FOR OFFICIAL USE ONLY

IPv6 Technology and Transition Challenges

Send to Overton & Manley

S. Chakravorty

R. C. Sivills

2 Dec. '03

Center for Innovative Computing and Informatics

FOR OFFICIAL USE ONLY

MITRE

Purpose

- Present IPv6 technology and DoD transition challenges
- Share the OSD perspective of IPv6 vision and goals
- Share technical and programmatic know-how - help build a consensus within the Mitre community on various IPv6 issues
- Discuss items that need further engineering and/or research
- Help DoD implement IPv6 technology effectively

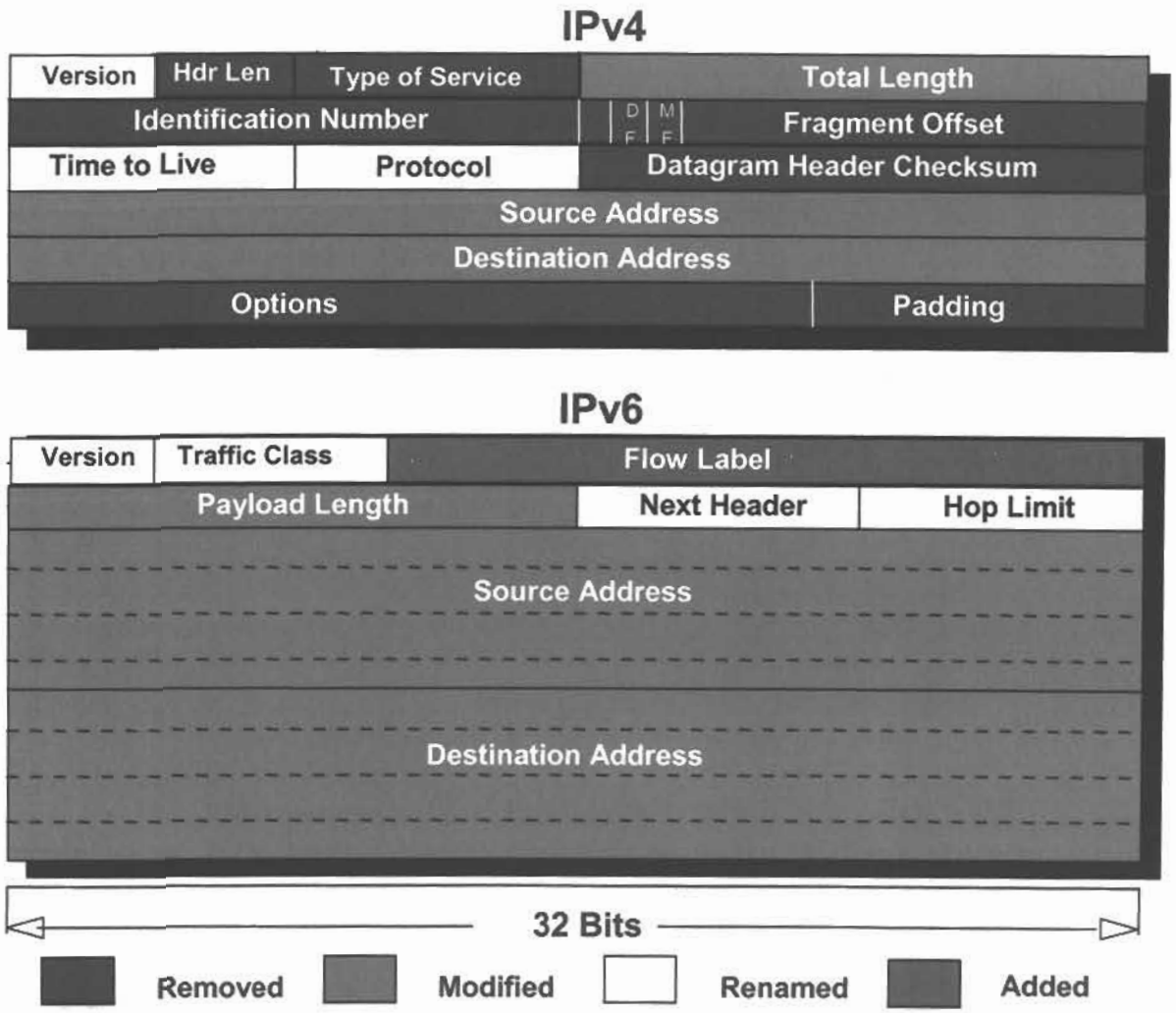
Agenda

- **Brief Background - IPv6 technology and transitions highlights**
  - Scope: only DoD
- **Identify <u>select</u> IPv6 technology challenges**
  - Present new concepts from the 58th IETF Meeting
  - Discuss available solutions
  - Future scrubs and enhancements
- **DoD transition goals and plans**
- **Transition issues and challenges**
  - Proposed solutions
- **Summary and Q&A**

This briefing does not address DoD agency-specific issues except for those known to us, such as from the DREN briefing.

