



IPv6 Transition

JITC

Oct 8-9, 2002

FT Huachuca, AZ

Jim Bound

HP Staff Fellow

Chair IPv6 Forum Technical
Directorate



Discussion Topics

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

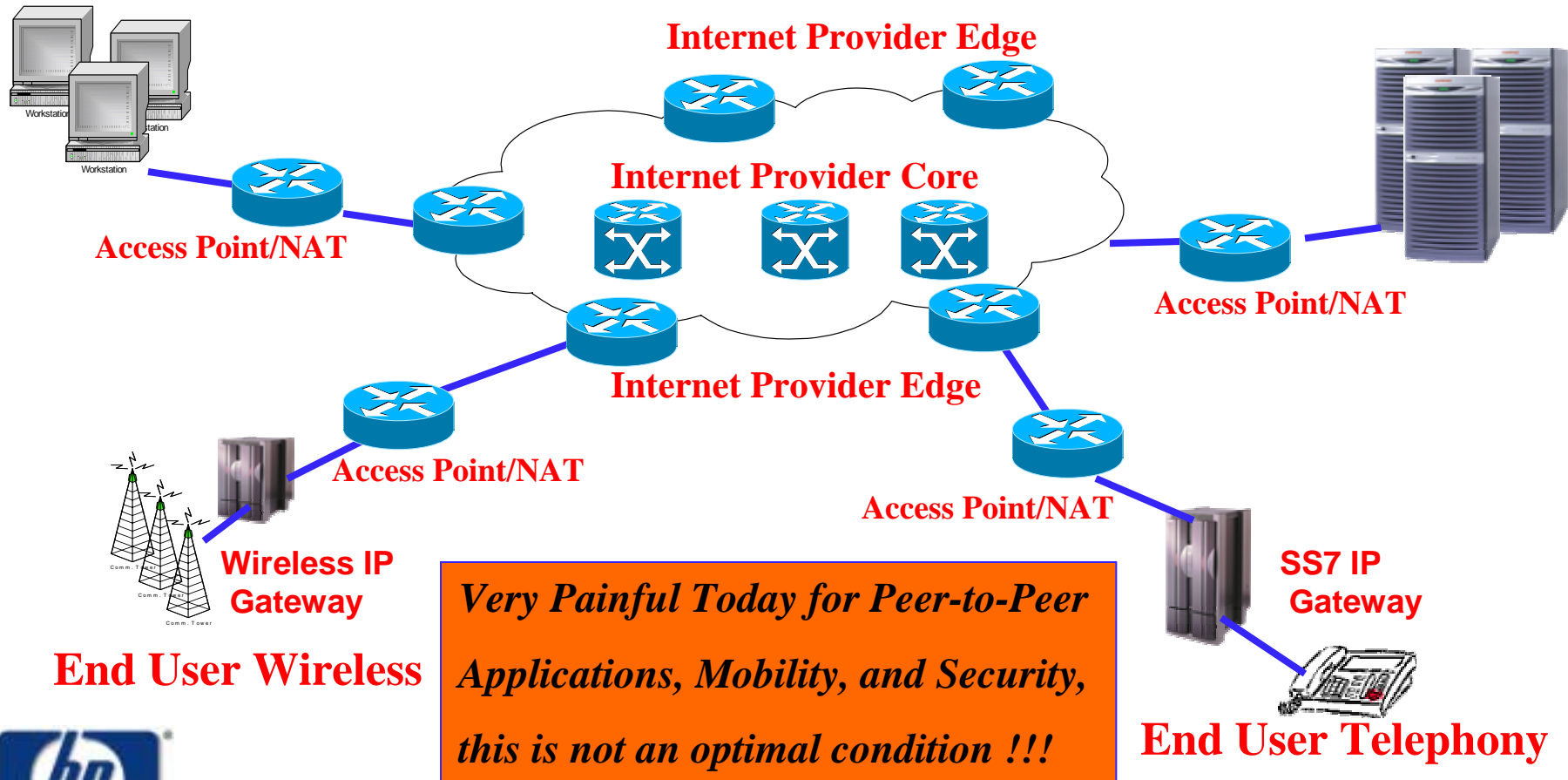
Note all Military U.S. Army Graphics were provided by CECOM FT Monmouth, New Jersey. Thanks to Ed Kierman and the PING Lab Team.



