



**NASA's
Secure Mobile Networking
Research and its Applicability
for the Future
Global Airspace Network**

Will Ivancic

wivancic@grc.nasa.gov

216-433-3494

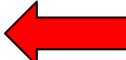


Outline

- Background
- Testing Philosophy
- NEMO Experiments
 - IPv4 and IPv6
- Cisco router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center
 - IPv4-based NetCentric Operations
- Mobility and Encryption
- Next Generation Global Airspace System Requirements
 - IPv6-based NetCentric Operations



Background

- IP Network Research for Commercial Communications Satellites
 - ACTS Experimental Ka-Band Satellite
- Non-reimbursable Space Act Agreement with Cisco since 1998 regarding space-based IP research
 - Satellite and the Internet leads to mobile router development due to interest by aeronautics community
- Secure Mobile Networking Research
 - US Coast Guard Neah Bay
 - Satellite and WiFi  If you want a DVD, Send me an email
 - Ohio State Highway Patrol
 - Cellular and WiFi
 - OSD
 - Satellite, Cellular and WiFi  NAT Traversal - SORRY
 - IPv4 and IPv6
 - CLEO/VMOC  http://roland.grc.nasa.gov/~ivancic/papers_presentations/
 - Bringing the Internet to Space
 - Merging of Ad Hoc and Mobile-IPv6



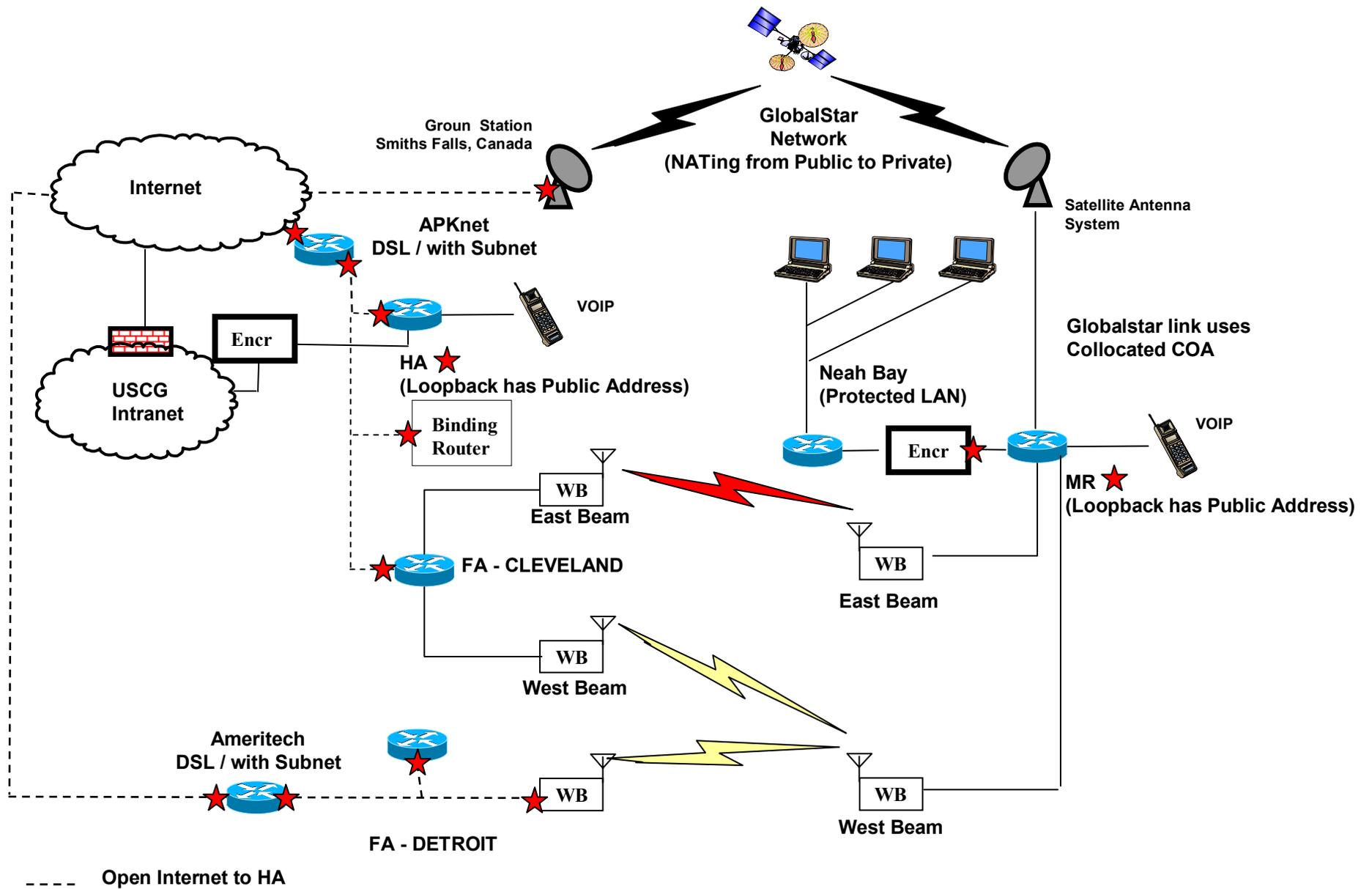
Testing Philosophy

- Prove functionality in the lab
- Prove security in operational networks!
 - The best way to address security issues is to be forced to address real operational security issues
 - US Coast Guard Neah Bay demonstration deployed IPv4 mobile networking in the US Coast Guard operational network
 - Used operationally in Summer of 2002 in NY, NY and Boston to provide Internet connectivity using Globalstar Satellite – Neah Bay providing escort service
 - Used operationally in fall of 2002 while Neah Bay was in dry dock – 11 Mbps far exceeded normal fractional T1 service
 - IPv4 NEMO deployed in GRC Operational Network
 - Required extensive security plan (a-typical network)



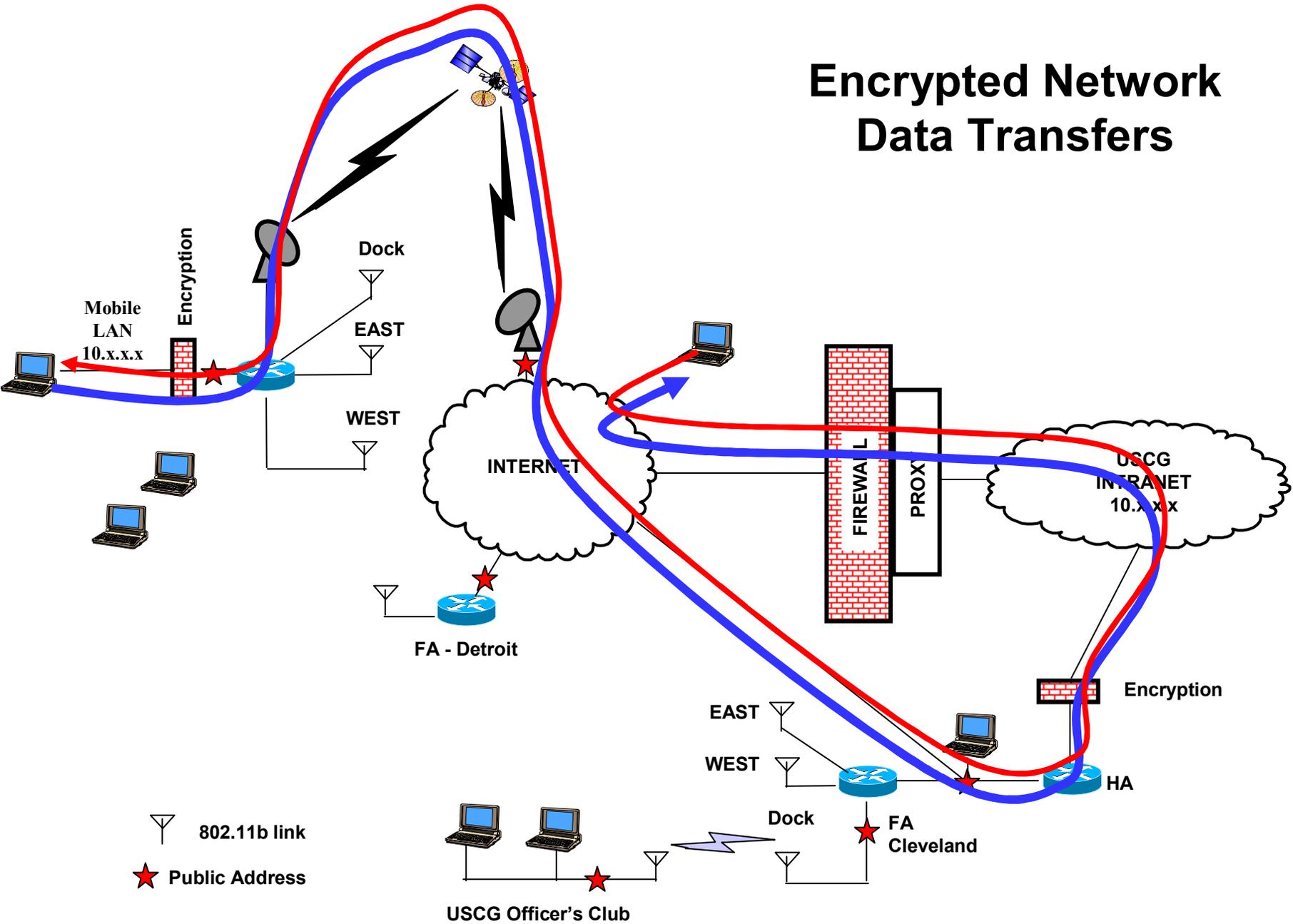
US Coast Guard IPv4 Secure Mobile Networking

