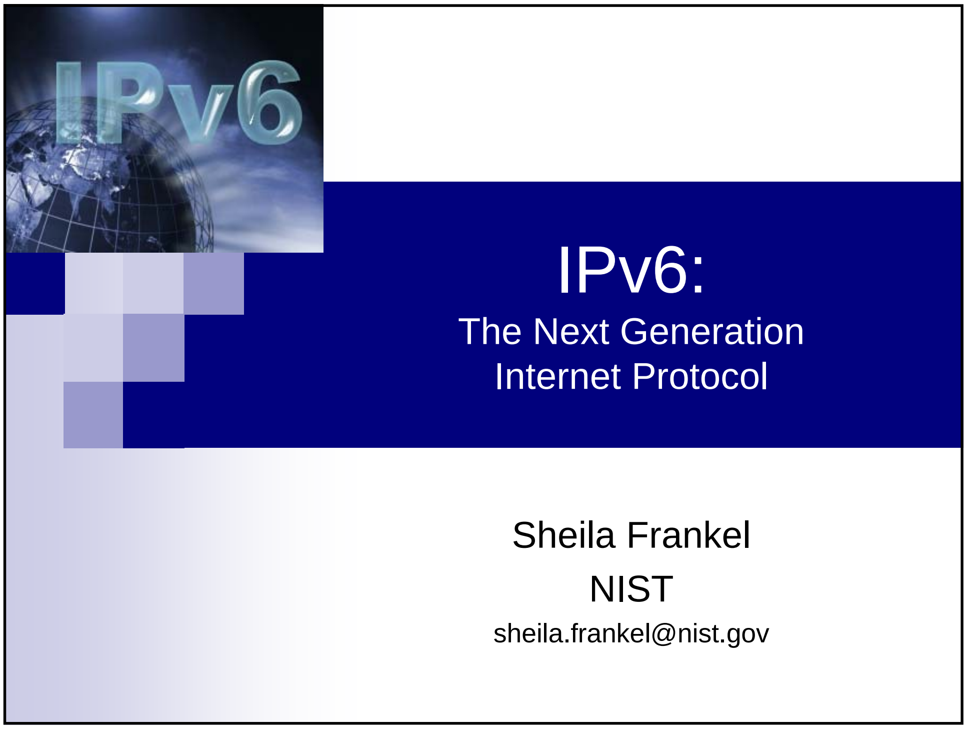


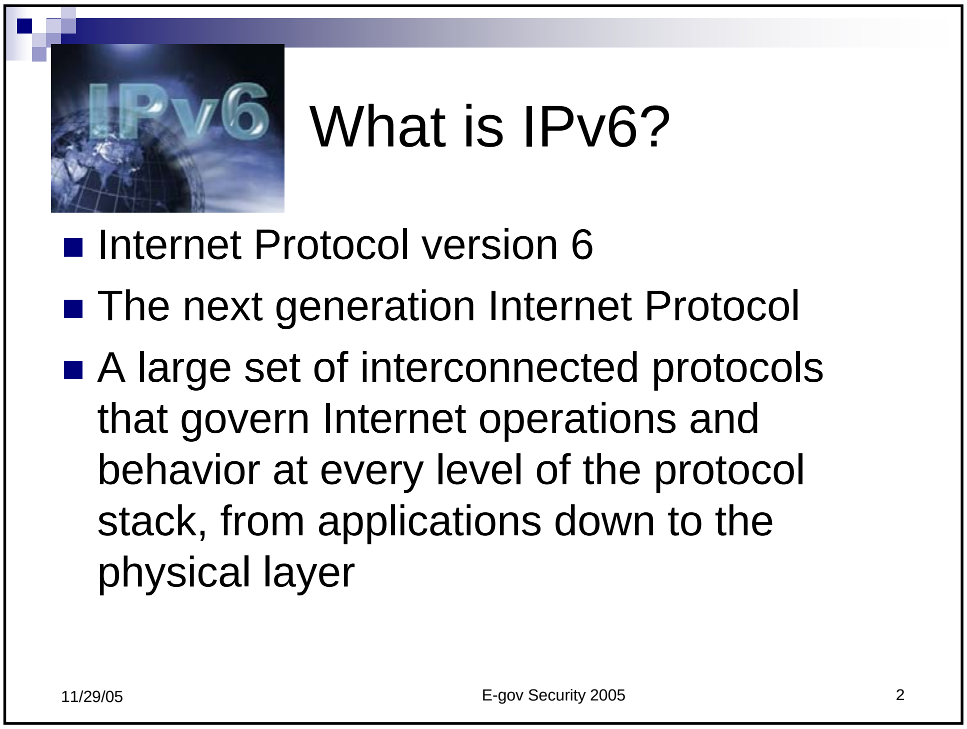
IPv6:

The Next Generation Internet Protocol

Sheila Frankel

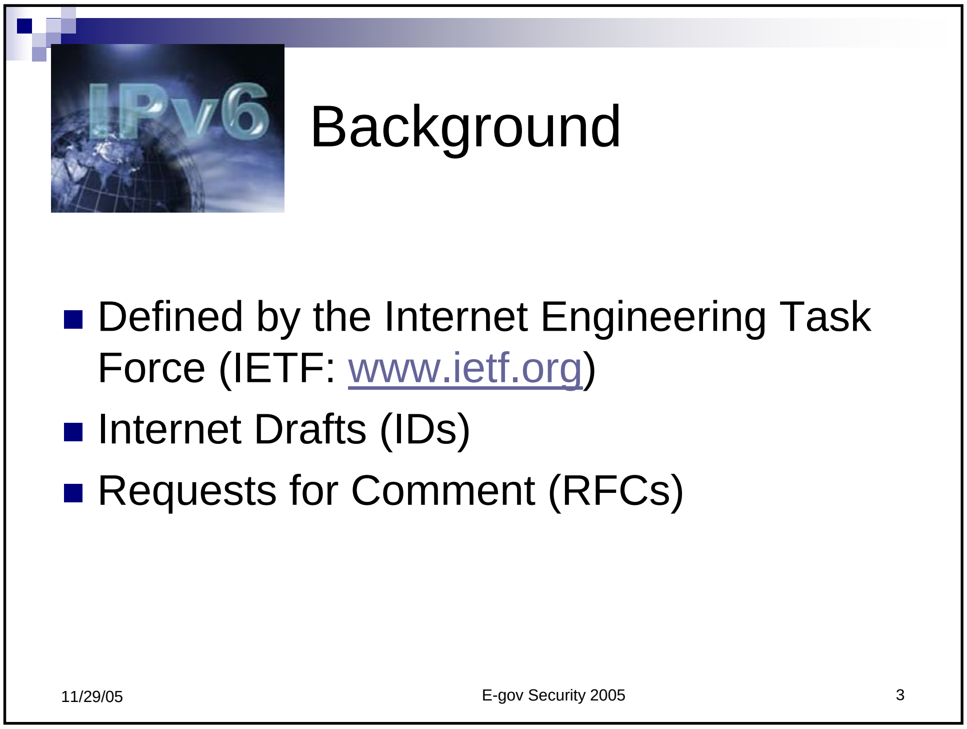
NIST

sheila.frankel@nist.gov



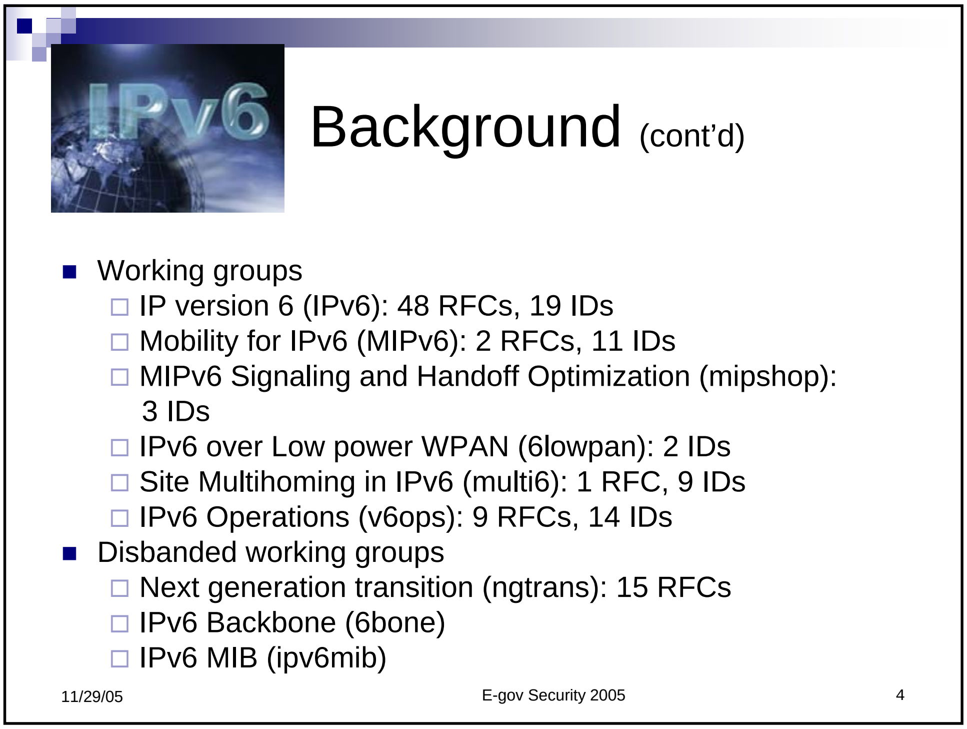
What is IPv6?

- 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

- Increased number of addresses
- Increased ease of network management and configuration
- Simplified/expandable IP header
- Device mobility
- Quality of service (QoS)
- Multicast/multimedia
- IPv4 operational experience/new technology
- Increased security: IP security (IPsec)

Transition

- Dual stack
- Tunneling
  - □ Manual or static
  - □ Automatic
  - □ IPv6-over-IPv4
  - □ IPv4-over-IPv6
- Translation
- Security/complexity challenges

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

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

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

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”