An Overview of This Lecture

- Handout 1: An Introduction of Computer Networks and the Internet
- Handout 2: Network layer (routing, addressing, forwarding, ARP, ICMP, NAT, IPv6, etc.)
- Handout 3: Transport layer (principles; TCP flow control, retransmission, congestion control; UDP, etc)
- Handout 4: Quality of Service (concepts and approaches: IntServ, RSVP, DiffServ, etc.)
- Handout 5: Mobile Internet

Credits:
- James Kurose, Keith Ross, Computer Networking (2nd Ed.), Addison-Wesley, 2002
- Nick McKeown, Stanford University
- Achim Schillings, Freie Universität Berlin

Outline

What is Quality of Service (QoS)?
- Principles and Mechanisms of QoS
- Proposed Techniques for QoS in the Internet
  - ReSource Reservation Protocol (RSVP)
  - Integrated Services
  - Differentiated Services

What is Quality of Service?

Example: Web transfer chain

- User computer

QoS network provides application with level of performance needed for application to function.
Why QoS?

1. Limited Resource

- QoS is an issue due to *limited resource* problem.
- If resources are unlimited, no "quality" problem.
- Got to consider in light of some predictions of bandwidth becomes "unlimited".

2. Variety of Services

- Problem of QoS simplifies under single objectives: single service.
  - e.g. - telephone system -- quality problem was not an issue.
  - e.g. -- buttt. Cellular phone -- quality is an issue.

Why QoS (cont)

- Problem of QoS magnifies in light of multiple objectives: multiple services.
- Two quality dimensions:
  - Time constraints (timely service)
  - Precision
- Two traffic characteristics
  - Quantity (rate)
  - Burstiness

Services

- Voice: Timely - high
  Precision - low
  Volume - medium
  Burstiness - high
- Email: Timely - low
  Precision - high
  Volume - variable (low - huge)
  Burstiness - might be high

Services (cont)

- Web: Timely - medium
  Precision - high
  Volume - medium
  Burstiness - high
- IRC: Timely - medium-high
  Precision - high
  Volume - small
  Burstiness - small
- FTP: Timely - low
  Precision - high
  Volume - high
  Burstiness - depends
**Effects of Variety**

- Makes mechanisms complex
- Can benefit from sophistication
  \[\Rightarrow\] can get good utilization!

**Outline**

- What is Quality of Service (QoS)?
  \[\Rightarrow\] Principles and Mechanisms of QoS
- Proposed Techniques for QoS in the Internet
  - ReSource Reservation Protocol (RSVP)
  - Integrated Services
  - Differentiated Services

**Improving QoS in IP Networks**

- Thus far: “making the best of best effort”
- Future: next generation Internet with QoS guarantees
  - RSVP: signaling for resource reservations
  - Differentiated Services: differential guarantees
  - Integrated Services: firm guarantees
- simple model for sharing and congestion studies:

**Principles for QoS Guarantees**

- Example: 1Mbps iP phone, FTP share 1.5 Mbps link.
  - bursts of FTP can congest router, cause audio loss
  - want to give priority to audio over FTP

- Principle 1
  packet marking/classifying needed for router to distinguish between different classes and new router policy to treat packets accordingly

**Principles for QoS Guarantees (more)**

- what if applications misbehave (audio sends higher than declared rate)
  - policing: force source adherence to bandwidth allocations
- marking and policing at network edge:
  - similar to ATM UNI (User Network Interface)

- Principle 2
  provide protection (aro-ban) for one class from others: shaping and policing

- Principle 3
  While providing isolation, it is desirable to use resources as efficiently as possible: scheduling

**Principles for QoS Guarantees (more)**

- Allocating fixed (non-shareable) bandwidth to flow: inefficient use of bandwidth if flows doesn’t use its allocation
Principles for QOS Guarantees (more)

• Basic fact of life: can not support traffic demands beyond link capacity

1 Mbps
R1 1 Mbps
R2
H1
H2
H3
H4

Principle 4
Call Admission: flow declared its needs, network may black call (e.g., busy signal) if it cannot meet needs.

