Post-modern E2E Principle (and lack thereof)

Presenter: Amit Shelawala

September 9, 2004

Introduction

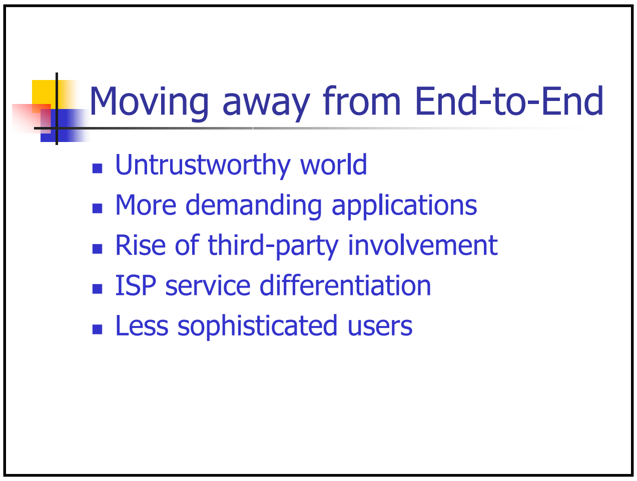
- Last Time
  - End-to-End Principle
  - Basis of principle
- Today
  - Newly Arising Problems pushing away from end-to-end

Required Readings

- Rethinking the design of the Internet: The end to end arguments vs. the brave new world
- The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture

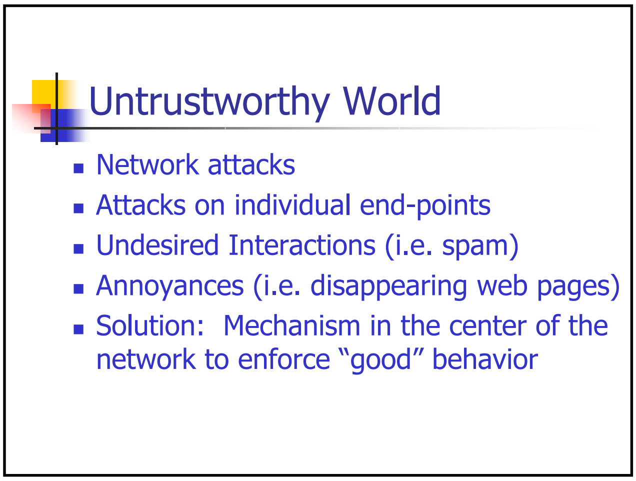
Rethinking the design of the Internet: The end to end arguments vs. the brave new world

- Published in 2001
- Reasons for End-to-end
- New situations arising call for a change from End-to-End
- Risks of deviation from End-to-end



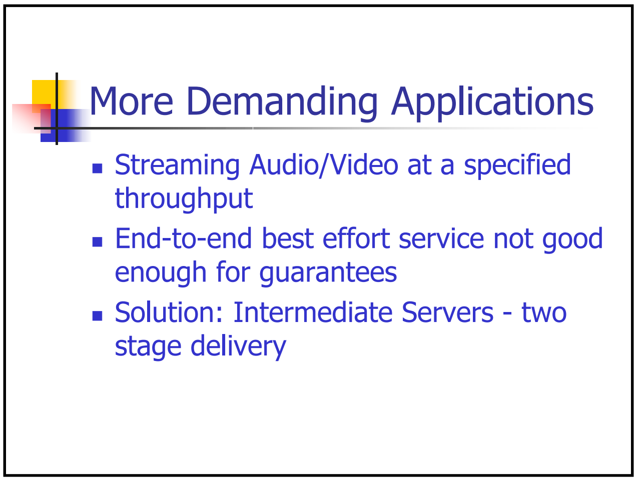
Moving away from End-to-End

- Untrustworthy world
- More demanding applications
- Rise of third-party involvement
- ISP service differentiation
- Less sophisticated users



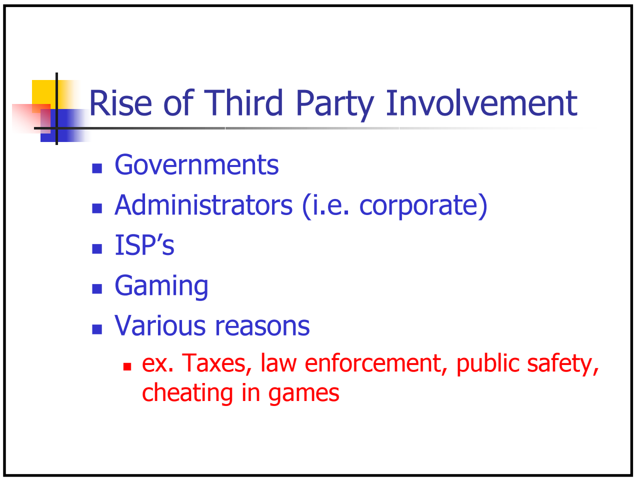
Untrustworthy World

- Network attacks
- Attacks on individual end-points
- Undesired Interactions (i.e. spam)
- Annoyances (i.e. disappearing web pages)
- Solution: Mechanism in the center of the network to enforce "good" behavior



