Analysis of MANET and NEMO

draft-boot-manet-nemo-analysis-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 28, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document provides an overview of models for MANET and NEMO. It describes the MANET and the NEMO characteristics. It also also lists problems using the MANET and NEMO technology, when problems are not described in other documents. It is claimed that MANET suits small mobile network topologies, providing optimal paths for communication within a MANET cloud and towards the outside. It is also claimed that NEMO suits small mobile subnets, providing sub-optimal paths for to Internet connected nodes. This document is used for evaluating a need for a MANET for NEMO, called MANEMO.
Table of Contents

1. Introduction .............................................. 4

2. Terminology ............................................. 5

3. MANET classification and models for hierarchy ............. 8
   3.1. Sub-IP MANET ....................................... 8
   3.2. Isolated MANET ..................................... 8
   3.3. Interconnected MANETs ............................... 9
   3.4. Stub MANET ......................................... 10
   3.5. Layered MANETs ..................................... 10

4. Fringe Stub models ........................................ 12
   4.1. Layer-2 Access ..................................... 12
   4.2. Layer-2 Meshing ..................................... 12
   4.3. Node Mobility ...................................... 13
   4.4. Network Mobility .................................... 14
   4.5. Nested NEMO ........................................ 14
   4.6. MANEMO ............................................. 15

5. MANET and NEMO Characteristics ................................ 17
   5.1. Scalability .......................................... 17
   5.2. Mobility ............................................ 17
   5.3. HA dependency ...................................... 18
   5.4. Route optimization .................................. 18
   5.5. Interface type ...................................... 18
   5.6. Multicast support .................................... 19

6. Problems found in MANET and NEMO .......................... 20
   6.1. Worst Path First Syndrome ........................... 20
   6.2. Break Before Make problem ........................... 21
   6.3. Routing loops in proactive routing protocols .......... 22
   6.4. Congested link avoidance ............................ 23
   6.5. MANET and NEMO at home problem ...................... 25
   6.6. MANET scale to infinity problem when peering to strangers ........................................ 27

7. IANA considerations ........................................ 29

8. Security Considerations .................................... 29

9. Acknowledgments ............................................ 29

10. References ................................................ 29
    10.1. Normative reference ................................ 29
    10.2. Informative Reference ............................... 29
Appendix A.  Change Log ........................................ 32
    A.1. Changes from version 00 to 01  ......................... 32

Author’s Address ............................................... 32
Intellectual Property and Copyright Statements ............. 33
1. Introduction

IP technology is increasingly being used in mobile networks. Many issues arise with mobility, for example wireless bandwidth and link quality are typically low related to fixed, wired infrastructures. Also routing protocols for mobile environments are faced with new challenges; connectivity comes and goes when nodes move and link quality increases and decreases instead of flapping between an OK and an NOT-OK state.

Two IETF mobility technologies are available, that is Mobile Ad-hoc NETworks (MANET) [1], [2] and Mobile IP (MIP).

The MANET workgroup is working on routing protocols, running on mobile or fixed routers; either in small isolated topologies or at edges of large IP infrastructures. Multiple types of MANET protocols exist; OLSR [3] is a proactive MANET protocol populating the routing table independent of any user traffic; DYMO [4] is a reactive protocol, providing path information for traffic flows and SMF [5] is a multicast flooding protocol.

The MIP4 and MIP6 workgroups are working on mobility support for hosts, enabling session continuity while moving. Other workgroups are working on improvements on MIP, for example MONAMI6 and MIPSHOP are working on using multiple interfaces towards the IP infrastructure. The NEMO workgroup extends MIP using the Mobile Router concept, providing MIP services for MR attached nodes. With NEMO, nesting can occur, introducing new challenges.

Currently, a number of communities are working on network architectures for mobile domains. Different communities work on different domains, all having their specific requirements. Work within the IETF would comply with all those requirements. Sample domains are military, public safety / emergency response networks, mobile networks used by enterprises and non-governmental organizations, provider based Internet access, license-free wireless networks and networks for intelligent transport systems / vehicle communication systems. Also combinations of multiple domains can be used, for example a mobile network for a disaster relief organization could use own licensed transmission means, provider based Internet access and license-free wireless networks; all used in cars also equipped with an inter-vehicle communication system / intelligent transport system.
2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [6].

Readers are expected to be familiar with all the terms defined in RFC3753: Mobility Related Terminology [7] and the NEMO Terminology draft [8].