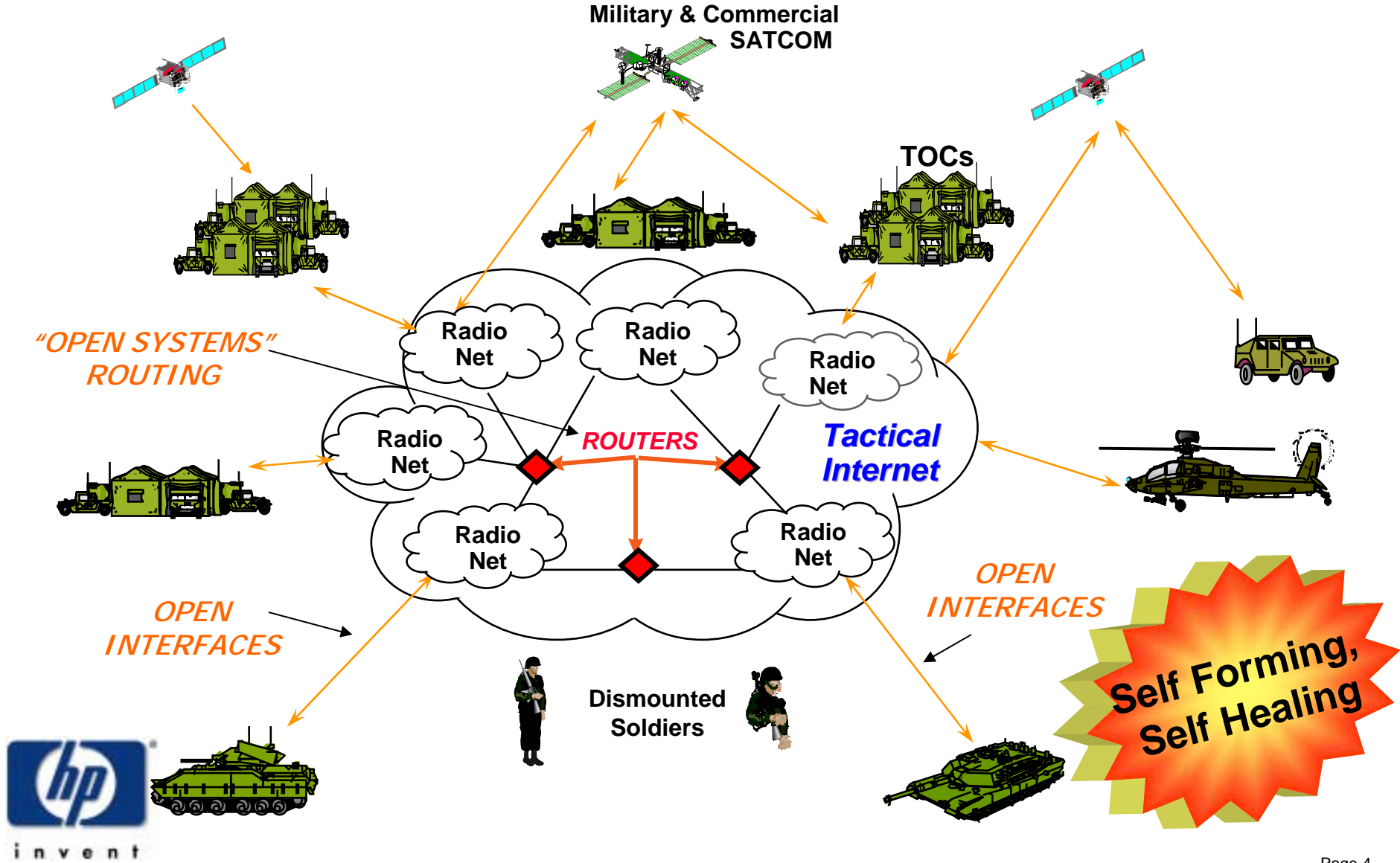
Internet Communications Today

End User Wireline & Broadband

Internet Services

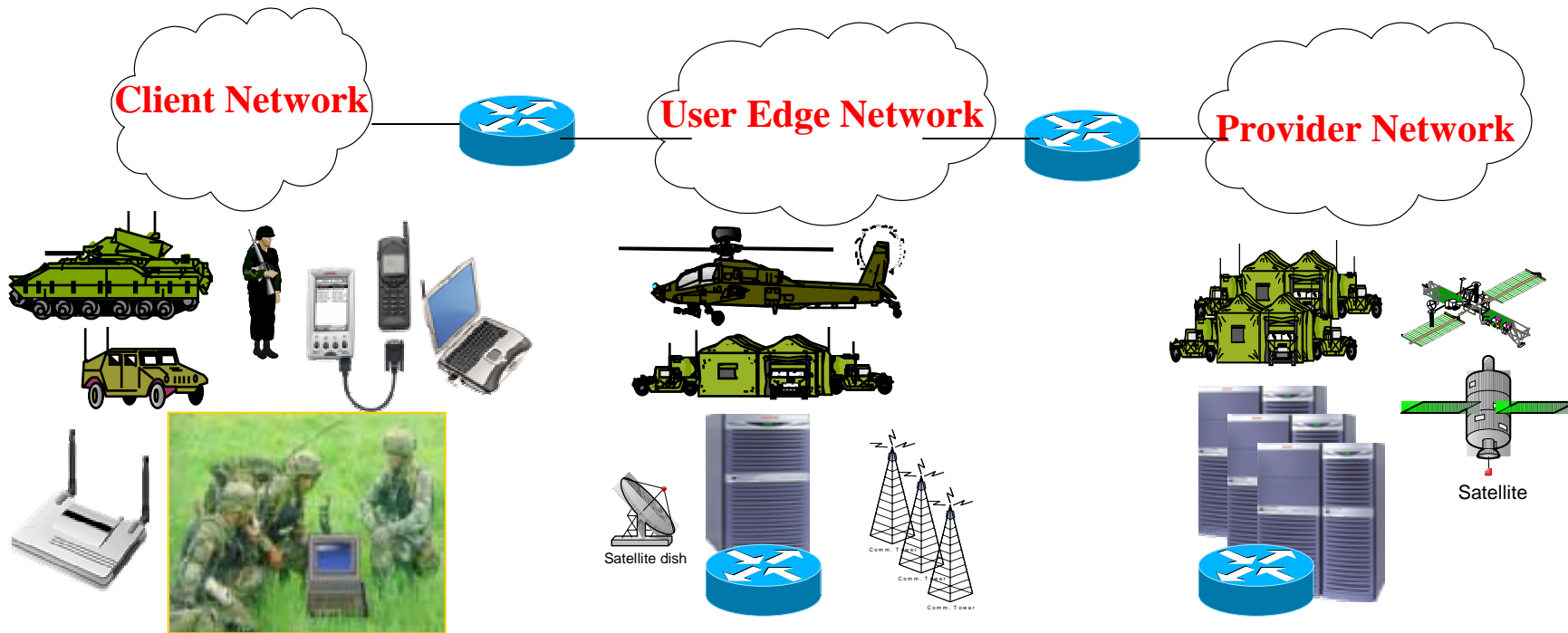