IPv6 Technology Highlights (1)

- A new stack – starting with the packet to routing protocols to QoS to ND to security, etc.

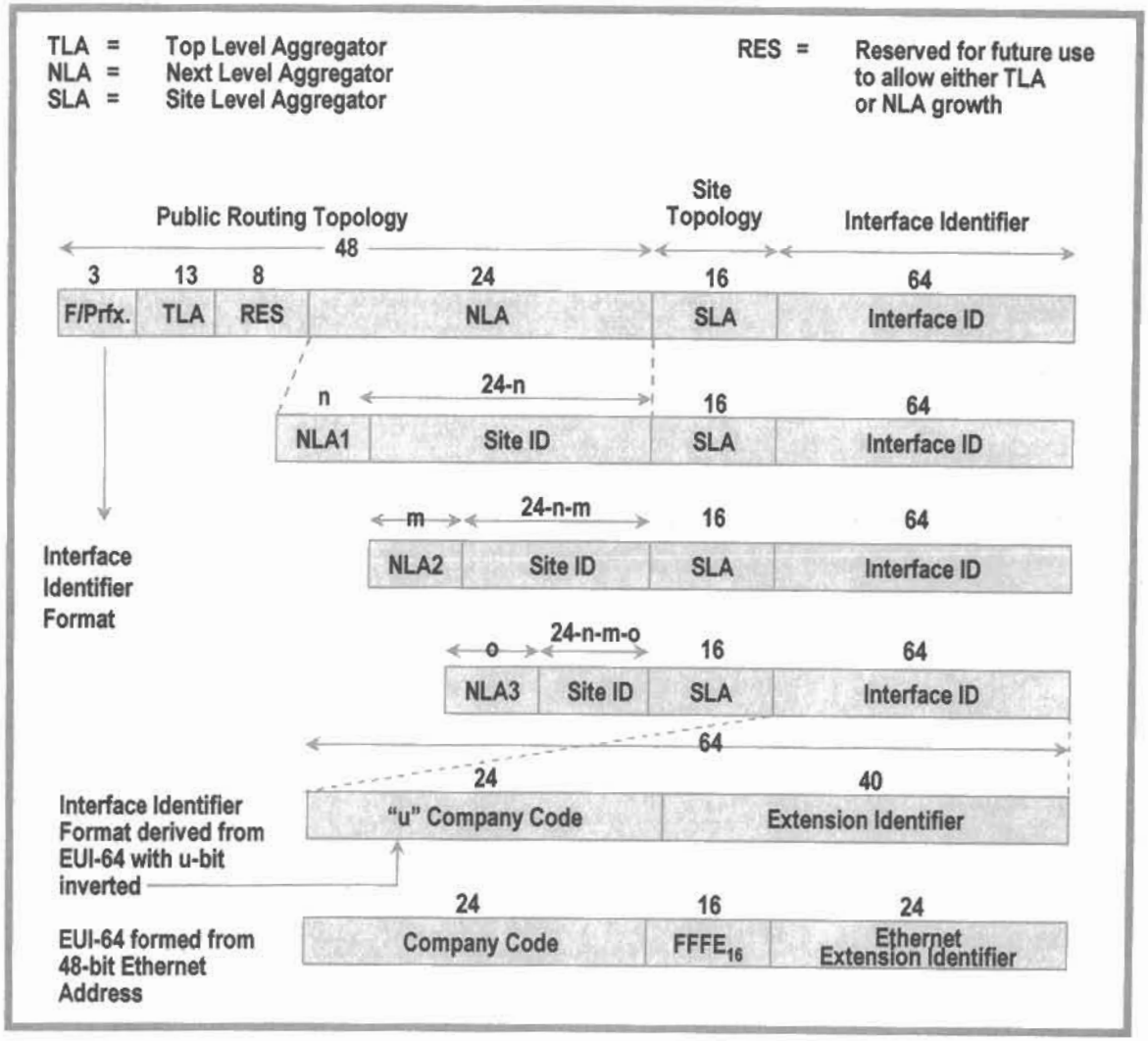


MITRE

IPv6 Technology Highlights (2)

