

**Meeting Notes:  
60<sup>th</sup> Internet Engineering Task Force (IETF)  
San Diego, August 2004**

**David Green  
SRI International  
Representing DISA  
[dave.b.green@us.army.mil](mailto:dave.b.green@us.army.mil)**

# Table of Contents:

1	Monday 2 August.....	4
1.1	MANET (9:00).....	4
1.1.1	AODVbis (Charlie Perkins).....	4
1.1.2	Route Discovery and Maintenance to Internet Gateways (Shubhranshu-Samsung).....	4
1.1.3	Link Buffering for MANET (Clausen et al).....	4
1.1.4	DSR Draft (Dave Johnson).....	5
1.1.5	ARP Over IPv6 (Dave Johnson).....	5
1.1.6	Integrating OSPF MANET and Wired Nets (Wenji Wu Arizona U).....	5
1.1.7	Requirements for MANET Autoconfiguration and IPv6.....	5
1.2	NSIS Working Group (1:30).....	5
1.2.1	NSIS in Mobile Networks (S. Lee).....	6
1.2.2	NSIS Signaling Layer Protocol (SNLP) updates in NAT/Firewalls.....	6
1.3	OSPF Working Group (3:30).....	6
1.3.1	OSPF Wireless Design Team/Charter Update (Rohit/Acee).....	6
1.3.2	OSPF MANET Considerations (Thomas Henderson).....	7
1.3.3	Extensions to OSPF to Support MANET (White of CISCO).....	7
1.3.4	OSPF Security.....	7
1.3.5	Multiple Topology Routing.....	8
1.4	IPv6 Operations Working Group (7:30).....	8
1.4.1	VLAN Usage for IPv6 transition (Chown).....	8
1.4.2	Enterprise solution case study: Campus Transition (Chown).....	8
1.4.3	Assisted Tunneling Requirements – (Durand).....	9
1.4.4	Moving forward with Mechanisms (Chairs/Ads).....	9
1.4.5	Secure IPv6 Tunneling – (Graveman).....	9
1.4.6	IPv6 Security Overview – (Savola).....	9
1.4.7	Tunnel-endpoint Discovery, (Palet).....	10
1.4.8	What do we do with NAT-PT.....	10
2	Tuesday 3 August.....	10
2.1	Mobile IPv6 (MIPv6) (9:00).....	10
2.1.1	MIPv6 Route Optimization security (Gabriel Montenegro - SUN).....	11
2.1.2	Bootstrap Problem Statement for MIPv6 (Alpesh Patel).....	11
2.1.3	Authentication Options for MIPv6 (Alpesh Patel et all).....	11
2.1.4	Network Address Identifier (NAI) Options for MIPv6 (Alpesh Patel et all) 12	
2.1.5	Preconfigured binding Mgt Keys for MIPv6 (C. Perkins).....	12
2.1.6	Manual IPSEC Keying for MIPv6 (Perkins).....	12
2.1.7	MIPv6 Plug Tests (Patrick Guillemin).....	12
2.1.8	IPSEC between MIPv6 MN and CN ().....	13
2.1.9	HA Load Balancing ().....	13
2.1.10	Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering ().....	13
2.1.11	Cryptographic Generated Address CGA for MIPv6().....	13

2.2	Geographic Location/Geo-Privacy (1:00, 2:00)	13
2.3	Robust Header Compression (3:30)	14
2.4	Operational Security Requirements for IP Networks Infrastructure (OPSEC)	
	BOF (5:00)	15
3	Wednesday 4 August	15
3.1	Multicast Backbone (MBONE) Deployment Group (9:00)	15
3.2	Control & Provisioning of Wireless Access Points WG (1:00)	16
3.3	IPv6 WG (3:00)	16
4	Thursday 5 August	19
4.1	IPv6 Operations Working Group (V6OPS)(9:00)	19
4.1.1	Transition Enterprise Scenarios (Jim Bound)	19
4.1.2	Assisted Tunneling for Transition (Karen E. Nielsen (AH/TED))	21
4.1.3	Assisted Tunneling for Transition (?)	21
4.1.4	Basic Transition Mechanisms for IPv6 Hosts and Routers bis (Chairs)	21
4.1.5	AutoTransition (Palet)	21
4.1.6	IP Mobility Scenario (Carl Williams)	22
4.1.7	Network Based Security (Palet)	22
4.1.8	Late Night Plenary Session	22
5	Conclusions	24

# 1 Monday 2 August

## 1.1 MANET (9:00)

- <http://www.ietf.org/html.charters/manet-charter.html>
- The purpose of this working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies. The fundamental design issues are that the wireless link interfaces have some unique routing interface characteristics and that node topologies within a wireless routing region may experience increased dynamics, due to motion or other factors.

### 1.1.1 AODVbis (Charlie Perkins)

- Route error messages issued when a link is broken for an “active route”
- Some possible routes are discovered but not used, called “available paths”
  - If available (not active) paths time out - no need for a route error message
- Unicast validation for expired available routes [feasible routes] to see if they work
  - Send a test packet down route and get a unicast message back if route works
  - If route fails use broadcast route discovery
  - Instead of test packet, can you use a data packet and have AODV routers send standard “route not available” ICMP error if data does not reach destination??
- By checking out feasible routes, eliminates many broadcast route discovery messages
- Charlie suggests using NS-2 for large MANET simulations

### 1.1.2 Route Discovery and Maintenance to Internet Gateways (Shubhranshu-Samsung)

- No work previously done to discover Mobile Multiple Gateways to Internet
- MANET nodes 1-hop from Internet access-router can advertise as Internet gateways
- There are default gateways and candidate (alternate) gateways allowed
  - A candidate gateway may be used if it is a shorter path for OSPF or for load balancing

