Network Virtualization & Network Security

2015-04-28

Announcements

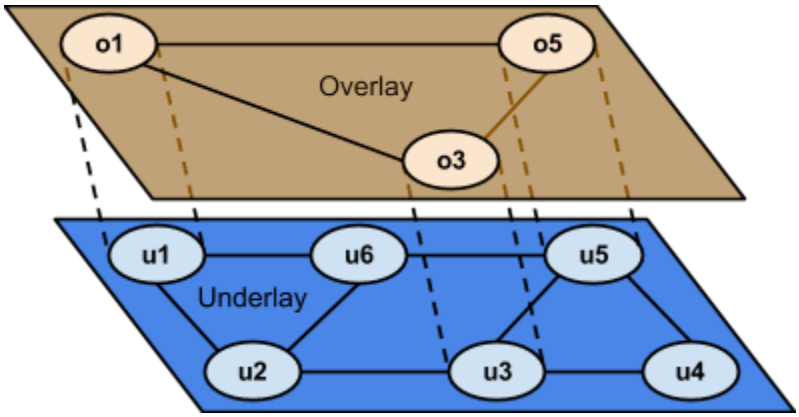
- Quiz #6 on Thursday

Outline

- Network virtualization
- Constructing overlays
- Resilient overlay networks
- Security threats and defenses

Network Virtualization

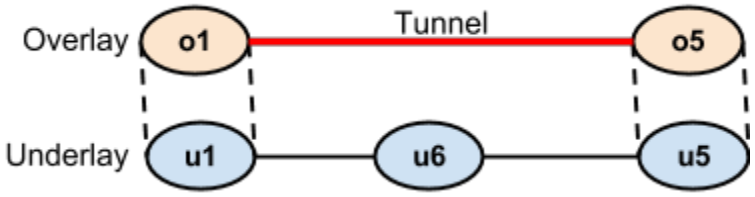
- Run a network on top of a network
- Similar to running a virtual machine on top of a machine
- Underlay network
    - Internet, data center network, campus network, or other network spanning 1+ admin domains
    - Topology = physical topology
    - IP addresses = globally unique addresses (or private addresses + NAT)
- Overlay network
    - Provides the illusion of a network with a different topology and address space



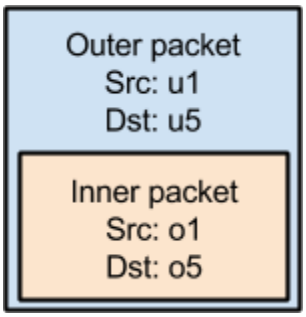
    - Forwarding decisions in the overlay network are made by overlay nodes, which are programmed/configure by whoever created the overlay network
- Layers of abstraction
    - Switches/routers in underlay are unaware of overlay -- from underlay's perspective, overlay traffic is regular IP traffic
    - Applications using the overlay are unaware of underlay -- from application's perspective, overlay is a regular network
- ***Why do we want overlay networks?*
    - Better control of performance
    - Isolation
    - Introduce new functionality -- e.g., custom routing applications

Constructing Overlay Networks

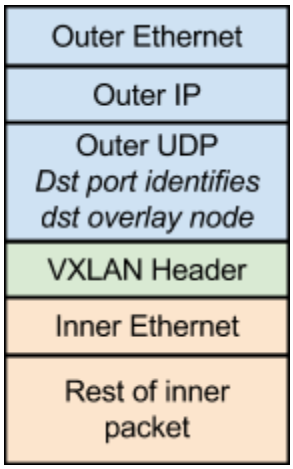
- Virtual links
  - Tunnels create the illusion of point-to-point links



  - ***Where else have we seen tunnels?* -- IPv4 over IPv6, and vice versa
  - Key idea: encapsulation
    - o1 puts packet destined for o5 inside another packet



