Computer Networks 1
(Mạng Máy Tính 1)

Lectured by: Dr. Phạm Trần Vũ
Lecture 5: Network Layer (cont’)

Reference:
Chapter 5 - “Computer Networks”,
Contents

- The network layer design issues
- Routing algorithms
- Congestion control algorithms
- Quality of services
- Internetworking
- The network layer in the Internet
Congestion Control Algorithms

- General Principles of Congestion Control
- Congestion Prevention Policies
- Congestion Control in Virtual-Circuit Subnets
- Congestion Control in Datagram Subnets
- Load Shedding
- Jitter Control
Network Congestion

When too much traffic is offered, congestion sets in and performance degrades sharply.

![Network Congestion Graph]

- **Perfect**
- **Maximum carrying capacity of subnet**
- **Desirable**
- **Congested**
General Principles of Congestion Control

- Open loop solutions
  - Solve the problems by good design
  - Prevent congestions from happening
  - Make decision without regard to state of the network

- Closed loop solutions
  - Using feedback loop
Closed Loop Solutions – Three Part Feedback Loop

- Monitor the system
  - detect when and where congestion occurs.
- Pass information to where action can be taken.
- Adjust system operation to correct the problem.
Open Loop Solutions - Congestion Prevention Policies

Policies that affect congestion.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Policies</th>
</tr>
</thead>
</table>
| Transport     | • Retransmission policy  
|               | • Out-of-order caching policy  
|               | • Acknowledgement policy  
|               | • Flow control policy  
|               | • Timeout determination                                                  |
| Network       | • Virtual circuits versus datagram inside the subnet  
|               | • Packet queueing and service policy  
|               | • Packet discard policy  
|               | • Routing algorithm  
|               | • Packet lifetime management                                              |
| Data link     | • Retransmission policy  
|               | • Out-of-order caching policy  
|               | • Acknowledgement policy  
|               | • Flow control policy                                                     |
(a) A congested subnet. (b) A redrawn subnet, eliminates congestion and a virtual circuit from A to B.
Congestion Control in Datagram Subnets

- **Warning bit**
  - Routers use a bit in the packet’s header to signal the warning state.
  - The receiver copies the warning bit from the packet’s header to the ACK message.
  - The source, on receiving ACK with warning bit will adjust transmission rate accordingly.

- **Choke Packets**
  - The router sends choke packet directly to the source host.
Hop-by-Hop Choke Packets

(a) A choke packet that affects only the source.

(b) A choke packet that affects each hop it passes through.
Load Shedding

- When routers are so heavily loaded with packets that they can’t handle any more, they just throw them away.
- Packets can be selected randomly or by using some selection strategy.
Random Early Detection

- It is more effective to detect and prevent congestion from happening.
- Routers monitor the network load on their queues, if they predict that congestion is about to happen, they start to drop packets.
Jitter Control

Jitter: variation in packet arrival times

(a) High jitter.  (b) Low jitter.
Quality of Service

- Requirements
- Techniques for Achieving Good Quality of Service
  - Integrated Services
  - Differentiated Services
  - Label Switching and MPLS
# Requirements

How stringent the quality-of-service requirements are.

<table>
<thead>
<tr>
<th>Application</th>
<th>Reliability</th>
<th>Delay</th>
<th>Jitter</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>File transfer</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Web access</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote login</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Audio on demand</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Video on demand</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Telephony</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Videoconferencing</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Techniques for Good QoS

- Overprovisioning
- Buffering
- Traffic shaping
- The leak bucket algorithm
- Token bucket algorithm
- Resource reservation
- Admission control
- Proportional routing
- Packet scheduling
Buffering

Smoothing the output stream by buffering packets.

Packet departs source: 1 2 3 4 5 6 7 8
Packet arrives at buffer: 1 2 3 4 5 6 7 8
Packet removed from buffer:

Time in buffer: 1 2 3 4 5 6 7 8

Gap in playback:

0 5 10 15 20

Time (sec)
The Leaky Bucket Algorithm

(a) A leaky bucket with water. (b) A leaky bucket with packets.
The Token Bucket Algorithm

(a) Before.  (b) After.
The Leaky Bucket Algorithm

(a) Input to a leaky bucket. (b) Output from a leaky bucket. Output from a token bucket with capacities of (c) 250 KB, (d) 500 KB, (e) 750 KB, (f) Output from a 500KB token bucket feeding a 10-MB/sec leaky bucket.
Resource Reservation

- Packets of a flow have to follow the same route, similar to a virtual circuit
- Resources can be reserved
  - Bandwidth
  - Buffer space
  - CPU cycles (of routers)
Admission Control

