

# Evolution IPv6 U.S. China IPv6 Global Summit Beijing, China April 12-14, 2004

Jim Bound

Chair North American IPv6 Task Force [www.nav6tf.org](http://www.nav6tf.org)

Chair IPv6 Forum Technical Directorate [www.ipv6forum.com](http://www.ipv6forum.com)

Hewlett Packard Fellow

[Jim.Bound@nav6tf.org](mailto:Jim.Bound@nav6tf.org)

# Discussion

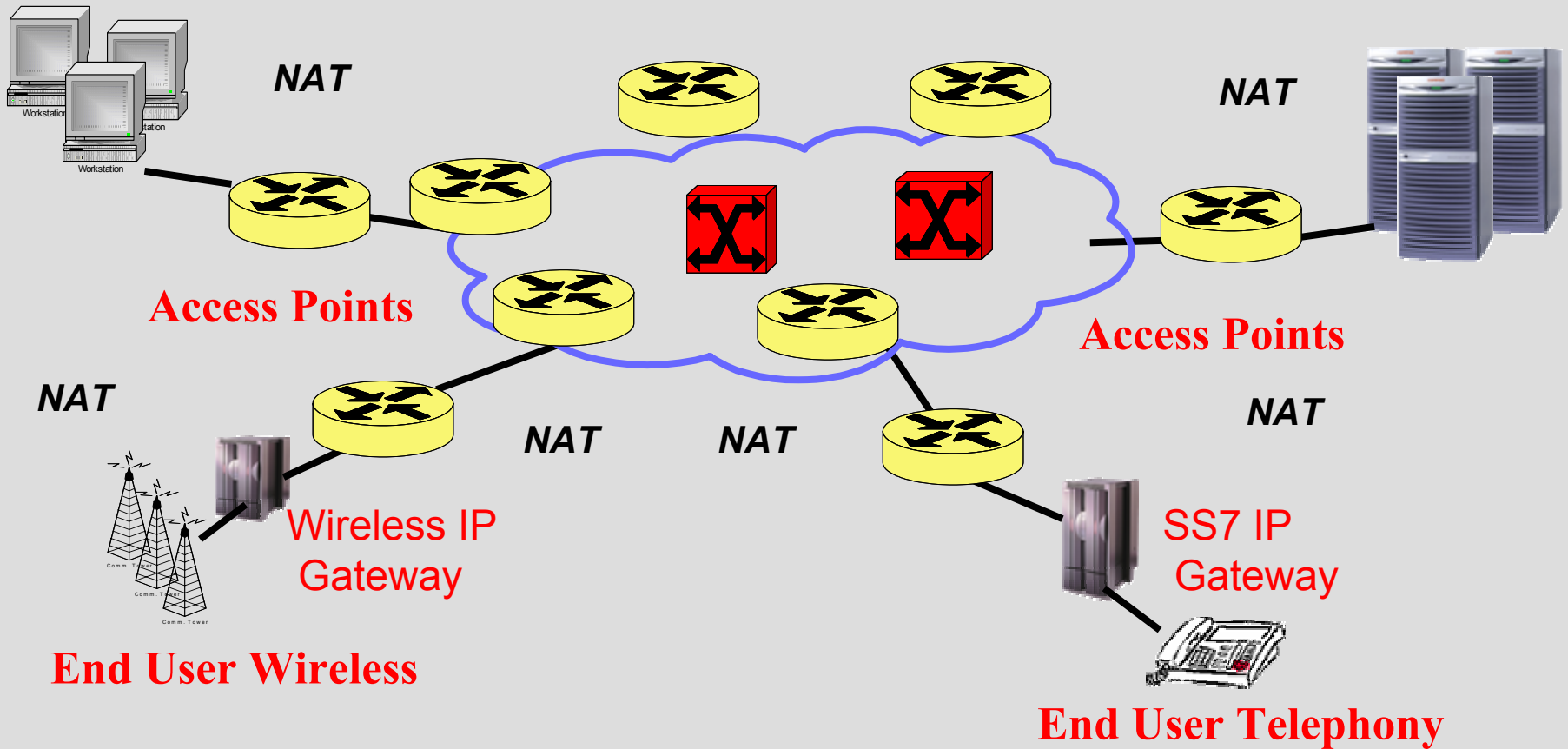
- The Internet Eco System
- Deployment Evolution and Effect
- Update on Moonv6 Network Pilot
- Next Steps for Deployment
- North American IPv6 Task Force

