51st IETF, London, UK
UCL Report
30 August 2001
Expires in 3 months

Ken Carlberg
Ian Brown
Gregorio Martinez
Piers O'Hanlon
Theo Pagtzis

51st Internet Engineering Task Force Meeting
Trip Report on monitored IETF WGs

Abstract

This report presents a summary of particular IETF Working Groups attended during the 51st IETF held in London, August 2001. A multitude of Working Groups have been closely monitored on their activities and their deliberations are reported in the following sections.

1 MAGMA WG

This is a BoF for Multicast Anycast Group Membership that will probably be turned into a working group. Some of the work in this group has been moved our of the IDMR working group into Magma. A Snooping Draft RFC has been produced – goal is that it become a Best Common Practice document. IPv6, requirements, and topology are the changes made from previous draft.

Multicast Source Filter API spec has been put out but no real feedback or implementations.

With respect to IGMP, Mcast routing interaction draft exists to better interoperate the different types of protocols with IGMP. Optimizations seemed to be identified for dense-mode and sparse-mode multicast.

As for MSNIP, the focus is to notify source when a receiver exists and when all receivers leave. only work for "include-mode" groups. Dave Thaler (Microsoft) gave a lot of discussion on issues – eg, doesn't have ability to deal with misconfigurations, or router failure for receivers/routers on the same LAN. This was a large waste of time because Nortel presentation talk about augmentations to address issues.

Note: anycast will NOT be a part of MAGMA.

2 MEGACO WG

Concern about rubber-stamp transfer of SG-16 work/documents into RFCs. The big advantage of doing it, however, is that it makes the documents easily accessable to ietf-folks. Note, it was stated in the meeting there are NO significant deployment of Media Gateway Control.

3 CDI WG

First order of business for the Content Delivery Internetworking WG is to reconcile a single model draft from previous RFCs. The group will become a formal working group – had been BoFs up to this point.

Two main documents were addressed:

- Scenarios document: uses model document as basis. Model document is umbrella for most work done within the group. Document also discusses need to prioritize scenarios.
- Architecture document: broken into 3 distinct elements:
  - request routing,
  - distribution
  - accounting

  The last one brought up a lot of discussion because of its uncertain relationship to the AAA work.

  Routing, presented by Brad Cain, involves content redirection. Various metrics are to be allowed. How this is done is out of scope and so are not addressed (QoS) is not addressed. There is a concern about security (in particuler with routing) because the draft doesn't address it at all. Authors say they will look into it.

4 RMT WG

During the session of Reliable Multicast Transport WG, Tony Speakman gave a presentation on Generic Router Assist (GRA). There are 2 drafts, the first covers building block motivation, and the second a functional specification. GRA is a network-based service that enables end-to-end multicast transport protocols to take advantage of information distributed across the network elements in a given multicast distribution tree. The service consists of a canonical set of simple functions which network elements may apply to selected packets in the transport session as they traverse the distribution tree. The functions are similar in nature to Active networking, with a number of restrictions for damage limitation, such as a general rule disallowing packet generation.

Mike Luby covered the latest drafts on:

- Layered Coding Transport (LCT) 'Building Block' (as defined in RFC3048), a massively scalable reliable content delivery and stream delivery transport, which can be used for multi-rate delivery to large sets of receivers.

- Asynchronous Layered Coding (ALC), for multi-rate reliable content delivery. ALC is a protocol instantiation as defined in RFC3048. ALC uses the LCT transport.
- Rich Content Control Protocol (RCCP), a session control protocol for client initiated content delivery.
- Congestion Control Building Blocks - it is tricky area as people don't want to standardise CC schemes unless there's been experience with it, but there's no experience unless its been standardised. There was a proposed process for new CC protocols, possibly becoming an experimental RFC as the first stage.
- Forward Error Correction (FEC) Building Blocks - Describes the abstract packet formats and IANA registration procedures for use of Forward Error Correction(FEC) codes within the context of reliable IP multicast transport. The basic information that may be present are:
  - FEC Encoding Identifier - Identifies FEC coding
  - FEC payload ID - ID's the symbols in packet payload
  - FEC Object Transmission Info

NACK-Oriented Reliable Multicast Protocol (NORM) Draft: - NACK repair process requires classification - Could be used for selective ACKing - May be necessary to specify additional segment NACK type to support large objects

General purpose NACK format: - Jon crowcroft mentioned that one could learn from TCP SACK options when thinking about NACK message formatting - Mark Handley suggested mapping session semantics to NACK bits at receiver. - RTT to sender is important, though more important is the RTT to where your NACKs are suppressed from.

TRACK Protocol Instance - There were complaints that the authors hadn't looked closely enough at the relevant Building blocks documents for the protocols suggested for use in construction of TRACK.