Deployment of IPv4 Mobile Networking in
an Operational Network



★ Public Address

Encrypted Network Data Transfers





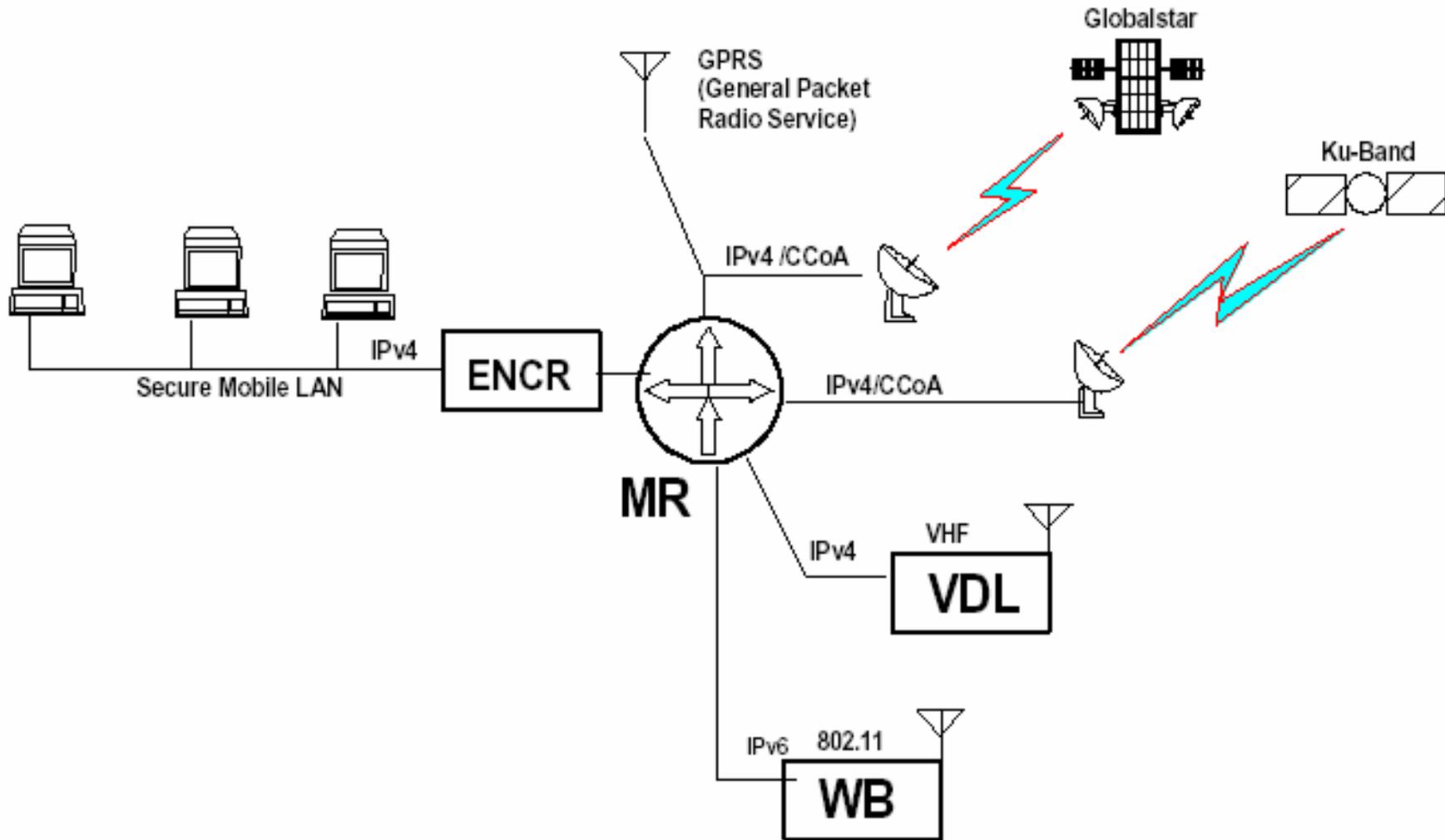
NEMO Experiments

IPv4 & IPv6

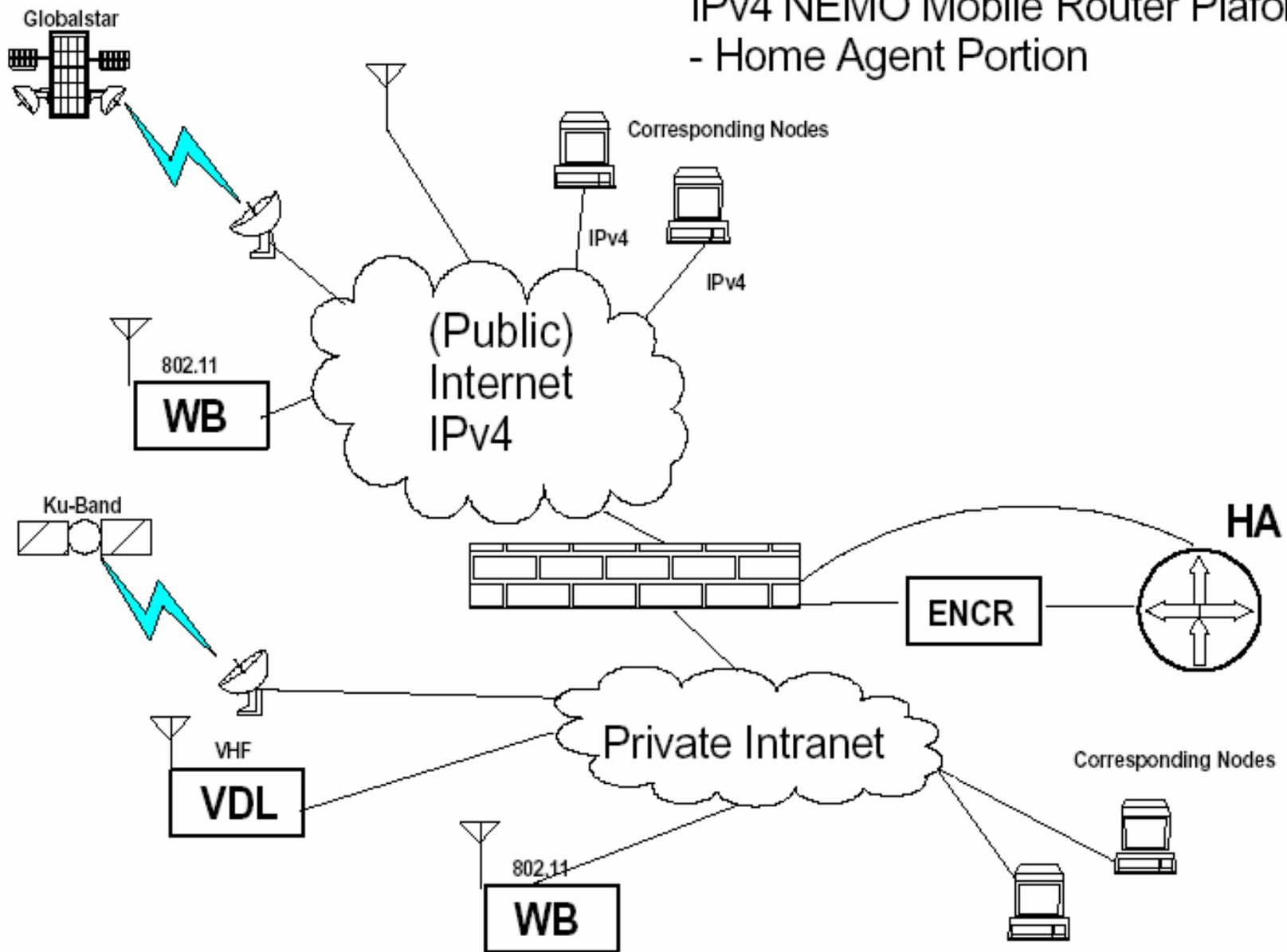
roland.grc.nasa.gov/~ivancic

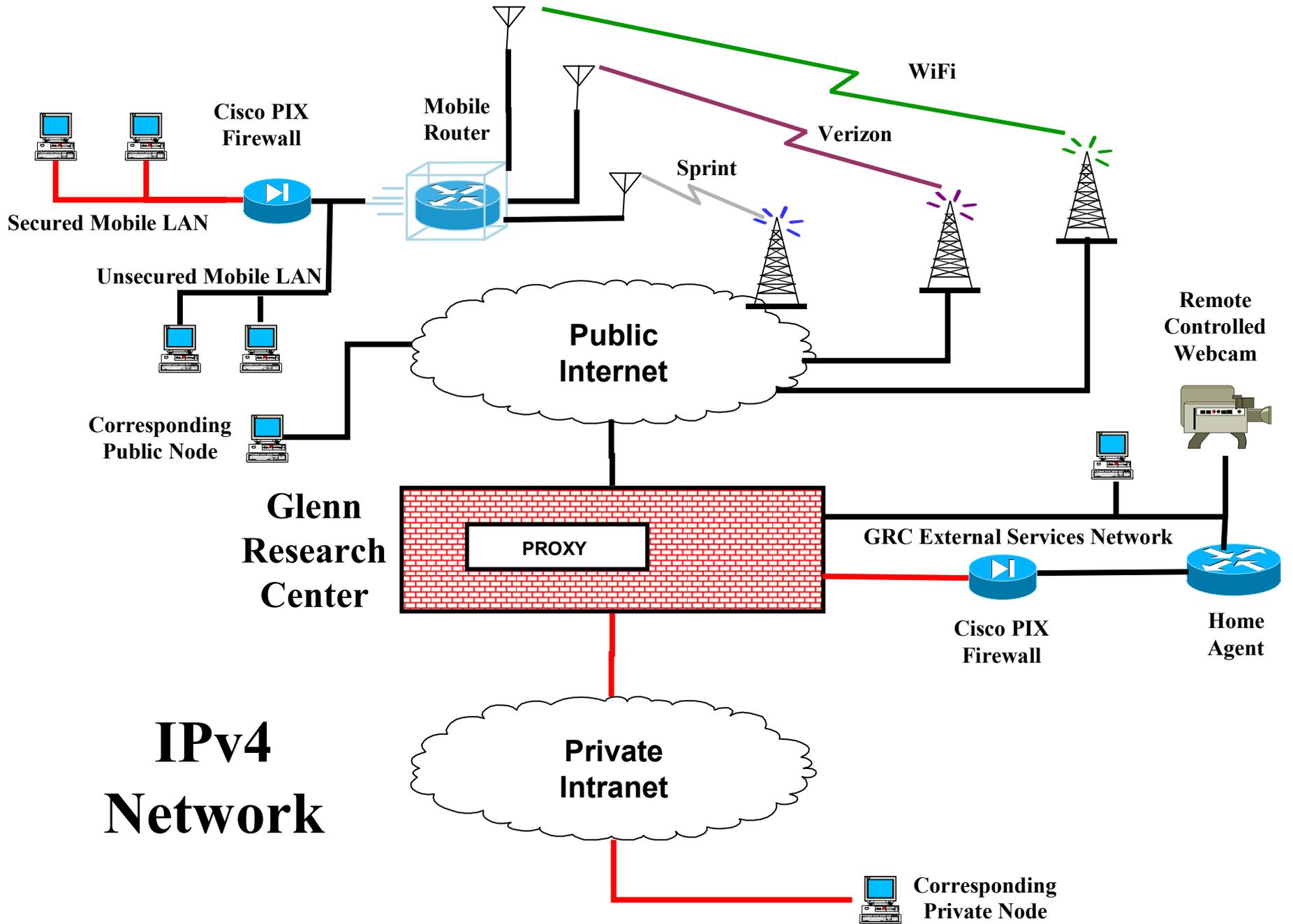
Pick ICNS Demonstration

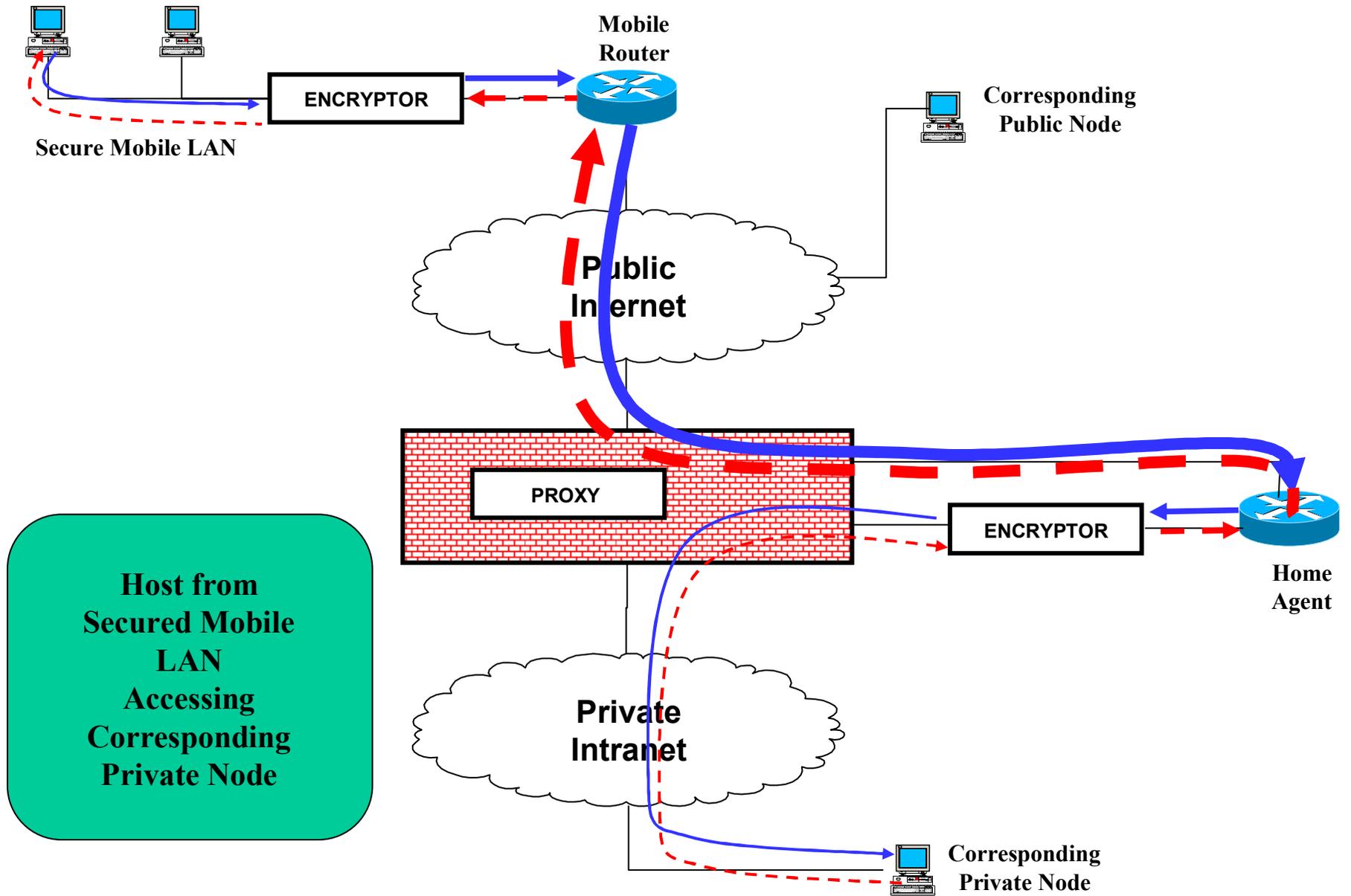
Aeronautical IPv4 NEMO Mobile Router Platform - Mobile Router Portion

