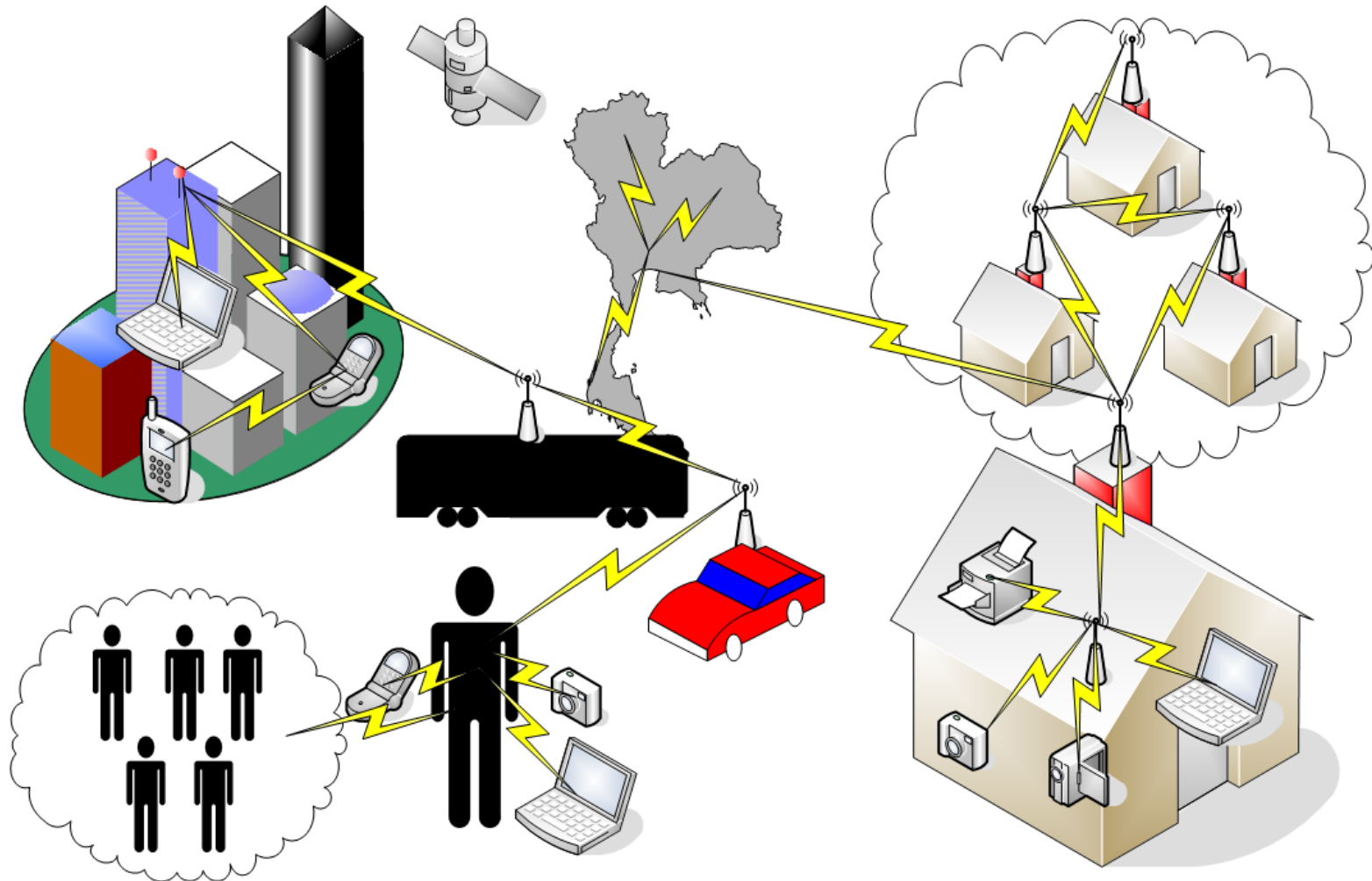


Mobile Networking

ITS 413 – Internet Technologies and
Applications

Next Generation Wireless Networks

Ubiquitous mobile access to Internet



Next Generation Wireless Networks

- Lets assume:
 - All communications are via IP (or similar packet switched) network
 - Data access, voice calls, video calls, radio, TV, video-on-demand, device control, ...
 - You (the user) want unrestricted access to the communication media anytime
 - Metropolitan network coverage
 - Coverage is available in buildings, streets, public transport, houses, across communities
 - Network access is available via usually more than one technology in all locations
 - Mobile phone (2G/3G), Wireless LAN hot spots, WiMax, Satellite
 - More than one network operator providing the service (different costs and quality)
- Example Scenarios
 - Home Area Networking
 - All devices are interconnected in your house
 - Personal: Phone, PDA, headset, camera, MP3 player, PC (and peripherals) ...
 - Entertainment: TVs, radio, game console, sound system, media players, ...
 - Control: A/C, lighting, security, watering system, ...
 - Appliances: fridge, washing machine, toilet?, ...
 - Vehicular Networking
 - The computer controllers in your car share information (tyre pressure, fuel level, speed, engine management, ...)
 - Your car receives updates on traffic conditions via roadside sensors and via data relayed via other cars
 - Consumer devices within the car are interconnected (stereo, DVD, game console, mobile phone, laptop), with Internet access (for data, voice/video calls, radio, video-on-demand) via satellite, WiFi, WiMax and/or relayed via other cars

Next Generation Wireless Networks

- Example Scenarios
 - Spontaneous or ad hoc networking
 - A group of users get together for a meeting and share information amongst their portable devices (phones, PDAs, laptops, MP3 players, ...)
 - Some of the users have direct access to wireless networks provided by operators (and hence to Internet); some users do not – they access via the users that do have access
 - Integration of all scenarios
 - A user moves between different networks/environments, all the time with no noticeable interruption in the communication services

Enabling Technologies

- What technologies will enable these scenarios?
 - Wired Networks
 - Even though many scenarios required freedom from wires, wired networks are still vital (providing access where possible; interconnecting networks; ...)
 - Wireless Networks (Physical, Data link layers)
 - Faster data rates, more efficient use of spectrum, energy efficiency, ...
 - 3G+ mobile networks: 14Mb/s download to mobile phone available
 - IEEE 802.16 (WiMax), IEEE 802.20: 10's Mb/s over km's
 - IEEE 802.11n (300Mb/s) and beyond
 - Internet Mobility (Network layer)
 - Ability to move between networks without changing your IP address (Host Mobility)
 - Ability for entire networks to move within Internet without changing network address or IP address of hosts on network (Network Mobility)
 - Infrastructure-less or Ad Hoc Networks (Network and other layers)
 - No longer rely on fixed (expensive) base stations with wired connections
 - Wireless connections between users for dynamic networks
 - Mesh networks, Mobile Ad Hoc Networks, Sensor Networks

Enabling Technologies

- What technologies will enable these scenarios?
 - Applications and Supporting Protocols (Transport, Application layers)
 - New applications that make it possible to use services across different networks
 - Video data rate automatically reduced when move from WiFi to WiMax
 - Take advantage of mobility
 - Location based services: maps, information updates, discovering services, ...
 - Devices
 - Support multiple wireless technologies
 - Many mobile phones have tri/quad-band 2G/3G access, Bluetooth, wireless LAN ... in future, WiMax and others (and your PDA, MP3 player, digital camera etc. also have access)
 - User interface
 - Energy efficiency
 - And many others ...
 - Security, quality of service, network management, ...
- Our Focus: Mobility Issues, especially at Layer 3 (Network)

Contents

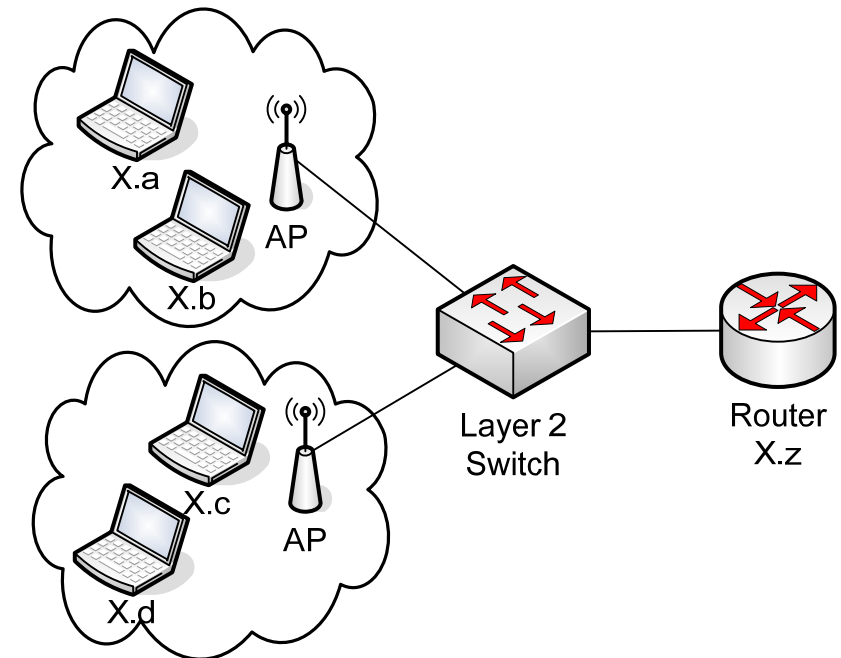
- Host Mobility
 - IP Mobility and Mobile IP
- Network Mobility
 - NEMO
- Ad Hoc Networking
 - MANETs

