Abstract

The IETF Integrated Directory Services (IDS) Working Group proposes to establish a set of specifications for a simple Internet white pages service without prejudice to existing recommendations or implementations. This set of I-Ds will document user and schema requirements.

Section 1.0 provides a brief introduction to related work and describes the purpose of this document.
Section 2.0 describes the scope of this document.

Section 3.0 presents several illustrative user scenarios in the form of descriptive application flows.

Section 4.0 summarizes, describes, and augments requirements documented by Postel and Anderson [3].

Section 5.0 restates security considerations in terms more commonly used to describe security features and services than those used in Section 4.0.

Section 6.0 includes acknowledgements of individual contributions to this document.

Section 7.0 provides a list of references.

Section 8.0 provides the editors’ addresses.

1.0 Introduction

The Internet community has done a significant amount of work in the analysis of Internet White Pages Services and several documents address the issue of IWPS requirements [2][3]. The work on this document has benefited from the review of this work and several implementations. Each implementation was developed to explore a solution set of requirements. A number of them are based on an underlying technology like X.500 [1]. Others have defined new or built on old systems [4]. With each approach we acquired a new understanding of the general problem set. The Internet always benefits from this type of implementation diversity and the most likely future for the IWPS is that it will consist of a number of directory like services that will interwork to provide the general IWPS.

The purpose of this document is to define a single set of user requirements for the Internet White Pages Service that accommodates the wide variety of information retrieval protocols which can be used to create a directory service. Based upon the work done to date on building and deploying directory service systems, many user-related issues and requirements become obviated. Therefore, a common set of user requirements will be documented in the sections that follow. It is not the purpose of this document to propose restrictions for the development of the independent implementations of the IWPS.
2.0 Scope

This document will describe user requirements and issues for a narrowly defined subset of white pages directory services intended to provide information about Internet Users. These requirements are based in part on the work performed in the inactive IETF WHIP Working Group and in part on the user scenario descriptions documented in section 3 of this document. This document attempts to establish a common set of requirements for different classes of users of an IWPS. The concerns of end-users, machine-users, and administrative users were considered and addressed during the process of writing the scenarios and requirements documented below.

3.0 User Scenarios

When writing user-driven service requirements, it is often useful to document operational or flow-based descriptions of how a service might be used. In the case of the IWPS, the following questions were used to frame these operational descriptions:

- What type(s) of information must the user specify?
- What type(s) of information might be optional?
- What type(s) of information should be returned?
- Is there a way for users to specify the type(s) of information they want returned?
- Can the user send in a request via electronic mail, or must they use a service via some protocol? Or does the user have an option to do either?
- Can the user specify a limit on the number of entries returned?
- Is a maximum number of entries that can be returned in response to a request set by some party other than a human user?
- What kinds of error and status indicators and messages are delivered to users?
- Does the user see some sort of indicator that looks different depending on how long the search could take?
- Do administrative users get faster response times than other types of users?

- How is modification handled? By who? How are such modifications authorized and authenticated?

Flow-based descriptions of how the IWPS might be used by different types of users are included below. These descriptions are not exhaustive in scope, but serve to clarify how the IWPS might be used. These scenarios are intended to neither restrict IWPS implementors nor imply that IWPS features illustrated are more important than other IWPS features. Scenarios for end-users, machine-users, and administrative users are included.

3.1 End-User Scenarios

3.1.1 End-User Search w/o Security

a. An End-User accesses a WWW-based form that acts as an interface to the IWPS.

b. The End-User sees a screen enabling them to submit a query based on one or more of the following search criteria:

- name
- voice telephone number
- e-mail address
- organization name
- favorite beer
- postal address

The End-User also sees indicators that they must specify at least one of either name, voice telephone number, or e-mail address.

A note might also be displayed to the End-User, suggesting that, while not mandatory, inclusion of other defined search criteria will generally result in a shorter response time and fewer listings returned.
c. The End-User specifies the name and organization for the person they wish to search for and clicks on the submit button.

d. The End-User’s browser encodes the form values into a CGI script call, with the keys "name" and "org" set equal to "Smith" and "AT&T" respectively.

e. The WWW server receiving the CGI script call invokes the appropriate CGI script, which queries AT&T’s public employee database and returns the first 100 listings retrieved to the user’s browser along with an indicator that the next 100 listings for name=Smith, org=AT&T can be retrieved if desired by clicking on a particular area of their screen. The WWW server also must also pass the context of this search session to the End-User’s client as hidden key-value pairs so that the next 100 listings can be returned if requested. No search context information is maintained on the WWW server in this case, but is passed back to the server upon indication by the End-User that they wish to retrieve the next 100 listings.

