Mobility in the Internet
Part II

CS 444N, Spring 2002

Instructor: Mary Baker

Computer Science Department

Stanford University

TRIAD approach

- Host on network gets temporary local name
- Host still contactable through home network
  - Home directory service is like a home agent
  - Home directory provides a redirect to temporary *name*
- If mobile host moves
  - Relay agents can forward packets for fast handoff
  - Local relay agents are like foreign agents
- Still contactable through real name at home network
  - Must register new address with home service
  - This is important if MH and CH both move
  - After how long do you re-contact home base?

TRIAD advantage?

+ Changes all made at naming level
+ Implies traffic doesn't need to flow through home net
  - But this assumes smart correspondent hosts
- Ultimately not much difference between TRIAD and mobile IP for mobility
- (There's no free lunch.)

TCP-level mobility support

- Use dynamic DNS for initial name lookup
- If name changes during a connect, use TCP migrate option
- If name changes between DNS lookup and TCP connection, then do another DNS lookup

TCP-level advantages and disadvantages

+ No tunneling
+ No need to modify IP layer
+ Possibly more input from applications
- Requires secure dynamic DNS
- Scalability issue not entirely dismissable
- What if both endpoints are mobile?
- Need to modify multiple transport layers
- More transport-level changes required than IP-level additions
- Security issues more severe (1st paragraph of Section 5 is false)
- Requires application-level changes for DNS retries

Overall TCP-level questions

- Are IP address changes a routing responsibility or an application responsibility?
- Is this really end-to-end?
- With dynamic DNS requirements, application-level changes, and TCP changes, why not just do DNS retry every time a connection fails?

What do you need for mobile routing?

- A way to translate from name to location
  - Through a name service like DNS?
    - Inform name service whenever you move
    - Reverse name lookups may even work
    - Lots of updates for a global name service
  - Through a “home base” like Mobile IP and TRIAD?
    - “Home agent” that knows where you are
    - Packets may take a longer route or else you need mobile-aware correspondent hosts

What do you need for fast handoffs?

- Local agents?
  - Until they lead to long forwarding chains
  - Should still notify name service or home base
- Mobile-aware correspondent hosts?
  - Maintain bindings of names with real locations?
  - Mobile host or foreign agents may update this information
  - Communicate change directly to non-mobile end-point
  - A problem if both endpoints are mobile
  - May ultimately have to contact name service or home base again
- How do you know when to do that
  - After how many packets?
  - Continuous use of home base solves this problem at expense of slower paths