Host Mobility

Mobile IP

Assumptions: Wireless Access Networks

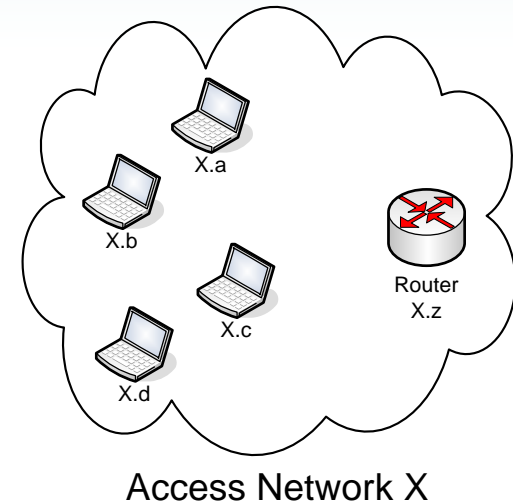
- Layer 2 technologies provide wireless access for mobile hosts
 - Wireless LAN, GSM, 3G, Satellite, Bluetooth, ...
- Mobility between layer 2 networks of same technology (owned by same person) is handled by layer 2 technology
 - Mobility between Wireless LAN APs within the same ESS is handled by IEEE 802.11
- But mobility between different access networks is harder!
 - Different technologies
 - Different owners



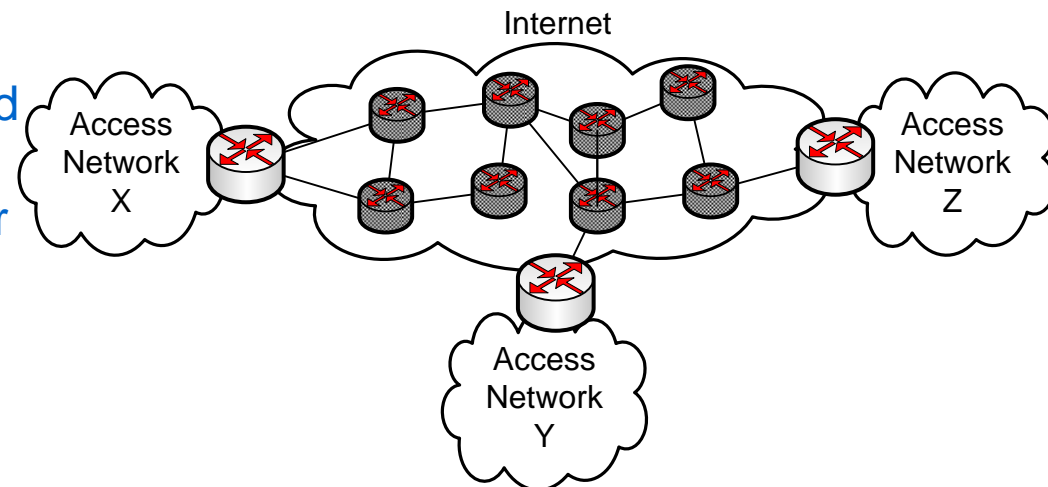
Notation: we will refer to IP addresses as *Network.Host* portion, e.g. X.a is an IP address on network X with host portion a

Assumptions: Wireless Access Networks

- Lets assume an “Access Network” is a single IP network where end-user hosts connect (via layer 2 technologies) to a router
 - Hosts and router all use same Network portion of IP address

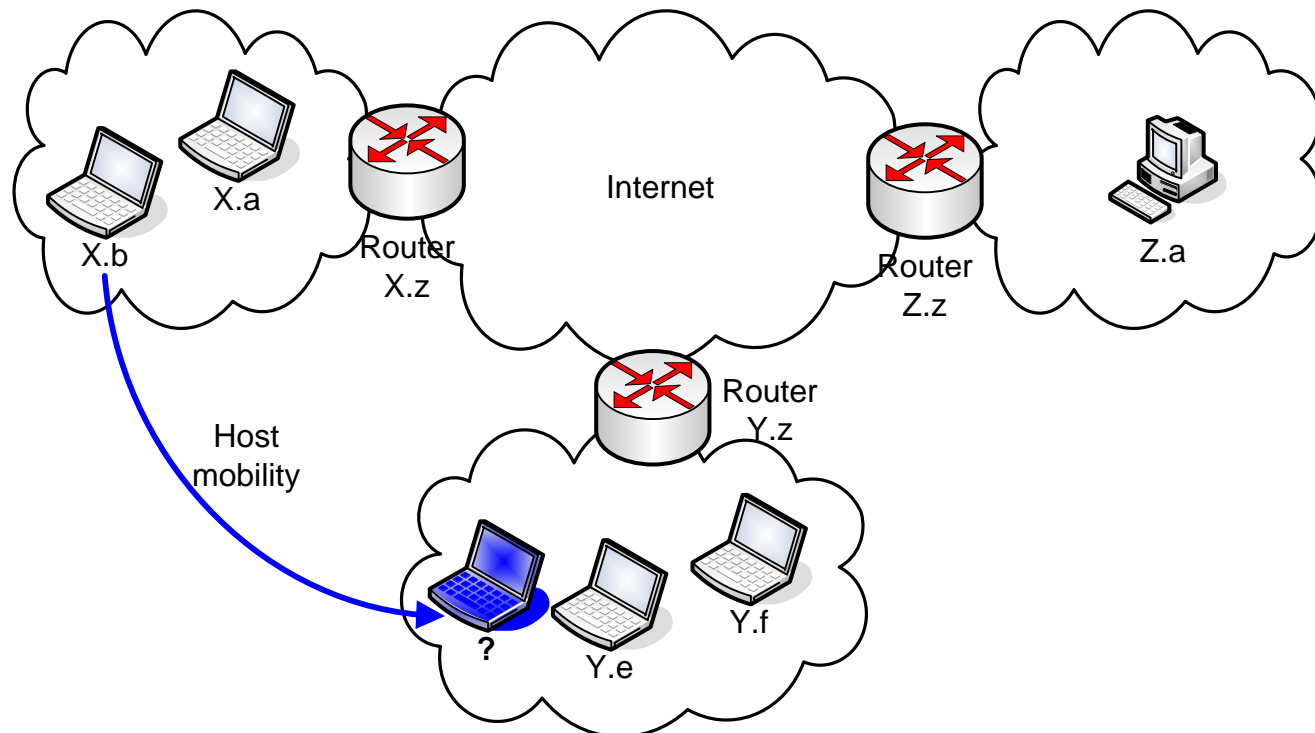


- Access Networks are connected together via other IP networks (often called Core, Backbone or Transport networks)



Problems with Mobility in Internet

- The Internet uses topologically correct routing
 - Routers in the Internet know about the location of other *Networks* (not hosts)
 - E.g. when Z.a sends to X.b, Internet routing finds a path to Network X, then Router X.z uses direct delivery to send to X.b
 - Therefore, if a mobile host changes Access Networks, then must change IP address, otherwise routing will not work
 - E.g. when X.b moves to Network Y, it cannot use the same IP address X.b!



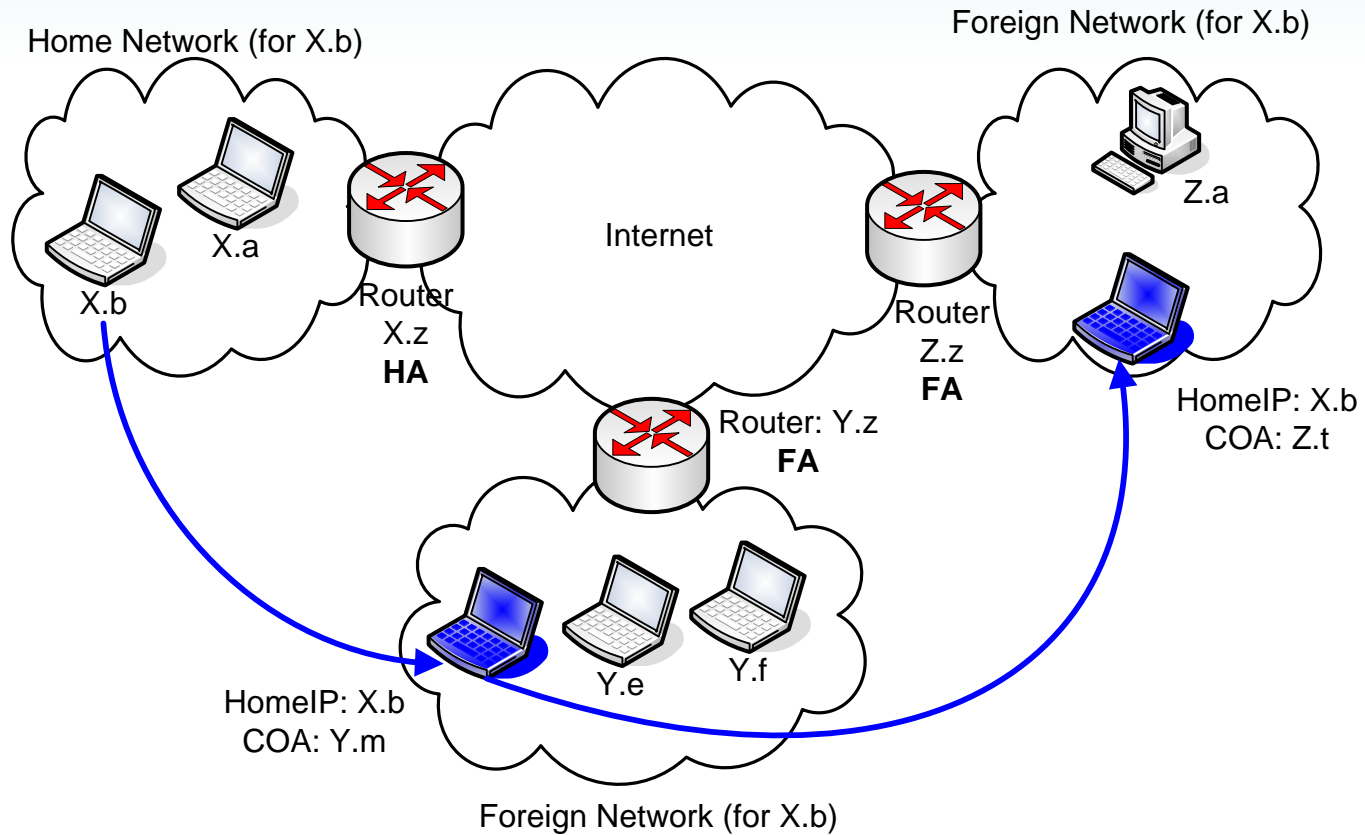
Problems with Mobility in Internet

- Application Sessions depend on IP address
 - Most Internet applications (and all using TCP) define a session as using the same:
 - Source IP address, Source Port, Destination IP address, Destination Port
 - Changing one of these identifiers, requires ending of the current session and starting a new session
 - E.g. stop a file transfer, lose context for web browsing, reconnect for a voice call, interrupt a database transaction
 - These interruptions are acceptable for *nomadicity*
 - Turning your laptop off, move to another location, and restart laptop
 - DHCP (and similar techniques) can be used to give your mobile host a new IP address
 - BUT these interruptions are not acceptable for *true mobility*
 - A user changing access networks should not be aware of the change
 - Mobility should be seamless (perhaps small delays of 10's to 100's of milliseconds incurred)
 - Very important for multimedia, streaming applications, e.g. voice over IP
- Solution: change the IP address, but hide the change from Transport/Application layers
 - Solution is implemented by Mobile IP, an IETF standard