3.1.2 End-User Search w/Sliding Geographic Scope Options

This application flow is similar to the one described in paragraph 3.1.1, with the exception that a list of mutually exclusive geographic search scope limits are shown. Specifically, the options shown consist of the following:

- City Scope (includes a text box to specify the city)

- State Scope (includes a text box to specify two letter state code)

- Multiple State/Province Scope (includes a text area to specify the list of states/provinces)

- Country Scope (includes a text box to specify the country)

- Multiple Country Scope (includes a text area to specify the list of countries)

- Global Scope

Selection of one of these options and completion of additional information as required by the particular option chosen is mandatory.

The End-User will also see a graphical indicator of relative response
time for each of these options as follows:

<table>
<thead>
<tr>
<th>Scope Option</th>
<th>Indicator of Relative Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>City Scope</td>
<td>Lightening Bolt</td>
</tr>
<tr>
<td>State/Province Scope</td>
<td>Stop Watch</td>
</tr>
<tr>
<td>Multiple State/Province Scope</td>
<td>Clock on a Wall</td>
</tr>
<tr>
<td>Country Scope</td>
<td>Grandfather Clock</td>
</tr>
<tr>
<td>Multiple Country Scope</td>
<td>Grandfather Clock w/ Spider Web</td>
</tr>
<tr>
<td>Global Scope</td>
<td>R.I.P.</td>
</tr>
</tbody>
</table>

Thus the user has some idea of relative response times when deciding upon the geographic limit to impose on the search scope. Note: these indicators are merely illustrative and most likely are not reflective of good user interface guidelines and practices.

Otherwise, the application flow is the same as that described in paragraph 3.1.1.

### 3.1.3 Encrypted End-User-Initiated Information Update

In this scenario, an End-User wants to change their electronic mail address and wishes to use encryption as an authentication mechanism.

a. The End-User submits an e-mail message (from their old e-mail address) encrypted with their private key to an Authoritative IWPS Information Base Update Agent with the following content:

```plaintext
for <name>=Christopher_W_Apple
{
  change <email>
  {
    from: "capple@arch4.att.com"
    to:   "capple@dir1.control.att.com"
  }
}
```

b. The Authoritative IWPS Information Base Update Agent retrieves the End-User’s public key based upon their old e-mail address and attempts to decrypt the message.

c. If the decryption process is successful, the Agent updates the master copy of the <email> attribute such that the new value replaces the old value and delivers a confirmation message, encrypted with the Agent’s private key, to both the new and the
old e-mail address.

If the decryption process is unsuccessful, the Agent logs the failed decryption event, and sends an error-indication message, encrypted with the Agent’s private key, to the old e-mail address.

d. For either case described in step c) of this application flow, the End-User’s browser fetches the public key of the Agent and decrypts the message.

3.1.4 End-User Batch Search Request w/o Security

a. The End-User sends an e-mail message to an IWPS server containing the following message body:

\[
\text{list}_n := \{ Chris\_Apple, Peter\_Jurg, April\_Marine \}
\]

\[
\text{foreach element of list}_n \{ \text{return } <\text{name}>; \text{return } <\text{org}>; \text{return } <\text{email}>; \text{return } <\text{telno}>; \}
\]

b. Upon receipt by the IWPS server mailing list processor, the End-User’s request is queued for query resolution processing. The mailing list processor also sends a confirmation e-mail to the "reply-to:" e-mail address indicating that the request has been queued.

c. Eventually, the request is processed and the names specified in the list are resolved into the fully-qualified name (<name>), organization (<org>), e-mail address (<email>), and voice telephone number (<telno>).

d. If it is not possible for one or more of names to be unambiguously resolved, a list of possible names is returned along with an indicator of receipt of an ambiguous request and any resolvable listings.

e. If a particular attribute is either undefined, defined but not populated, or defined but indicated as private, an indication
of the status of missing attribute values is returned.

f. The results of query resolution are e-mailed to the "reply-to:" address referred to in step b of this application flow.