Army Transformation Network View



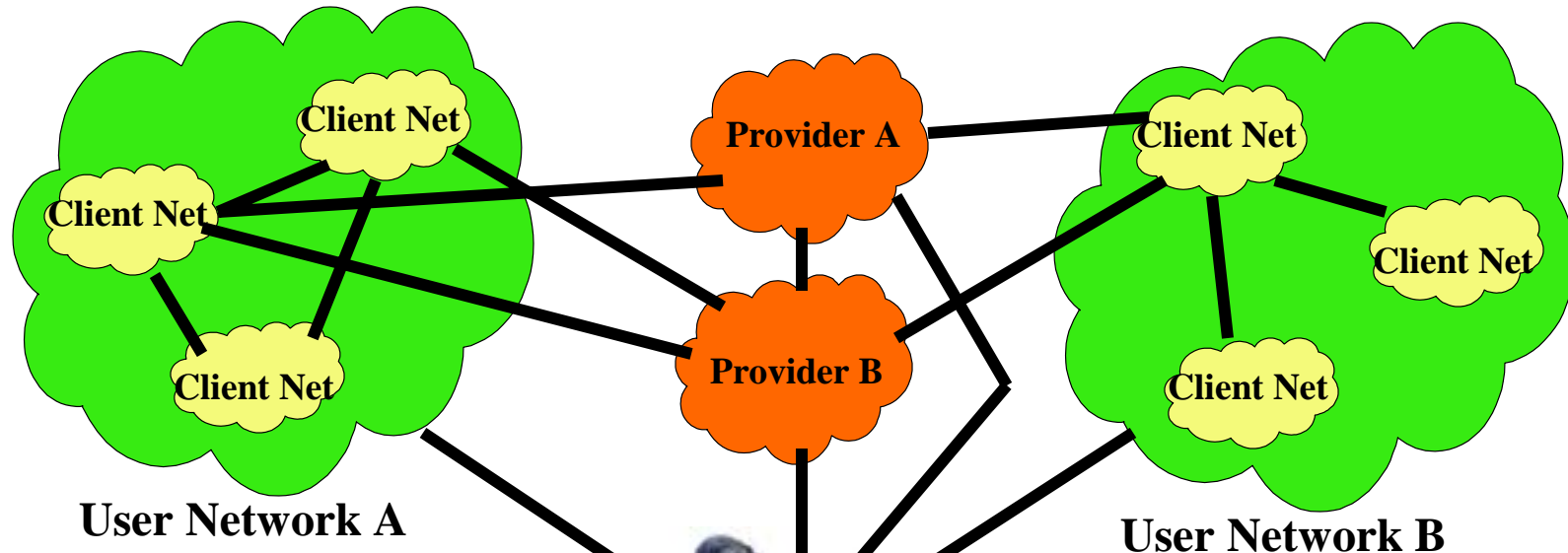
Where can Network Topology Transition take place?

