Case for IPv6 in the Internet2 Community

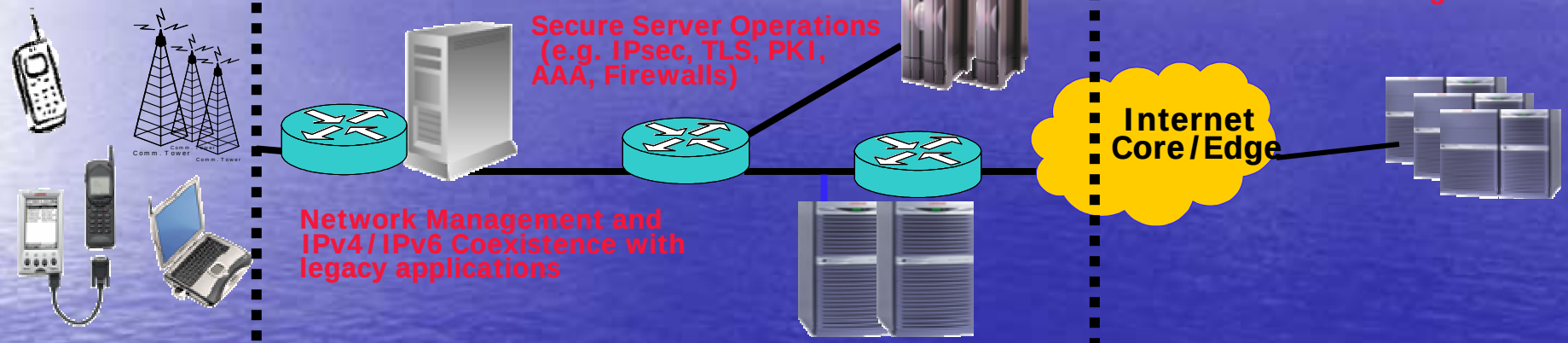
Internet2 Fall Conference
Oct 15, 2003

Jim Bound
Chair North American IPv6 Task Force www.nav6tf.org
Chair IPv6 Forum Technical Directorate www.ipv6forum.com
Hewlett Packard Fellow

Discussion

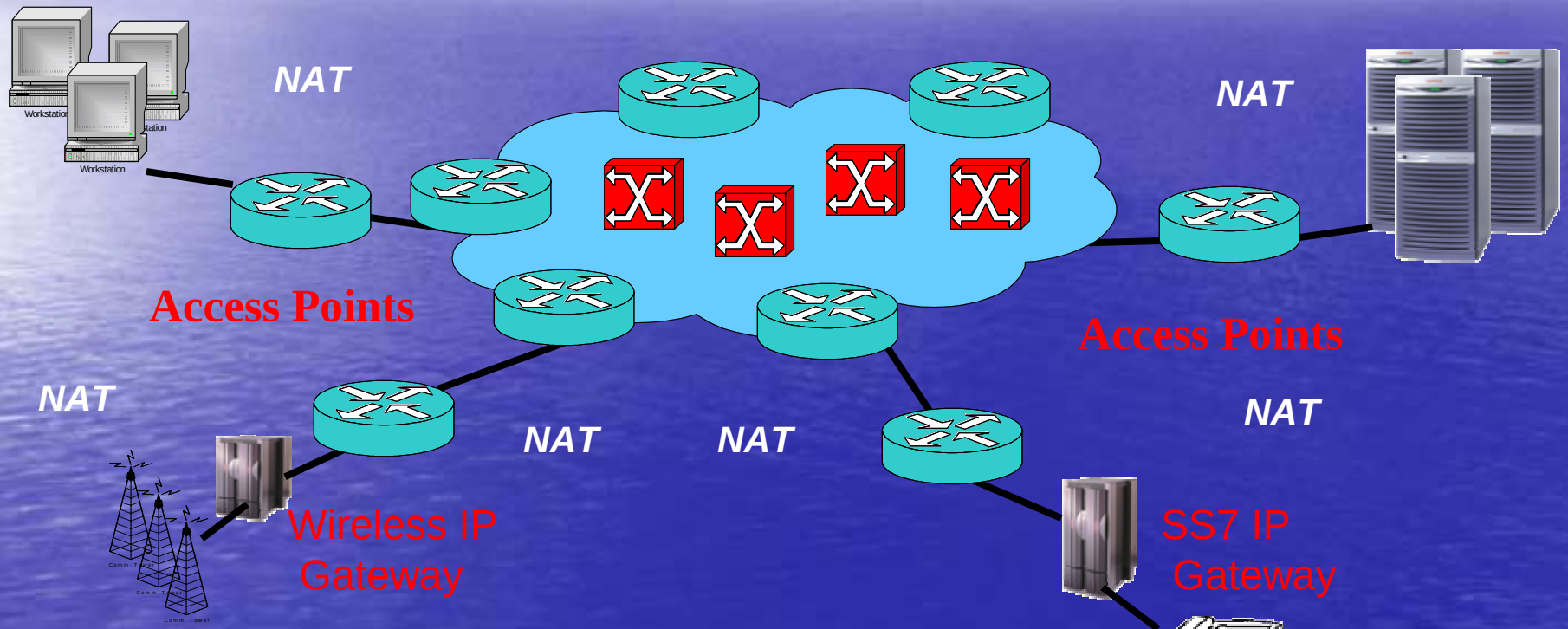
- The Internet Eco System
- Why IPv6 makes Internet2 Better
- Transition Deployment Roadmap for IPv6
- IPv6 Use Examples
- Update on Moonv6 Network Pilot
- Prediction for 2004