5 OPES WG - BoF

name change: Open Pluggable Endpoint Services

OPES (Open Pluggable Endpoint Services) provides a framework for services that operate on and provide a value-add to the content to be delivered from a content network. The concept of an edge services overlay network is introduced. The core elements of OPES are:

- OPES Intermediary - The intermediary between the client and origin server
- OPES Admin Server

- Remote Call-out Server - Server that performs various services on content via the OPES Intermediary

Concerns from Mike O'Dell about unauthorised altering of content. There may be overlap with this group and MIDCOM as far as AAA interatction goes, though in general they are complimentary as MIDCOM deals at the transport layer, whereas OPES is at the application layer.

Jon Crowcroft mentioned some insights might be gained from looking at the paper from ACIRI: "content addressable networks"

Christian Maciocco made a presentation on the suitability of Internet Content Adaptation Protocol (iCAP), and Simple Object Access Protocol (SOAP) for use as the OPES callout Protocol. ICAP is a lightweight protocol for executing a "remote procedure call" on HTTP messages. That is, it allows ICAP clients to pass HTTP messages to ICAP servers for "adaptation" – some sort of transformation or other processing. SOAP is a protocol specification for invoking methods on servers, services, components and objects, currently based on using XML over HTTP (though there's draft describing SOAP over BEEP). SOAP was seen as too generic for the purpose, though that wasn't unanimous.

Code samples for ICAP are available from from John Martin

Edge Side Includes (ESI) is a simple XML based mark-up language used to define Web page components for dynamic assembly and delivery of Web applications at the edge of the Internet. OPES is intermediaries centric, with callout servers, while ESI aims to be content centric and does things on the edge. Published as a note by W3C (http://www.w3.org/TR/esi-lang) http://xml.coverpages.org/esi.html

OPES personalised content framework (PCF): Presented by Abbie Barbir(Nortel): An example of an OPES callout server, a personalization service based on the PCF, Which will be developed as an OPES draft.

It was mentioned that the OPES devices including the callout servers will be transparent to clients.

6 SIP WG

The discussion in the Session Initiation Protocol WG revolved around how to get around firewalls with RTP/RTCP. A presentation on "Added behavior of SIP and implicit use of RTCP" was given and shot down by Jonathon Rosenburg.

Rosenburg put together a nonse scheme that does not need any standardization because it uses existing info from current documents. He is advocating adding a couple of paragraphs in teh BIS draft to make sure people don't make changes that would break his nonce scheme.

A draft RFC on a SIP extension of the INITIAL request message for discovery capability of SIP Proxies. Doubts exist about the usefulness of this approach because it could probably be done by other ways. This proposal was shot down in flames.

7 FORCES WG - BoF

This BoF (Forwarding and Control Element Separation) has now been turned into a working group. The current focus is on defining a set of requirements for now. A protocol will be defined afterwards.

Changes from the previous requirements draft include the addition of an applicability statement. An editor will be used to consolidate the different requirements drafts that have been produced to date.

Presentation was given on Linux-Netlink Kernel. Accomplishes separation of data and control plane that is desired by Forces. The rough consensus is that the draft is to be published as an informational RFC. There was one avid individual who disagreed, but it was deemed as not the rough consensus of the group.

8 ITRACE WG

During the ICMP Traceback WG session the itrace was discussed. A suggestion was made to provide a URL in the itrace system to point to keys used, with time stamps. Also a suggestion was made to include the probability used to send the itrace message in the message itself.

The intention driven Itrace (draft-wu-itrace-intention-01.txt) was discussed. There were problems with the stats in draft - taken on board.

9 TEWG WG

In the traffic engineering session, a draft RFC has presented on Network Surviveability for Traffic engineered IP networks. The presentation seemed to suggest that the document is rather light and looks a "feel good" document. In other words, it sounds nice and makes you feel good, but it doesn't say much. However, this document should be read to determine its actual value.

A draft RFC continues to be worked on involving diff-serv for Traffic Engineering. New items involve scenarios and requirements. This document should be read for informational purposes. But its important to keep in mind that few ISPs will use diff-serv in the near future.

10 OPSAREA WG

Draft RFC on Operator Requirements for Infrastructure Management Methods. It talks about the basics. For example, the requirement of using SSH, and optional support for HTTP/Forms. The author wants a standard Command Line Configuration (ie, syntax) as the basis for device configuration. The revealing comment from the author was that SNMP is NOT used as the standard way for setting devices.

11 AVT WG

RTP interop Matrix is 100% (draft-ietf-avt-rtp-interop-08.txt) Added back: G723, GSM-EFR, H263 ('96), MP2T

It was noted that audio jitter calculation is not accurate for variable-duration packets. Amos Guler suggested redefining packet "sending time" to be RTP timestamp + packet duration (as in sample size).