An example of flow specification.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token bucket rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Token bucket size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Peak data rate</td>
<td>Bytes/sec</td>
</tr>
<tr>
<td>Minimum packet size</td>
<td>Bytes</td>
</tr>
<tr>
<td>Maximum packet size</td>
<td>Bytes</td>
</tr>
</tbody>
</table>
Packet Scheduling

(a) A router with five packets queued for line O.
(b) Finishing times for the five packets.
Integrated Services

- An architecture for streaming multimedia
- Flow-based reservation algorithms
- Aimed at both unicast and multicast application
- Main protocol: RSVP – Resource reSerVation Protocol
RSVP-The Resource reSerVation Protocol

(a) A network,  (b) The multicast spanning tree for host 1.  
(c) The multicast spanning tree for host 2.
RSVP-The Resource reSerVation Protocol (2)

(a) Host 3 requests a channel to host 1. (b) Host 3 then requests a second channel, to host 2. (c) Host 5 requests a channel to host 2.
RSVP-The Resource reSerVation Protocol (3)

- Flow-based algorithms (e.g. RSVP) have the potential to offer good quality of service

- However:
  - Require advanced setup to establish each flow
  - Maintain internal per-flow state in routers
  - Require changes to router code and involve complex router-to-router exchanges

- Very few, or almost no implementation, of RSVP
Differentiated Services

- Class-based quality of service
- Administration defines a set of service classes with corresponding forwarding rules
- Customers sign up for service class they want
- Similar to postal mail services: Express or Regular
- Examples: expedited forwarding and assured forwarding

29
Expedited Forwarding

Expedited packets experience a traffic-free network.
Assured Forwarding

A possible implementation of the data flow for assured forwarding.
Label Switching and MPLS

Transmitting a TCP segment using IP, MPLS, and PPP.

Diagram showing the headers and bits involved in the process.
Internetworking

- How Networks Differ
- How Networks Can Be Connected
- Concatenated Virtual Circuits
- Connectionless Internetworking
- Tunneling
- Internetwork Routing
- Fragmentation
Connecting Networks

A collection of interconnected networks.

Diagram of various network components including a Mainframe, SNA network, ATM network, FDDI ring, Router, Switch, Ethernet, Notebook computer, and 802.11.
## How Networks Differ

Some of the many ways networks can differ.

<table>
<thead>
<tr>
<th>Item</th>
<th>Some Possibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service offered</td>
<td>Connection oriented versus connectionless</td>
</tr>
<tr>
<td>Protocols</td>
<td>IP, IPX, SNA, ATM, MPLS, AppleTalk, etc.</td>
</tr>
<tr>
<td>Addressing</td>
<td>Flat (802) versus hierarchical (IP)</td>
</tr>
<tr>
<td>Multicasting</td>
<td>Present or absent (also broadcasting)</td>
</tr>
<tr>
<td>Packet size</td>
<td>Every network has its own maximum</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Present or absent; many different kinds</td>
</tr>
<tr>
<td>Error handling</td>
<td>Reliable, ordered, and unordered delivery</td>
</tr>
<tr>
<td>Flow control</td>
<td>Sliding window, rate control, other, or none</td>
</tr>
<tr>
<td>Congestion control</td>
<td>Leaky bucket, token bucket, RED, choke packets, etc.</td>
</tr>
<tr>
<td>Security</td>
<td>Privacy rules, encryption, etc.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Different timeouts, flow specifications, etc.</td>
</tr>
<tr>
<td>Accounting</td>
<td>By connect time, by packet, by byte, or not at all</td>
</tr>
</tbody>
</table>
How Networks Can Be Connected

(a) Two Ethernets connected by a switch.
(b) Two Ethernets connected by routers.
Concatenated Virtual Circuits

Internetworking using concatenated virtual circuits.
Connectionless Internetworking

A connectionless internet.

Packets travel individually and can take different routes.
Tunneling

Tunneling a packet from Paris to London.

Acts like a serial line

Ethernet in Paris

1.

Multilayer

router

WAN

Tunnel

Ethernet in London

1. IP packet inside payload field of the WAN packet

2.
Tunneling (2)

Tunneling a car from France to England.
Internetwork Routing

(a) An internetwork.  (b) A graph of the internetwork.
Fragmentation (1)

(a) Transparent fragmentation.
(b) Nontransparent fragmentation.
Fragmentation (2)

Fragmentation when the elementary data size is 1 byte.

(a) Original packet, containing 10 data bytes.
(b) Fragments after passing through a network with maximum packet size of 8 payload bytes plus header.
(c) Fragments after passing through a size 5 gateway.