IETF IP Mobility Solutions

- IETF began working on extensions of IPv4 to support mobility in 1990's
 - Major development was protocol generally referred to as *Mobile IP* in RFC 3344
 - Significant amount of research and development continues in IETF and elsewhere to:
 - Add new features Mobile IP: security, route optimisation, handover smoothing
 - Support IPv6
 - Cover specialised scenarios: Network Mobility, ad hoc networks
 - Mobile IPv4 is optional (FA's and HA functionality not required in IPv4 routers)
 - Mobile IPv6 is built-in to IPv6 (IPv6 routers contain functionality for FA/HA operations)
 - We will focus on Mobile IPv4, but similar concepts apply to Mobile IPv6

Mobile IP Basics



- A Mobile Node is assigned a visiting, or Care-Of-Address, at the networks it visits
 - Application sessions still use to original Home IP address
 - Normal IP Routing forwards packets to the Home Network
 - Mobile IP then forwards packets from the Home Network to the Mobile Nodes current Foreign Network

Mobile IP Components

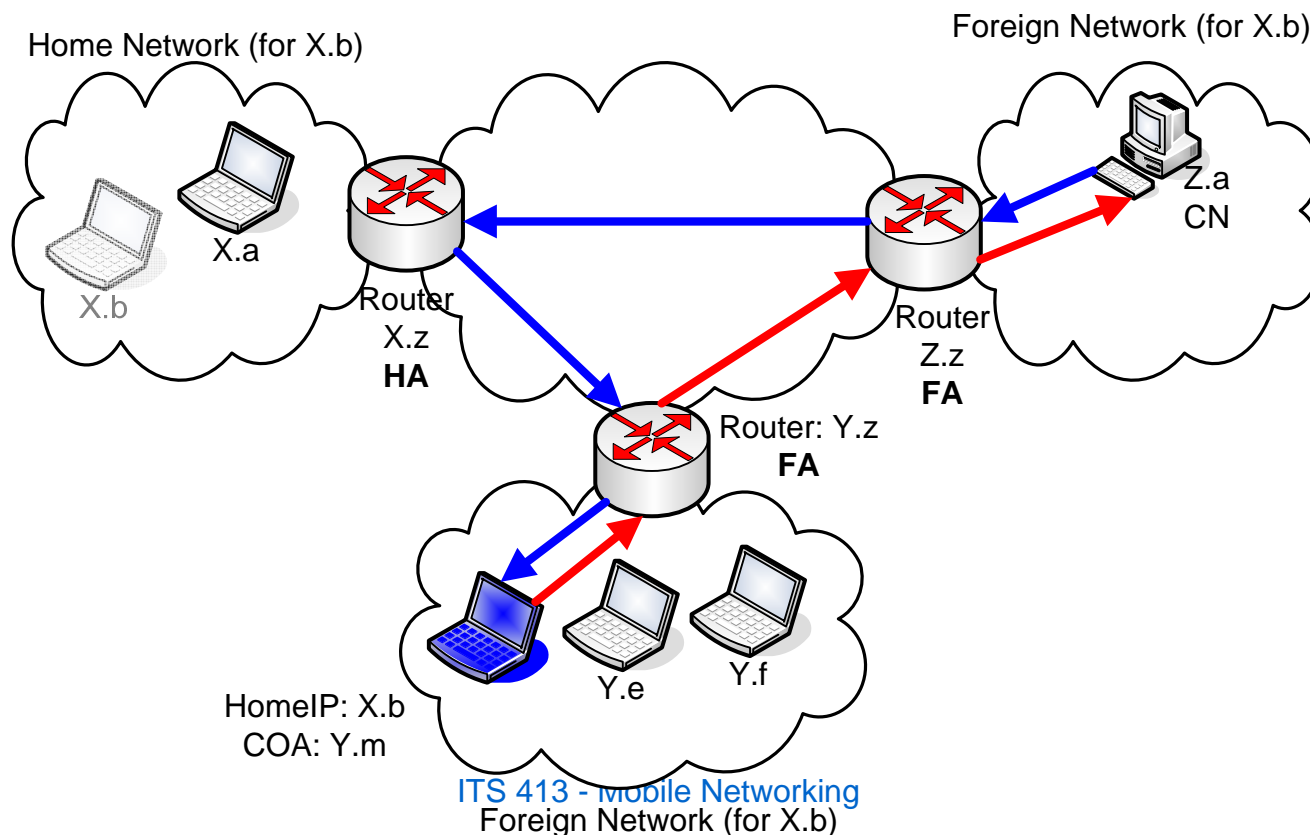
- Nodes (or Hosts):
 - Mobile Node (MN): a node that uses Mobile IP
 - Correspondent Node (CN): a node that communicates with a MN (may or may not use Mobile IP)
- Home:
 - Every node has a single *Home Network*; the network in which the host is assigned its normal IP address
 - From a nodes point of view, all networks other than the Home Network are Foreign Networks
- Home Agent (HA)
 - A server on the Home Network that keeps track of where the Mobile Nodes associated with that Home Network are
 - Maintains a *Mobility Binding Table*: for its own MNs, records their current COA
 - Implemented on a router in the Home Network
- Foreign Agent (FA)
 - A server that keeps track of Mobile Nodes visiting its network, providing the necessary addresses and forwarding for those visiting Mobile Nodes
 - Maintains a *Visitors List*: for the visiting MNs, records their Home IP, Home Agent and Layer 2 address
 - Implemented on a router in a Foreign Network

Mobile IP Components

- Home IP Address
 - The IP address assigned to the MN in its Home Network
 - The Home IP address is within the Home Network address range
 - E.g. home network: 25.105.0.0/16; home address: 25.105.23.88/16
- Care-of-Address (COA)
 - An IP address assigned to MN visiting a Foreign Network
 - The COA is an IP address within the Foreign Network address range
 - E.g. foreign network: 172.16.37.0/24; COA: 172.16.37.65/24

Mobile IP Forwarding

- Correspondent Node to Mobile Node
 - CN is not aware that MN is “mobile”
 - Sends packets to Home IP, e.g. X.b
 - HA intercepts and realises the MN is not home, and forwards to Foreign Network where MN is visiting
- Mobile Node to Correspondent Node
 - MN sends packets to CN (e.g. Z.a) via the local FA
 - Source Address is MN's Home IP (e.g. X.b)

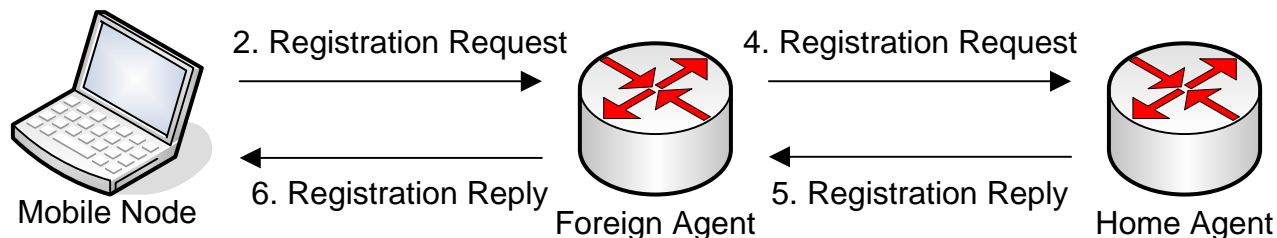


Mobile IP Issues

- First Registration (in a Foreign Network)
 - When a MN visits a Foreign Network it must inform the FA and its HA
 - Mobile IP Registration
 - BUT how does a MN know it is in a Foreign Network
 - Mobile IP Agent Discovery
- Forwarding from HA to FA
 - For packets sent from the CN to HA, the HA must then forward the packets to the current FA
 - Mobile IP Tunnelling
- Handover between Foreign Networks
 - As a MN moves from one Foreign Network to another Foreign Network, need to inform HA of change AND “cleanup” at the old FA
 - Mobile IP Handover
- Minimising the Delay
 - Routing from CN to HA then to FA can be wasteful
 - Mobile IP Route Optimisation
 - Handovers can take a long time (discovering new FA, informing HA)
 - Mobile IP Handover Smoothing

Mobile IP Registration

- First Registration (for example, Mobile Node powers on in a new Foreign Network)
 1. MN discovers it is in a Foreign Network (see Agent Discovery)
 2. MN sends a Mobile IP Registration Request to the FA
 - Source IP: Home IP; Dest IP = FA
 - Registration Request contains the IP address of the MN's HA
 - Note FA is configured to receive Mobile IP messages from nodes with an IP address *not on the local network*
 3. FA notes the MN's Home IP and allocates a COA
 4. FA sends Registration Request to HA (including the allocated COA)
 5. HA authenticates the MN, updates its Mobility Binding Table and returns a Registration Reply to FA
 6. Upon receipt of positive Registration Reply, FA updates its Visitors List, and forwards reply to MN. FA will now *service* the MN

