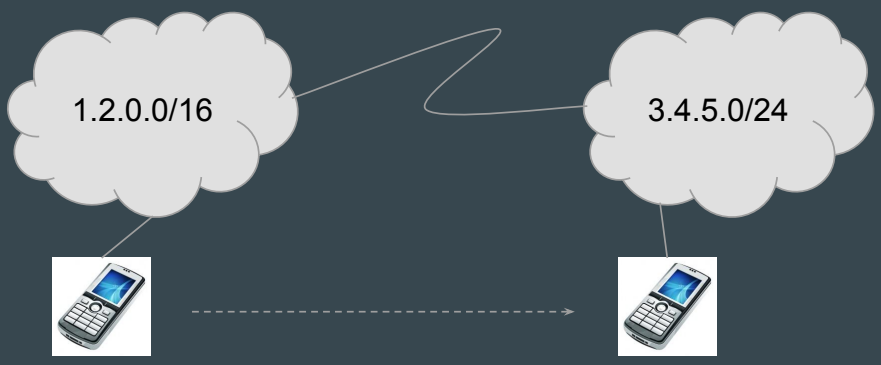
Mobile IP

- Ability to retain IP address while being mobile
- Ordinarily, it does not:



We really want to be able to maintain our ipaddress as we move around and jump between networks. Currently no one actually does this, but it'd be cool.

Mobile IP - basic ideas

- Mobile host has a “home network”
- Host’s IP address is in the subnet of its home network
- When in home network, just like any other host
- When in foreign network, it retains its IP address from home
  - Special kind of forwarding needed

Basically we do special routing when an device is on a foreign network.

Assumptions from RFC 5944

"...no additional constraints on the assignment of IP addresses. That is, a mobile node can be assigned an IP address by the organization that owns the machine."

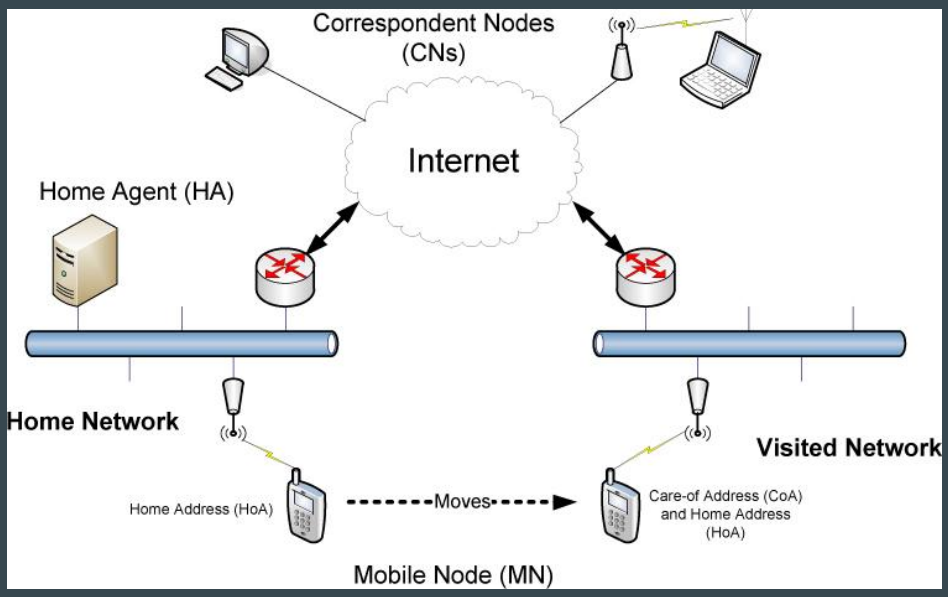
"...mobile nodes will generally not change their point of attachment to the Internet more frequently than once per second."

"...IP unicast datagrams are routed based on the Destination Address in the datagram header (and not, for example, by source address)."

The RFC for mobile routing makes some assumptions. The big one is the assumption that all routing is destination address based. This is not necissarily true because people will often put values in and use those to take short cuts to speed up internet.

Applicability

- “Macro” vs. “micro” mobility
  - Distinction: does host retain IP address or not?

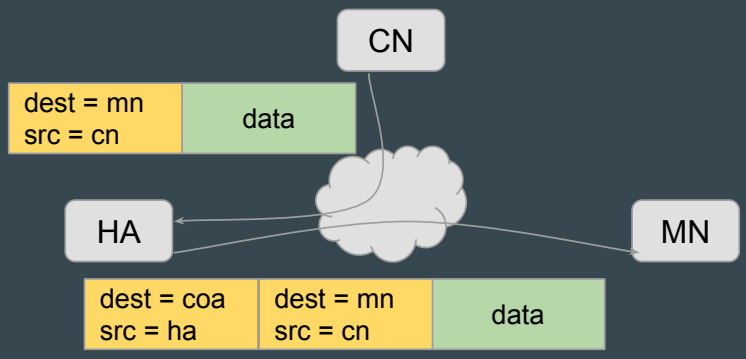

Correspondent Nodes
(CNs)
Internet
Home Agent (HA)
Home Network
Visited Network
Home Address (HoA)
Moves
Care-of Address (CoA)
and Home Address
(HoA)
Mobile Node (MN)

How it works

- Mobile node acquires a “Care-Of Address,” (CoA)
- Mobile node sends a “binding update” to Home Agent (HA)
- HA forwards messages between mobile node and Correspondent Nodes (CNs) using *tunneling*
    - An implementation of tunneling: *encapsulation*