# Internet Access Today

**End User Wireline**

**Internet Edge and Core**

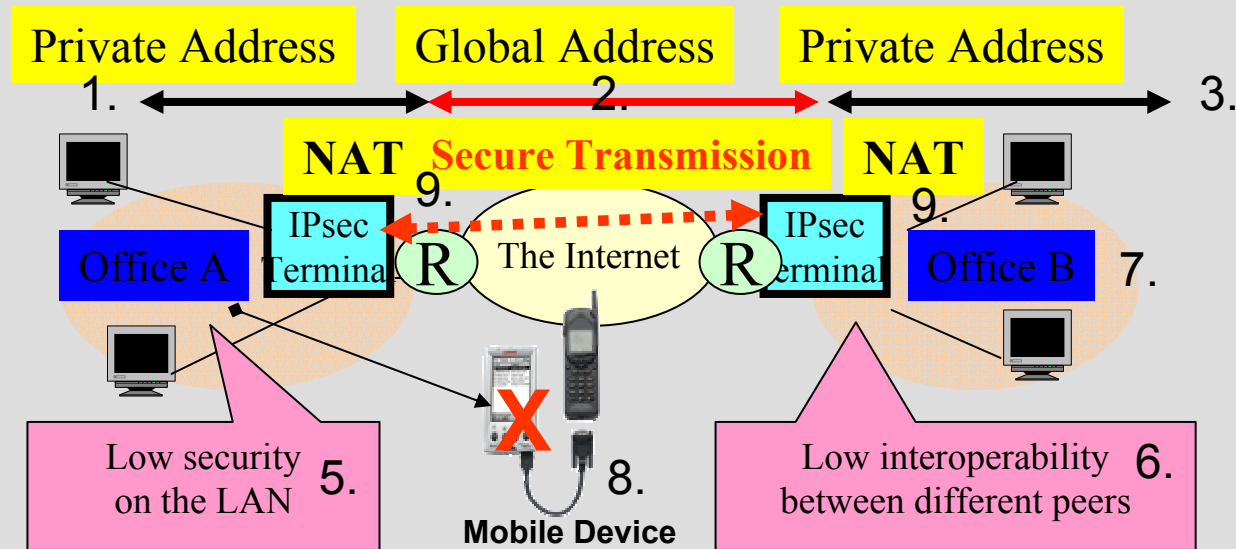
**Internet Services**



# Cost of IPv4 NAT

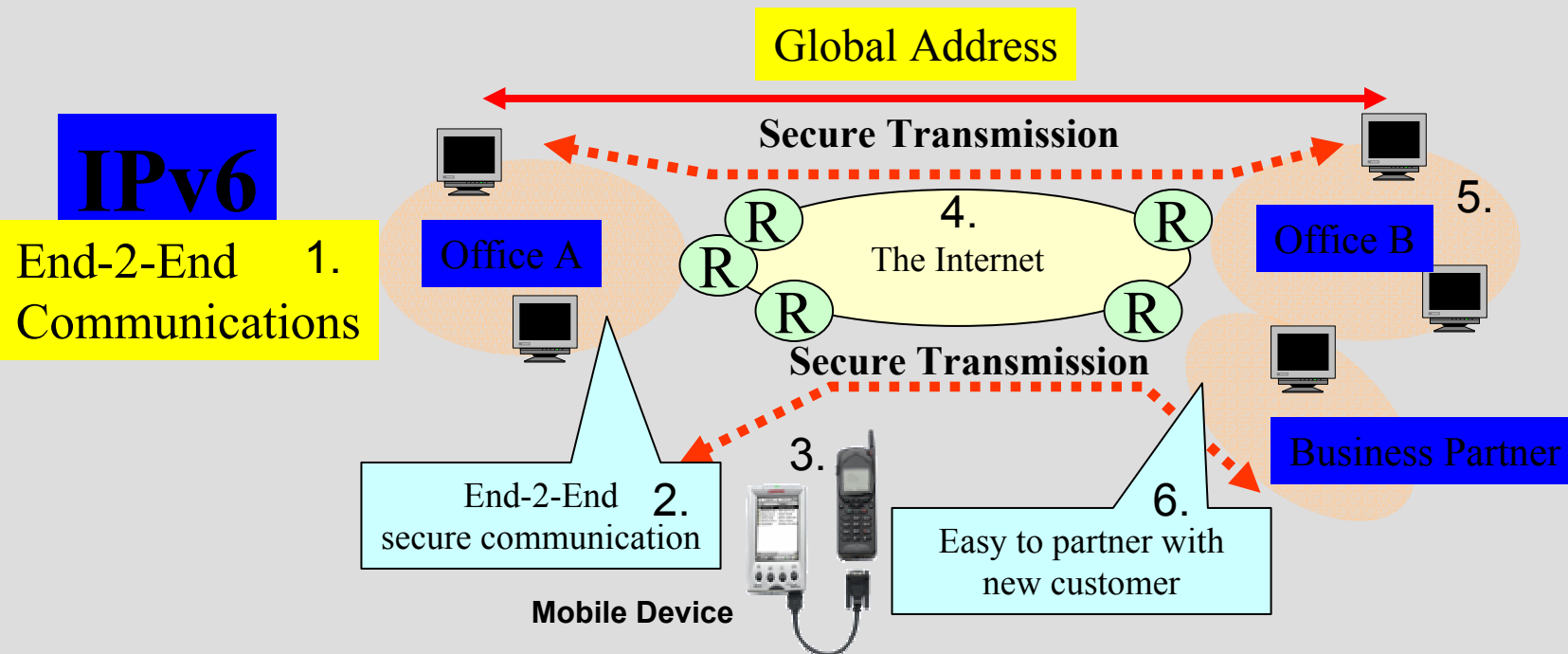
## IPv4-NAT

Site-to-Site  
Secure  
Communication



1. Node can only communicate out of site with peer through a NAT and has reduced capability of applications.
  2. Communications has only one entry point to Office A node through one router and single point of failure.
  3. Attacker only has to masquerade the packet between the NATs and they will be able to enter either network.
  4. Peer-to-Peer communications and security can only be done within a site behind a NAT.
  5. Security on the LAN is only by NAT once attacker gets passed the NAT it can attack a node on any LAN.
  6. Interoperability between peers out of the site, suppliers, partners, or other vendors has greater cost, if even possible.
  7. A node not within the site cannot initiate a connection with a node behind a NAT site reducing communications.
  8. Mobile Nodes cannot roam out of a site with a private address because it does not exist out of the site.
  9. NAT state for translation, namespace, security, and routing must be maintained at all entry/exit points to the network.
- All of these points are a cost to an entity deploying networks who need for their business or operation to communicate out of the site to peers or applications. Not being able to perform communications and not having true security associations with peers out of the site for one-way communications has a significant cost. Each of these points also causes extra software and state to be maintained and administered by the network operations within the entity.

# Profit from No-NAT



1. End-2-End communications permits nodes to communicate in the site or out of the site without NAT additions.
2. End-2-End security methodology and architecture permits pervasive security in the site, and out of the site.
3. Global Addresses and End-2-End communications and security permit nodes to roam and be mobile out of the site.
4. Entry into to out of the network does not have to be a single point of failure and provide redundancy and failover.
5. A node in another site can initiate a peer-2-peer communications session with a node in another site.
6. Partners, Suppliers, or Applications can now be accessed as peer-2-peer nodes or applications.

Profit from No-NAT can be realized with greater application support and availability which cannot run in a NAT Environment, communications with peers can be initiated by a site or peers out of the site, security is based on security within the node and provides End-2-End secure communications trust and privacy model, and the business options are greater for communications and the cost of managing all the NAT state is removed.

