NIST's Guidance on IPv6:

Helping Agencies to "Look under the Hood"

Sheila Frankel

Computer Security Division

NIST

sheila.frankel@nist.gov

What is IPv6?

- Internet Protocol version 6

- The next generation Internet Protocol

- A large set of interconnected protocols that govern Internet operations and behavior at every level of the protocol stack, from applications down to the physical layer

Background

- Defined by the Internet Engineering Task Force (IETF: www.ietf.org)
- Internet Drafts (IDs)
- Requests for Comment (RFCs)

Background (cont'd)

- **Working groups**
  - ☐ IP version 6 (IPv6): 48 RFCs, 19 IDs
  - ☐ Mobility for IPv6 (MIPv6): 2 RFCs, 11 IDs
  - ☐ MIPv6 Signaling and Handoff Optimization (mipshop): 3 IDs
  - ☐ IPv6 over Low power WPAN (6lowpan): 2 IDs
  - ☐ Site Multihoming in IPv6 (multi6): 1 RFC, 9 IDs
  - ☐ IPv6 Operations (v6ops): 9 RFCs, 14 IDs
- **Disbanded working groups**
  - ☐ Next generation transition (ngtrans): 15 RFCs
  - ☐ IPv6 Backbone (6bone)
  - ☐ IPv6 MIB (ipv6mib)

Advantages
(Real and Perceived)

- Increased number of addresses
- Increased ease of network management and configuration
- Simplified/expandable IP header
- End-to-end/peer-to-peer communications
- Mobility
- Security
- Multicast/multimedia
- Quality of service

What is IPsec?

- Security provided at the Internet layer of communications
- Provided by security headers
  - ☐ Encapsulating Security Payload (ESP)
  - ☐ Authentication Header (AH)
- Dynamic negotiation, update and management of symmetric secret keys
  - ☐ Internet Key Exchange (IKE)
- Optional for IPv4, mandatory for IPv6

Advantages of IPsec

- Implement once, in a consistent manner, for multiple applications

- Centrally-controlled access/security policies

- Enable multi-level, layered approach to security

Types of Security Provided by IPsec

- Data origin authentication
- Connectionless integrity
- Replay protection
- Confidentiality (encryption)
- Traffic flow confidentiality
- Access control

Types of Attacks Prevented by IPsec

- Address spoofing
- Replayed packets
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)
- Traffic analysis

NIST's Advice

- Create a business case
- Acquire IPv6-capable hardware/software
- Acquire expertise
- Support research

Until …

OMB Directive

- Partial Inventory and impact analysis (11/15/05)

- Transition plan (2/06)

- Complete inventory and impact analysis (6/30/06)

- Operational IPv6 backbone (6/30/08)

- NIST FIPS and/or guidance

NIST IPv6 Guidance Document

- **Introduction**
    - IPv4 Limitations
    - IPv6 Benefits/Advances
- **IPv6 Protocols**
- **IPv6 Core Services**
- **IPv6 Security and Privacy**
    - Dual stack threats and attacks
    - IPv6 threats and attacks
    - IPsec
    - IPv6 security controls

NIST IPv6 Guidance Document (cont'd)

- **IPv6 Deployment**
  - ☐ Transition
  - ☐ Integration
  - ☐ Configuration
  - ☐ Testing

Security issues

- **Transition complexity**
- **New protocols**
  - Lack of operational experience
  - Interactions
- **Address scanning no longer practical**
- **Address autoconfiguration vs. privacy addresses**
- **IPsec complexity, interoperability, applicability, interaction with other procotols**

Complications

- **Missing pieces**
  - Availability and completeness of implementations
- **Protocol interactions**
- **Cost**
  - Testing
  - Transition
- **Education of administrators and users**
- **Unknowns**
  - Performance
  - Scalability

Transition

- **Dual stack**
- **Tunneling**
  - ☐ Manual or static
  - ☐ Automatic
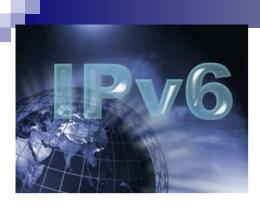 - ☐ IPv6-over-IPv4
  - ☐ IPv4-over-IPv6
- **Translation**

Transition (cont'd)

- Security/complexity challenges
- Entities involved:
    - Hardware (network and host)
    - Software (operating system and applications; local and client/server)
- Applications may be a major impediment to an easy transition

IPv6 Myths (or partial truths)

- **Restoration of end-to-end communications**
  - ☐ Topology-defined network
  - ☐ Policy-defined network
- **The end of NAT (Network Address Translation) boxes**
- **IPsec is the "silver bullet"**

Who needs it now?

- **DOD**
  - Soldier as "network"
- **First responders**
  - Rapid network set-up and configuration
  - Mobility
  - Security

Moonv6

- **Joint effort**
  - ☐ North American IPv6 Task Force (NAv6TF)
  - ☐ University of New Hampshire
  - ☐ DOD
  - ☐ Commercial ISPs
- **Testing underway:**
  - ☐ Core IPv6 specifications
  - ☐ Transition mechanisms
  - ☐ Routing
- **Not yet tested:**
  - ☐ Mobility
  - ☐ Security

IPv6 workshops/info

- **North American V6 Task Force (NAv6TF)**
  - Jim Bound (jim.bound@hp.com)
- **IPv6 Forum**
  - Latif Ladid