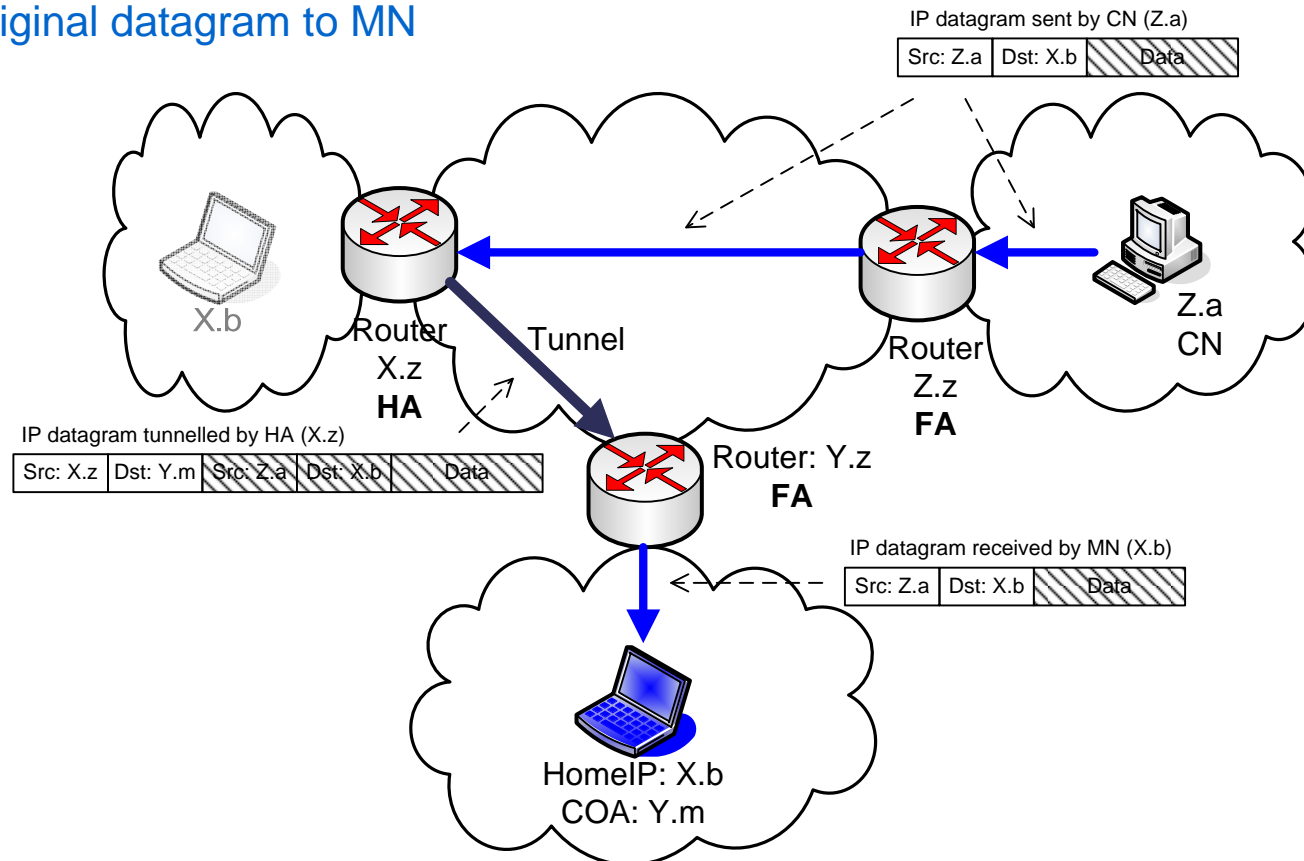


Mobile IP Agent Discovery

- How does a MN know the IP address of the FA?
 - When it first powers up?
 - When it performs a handover from an old FA to a new FA?
- Three options for Agent Discovery:
 - IP Level Agent Advertisements
 - Agent broadcasts periodic advertisements, indicating its own IP address
 - ICMP Router Advertisement messages, extended to carry Mobile IP information
 - Rate at which advertisements are sent must be limited (default: 1 per sec)
 - Agent *may* be configured to only send advertisement after receiving solicitation
 - IP Level Router Solicitation
 - MN broadcasts a solicitation message to the network
 - ICMP Router Solicitation messages are used
 - Rate **MUST** be limited (1 per second for the 3 initial solicitation messages, and then with exponential back-off)
 - The FA has to respond to solicitation with an advertisement message
 - Layer 2 Supported Techniques
 - Local broadcasts of L2 beacon frames with all necessary information (including FA address, supported functionality, CoA etc...)
 - MN can solicit beacon (or other L2 “welcome”) frames upon gaining L2 connectivity
 - Example: Wireless LAN beacons are extended to carry Mobile IP information, such as FA address

Mobile IP Tunnelling

- CN sends IP datagrams to the Home IP address
- When HA receives datagram, it checks Mobility Binding Table: if destination node is mobile, then encapsulate original datagram in another IP datagram
 - Source: HA; Destination: COA
- FA will receive datagram, check its Visitors Table, decapsulate the datagram, and send original datagram to MN

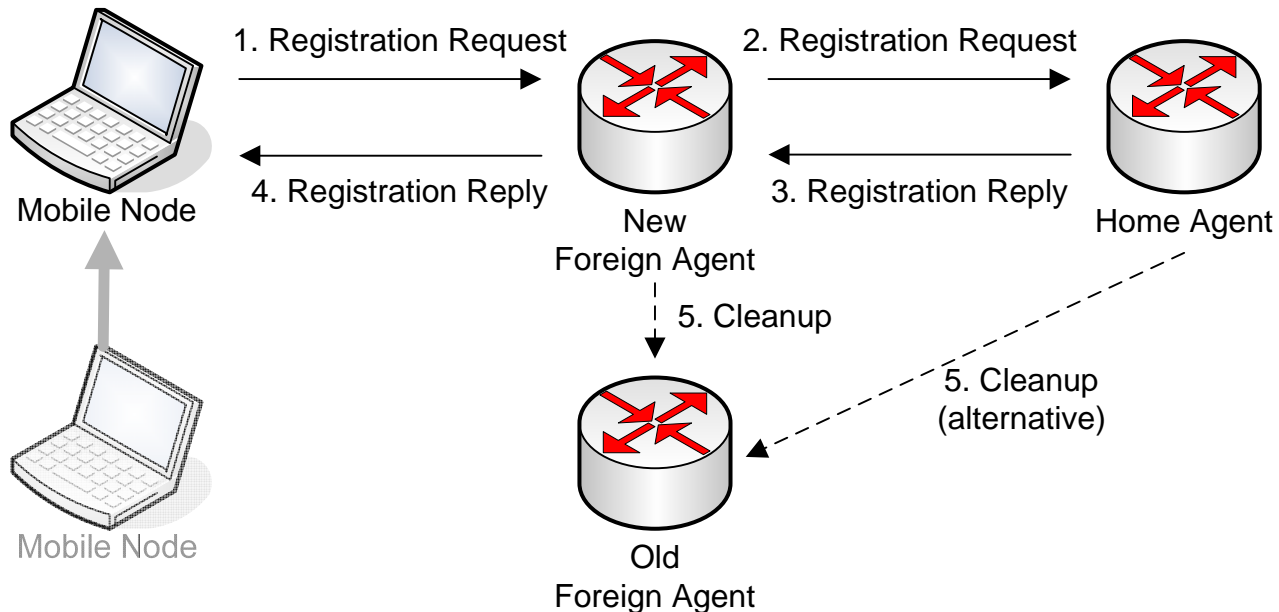


Mobile IP Route Optimisation

- Routing via the HA all the time can be inefficient
 - Triangular Routing Problem
 - If CN and MN are “near each other”, but HA is “far away”
 - E.g. CN is in Toshiba Bangkadi; MN from Toshiba US is visiting SIIT
 - CN (in Bangkadi) sends to HA in US, which then sends to FA/MN in Bangkadi
- Route Optimisation is an extension of original Mobile IP that allows CN to send directly to MN’s COA
 - MN’s and FA’s may send Binding Warnings to HA if they see a need for route optimisation
 - HA sends Binding Updates to CN, informing the CN of the MN’s current COA (a lifetime is associated with this COA)
 - CN maintains a Binding Cache, storing the COA of MN’s
 - If COA exists in Binding Cache, CN sends with destination set to COA
 - If COA does not exist, CN sends with destination set to Home IP
- Reduces delay of triangular routing, but:
 - Requires CN to maintain Binding Cache (not supported in some nodes)
 - Need to have security association between HA and CN
 - Some security techniques that filter packets that “come from the wrong network” may not allow the packets (*ingress filtering*)

Mobile IP Handover

- When a MN using an old FA detects (and chooses to connect to) a new FA, it performs a handover
 - Mobile IP Registration procedure is used with the new FA
 - Cleanup at the old FA may occur, e.g. so it can delete entry from Visitors List
 - Issues:
 - Delay may be high: during handover often cannot send/receive packets
 - Packet loss: some packets may be sent to old FA, when MN is at new FA
 - Security: need to ensure MN's cannot replay messages to gain unauthorised access

