Infrastructure-less networks

Csaba Simon
Dept. of Telecommunications and Media Informatics
simon@tmit.bme.hu

Convergent Networks and Services (VITMM156)

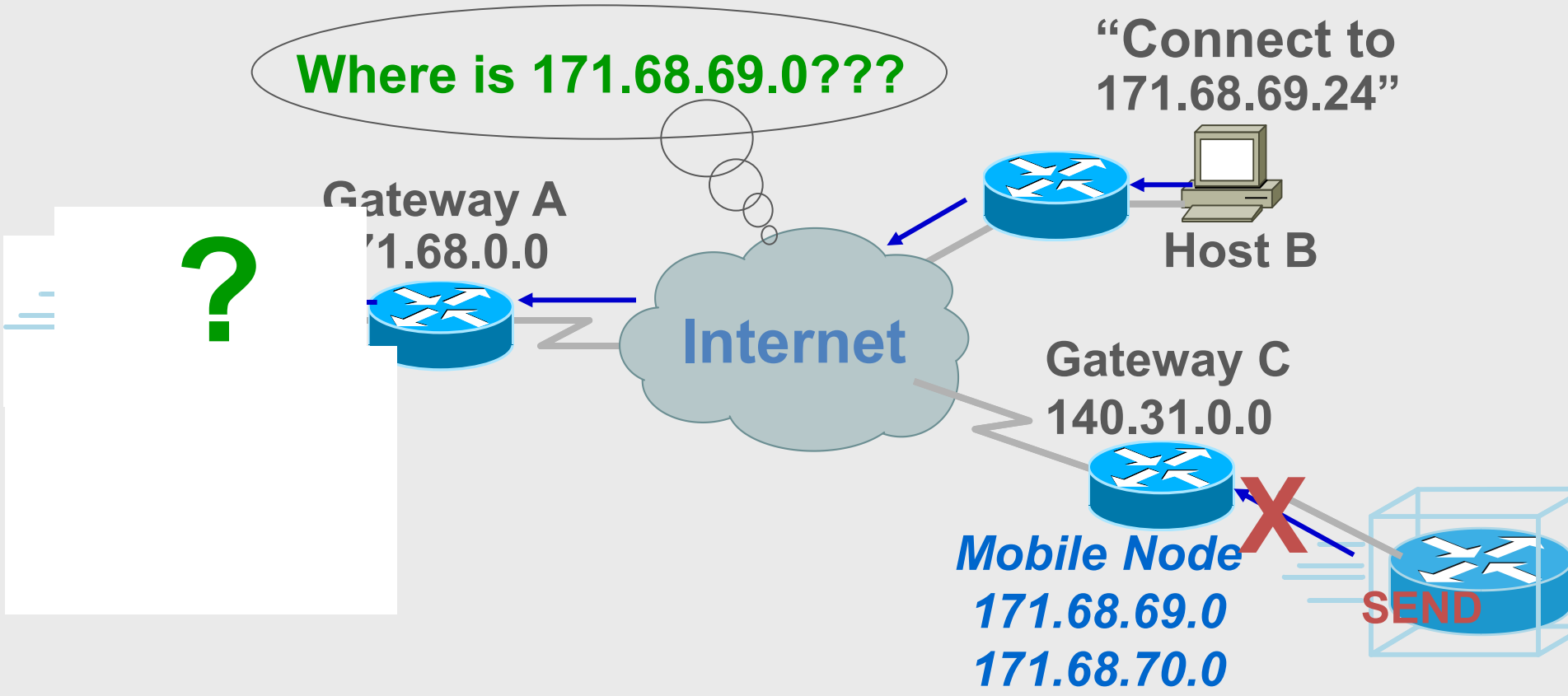
Mobility management

Mobility

- Mobile station, mobile node (MN)
  - Moves from its usual, default network to a different subnetwork
  - Home Network -> Foreign Network
- If it keeps its old IP address
  - IP packets can not be routed to the MN
  - According to its IP address, the packets a routed to its Home NW.
- If it receives a new IP address
  - It will be valid in the Foreign NW
  - packets addressed to this new IP addr. will reach the MN
  - The connections will be interrupted – since they were setup based on the original IP address
- Several protocols have been proposed to handle this mobility issue

source: cisco.com / Cisco Mobile Router Module 2-6 / CEE_NET 2002

Mobility problem

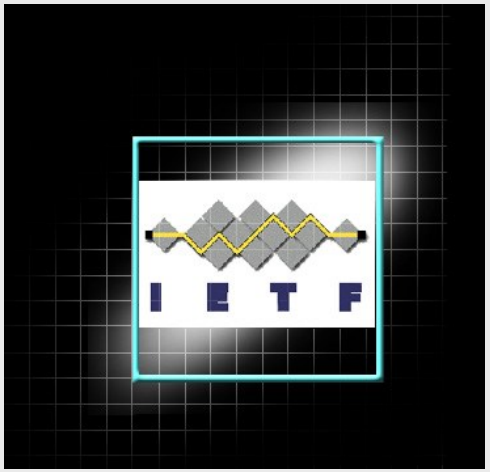


- The Mobile Node represents the moving nodes
- „A" (home) router answers to node "B": ICMP unreachable
- „C" (foreign) router cuts the Mobile Node from its network

- A routing protocol does not allow the advertisment of the same IP addr from two different subnetworks

IETF standards for IP mobility management

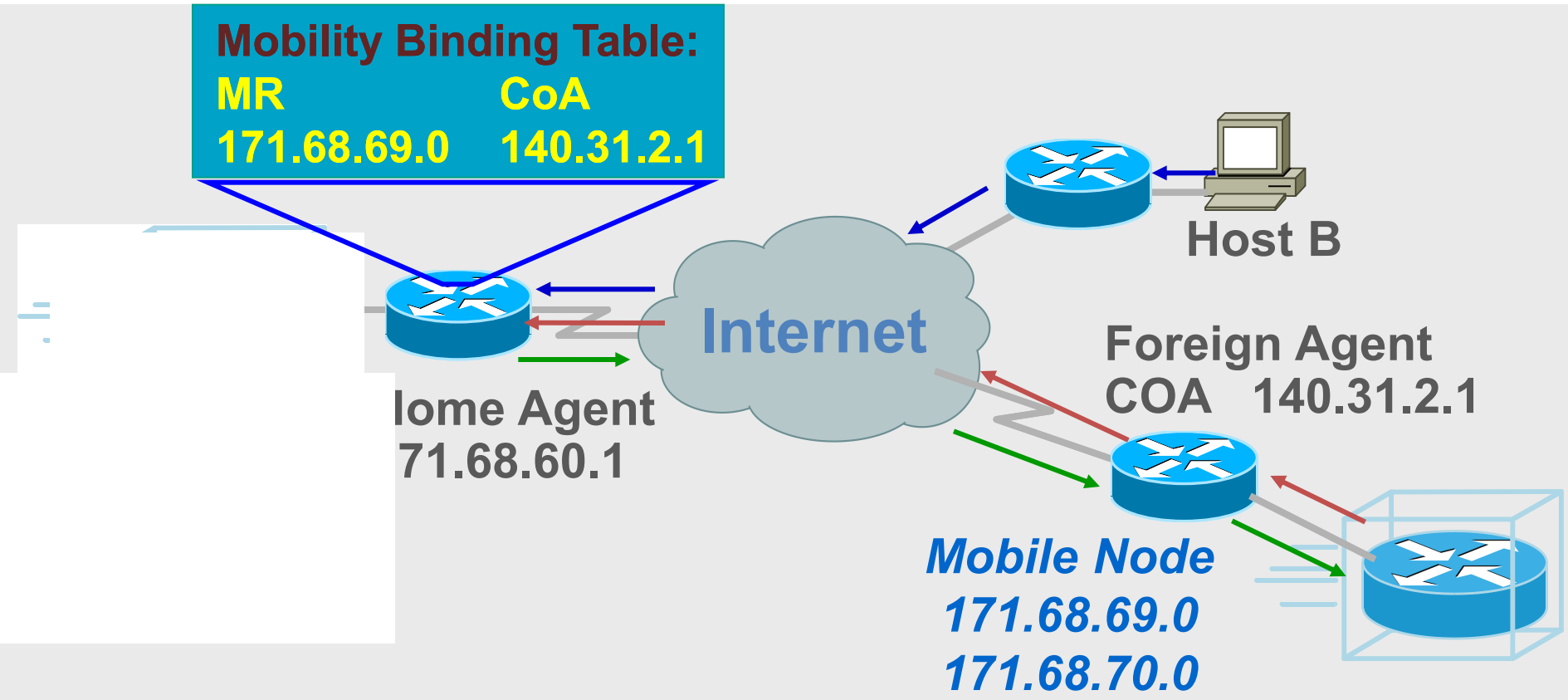
- Internet Engineering Steering Group (IESG) / June 1996 / open standard November 1996
- Mobile IP
  - IETF standard for IP level mobility management (Layer 3 mobility)
  - RFC2002/3220 - Mobile IP – basic protocol
  - RFC2003 an RFC2004 - tunneling
  - RFC2005 - Mobile IP applicability
  - RFC2006 - Mobile IP MIB
- Other RFCs
  - RFC1701 GRE – Generic Routing Encapsulation
  - RFC3024 - Reverse Tunneling for Mobile IP