Summary of QoS Principles

• Per-session
  – Call setup, call admission and resource reservation
    • "Can the network accept the call and provide the QoS?"

• Per-packet
  – Packet Classification: "What flow does this packet belong to, and when should I send it?"
  – Shaping: "Am I keeping my side of the contract?"
  – Policing: "Did the user keep his/her side of the contract?"
  – Packet Scheduling: "Sending the packet at the right time."

Let’s next look at mechanisms for achieving this ...

Scheduling And Policing Mechanisms

• scheduling: choose next packet to send on link
  • FIFO (first in first out) scheduling: send in order of arrival to queue
    – real-world example?
    – discard policy: if packet arrives to full queue: who to discard?
      • Tail drop: drop arriving packet
      • priority: drop/remove on priority basis
      • random: drop/remove randomly

• Scheduling Policies: more
  • Priority scheduling: transmit highest priority queued packet
  • multiple classes, with different priorities
    – class may depend on marking or other header info, e.g. IP source/dest, port numbers, etc...
    – Real-world example?

Scheduling Policies: still more

• round robin scheduling:
  • multiple classes
  • cyclically scan class queues, serving one from each class (if available)
  • real world example?
Policing Mechanisms

- **Goal:** limit traffic to not exceed declared parameters
- Three common-used criteria:
  - *(Long term)* Average Rate: how many pkts can be sent per unit time (in the long run)
    - crucial question: what is the interval length: 100 packets per sec or 6500 packets per min have same average!
  - Peak Rate: e.g., 6000 pkts per min. (ppm) avg.; 1500 ppm peak rate
  - *(Max.)* Burst Size: max. number of pkts sent consecutively (with no intervening idle)

Policing Mechanisms (more)

- token bucket, WFQ combine to provide guaranteed upper bound on delay, i.e., *QoS guarantee*

Resource Reservation: RSVP

- **RSVP** is a protocol for establishing a guaranteed QoS path between a sender and receiver(s).
- RSVP establishes end-to-end reservations over a connectionless network.
- RSVP is robust when routers/links fail: traffic is re-routed and new reservations are established.
- RSVP is receiver-initiated and so is designed with multicast in mind.

Outline

- What is Quality of Service (QoS)?
- Principles and Mechanisms of QoS
- Proposed Techniques for QoS in the Internet
  - ReSource Reservation Protocol (RSVP)
    - Integrated Services
    - Differentiated Services

Resource Reservation: RSVP

The network needs to know the TSpec, the RSpec and the Path followed by packets.
- The TSpec (specification of the transmitted traffic) is only known by the source.
- The Path is only known by the network.
- The RSpec (specification of what the receiver would like to receive).
Resource Reservation: RSVP

So, the sender periodically sends the Tspec to the whole multicast group (“PATH messages”).
- The network learns the Path taken by packets in the multicast group.
- The receiver/network learns the TSpec.

To initiate a new reservation, a receiver sends messages to reserve resources “up” the multicast tree (“RESV messages”).
- The routers forward RESV messages towards the source.
- The routers determine if the reservation can be fulfilled.
- If necessary/possible, the routers merge the requests from different receivers.

Establishing a reservation
1: The multicast group is established

Establishing a reservation
2: RSVP Path messages sent by source(s)

Establishing a reservation
3: RSVP RESV messages sent by receiver(s)

Establishing a reservation
Merging RESV messages

Examples:
1. Router receives RESVs from two receivers, A and B, asking for 100ms delay and 50ms delay respectively. Router passes up request for 50ms.
2. Router receives RESVs for a audio teleconference call with 100 participants requesting 1.5Mb/s each. The tree needs support only 1.5Mb/s total data rate.

RSVP supports many styles of RESV merging.
Outline

- What is Quality of Service (QoS)?
- Principles and Mechanisms of QoS
- Proposed Techniques for QoS in the Internet
  - ReSource Reservation Protocol (RSVP)
  - Integrated Services
  - Differentiated Services

IETF Integrated Services

- architecture for providing QoS guarantees in IP networks for individual application sessions
- resource reservation: routers maintain state info (a la VC) of allocated resources, QoS req's
- admit/deny new call setup requests:

Question: can newly arriving flow be admitted with performance guarantees while not violating QoS guarantees made to already admitted flows?

