Network Working Group
Request for Comments: 3154
Category: Informational

J. Kempf
C. Castelluccia
P. Mutaf
N. Nakajima
Y. Ohba
R. Ramjee
Y. Saifullah
B. Sarikaya
X. Xu

August 2001

Requirements and Functional Architecture for an IP Host Alerting Protocol

Status of this Memo

Copyright Notice

Abstract

This document develops an architecture and a set of requirements needed to support alerting of hosts that are in dormant mode. The architecture and requirements are designed to guide development of an IP protocol for alerting dormant IP mobile hosts, commonly called paging.

Table of Contents

1. Introduction

In [1], a problem statement was developed to explain why an IP protocol was desirable for alerting hosts in dormant mode, commonly called paging. In this document, a set of requirements is developed for guiding the development of an IP paging protocol. Based on the requirements, an architecture is developed to represent the functional relationships between logical functional entities involved.

2. Terminology

Please see [1] for definition of terms used in describing paging. In addition, this document defines the following terms:

Wide Casting - Either broadcasting or multicasting.

Inactive Mode - The host is no longer listening for any packets, not even periodically, and not sending packets. The host may be in a powered off state, it may have shut down all interfaces to drastically conserve power, or it may be out of range of a radio access point.

3. Security Considerations

An IP paging protocol introduces new security issues. In this section, security issues with relevance to formulating requirements for an IP paging protocol are discussed.

3.1. DoS Amplification

A DoS (Denial-of-Service) or DDoS (Distributed DoS) attack generally consists of flooding a target network with bogus IP packets in order to cause degraded network performance at victim nodes and/or routers. Performance can be degraded to the point that the network cannot be used. Currently, there is no preventive solution against these attacks, and the impacts can be very important.

In general a DoS attacker profits from a so-called "amplifier" in order to increase the damage caused by his attack. Paging can serve for an attacker as a DoS amplifier.

An attacker (a malicious correspondent node) can send large numbers of packets pretending to be sent from different (bogus) correspondent nodes and destined for large numbers of hosts in inactive and dormant modes. This attack, in turn, will be amplified by the paging agent which wide casts paging messages over a paging area, resulting in more than one networks being flooded. Clearly, the damage can be

more important in wireless networks that already suffer from scarce radio bandwidth.

Alternatively, an attacker can sort out a host which:

1. sends periodic messages declaring that it is in dormant mode,

2. never replies to paging requests.

Such a node may be the attacker's node itself, or a second node participating in the attack.

That node is never in inactive mode because of behavior 1 above. In this case, the attacker can send large numbers of packets destined for that host which periodically declares that it is in dormant mode but never replies to paging messages. The impact will be the same as above however in this case the attack will be amplified indefinitely.

3.2. Queue Overflow

For reliability reasons, the paging protocol may need to make provisions for a paging queue where a paging request is buffered until the requested host replies by sending a location registration message.

An attacker can exploit that by sending large numbers of packets having different (bogus) correspondent node addresses and destined for one or more inactive hosts. These packets will be buffered in the paging queue. However, since the hosts are inactive, the paging queue may quickly overflow, blocking the incoming traffic from legitimate correspondent nodes. As a result, all registered dormant hosts may be inaccessible for a while. The attacker can re-launch the attack in a continuous fashion.

An attacker together with a bogus host that fails to respond to pages can overflow the buffering provided to hold packets for dormant mode hosts. If the attacker keeps sending packets while the dormant mode host fails to reply, the buffer can overflow.

3.3. Selective DoS against Hosts

The following vulnerabilities already exist in the absence of IP paging. However, they are included here since they can affect the correct operation of the IP paging protocol.

These vulnerabilities can be exploited by an attacker in order to eliminate a particular host. This, in turn, can be used by an attacker as a stepping stone to launch other attacks.

Forced Battery Consumption

An attacker can frequently send packets to a host in order to prevent that host from switching to dormant mode. As a result the host may quickly run out of battery.