Mobile IP (MIP)

- The mobile node originally has a **home address**
  - All of its communicating partners know this address
  - In a foreign network the routing problem is temporarly solved by the **care-of address**
- Mobility binding
  - A dedicated router (**home agent** - HA) keeps records about the actual care-of-address
  - HA is responsible to reach the MN if it is not “at home”
- Advantages of Mobile IP
  - All the legacy applications can be kept, they need not to be modified
  - Network shifts (handovers) can be controlled by the home agents
  - Transparent to all access (L2) technologies

Mobile IP



- Mobile Node notifies its HA with a Registration Request [RRQ] message
  - HA forwards the packets to the Mobile Node
    - Using the Care of Address [CoA]
    - CoA assigned in the foreign (visited) network

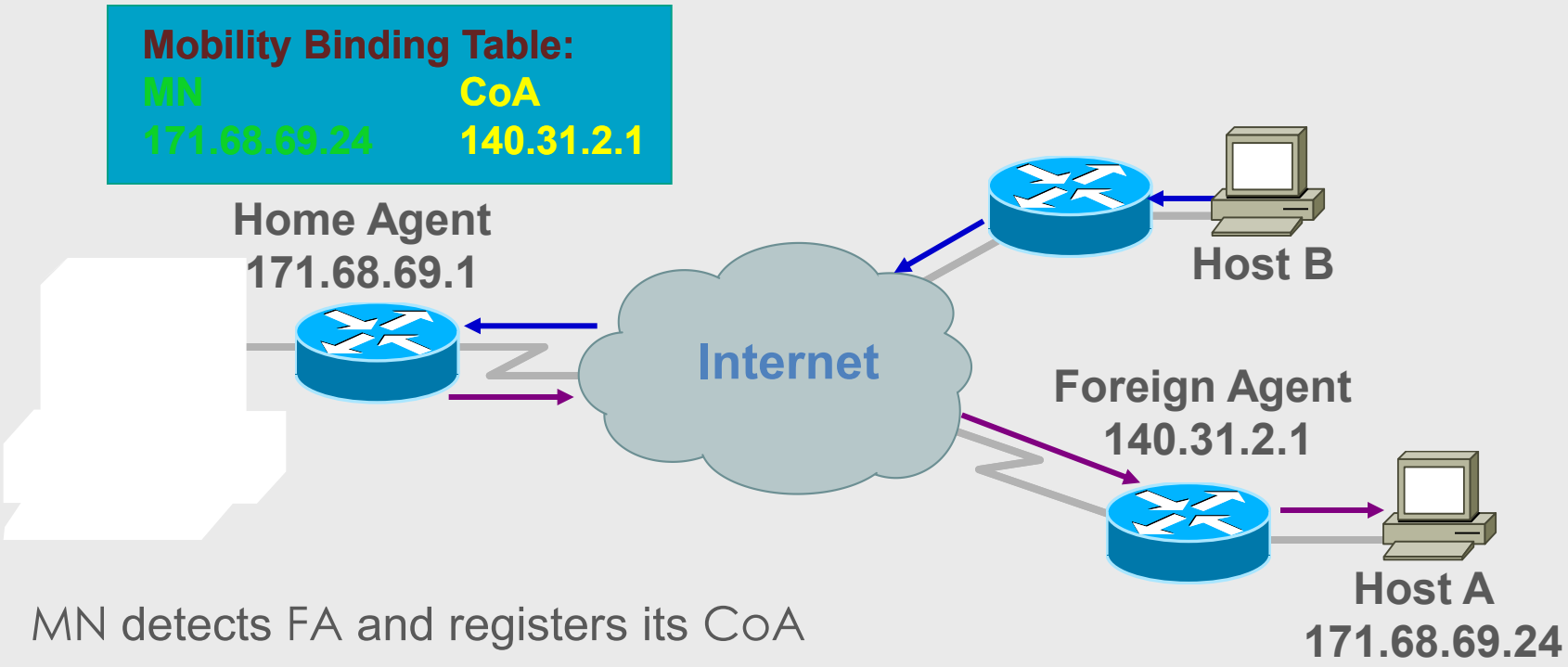
Devices in the Mobile IP (MIP)

1. Mobile Node (MN): clients running the MIP.
    1. Have a home address
    2. If they are located in a foreign network, they have a care-of-address CoA
2. Home Agent (HA): routers running the MIP.
    1. Besides acting as routers, work as localization registries, as well
3. Foreign Agent (FA): routers running the MIP.
    1. Help the registration of MNs in the foreign networks
    2. They are optional, if they are not present, the MN has more tasks to do
4. Correspondent Node (CN): a node connected to the MN
    1. A fixed node that communicates with the MN
    2. It does not know wether the MN runs a MIP or not

Mobile IP operations

- What does a MN in the foreign networks? How does it find its FA and CoA?
  - Mobility Agent Advertisements
  - Agents advertise themselves
- How does the HA know where has its MN gone?
  - Registration
  - MN updates its state at its HA if it gets a new CoA
- How does the HA send the packets to the MN?
  - Tunneling
  - HA adds a new IP header (using the CoA as source address) to the original packet

Mobile IP Activities Example



- MN detects FA and registers its CoA
- HA updates the position of MN in its table
  - Sets up a tunnel until FA
  - FA „unpacks” the packet received from HA over the tunnel – forwards it to MN