When ID opens again: Submit revised RTP spec which is a revision of RFC 1889 in preparation for advancement from Proposed Standard to Draft Standard status.

Presentation from J. RosenBerg (dynamicsoft) on RTP FireWall/NAT traversal SIP use of RTP not NAT friendly:

- A calls B SDP includes A's IP/port for RTP
- B replies OK and includes its IP/port to receive RTP traffic

It was suggested to change RTP/RTCP port +1 rule, so that separate ports numbers (as opposed to consecutive) could be supplied for RTP and RTCP. Christian Huitema proposed an SDP extension (TBD in mmusic WG)

Another solution presented was 'symmetric RTP' where both parties use the same port number for source and destination when sending RTP/RTCP. This is in fact not excluded by the existing spec and is actually the mode of operation in some tools (but not all).

It was suggested to have different sessions on same port. There was a proposal to reduce the SSRC and use some bits to differentiate. This causes too many problems with SSRC collision detection and blurs abstractions created by RTP for different media types implicitly designated by port number.

A Well known port for RTP may be possible but multiple tools, etc. mean there will need for a range.

Mark Handley(ACIRI): Datagram Control Protocol (DCP) - A new transport protocol which provides unreliable transport protocol, intended for kernel implementation on top of IP. It has been suggested as different apps want different congestion control dynamics(eg AIMD, TFRC). These apps may poorly implemented application-level congestion control and concerns about deploying ECN with UDP applications. It provides three-way handshake for connection setup, and allows negotiation of congestion control algorithm and parameters, with mandatory support for SYN cookies. Possible alternatives: SCTP is in process of gaining unreliable mode

Julian Chesterfield presented draft-chesterfield-avt-rtcpssm-01.txt regarding RTCP feedback in Single Source Multicast (SSM) sessions - It is suggested that the RTCP is unicast back to sender and these are reflected on to the receivers. C.Huitema mentioned Ian Wakeman paper.

Secure RTP draft-ietf-avt-srtp-01.txt - For secure RTP which leaves the RTP headers untouched and provides for encryption and/or authentication of packet. Implemented as a RTP extension so it can be implemented as a bump-in-the-stack. This revision adds source origin authentication (SOA)which may be acheived by delayed authentication using TESLA (draft-irtf-smug-tesla-00.txt), as SOA does not follow automatically from integrity protection. There are two ways of retrieving the security parameters to process the packet. The first is implicit though the SSRC, the second (and only robust method) is to use a Security Parameter Index (SPI) which would be appended to the RTP packet, before the authentication tag. There was discussion regarding whether to hide the additional security payload by including it in the padding. It was stated that SRTP, as a security protocol should be independent of key management. An SDP attribute format has been suggested. There plans to elaborate on interactions with RFC2733 (Generic FEC in RTP) and SRTP plus other FEC schemes. Note: RTCP encryption prefix of RFC1889 must not be used. There was discussion concerning making it work with unicast and not getting too involved in complex multicast solutions.

12 IPFX WG - BoF

A new working group for IP Flow Export meant to help operators. Its focus involves a means of identifying flows and exporting them to other routers, network management, and billing devices. In addition, it would support security in the form of keeping track of audit trails. The initial focus of the group is to come up with a standard terminology. The output of the group is not to come up with another accounting mechanism. The group may look into how MPLS fits into its agenda.

13 IPSEC WG

Management Information Base drafts are just about ready for working group Last Call.

How should Counter mode AES be implemented? If counter inputs can be managed on IPSEC chips security evaluators will be happier with security-in-depth. A discussion will be happening at the NIST mode workshop later this year.

13.1 Son-of-IKE

Main issues are SETP compatibility and NAT/firewall traversal. NAT draft authors hope for advancement ASAP for implementation. UDP encapsulation draft has interoperability test next week. WG agreed AH support should not be included. Last call should occur in about 3 weeks.

First version of FreeSWAN opportunistic encryption is out, along with a draft describing the combination of IPSEC and DNSSEC used. Concerns over CPU load on webservers and lack of user incentives but group felt documents should be published as experimental to gain operational experience.

Security area directors have decided that IKE is just too complex to ask "is it correct" – but not insecure. Therefore groups should not extend it at this point.

Using implementation experience, WG intends to develop design criteria for filtering future IKE change requests and discuss what to do with IKE. Suggestions include: remove aggressive mode (halves complexity); remove public key encryption (removes half the key types) – reduces phase 1 from 8 to 2 protocols; allow stateless operation; more compact parameter negotiation using multiple proposals. Maybe remove phase 2? Invert identity protection – better addresses threat model, Remove phase 2 PFS (already in phase 1) and commit bit? Additional functionality requested: unidirectional authentication, strong password support (eg EKE).