- 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 IP Computing further complicates the Transition and creates a new decision point of IPv4 with NAT or IPv6 without NAT.



Mobile user must be able to connect to both User Networks and both 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 War Fighter, Mobile IP Networking Components, New Simulation Programs, Home Land Defense Surveillance)



Deployment Transition Mechanisms

- Configured Tunnels
 - Base IPv6 Transition Spec
 - 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 and using 6to4



Deployment Transition Mechanisms (continued)

- Network Translation (the last alternative)
 - NAT-PT (stateful translator)
 - SIIT (stateless translator)
 - IPv6-ONLY to IPv4-ONLY Communications
 - Routers and Gateways
- Basic and Advanced API and Bump-in-the-API Mechanisms
 - Port Applications to use IPv4 and IPv6 communications
 - Port Applications to use IPv6 communications where IPv4 is represented as IPv6
 - Bump-in-the-API mechanisms for Software where the sources are lost or so old reporting them is not an option and they must be replaced eventually !!!! Recommended as last resort only !!!!



Transition Hot Spots

- Wireless Communications and integration with Wireline (Broadband) Communications
- Mobile IP 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
- Use of AAA Servers and Clients for initial security and tracking (Ethernet, 802.11, 3G, PPP-over-Ethernet (PPOE))
- Cost is mostly people investment and training, not software, and some hardware.
- Europe + Asia adoption exceeds the U.S. and this will affect the initial transition mechanisms vendors engineer first.
- Key Management for IPsec and Public Key Infrastructure



Impact of Transition on the DoD

- Internet infrastructure will be done by the vendors as off the shelf commercial transition tools.
- Determine the network applications that are needed to be ported or invented.
- Determine the Geographical scope within the Network Nodes and Software required for the scope.
- Transition Mechanisms have a dependence on critical execution points where transition occurs.
- For applications that are DoD geographic specific you may want to assume IPv6 ONLY communications (this does not mean you cannot have dual IP layer)



Impact of Transition on the DoD (continued)

- Need to determine methodology for porting applications.
- Need to determine if Dual IP layer support is required for all DoD nodes.
- Need to consider more of the leading edge issues for IPv6 like Mobile Ad-Hoc Networking
- Most cost will be in requirements definition, planning, system analysis, and training of personnel.
- Wireless and Wireline will use different transition mechanisms.