Bogus Paging Areas

An attacker can periodically emit malicious packets in order to confuse one or more hosts about their actual locations. Currently, there is no efficient way to authenticate such packets.

In the case of IP paging, these packets may also contain bogus paging area information. Upon receipt of such a packet, a host may move and send a location registration message pointing to a non-existing or wrong paging area. The functional entities of the IP paging protocol may loose contact with the host.

More importantly, this attack can serve for sorting out a host which shows the behaviors 1 and 2 described in Section 3.1.

Bogus Paging Agents

An attacker can wide cast fake paging messages pretending to be sent by a paging agent. The impacts will be similar to the ones described in Sections 4.1 and 4.3.1. However, depending on how the IP paging protocol is designed, additional harm may be caused.

4. Requirements

The following requirements are identified for the IP paging protocol.

4.1. Impact on Power Consumption

The IP paging protocol MUST minimize impact on the Host’s dormant mode operation, in order to minimize excessive power drain.

4.2. Scalability

The IP paging protocol MUST be scalable to millions of Hosts.

4.3. Control of Broadcast/Multicast/Anycast

The protocol SHOULD provide a filter mechanism to allow a Host prior to entering dormant mode to filter which broadcast/multicast/anycast packets active a page. This prevents the Host from awakening out of dormant mode for all broadcast/multicast/anycast traffic.

4.4. Efficient Signaling for Inactive Mode

The IP paging protocol SHOULD provide a mechanism for the Tracking Agent to determine whether the Host is in inactive mode, to avoid paging when a host is completely unreachable.

4.5. No Routers

Since the basic issues involved in handling mobile routers are not well understood and since mobile routers have not exhibited a requirement for paging, the IP paging protocol MAY NOT support routers. However, the IP paging protocol MAY support a router acting as a Host.

4.6. Multiple Dormant Modes

Recognizing that there are multiple possible dormant modes on the Host, the IP paging protocol MUST work with different implementations of dormant mode on the Host.

4.7. Independence of Mobility Protocol

Recognizing that IETF may support multiple mobility protocols in the future and that paging may be of value to hosts that do not support a mobility protocol, the IP paging protocol MUST be designed so there is no dependence on the underlying mobility protocol or on any mobility protocol at all. The protocol SHOULD specify and provide support for a mobility protocol, if the Host supports one.

4.8. Support for Existing Mobility Protocols

The IP paging protocol MUST specify the binding to the existing IP mobility protocols, namely mobile IPv4 [2] and mobile IPv6 [3]. The IP paging protocol SHOULD make use of existing registration support.

4.9. Dormant Mode Termination

Upon receipt of a page (either with or without an accompanying L3 packet), the Host MUST execute the steps in its mobility protocol to re-establish a routable L3 link with the Internet.

4.10. Network Updates

Recognizing that locating a dormant mode mobile requires the network to have a rough idea of where the Host is located, the IP paging protocol SHOULD provide the network a way for the Paging Agent to inform a dormant mode Host what paging area it is in and the IP paging protocol SHOULD provide a means whereby the Host can inform

the Target Agent when it changes paging area. The IP paging protocol MAY additionally provide a way for the Host to inform the Tracking Agent what paging area it is in at some indeterminate point prior to entering dormant mode.

4.11. Efficient Utilization of L2

Recognizing that many existing wireless link protocols support paging at L2 and that these protocols are often intimately tied into the Host's dormant mode support, the IP paging protocol SHOULD provide support to efficiently utilize an L2 paging protocol if available.

4.12. Orthogonality of Paging Area and Subnets

The IP paging protocol MUST allow an arbitrary mapping between subnets and paging areas.

4.13. Future L3 Paging Support

Recognizing that future dormant mode and wireless link protocols may be designed that more efficiently utilize IP, the IP paging protocol SHOULD NOT require L2 support for paging.