Matt Blaze working on Just Fast Keying protocol as a replacement; he felt making small iterative changes to IKE will not make it easier to prove its security.

14 SMUG WG

Should group change its name to Secure Multicast and Group Security (SMUGS) or Group Security (GSec)? Will be discussed further on the group mailing list.

Future research areas suggestions: group policy management, decentralised group key management, closed vs open groups, security for multiple senders, non-multicast security, reliable multicast security.

A research scheme was presented using key trees to provide efficient revocation even in large groups.

Another method to bound communications update messages by finding optimal hybrid tree was presented.

The results of an investigation into wireless/mobile key management were described; immediate rekeying when clients move between different areas within the same domain was found to be the most efficient method.

A scheme was proposed to provide authenticated group joins using new IGMP authentication query and response messages; the group controller/key server gives signed tokens to authorised clients which are verified by routers before permitting joins.

15 MSEC WG

The Multicast Security WG address intially, Which applications should be targetted by this group's key management protocols. Reliable Multicast Transport and Secure Real-time Transport Protocol were suggested.

A re-key protocol was presented: it should support fast and efficient group and key-based keying, reliable transport payloads, and reduce key tree traffic.

Group members can optionally unicast status messages and leave/renew notifications to a Key Distribution Centre. Could this be used to do secure subgroup communication? WG thought that would add too much complexity for little benefit.

Group Security Association Key Management Protocol Lite (by Hugh Harney (hh@sparta.com) was reviewed: authors are trying to remove requirement for unicast Security Associations in group establishment and management.

A key management (TESLA) for multimedia sessions (including SRTP) draft was presented. These sessions require low CPU overhead, little packet expansion and the preservation of header compression. Protocol is based on current session control mechanisms and has one return trip setup time. The WG thought that security aspects of the draft should be managed in this group, while the multimedia aspects should go to the MMUSIC group.

A Group Domain of Interpretation draft was presented. This protocol coexists with IKE, using IKE's phase 1 but providing a new phase 2 that listens on a separate port. This phase is responsible for registration and rekey exchanges.

16 HIP WG- BoF

The Host Identity Payload was addressed. It aims to decouple transport from internetworking layer by providing new authenticated host namespace.

Core draft is nearly finished, others on NAT and mobility are coming along.

HIP has benefits for mobility and multihoming: it removes difficulties with "does the same entity own these addresses?" problem. Also with NAT, changed IP addresses no longer break security if Security Association is instead bound to HIP name.

Speakers suggested that the group needs specific problems to work on; mobility and multihoming were suggested as both have WGs with specific requirements.

17 GEOPRIV WG

The Geographic Location and Privacy WG has tight schedule which has slipped 1-3 months.

Privacy framework draft will be developed first as an informational RFC, then used to improve privacy in HTML and HTTP location services, create API, and finally submitted as a standards-track protocol.

Internet Architecture Board will take results of the WG and develop Best Common Practice document specifying rules other WGs must follow in this area.

First document should include threat analysis.

WAP forum and 3GPP both have work that should be considered on location services.

WG won't be choosing actual format or payload but developing guidelines that other WGs can use to do so.

18 Open Security Area Directorate Meeting

Should the Performance Implications of Link Characteristics WG recommend link layer security? Group was divided: some felt it will just discourage people from using end-to-end security, others that link layer security is out there and IETF should tell people how to use it properly. The security Area Director thinks Wired Equivalent Privacy has been a complete failure and that is what will happen with other such protocols.

19 MIDCOM WG

The relationship of the Middlebox Communication WG to the Open Pluggable Edge Services WG is expected to be the transport and application layer.

It is questioned whether MIDCOM is a client/server or peer-to-peer protocol? There was some discussion over which party initiates each transaction but generally group thought it was client/server.

Long discussion was held over directionality of transactions; eventually transport AD said the discussion was on another planet and should be limited and discussed by mail.

20 IPSP WG

The IP Security Policy WG addressed with comments the complexity of IKE. It was agreed to limit activities to the currently existing IPsec RFCs and drafts.

A set of changes were presented on ICPM (IPsec Configuration Policy Model). Some of these changes are related to IP filtering and the addition of an execution strategy termed as "Do Until Failure".

Policy Information Base (PIB) specifics were also presented; these are used by policy servers to distribute policies to IPsec-enabled devices such as gateways, routers or hosts using the COPS protocol. Nokia is implementing this model; Intel was also working on it, but nobody in the room knows which is the current status of this work from Intel.

Most of the drafts of this WG are going to be conducted to WG last call. Then, they will be sent to the IESG to be considered as RFC docs.

The design of the Secure Gateway Discovery Protocol and the new version of the Security Policy Specification Language (SPSL) will be priorities for the next few months.