NEMO

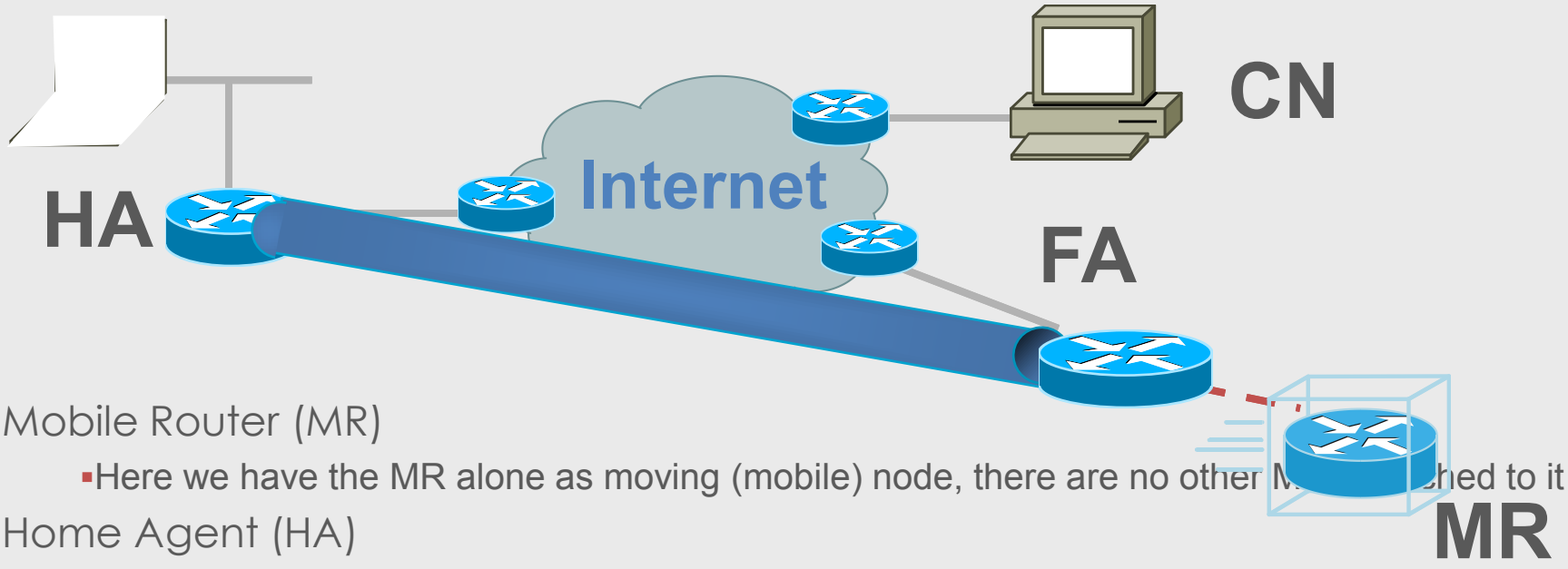
NEMO

- Many MNs move together
  - Moving Network (MONE)
  - Network in motion (NEMO)
- Let's manage their mobility together
  - Moving Network Nodes (MNN)
  - The nodes forming the NEMO
- MR (mobil router) – default gateway
  - Assures the connection between NEMO-members and outside world
  - MRs usually have the largest battery-lifetime, the largest bandwidth, etc
  - E.g., a dedicated router installed on a vehicle, connected to the power system of the vehicle
- The MNNs must register at the MR
  - They belong to the subnetwork of the MR
  - They are "fixed" into that network, do not change their relative position to the MR – alternativley named Fixed Local Node (FLN)
- Advantages
  - only one mobility management event at network-change

Efficiency of NEMO depend on the environment it is deployed

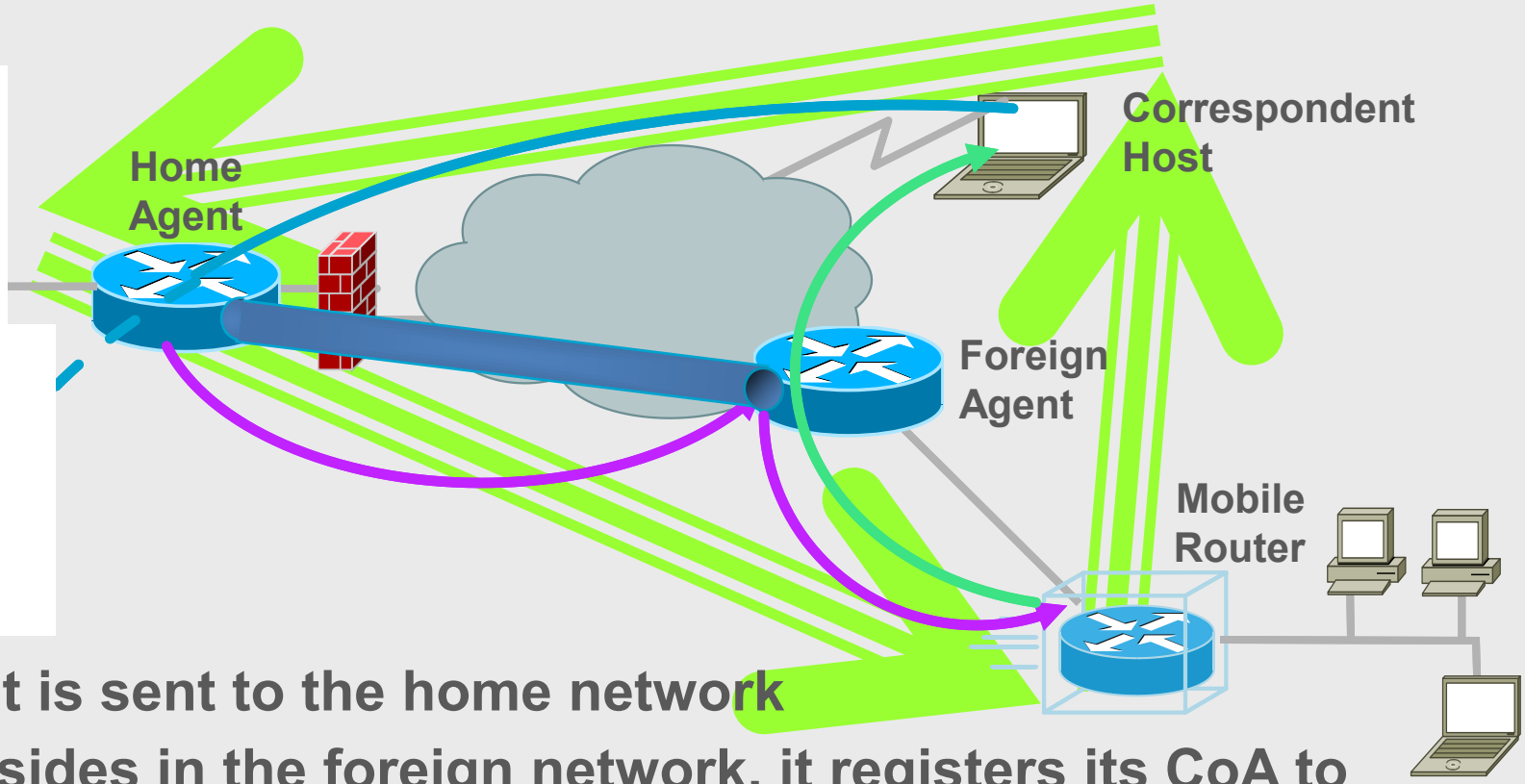
- (Potential) disadvantage:
  - E.g., 100 MNs use cellular mobile internet access in a urban environment
  - If the MNNs do not join the NEMO
    - - They manage their mobility individually
    - + Each of them will receive individually a BW specific to the technology
  - If the MNNs join a single NEMO
    - The bottleneck will be the MR's link capacity
    - If it uses the same public access, in the worst case an MNN will receive only 1/100th of the BW compared to the previous case
- (Potential) advantage:
  - E.g., the same 100 MNs request for access on a plane
    - Practically this means that the MN has no other access except an MR
  - In this case at least the mobility management is optimized over the sparse wireless resource

Mobile IP Terminology



- Mobile Router (MR)
  - Here we have the MR alone as moving (mobile) node, there are no other M… …hed to it
- Home Agent (HA)
- Foreign Agent (FA) [1 Hop Away from MR]
- Care of Address (CoA) [Tunnel Endpoint]
- Correspondent Node (CN)
- Security Association (SA) [SPI/Key]
- ICMP Router Discovery Protocol (IRDP) [Advertisement]
- Registration Request (RRQ)

Triangle routing



- Packet is sent to the home network
- MR resides in the foreign network, it registers its CoA to the HA
- HA forwards the packet towards the MR,

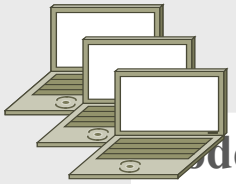
  using the HA-FA tunnel
- The packets from MR are addressed directly to CN