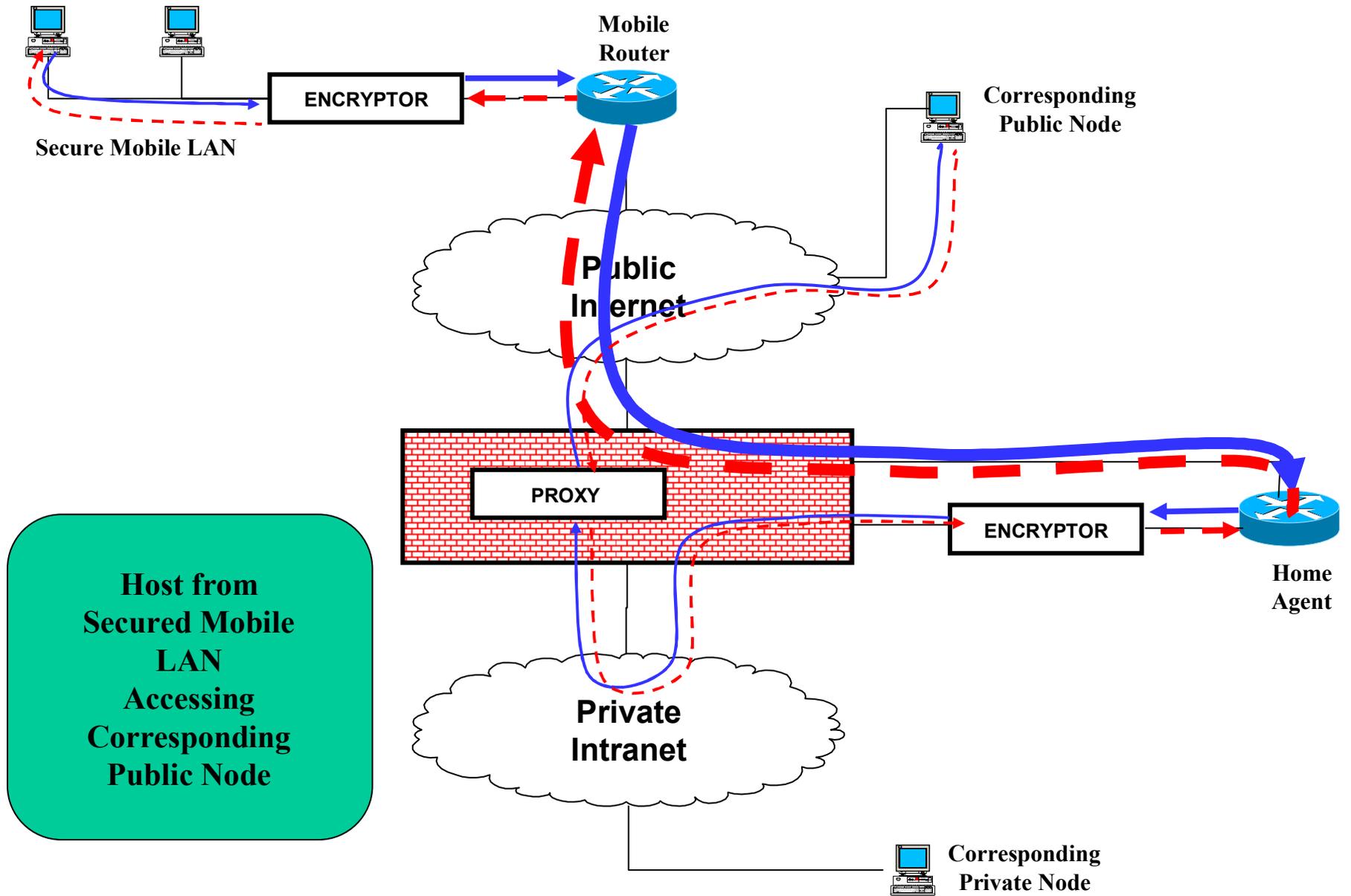


Aeronautical IPv4 NEMO Mobile Router Platform - Home Agent Portion

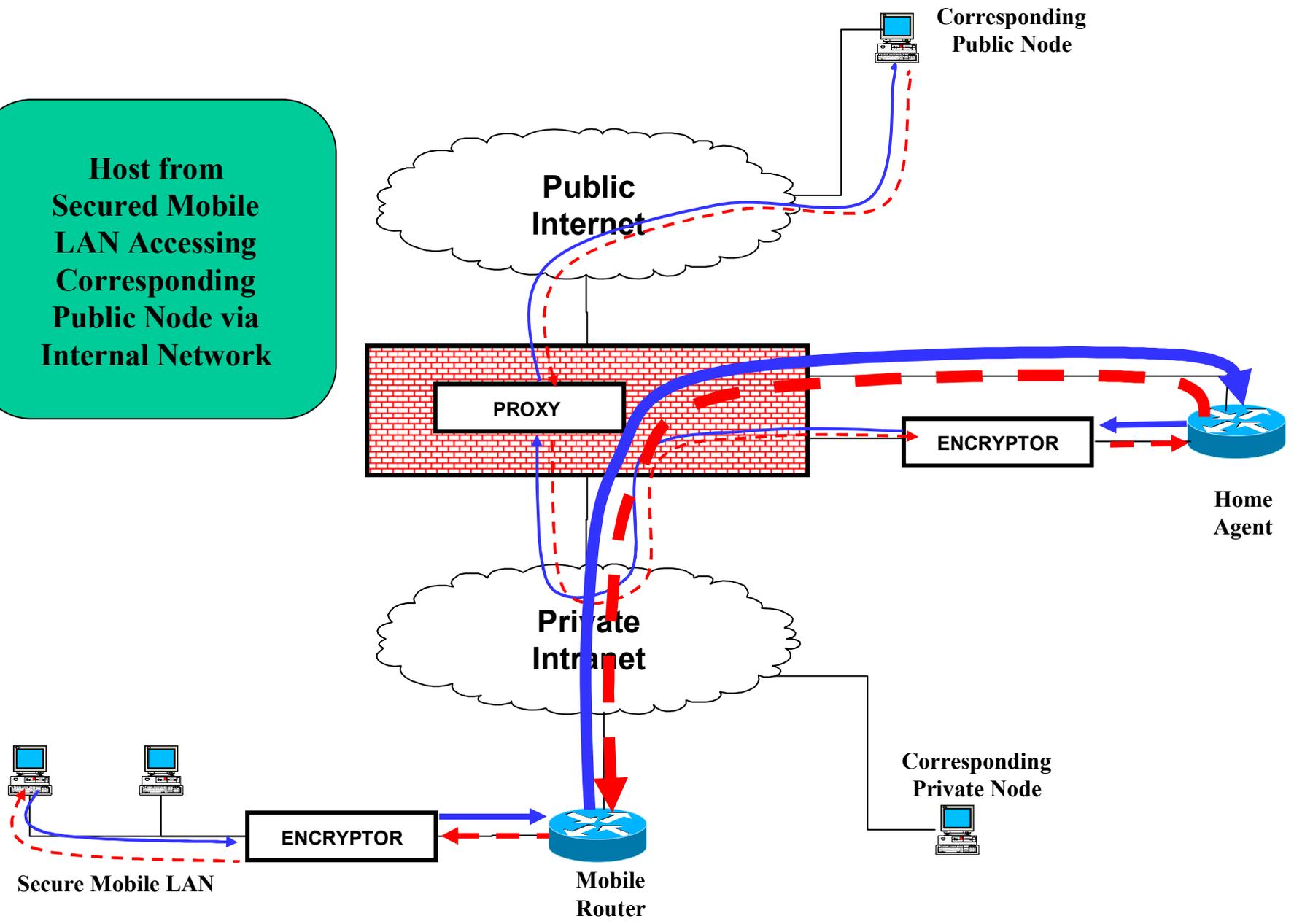




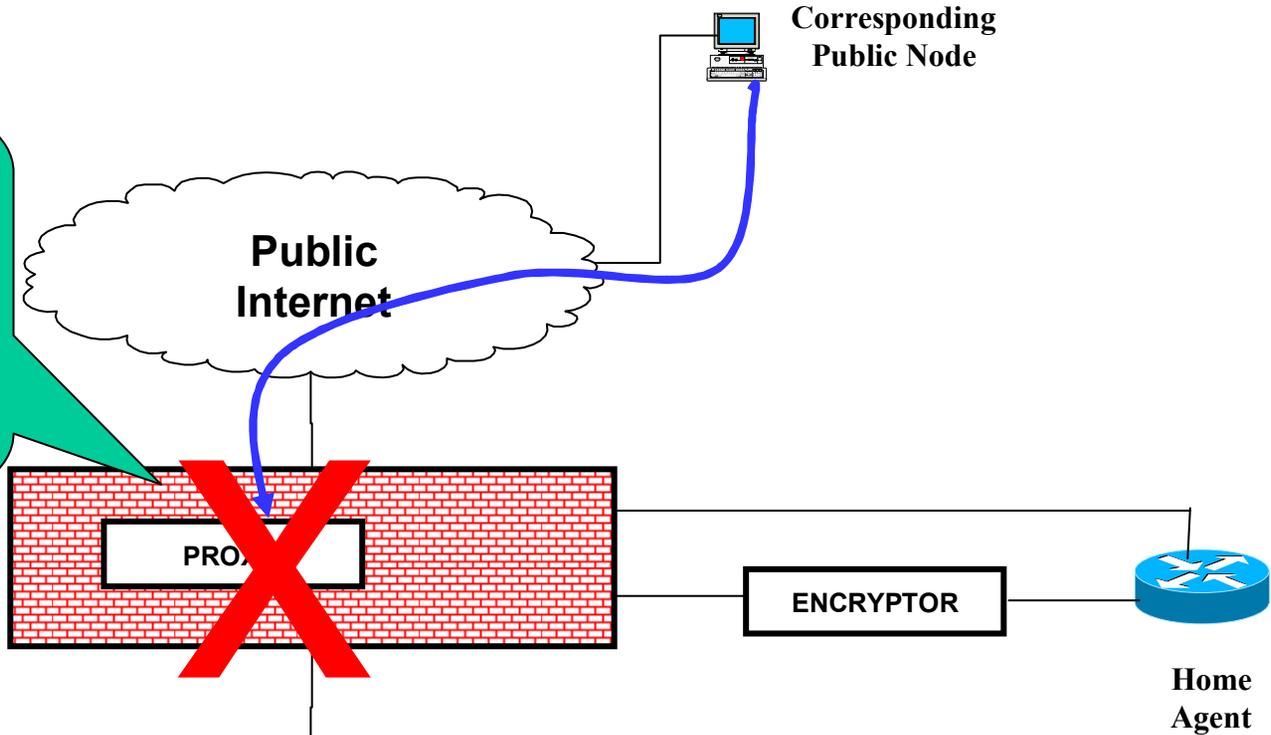




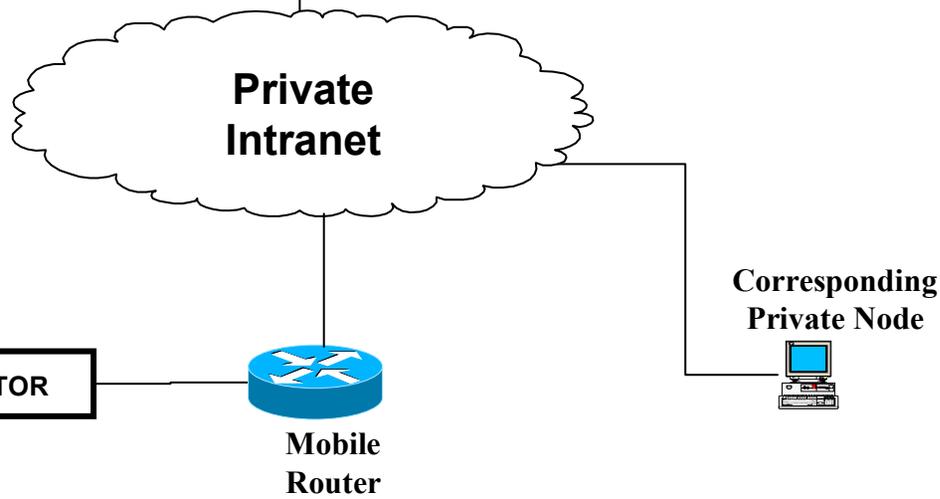
Host from Secured Mobile LAN Accessing Corresponding Public Node via Internal Network



Proxy blocks
Communication
Initiated outside
the Firewall

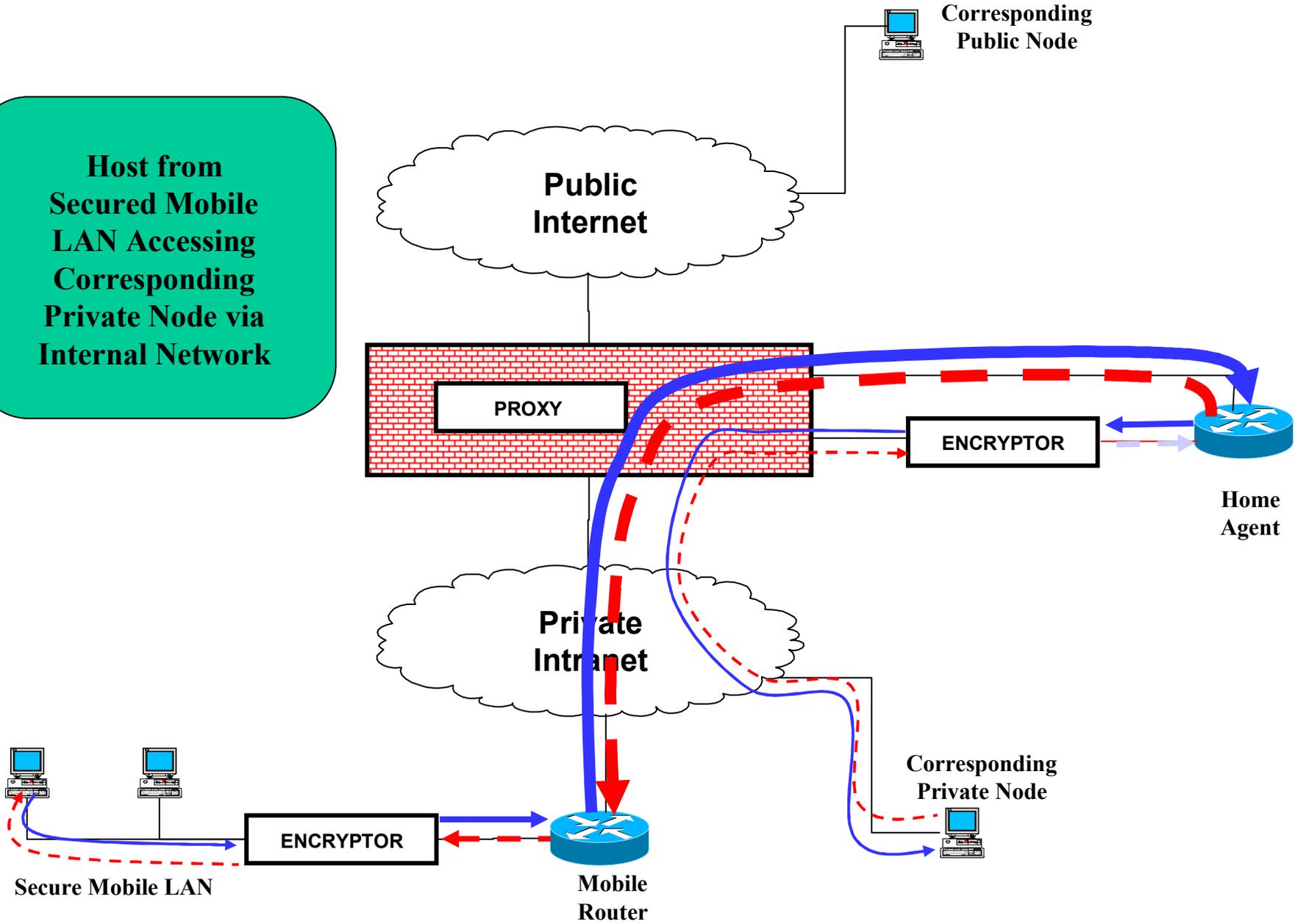


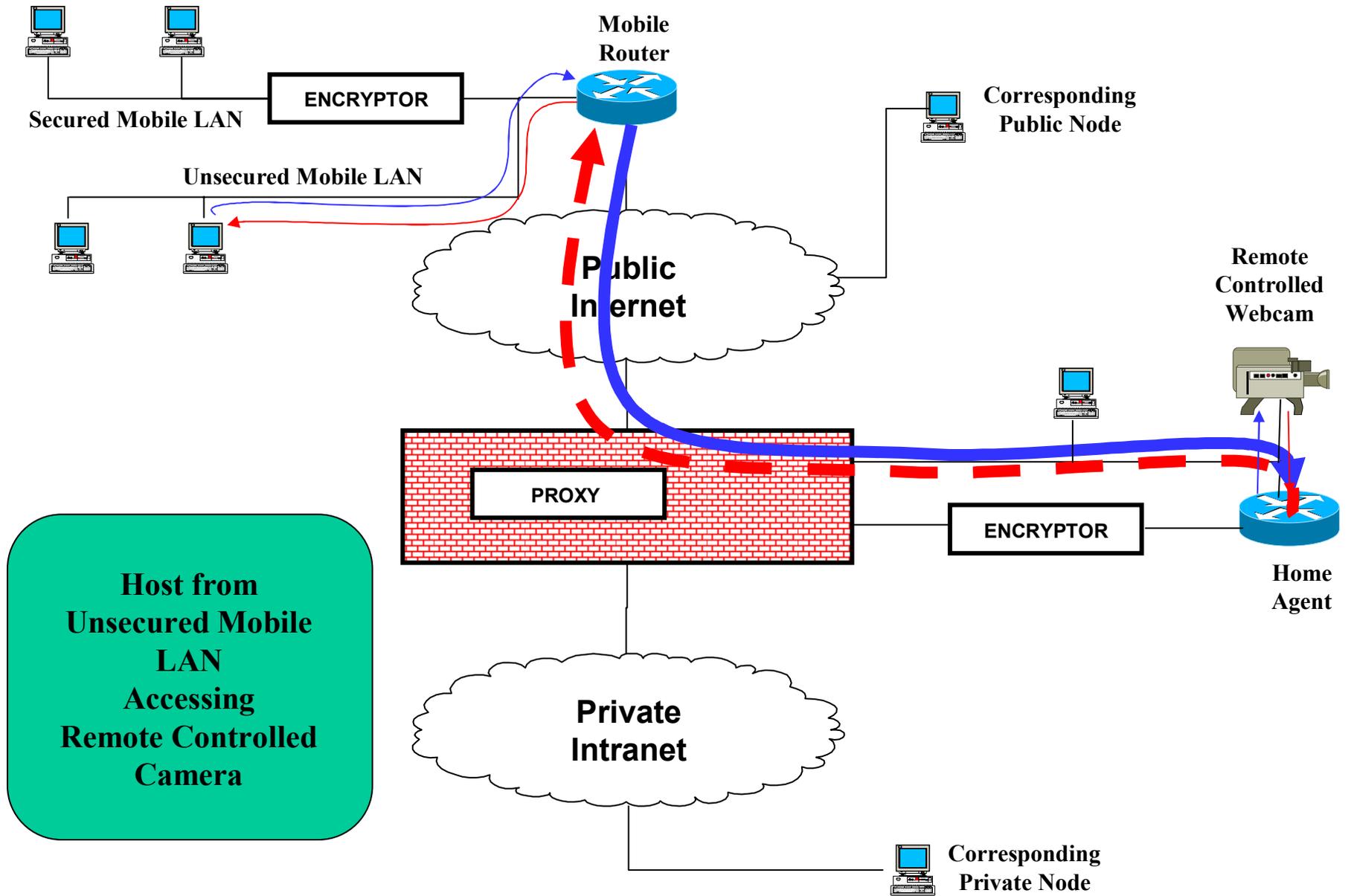
Corresponding
Public Node
Initiating
Conversation

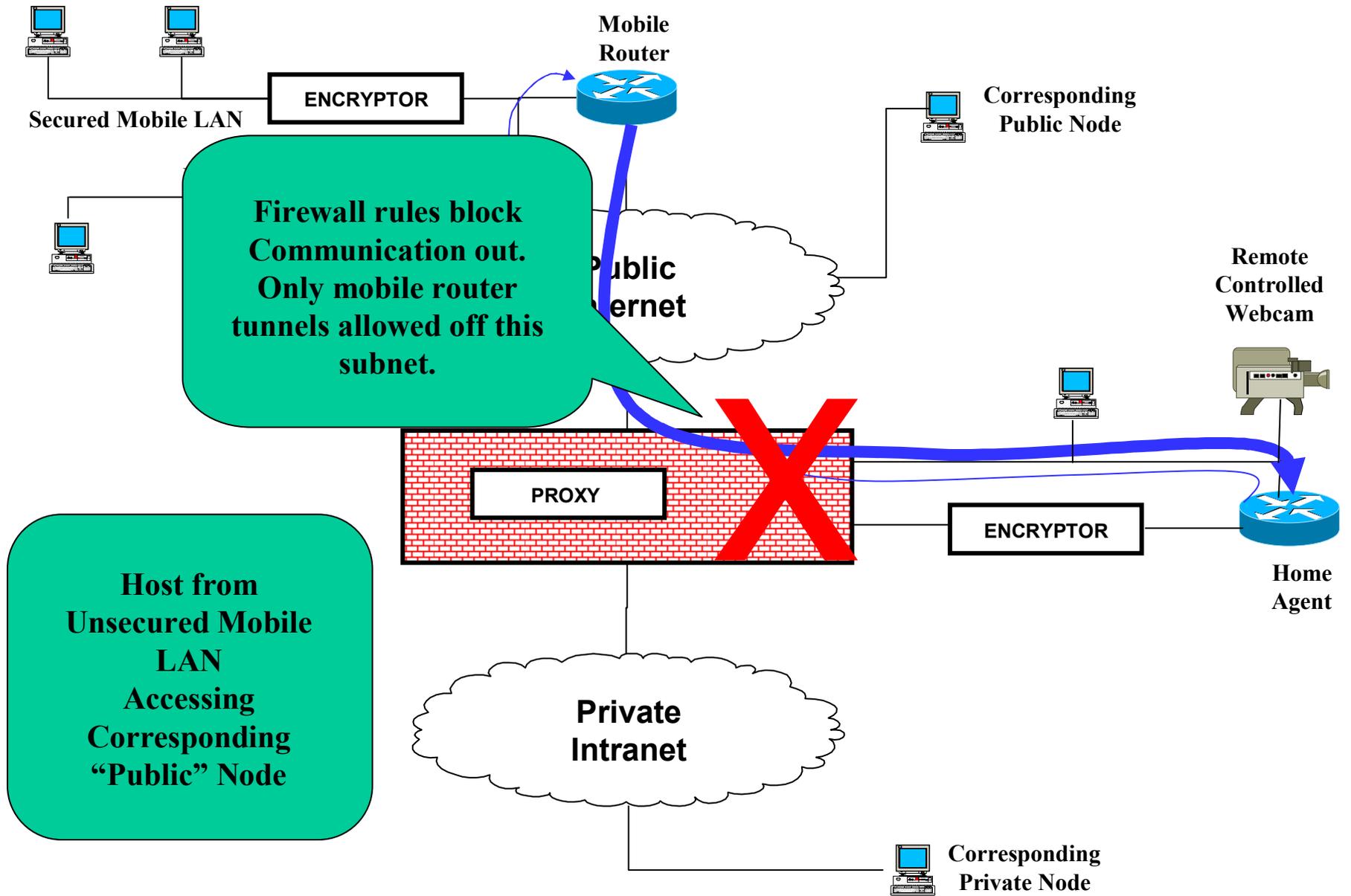


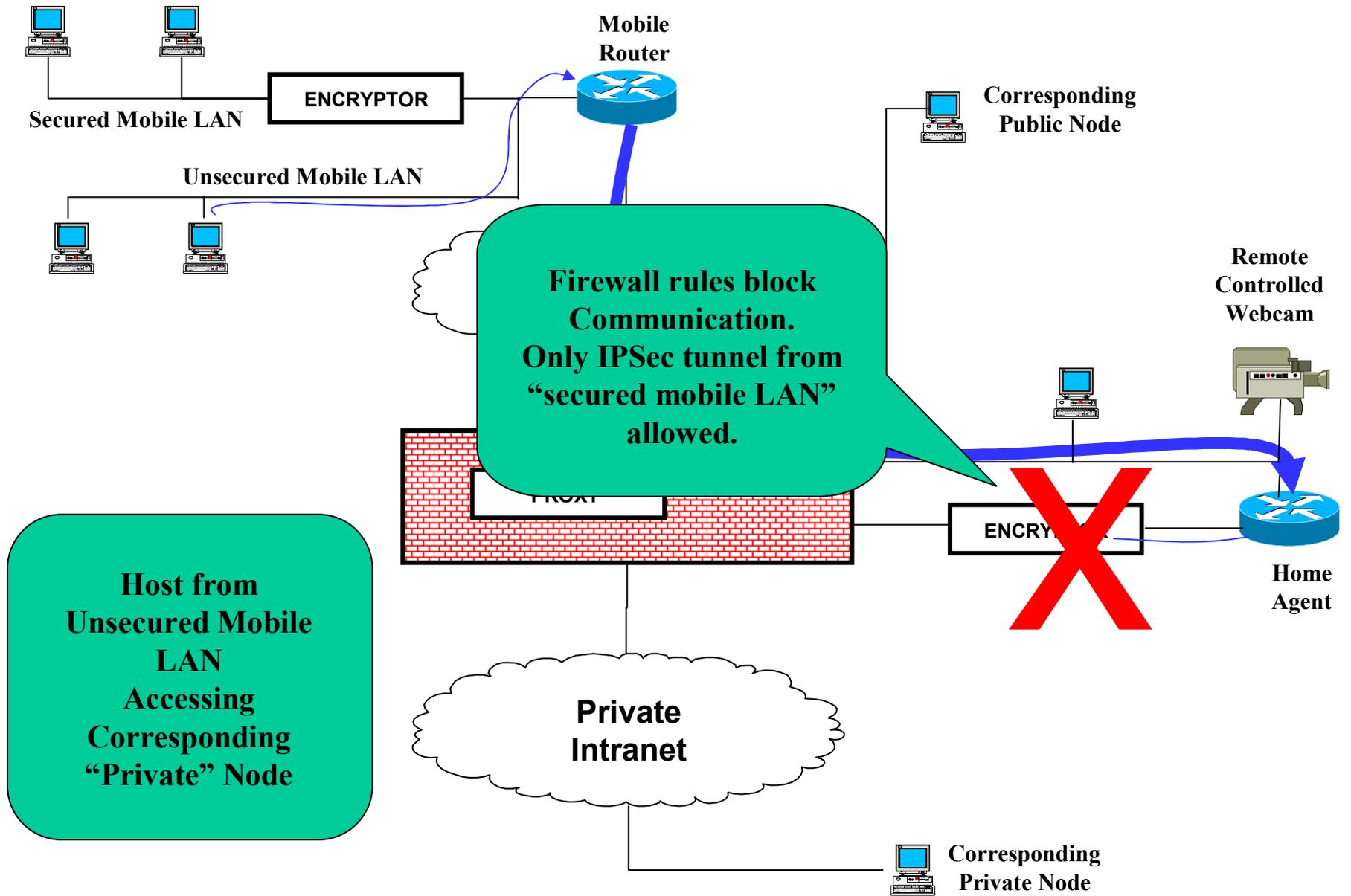
Secure Mobile LAN

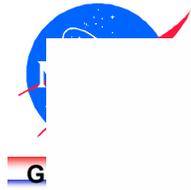
Host from Secured Mobile LAN Accessing Corresponding Private Node via Internal Network