More Demanding Applications

- Streaming Audio/Video at a specified throughput
- End-to-end best effort service not good enough for guarantees
- Solution: Intermediate Servers - two stage delivery



Rise of Third Party Involvement

- Governments
- Administrators (i.e. corporate)
- ISP's
- Gaming
- Various reasons
  - ex. Taxes, law enforcement, public safety, cheating in games

ISP Service Differentiation

- Competition with one another
- Can't really compete with pricing
- Want to provide services that are better than competition

Less Sophisticated Users

- People are less inclined to configure things correctly at the end
- May not care about security

Implications

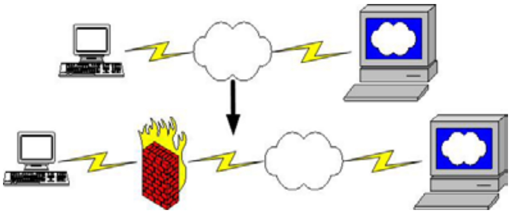
- Society may desire to impose on its network-based communication
- End-to-end states that all requirements can be implemented correctly at the end points
- *If implementation* inside *the network is the* only *way to accomplish the requirement, then an end-to-end argument isn't appropriate in the first place*

Technical Responses

- Firewalls
- Traffic Filters
- NAT boxes
- Content caches

Firewalls

- Intercepts packets and filters for the network



Firewalls (cont.)

- Prevent DoS attacks
- Creates a barrier for resources
  - Prevents others from changing internal material
  - Authorize some usage inside network
- Firewall not at the end -> breaks end-to-end

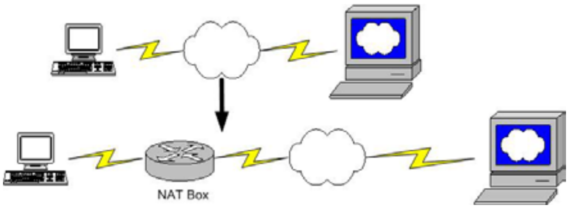
Traffic Filters

- Filters packets that have “unwanted” information
- Like firewalls, located in the network before the end

NAT Boxes

- Allow for multiple machines to use the same IP address
- NAT router maps an IP and port number of an internal machine to the router’s IP and a port number
- Datagrams need to be modified in transit
- Needs to be taken in account by applications -> breaks end-to-end

NAT (cont.)



Content caches

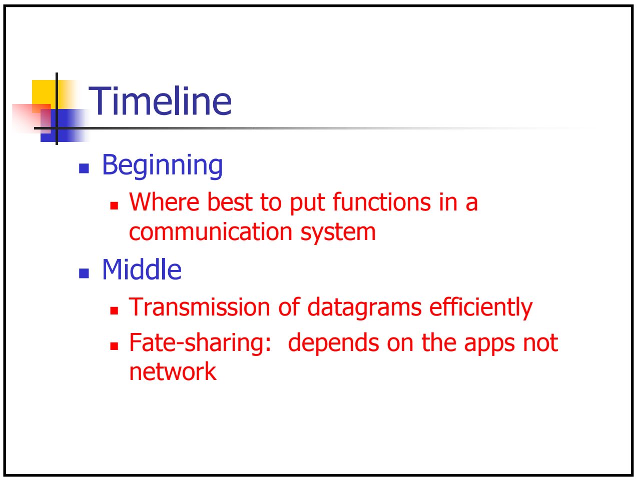
- Store data for faster retrieval at end
- Does not require end to send across network
- Other end is not notified when data is retrieved from the cache

Technical Responses (cont.)

- All of these trends push away from end-to-end
- Leading to badness

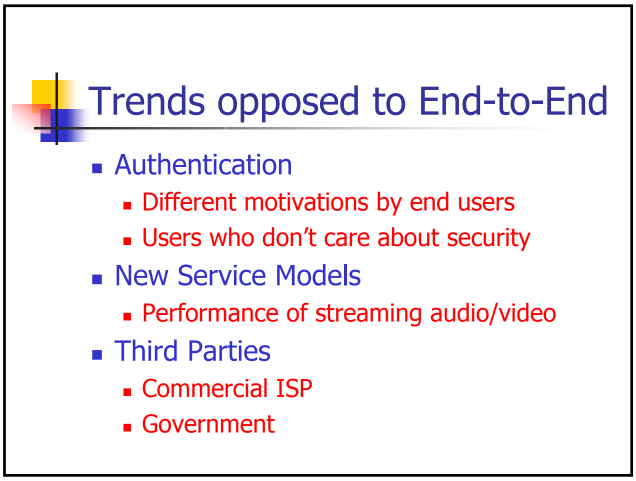
The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture

- RFC3724
- March 2004
- Studies trends of End-to-End
- Particularly trends away from it



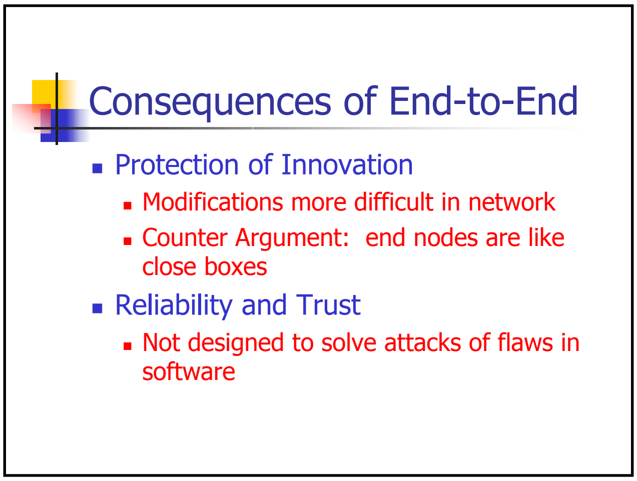
Timeline

- Beginning
  - Where best to put functions in a communication system
- Middle
  - Transmission of datagrams efficiently
  - Fate-sharing: depends on the apps not network



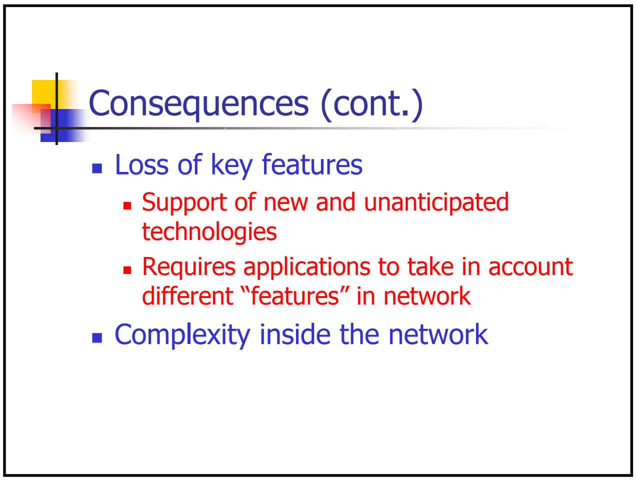
Trends opposed to End-to-End

- Authentication
  - Different motivations by end users
  - Users who don't care about security
- New Service Models
  - Performance of streaming audio/video
- Third Parties
  - Commercial ISP
  - Government



Consequences of End-to-End

- Protection of Innovation
  - Modifications more difficult in network
  - Counter Argument: end nodes are like close boxes
- Reliability and Trust
  - Not designed to solve attacks of flaws in software



Consequences (cont.)

- Loss of key features
  - Support of new and unanticipated technologies
  - Requires applications to take in account different "features" in network
- Complexity inside the network

Application Design

- Ensure that there aren't any dependences that would break end-to-end
- Identify end points in a consistent fashion

Conclusions

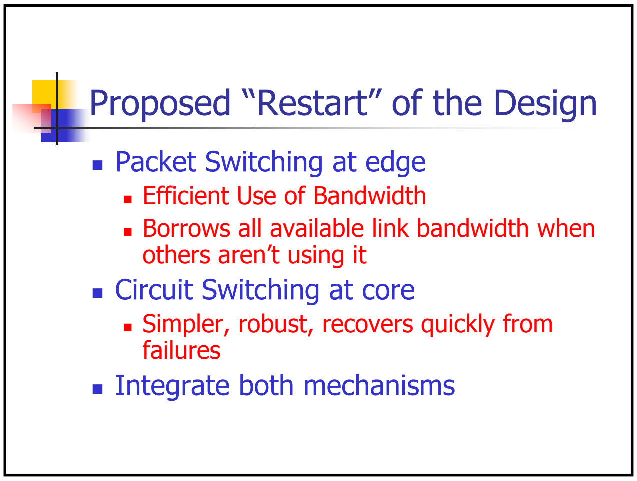
- End-to-end continues to guide development
- New problems require moving away from end-to-end
- Trade offs
- What does everyone think about end-to-end vs. newer trends?

Extra Readings

- Is IP going to take over the world?
  - Will Packet Switching networks take over all communication systems?
  - Telephony
  - Cable Television

IP Folklore

- IP already dominates global communications
- IP is more efficient
- IP is robust
- IP is simpler
- Support of telephony and other real-time applications over IP networks



Proposed "Restart" of the Design

- Packet Switching at edge
  - Efficient Use of Bandwidth
  - Borrows all available link bandwidth when others aren't using it
- Circuit Switching at core
  - Simpler, robust, recovers quickly from failures
- Integrate both mechanisms