IPv6 Maturity from an ISP's Perspective

United States IPv6 Summit: Reston, VA

STAN BARBER
December 10, 2004

NTT Communications IPv6 Service History

1996: NTT Labs started one of the world's largest global IPv6 research networks

1999: NTT Com begins IPv6 tunneling trial for Japanese customers

2001: NTT Com pioneers worlds first IPv6 connectivity services on a commercial basis

2003: Verio launches IPv6 Native, Tunneling, and Dual Stack commercial service in North America

2004: NTT IPv6 Native and Dual Stack services available around the globe

NTT Communications IPv6 Service History

1998: Verio begins participation in PAIX native IPv6 IX

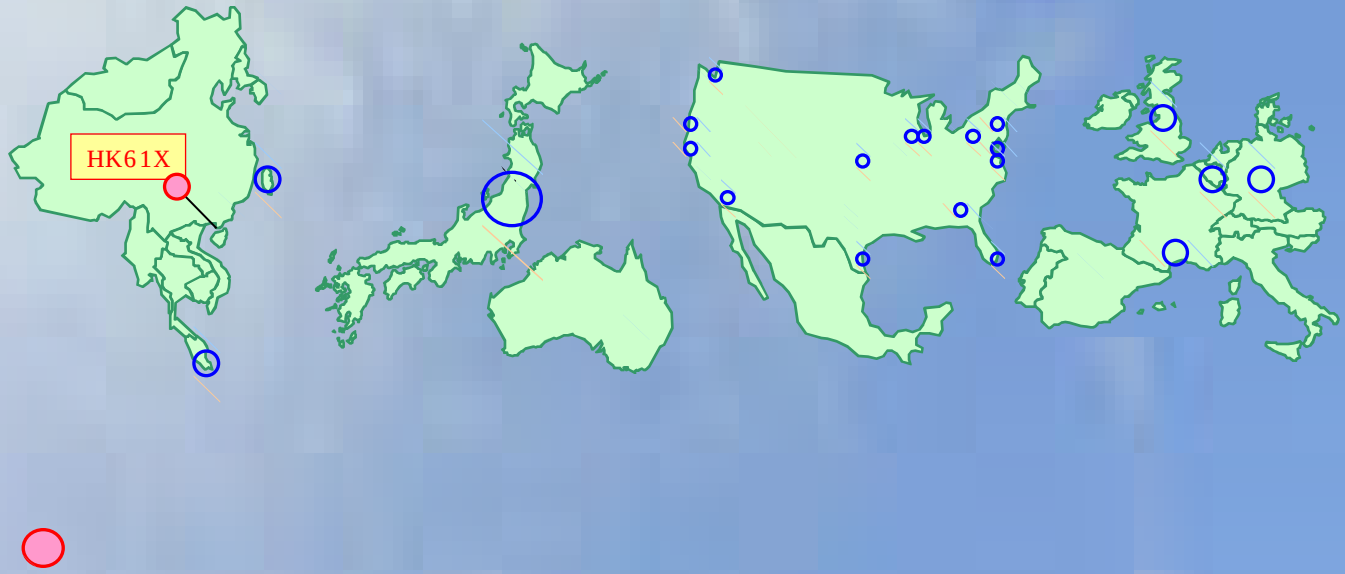
2000: Verio obtains IPv6 sTLA from ARIN

2002: World Communications Awards (WCA) awards NTT Communications with "Best Technology Foresight" for its IPv6 Global products

2003: Communications Solutions magazine names NTT/VERIO IPv6 Gateway Services "Product of the Year"

2004: NTT Com wins the World Communications Awards "Best New Service" award for IPv6/IPv4 Global Dual Service

NTT Communications Global IP Backbone



IPv6 Continues to Mature

- **As IPv6 matures, tools are being developed to help network operators using IPv6 to manage their networks with more efficiency and with greater ease.**

- **This maturation has led to advancements in the following areas:**
  - **Bringing IPv6 to the Web Hosting Environment**
  - **Network Management with IPv6**
  - **IPv6 and SSL -> Security**
  - **Mobile IP**

Bringing IPv6 to the Web Hosting Environment

- **By utilizing NTT Communications Virtual Private Server (VPS) Hosting Solutions customers will soon be able to utilize IPv6 within a web hosting environment.**

- **This advancement will launch in the first quarter 2005 in the Asia Pacific region.**

- **The VPS product will first be commercially available in Asia Pacific then in the United States.**
  - United States launch date is TBD.

History of Network Management and IPv6

- **Then - Ping**

- **Now - Simple Network Management Protocol**
  - A set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units *(*PDUs*)*, to different parts of a network.

  - In August 2004, we saw the first integration of an IPv6 protocol stack with an IPv6 SNMP agent. This is a solution for deploying standards-based IPv4 and IPv6 networking and management capabilities for embedded systems.

  - "...customers will benefit from these new capabilities as they are creating the next generation of embedded IPv6-enabled applications."
    - Dan Mender, Director, Business Development at Green Hills Software

- **Tomorrow –**
  - Additional network management tools are needed.