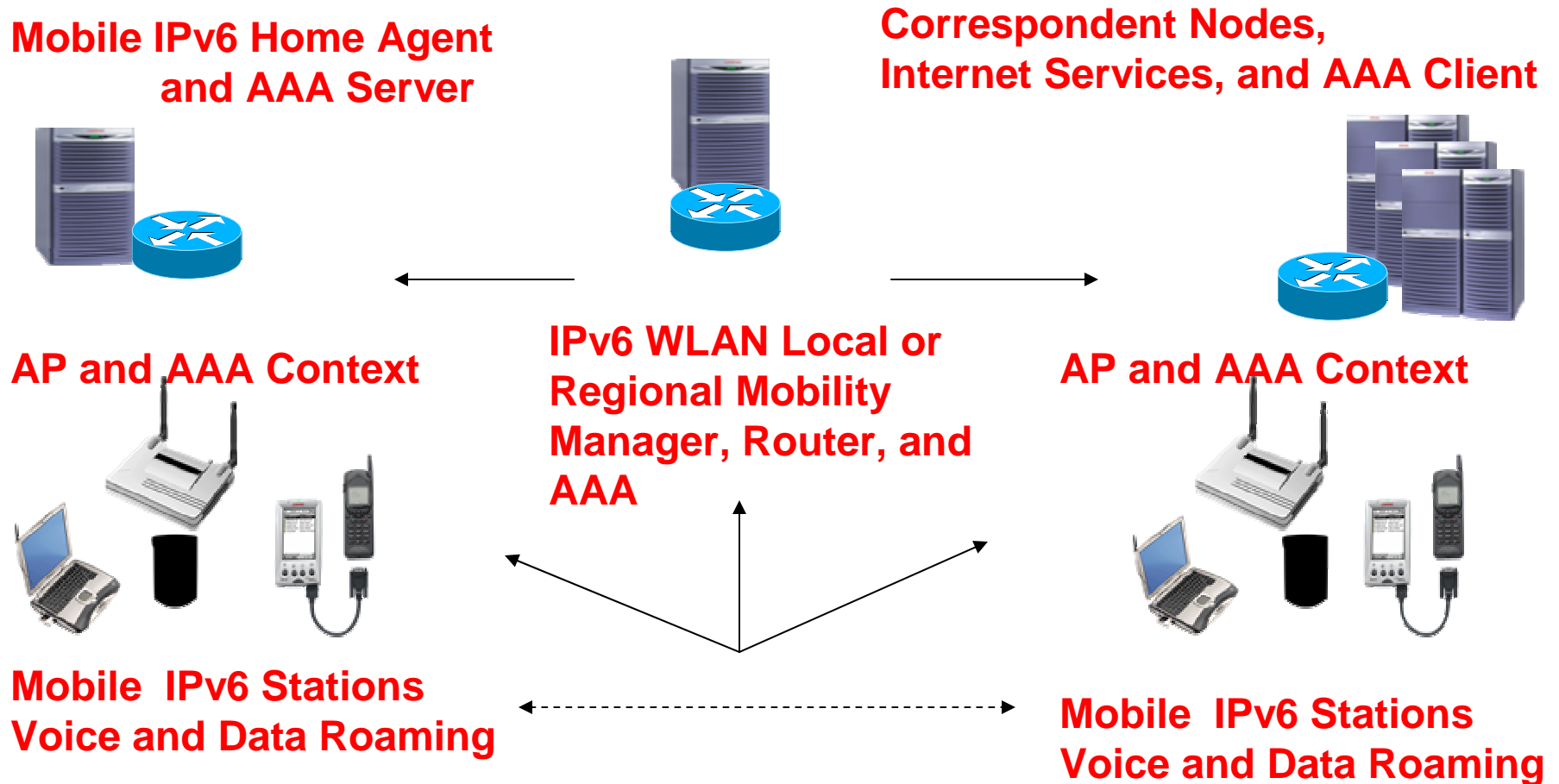
Current IPv6 Deployment State

- 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 has still not produced IPv6 deployment but is in waiting.
- 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 is leading with work at SPAWAR CECOM at FT Monmouth, DISA, OSD, and other activities
- Good News:
 - All major vendors have shipped first and second version of IPv6 Products.
 - ISPs worldwide are beginning to do trials 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.