Internet Network, Mobile, and Secure Eco System



October 2003

Internet Access Points Today



IPv6 Benefits

- Increased address space
  - 128-bit address size (2^128 addresses)
  - Efficient addressing and routing topology
  - NAT is not required
- Performance
  - Simplified header
  - Optimized for 64-bit hardware architecture
  - Efficient and extensible IP datagram
  - Improved host and router discovery
  - Improved Multicast scalability

IPv6 Benefits

- Plug and Play
  - Stateless Paradigm Inherent in Design
  - Dynamic address autoconfiguration
  - Dynamic renumbering of networks
- Mobile IPv6 support optimized over IPv4
- Security is required and avoids IPv4 NAT Band-aid
- Simple interoperation with IPv4
- Other functions still evolving from the extensibility of the architecture

IPv6 Benefit - Simplified Network Administration

- Autoconfiguration means:
  - Devices plug into the network and begin operating (plug-and-play) using Stateless Autoconfiguration
  - DHCP version 6 support
    - Every host can download its network configurations from a server at startup time
- Renumbering in IPv6 is designed to happen
  - Flexibility to switch ISPs whenever you want, for whatever reason
  - No more “lock-in”

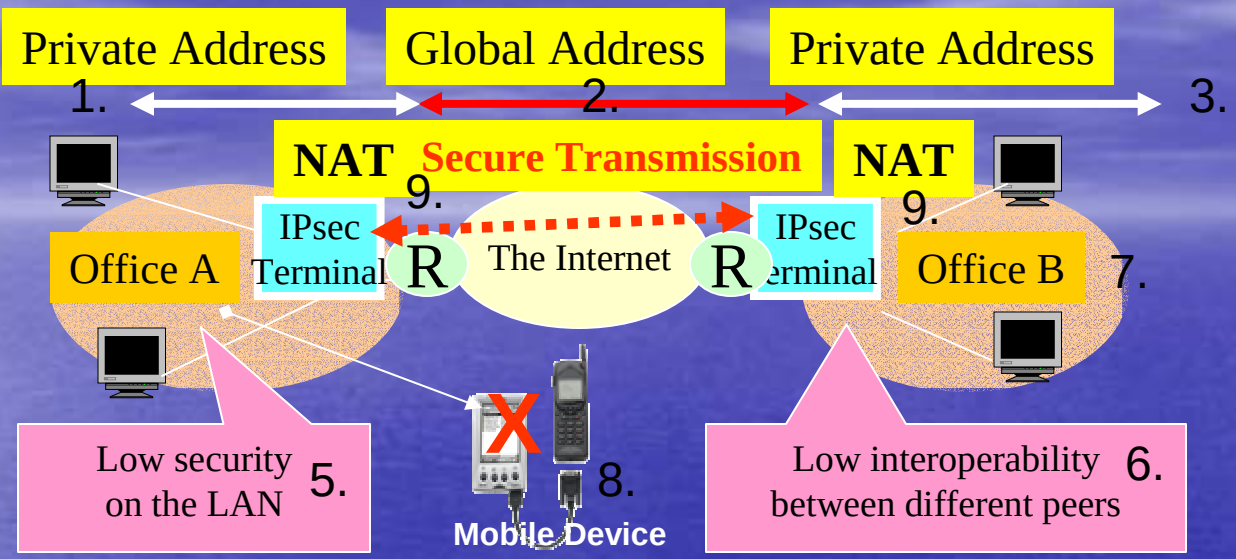
IPv6 Benefit - Life Is Easier for Operations

- Better manageability
- IPv6 address scope
  - GLOBAL or LOCAL
- Configuration Policy Control
  - Stateless
  - Stateful (DHCPv6)
  - Routers dictating configuration policy and MTU size for the link

Cost of IPv4 NAT

IPv4-NAT

Site-to-Site Secure Communication 4.



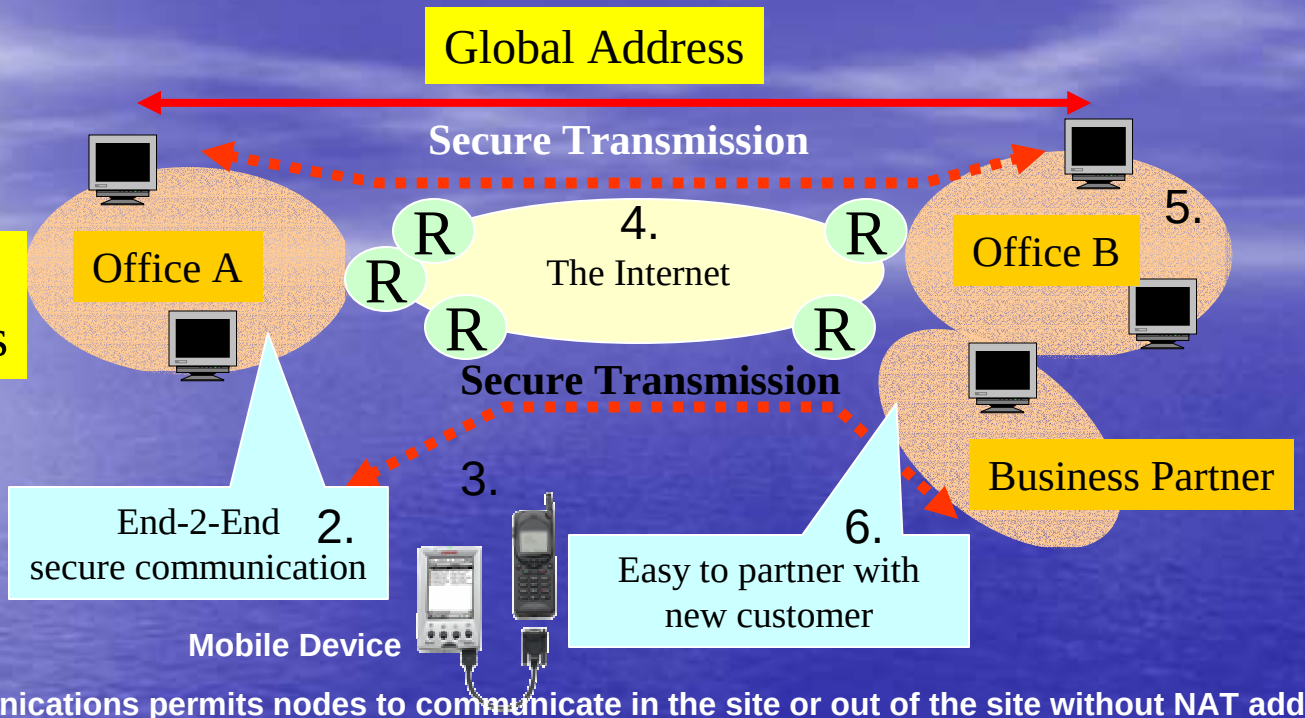
1. Node can only communicate out of site with peer through a NAT and has reduced capability of applications.
2. Communications has only one entry point to Office A node through one router and single point of failure.
3. Attacker only has to masquerade the packet between the NATs and they will be able 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