Intserv: QoS guarantee scenario

- Resource reservation
  - call setup, signaling (RSVP)
  - traffic, QoS declaration
  - per-element admission control
  - QoS-sensitive scheduling (e.g., WFQ)

Call Admission

Arriving session must:
- declare its QoS requirement
  - R-spec: defines the QoS being requested
  - T-spec: defines traffic characteristics
- characterize traffic it will send into network
- signaling protocol: needed to carry R-spec and T-spec to routers (where reservation is required)
  - RSVP

Intserv QoS: Service models [rfc2211, rfc2212]

Guaranteed service:
- worst case traffic arrival: leaky-bucket-policed source
- simple (mathematically provable) bound on delay
  [Parikh 1992, Cruz 1988]

Controlled load service:
- "a quality of service closely approximating the QoS that same flow would receive from an unloaded network element."

Outline

- What is Quality of Service (QoS)?
- Principles and Mechanisms of QoS
- Proposed Techniques for QoS in the Internet
  - ReSource Reservation Protocol (RSVP)
  - Integrated Services
  - Differentiated Services
IETF Differentiated Services

Concerns with Intserv:
- **Scalability**: signaling, maintaining per-flow router state difficult with large number of flows
- **Flexible Service Models**: Intserv has only two classes. Also want “qualitative” service classes
  - "behaves like a wire"
  - relative service distinction: Platinum, Gold, Silver

Diffserv approach:
- simple functions in network core, relatively complex functions at edge routers (or hosts)
- Don’t define define service classes, provide functional components to build service classes

Differentiated Services

- Instead of *per-flow queues and rates*, uses *per-class queues and rates*.
- Much simpler to implement, introduce and manage.
- But… means that many flows share the same queue, state and capacity. So, it is like a simple approximation to Integrated Services.

Diffserv Architecture

- **Edge router**: per-flow traffic management
  - mark packets as in-profile and out-profile
- **Core router**: per-class traffic management
  - buffering and scheduling based on marking at edge
  - preference given to in-profile packets
  - Assured Forwarding

Edge-router Packet Marking

- profile: pre-negotiated rate A, bucket size B
- packet marking at edge based on *per-flow profile*

Possible usage of marking:
- class-based marking: packets of different classes marked differently
- intra-class marking: conforming portion of flow marked differently than non-conforming one

Classification and Conditioning

- Packet is marked in the Type of Service (TOS) in IPv4, and Traffic Class in IPv6
- 6 bits used for Differentiated Service Code Point (DSCP) and determine PHB that the packet will receive
- 2 bits are currently unused
Forwarding (PHB)

• PHB result in a different observable (measurable) forwarding performance behavior
• PHB does not specify what mechanisms to use to ensure required PHB performance behavior
• Examples:
  – Class A gets x% of outgoing link bandwidth over time intervals of a specified length
  – Class A packets leave first before packets from class B

Quality of Service in the Internet

Some Interesting Questions

• How can we implement per-flow buffering and scheduling when the number of flows is large?
• How can we encourage/force users to ask for only the resources they need?
• How can we bill users for the service they receive?

Mobile Internet

(Handout 5)
Computers for the next decades?
Computers are integrated
- small, cheap, portable, replaceable - no more separate devices
Technology is in the background
- computer are aware of their environment and adapt (“location awareness”)
- computer recognize the location of the user and react appropriately
  (e.g., call forwarding, fax forwarding, “context awareness”)
Advances in technology
- more computing power in smaller devices
- flat, lightweight displays with low power consumption
- new user interfaces due to small dimensions
- more bandwidth per cubic meter
- multiple wireless interfaces: wireless LANs, wireless WANs, regional
- wireless telecommunication networks etc. (“overlay networks”)

Mobile communication
- Two aspects of mobility:
  - user mobility: users communicate (wireless) “anytime, anywhere, with anyone”
  - device portability: devices can be connected anytime, anywhere to the network
- Wireless vs. mobile
  Examples
  - stationary computer
  - notebook in a hotel
- wireless LANs in historic buildings
- Personal Digital Assistant (PDA)
- The demand for mobile communication creates the need for integration of wireless networks into existing fixed networks:
  - local area networks: standardization of IEEE 802.11, ETSI (HIPERLAN)
  - Internet: Mobile IP extension of the internet protocol IP
  - wide area networks: e.g., internetworking of GSM and ISDN