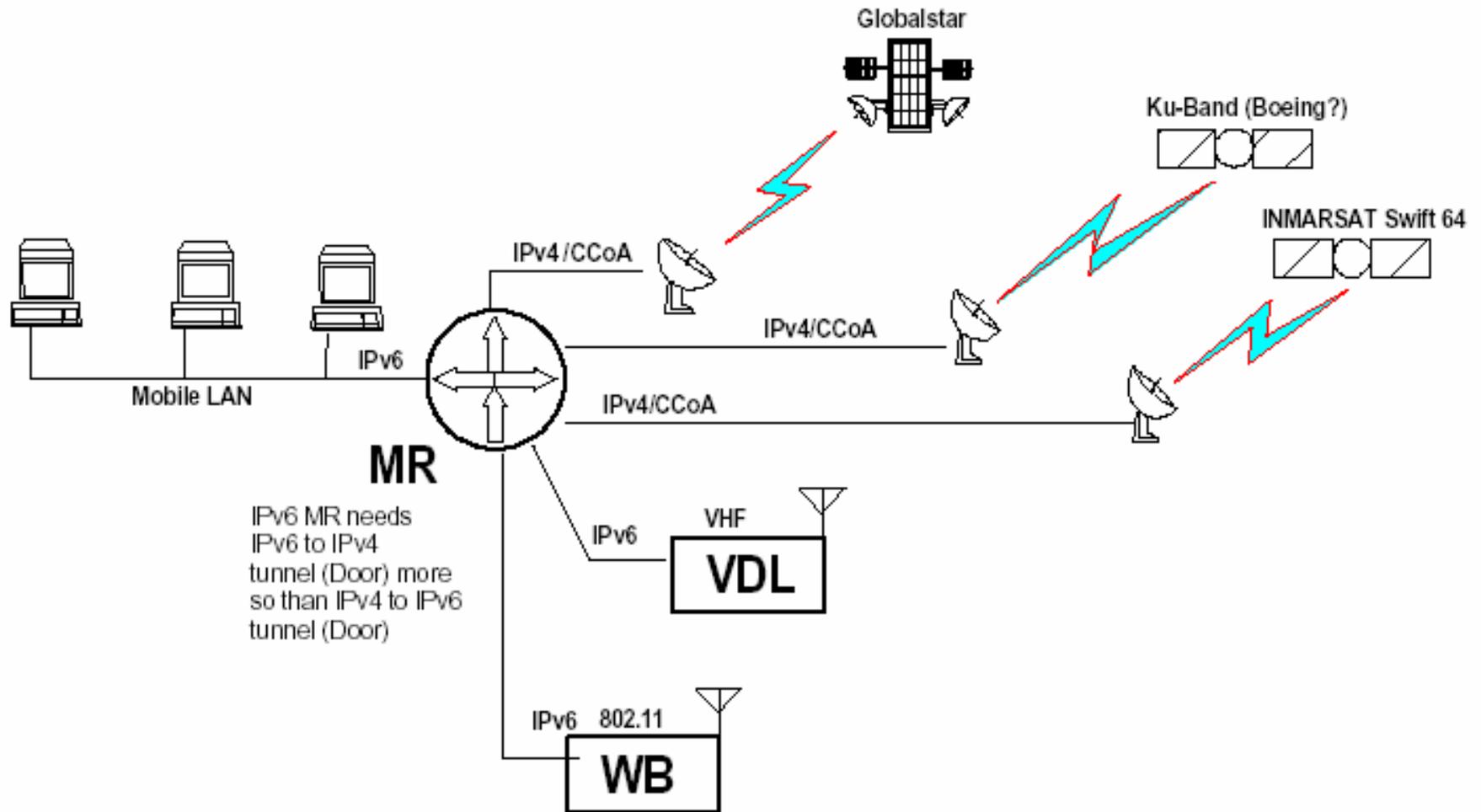






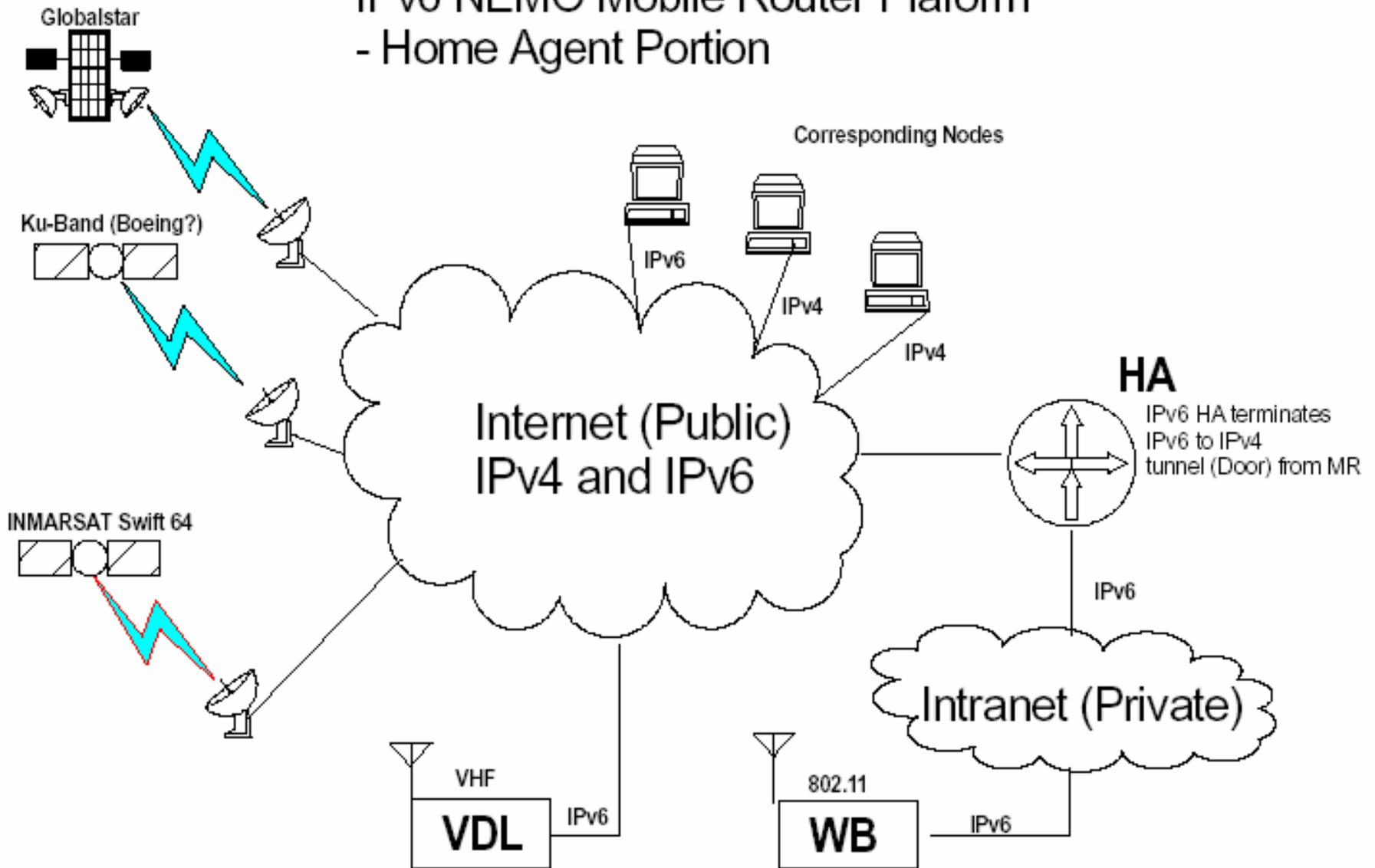


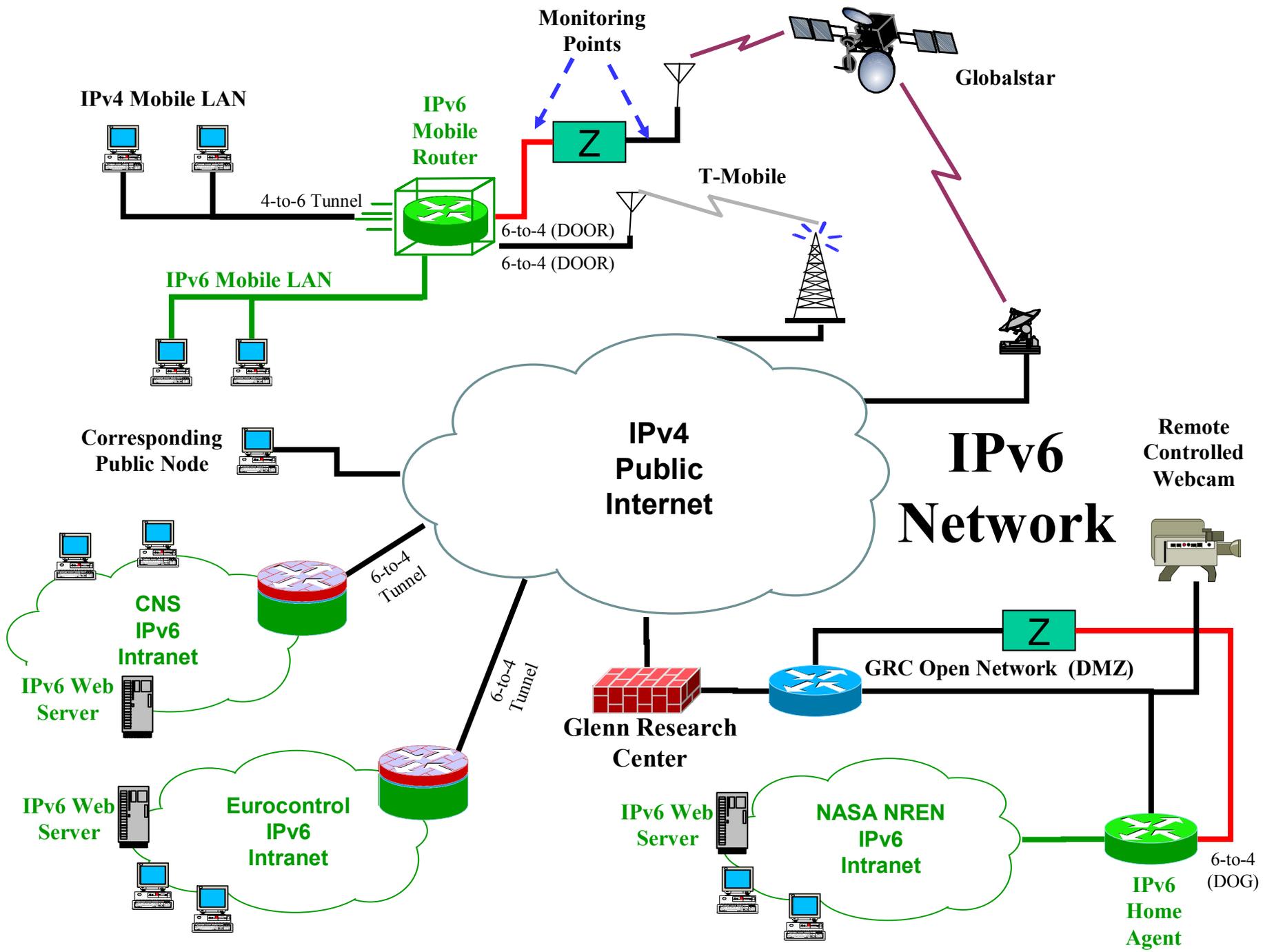
Aeronautical IPv6 NEMO Mobile Router Platform - Mobile Router Portion





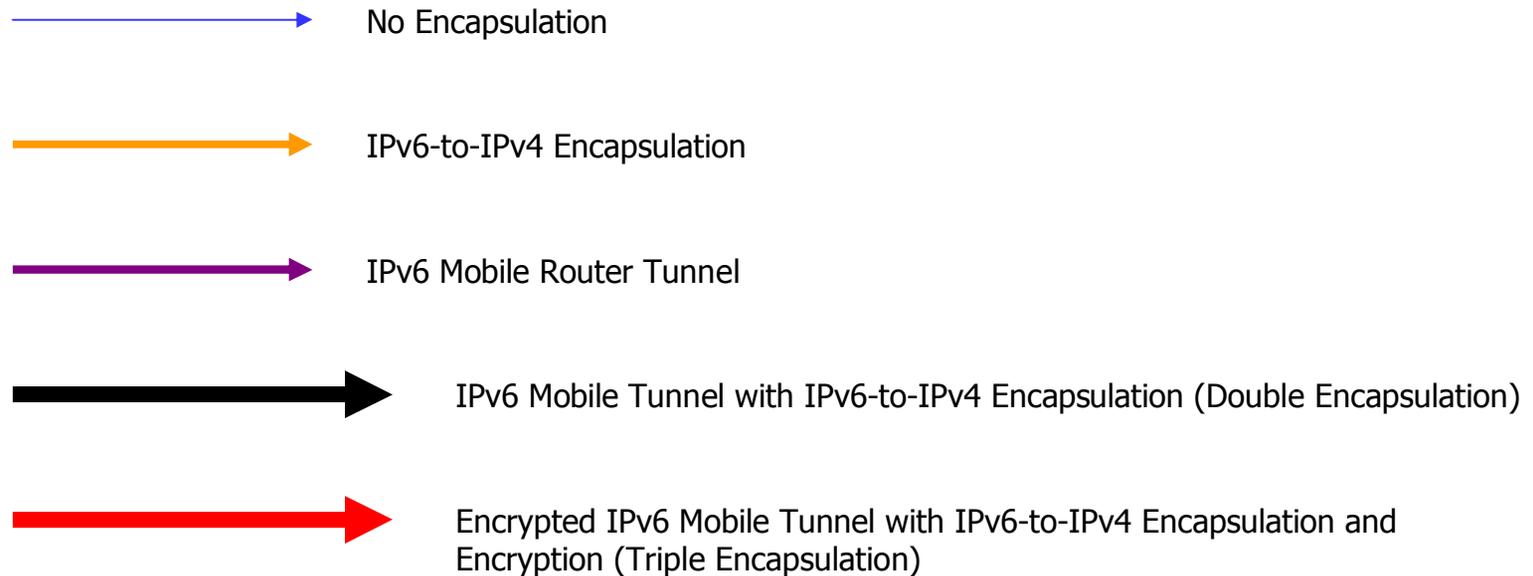
Aeronautical IPv6 NEMO Mobile Router Platform - Home Agent Portion



