

15-441

Computer Networks

Review
May 3, 2006

Dave Eckhardt

Peter Steenkiste

Synchronization

P3 “interviews”

- We will focus on groups with issues
- If you don't hear from us, that's good news

Don't forget about

- Homework 4 – due Friday, no extensions
- Lab assignment
 - Please try logging in *early*

Exam

- Closed-book, closed-notes
- See final exam schedule for official time & place

Synchronization

Faculty evaluation

- Did you get the reminder e-mails?

About today's "review"

- More "reminders" than "course outline"
 - Un-mentioned topic implies "text & lectures straightforward"
- Reading *some* of the textbook is advisable!
 - Web site "reading list" has been updated

“Conceptual” Topics

We *could* ask a question...

- ...we would give you guidance/refresh your memory

Examples

- ZigBee
- BitTorrent
- PGP

“Core” Topics

We expect solid mastery

Examples

- **IP, TCP, routing (you built these!)**
- **Layer responsibilities, challenges, techniques**
- **Key problems, how to address them, parameters, relationships**
 - **Latency, loss, corruption, congestion**
- **Key concepts**
 - **Address spaces (including mapping), connection**
- **Key approaches**
 - **Trees/graphs, backoff, fragmentation, multiplexing**

Core “Mid-term” Concepts

Stacks, Layering

Socket programming

Experience: what's a protocol?

Link-layer issues

- Medium Access Control
- Interconnection: switching, bridging

IP

- Addressing, forwarding

Routers and routing

- Three approaches for two domains

“More IP”

NAT

- What, why

Tunneling

- What, why

IPv6

- Goals, techniques

Network management/monitoring

IP Multicast

- Recall: first-cut design, not widely deployed
- Concepts: service model, scope, membership, routing

“Putting Things Together”

Three names for your PC

- What/who is a name for?
- Other questions about names

Two resolution (mapping) protocols

- DNS, ARP
- Same conceptual job, different approaches

Turning on (DHCP)

Virtual Circuits, ATM

Packet switching versus circuit switching

- What (analogy: letter vs. phone call)
- Why (tradeoffs)?

“Real” versus “virtual” circuits

- Nature of v-c forwarding

ATM

- Goals, origins, layers
- Per-hop addressing and label swapping
- Virtual circuits vs. virtual paths
- Adaptation layers, IP over ATM, LAN over ATM
- Traffic classes, signalling, fair share

SONET

“Industrial strength” network

- Strong support for legacy telco voice connections
- Integration of high-speed data traffic

Framing, multiplexing, add/drop

Rings and healing

PoS

MPLS

“IP Switching” over ATM

- **“Cache” multiple hops of next-hop lookup via v-c setup**
 - **For “thin flows” or aggregates**
- **Acceleration/fall-back**

Generalization to “tag switching”

- **Tag stacking concept**
- **MPLS realization**
 - **Per-flow QoS (in theory)**
 - **Policy-based “traffic engineering” (in practice)**

Transport/UDP/TCP

Internet architecture history & principles

- Why do we have TCP and UDP?
- Hourglass model

What's a transport protocol?

- Layering, duties
- UDP as a simple example
- UDP as a key Internet protocol

The “byte stream” model

TCP

- Setup, transmission, teardown
- Nagle, sockets

More TCP

Connection management details

- More setup
- Teardown

Reliability and Error Control

- Network threats
- Techniques – Acknowledgement and timeouts
- Stop&wait versus sliding-window
- Acknowledgement styles
- Sizes (sequence numbers; windows)
- RTT estimation
- Flow control
- TCP transmission flow of events

Wireless/Mobility

Background

- What's special about wireless?
 - Threats and responses
 - Medium Access Control (again)
 - » Problems, RTS/CTS
 - Routing isn't so easy

802.11

- People will expect you to know something about this

Not 802.11

- Cellular, WiMax, Bluetooth, ZigBee
 - Remember goals/concepts/outcomes
 - Not responsible for specific numbers (b/s, Ghz)