3.2 Machine User Scenarios

3.2.1 Addressing Electronic Mail by Local Recipient’s Name

a. End-User types in their preferred electronic mail tool at an operating system shell prompt followed by one or more recipient names:

   $mailx Chris_Apple

b. End-User proceeds to compose electronic mail message and indicates that the message should be delivered to the list of recipients as they normally would.

c. Before the mail-tool process terminates, it performs a local white pages directory query, attempting to resolve the recipient names into electronic mail addresses.

d. The local white pages directory query results in the following information being displayed to the End-User:

   Recipient-Name: Chris_Apple cannot be resolved unambiguously.

   Please select one of the following:

   1) Chris_Apple: capple@arch4.ho.att.com : preferred
   2) Chris_Apple: capple@orb.att.com

   Enter your choice here:

e. Since the End-User can see that Chris prefers to have mail sent to capple@arch4.ho.att.com they enter 1.

f. The mail-tool sends the electronic mail address retrieved and indicated by the End-User as the value of the "to:" field in the electronic mail message header to the local mail delivery agent.

g. The mail message is delivered to the capple@arch4.ho.att.com mailbox for Chris_Apple.
3.2.2 Addressing Electronic Mail by Remote Recipient’s Name

a. End-User types in their preferred electronic mail tool at an operating system shell prompt followed by one or more recipient names:

   $mailx April_Marine

b. End-User proceeds to compose electronic mail message and indicates that the message should be delivered to the list of recipients as they normally would.

c. Before the mail-tool process terminates, it performs a local white pages directory query, attempting to resolve the recipient name into an electronic mail address.

d. The local white pages directory query results in the following information being displayed to the End-User:

   Recipient-Name: April_Marine is unknown to this system.

   Search Alternate Directory at:

   1) NASA
   2) SRI

   Please enter choice:

e. The End-User knows that April currently works at NASA and enters 1.

f. The mail-tool process initiates a query of the white pages directory for NASA and receives April’s electronic mail address which it stores for later use.

g. The mail-tool sends the electronic mail address retrieved and indicated by the End-User as the value of the "to:" field in the electronic mail message header to the local mail delivery agent.

h. The mail message is delivered to the address for April_Marine at NASA.

3.3 Administrative User Scenarios
3.3.1 Changing the Content of an Authoritative IWPS Resource Record (RR)

An employee moves from one department inside of an organization to another. The authoritative IWPS RR for an employee is maintained by the administrator of an associated group of departmental IWPS servers. This organization has established a policy that the IWPS administrator is the only person authorized to modify department numbers and may only do so upon receipt of an electronic mail message signed by the human resources department of that organization. Digital signatures are applied to messages requesting that changes to IWPS RRs be made to authenticate and confirm the integrity of change requests.

a. Human resources representative receives appropriate paperwork indicating an approved transfer of an employee from department XYZ-123 to department ABC-456.

b. Human resources representative sends a digitally signed electronic mail message to the IWPS server administrator, requesting that this employee’s department number be changed from XYZ-123 to ABC-456.

c. IWPS server administrator retrieves public key for human resources representative to verify the digital signature of the message.

d. If the digital signature is verified, the IWPS server administrator logs into an administration tool for the IWPS RR database and queries it to verify that the current department number is set to XYZ-123.

Otherwise, the IWPS server administrator logs the failed digital signature verification, notifies human resources of the nature of the message received, and the application flow ends.

e. The IWPS server is currently loaded quite heavily, but recognizes that this query originated from an administrative user and assigns a higher priority to the processing of this request.

f. The IWPS server query results indicate that the department number for the employee in question is currently XYZ-123.

g. The IWPS server administrator instructs the administrative tool to create a delayed IWPS RR database update request since they noticed that the server was a bit slow in responding to their initial query.
h. The IWPS RR database administrative tool stores the update request in a batch file of other such requests for processing at a pre-designated time (e.g., a time of day during which IWPS server utilization is expected to be low).

3.3.2 Moving an Authoritative IWPS RR into another Administrative Domain

Similar to the application flow described above in paragraph 3.3.1, an employee has transferred from one department to another. However, in this case, the IWPS servers for the old and the new department fall into different administrative domains. In addition to the organizational policies defined above in paragraph 3.3.1, the organization also has a statement of policy indicating that IWPS RRs that are moved from one administrative domain to another mandate that an alias for the new location of the authoritative IWPS RR be created and maintained for 2 months after the effective date of the employee’s transfer.

a. Human resources representative receives appropriate paperwork indicating an approved transfer of an employee from department XYZ-123 to department EFG-789.

b. Human resources representative sends a digitally signed electronic mail message to the administrator of the IWPS server in the administrative domain corresponding to the employee’s old department indicating that the employee has been transferred from department XYZ-123 to department EFG-789.

c. IWPS server administrator retrieves public key for human resources representative to verify the digital signature of the message.

d. If the digital signature is verified, the IWPS server administrator logs into an administration tool for the IWPS RR database and queries it to verify that the current department number is set to XYZ-123.

