Network Working Group
Request for Comments: 2779
Category: Informational

M. Day
Lotus
S. Aggarwal
Microsoft
G. Mohr
Activerse
J. Vincent
Into Networks
February 2000

Instant Messaging / Presence Protocol Requirements

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

Presence and Instant Messaging have recently emerged as a new medium of communications over the Internet. Presence is a means for finding, retrieving, and subscribing to changes in the presence information (e.g. "online" or "offline") of other users. Instant messaging is a means for sending small, simple messages that are delivered immediately to online users.

Applications of presence and instant messaging currently use independent, non-standard and non-interoperable protocols developed by various vendors. The goal of the Instant Messaging and Presence Protocol (IMPP) Working Group is to define a standard protocol so that independently developed applications of instant messaging and/or presence can interoperate across the Internet. This document defines a minimal set of requirements that IMPP must meet.

Table of Contents

1. Terminology

The following terms are defined in [RFC 2778] and are used with those definitions in this document:

ACCESS RULES
CLOSED
FETCHER
INSTANT INBOX
INSTANT MESSAGE
NOTIFICATION
OPEN
POLLER
PRESENCE INFORMATION
PRESENCE SERVICE
PRESENTITY
PRINCIPAL
PROXY
SERVER
STATUS
SUBSCRIBER
SUBSCRIPTION
WATCHER

The terms MUST and SHOULD are used in the following sense while specifying requirements:

MUST: A proposed solution will have to meet this requirement.
SHOULD: A proposed solution may choose not to meet this requirement.

Note that this usage of MUST and SHOULD differs from that of RFC 2119.

Additionally, the following terms are used in this document and defined here:

ADMINISTRATOR: A PRINCIPAL with authority over local computer and network resources, who manages local DOMAINS or FIREWALLS. For security and other purposes, an ADMINISTRATOR often needs or wants to impose restrictions on network usage based on traffic type, content, volume, or endpoints. A PRINCIPAL's ADMINISTRATOR has authority over some or all of that PRINCIPAL's computer and network resources.

DOMAIN: A portion of a NAMESPACE.

ENTITY: Any of PRESENTITY, SUBSCRIBER, FETCHER, POLLER, or WATCHER (all defined in [RFC 2778]).

FIREWALL: A point of administrative control over connectivity. Depending on the policies being enforced, parties may need to take unusual measures to establish communications through the FIREWALL.

IDENTIFIER: A means of indicating a point of contact, intended for public use such as on a business card. Telephone numbers, email addresses, and typical home page URLs are all examples of IDENTIFIERS in other systems. Numeric IP addresses like 10.0.0.26 are not, and neither are URLs containing numerous CGI parameters or long arbitrary identifiers.

INTENDED RECIPIENT: The PRINCIPAL to whom the sender of an INSTANT MESSAGE is sending it.

NAMESPACE: The system that maps from a name of an ENTITY to the concrete implementation of that ENTITY. A NAMESPACE may be composed of a number of distinct DOMAINS.

OUT OF CONTACT: A situation in which some ENTITY and the PRESENCE SERVICE cannot communicate.

SUCCESSFUL DELIVERY: A situation in which an INSTANT MESSAGE was transmitted to an INSTANT INBOX for the INTENDED RECIPIENT, and the INSTANT INBOX acknowledged its receipt. SUCCESSFUL DELIVERY usually also implies that an INBOX USER AGENT has handled the message in a way chosen by the PRINCIPAL. However, SUCCESSFUL DELIVERY does not imply that the message was actually seen by that PRINCIPAL.

2. Shared Requirements

This section describes non-security requirements that are common to both an PRESENCE SERVICE and an INSTANT MESSAGE SERVICE. Section 6 describes requirements specific to a PRESENCE SERVICE, while Section 7 describes requirements specific to an INSTANT MESSAGE SERVICE. Section 8 describes security considerations. The reader should note that Section 11 is an appendix that provides historical context and aids in tracing the origins of requirements in Section 8. Section 11 is not, however, a statement of current IMPP requirements.

It is expected that Presence and Instant Messaging services will be particularly valuable to users over mobile IP wireless access devices. Indeed the number of devices connected to the Internet via wireless means is expected to grow substantially in the coming years. It is not reasonable to assume that separate protocols will be available for the wireless portions of the Internet. In addition, we note that wireless infrastructure is maturing rapidly; the work undertaken by this group should take into account the expected state of the maturity of the technology in the time-frame in which the

Presence and Instant Messaging protocols are expected to be deployed.

To this end, the protocols designed by this Working Group must be suitable for operation in a context typically associated with mobile wireless access devices, viz. high latency, low bandwidth and possibly intermittent connectivity (which lead to a desire to minimize round-trip delays), modest computing power, battery constraints, small displays, etc. In particular, the protocols must be designed to be reasonably efficient for small payloads.

2.1. Namespace and Administration

2.1.1. The protocols MUST allow a PRESENCE SERVICE to be available independent of whether an INSTANT MESSAGE SERVICE is available, and vice-versa.

2.1.2. The protocols must not assume that an INSTANT INBOX is necessarily reached by the same IDENTIFIER as that of a PRESENTITY. Specifically, the protocols must assume that some INSTANT INBOXes may have no associated PRESENTITIES, and vice versa.

2.1.3. The protocols MUST also allow an INSTANT INBOX to be reached via the same IDENTIFIER as the IDENTIFIER of some PRESENTITY.

2.1.4. The administration and naming of ENTITIES within a given DOMAIN MUST be able to operate independently of actions in any other DOMAIN.

2.1.5. The protocol MUST allow for an arbitrary number of DOMAINS within the NAMESPACE.

2.2. Scalability

2.2.1. It MUST be possible for ENTITIES in one DOMAIN to interoperate with ENTITIES in another DOMAIN, without the DOMAINS having previously been aware of each other.

The protocol MUST be capable of meeting its other functional and performance requirements even when

-- (2.2.2) there are millions of ENTITIES within a single DOMAIN.

-- (2.2.3) there are millions of DOMAINS within the single NAMESPACE.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.