Handouts
Please pick up one copy of the handout as you enter. Handouts are located in the front row by the aisles.

All slides from lectures will be available on the course webpage in PDF format.

Outline

Administration
Introduction
Motivation for (definition of) switching
Evolution of networks
Network elements
Layering
Switching at various layers
Types of information in a network
User characteristics/requirements
Spatial aspects
Volume aspects
Temporal aspects
Initiation
"Quality of Service"
Other aspects

Focus & form of the course

Objectives:
- Appreciate the reasons for switching†, and the relative merits of the possible switching modes.
- Understand the principles of the internal design and operation of communication switches†.
- Understand the essence of the key protocols that are used with switched networks.
- Emphasis on understanding concepts rather than nitty-gritty detail of every protocol
- Mainly descriptive, no labs

† Yet to be defined. Includes products marketed as "routers" as well as "switches".
Course outline

Administration
Introduction to Switching
Fabrics
Switching fabrics: Overview
Switching fabrics: Time-division, Space-division
Optical switching
Functions surrounding fabrics
Packet classification
Forwarding modes and buffer management
Traffic management and scheduling
Distributed switching and protocols
Bridges
Prioritisation, Virtual LANs, Virtual Private Networks
Signalling principles
SS7 signalling and public telephone networks
Early public data networks: X.25, End-to-end arguments, Frame Relay
Asynchronous Transfer Mode
MPLS
Integrated Services (RSVP) and Differentiated Services

Resources

Course presentation
- Lectures
- The lecturer
Electronic resources
- Text book
- Finding other material

Lectures

Slides will be available after the lecture on the course web page in PDF.
- “after”: Notes from last year are available on the course web page now, well before lectures & are very similar to this year’s notes.
- This year’s notes are being revised until just before the lecture, so I can’t guarantee availability before the lecture.
- “PDF”: This allows people to view them without buying Microsoft products, but sacrifices Powerpoint’s timing information for animations.
- “Video”: of lectures (audio + screen capture) will also be available online.
  Bulky ⇒ only accessible within UNSW
Slide numbers
- Use these to relate notes taken in lectures to slides printed out after lectures.
- May skip certain numbers (slides that are still “under construction”)
Questions

Hopefully your exposure to the material in this course will raise many questions, and you are encouraged to seek answers to these questions.

Questions about course subject matter:
1. Ask another student.
2. Look through the textbook to try to find an answer.
3. Ask the question in the appropriate webCT discussion forum & wait a while for someone to answer.
4. Ask the lecturer verbally during consultation time.

Questions about the course administration (e.g. your marks for the test) to the lecturer...

The lecturer

He talks too fast...

Best way to contact:
1. During consultation times
   Tuesday 5-6pm in office 341 of building G17
2. By email to tele9301admin@ee.unsw.edu.au
   include “TELE 9301” in subject

Don’t try:
- Email to other addresses
- Telephone
- Visiting office outside consultation times

These avenues simply don’t scale well enough to deal with hundreds of students p.a.

Electronic resources

Course web page: http://subjects.ee.unsw.edu.au/tele9301/
- Lecture notes
- Logistics for the mid-session test
- Recommended Reading List

webCT: http://www.webct.unsw.edu.au
- Discussion forums
- Viewing marks
- Mid-session test and preview

Resources: Textbook

Textbook:

This text is recommended, not required.

You may find this useful if you want to read a single text that touches on many (but not all) of the topics treated in this course.

1997 publication date: Fundamentals of networks that apply to switched networks have not changed substantially since the date of publication.

The author: S. Keshav
Switching-specific books

All available in the UNSW library.

Finding other material
Publications (technical papers):
Free sources: Citeseer, Google
Commercial databases: IEEE Xplore, ACM Digital Library ...
Standards:
Internet Engineering Taskforce (IETF) Requests for Comments (RFCs)
ITU recommendations
IEEE standards ...
Links: http://uluru.ee.unsw.edu.au/~tim/misc/standards.html

Terminology and inconsistency
Networking terminology tends to be inconsistent:
- Immature field
- Little formal checking of prose (unlike mathematics)
- Marketing hype
  - e.g. router vs. switch; definitions of circuit switching
Course must balance range of terminology (for familiarity) with consistency (to avoid confusion).
Pointers to several glossaries of terms at:

Lecture shorthand
Some abbreviations that you may see in lectures:

- standard mathematics: $\Rightarrow$ implies, $\equiv$
- $\exists$ there exists, $\forall$ for all
- $\uparrow\downarrow$ increases/decreases
- $\checkmark\times$ advantages/disadvantages
- c.f. compare with
- s.t. such that
- wrt with respect to
- aka: also known as
- a la: in the manner of
- b bits, B bytes, k 1000, K 1024
Assessment

