

Network Working Group
Request for Comments: 2194
Category: Informational

B. Aboba
Microsoft
J. Lu
AimQuest Corp.
J. Alsop
i-Pass Alliance
J. Ding
Asiainfo
W. Wang
Merit Network, Inc.
September 1997

Review of Roaming Implementations

1. Status of this Memo

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

2. Abstract

This document reviews the design and functionality of existing roaming implementations. "Roaming capability" may be loosely defined as the ability to use any one of multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one. Examples of cases where roaming capability might be required include ISP "confederations" and ISP-provided corporate network access support.

3. Introduction

Considerable interest has arisen recently in a set of features that fit within the general category of "roaming capability" for Internet users. Interested parties have included:

Regional Internet Service Providers (ISPs) operating within a particular state or province, looking to combine their efforts with those of other regional providers to offer service over a wider area.

National ISPs wishing to combine their operations with those of one or more ISPs in another nation to offer more comprehensive service in a group of countries or on a continent.

Businesses desiring to offer their employees a comprehensive package of access services on a global basis. Those services may

include Internet access as well as secure access to corporate intranets via a Virtual Private Network (VPN), enabled by tunneling protocols such as PPTP, L2F, or L2TP.

What is required to provide roaming capability? The following list is a first cut at defining the requirements for successful roaming among an arbitrary set of ISPs:

- Phone number presentation
- Phone number exchange
- Phone book compilation
- Phone book update
- Connection management
- Authentication
- NAS Configuration/Authorization
- Address assignment and routing
- Security
- Accounting

In this document we review existing roaming implementations, describing their functionality within this framework. In addition to full fledged roaming implementations, we will also review implementations that, while not meeting the strict definition of roaming, address several of these problem elements. These implementations typically fall into the category of shared use networks or non-IP dialup networks.

3.1. Terminology

This document frequently uses the following terms:

home ISP This is the Internet service provider with whom the user maintains an account relationship.

local ISP This is the Internet service provider whom the user calls in order to get access. Where roaming is implemented the local ISP may be different from the home ISP.

phone book

This is a database or document containing data pertaining to dialup access, including phone numbers and any associated attributes.

shared use network

This is an IP dialup network whose use is shared by two or more organizations. Shared use networks typically implement distributed authentication and accounting in order to facilitate the relationship among the sharing parties. Since these facilities are also required for implementation of roaming, implementation of shared use is frequently a first step toward development of roaming capabilities. In fact, one of the ways by which a provider may offer roaming service is to conclude shared use agreements with multiple networks. However, to date the ability to accomplish this has been hampered by lack of interoperability among shared use implementations.

non-IP dialup network

This is a dialup network providing user access to the member systems via protocols other than IP. These networks may implement phone book synchronization facilities, in order to provide systems, administrators and users with a current list of participating systems. Examples of non-IP dialup networks supporting phone book synchronization include FidoNet and WWIVnet.

4. Global Reach Internet Consortium (GRIC)

Led by a US-based Internet technology developer, AimQuest Corporation, ten Internet Service Providers (ISPs) from the USA, Australia, China, Japan, Hong Kong, Malaysia, Singapore, Taiwan, and Thailand formed the Global Reach Internet Connection (GRIC) in May, 1996. The goals of GRIC were to facilitate the implementation of a global roaming service and to coordinate billing and settlement among the membership. Commercial operation began in December of 1996, and GRIC has grown to over 100 major ISPs and Telcos from all over the world, including NETCOM, USA; KDD and Mitsubishi, Japan; iStar, Canada; Easynet, UK; Connect.com, Australia; Iprolink, Switzerland; Singapore Telecom; Chunghwa Telecom, Taiwan; and Telekom Malaysia. Information on GRIC is available from <http://www.gric.net/>.

In implementing their roaming service, GRIC members have chosen software developed by AimQuest. AimQuest Corporation's roaming implementation comprises the following major components: the AimTraveler Authentication Server (AAS), the AimTraveler Routing Server (ARS), and the AimQuest Internet Management System (AIMS), software designed to facilitate the billing process. Information on the AimQuest roaming implementation is available from <http://www.aimquest.com/>.

The AimTraveler Authentication Server (AAS) runs at each member ISP location, and handles incoming authentication requests from NAS devices and other AASes. The AimTraveler Routing Server (ARS) can run anywhere. A single routing server can be used where centralized routing is desired, or multiple routing servers can be run in order to increase speed and reliability or to gateway to networks of particularly large partners.

The first version of the AimTraveler software, deployed by AimQuest in May, 1996, supported direct authentication between members of the roaming consortium, but as GRIC grew, management of the relationships between the authentication servers became a problem. In August, 1996, AimQuest began development of the AimTraveler Routing Server (ARS) in order to improve scalability.

The routing server is comprised of two elements: The Central Accounting Server and the Central Routing Server. The Central Accounting Server collects all the roaming accounting data for settlement. The Central Routing Server manages and maintains information on the authentication servers in the roaming consortium. Adding, deleting, or updating ISP authentication server information (e.g. adding a new member ISP) may be accomplished by editing of a configuration file on the Central Routing Server. The configuration files of the AimTraveler Authentication Servers do not need to be modified.

The AimTraveler Authentication and Routing Servers are available for various UNIX platforms. Versions for Windows NT are under development. The AimTraveler Authentication Server supports both the UNIX password file and Kerberos.

The AimQuest Internet Management System (AIMS) is designed for large ISPs who need a centralized management system for all ISP operations, including sales, trouble-ticketing, service, and billing. AIMS produces usage and transaction statement reports, and includes a settlement module to produce settlement/billing reports for the roaming consortium members. Based on these reports, the providers charge their ISP/roaming customers, and pay/settle the roaming balance among the providers. AIMS currently runs on Sun/Solaris/Oracle. A version for Windows NT and SQL Server is expected to become available in Q4 1996.

4.1. Phone number presentation

Currently there are two principal methods by which GRIC users can discover available phone numbers: a Web-based directory provided by the GRIC secretariat, and a GRIC phone book client on the user PC with dialing capability.

4.1.1. Web based directory

A directory of GRIC phone numbers is available on the GRIC home page, <http://www.gric.com/>. The list of numbers is arranged by country and provider. For each provider within a country, this directory, provided in the form of a table, offers the following information:

- Provider address, voice phone and fax
- Customer support phone number
- Provider domain name
- Primary Domain Name Server
- Secondary Domain Name Server
- Dial-up IP Address
- News server
- Web page
- POP phone numbers (i.e. 1-408-366-9000)
- POP locations (i.e. Berkeley)
- Proxy addresses
- Dialer configuration

In order to discover phone numbers using the Web-based directory, it is expected that users will be online, and will navigate to the appropriate country and provider. They then look up the number and insert it into the AimQuest Ranger dialer.

