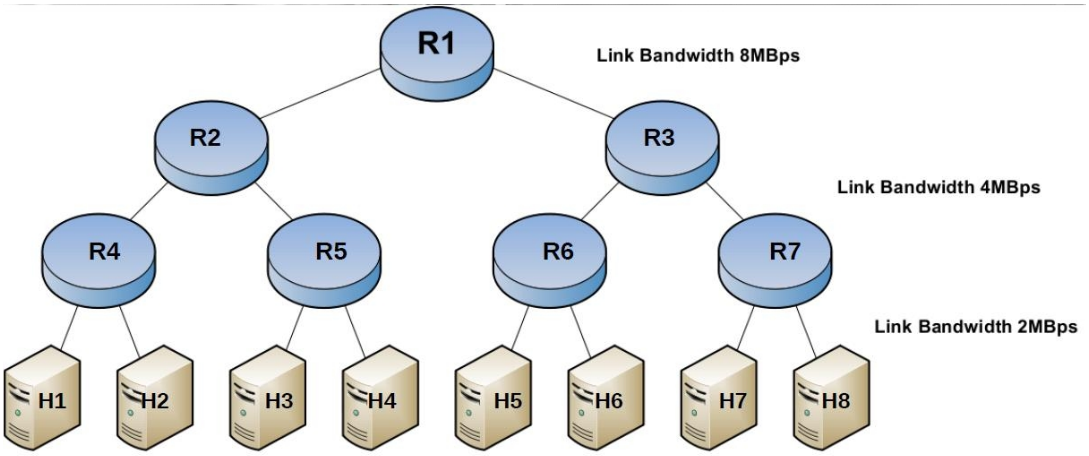


Figure 1: **Network Topology for Exercise**

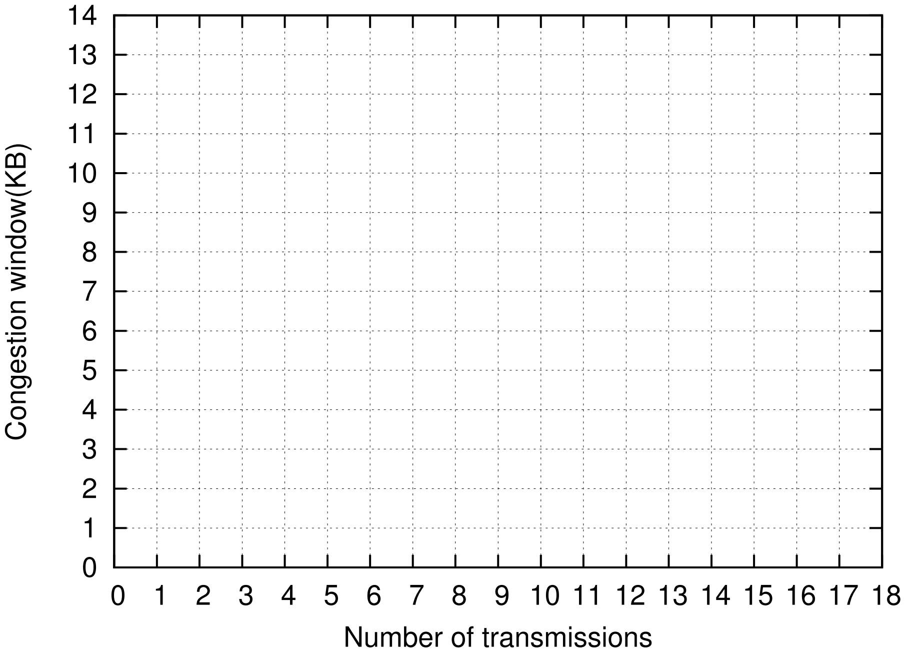
(a) Show that the links of `R1` cannot become a bottleneck of the network.

(b) For all other links, give an example traffic pattern that congests that link. Assume that all the traffic is generated exclusively by messages between two hosts; that is, routers only forward messages and are never the source nor the destination of a message.

3 Congestion 3

In the lectures, we saw two types of congestion control techniques: *Additive Increase/Multiplicative Decrease* and *Slow Start*. This question focuses on Slow Start. A TCP connection uses a threshold of 8KB for congestion control. The maximum segment size should be 1KB and the receiver's window is 16KB. After the 8th, the 11th, and the 17th transmission, timeouts are occurring, which are interpreted as network overload.

Sketch the size of congestion window and the threshold into the following diagram.



4 Plain DNS Hands On

In this section, you will use the Linux command line tool `dig` to query DNS servers for information.

Using the following command: `$dig www.ethz.ch`

(1) What is the TTL of the A record for `www.ethz.ch`

(2) Looking at the output, a list of authoritative name servers, A records, and AAAA records is returned by a DNS server. Which DNS server is returning this information?

(3) Notice the `flags` line in the output. What do the flags `qr rd ra` mean? Hint: look up the DNS header format at `http://www.networksorcery.com/enp/protocol/dns.htm`

(4) Can the server in answer 2 replace the information, for example, returning `1.2.3.4` as the A record for www.ethz.ch?

5 DNSSEC Hands On

The `dig` command supports the `+dnssec` parameter, which enables the retrieval of DNSSEC data if available.

Issue the following command `$dig www.google.com +dnssec`

(1) Look at the output. Does the domain support dnssec?

Now compare the output of `$dig .` and `$dig .  +dnssec`

(2) Compared the the output of the command in 1, which additional fields indicate support for DNSSEC?

6 Swiss DNS names

RFC 1912 (`https://www.ietf.org/rfc/rfc1912.txt`) states the following.

> DNS domain names consist of 'labels' separated by single dots. The DNS is very liberal in its rules for the allowable characters in a domain name. However, if a domain name is used to name a host, it should follow rules restricting host names. Further if a name is used for mail, it must follow the naming rules for names in mail addresses.
>
> Allowable characters in a label for a host name are only ASCII letters, digits, and the '-' character. Labels may not be all numbers, but may have a leading digit (e.g., 3com.com). Labels must end and begin only with a letter or digit. See [RFC 1035] and [RFC 1123]. (Labels were initially restricted in [RFC 1035] to start with a letter, and some older hosts still reportedly have problems with the relaxation in [RFC 1123].) Note there are some Internet hostnames which violate this rule (411.org, 1776.com). The presence of underscores in a label is allowed in [RFC 1033], except [RFC 1033] is informational only and was not defining a standard. There is at least one popular TCP/IP implementation which currently refuses to talk to hosts named with underscores in them.

Explain how names such as `www.grüezi.ch` can be resolved. What does a DNS request for non-ASCII domains look like?

7 DNSSEC

Cache poisoning or DNS spoofing attacks are used by attackers to attract traffic.

(a) Explain the intention behind traffic attraction attacks.

(b) Explain how attackers mount DNS spoofing attacks.

(c) Explain countermeasures.