NEMO dual tunnel

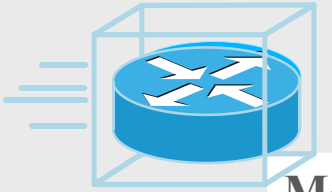
- In the case of NEMOs there is an additional problem apart of the triangle routing
- MNNs register to the MR
- Every packet originally sent to MNN arrives to the Home Network of the MR
  - The MR will then forward it to the MNN
  - We already use a tunnel: on the Home NW – MR path
- If the NEMO moves to a foreign network
  - Intervenes a new HA-FA

Mobile Network Routing – Packet Flow

Mobile Networks



de on MR



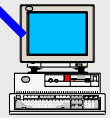
Mobile Router

Foreign Agent

Internet

Mobile Networks appear to be here

Home Agent

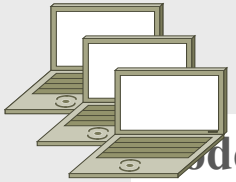


Correspondent Node

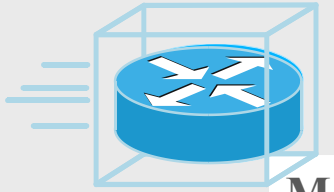
Edited slide from original by Lawrence Searcy, Cisco Systems

Mobile Network Routing – Packet Flow

Mobile Networks



ode on MR



Mobile Router

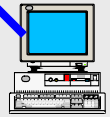
HA-FA Tunnel

Foreign Agent

Internet

Mobile Network appears to be here

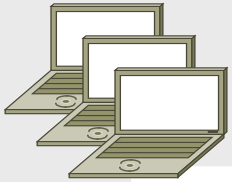
Home Agent



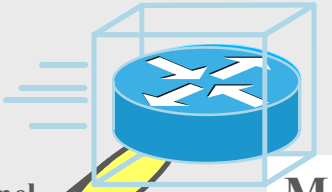
Correspondent Node

Mobile Network Routing – Packet Flow

Mobile Networks



Nodes on MR



Mobile Router

HA-MR Tunnel

FA WAN

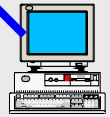
HA-FA Tunnel

Foreign Agent

Internet

Mobile Network appears to be here

Home Agent



Correspondent Node

Mobile Network Routing – Packet Flow

Mobile Networks

de on MR

Mobile Router

HA-MR Tunnel

FA WAN

HA-FA Tunnel

Foreign Agent

Internet

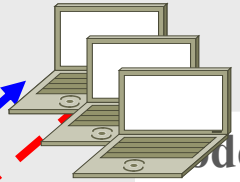
Mobile Network appears to be here

Correspondent Node