4.1.2. GRIC phone book client

The GRIC phone book client software provides for phone book presentation as well as automated updating of phone numbers. The GRIC phone book includes a list of countries, states, cities and area/city codes, as well as detailed provider information, including the customer support phone number, and Internet server configuration info. The Phone book, developed with Java, is available for download from the AimQuest Web site:

<http://www.aimquest.com/dialer.html>

4.2. Phone number exchange

GRIC members submit information both about themselves and their POPs to the GRIC secretariat, which is run by AimQuest. The GRIC secretariat then compiles a new phone book and provides updates on the GRIC FTP and Web servers.

GRIC users then download the phone numbers either in Windows .ini file format or in HTML.

4.3. Phone book compilation

GRIC phone books are compiled manually, and represent a concatenation of available numbers from all the members of the roaming consortium, with no policy application. As new POPs come online, the numbers are forwarded to GRIC, which adds them to the phone book servers.

4.4. Phone book update

Phone numbers in the GRIC phone book client are updated automatically upon connection. The AimTraveler server includes an address book which contains the phone numbers of all the roaming consortium members.

4.5. Connection management

The AimTraveler software supports SLIP and PPP, as well as PAP and CHAP authentication.

4.6. Authentication

GRIC implements distributed authentication, utilizing the user's e-mail address as the userID (i.e. "liu@Aimnet.com") presented to the remote NAS device.

After the initial PPP authentication exchange, the userID, domain, and password information (or in the case of CHAP, the challenge and the response) are then passed by the NAS to the AimTraveler Authentication Server which supports both TACACS+ and RADIUS.

If the authentication request comes from a regular customer login, normal user id and password authentication is performed. If the user requesting authentication is a "roamer," (has a userID with an @ and domain name), the authentication server sends an query to the closest routing server. When AimTraveler Routing Server receives the authentication request, it first authenticates the AAS sending the request, and if this is successful, it checks its authentication server table. If it is able to match the domain of the user to that of a "Home ISP", then the Home ISP authentication server's routing information are sent back to the local ISP's authentication server. Based on the information received from the routing server, the AAS makes an authentication request to the user's Home ISP AAS for user id and password verification.

If the user is a valid user, the Home ISP authentication server sends a "permission granted" message back to the Local ISP authentication server. The Local ISP authentication server then requests the NAS to grant the user a dynamic IP address from its address pool. If the

username or password is incorrect, the Home ISP AAS will send a rejection message to the Local ISP AAS, and the user will be dropped by the NAS.

If multiple routing servers are installed, and the query to the first routing server does not result in a match, the query is forwarded to the next routing server. The server queries are cached on the routing servers, improving speed for repeated queries. The cache is sustained until a routing server table entry is updated or deleted. Updating or deleting results in a message to all neighbor routing servers to delete their caches.

The local authentication server also receives the accounting data from the NAS. If the data is for a regular customer login, the data is written to the Local ISP AAS log file. If the data is for a "roamer," the data is written to three places: the Local ISP AAS log file, the Home ISP AAS log file, and the ARS log file.

If the local ISP authentication server has caching turned on, then it will cache information on Home ISP authentication server configurations sent by the routing server. This means that if the same domain is queried again, the local authentication server does not need to query the routing server again. The local cache is cleared when the local authentication server receives an update message from the routing server or system manager.

4.7. NAS Configuration/Authorization

AimTraveler is comprised of two components, a Client(AAS) and a Server(ARS).

The AimTraveler Client acts as the PPP dial-up authentication server. When it detects an '@' sign in the userID field, it queries the AimTraverler Server for routing information, then forwards the authentication request to user's home authentication server. The AimTraveler Server, a centralized routing server, contains the authorized ISP's domain name, authentication servers and other information.

The AimTraveler currently supports RADIUS and TACACS+, and could be extended to support other authentication protocols. It also receives all the accounting records, which are subsequently used as input data for billing.

Since ISPs' NAS devices may be configured differently, the attributes returned by the home ISP AAS are discarded.

4.8. Address assignment and routing

All addresses in GRIC are assigned dynamically from within the address pool of the local ISP. Static addresses and routed LAN connections will be considered in the future, when GRIC offers corporate roaming service, with the implementation of tunneling protocols

4.9. Security

The user's password is hashed with MD5 before being sent from the Local ISP AAS to the Home ISP AAS. An encryption key is shared between the AAS and ARS. The current version of AimTraveler AAS does not support token cards or tunneling protocols.

4.10. Accounting

The AimTraveler Authentication Server (AAS) software can act as either a RADIUS or TACACS+ accounting server. When accounting information is received from the NAS, the local AimTraveler Authentication Server (AAS) sends accounting data (user name, domain name, login time) to both the Central Accounting Server (part of the ARS) and the user's Home ISP AimTraveler authentication server. In the case of GRIC, the Central Accounting Server is run by AimQuest.

The data sent to the central accounting server and home ISP are identical except for the form of user id and time stamp. For a traveler whose home ISP is in the US, but who is traveling in Japan, the Local (Japanese) ISP AimTraveler authentication server will receive an accounting record timestamped with Japan time while the Home (US) ISP AimTraveler authentication server will receive an accounting record timestamped with the appropriate US timezone.

The accounting data includes 2 new attributes for settlement reporting:

Attribute	Number	Type
-----	-----	----
Roaming-Server-ID	101	string
Isp-ID	102	string

The Roaming-Server-ID attribute identifies the AAS sending the authentication request. The Isp-ID attribute identifies the local ISP. Using this information the home ISP can track the roaming activities of its users (where their users are logging in).

The AimTraveler Server running at AimQuest keeps a record of all roaming transactions, which are used as input to the settlement and billing process. At the end of each month, AimQuest provides a roaming transaction summary to GRIC members using AIMS. The AIMS software is configurable so that it takes into account the settlement rules agreed to by GRIC members.

5. i-Pass implementation

5.1. Overview

i-Pass Alliance Inc., based in Mountain View, California, has developed and operates a commercial authentication and settlement clearinghouse service which provides global roaming between Internet service providers. The service is fully operational.

i-Pass Alliance Inc. has additional offices in Toronto, Singapore, and London. More information on i-Pass can be obtained from <http://www.ipass.com>.

The i-Pass network consists of a number of servers that provide real-time authentication services to partner ISPs. Authentication requests and accounting records for roaming users are encrypted and sent to an i-Pass server where they are logged, and then forwarded to a home ISP for authentication and/or logging.

Periodically, i-Pass reconciles all accounting records, generates billing statements, and acts as a single point for collecting and remitting payments.

i-Pass provides its service only to ISPs and channel partners. It does not attempt to establish a business relationship with individual-user customers of an ISP.