Aggregatable Global Unicast Address

Deprecated (RFC 2373)



MITRE

IPv6 Technology Highlights (3)

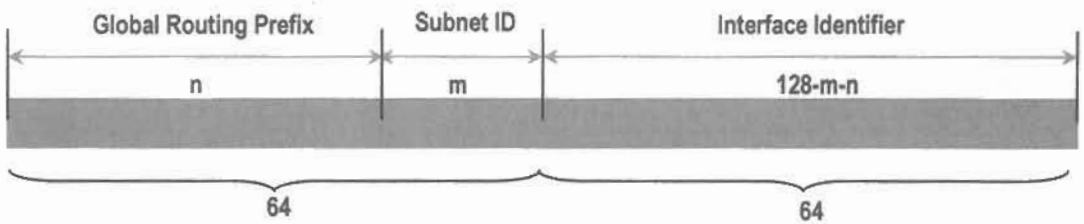
Global
Unicast Address
Format

Revised (RFC 3513)
Allows for IPv4/v6 mixed environs.
x:x:x:x:x:x:d:d:d:d

Prefixes of variable bit-lengths – like in IPv4 CIDR, however, if not starting with 000, need interface ID of 64 bits

Distr. - hierarchical

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00……0 (128 bits)	::/128
Loopback	00……1 (128 bits)	::1/128
Multicast	11111111	FF00::/128
(Additional bits for types of Multicasts)		
Link-local Unicast	1111111010	FE80::/10
Site-local Unicast	1111111011	FEC0::/10 (????)
Global Unicast	Everything else	

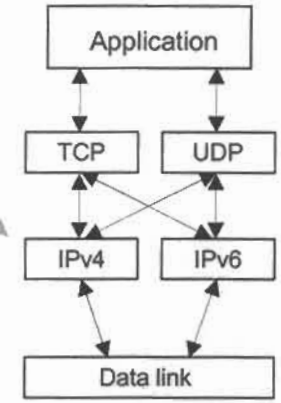


64 bits => $2^{64} = 18.447 \times 10^{18}$ = 18.447 Billion billions

MITRE

IPv6 Technology Highlights (4)

- **Tunneling Mechanisms – "Transition Toolkit" - IETF**
  - Configured or Automatic Tunneling of IPv6 over IPv4 (RFC 2893)
    - Dual stack in hosts and routers
    - IPv4-compatible IPv6 addresses (for auto. tunneling)
      - **0:0:0:0:0:0:[IPv4 Address]**



  - 6to4 (RFC 3056)
    - IPv4 network as pt.-to-pt. link layer - no explicit tunnel setups
    - Use of relay routers;
    - Address - **2002:[IPv4 Addr]::/48**
    - Limited scalability
  - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) (draft-ietf-ngtrans-isatap-16.txt)
    - Intra-site – no need for IPv6 routers
    - Automatic IPv6/v4 tunneling – no multi-cast support
    - IPv4 infrastructure as a Non-Broadcast, Multiple Access (NBMA) link layer
    - Address format - **64-bit global/link prefix:00005EFE:[IPv4 Addr.]**
    - Being revised

IPv6 Technology Highlights (5)

- **Transition Mechanisms (contd.)**
  - Toredo
    - IPv6 for hosts through NAT-ing
    - Approach abandoned by the IETF
- **Other**
  - Translation at IP or transport layer
    - Stateless IP/ICMP Translation Algorithm (SIIT) – RFC 2765
    - Network Addr. Protocol Translation (NAPT) – RFC 2766
    - Bump-in-the-stack – translates IP headers
    - Bump-in-the-api – translates API functions
    - Transport-layer Translator
  - Tunneling IPv4 over IPv6
    - DSTM (with DHCP, RPC, TSP)
  - Application-layer Gateways (ALGs)
  - Tunnel broker (draft status?)