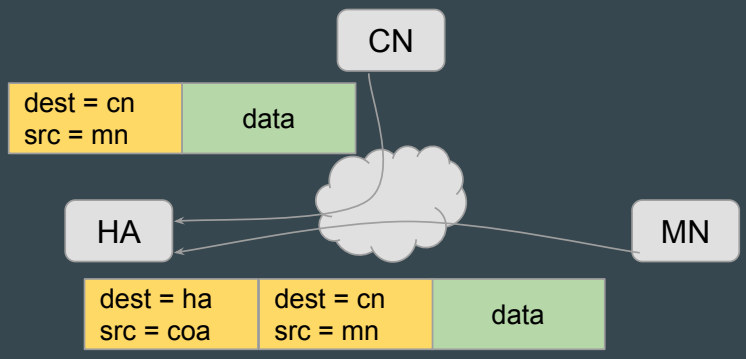
Each device actually get two addresses, the one it has on the home address and the care of address from the foreign network. When the mobile device joins a foreign network it notifies the home agent what its new care of address. The home agent passes packets from the device to corresponding nodes, called **tunneling**.

CN → MN



A common form of tunneling is encapsulation. This is basically just appending another header with new data onto the packet.

MN → CN



While a mobile address is on a foreign address its legitimate address is its home address, but it can send out a packet saying that the source address is its care of address.

Variants

- A *foreign agent* may be tunnel-termination point at visited network
- *Route optimization*:
  - MN informs CN of move
  - CN sends packets directly to CoA
  - Need a kind of “hand off” from HA

Mobile routing adds a bunch of hops which can slow things down. To optimize this the mobile node passes a bunch of data around to try to notify everyone (its a stupid complicated thing, don't bother learning too much about it).

Question - how would HA work?

How does HA become a proxy for the MN in the home network?

- How does it get IP packets destined for MN to be forwarded to it?

Host choices with regards IP datagrams

If a host is multi-homed:

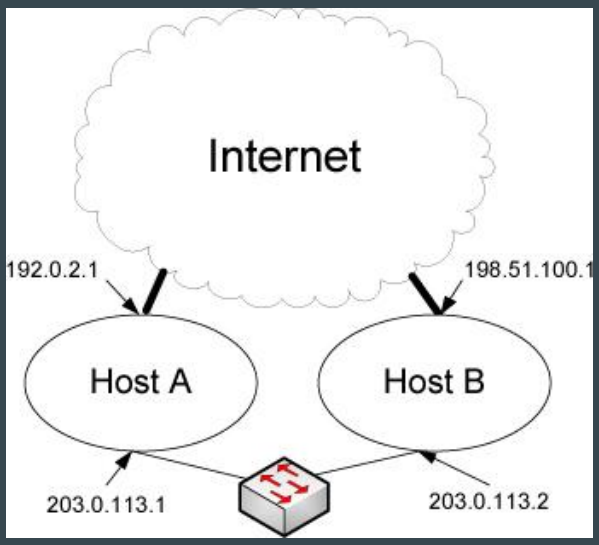
- Issue 1: if packet is received on interface i, what destination addresses are considered valid for acceptance?
- Issue 2: which interface should it use to send out a particular IP packet?

Issue 1

- *Strong host*: accept only IP packets whose destination address corresponds to interface.
- *Weak host*: accept IP packets whose destination address corresponds to any interface.

Why is this a big deal?

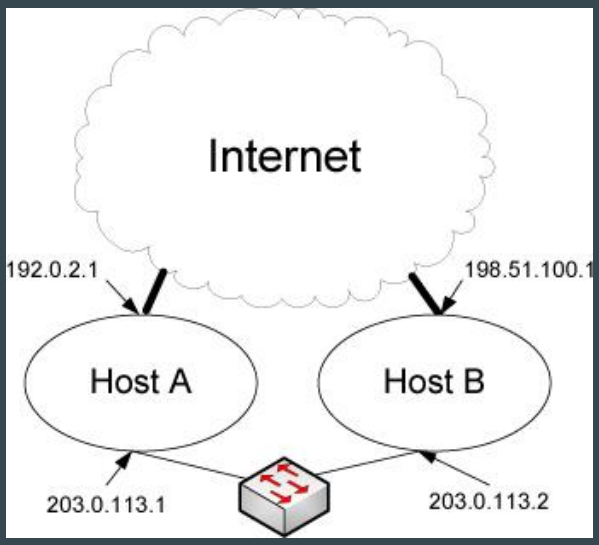
There are two models discussed for problem 1. Strong hosts only look for packets going to a specific interface, and weak hosts look for a packet going to any interface. With weak host models.



- If Host A is a strong host, Host B cannot send packets destined for 192.0.2.1 via local network.
- If Host B is weak host, attacker from Internet may spoof packet and make it appear as though it originated in local network.

A host B might want to address a packet to the public interface of host A (not to its internal ethernet address) if it is using a domain name service to find it. You could also have an application that only binds itself to the public ipaddress of A. Problems can occur if you mix strong and weak hosts. For instance a weak host cannot sent to a strong host and attackers can spoof a packet to look like it originates from the local network (like its id is 2030.113.2) then the weak host will think its trusted and forward it making it seem more trustworthy than it actually is.

Ipaddress spoofing is when someone lies about their source address.



- If Host A is a strong host, Host B cannot send packets destined for 192.0.2.1 via local network.
- If Host B is weak host, attacker from Internet may spoof packet and make it appear as though it originated in local network.

Issue 2: address selection

- Particularly an issue with “dual-stack” hosts
  - Host runs both IPv4 and IPv6 on same interface
- Multiple addresses configured on same interface

Issues 2, contd.

Follow a bunch of rules to choose from amongst possibilities.

Similar rules for selection of destination and source address.

Intent of rules: establish a partial-order of possibilities.

What address do we use as the source address when we send something? Basically we just come up with some rules to decide. This is a common problem for load balancing.