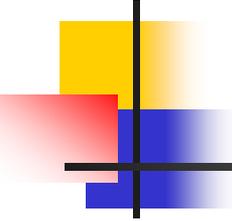


Mobile Networking

As Applied to Any Mobile Network Including Aeronautical Internets

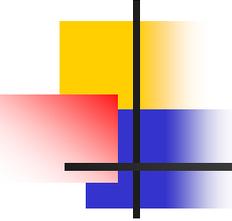
Airborne Internet Collaboration Group meeting April 17, 2003

Will Ivancic – wivancic@grc.nasa.gov



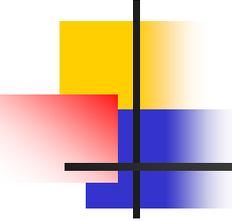
Outline

- Mobile Networking Solutions
- Aeronautical Telecommunication Network (ATN)
- Mobile-IPv4 Operation
- Secure Mobile Network Demonstration
- Mobile-IPv6 Operation
- Networks In Motion (NEMO)
- NASA Glenn Research Center Research



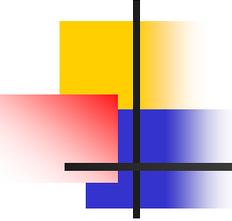
Mobile Networking Solutions

- Routing Protocols
 - 😊 Route Optimization
 - 😞 Convergence Time
 - 😞 Sharing Infrastructure – who owns the network?
- Mobile-IP
 - 😞 Route Optimization
 - 😊 Convergence Time
 - 😊 Sharing Infrastructure
 - 😊 Security – Relatively Easy to Secure
- Domain Name Servers
 - 😊 Route Optimization
 - 😞 Convergence Time
 - 😞 Reliability



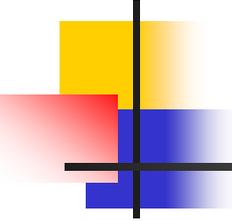
Aeronautical Communication Requirements for ATN

- Interoperability with existing subnetworks
- High availability
- Mobile Communication
- Message prioritization
- Policy based routing
- Security
 - Just now being considered
- Bit Efficiency
- Support for multiple mobile subnetworks
- Mobile platform forms its own Routing domain



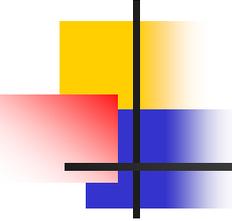
Aeronautical Communication Requirements – Questions?

- How much is politics, how much is technical requirements.
 - Policy based routing
 - Is this a political or technical requirement?
 - Security – Previously undefined
 - Can Links handle Authentication, Authorization, Accounting and Encryption?
- Bit Efficiency
 - Is this due to limited links.
- Load Sharing of RF links
 - Is this specified, implied or not necessary
 - Current (and perhaps future) implementations of Mobile Networking do not support this.



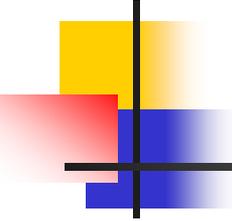
ATN Non-Requirements

- Sharing Infrastructure
- Multicasting
- Interoperate with non-ATN applications
- Unidirectional Link Routing
- Use of Commodity products and protocols
- Cost Effective
- Flexible
- Adaptable
- Evolvable



ATN Solutions for Mobility

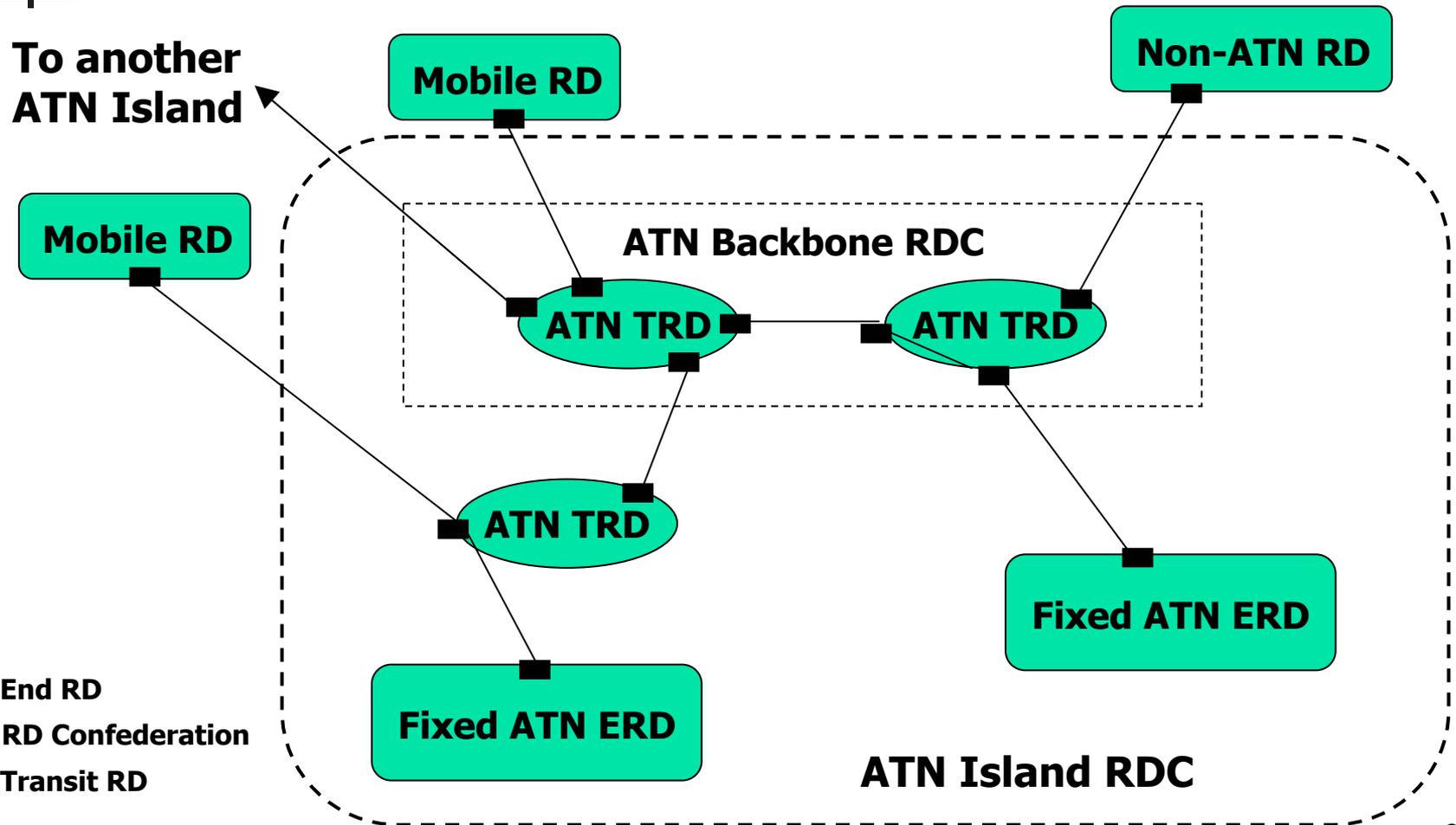
- Uses Inter-Domain Routing Protocol (IDRP) for routing
- Implements distributed IDRP directory using Boundary Intermediate Systems (BISs)
- Two level directory
 - ATN Island concept consisting of backbone BISs
 - Home BISs concept
- Scalability obtained by the two level structure
- Resilience is provided by the distributed approach



ATN

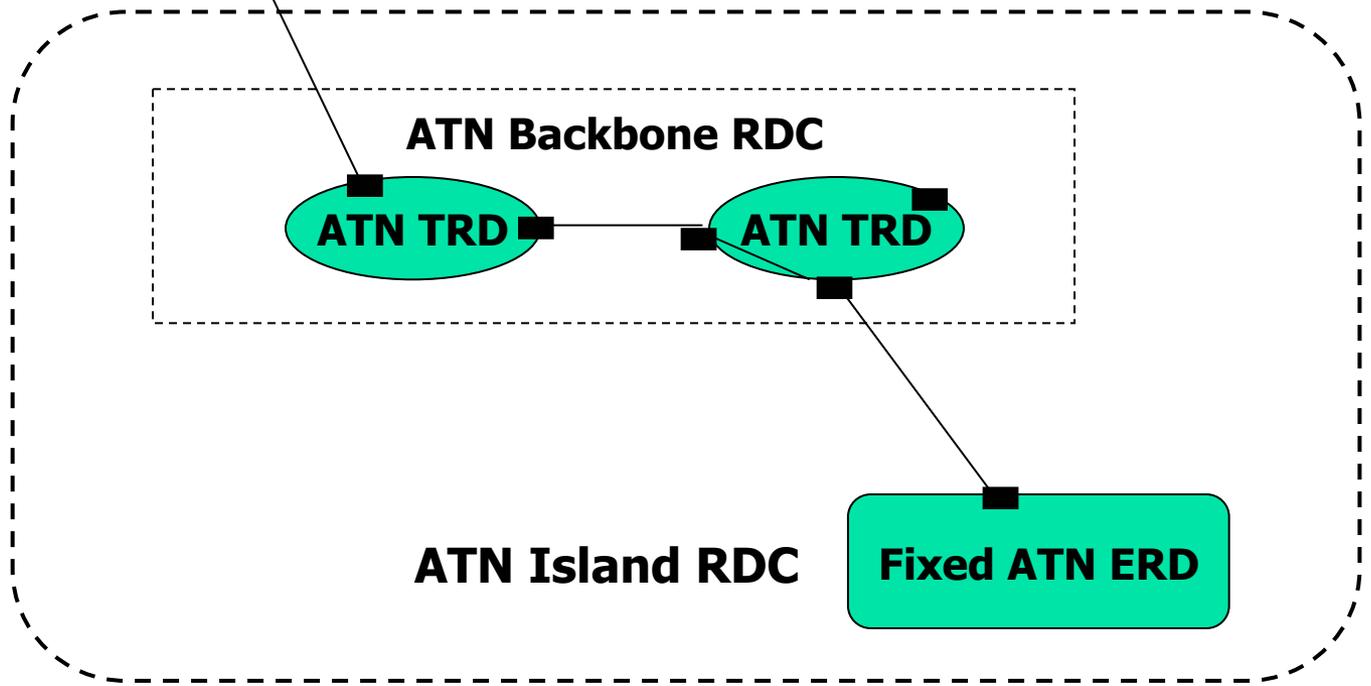
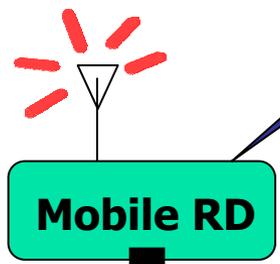
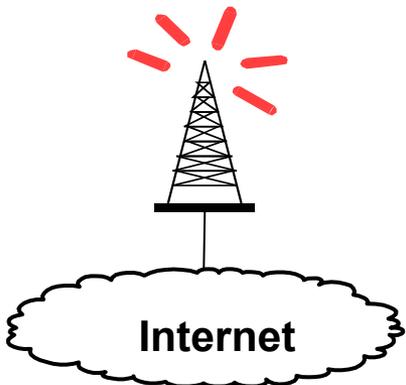
- ATN Routing uses the IDRPs Routing Protocol
 - IDRPs supports policy based routing which allows administrations to autonomously control use of their network
 - IDRPs supports mobility by permitting aggregate routes to be selectively propagated through the network