21 PKIX WG

Really "boring" session where nothing really interesting was presented. Just a logotypes draft, proposing the inclusion of one picture or logo in every X.509v3 certificate, and one method for recovering from disasters when, for example, the CA private key is compromised.

22 IPNG WG

The WG name will change from "IP Next Generation" to "IP Version 6".

The current status of the collaboration between the 3GPP and this group was presented, in terms of revising and improving the use of IPv6 in 3GPP. The 3GPP architecture will deliberately not be under question which means, for example, that won't be recommended by this group to change the current mobility design in 3GPP to Mobile IPv6.

Some options for the IPv6 dialup process were presented like, for example, the usage pattern (static vs roaming users), the kind of address space to use (never /128), static vs dynamic routing and so on.

Presentation on multilink subnets, defined as a collection of independent links, connected by routers, but sharing a common subnet prefix. The benefits are simplified management (e.g. in the home). The different entities are connected via multilink subnets router. A number of approaches are detailed, with a later version which will narrow the solution space to a recommended approach.

Short presentation on the DHCPv6 draft status, which will be in a last call after August.

A proposal for minimum IPv6 functionality required for a cellular host was given, which seems to be the previous document for an IPv6 host requirement document. This cellular hosts, or terminals using an air interface to connect to a cellular access network, are characterised by having very limited size, memory, processor and battery capacity, which implies that the size and complexity of the SW must be minimized, avoiding those not-essential characteristics of IPv6. Some of the characteristics to be supported by every cellular host are: neighbour discovery (although some messages can be avoid in some specific cases), IPsec, and CN functionality. This work will be used as an input from the IETF to the Release 5 of 3GPP.

Basic discussion on AAAv6 was produced but it was not considered by the assistants as a topic to be managed by this group. The AAA just wanted a 'reality check' on the draft from the IPNG WG. Charlie Perkins raised the question whether IPv6 might eliminate need for NAI?

23 POLICY WG

The terminology for the policy framework is scheduled to be sent to the IESG to be considered as RFC.

The PCIMe (Policy Core Information Model extension) needs some changes in IPHeaderFilters, to add a level of criticallity of conditions and actions, and to revise the list of fields to be filtered on.

Great consensus on the good work during last year on QPIM (QoS Policy Information Model). It seems to be very advanced and ready to start to be implemented. There will be a new version of the draft and then it will be sent to last call.

24 SeaMoby WG

The topics of discussion in the SeaMoby group comprized of:

24.1 L2 triggers

During the first session L2 triggers with respect to mobilty were addressed. The goal has been to collect requirements from various WGs for L2 triggers to optimize handoff. The output from such effort would be used to design an API or protocol if desired. Draft discusses requirements from the following FMIPv6 and low latency MIPv4 Seamoby context transfer.

The WG addressed the issue about reason for existence of two sets of requirements, one for MIP and one for SeaMoby. The argument for such separation has been the existence of two (somewhat) different application areas, although a merge of both into a single requirement set was left as a dangling issue.

As the process of MIP handover and seamoby CT were immediate generator of requirements for L2 triggers, a common decision was to include their requirements set into a unified one.

While CAR is also relevant to the both MIP and CT, it was questioned whether QoS bears also similar relevance for consideration for a requirements merge.

L2 triggers may well constitute a reason for the creation of a joint WG with Seamoby created under the Sub-IP area.

24.2 Issues in CAR

Seamless IP mobility protocols assume that the identity of the target AR (TAR) for MN's handover is known to the current AR. TAR needs to be selected based on MN's requirements, AR capabilities and local policies.

The problem identified is to determine a set of CARs (i.e. the ARs that physically adjacent (PAARs) to the current AR and have the capabilities to support the MN's requirements). A new draft specification was also proposed by UCL (pagtzis-proactivev6) that describes a scheme for identifying a set of neighbouring CARs. This information serves as input to the TAR selection process at the time of handoff.

Pros and cons of anticipated vs. dynamic CAR discovery vs hybrid CAR discovery were discussed:

- Radio traffic
- East of PAAR identification
- Control over TAR selection
- Simultaneous connections to two ARs from MN
- Power conservation issues
- capabilities exchange

It was questioned whether seamoby should develop protocols separately for the anticipated and the dynamic case, and leave it to the network operator to choose one over the other; A hybrid CAR discovery protocol may emerge.

It was pointed out that mobiles may be simultaneously attached to several wireless networks. As such it was questioned how to handle ping-pong effects in such cases.

Handoff candidate will require some security relationships; as such scalability is to be addressed. Nevertheless fast handoffs at L3 suggest that such work is imperative.