Otherwise, the IWPS server administrator logs the failed digital signature verification, notifies human resources of the nature of the message received, and the application flow ends.

e. The IWPS server query results indicate that the department number for the employee in question is currently XYZ-123.

f. The IWPS server administrator recognizes that department number EFG-789 falls outside of the scope of their administrative domain and sends a digitally signed e-mail message to the administrator of the IWPS server within the administrative domain authoritative
for the IWPS RRs of department EFG-789. This e-mail message contains a copy of the e-mail from the human resources representative along with an encrypted copy of the current employee IWPS RR.

g. The administrator for the EFG-789-authoritative IWPS server retrieves the public key for the XYZ-123-authoritative IWPS server administrator to verify the digital signature and decrypt the IWPS RR for the transferred employee.

h. If the signature is verified, the administrator for the EFG-789-authoritative logs into an administrative tool for the IWPS RR database and creates a new RR for the transferred employee with the new department number populated.

Otherwise, the digital signature verification failure is logged and reported to the administrator of the XYZ-123-authoritative IWPS server.

i. The EFG-789-authoritative IWPS server generates a digitally signed message indicating that an automated IWPS RR database update agent in the XYZ-123-authoritative domain should change the IWPS RR type from an authoritative RR to that for an alias pointing to the new RR and that this alias should have a time-to-live value of 2 months from the effective date of the employee transfer.

j. Upon retrieval of an appropriate public key and successful digital signature verification, the changes described above are made. The XYZ-123-authoritative IWPS RR database update agent also triggers the creation of a record in an add-modify-delete database activity log for the IWPS server authoritative for the XYZ-123 department.

4.0 Requirements

Included below are requirements which were documented in one form or another in RFC 1588[3]. General requirements about white pages directory services are presented. More specific requirements are grouped according to the user classes mentioned above and are accompanied by text describing the intent or need for each.

4.1 General Requirements

In finding people, the service should work fast when searching for people by name, even if search criteria values regarding location or organization is vague. In finding information about people, the service should retrieve information associated with people, such as a
phone number, a postal or email address, or even a certificate for
security applications (authentication, integrity, and privacy).
Additional information associated with people can also be provided by
a directory service, such as a list of publications, a description of
current projects, or a current travel itinerary.

A white pages directory should be flexible, should have low resource
requirements, and should integrate into other systems that may be
currently in use; it should not cost a lot, so that future
transitions are not too costly; there should be the ability to
migrate to improved technology, if a better solution becomes
available; there should be a way to share local directory information
with the Internet in a seamless fashion and with little extra
administrative effort; the query responses should be reliable enough
and consistent enough that automated tools search, retrieval, and
administration tools can be used.

4.2 End-User Requirements

Searching - Searching is the ability to find information about people
given some information about them. This information can be fuzzy
("Find Apple in New Jersey") or more specific ("Find Chris Apple in
Aberdeen, NJ who works at AT&T Bell Laboratories"). Generally, more
specific search criteria should result in less voluminous results
than will searches based on fuzzy search criteria. Often, a list of
results will be returned.

Relaxed Spelling - Users will want to be able to submit truncated
search criteria.

Information Retrieval - Retrieval is defined as obtaining additional
information associated with a person, such as an address, telephone
number, email mailbox, or security certificate.

Authentication of Results - Users want to be assured that information
search and retrieval results are authentic.

Reasonable level of data quality - Data should be up to date. "Live"
data should be used to populate Internet WPS, to avoid stale data.

Supports privacy requirements of various individual end-users -
individuals may or may not want to be listed with the IWPS and should
be given a mechanism by which such preferences can be indicated to
administrators of the service. Individuals may want to limit or
prevent access to specific types of information contained in their
IWPS RR.
Registration with Service - individuals should be able to obtain a globally unique identifier (Uniform Person Identifier)

Fast response times for both search and retrieval - Users want fast searching across the distributed database on attributes different from the database structure. Pre-computed indices satisfy this desire, though only for specified searches.