ATN Island Routing Domain Confederation Structure



**Pick Your Radio
(i.e.802.11)**

**Pick Your
Satellite Service
Suppliers**



Internet

Mobile RD

Internet

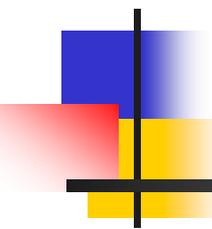
ATN Backbone RDC

ATN TRD

ATN TRD

ATN Island RDC

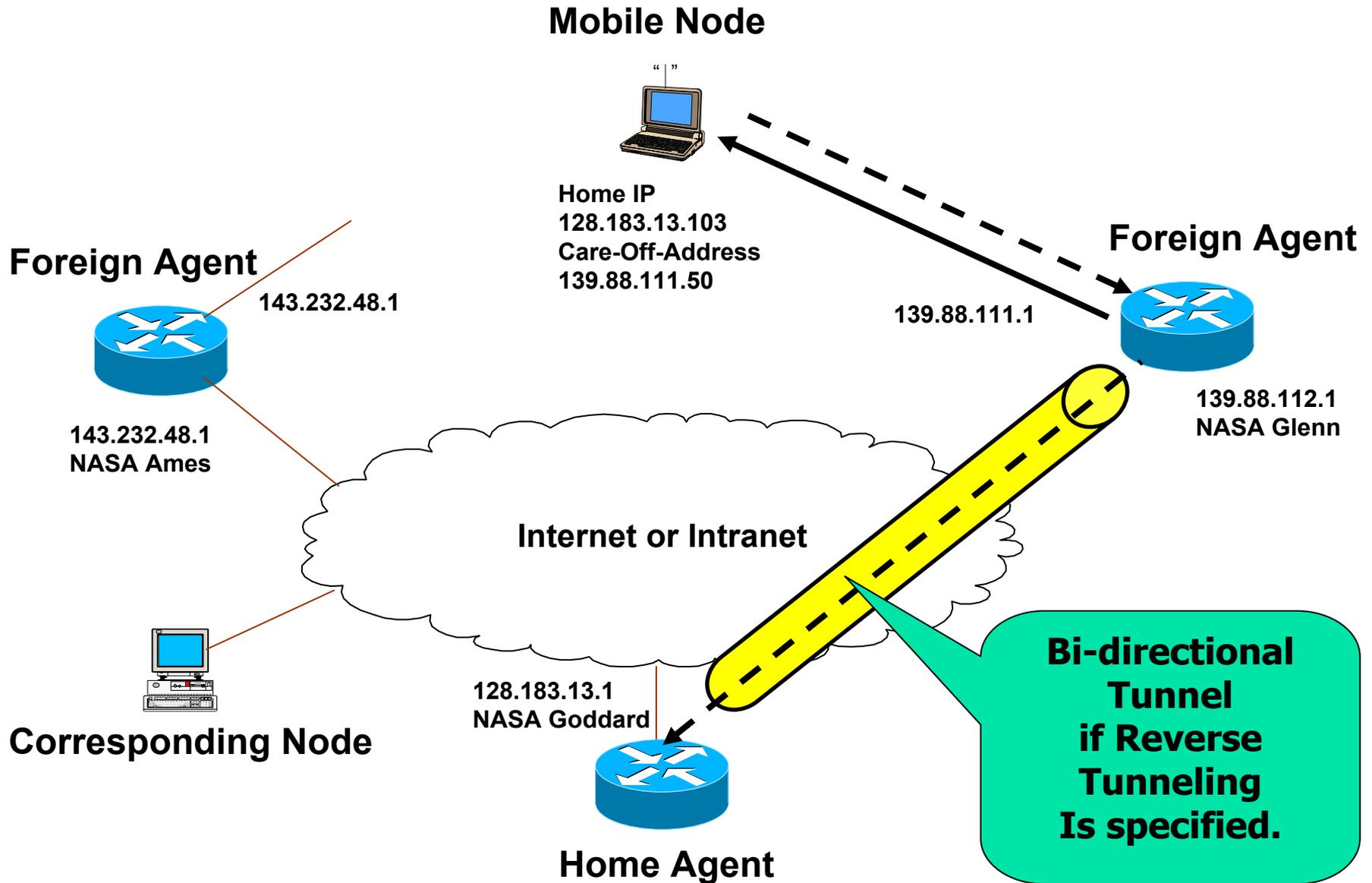
Fixed ATN ERD



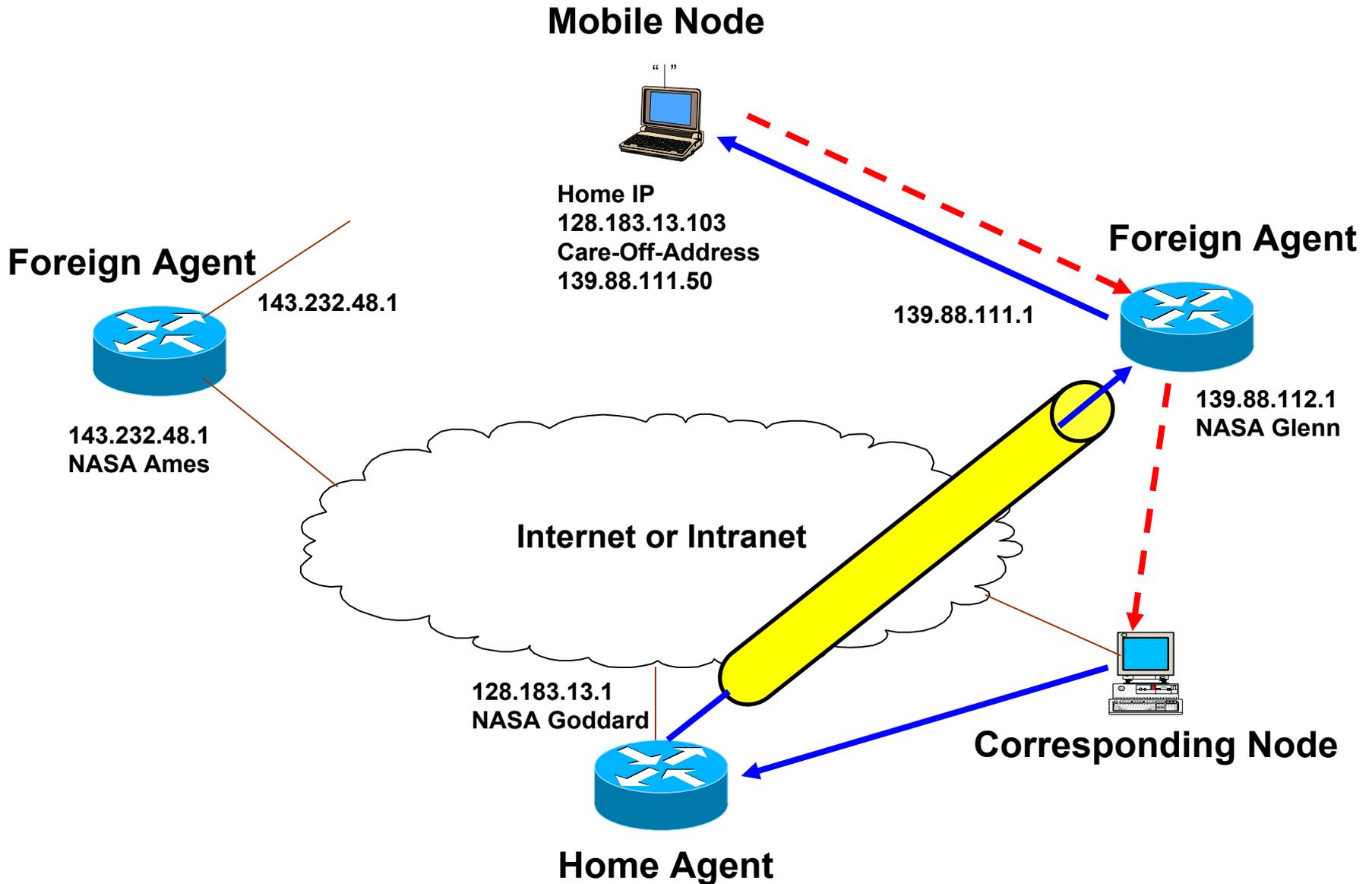
Mobile-IP Operation

IPv4

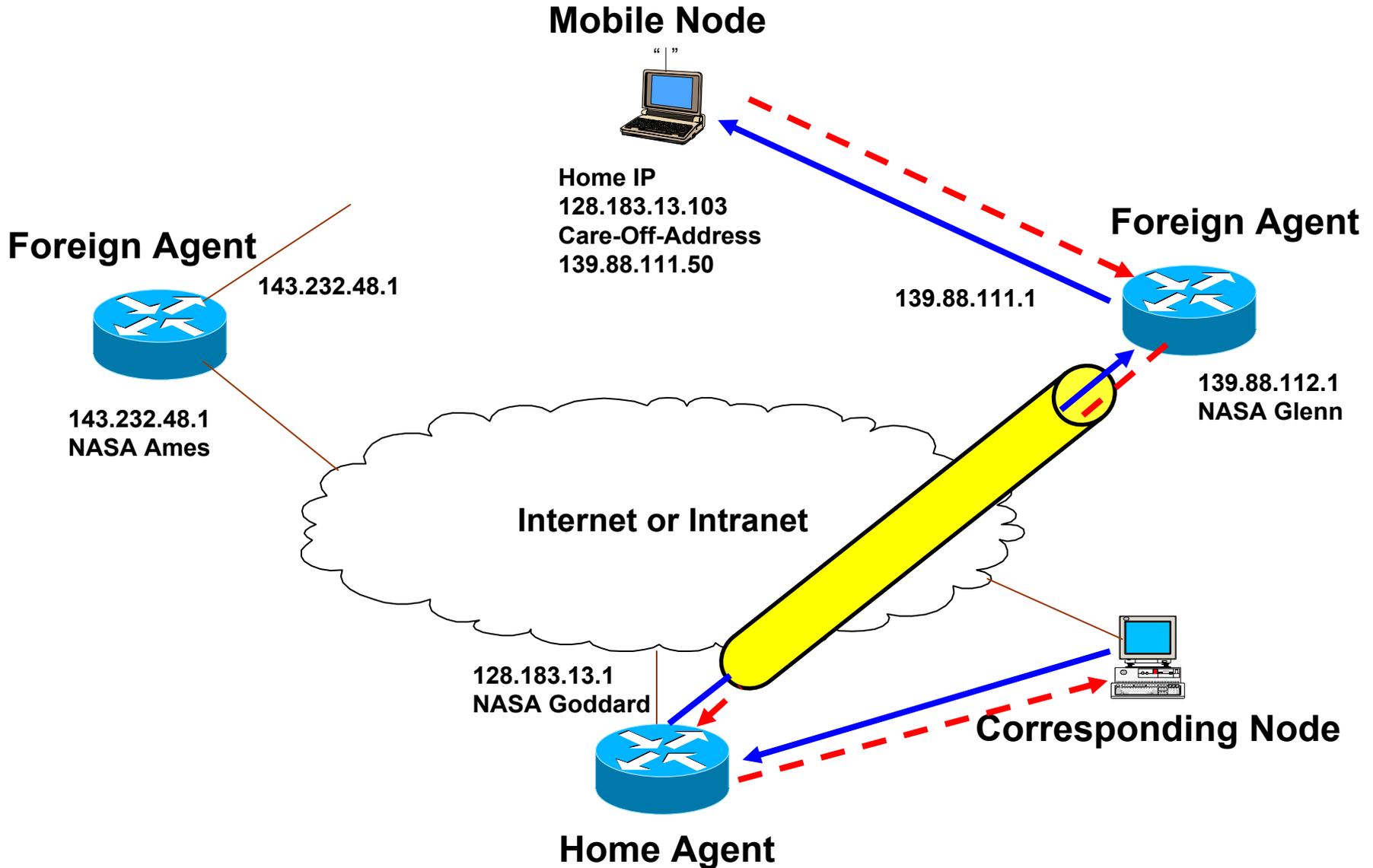
Mobile-IP (IPv4) using Foreign Agents



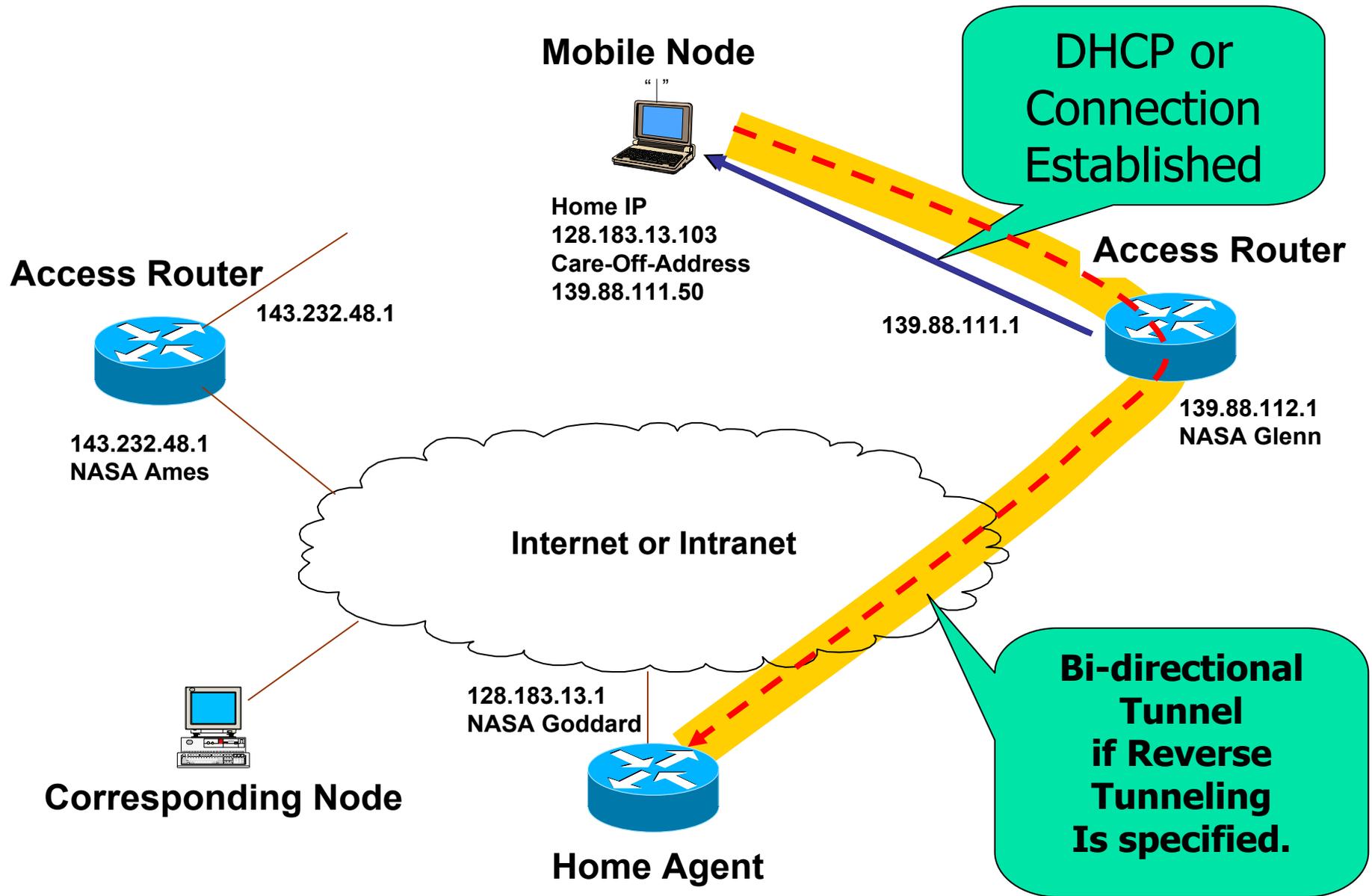
Mobile-IP (IPv4) using Foreign Agents



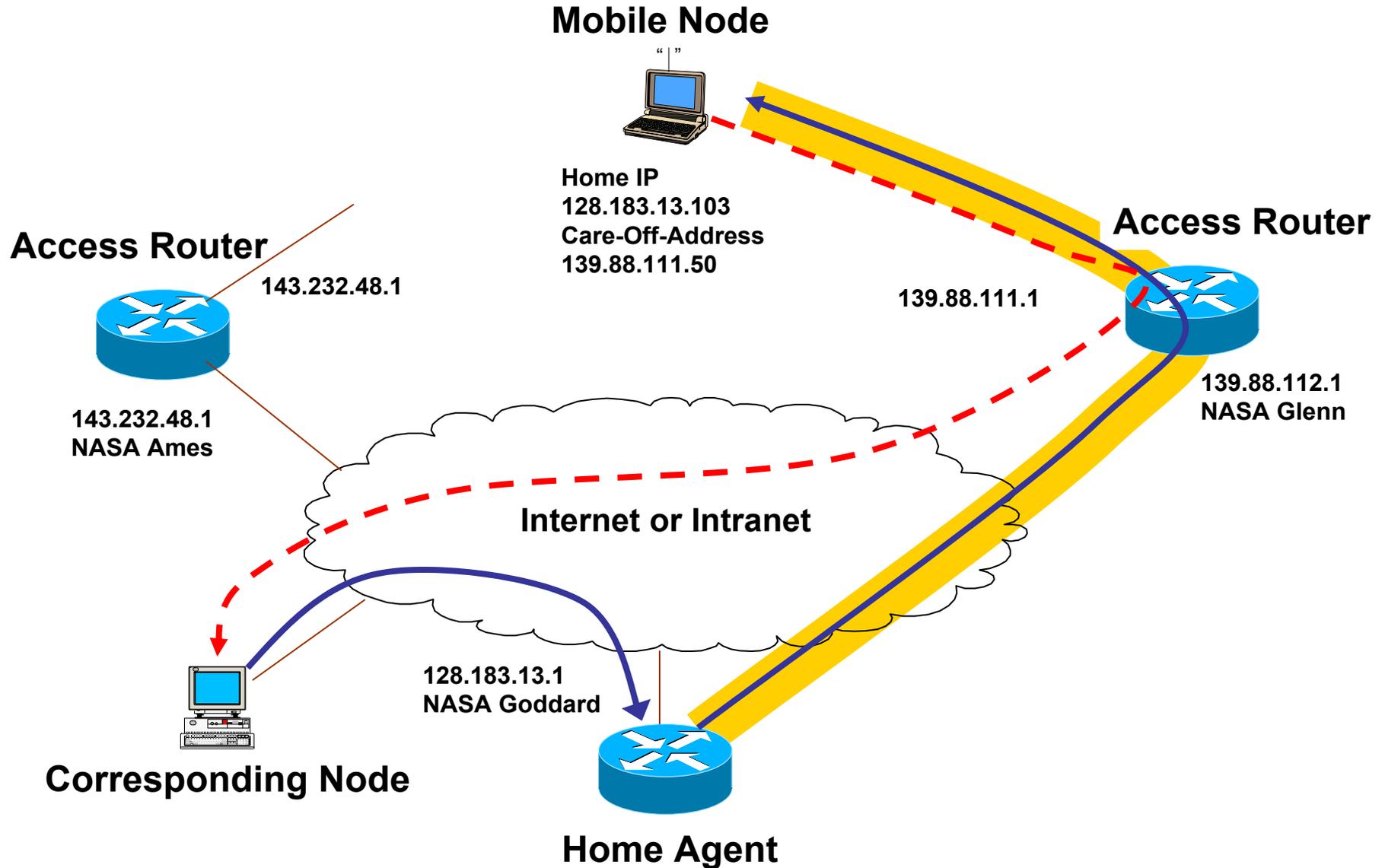
Mobile-IP (IPv4) using Foreign Agents (Reverse Tunneling)



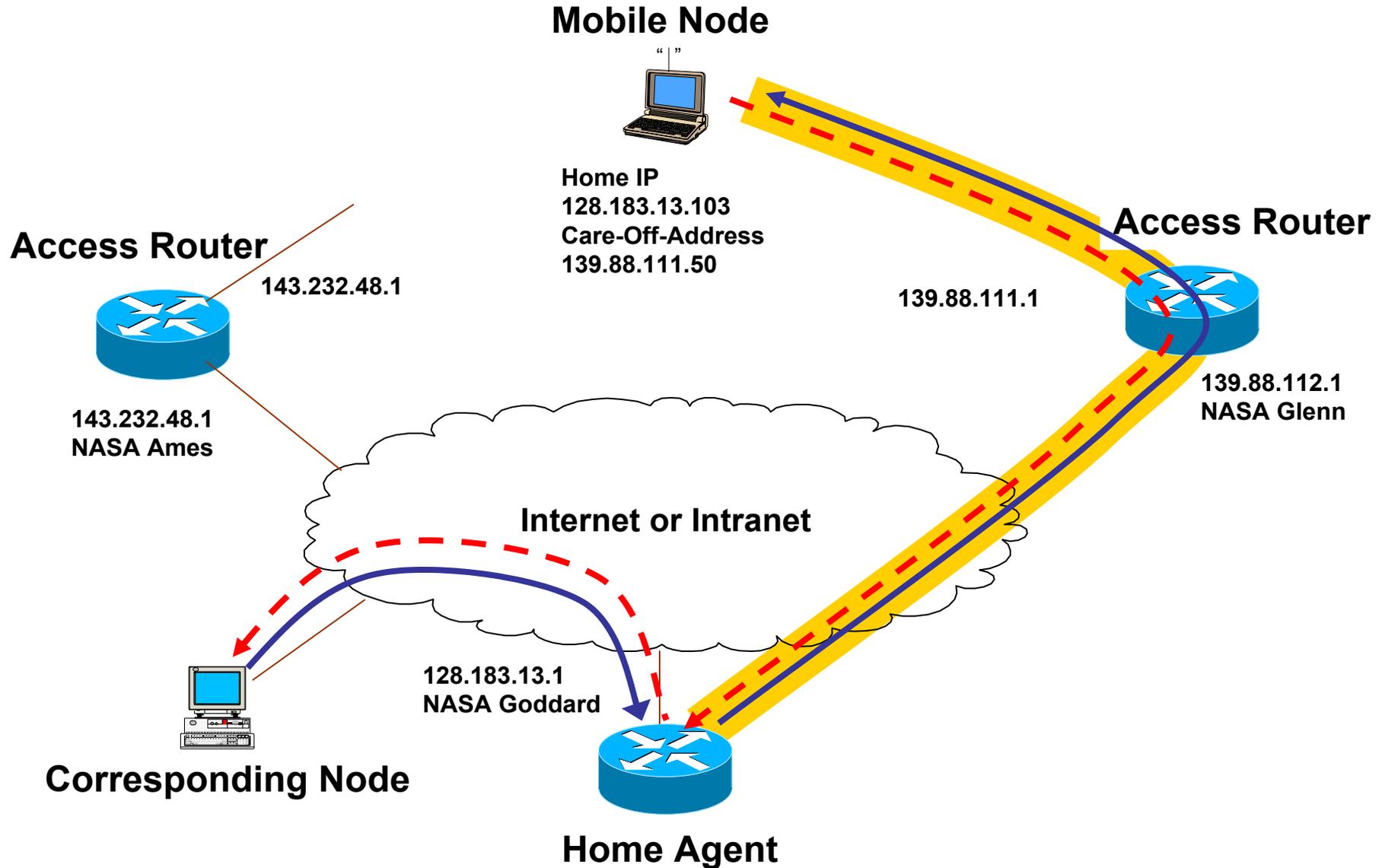
Mobile-IP (IPv4) using Collocated Care-Of-Address



Mobile-IP (IPv4) using Collocated Care-Of-Address



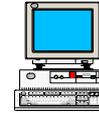
Mobile-IP (IPv4) using Collocated Care-Of-Address (Reverse Tunneling)



Mobile-Router (IPv4)

Mobile Router

128.184.24.1
Virtual LAN
Interface

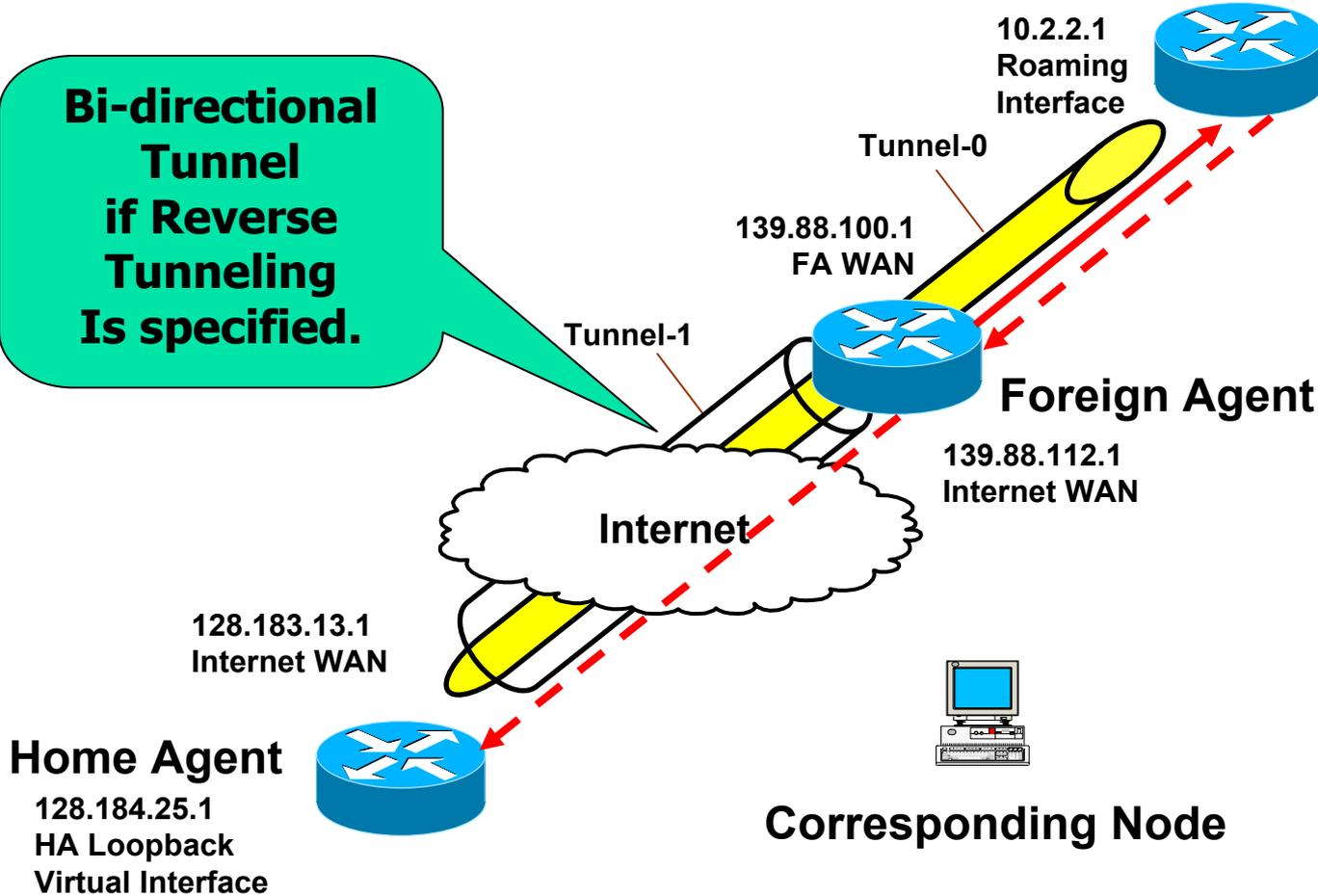


128.184.24.2

Mobile Router (Mobile Node)

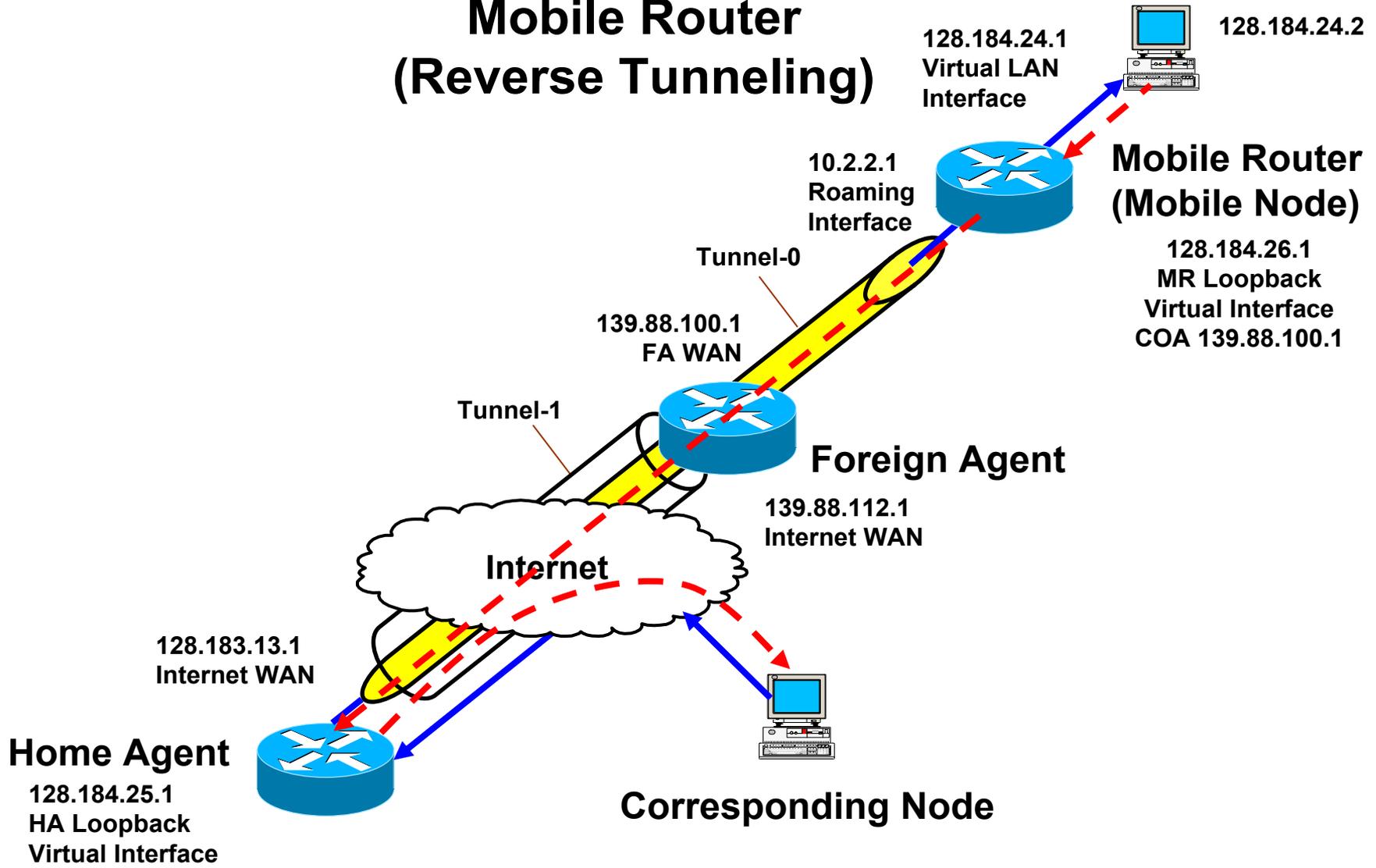
128.184.26.1
MR Loopback
Virtual Interface
COA 128.184.26.1