Technology Challenges (1)

- **Transition/Tunneling**
  - Many techniques – not *one* for all scenarios
  - Concepts from the IETF with issues and solutions
    - Introduction of IPv6 into ISP networks <draft-lind-v6ops-isp-scenarios-01.txt>
      - Many scenarios but no best solution offered – adopted as WG document
    - Tunneling in small end sites <draft-chown-v6ops-unmanaged-connectivity-00.txt>
      - Drivers for IPv6 tunneling – on-going work
    - Dual Stack IPv6 on by Default <draft-ietf-v6ops-v6onbydefault-00.txt>
      - When dual stack nodes with IPv6 enabled is introduced in IPv4 or mixed environments: app. connection delays, poor connectivity and security
      - Solutions: use default address selection (v4 before v6), not leave out dest. address as unusable, abort TCP connection attempts when receiving a soft-error
    - NAT-PT Applicability <draft-satpati-v6ops-natpt-applicability-00.txt>
      - Based on use of SIIT – stateless IP/ICMP translation
      - Issues – translation semantics difficult to use – some ICMP error messages do not have ICMPv6 counterparts, IPv4-mapped addresses in basic API as well as by SIIT – ambiguous dual use, a security threat, multicast will not work – cannot map an IPv4 multicast address into its IPv6 counterpart, ALGs are required for application deployment, many others
      - Not very deployable - work to continue
  - Hard to ascertain which ones will succeed in the market (DREN and others)
    - Need for selecting the best technique for DoD
    - Recommendations from the IETF
      - Don't add AAA records until services on a node IPv6
      - For DNS, use of AAAA records instead of A6
      - Use AH/ESP for greater security – ingress filtering

Technology Challenges (2)

- Good News: In Japan, IPv6/IPv4 dual-stack Internet services are being provided successfully
  - <draft-shirasaki-dualstack-service-02.txt>
  - Issues - DNS discovery at customer sites, solution –DHCPv6-lite

- **Neighbor Discovery (ND)**
  - From the IETF
    - IPv6 ND Discovery On-link Assumption Considered Harmful
      - <draft-lind-v6ops-onlinkassumption-00.txt>
      - Undefined in multihomed scenarios and has security implications
      - Work in progress
    - For the NAT Challenge
      - Draft:: Bridge-like ND Proxies – bridge multiple links into single entity => one prefix for multiple links <draft-thaler-ipv6-ndproxy-01.txt>
      - Multiple issues
      - Proposed solution: STP packet after the IPv6 header but needs IANA allocation of the Next Hdr. Option (for STP over non-802.11 media)
      - Removes incentive use NAT, simplifies management

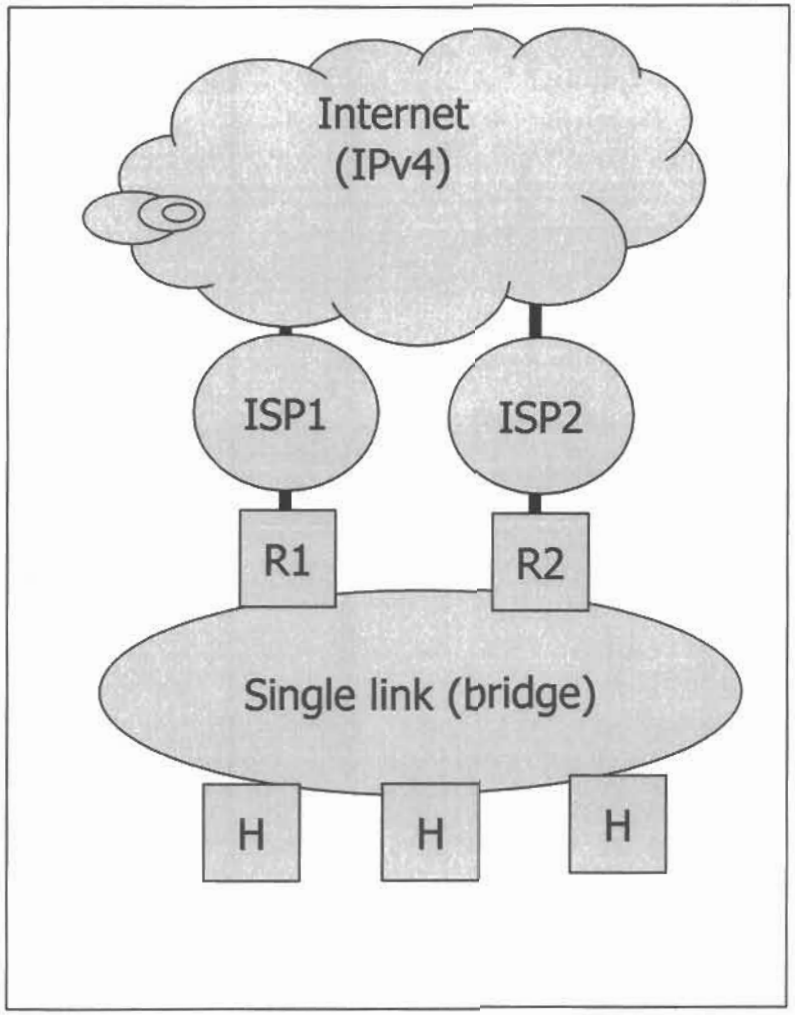
- **Routing**
  - Larger addresses – more memory, processing
  - Longer prefixes – greater amount of matching (but no subnet matching)
    - Discussions in RFC 3178
  - Addresses are not hierarchical (*aggregatable?*) anymore
    - Larger routing tables

