IP Routing Improvements

Prométhée Spathis

Goals of Today's Lecture

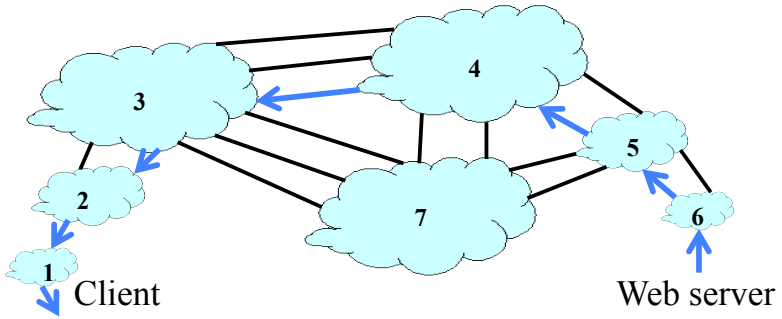
- Limitations of IP routing and forwarding
  - Same paths used for all kinds of traffic
  - Routing protocols are oblivious to performance
  - Different ASes have different objectives
  - Routing changes lead to transient disruptions
- Some improvements what can help
  - Multi-path routing
  - Adaptation to changes in load
  - Faster routing convergence
  - Traffic engineering
- Overlay networks

Two-Tiered Routing System

	Intradomain	Interdomain
Objectives	Efficiency, performance, robustness	Business relationships
Scale	Tens to hundreds of routers	Tens of thousands of ASes
Trust	All routers run by the same entity	ASes run by different entities
Protocols	Metric-based (e.g., OSPF)	Policy-based (e.g., BGP)

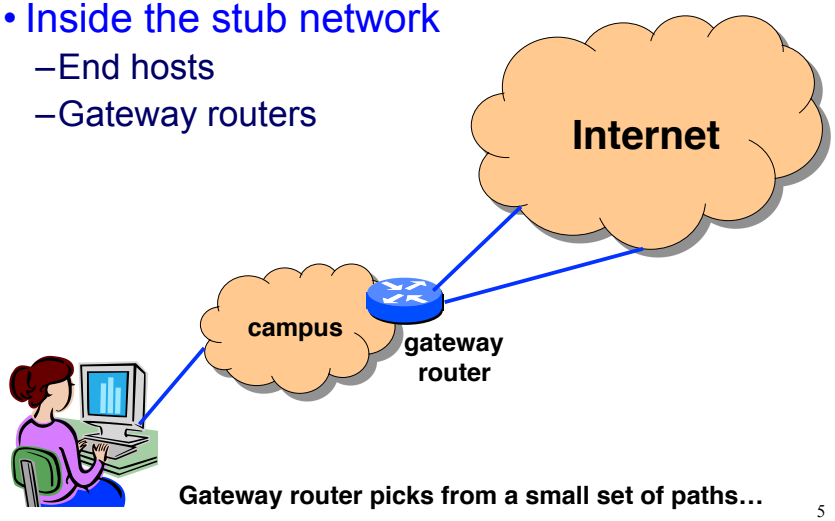
End-to-End Paths are a Composition

- Between the end hosts and the Internet
- Interdomain AS path across multiple ASes
- Intradomain path inside each transit ASes



Delivering Packets in Stub Networks

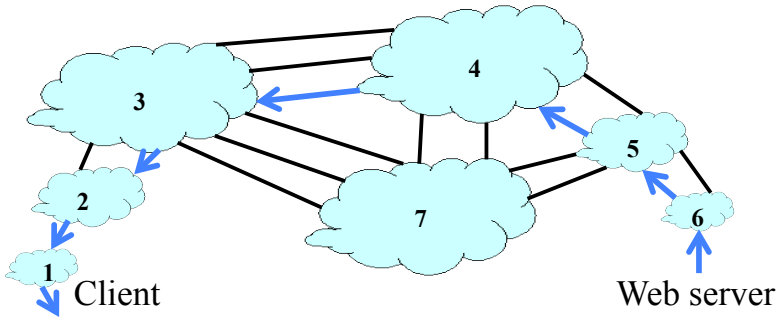
- Inside the stub network
  - End hosts
  - Gateway routers



Gateway router picks from a small set of paths…

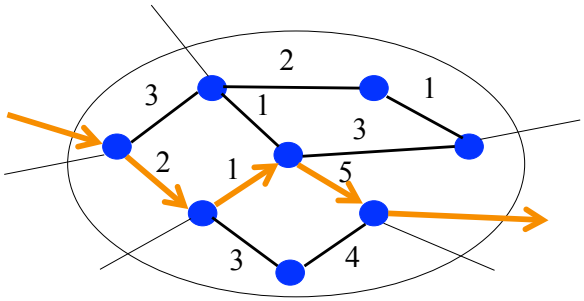
Interdomain Routing With BGP

- Each AS picks a "best path" to the destination
- Among the choices advertised by its neighbors
- Based on each ASes' local policy objectives



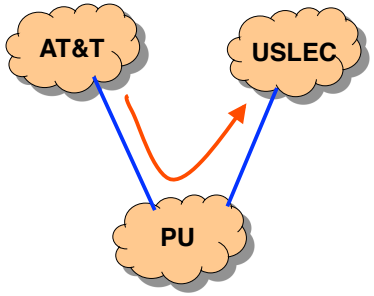
Intradomain Routing

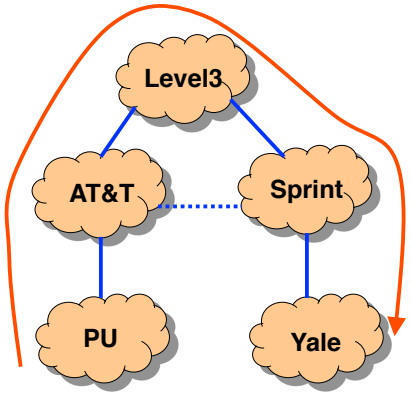
- Routers compute shortest paths
- Based on configurable link weights
- Operators set weights to satisfy network goals



Routing Policy Constrains Paths

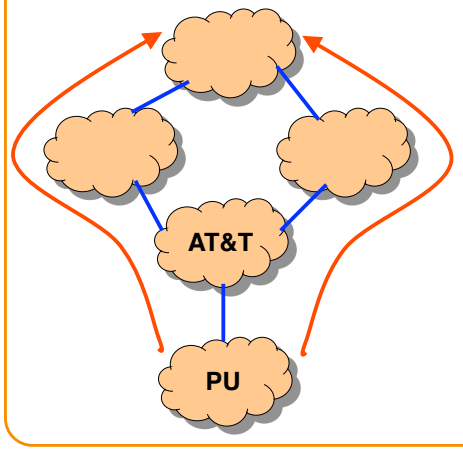
- Paths that violate policy cannot be used
- Some failures may disconnect hosts