### 1.1.3 **Link Buffering for MANET (Clausen et al)**

- Allows intermediate routers to store datagrams until a new route is discovered
- Provide a common mechanism for proactive and reactive MANET protocols to respond to topology changes and link disconnection
- When IP datagrams become undeliverable, they are buffered for later delivery when/if a route is available
- Must see if local route repair is applicable to decide if buffer is required
- If packets are buffered,
  - Route discovery must be run for reactive protocols (AODV)
  - Must wait for periodic route update for active protocols (OLSR, OSPF)

- If route is not available in a reasonable time, packets may be discarded (DG comment: Perhaps discard should be moderated by QOS requirements /DIFFSERV???)
- May have a scalability problem since large flows may not buffer well
- In reactive protocols like AODV, a few packets are cached while route discovery happens, may not scale well for larger flows that begin after initial route discovery
- May disrupt transport protocols – TCP may see this as congestion
- Alex Zinnin and others argue against link buffering and say reliability should be at transport layer or other and routing should be concerned with maximum convergence speed only....
- [DARPA connectionless networks](#) project sounds like it is a little related to this...

#### 1.1.4 DSR Draft (Dave Johnson)

- Specifies how DSR uses ARP – a node may refresh ARP cache if it discovers node/MAC changes from received packets other than ARP
- Many minor changes
- Plug for ACM's MOBICOM 2004 [www.sigmobile.org/mobicom/2004/](http://www.sigmobile.org/mobicom/2004/) in Philly

#### 1.1.5 ARP Over IPv6 (Dave Johnson)

- Nodes should buffer more than 1 packet while waiting for an ARP on MANET
- Node should retransmit ARP request for a given target if no ARP reply comes and packets are in buffer
- Nodes should use a binary exponential backoff algorithm in timing the generation of ARP request retransmissions
- Nodes should have a maximum number of ARP retransmission tries

#### 1.1.6 Integrating OSPF MANET and Wired Nets (Wenji Wu Arizona U)

- 1 minute presentation to let us know he is looking at Wireless OSPF and integrating it with wired networks at access points
- Allows non-MANET nodes to interface with MANET and MANET access to wide-area and global Internet infrastructure

#### 1.1.7 Requirements for MANET Autoconfiguration and IPv6

- 4 MANET experimental RFCs AODV, DSR, OLSR, TBRPF
- Next Step for MANET – Autoconfiguration?
- How to handle nodes entering and leaving MANETs?
- Address selection, Duplicate Address Detection (DAD), etc...
- [Draft-jeong-manetoaddr-autoconf-reqts-02.txt](#)

### 1.2 NSIS Working Group (1:30)

- <http://www.ietf.org/html.charters/nsis-charter.html>

- The Next Steps in Signaling Working Group is responsible for standardizing an IP signaling protocol with QoS signaling as the first use case.
- The intention is to re-use, where appropriate, the protocol mechanisms of RSVP, while at the same time simplifying it and applying a more general signaling model.
- Group is working to create a single, simple, extensible general purpose signaling protocol than can be extended to special cases like RSVP
- Problems: Signaling through NATS, implementation issues
- General Internet Messaging Protocol for Signaling (GIMPS) provides a universal service for diverse signaling applications.
- GIMPS manages its own internal state and the configuration of the underlying transport and security protocols to enable the transfer of messages in both directions along the flow path

### 1.2.1 NSIS in Mobile Networks (S. Lee)

- In mobility scenarios, operation of NSIS signaling is affected by the following issues:
  - GIMPS needs to be able to detect route changes and mobility
  - How to set up QOS paths after mobility occurs?
  - How to handle IP address changes after mobility?
  - How to handle firewall bindings and NAT bindings change after mobility
  - IP in IP encapsulation

<http://www.ietf.org/internet-drafts/draft-manyfolks-signaling-protocol-mobility-01.txt>

### 1.2.2 NSIS Signaling Layer Protocol (NSLP) updates in NAT/Firewalls

- NSLP allows hosts to signal along their data path so NATs and firewalls can be configured according to their data flow needs.
- Open issues:
  - Initiator is outside of firewall/NAT - how to pre-set firewall policy efficiently
  - Currently NSLP only works if initiator is behind NAT/firewall and supports NSIS NATFW NSLP
  - NSIS unaware firewalls –how to detect them and transit them....
  - How to select one of several addresses when IPv6 is used...

<http://www.ietf.org/internet-drafts/draft-ietf-nsis-nslp-natfw-03.txt>

## 1.3 OSPF Working Group (3:30)

- <http://www.ietf.org/html.charters/ospf-charter.html>
- The majority of the group's discussion was on OSPF Wireless – MANET extensions

### 1.3.1 OSPF Wireless Design Team/Charter Update (Rohit/Acee)

- Should be compatible with current OSPFv3
- Free from IPR

- All proposals attack flooding optimization problem

### 1.3.2 OSPF MANET Considerations (Thomas Henderson)

- IETF draft from June by Henderson, Spagnolo, Pei:  
<http://ietfreport.isoc.org/ids/draft-spagnolo-manet-ospf-design-00.txt>
- OSPF does not have a suitable interface type for MANET – bad scalability in wireless
- Fundamental problems for OSPF in MANET:
  - Network size, network density, network churn
- Performance trends of different OSPF MANET proposals
  - Best reduction: unreliable Link Ste Update (LSU) flooding: 84% reduction
  - Unreliable flooding was not shown to reduce packet delivery ratio
  - Reliable flooding schemes not better than 50% reduction
  - Did not model performance in different congestion levels.....
- Future work:
  - Find the best flooding algorithm
  - Determine if database synchronization optimizations are needed
  - Limit the number of adjacencies
  - Adjust packet formats for differential encoding....