IPv6

End-2-End Communications 1.

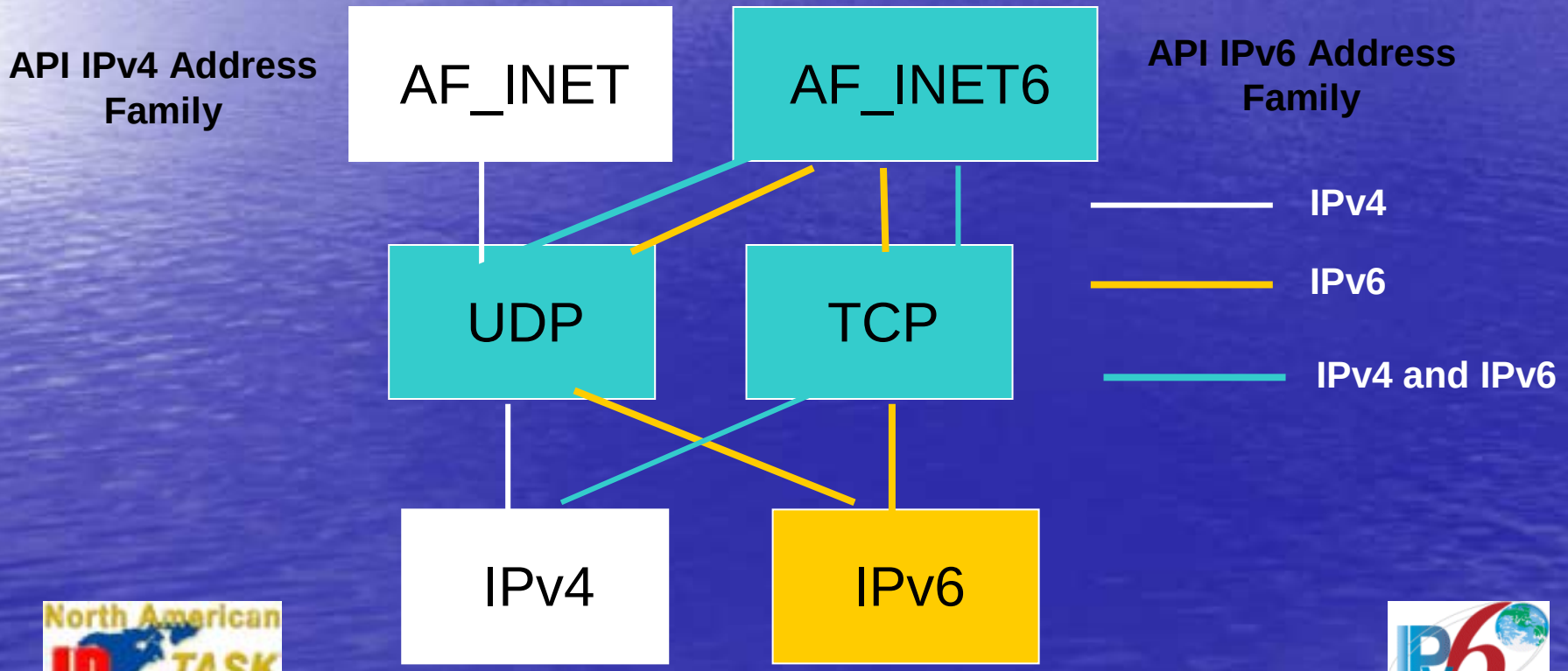


1. End-2-End communications permits nodes to communicate in the site or out of the site without NAT additions.
2. End-2-End security methodology and architecture permits pervasive security in the site, and out of the site.
3. Global Addresses and End-2-End communications and security permit nodes to 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.