Technology Challenges (3)

- Multiple routing protocols in use
  - OSPFv2 for IPv4 along with OSPFv3 for IPv6 – incompatible, other
- Authentication issue between OSPFv3 routers from different sources?

- **Addressing**
  - Hierarchical versus the new "*flat*" addressing schema
  - Address distribution is hierarchical through organizations
    - ICANN to ARIN (RIR = /23) to ISP (LIR = /32) to organization (64k Site = /48)
    - Advantage – greater flexibility, more space
  - No operational guidelines on how to use global and local-use unicast addresses
    - A current Internet draft provides some help for MANET and test network scenarios
  - Need for multiaddressing for mobility and multihoming
    - Barriers to adoption, admin. overhead and operational efficiency are some of concern
    - Solutions proposed in - <draft-crocker-multiaddr-analysis-01.txt>
    - Shim layer between IP-EP (End-Point) ?
  - Renumbering networks – work in progress in the IETF
  - DNS - DNS responses are limited to 512 bytes, so only two AAAA records can be added to the root zone without making any changes to the protocol, servers, or client resolver libraries (DREN)

Technology Challenges (4)



- **Multihoming**
  - A site's ISPs advertises addr. prefix to some or all of their upstream connections and the route for the prefix may propagate to all of the routers connected to default-free zone (DFZ)
  - Scalability Issue:
    - The current Internet routing architecture does not provide for a scalable multi-homing solution
    - Proposed solution - multi-addressing mechanism and source address selection mechanism instead of using the routing system
  - TCP Issues: In the existing TCP, only one local and one remote address is used through a TCP session, even when a client or a server is located under multi-homed site and has multiple IP addresses
  - When a network outage occurs and the access-line associated with the local and remote addresses is down, the TCP session itself gets lost even if another access-line is alive

Note: Materials covered under Multihoming are from IETF drafts and RFCs.

Technology Challenges (5)

- **Multihoming contd.**
  - Proposed solution: Use of special TCP MH options with the remote peer <draft-arifumi-tcp-mh-00.txt>
    - A session can even switch from IPv4 address to IPv6 address and vice versa
    - These processes resemble SCTP's [SCTP] multi-homing method
  - Simple Dual Homing Experiment <draft-huitema-multi6-experiment-00.txt>
    - Issue: No coordination between ISP
    - Proposed solution: Each ISP allocates a prefix or each ISP allocates an IPv4 address, and the routers use 6to4
      - Multi-Addressing
        - Each router advertises a prefix
        - Hosts configure addresses with each prefix

Technology Challenges (6)

- **Multihoming contd.**
  - Five issues need resolution
    - Ingress filtering - host picks address from ISP1, sends through R2?
    - Dead default exit router, or dead ISP - host keeps sending packets through a black hole?
    - Inbound connection through wrong ISP - peers send packet to the black-holes address?
    - Maintaining TCP connections - keep TCP going if the Router or the ISP fails?
    - Use the right exit/entrance – may be some amount of load balancing
  - Ideas, Ingress Filtering
    - Choice by host - host treats multiple "auto-config" prefixes as "sub-interfaces", associates individual IPv6 address and default router. - easy to implement in "new hosts".
    - Redirect at routers - no need for tunnels in single link network, guarantees that "old hosts" keep working.
    - There may be other solutions - new services, ISP involvement, etc.
  - Ideas, dead exit router or dead ISP
    - If the router notices the problem - advertises prefix as "deprecated", or stop advertising, will not be used for new connections, will work for old and new hosts.
    - If the problem is not really detected - new host tries multiple source addresses when establishing a new connection, host may keep track of the quality of each router connection