<http://www.nav6tf.org/>

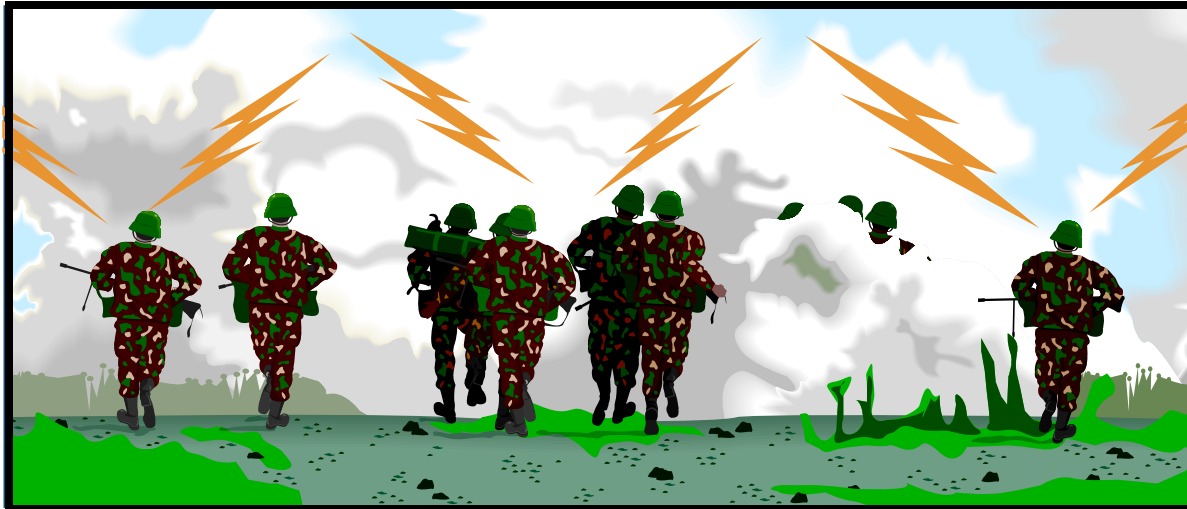


WLAN Internet Mobile IPv6 Network

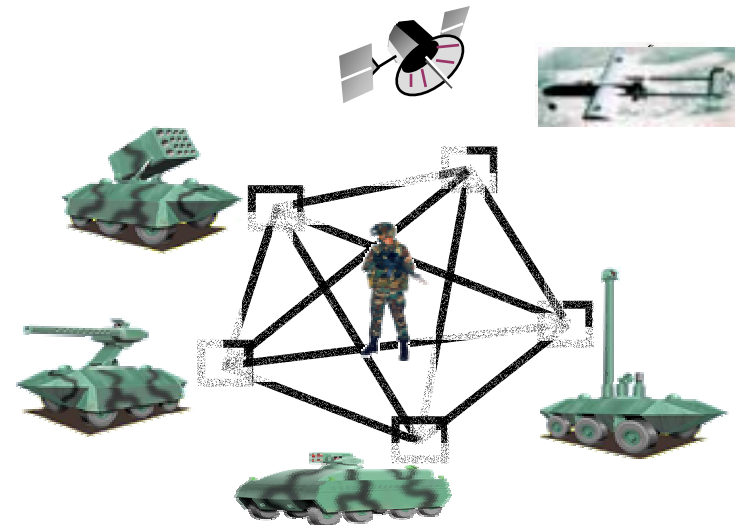


See the HP and Cisco joint IPv6/Mobile IPv6 Technology Demo Right Here at SPAWAR

Mobile IP Soldier requires the previous slides Technology (and Home Land Defense Law Enforcement)

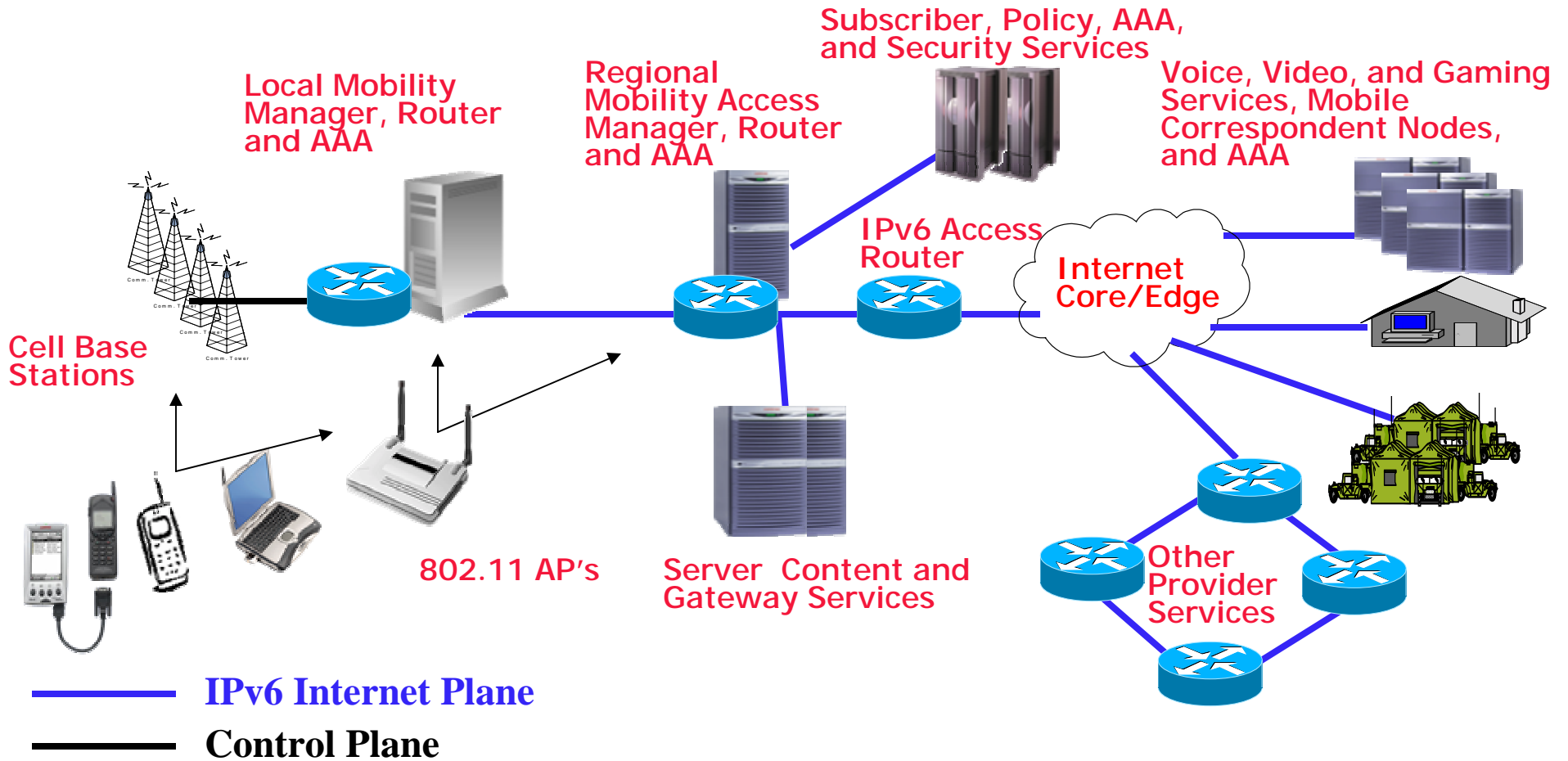


**Teams drop in with Mobile IP router,
Access Points, Server, and Handhelds
for GPS, Commands, and Intelligence
Communications, with Correspondent
Nodes at Command Checkpoint**