5.2. Access Point Database (APD)

i-Pass maintains a list of roaming access points in an Oracle database. This list is searchable by geographical region using a Web browser, and may be downloaded in its entirety using FTP. The information stored for each access point includes:

- Name of service provider
- Country
- State or Province
- City or Region
- Telephone number
- Technical support phone number
- Service types available

Technical information (help file)
Service pricing information

The Access Point Database is maintained by i-Pass staff, based on input from i-Pass partners.

5.3. Phone number presentation

i-Pass has developed a Windows application with a simple point and click interface called the "i-Pass Dial Wizard", which assists end-users in selecting and connecting to a local Internet access point.

The Dial Wizard allows users to first select the country in which they are roaming. A list of states, provinces, or other regions in the selected country is then presented. Finally a list of access points within the state or province is presented. The Dial Wizard displays the city name, modem phone number, and price information for each access point within the state or region.

When the user selects the desired access point, a Windows 95 "DialUp Networking" icon is created for that access point. If there is a login script associated with the access point, the DialUp Scripting tool is automatically configured. This means that end-users never have to configure any login scripting requirements.

The Dial Wizard has a built-in phonebook containing all the i-Pass access points. The phonebook may be automatically refreshed from a master copy located on ISPs web site.

The Dial Wizard is provided free of charge to i-Pass partners. i-Pass also provides the i-Pass Dial Wizard Customization Kit which allows ISP partners to generate customized versions of the Dial Wizard with their own logo, etc.

5.4. Authentication

There are three entities involved in servicing an authentication request:

Local ISP At the local ISP, the authentication server is modified to recognize user IDs of the form username@auth_domain as being remote authentication requests. These requests are forwarded to an i-Pass server.

i-Pass Server

The i-Pass server receives the authentication request, logs it, and forwards it to the home ISP identified by the auth_domain portion of the user ID.

Home ISP The home ISP receives the authentication request, performs authentication using its normal authentication method, and returns a YES/NO response to the i-Pass server, which in turn forwards the reply to the originating ISP.

i-Pass provides software components which run on the authentication servers of the local and home ISPs. Each member ISP must integrate these components with the native authentication method being used by the ISP. To simplify this task, i-Pass has developed "drop-in" interfaces for the most commonly used authentication methods. At the date of writing, the following interfaces are supported:

- Livingston RADIUS
- Ascend RADIUS
- Merit RADIUS
- TACACS+
- Xylogics erpcd (Versions 10 and 11)

A generic interface is also provided which authenticates based on the standard UNIX password file. This is intended as a starting point for ISPs using authentication methods other than those listed above.

The software integration effort for a typical ISP is on the order of 2-5 man-days including testing. Platforms currently supported include:

- Solaris 2.5 (Sparc).LI
- Solaris 2.5 (Intel)
- BSDI
- Digital Unix
- Linux
- FreeBSD
- HP/UX

ISPs may choose to provide authentication for their end-users roaming elsewhere, but not to provide access points to the i-Pass network. In this case the software integration effort is greatly reduced and can be as little as 1/2 a man-day.

5.5. Accounting

Accounting transactions are handled in the same way as authentication requests. In addition to being logged at the i-Pass servers,

accounting transactions are sent in real-time to the home ISP. This is intended to allow ISPs to update users' credit limit information on a real-time basis (to the extent that this capability is supported by their billing and accounting systems).

Settlement is performed monthly. The settlement process involves calculating the costs associated with each individual session, and aggregating them for each ISP. A net amount is then calculated which is either due from i-Pass to the ISP, or from the ISP to i-Pass, depending on the actual usage pattern.

The following reports are supplied to member ISPs:

- A Monthly Statement showing summaries of usage, service provided, and any adjustments along with the net amount owing.

- A Call Detail Report showing roaming usage by the ISP's customers.

- A Service Provided report showing detailed usage of the ISP's facilities by remote users.

The above reports are generated as ASCII documents and are distributed to i-Pass partners electronically, either by e-mail or from a secure area on the i-Pass web site. Hard-copy output is available on request.

The Call Detail Report is also generated as a comma-delimited ASCII file suitable for import into the ISP's billing database. The Call Detail Report will normally be used by the ISP to generate end-user billing for roaming usage.

5.6. Security

All transactions between ISPs and the i-Pass servers are encrypted using the SSL protocol. Public key certificates are verified at both the client and server. i-Pass issues these certificates and acts as the Certificate Authority.

Transactions are also verified based on a number of other criteria such as source IP address.

5.7. Operations

i-Pass operates several authentication server sites. Each site consists of two redundant server systems located in secure facilities and "close" to the Internet backbone. The authentication server sites are geographically distributed to minimize the possibility of failure due to natural disasters etc.

i-Pass maintains a Network Operations Center in Mountain View which is staffed on a 7x24 basis. Its functions include monitoring the i-Pass authentication servers, monitoring authentication servers located at partner facilities, and dealing with problem reports.

6. ChinaNet implementation

ChinaNet, owned by China Telecom, is China's largest Internet backbone. Constructed by Asiainfo, a Dallas based system integration company, it has 31 backbone nodes in 31 Chinese provincial capital cities. Each province is building its own provincial network, has its own dialup servers, and administers its own user base.

In order to allow hinaNet users to be able to access nodes outside their province while traveling, a nationwide roaming system has been implemented. The roaming system was developed by AsiaInfo, and is based on the RADIUS protocol.

6.1. Phone number presentation

Since China Telecom uses one phone number (163) for nationwide Internet access, most cities have the same Internet access number. Therefore a phone book is not currently required for the ChinaNet implementation. A web-based phone book will be added in a future software release in order to support nationwide ISP/CSP telephone numbers and HTTP server addresses.

6.2. Connection management

The current roaming client and server supports both PPP and SLIP.

6.3. Address assignment and routing

ChinaNet only supports dynamic IP address assignment for roaming users. In addition, static addresses are supported for users authenticating within their home province.

6.4. Authentication

When user accesses a local NAS, it provides its userID either as "username" or "username@realm". The NAS will pass the userID and password to the RADIUS proxy/server. If the "username" notation is used, the Radius proxy/server will assume that the user is a local user and will handle local authentication accordingly. If "username@realm" is used, the RADIUS proxy/server will process it as a roaming request.

When the RADIUS proxy/server handles a request from a roaming user, it will first check the cache to see if the user information is already stored there. If there is a cache hit, the RADIUS proxy/server do the local authentication accordingly. If it does not find user information in its cache, it will act as a proxy, forwarding the authentication request to the home RADIUS server. When the home RADIUS server responds, the local server will forward the response to the NAS. If the user is authenticated by the home server, the local RADIUS proxy will cache the user information for a period of time (3 days by default).

Caching is used to avoid frequent proxying of requests and responses between the local RADIUS proxy and the home RADIUS server. When the home RADIUS server sends back a valid authentication response, the local RADIUS proxy/server will cache the user information for a period of time (3 days by default). When the user next authenticates directly against the home RADIUS server, the home RADIUS server will send a request to the local server or servers to clear the user's information from the cache.