### 1.3.3 Extensions to OSPF to Support MANET (White of CISCO)

- Cisco's views slightly out of sync with Boeing's
- draft-chandra-ospf-manet-ext-00.txt
- CISCO's Protocol highlights:
  - CISCO does want to implement a form of differential Hello using a sequence number to indicate if state change in neighbor table has occurred
  - Database exchange: By listening to other nodes LSDB, you can build some adjacency table entries....
  - Optimized flooding: Carry 2-hop neighbors in hello to determine who can reach most neighbors – router with most adjacencies has lower flooding back-off timer, or if two nodes are equal, one will have a lower back-off (Similar to OLSR?) If another node transmits the flood message before your timer expires and an ACK comes back from the downstream neighbor, you cancel your flood broadcast. If no ACK comes back node with higher timer wait will then broadcast flood message...

### 1.3.4 OSPF Security

- Decided to go with old IPSEC RFCs vs. new IPSEC drafts
- Lots of discussion and nitpicking....

### 1.3.5 Multiple Topology Routing

- Cisco presentation on how to route different traffic types over different links....

## 1.4 IPv6 Operations Working Group (7:30)

- <http://www.ietf.org/html.charters/v6ops-charter.html>
- CHAIRS: Pekka Savola [pekkas@netcore.fi](mailto:pekkas@netcore.fi) & Jonne Soininen [jonne.soininen@nokia.com](mailto:jonne.soininen@nokia.com)
- 6PE (BGP Tunneling) and Teredo are being advanced toward RFC
- ISATAP may also be forwarded
- 6to4 and 6to4 anycast security analysis past AD and being sent to RFC editor

### 1.4.1 VLAN Usage for IPv6 transition (Chown)

- draft-chown-v6ops-vlan-usage-01.txt
- VLAN tagging support for IPv6 in L2/L3 switches
- Software VLAN support for internal use of IPv6 in IPv4 subnets
- Can use NativeV6 address prefixes
- Usually use a BSD or UNIX router to tag IPv6 for IPv4 VLAN support
- No IPv4 host or router changes necessary
- Discuss whether to go for Informational RFC

### 1.4.2 Enterprise solution case study: Campus Transition (Chown)

- draft-chown-v6ops-campus-transition-00.txt (Full text will be released by IETF61)
- Examines a case study of applying the IETF IPv6 Enterprise Scenarios document
- Give input to the Enterprise solutions work and the necessity of transition tools
- Preferred legacy interaction via dual-stack
- No non-upgradeable systems identified in this scenario
- Requirements discussed
  - DNS
  - Routing
  - Host Config
  - Etc...
- What they found missing:
  - Access control for WLAN (AAA, PKI)
  - Where hardcoded IPv4 addresses are used
  - Network backup
  - Missing components L2/L3 switch support
  - NFS/SAMBA
  - MS Exchange
  - Active Directory
  - Many Apache Web Server modules
- Need to put out transition services on edge of campus net – tunnel broker, 6to4, etc... for external users needing to reach campus net via non-IPv6 ISPs

- Most gaps not in standards – *gaps are in implementations!*
- **Complexity not in enabling IPv6 on the wire, it is enabling IPv6 in services and applications!!!**

### 1.4.3 Assisted Tunneling Requirements – (Durand)

- draft-ietf-v6ops-assisted-tunneling-requirements-00.txt
- Defines requirements for a tunnel set-up protocol that could be used by an ISP to jumpstart its IPv6 offering to its customers by providing them IPv6 connectivity without having to upgrade its access network.
- Issues from WG last call
  - Should assign a /64 or a /128 on link
  - Tunnel endpoint discoveru – accept
  - Add requirement for load balancing/load brokering on ISP tunnel broker
  - Securing the setup session – use registered mode to protect authentication?
  - Secure tunnel though IPSEC? - - Perhaps a MAY
    - How about IPSEC implementation as a MUST, use is a MAY
  -
- GOAL: resolve issues, revise and advance after IETF60

### 1.4.4 Moving forward with Mechanisms (Chairs/Ads)

- Discuss the procedure of how to move forward with work of IPv6 Ops
- What working group must do:
  - Move BGP and Teredo forward
  - IPv4/V6 transtion for SIP – move to SIPPING group
  - Assisted Tunneling
  - Zero-config tunneling
  - Configured tunneling through NAT (Could be covered in assisted tunneling)
  - Tunneling of IPv4 over IPv6 needs to be addressed
  - **Meet deadlines or this group will die!**

### 1.4.5 Secure IPv6 Tunneling – (Graveman)

- draft-tschofenig-v6ops-secure-tunnels-01.txt
- discuss the method of using IPsec to create secure v6-in-v4 tunnels
- draft-bellovin-useipsec-03 adds additional explanation on how to use IPSEC
- Recommends using IKEv2 and IPSECRFC2401bis-02
- May want to use IPSEC Transport mode to allow dynamic tunnel routing
- Needs more work on transport mode vs. tunnel mode

### 1.4.6 IPv6 Security Overview – (Savola)

- draft-savola-v6ops-security-overview-02.txt
- An overview of security with IPv6 in 3 areas:
  - IPv6 protocol
  - Transition mechanisms

- o Deployment
- Author's view that document should be updated and published as Informational RFC

### 1.4.7 Tunnel-endpoint Discovery, (Palet)

- draft-palet-v6ops-tun-auto-disc-01.txt
- Discusses different approaches to discover the v6-in-v4 endpoint
- Used with assisted tunneling and maybe others
- 4 scenarios:
  - o Initial IPv6 deployment - ISP does not have Native6, but sets up tunneling
  - o 2<sup>nd</sup> ISP offers IPv6 tunneling through your ISP
  - o Nomadic users must discover tunnels
  - o Advanced IPv6 deployment- must use load balancing
- How to discover TEPs?
  - o DNS
  - o Reverse DNS
  - o Central broker
  - o Shared anycast
  - o DHCP
- GOAL: get more feedback, adopt as WG item?