Technology Challenges (7)

- **Multihoming concluded**
  - Ideas, peer using dead address
    - If the problem is detected - update the name server?
    - If the problem is not detected - DNS advertises multiple addresses, peer tries several addresses - issue: TCP timers?
- **Application Interface**
  - In a mixed environment, client application cannot be certain of the version of peer application by only doing a DNS name lookup
    - Bad practice to add an AAAA record for node that does not support all the services using IPv6 - consequence, the application has to be able to handle all IP versions returned from the DNS
    - One proposed solution: "Wrapper application" which performs certain tasks (like figures out which protocol version will be used) and calls the IPv4/IPv6-only applications as necessary
    - Another: Version independent applications
    - Work in progress at the IETF on finding effective solutions

Technology Challenges (8)

- **Security**
  - Security of tunneling: needs to be aware that while a tunnel is a link (as defined in [RFC 2460]), the threat model for a tunnel might be different from other links
  - Proposed solution: Need to verify that the IPv4 addresses in the encapsulated packet matches what was configured for the tunnel
  - Added precaution: Use of ingress filtering in IPv4
  - Recommendation: an implementation must treat interfaces to different links as separate, e.g. to ensure that Neighbor Discovery packets arriving on one link does not effect other links - this is especially important for tunnel links
    - When dropping packets due to failing to match the allowed IPv4 source addresses for a tunnel the node should not "acknowledge" the existence of a tunnel, otherwise this could be used to probe the acceptable tunnel endpoint addresses
  - Redirection Attacks
    - Proposed solutions: NOID draft – Introduces concept of sets of locators to prevent redirection attacks
      - Shim layers under the transport protocols treating the set as a unit

      draft-nordmark-multi-noid-01.txt>
    - SIM draft – This proposed solution uses crypto-based identifiers [CBID] properties to perform enough validation to prevent redirection attacks

      <draft-nordmark-multi-sim-01.txt>

Technology Challenges (9)

- **Security concluded**
  - IPSec for IPv6 not ready – few implementations, HAIPE version 2 includes IPv6
  - Product support is generally weak - most implementations are functionally incomplete with respect to IPv6 IPSec, even IPv4 implementations need improvement (DREN)
- **Mobility**
  - IPv4-like challenges
    - MANET and other concepts
  - Location Independent Networking (LIN6) - new concept from the IETF
    - Introduces node id (LIN6 generalized and LIN6 addr.) – for each node
    - Uses a mapping agent
    - TCP connections and security associations can be preserved when the node moves – even when the node changes its current interface - <draft-teroka-ipng-02.txt>
- **QoS**
  - IPv4-like challenges – use of flow labels
  - IPv6 includes Next Header identifier of 46 for RSVP
  - DS-TE - IPv6 capable
  - RSVP TE – EXPLICIT_ROUTE Object (ERO) and RECORD_ROUTE Object (RRO) sub-objects definitions includes IPv6 prefix

Technology Challenges (10)

- **Network Management**
  - Managed objects for managing tunnels of any type
    <draft-thaler-inet-tunnel-mib-00.txt>
    - Allows extensions for protocol and security specific objects
  - Network management tools are not there yet (DREN)
- **Header Compression**
  - No commonly implemented, robust solution
  - RFC 2507 – includes TCP, UDP, IPv4, and IPv6 base and extension headers, packets may be grouped together into packet streams, use of context id's (CIDs) for decompression
  - On-going work
  - Propose DoD/Mitre initiatives
- **NTP (Network Time Protocol)**
  - RFC 2030, SNTP
  - Software available
  - Commercial product available since 2001 – GPS source (see Hexago)
  - DREN: There are no commercially available IPv6 NTP servers
    - The first production release of NTP 4.x code with IPv6 support was on 15 Oct 2003

Technology Challenges (11)