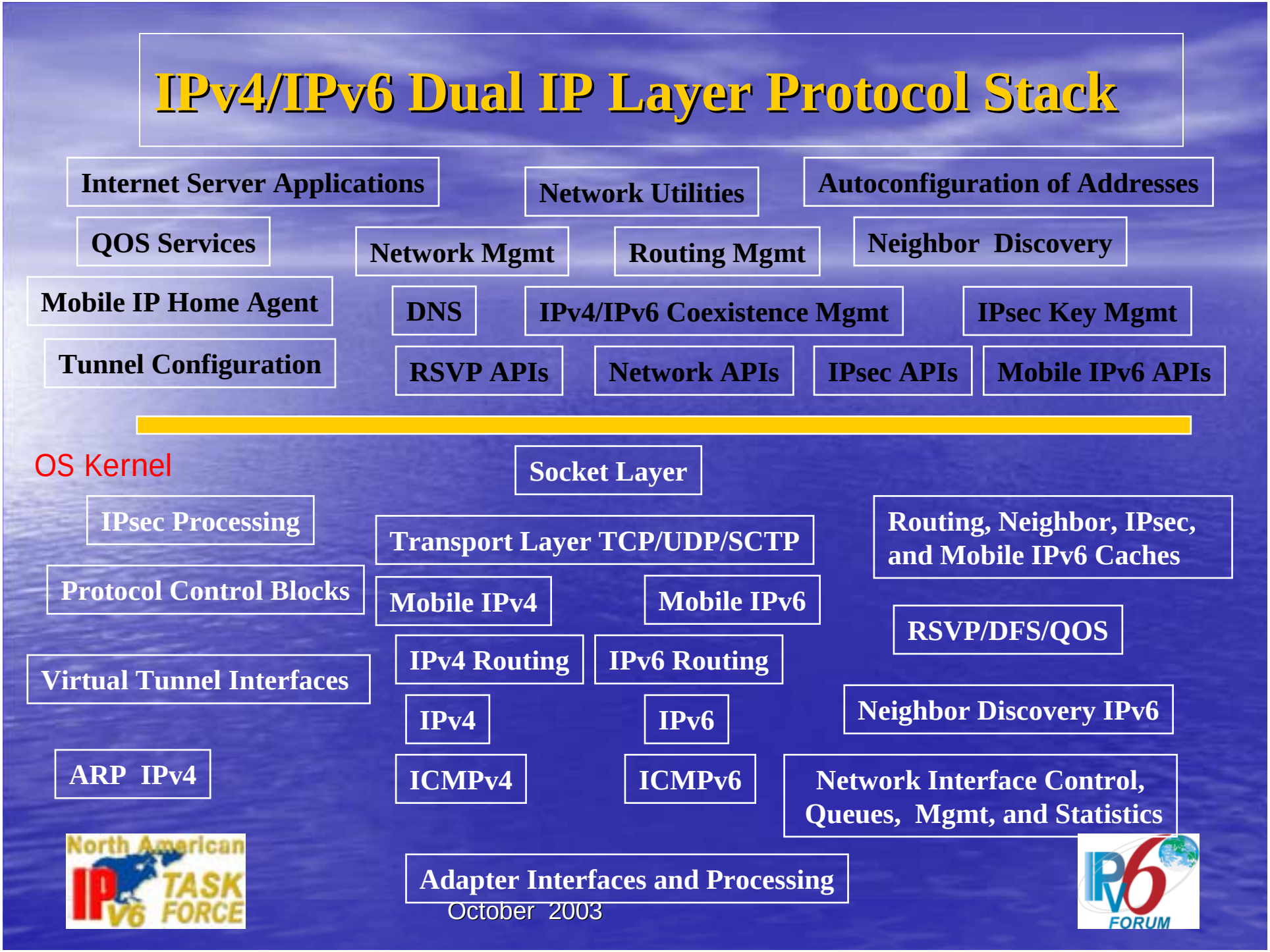
Profit from No-NAT can be realized with greater application support and availability which cannot run in a NAT Environment, communications with peers can be initiated by a site or peers out of the site, security is based on security within the node and provides End-2-End secure communications trust and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

IPv4/IPv6 Hybrid stack

- Misnomer in industry most implementations are a Dual IP Layer Hybrid Stack (below), not a pure Dual TCP/IP Stack duplicating other common IP suite functions.
- IPv6 API developed so IPv4 addresses can be used as IPv6 through IPv4 Mapped Address Representation.