Outline
- Introduction
  - Mobile communication
  Mobile applications
- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
  - Micro-mobility solutions, e.g.:
    - Hierarchical Mobile IP
    - Cellular IP
  - Transport-layer mobility, eg.:
    - I-TCP

Applications I
- Vehicles
  - transmission of news, road condition, weather, music via DAB
  - personal communication using GSM
  - position via GPS
  - local ad-hoc network with vehicles close-by to prevent accidents, guidance system, redundancy
  - vehicle data (e.g., from busses, high-speed trains) can be transmitted in advance for maintenance
- Emergencies
  - early transmission of patient data to the hospital, current status, first diagnosis
  - replacement of a fixed infrastructure in case of earthquakes, hurricanes, fire etc.
  - crisis, war, …

Applications II
- Travelling salesmen
  - direct access to customer files stored in a central location
  - consistent databases for all agents
  - mobile office
- Replacement of fixed networks
  - remote sensors, e.g., weather, earth activities
  - flexibility for trade shows
  - LANs in historic buildings
- Entertainment, education, …
  - outdoor Internet access
  - intelligent travel guide with up-to-date location dependent information
  - ad-hoc networks for multi user games
Mobile devices

- PDA
  - simple graphical displays
  - character recognition
  - simplified WWW
- Laptop
  - fully functional
  - standard applications

- Mobile phones
  - voice, data
  - simple text displays

- Palmtop
  - tiny keyboard
  - simple versions of standard applications

- Sensors, embedded controllers

World Wide Web and mobility

- Protocol (HTTP, Hypertext Transfer Protocol) and language (HTML, Hypertext Markup Language) of the Web have not been designed for mobile applications and mobile devices, thus creating many problems.
- Typical transfer sizes:
  - HTTP request: 100-350 bytes
  - responses avg. <10 kbyte, header 160 byte, GIF 4.1kbyte, JPEG 12.9 kbyte, HTML 5.6 kbyte
  - but also many large files that cannot be ignored.
- The Web is not file system:
  - Web pages are not simple files to download
  - static and dynamic content, interaction with servers via forms, content transformation, push technologies etc.
  - many hypertext, automatic loading and reloading, redirecting
  - a single disk might have big consequences

Web pages ignore the heterogeneity of end-systems!
- e.g. without additional mechanisms, large high-resolution pictures would be transferred to a mobile phone with a low-resolution display causing high costs.

Solutions: application gateways, enhanced servers/browsers, proxies... e.g., WAP

WAP – Wireless Application Protocol

Outline

- Introduction
  - Mobile communication
  - Mobile applications

- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
  - Micro-mobility solutions, eg.:• Hierarchical Mobile IP
  • Cellular IP
  • Transport-layer mobility, eg.:• T-CP

What is mobility?

- spectrum of mobility, from the network perspective:

  low mobility
  
  mobile user, using same access point
  high mobility
  
  mobile user, connecting/ disconnecting from network using DHCP
  mobile user, pasing through multiple access points while maintaining ongoing connection (like cell phone)

Mobility: Vocabulary

- Home network: Permanent “home” of mobile (e.g., 269.19.42.0/4)
- Home agent: entry that will perform mobility functions on behalf of mobile, when mobile is remote
- Mobile: permanently attached to a fixed network
- Mobile network: mobile’s current network
- Mobile IP address: address in mobile network, can always be used to reach mobile (e.g., 269.19.42.38b
- Public home address: temporary (w/o assigned name)
- Permanent address: address in home network, can always be used to reach mobile (e.g., 269.19.42.0/4)

- WPML: wireless protocol model language
Mobility: more vocabulary

- Permanent address: remains constant (e.g., 209.201.10.26)
- Visited network: network in which mobile currently resides (e.g., 193.201.2.4)
- Correspondent wants to communicate with mobile
- Correspondent wants to communicate with mobile
- Home agent: entity in visited network that performs mobility functions on behalf of mobile

How do you contact a mobile friend:

Consider friend frequently changing addresses, how do you find her?
- search all phone books?
- call her parents?
- expect her to let you know where he/she is?