70% exam
30% mid-session test using webCT April 28 2005, 6-7pm or 7-8pm
Schedule:
  Now: Sample questions online
  Week 5: Deadline to email lecturer about scheduling constraints
  Week 6: Announcement of allocations of students to slots & labs
  Week 8: Test
  Week 8: Return of marks & diagnostic feedback information
Bonus marks: Up to 5% more for participation, e.g. for:
  • attendance
  • asking thought-provoking questions
  • giving insightful answers to questions
  • suggesting test/exam questions

Education pep talk

“The mind is not a vessel to be filled, but a fire to be ignited.” – Plutarch

Question everything

Query individuals: Lecturers and authors make as many mistakes as students, if not more.
The only difference is that the grading isn’t as explicit!
Query whole fields: Networking is a developing field; if you don’t understand a concept, then it might be because it is fundamentally wrong (not you).

Don’t just accept what is, think about what should be.

“uncertainty can be a guiding light”
  • Accepting incongruous material is the easy way out
  • Try to mark it as incongruous, rather than assimilating it, and find out why. You might be able to contribute a new solution that advances the field
  • Interact with others. That’s the advantage of university over self-study using books & web sites.

Outline

Motivation for (& definition of) switching
Non-switched networks

Full mesh:
- Each terminal directly connects to every other terminal (that it communicates with)
  - Uneconomical: large number of poorly utilized connections
  - Unreliable: single path between endpoints (unless willing to forward for others)

Non-switched networks (continued)

Broadcast and select:
- Each terminal connects to a common shared medium.
- Sources broadcast information
- Destinations select appropriate information
  - Poor scalability: Shared medium is a bottleneck
    - As # nodes increases, transmission time spent arbitrating access (e.g., Ethernet collisions) also increases
  - Poor security: Information is visible to everyone
  - Poor reliability: Single failure point
  - Difficult upgrade: Requires wholesale replacement

Switched networks

Most traffic is directed and bursty (details later)

Switches
- Forward traffic only towards its destination(s)
- Multiplex traffic from multiple sources

Advantages:
- Economical for large scale
- Relatively secure
- Reliable
- Simple to upgrade ⇒ supports heterogeneity

Caveats:
- Switches cost
- Switches may get congested or “block”
- Switches introduce delay

“Switch” defined

Switch: Any device with multiple I/O ports that aims to direct input traffic only to the port(s) that leads to the destination(s).
- The traffic may have multiple destinations, e.g., for multicast traffic.

What isn’t a switch:
- A multi-port device that directs input traffic to all ports.
  - Call it a hub, combiner, etc.
- A single-port device (one input, one output).
  - Call it a filter or switching element

We’ll consider detailed definitions of types of switches (routers, bridges, etc.) later.
Outline

Evolution of networks

Communication networks of the 1970s

Master-slave relationship between dumb “terminals” and sophisticated mainframe. Terminals often directly connected to mainframe ("star" topology).

Communication networks of the 1980s

Spread of microprocessors raises the sophistication of end-user systems. Distinction between:
- clients (initiate communication, usually low-performance devices) and
- servers (respond, usually high-performance devices)
LANs deployed to interconnect clients and servers. Some LAN interconnection.

Communication networks of the 1990s

Heterogeneous terminals
Wireless links and mobility
Communication networks of the 21st C

Merger between terminals and network elements:
- **Content Distribution Networks** locate services within the network, near clients
- **Active networks**: Network elements transform payload as it propagates
- **Peer-to-peer systems** employ computers in the distribution process
- **Mobile ad-hoc networks** employ hosts to forward traffic for others (to concatenate wireless links & save power)
- **Sensor networks** low power sensor devices collect and amalgamate data.

Outline

Network elements

Names of network entities

3 Primary entities:
- **Nodes**: 
  - Hosts (aka end-systems, terminals, computers, stations)
  - Source (aka origin, transmitter)
  - Destination (aka sink, receiver)
  - Intermediate systems: Routers, switches, bridges, gateways, access points, caches, middleboxes
- **Links**: Concatenated to form paths, routes
- **Networks**: Subnetworks, internetworks, The Internet; areas, domains, regions, clouds

Node/link/network terminology comes from graph theory

† "aka" = “also known as”

Symbols used by one vendor (Cisco)

Interconnection devices

Nodes & networks

Hybrid interconnection devices
Layering of communication systems

Decompose complicated communication system into modules.
Stack one module ("layer") on top of another to refine its service to be more appropriate to the end-user ⇒ "Protocol stacks"
Layers insulate upper layers from changes below.
Layers insulate lower layers from changes above.