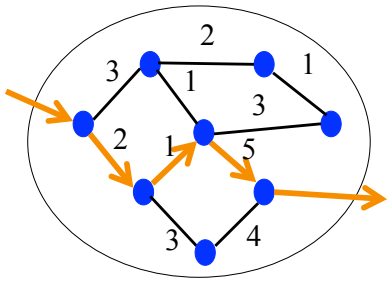




Single-Path Routing is Restrictive

- BGP routers pick a single best path
- Shortest-path protocols use only shortest paths



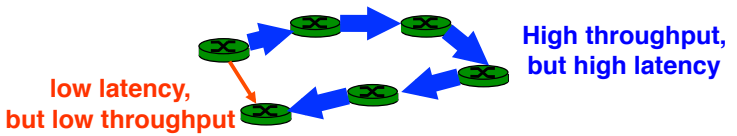


Routing Doesn't Consider Performance

- Routing protocols do not react to load
  - Routing based on routing policies or link weights
  - Static configuration that changes infrequently
- Routers have limited visibility
  - Routers cannot see the topology in other ASes
  - Routers do not keep state about performance
- Network operators weigh many objectives
  - Minimizing cost or maximizing revenue
  - Balancing load in the network
  - Not just the end-to-end performance

All Traffic Follows the Same Paths

- IP does destination-based forwarding
  - All traffic follows the same paths
  - Independent of the application requirements
- Yet, applications have different needs
  - Voice and gaming: low latency and loss
  - File sharing: high bandwidth



Disruptions During Convergence

- Changes to the network are disruptive
  - Topology changes, due to failures and recovery
  - Configuration changes, e.g., tweak link weights
- Routers have to reach agreement again
  - Detect the change in the network
  - Propagate new information among themselves
- In the meantime, performance suffers
  - Blackholes: packets dropped on the floor
  - Loops: packets spin around in a loop
  - Delays: packets take a circuitous path

Does IP Routing Really Stink?

- Some improvements would help
  - Multi-path routing
  - Adaptation to changes in load
  - Faster routing convergence
- But, IP routing is solving a hard problem
  - Decentralized control with common protocols
  - Different, sometime competing, objectives
  - Large scale (200,000 prefixes and 20,000 ASes)
- IP routing does an okay job for everyone
  - Rather than an optimal job for anyone
  - And leaves everything else to the end hosts…

Multipath Routing

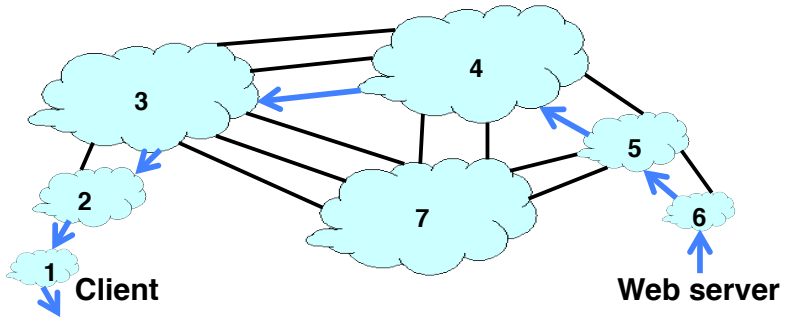
Outline

- Mostly single-path routing today
  - BGP and IGPs
- Multipath intradomain
  - Equal-cost multipath
  - MultiProtocol Label Switching
- Multipath interdomain
  - Intelligent route control by stub ASes
  - Overlay routing through intermediate node
  - Multipath extensions to BGP
- Preventing out-of-order packets

Conventional IP Routing Protocols

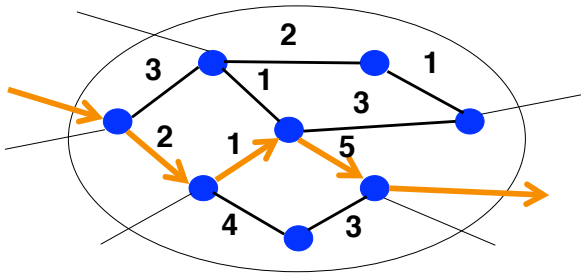
BGP is a Single-Path Protocol

- Each router picks a single best route
  - From the routes learned from its neighbors
- And announces that route to its neighbors



Intradomain Routing is (Mostly) Single Path

- Shortest-path routing as sum of link weights
  - Equal splitting over multiple shortest paths
- No traffic sent along the non-shortest paths



Why Single Path?

- Simple routing protocol
  - Low computational overhead
  - Limited control-plane messages
- Simple packet forwarding
  - One, or at most a few, forwarding-table entries
  - Easy to do hop-by-hop forwarding
  - Packets generally delivered in-order
- More control over the flow of traffic
  - Little control relinquished to upstream neighbors
  - Use the announced path, or not… ☺

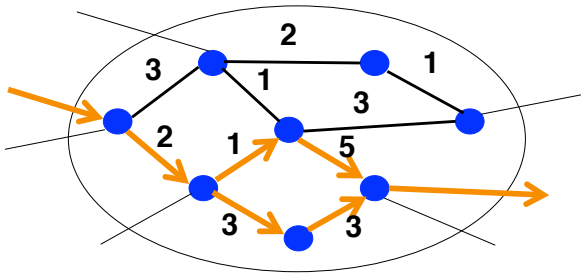
Motivations for Multipath

- Better efficiency
  - Splitting load over multiple paths
- Better performance
  - Selecting the low-delay (or high-throughput) path
- Better reliability
  - Faster failover from one path to another
- Better security
  - Prevent on-path adversary from seeing all packets
- More control
  - Providing greater flexibility to upstream ASes

Intradomain Multipath

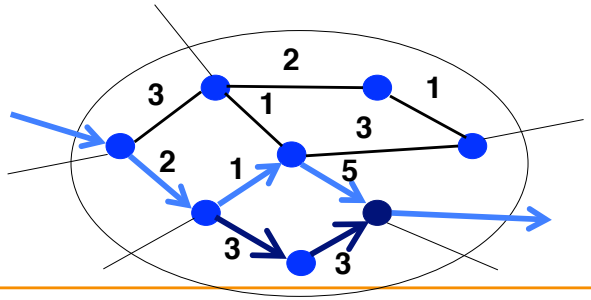
Relatively Easy in Equal-Cost Multipath

- Routers compute shortest paths
  - Identify next-hops along shortest paths
  - Put multiple entries in the forwarding table
  - Split traffic evenly over the paths
- Still, no global information for smarter splitting