**Bi-directional
Tunnel
if Reverse
Tunneling
Is specified.**

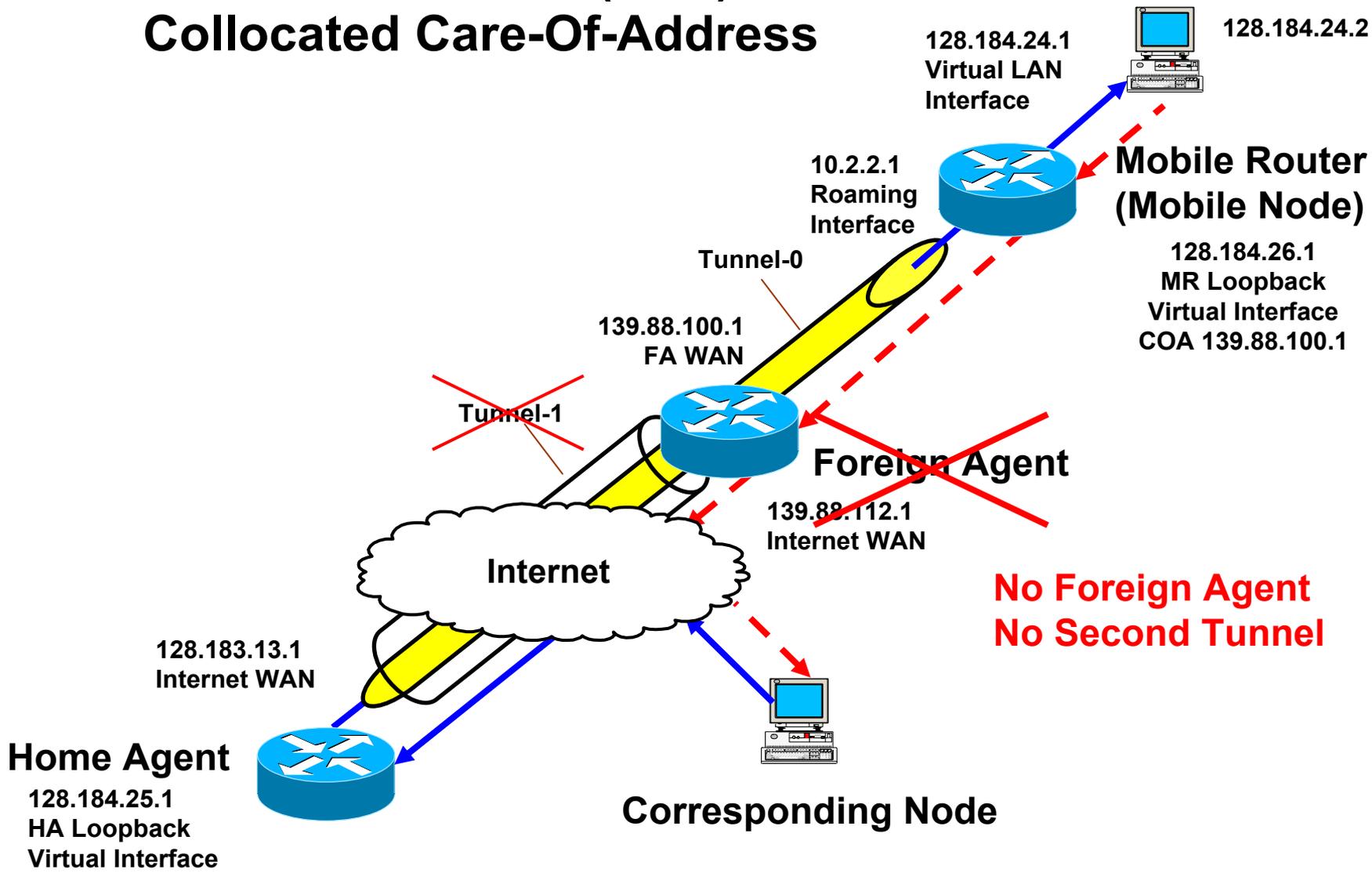


Corresponding Node

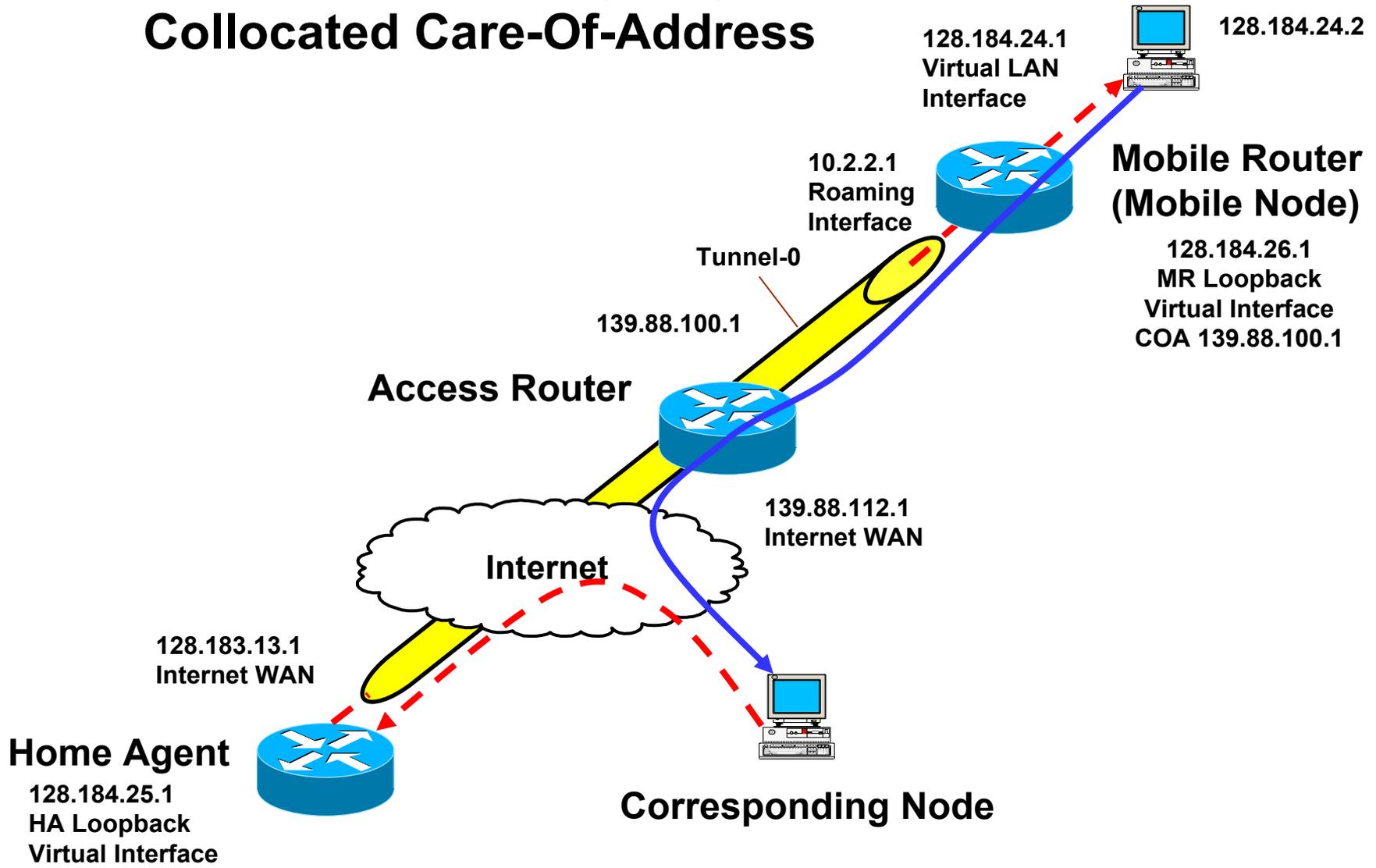
Mobile-Router (IPv4) Mobile Router (Reverse Tunneling)

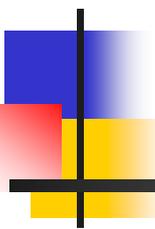


Mobile-Router (IPv4) Collocated Care-Of-Address



Mobile-Router (IPv4) Collocated Care-Of-Address

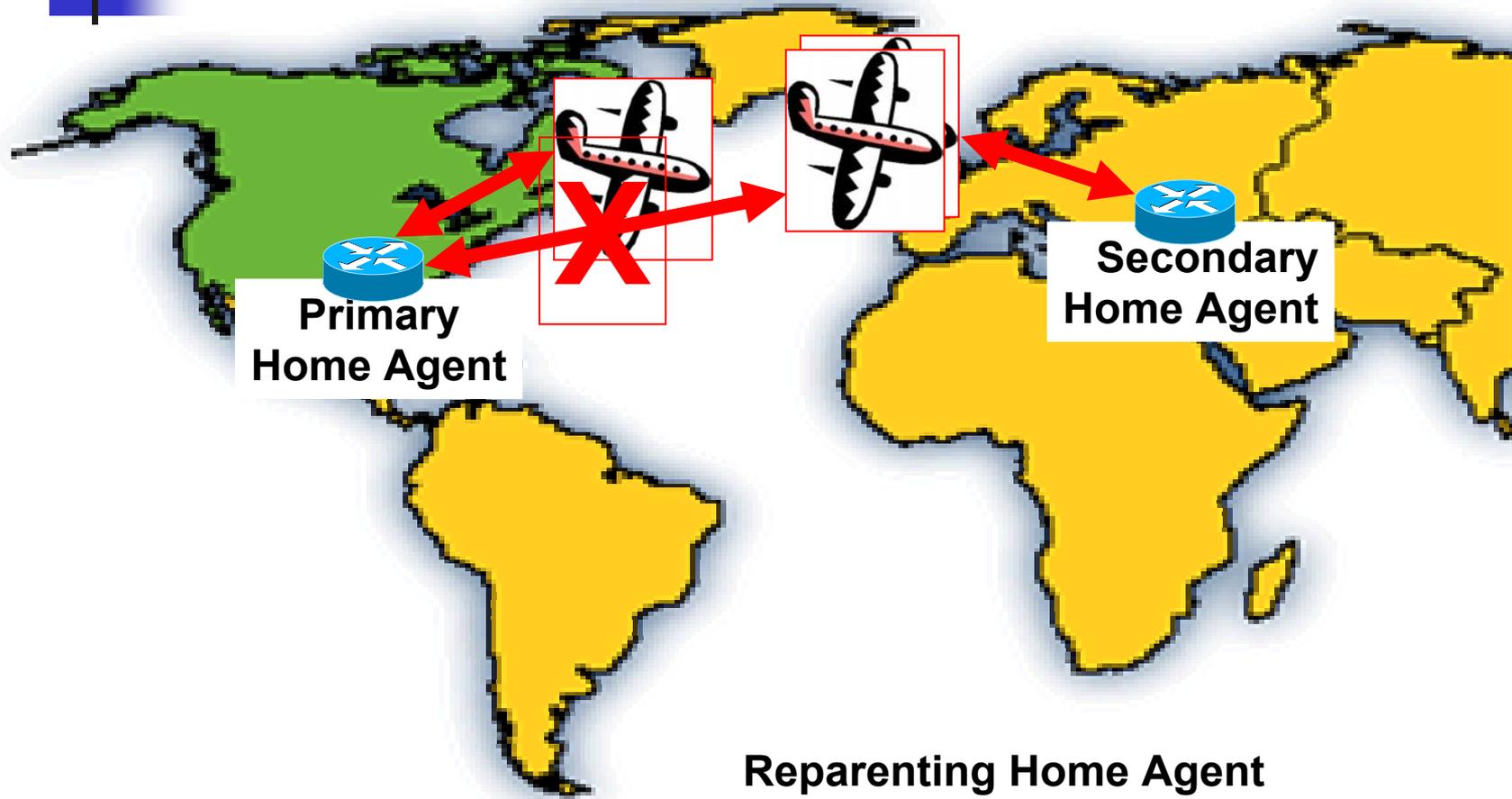




Mobile Networking Additional Features

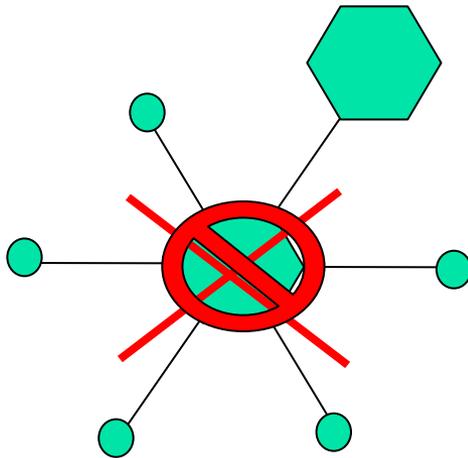
- Geographically Distributed Home Agents
- Asymmetrical Pathing

Secondary Home Agent (reparenting the HA)



**Reparenting Home Agent
Helps resolve triangular routing
Problem over long distances**

Emergency Backup (Hub / Spoke Network)

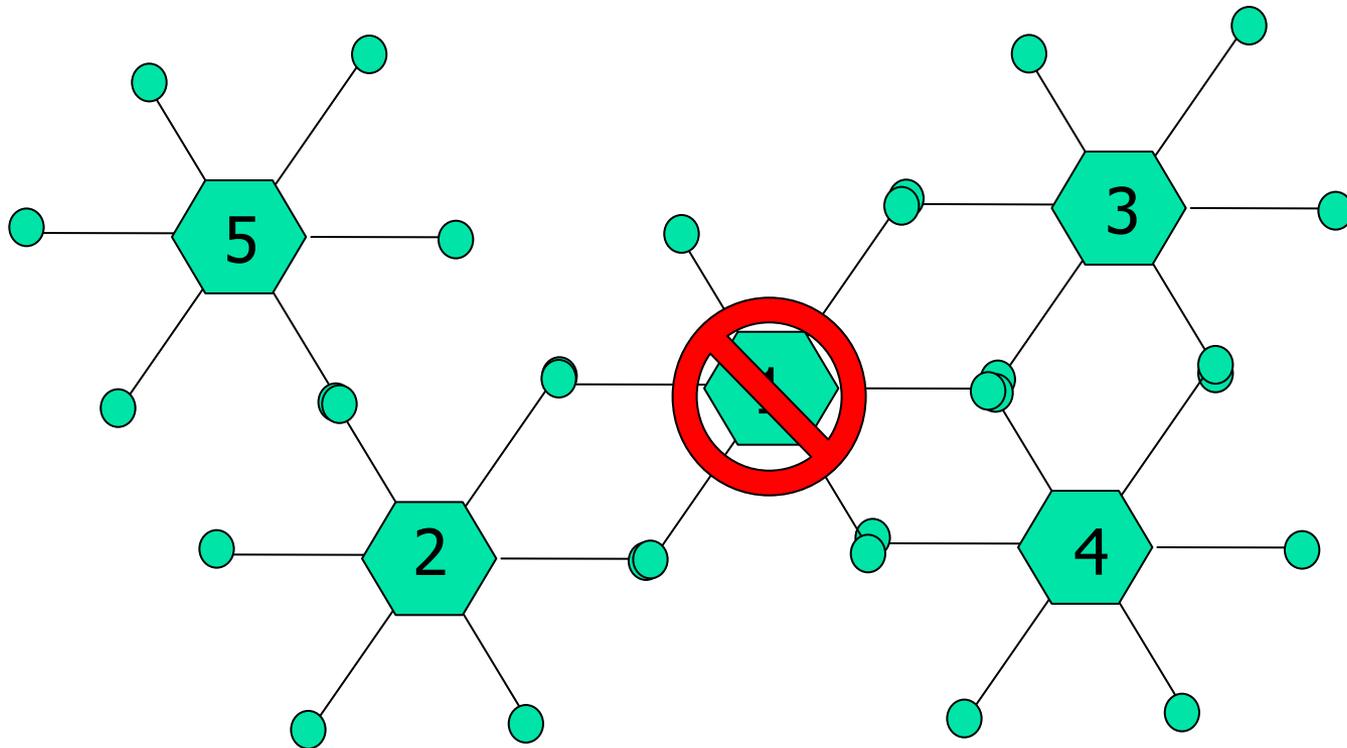


If primary control site becomes physically inaccessible but can be electronically connected, a secondary site can be established.

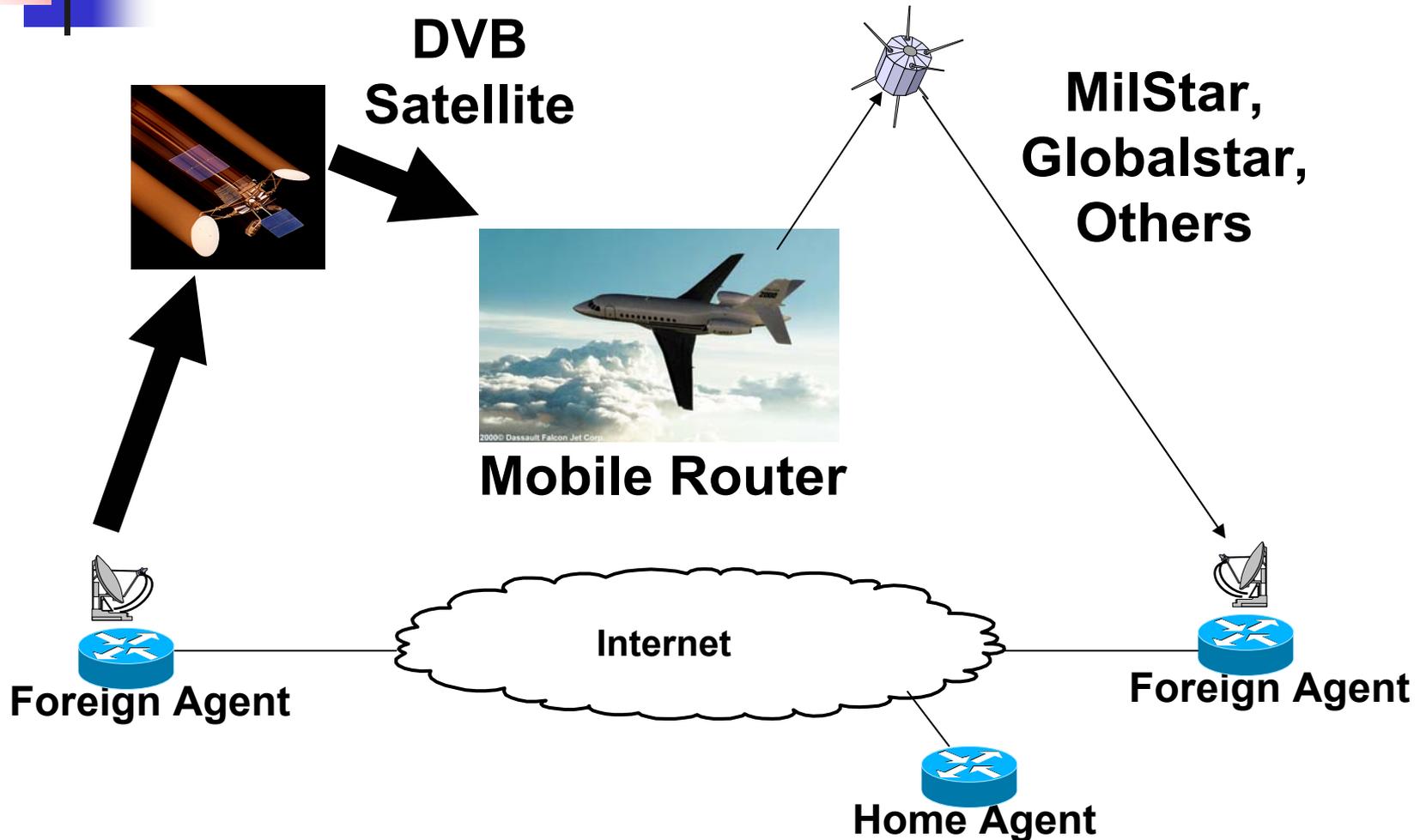
If primary control site is physically incapacitated, there is no backup capability.

Secondary Home Agent (Fully Meshed Network)

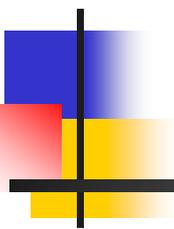
If primary control site is physically incapacitated, a second or third or fourth site take over automatically.



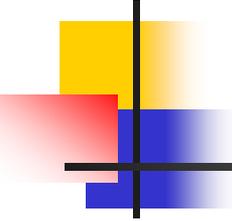
Asymmetrical Pathing



Securing Mobile and Wireless Networks



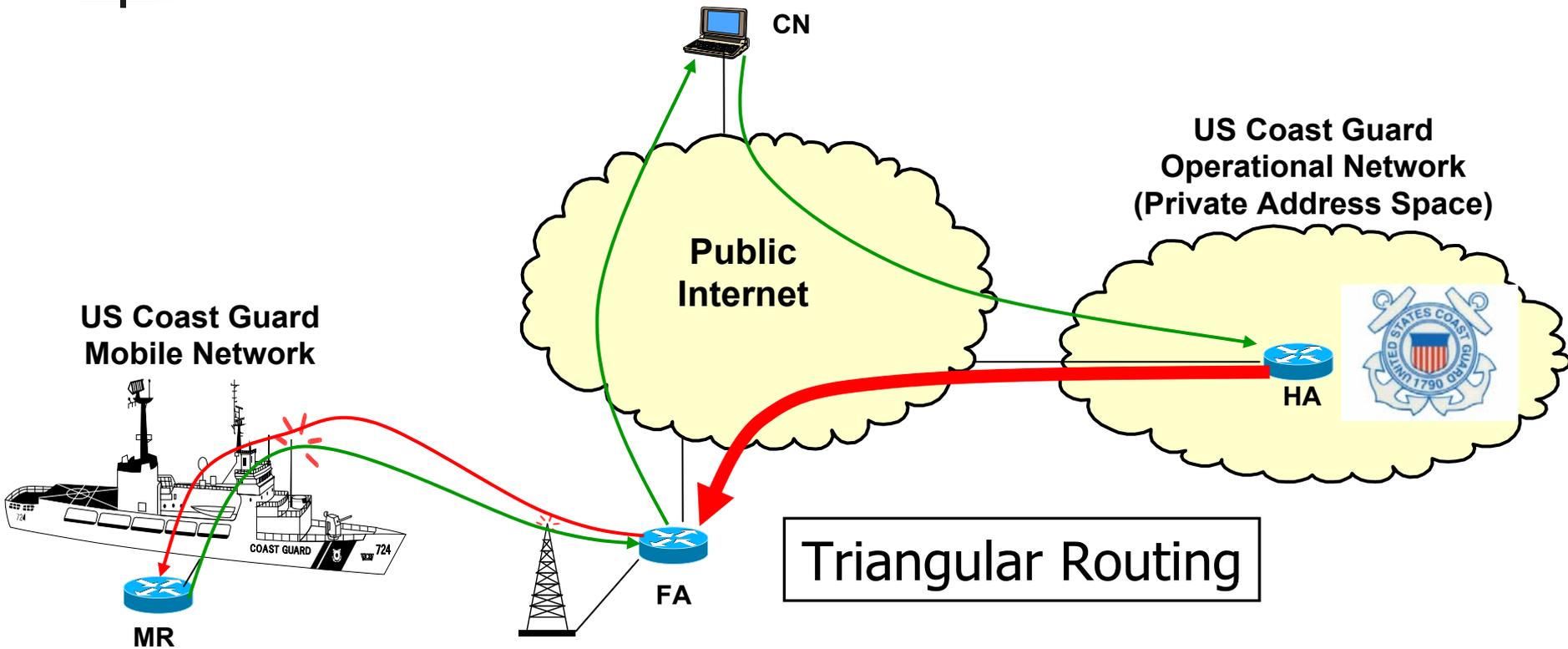
Some ways may be “better”
than others!

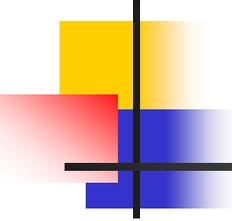


Constraints / Tools

- Policy
- Architecture
- Protocols

IPv4 Utopian Operation

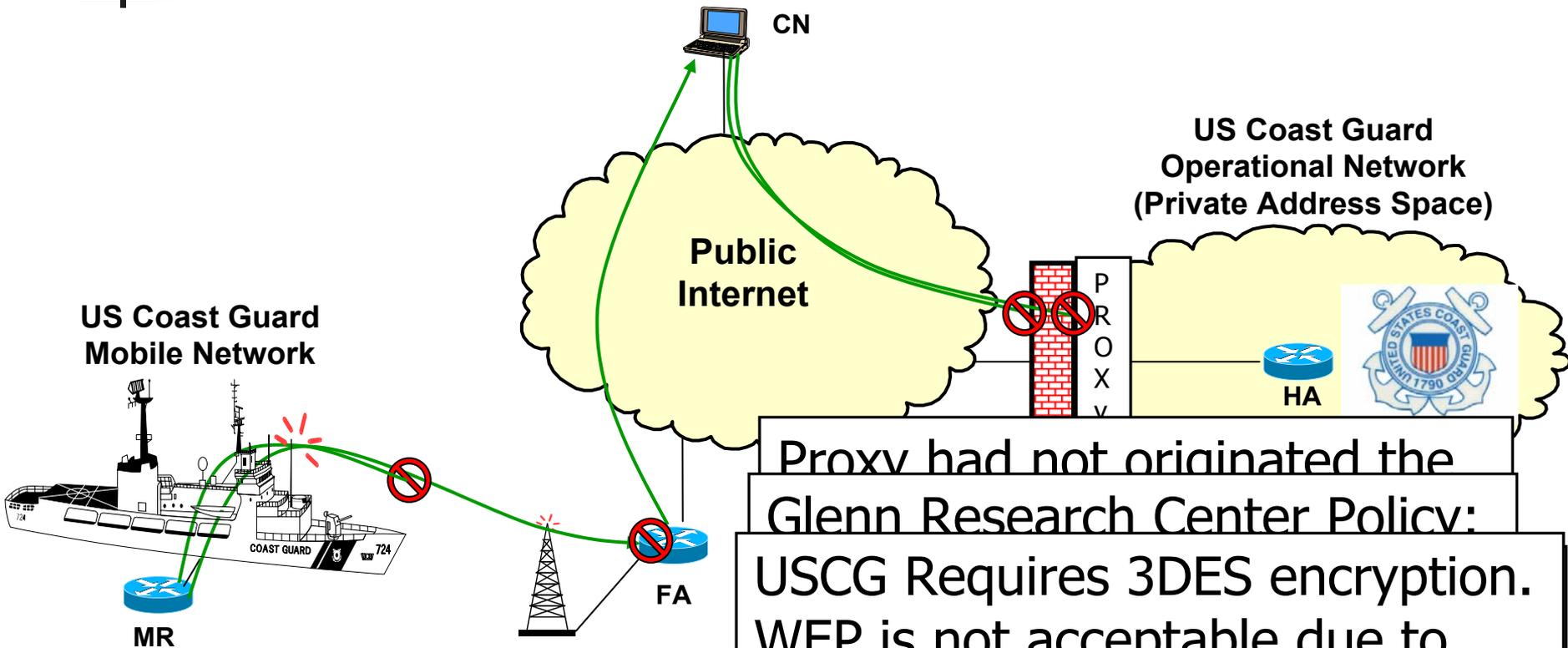




IPv4 Mobile-IP Addressing

- Source Address is obtained from
 - Foreign Agent
 - Static Collocated Care-of-Address (CCoA)
 - DHCP via Access Router (Dynamic CCoA)
- Private Address space is not routable via the Open Internet
- Topologically Incorrect Addresses should be blocked via Ingress or Egress filtering