### 1.4.8 What do we do with NAT-PT

- Usage cases for NAT-PT
- Had a strong "do not do it if possible" statement – IETF does not encourage NAT
- CISCO rep (Tony Hain) argued that we need a document to define the narrow cases where a NAT-PT is appropriate
- Do we want to continue work with NAT-PT? There was a mixed response to this question...

## 2 Tuesday 3 August

### 2.1 Mobile IPv6 (MIPv6) (9:00)

- <http://www.ietf.org/html.charters/mip6-charter.html>
- Mobile IPv6 (MIPv6) specifies routing support to permit an IPv6 host to continue using its "permanent" home address as it moves around the Internet. Mobile IPv6 supports transparency above the IP layer, including maintenance of active TCP connections and UDP port bindings.
- Since 59<sup>th</sup> IETF published RFC s
  - o [Mobility Support in IPv6 \(RFC 3775\)](#)

- [Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents \(RFC 3776\)](#)
- Current work
  - Bootstrapping solution
  - MIPv6 in the presence of firewalls
  - Separate specs for Home Agent (HA) Discovery, Route Optimization, Renumbering to IESG

### 2.1.1 MIPv6 Route Optimization security (Gabriel Montenegro - SUN)

- <http://www.ietf.org/internet-drafts/draft-ietf-mip6-ro-sec-01.txt>
- Improvements to prevent spurious binding updates to CN
- Passive attack against privacy – decided to not address in draft
- Can DNSSEC be used to provide PKI for MIPv6?

### 2.1.2 Bootstrap Problem Statement for MIPv6 (Alpesh Patel)

- <http://www.ietf.org/internet-drafts/draft-ietf-mip6-bootstrap-ps-00.txt>
- Must get enough information to register MN to HA
- User information may be stored in AAA server
- Identifies the minimum set of information needed to accomplish bootstrapping
- Does not address prefix re-numbering in the home network
- Does not address case where no previous trust relationship was established between the MN and the home ISP
- Bootstrapping minimizes the manual configuration necessary to set up MIPv6 MN and anchors the MN to the HA automatically
- 4 Scenarios for Bootstrapping Operation
  - Mobile Service Subscription – Pre arranged relationship with Mobile Service Provider (MSP) allows bootstrapping anywhere within an MSP's network
  - Integrated Access Service Provider (ASP) network - both the ASP and MSP are owned by same company (1 (or 2?) Authentications) Could bootstrap MIPv6 during access authentication or later during separate exchange
  - 3<sup>rd</sup> party MSP needed to access home network – 3<sup>rd</sup> party provider and home network provider both have trust relationships with MN. One company provides MIPv6 service but another provides mobile access. Ex: Corporate network and ISP
  - Infrastructure-less scenario – no equipment for AAA or trust on access network (Ex: Open 802.11 hotspots)

### 2.1.3 Authentication Options for MIPv6 (Alpesh Patel et al)

- <http://www.ietf.org/internet-drafts/draft-ietf-mip6-auth-protocol-00.txt>
- Document defines new mobility options to enable authentication between mobility entities. These options can be used in addition to or in lieu of IPsec to authenticate mobility messages as defined in the base Mobile IPv6 specification.

- Trying to minimize over the air signaling required for AAA for MN
- Reduce latency of session setup and handoff
- Reduce security overhead to minimum while still protecting binding updates and other MIPv6 exchanges
- Used for CDMA2000 and 3GPP2
- Can DNSSec be used to provide PKI for MIPv6?
- Group members 50/50 split for and against adopting this draft
- 

#### **2.1.4 Network Address Identifier (NAI) Options for MIPv6 (Alpesh Patel et al)**

- <http://www.ietf.org/internet-drafts/draft-ietf-mip6-nai-option-00.txt>
- Document defines how mobility entities can be identified using a network access identifier (NAI). NAI can have varied applicability, for instance, can be used to authenticate mobility entities using existing authentication infrastructure (AAA), to dynamically allocate a mobility anchor point, to dynamically allocate an address etc.
- NAI is a mobile service enabler
- Gives users a unique identifier
- Presents user to the network instead of his devices to the network
- Ref: Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, 1999.
- NAI example: [John@bigorganization.com](mailto:John@bigorganization.com) (Similar to e-mail addresses)

#### **2.1.5 Preconfigured binding Mgt Keys for MIPv6 (C. Perkins)**

- <http://www.ietf.org/internet-drafts/draft-ietf-mip6-precfgKbm-00.txt>
- A mobile node and a correspondent node may preconfigure a Binding Management Key for authorizing Binding Updates.
- Already in use in most MIPv6 implementations
- Could use the new care-of-address as a keygen token to change secret shared key at every new care-of-address

#### **2.1.6 Manual IPSEC Keying for MIPv6 (Perkins)**

- Addressed in draft-ietf-mobileip-mipv6-ha-ipsec-03.txt
- Alternative to IKE – just use manual typed or manually loaded keys
- Simplifies IPSEC implementation because IKE and PKI not needed
- Use block ciphers (AES-CBC) instead of any stream ciphers with manual keys
- Supports DoD's current private key infrastructure for high security encryption

#### **2.1.7 MIPv6 Plug Tests (Patrick Guillemin)**

- Testing procedures for MIPv6 interoperability
- draft-kniveton-mipv6-remote-testing-00.txt

- <http://mip6.plugtests.org/>

### **2.1.8 IPSEC between MIPv6 MN and CN ()**

- Adds additional security on top of return routability procedure
- Protects route-optimization security

### **2.1.9 HA Load Balancing ()**

- Allows HA to balance work load via a home agent handover to another agent for distributed load balancing among distributed HAs
- Proactive ID message from HA to MN about load balancing
- Load balancing could occur at bootstrapping