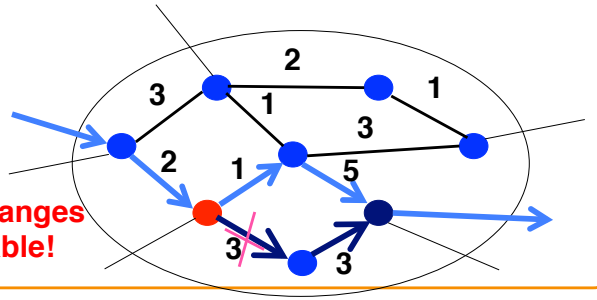
Equal-Cost Multi-Path (ECMP)

- Multiple shortest paths
  - Router can compute multiple shortest paths
  - Forwarding table has multiple outgoing links
  - Router splits traffic evenly over the links



ECMP Reduces Forwarding-Plane Convergence

- Suppose one of the outgoing link fails
  - Incident router detects the failure
  - Quick recomputation of paths without this link
  - Local forwarding table updated to use other link
  - Other routers have no forwarding-table change!!!



Only red router changes its forwarding table!

Exploiting This Observation in Traffic Engineering

- Traffic engineering
  - Given a topology and a traffic matrix
  - … set link weights to control the flow of traffic
  - … to minimize some objective function
- Bias toward solutions with "ties"
  - Penalize solutions with just one shortest path
  - Favor solutions that lead to multiple paths
  - … even if the link loads are a little less balanced
- Applied in some traffic-engineering tools
  - Demand from ISPs buying the tools
  - … with customers demanding fast convergence

Examples of Planned Failures

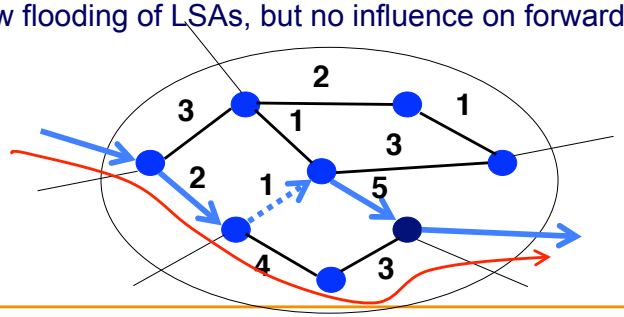
- Upgrades
  - Changing link to higher capacity
  - Loading new operating system on a router
  - Swapping out an old interface card
- Maintenance
  - Fixing a flaky optical amplifier
  - Configuration changes that require a reboot
- Cable intrusions
  - Construction activities near a fiber

Planned Events Happen Often

- Sprint study
  - Maintenance window
    - From 10pm to 6am EST, covering east to west
    - Period of low network traffic, so less congestion
    - Not much business-critical traffic
  - Responsible for 50% of intradomain failures
- Significance
  - Planned events should be easier to handle
  - The operator knows the failure(s) will happen
  - … but, how to tell the routing protocol?
  - … or, how to prepare the network in advance?

"Costing Out" of Equipment

- Increase cost of link to high value
  - Triggers immediate flooding of LSAs
- Leads to new shortest paths avoiding the link
  - While the link still exists to forward during convergence
- Then, can safely disconnect the link
  - New flooding of LSAs, but no influence on forwarding



Bigger Picture

- Learn about a planned event
  - E.g., replace optical amplifier
- Map the event to the IP equipment
  - E.g., find link(s) that traverse the amplifier
- Increase the weight on each link
  - Slowly, perhaps one at a time to reduce overhead
- Disable the equipment
  - Disconnect amplifier and replace with new one
- Reintroduce the links into the network
  - Slowly, change one link weight at a time

Even Bigger Picture

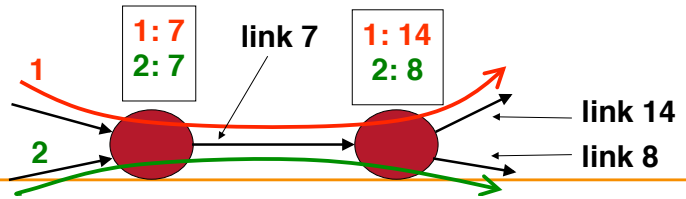
- What if maintenance would cause congestion?
  - Reducing the capacity of the network
  - Link weights not optimized to new topology
- Compute weight changes to make
  - Re-optimize the setting of the link weights
  - … based on the soon-to-be new topology
- Then, do the maintenance
  - Cost out the IP links
  - Fix/upgrade the equipment
  - Cost in the IP links
- Then, go back to the old weight setting

Multi-Topology Routing

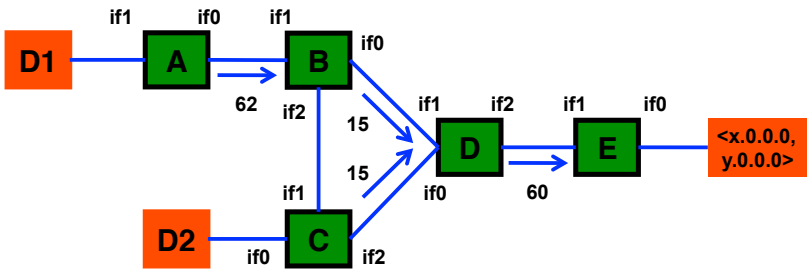
- Extension to existing intradomain routing
  - Multiple weights on each link
  - Compute shortest paths with each set of weights
- Separate paths for different traffic classes
  - Minimize delay for VoIP and gaming
  - Maximize throughput for Web downloads
- Forward packets selectively on the paths
  - E.g., based on type-of-service bits in IP header

Flexible Multipath With Virtual Circuits

- Establish one or more paths within an AS
  - Explicit signaling of the path in advance
  - Control over which packets use each path
- Virtual Circuit Identifier (VC ID)
  - Source set-up: establish path for the VC
  - Switch: mapping VC ID to an outgoing link
  - Packet: fixed length label in the header



An example of label switching



LFIB	Incoming label	Outgoing label	Next hop	Outgoing interface
LSR A		62	LSR B	if 0
LSR B	62	15	LSR D	if 0
LSR C		15	LSR D	if 2
LSR D	15	60	LSR E	if 2
LSR E	60		LSR E	if 0