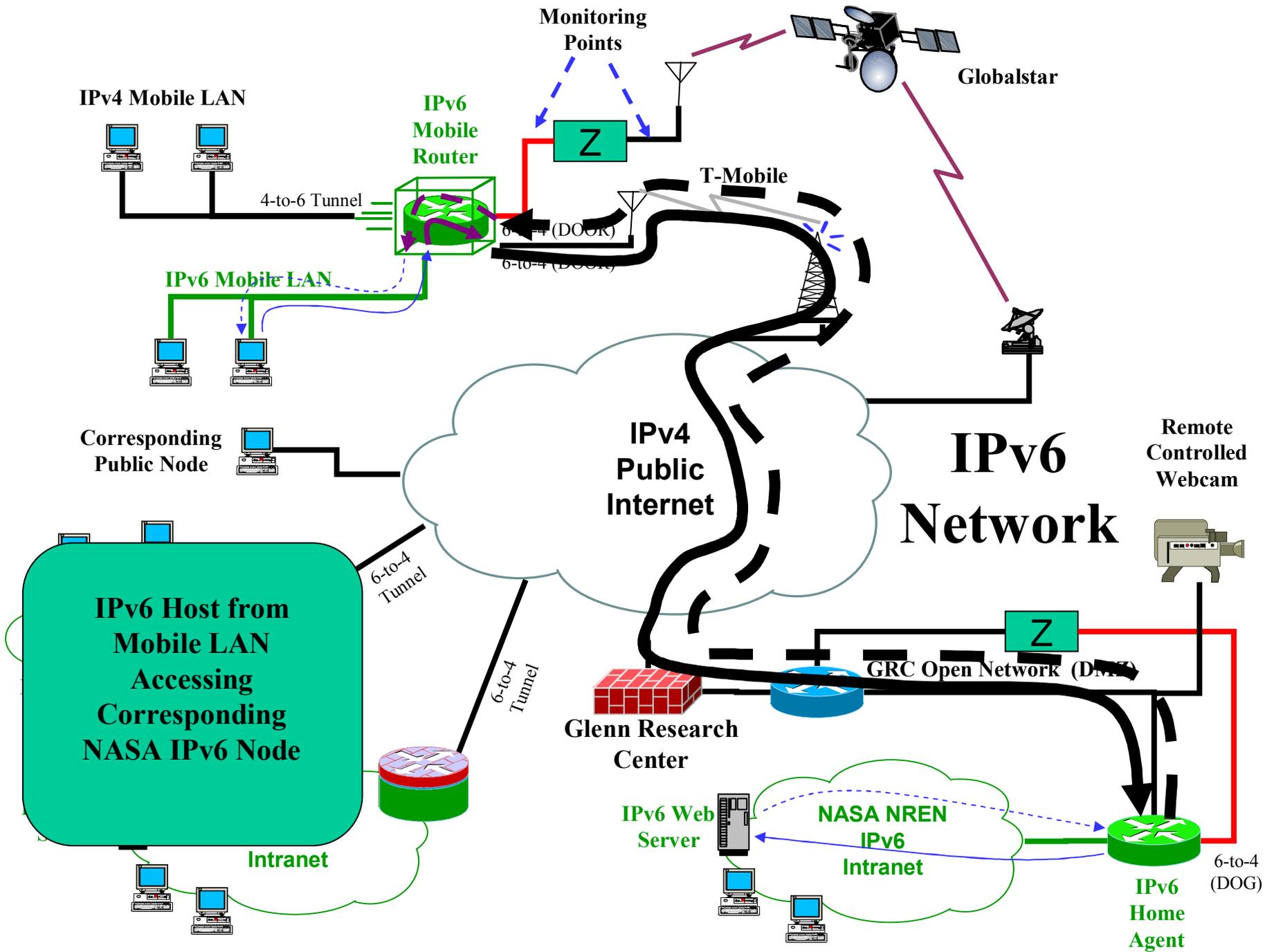


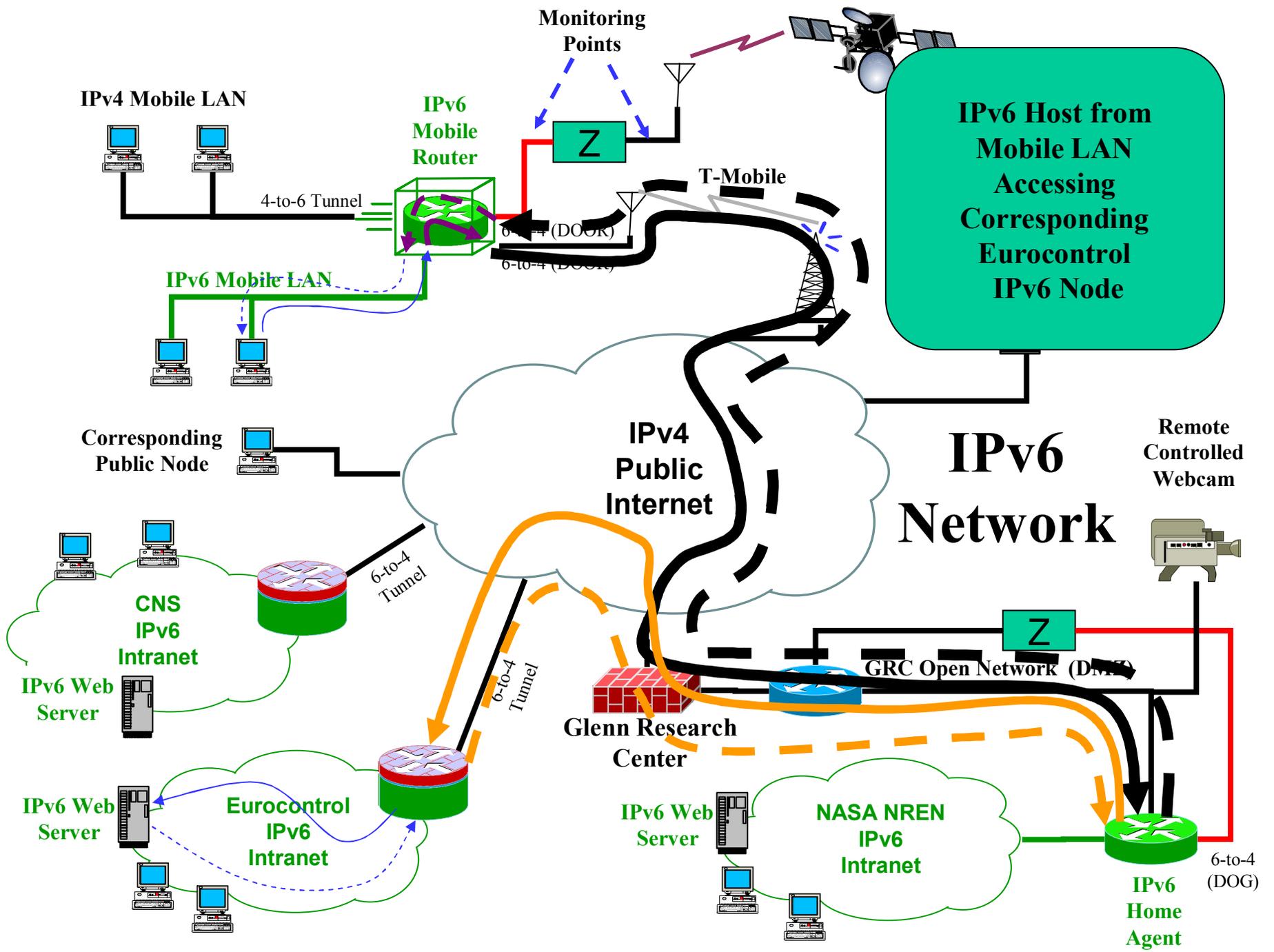


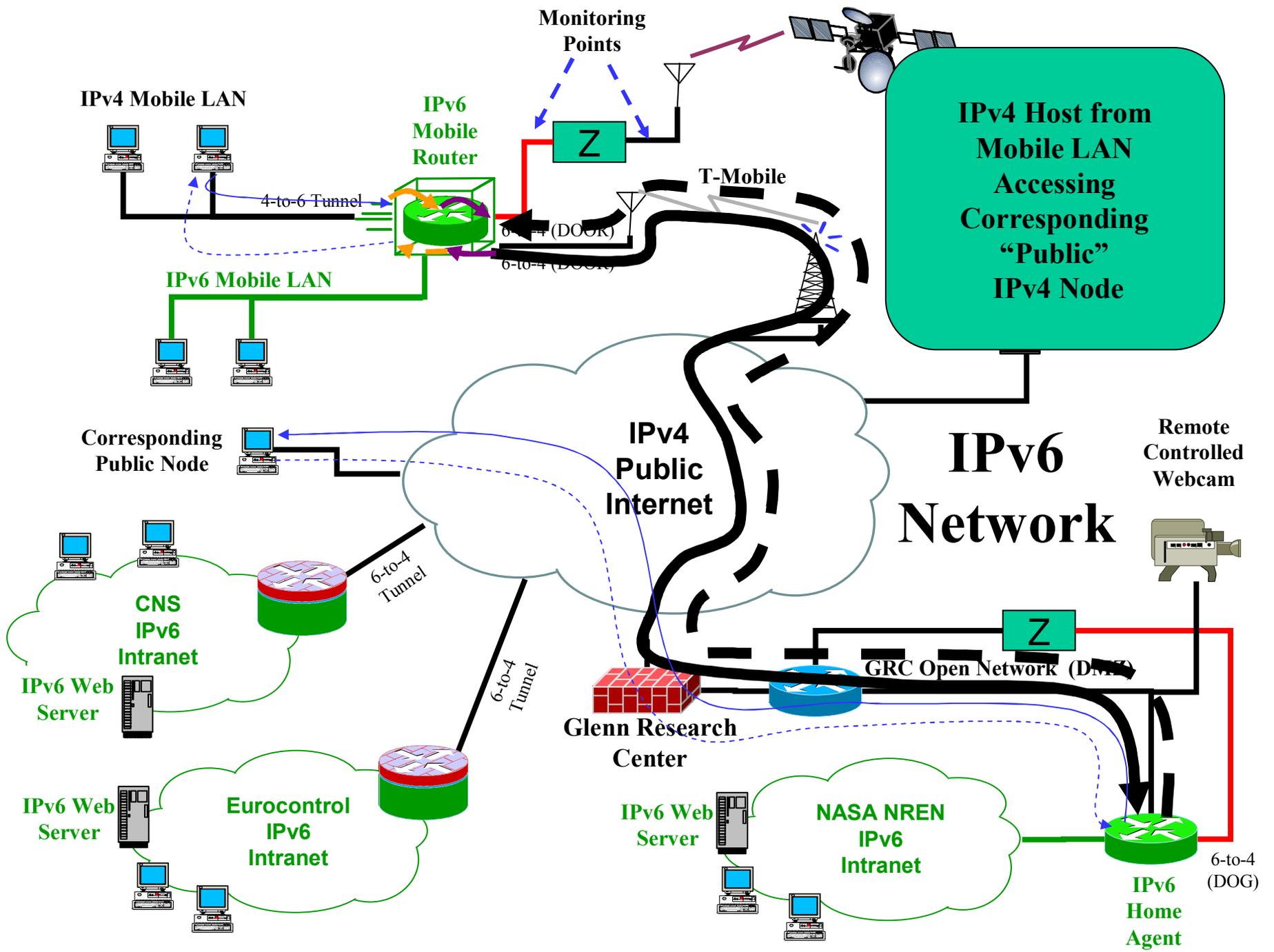
Data Flow Key

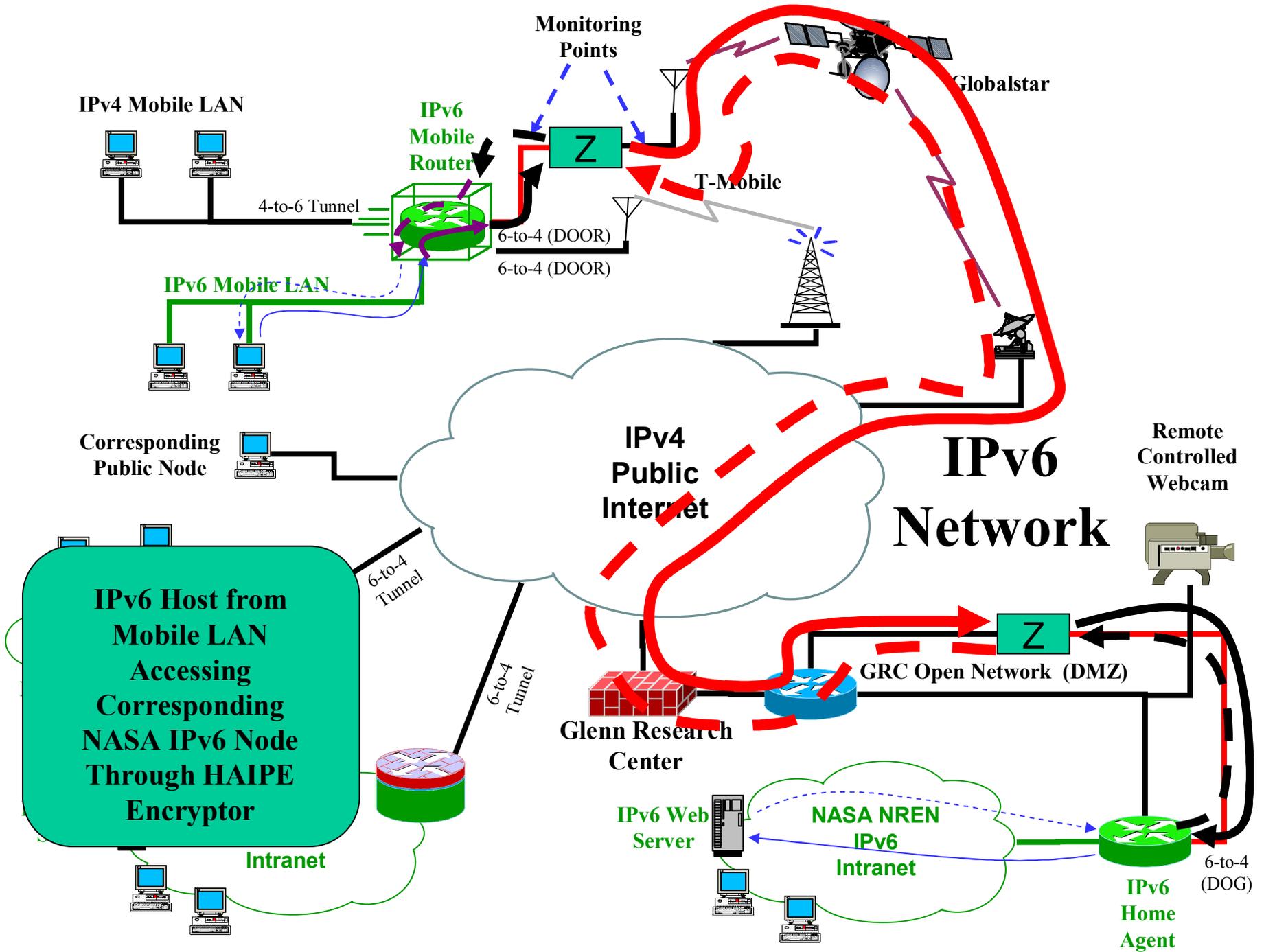


Note, the Secured IPv4 mobile network data passing through the Globalstar network actually experiences five layers of encapsulation: 1) IPv4-to-IPv6; 2) IPv6 Mobile Tunnel; 3) IPv6-to-IPv4 "Door" tunnel; 4) HAIPE encapsulation for encryption; 5) an additional tunnel between the Globalstar Smiths Falls ground station and the Qualcomm facility in San Diego, CA unencapsulated and reencapsulated for transmission to Glenn Research Center through the NAT at Qualcomm.