IPv4 "Real World" Operation



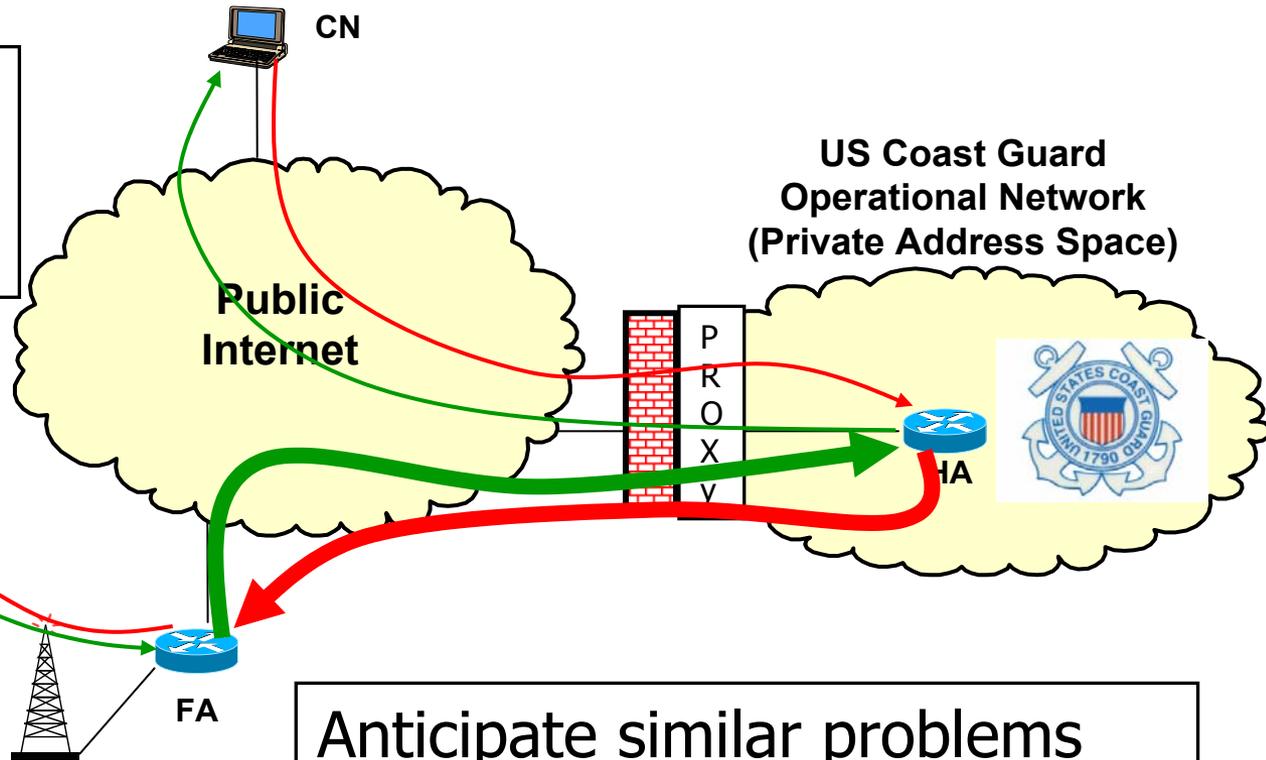
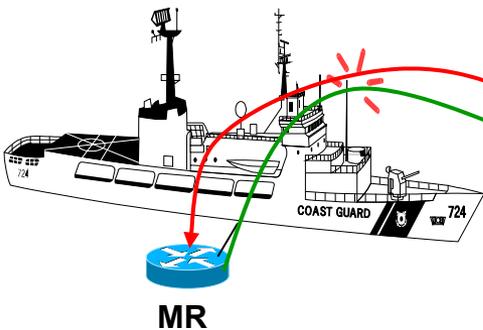
Proxy had not originated the
Glenn Research Center Policy:
USCG Requires 3DES encryption.
WEP is not acceptable due to
known deficiencies.

Corrects this problem.

Current Solution – Reverse Tunneling

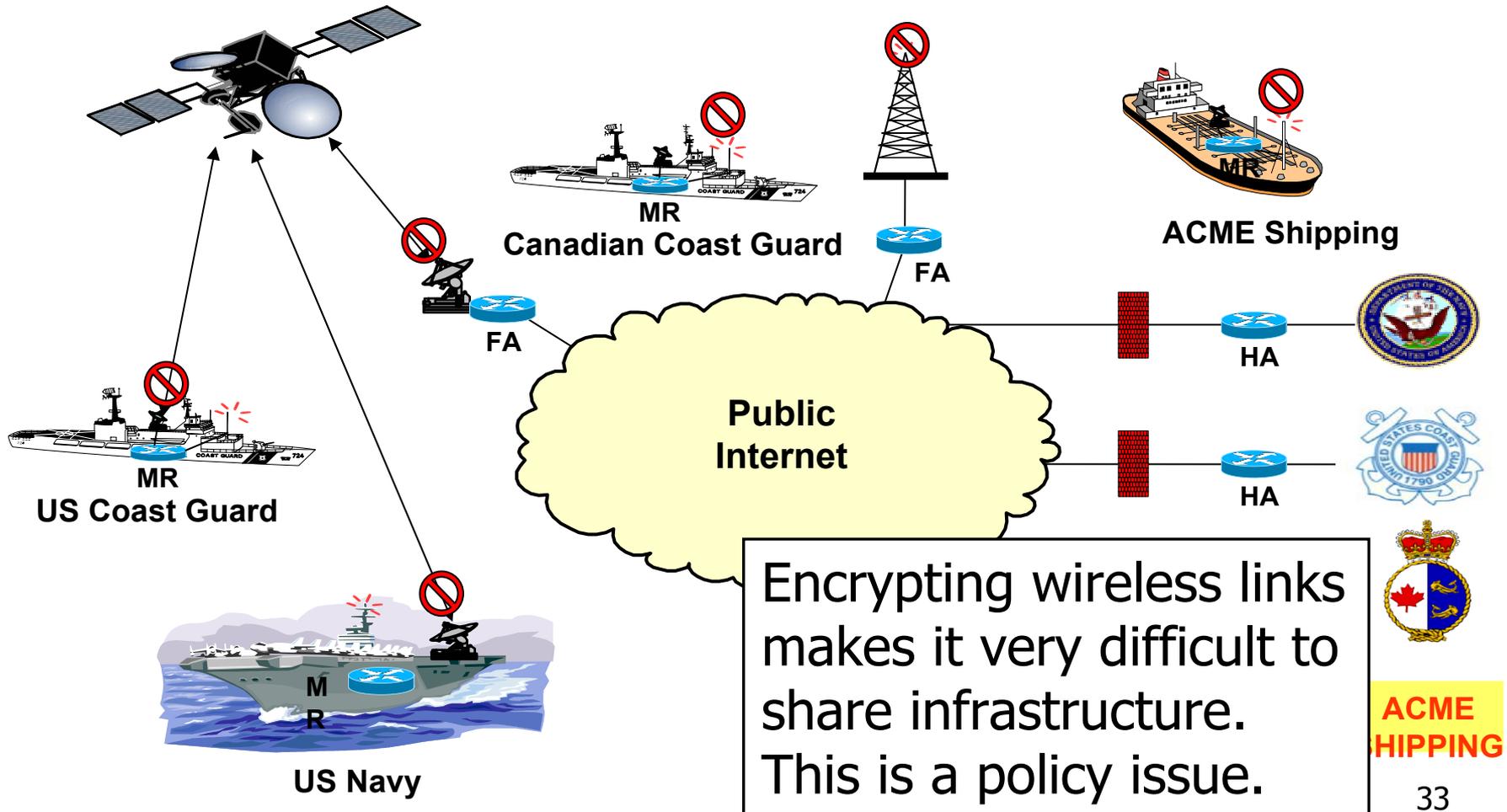
Adds Overhead and kills route optimization.

US Coast Guard Mobile Network



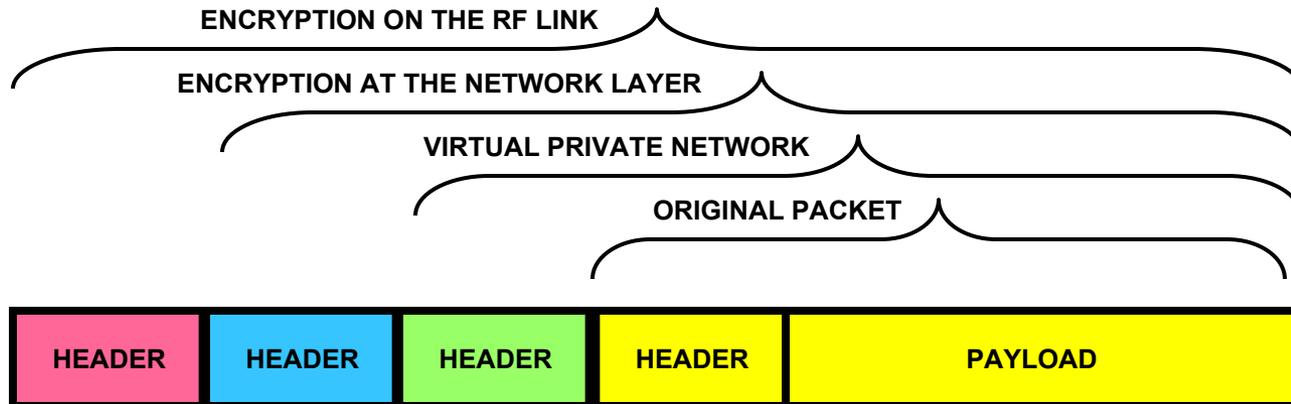
Anticipate similar problems for IPv6.

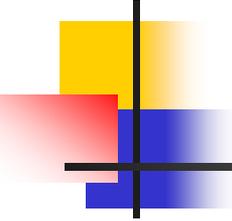
Shared Network Infrastructure



Security

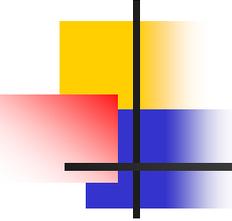
- Security ↑ Bandwidth Utilization ↓
- Security ↑ Performance ↓
- Tunnels Tunnels Tunnels and more Tunnels
- Performance ↓ Security ↓
⇒ User turns OFF Security to make system usable!
- Thus, we need more bandwidth to ensure security.





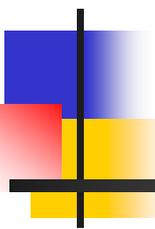
Additional and Future Security Solutions

- AAA
 - Routers (available today)
 - Wireless bridges and access points (available 2002)
- IPSec on router interface
- Encrypted radio links
 - IPSec, type1 or type2, and future improved WEP



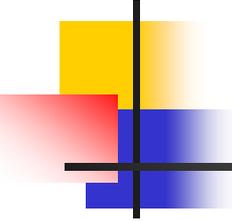
Conclusions

- Security Breaks Everything ☹
 - At least it sometimes feels like that.
- Need to change policy where appropriate.
- Need to develop good architectures that consider how the wireless systems and protocols operate.
- Possible solutions that should be investigated:
 - Dynamic, Protocol aware firewalls and proxies.
 - Possibly incorporated with Authentication and Authorization.



USCGC Neah Bay Project

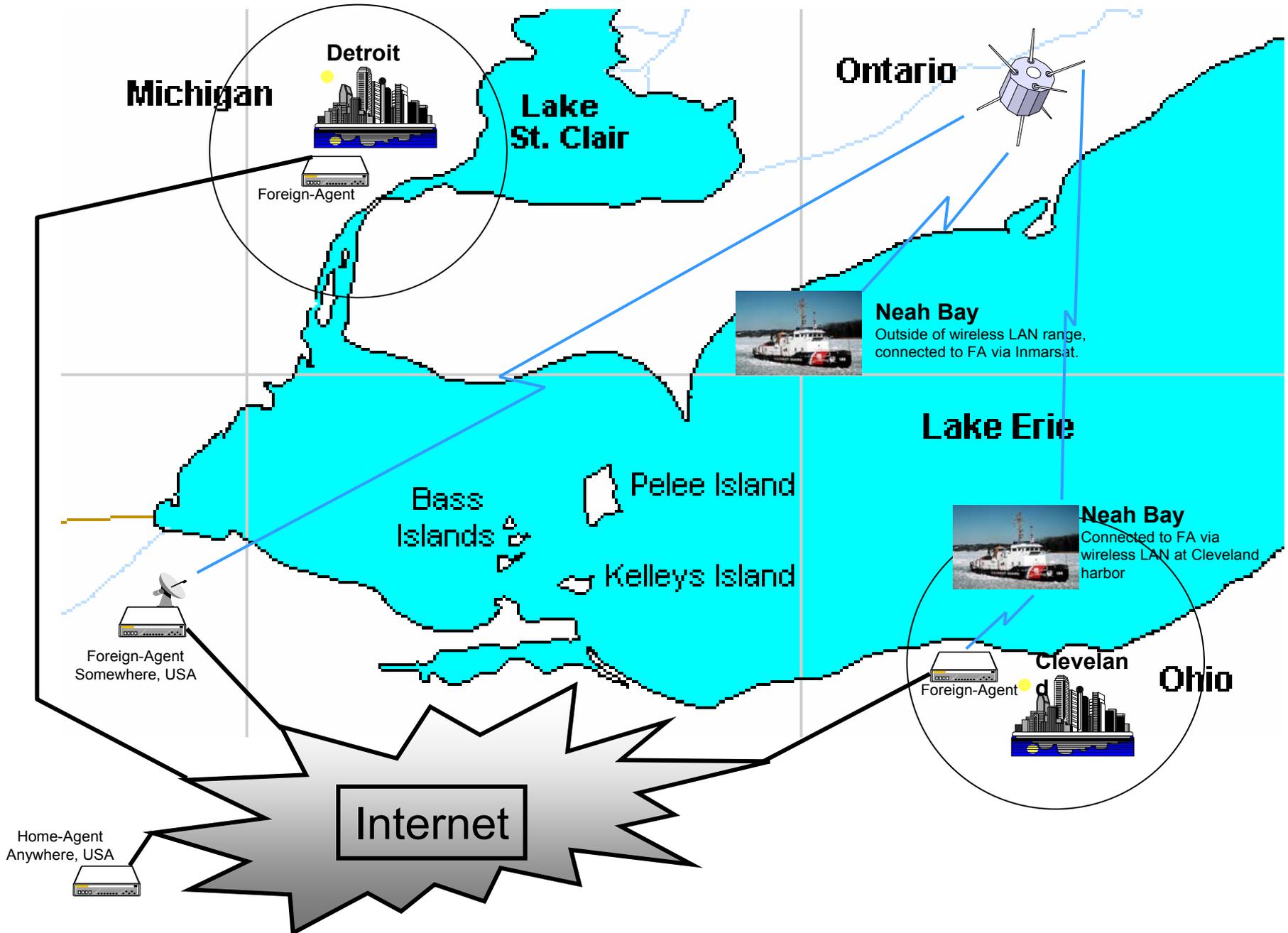
Mobile Networking in an
Operational Network

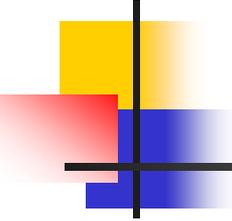


Mobile Network Design Goals

- Secure
- Scalable
- Manageable
- Ability to sharing network infrastructure
- Robust

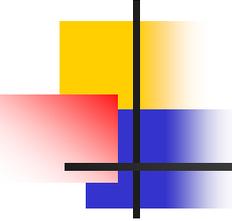
Neah Bay / Mobile Router Project





Why NASA/USCG/Industry

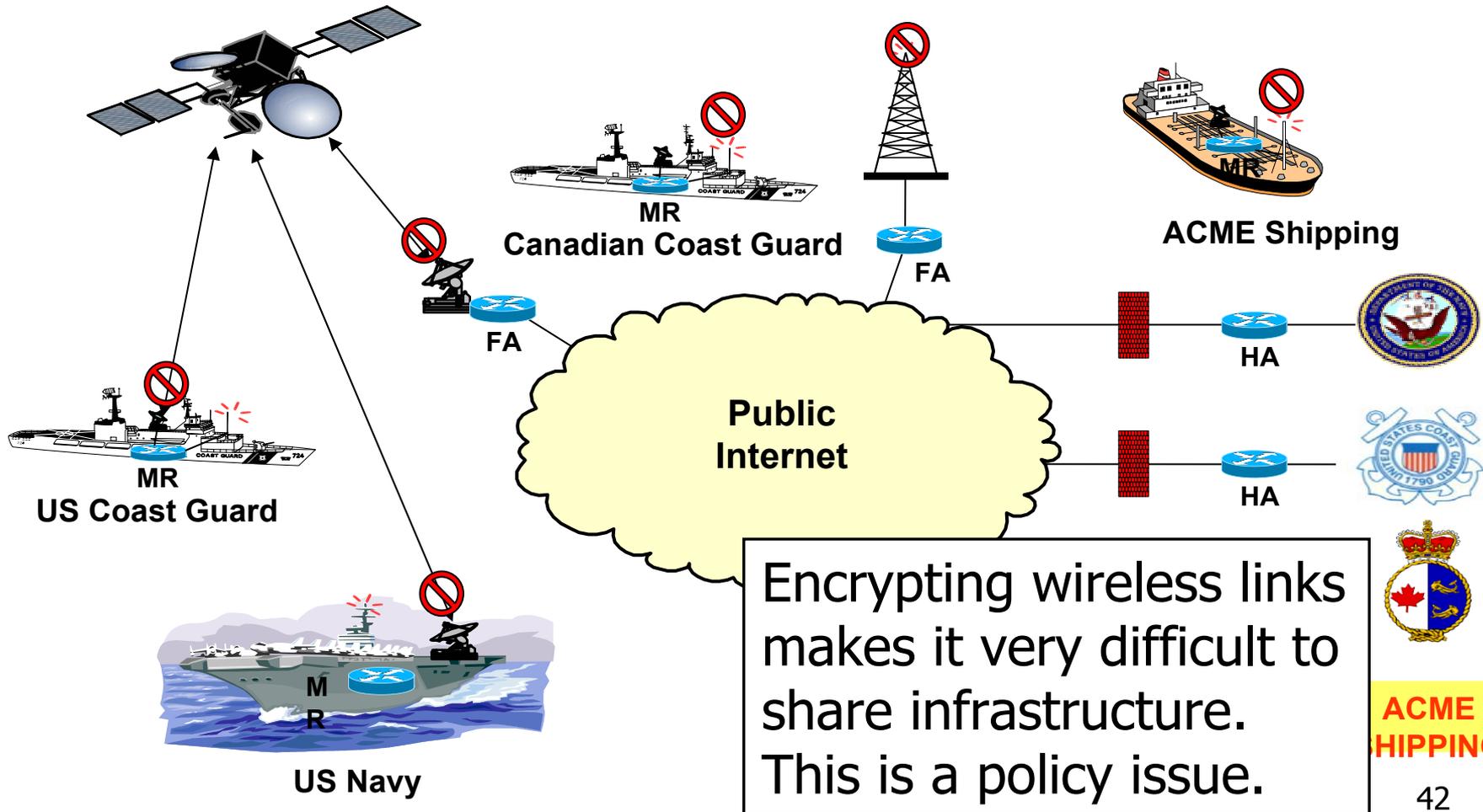
- Real world deployment issues can only be addressed in an operational network.
- USCG has immediate needs, therefore willingness to work the problem.
- USCG has military network requirements.
- USCG is large enough network to force full us to investigate full scale deployment issues
- USCG is small enough to work with.
- NASA has same network issues regarding mobility, security, network management and scalability.

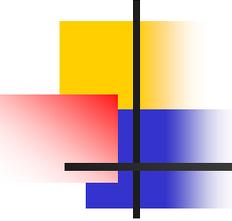


Mobile-Router Advantages

- Share wireless and network resources with other organizations
 - \$\$\$ savings
- Set and forget
 - No onsite expertise required
 - However, you still have to engineer the network
- Continuous Connectivity
 - (May or may not be important to your organization)
- Robust
 - Secondary Home Agent (Reparenting of HA)

