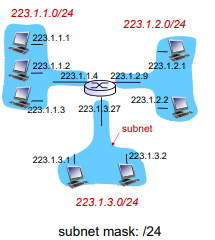
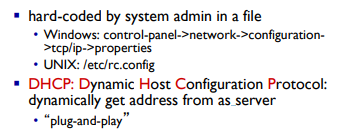
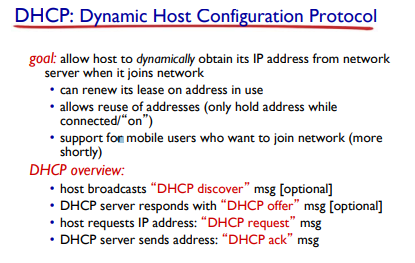
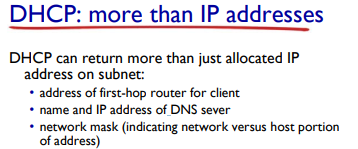
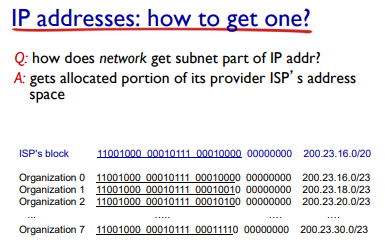
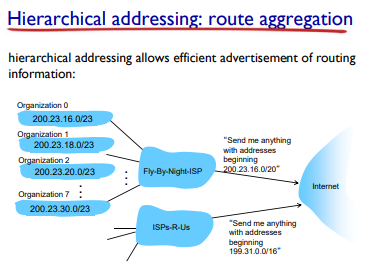
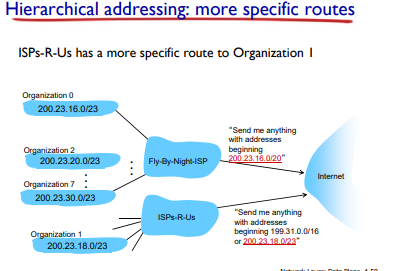
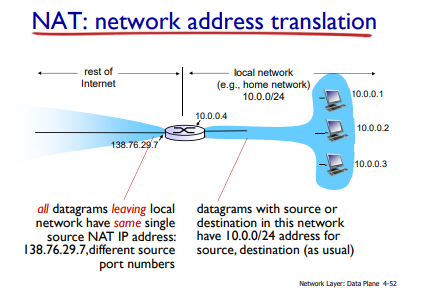
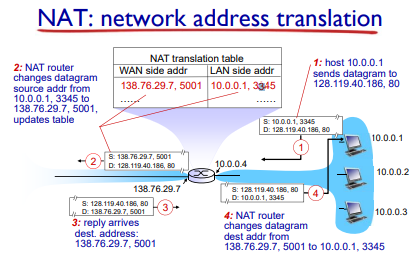
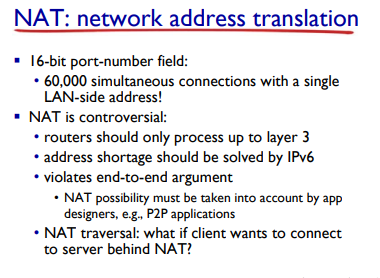
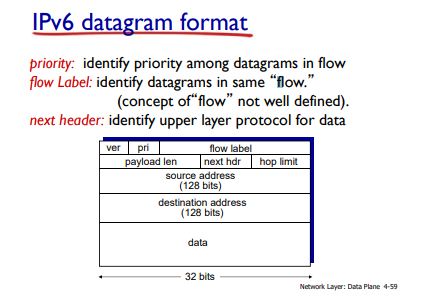
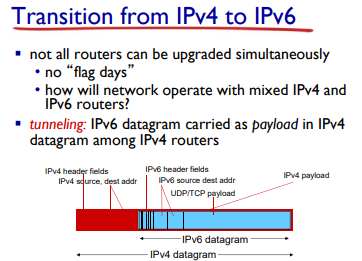
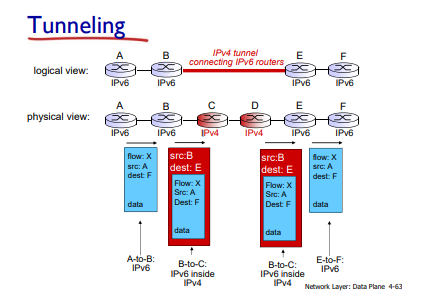
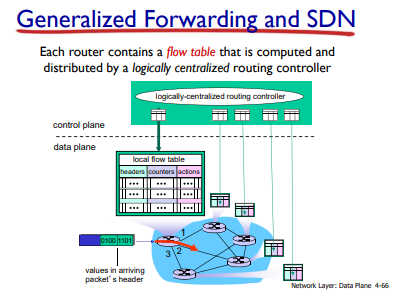
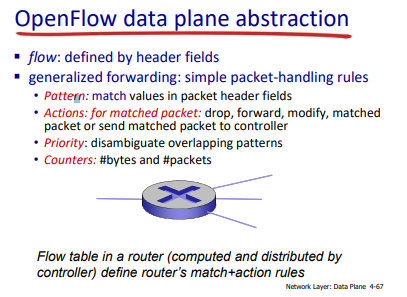
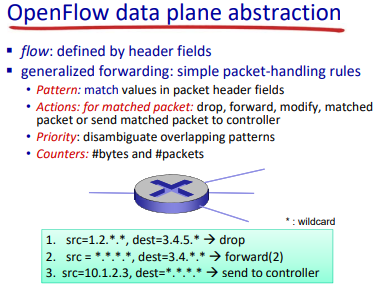
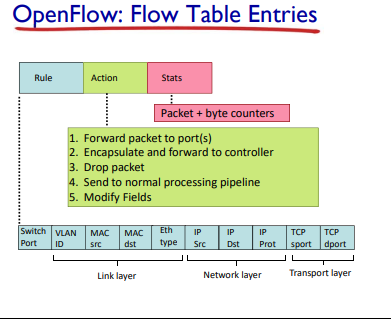
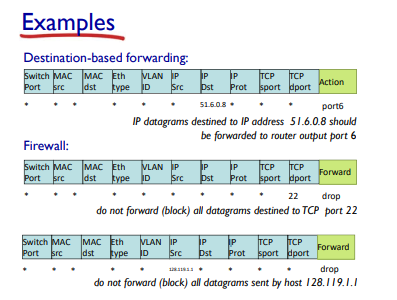
* IP Addressing
  + 32-bit identifier for host, router interface
  + Inference: connection between host/router and physical link
    - Router’s typically multiple interfaces
    - Host typically has one or two interfaces (eg wired ethernet, wireless 802.1
  + IP addresses associated with each interface
* Subnet
  + IP Address
    - Subnet part - higher order bits
    - Host part - low order its
  + What?
    - Device interface with same subnet part of IP Address
    - Can physically reach each other without intervening router
  + How?
    - To determine the subnets, detach each inference from its host or router, creating islands of isolated networks
    - Each isolated network is called a subnet.
* CIDR: Classless InterDomain Routing
  + Subnet portion of address of arbitrary length
  + Address format: a.b.c.d/x where x is # bits in subnet portion of

Address.

* How to get IP
  + 
* DHCP
  + 
* 
* How to get IP Address
  + 
* Hierarchical addressing: route aggregation
  + 
* 
* NAT: Network Address Translation
  + 
  + Motivation: local network uses just one IP address as far as outside world is concerned.