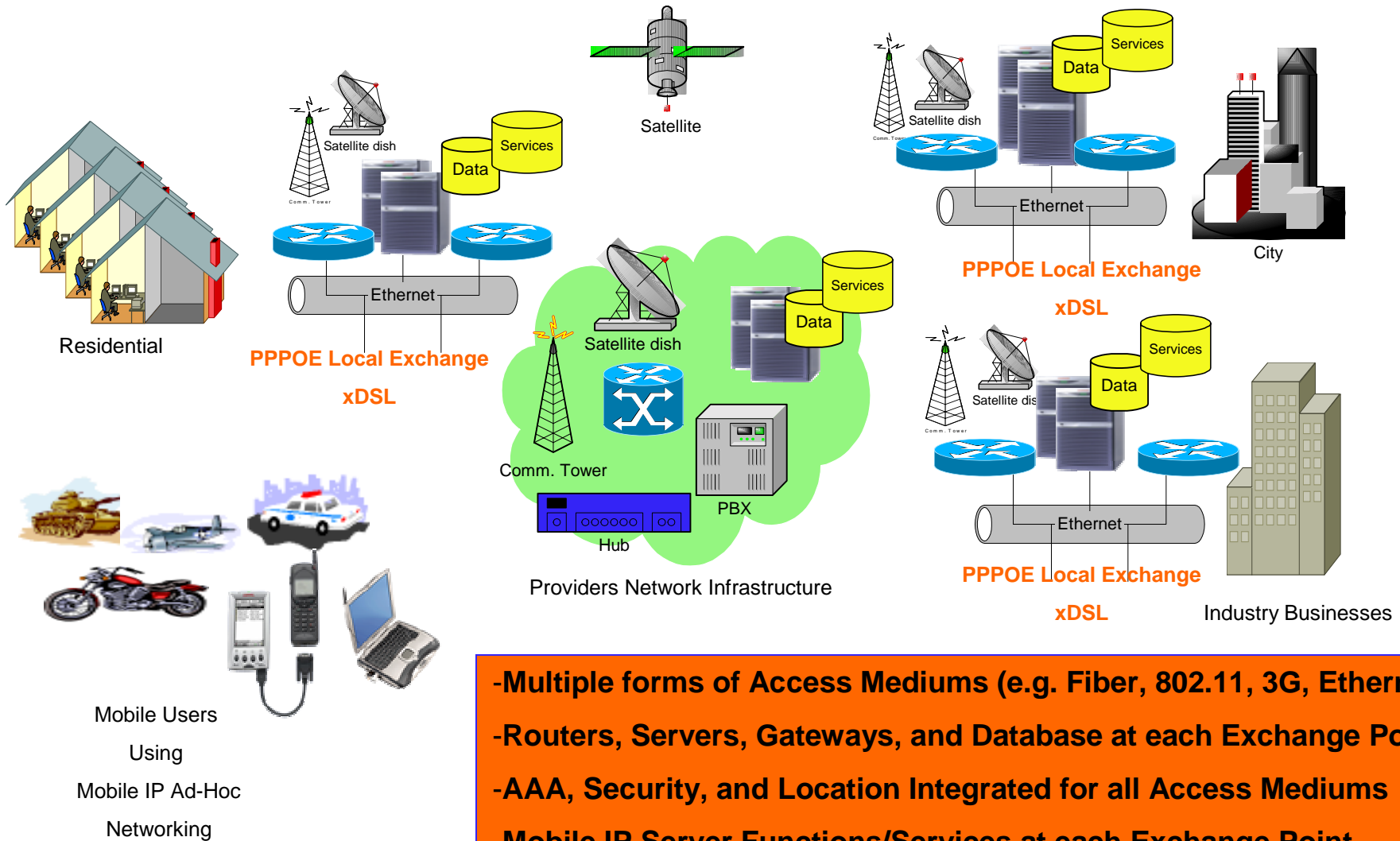
End-2-End IPv6 Mobile Wireless Services

Wireline and Wireless Integration



Note with IPv6 the Signal Planes are reduced from previous Wireless Architectures!! Oh and NAT is Gone !!!