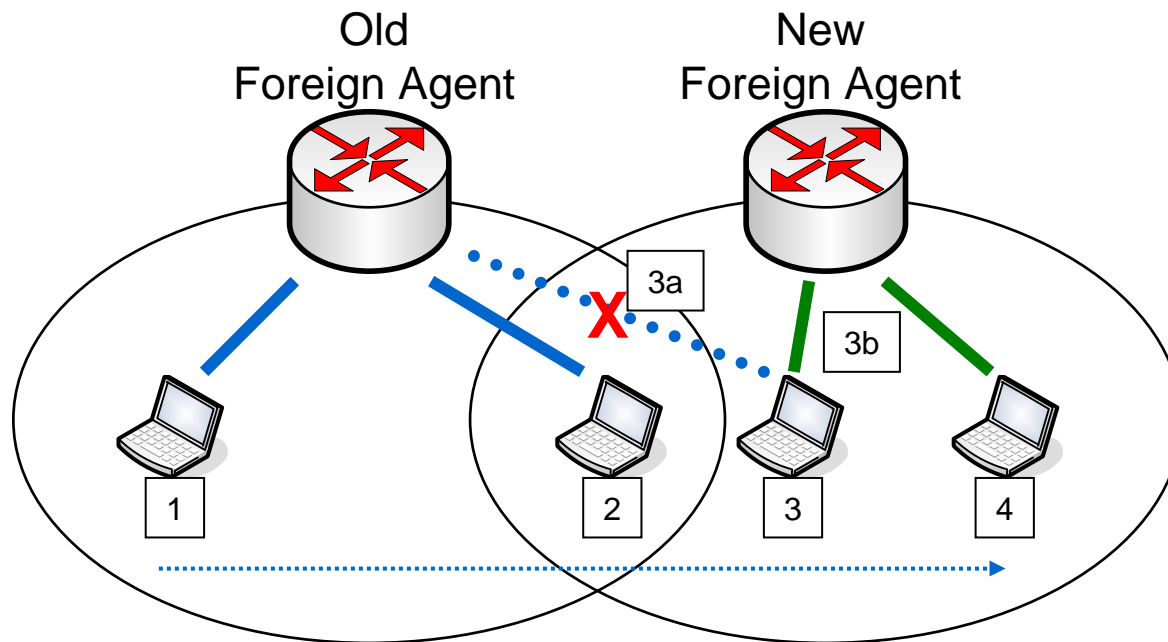


Mobile IP Movement Detection

- Agent Discovery is used to find out about FAs
 - These techniques can be used to detect new FAs
 - Option 1: No New Advertisements
 - If MN does not receive advertisements from a FA after a period of time, then assumes that old FA is not available and will listen for advertisements from another FA (or solicit advertisements)
 - Option 2: Receive Advertisements from new FA
 - If MN receives advertisements from a new FA, while still connect to old FA, then it may decide to handover
 - Option 3: Layer 2 Detection
 - If MN receives Layer 2 notification of new FA (e.g. wireless LAN beacons carrying IP address of new FA), then can decide to handover
- Layer 2 Connectivity
 - Some devices/networks will allow simultaneous connectivity to 2 or more Layer 2 networks, others will not
- Changing between networks may be referred to as *cell switching*

Mobile IP Handover Methods

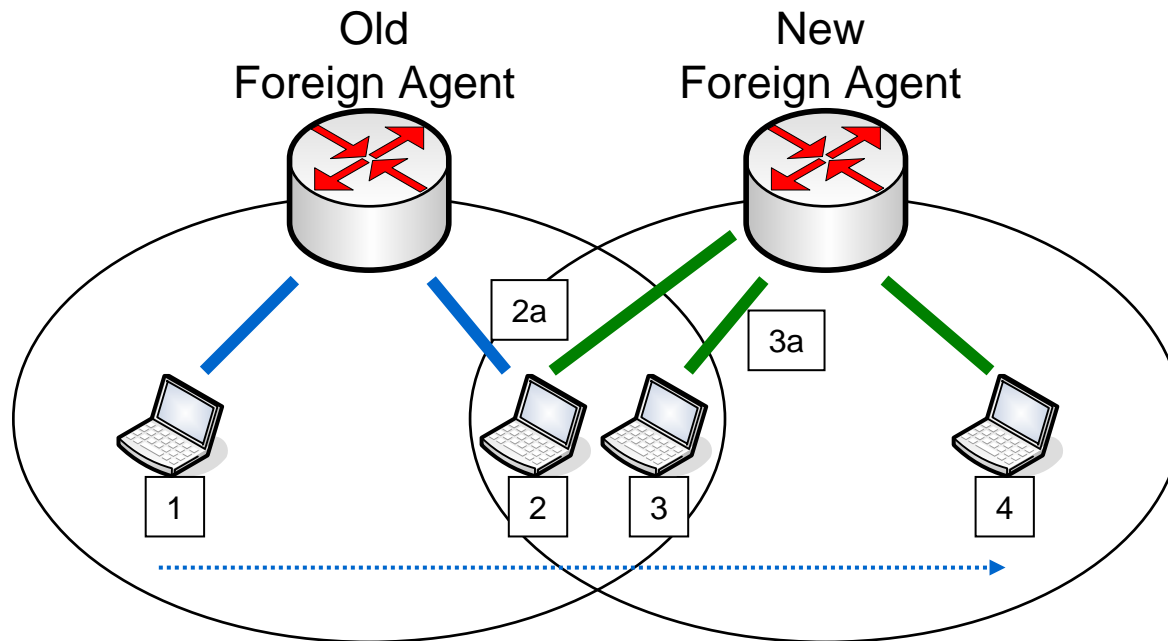
- Lazy Cell Switching (LCS), or “break-before-make”



- Connection with old FA is maintained for as long as possible, until it is no longer available (break, 3a); then connection with a new FA is established (make, 3b)

Mobile IP Handover Methods

- Eager Cell Switching (ECS), or “make-before-break”

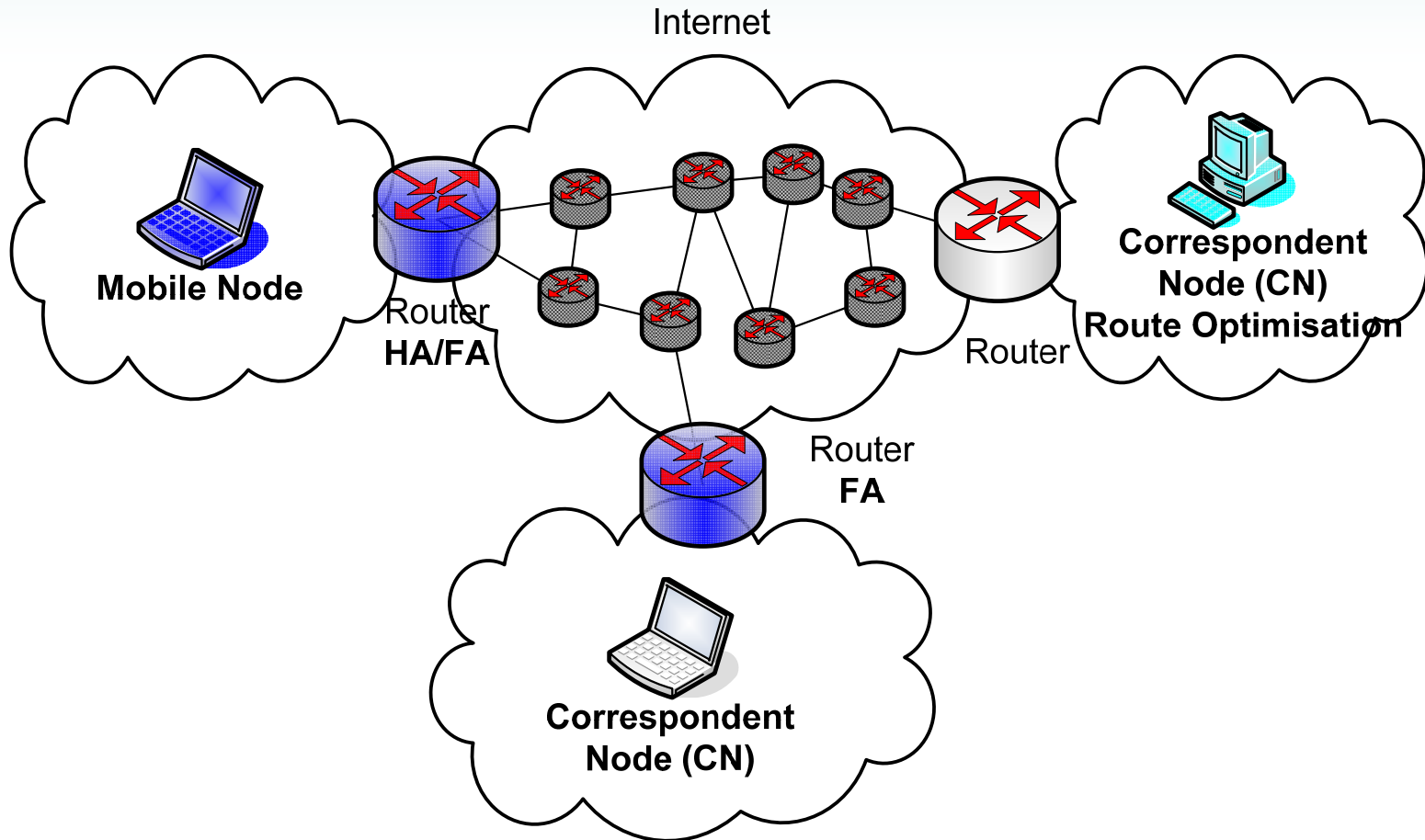


- Contact with new FA is established as soon as Layer 2 connectivity is available (2a)
- Connection with old FA may be dropped immediately or when Layer 2 connectivity is lost (3a)
- Requires Layer 2 wireless technology to support simultaneous active links

Mobile IP Handover Smoothing

- Delay incurred by handovers can be significant: 100msec to seconds
 - Hence, the user will notice the mobility; impact on performance of applications
 - Data may be dropped or delayed
- Various optimisations have been proposed to reduced handover delay
 - Handover Smoothing using:
 - Buffering
 - Bicasting
 - Regional Registrations
 - Fast Handover Mobile IP
- Buffering
 - Just before the handoff, data destined to MN is buffered at the old FA
 - When the handoff is finished, buffered data is forwarded from the old FA to the new FA
 - Buffering trade-off: data loss vs. data delay (may not be suitable for Real-Time applications)
 - Problems include: when to start and stop buffering; synchronisation of actions among the involved entities (MN, oFA, nFA, HA); signalling overhead; data duplication and/or loss
- Bicasting
 - Start bicasting to both old and new FAs when handoff starts
 - Problems: as for buffering, with more data duplication and synchronisation challenges
- Regional Registrations
 - Hierarchy of FAs, so only re-register with lower level FAs, not necessarily HA
 - Improves handover delay but increases signalling load

Mobile IP Implementations



Mobile IP needs to be implemented on:

- Routers that act as Home Agents, allowing home nodes to be mobile
- Routers that act as Foreign Agents, allowing visiting nodes
- Mobile Nodes that can be mobile between networks
- (Optionally) Correspondent Nodes if route optimisation is to be used

The Status of Mobile IP Today

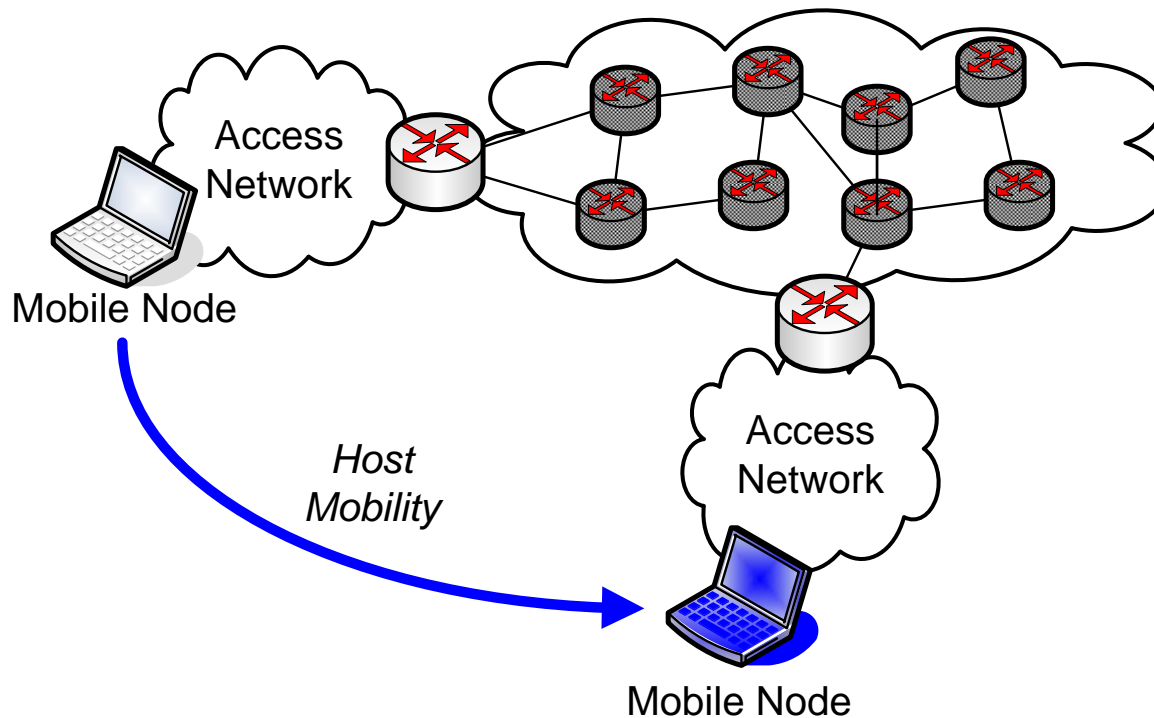
- Standardisation
 - IP Mobility for IPv4: mature; enhancements for optimisations
 - IP Mobility for IPv6: mature; enhancements for optimisations
 - Note: in IPv6 all routers can perform functions of FA, hence Mobile IPv6 (compared to IPv6) defines the functionality of MNs, HAs and CNs
- Implementation
 - Hosts
 - MN support NOT in MS Windows XP/Vista/Mobile
 - MN support is in most variants of BSD and some Linux distributions
 - Routers and servers (foreign agents, home agents)
 - Most commercial routers support HA/FA functionality (e.g. Cisco)
- Use
 - Currently not in widespread consumer use (e.g. laptops, PDAs)
 - Technical and commercial limitations make changing between networks difficult (Bluetooth to Wireless LAN to 3G to ...)
 - Used in some business networks
 - Some current and many future 3G networks will use Mobile IP, i.e. implemented in mobile phones, e.g. CDMA2000 (Hutch/CAT?)
 - Expected to be implemented in most new mobile devices, and used when coverage and operator agreements make it feasible

Network Mobility

NEMO

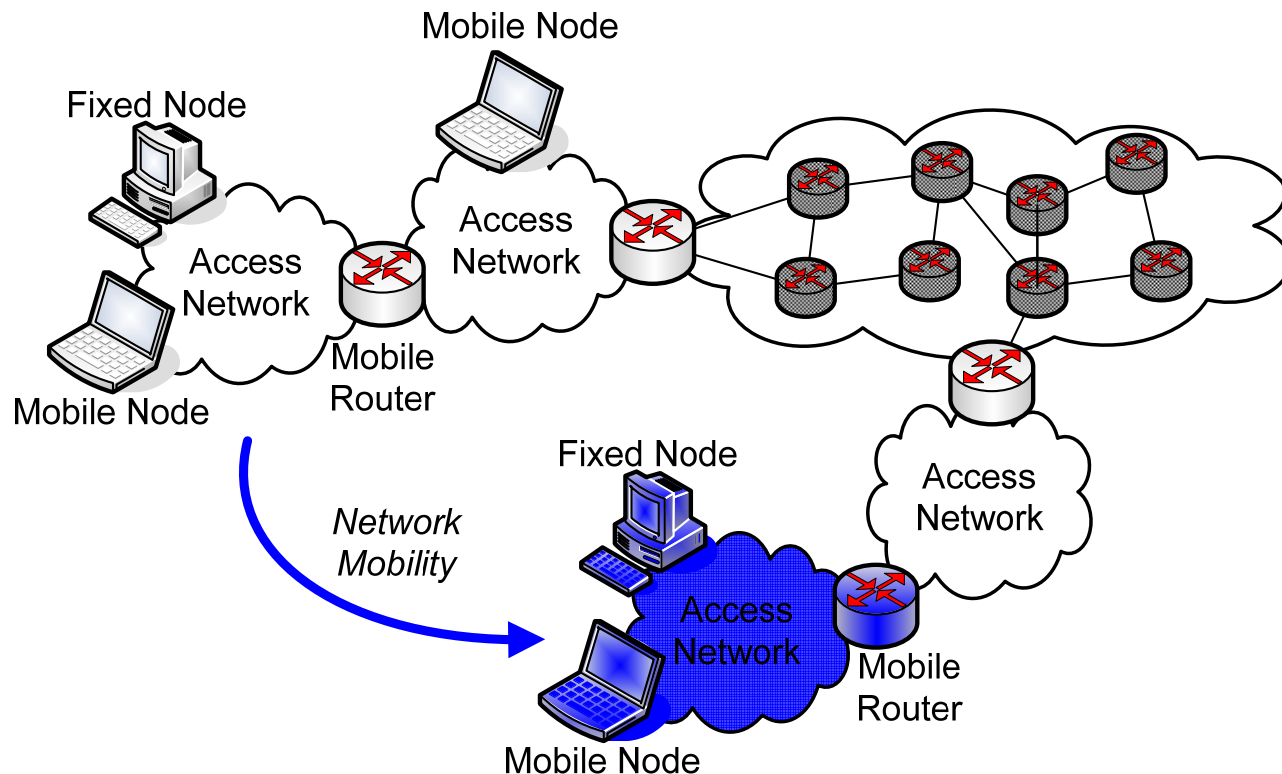
Host Mobility versus Network Mobility

- Host mobility allows a single host/node to move from one access network to another
 - At layer 2, implemented by Wireless LAN, Bluetooth, etc.
 - At layer 3, implemented by Mobile IP



Host Mobility versus Network Mobility

- Network mobility allows an entire access network to move
 - Implemented at Layer 3 using extensions of Mobile IP called *Network Mobility (NEMO)* by IETF



Applications of Network Mobility

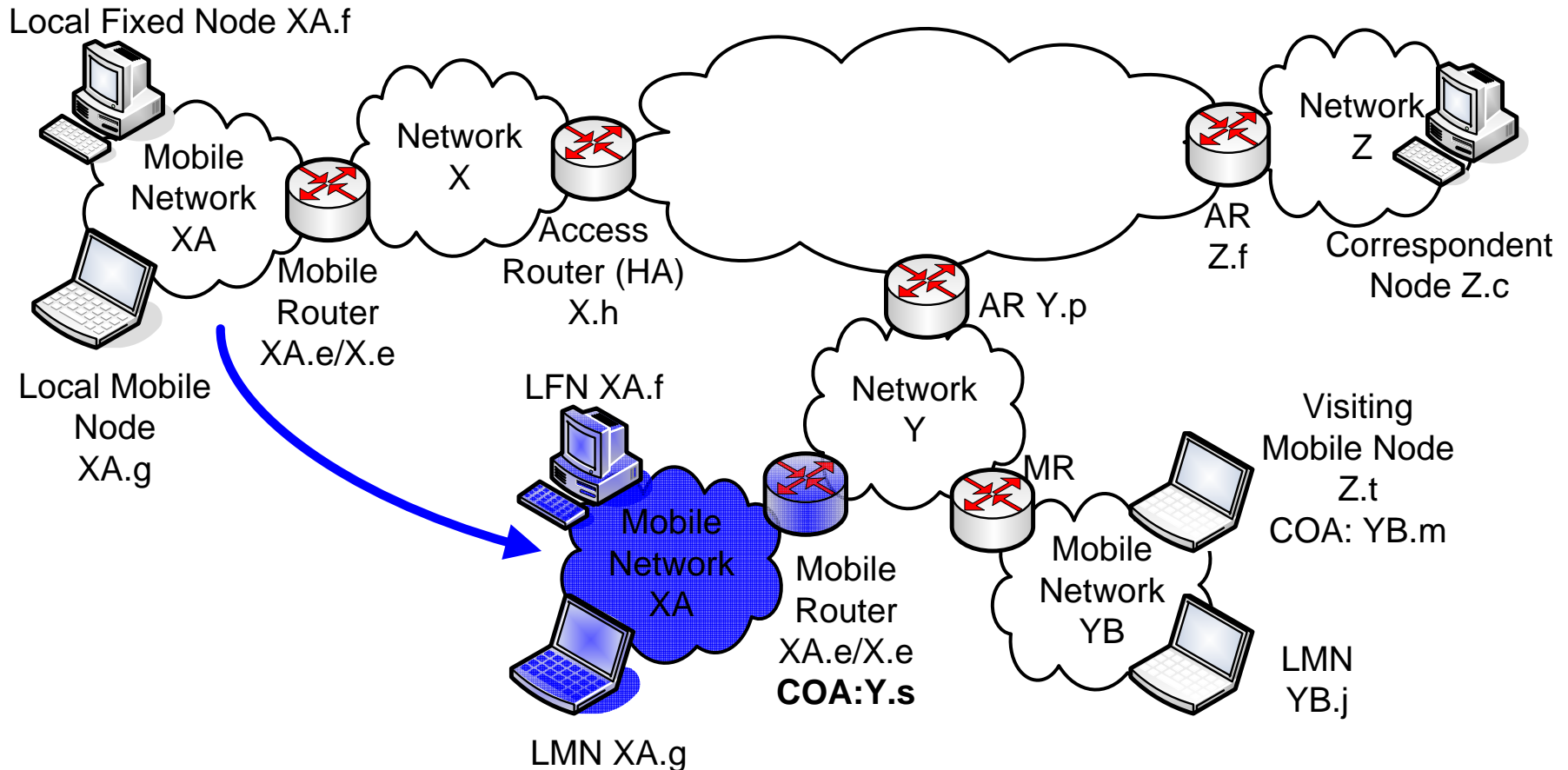
- When do you want to move an entire network *and* have continuous connectivity?
 - Private Vehicles
 - A Mobile Router inside your car provides wired and wireless connectivity between all the devices (TV, mobile phone, PDA, sensors, engine management, entertainment system)
 - As the car drives along a highway, the entire vehicular network must handover between different networks (routers)
 - Public Transport
 - A train has a Mobile Router providing Wireless LAN access to all users with PDAs and laptops
 - As the train moves, the entire network must handover between satellite, WiMax, 3G networks along the tracks, and other networks within stations
 - Similar scenario for busses, ships and aircraft
 - Personal Area Networks
 - Your PDA acts as a Mobile Router for all the other devices you carry (music player, camera, mobile phone, headset, ...). Those devices access the Internet via your PDA
 - As you move, the entire network moves