    - Range of addresses not need from ISP: just one IP address for all devices
    - Can change address of devices in local network without notifying outside world
    - Can change ISP without changing address of devices in local network
    - Devices inside local net not explicitly addressable visible by outside world (a security plus)
  + Implementation: NAT router must:
    - outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #) . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr
    - remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair
    - incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table
  + 
  + 
* IPv6
  + Initial motivation: 32-bit address space soon to be completely allocated.
  + Additional motivation
    - Header format helps speed processing/forwarding
    - Header changes to facilitate QoS
  + IPv6 datagram format:
    - Fixed-length 40 byte header
    - No fragmentation allowed
* 
* Changes with IPv4
  + Checksum: removed entirely to reduce processing time at each hop
  + Options: allowed, but outside of header, indicated by “next header” field
  + ICMPv6: new version of ICMP
    - Additional messages types, eg “Packet too Big”
    - Multicast group management functions.
* Transition from IPv4 to IPpv6
  + 
* Tunneling
* 
* Generalizing Forwarding and SDN
  + 
* OpenFLow data plane abstraction
  + 
  + 
* 
* 
* OpenFlow Abstraction
  + Match + action: unified different kind of devices
  + Router:
    - Match: longest destination IP prefix
    - Action: forward out a link
  + Switch:
    - Match: destination MAC address
    - Action: forward or flood
  + Firewall:
    - Match: IP addresses and TCP/UDP port numbers
    - Action: permit or deny
  + NAT:
    - Match: IP address and port
    - Action: rewrite address and port
* 