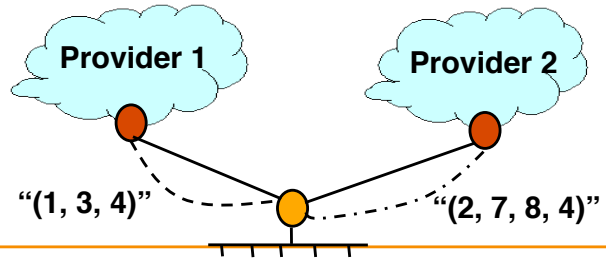
Multipath Routing With MPLS

- Establish multiple paths
  - Signaling message to explicitly set-up the paths
- Flexible splitting over the paths
  - Configurable splitting ratios
- Flexible control over which traffic uses paths
  - Configurable "forwarding equivalence classes"
- Fast recovery from failures
  - Pre-configuration of backup paths
  - To protect primary paths, or even individual links

Interdomain Multipath: Multihoming

Outbound Traffic: Pick a BGP Route

- Easier to control than inbound traffic
  - IP routing is destination based
  - Sender determines where the packets go
- Control only by selecting the next hop
  - Border router can pick the next-hop AS
  - Cannot control selection of the entire path



Outbound Traffic: Primary and Backup

- Single policy for all prefixes
  - High local-pref for session to primary provider
  - Low load-pref for session to backup provider
- Outcome of BGP decision process
  - Choose the primary provider whenever possible
  - Use the backup provider when necessary
- But…
  - What if you want to balance traffic load?
  - What if you want to select better paths?

Outbound Traffic: Load Balancing

- Selectively use each provider
  - Assign local-pref across destination prefixes
  - Change the local-pref assignments over time
- Useful inputs to load balancing
  - End-to-end path performance data
    - E.g., active measurements along each path
  - Outbound traffic statistics per destination prefix
    - E.g., packet monitors or router-level support
  - Link capacity to each provider
  - Billing model of each provider

Outbound Traffic: Shortest AS Path

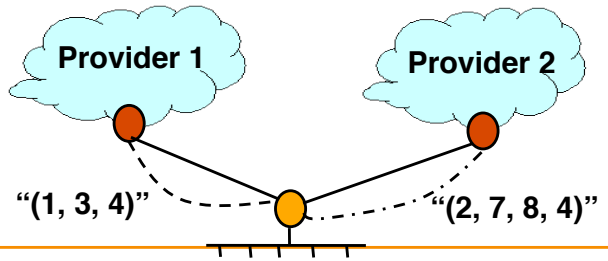
- No import policy on border router
  - Pick route with shortest AS path
  - Arbitrary tie break (e.g., smallest router-id)
- Performance?
  - Shortest AS path is not necessarily best
  - Could have high delays or congestion
- Load balancing?
  - Could lead to uneven split in traffic
  - E.g., one provider with shorter paths
  - E.g., too many ties with skewed tie-break

Outbound Traffic: Load Balancing

- Selectively use each provider
  - Assign local-pref across destination prefixes
  - Change the local-pref assignments over time
- Useful inputs to load balancing
  - End-to-end path performance data
    - E.g., active measurements along each path
  - Outbound traffic statistics per destination prefix
    - E.g., packet monitors or router-level support
  - Link capacity to each provider
  - Billing model of each provider

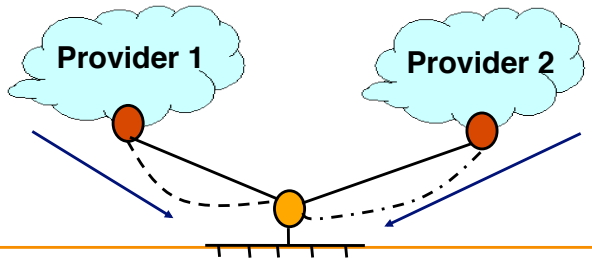
Splitting Over Multiple Paths

- Use multiple outbound paths at the same time
  - Completely under the control of the edge router
  - No announcements sent to any neighbors
  - No need to encapsulate or mark the packets
- Still can only pick among the next-hop ASes



Inbound Traffic: Influencing What Others Do

- Harder to control than outbound traffic
  - IP routing is destination based
  - Sender determines where the packets go
- Control only by influencing others' decisions
  - Explicitly tell the providers what to do
  - Indirectly try to influence their decisions



Research Challenges

- How to monitor performance efficiently?
  - Ping? TCP transfers? HTTP downloads?
  - Per prefix? Per popular prefix?
- How to optimize the load balancing?
  - Considering load, performance, and cost
- Impact on the upstream providers?
  - Uncertainty about the offered load
- How to ensure global stability?
  - What if everyone starts doing it?
- How to balance goals of sender and receiver?
  - Joint control over path selection?

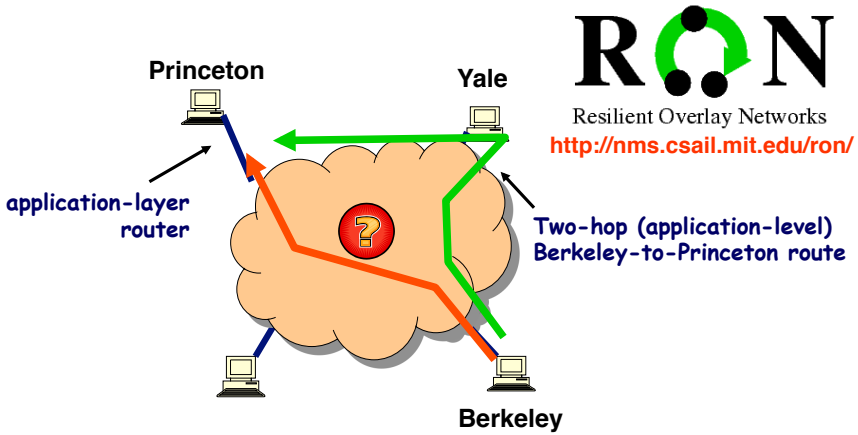
More Flexible Interdomain Multipath

Source Routing

- Source routing
  - Propagate topology information
  - Let end hosts or edge routers pick paths
  - Carry the path information in the packets
- Scalability challenges
  - Large topology and frequent churn
  - Can operate at (say) the AS level
- Tussles over control
  - End-hosts/edge-routers wanting more control
  - ISPs not wanting to relinquish control

Multipath Through Overlays

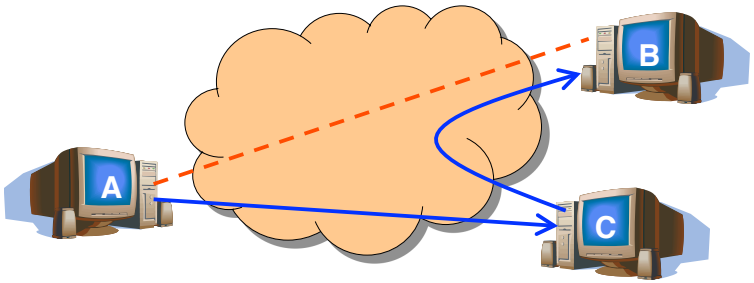
Premise: by building application overlay network, can increase performance and reliability of routing



More when we talk about overlays later in the lecture.