Why Not Just Use Mobile IP?

- Mobile IP does not allow the entire network to move as one, keeping the move unnoticeable by the mobile nodes
- Why not let all the nodes on the mobile network to use Mobile IP (and manage their own mobility)?
 - Requires all mobile nodes to implement Mobile IP
 - E.g. on a plane, all the laptops/PDAs/phones must implement mobile IP
 - Signalling overhead would be excessive
 - Even if all mobile nodes did implement Mobile IP, each would have to do their signalling (registration, agent discovery) separately
 - Better to have one device perform the signalling on their behalf
 - Requires all mobile nodes to have the appropriate layer 2 technology
 - E.g. a train passes via a Wireless LAN, WiMax, Satellite and 3G network; using Mobile IP only would require every mobile device to support these four technologies
- So IETF extended Mobile IP to support Network Mobility

NEMO Basics

- The basic features of NEMO are an extension of Mobile IPv6



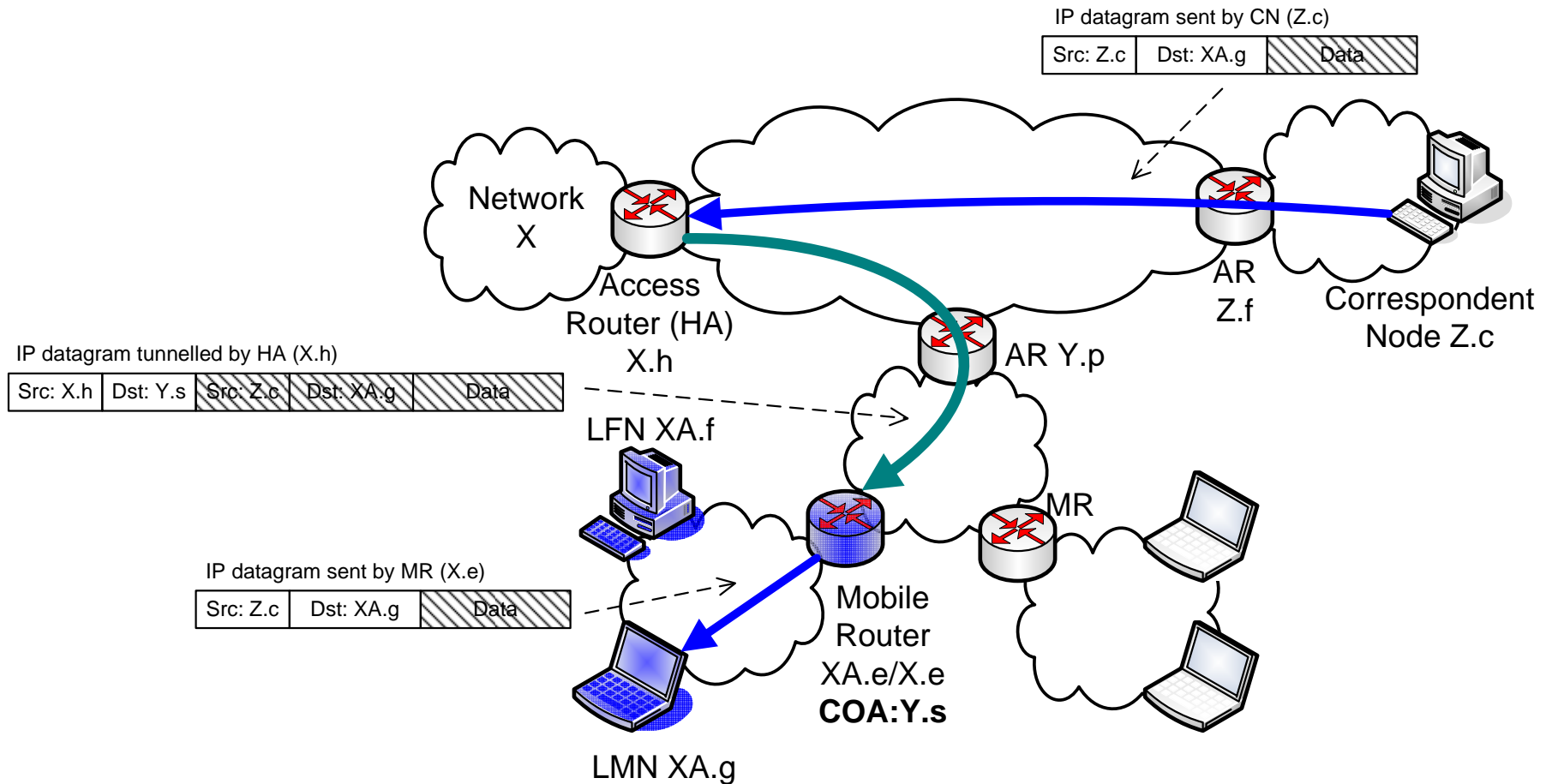
- A Mobile Router is assigned a COA when it moves to a foreign network
- The Mobile Router informs its HA if the new COA

NEMO Components

- Mobile Routers (MR)
 - Routers that can move, thereby resulting in the move of an entire network (the router plus the MNNs)
- Mobile Network Nodes (MNN)
 - Nodes attached to MR via one or more layer 2 technologies
 - Three types of MNN:
 - Local Fixed Node (LFN): a normal node with a fixed connection to the MR; it does not use Mobile IP for its own mobility (e.g. always connected to the same MR)
 - Local Mobile Node (LMN): a Mobile IP-enabled node, with its Home Network being that of the current MR; it can change networks using standard Mobile IP
 - Visiting Mobile Node (VMN): a Mobile IP-enabled node, visiting the current MR; its Home Network is somewhere else
- Access Router (AR)
 - The Router the MR connects to
 - This is similar to FA in Mobile IP (but in IPv6 and Mobile IPv6) the role of a FA is performed by a normal IPv6 router, hence the name change!
- Note: there are other differences, especially in terminology, between IPv4 and IPv6, and hence between Mobile IPv4 and Mobile IPv6. NEMO was first defined for IPv6. However, the main concepts of supporting mobility remain the same. In this lecture we will just explain concepts.