MANET

Mobile Ad-hoc NETworks [7]

NEMO

NETork MObility [8]

NEMO BS

Network Mobility Basic Support Protocol [9]

NEMO RO


MIP

Mobile IP [8]

MIP4

IP Mobility Support for IPv4 [13]

MIP6

Mobility Support in IPv6 [14]

OLSR

Optimized Link-State Routing Protocol [3]

DYMO

Dynamic MANET On-demand Routing [4]
SMF

Simplified Multicast Forwarding for MANET [5]

OSPF

Open Shortest Path First [15][16]

MONAMI6

Mobile Nodes and Multiple Interfaces in IPv6

MIPSHOP

Mobility for IP: Performance, Signaling and Handoff Optimization

HAHA

Global HA to HA protocol [17]; [18]

MNR

MANET Router [2]

MR

Mobile Router [7] [8]

MH

Mobile Host [7]

HA

Home Agent [8]

CN

Correspondent Node [8]

LFN

Local Fixed Node [8]

RA
Router Advertisement [19]
3. MANET classification and models for hierarchy

MANETs can be classified based on different deployment scenarios. The classical MANET approach focused on a single, contiguous MANET region. Now MANET technology is getting mature, focus is shifting towards interfacing between different MANETs and MANETs connected to the Internet. This section provides a classification of MANETs and models for MANET hierarchy.

Deployed MANETs can inherit characteristics of different models.

3.1. Sub-IP MANET

MANET technology can be used below the IP layer. The MANET forms a single IP subnet, where nodes can reach each other transparently. The subnetwork provides full connectivity for unicast and multicast / broadcast. RFC3819 [20] provides advice on subnetworks.

```
+-----------------------+
|                       |
|     Sub-IP MANET      |
|                       |
+-----------------------+
:+---+            +---+: = Classic IP Interface
| N |  * * * * | N |
++--++            +---+
```

Figure 1: Sub-IP MANET

Sub-IP MANETs are transparent for the IP layer and do not introduce special requirements.

3.2. Isolated MANET

An Isolated MANET is a single, contiguous MANET region. MANET routers within the MANET region provide connectivity to attached hosts. No Routers are attached to an Isolated MANET.
3.3. Interconnected MANETs

MANETs can be connected to each other, forming a single network infrastructure.

The MANET Border Interface connects the two routing regions. Route filtering and summarization can be configured. Border Interfaces are typically not formed ad-hoc.
3.4. Stub MANET

Stub MANETs are connected to a Fixed Infrastructure or the Internet. Connectivity to the Fixed Infrastructure is provided with default routes. Connectivity to the Stub MANET can be provided with an aggregated prefix.

A Stub MANET could have redundant MANET Border Interfaces. The Stub MANET will not act as transit region.

3.5. Layered MANETs

MANETs can have a layered structure. Connection to the top level is similar to a Fixed Infrastructure connection. The lowest level can be configured as Stub MANETs. MANETs in the middle layers provide transit services.
Layered MANETs have a fixed structure. Mobility within the MANET is supported. Dynamic border router formation between the MANETs is currently not foreseen.
4. Fringe Stub models

In the (Wireless) Fringe Stub, an almost infinite wireless ad-hoc topology is connected to a Fixed Infrastructure. The Fringe Stub is not required to be continuous, the Fixed Infrastructure is used to interconnect isolated segments. Mobile Routers can roam between isolated segments without any reconfiguration.

In the Fringe Stub models, Layer-2 Access, Layer-2 Meshing, Mobile IP, NEMO and MANET technologies are used. Deployed Fringe Stubs can inherit characteristics of different models.

4.1. Layer-2 Access

Mobile nodes can use a layer-2 Access service provided by telecommunication providers. Classical IP interfacing is used, so special requirements are introduced. Depending on the provider or the technology used, micro mobility or macro mobility is provided.

```
<----------------------------->
<                       >
< Fixed Infrastructure    >
<                       >
< :---------------:R:---------------:R:---------------: >
< R                  R      R                  >
<----------------BS----------------BS----------------BS-------->
   BS = Base Station
```

Figure 6: Layer-2 Access

4.2. Layer-2 Meshing

For reducing costs of the infrastructure or to extend area of reach, Relay Stations can be used to enhance the Layer-2 Access model. This provide also some kind of redundancy. When the Base Station is isolated from the backbone, an alternative path via another Base Station can be used.
4.3. Node Mobility

MIP (MIP4 [13] and MIP6 [14]) provide mobility and handover functionalities to mobile nodes. Mobile IP is targeted for providing "macro mobility". It provides session continuity over different heterogeneous network types and provides global roaming. "Micro mobility" using link-layer mobility services would provide better handover performance [13]. Optimizing handover using IP technology is work-in-progress.