How Does RON Work?

- Exchange the results of the probes
  - Each host shares results with every other host
  - Essentially running a link-state protocol!
  - So, every host knows the performance properties
- Forward through intermediate host when needed



Out-of-Order Packets

- Multipath can lead to out-of-order delivery
  - Packets on different paths may get out of order
- No problem for packets from different flows
  - E.g., different TCP connections
- Can direct related packets onto the same path
  - Hash-based splitting of traffic
- Can direct bursts of packets onto same path
  - "Flow-let" switching, change paths only after gap
- Maybe transport shouldn't be so sensitive
  - Being less sensitive to out-of-order delivery

Conclusions

- Multipath routing is useful
  - Load balancing, reliability, security, performance
- Multipath routing is challenging
  - Scalability, control over data plane, tussle over control over the flow of traffic
- Variety of techniques
  - Flexible splitting, multi-homing, MPLS, deflection through an intermediate node, …
- Many open research questions
  - Scalability, stability,

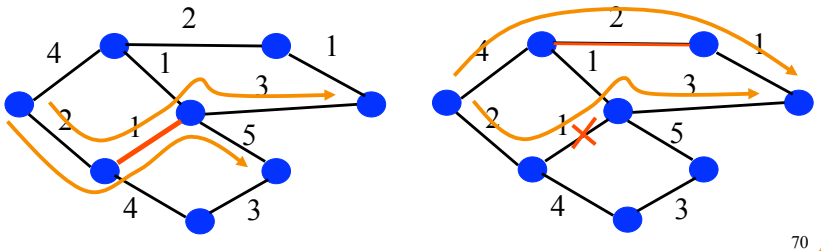
Adapting Routing to the Traffic

Adapting Routing to the Traffic

- Challenges
  - Reacting quickly to alleviate congestion
  - Avoiding over-reacting and causing oscillations
  - Limiting bandwidth & CPU overhead on routers
- Load-sensitive routing
  - Routers adapt to link load in a distributed fashion
  - At the packet level, or on "group of packets"
- Traffic engineering
  - Centralized computation of routing parameters
  - Network-wide measurements of offered traffic

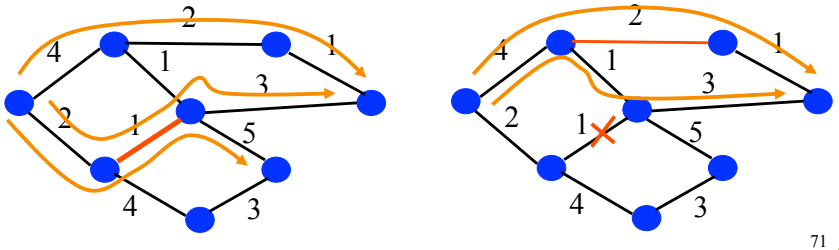
Do IP Networks Manage Themselves?

- TCP congestion control
  - Senders react to congestion
  - Decrease sending rate
  - But… the TCP sessions receive lower throughput
- IP routing protocols
  - Routers react to failures
  - Compute new paths
  - But… the new paths may be congested



Do IP Networks Manage Themselves?

- In some sense, yes:
  - TCP senders send less traffic during congestion
  - Routing protocols adapt to topology changes
- But, does the network run *efficiently*?
  - Congested link when idle paths exist?
  - High-delay path when a low-delay path exists?



Adapting the Routing to the Traffic

- Goal: modify the routes to steer traffic through the network in most effective way
- Approach #1: load-sensitive protocols
  - Distribute traffic & performance measurements
  - Routers compute paths based on load
- Approach #2: adaptive management system
  - Collect measurements of traffic and topology
  - Management system optimizes the parameters
- Debates still today about the right answer

Load-Sensitive Routing Protocols

- Advantages
  - Efficient use of network resources
  - Satisfying the performance needs of end users
  - Self-managing network takes care of itself
- Disadvantages
  - Higher overhead on the routers
  - Long alternate paths consume extra resources
  - Instability from out-of-date feedback information

Packet-Based Load-Sensitive Routing

- Packet-based routing
  - Forward packets based on forwarding table
- Load-sensitive
  - Compute table entries based on load or delay
- Questions
  - What link metrics to use?
  - How frequently to update the metrics?
  - How to propagate the metrics?
  - How to compute the paths based on metrics?

Balancing Load, Performance, and Cost

- Balance traffic based on link capacity
  - Measure outbound traffic per prefix
  - Select provider per prefix for even load splitting
  - But, might lead to poor performance and high bill
- Balance traffic based on performance
  - Select provider with best performance per prefix
  - But, might lead to congestion and a high bill
- Balance traffic based on financial cost
  - Select provider per prefix over time to minimize the total financial cost
  - But, might lead to bad performance

A Fundamental Problem

- Everyone is acting alone
  - Internet is highly decentralized
  - Each AS is adapting its routes alone
- Toward greater coordination
  - End hosts or edge routers pick the entire path?
  - Neighbor ASes cooperate to pick better paths?
- A largely unsolved problem
  - The price of anarchy
  - Is there a better way?

Conclusions

- Adapting routing to the traffic
  - To alleviate congestion
  - To minimize propagation delay
  - To be robust to future failures
- Two main approaches
  - Load-sensitive routing protocol
  - Optimization of configurable parameters

Add New Features in an Overlay: Resilient Overlay Networks

Overlays

- Motivation
  - Problems with the underlying routing system
  - Source routing, overlay networks, and hybrids
- Overlay networks
  - Pros: flexibility, limited overhead, & value-added
  - Cons: data-path overhead, probes, & feedback
- Negative interactions
  - With other overlays: the price of anarchy
  - With the underlay: influence on traffic engineering
  - With itself: bi-stability and trunk reservation
- Future directions

What's Wrong With Internet Routing?