IPv4/IPv6 Dual IP Layer Protocol Stack

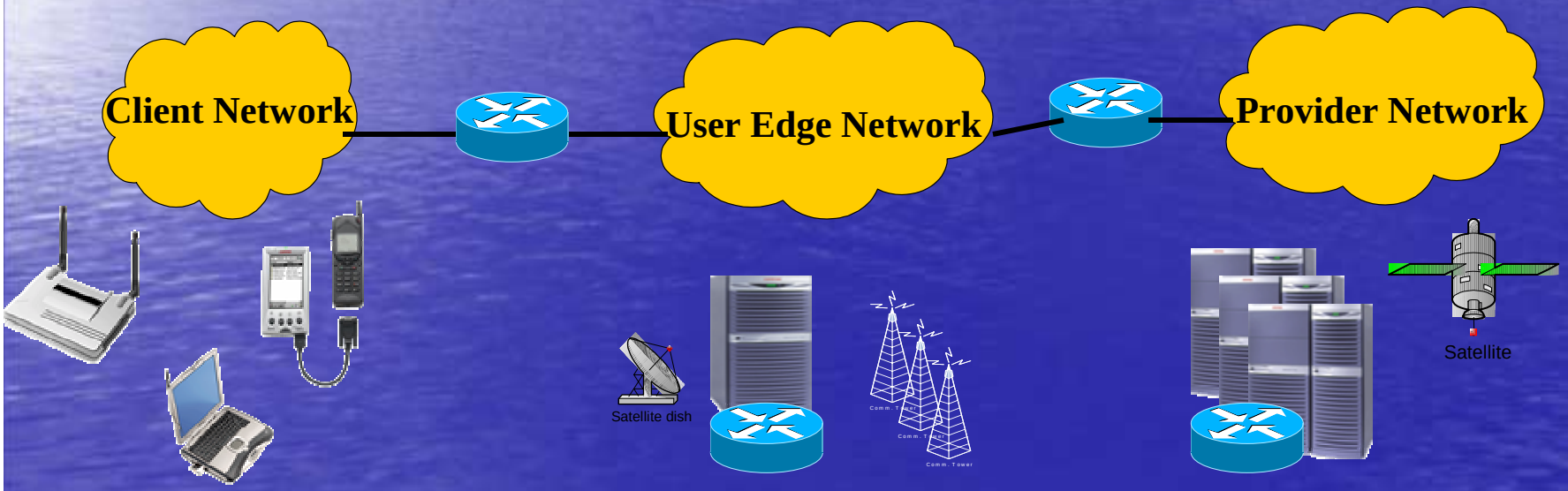


Deployment Perspective Topics

- Points of Transition
- Transition Solutions
- Deployment Roadmap
- Current Deployment Models

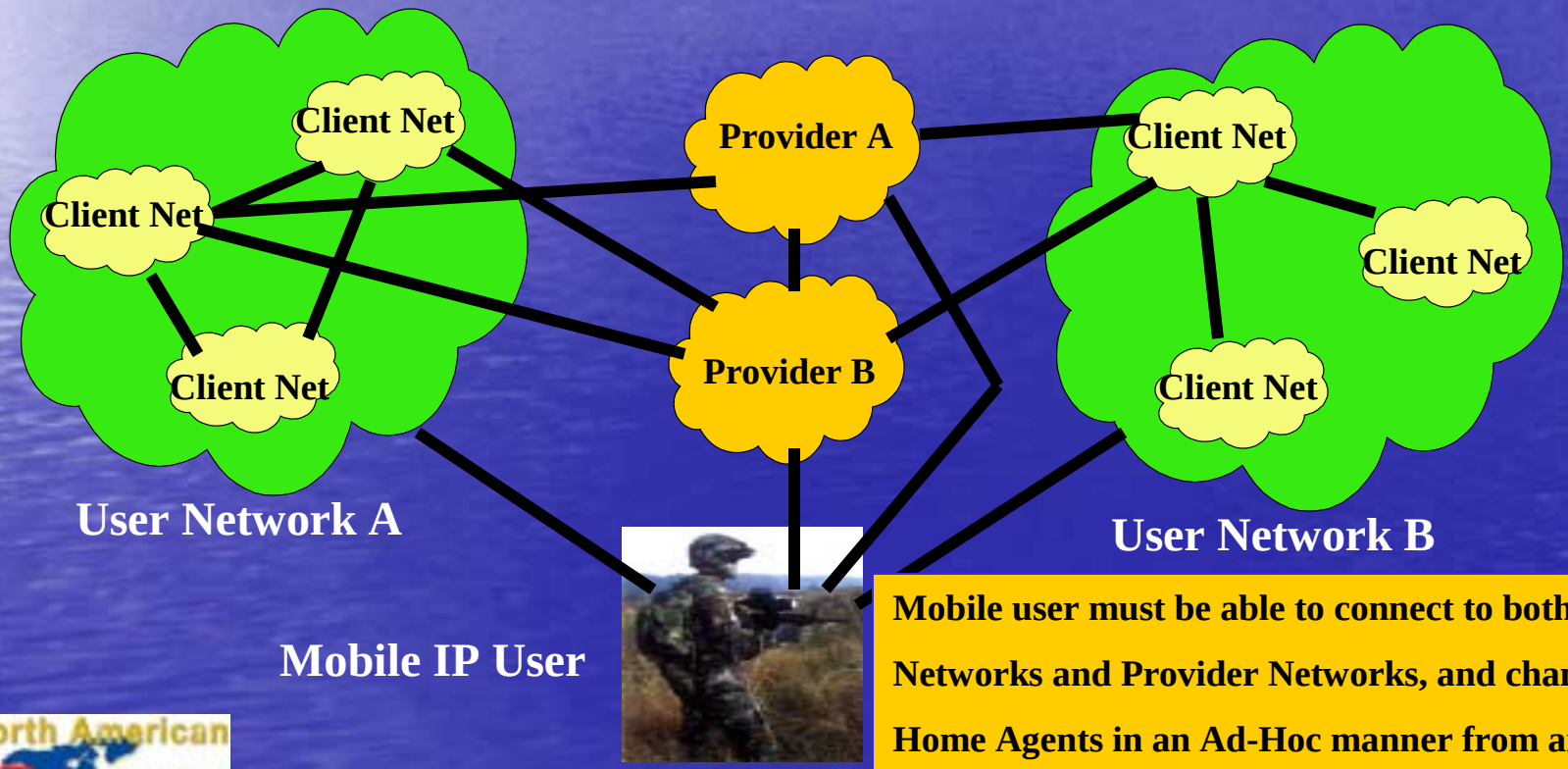
Where can Network Topology Transition take place?

- At the client network within the user network.
- At the edge of the user network to the provider.
- At the provider network for the user network.



The Transition complexity will be exponential with a larger Mesh network topology

- Multiple client, edge, and provider networks will increase transition planning and staged deployment.
- Mobile IPv6 Computing further complicates the Transition and creates a new decision point for deployment.