The Home Agent (HA) takes care of reachability for served Mobile
Nodes. The Corresponding Nodes (CN) find the path to Mobile Nodes via the HA.

4.4. Network Mobility

Network Mobility (NEMO basic, [9]) extends Mobile IP for roaming subnets. Local Fixed Nodes (LFN) connected to the Mobile Router (MR) benefit form the MR MIP service.

Figure 9: Network Mobility

The MR serves local connected hosts and local connected routers, called Local Fixed Nodes (LFN). The "Egress Interface" is used for reaching the HA, either directly when at home or via the MIP tunnel when the MR is at a foreign network. Mobility service is provided via the "Ingress Interface" for a Mobile Subnet.

4.5. Nested NEMO

With NEMO, visiting mobile nodes are supported, this is because MRs are able to connect to the Ingress interface of other MRs and configure their CoAs/receive connectivity via the MR they are
temporarily attached to. Mobile Hosts are stubs, as they do not provide forwarding. Nested Mobile Routers can form an arbitrary level of nested HA tunnels.

Figure 10: Nested NEMO

Nested Mobile Routers form tree topologies. Pin-ball routing is introduced, discussed in a section on Route Optimization below.

4.6. MANEMO

With MANEMO [21], [22], MANET technology is introduced in Nested NEMO. The main goals are implementing NEMO Route Optimizing, supporting floating Nested NEMO topologies and providing optimized paths within the MANEMO Fringe Stub without using NEMO tunneling.

A suggested solution is using a tree discovery protocol [23]. The tree structure is used for optimizing packet forwarding between Mobile Nodes and the Exit Router [24], [25]. The tree can also be used for inner-tree communication and multicast support.

Another suggested solution is to use direct communication between
1-hop neighbors by advertising the mobile subnet prefix using IPv6 Neighbor Discovery [25], [26].

Also using MANET technology is suggested [22], [27].

In MANEMO, the interface types Ingress, Egress and MANET could be logical roles. Physical interfaces could have any role and policies on MRs can limit the roles on particular interfaces. This relax the definition of a NEMO MR [9].

Exit Routers are Fixed Access routers running MANEMO protocols or top level Mobile Routers.

MANEMO Fringe Stub is work in progress. MANET proactive, reactive and source-routing technology is used in addition to Nested NEMO.
5. MANET and NEMO Characteristics

5.1. Scalability

MANET and NEMO have very different goals. MANET can provide optimized paths within a limited topology, where NEMO provides Internet scale end-to-end connectivity. Therefore, scalability characteristics for MANET and NEMO are very different.

MANET scalability is researched and many improvements are proposed. But still MANET networks have their limits, a large number (100 or more) of Mobile Routers in a flat area is a topic for active research [2]. Other technology must be used to provide Internet scale deployment.

The OSPF MANET extension [28], [29] is applicable for a limited number of routers interconnected with radio interfaces. Such a MANET subnetwork would be part of an OSPF area, and OSPF (and BGP) routing state flooding reduction mechanisms enable large scale deployment. Many independent OSPF MANET subnetworks can be deployed, similar to for example Ethernet segment scalability.

Other MANET protocols could use the same approach. A MANET domain can be connected to a fixed infrastructure and route aggregation hides routing state flooding.

NEMO makes use of the MIP tunnel overlay, hiding mobility on the fixed Internet infrastructure. The number of mobile networks scales with the number of home agents, and address aggregation enables huge scale NEMO deployment.

5.2. Mobility

With MANET, a MNR can roam within an area where sufficient coverage is available. When the number of MANs increase, coverage will improve or the area will be enlarged. Scalability issues restrict the number of MANs, which implies restrictions on mobility. Zoned or hierarchical models are proposed, but world wide mobility would not be provided by MANET.

With NEMO, "macro mobility" is inherited from Mobile IP. Worldwide mobility can be provided for an almost unlimited number of MRs, all having end-to-end connectivity.

For both MANET and NEMO, mobility is also related to radio coverage. No coverage implies no connectivity.
5.3. HA dependency

MANET does not depend on Mobile IP and doesn’t need a home agent.

NEMO extends Mobile IP using a Mobile Router. The Mobile Router maintains a tunnel to its home agent. Traffic between LFN and CN flows through the tunnel and thus the home agent is a critical element for communication. HA dependency can be relaxed by HA redundancy or new protocols, like Global HA to HA protocol (HAHA) [17] / [18]. MIP and NEMO Route Optimization could also relax the HA dependency.