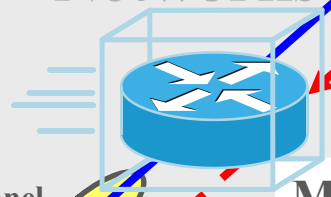
Home Agent

Mobile Network Routing – Return Packet Flow

Mobile Networks



de on MR



Mobile Router

HA-MR Tunnel

FA WAN

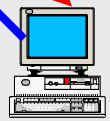
HA-FA Tunnel

Foreign Agent

Internet

Mobile Network appears to be here

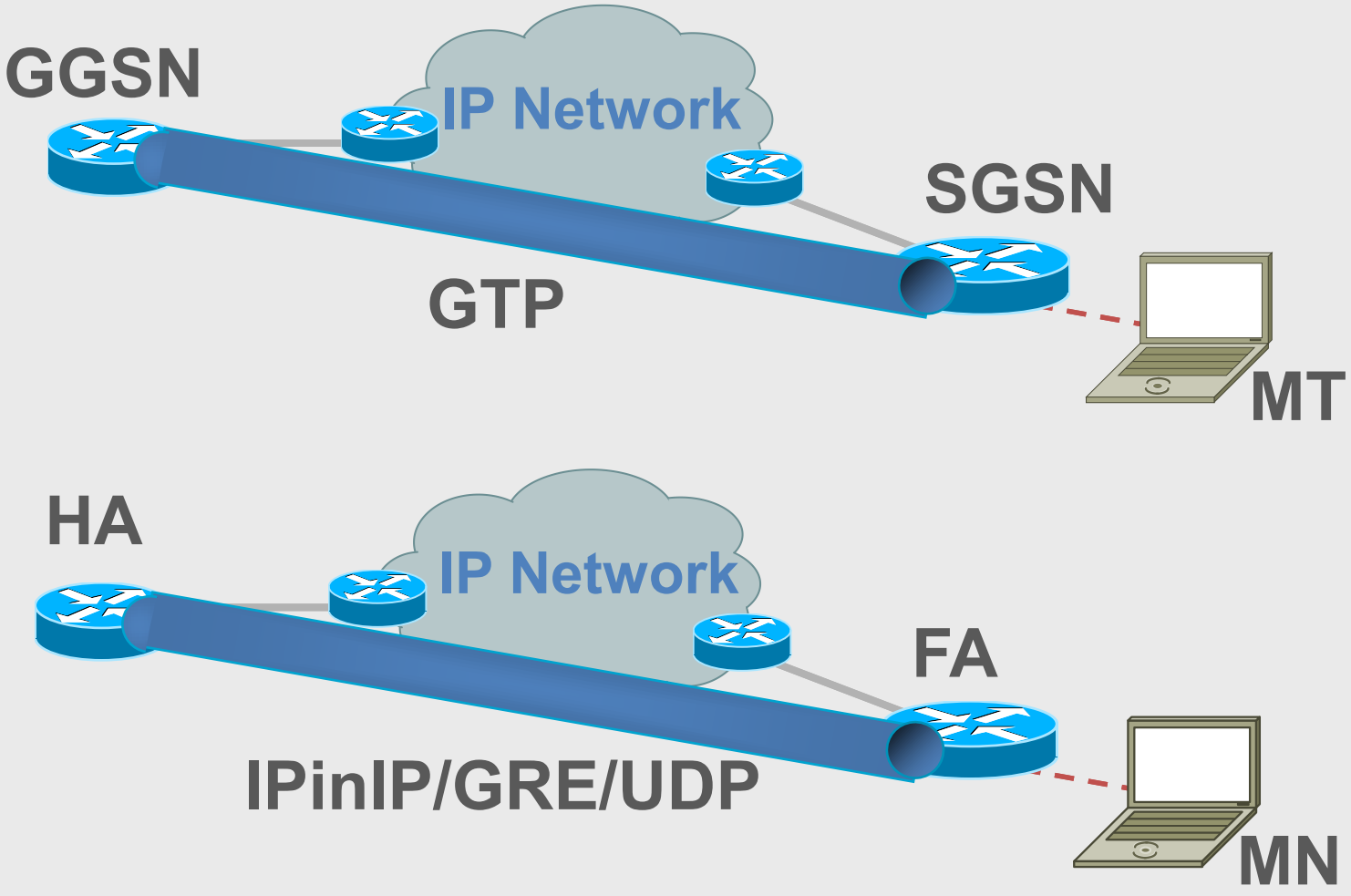
Home Agent



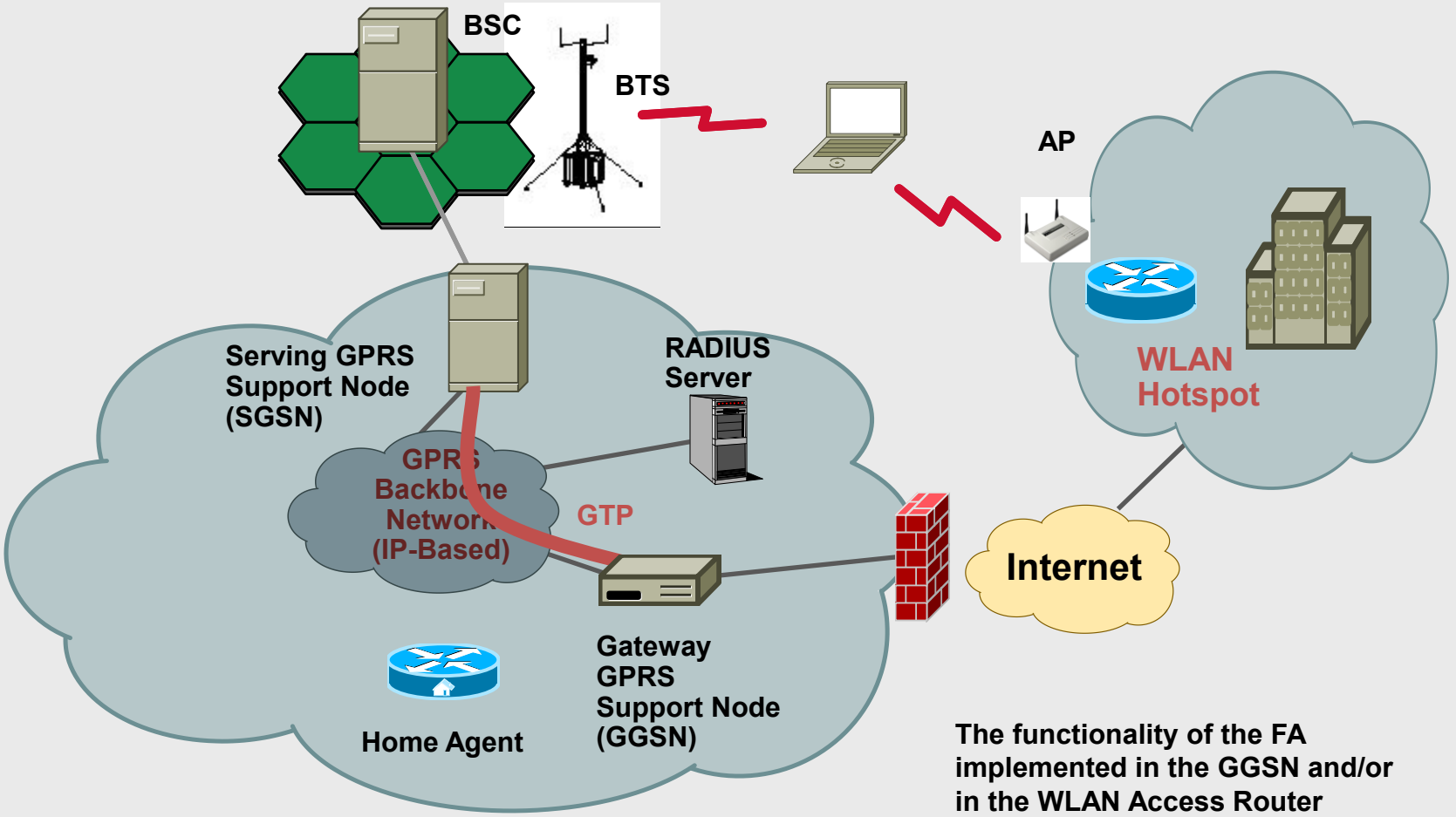
Correspondent Node

Where are MobileIP-like solutions used in current telecom networks?

Similarities in the Mobile IP and GPRS



Mobile IP and GPRS



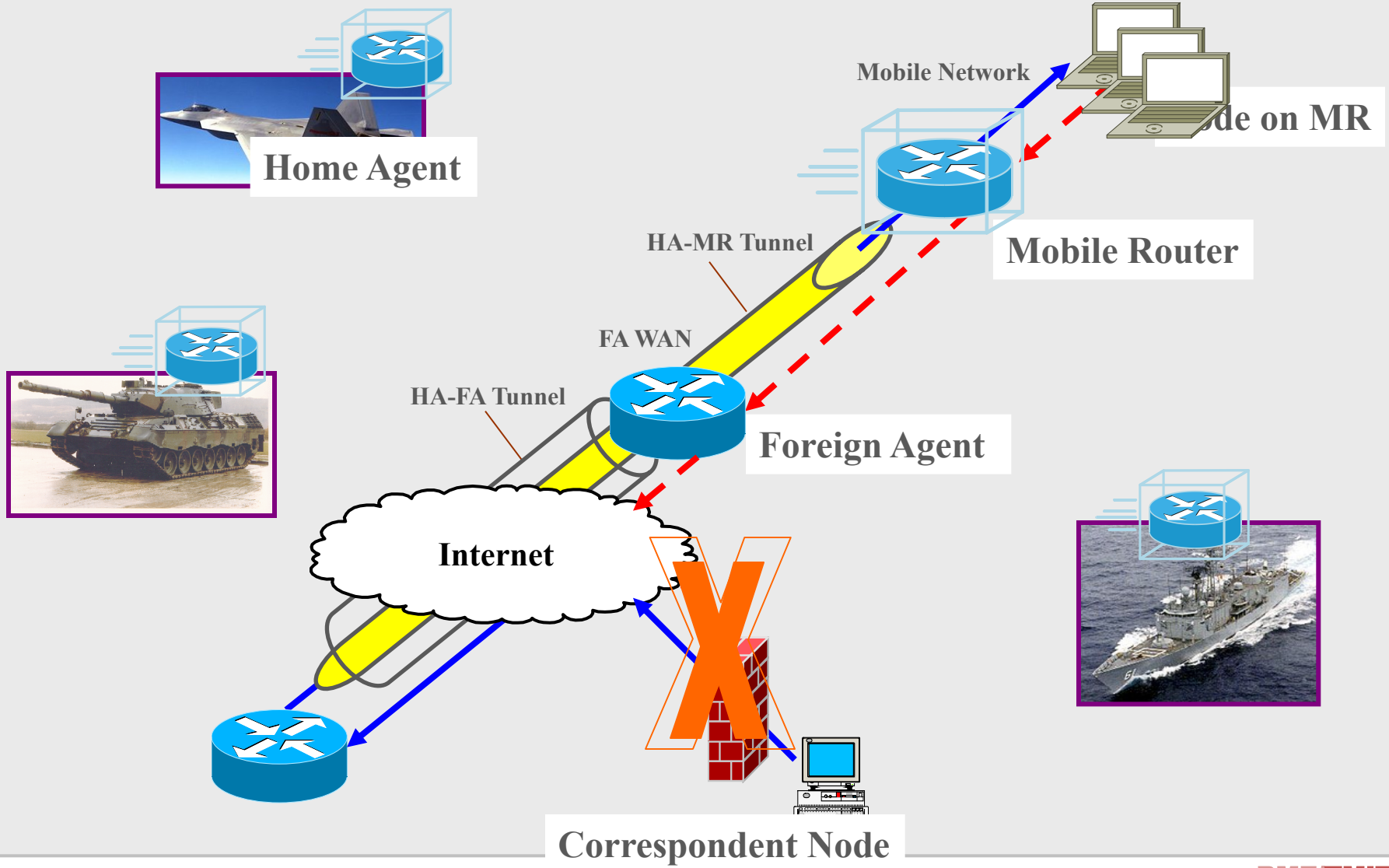
Reverse Tunneling (bi-directional tunneling)

Reverse Tunneling

- Usually routers check only the destination address
- Firewalls take a look at the source address, as well
  - detecting the spoofing attacks
  - ingress filtering (based on the source address) – if the packet is not coming from the subnet of the source address
- MIP often uses tunneling
  - E.g., the MNN is not coming from a subnet compatible with the source address of the header

Mobile Network Routing – datapath

According to its access, the NEMO is here – but the packet arrives from a different direction, thus the firewall considers it as an attack



Reverse Tunneling

- Reverse tunneling
  - avoids the „ingress filtering” problem
- We need a different tunnel to send the packet back on
  - Reverse tunneling or bi-directional tunneling
- HA de-capsulates the packet and forwards it according to the usual routing process
- The address of the packet ”covers” the topology
  - The packet is coming from the subnet that corresponds to the source address