24.3 Paging

Work relating to paging is aligning around the paging requirements. Protocols are to be submitted by 14th of September. Comparison against the requirements is mandatory for each protocol. The relevant reference requirements document must be in place for relevant use by the 28th of September. Protocols would be considered against this set of paging requirements with the intent to identify a winer.

24.4 Considerations for Context Transfer

The basic issue is that it is not known beforehand which direction in which a mobile may be going. There are special cases where this is not true. It is possible that CT can happen at anytime, before, during or after a handoff.

If this does happen, then you may need to CT to many ARs. This is a one-to-many CT requirement; it is thus, argued whether this issue should be in the requirements Internet-Draft.

It is also argued that CT shouldn't be tied to a CAR.

The discussion addressed the need for consideration whether CT must be done at the edges as opposed in the core network. It was further argued that CT must be initiated either by the network or by the mobile. It arises as a requirement that initiation signalling for CT must be separate from the CT itself. This is mainly useful when no L2 triggers exist.

The discussion also addressed the introduction of proactive versus reactive CT whether it merits existence in the requirement set. However, people felt that it lead to modes which look more like a solution rather than a requirement.

However, constituents argued that it is really the timing issue that the words attempt to convey rather than a set of modes.

The issue of Multiphasic requirement was also considered. It was agreed that transfer of context in phases would allow time critical state first, and non-critical later. CT addresses performance of transport protocols assuming IP connectivity is available.

From a MIP-seamlessness perspective the handover is not complete without CT. It is a question of how to reinitialize features if not transfered through CT. A case for profile types may be in order.

CT negotiation was brought up. However, it was considered as too slow in the light of seamlessness.

It was also mentioned that MN may carry its own context. That would also present as more imperative the need for authenticated context transfer. However, this may have to rely on transmission over the air of context. It was argued that there may not always be bandwidth available to push CT from MN to router. Looking at simplest case, AR to AR, sec assc., etc. Could establish associate. BU in MIP, problem. Req doc should not prohibit.

25 MIP WG

The following topics were discussed during the MIP sessions:

25.1 MIPv4 to draft standard

Current status and reasoning of why RFC2002 should move toward draft standards from its current status as proposed standards. He mentioned that multiple interoperability tests have been performed and there has been significant deploymen

The following implemented options were pointed out:

- 'R' bit in the agent advertisement =¿ may be superseded by AAA work.
- Prefix length extension in agent advertisement =¿ never implemented and not interoperated.
- 'S' bit in registration request message =¿ haven't shown interoperability, refers to simultaneous registration with separate COAs.

As per 2002bis-06, Mobile IP implementations should include HMAC-MD5 as one of the additional authentication algorithms. This algorithm is used for producing and verifying the authentication data in Mobile IP registration messages.

If the requirement of using HMAC-MD5 is mandated, it may take six more months before draft moves for the last call. The alternative suggested was to remove this portion from it and proceed taking the draft spec to the proposed standards. It is noted that it is not required to have implementation of HMAC-MD5 in order to progress toward proposed standards.

25.2 MIPv6 security update

The discussion was based on MIPv6 protocol and the requirements for a security solution discussed in draft. It was mentioned that the draft has an approval from security ADs and pointed out a couple of outstanding items like implementation and usage of IPSec. The goal is to progress MIPv6 draft to PS by the end of year 2001.

The current proposals that specify alternative solutions for the binding update problem are:

- draft-thomas-mobileip-ha-cookies-00.txt
- draft-perkins-bake-01.txt
- draft-montenegro-sucv-01.txt

The intent is to have an agreed upon solution that is acceptable to the security area directors and meets the requirements specified in the requirements I-D.

Further discussion lead to whether Routing Optimization should be a part of this draft and its impact on 3GPP2 work.

25.3 Mobile IPv6 update

The issue related to authentication data passed with a BU destination option. It was felt as, currently unclear on how IPSec can be used and how to handle potential IPSec problems. Also the issue with piggybacking IPSec on binding update data is still open. The further discussions on ESP vs AH may be continue on the mailing list.

It seems home agent discovery may need more work, however, the draft is pushed for the WG last call.

25.4 Low Latency Handover

This draft was considered completed and may be ready for the WG last call. The discussion lead toward using trigger defined from mayfolks-l2-trigger draft rather than defining separate subset-specific to this work.

Individuals mentioned that there might be a problem of introducing dependency. No decision was made in the meeting on this issue.

25.5 Fast Handover

As per this draft, the mobile node can initiate a handover while it still has L2 connectivity to the current access router and about to move to a new access router. Minor editorial changes required to this draft.

L2 and L3 were claimed to be decoupled. It was felt that AP was nothing but the foreign agent and hence it will have L3 address. However, it was said L3 information is generally obtained from L2. There is no agent advertisement involved here and hence may reduce delay. Also old CoA is reused.

