What does the Internet provide?

- Best-effort service
  - Guarantee only one thing - delivery of data
  - That is, making the “best of the best effort”
  - But, many things required by the application layer can’t be guaranteed if lower layers do not
    - E.g. delay and bandwidth may be important to multimedia related applications

What is QoS?

- Mechanism to provide certain service grade regardless network conditions
QoS Metrics

- Available bandwidth
- Packet loss rate
- Estimated delay
- Packet jitter
- Hop count
- Path reliability

QoS in the Internet

- QoS Models
  - IntServ (Integrated Services)
  - Resource reservation
  - DiffServ (Differentiated Services)
  - Traffic classification and policing
  - MPLS (Multi-Protocol Label Switching)
- QoS routing
  - How do we find good paths with good QoS properties?
**IntServ**

[IntServ][1]

- All flows start after resource reservation
- Only two classes
  - Guaranteed or controlled-load
- Components
  - RSVP (Resource Reservation Protocol)
    - [RFC2205 1997][2]
    - On per-flow basis - routers maintain flow-specific info
  - Admission control
  - Classification
  - Packet scheduling
- Disadvantages?

**DiffServ**

[DiffServ][3]

- Packets are divided into classes
  - The TOS (type of services) byte in IPv4 header is now called DiffServ Field
  - Packet forwarding treatment - PHB (per-hop behavior)
- Essentially a relative-priority scheme
- SLA (Service Level Agreement) – a contract between customer and ISP
  - Service classes supported
  - Amount of traffic allowed in each class
- Customer (or its leaf router) marks packets individually
- Ingress (edge) router of ISP classifies and polices the packet flows
- Core routers forward (and possibly drop in case of congestion) packets according DiffServ Field marks

---

[1]: [Braden, Clark & Shenker RFC1633 1994](#)
[2]: [Braden, Zhang, Berson, Herzog & Jamin RFC2205 1997](#)
[3]: [Blake, Black, Carlson, Davies, Wang & Weiss RFC2475 1998](#)
Diffserv Architecture Illustrated

Edge router:
- per-flow traffic management
- marks 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

Scheduling and Dropping Mechanisms

- **FIFO (FCFS)**
- Priority queuing
- Round robin and WFQ (Weighted Fair Queuing)

- Drop tail
- RED (Random Early Detection)
- RIO (RED with In and Out)
**RED Packet Drop Explained**

- Use exponential average of queue length to determine when to drop
  - Avoid overly penalizing short-term bursts
  - React to longer term trends
- Tie drop prob. to weighted avg. queue length
  - Avoids over-reaction to mild overload conditions

---

**Why QoS Routing?**

- **Causes of congestion**
  - Lack of network resources
  - Uneven traffic load distribution
    - Direct results of many dynamic routing protocols such as RIP, OSPF, IS-IS etc.
- **Goal** - Arrange how traffic flows through the network so that congestion caused by uneven network utilization is avoided
- **Constraint-based routing** - calculate routes subject to multiple constraints
Constraint-Based Routing

- **Goals**
  - Select routes that meet QoS requirements
  - Increase network utilization
- **In addition to topology, routers should know**
  - Flow requirements
  - Routing policies
  - Route metrics
    - E.g. monetary cost, hop-count, bandwidth, delay, reliability, jitter
- **Routing algorithms select routes that optimize one or more of these metrics**

Route Computation

- **Types of route metrics**
  - **Additive** if \( c(P) = c(i, j) + c(j, k) + \ldots + c(l, m) \)
  - **Multiplicative** if \( c(P) = c(i, j) \times c(j, k) \times \ldots \times c(l, m) \)
  - **Concave** if \( c(P) = \min\{ c(i, j), c(j, k), \ldots, c(l, m) \} \)

- **Computing optimal routes subject to constraints of two or more additive and/or multiplicative metrics is NP-complete**
- **Sorts of heuristics or approximations**
- **Can be computation-intensive**
Flexible QoS Model for MANETs