Layering of communication systems (continued)

Layering describes the required functionality of the system, but not how the system should be implemented.
Layered implementations can be highly inefficient (e.g. buffer double-handling).
In practice: sublayering and overlay networks produce layers ad infinitum

3 essential layers for internetworks

Example protocols

HTTP / SMTP
IP / BGP / OSPF
Ethernet / PPP
7 layer theoretical Reference Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Service/Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data link</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
</tbody>
</table>

- Application: Service to the end-user
- Presentation: Represent information, compression, encryption
- Session: Begin, end, suspend sessions, integrate connections
- Transport: End-to-end reliable transfer and flow control
- Network: End-to-end connectivity
- Data link: Point-to-point communication
- Physical: Connectors, signal form, modulation

E.g., "layer 4 switching" refers to awareness of transport protocol.

Network terminology

<table>
<thead>
<tr>
<th>Layer</th>
<th>Data unit</th>
<th>Interconnection device</th>
<th>Maximum extent (in the LAN context)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Gateway</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>Segment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Packet</td>
<td>Router</td>
<td>Internetwork or internet</td>
</tr>
<tr>
<td>Data link</td>
<td>Frame</td>
<td>Bridge</td>
<td>Catenet or Bridged LAN</td>
</tr>
<tr>
<td>Physical</td>
<td>Symbol</td>
<td>Repeater</td>
<td>Local Area Network</td>
</tr>
</tbody>
</table>

The term “switch” doesn’t appear anywhere in this table! They can appear in multiple layers.

Based on Table 1.2 of R. Seifert: The Switch Book, p. 60

Outline

- Switching at various layers
  - Lower layer switching
  - Higher layer switching
    - Transport layer switching
    - Application layer switching
  - Most common layers for switching

Lower Layer Switching

- Physical: all-optical networks: Wavelength Division Multiplexing, MicroElectroMechanical Systems (MEMS)
- Data link: bridging
- Network: routing
Higher-layer (4+) switching

The switches that we’ve considered so far implement all functions of the layers that they use for switching:
- Layer 2 (link): MAC & framing
- Layer 3 (network): routing

Another type of switch (common at higher layers) only implements a subset (possibly null) of the functions of a layer, but is influenced by the information sent by that layer. i.e. it depends on what protocol is used at that layer, but it doesn’t implement all of the functions of that protocol.

Transport layer switching

Strict interpretation: Switching above network layer processing. Switching between processes, e.g. for load balancing on a web server: might construct what clients perceive as a singular “server” by placing a switch between the Internet & a server farm.

might use the source port number to determine which machine receives the request: odd → machine 1, even → machine 2

(Strictly, you could argue that end-systems implement a form of layer 4 switching because they forward segments to the appropriate process, as indicated by their port numbers.)

Loose interpretation: Switching below the transport layer that depends on transport layer fields, e.g. Network layer that gives telnet (TCP port 23) priority over FTP data (TCP port 20)

Application layer switching

E.g. consider a web service, handling HTTP GET requests
1. Could use cookies† (identifiers included in requests) that identify users to direct them to a specific machine (helps in providing consistent state between consecutive requests)
2. Could direct GET requests for different information to specialised machines (less content each ⇒ higher cache hit rates etc):
   - image requests (file with .JPG extension) to one machine
   - HTTPS to machine with crypto hardware
   - cgi-bin to another
   - ...

† No need to understand these in depth for TELE 9301

Outline

Types of information in a network
Types of information in a network

**Payload**: Content that end-users want to exchange
(the load for which users are willing to pay to be carried)

**Control information**: Specifies how end-users want to exchange payload
e.g. destination address and specify service requirements (e.g. low delay)

**Overheads**: Introduced by the communication system to provide communication.
Examples:
- protocol headers, congestion control signals, topology updates for routing
- source address – e.g. for demultiplexing, replies and error messages, charging, flow identification

Encapsulation

Payload from the application tends to be progressively encapsulated as it descends the protocol stack. Reverse on ascent.

“Ethernet” frame format

**Type encapsulation** – used for IP, IPX

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Type</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6B</td>
<td>6B</td>
<td>6B</td>
<td>2B</td>
<td>46–1500B</td>
<td>4B</td>
</tr>
</tbody>
</table>

**Overhead** | **Control** | **Payload**

Transmission order: ⇒

“Ethernet” frame format

**Length encapsulation** – used for Appletalk, NetBIOS

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination Address</th>
<th>Source Address</th>
<th>Length</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6B</td>
<td>6B</td>
<td>6B</td>
<td>2B</td>
<td>46–1500B</td>
<td>4B</td>
</tr>
</tbody>
</table>

DA in header s.t. can be processed while waiting for remainder.
We’ll consider addressing in detail later, in the context of packet classification.
Type/protocol in header for distribution to appropriate process
CRC in trailer s.t. can be generated as remainder is transmitted
MAC requires minimum Data+Pad of 46B (short frames are “runts”)
Outline