- **Hardware Availability**
  - Network hardware not ready – software implementation of IPv6 => performance penalty
  - IPv6 – new stack => might require memory and/or processor upgrade (DREN)
  - Should not be a major problem – memory and processor prices keep coming down
- **Miscellaneous**
  - Test Tools and Appliances
    - Most testing and assessment tools do not support IPv6 (DREN)
    - Performance testing tools and appliances are lacking (DREN)
    - Many important components are either not IPv6 aware or cannot operate using IPv6 protocols (DREN)
    - Peripherals and appliances like printers/scanners are not IPv6 aware (DREN)
  - But the vendors are moving in the direction - providing the tools and appliances and these problems should go away with time

Summary - Technology Challenges

- **Many challenges exist but solutions are aggressively being pursued in the IETF and by the vendors**
- **IPv6 engineering and deployment efforts are on the increase**
  - Need to coordinate Services efforts within Mitre and DoD
  - Need to push standards bodies and vendors
  - Need advance inputs for problem resolution
- **We see IPv6 as a high-priority system engineering process**
- **Recommendations:**
  - Active participation in standards meetings
  - Close collaboration with the vendors and research communities

References

- *Internet drafts and RFCs as identified in the main briefing*
- *S. Hagen, IPv6 Essentials, O'Reilly*
- *M. Blanchet, Hexago, Briefing on IPv6 Transition – Main Mechanisms, IPv6 North American Summit, June '03*
- *S. Chakravorty, IPv6 Technology – an Overview, Briefing for the Army, March '00*
- *Dr. R. Nieporent and Dr. S. Bhanji, Mitre, IPv6 – TCP/IP II, Johns Hopkins Univ. Lecture*
- *Ron Broersma, DREN Chief Engineer, DREN and IPv6 Briefing, Nov 19 2003*
- *C. Semeria, RSVP Signaling Extensions for MPLS Traffic Engineering, Juniper Networks, Inc., 2000*

Transition Strategy, Planning and Challenges

A Brief History

• May 03	DoD IPv6 Working Group Formed
• Jun 03	ASD/NII Memo—IPv6 North American IPv6 Global Summit
• Jul 03	Formed JTA IPv6 WG Identified initial set of IPv6 standards
• Aug 03	Initial Draft of DoD IPv6 Transition Plan
• Sept 03	ASD/NII Memo—IPv6 Interim Guidance ASD/NII In Progress Review IPv6 Standards Profile
• Oct 03	Joint Staff Msg—Operational Criteria
• Dec 03	Coordination Draft of DoD IPv6 Transition Plan

The ASD/NII Vision and Goals

The Vision: "People throughout the **trusted, dependable and ubiquitous network** are empowered by their ability to access information ……"

The Goals: **"Make information available on a network that people depend on and trust.**
"Populate the network with new, dynamic sources of information ….
"Deny the enemy advantages and exploit weaknesses."

IPv6 is a critical link in the Department's drive toward Net Centricity.

ASD/NII Guidance
9 June 03 Memo—IPv6

- Directs enterprise-wide deployment of IPv6
- Recognizes an extended transition period will be required
- Establishes a strategy to minimize overall transition costs
- Effective 1 Oct 03 all GIG assets being developed, procured or acquired shall be IPv6 capable
- Segments of GIG to transition to IPv6 during FY 05-07
- IPv6 pilots, demos and testbeds to be identified
- No use of IPv6 on networks with operations traffic at this time
- DISA to initiate actions acquire DoD IPv6 address space
- DISA retains its enterprise role as CRA for IP address space
- Directs development and publication of an IPv6 Transition Plan

NII's Goal--Transition to IPv6 by FY 08

ASD/NII Guidance
29 Sept 03 Memo—IPv6 Interim Guidance

- **Provides interim guidance on the requirement that all GIG assets being developed, procured or acquired after 1 October 03 shall be "IPv6 capable"**
- **Provides definition of what it means to be** "IPv6 capable"
- **Identifies the** IPv6 standards profile **to be used**
- **Establishes a provisional** waiver process
  - Component CIOs can waive IPv6 requirement based on criteria
  - DoD CIO shall have ten days to review waiver rationale