Congestion Control

The Problem

- Not an end-to-end problem (flow control) – “middle problem”
- Buffering, congestion, congestion collapse
- Open-loop, closed-loop
- Endpoint contributions – adaptation

Fairness models, WFQ

Congestion control examples

- DECbit, ATM, packet-pair probing
- TCP (intro)
 - “Slow” start, packet-pacing, “fast retransmit”

TCP Congestion Control

Implementation

Hard questions

- Multiple/many losses per window

TCP flavors

- Tahoe, Reno, NewReno

Deciding when to send a packet

Why TCP-style congestion control works

Issues – fairness, performance

RED

“Other Transports”

TCP options/extensions

- Window scaling
- ECN – marking, loopback

TCP conformance (aka “TCP-friendly”) notion

RPC

- Reliability, flow/congestion control, semantics

Streaming audio/video

- (requirements)

Quality of Service

Performance vs. Satisfaction

- Applications have their own mapping functions

QoS is “desirable unfairness”

Key components

- Admission control
- Traffic classification/shaping/enforcement
 - “Token bucket” concept
- Scheduling

ATM model, Internet models

RSVP, COPS

Multimedia

Application classes

- Stored, 1-way, interactive
 - How characteristics help/constrain

Challenges

- Delay/througput/jitter/loss

Encoding – JPEG, MPEG, audio

- Forward Error Correction, iinterleaving, multi-rate streams

VoIP, video

RTP, RTCP, H.323

- Understand “shape” of problems, solutions

Peer-to-Peer

Styles

- File “sharing”, File distribution, Streaming

Challenges

- Scalability, content description, content location

Architectures

- Central index, flooding, overlays

Components: Join/Publish/Search/Fetch

Examples

- Distributed Hash Tables, BitTorrent
- End-System Multicast

- 20 - ▪ Be sure to compare vs. original “IP Multicast”

Security – Technology

Threats and responses

- Impersonation, secrecy, repudiation, ..., DoS
- Multi-level defense aka “defense in depth”

Encryption

- Symmetric, one-time pad, public-key, cryptographic hash
- Understand them as primitives/tools
- Examples: DES, RSA
- Key-distribution problem

Attack styles

Protocols and beliefs

- Authentication-server example

Security – Technology

Replay attacks

- Key technique: “nonce”

Digital signatures

- Do cryptographic hashes really exist?

IPsec

- AH – essentially, signed packets
- ESP – secret packets
- Security Association
- “Transport mode” vs. “Tunnel mode”

Security Applications

Tools and attacks

- Ping, port scanning, ...
- TCP spoofing/hijacking
- Buffer overflow, social engineering, DoS, SMURF

SSL and certificates

- “Chain of trust” - browser, Certificate Authority, server certificate

Kerberos - “trusted third party” authentication

- Short keys, fast crypto – without n^2 key problem
- Standard technique: (ephemeral) *session* keys
- “Ticket” model of authentication

Security Applications

PGP

- “Web of trust”
 - Instead of “chain of trust” or “trusted third party”
- Structure of PGP message
 - One encrypted message body, session key
 - N “key packets” convey session key to recipients

Firewalls, application gateways

Intrusion detection

Web

HTTP

- Intro, details
 - Request headers, response headers
- Persistent connections

Content Distribution Networks

- System architecture
- How DNS is used to direct clients to nearby servers

Preparation Suggestions

Sleep well (*two* nights)

Scan lecture notes

Read any skipped textbook sections

- Well, the most-important ones, anyway

Understand the code you turned in

- Even what your partner wrote
- What was the exercise “about”? What did you learn?

Don't panic!

- Budget time wisely during exam
 - (don't get bogged down on one question)

15-441 on One Slide

Layering

Notion of “protocol”

Standard challenges, techniques

IP and TCP

Naming, addressing

Working together (bridging/routing)

Sliding window

Lots of examples