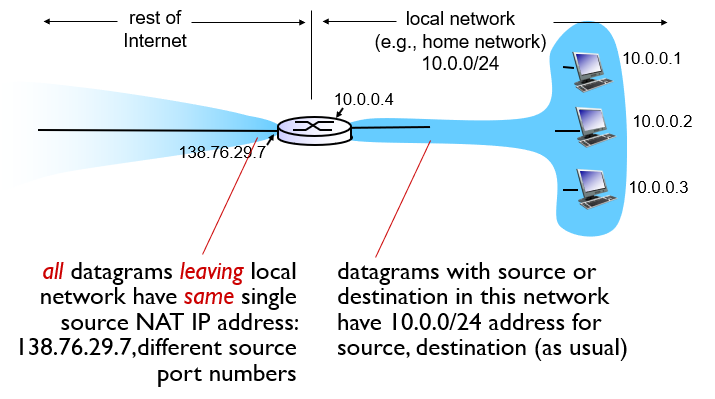
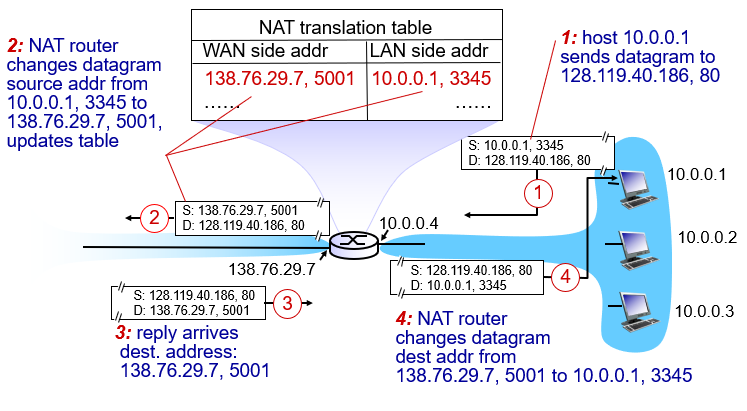
# Network Layer – Part 3

## Network Address Translation (NAT)



* motivation: local net uses just one IP address as far as outside world is concerned:
  + range of addresses not needed from ISP; just one IP address for all devices
  + can change addresses of devices in local net without notifying outside world
  + can change ISP without changing addresses of devices in local network
  + devices inside local net not explicitly addressable/visible by outside world (a security plus)
* *implementation:* NAT router must:
  + 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
  + replace (NAT IP address, new port #) in dest fields of every **incoming** datagram with corresponding (source IP address, port #) stored in NAT table

  
*How NAT works*

## Internet Control Message Protocol (ICMP)

Type Code description

0 0 echo reply (ping)

3 0 dest. network unreachable

3 1 dest host unreachable

3 2 dest protocol unreachable

3 3 dest port unreachable

3 6 dest network unknown

3 7 dest host unknown

4 0 source quench (congestion

control - not used)

8 0 echo request (ping)

9 0 route advertisement

10 0 router discovery

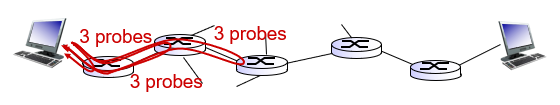
11 0 TTL expired

12 0 bad IP header

* used by hosts & routers to communicate network-level information
  + error reporting: unreachable host, network, port, protocol
  + echo request/reply (used by ping)
* network-layer “above” IP:
  + ICMP msgs carried in IP datagrams
* ICMP message: type, code plus first 8 bytes of IP datagram causing error

## Traceroute and ICMP

* source sends series of UDP segments to dest
  + first set has TTL =1
  + second set has TTL=2, etc.
  + unlikely port number
* when *n*th set of datagrams arrives to nth router:
  + router discards datagrams
  + and sends source ICMP messages (type 11, code 0)
  + ICMP messages includes name of router & IP address
* when ICMP messages arrives, source records RTTs
* *stopping criteria:*
  + UDP segment eventually arrives at destination host
  + destination returns ICMP “port unreachable” message (type 3, code 3)
  + source stops



## Routing

* **Unicast** - one computer to another computer
* **Broadcast** - one computer to all computers in the network
* **Multicast** - one computer to a group of computers (e.g., videoconference)
  + Same data needs to reach multiple receivers and avoid transmitting it once for each receiver
  + Particularly useful if access link has bandwidth limitations
  + Many implementations at different layers
  + In IP multicast, hosts dynamically join and leave multicast groups using Internet Group Management Protocol (IGMP)

## Routing Algorithm Classification

* Global vs Decentralized:
  + In global routing, all routers have complete topology, link cost info; example is “link state” algorithms.
  + In decentralized routing, router knows physically-connected neighbors, link costs to neighbors; this is an iterative process of computation, exchange of info with neighbors; example is “distance-vector” algorithms
* Static vs Dynamic
  + In static routing, routes change slowly over time
  + In dynamic routing, routes change more quickly, periodically updating in response to link cost changes.