Shared Network Infrastructure





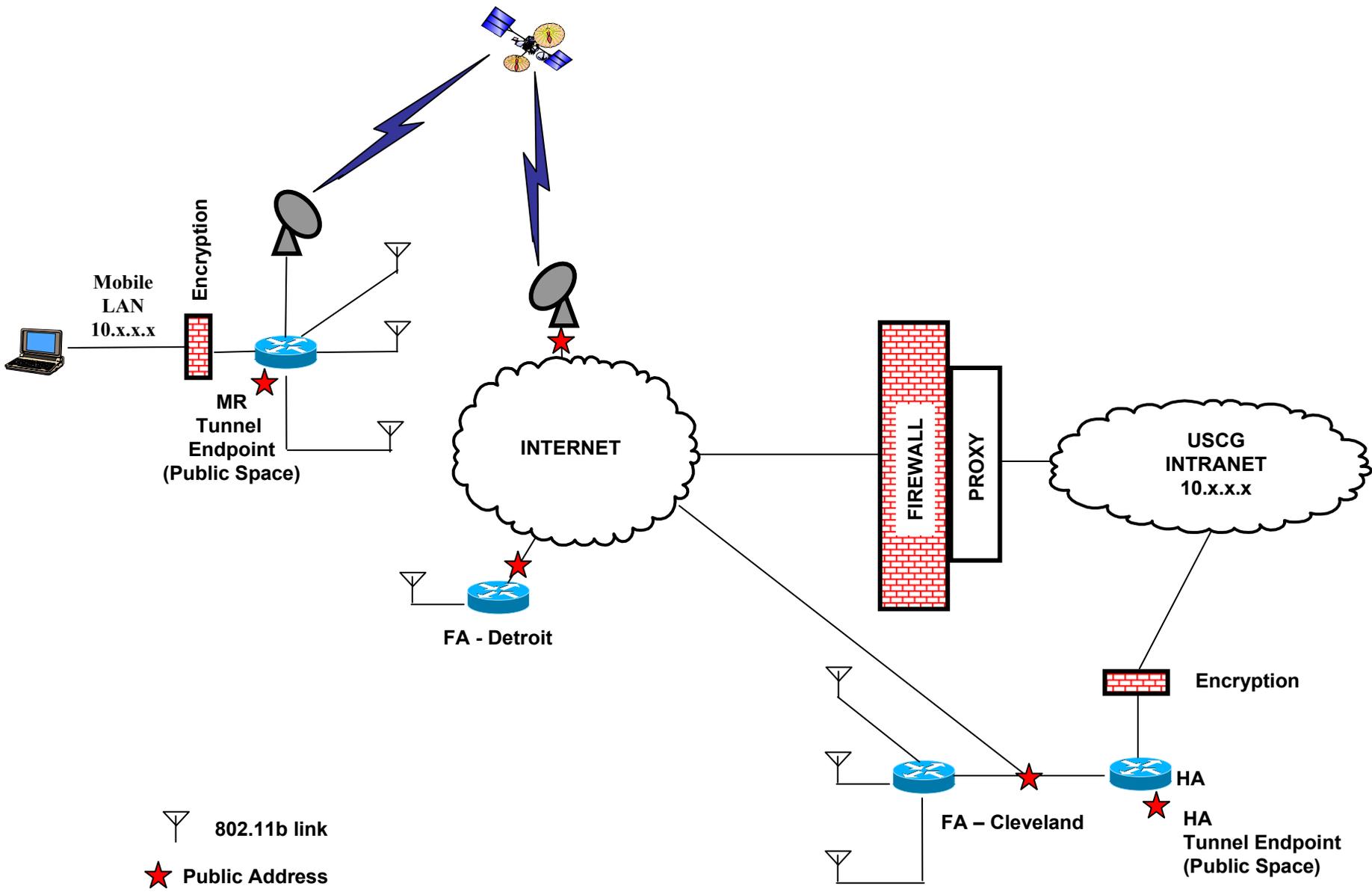
We Are Running with Reverse Tunneling

- Pros

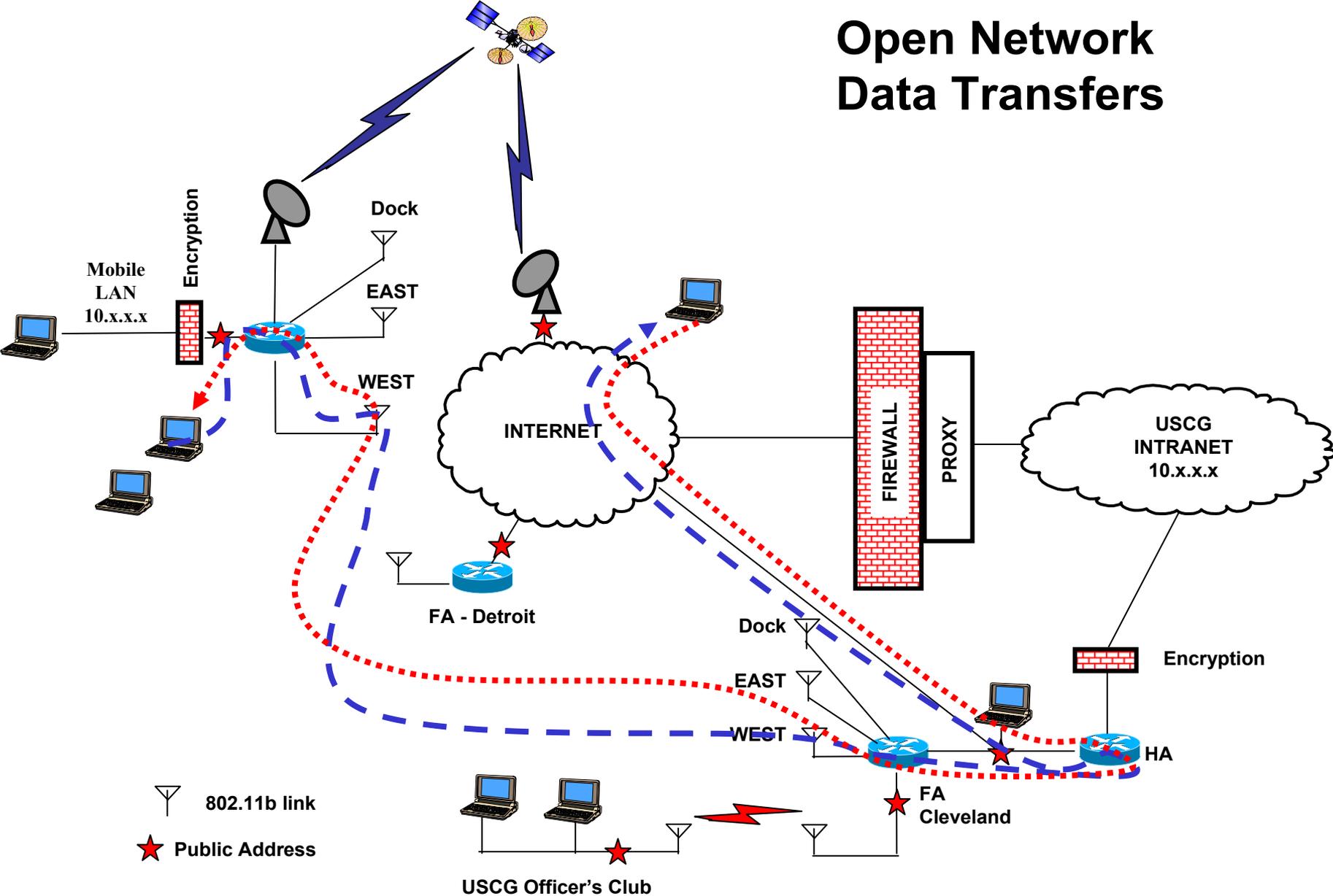
- Ensures topologically correct addresses on foreign networks
- Required as requests from MR LAN hosts must pass through Proxy inside main firewall
- Greatly simplifies setup and management of security associations in encryptors
- Greatly simplifies multicast – HA makes for an excellent rendezvous point.

- Cons

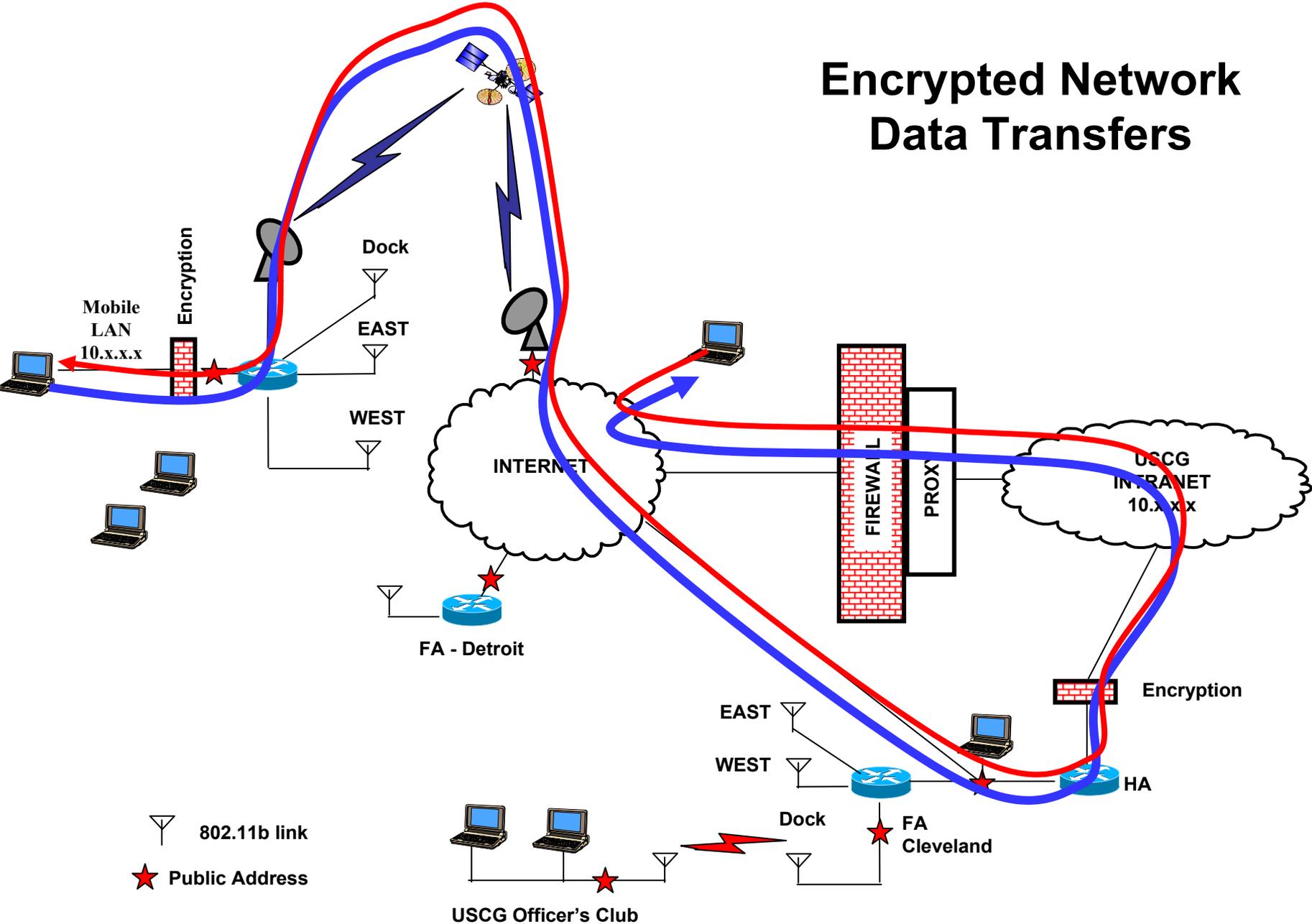
- Uses additional bandwidth
- Destroys route optimization



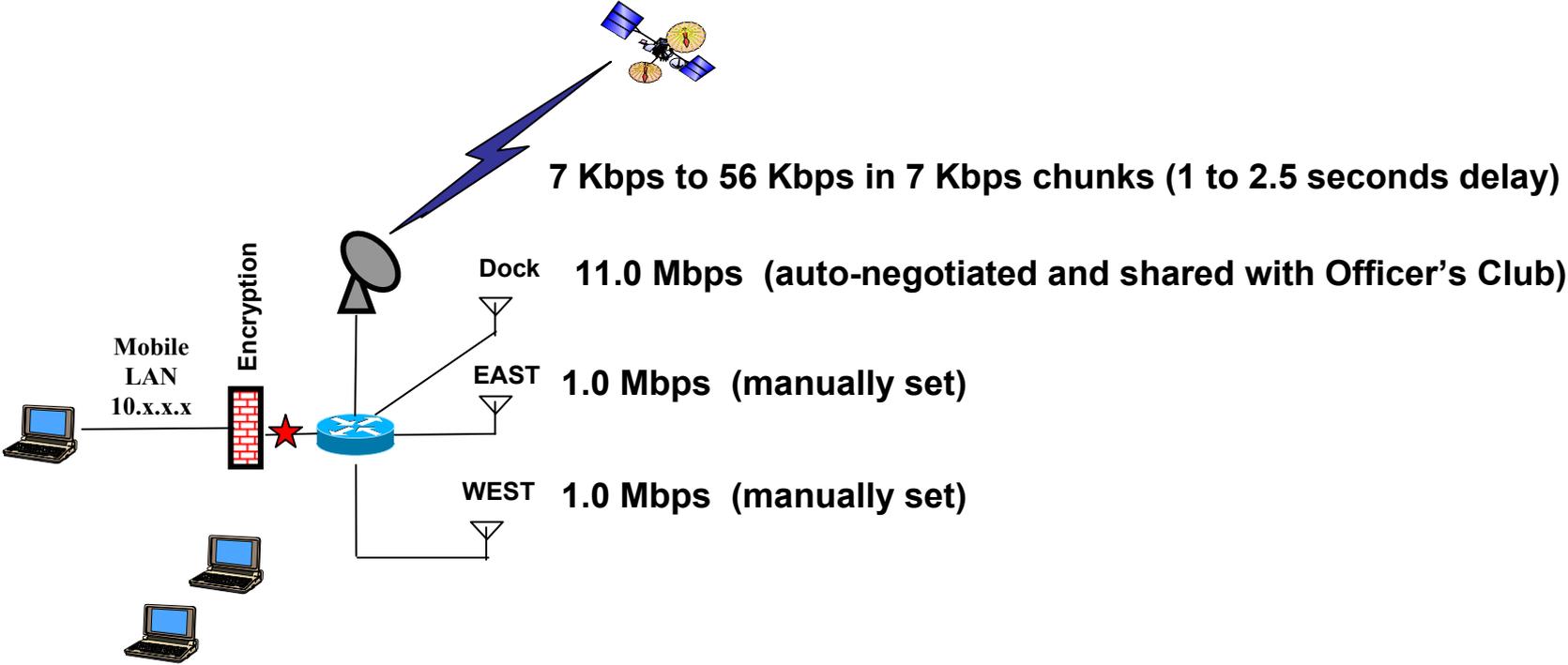
Open Network Data Transfers

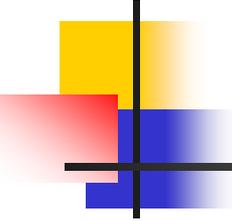


Encrypted Network Data Transfers



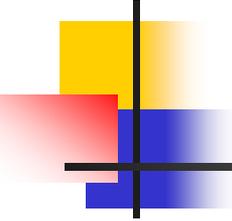
RF Bandwidth





Globalstar/Sea Tel MCM-8

- Initial market addresses maritime and pleasure boaters.
- Client / Server architecture
 - Current implementation requires call to be initiated by client (ship).
 - Multiplexes eight channels to obtain 56 kbps total data throughput.
 - Full bandwidth-on-demand.
- Requires use of Collocated Care-of-Address



RF Technologies

- Globalstar (L-Band)
 - Globalstar MCM-8 (Client/Server)
 - Seatel MCM-3 (Client/Server)
 - Qualcomm MDSS-16
- Boeing Connex (Ku-Band)
- INMARSAT Swift 64
- General Packet Radio Service (GPRS)
- 802.11
- VHF

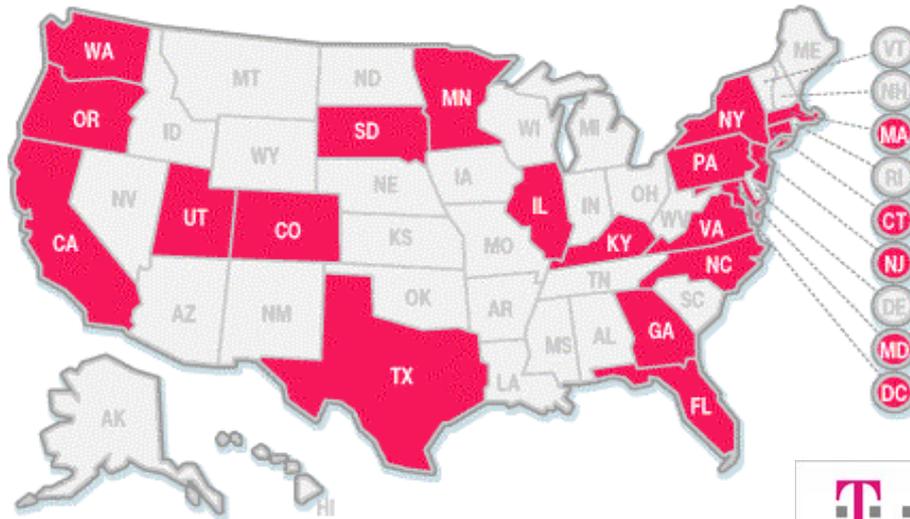
..T..Mobile

Get more from the internet

Hot Spot Partners – 2500+ sites (4/1/03)



..T..Mobile



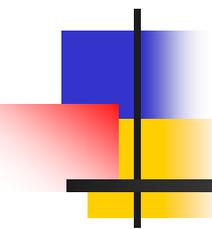
T..Mobile
HotSpot

Wireless broadband Internet access for your laptop or PDA.



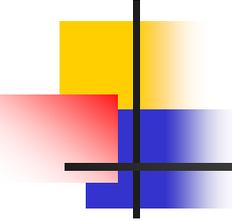
American Airlines





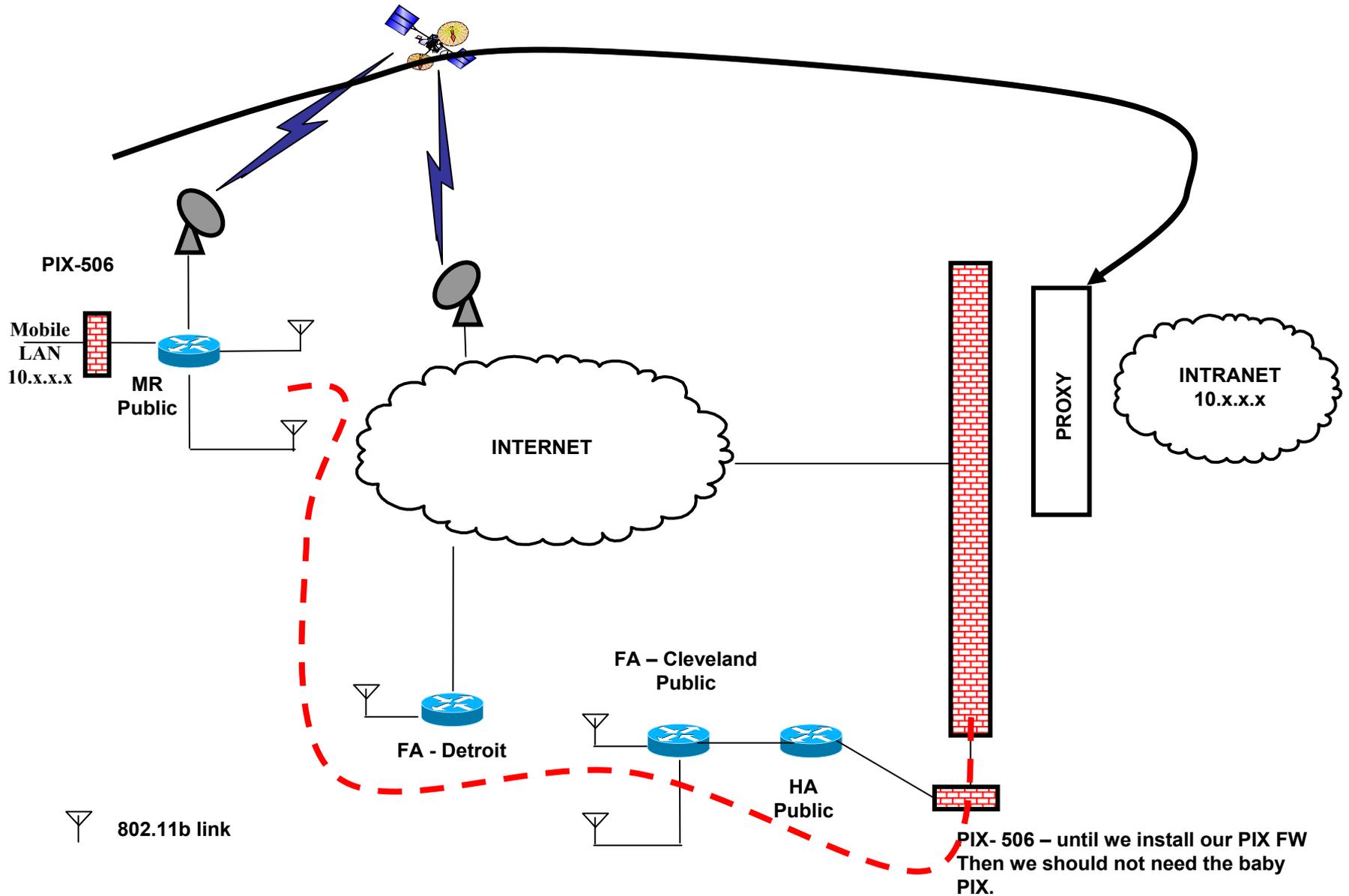
What's Next

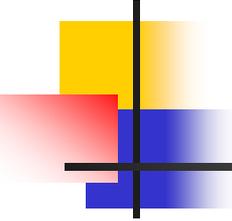
The End Game



Mobile Networks

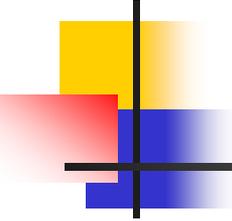
- Share Network Infrastructure
 - USCG, Canadian Coast Guard, Commercial Shipping, Pleasure Boaters
 - Open Radio Access / Restricted Network Access
 - Authentication, Authorization and Accounting
- Architecture
 - Limited, experimental deployment onboard Neah Bay
 - Move RIPv2 routing from Fed. Bldg to Neah Bay
 - Move to full scale deployment
 - Requires full commitment





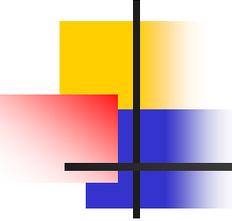
HA Outside Main Firewall

- Firewall between MR interfaces and public Internet as well as the HA and Private Intranet.
- Reverse tunneling required as requests from MR LAN hosts must pass through Proxy inside main firewall.



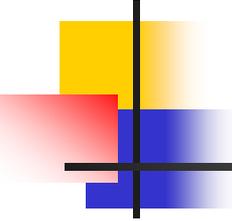
Areas that need to be addressed

- Home Agent Placement
 - Inside or Outside the Firewall
- AAA Issues
 - Open Radio Access / Restricted Network Access
 - Secure Key Management
- IPv6 Mobile Networking Development
 - Work with industry and IETF
- Develop radio link technology
 - Enable better connectivity throughout the world for both military and aeronautical communications (voice, video and data).