### **2.1.10 Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering ()**

- Highlights problems of using MIPv6 in 3GPP UMTS networks

### **2.1.11 Cryptographic Generated Address CGA for MIPv6()**

- <http://www.ietf.org/internet-drafts/draft-haddad-mip6-cga-omipv6-02.txt> suggests a new and enhanced route optimization security mechanism for Mobile IPv6 (MIPv6). The primary motivation for this new mechanism is the reduction of signaling load and handoff delay. The performance improvement achieved is elimination of all signaling while not moving, and 33% of the per-movement signaling.
- 

## **2.2 Geographic Location/Geo-Privacy (1:00, 2:00)**

- <http://www.ietf.org/html.charters/geopriv-charter.html>
- Group assesses the authorization, integrity and privacy requirements that must be met in order to transfer geographic location information, or authorize the release or representation of such information through an agent.
- Location-based services, navigation applications, emergency services, management of equipment in the field, and other location-dependent services need geographic location information about a Target (such as a user, resource or other entity). There is a need to securely gather and transfer location information for location services, while at the same time protect the privacy of the individuals involved.
- This group has released documents focused on the authorization, security and privacy requirements for such location-dependent services. Specifically, it has described the requirements for the Geopriv Location Object (LO) and for the protocols that use this Location Object. This LO is envisioned to be the primary data structure used in all Geopriv protocol exchanges to securely transfer location data.
- AAA server or other access server on mobile network may act as location server

- The way geographic location objects are handed out via a central server as defined by this group may not be relevant to DOD tactical networks. In DOD tactical mobile networks, generally all nodes requiring geo-location services have geo-location capability via GPS, inertial navigation, TOA ranging, or a combination of these three.
- DOD may be interested in using the group's location object definition and in the groups work related to the transfer of geographic related information objects from an end-user to a server or between end-users

## 2.3 Robust Header Compression (3:30)

- <http://www.ietf.org/html.charters/rohc-charter.html>
- The purpose of ROHC is to develop generic header compression schemes that perform well over links with high error rates and long roundtrip times, as well as related signaling compression schemes. The schemes must perform well for cellular links built using technologies such as WCDMA, EDGE, and CDMA-2000. However, the schemes should also be applicable to other future link technologies with high loss and long roundtrip times such as tactical radios, SATCOM, and other DOD wireless technologies.
- ROHC may develop multiple compression schemes, for example, some that are particularly suited to specific link layer technologies like JTRS WNW or SRW.
- Since 59<sup>th</sup> IETF the ROHC WG published three RFCs:
  - RFC3759 - "ROBust Header Compression (ROHC): Terminology and Channel Mapping Examples" (An informational RFC to clarify terms and concepts presented in RFC 3095)
  - RFC3816 - "Definitions of Managed Objects for ROBust Header Compression" which defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes a set of managed objects that allow monitoring of running instances of ROBust Header Compression (ROHC).
  - **RFC 3843 – "ROBust Header Compression (ROHC): A Compression Profile for IP"** defines a ROHC compression profile for IP, similar to the IP/UDP profile defined by RFC 3095, but simplified to exclude UDP, and enhanced to compress IP header chains of arbitrary length. When considering that normally all packets are expected to be IP packets [RFC-791 for IPv4, RFC-2460 for IPv6], and that the IP header often represents a major part of the total header, a useful alternative to no compression would for most packets be compression of the IP header only.
- Note from David Green: Work on DOD specific ROHC for SATCOM and tactical radio links is being done at US Army CERDEC via contracts with Procito & U. of Arizona and a proposed FCT with EFFNET. Their funding for this research is extremely limited and currently is not addressing development of link layer- assisted ROHC technology for JTRS or SATCOM. The FCT proposal to EFFNET requests that EFFNET prototypes an approach to ROHC for multipoint links (for multicast and

broadcast) but is probably insufficiently funded to develop a complete solution and present it to the IETF for standardization.

## 2.4 **Operational Security Requirements for IP Networks Infrastructure (OPSEC) BOF (5:00)**

- Founding an OSEC working group to progress the related operational security work. The goal is to codify knowledge about feature sets that are required to securely deploy and operate managed network elements providing transit services at OSI layers 2 and 3.
- URL will be: <http://www.ietf.org/html.charters/opsec-charter.html>
- draft-jones-opsec-06.txt has been approved for publication as an informational RFC <http://www.ietf.org/internet-drafts/draft-jones-opsec-06.txt>

## 3 Wednesday 4 August

### 3.1 **Multicast Backbone (MBONE) Deployment Group (9:00)**

- <http://www.ietf.org/ietf/04aug/mboned.txt>
- The MBONE Deployment Working Group is a forum for coordinating the deployment, engineering, and operation of multicast routing protocols and procedures in the global Internet
- Since 59<sup>th</sup> IETF MBONE WG published RFC s –NONE!
- Since 59<sup>th</sup> IETF Active Internet Drafts:
  - draft-ietf-mboned-auto-multicast-02.txt Thaler, et al
    - Thaler looking for more interest before continuing, WG members are clearly interested in auto-tunneling so draft will be updated & continue
  - draft-ietf-mboned-ssm232-08.txt Shepherd, et al
    - 2-3 yr old draft had to be changed to reference new PIM spec (PIM spec last revision going to IESG for RFC#) and will go to the RFC editor soon
  - draft-ietf-mboned-embeddedrp-06.txt Savola/Haberman
    - Past IESG evaluation waiting for AD to pass to RFC editor
    - May have a minor change to allow a new address prefix
  - draft-ietf-mboned-ipv4-uni-based-mcast-01.txt Thaler
    -
  - draft-ietf-mboned-mroutesec-02.txt Savola et al
    - Past IESG evaluation waiting for AD to pass to RFC editor
    - May have a minor change before submission

