CSE 222
Graduate Networking

Winter 2001

Lecture 20: Network Potpourri

Geoffrey M. Voelker

Last Lecture

- Potpourri of networking research topics
  - Intserv, diffserv
  - IPv6
  - Anycast
  - IPSEC
  - Active Networks
  - Content distribution networks (CDNs)
  - Peer-to-peer networks

Integrated Services (intserv)

- Fine-grained QoS to individual apps or flows
  - Think RSVP
- Goal: Support applications according to service classes
  - Guaranteed service: No packet arrives late
  - Controlled load: Preferential service without guarantees
- Mechanisms
  - Flowspecs – application requirements
  - Admission control – resource control
  - Reservation – RSVP
  - Scheduling – which packets to send, and when

Flowspecs

- RSpec: Service requested
  - Guaranteed w/ delay, or controlled load
- TSpec: Traffic characteristics
  - Complicated, but essentially the bandwidth requirements
  - Average bandwidth not enough because of variable bit rates
    - » Audio, video, etc.
  - Token bucket is one model
    - » Rate at which tokens are consumed (average)
    - » Depth of buckets for holding tokens

Admission Control

- Based upon TSpec and RSpec, decide if the flow can be supported by network
  - Exact or approximate accounting (bandwidth, delay)?
  - Support from routers?
    - » WFQ to isolate controlled load traffic
- Reservation
  - RSVP

Packet Scheduling

- At routers, need to
  - Classify: Associate packets with a reservation
  - Schedule: Decide which packets to send, and when
- Classifying
  - Use header information to decide service class
- Scheduling
  - Router scheduling discipline
  - WFQ for guaranteed service (bandwidth and delay)
  - Smaller # (one?) of flows for all controlled traffic
  - Can have multiple scheduling algorithms interacting

Differentiated Services (diffserv)

- Coarse-grained QoS to aggregated traffic
  - Poor man's intserv
  - Base case is two classes, best-effort and premium
- Who sets the premium bit?
  - ISP based upon some negotiation (customer pays more)
- What do routers do with packets with premium bits?
  - Many approaches
  - Define per-hop behaviors (PHBs) for routers
    1. Expedited forwarding: minimal delay and loss
    2. Assured forwarding: different drop rates for "in" and "out" packets
    3. Use WFQ w/ two queues

IPv6

- Originally motivated by crisis in IP address space
  - 32 bits not enough if everything gets an IP address
  - Subnetting and CIDR help, but not a long-term solution
- Solution: Increase the size of IP addresses
  - Originally to 64, then to 128 bits
  - Requires changes to IP header
- If we're going to change the header, might as well change other aspects of IP
- But we need to be able to have IPv6 and IPv4 coexist

IPv6 (2)

- IP addresses are 128 bits
  - Unicast, multicast, local, etc.
  - 1234:ABCD:1234:ABCD:1234:ABCD:1234:ABCD
  - Interface ID used as lowest 6 bytes
- Simplified headers
  - 40 bytes (20 for IPv4)
  - Use header extensions for options (e.g., fragmentation)
- Autoconfiguration
  - Leverage Interface ID portion of address
- FlowLabel (routing), TrafficClass (QoS), security, mobility

IPv6 and IPv4 Interoperability

- Dual-stack operation
  - IPv6 nodes that support both IPv4 and IPv6
- Tunneling
  - IPv6 packets encapsulated within IPv4 packets
  - End-points speak IPv6, but use IPv4 packet to use standard Internet routing
  - Easy mapping if IPv6 embeds IPv4 address, otherwise need to configure a table

Anycast

- Packets sent to anycast addresses are delivered to nearest anycast receiver
  - Nearest depends upon routing system
- Why do this?
  - Host and service discovery, auto-configuration, multicast
- Straightforward in LANs, tough to scale to Internet
- GIA – Global IP-Anycast
  - Internal groups – unicast routing to deliver to shortest path
  - Unpopular groups – use default routes, home domain member
  - Popular groups – search for groups, establish shortest path routes

IPSEC

- Security at lowest layer: IP
- Framework for security
  - Select different encryption algorithms, security protocols
  - Select security services (e.g., integrity, authentication, etc.)
  - Select granularity (e.g., connection, all end-point flows)
- Two parts
  - Authentication Header (AH)
    - » Access control, integrity, authentication, anti-replay
  - Encapsulating Security Payload (ESP)
    - » Confidentiality in addition to above
    - » Relies upon an encryption algorithm

IPSEC (2)

- Security Association (SA) binds AH and ESP
  - The "association" defines a set of security services between end-points (security gateways)
  - Simplex – only defined for a single direction
    - » Need two for both directions of a connection
- Negotiation
  - Internet Security Association and Key Management (ISAKMP)
    - » Procedures and formats to establish, negotiate, modify, delete security associations
    - » Again, a framework
  - Internet Key Exchange (IKE)
    - » Specific protocol for exchanging keys

Active Networks

- Problem: How can we change the network without replacing the network?
  - Routing algorithms (multicast), queueing disciplines (WFQ, RED), mobility, measurement, etc.
- Approach: Active Networks
  - Make routers programmable
  - Packets carry programs, or pointers to programs
  - Programs executed on arrival of packets
  - Need platform, execution environment, resource control, security, storage, etc. – essentially, a whole new OS
  - Many different incarnations, some small testbeds
  - Controversial

Real-time Transport Protocol

- Application-level protocol for real-time data
  - RTP: Data transmission
  - RTCP: Control transmission
- Uses ALF to support varied classes of applications
  - Profile: Definition of use of header fields (timestamp, etc.)
    - » App decides how to interpret timestamp field (units)
  - Formats: Interpretation of payload data
    - » Audio samples vs. mpeg frame
- RTCP
  - Performance feedback of application and network
  - Correlate and synchronize multiple media streams
  - Identify sender (e.g., video conferencing)

Content Distribution Networks

- CDNs accelerate Web traffic
  - Akamai, Digital Island, etc.
  - Contract with content providers (espn, nytimes, etc.)
  - Distribute content using “internal” network to edges
    - » Load balancing (many edge servers vs. single machine room)
    - » Low delay (edge servers closer to clients)
  - Implemented as an overlay network
- Traffic
  - Currently handle “easy” content (images)
  - Poised to handle “tough” content (streaming media, dynamic data)

Peer-To-Peer Networks

- Application networks in which every node is both a client and a server
  - Overlayed on underlying physical network (Internet)
- Hot topic, many examples
  - Napster, Gnutella, FreeNet, etc.
- Many architectures
  - Centralized directory (Napster)
  - Broadcast mesh (Gnutella)
- Stuff is too new to predict how it is going to pan out
  - But expect to see papers on it in coming years

Thanks

- I had a great time teaching this class
- Hope you had a great time taking it…

For Next Time...

- Final project writeups due Monday, 3/19, at midnight
- Final presentations Thursday, 3/22, at 11:30am