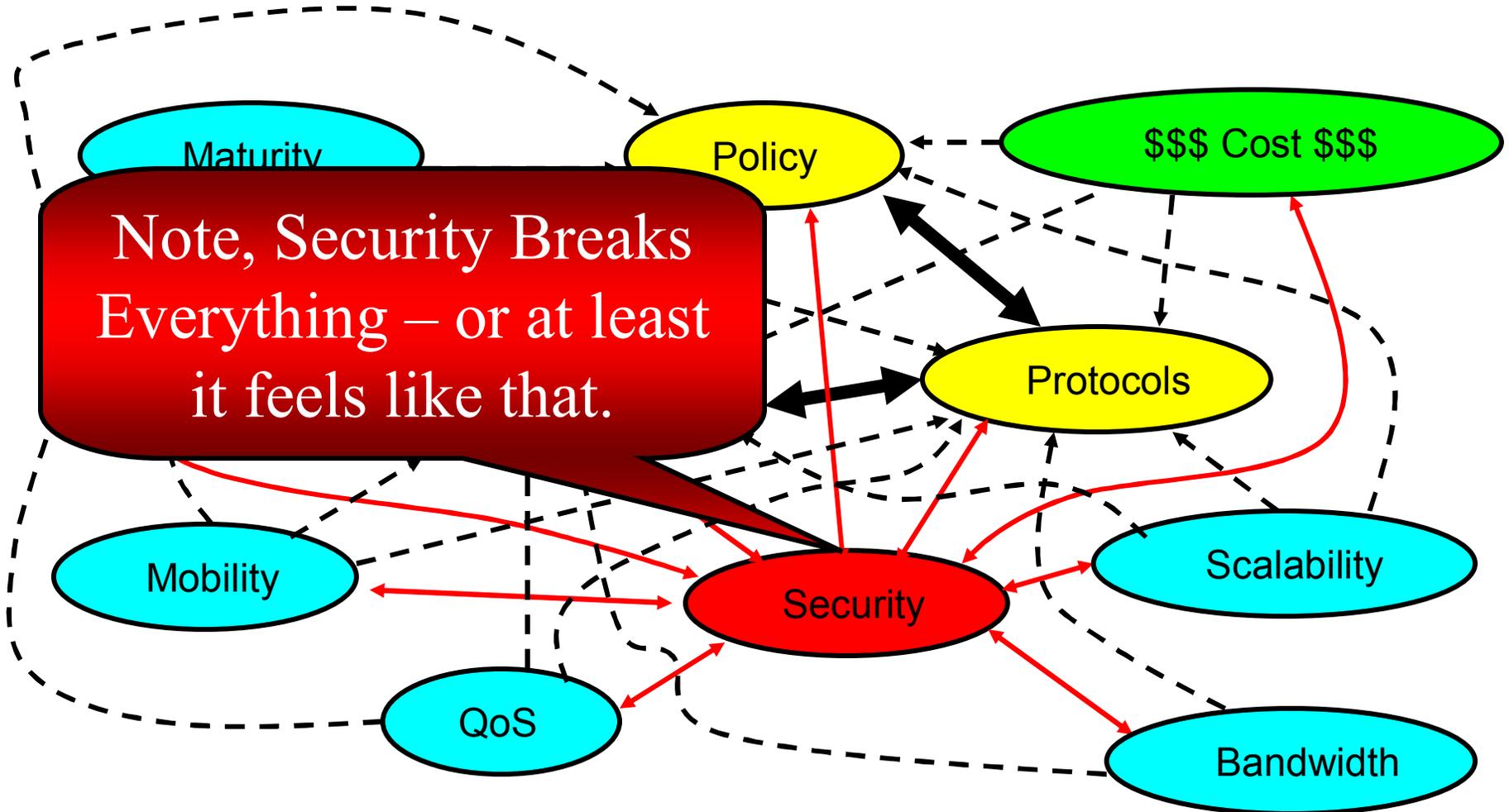


Mobility and Encryption

Issues To Be Addressed



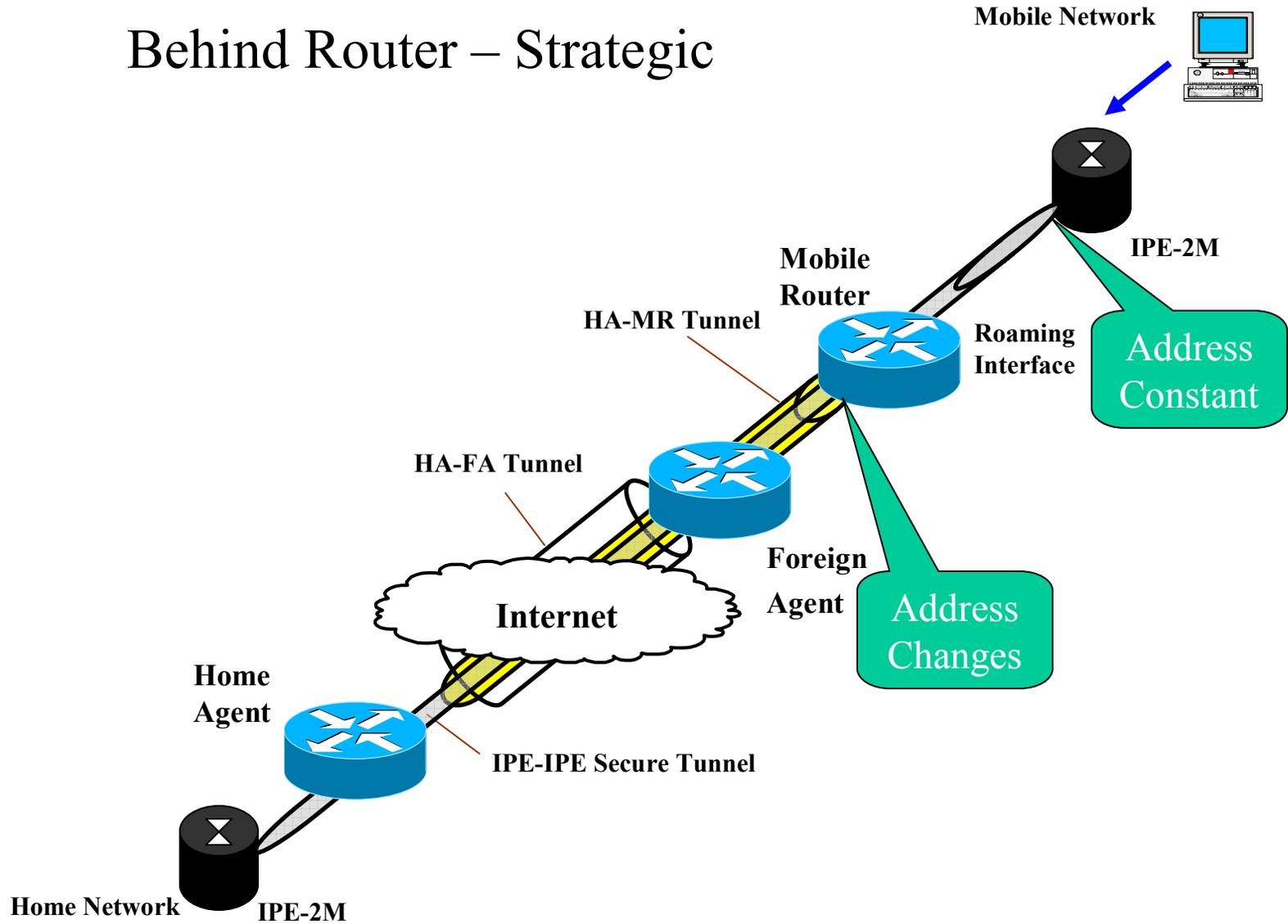
Network Design Triangle





Layer-3 Network Security (Strategic)

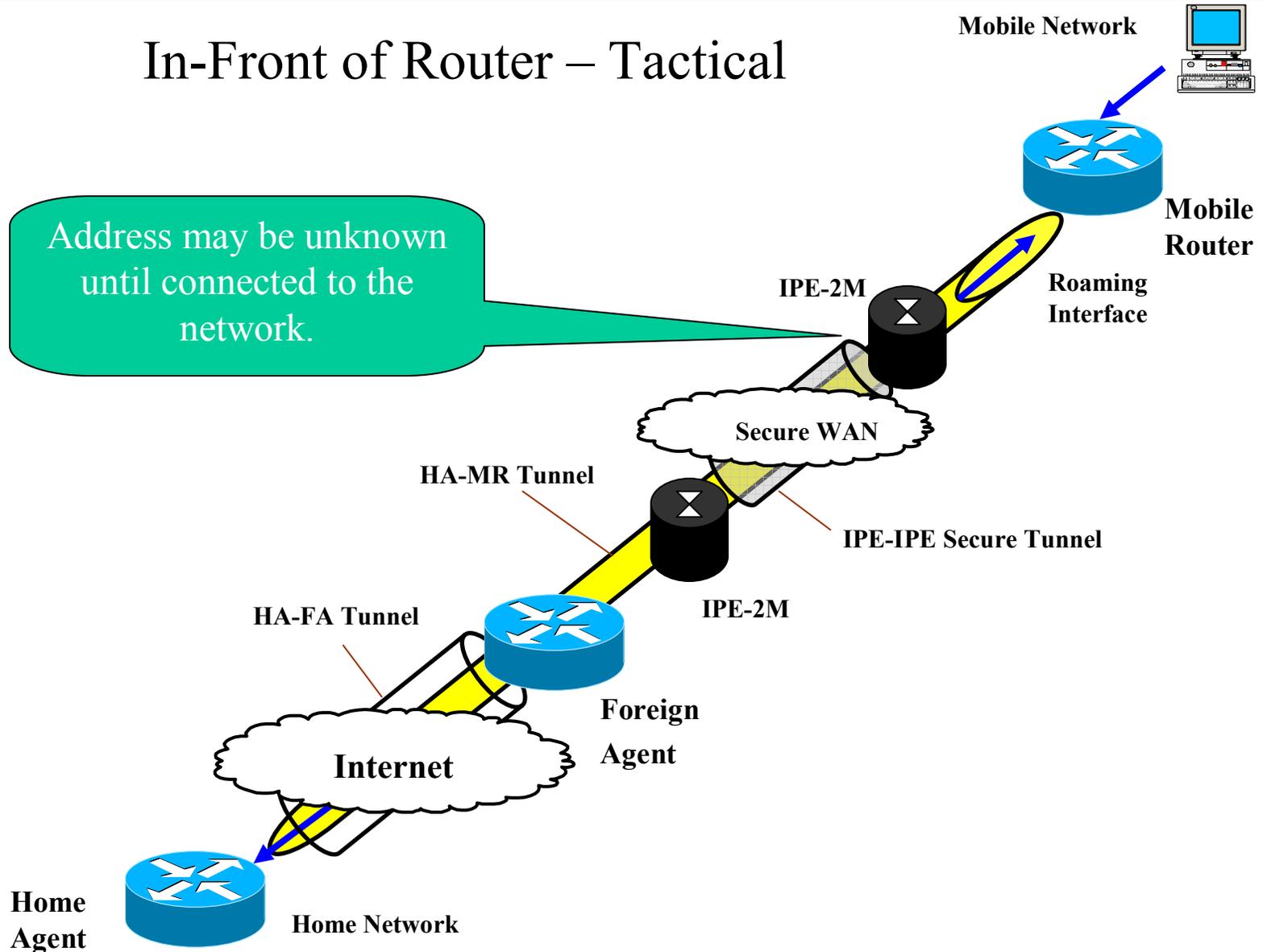
Behind Router – Strategic





Layer-3 Network Security (Tactical)

In-Front of Router – Tactical

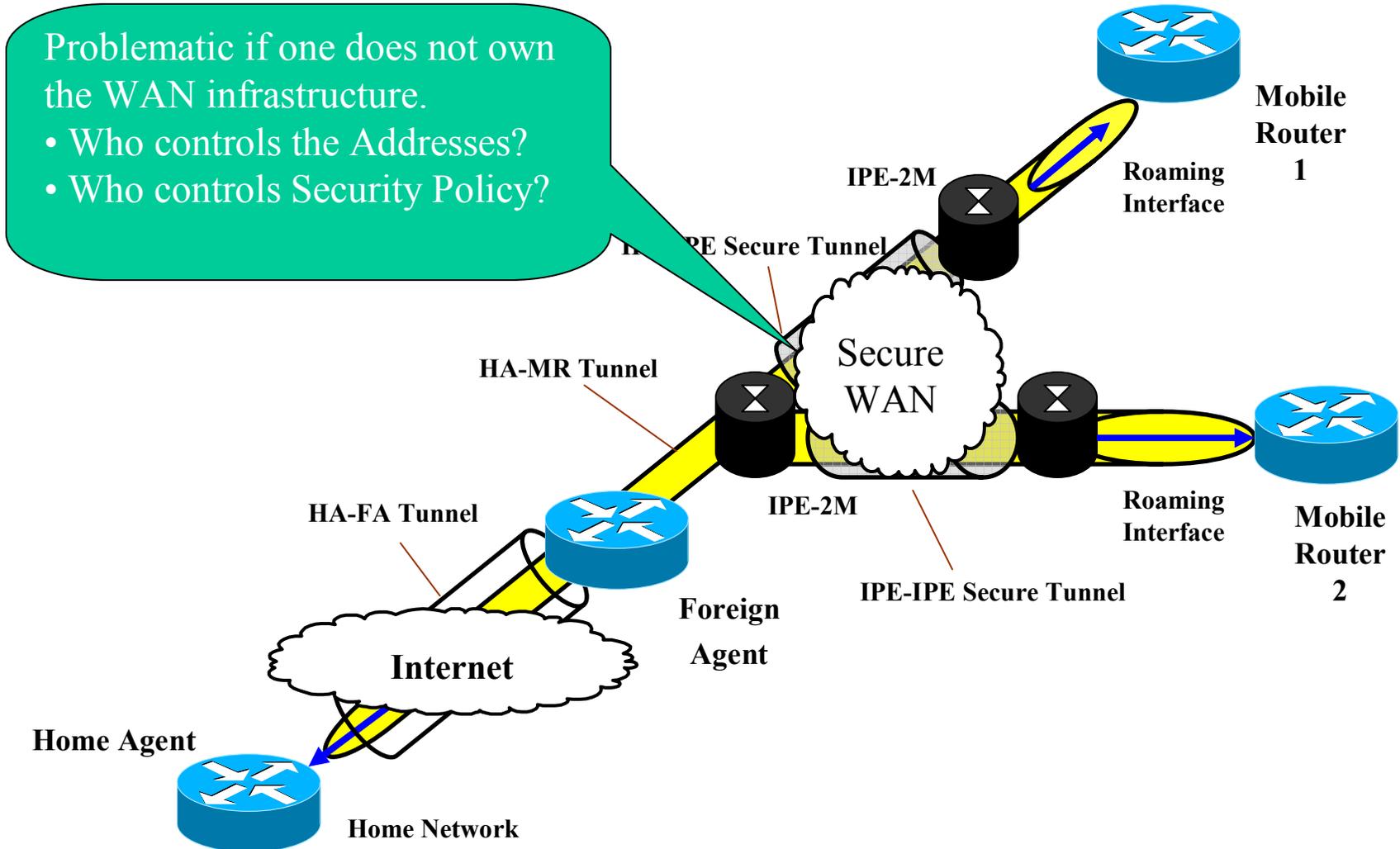




Layer-3 Network Security

(Security Policy in a Non-Static Environment aka IPv6)

Multiple Devices





Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)



Agenda

- Why
- CLEO/VMOC overview
- Participating Organizations
- The Network
- Data Flow
- Timeline of Events
- CLEO/VMOC Lessons Learned
- Future Work
- New Capabilities
- NCO Experiences



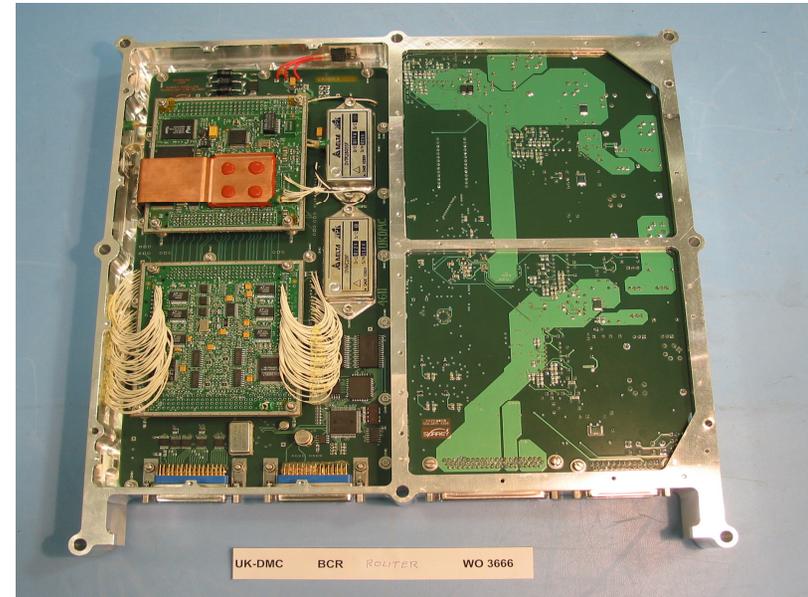
Why?

- Shared Network Infrastructure (Mobile-IP)
 - \$\$\$ Savings
 - Ground Station ISP
 - \$400- \$500 per satellite pass
 - No salaries
 - No health benefits
 - No infrastructure costs
 - System Flexibility
 - Greater Connectivity
 - Relatively easy to secure
- TCP/IP suite
 - COTS Standard
 - Free tools
 - Skilled professionals available
 - Tested via general use by 100s of 1000s daily



The Cisco router in low Earth orbit (CLEO)

- Put a COTS Cisco router in space
- Determine if the router could withstand the effects of launch and radiation in a low Earth orbit and still operate in the way that its terrestrial counterparts did.
- Ensure that the router was routing properly
- Implement mobile network and demonstrate its usefulness for space-based applications.
 - Since the UK–DMC is an operational system, a major constraint placed on the network design was that any network changes could not impact the current operational network



Note: Mobile Access Router is IPv6 capable however that image was not available prior to time of launch.