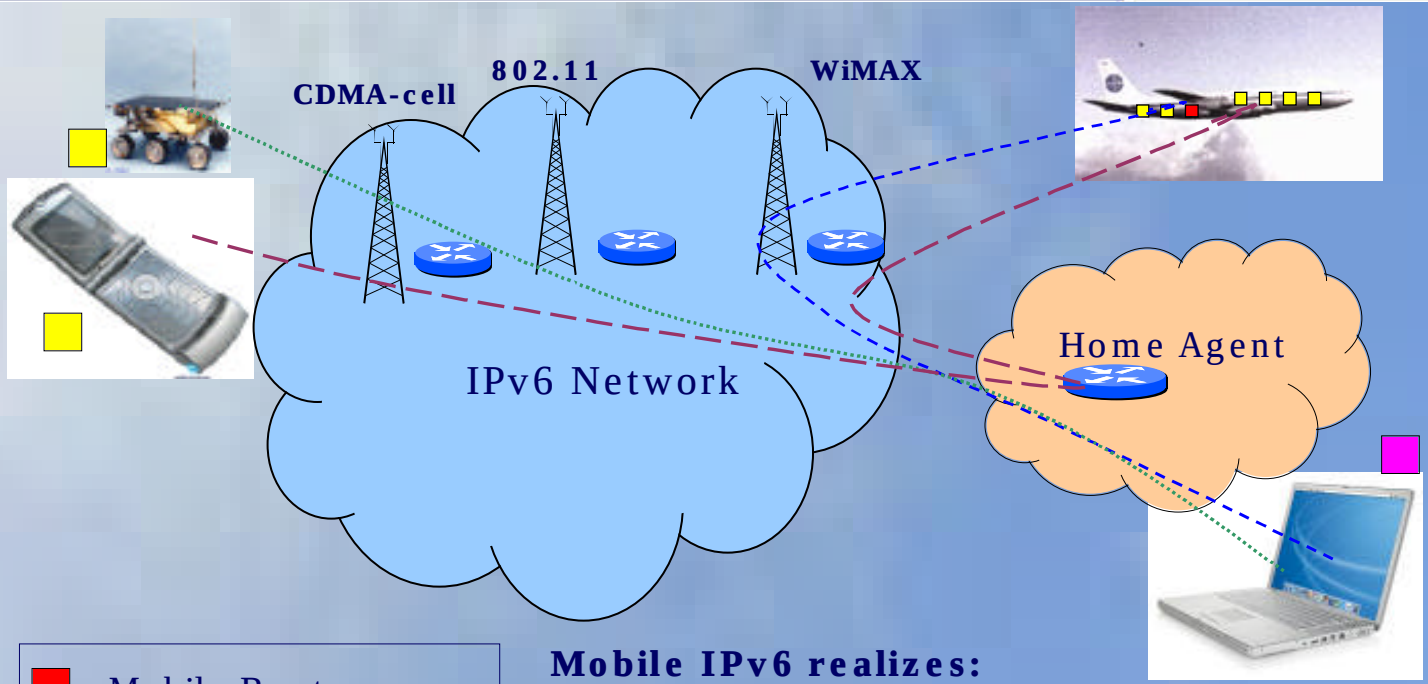
IPv6 vs. Secure Sockets Layer (SSL)

- **Key management issue**
  - **IPv6**
    - One of the most important mechanisms, the key exchange, is still not defined for the IPv6 protocol. It is vital that this will be an universal standard.
    - As long as no such mechanism exists, IPv6 security can be used only on a very limited basis as manual key exchange is not realistic in large networks and particularly not on the Internet.
  - **SSL**
    - SSL has built in key exchange capabilities. It supports Server key exchange messages as well as Client key exchange messages.
    - With this capability of key exchange, SSL can be used for spontaneous secure communications between a Server and a Client.
  - **At our booth (#7), NTT Communications demonstrated our solution to this problem with the m2m-x product platform.**

IPv6 vs. Secure Sockets Layer (SSL)

- **Encryption**
  - **IPv6**
    - IPv6 has two possibilities to provide confidentiality:
    - **Tunnel mode ESP (Encapsulating Security Payload)**
      - In this mode, the original IP datagram (including header) is encrypted. This entire ESP frame is placed within a new datagram having an unencrypted IP header. All additional unencrypted information as routing header are placed between the IP header and the encapsulated security payload.
    - **Transport mode ESP (Encapsulating Security Payload)**
      - In this mode, only the payload is encrypted. The IP header and the IP options are unencrypted and are used for routing the packet. The receiver decrypts the ESP and uses the unencrypted header as IP header further if necessary.
      - The transport mode ESP provides approximately the same capabilities as the SSL protocol except that it provides its services to all packets.
  - **SSL**
    - SSL only has the option to encrypt the whole (HTTP, NNTP or SMTP) packet on its layer.

Mobile IPv6



Mobile Router
Mobile Node
Correspondent Node

Mobile IPv6 realizes:

- True end-to-end connectivity and session continuity
- Achieves anytime, anywhere, anyplace availability
- Seamless handoff from network to network
- End-to-end security achievable
- Application independence

Mobile Communication with IPv6

- **Support for Mobile IP is built into IPv6**
  - IPv6 Neighbor Discovery and Address Autoconfiguration allow hosts to operate in any location without any special support
  - Signaling mechanisms built into to the protocol to eliminate triangular routing
  - Foreign Agents are eliminated in Mobile IPv6
  - IPv6 enables simple and efficient mobile communication

DoD's "NetCentric Soldier" Technical Vision

- **Soldiers, weapons, vehicles, aircraft, and other systems are networks.**
- **Net Centricity demands ubiquity, mobility and ad hoc networking, Quality of Service, Security, and manageability, all of which IPv6 provides.**
- **Out Model**
  - **private data**
  - **data push/broadcast**
  - **separate infrastructures**
  - **interoperability problems**
  - **individual stovepipes**
  - **perimeter security**
- **New Vision**
  - **shared data**
  - **bi-directional data communications**
  - **collaboration**
  - **end to end security**
  - **mobility and ad hoc networking**
  - **QoS**
  - **manageability**
- **Deploy 'net-ready' nodes of platforms, weapons, and forces.**

Additional Information

- We hope you had an opportunity to stop by the NTT Communications booth (#7) for information and a demonstration of our applications utilizing IPv6.

- Additional questions and comments about IPv6 can be addressed to usipv6@verio.net