6.4.1. Extended hierarchy

In some provinces, the local telecommunications administration (Provincial ISP) further delegates control to county access nodes, creating another level of hierarchy. This is done to improve scalability and to avoid having the provincial ISP databases grow too large. In the current implementation, each provincial ISP maintains its own central RADIUS server, including information on all users in the province, while county nodes maintain distributed RADIUS servers. For intra-province roaming requests the local RADIUS proxy/server will directly forward the request to the home RADIUS server.

However, for inter-province roaming requests, the local RADIUS server does not forward the request directly to the home RADIUS server. Instead, the request is forwarded to the central provincial RADIUS server for the home province. This implementation is suitable only when county level ISPs do not mind combining and sharing their user information. In this instance, this is acceptable, since all county level ISPs are part of China Telecom. In a future release, this multi-layer hierarchy will be implemented using multi-layer proxy RADIUS, in a manner more resembling DNS.

6.5. Security

Encryption is used between the local RADIUS proxy/server and the home RADIUS server. Public/Private key encryption will be supported in the next release. IP tunneling and token card support is under consideration.

6.6. Accounting

Accounting information is transferred between the local RADIUS accounting proxy/server and home RADIUS accounting server. Every day each node sends a summary accounting information record to a central server in order to support nationwide settlement. The central server is run by the central Data Communication Bureau of China Telecom. Every month the central server sends the settlement bill to the provincial ISPs.

6.7. Inter-ISP/CSP roaming

ChinaNet supports both ISP and CSP (Content Service Provider) roaming on its system. For example, Shanghai Online, a Web-based commercial content service, uses RADIUS for authentication of ChinaNet users who do not have a Shanghai Online account. In order to support this, the Shanghai Online servers function as a RADIUS client authenticating against the home RADIUS server. When users access a protected document on the HTTP server, they are prompted to send a username/password for authentication. The user then responds with their userID in "user-name@realm" notation.

A CGI script on the HTTP server then acts as a RADIUS authentication client, sending the request to the home RADIUS server. After the home RADIUS server responds, the CGI script passes the information to the local authentication agent. From this point forward, everything is taken care of by the local Web authentication mechanism.

7. Microsoft implementation

Microsoft's roaming implementation was originally developed in order to support the Microsoft Network (MSN), which now offers Internet access in seven countries: US, Canada, France, Germany, UK, Japan, and Australia. In each of these countries, service is offered in cooperation with access partners. Since users are able to connect to the access partner networks while maintaining a customer-vendor relationship with MSN, this implementation fits within the definition of roaming as used in this document.

7.1. Implementation overview

The first version of the Microsoft roaming software was deployed by the MSN partners in April, 1996. This version included a Phone Book manager tool running under Windows 95, as well as a RADIUS server/proxy implementation running under Windows NT; TACACS+ is

currently not supported. Additional components now under development include a Connection Manager client for Windows 95 as well as an HTTP-based phone book server for Windows NT. The Phone Book manager tool is also being upgraded to provide for more automated phone book compilation.

7.2. Phone number presentation

The Connection Manager is responsible for the presentation and updating of phone numbers, as well as for dialing and making connections. In order to select phone numbers, users are asked to select the desired country and region/state. Phone numbers are then presented in the area selected. The primary numbers are those from the users service provider which match the service type (Analog, ISDN, Analog & IDN), country and region/state selected. The other numbers (selected clicking on the More button) are those for other service providers that have a roaming agreement with the users service provider.

7.2.1. Cost data

Cost data is not presented to users along with the phone numbers. However, such information may be made available by other means, such as via a Web page.

7.2.2. Default phone book format

The Connection Manager supports the ability to customize the phone book format, and it is expected that many ISPs will make use of this capability. However, for those who wish to use it "off the shelf" a default phone book format is provided. The default phone book is comprised of several files, including:

- Service profile
- Phone Book
- Region file

The service profile provides information on a given service, which may be an isolated Internet Service Provider, or may represent a roaming consortium. The service profile, which is in .ini file format, is comprised of the following information:

- The name of the service
- The filename of the service's big icon
- The filename of the service's little icon
- A description of the service
- The service phone book filename

- The service phone book version number
- The service regions file
- The URL of the service phone book server
- The prefix used by the service (i.e. "MSN/aboba")
- The suffix or domain used by the service (i.e. "aboba@msn.com")
- Whether the user name is optional for the service
- Whether the password is optional for the service
- Maximum length of the user name for the service
- Maximum length of the password for the service
- Information on service password handling (lowercase, mixed case, etc.)
- Number of redials for this service
- Delay between redials for this service
- References to other service providers that have roaming agreements
- The service profile filenames for each of the references
- Mask and match phone book filters for each of the references
 - (these are 32 bit numbers that are applied against the capability flags in the phone book)
- The dial-up connection properties configuration
 - (this is the DUN connectoid name)

The phone book file is a comma delimited ASCII file containing the following data:

- Unique number identifying a particular record (Index)
- Country ID
- A zero-base index into the region file
- City
- Area code
- Local phone number
- Minimum Speed
- Maximum speed
- Capability Flags:
 - Bit 0: 0=Toll, 1=Toll free
 - Bit 1: 0=X25, 1=IP
 - Bit 2: 0=Analog, 1=No analog support
 - Bit 3: 0=no ISDN support, 1=ISDN
 - Bit 4: 0
 - Bit 5: 0
 - Bit 6: 0=No Internet access, 1=Internet access
 - Bit 7: 0=No signup access, 1=Signup access
 - Bit 8-31: reserved
- The filename of the dialup network file
 - (typically refers to a script associated with the number)

A sample phone book file is shown below:

```
65031,1,1,Aniston,205,5551212,2400,2400,1,0,myfile
200255,1,1,Auburn/Opelika,334,5551212,9600,28800,0,10,
200133,1,1,Birmingham,205,5551212,9600,28800,0,10,
130,1,1,Birmingham,205,3275411,9600,14400,9,0,yourfile
65034,1,1,Birmingham,205,3285719,9600,14400,1,0,myfile
```

7.2.3. Additional attributes

As described previously, it is likely that some ISPs will require additional phone number attributes or provider information beyond that supported in the default phone book format. Attributes of interest may vary between providers, or may arise as a result of the introduction of new technologies. As a result, the set of phone number attributes is likely to evolve over time, and extensibility in the phone book format is highly desirable.