For communication from a NEMO LFN to a far away CN, the HA dependency may not be a problem. But for local communication, this could be unacceptable, especially in military and public safety / emergency response networks, where local communication availability is a primary concern.

5.4. Route optimization

MANET protocols would select a shortest path (fewest hops, lowest metric) or an optimized path based on cross-layer metrics. Problems with optimized path selection based on fewest hop count are described below in section Worst Path First Syndrome.

Currently, nested NEMO based on NEMO BS [9] lacks intelligent path selection. RA sent by MR are equivalent to RA sent by a fixed Access Router. Selecting an Attachment Router without any knowledge on path metrics would select non-optimal paths. Nested NEMO has high tunnel header overhead and a pinball route problem. Also route loops can occur (NEMO RO) [10].

5.5. Interface type

In the MANET architecture, a MANET-Interface is an interface with a MANET protocol enabled. Typical behavior is the relay function, incoming traffic on this interface can be relayed to serve other nodes increasing connectivity in the MANET topology [30].

In Mobility Related Terminology [7], The Ingress and Egress Interface types are introduced. Terms are related to the NEMO mobile Router model [9]. The Ingress Interface is the interface with the Mobile Network Nodes connected to. The Egress Interface is the interface the Mobile Router uses to attach to the fixed infrastructure.

When discussions started about integrating MANET and NEMO, the difference between the MANET and Egress interface faded. Also a discussion about the need for a MANEMO Ingress Interfaces started, as
in MANET there is no need for special handling, and in MANEMO any router interface could be MANET enabled. For policy reasons, a MANEMO router interface could be defined as Ingress only.

5.6. Multicast support

In MANET environment, classical multicast forwarding using a Reverse Path Forwarding Check cannot be used. The MANET interface is used for relaying IP packets, and a basic forwarding rule is broken, specifying that an IP multicast packet is never sent back over the incoming interface.

Multiple MANET multicast protocols are proposed, but many of them showed large overhead for keeping state information. Currently the MANET workgroup is working on SMF [5]. SMF use 2-hop neighbor state provided by another protocol (currently NHDP [31]) for efficient flooding combined with duplicate packet detection.

In NEMO, multicast service can be provided. Within the Mobile Network itself, basic multicasting is used. Global multicast supported can also be provided; the MR relays the multicast to the HA, where the multicast flow is injected in the fixed infrastructure. Receiving multicast from the fixed infrastructure is also supported, the HA relays the multicast flow via the tunnel to the MR and the FLNs.

Multicasting between nearby NEMO MRs would have large overhead, as the multicast is lead over the HAs. Also multicast from the fixed infrastructure to multiple nearby NEMO MRs is inefficient, as the multicast flow is pseudo-broadcasted over multiple tunnels to these MRs. Options for improved NEMO multicast support are proposed, e.g. using MLD-proxy [32].
6. Problems found in MANET and NEMO

This section is used as placeholder for problems in MANET or NEMO, which are not maintained in separate IETF Problem Statement documents.

6.1. Worst Path First Syndrome

Classic routing protocols use the hop-count as metric for best path selecting. Hop-count is still used in modern MANET routing protocols. For homogeneous topologies, where all links have similar capabilities, this could be seen as sufficient. But when different link types are used or link characteristics vary in time and on a neighbor by neighbor basis, problems are introduced. Using cross-layer information is seen as helpful for MANET environments[2].

NEMO / nested NEMO do currently not select a path based on metrics.

The Worst Path First Syndrome is a name given to a behavior of a path selection algorithm, selecting the path to a destination using the fewest hops, but also the worst quality links. Using ad-hoc networks with broadcast radios, link quality and data rate would be a function of distance and influenced by obstacles. In the example below, a high quality radio link uses a data rate of 11Mbps and has a packet loss below 1%. A bad quality radio link uses a data rate of 1Mbps and has a packet loss around 50%.

```
+----+  |
| R1 |  |
+----+  |
     | 11Mbps / |
     |      /   |
     | <1% /    |
     +-----+  |
     |      loss / |
     |      /    |
     | <1% /     |
     +-----+  |
     |      1Mbps |
     |      /     |
     |      loss ~50% |
     +-----+  |
     |      | |
     |      |  |
     |      | R2  |
     +-----+  |
     |      11Mbps \ |
     |      loss \  |
     |      \    |
     |      <1% \ |
     +-----+  |
     |      | |
     |      |  |
     |      | R3  |
     +-----+  |

Figure 12: Worst Path First Syndrome Network Topology
```

R3 can select R1 or R2 as attachment router, router advertisements.
from both R1 and R2 are received. A MANET protocol, selecting a path based on hop-count, selects the direct path to R1. NEMO would select R1 or R2, as it has no knowledge of the topology.