# Secure and Mobile Internet Eco System

**Internet Access Operations**



**Intranet Provider and Enterprise Operations**

**Enterprise Applications and Network Infrastructure Services**

**Distributed Server Operations supporting Grid Services**

**Secure Server Operations (e.g. IPsec, TLS, PKI, AAA, Firewalls)**

**Network Management and IPv4/IPv6 Coexistence with legacy applications**

**Internet Provider Operations**

**Internet Application Services Internet Core and Edge**

**Internet Core/Edge**

**Server Application Access to Internet Core and Edge Nodes**

**Network and Applications Points of Presence**

**Network and Applications Support Infrastructure**

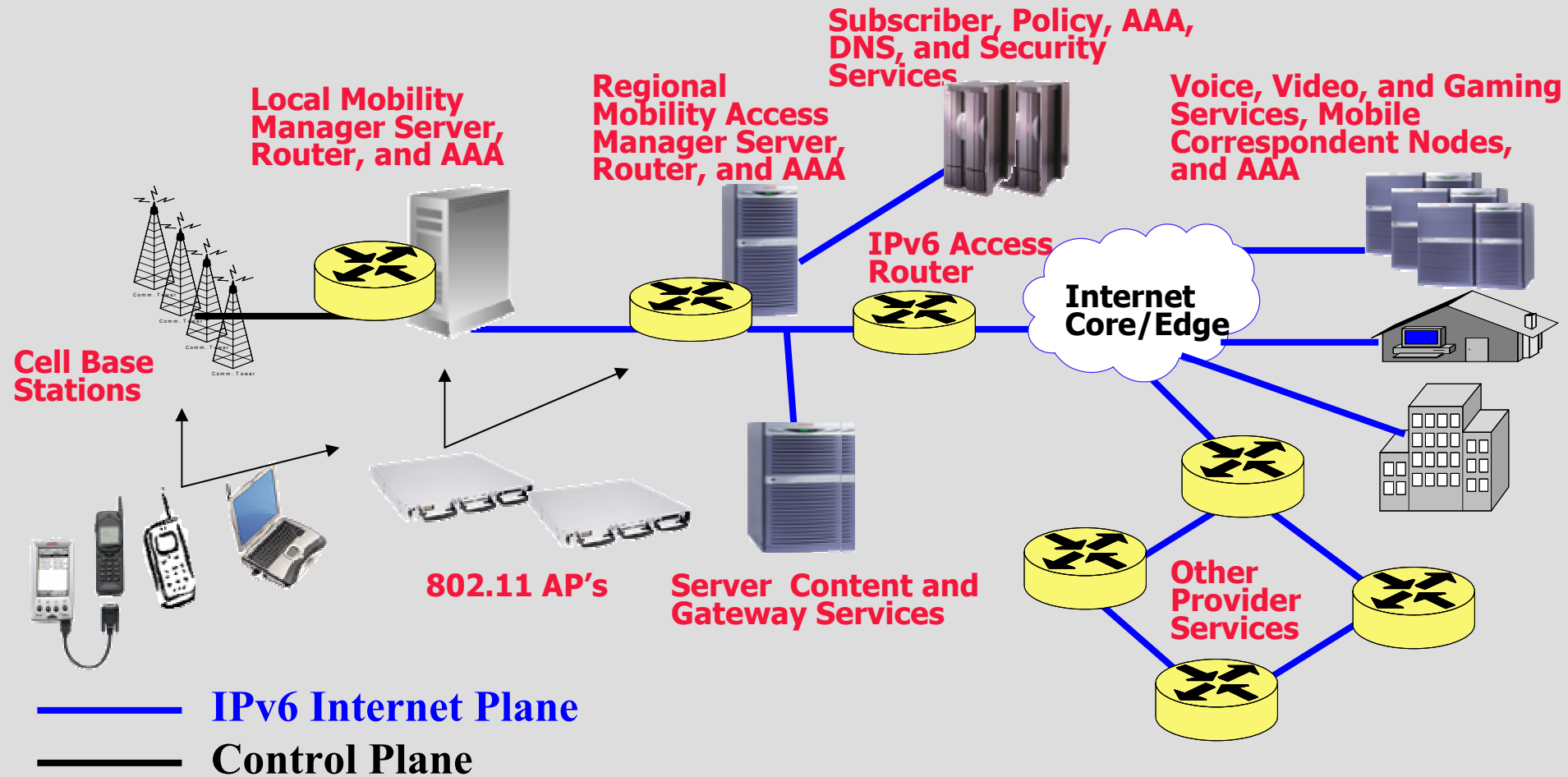
**Server Application Access to Internet Core and Edge Nodes**

**User Operations and Network Interface.**

# Prioritization of core IPv6 Advantages

- Restoration of the End-2-End (E2E) Internet Model (No NAT)
- Larger IP Address Space
- Stateless Autoconfiguration
- Mobile IPv6
- Mandatory IPsec Requirement for Nodes
- There are many other technical, operational, and business advantages ...