25.6 BETH

Brief overview of BETH. Claims an extension to the Fast Mobile IPv6 handover protocol described in that reduces the amount of L3 latency in Mobile IPv6 handover to zero. It also removes routing loop problem.

However, the addressing that is being used is topologically incorrect until the MN decides to surrender it old care-of address. The feeling of the authors was that such issue was simply philosophical. This is not necessarily the feel of all constituents.

There were many questions raised by the group like how the new AR detects when the MN has an operational new CoA and tunnel tear down is started; bicasting is specified but the smoothing is not well understood; this draft may be dealing with rare cases only; for certain type of radio links the solution provided by this draft may not work etc.

The proposed plan is to incorporate BETH into the FMIPv6 specification as another way for achieving fast handoff. The scheme currently existing in the low-latency (v4) will also be aligned with the BETH proposal.

25.7 FMIPv6 Implementation experience report

Brief summery of FMIPv6 implementation experience. Handovers are all network initiated using UNIX based router, LINUX MN on 11 Mbps WLAN. The following issues were identified:

- What destination address to use in the F-BU? It was confirmed by group that global IP address should be used instead of local address as suggested by current specifications.
- Creating binding cache entry on previous access router (after receiving Hack and after sending F-Back to the old link). It was concluded that this is implementation specific and doesn't really have any protocol impact.
- What source address to use when sending F-BU from newer AR?
- Issues may be related to sending of F-NA (including only one IP address suffices). The group provided comments that it is essential to know both Hack and F-Back.
- When to change default router? There are two options proposed: after receiving proxy PA (may be not) or after actually attaching to the new link (the new AR).

25.8 Handover Smoothing

Handoff smoothing is currently part of low latency draft along with simultaneous binding and currently it is not supported in FMIPv6. The current proposal is to add handover smoothing to the FMIPv6 draft and remove it from the low latency draft. The following comments/proposals were received from the group:

- FMIPv6 and smoothing may be defined as optional
- Bicasting may be treated as implementation specific.
- Bicasting is a useful feature needed for handovers
- There may be lot more work involved in removing smoothing from the low latency draft
- Bicasting is meant for achieving fast handovers and not necessarily for the handover smoothing

Discussion on smoothing vs bicasting and buffering. It was determined that smoothing has a larger scope than either bicasting and/or buffering and should be considered as a separate work item. However for the fast handoff work a consensus call was done to determine if bicasting should be included as part of the FMIPv6 specification.

The final consensus was to move bicasting to a separate document for both the v4 and v6 fast handoff drafts.

Consensus call for including bicasting in the fast handoff document was not very clear at the previous meeting. Clarified the question requiring consensus. The consensus call essentially was to see if people wanted to see bicasting as another option within the fast handoff specification. Consensus reached: Separate bicasting from fast handoff.

25.9 LMM Requirements

Presentation of the major issues that have been raised on the Mobile IP mailing list since the last IETF[50] w.r.t LMM. The edited draft captures the requirements for an LMM solution. Discussion focused around obtaining consensus on the requirements and also to clarify the issues that have been previously discussed.

One major issue that continues to persist is the one dealing with the levels of hierarchy. A long discussion on the pros and cons of single vs multiple levels of hierarchy ensued.

Since there was no conclusion on levels of hierarchy, it was decided that the editor would work with some of the interested people on this topic to arrive at some consensus. This should be documented in the next revision of the requirements document.

25.10 Mobile Network Suppport

Thierry Ernst presented the draft on support for mobile networks and routers for IPv6 using Mobile IPv6.

Obviously this topic needs to be investigated more as it raised more questions than answers at this time. Basavaraj mentioned that the work does fit into the Mobile IP WG as the charter does not limit the scope to just mobile hosts. There were some concerns about stepping into MANETboundaries.

Erik Nordmark mentioned that the issue of authorization for mobile networks is a hard problem to solve and hence suggested that more work needs to be done in this area.

Opinions on the need for this work being done in the MIP WG were expressed by many people.

Conclusion was that more work needs to be done in this area. This draft is a good starting point and could be used to investigate the issues raised by Thierry in his presentation.

25.11 Nat Support in Mobile IPv4

Conclusion reached at this meeting was that Mobile iPv4 does not currently work very well in a NAT world and scenarios where support for MIPv4 with NATs is required were discussed. The need for a solution for Mobile IPv4 over NATs was identified.

Most WG members agreed that this work is important for MIPv4 deployment. A discussion list will be setup to discuss the scenarios and requirements for NAT support in MIPv4. The WG will make a decision regarding the inclusion of supporting NATs as a WG item at a later time.

25.12 Mobile IP Component Redundancy

This could not be presented due to a lack of time.