Support for batch/off-line search/retrieval requests - users may want to submit batch requests for off-line processing and subsequent delivery via e-mail.

Service Status Notification - users will want to receive an indication that service is unavailable as well as the reason for said unavailability

Service Request Error Results - Users will want to receive indication of the nature of errors that occur during the processing of search and retrieval requests.

Ease-of-Use - service must be easy to use. There must be a shallow learning curve for novice users.

Support storage and retrieval of security certificates and/or public keys - Security certificates (a type of information associated with an individual) are essential for the use of end-to-end authentication, integrity, and privacy in Internet applications. The development of secure applications in the Internet is dependent on a directory system for retrieving the security certificate associated with an individual. For example, the privacy enhanced electronic mail (PEM) system has been developed and is ready to go into service, and is now hindered by the lack of an easily used directory of security certificates. An open question is whether or not such a directory needs to be internally secure.

Availability/Reliability - Service should be highly reliable and available a large percentage of the time.

Support Multiple interfaces - Service should be accessible via multiple protocol interfaces

Support multiple clients - Service should be accessible via many different client types (e.g. support for different types of content browsers).

Low Resource Requirements - Service should place low resource
requirements on client platforms.

Inexpensive - Service should be inexpensive or free to use.

Evolvability - Service should be evolvable such that new features and access to additional information types can be provided when demand is sufficient to justify it.

Information Integrity - Assurance that data about themselves will not be changed by an unauthorized party.

Navigation - the service should include options that allow the distributed information tree to be navigated to locate globally unique person names.

Support for Multimedia Content - users will want the IWPS to be capable of locating multimedia content associated with people; perhaps an image or a sound or video clip.

User Manuals - Guidelines are needed for methods of searching and using directory information.

Local Value - Adds value if run strictly as local service.

Ambiguous Criteria Feedback - the user should receive feedback on how to better specify search criteria, either in the form of instructions or of a list of options that have some approximate relationship to criteria submitted.

Support for Multiple Languages - the user should be able to indicate language preferences as a part of IWPS requests; help, error, and status messages should be presented in the language of the user’s choice; on-line documentation for users should be made available in multiple languages.

Data Completeness - The IWPS should be able to provide a user with an indication of the data completeness. For example if you search for someone named xxx within an organization and the result is that xxx cannot be found, you would like to know whether or not all employees of this organization are in the database. In the first case you know that xxx doesn’t exist over there, in the latter case you’re not sure about that and the IWPS could point you to a general address of the organization where you can get more information. Such a feature is especially important if commercial organizations decide not to reveal all internal address information through the IWPS.
Data Age - As a user you would like to know when the last update was done on parts of the data.

4.3 Machine User Requirements

In addition to the requirements above in 2.1, the following are requirements of machine users of a white pages directory service:

Contextual Views - Service must be capable of providing contextual views of directory information to machine users of directory services. An example of this could be thought of in terms of electronic mail addressing by name, rather than e-mail address. A user would key in a globally unique person name as the e-mail address, perhaps preceeded with some reserved character that indicates that the local mail server should use the IWPS to resolve the unique person name into that person’s (hopefully) current e-mail address.

Query Automation - the ability to automate Internet WPS queries is essential for providing an IWPS to machine users. See example for Contextual Views.

Common Interface Definition - having a common interface defined for machine users of directory services is essential. This machine interface should allow machine users to issue appropriate commands from a common set to the directory service that enable it to search for and retrieve information necessary to perform its functions. This could take the form of an API library used to build proxy clients or of an SQL-like interface to IWPS servers. As a minimum, this Common Interface Definition should include the following components:

- Standard protocols for directory queries
- Standard query format
- Standard field names
- Standard searching algorithms and strategies

4.4 Administrative User Requirements

Ease-of-Use - Ability to externalize existing local directory to Internet (with minimum effort) -- or -- Ability to easily export local directory info to Internet WPS (data conversion tools?) Simple site registration processes. Easy to install servers. Clear idea of
naming authorities.

Level-of-Complexity - Allow site to choose level of complexity they choose to deploy. This complexity will be proportionate with site needs.

Low Entry Cost - Software freely available / public domain versions; low resource consumption; short installation time.

