IPv6 Appli-Contest 2003 Idea Award Submission:

Individual Internet Protocol Addressing Service

by

The Saudi Networking Research Group

Members:

Bander Ajba
Abdulaziz Al-Ghunaim
Majid Al-Gwaiz
Hytham Al-Saati
Raji Al-Tabshi
Yaser Al-Yami
Nidhal Jamal
Faisal Saddique

Submission Date: April 10, 2003

Abstract:

The Individual Internet Protocol Addressing Service consists of a reserved IPv6 address space, servers, data, communication protocols, and an IPv6 protocol extension. These reserved addresses are each assigned to one individual permanently. Any application may then communicate with this user using this reserved address, which is actually a virtual address. The application resolves the virtual address to a physical address by accessing the servers, via the designed protocol, whose job it is to map every user's virtual IP address to the physical IP address of the machine that user is currently at. The servers must also update these maps dynamically as the user moves from one device to another. Hence, any application can communicate with the desired user, regardless of the machine he/she is currently using.

Introduction:

Communication across networks is always done from networking device to networking device. That is, the goal is (almost) always to reach a specific computer and hope that the individual you want to contact is at that computer. However, there are more personal methods of communication in use, such as email and instant messaging. These allow a message to be delivered to a particular recipient regardless of his/her physical location. In the case of email, the user checks his/her account from any device and can view the message from the mail server. In essence the message is still sent to the server and not the user. Instant messaging is different in that the message is sent to the user and is then routed to the appropriate device in order to reach the specified user. This allows for person-to-person communication rather than device-to-device communication. The message is still routed based on device addresses, but the selection of the device address is dependent on the user's physical location, not the other way around. Messaging services are varied but are subject to protocol and application limitations imposed by the messaging software programmer. It is also limited to person-to-person communication. For example, a web server does not attempt to contact the user that made the request for the web page, but the machine from which the request was made. If the user gets up and walks away from the computer, the web server couldn't care less.

The purpose of this paper is to propose a service that will allow for person-to-person and service-to-person communication. This will allow for information to be routed to an individual directly, regardless of the physical device that the individual is currently located at, and regardless of the mobility of the user. We have dubbed this service Individual Internet Protocol Addressing (IIP) Service.

Individual Internet Protocol Addressing (IIP) Service Overview:

This service consists of an IPv6 addressing range allocation, an IPv6 protocol extension, data, servers, and a custom protocol.

First of all a range of IPv6 addresses must be allocated as *Individual Internet Protocol Addresses* (IIP Addresses). Once this is done, an individual registers to receive an IIP address. The IIP address is registered to this individual and remains assigned to him/her permanently.

The *IIP Server* holds the IIP address of the individual, which is a virtual address, and the physical IP Address of the device the user is connecting from. There will be several classes of IIP Servers, as there are DNS Servers. Ideally, each ISP will be responsible for providing IIP Servers to their subscribers.

The *IIP Protocol* is used by the IIP client to communicate with the IIP server. The IIP client resides on every internet-connected device and serves two purposes. The first is that it allows the user to send a message to the server binding his IIP Address to his current physical IP Address. The second is that it allows a device that wants to send a packet to the specific individual to lookup his/her current physical IP Address from the server. The clients are also allowed to send messages to each other. In this case, a client can play the role of the server, but is not authorized to generate ALL control messages.

The IPv6 protocol extension is used to inform the user's device that the messages are being sent via the IIP address instead of the IP address. In this wall all connections that use the IIP are monitored and flagged on the recipient's side. This is important for updating the sending devices when the physical IP address is changed.

IPv6 Address Allocation:

A specific range of IPv6 addresses must be reserved for IIP addresses. This allocation will automatically allow for any given IP address to be identified as an IIP address quite easily. It is theoretically possible to use the user's actual name for this service, but it would make lookup inefficient on the server. IPv6 addresses have a standard format and length and would be easier to search when a client makes a request to resolve an IIP address to a physical IP address. Once a user registers for an IIP address from some authority, possibly his/her ISP, this address should be allocated to the user for the duration of his/her lifetime (ideally).

IPv6 Protocol Extension:

The IPv6 protocol extension is a simple addition that holds a flag indicating that this packet was originally sent using user's IIP address. The machines that have this flag set are tracked by the recipient. The reason for this is discussed below in the *IIP Protocol* section.

IIP Servers:

The IIP Servers hold several pieces of information all of which are indexed by the IIP address:

- IIP Address (used as an index).
- Status of User (Active/Inactive): If the user is not logged onto any Internet-connected device or does not wish to be disturbed he/she can set his/her IIP address mode to *Inactive*. If a user tries to send a message to an Inactive IIP address he will receive a message from the server indicating that the user is inactive. An Inactive status is also assigned to an unused IIP address.
- Associated Device IP Address: The physical IP address of the device that the user is currently at.

The IIP Servers should be created and maintained by the ISPs.

IIP Protocol:

The protocol is used for communicating with the IIP server and serves two purposes. It allows the user to update his/her status and current device IP address and it allows a user to resolve an IIP address to a physical IP address.