Mobile Network Routing – Reverse Tunneling

Mobile Network

Roaming Interface

Mobile Router

HA-MR Tunnel

FA WAN

HA-FA Tunnel

Foreign Agent

Internet

NEMO appears to be here

Home Agent

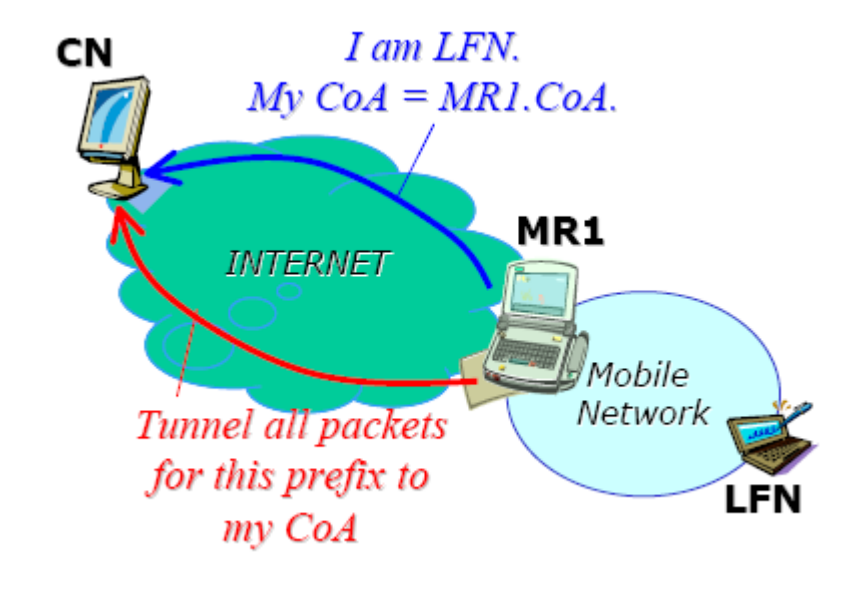
Correspondent Node

Edited slide from original by Lawrence Searcy, Cisco Systems

Routing Optimizations (RO)

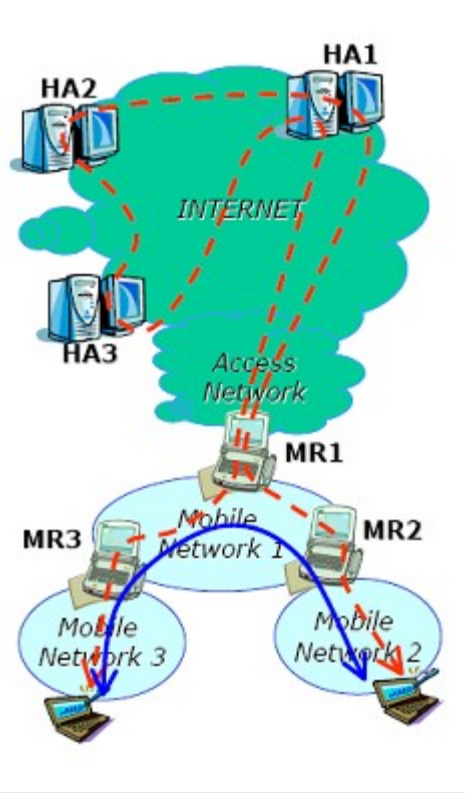
Routing optimization (RO)

- Between the MR and CN
- LFN – local fixed node (in the NEMO, registered to the MR)
- Prefix-based Binding Update – every packet addressed to the LFN registered to MR1 is forwarded to MR1
- We eliminate the Home Agent (HA) of LFN from the path



Advantages of RO

- Nested NEMOs
  - E.g., two Personal Area Networks - PANs (MR2, MR3) on a traing (MR1)
- Eliminating the tunneled path
  - Avoid walking on the redundant HA1-HA2-HA3 path
  - Solve the communication locally, within the MR1



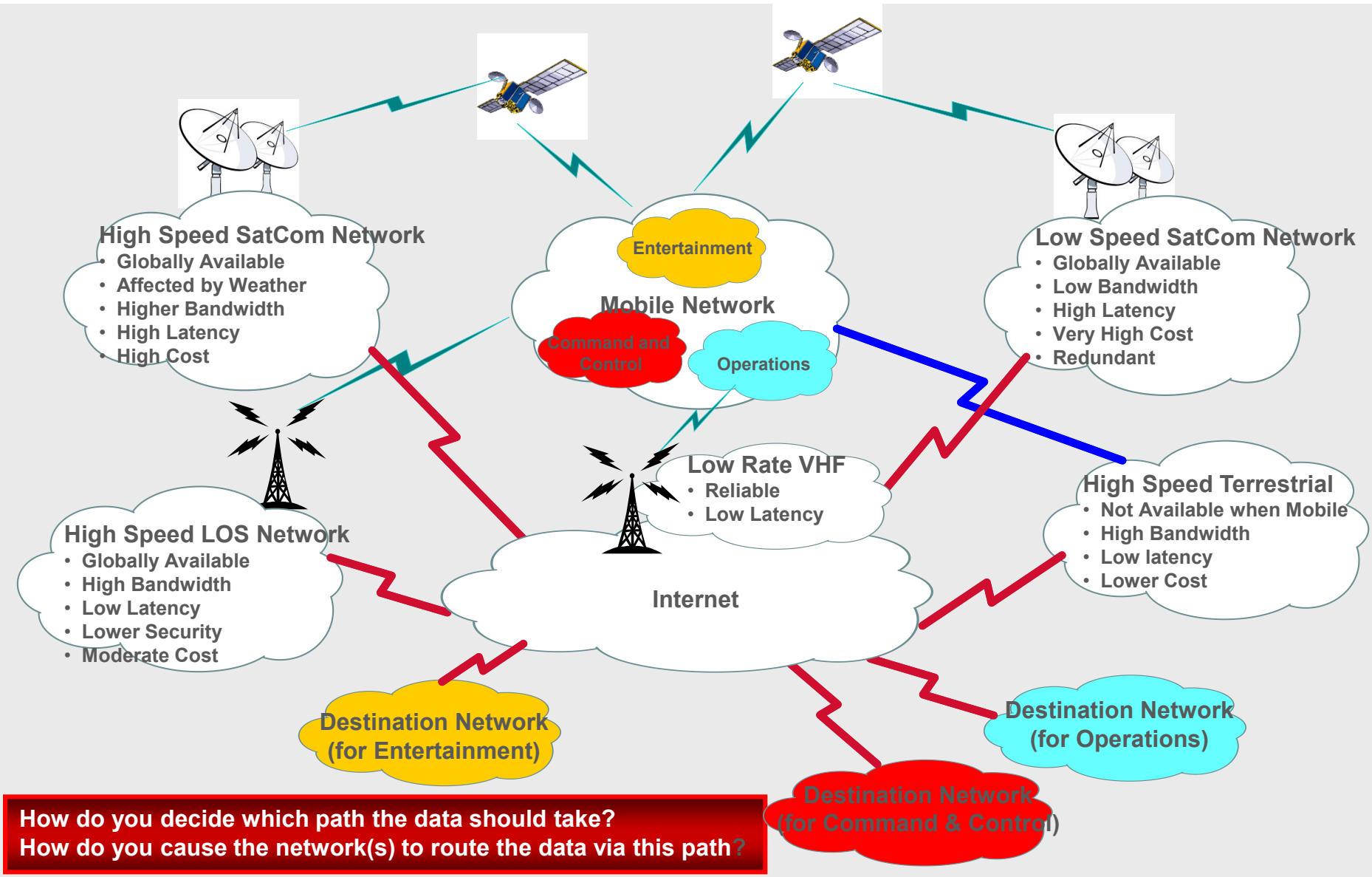
Case study: NEMOs in the airline industry

Multi-Domained, Multi-Homed Mobile Networks

To Join to the Mobile Platform Internet (MPI) mailing list, E-mail to:
MPI-subscribe@multicasttech.com

Terry Davis – Boeing (terry.l.davis@boeing.com)
Will Ivancic – NASA Glenn (william.d.ivancic@nasa.gov)

How Do You Select and Implement the Routing Path?