For example, in addition to the attributes provided in the default phone book, the following additional attributes have been requested by customers:

- Multicast support flag
- External/internal flag (to differentiate display between the "internal" or "other" list box)
- Priority (for control of presentation order)
- Modem protocol capabilities (V.34, V.32bis, etc.)
- ISDN protocol capabilities (V.110, V.120, etc.)
- No password flag (for numbers using telephone-based billing)
- Provider name

7.2.4. Addition of information on providers

The default phone book does not provide a mechanism for display of information on the individual ISPs within the roaming consortium, only for the consortium as a whole. For example, the provider icons (big and little) are included in the service profile. The service description information is expected to contain the customer support number. However, this information cannot be provided on an individual basis for each of the members of a roaming consortium. Additional information useful on a per-provider basis would include:

- Provider voice phone number
- Provider icon
- Provider fax phone number
- Provider customer support phone number

7.3. Phone number exchange

Currently phone number exchange is not supported by the phone book server. As a result, in the MSN implementation, phone number exchange is handled manually. As new POPs come online, the numbers are forwarded to MSN, which tests the numbers and approves them for addition to the phone book server. Updated phone books are produced and loaded on the phone book server on a weekly basis.

7.4. Phone book compilation

The Phone Book Manager tool was created in order to make it easier for the access partners to create and update their phone books. It supports addition, removal, and editing of phone numbers, generating both a new phone book, as well as associated difference files.

With version 1 of the Phone Book Administration tool, phone books are compiled manually, and represent a concatenation of available numbers from all partners, with no policy application. With version 1, the updates are prepared by the partners and forwarded to MSN, which tests the numbers and approves them for addition to the phone book. The updates are then concatenated together to form the global update file.

The new version of the Phone Book Administration tool automates much of the phone book compilation process, making it possible for phone book compilation to be decentralized with each partner running their own phone book server. Partners can then maintain and test their individual phone books and post them on their own Phone Book Server.

7.5. Phone book update

There is a mechanism to download phone book deltas, as well as to download arbitrary executables which can perform more complex update processing. Digital signatures are only used on the downloading of executables, since only these represent a security threat - the Connection Manager client does not check for digital signatures on deltas because bogus deltas can't really cause any harm.

The Connection Manager updates the phone book each time the user logs on. This is accomplished via an HTTP GET request to the phone book server. When the server is examining the request, it can take into account things like the OS version on the client, the language on the client, the version of Connection Manager on the client, and the version of the phone book on the client, in order to determine what it wants to send back.

In the GET response, the phone book server responds with the difference files necessary to update the client's phone book to the latest version. The client then builds the new phone book by successively applying these difference files. This process results in the update of the entire phone book, and is simple enough to allow it to be easily implemented on a variety of HTTP servers, either as a CGI script or (on NT) as an ISAPI DLL.

The difference files used in the default phone book consist of a list of phone book entries, each uniquely identified by their index number. Additions consist of phone book entries with all the information filed in; deletions are signified by entries with all entries zeroed out. A sample difference file is shown below:

```
65031,1,1,Aniston,205,5551212,2400,2400,1,0,myfile
200255,1,1,Auburn/Opelika,334,5551212,9600,28800,0,10,
200133,0,0,0,0,0,0,0,0,0
130,1,1,Birmingham,205,5551211,9600,14400,9,0,yourfile
65034,1,1,Birmingham,205,5551210,9600,14400,1,0,myfile
```

7.6. Connection management

The Connection Manager can support any protocol which can be configured via use of Windows Dialup Networking, including PPP and SLIP running over IP. The default setting is for the IP address as well as the DNS server IP address to be assigned by the NAS. The DNS server assignment capability is described in [1].

7.7. Authentication

The Connection Manager client and RADIUS proxy/server both support suffix style notation (i.e. "aboba@msn.com"), as well as a prefix notation ("MSN/aboba").

The prefix notation was developed for use with NAS devices with small maximum userID lengths. For these devices the compactness of the prefix notation significantly increases the number of characters available for the userID field. However, as an increasing number of NAS devices are now supporting 253 octet userIDs (the maximum supported by RADIUS) the need for prefix notation is declining.

After receiving the userID from the Connection Manager client, the NAS device passes the userID/domain and password information (or in the case of CHAP, the challenge and the response) to the RADIUS

proxy. The RADIUS proxy then checks if the domain is authorized for roaming by examining a static configuration file. If the domain is authorized, the RADIUS proxy then forwards the request to the appropriate RADIUS server. The domain to server mapping is also made via a static configuration file.

While static configuration files work well for small roaming consortia, for larger consortia static configuration will become tedious. Potentially more scalable solutions include use of DNS SRV records for the domain to RADIUS server mapping.

7.8. NAS configuration/authorization

Although the attributes returned by the home RADIUS server may make sense to home NAS devices, the local NAS may be configured differently, or may be from a different vendor. As a result, it may be necessary for the RADIUS proxy to edit the attribute set returned by the home RADIUS server, in order to provide the local NAS with the appropriate configuration information. The editing occurs via attribute discard and insertion of attributes by the proxy.

Alternatively, the home RADIUS server may be configured not to return any network-specific attributes, and to allow these to be inserted by the local RADIUS proxy.

Attributes most likely to cause conflicts include:

Framed-IP-Address Framed-IP-Netmask Framed-Routing Framed-Route
Filter-Id Vendor-Specific Session-Timeout Idle-Timeout
Termination-Action

Conflicts relating to IP address assignment and routing are very common. Where dynamic address assignment is used, an IP address pool appropriate for the local NAS can be substituted for the IP address pool designated by the home RADIUS server.

However, not all address conflicts can be resolved by editing. In some cases, (i.e., assignment of a static network address for a LAN) it may not be possible for the local NAS to accept the home RADIUS server's address assignment, yet the roaming hosts may not be able to accept an alternative assignment.

Filter IDs also pose a problem. It is possible that the local NAS may not implement a filter corresponding to that designated by the home RADIUS server. Even if an equivalent filter is implemented, in order to guarantee correct operation, the proxy's configuration must track changes in the filter configurations of each of the members of the

roaming consortium. In practice this is likely to be unworkable. Direct upload of filter configuration is not a solution either, because of the wide variation in filter languages supported in today's NAS devices.

Since by definition vendor specific attributes have meaning only to devices created by that vendor, use of these attributes is problematic within a heterogeneous roaming consortium. While it is possible to edit these attributes, or even to discard them or allow them to be ignored, this may not always be acceptable. In cases where vendor specific attributes relate to security, it may not be acceptable for the proxy to modify or discard these attributes; the only acceptable action may be for the local NAS to drop the user. Unfortunately, RADIUS does not distinguish between mandatory and optional attributes, so that there is no way for the proxy to take guidance from the server.

Conflicts over session or idle timeouts may result if since both the local and home ISP feel the need to adjust these parameters. While the home ISP may wish to adjust the parameter to match the user's software, the local ISP may wish to adjust it to match its own service policy. As long as the desired parameters do not differ too greatly, a compromise is often possible.

7.9. Address assignment and routing

While the Connection Manager software supports both static and dynamic address assignment, in the MSN implementation, all addresses are dynamically assigned.

However, selected partners also offer LAN connectivity to their customers, usually via static address assignment. However, these accounts do not have roaming privileges since no mechanism has been put in place for allowing these static routes to move between providers.