Virtual Mission Operations Center (VMOC)

Glenn Research Center

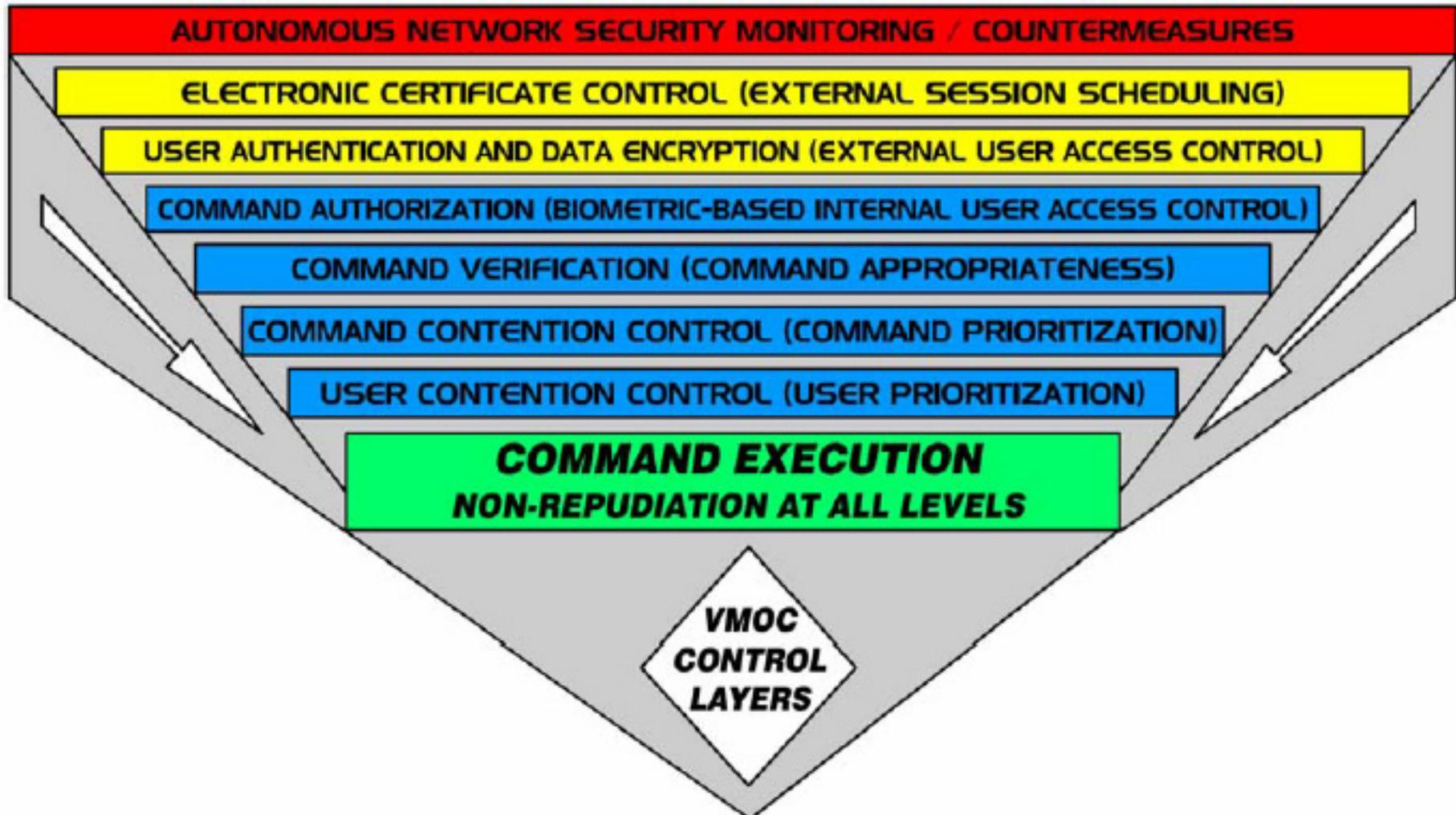
Communications Technology Division

Satellite Networks & Architectures Branch

- Enable system operators and data users to be remote
- Verify individual users and their authorizations
- Establish a secure user session with the platform
- Perform user and command prioritization and contention control
- Apply mission rules and perform command appropriateness tests
- Relay data directly to the remote user without human intervention
- Provide a knowledge data base and be designed to allow interaction with other, similar systems
- Provide an encrypted gateway for “unsophisticated” user access (remote users of science data)



Virtual Mission Operations Center





Mutually Beneficial Interests

- Projects are complementary in their shared use of the Internet Protocol (IP)
- Overall goal of network-centric operations.
 - (and NetCentric Operations)