- draft-ietf-mboned-msdp-deploy-06.txt                      McBride, et al
  - This one depended on old PIM and experimental MSDP specs and is waiting for the new PIM spec and for a variance from IESG to allow it to reference the MSDP experimental spec
- draft-ietf-mboned-rfc3171bis-02.txt                      Albanna, et al
  - Ipv4 multicast address assignment guidelines for IANA – being sent to WG last call and sent to IESG
- Current work discussed in meeting
  - Assignment of IPv6 Multicast Addresses with DHCPv6 (Jerome Durand)
    - draft-jdurand-assign-addr-ipv6-multicast-dhcpv6-00.txt
    - Method provides a simple solution to solve IPv6 multicast address assignment problem using the DHCPv6 protocol.
    - (Dave Green Comment) Is there a need for a new DHCPv6 assigned multicast scheme – we already have MADCAP and almost no-one uses it....
  - Embedded-RP and control mechanisms (Jerome Durand)
    - Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple Protocol Independent Multicast sparse mode (PIM-SM) domains.
    - MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains.
    - Problem: External users connect to a site's RP and register multicast groups but abuse of this can overuse resources in a site –not a security problem but a resource control problem
    - Durand thinks that group address filtering and PIM register filtering are not enough – proposes a mechanism to not allow external users to register a group with an RP, but only use the RP to join groups registered by users from within the site
    - Session chair asked Durand to take this problem to the WG list
- Multicast issues outstanding for the group
  - Need to document deployment issues for multicast IPv6 deployment – like problems with WLAN AP and some cable modem networks not able to support multicast/anycast autoconfiguration for IPv6 Auto-Address Configuration

## 3.2 Control & Provisioning of Wireless Access Points WG (1:00)

- <http://www.ietf.org/html.charters/capwap-charter.html>
- Configuration and Provisioning for Wireless Access Points (CAPWAP) is designing a control and bridging control protocol to allow for interoperability of WLAN controllers for centralized administration of large scale WLAN deployments

## 3.3 IPv6 WG (3:00)

- <http://www.ietf.org/html.charters/ipv6-charter.html>
- The IPv6 working group is responsible for the specification and standardization of the Internet Protocol version 6 (IPv6).
- The following drafts were reviewed:
  - 2461bis Soliman
    - draft-soliman-ipv6-2461-bis-01.txt
    - Main changes were for mobility and security
    - Newly added: Enabling forwarding per interface since some mixed nodes have routing on some interfaces, host behavior on others
    - Open issue: The on by default assumption is being re-written
    - 2461 BIS is going through WG last call
  - 2462bis Jinmei
    - draft-ietf-ipv6-rfc2462bis-02.txt
    - WG last call on July 13<sup>th</sup>
    - One more revision by Aug9th, then on to IESG
    - New revision 2462bis-03.txt addresses 4 suggestions from WG last call
    - Major changes:
      - Interface Identifier length clarified
      - Duplicate Address Detection (DAD) change so that all nodes MUST do DAD for unicast addresses,
      - introduced random delay when creating multicast RA
      - Clarified "interrupt operations" to mean disable IPv6 operations on an interface
      - Clarified use of M/O flags for DHCPv6
  - ICMP Updates RFC2463 Gupta/Hinden
    - draft-ietf-ipngwg-icmp-v3-03.txt
    - Requests for ICMP type value assignments from outside of the IETF will be sent to the IETF (IANA or IESG?) for review. If an outside organization requests for multiple type value assignments will be sent to IESG for approval.
    - Other changes are trivial...
    - Minor changes will be made, a WG last call will take place, and this will go to the IESG soon
  - Optimistic DAD N. Moore
    - draft-ietf-ipv6-optimistic-dad-01.txt
    - Dec 04 will submit DAD optimizations to the IESG for Proposed Standard
    - DAD optimization modifies DAD as defined in RFC 2461/2462 to make it happen faster
    - Issues:
      - Definition of "well distributed" addresses in description of generating random addresses
      - Protocol defines an "available" address as one that is created but has not undergone DAD yet
      - Probability of address collision for manually configured addresses is high - is optimistic DAD suitable for manual addressing?
      - For predictive handovers, MIPv6 nodes MAY send unsolicited neighbor advertisement (NA) - changed to

nodes may not send unsolicited NA if they have not finished opti-DAD check

- Collisions with nodes discovered by proxy Neighbor Discovery (ND) has been deemed a "no problem" since this will cause the node state in the Neighbor Cache (NC) to be changed to from 'incomplete' to 'Stale' and the disruption caused by this will be recovered almost immediately by the standard neighbor Unreachability Detection (NUD) mechanism
- (Dave Green Comment) The risk of having an address collision is so incredibly low in IPv6 addresses, and the consequences of a collision are so minor and quickly recovered from- why are we worrying so much about this?
- M&O Flags in RA's Park
  - draft-daniel-ipv6-ra-mo-flags-00.txt
  - This document clarifies the processing and behavior of the IPv6 Router Advertisement "ManagedFlag" and "OtherConfigFlag" (M&O flags) and proposes a solution for invoking the DHCPv6 based DHCPv6 administrator policy.
  - M flags in Ipv6 indicate whether the Dynamic Host Configuration Protocol [RFC3315] is available for address autoconfiguration in addition to any addresses autoconfigured using stateless address Autoconfiguration.
  - O Flag, the "Other stateful configuration" flag indicates a subset of DHCPv6 [RFC3736] is available for autoconfiguration of other (non-address) information. Examples of such information are DNS-related information or information on other servers within the network.
- DNS configuration (RA option) chairs
  - draft-ietf-dnsop-ipv6-dns-configuration-01.txt
  - Group decided that there is interest in supporting Router Advertisements for DNS discovery, but group is 50/50 split on taking on this work
- Anycast Analysis chairs
  - draft-ietf-ipngwg-ipv6-anycast-analysis-02.txt
  - The anycast analysis draft is stagnant -has been in AD follow up for 362 days.
  - Disagreement over how useful the document is
  - IESG thinks that an overview documenting anycast functionality is useful, but the author is not updating the document anymore
  - What to do about the Anycast analysis - A new editor/author will take over the document and move it to closure.
- IPv6 over PPP update Varada
  - draft-ietf-ipv6-over-ppp-v2-01.txt
  - Clarifies autoconfiguration of global unicast and link-local addresses generation for 3GPP and 3GPP2 mobile networks
  - Presents a snapshot of how IPv6 global addresses are generated using I-IDs in PPPv6
  - Mostly minor updates in latest document
- Link-scoped Multicast Shin
  - draft-ietf-ipv6-link-scoped-mcast-04.txt