Mobile user must be able to connect to both User Networks and Provider Networks, and change Home Agents in an Ad-Hoc manner from any Network point of attachment.

Points of Transition (Geography)

- Packets over a local link
- Packets over a site
- Packets within an Intranet (multiple sites')
- Packets over a private Internet (multiple Intranets')
- Packets over the public Internet
- Packets over a Mobile IP Network (Wireless)
- Packets over a Mobile IP Network (Wireless) and to a Broadband Network (Wireline) or the Reverse
- Packets from IPv6 Network thru IPv4 Cloud to IPv6 Network
- Packets from IPv4 Network thru IPv6 Cloud to IPv4 Network

Points of Transition (Network – Nodes)

- Clients
- Servers
- Routers
- Gateways
- Mobility Management
- Voice over IP (VoIP) Networks
- Network Management
- Transition Nodes
- Firewalls
- Public Key Infrastructure Servers for Security

Points of Transition (Network – Software)

- Network Management and Utilities
- Network Internet Infrastructure Applications
- Network Systems Applications
- Network End User Applications
- Network High Availability Software
- Network Security Software

Deployment Roadmap Model

- Step 1 - Determine the set of network applications that must be ported or invented (where packets go over the network)
- Step 2 – Determine the Geography your applications must span.
- Step 3 – Identify the Network components that must support IPv6.
- Step 4 – Identify the Network components that require IPv6 Transition Mechanisms.
- Step 5 – Identify the Network components that are new or being developed and can be initiated with IPv6 using IPv4 as scarce resource only, especially new technology deployment models (e.g. Network Routers and Servers, Mobile IP Networking Components, New Simulation Programs, Security Surveillance)

Deployment Transition Mechanisms

- Configured Tunnels
  - Base IPv6 Transition Specification
  - Dual IP Layer Model
  - 6to4 Gateways
  - ISATAP
  - Pseudo Tunnels (Clients, Servers, Routers, and Gateways)
- Dynamic Tunnels to avoid IPv6 and IPv4 NATs
  - DSTM
  - Dynamically Assigning Tunnel Endpoints
  - Dynamically Assigning Temporary Global IPv4 Addresses
  - Pseudo Tunnels (Clients, Servers, Routers, and Gateways)
  - Teredo to bypass IPv4 NAT

Transition Hot Spots

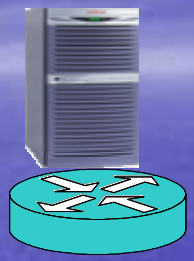
- Wireless Communications and integration with Wireline (Broadband) Communications
- Mobile IPv6 for Cellular Handoffs and Mobile Ad-Hoc Routing
- Application Porting Methodology
- Tunnels around IPv4 encryption-devices that cannot be upgraded to IPv6 immediately and performance of that tunnel
- IPv6 Security infrastructure requirements.
- IPv6 Intrusion Detection.
- Training, Porting applications, and Hardware Upgrades for some nodes will have cost.
- Network Management of new IPv6 infrastructure and points of transition.
- Key Management for IPsec and Public Key Infrastructure
- Tunnels around IPv4 encryption-devices that cannot be upgraded to IPv6 immediately and performance of that tunnel

Current Industry IPv6 Deployment State

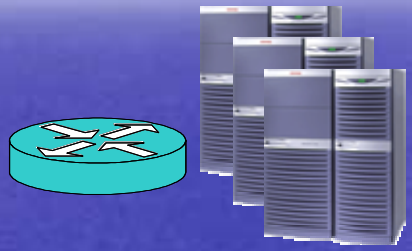
- Asia is leading the pack geographically, deploying high tech devices, wireless, and wireline IPv6 infrastructure.
- European and Asian High-Up Officials within Government have made formal statements regarding the importance of IPv6.
- 3G Deployment has begun in 2003.
- 802.11 Wi-Fi is potential High End Deployment for IPv6 and Mobile IPv6:
  - First with reconnect strategy when roaming
  - Then Mobile IPv6 always-on-anytime roaming
- U.S. is still lagging in industry, but DoD IPv6 announcement is strong catalyst for U.S., and DoD Pilots in Process.
- Good News:
  - All major vendors have shipped first and second version of IPv6 Products.
  - ISPs worldwide are beginning to do Pilots with IPv6 (including the U.S.)
  - Early Adopters worldwide have procured systems to begin to build IPv6 labs and test beds.
- North American IPv6 Task Force (NAV6TF) is established and in process www.nav6tf.org
- U.S. Wide Moonv6 IPv6 Pilot October 2003 driven by NAv6TF www.moonv6.com