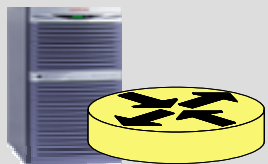
# IT IPv6 Evolved Infrastructure



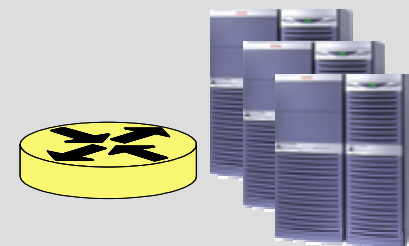


# WLAN IPv6 Mobile Wireless

**Mobile IPv6 Home Agent  
and AAA Server**



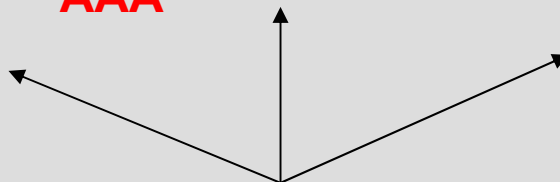
**Correspondent Nodes  
and Services and AAA Client**



**AP and AAA Context**



**IPv6 WLAN Local or  
Regional Mobility  
Manager, Router, and  
AAA**



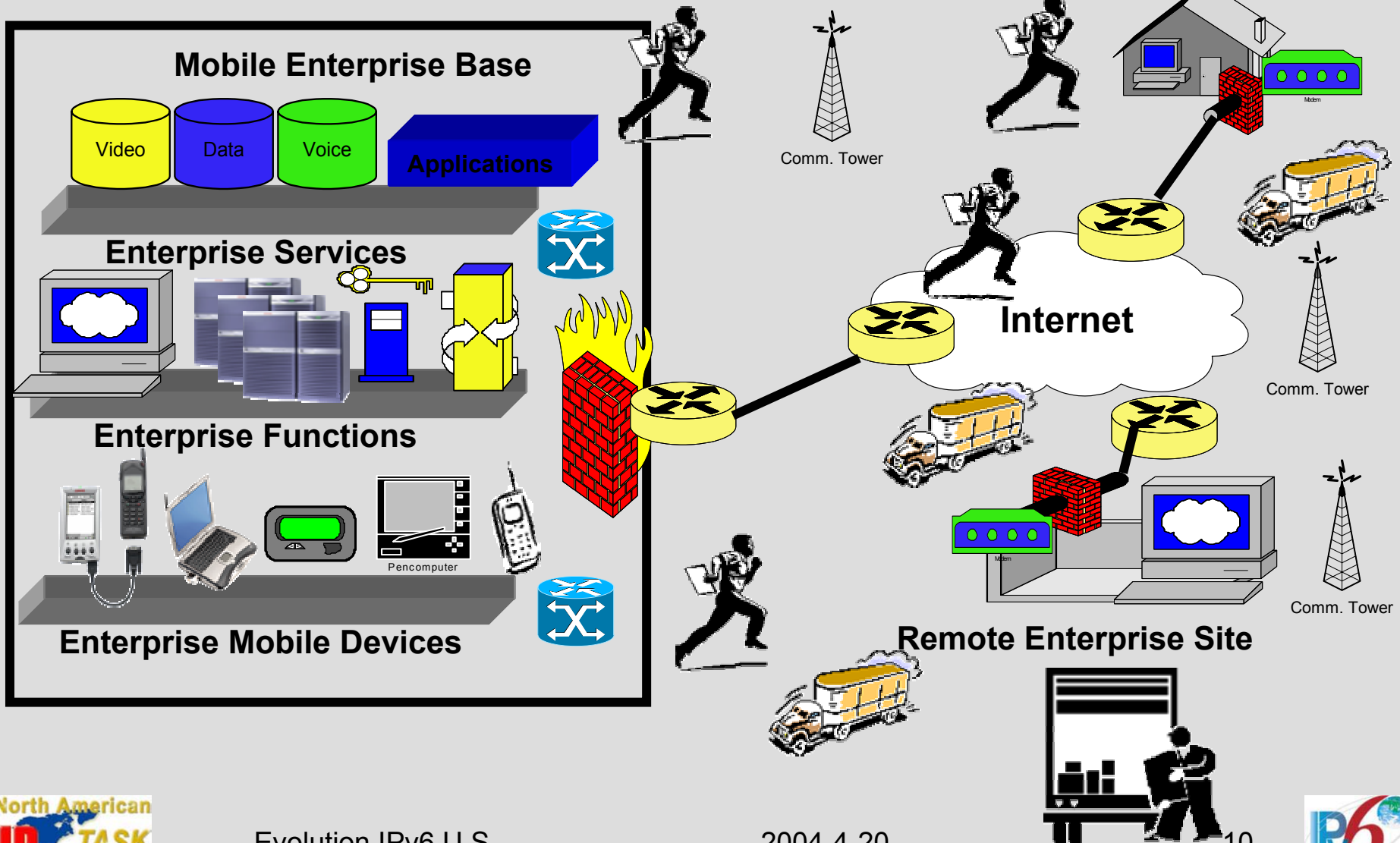
**AP and AAA Context**



**Mobile IPv6 Stations  
Voice and Data Roaming**

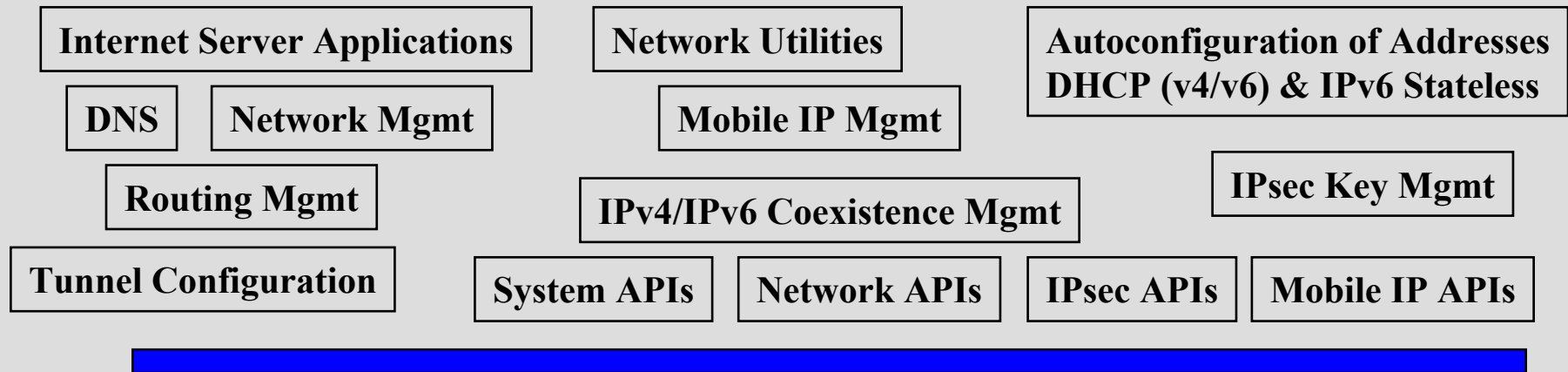
**Mobile IPv6 Stations  
Voice and Data Roaming**