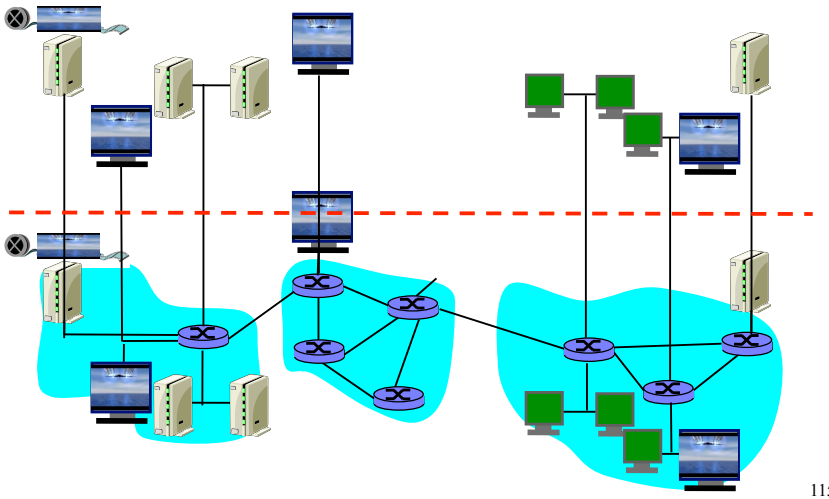
- Restrictive path-selection model
  - Destination-based packet forwarding
  - Single best BGP path per prefix
  - BGP routing constrained by policies
  - Ignoring congestion and delay
  - Ignoring application requirements
- Unappealing protocol dynamics
  - Persistent oscillation (due to policy conflicts)
  - Slow convergence (due to path exploration)
  - Lost reachability (due to route-flap damping)

Stems from the need for routing to scale to millions of routers

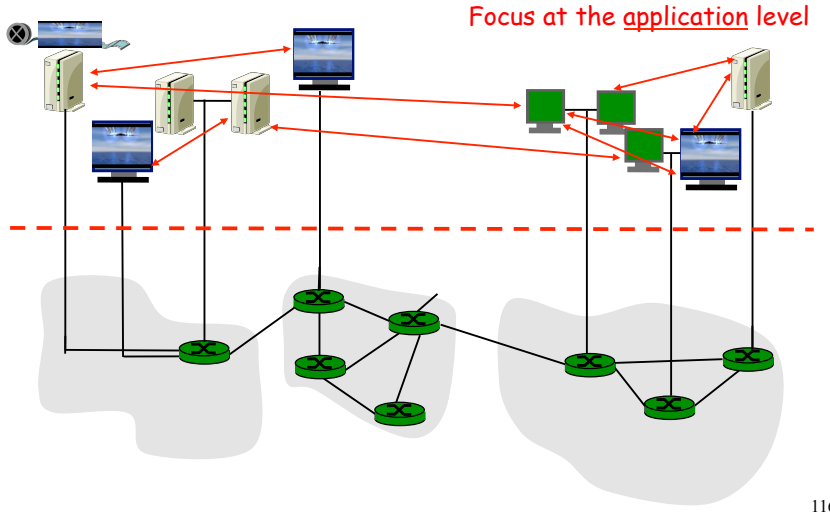
Putting More Power in End Hosts

- Source routing (e.g., Nimrod)
  - End host selects the end-to-end path
  - Routers simply forward packets on the path
  - Requires the routers to agree to participate
- Overlay networks (e.g., RON)
  - Conventional computers act as logical routers
  - Real routers deliver packets to intermediate hosts
  - No need for cooperation from the real routers
- Hybrid schemes
  - Source routing at the AS level
  - Source routing in the overlay network

Overlay Networks

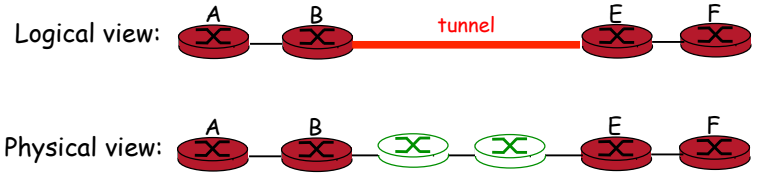


Overlay Networks



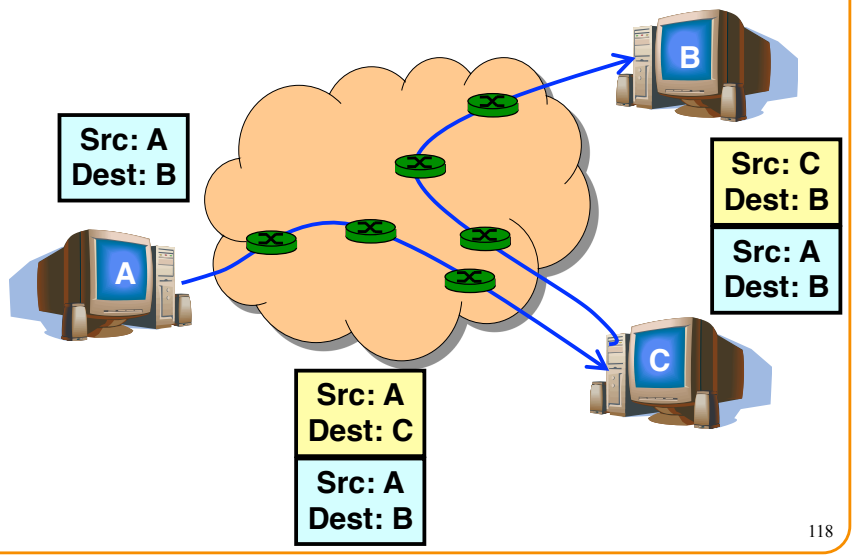
IP Tunneling to Build Overlay Links

- IP tunnel is a virtual point-to-point link
  - Illusion of a direct link between two separated nodes



- Encapsulation of the packet inside an IP datagram
  - Node B sends a packet to node E
  - … containing another packet as the payload