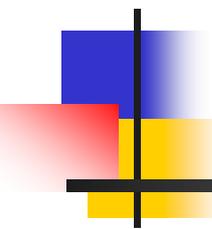
Relevant NASA Aeronautics Programs

- Advanced Air Transportation Technology (AATT)
- Weather Information Communication (WINCOMM)
- Small Aircraft Transportation System (SATS)

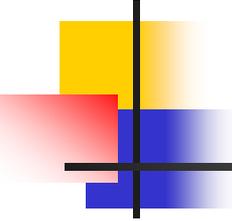


Aeronautic Networking Issues

- Move to IPv6
 - IPv6 Mobile Networking
- Authentication, Authorization and Accounting
- Bandwidth, Bandwidth, Bandwidth
- Media Access
- Policy
 - Sending of Operations over Entertainment Channels

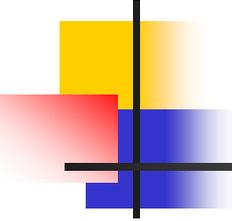


IPv6 Mobile-IP

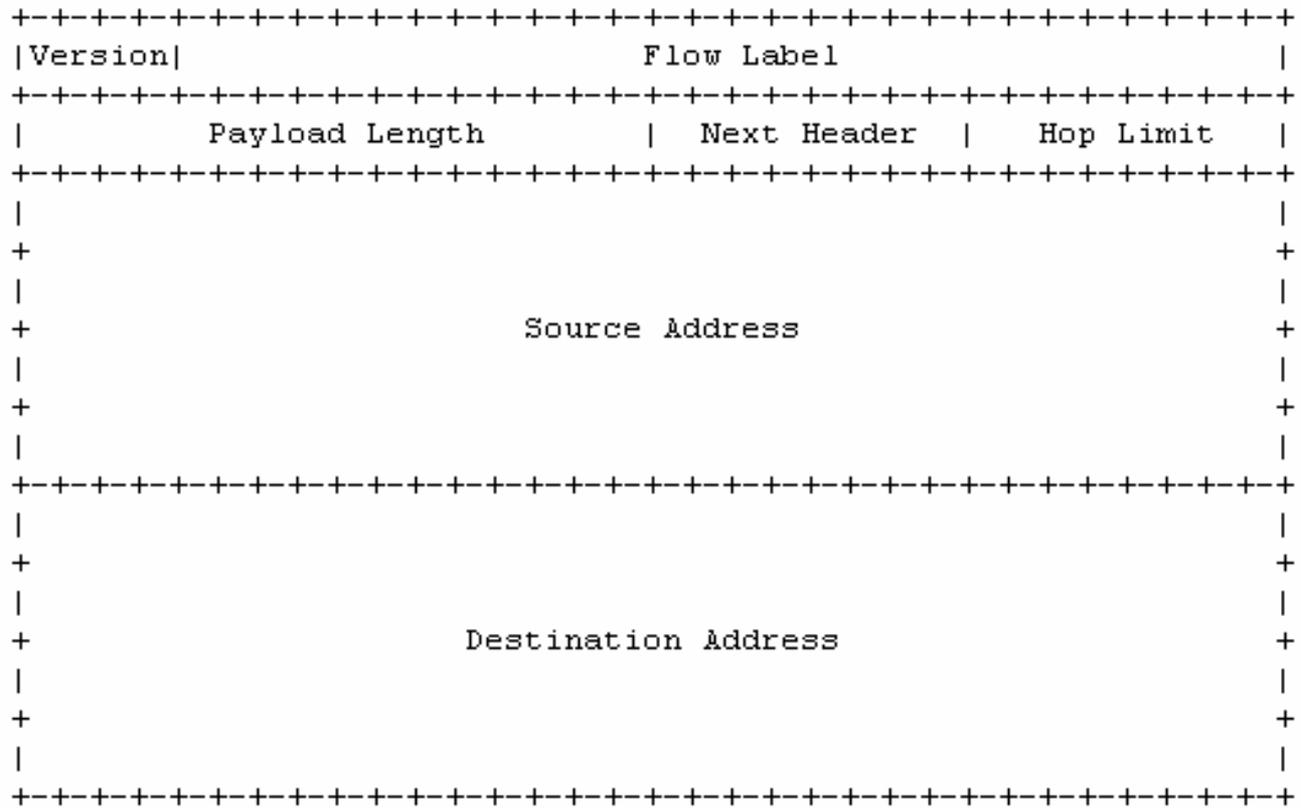


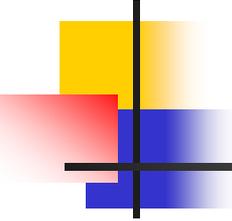
Mobile-IPv6

- No "foreign agent" routers
- Route optimization is a fundamental part of the protocol
- Mobile IPv6 route optimization can operate securely even without pre-arranged security associations
- Route optimization coexists efficiently with routers that perform "ingress filtering"
- The movement detection mechanism in Mobile IPv6 provides bidirectional confirmation of a mobile node's ability to communicate with its default router in its current location
- Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation



IPv6





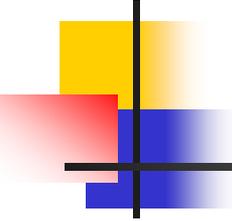
Options Examples

Fragmentation Header

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Next Header | Reserved   | Fragment Offset | Res|M|
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Identification                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