[Xiao, Seah, Lo & Chua 2000]

- FQMM (Flexible QoS Model for MANETs)
  - Consider characteristics of MANETs
  - Combination of IntServ and DiffServ
- Per-flow
  - As in IntServ
  - Tries to preserve per-flow granularity for a small portion of traffic
- Per-class
  - As in DiffServ
  - Done for the mass majority of the traffic

QoS in MANETs

- Signaling
  - INSIGNIA
  - dRSVP (dynamic RSVP)
- Routing
  - CEDAR (Core Extraction Distributed Ad Hoc Routing)
  - Ticket-based routing
  - Bandwidth routing
- Link layer
  - MACA/PR
  - IEEE 802.11e
INSIGNIA

[Ahn, Campbell, Lee & Zhang 1998]

- Per-flow
- In-band signaling for less overhead
  - Unlike RSVP which has an explicit resource reservation phase before data transportation
  - Info used for resource reservation is piggybacked on data packets
  - No flow rejected – if QoS requirement satisfied, forward as RES (reservation); otherwise, forward as BE (best effort)
- Soft-state
- QoS reporting – periodic report from destination to source about stats
- Restoration – depending on underlying routing protocol

CEDAR

[Sivakumar, Sinha & Bharghavan 1999]

- Core extraction
  - Core – a small dominating set of nodes
  - Core graph – graph on the dominators
  - Distributed algorithm for small dominating sets
  - For local topology control and smart broadcast
- Link state propagation
  - Significant bandwidth changes are broadcast (by dominators) throughout network
- Route computation
  - On-demand source routing
  - Routes established first within core graph
IEEE 802.11 Standard Family

802.11 PHY Layer
- Infra-Red (IR), 1/2Mbps
- 2.4GHz FHSS (Frequency Hopping Spread Spectrum)
- 2.4GHz DSSS (Direct Sequence Spread Spectrum)
- 5GHz-OFDM (Orthogonal Frequency Division Multiplexing)
- 802.11a MIMO (Multiple-Input Multiple-Output)

802.11 MAC Layer
- 802.11e QoS Enhancement
- 802.11e Access Point Frame
- 802.11i Enhanced Security
- 802.11h Enhanced MAC

802.11 is Best Effort
- DCF’s limitations
- PCF’s limitations
Transport Layer Issues in MANETs

Part 8
CS-6777 Mobile Ad Hoc Networking
Memorial University of Newfoundland

Transport Layer Services

- End-to-end logical communications between two "processes"
  - Demux through port numbers

- Two styles of services
  - Fast and unreliable
  - Mild and reliable
UDP & TCP

**UDP – User Datagram Protocol**
- No error control
- No flow/congestion control
- Short header – how many bytes?

**TCP – Transmission Control Protocol**
- Error control
- In-order delivery
- Flow/congestion control
- Longer header – how many bytes?

---

TCP Features

- **AIMD**
  - Additive increase
  - Multiplicative decrease
- **Retransmit timer**
  - Time-out interval and exponential backoff
- **Slow start**
  - Versus fast recovery in response of segment loss
- **ACK-clocking**
What is Wrong with TCP? (I)

Misinterpretation of segment losses
- Performing congestion control in cases of losses not induced by network congestion
  - Many losses in MANETs are not caused by congestion
- Where are the losses from?
  - Lossy channels
  - Path asymmetry - bandwidth, loss rate, route
  - Power constraints
  - Route failure
  - Network partition
  - Multi-path routing and out-of-order (OOO)

What is Wrong with TCP? (II)

Oversized maximum congestion window size
- In high speed networks
  - “bandwidth-delay product”
  - [RFC 1323 - TCP Extensions for High Performance]
- In a chain of 802.11 nodes
  - Much smaller due to interference among neighboring nodes
Solutions