26 MANET WG

The agenda for this session involved:

- Unicast: It involved
  - Updates to Core OLSR.
  - Updates to TBRPF.
  - DSR Performance results with Flow State.
- Addressing
  - ZeroConf and Manet Issues
  - Stateless address autoconfiguration in Mobile Ad Hoc Networks using site-local addresses
  - General WG discussion of manet addressing
- Unidirectional Links
  - Unidirectional link support draft
  - General WG discussion of manet unidirectional link support

- Performance
  - MANET TCP Performance via ns2 simulation
- Multicast
  - OLSR Multicast draft
  - ADMR Multicast draft
  - General WG discussion of multicast status

26.1 OLSR CORE UPDATE

An updated version of the Optimized Link State Routing (OLSR) specification was discussed. The authors missed the ID cutoff date for London but will submit a revised ID shortly after the IETF. An initial document was provided to the mailing list for comment and perusal prior to the London meeting. Some of the significant changes include the following:

- support for multiple interfaces: This capability is provided by a routing node using one of its addresses as its "main address" or "router ID"- and having control messages transmitted on all interfaces.
- adds the ability to support routing advertisement of associated hosts and networks. A new message type is added that allows for host/network route injection for non-participating OLSR nodes within an OLSR cloud.
- provide mechanisms for improved neighbor sensing and control packet jitter. The random jitter helps prevent transmission syncing among clusters of nodes and improves performance in 802.11 MAC layers with multi-hop channel contention. Recent OLSR implementors have been experimenting with Jitter and improved neighbor sensing algorithms.

26.2 TBRPF UPDATE

An updated version of the TBRPF specification was discussed. Some of the discussion included the following:

- further work on a partial topology (PT) version of TBRPF that is intended for improved performance in for dense topologies (vs. full-topology)
- changes to reduce overhead and to modularize the neighbor discovery method. The use of differential HELLOs introduced along with periodic HELLOs, and the use of NACKs for reliable control delivery was dropped.

A potential merge of the hello mechanisms was proposed between TBRPF and OSLR

There was discussion that the proactive routing team had some early goals to explore commonalities of approaches. There appeared to be some recent convergence but still numerous differences were cited. There was agreement that since the updated IDs were due out soon that further technical discussion and debate could be taken to the list at the appropriate time.

26.3 EVALUATION OF FLOW STATE IN DSR

An overview of the DSR flow state extensions and studies was provided. The flow state in DSR used a IP source, dest, flowID concatenation, FlowID can be handled implicitly or explicitly.

A route error is sent if a flow is not recognized.

There were numerous simulations performed and these will be discussed at the upcoming Mobihoc 2001.

26.4 ZEROCONF CONSIDERATIONS

Discussion of zeroconf issues and emerging questions and how they potentially relate to the manet WG. Some related peripheral issues had recently been raised on the manet mailing list regarding generic multihop flooding and multicast services. E.g., consideration of ALL-MANET-ROUTER addressing and forwarding schemes,etc.

In summary, claim and defend approaches typically used to autoconf. The possibility to apply autoconf to MANET exists with complex issues to be addressed than are typically considered with infrastructure autoconf. There is a need to consider and address scoping issues given the ad hoc and multihop wireless nature of a manet.

Tradeoff of periodic messaging vs. de-conflict through normal usage. The latter implies some aspect of multicast in normal usage.

The presentation continued with zeroconf vs. configured modes of operation. It identified the need for ALL-NODES-MULTICAST address (DAD), scoping and reasonable flood mechanisms. mini-DHCP server interaction was also considered. It was questioned whether all host routes may be available.

26.5 STATELESS ADDRESS AUTOCONFIG

A short proposal was presented relating to stateless address autoconfiguration for manet.

26.6 BUILDING TOPOLOGY GRAPH IN OLSR

Brief description of work done with OLSR to further explore unidirectional routing links within the topology. The challenge currently is how to transmit data over a unidirectional link. How to make ARP work, 802.11 issues, etc

26.7 TCP PERFORMANCE IN MANET

Brief description on how to explore TCP interaction with some example manet routing protocols. Through simulations between OLSR and AODV (w/o link layer detection) there was a trend for OLSR to demonstrate significantly improved TCP throughput in some scenarios, while the CBR test results demonstrated similar perfomrance. The main point was that under different traffic scenarios and topologies routing end-to-end results can vary greatly.

26.8 MULTICAST IN OLSR

Findings and thoughts on working with a multicast version of OLSR. It was felt by the authors that IGMP and wireless multi-hop operation is broken since the link has a semi-broadcast nature. In an approach he has been evaluating each node chooses its multicast router. (routers periodically announce themselves).

26.9 ADMR

Multicast extensions to DSR were presented. The chairs pointed out the the ADMR ID would be downgraded to personal until the WG had come to consensus on future multicast work and direction.