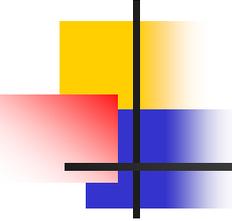
Authentication Header

```
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Next Header | Auth Data Len | Reserved           |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                     Security Association ID                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                                                                                                                 |
|                                                                                                                                 |
|                                     Authentication Data                                     |
|                                                                                                                                 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

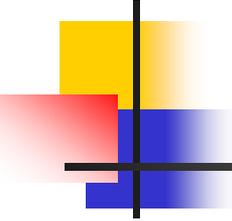
Mobility Message Types

- Binding Refresh Request Message
- Home Test Init Message
- Care-of Test Init Message
- Home Test Message
- Care-of Test Message
- Binding Update Message
- Binding Acknowledgement Message
- Binding Error Message



Mobility Options

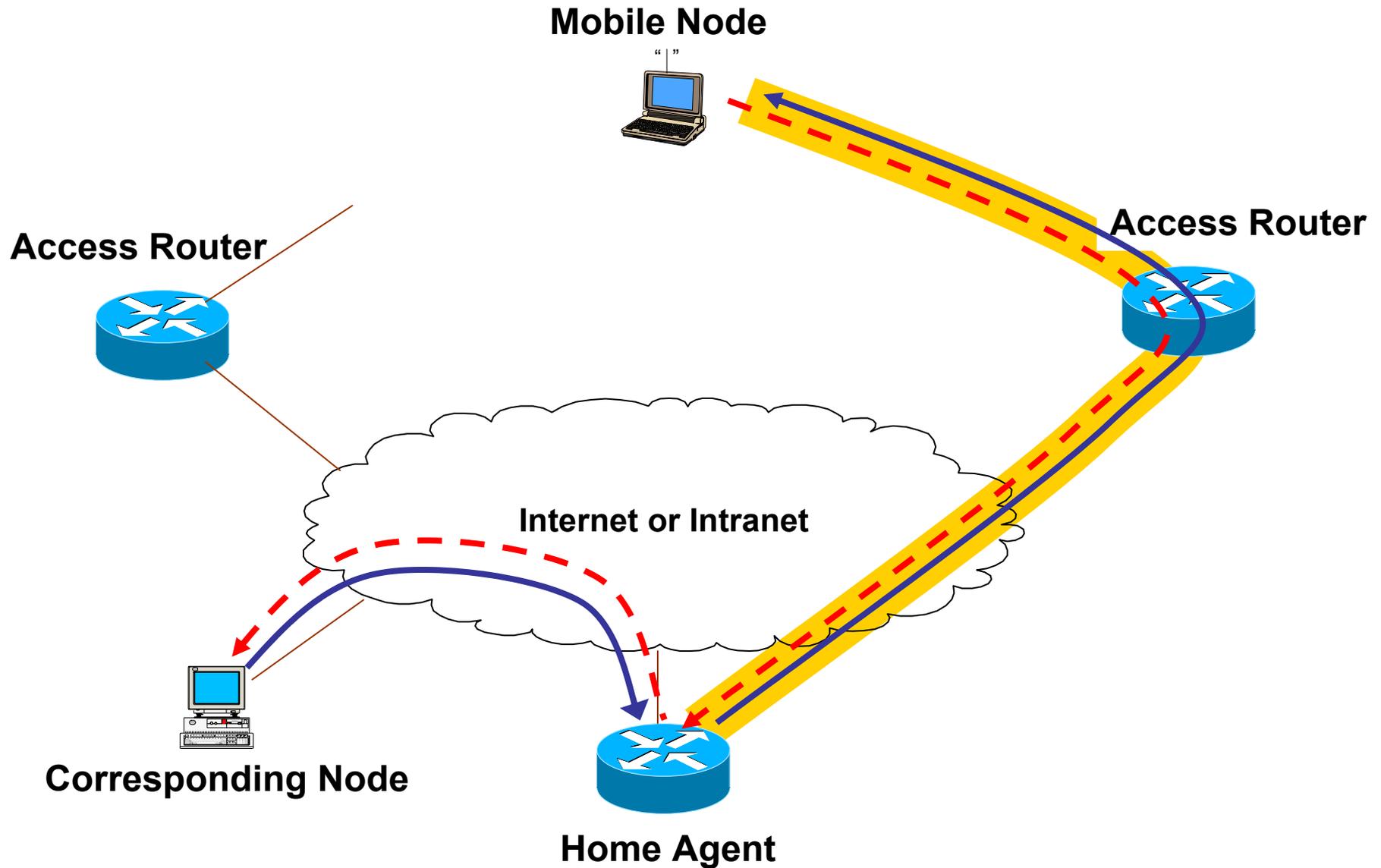
- Pad1
- PadN
- Binding Refresh Advice
- Alternate Care-of Address
- Nonce Indices
- Binding Authorization Data
- Home Address Option
- Type 2 Routing Header



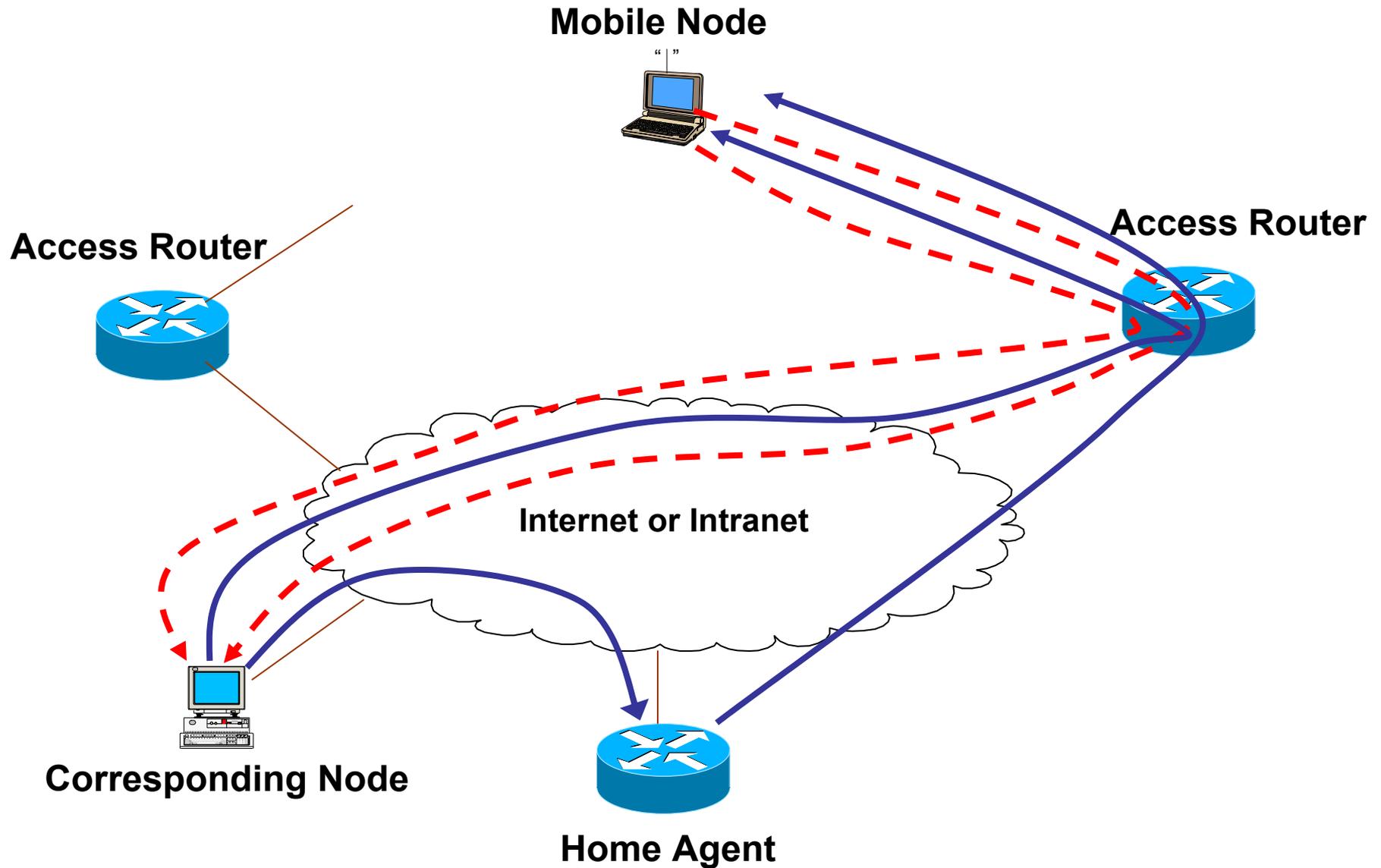
Mobile-IPv6

- Modes for communications between the mobile node and a correspondent node
 - Bidirectional tunneling
 - Does not require Mobile IPv6 support from the correspondent node
 - “Route Optimization”
 - Requires the mobile node to register its current binding at the correspondent node.
 - Packets from the correspondent node can be routed directly to the care-of address of the mobile node

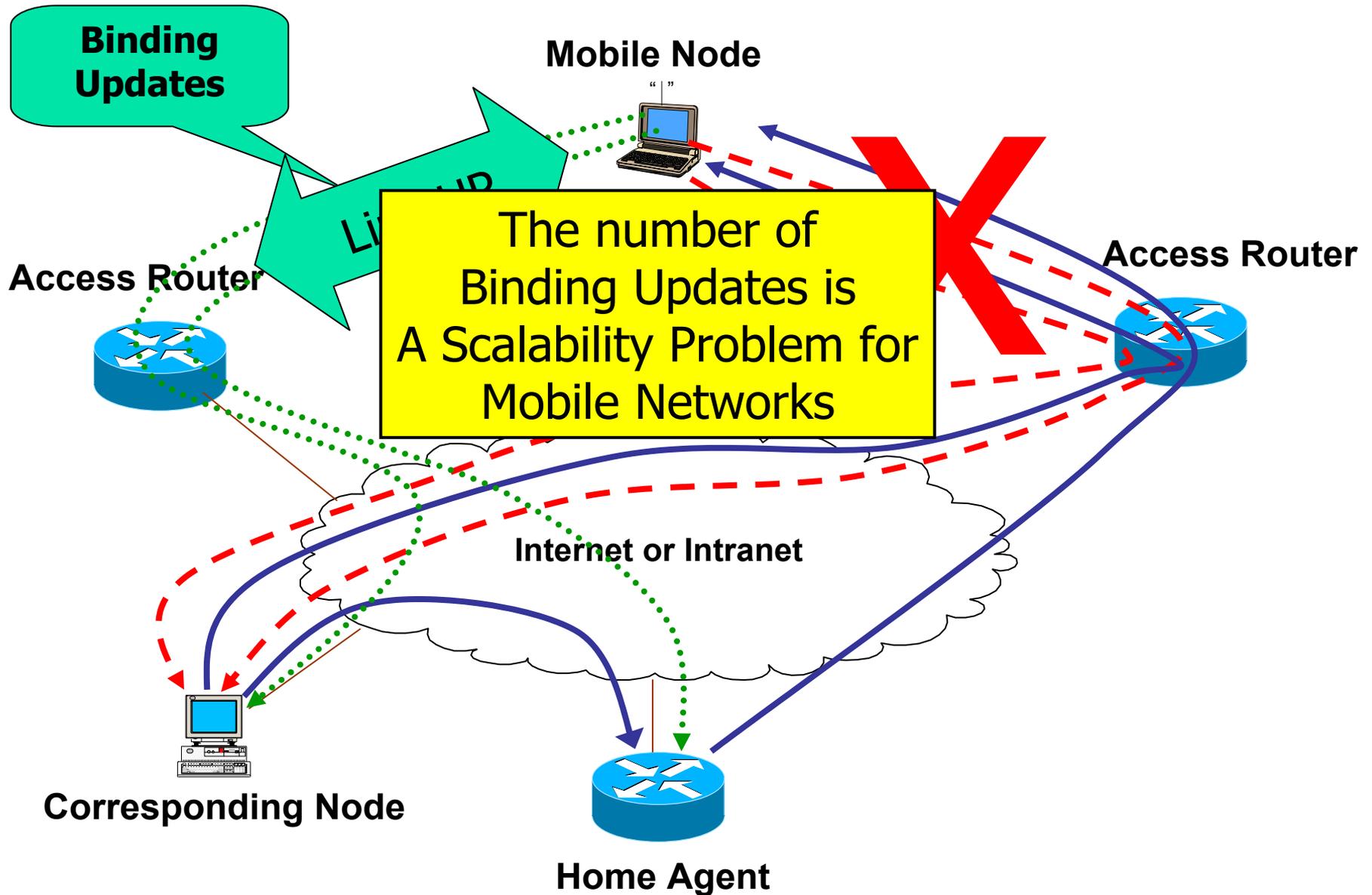
Mobile-IPv6 using Reverse Tunneling

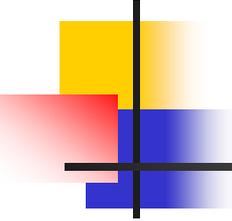


Mobile-IPv6 using Route Optimization



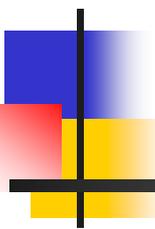
Mobile-IPv6 Binding Updates





Mobile IPv6 Security

- Binding Updates use IPsec extension headers, or by the use of the Binding Authorization Data option
- Prefix discovery is protected through the use of IPsec extension headers
- Mechanisms related to transporting payload packets - such as the Home Address destination option and type 2 routing header have been specified in a manner which restricts their use in attacks

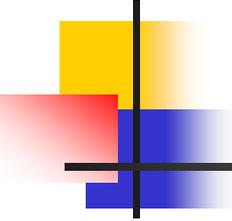
The logo graphic consists of a vertical black line intersecting a horizontal black line. To the left of the intersection, there are three overlapping squares: a blue one on top, a red one on the left, and a yellow one on the bottom. The word "NEMO" is written in a blue, sans-serif font to the right of the vertical line.

NEMO

NEtworks in Motion

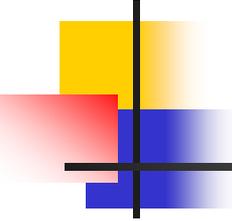
<http://www.ietf.org/html.charters/nemo-charter.html>

<http://www.nal.motlabs.com/nemo/>



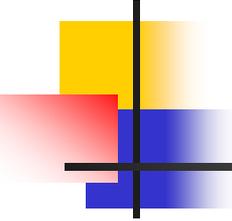
Networks In Motion (NEMO)

- Working Group established in IETF in December 2002
- Concerned with managing the mobility of an entire network, which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology.



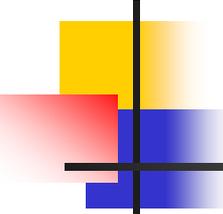
Goals

- Standardizing some basic support mechanisms based on the bidirectional tunneling approach
- Study the possible approaches and issues with providing more optimal routing



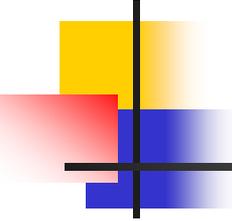
Milestones

- MAR 03 Submit terminology and requirements documents (for Basic support).
- MAY 03 Submit Threat analysis and security requirements for NEMO.