- Overhaul
- Fix/tweak existing protocols
  - Cross layer
  - Layered

TCP – Network Cross Layer

- Use feedback from network layer to clarify cause of packet losses to avoid starting congestion control blindly
- Even to break the end-to-end semantics of TCP
TCP-F

Feeder based
- To minimize throughput degradation resulting from path breaks

TCP sender gets notified of route failures
- In TCP-F, when an intermediate node (called failure point, FP) detects a path failure (how?), it sends a Route Failure Notification (RFN) to the TCP sender
- Upstream node may discard the RFN if knowing alternative routes
- After TCP sender receives RFN, it enters a snooze state by freezing all TCP variables

TCP-F (cont’d)
- When broken link is fixed, FP sends a Route Re-establishment Notification (RRN) to TCP sender, which in turn returns to normal state
- TCP sender may also return to normal state after a timeout
TCP-ELFN  [Holland and Vaidya 2002]

- Similar feedback based approach
  - TCP with Explicit Link Failure Notification
  - TCP sender snoozes when notified of route break
- When in snooze state, TCP sender periodically probes the destination to see if break has been fixed so as to return to normal state

TCP-BuS  [Kim, Toh and Choi 2001]

- Similar feedback based approach
  - TCP with Buffering capability and Sequence information
- TCP sender freezes when notified of route break
- Intermediate nodes buffer segments until route reconstructed
- Utilize the SACK option of TCP s.t. sender does not need to resend segments
**ATCP**

[Liu and Singh 2001]

- **Ad hoc TCP**
  - Uses Explicit Congestion Notification (ECN) of IP [RFC 3168]
  - ECN is part of Active Queue Management (AQM) of IP, in contrast to Random Early Detection (RED)
- A layer inserted between TCP and network layers of the sender
  - No modification to TCP
- TCP sender starts congestion control when receiving ECN; freezes on DUACKs and TIMEOUTs

**TCP-Split**

[Kopparty, Krishnamurthy, Faloutsos, and Tripathi, 2002]

- Split long TCP connections into short ones
  - Observing that TCP throughput decreases rapidly as hop length increases (why?)
- Sender → proxies → destination
  - Local ACK (LACK) vs. End-to-end (EACK)
  - Sender maintains two CW's while proxies maintain one
- Separate error control from congestion control
Network – PHY Cross Layer

- Preemptive routing
  - [Goff, Abu-Ghazaleh, Phatak and Kahvecioglu 2001]
  - To reduce route failures
  - Routing module finds and switches to new routes when capacity of a link on current route drops below a threshold

- Signal strength based link management
  - [Klemm, Krishnamurthy and Tripathi, 2003]
  - Similar to above, when locating new route, increase transmission power to keep the link alive temporarily

TCP Layer Proposals

- Dynamic delayed ACK
  - [Altman and Jimenez 2003]
  - Reduce the number of ACKs to reduce channel contention
    - May cause sender burst (why?)

- Adaptive CWL setting
  - [Chen, Yue and Nahrstedt 2003]
  - Set contention window length (upper limit of CW) according to path length, e.g. 1/5 of RTHC (round trip hop count)
Link Layer Proposals

- Link RED
  - [Fu, Zerfos, Luo, Lu, Zhang and Gerla 2003]
  - Drop/mark frames (as in AQM) when link quality drops below threshold
- Neighborhood RED
  - [Xu, Gerla, Qi and Shu 2003]
  - Refer to (up/down stream) neighbors when calculating drop/mark probability

Non-TCP Transport Layer Protocols

- ACTP – application controlled transport protocol
  - [Liu and Singh 1999]
  - Like UDP with feedback and state maintenance
  - No congestion window maintained
  - Application layer responsible for retransmission
- ATP – ad hoc transport protocol
  - [Samdaresan, Anantharaman, Hsieh and Sivakumar 2003]
  - A light-weight TCP like protocol
  - Uses feedbacks from layers below
Cross-Layer Design