Selecting the direct path to R1 is the worst in terms of bandwidth (1Mbps where 11Mbps is available), packet loss (50% where less than 2% is available) and used spectrum (single transmission over 1Mbps takes more time for sending a packet than 2 times over 11Mbps). The direct path to R1 would require more retransmissions if reliable data transfer is supported.

In a heterogeneous topology, the problem becomes totally unacceptable. Imagine that the three Rs are temporally "on the pause" and R2 and R3 are near to each other. Because R3 has bad user experience, it can be serviced by using cabling to R2 and the bandwidth is increased to 100Mbps and the packet loss is zero. Still, user experience is not enhanced at all, and R1 would be selected.

Defining solutions for this problem is out of scope of this document. A suggested approach is using path metrics based on cross layer metrics.

6.2. Break Before Make problem

The Break Before Make (BBM) [7], problem occurs when links suddenly fail and there is no pre-warning mechanism. Classic routing protocols suffer from BBM, as problems in fixed infrastructures are mostly caused by equipment failures and these problems are hard to predict. Modern protocols have support for L2-triggers, speeding up connection repair time.

Graceful shutdown is a mechanism that is for predicted outages. Before the outage, neighbors are signaled the node or link is taken out of service and an alternative path is selected, if available. In a wireless infrastructure, especially when elements are moving, link quality is varying and getting out-of-reach can be detected by layer-2 mechanisms or by detecting packet loss, e.g. provided by a hello protocol. The decreased link quality can be signaled to the neighbors, and alternative paths can be selected before the link breaks. Such concepts are called Make Before Break (MBB) [7].

When hop count metrics are used, varying link quality is not taken into account and links are used until the become really out of reach. This is similar to the WPF syndrome described above.

Defining solutions for this problem is out of scope of this document. A suggested approach is using path metrics based on cross layer link
6.3. Routing loops in proactive routing protocols

Loops in classical unicast routing could take place when an interface state changes. When an interface goes down, the routing table is adjusted quickly for removing entries with a next hop via this interface. Alternative routes could be used quickly also. Other router routing tables are updated after routing protocol activity; this could take milliseconds up to minutes, depending on protocol and timer settings. During this convergence, routing loops can occur and packet starvation is handled by TTL mechanism.

On wireless media, using TTL for starvation could have a high impact on radio resources and spectrum utilization.

In the following scenario, a hop-count based metric is used. Routers are located around an obstacle and a ring topology is formed due to radio propagation. In the scenario, R5 is moving away from R4.

```
+----+        +----+        +----+
| R1 |--------| R2 |--------| R3 |
+----+        +----+        +----+
    |                          |
    |    +=+= obstacle +=+=    |
+----+        +----+        +----+
| R4 |----------------------| R5 |  R5 moves this way --->
+----+        +----+        +----+
```

Figure 13: MANET routing loop scenario

When R5 is moved, the neighbor state for R4 and R5 goes down.

```
+----+        +----+        +----+
| R1 |--------| R2 |--------| R3 |
+----+        +----+        +----+
    |                          |
    |    +=+= obstacle +=+=    \
+----+        +----+        +----+
    |                          |
    |                          \
+----+                      +----+
| R4 |                      | R5 |  R5 moves this way --->
+----+                      +----+
```

Figure 13: MANET routing loop scenario (continued)
R4 and R5 detect the change due to the hello mechanism or L2 triggers. After R4 is aware of the failure, it immediately adjusts its routing table. It uses R1 as next hop for traffic to R5. However, R1 is still not aware of the topology change and still uses R4 as next hop for traffic towards R5. Now the routing loop occurs:

```
+-----+        +-----+        +-----+
| R1  |--------| R2 |--------| R3 |
+-----+        +-----+        +-----+
 ^         |
| v         
```

Loop: | | ++== obstacle ++== 
| | 

```
| R4 |   | R5 | R5 moved
+-----+   +-----+
```

**Figure 14: Neighbor down detected**

The loop is solved as soon as R1 is aware of the new topology. Time for convergence is caused by routing protocol packet transfer, timers and processing time. Protocol timers that slow down packet transfer or introduce jitter in SPF calculation increase convergence time and thus loop duration. So jitter introduced by [draft-clausen-manet-jitter](#) emphasizes the routing loop problem.