The Strategy

- **Ensure that information technology built or bought today will operate in the IPv6 world of 2008.**
  - Minimizes transition costs
  - Component acquisition executives and CIO responsibility
- **Use IPv6 implementation pilots, testbeds and demonstrations in FY 04-07 to minimize risks**
- **Maintain IPv4 compatibility during transition**
- **Maintain adequate IA posture during transition**
- **IPv6 transition to occur in an integrated, timely manner**
  - **IPv6 Transition Implementation Panel** —DCIO Chair
    - Flag-level oversight and direction
    - Component participation
  - **DoD IPv6 Transition Office** to provide technical lead
    - Enterprise approach to critical support activities (e.g., IPv6 addressing, common engineering solutions)
  - **Distributed implementation responsibilities** among Components
  - Development and maintain a **DoD-wide transition plan**

Planning Activities --The DoD IPv6 Transition Plan

- Coordination Draft completed
- Updated to incorporate Component comments as appropriate
- Establishes enterprise-level management oversight structure and process for IPv6
- Identifies roles and responsibilities
- Lays out an initial set of tasks and completion dates for IPv6 implementation
- Identifies a top level transition roadmap for IPv6
- Identifies Pilots and related Operational Capabilities
- Identifies IPv6 Distributed Testbed participants

Planning Activities --Key Products

- DoD IPv6 Transition Implementation Plan
- IPv6 Master Test Plan—updated annually
- Component IPv6 Implementation Guidance
- Component IPv6 Implementation Plans
- Component Pilot Implementation Plans
- Component Application Lists
- Master IPv6 Implementation Schedule
- IPv6 Network and IA System Transition Design (time phased)
- IPv6 Addressing Architecture and Plan
- IPv6 Standards Profile

Planning Activities --The Management Structure

Need for long-term, systematic approach to transition issues

A DoD IPv6 Transition Office will be established within DISA to provide overall technical guidance and assistance

DoD CIO/CIO Executive Board — Leadership Level

IPV6 Transition Implementation Panel — Flag Level, DCIO Chair

Secretariat — DISA

Integration with GES governance still needed

Architecture & Planning

- Netwk & IA Design
- ConOps
- Master Planning
- Policy
- Budget

Networking & Infrastructure

- IPv6 Network Protocols
- IETF Presence
- Strat/Tact Network Transitions
- Pilot Implementations

Applications

- IPv6 App Protocols
- Transition Guidelines
- App Testing & Evaluation

IPv6 Services

- Addressing
- Domain Name Service
- NTP, Etc.

Security & IA

- E2E Security
- IA Infrastructure
- HAIPE IPv6
- PKI

Net Mngmt PBN

- E2E Net Management
- Policy Based Networking
- Processes & Procedures

Standards

- JTA
- IETF
- Industry Input
- ARIN Board

Planning Activities --Proposed Pilots and Schedule

D R A F T – Still in Coordination

DREN	DISN-LES	GBS	VOIP ?						FY04
NMCI	GSRNet	DCTS ?	WARP	Net-BLTS NORA					FY05
	NIPRNET	GIG-BE (Secret, SCI)	GCCS	GCSS	CITS	NCES	GNCST		FY06
	SIPRNET	JWICS	DCGS	DMLSS	JIVA	WIN-T			FY07
			Everyone						FY08

Network

Application

Service Activities

- Component Transition Plans
- IPv6 Implementation Guidance
- IPv6 Transition WGs
- IPv6 in FY 06 POM
- In most cases just getting started

The Challenges (1)

- **Managing/Resourcing the Transition**
  - Funding for FY 04 and 05 for IPv6 Transition Office
  - Funding for POM 06—need warfighter buy-in
- **The scope IS HUGE: "IPv6 TOUCHES EVERYTHING"**
- **Programmatic coordination and harmonization**
  - DISN, TCS, WIN-T, ForceNet, NMCI, CITS, C2 Constellation, JTRS, GIG-BE, …
- **IP convergence—data, voice and video over IP**
- **Network backbone convergence**
  - Availability and scalability of IPv6 HAIPE
- **Network performance in end-to-end IPv6 environment**
- **IPv6 IA issues**
  - Policy guidance for IPv6 implementation
  - Availability of products and approved solutions
  - End-to-end solutions
  - HAIPE

The Challenges (2)

- **Transition strategies, solutions and management**
  - **Maintaining Interoperability** and Security During Transition (and after)
- **IPv6 in the low-bandwidth/mobile environment**
- **Evolving IPv6 standards/products**
- **Residual Legacy IPv4**
- **Non-IPv4 legacy systems—e.g., data links**
- **APPLICATIONS, APPLICATIONS, APPLICATIONS, ...**
- **The SCHEDULE**