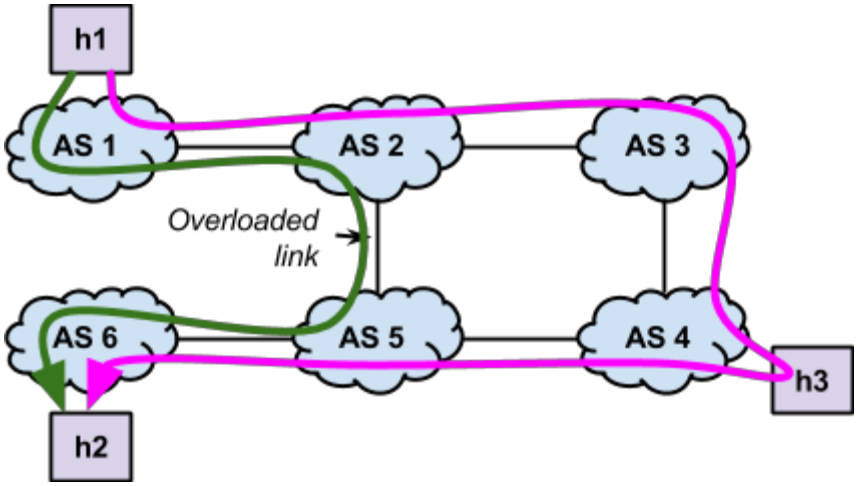
      - Headers of outer packet contain addresses routable in the overlay
    - o1 passes full packet to u1
    - u1 forwards full packet to u6, which forwards to u5
    - u5 passes full packet to o5
    - o5 removes inner packet, and processes accordingly
  - Concrete protocol: VLXAN
    - Provides Ethernet-in-UDP encapsulation



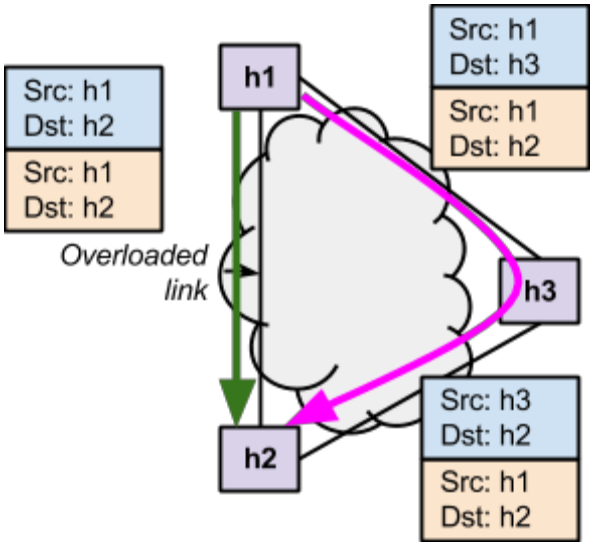
- Virtual switches/routers
  - Implement forwarding/routing in the overlay
    - May implement standard distance vector, link state, or BGP routing
    - Or, use custom routing algorithms
  - Responsible for encapsulation/decapsulation for tunnels
  - Usually implemented on end hosts, not physical switches/routers
    - Use custom application
    - Or, standard virtual switch software -- e.g., Open vSwitch

Example: Resilient Overlay Networks (RON)

- Motivation: try to fix limitations of today's BGP-based routing without cooperation from ASes
  - Routing is subject to ISP's policies
  - Want better performance and resiliency
- Construct application-specific overlay
  - Establish tunnels between a set of end-hosts running a specific application
  - Application traffic sent via one or more end-hosts to reach destination end-host
- Underlay view



- Overlay view



- Periodically measure performance of each virtual link (composite of performance of physical links) to compute the "best" paths between hosts in the overlay
- Keep overlay network small to avoid scaling problems
- Benefits
  - Better end-to-end paths
  - In most cases, one indirect hop is enough
- Limitations
  - Software delays at hosts to forward to next hop host
  - Resource overhead (CPU, memory, network) on intermediate hosts
  - Network overhead for measuring performance of virtual links

Network Security

- ***What network-related attacks must we defend against?*
  - Unauthorized access to hosts (e.g., SSH)
    - Often depends on carefully crafted packets or data
  - Sending malicious code to hosts (e.g., viruses, worms)
  - Denial of Service (DoS) -- causes bottlenecks that prevent legitimate access
    - If many hosts are used to launch the attack (e.g., hosts in a botnet), it's called a distributed denial of service attack (DDoS)
    - Often, set up lots of TCP connections but not send any data -- consumes host resources to perform handshake and maintain connection state
  - DNS hijacking -- resolve domain names to IP address for servers with malicious code or phishing sites
  - Route hijacking -- send BGP announcements for prefixes you do not own or cannot reach
  - Eavesdropping on data
- ***How do we protect against these attacks?*
  - Encryption -- make sure data remains confidential
  - Authentication -- identify and assure origin of information; e.g., communicating with your bank
  - Middleboxes -- firewalls, intrusion prevention systems
  - Software on end-hosts -- anti-virus, firewall