# IPv6 Enterprise Network Mobility

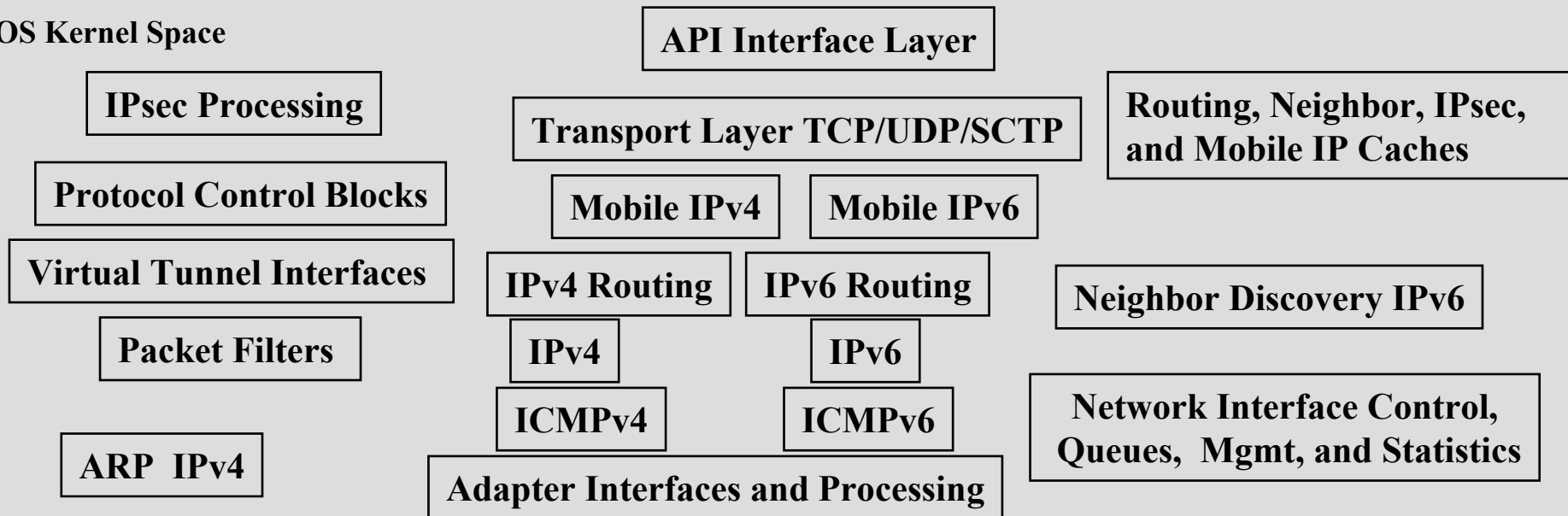


# IPv4/IPv6 Dual IP Layer Protocol Hybrid Stack Approach to Deployment

OS User Space



OS Kernel Space



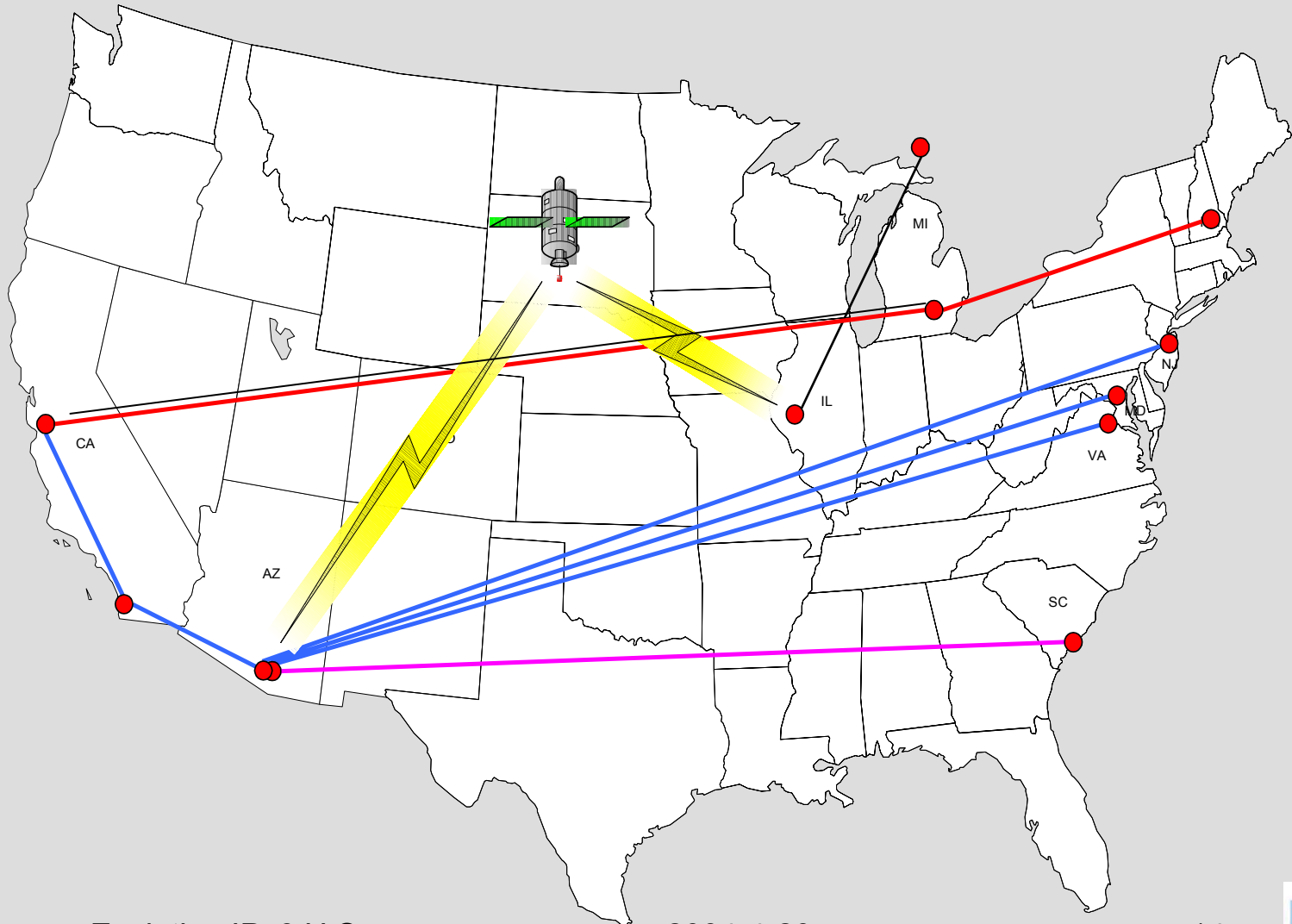
# IPv6 Deployment Revenue Opportunities

- U.S. Government agencies adopting IPv6.
- U.S. Government suppliers to support IPv6 efforts.
- Evolution of Wireless Providers and “True” Internet enabled Mobile Devices.
- IPv6 and the Net-Centricity requirement for an End-2-End Secure Network and Mobile Infrastructure within Enterprises.