Mobility: approaches

- Let routing handle it: routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- Let end-systems handle it:
  - indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - direct routing: correspondent gets foreign address of mobile, sends directly to mobile

Mobility: registration

End result:
- Foreign agent knows about mobile
- Home agent knows location of mobile

Mobility via Indirect Routing

- Correspondent address a packets using home address of mobile
- Home agent intercepts packets, forwards to foreign agent
- Foreign agent receives packets, forwards to mobile
- Mobile replies directly to correspondent
Indirect Routing: comments

- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is transparent to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network

Indirect Routing: moving between networks

- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- Mobility, changing foreign networks
  transparent: on going connections can be maintained!

Mobility via Direct Routing: comments

- overcome triangle routing problem
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - What happens if mobile changes networks?

Outline

- Introduction
  - Mobile communication
  - Mobile applications
- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
    - Micro-mobility solutions, eg.:
      - Hierarchical Mobile IP
      - Cellular IP
    - Transport-layer mobility, eg.:
      - iTCP
Mobile IP

- RFC 3220
- has many features we’ve seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - agent discovery
  - registration with home agent
  - indirect routing of datagrams

Mobile IP

- Both ends of a TCP session (connection) need to keep the same IP address for the life of the session.
  - home address, used for end-to-end communication
- IP needs to change the IP address when a network node moves to a new place in the network.
  - care-of-address, used for routing

Mobile IP considers the mobility problem as a routing problem
- managing a bonding – that is, a dynamic tunnel between a care-of address and a home address
- Of course, there is a lot more to it than that!

Mobile IP: agent discovery

- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (type field = 9)

Mobile IP: registration example

Data Transfer to the Mobile System

1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data Transfer from the Mobile System

1. Sender sends to the IP address of the receiver as usual, FA works as default router
Mobile IPv6 protocol overview

- Advertisement from local router contains routing prefix
- Seamless Roaming: mobile node always uses home address
- Address autoconfiguration for care-of address
- Binding Updates sent to home agent & correspondent nodes
  - (home address, care-of address, binding lifetime)
- Mobile Node "always on" by way of home agent

Address Autoconfiguration

- Stateless Address Autoconfiguration
  - First, use routing prefix — FE80::/64 for link-local address
  - Then, construct Link-Local Address — Global Address by changing link-local prefix to advertised routing prefix

<table>
<thead>
<tr>
<th>Routing Prefix</th>
<th>MAC address</th>
</tr>
</thead>
</table>

- A new care-of address on every link
- Stateful Autoconfiguration (DHCPv6)
  - Movement Detection
    - by monitoring advertisement of new prefix
    - by hints from physical layer and/or lower-level protocol
    - by monitoring TCP acknowledgements, etc.

Destination Options used by Mobile IPv6

- Destination Options much better than IPv4 options
- Binding Updates sent in data packets to Correspondent Nodes
  - allows optimal routing with minimal packet overhead
  - SHOULD be supported by all IPv6 network nodes
- Binding Update also sent (typically with no data) to Home Agent
  - replaces IPv4 Registration Request messages
- Home Address option
  - better interaction with ingress filtering
  - MUST be supported by all IPv6 network nodes
- Binding Acknowledgement Destination Option
  - replaces Registration Reply

Problems with Mobile IP

- Ingress filtering for packets with topologically incorrect IP address
- Indirect routing increases delay and data overhead
- Signalling latency due to distance between FA and HA
- No user mobility concept
- Vertical handover
  - Open questions regarding handover policies
  - No differentiation between mobility types
    - "One scheme fits all"

Some of the problems have been addressed by MIP extensions
(e.g. route optimization)

Hierarchical Mobile IPv4

- Signaling delay in Mobile IP may be high
- FA functionality is distributed between multiple FA
- Improved support for local mobility
- Advantages
  - Rerouting node close to mobile
  - Reduced signaling overhead