- o Conflicts with address range assigned as Scoped Site Multicast (SSM) addresses (FF32::/32)
- o Redesign LSM address to make it obviously unique
- o Goal: Resolving open issues from WG Last Call
- IPv6 over WLAN/802.11 chairs
  - o Goal: Should the WG be doing something?
  - o DG Comment - some 802.11 access points seem to interfere with Duplicate Address Detection and other autoconfiguration protocols

## 4 Thursday 5 August

### 4.1 IPv6 Operations Working Group (V6OPS)(9:00)

- <http://www.ietf.org/html.charters/v6ops-charter.html>
- CHAIRS: Pekka Savola [pekkas@netcore.fi](mailto:pekkas@netcore.fi) & Jonne Soininen [jonne.soininen@nokia.com](mailto:jonne.soininen@nokia.com)

#### 4.1.1 Transition Enterprise Scenarios (Jim Bound)

- Showed Steve Klynsma's matrix of transition scenarios
- Jim talked of updating enterprise transition scenarios with help from Steve Klynsma, myself (David Green), Mike Brigg
- Group chair gave Jim the task of updating the scenarios in three weeks in order to submit them to the IESG for Informational RFC status
- Jim stated that the group will match transition mechanisms to all useful scenarios submitted by Enterprise transition architects
- In order to define Defense Enterprise Network Scenarios for Jim Bound so we can work with him to analyze transition mechanism needs for Enterprise Scenarios, I defined the following three scenarios to reflect my projected state of defense networks in ten years:

##### IPv6 Dominant Defense Enterprise Network (US DOD Goal)

Scenario 1: IPv6-dominant network with some IPv6-only network infrastructure. Enterprise has some limited IPv4-capable/only nodes/applications needing to communicate over the IPv6 infrastructure. Defense Enterprise restructuring an existing network, decides to pursue aggressive IPv6 transition as an enabler for network-centric services and wants to run Native IPv6 backbone to eliminate cost/complexity of supporting a dual stack. Some legacy IPv4 capable nodes/applications within the defense enterprise will have slow technical refresh/replacement path and will need to communicate over the IPv6 dominant infrastructure for years until they are replaced. The IPv6 dominant defense enterprise network will need to be interoperable with legacy, commercial, reserve force, allied, and coalition networks that will remain IPv4 dominant during a long transition period. Reserve force components, allied, and

coalition forces may need IPv4 service across IPv6 backbone.

**Assumptions:** Required IPv6 network infrastructure is available, or available over some defined timeline, supporting the aggressive transition plan.

**Requirements:** Interoperation and coexistence with legacy IPv4 networks and applications is required. Legacy IPv4 nodes/applications/networks will need to be able to operate across the IPv6 backbone and need to be able to interoperate with the IPv6-dominant network's nodes/applications.

#### **Dual Stack Defense Enterprise Network (US Allied Countries - NATO)**

**Scenario 2:** Wide-scale/total dual-stack deployment of IPv4 and IPv6 capable hosts and network infrastructure. Defense Enterprise with an existing IPv4 network wants to deploy IPv6 in conjunction with their IPv4 network in order to take advantage of emerging IPv6 network-centric capabilities and to be interoperable with allied forces and commercial enterprises that are deploying an IPv6 architecture.

**Assumptions:** The IPv4 network infrastructure used has an equivalent capability in IPv6.

**Requirements:** Do not disrupt existing IPv4 network infrastructure with IPv6. IPv6 should be equivalent or "better" than the network infrastructure in IPv4, however, it is understood that IPv6 is not required to solve current network infrastructure problems, not solved by IPv4. It may also not be feasible to deploy IPv6 on all parts of the network immediately. Dual stacked defense enterprise network must be interoperable with both IPv4 and IPv6 networks and applications.

#### **Limited IPv6 Deployment Defense Enterprise Network (Coalition Forces)**

**Scenario 3:** Sparse IPv6 dual-stack deployment in existing IPv4 network Infrastructure. Enterprise with an existing IPv4 network wants to deploy a set of particular IPv6 "applications" and have some ability to interoperate with other forces that are IPv6 dominant. The IPv6 deployment is limited to the minimum required to operate this set of applications.

**Assumptions:** IPv6 software/hardware components for the application are available, and platforms for the application are IPv6 capable.