Broadband+Wireless Connectivity



- Multiple forms of Access Mediums (e.g. Fiber, 802.11, 3G, Ethernet)
- Routers, Servers, Gateways, and Database at each Exchange Point
- AAA, Security, and Location Integrated for all Access Mediums
- Mobile IP Server Functions/Services at each Exchange Point
- Moves "Traditional Servers" to the Network Edges



IPv6 Extended Infrastructure Requirements 2003-2005

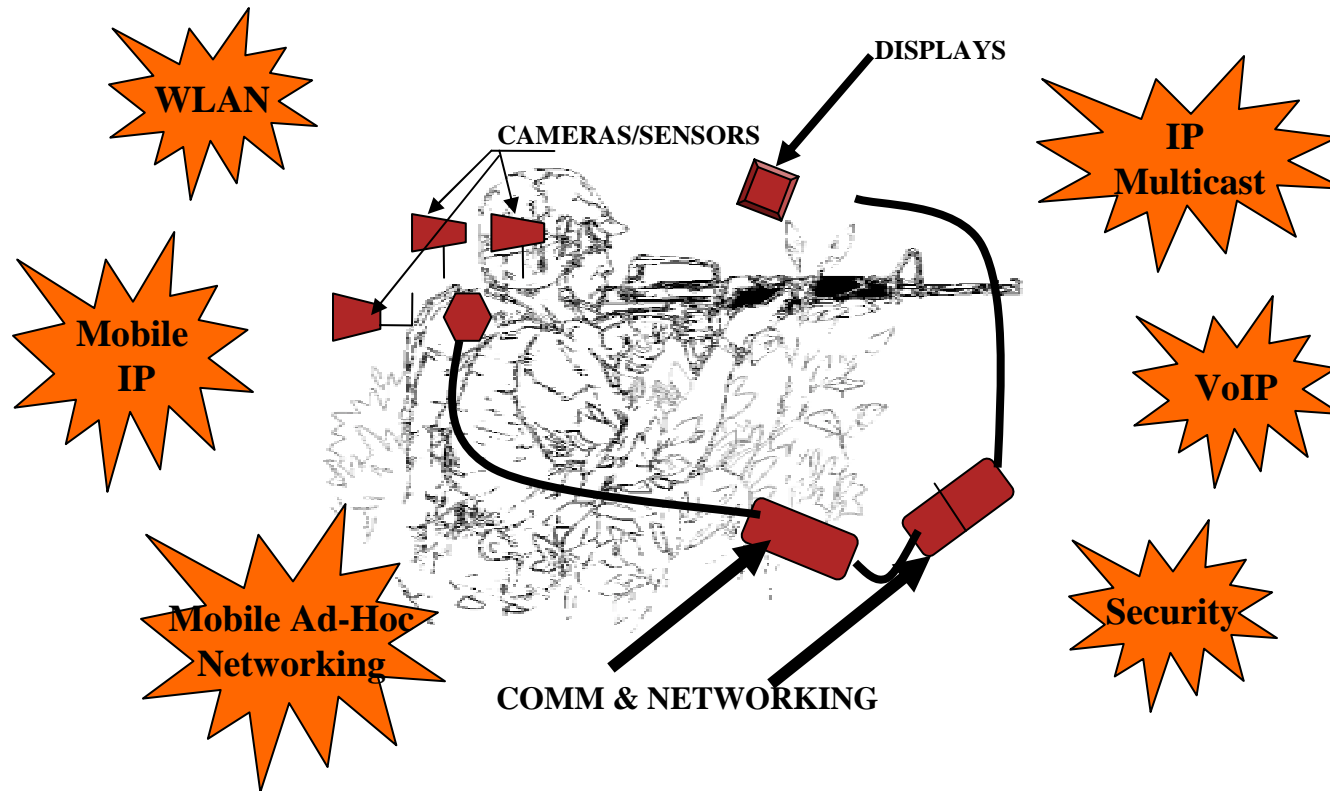
	Telco ISP Provider	ISVs and ASPs	Mobile Wireless	Consumer In-Home	Military	Enterprise	xDSL Wireline	HPTC
MIPv6	●	●	●	●	●	●	●	●
MIPv6 AAA	●	●	●	●	●	●	●	●
MIPv6 Managers	●	●	●	●	●	●	●	●
Ext-IPv6	●	●	●	●	●	●	●	●
Ext-Trans	●	●	●	●	●	●	●	●
Ext-Apps	●	●	●	●	●	●	●	●
Ext-Net Mgmt	●	●	●	●	●	●	●	●
Ext-Security	●	●	●	●	●	●	●	●
Ext- Provider	●	●	●	●	●	●	●	●

2003 ● 2004 ● 2005 ●

**Note Military, Provider, Mobile and Enterprise have same requirements
This will assure commercial off the shelf products for the DoD**



IPv6 Intelligent War Fighter



We don't want the bad guys to have stuff we don't have, or our friends to have stuff we cannot interoperate with (paraphrase of conversation with Mike Brig at SPAWAR 3 years ago !!!)



i n v e n t