Tunnels Between End Hosts

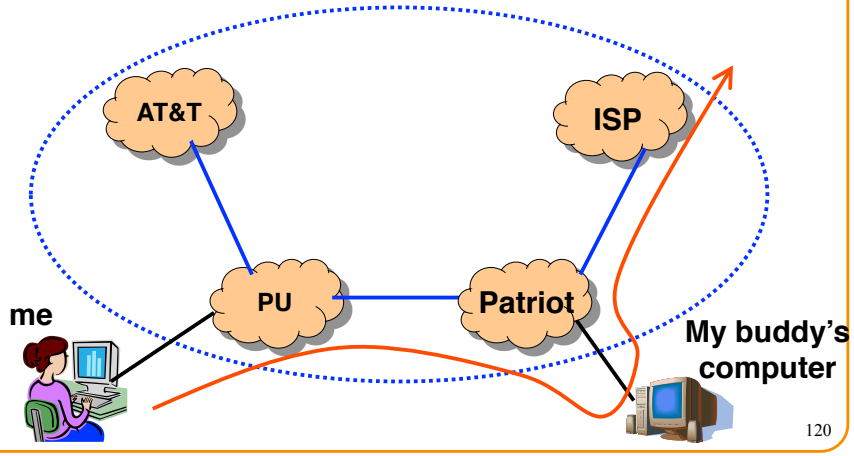


Overlay Networks

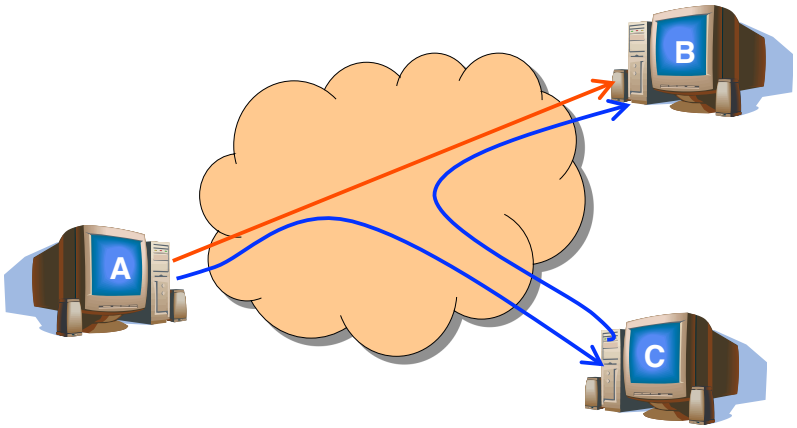
- A logical network built on top of a physical network
  - Overlay links are tunnels through the underlying network
- Many logical networks may coexist at once
  - Over the same underlying network
  - And providing its own particular service
- Nodes are often end hosts
  - Acting as intermediate nodes that forward traffic
  - Providing a service, such as access to files
- Who controls the nodes providing service?
  - The party providing the service
  - Distributed collection of end users

Circumventing Policy Restrictions

- IP routing depends on AS routing policies
  - But hosts may pick paths that circumvent policies

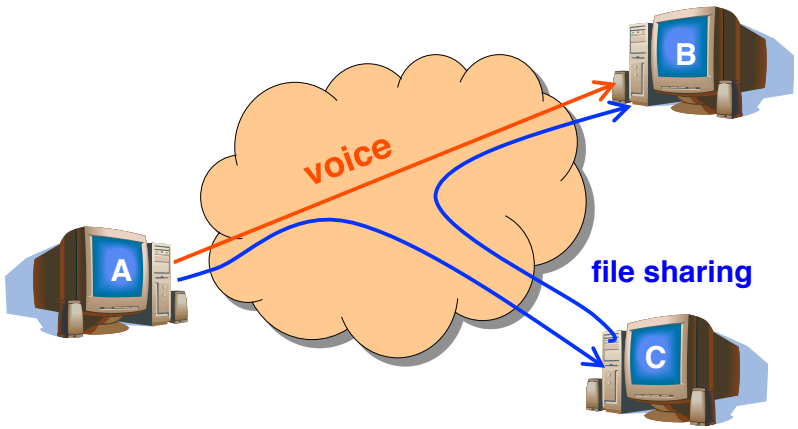


Adapting to Network Conditions



- Start experiencing bad performance
  - Then, start forwarding through intermediate host

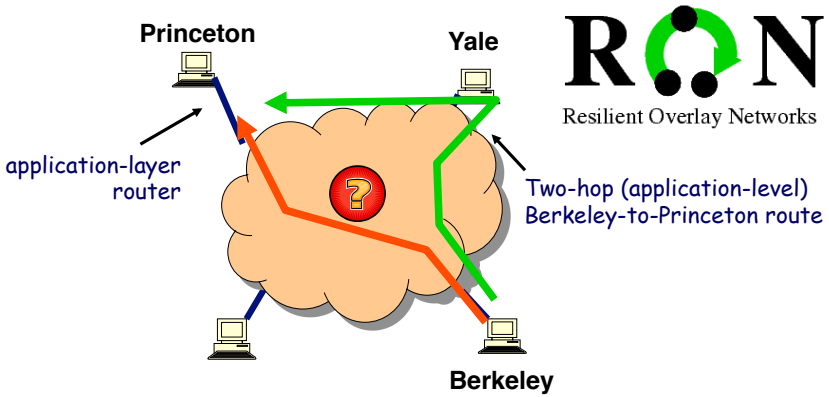
Customizing to Applications



- VoIP traffic: low-latency path
- File sharing: high-bandwidth path

RON: Resilient Overlay Networks

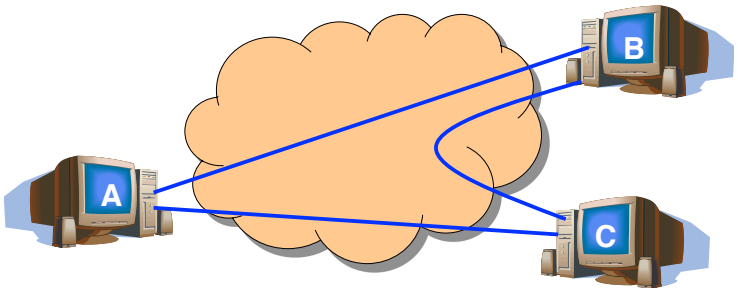
Premise: by building application overlay network, can increase performance and reliability of routing



http://nms.csail.mit.edu/ron/

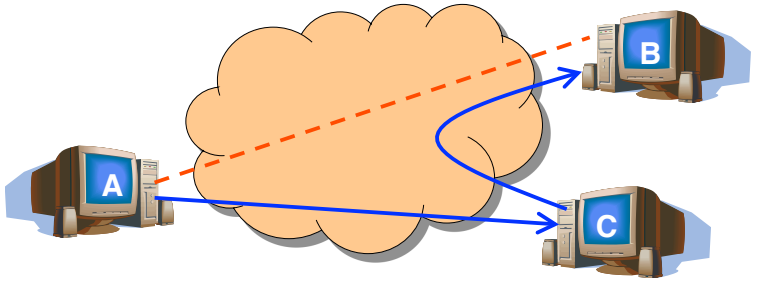
How Does RON Work?

- Keeping it small to avoid scaling problems
  - A few friends who want better service
  - Just for their communication with each other
  - E.g., VoIP, gaming, collaborative work, etc.
- Send probes between each pair of hosts



How Does Ron Work?