Participating Organizations

Glenn Research Center

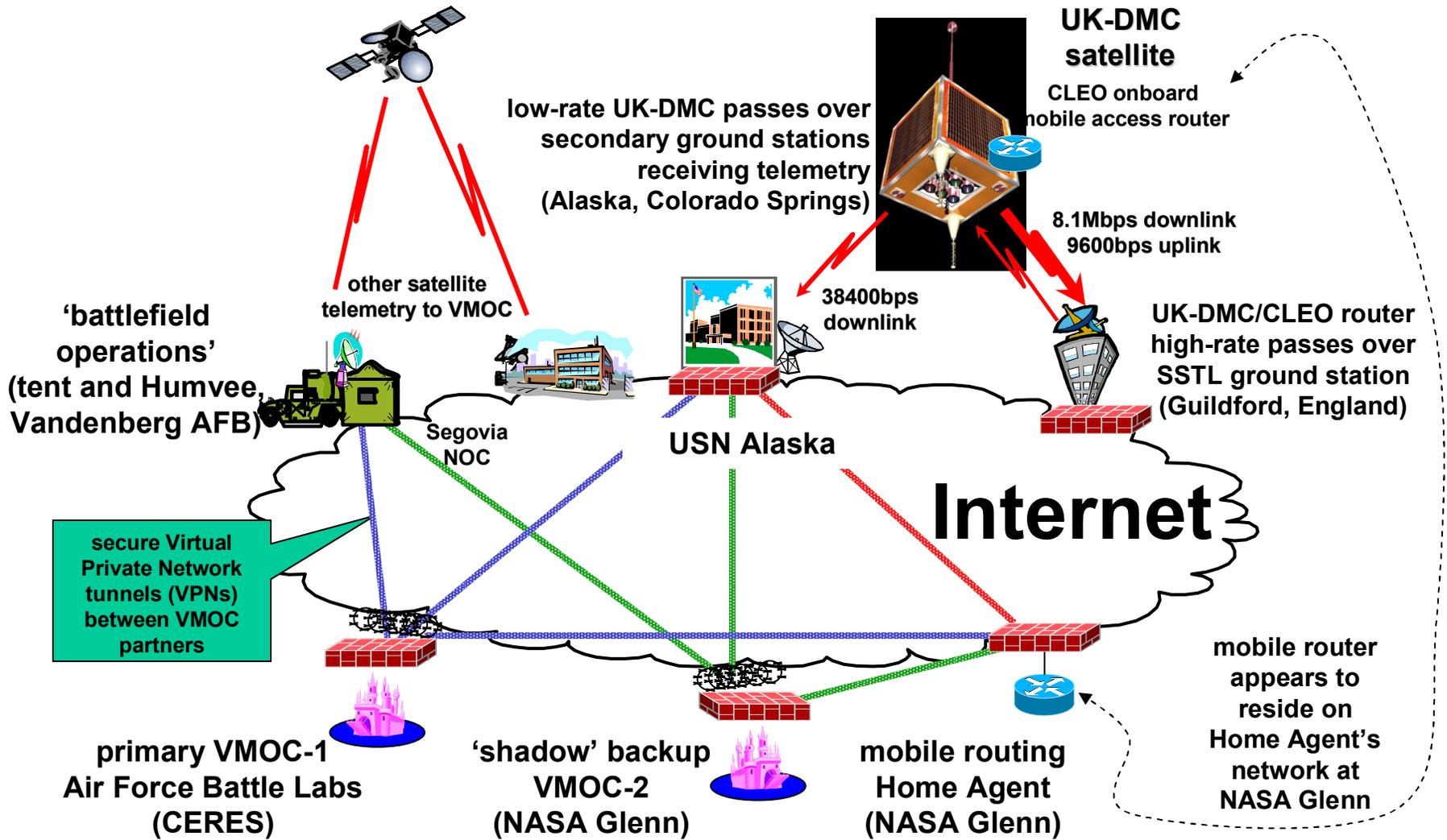
Communications Technology Division

Satellite Networks & Architectures Branch





CLEO/VMOC Network

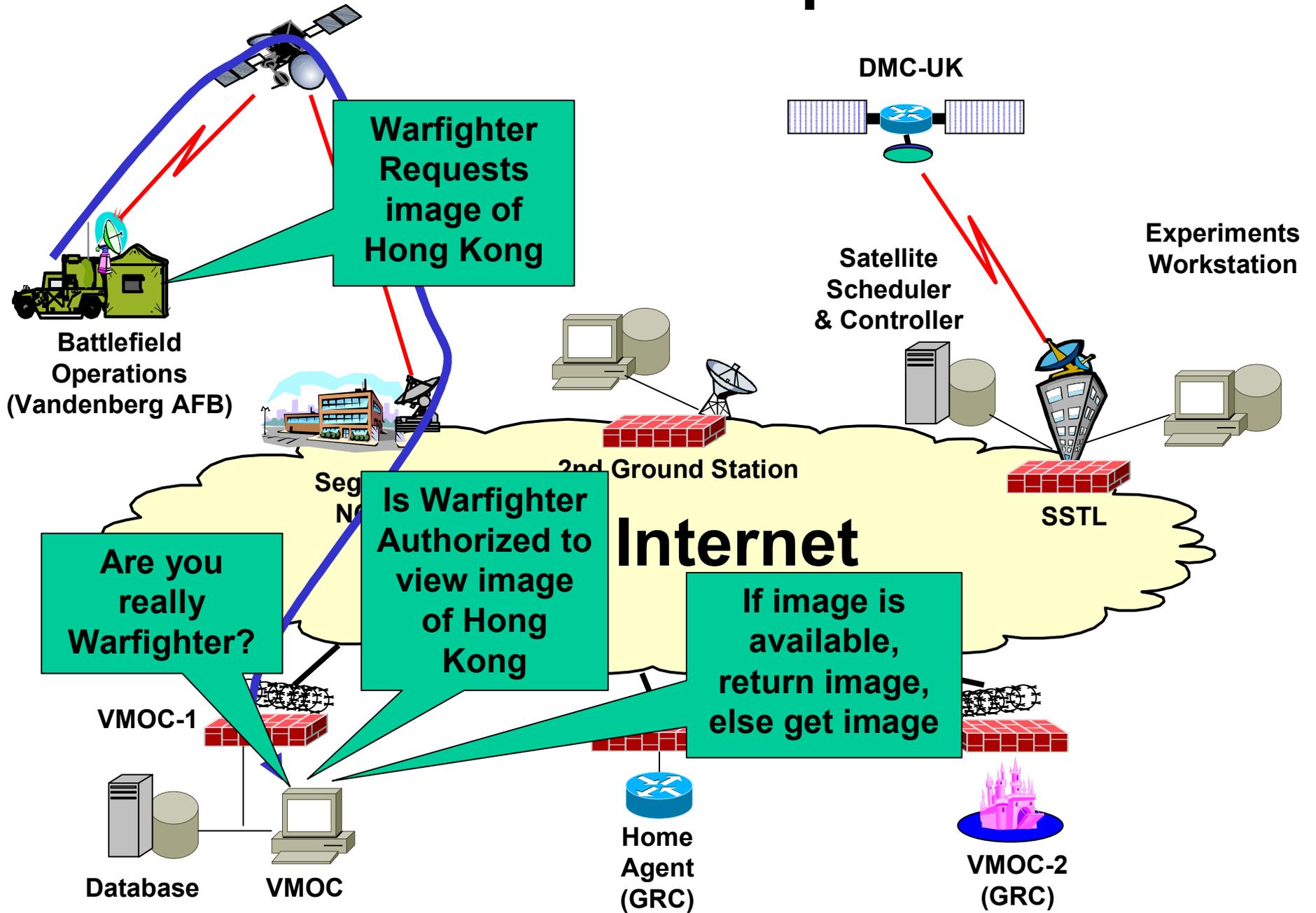




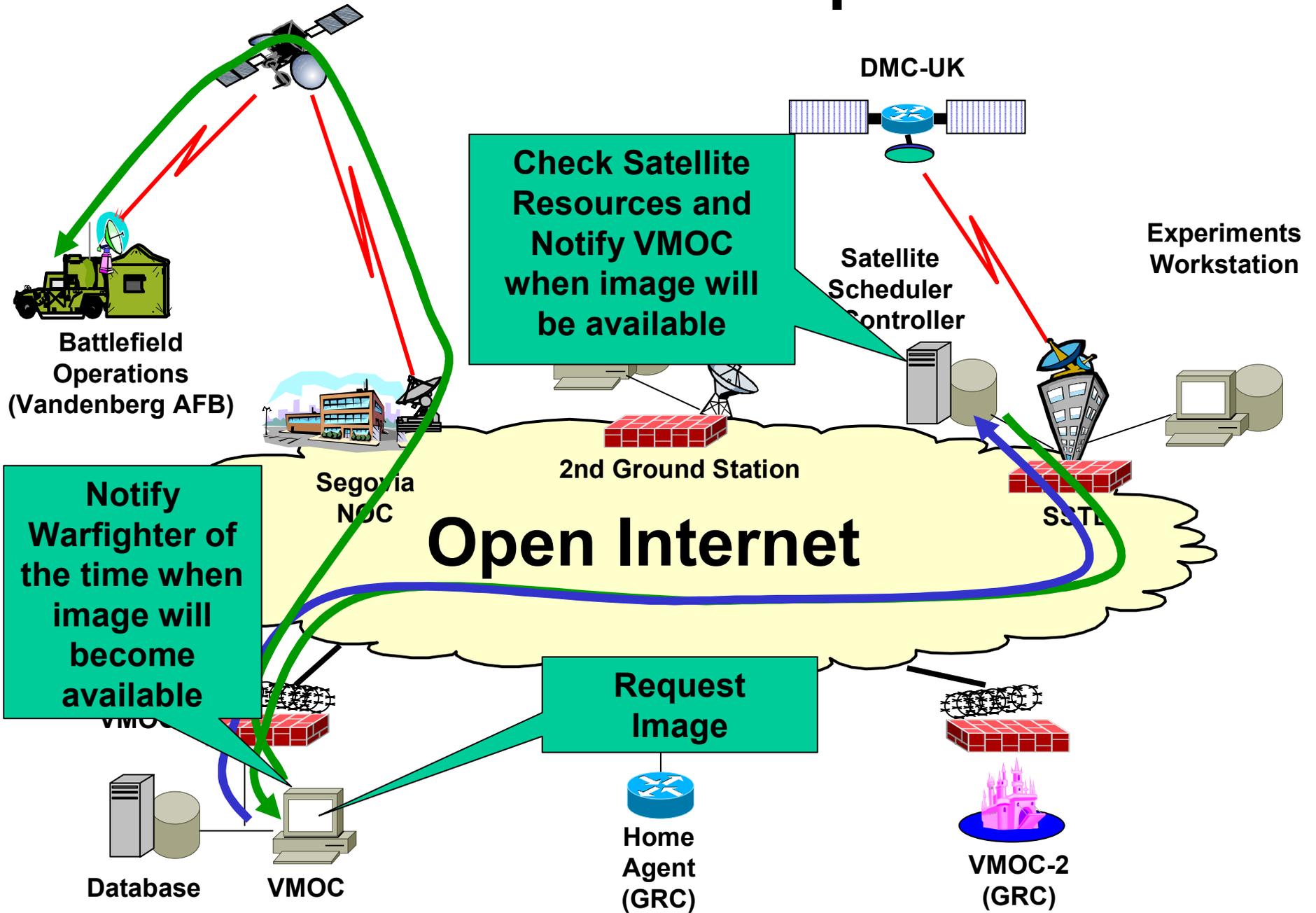
Data Flow

Mobile Router Using Mobile-IPv4 and Triangular Routing

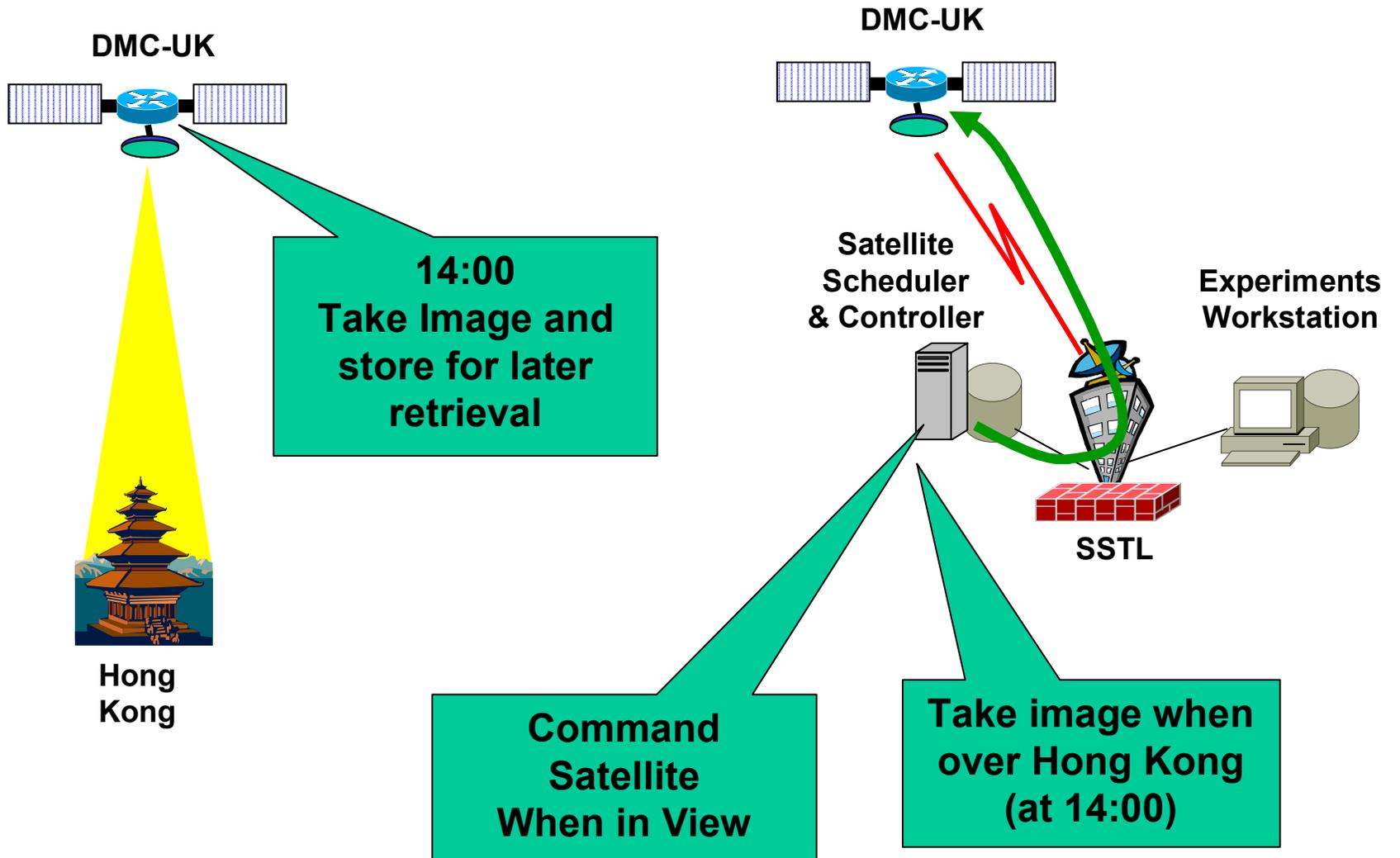
Remote Request



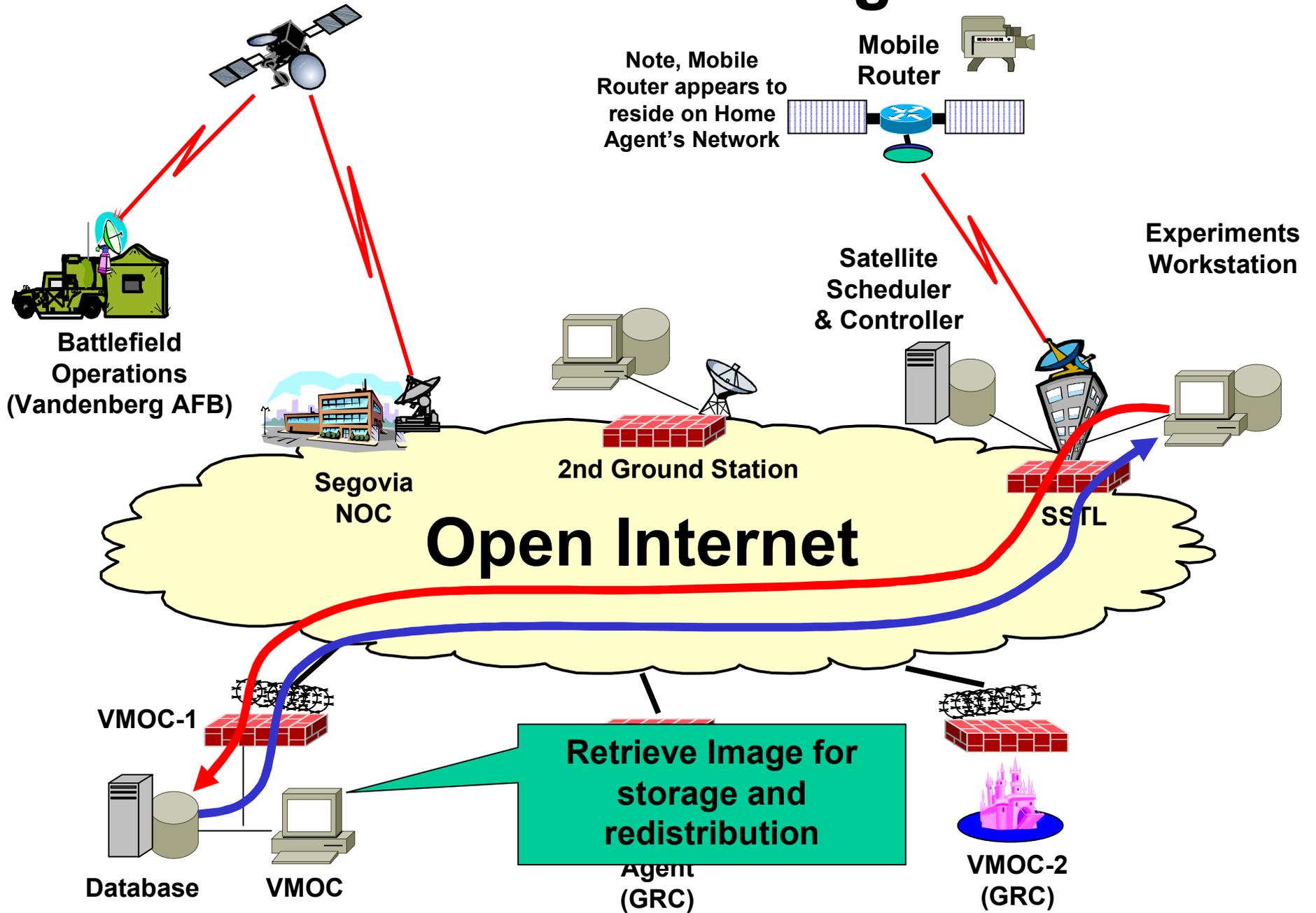
Schedule Request



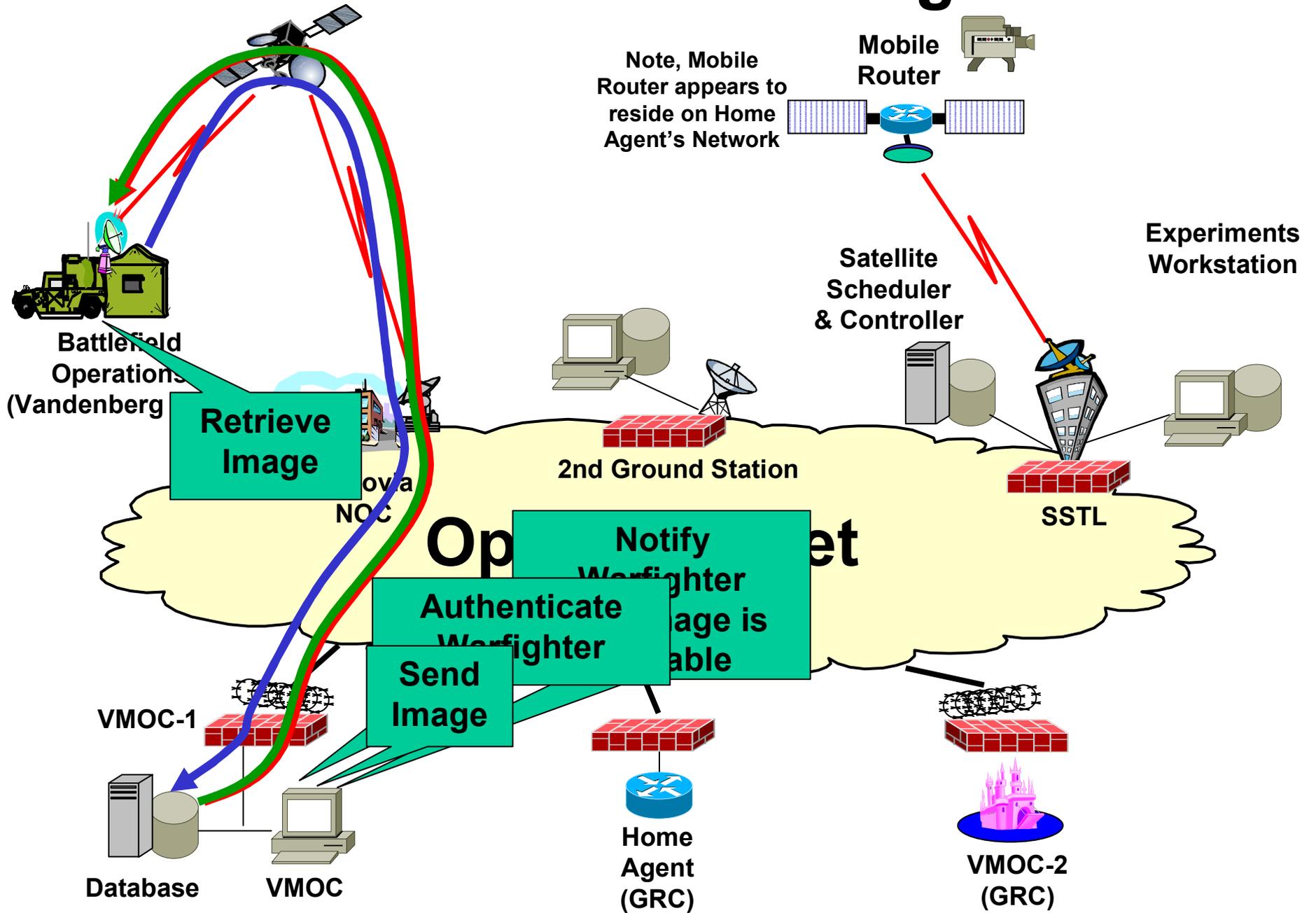
Command Satellite



Retrieve Image



Redistribute Image





CLEO/VMOC Lessons Learned

- **The interface between asset owners will have to be identified and some special software written when sharing infrastructure**
 - Use of commercial standards (IP, Simple Object Access Protocol , XML) make implementing these software interfaces much quicker and easier than if noncommercial standard protocols were used.
- **Mobile networking greatly simplifies network configurations at the ground stations and adds an extremely insignificant amount of overhead (three small packets per session for binding setup).**
- **The ability to have all the tools available in a full IOS on the onboard router proved invaluable**
 - Argument for slimmed-down IOS
 - May be more robust or easier to qualify rigorously for the space environment.
 - Argument for full IOS
 - Removing functionality may result in less stable code rather than more stable code, as any change in software can affect the robustness of software and second.
 - Full IOS has been tested daily by hundreds of thousands of users
 - It is quite probable the functionality taken out will end up being the functionality one needs for some later, unforeseen configuration need.



NCO Experiences

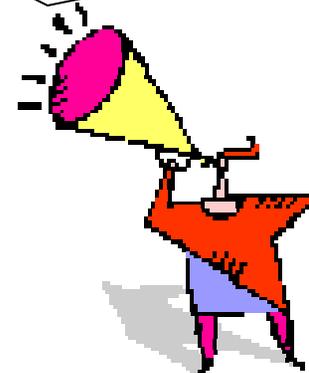
- *Successful NCO has more to do with building trust relationships at the “people level” than it has to do with technology.*
- **Putting NCO in an operational system is the true test.**
 - *This forces ALL security issues to be address!*
- **Internetwork Centric Operations, NCO across various networks owned and operated by various entities if far different the NCO within your own network.**
 - Everybody has to expose themselves to some degree. That degree has to be negotiated up front.
 - I need to understand how your system works and you need to understand how my system works.
 - Strengths and vulnerabilities are exposed to some degree.
 - **Internetworking NCO is like a marriage**
 - **50/50 is doomed to failure. 100% commitment is required by all parties.**
 - You MUST understand and accept the needs of the other parties.
 - Patience and Persistence, Patience and Persistence, and more Patience and Persistence!



The complete technical report and this presentation are available at:

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

We are always willing to bring the demonstration to you, if so desired.





NASA's Request for Comments on the Global Air Space System Requirements

Will Ivancic

wivancic@grc.nasa.gov

216-433-3494



Global Airspace System Requirements

1. Must be value added
 - Cannot add cost without a return on investment that meets or exceeds those costs.
2. Must be capable of seamless global operation.
3. Must be capable of operating independently of available communications link. Must support critical Air Traffic Management (ATM) functions over low-bandwidth links with required performance.
4. Must use same security mechanisms for Air Mobile and Ground Infrastructure (surface, terminal, en router, oceanic and space)
 - Critical ATM messages must be authenticated.
 - Must be capable of encryption when deemed necessary
 - Security mechanisms must be usable globally
 - Must not violate International Traffic in Arms Regulations
5. Must operate across networks owned and operated by various entities
 - Must be able to share network infrastructure
6. Must make maximum use of standard commercial technologies (i.e. core networking hardware and protocols)
7. Must enable sharing of information with proper security, authentication, and authorization
 - Situational Awareness
 - Passenger Lists
 - Aircraft Maintenance
8. Same network must accommodate both commercial, military and general aviation.



Design Concepts

- Must be IPv6 based.
- Must be capable of a prioritized mixing of traffic over a single RF link (e.g. ATM, maintenance, onboard security, weather and entertainment).
- Must utilize IPsec-based security with Security Associations (SAs) bound to permanent host identities (e.g. certificates) and not ephemeral host locators (e.g. IP addresses).
- Must be capable of accommodating mobile networks.
- Must be capable of multicasting
- Must be scalable to tens of thousands of aircraft



Consensus

- IPv6 is *the* way to go, virtually everyone agrees.
- There seems to be consensus that links should be shared, and the system should be provider-independent, and this makes QoS a requirement.
- There is a need for some type of mobile networking (mobile-IP, NEMO, ad hoc)
 - Placement of home for mobile-IP or NEMO is being addressed, but needs further study.
- Everyone agrees that some work is still to be done cleaning up IPsec multicast, envisioning the certificate architecture, and figuring out how exactly to do QoS.



Value Added

- Lower Telecommunication Costs of IP-based networks as compared to dedicated point-to-point links
- Competition among information providers
- Economies of scale
- Lower development costs for new applications and maintenance due to standardization of interfaces



Link Independence

- Most important considerations for this is not technical, but related to cost, safety, and politics
- Facilitates globalization and supports positive ROI
- Requires change in policy 
- Change in use of spectrum
 - World Radio Conference to allow use of other frequencies for air traffic control messages
- Air Traffic Controller is now networked.

These are some very different modes of operation from what the aeronautics community is comfortable with.



Security Mechanisms

- Encryption mechanisms should be limited to those that are free of ITAR restrictions
- Other countries also have regulations restricting the exportation of cryptography technology
 - These regulations may limit the ability to realize cost and schedule advantages that could be gained by using a single set of proven security infrastructure software throughout the world.
- Multicast and *current* IPSec implementations do not necessarily work well together.
- Support for IPSec-base security with Security Associations bound to permanent host (multicast group) identities (e.g. certificates)
 - Location, control, and responsiveness of the authentication authority servers is critical.



Significant Comments

- IPv6 improves interoperability between Civilian, Military and Homeland Security portions of the GAN
- Any future GAN will need to exceed the current network capacity, and reduce operational cost while meeting system safety and passenger needs in order to justify its cost.
- Message delivery costs were a contributing factor to the FAA's decision to terminate CPDLC operations at the Miami ARTCC.
- Need assurances that mixing ATM messages with general Internet traffic on public networks does not introduce unacceptable hazards.
- Scalability is an absolute requirement for a global solution



Further Studies and Investigation

- QoS related to mixing ATM traffic with other information
- Much research is needed regarding network mobility
- Networking ATM traffic for use over multiple links and service providers
- IP over narrow-band aeronautical links.
- Mobile-IP, NEMO and Ad Hoc networking
 - Route Optimization
 - Placement of Location Manager (Home Agent)
 - Ping-pong routing
 - QoS and delay issues
 - Multi-homing (use of best available link)
 - To load balance or not to load balance?
 - Make before break or not?
 - Policy-based routing (current aeronautical requirement - Ouch!)? 
- Application of Ad Hoc type networking for Oceanic to extend networks (MANETs or Mobile-IPv6)