Users looking to do LAN roaming between providers are encouraged to select a router supporting Network Address Translation (NAT). NAT versions implemented in several low-end routers are compatible with the dynamic addressing used on MSN, as well as supporting DHCP on the LAN side.

7.10. Security

The RADIUS proxy/server implementation does not support token cards or tunneling protocols.

7.11. Accounting

In the MSN roaming implementation, the accounting data exchange process is specified in terms of an accounting record format, and a method by which the records are transferred from the partners to MSN, which acts as the settlement agent. Defining the interaction in terms of record formats and transfer protocols implies that the partners do not communicate with the settlement agent using NAS accounting protocols. As a result, accounting protocol interoperability is not be required.

However, for this advantage to be fully realized, it is necessary for the accounting record format to be extensible. This makes it more likely that the format can be adapted for use with the wide variety of accounting protocols in current use (such as SNMP, syslog, RADIUS, and TACACS+), as well as future protocols. After all, if the record format cannot express the metrics provided by a particular partner's accounting protocol, then the record format will not be of much use for a heterogeneous roaming consortium.

7.11.1. Accounting record format

The Microsoft RADIUS proxy/server supports the ability to customize the accounting record format, and it is expected that some ISPs will make use of this capability. However for those who want to use it "off the shelf" a default accounting record format is provided. The accounting record includes information provided by RADIUS:

- User Name (String; the user's ID, including prefix or suffix)
- NAS IP address (Integer; the IP address of the user's NAS)
- NAS Port (Integer; identifies the physical port on the NAS)
- Service Type (Integer; identifies the service provided to the user)
- NAS Identifier (Integer; unique identifier for the NAS)
- Status Type (Integer; indicates session start and stop, as well as accounting on and off)
- Delay Time (Integer; time client has been trying to send)
- Input Octets (Integer; in stop record, octets received from port)
- Output Octets (Integer; in stop record, octets sent to port)
- Session ID (Integer; unique ID linking start and stop records)
- Authentication (Integer; indicates how user was authenticated)
- Session Time (Integer; in stop record, seconds of received service)
- Input Packets (Integer; in stop record, packets received from port)
- Output Packets (Integer; in stop record, packets sent to port)
- Termination Cause (Integer; in stop record, indicates termination cause)
- Multi-Session ID (String; for linking of multiple related sessions)
- Link Count (Integer; number of links up when record was generated)
- NAS Port Type (Integer; indicates async vs. sync ISDN, V.120, etc.)

However, since this default format is not extensible, it cannot easily be adapted to protocols other than RADIUS, services other than dialup (i.e. dedicated connections) or rated events (i.e. file downloads). This is a serious limitation, and as a result, customers have requested a more general accounting record format.

7.11.2. Transfer mechanism

Prior to being transferred, the accounting records are compressed so as to save bandwidth. The transfer of accounting records is handled via FTP, with the transfer being initiated by the receiving party, rather than by the sending party. A duplicate set of records is kept by the local ISP for verification purposes.

8. Merit Network Implementation

8.1. Overview

MichNet is a regional IP backbone network operated within the state of Michigan by Merit Network, Inc., a nonprofit corporation based in Ann Arbor, Michigan. Started in 1966, MichNet currently provides backbone level Internet connectivity and dial-in IP services to its member and affiliate universities, colleges, K-12 schools, libraries, government institutions, other nonprofit organizations, and commercial business entities.

As of May 1, 1997, MichNet had 11 members and 405 affiliates. Its shared dial-in service operated 133 sites in Michigan and one in Washington, D.C, with 4774 dial-in lines. Additional dial-in lines and sites are being installed daily.

MichNet also provides national and international dial-in services to its members and affiliates through an 800 number and other external services contracting with national and global service providers.

The phone numbers of all MichNet shared dial-in sites are published both on the Merit web site and in the MichNet newsletters. Merit also provides links to information about the national and international service sites through their respective providers' web sites. Such information can be found at <http://www.merit.edu/mich-net/shared.dialin/>.

8.1.1. MichNet State-Wide Shared Dial-In Services

Each MichNet shared dial-in service site is owned and maintained by either Merit or by a member or affiliate organization. All sites must support PPP and Telnet connections.

Each organization participating in the shared dial-in service is assigned a realm-name. Typically the realm-name resembles a fully qualified domain name. Users accessing the shared dial-in service identify themselves by using a MichNet AccessID which consists of their local id concatenated with "@" followed by the realm-name - e.g. user@realm

Merit operates a set of Authentication, Authorization and Accounting (AAA) servers supporting the RADIUS protocol which are called core servers. The core servers support all the dial-in service sites and act as proxy servers to other AAA servers running at the participating organizations. For security reasons, Merit staff run all core servers; in particular, the user password is in the clear when the proxy core server decodes an incoming request and then re-encodes it and forwards it out again,

The core servers also enforce a common policy among all dial-in servers. The most important policy is that each provider of access must make dial-in ports available to others when the provider's own users do not have a need for them. To implement this policy, the proxy server distinguishes between realms that are owners and realms that are guests.

One piece of the policy determining whether the provider's organization has need of the port, is implemented by having the proxy core server track the realms associated with each of the sessions connected at a particular huntgroup. If there are few ports available (where few is determined by a formula) then guests are denied access. Guests are also assigned a time limit and their sessions are terminated after some amount of time (currently one hour during prime time, two hours during non-prime time).

The other part of the policy is to limit the number of guests that are allowed to connect. This is done by limiting the number of simultaneous guest sessions for realms. Each realm is allocated a number of "simultaneous access tokens" - SATs. When a guest session is authorized the end server for the realm decrements the count of available SATs, and when the session is terminated the count of SATs is incremented. A Merit specific attribute is added to the request by the core if the session will be a "guest" and will require a SAT. The end server must include a reply with an attribute containing the name of the "token pool" from which the token for this session is taken. The effect of this is to limit the number of guests connected to the network to the total number of tokens allocated to all realms.

Each realm is authenticated and authorized by its own AAA server. The proxy core servers forward requests to the appropriate server based on a configuration file showing where each realm is to be authenticated. Requests from realms not in the configuration are dropped.

The Merit AAA server software supports this policy. Merit provides this software to member and affiliate organizations. The software is designed to work with many existing authentication servers, such as Kerberos IV, UNIX password, TACACS, TACACS+, and RADIUS. This enables most institutions to utilize the authentication mechanism they have in place.

8.1.2. MichNet National and International Dial-In Services

In addition to the MichNet shared dial-in service, Merit also provides access from locations outside of Michigan by interconnecting with other dial-in services. These services are typically billed by connect time. Merit acts as the accounting agent between its member and affiliate organizations and the outside service provider.

The services currently supported are a national 800 number and service via the ADP/Autonet dial-in network. Connection with IBM/Advantis is being tested, and several other service interconnects are being investigated.