User characteristics/requirements

Spatial aspects
- Directivity
- Spatial distribution

Volume aspects
- Symmetry of data flow

Temporal aspects
- Variability of data flow
- Duration of transfer

Initiation
- "Quality of Service"
  - Timeliness
  - Reliability

Other aspects
- Security, privacy
- Economy, accountability

“Flows”

Flows, conversations (Keshav), streams, sessions, connections, calls, ...
All describe a sequence of data units being sent between common endpoints
Often using common service type, though sometimes may have sub-flows, e.g., lecture consists of flow of PPT slides + flow of audio

Reasons for flows:
- Segmentation of large data, e.g., file >> 1500 B limit for Ethernet
- Source progressively produces information, e.g., telephone call
- Repeated interactions with same node, e.g., with a web server: connect, send request, download page, think, repeat, disconnect

How to determine when a flow ends?
- Connection-oriented: Explicit setup and release mark beginning and end
- Connectionless: Timeout after prolonged inactivity

Directivity of traffic flow

<table>
<thead>
<tr>
<th>Name</th>
<th>From</th>
<th>To</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>unicast</td>
<td>one</td>
<td>one</td>
<td>most</td>
</tr>
<tr>
<td>anycast</td>
<td>one</td>
<td>any</td>
<td>when multiple targets provide identical service, e.g., telephone operators</td>
</tr>
<tr>
<td>multicast</td>
<td>one</td>
<td>many</td>
<td>distribution, e.g., advertising, lectures</td>
</tr>
<tr>
<td>broadcast</td>
<td>one</td>
<td>all</td>
<td>used for multicast apps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>broadcast itself is never really justified</td>
</tr>
<tr>
<td>concast</td>
<td>many</td>
<td>one</td>
<td>gathering information, e.g., monitoring weather sensors, multi-source file 1x</td>
</tr>
<tr>
<td>Multis-</td>
<td>many</td>
<td>many</td>
<td>bidirectional distribution, e.g., videoconference</td>
</tr>
</tbody>
</table>

Importance:
- Multicast allows sources to heavily load switches, affecting performance & favoring shared-media switches.
- Anycast reduces chances of switch blocking
Constructing one type of flow from another

Multicast by iterated unicast
Burdens the source and links
Distributed expansion can increase throughput

Multiaccess from multiple multicast
Requires many identifiers within the network

Spatial distribution

Traditionally, networks have been designed assuming "80/20" or "90/10" rules, suggesting that of the traffic originating in a subnetwork:
80% is destined to other nodes in that subnetwork
20% is destined to nodes in other networks

Justification: Originated in telephony, but perpetuated through folklore (e.g. analogous to Pareto distribution)

Actual numbers depend greatly on the technology, e.g.
- Phone network:
  - Rarely call someone in an adjacent office
  - Frequently call colleague on another floor of building and others in same city
  - Cost & time zones inhibit international calls
- Web browsing:
  - Little care for location; origin sources might be uniformly distributed around the world (though may have local caches)

Hard to generalise, but worth considering – some traffic will be local.

Symmetry of data flow

Most flows are asymmetrical:
- Short requests to server elicit long replies
- Participants in group interactions are usually silent
- At periphery of network, more traffic propagates towards the edges ("downstream") than towards the core ("upstream").

UNSW stats from 2004: campus: 40Mb/s outbound, 60Mb/s inbound
- Acknowledgements often can’t be piggybacked with payload ⇒ large number of short packets

Important exceptions:
- Interactive media – telephony, videoconference, etc
- Modern file sharing – discourage freeloaders; encourage content providers

Outline

Temporal aspects
Variability of data flow

Network traffic tends to be bursty:
- Users download information, pause to think, download more
- Video and other streaming media that can be compressed & degree of compression depends on content.

Strong motivation for switching:
- Multiple users sharing a channel can exploit each other’s idleness ⇒ higher end-to-end throughput from same capacity channel.

Burstiness can be smoothed by buffering

More consequences later on “Statistical multiplexing” slide
Multiplexing points affect burstiness

Predictability of bandwidth

“Constant Bit Rate (CBR): for sources with continuous traffic or requiring guaranteed bandwidth (uncompressed voice, video)
Variable Bit Rate (VBR): for sources with some traffic variation and ability to tolerate some data loss (compressed voice, video)
Available Bit Rate (ABR): for bursty traffic sources requiring low loss and ability to adapt rate based on feedback
Unspecified Bit Rate (UBR): for bursty traffic requiring just best effort cell delivery with no guarantees”

Duration/volume of traffic flow

Transactions tend to be short: request/response
Interactions tend to be long
Duration of transfer determines significance of signaling overheads
e.g. 80ms RTT insignificant compared to voice call of minutes, but appreciable compared to transaction of single packet
Often can’t predict duration/volume of transfer before it happens
Important exception: file transfers $\rightarrow$ scheduling