IP Address Update:

When a user registers for an IIP address, he is given some form of a key. This key is used to verify the user's identity for changing his/her status from Inactive to Active. This key means that the user must always communicate with his/her ISP IIP server in order to change his/her status to Active and not any random IIP server. Upon changing his status to Active, the server is also updated with the current physical IP address of the device the user logged on from.

They key feature of IIPA Service is shown here. If the user switches devices, e.g. is sitting in the office and walks out of the office with an Internet-enabled PDA, the service automatically sends a message to the IIP server changing the physical IP address from the previous device to the current device. This is done on the fly. The implementation of this on-the-fly changing service is still too early in development to discuss, and therefore, in this paper we assume that the user must manually send a message from device 1, ordering the switch to device 2, and then confirm on device 2. However, the idea is for this switch to be done automatically and with transparency to the user. It is also possible for the user to deactivate the service by sending an appropriate message to the server setting the IIP address to Inactive mode.

When the user switches devices, the client must send a message not only to the IIP server, but also to all devices currently sending to the user. This list of devices is monitored by the user's device (as discussed above). Hence, a multicast message is sent to all relevant devices.

It should be noted that they physical IP address is NOT updated on the server when a mobile device moves across cells as the routing procedures for those transitions are already taken care of.

IIP Address Resolving:

In order for a device to communicate with a specific user directly it requires his/her IIP address. The **IIP address/individual's name** affiliation should not be available publicly to protect user's privacy. Hence, the device, or its user, must have already been given the IIP address by the intended recipient.

Now the device has the user's IIP address. It must first send a message to the IIP server requesting the current physical IP address of that user. The IIP server will send a response that indicates if the user is active or not and if so will send the physical IP address. This address is then cached on the client and used until it receives a change message from the user. However, if the device has not communicated with the user recently, it should lookup the physical IP address from the server to be sure about his/her location.

Why this Idea is Ideal for IPv6:

- The sheer number of IP addresses needed to assign everyone an Individual IP address was not available before. IPv4 only supplied approximately 4.5 billion addresses which is less than the population of earth.
- The Mobility of IPv6. Mobile IPv4 is complex and bulky, hence it would be difficult to reliably route data to a mobile device. Since the purpose of this service is to offer packet-to-user connectivity, mobility is a key factor since users are usually hard to find when they are mobile, not stationary.
- The well developed multicast ability of IPv6. Multicasting was limited in IPv4. With IPv6 it is possible to multicast to any group, which is necessary for this service.
- Ease of IPv6 protocol extensions. The simple extension of noting that a connection uses an IIP address would have meant extra data for the routers to analyze in IPv4 which would have meant slower routing times. But thanks you IPv6 encapsulation of protocol extensions, it is easy to add a simple protocol with a lot of functionality.

Issues that need to be addressed:

Of course this description of the service is very basic at best. There are a host of issues that still need to be addressed such as:

- SPAM control (potentially a huge problem).
- Specific format of IIP protocol control messages and number of messages needed.
- IIP protocol packet format (needs to be designed to be flexible).
- IIP address registration procedures. (Key generation and authentication with local ISP IIP server).

- IIP server structure and types. (How information should be shared among IIP servers).
- IPv6 protocol extension to indicate IIP address usage in connection. (Extension details and format).
- Exactly how automatic handoff will be performed for this service. (One possibility is using BlueTooth ™ technology to have adjacent devices communicate their presence to one another and have the IIP servers hold a database of valid devices that the user can add to such that these devices automatically ask the user to switch if he/she moves them far enough apart. Also, a smart client can be written that learns the user's habits and adapts accordingly).

  Using manual switching, as mentioned earlier in the document, defeats the purpose of the feature to seamlessly switch the user's IIP address automatically to point to his/her current physical IP address, but the technical issues of this implementation are still being worked out and will hopefully be finalized in our Implementation Award submission.
- Exactly what data to store on the client and server, and when to poll the server and when to use the cache. It may be beneficial to know something about the recipient's device. E.g. if the last known physical IP address for a user was an office computer at 3pm, then it would be wise to resolve the IIP address to the current IP address from the server if the next communication takes place at 9pm.

In addition, there are issues that need to be considered to extend the functionality of this service. One of these is:

- While this service is not designed to be use for secure communication, further research may reveal techniques for using this service to do exactly such a thing. Dynamic VPNs, fox example, may be a possibility.

Uses of this service:

There are several potential uses of this service. However, we are confident that as it becomes available the creativity of the networking community will find uses for it that we have not even imagined. Some uses that we suggest are:

- Person-to-person messaging (although similar functionality already exists via mobile messaging services such as AOL. However this system uses a standard protocol.)
- Follow-me streaming video. (For example you can view a video stream from your office and, as you walk out to your car, continue to view the stream on your PDA automatically)

References:

There is not enough space to list them all.
Most used resources were RFCs and IETF mailing list archives.
Detailed references can be made available upon request.

Note from the Saudi Networking Research Group:

We thank the IPv6 Promotion Council of Japan for sponsoring this competition and raising our interest in IPv6. It was a wonderful learning experience, if nothing else. We hope to contribute something to the movement towards IPv6. We consider this document our first, albeit small, step in that direction.