**Requirements:** Do not disrupt IPv4 infrastructure.

#### **4.1.2 Assisted Tunneling for Transition (Karen E. Nielsen (AH/TED))**

- An operational solution guide to assisted tunneling for transition
- Informational? Just gives the goals for a solution
- A new internet draft will be available soon
- A tunnel setup protocol or tunnel broker? – Not clear

#### **4.1.3 Assisted Tunneling for Transition (?)**

- Comparison of solutions against the goals for assisted tunneling
- ISATAP, TSP, STEP, PPP based (L2TP, TCP, UDP)
- All of these solutions require TEP discovery – there is no published TEP discovery solution yet...
- ISATAP- Fails prefix delegation & NAT traversal
- STEP-Pass most concerns, but: no implementations, out-of-band
- TSP- Pass most concerns, needs minor updates
- PPP Tunneling L2TP- Pass most concerns, but extremely heavy on bandwidth for tunneling with multiple encapsulations, difficult to deploy for those not using L2TP
- PPP Tunneling TCP- Pass most concern, but bad for links with high loss, high overhead for small packets, can use SSL for security. Needs better documenting and port number definition
- PPP Tunneling UDP- Pass most concern, needs to keep alive to preserve NAT mapping, needs better documentation and port number
- Jim Bound suggests that an administrative services solution to discover TEPs may be to have DHCPv6 hand out TEP addresses

#### **4.1.4 Basic Transition Mechanisms for IPv6 Hosts and Routers bis (Chairs)**

- Draftg-ietf-v6ops-mech-v2-04.txt
- Waiting for clarification on DNS address ordering for IPv6 preference before IESG approval
- This draft is a major re-write of RFC2893 and eliminates two transition mechanisms: IPv4 Compatible IPv6 Addresses and Automatic tunneling using IPv4 Compatible IPv6 Addresses

#### **4.1.5 AutoTransition (Palet)**

- draft-palet-v6ops-auto-trans-00.txt
- Looking for a method for auto-service discovery of best IPv6 connections
- Native IPv6 is preferred, but users could decide to use a transition mechanism if it offers better service
- Possible mechanisms to auto-check for (In order of preference):
  - Native IPv6

- TS with proto-41 (IPv6-over-IPv4 configured tunnel packets (protocol 41))
- TS with UDP
- ISATAP
- STEP
- 6to4
- Teredo
- Need to work on a good universal solution for NATs and Firewalls
- Want to design a mechanism that is also good for IPv4 in IPv6 tunneling

#### 4.1.6 **IP Mobility Scenario (Carl Williams)**

- Showed a scenario table for Mobile IPv4 and MIPv6 and how to choose which to use
- Jim Bound remarked that MIPv6 should be the concern, MIPv4 is only deployed in some 3G (2G+?) phone service networks

#### 4.1.7 **Network Based Security (Palet)**

- draft-palet-v6ops-ipv6security-01.txt
- The security policies currently applied in Internet with IPv4 doesn't longer apply for end-to-end security models which IPv6 will enable.
- Today, each network is often secured by one or several devices (i.e. security gateway or border firewall in the simplest configuration), which become a bottleneck for the end-to-end security model with IPv6.
- In addition, users and devices start to be nomadic, moving between different networks that could have different security policies.
- A distributed and dynamic approach is consequently required, as already described by Bellovin, S., "Distributed Firewalls", November 1999, <<http://www.research.att.com/~smb/papers/distfw.pdf>>.
- Centrally defined security via a policy based device
- Network entities must authenticate (certificates?) to security policy controller
- Security controller sets up security and regulates network access
- Assumptions: Threats can come from inside network,
- Security can be from application, transport, or network
- Security controller could also update anti-spam and anti-virus
- (Dave Green Comment) This sounds very similar to the moderated end-user security behind firewalls that I've been trying to push as a defense-in-depth security model. I will bring this work to the attention of Cas Potryaf

#### 4.1.8 **Late Night Plenary Session**

- SPAM is Bad!! (John Levine – chair IRTF ASRG) <http://asrg.sp.am> – Claims that in 2 years we will have a handle on SPAM prevention

- Process reform in IETF (Harald Alverstrand, General AD)
  - We want to create good tech specs, the right spec at the right time
  - The goal of the IETF is to make the Internet work better.
  - The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices and informational documents of various kinds.
  - Update to RFC 2418 regarding the mgt of IETF Mailing lists allows WG area directors to suspend posting privileges of members who are abusing posting privileges
  - Streamlined procedure to shorten IESG delay on RFC-Editor docs

## 5 Conclusions

Many key areas of concern from the previous IETF are now being addressed. The highlights are:

### Routing:

- The routing area has moved MANET improvements for OSPF to the OSPF WG to create a standards track wireless routing protocol.
- A draft for a dual stacked version of OSPF, “Support for Multiple Address Families in OSPFv3” has been released and addresses our concerns about dual stack routing overhead since OSPF dominates DOD’s routing backbones.

### V6OPs:

- After years of inactivity, there is a flurry of action in the group as apparently the IETF leadership threatened to dissolve the group if the pace of milestone accomplishment does not pick up.
- The group chair asked Jim Bound (HP and NAv6 TF Chair) to write a new “IPv6 Enterprise Transition
- Chair wants to move Teredo and BGP Tunneling for IPv6 (6PE) to RFC status

### Security:

- Jordi Palet presented IPv6 Distributed Security Requirements (draft-palet-v6ops-ipv6security-01.txt) which highlights the requirements supporting true end-to-end IPSEC security model with local IPv6 domain policy controllers. This specification would be vital for implementing emerging end-to-end host based security as suggested by NSA’s Casimir Potyraj and others. We are planning on discussing the requirements for a distributed firewall/policy server at the next North American IPv6 TF Meeting
- Manual IPSEC keying for MIPv6 using private keys is addressed in draft-ietf-mobileip-mipv6-ha-ipsec-03.txt. DOD Type 1 COMSEC is usually manually keyed using private keys.
- R. Graveman presented draft-tschofenig-v6ops-secure-tunnels-01.txt to standardize the method of using IPsec to create secure v6-in-v4 tunnels

### QOS:

- We finally have a useful idea about how to get better QOS via the IPv6 flow label. Sham Chakravorty submitted the draft: IPv6 Label Switching Architecture (6LSA) (draft-chakravorty-6lsa-00.txt)
- We still don’t have a complete end-to-end solution for guaranteed, bounded QOS or

### General:

- Process Reform – The IETF is *trying* to streamline the RFC process to create good, relevant technical specifications at the right time. Useful reforms include shortening the IESG delay on RFC-Editor docs