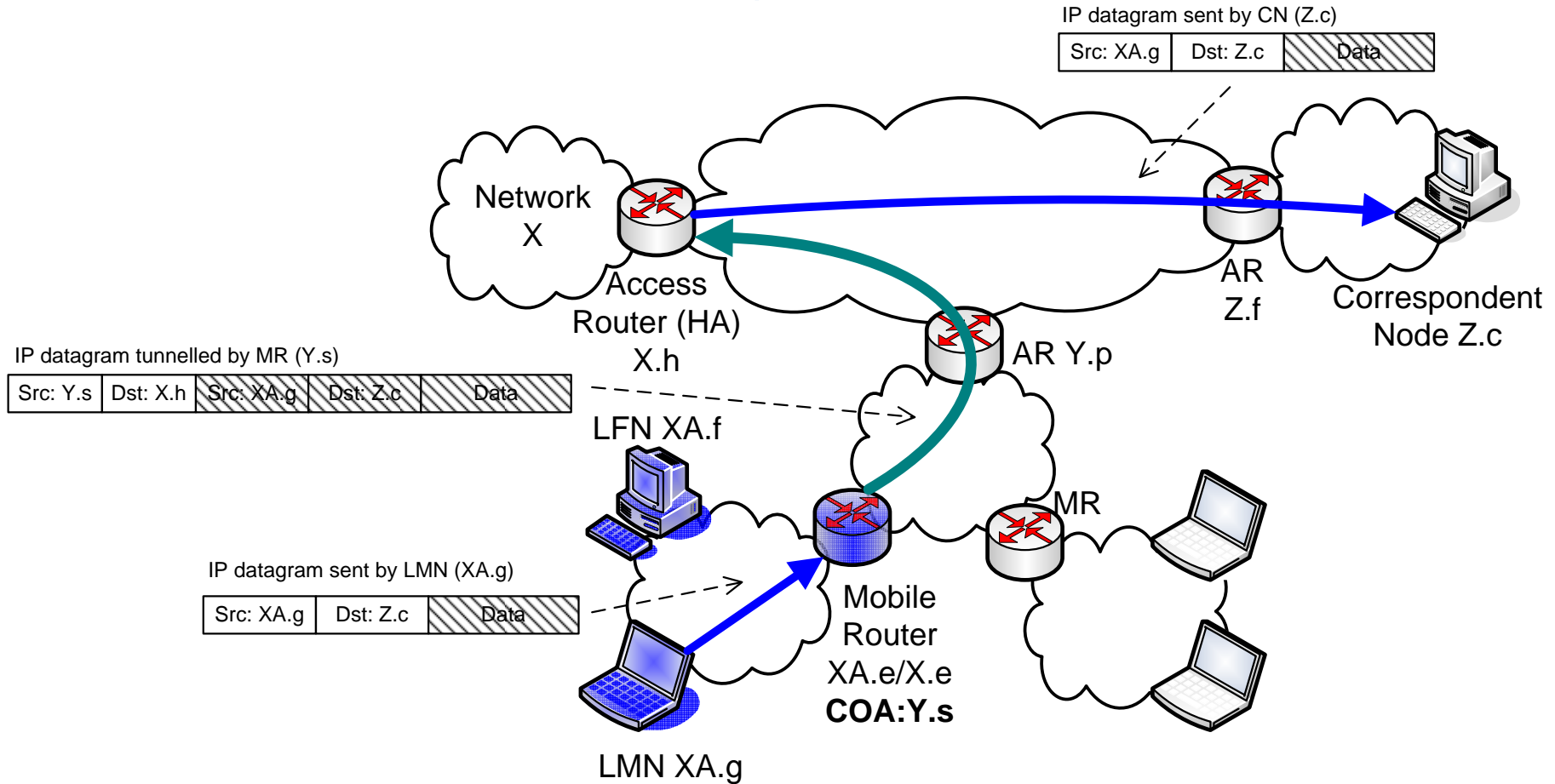
NEMO Forwarding

- Correspondent Node to Mobile Network Node



NEMO Forwarding

- Mobile Network Node to Correspondent Node



NEMO Details

- There are many details that we will not cover
 - COA assignment to MRs
 - Tunnelling
 - In Mobile IP, tunnelling was NOT needed from Mobile Node to CN
 - In NEMO, tunnelling IS needed from MR to CN, because many routers in the Internet have security policies that will not allow traffic from “topologically incorrect” addresses (that is, packets that say they come from a network which in the normal Internet could not). Tunnelling avoids this problem.
 - The differences of handling LMN, VMN, LFNs
 - MR informing HA of new foreign network
 - Similar to Mobile IP Registration, but performed using Binding Updates
 - Nested Mobile Networks
 - Multihoming
 - Route Optimisation
 - ...

Status of NEMO

- Standardisation
 - NEMO Basic Support is mature: RFC3963
 - Still working (and researching) on optimisations such as route optimisation, nested NEMO and multi-homing
- Implementation
 - Several commercial routers implement MR/HA features of NEMO (e.g. Cisco)
 - MR and MNN features are implemented as extensions to BSD variants of Unix (e.g. FreeBSD, OpenBSD)
- Use
 - Only used in experimental/research purposes
 - E.g. several “Internet Car” projects have used NEMO
 - May become more widespread as Internet access becomes ubiquitous in public and private vehicles

Ad Hoc Networking

MANETs

Infrastructure-Based Wireless Networks

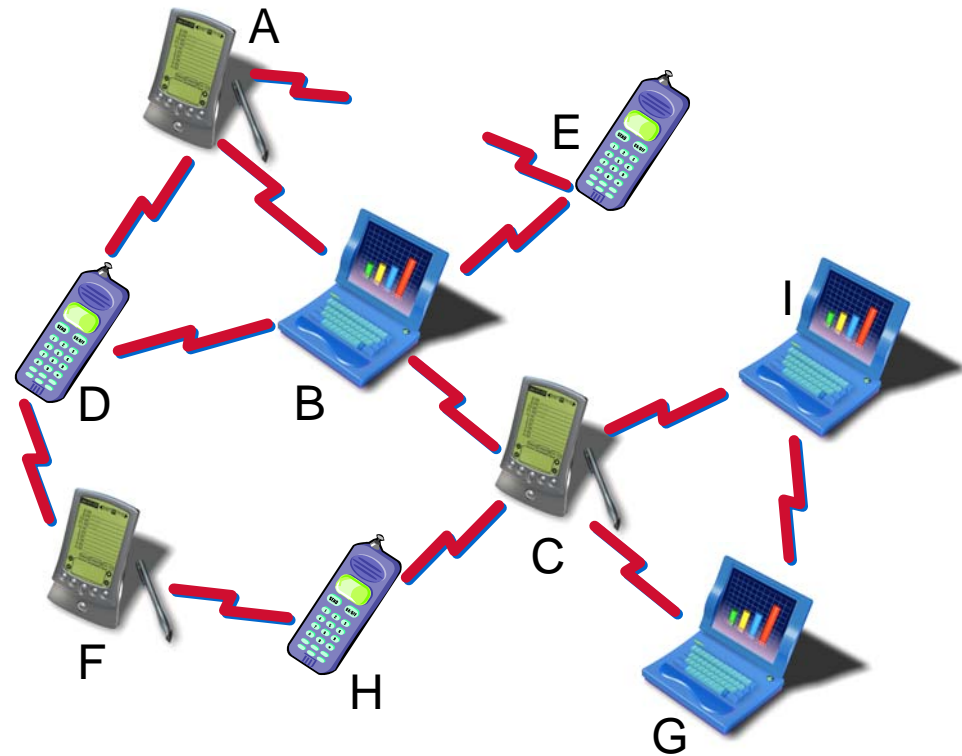
- Almost all wireless networks today are *infrastructure-based* or *centralised*:
 - A fixed base station (access point) provides wireless connectivity to mobile clients within some area (e.g. cell)
 - Base stations are connected via wires to other networks (e.g. Internet)
 - Examples: wireless LANs, mobile phones, satellite, WiMax, ...
 - Single-hop wireless: mobile client to base station (the rest is wired)



- Infrastructure-based wireless networks work well because they are designed for performance/coverage; can control the resources
- But some problems:
 - Difficult to deploy: large amount of time and money to deploy
 - Restricted coverage: mobile clients can only have access if within a cell
 - Centralised: failure of a base station, means failure for all mobile clients

Infrastructure-less Wireless Networks

- As an alternative, we can create wireless networks without infrastructure (base stations, access points, wires, servers), or as a *decentralised network*
- Key Characteristics and Constraints:
 - No existing infrastructure is needed
 - Multiple wireless hops; all nodes are routers, therefore they must forward on other nodes behalf
 - Node mobility, dynamic topology
 - Lack of pre-configuration, self-organising
 - Resource limited devices
 - Resource limited wireless communications
 - Large networks, scalability
- Called: ad hoc networks; mobile ad hoc networks (MANETs); wireless ad hoc networks; multi-hop wireless networks; ...



Applications of MANETs

- Useful when:
 - Rapid network deployments are needed
 - Seconds/minutes rather than days/months
 - Too costly to deploy infrastructure
 - E.g. only need the network for a short time; no physical ability to deploy base stations/wires
 - Network survivability is vital
 - If one node fails, the rest of the network adapts and keeps working
- Examples
 - Defence: Military battlefield communications, distribution of situational awareness information
 - Emergency Services: Communications in disaster relief operations
 - E.g. an earthquake destroys large parts of a major city, including the normal Internet access, mobile phones, wireless LANs; emergency service workers (carrying mobile devices: laptops, PDAs, phones) form a network amongst themselves to exchange information
 - Business, community and home temporary networks
 - E.g. friends/colleagues meet and form a network amongst mobile devices to share files/data

Applications of MANETs

- Two types of networks that are similar to MANETs have many commercial applications
- Mesh Networks
 - Some fixed wireless nodes, e.g. to form a backhaul network
 - Network is not as dynamic as “pure” MANET
 - Examples:
 - Mobile broadband access for emergency services
 - Low cost network deployment in rural/remote areas
 - Community-based wireless networks
- Sensor Networks
 - Dynamic deployment, but nodes fixed
 - Severe resource constraints on nodes, e.g. KB of memory, MHz CPU, battery power for months
 - Examples:
 - Environmental monitoring
 - Precision agriculture
 - Surveillance and security

Technical Challenges of MANETs

- The dynamic nature of MANETs lead to their main benefits, but also create many technical problems
- The main problems are routing and performance
 - Routing
 - In the Internet, routing protocols (e.g. OSPF, BGP, RIP) are used to ensure routers have “up-to-date” information about routes/paths. If the network topology changes (e.g. a new router added, a link goes down), routing protocols will detect this and update the routers accordingly
 - Topology changes occur on a minute/daily/monthly basis
 - In MANETs, routing protocols are also needed, since in effect, every mobile device is a router. But topology changes (e.g. a mobile node moves) may occur every second.
 - Normal Internet routing protocols cannot handle such frequent changes
 - New MANET routing protocols have been developed, but still a difficult task
 - Performance
 - In MANETs, every node uses wireless transmission, and potentially can interfere with many other nodes. Also, only half-duplex communication is possible.
 - Performance of MANETs is significantly less than most other networks, e.g. throughput about 1/3 to 1/10 of a wireless LAN
- Many other problems: security, connecting to Internet, applications, wireless transmission, costs, energy efficiency, ...

Status of MANETs

- Standardisation and Research
 - IETF MANET Working Group has standardised several routing protocols
 - Still working on methods for configuring MANETs, and connecting to Internet
 - Many open research problems remain unanswered
- Implementation
 - Most implementations of MANET routing protocols are experimental
 - Not in common operating systems by default, but can install different MANET routing protocols
- Use
 - Used in some commercial Mesh Networks, Sensor Networks, and by Military
 - Not in widespread consumer use