4.14. Robustness Against Failure of Network Elements

The IP paging protocol MUST be designed to be robust with respect to failure of network elements involved in the protocol. The self-healing characteristics SHOULD NOT be any worse than existing routing protocols.

4.15. Reliability of Packet Delivery

The IP paging protocol MUST be designed so that packet delivery is reliable to a high degree of probability. This does not necessarily mean that a reliable transport protocol is required.

4.16. Robustness Against Message Loss

The IP paging protocol MUST be designed to be robust with respect to loss of messages.

4.17. Flexibility of Administration

The IP paging protocol SHOULD provide a way to flexibly auto-configure Paging Agents to reduce the amount of administration necessary in maintaining a wireless network with paging.

4.18. Flexibility of Paging Area Design

The IP paging protocol MUST be flexible in the support of different types of paging areas. Examples are fixed paging areas, where a fixed set of bases stations belong to the paging area for all Hosts, and customized paging areas, where the set of base stations is customized for each Host.

4.19. Availability of Security Support

The IP paging protocol MUST have available authentication and encryption functionality at least equivalent to that provided by IPSEC [5].

4.20. Authentication of Paging Location Registration

The IP paging protocol MUST provide mutually authenticated paging location registration to insulate against replay attacks and to avoid the danger of malicious nodes registering for paging.

4.21. Authentication of Paging Area Information

The IP paging protocol MUST provide a mechanism for authenticating paging area information distributed by the Paging Agent.

4.22. Authentication of Paging Messages

The IP paging protocol MUST provide a mechanism for authenticating L3 paging messages sent by the Paging Agent to dormant mode Hosts. The protocol MUST support the use of L2 security mechanisms so implementations that take advantage of L2 paging can also be secured.

4.23. Paging Volume

The IP paging protocol SHOULD be able to handle large numbers of paging requests without denying access to any legitimate Host nor degrading its performance.

4.24. Parsimonious Security Messaging

The security of the IP paging protocol SHOULD NOT call for additional power consumption while the Host is in dormant mode, nor require excessive message exchanges.

4.25. Noninterference with Host’s Security Policy

The IP paging protocol MUST NOT impose any limitations on a Host’s security policies.

4.26. Noninterference with End-to-end Security

The IP paging protocol MUST NOT impose any limitations on a Host's ability to conduct end-to-end security.

4.27. Detection of Bogus Correspondent Nodes

The IP paging protocol SHOULD make provisions for detecting and ignoring bogus correspondent nodes prior to paging messages being wide cast on behalf of the correspondent node.

5. Functional Architecture

In this section, a functional architecture is developed that describes the logical functional entities involved in IP paging and the interfaces between them. Please note that the logical architecture makes absolutely no commitment to any physical implementation of these functional entities whatsoever. A physical implementation may merge particular functional entities. For example, the Paging Agent, Tracking Agent, and Dormant Monitoring Agent may all be merged into one in a particular physical implementation. The purpose of the functional architecture is to identify the relevant system interfaces upon which protocol development may be required, but not to mandate that protocol development will be required on all.

5.1. Functional Entities

The functional architecture contains the following elements:

Host - The Host (H) is a standard IP host in the sense of [4]. The Host may be connected to a wired IP backbone through a wireless link over which IP datagrams are exchanged (mobile usage pattern), or it may be connected directly to a wired IP network, either intermittently (nomadic usage pattern) or constantly (wired usage pattern). The Host may support some type of IP mobility protocol (for example, mobile IP [2] [3]). The Host is capable of entering dormant mode in order to save power (see [1] for a detailed discussion of dormant mode). The Host also supports a protocol allowing the network to awaken it from dormant mode if a packet arrives. This protocol may be a specialized L2 paging channel or it may be a time-slotted dormant mode in which the Host periodically wakes up and listens to L2 for IP traffic, the details of the L2 implementation are not important. A dormant Host is also responsible for determining when its paging area has changed and for responding to changes in paging area by directly

or indirectly informing the Tracking Agent about its location. Since routers are presumed not to require dormant mode support, a Host is never a router.