Availability/Reliability - a highly available/reliable service infrastructure (authoritative name servers and index servers)

Registration Process - Clear mechanisms defined for new sites to join Internet WPS. Assistance available for new sites to join Internet WPS. Simple centralized organization registration procedures (if used at all).

Privacy/Confidentiality - Ability to limit information exposed outside an organization from a local site. Ability to limit information exposed to end-users or machine users based on legal and regulatory restrictions imposed by various national, regional, and local legislative bodies.

Easy to build client software (user agents).

Synchronization/Replication Tools - administrators should have access to directory synchronization, replication, and partitioning tools.

Ability to develop & deploy high performance servers for upper layers of tree (if tree structure used) or centroids

Local service easy to integrate into global service.

Flexible Technology Choices - Ability for local sites to decide what protocol or technology they choose to deploy or externalize in providing access to locally owned and administered information.

Access Control - Administrative users must have appropriate access control tools available to them such that unauthorized parties cannot modify the contents of either local directory information servers or IWPS index/name resolution servers.

Data Trawling - Administrative users must have tools that enable them to prevent data trawling activities.

Data Update/Modification - Administrative users must have secure
updating and modification utilities at their disposal. Data should be maintained by local organizations.

Help - Cookbooks for administrators wishing to install servers, register their local site, or otherwise configure service options should be made freely available. New administrators may need assistance in getting their servers up and linked to a central server.

Search Scope - Administrators should be provided with capabilities that allow them to place a ceiling over the number of servers that can be contacted in a given search. Administrators should be provided with configurable facilities that enable application of searching heuristics to minimize the effect of ill-formed queries. Knowledge servers are another option to consider.

Indexing - Administrators should be provided with tools that enable them to retrieve/exchange/construct indices of various portions of the distributed directory.

Upgrade Manageability - Administrative users should be provided with a reasonably painless upgrade path from one successive version of service related software to another.

Data Feeds - Administrators should have authoritative data feeds for all information that is to be a part of the distributed directory database. Administrators should have tools that assist them in maintaining data feeds associated with rapidly changing information.

Data Caching - Administrative users should be able to configure data caching methods appropriate for the lifetime of the information contained in their portions of the distributed directory database.

Evolvability - Administrative users will want any naming schema used to be extensible and flexible but consistent so that it is easier to administer and to maintain across service-related software patch application and upgrade installation.

Ability to Point to Multimedia Resources - IWPS content should be confined to searchable attributes (names, etc.) and should be able to contain pointers to non-searchable information stored elsewhere (images, video clips, sound clips, etc.). This requirement arises from the inclination of administrative users to reduce storage requirements for directory services.
5.0 Security Considerations

Based on the requirements documented in Section 4.0, the IWPS will require the following security features:

   a. the capability to generate and verify electronic information signatures
   b. the capability to encrypt and decrypt electronic information with public and private keys
   c. a key management and distribution infrastructure
   d. a mechanism for hiding white pages directory data from users outside of an authorized user group
   e. a mechanism for the detection and prevention of data trawling

To be implemented in a scalable manner, these features require the provision of confidentiality, authentication, integrity, privacy, and data protection infrastructure services on the Internet.

6.0 Acknowledgements

April Marine and Tony Genovese contributed to this I-D by suffering through telephone conversations with Chris Apple about the scope and nature of this paper.

Tony Genovese, Peter Jurg, and April Marine provided editorial comment and feedback during numerous rough draft reviews of this I-D.

7.0 References


8.0 Editors’ Addresses

Chris Apple
AT&T Bell Laboratories
Room 1L-338, 101 Crawfords Corner Road
P.O. Box 3030
Holmdel, NJ 07733-3030
USA

Phone: (908) 949-5937
E-mail: capple@arch4.ho.att.com

Tony Genovese
The Microsoft Corporation
One Microsoft way
Redmond, Washington 98007
USA

Phone: (206) 703-0852
E-mail: tonyg@microsoft.com

Peter Jurg
SURFnet bv
Postbus 19035
NL-3501 DA Utrecht
The Netherlands

Phone: +31 30 310290
Fax: +31 20 340903
E-mail: Peter.Jurg@surfnet.nl
X.400: C=nl; ADMD=400net; PRMD=surf; O=surfnet; S=jurg

April N. Marine
Network Applications and Information Center
NASA Ames Research Center
M/S 204-14
Moffett Field, CA 94035-1000
USA

Phone: (415) 604-0762
E-mail: amarine@atlas.arc.nasa.gov