# Moonv6 Network Pilot

- Site peering Native IPv6 network across U.S. and other sites world wide.
- Each Site is a portal to the Moonv6 virtual site peering network.
- Site peering can include any geography.
- Moonv6 vision is to evolve to a pre-production IPv6 network enabler.
- Moonv6 status and evolution  
[www.moonv6.org](http://www.moonv6.org)

# Moonv6 Participating Sites



# IPv6 Deployment Road Map

**Core Standards Defined  
1993-2000**

**Initial Network Pilots on Internet and Labs  
1996-2000**

**Evolving Dejure + Defacto  
Standards, Features, & Models  
2000-????**

**Base Network Products and Platforms Ship in the Market  
2000-2003**

**RFP's, Requirements Definition for IPv6, Moonv6  
2003-2007**

**Internet Service Providers begin Infrastructure  
2004-2007**

**Applications Development Heterogeneous Platforms  
2004-2006**

**Complete IPv6 Networks and Systems 2008**



# Next Steps 2004-2006

- For applications to run over IPv6 an IPv6 network infrastructure is required.
- Applications are just beginning to be ported to IPv6.
- Now is the time to begin to plan and deploy IPv6 with the IPv6 products that exist today.
- Then you will be able to run applications that support IPv6 over your networks.
- Think IPv6 transition, not “migration”, IPv4 and IPv6 will coexist for some time.
- Must think IPv6 Mobility when deploying the infrastructure.
- Applications must begin to be ported to support the Enterprise, ISPs/Telco's, and Multimedia.



# Critical Work To Be Done

- ISP's/Telco's to build robust IPv6 Network Infrastructure (Moonv6, 3G/GPRS, WiFi Nets, and Internet2 missions are helping greatly with this effort)
- Solution to the Internet Multihoming problem for IPv6, and problem for IPv4 today.
- Key Applications ported for initial emerging IPv6 Target Markets.
- Security Infrastructure must support both IPv4 and IPv6.
- Vendor platforms products are IPv6 capable today, but now they must support IPv6 Security, beginning with robust IPsec support.
- Public Key Infrastructure methods to support IPsec.
- Authentication, Accounting, and Authorization (AAA).
- Intrusion Detection for a network and a federation of networks.
- Move from Test Beds to "Open" Industry and Government Semi-Commercial Network Pilots like Moonv6.
- Continued Promotion and Education about IPv6 and need for E2E, but not marketing hype of IPv6, its infrastructure not a product or technology!!!

# Predictions 2004

- More Providers will provide users access to IPv6.
- Wireless Mobile IPv6 Hot Spots will begin Trials.
- DoD IPv6 Network Pilots will evolve extensively.
- Additional Government Agencies will adopt IPv6.
- Moonv6 Network Pilot will provide access to International IPv6 Network Pilots.
- Home Cable Routers, Modems, and Network Access Points will participate in IPv6 Network Pilots with some early adopter products.
- Large Application Providers will announce support time frames for IPv6 production support and some prototypes will exist.
- Enterprise Businesses will begin IPv6 Network Pilots.
- Vendors, Systems Integrators, and IPv6 Business Leaders will see first phase revenue streams from IPv6.
- Mobile IPv6 Phone will participate in IPv6 Network Pilots.

# North American IPv6 Task Force (NAv6TF)

- Promote the deployment of IPv6 across North America.
- Technology and Deployment Partnership with Internet2 and University of New Hampshire IPv6 Interoperability Lab.
- Provide business, marketing, educational, and technical center of expertise for IPv6 in North America to any entity building, deploying, or developing IPv6 for deployment.
- Lead specific projects to support North American deployment efforts as we have done for Department of Defense and in process with the Department of Commerce.
- Continue to lead the Moonv6 IPv6 Network Pilot and expand that backbone network as a worldwide IPv6 backbone Network Pilot.
- Develop technology partner relationships with other consortia's and standards bodies working on IPv6.
- Participate in North American industry trade show events, seminars, and technology briefings as IPv6 center of expertise.