WLAN Internet Mobile IPv6 Network

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

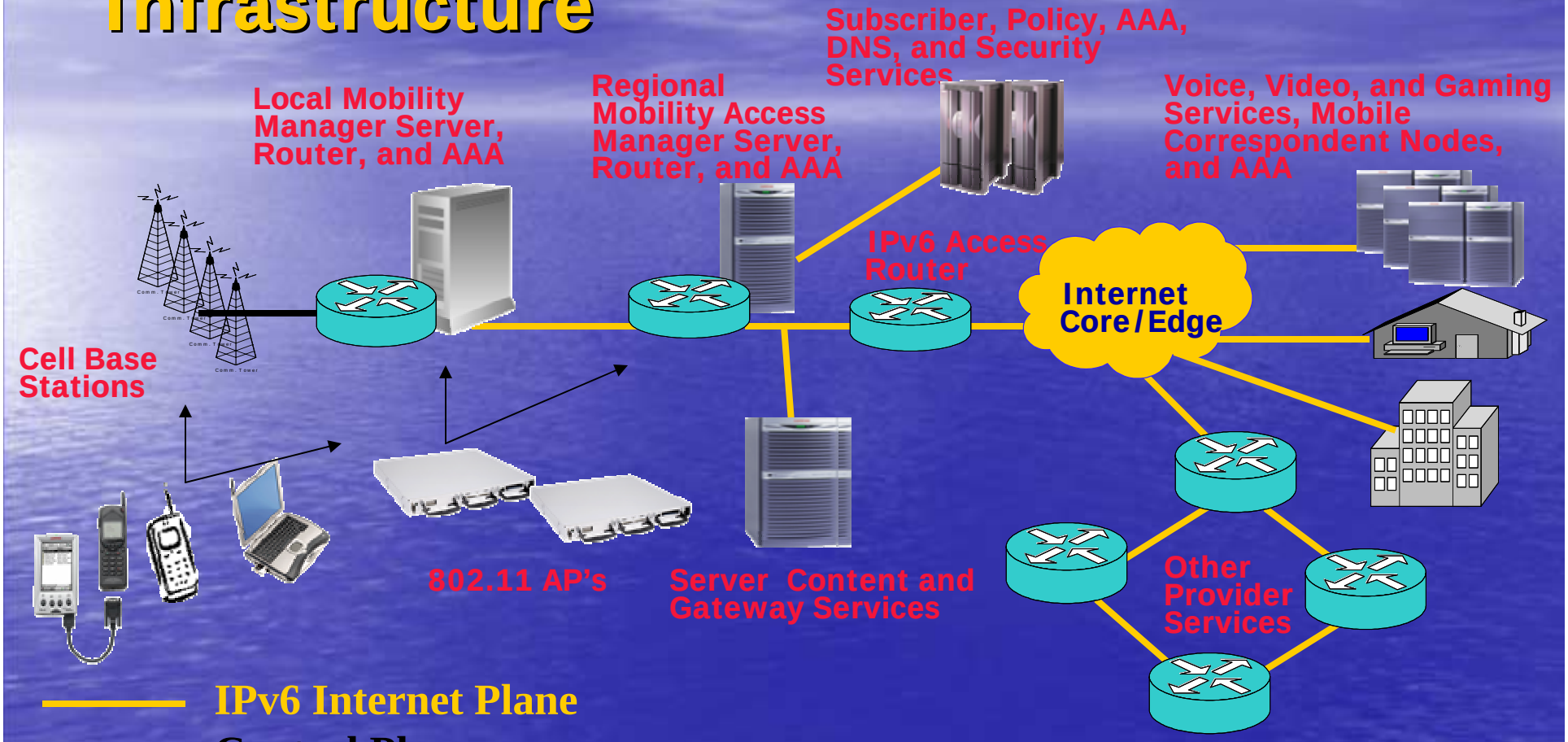
Mobile IPv6 Stations Voice and Data Roaming