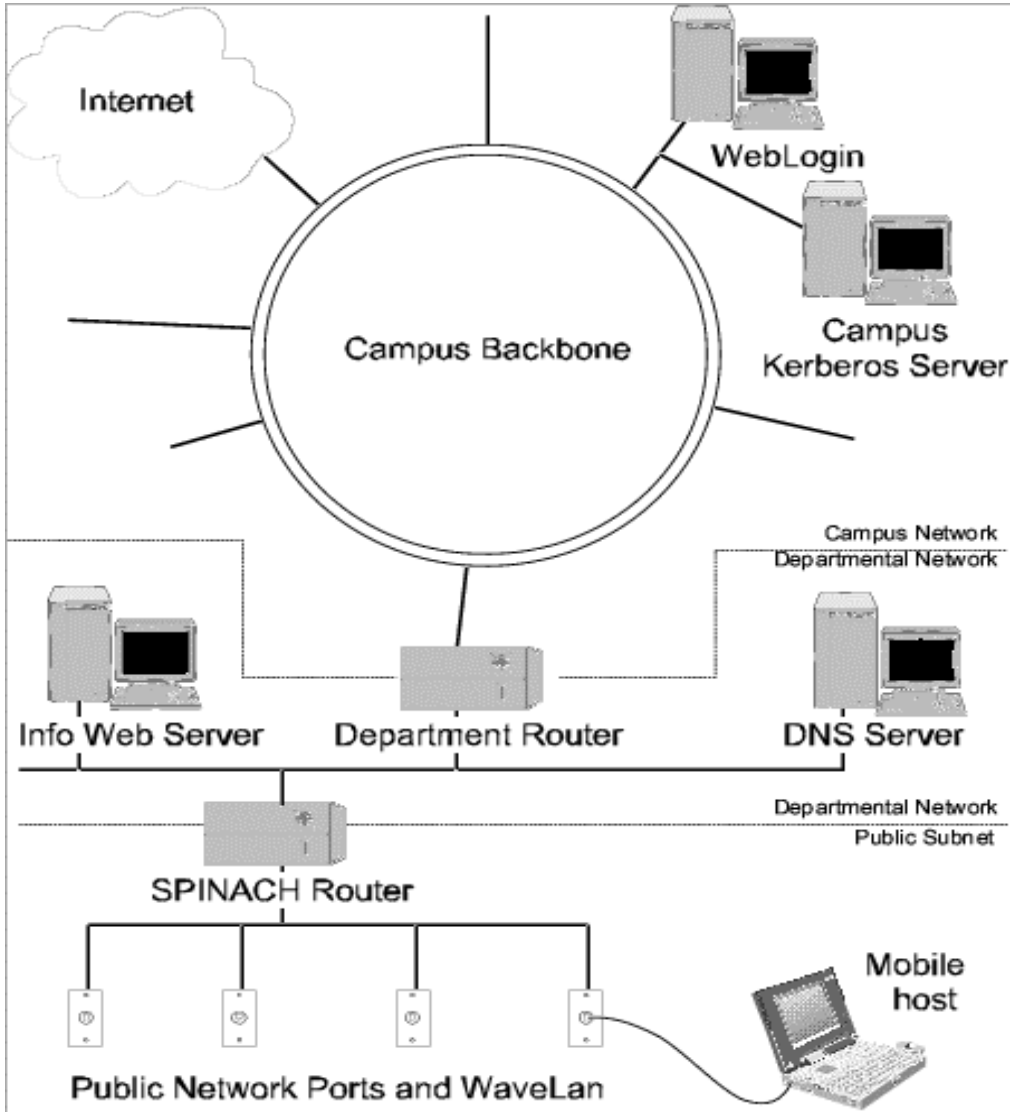
Providing networks for visitors

- The flip side of mobility
- Several questions:
  - For small or medium-sized institutions, who will create and maintain special visitor networks?
  - Can we instead leverage our own existing networks?
    - But do you trust visitors to use your own network?
- Solution requirements:
  - Enough security to make system administrators content
  - Ease of use and deployability
    - No special hardware or software on mobile hosts
    - No special hardware in network

Our visitor network solution

- Subnet(s) of existing net dedicated to visitors
- Inverse firewall (a “prison-wall”)
  - Visitor packets can’t get out unless authenticated
  - Life inside the subnet may be harsh
- Only requires browser with secure socket layer

SPINACH illustration



SPINACH vulnerabilities

- Window of vulnerability:
  - One user leaves system before lease times out
  - Another user spoofs previous user's IP/MAC address information
- Solutions:
  - Can be fixed with network hardware
  - May be reduced with "pings" from router to hosts
  - May be reduced with shorter leases
  - But users like longer leases
- Better solution might be PANS [Miu & Bahl, USITS 2001]

PANS

- Protocol for Authorization and Negotiation of Services
- Client can download necessary software from local agent
- Client and “gateway” negotiate session key
- Packets tagged with this key to prevent unauthorized traffic
- Overhead of packet tagging doesn’t seem too severe

SPINACH lessons learned

- Security is a spectrum with parameters
  - Airtight/awkward …….. Weak protection/easy to use
  - We aim for the middle in this case
  - With further facilities (software download, etc), ease of use migrates towards more secure solutions