Paging Agent - The Paging Agent is responsible for alerting the Host when a packet arrives and the Host is in dormant mode. Alerting of the Host proceeds through a protocol that is peculiar to the L2 link and to the Host's dormant mode implementation, though it may involve IP if supported by the L2. Additionally, the Paging Agent maintains paging areas by periodically wide casting information over the Host's link to identify the paging area. The paging area information may be wide cast at L2 or it may also involve IP. Each paging area is served by a unique Paging Agent.

Tracking Agent - The Tracking Agent is responsible for tracking a Host's location while it is in dormant mode or active mode, and for determining when Host enters inactive mode. It receives updates from a dormant Host when the Host changes paging area. When a packet arrives for the Host at the Dormant Monitoring Agent, the Tracking Agent is responsible for notifying the Dormant Monitoring Agent, upon request, what Paging Agent is in the Host's last reported paging area. There is a one to one mapping between a Host and a Tracking Agent.

Dormant Monitoring Agent - The Dormant Monitoring Agent detects the delivery of packets to a Host that is in Dormant Mode (and thus does not have an active L2 connection to the Internet). It is the responsibility of the Dormant Monitoring Agent to query the Tracking Agent for the last known Paging Agent for the Host, and inform the Paging Agent to page the Host. Once the Paging Agent has reported that a routable connection to the Internet exists to the Host, the Dormant Monitoring Agent arranges for delivery of the packet to the Host. In addition, the Host or its Tracking Agent may select a Dormant Monitoring Agent for a Host when the Host enters dormant mode, and periodically as the Host changes paging area.

5.2. Interfaces

The functional architecture generates the following list of interfaces. Note that the interfaces between functional entities that are combined into a single network element will require no protocol development.

Host - Paging Agent (H-PA) - The H-PA interface supports the following types of traffic:

- Wide casting of paging area information from the Paging Agent.

- The Paging Agent alerting the Host when informed by the Dormant Monitoring Agent that a packet has arrived.

Host - Tracking Agent (H-TA) - The H-TA interface supports the following types of traffic:

- The Host informing the Tracking Agent when it has changed paging area, and, optionally, prior to entering dormant mode, in what paging area it is located.

- Optionally, the Host informs the Tracking Agent at a planned transition to inactive mode.

Dormant Monitoring Agent - Tracking Agent (DMA-TA) - The DMA-TA interface supports the following types of traffic:

- A report from the Dormant Monitoring Agent to the Tracking Agent that a packet has arrived for a dormant Host for which no route is available.

- A report from the Tracking Agent to the Dormant Monitoring Agent giving the Paging Agent to contact in order to page the Host.

- A report from the Tracking Agent to the Dormant Monitoring Agent that a Host has entered inactive mode, if not provided directly by the Host

- A report from the Tracking Agent to the Dormant Monitoring Agent that a Host has entered dormant mode, if not provided directly by the Host.

Dormant Monitoring Agent - Paging Agent (DMA-PA) - The DMA-PA interface supports the following types of traffic:

- A request from the Dormant Monitoring Agent to the Paging Agent to page a particular Host in dormant mode because a packet has arrived for the Host.

- Negative response indication from the Paging Agent if the Host does not respond to a page.

- Positive response from the Paging Agent indication if the Host does respond to a page.

- Delivery of the packet to the Host.

Host - Dormant Monitoring Agent (H-DMA) - The H-DMA interface supports the following types of traffic:

- The Host registers to the Dormant Monitoring Agent prior to entering dormant mode, (if needed) with filtering information on which broadcast/multicast/anycast packets trigger a page.

- The Host informs the Dormant Monitoring Agent, when it directly deregisters from the Dormant Monitoring Agent due to a change from dormant mode to active or inactive mode.

5.3. Functional Architecture Diagram

The functional architecture and interfaces lead to the following diagram.