North American IPv6 TASK FORCE

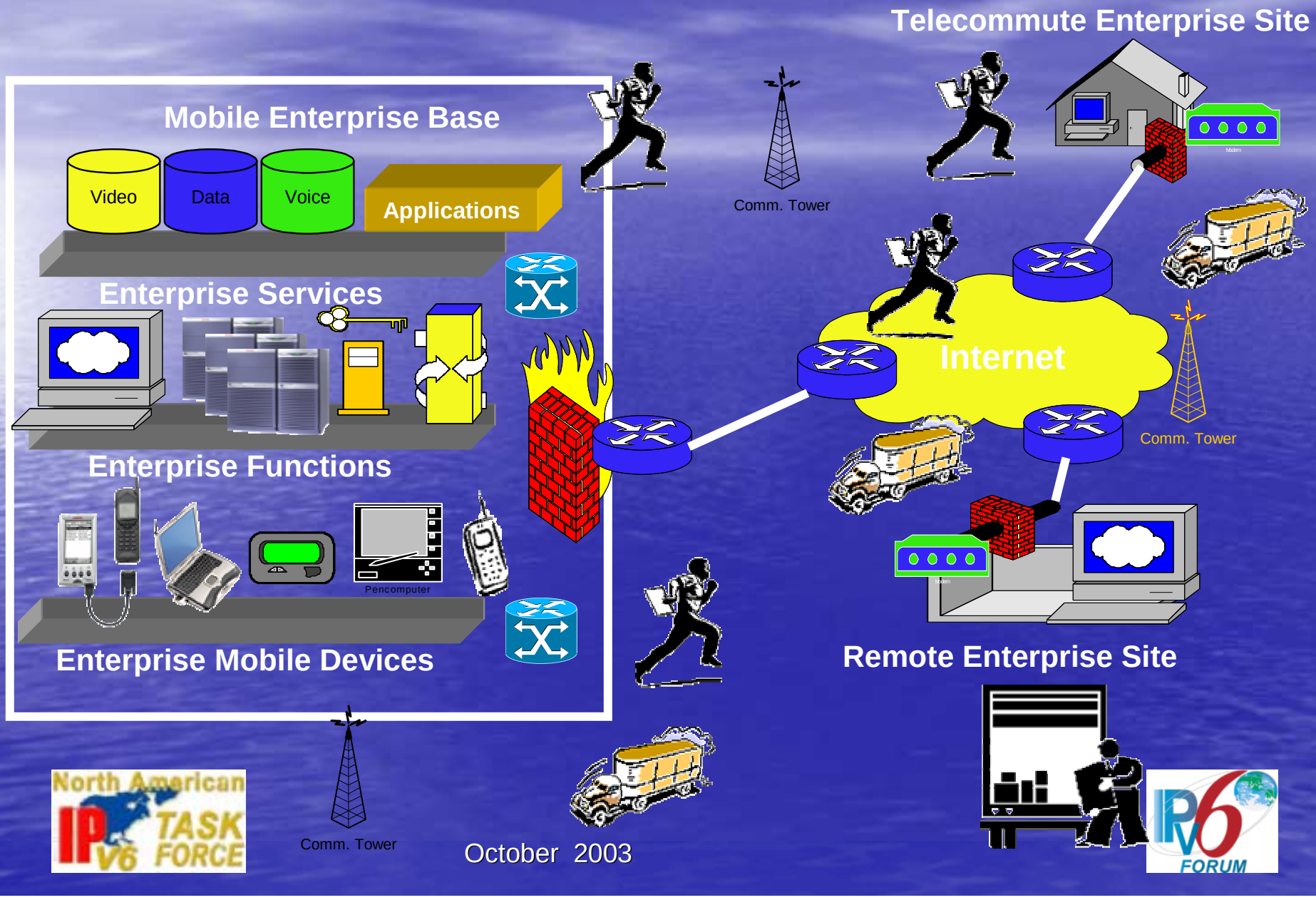
October 2003

IPv6 FORUM

IT Provider IPv6 Network Mobility Infrastructure

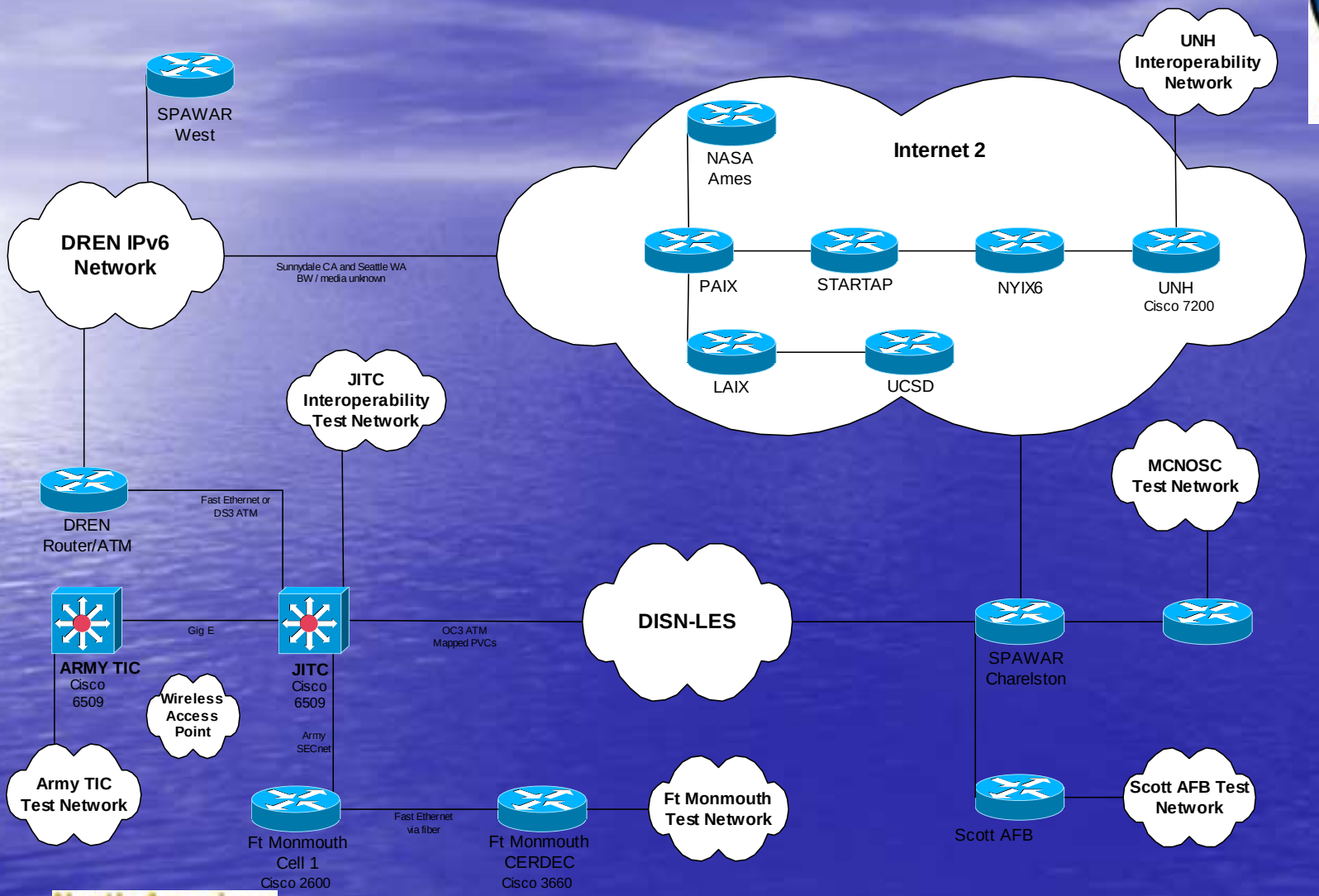


Enterprise IPv6 Network Mobility



October 2003

Moonv6 Network Pilot



October 2003

2004 Predictions North America

- 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.

/jim
"if its real, you'll feel it"
Kid Rock