Calls placed by a Merit member/affiliate user to these external dial-in services are authenticated by having each of those services forward RADIUS authentication requests and accounting messages to a Merit proxy core server. The core forwards the requests to the member/affiliate server for approval. Session records are logged at the Merit core server and at the member/affiliate server. Merit bills members/affiliates monthly, based on processing of the accounting logs. The members and affiliates are responsible for rebilling their users.

The Merit AAA software supports the ability to request positive confirmation of acceptance of charges, and provides tools for accumulating and reporting on use by realm and by user.

8.2. Authentication and Authorization

Authentication of a Telnet session is supported using the traditional id and password method, with the id being a MichNet AccessID of the form user@realm, while a PPP session may be authenticated either using an AccessID and password within a script, or using PAP. Support for challenge/response authentication mechanisms using EAP is under development.

When a user dials into a MichNet shared dial-in port, the NAS sends an Access-Request to a core AAA server using the RADIUS protocol. First the core server applies any appropriate huntgroup access policies to the request. If the Request fails the policy check, an Access-Reject is returned to the NAS. Otherwise, the core server forwards it to the user's home authentication server according to the user's realm. The home authentication server authenticates and authorizes the access request. An Access-Accept or Access-Reject is sent back to the core server. If an Access-Accept is sent, the home server will create a dial-in session identifier which is unique to this session and insert it in a Class attribute in the Access-Accept. The core server looks at the request and the response from the home server again and decides either to accept or reject the request. Finally, the core server sends either an Access-Accept or Access-Reject to the NAS.

When a user dials into a contracted ISP's huntgroup (MichNet National and International Service), the ISP sends a RADIUS access request to a Merit core server. The rest of the authentication and authorization path is the same as in the shared dial-in service, except that no huntgroup access policy is applied but a Huntgroup-Service attribute is sent to the home authentication server with its value being the name of the service, and a copy of the attribute must be returned by the home server with a flag appended to the original value to indicate a positive authorization of user access to the specified service.

The MichNet shared dial-in service typically requires authorization of some sort, for example, a user dialing into a huntgroup as a guest must be authorized with a token from the user's realm. Participating institutions have control in defining authorization rules. Currently authorization may be done using any combination of the user's group status and user's account status. A set of programming interfaces is also provided for incorporating new authorization policies.

8.3. Accounting

In the Merit AAA server, a session is defined as starting from the moment the user connects to the NAS, and ending at the point when the user disconnects. During the course of a session, both the core server and the home server maintain status information about the session. This allows the AAA servers to apply policies based on the current status, e.g. limit guest access by realm to number of

available tokens, or to limit number of simultaneous sessions for a given AccessID. Information such as whether the session is for a guest, whether it used a token, and other information is included with the accounting stop information when it is logged. Merit has made enhancements to the RADIUS protocol, that are local to the AAA server, to support maintenance of session status information.

When a user session is successfully authenticated, the NAS sends out a RADIUS accounting start request to the core server. The core server forwards that request to the user's home server. The home server updates the status of the session and then responds to the core. The core server in turn responds to the NAS. In the accounting Start request, a NAS conforming to the RADIUS specification must return the Class attribute and value it received in the Access-Accept for the session, thus sending back the dial-in session identifier created by the session's home server.

When a user ends a session, an accounting stop request is sent through the same path. The dial-in session identifier is again returned by the NAS, providing a means of uniquely identifying a session. By configuring the finite state machine in each of the AAA servers, any accounting requests may be logged by any of the servers where the accounting requests are received.

Because the same session logs are available on every server in the path of a session's authorization and accounting message, problems with reconciliation of specific sessions may be resolved easily. For the shared dial-in service, there are no usage charges. Merit has tools to verify that organizations do not authorize more guest sessions than the number of SATs allocated to the organization. For surcharged sessions, Merit sends each organization a summary bill each month. Files with detail session records are available for problem resolution. Each organization is responsible for billing its own users, and should have the same session records as are collected by Merit.

Merit receives a monthly invoice from other dial-in service providers and pays them directly, after first verifying that the charges correspond to the session records logged by Merit.

8.4. Software and Development

Merit has developed the AAA server software which supports the above capabilities initially by modifying the RADIUS server provided by Livingston, and later by doing a nearly total rewrite of the software to make enhancement and extension of capabilities easier. Merit makes a basic version of its server freely available for noncommercial use.

Merit has started the Merit AAA Server Consortium which consists of Merit and a number of NAS vendors, ISPs and server software vendors. The consortium supports ongoing development of the Merit AAA server. The goal is to build a server that supports proxy as well as end server capabilities, that is feature rich, and that interoperates with major vendors' NAS products.

The building block of the Merit AAA server, the Authentication/Authorization Transfer Vector (AATV), is a very powerful concept that enables the ultimate modularity and flexibility of the AAA server. The structure and methods of the AATV model are published with all versions of the AAA server.

Objects for extending the authorization server are also available in the enhanced version of the AAA server. Merit is also looking at ways to provide a method of extending the AAA server in its executable form, to improve the server efficiency and scalability, and to provide better monitoring, instrumentation and administration of the server.

9. FidoNet implementation

Since its birth in 1984, FidoNet has supported phone book synchronization among its member nodes, which now number approximately 35,000. As a non-IP dialup network, FidoNet does not provide IP services to members, and does not utilize IP-based authentication technology. Instead member nodes offer bulletin-board services, including access to mail and conferences known as echoes.

In order to be able to communicate with each other, FidoNet member systems require a synchronized phone book, known as the Nodelist. The purpose of the Nodelist is to enable resolution of FidoNet addresses (expressed in the form zone:network/node, or 1:161/445) to phone numbers. As a dialup network, FidoNet requires phone numbers in order to be deliver mail and conference traffic.

In order to minimize the effort required in regularly synchronizing a phone book of 35,000 entries, the weekly Nodelist updates are transmitted as difference files. These difference files, known as the Nodediff, produce the Nodelist for the current week when applied to the previous week's Nodelist. In order to minimize transfer time, Nodediffs are compressed prior to transfer.

Information on FidoNet, as well as FidoNet Technical Standards (FTS) documents (including the Nodelist specification) and standards proposals are available from the FidoNet archive at <http://www.fidonet.org/>.

9.1. Scaling issues

With a Nodelist of 35,000 entries, the FidoNet Nodelist is now 3.1 MB in size, and the weekly Nodediffs are 175 KB. In compressed form, the Nodelist is approximately 1 MB, and the weekly Nodediff is 90 KB. As a result, the transfer of the Nodediff takes approximately 45 seconds using a 28,800 bps modem.

In order to improve scalability, the implementation of a domain name service approach is examined in [8]. The proposal envisages use of a capability analagous to the DNS ISDN record in order to map names to phone numbers, coupled with an additional record to provide the attributes associated with a given name.