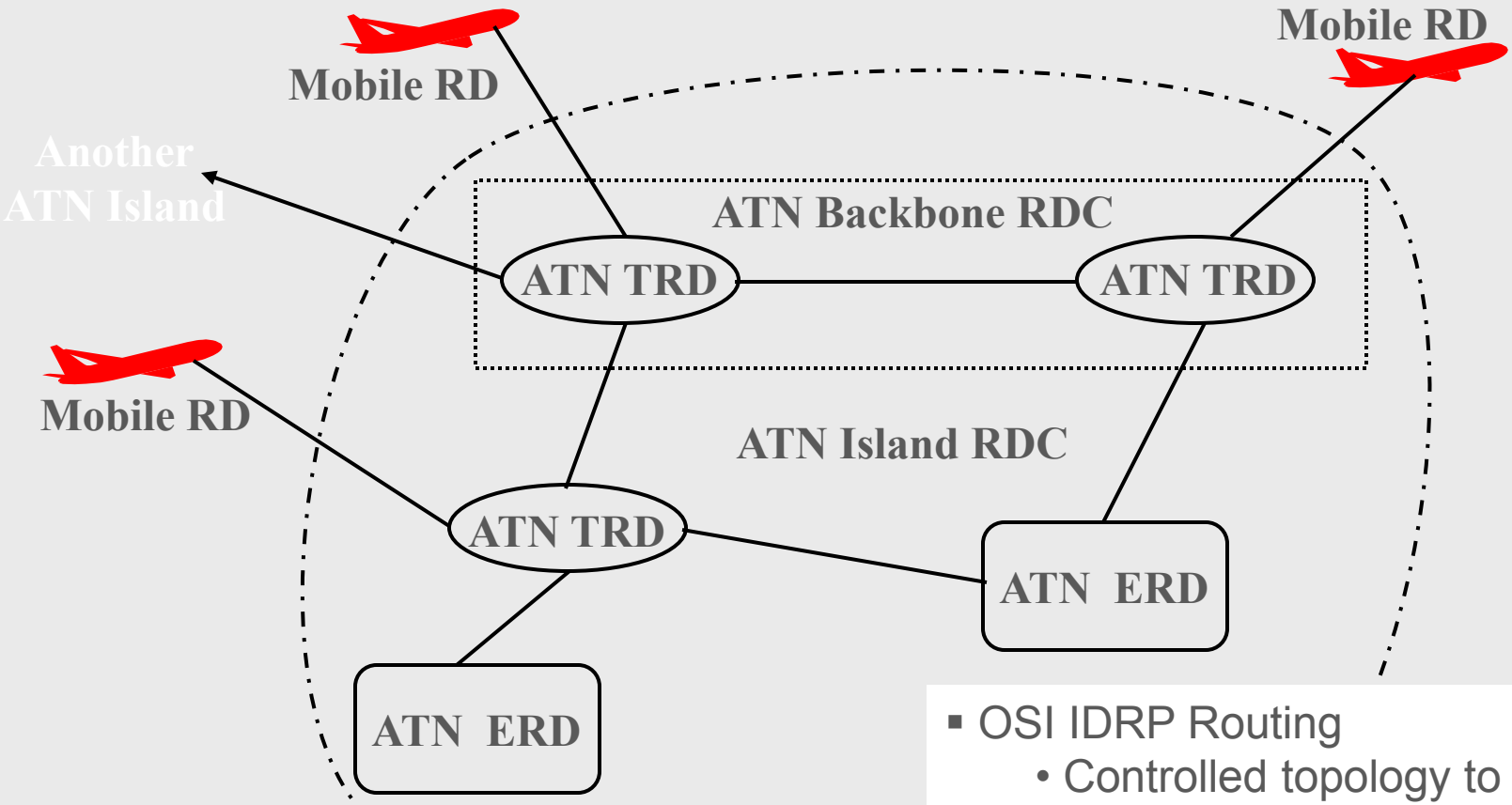


How do you decide which path the data should take?
How do you cause the network(s) to route the data via this path?

In-Air Communication

- Many networks work in parallel on a plane
  - Different requirements
  - Aircraft Control Domain
  - Airline Information Services Domain
  - Passenger Information and Entertainment Services Domain
- Several times the same function is served by parallel connections
- Connected to ten, or more ISPs (internet service provider)
  - Autonomic (independent) connection/switch to/between the ISPs
  - The contracts with the ISPs are managed by the airports

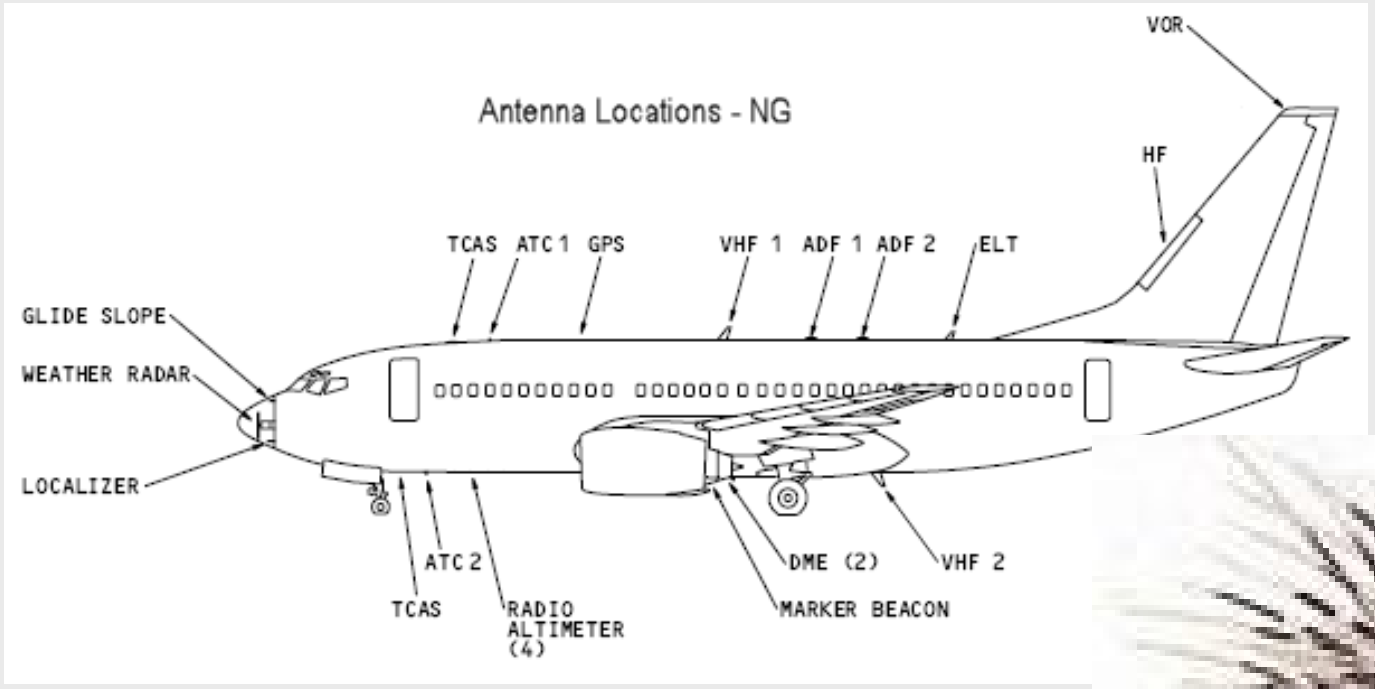
ISO Aeronautics Telecommunication Network (ATN) Island Routing Domain Confederation