Outline

- Introduction
  - Mobile communication
  - Mobile applications
- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
  - Micro-mobility solutions, eg.: Hierarchical Mobile IP
    - Cellular IP
    - Transport-layer mobility, eg.: I-TCIP
Hierarchical Mobile IPv4

- Advertise multiple foreign agents in the agent advertisements (e.g., IP addresses of FAs 4,2,1 for FA1)
- Mobile host registers with home agent using the address of FA1
- A packet for mobile host tunneled to FA1, then down to each FA

Hierarchical Mobile IPv6

- New entity: Mobility Access Point (MAP)
- Mobile host uses MAP address as alternate care-of-address and MAP receives and tunnels packets to mobile host's current address
- Mobile host can register with more than one MAP simultaneously and use each map address for a specific group of correspondent hosts
- Mobile Host sends Binding Update to MAP then to Home agent with alternate CoA
- MAP can keep simultaneous bindings and bicast packets to mobile host on both paths when mobile host does handover

Cellular IP

- Motivation
  - Mobile IP results in high latency and high control overhead for local mobility
  - Scaling
- Addressing
  - Stand-alone Cellular IP: Unique identifier
  - Unique identifier does not change as long mobile remains in Cellular IP access network
- Infrastructure
  - Base stations and router „Cellular IP-enabled“
- Goals:
  - No address translation in Cellular IP domain
  - hides local mobility from HA
  - Differentiation between active and idle users

Outline

- Introduction
  - Mobile communication
  - Mobile applications
- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
  - Micro-mobility solutions, eg.:
    - Hierarchical Mobile IP
    - Cellular IP
  - Transport-layer mobility, eg.:
    - fTCP

Cellular IP Local Mobility

- X from E
- X from C
- X from B

- X from E
Cellular IP Local Mobility

- Cellular IP nodes keep:
  - Paging cache and Routing cache:
    - IP address, interface, MAC address, expiration time, timestamp
    - where interface & MAC address correspond to downlink neighbor towards mobile host
- Uplink routing for packets from mobile host follows uplink neighbors which are usually manually set up, every packet goes to gateway
- Gateway sends beacons periodically
- Downlink routing for packets to mobile host follow route cache
- Mobile host may send ICMP Route-update message when active to update route cache
- Idle mobile host sends ICMP Paging update message every 3min

HAWAIL: Handover (Forwarding Path Setup)

Outline

- Introduction
  - Mobile communication
  - Mobile applications
- Mobility support for the Internet
  - Mobile IP and Mobile IPv6
  - Micro-mobility solutions, eg:
    - Hierarchical Mobile IP
    - Cellular IP
  - Transport-layer mobility, eg:
    - I-TCP

Or alternative: How about adapting TCP-mechanisms to deal with mobility?

- TCP assumes congestion if packets are dropped
  - Typically wrong in wireless networks, here we often have packet loss due to transmission errors
  - Furthermore, mobility itself can cause packet loss, e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible
- The performance of an unchanged TCP degrades severely
  - However, TCP cannot be changed fundamentally due to the large base of installation in the fixed network, TCP for mobility has to remain compatible
  - The basic TCP mechanisms keep the whole Internet together
Indirect TCP

- Indirect TCP (I-TCP) segments the connection
  - no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
  - optimized TCP protocol for mobile hosts
  - splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
  - hosts in the fixed part of the net do not notice the characteristics of the wireless part

Course Review

- Basic Concepts of Computer Networks and the Internet
- Network layer: routing, addressing, forwarding, DNS, ARP, ICMP, NAT, IPv6
- Transport layer: TCP mechanisms, UDP, SCTP
- Quality of Service: concepts and mechanisms, IntServ, RSVP, DiffServ
- Mobile Internet: trends and applications, Mobile IP and micro-mobility, transport layer mobility

What’s beyond?

- To be studied e.g., in advanced courses
  - Application layer: http, telnet, SMTP, RTP…
  - Middleware: event/object/msg-oriented, Cronus, TAO, MOM…
  - Peer-to-peer communications: Napster, Gnutella…
  - Network security: AAA, IPsec, TLS…
  - Network management: SNMP, MIB…