Defining solutions for this problem is out of scope of this document. A suggested approach is using:

- a) path metrics based on cross layer metrics;
- b) implementing a reverse path check on the previous forwarder address, when this address is available and
- c) implementing a duplicate packet detection mechanism.

### 6.4. Congested link avoidance

In MANET environment, the shortest path mechanism can select a link connecting two MANET islands for relaying all traffic flows between these islands. This is also the case when many exit routers to a high speed backbone are available.
In (Nested) NEMO, low bandwidth paths to scarce exit routers can become congested, also caused by local traffic. Unoptimized tree topologies can also introduce congestion.
In wireless infrastructures, using bandwidth efficiently is a primary concern. Advanced QoS mechanisms are needed, utilizing radio interface characteristics. Call admission control mechanisms like RSVP should be considered, especially for real-time traffic.

Attention is required for bridging layer-2 devices, where the router and the layer-2 device are linked with a high speed interface. Flow control and layer-2 metric transfer between router and the layer-2 device as described in "PPP Over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics" [33] can solve introduced problems.

Also attention is required for an ad-hoc dense crowd of nodes requiring lots of bandwidth. In such a scenario, available transmission means will be overloaded.

6.5. MANET and NEMO at home problem

In MIP, a Mobile Node is at home when it is connected to the Home Link. For wireless nodes in the home region, a MANET protocol could be used for extending the home link, using the HA as exit router.
This introduces a problem, the node could be classified as "at home" because it can reach any CN using the MANET and its own HA as exit router, but it is also "far from home" because it is not on the home link, in the meaning that it does not receive HA RA with the Home Agent Information Option.

MR1 receives the HA RA with HAIO, thus MR1 is at home. MR2 is not receiving the HAIO and is thus far from home. But MR2 is able to communicate with the fixed infrastructure using MANET routing and the HA acting as MANET Border Router.

Another problem is introduced when the MANET protocol is used on the NEMO tunnel. This introduces a routing shortcut, the native MANET route is in parallel with the MANET route via the NEMO tunnel. The next hop to the HA and thus to the NEMO tunnel endpoint could be learned through the tunnel, this introduces tunnel interface instability.
The impact of the MANET and NEMO at home routing shortcut problem is to be analyzed. Problem areas are tunnel instability and multicast packets sent to HA via MANET and the tunnel.

6.6. MANET scale to infinity problem when peering to strangers

In a dense deployment of MANET routers, all configured for roaming in a large area and peering to all other routers, the MANET will melt down due to flooding topology information from any to all. A sample scenario is car to car communication in a metropolis with say a million cars. Current IETF MANET protocols provide a flat routing domain, where reachability is provided between ALL MANET routers.

In a chain of MANET routers, where each router has two neighbors (or one neighbor on the end routers), there is no problem with neighbor discovery or 2-hop neighbor state maintenance. But prefix flooding (proactive routing) or route requests (reactive routing) are flooded over all routers in the MANET.

This problem occurs independent of the existence of a fixed backbone infrastructure.
Some would suggest MANETs can be designed for using hierarchy. Current IETF MANET protocols do not support such. Others would suggest automatic hierarchy can be added in future extensions on the basic protocol. There is no evidence that options for such are realistic.
7. IANA considerations

This document does not require any IANA action.

8. Security Considerations

This document does not create any security threat. It discusses and analyses the concepts of MANET and NEMO.

9. Acknowledgments

I would like to thank all the people involved in MANET and NEMO technology. I would particularly like to thank (in alphabetical order) people involved in MANEMO: Jari Arkko, Thomas Clausen, Ian Chakeres, Ben McCarthy, Alexandru Petrescu, Pascal Thubert, Ryuji Wakikawa and all that I forgot.

10. References

10.1. Normative reference

10.2. Informative Reference


draft-wakikawa-manemo-problem-statement-00 (work in progress), February 2007.


Appendix A. Change Log

A.1. Changes from version 00 to 01

- Added MANET and Fringe Stub models sections.
- Added Routing Loop problem in proactive protocols.
- Added Break Before Make problem.
- Added Congested Link problem.
- Added MANET and NEMO at home problem.
- Added MANET scale to infinity problem when peering to strangers.

Author’s Address

Teco Boot
Infinity Networks B.V.
Elperstraat 4
Schoonloo 9443TL
Netherlands

Email: teco@inf-net.nl
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).