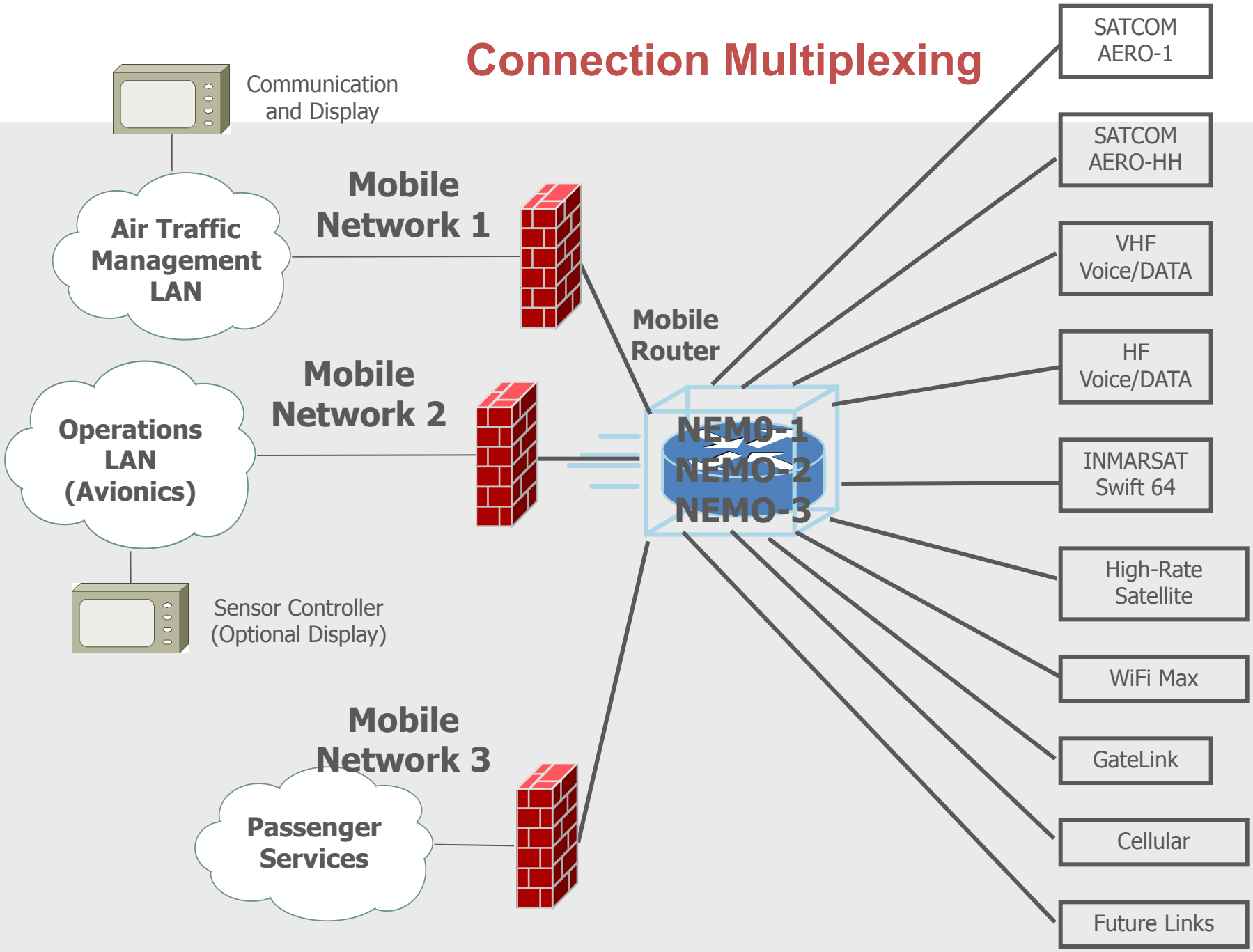
- OSI IDRP Routing
  - Controlled topology to ensure rapid route prorogation
- Routing Protocols requires ownership/coordination of infrastructure
  - Injecting routes
  - Not deployed due to cost

ERD – End Routing Domain
RD – Routing Domain
RDC – Routing Domain Confederation
TRD – Transit Routing Domain

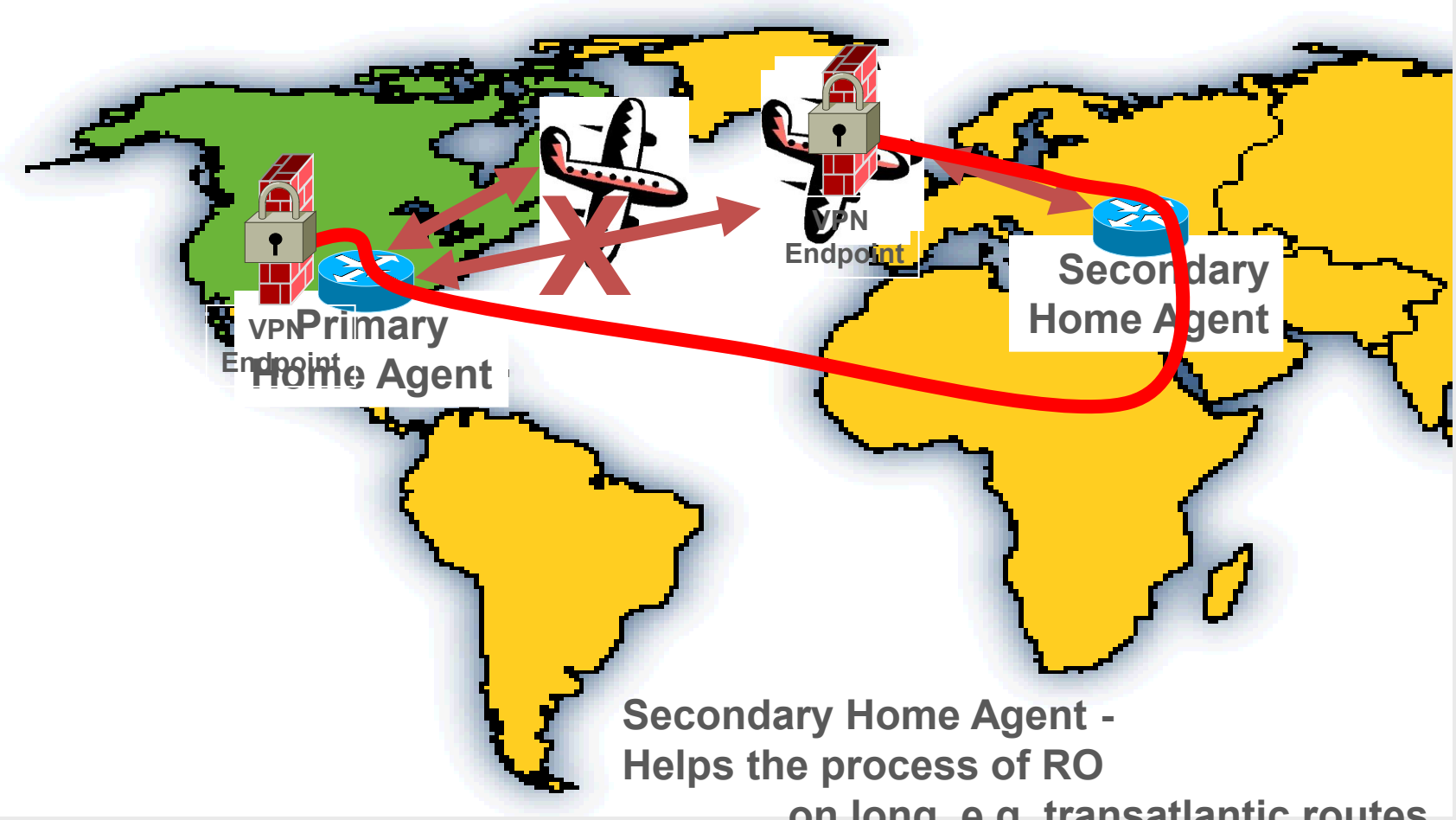
Independent radio interfaces on a plane



Connection Multiplexing



RO with two HAs



Use of VPN tunnels

If they are not prepared to handle VPNs, RO is not working ☹

End of case study