- AUG 03 Submit solution for basic support
- NOV 03 Submit MIB for Basic support
- MAR 04 Submit the analysis of the solution space for route optimization
- JUN 04 Shut down or recharter the WG to solve the route optimization



draft-ietf-nemo-requirements-00.txt

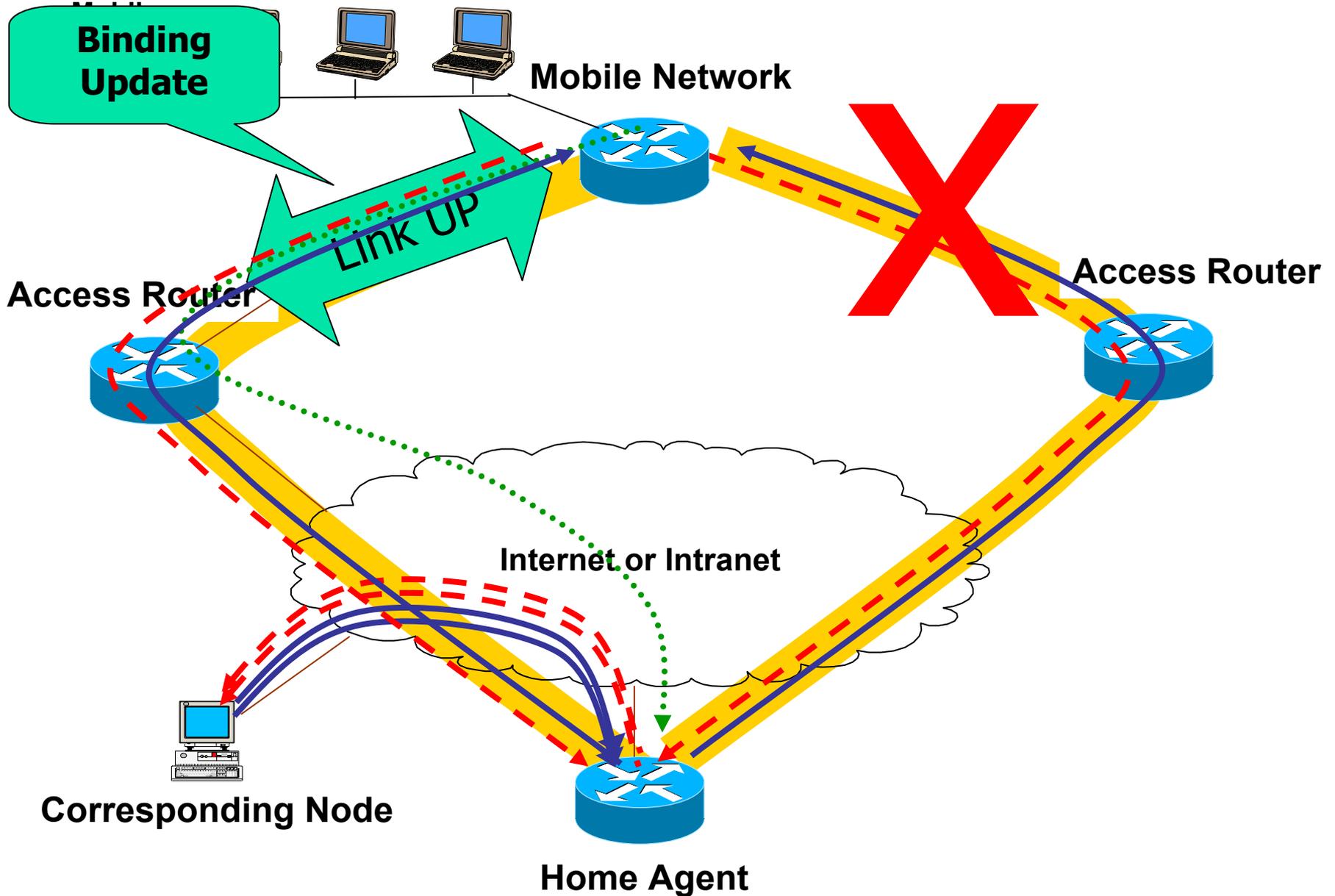
- The basic solution MUST use bi-directional tunnels
- MNNs MUST be reachable at a permanent IP address and name.
- MUST maintain continuous sessions (both unicast and multicast) between MNNs and arbitrary CNs after IP handover of (one of) the MR.
- The solution MUST not require modifications to any node other than MRs and HAs.
- The solution MUST support fixed nodes, mobile hosts and mobile routers in the mobile network.
- The solution MUST not prevent the proper operation of Mobile IPv6 (i.e. the solution MUST support MIPv6-enabled MNNs and MUST also allow MNNs to receive and process Binding Updates from arbitrary Mobile Nodes.)
- The solution MUST treat all the potential configurations the same way (whatever the number of subnets, MNNs, nested levels of MRs, egress interfaces, ...)
- The solution MUST support mobile networks attaching to other mobile networks (nested mobile networks).

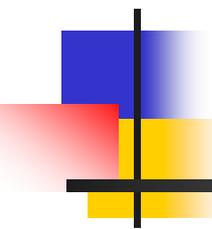


Not Yet required

- Route Optimization
- Load Sharing
- Policy Based Routing
- Multiple Home Agents from different Service Providers
 - Security Issues
 - Desirable for some applications (i.e. air traffic control, airline maintenance, entertainment)

Basic Mobile Network Support for IPv6

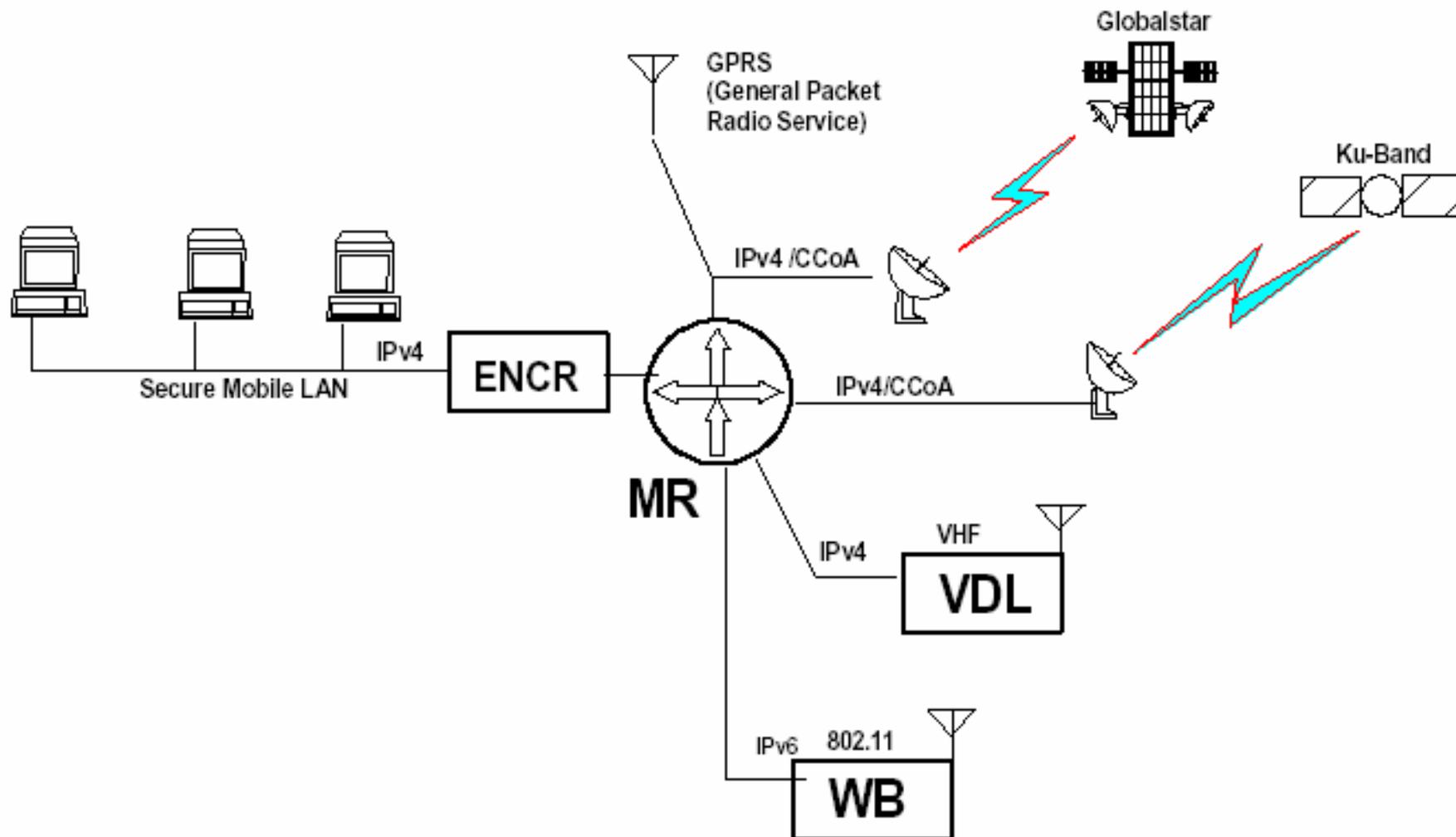




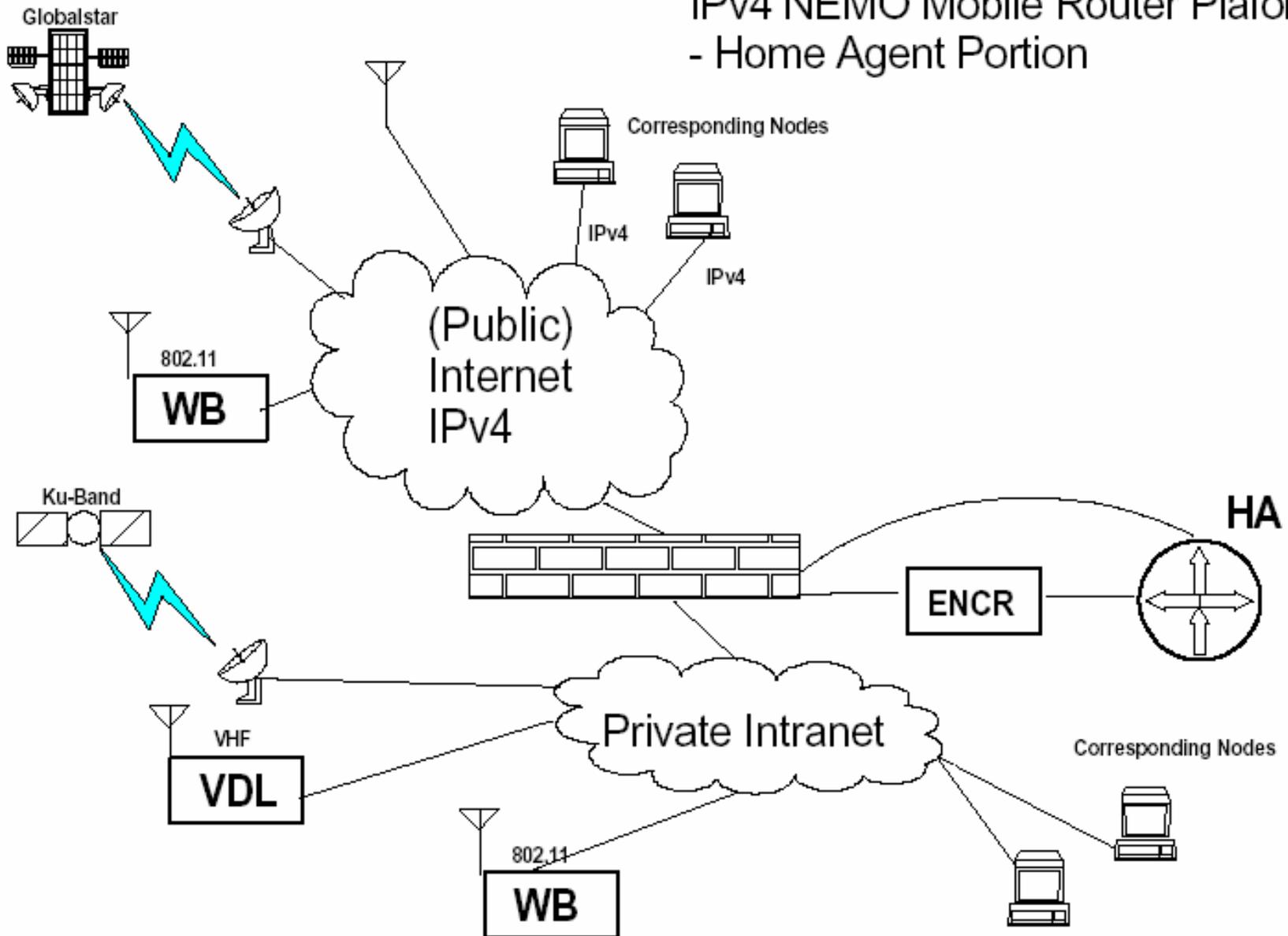
NEMO Experiments

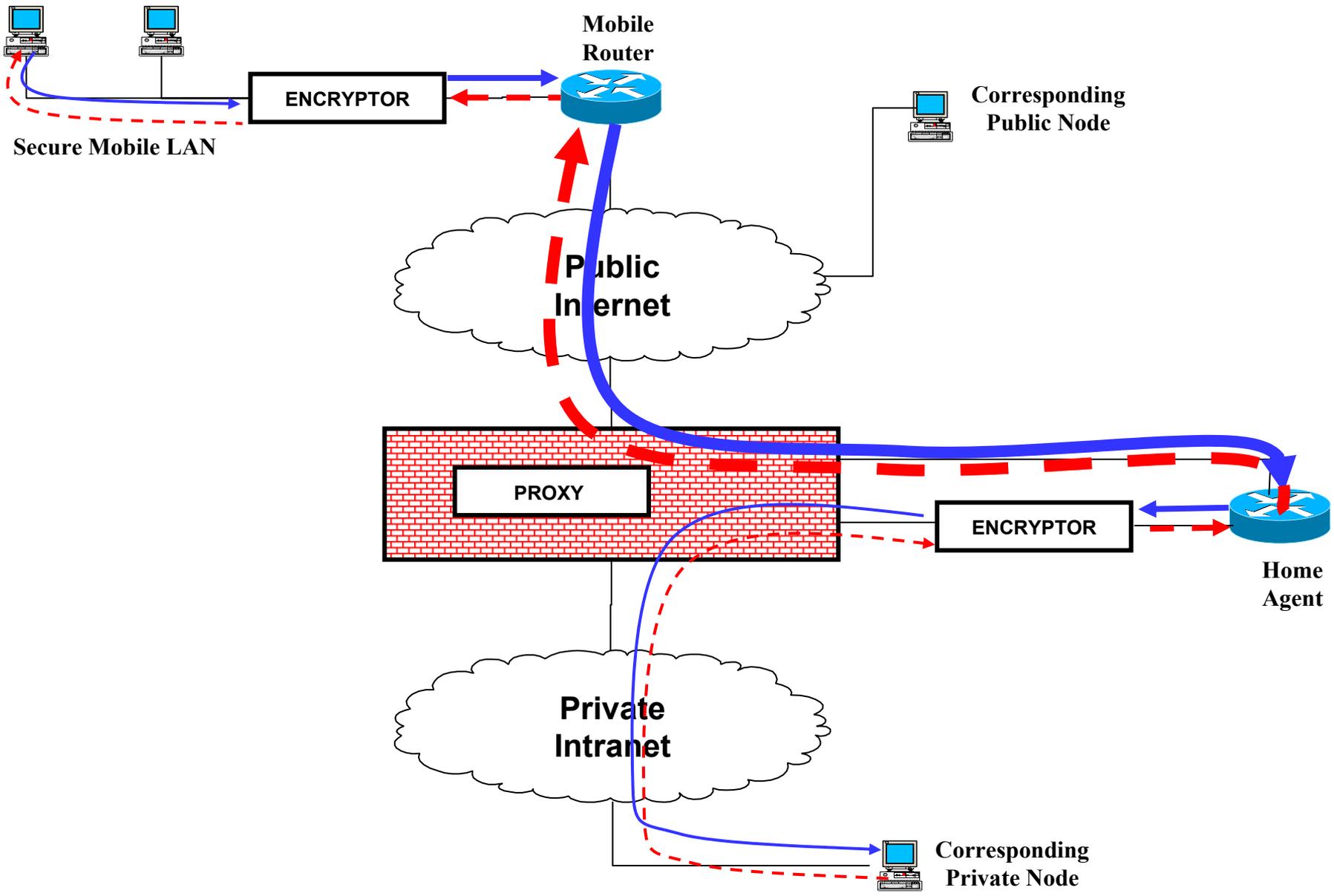
IPv4
&
IPv6

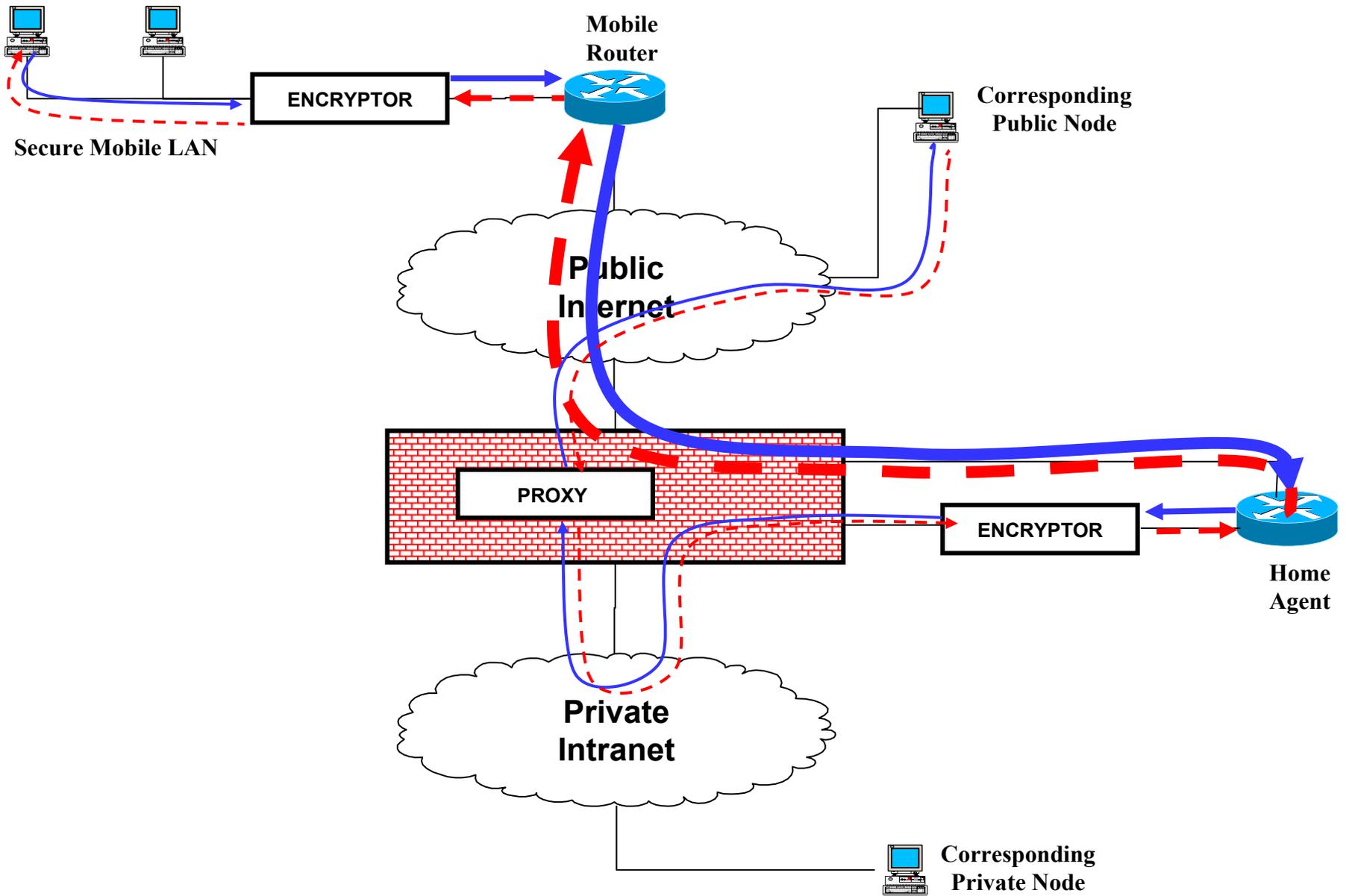
Aeronautical IPv4 NEMO Mobile Router Platform - Mobile Router Portion

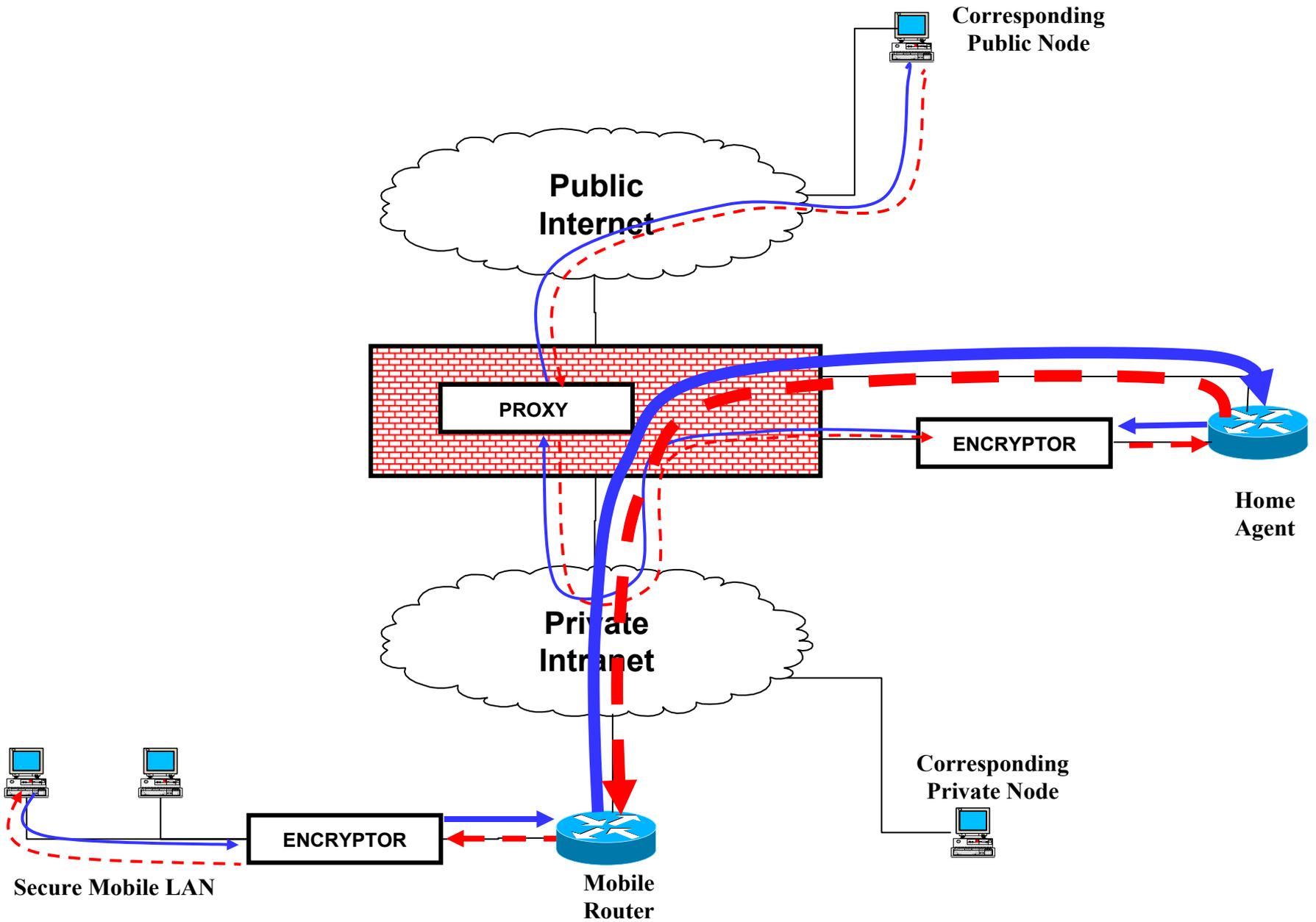


Aeronautical IPv4 NEMO Mobile Router Platform - Home Agent Portion

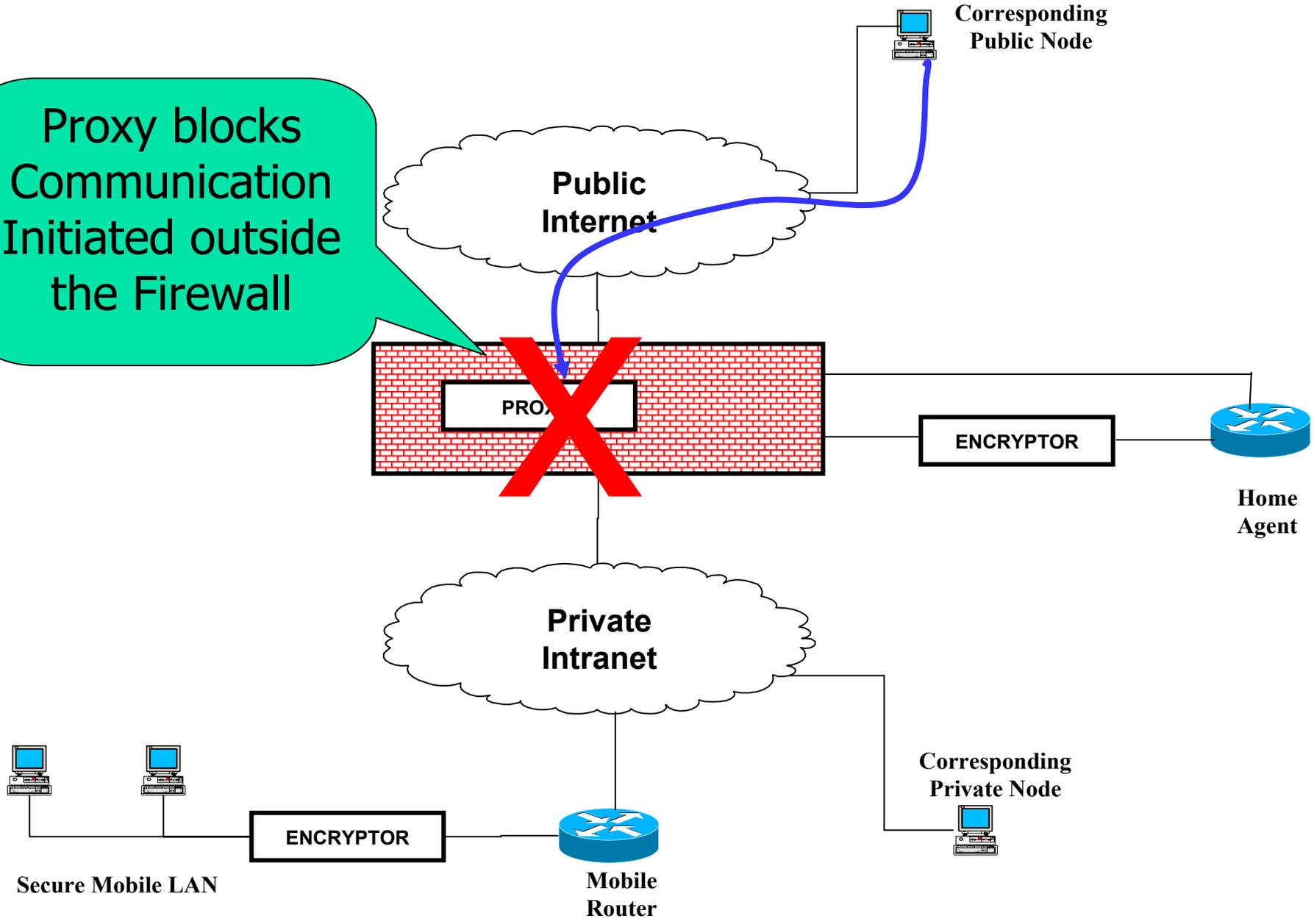


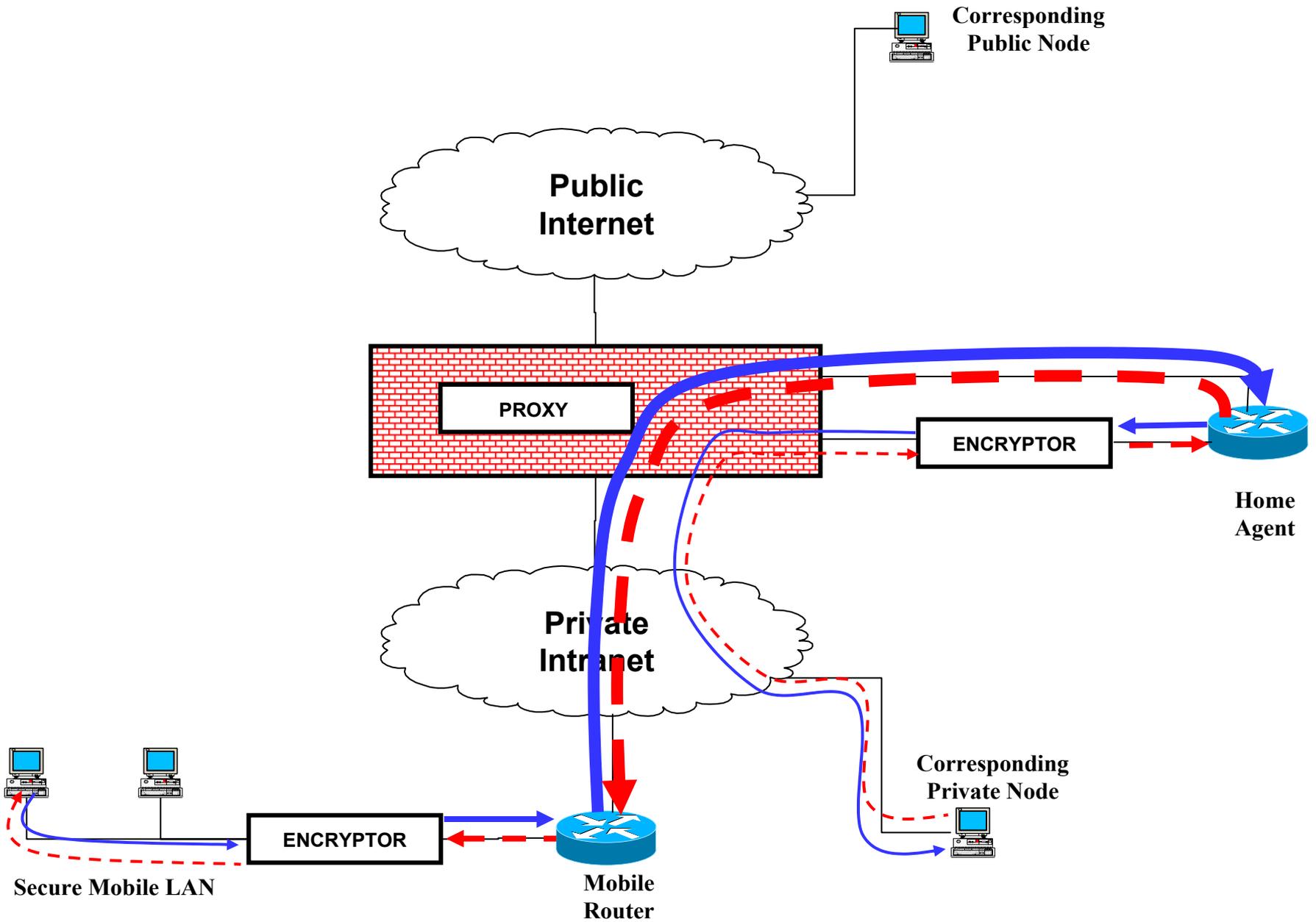




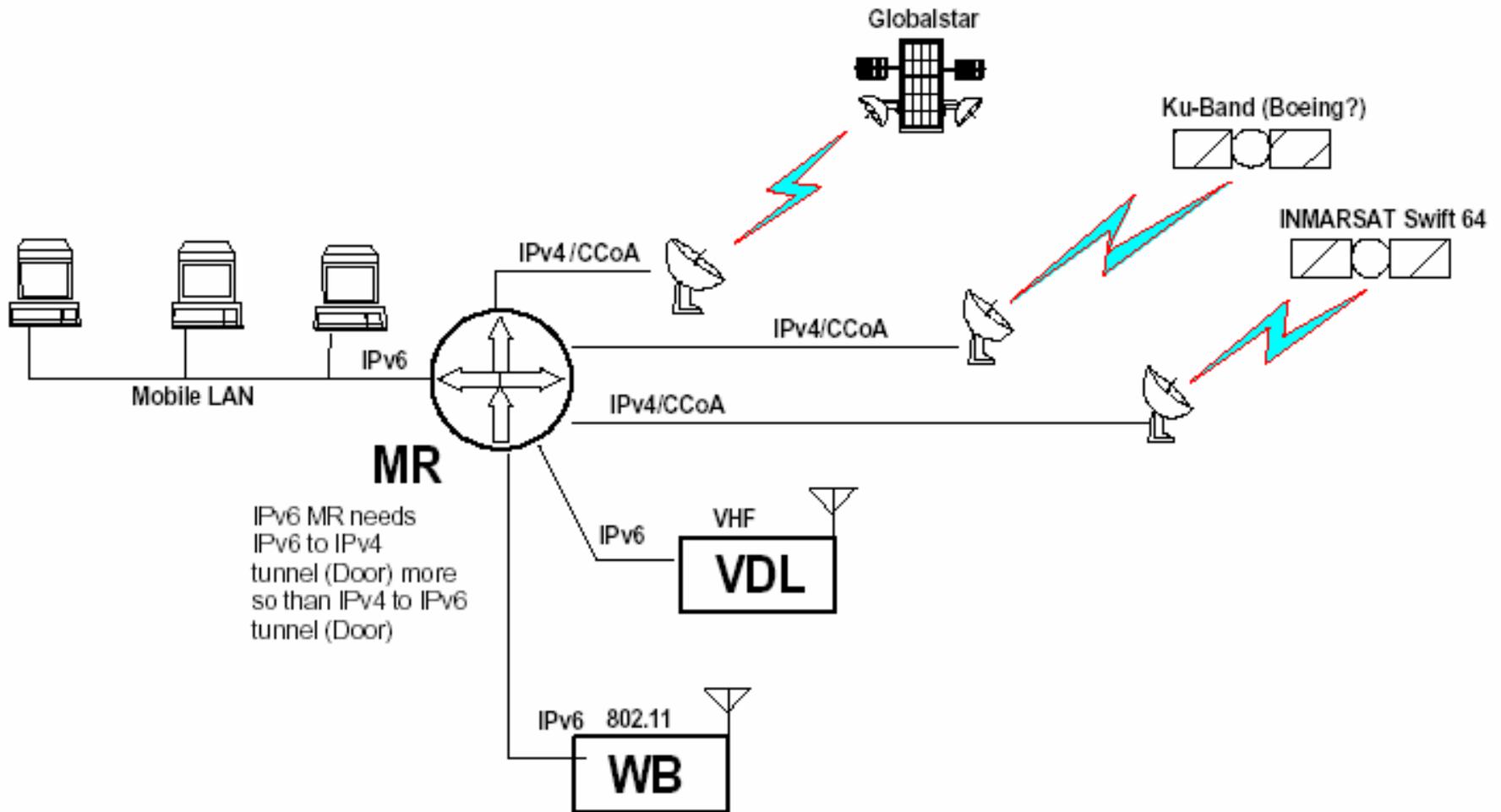


Proxy blocks
Communication
Initiated outside
the Firewall

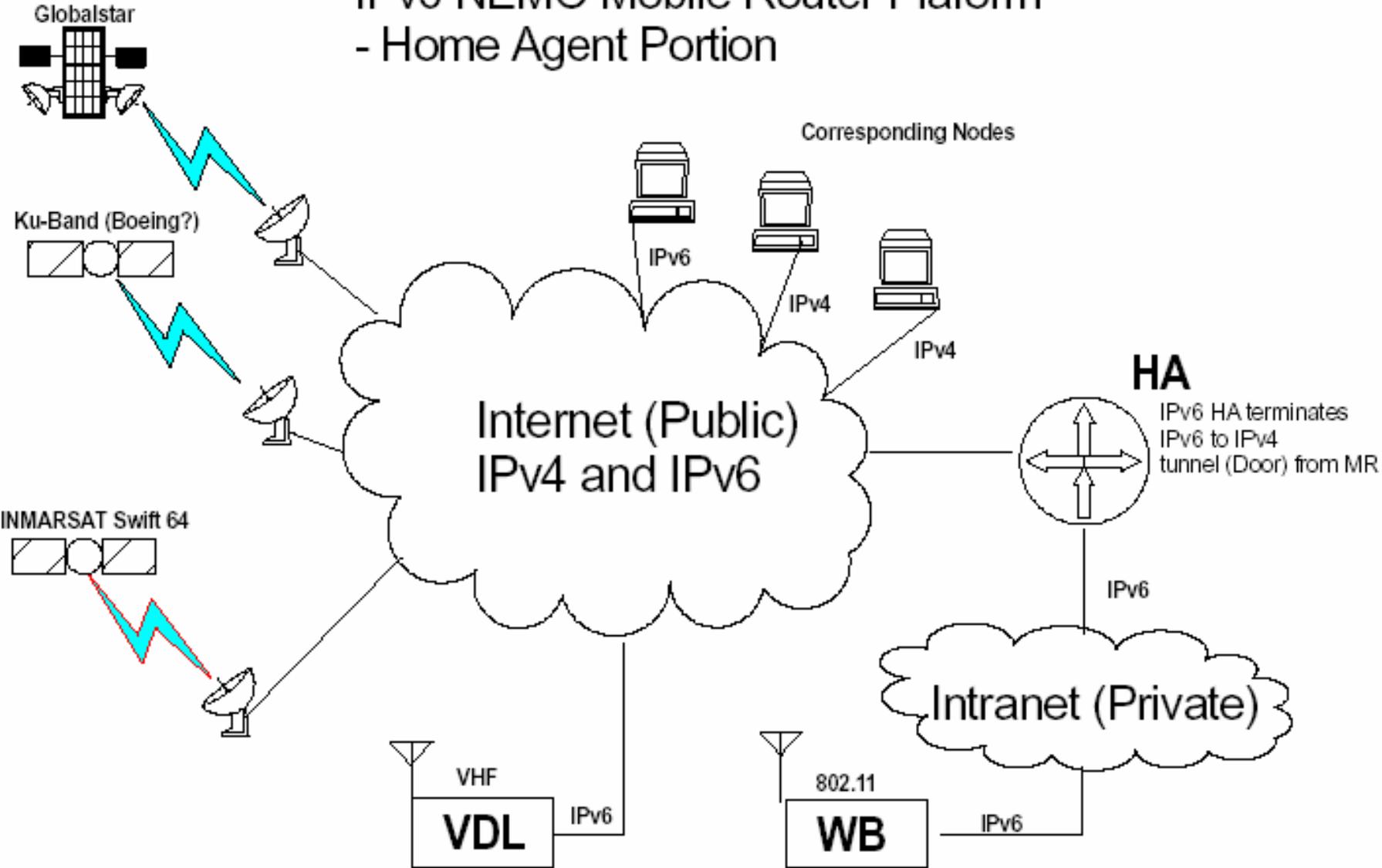


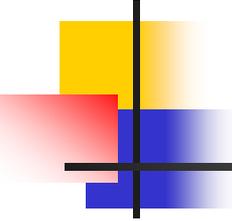


Aeronautical IPv6 NEMO Mobile Router Platform - Mobile Router Portion



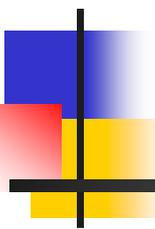
Aeronautical IPv6 NEMO Mobile Router Platform - Home Agent Portion





Additional Possibilities

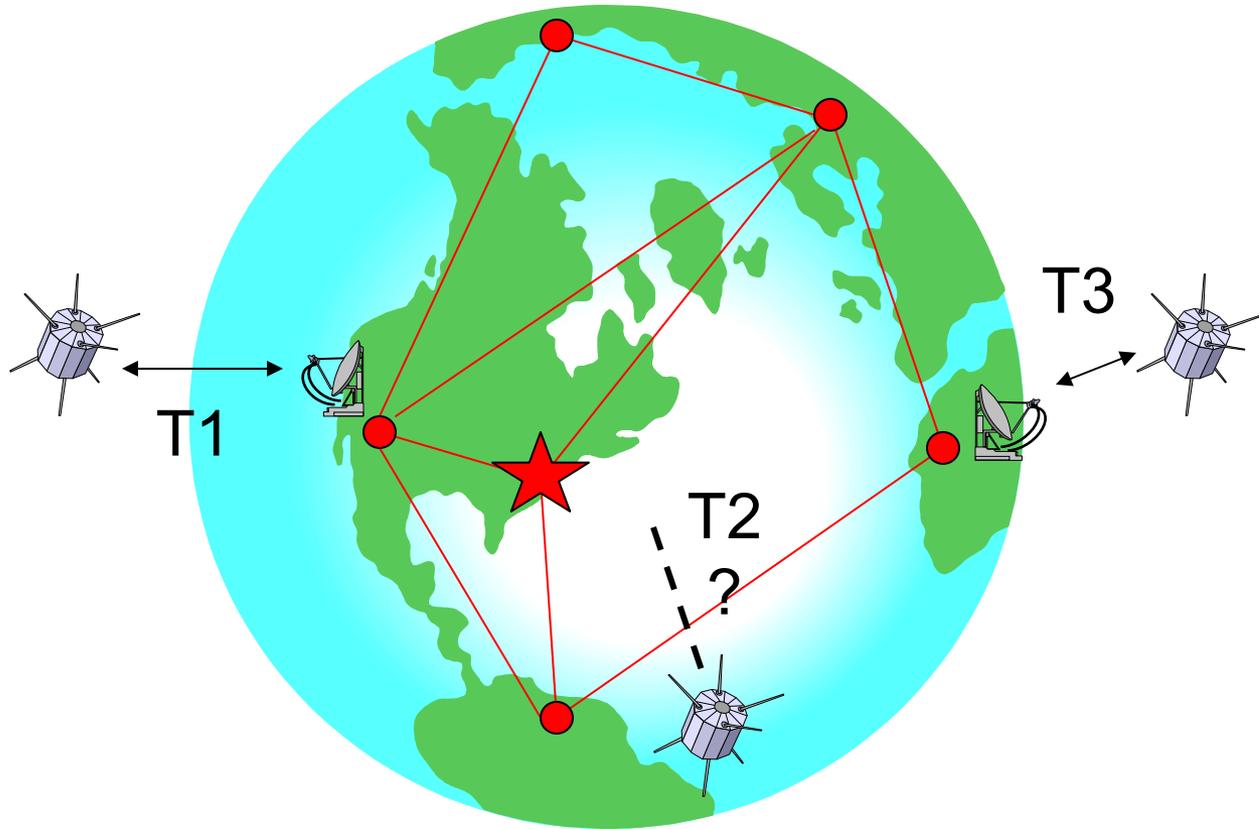
- Joint work with Eurocontrol
- Wireless Cabin work being performed by European Consortium using IPv6

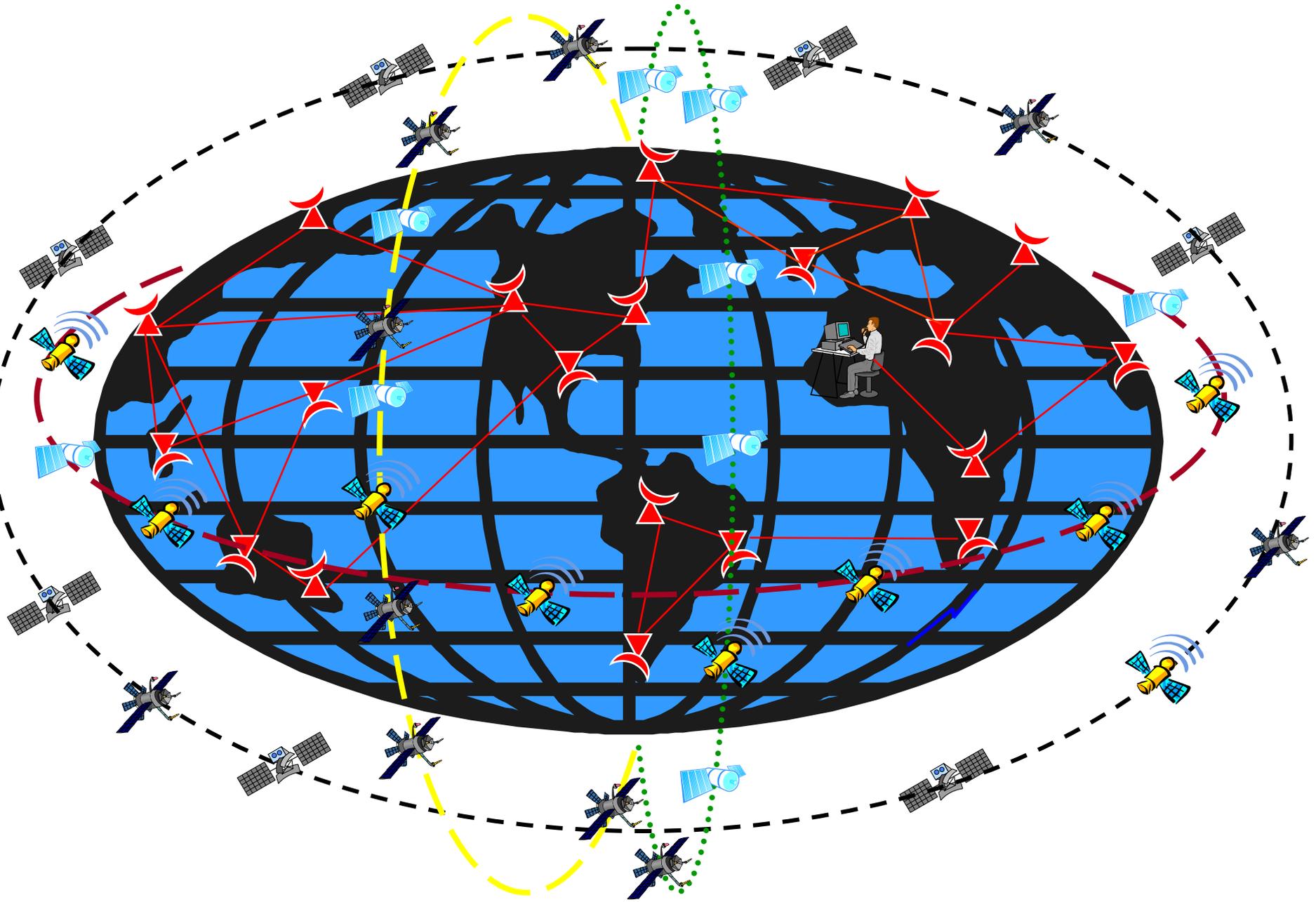


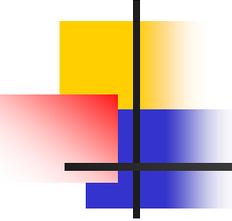
NASA's Space-Based Needs

Mobile Networks

Earth Observation







Space Flight Implementation

- Sharing Infrastructure
 - Common Media Access
 - Common Ground Terminal Capabilities
 - Common Network Access
 - AAA
 - Common Modulation and Coding
 - Software Radio

Backup

Neah Bay



Layer 2 Technology



**Globalstar
MCM-8**



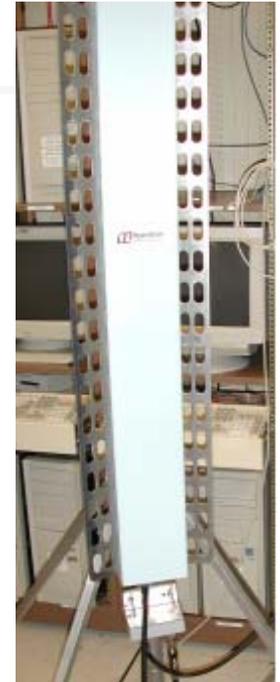
**L3-Comm
15 dBi
Tracking Antenna**



**Sea Tel Tracking
Antenna**

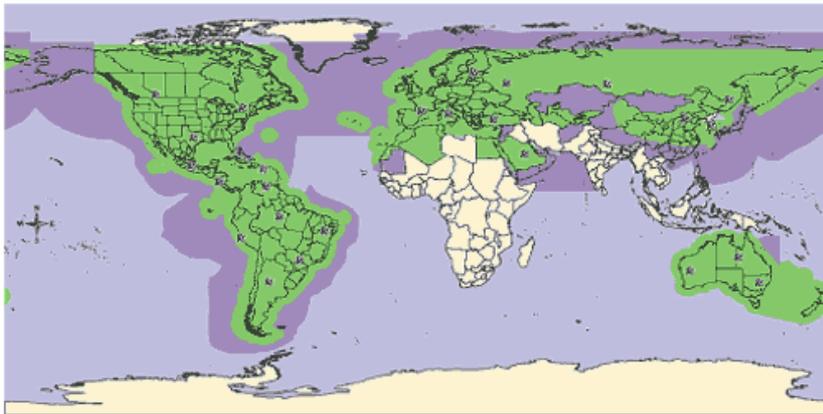


**8 dBi
Dipole**



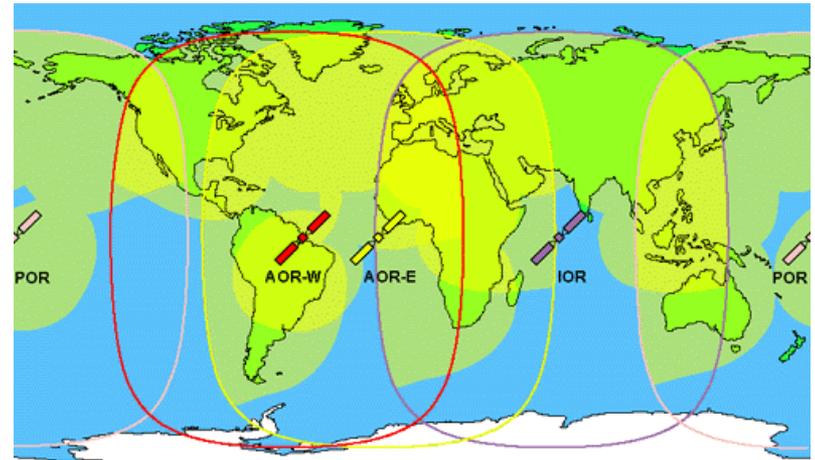
**Hypergain
802.11b
Flat Panel**

Satellite Coverage

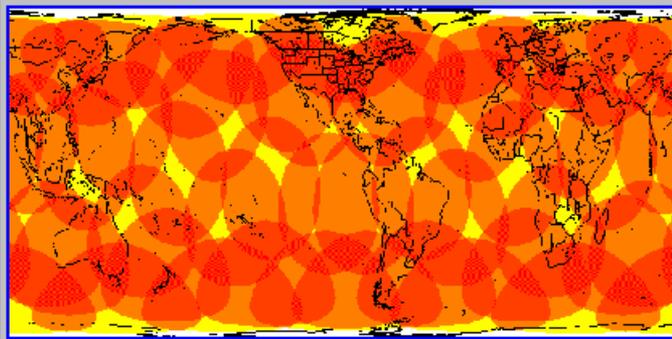
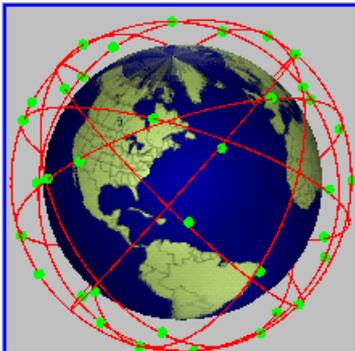


■ Globalstar Basic Coverage as of 1 April 2002
■ Extended Service Coverage
📡 Gateway

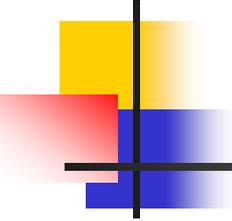
Globalstar



INMARSAT



From SaVi



Papers and Presentations

http://roland.grc.nasa.gov/~ivancic/papers_presentations/papers.html

or

<http://roland.grc.nasa.gov/~ivancic/>

and pick

“Papers and Presentations”