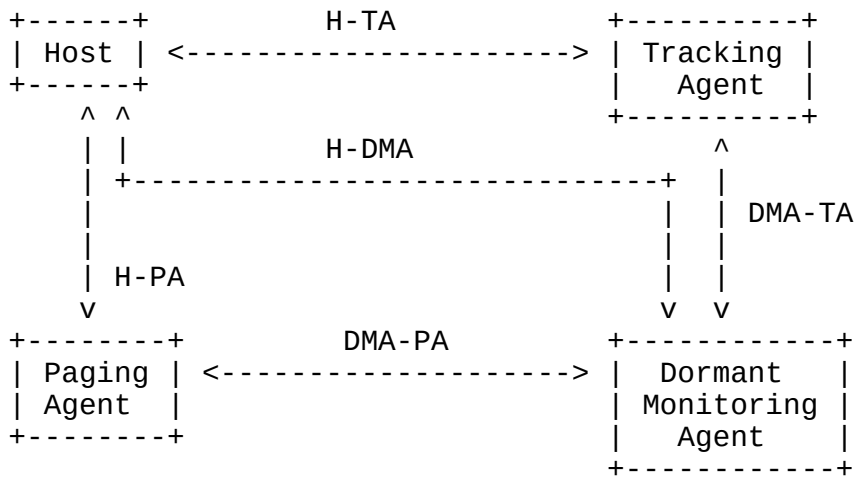

Figure 1 - Paging Functional Architecture

6. Acknowledgements

The authors would like to thank Arthur Ross for helpful comments on this memo.

7. References

[1] Kempf, J., "Dormant Mode Host Alerting ("IP Paging") Problem Statement", RFC 3132, June 2001.

[2] Perkins, C., ed., "IP Mobility Support", RFC 2002, October, 1996.

[3] Johnson, D., and Perkins, C., "Mobility Support in Ipv6", Work in Progress.

[4] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[5] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

8. Authors' Addresses

James Kempf
Sun Microsystems Laboratories
901 San Antonio Rd.
UMTV29-235
Palo Alto, CA
95303-4900
USA

Phone: +1 650 336 1684
Fax: +1 650 691 0893
EMail: James.Kempf@Sun.COM

Pars Mutaf
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
FRANCE

Phone:
Fax: +33 4 76 61 52 52
EMail: pars.mutaf@inria.fr

Claude Castelluccia
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
FRANCE

Phone: +33 4 76 61 52 15
Fax: +33 4 76 61 52 52
EMail: claude.castelluccia@inria.fr

Nobuyasu Nakajima
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ
07961-0136
USA

Phone: +1 973 829 4752
EMail: nnakajima@tari.toshiba.com

Yoshihiro Ohba
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ
07961-0136
USA

Phone: +1 973 829 5174
Fax: +1 973 829 5601
EMail: yohba@tari.toshiba.com

Ramachandran Ramjee
Bell Labs, Lucent Technologies
Room 4g-526
101 Crawfords Corner Road
Holmdel, NJ
07733
USA

Phone: +1 732 949 3306
Fax: +1 732 949 4513
EMail: ramjee@bell-labs.com

Yousuf Saifullah
Nokia Research Center
6000 Connection Dr.
Irving, TX
75039
USA

Phone: +1 972 894 6966
Fax: +1 972 894 4589
EMail: Yousuf.Saifullah@nokia.com

Behcet Sarikaya
Alcatel USA, M/S CT02
1201 Campbell Rd.
Richardson, TX
75081-1936
USA

Phone: +1 972 996 5075
Fax: +1 972 996 5174
EMail: Behcet.Sarikaya@usa.alcatel.com

Xiaofeng Xu
Alcatel USA, M/S CT02
1201 Campbell Rd.
Richardson, TX
75081-1936
USA

Phone: +1 972 996 2047
Fax: +1 972 996 5174
Email: xiaofeng.xu@usa.alcatel.com

9. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.