- Exchange the results of the probes
  - Each host shares results with every other host
  - Essentially running a link-state protocol!
  - So, every host knows the performance properties
- Forward through intermediate host when needed



RON Works in Practice

- Faster reaction to failure
  - RON reacts in a few seconds
  - BGP sometimes takes a few minutes
- Single-hop indirect routing
  - No need to go through many intermediate hosts
  - One extra hop circumvents the problems
- Better end-to-end paths
  - Circumventing routing policy restrictions
  - Sometimes the RON paths are actually shorter

RON Limited to Small Deployments

- Extra latency through intermediate hops
  - Software delays for packet forwarding
  - Propagation delay across the access link
- Overhead on the intermediate node
  - Imposing CPU and I/O load on the host
  - Consuming bandwidth on the access link
- Overhead for probing the virtual links
  - Bandwidth consumed by frequent probes
  - Trade-off between probe overhead and detection speed
- Possibility of causing instability
  - Moving traffic in response to poor performance
  - May lead to congestion on the new paths

Should All This Bother ISPs?

- Overlays circumventing routing policies
  - Sending traffic on paths that are not permitted
  - But, then again, the stub ASes are paying their bills!
- Overlays introducing unexpected shifts in traffic
  - Routing changes at multiple layers may interact
  - But, then again, small overlays may have little impact
- Overlays competing with provider services
  - Why pay for better performance, or commercial VoIP?
  - When you can get by with a little help from your friends
  - But, is the cost-performance trade-offs worth it?

Advantage: Flexible Routing

- Paths that violate BGP routing policy
  - E.g., A to C goes through AT&T and Sprint
  - … and C to B goes through UUNET
  - BGP would not allow AT&T-Sprint-UUNET path
- Quick adaptation to network problems
  - Fast detection of congestion and outages
  - … by probing as aggressively as necessary
- Selecting paths based on different metrics
  - E.g., overlay selects paths based on latency
  - … whereas the underlay might try to balance load

Advantage: Fewer Worries About Scalability

- Small number of nodes
  - Just enough nodes to have diverse paths
  - A few friends who want better service
  - Virtual Private Network of several corporate sites
- Balancing the trade-offs
  - High probe frequency for maximum adaptivity
  - Low probe frequency for minimum overhead
- Simple routing protocol
  - Link-state protocol to learn probing results
  - Selecting a good intermediate hop when needed

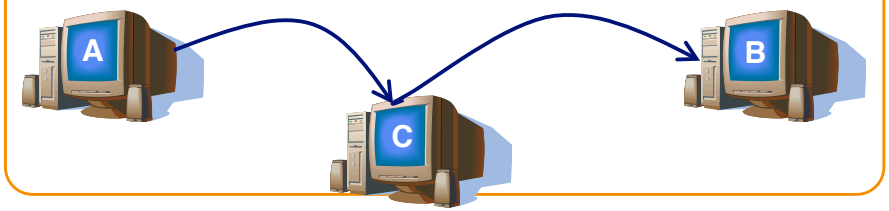
Deploy multiple small overlay networks, if necessary

Advantage: Customizing Packet Delivery

- Recovering from packet loss
  - Packet retransmission
  - Forward error correction
- Quality-of-service differentiation
  - Classify packets based on header bits
  - Schedule packet transmissions based on result
- Incremental deployment of new features
  - Multicast communication (e.g., MBone)
  - IPv6 (e.g., 6Bone)
  - Encryption of packet contents

Disadvantage: Traversing Intermediate Nodes

- Processing delay
  - Packets going through multiple software nodes
- Network performance
  - Propagation delay on circuitous path
  - Network congestion from extra load
- Financial cost
  - Bill for traffic going in/out of intermediate node



Disadvantage: Limitations of Active Probes

- Bandwidth overhead
  - Probe traffic between two nodes
  - Propagating probe results to other nodes
- Limited accuracy of end-to-end probes
  - Available bandwidth of logical link?
  - Losses due to congestion vs. failure?
  - Problem on forward vs. reverse path?
- Limited visibility
  - Logical links may share underlay routers/links
  - May be hard to detect the dependencies

Disadvantage: Feedback Effects

- Background traffic
  - Overlay traffic consumes extra resources
  - … at the expense of regular background traffic
  - But, the overlay traffic *does* get out of the way!
- Other overlays
  - Potential competition between multiple overlays
  - E.g., one overlay picks a (longer) alternate path
  - … and extra load causes another overlay to adapt
- Underlying network
  - Overlay network changes the traffic matrix
  - … forcing operators to adapt the underlay routing

Are these effects significant? Any positive effects?

Discussion

- Should we try to fix the underlying network?
  - Do overlays exist only because regular people aren't allowed to change the way the network works?
  - Or, is it fundamentally hard to improve the network? Perhaps we can't really do much better?
  - Even if we knew how to fix it, could we ever deploy the solution anyway?
- How should ISPs react to overlay services?
  - Happily charge money for the access bandwidth?
  - Offer overlay services of their own?
  - Make their networks simple and let the overlays adapt?
  - Add support to the routers to make overlays work better?

Discussion

- Are overlay networks a good idea?
  - Just a hack to avoid changing the underlay?
  - What if we could "fix" the underlying network?
  - Would we still have a need for overlay networks?
- Should we have overlay-friendly underlays?
  - Or underlay-friendly overlays, or both?
  - Visibility, control, economics, efficiency, …
  - Or, are the two systems inherently at odds?
- What about interactions between overlays?
  - Cooperate to reduce measurement cost and prevent suboptimality and instability?
  - Compete because that's the way life works?

Using Overlays to Evolve the Internet

- Internet needs to evolve
  - IPv6
  - Security
  - Mobility
  - Multicast
- But, global change is hard
  - Coordination with many ASes
  - "Flag day" to deploy and enable the technology
- Instead, better to incrementally deploy
  - And find ways to bridge deployment gaps

Conclusions

- Overlays
  - Enables innovation in routing and forwarding
  - … without changing the underlying network
- Interaction effects
  - With background traffic
  - With other overlays
  - With traffic engineering
- Avenues for new work
  - Possibility the interaction effects are good?
  - Ensuring stability and efficiency are achieved?
  - Right interplay between underlay and overlay?

Conclusions

- Overlay networks
  - Tunnels between host computers
  - Hosts implement new protocols and services
  - Effective way to build networks on top of the Internet
- Benefits of overlay networks
  - Customization to the applications and users
  - Incremental deployment of new technologies
  - Ironically, may perform better than underlying network