9.2. Phone number presentation

While FidoNet member systems perform hone book synchronization, users need only know the FidoNet address of the systems they wish to contact. As a result users do not need to maintain copies of the Nodelist on their own systems. This is similar to the Internet, where the DNS takes care of the domain name to IP address mapping, so that users do not have to remember IP addresses.

Nevertheless, FidoNet systems often find it useful to be able to present lists of nodes, and as a result, FidoNet Nodelist compilers typically produce a representation of the Nodelist that can be searched or displayed online, as well as one that is used by the system dialer.

9.2.1. FidoNet Nodelist format

The FidoNet Nodelist format is documented in detail in [3]. The Nodelist file consists of lines of data as well as comment lines, which begin with a semi-colon. The first line of the Nodelist is a general interest comment line that includes the date and the day number, as well as a 16-bit CRC. The CRC is included so as to allow the system assembling the new Nodelist to verify its integrity.

Each Nodelist data line contains eight comma separated fields:

- Keyword
- Zone/Region/Net/Node number
- Node name
- Location
- Sysop name
- Phone number
- Maximum Baud rate
- Flags (optional)

FidoNet Nodelists are arranged geographically, with systems in the same zone, region, and network being grouped together. As a result, FidoNet Nodelists do not require a separate regions file. Among other things, the keyword field can be used to indicate that a system is temporarily out of service.

Reference [3] discusses Nodelist flags in considerable detail. Among other things, the flags include information on supported modem modulation and error correction protocols. Reference [4] also proposes a series of ISDN capability flags, and [5] proposes flags to indicate times of system availability.

9.3. Phone number exchange

FidoNet coordinators are responsible for maintaining up to date information on their networks, regions, and zones. Every week network coordinators submit to their regional coordinators updated versions of their portions of the Nodelist. The regional coordinators then compile the submissions from their network coordinators, and submit them to the zone coordinator. The zone coordinators then exchange their submissions to produce the new Nodelist. As a result, it is possible that the view from different zones may differ at any given time.

9.3.1. The Nodediff

The format of the Nodediff is discussed in detail in [3]. In preparing the Nodediffs, network coordinators may transmit only their difference updates, which can be collated to produce the Nodediff directly.

One weakness in the current approach is that there is no security applied to the coordinator submissions. This leaves open the possibility of propagation of fraudulent updates. In order to address this, [6] proposes addition of a shared secret to the update files.

9.3.2. Addition of nodes

In order to apply for allocation of a FidoNet address and membership in the Nodelist, systems must demonstrate that they are functioning by sending mail to the local network coordinator. Once the local network coordinator receives the application, they then allocate a new FidoNet address, and add a Nodelist entry.

9.3.3. Deletion of nodes

Since FidoNet nodes are required to be functioning during the zone mail hour in order to receive mail, and since nodes receive the weekly Nodelist from their local network coordinators on a weekly basis, there is a built-in mechanism for discovery of non-functional nodes.

Nodes found to be down are reported to the local network coordinator and subsequently marked as down within the Nodelist. Nodes remaining down for more than two weeks may be removed from the Nodelist, at the discretion of the network coordinator.

9.4. Phone book update

The Nodelist contains the phone numbers and associated attributes of each participating system. New Nodestats become available on Fridays, and are made available to participating systems by their local network coordinators, who in turn receive them from the regional and zone coordinators.

While it is standard practice for participating systems to get their Nodestats from their local network coordinators, should the local network coordinator not be available for some reason, either the updates or the complete Nodelist may be picked up from other network, or regional coordinators. Please note that since the view from different zones may differ, nodes wishing to update their Nodestats should not contact systems from outside their zone.

9.5. Phone book compilation

Once FidoNet systems have received the Nodediff, they apply it to the previous week's Nodelist in order to prepare a new Nodelist. In order to receive Nodediffs and compile the Nodelist, the following software is required:

- A FidoNet-compatible mailer implementation, used to transfer files
- A Nodelist compiler

One of the purposes of the Nodelist compiler is to apply Nodediffs to the previous Nodelist in order to produce an updated Nodelist. The other purpose is to compile the updated Nodelist into the format required by the particular mailer implementation used by the member system. It is important to note that while the Nodelist and Nodediff formats are standardized (FTS-0005), as is the file transfer protocol (FTS-0001), the compiled format used by each mailer is implementation dependent.

One reason that compiled formats to differ is the addition of out of band information to the Nodelist during the compilation process. Added information includes phone call costs as well as shared secrets.

9.5.1. Cost data

Although cost information is not part of the Nodelist, in compiling the Nodelist into the format used by the mailer, Nodelist compilers support the addition of cost information. This information is then subsequently used to guide mailer behavior.

Since phone call costs depend on the rates charged by the local phone company, this information is local in nature and is typically entered into the Nodelist compiler's configuration file by the system administrator.

9.5.2. Shared secrets

In FidoNet, shared secrets are used for authenticated sessions between systems. Such authenticated sessions are particularly important between the local, regional and zone coordinators who handle preparation and transmission of the Nodediffs. A single shared secret is used per system.

9.6. Accounting

Within FidoNet, the need for accounting arises primarily from the need of local, regional and zone coordinators to be reimbursed for their expenses. In order to support this, utilities have been developed to account for network usage at the system level according to various metrics. However, the accounting techniques are not applied at the user level. Distributed authentication and accounting are not implemented and therefore users may not roam between systems.

10. Acknowledgements

Thanks to Glen Zorn of Microsoft and Lynn Liu and Tao Wang of AimQuest for useful discussions of this problem space.

Security Considerations

Security issues are discussed in sections 5.6 and 6.5.

11. References

- [1] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", RFC 1877, Microsoft, December 1995.
- [2] Fielding, R., et al., "Hypertext Transfer Protocol - HTTP/1.1.", RFC 2068, UC Irvine, January, 1997.
- [3] Baker, B., R. Moore, D. Nugent. "The Distribution Nodelist." FTS-0005, February, 1996.
- [4] Lentz, A. "ISDN Nodelist flags." FSC-0091, June, 1996.
- [5] Thomas, D. J. "A Proposed Nodelist flag indicating Online Times of a Node." FSC-0062, April, 1996.
- [6] Kolin, L. "Security Passwords in Nodelist Update Files." FSC-0055, March, 1991.
- [7] Gwinn, R., D. Dodell. "Nodelist Flag Changes Draft Document." FSC-0009, November, 1987.
- [8] Heller, R. "A Proposal for A FidoNet Domain Name Service." FSC-0069, December, 1992.
- [9] Rigney, C., Rubens, A., Simpson, W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2058, Livingston, Merit, Daydreamer, January 1997.
- [10] Rigney, C., "RADIUS Accounting", RFC 2059, Livingston, January 1997.

12. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 206-936-6605
EMail: bernarda@microsoft.com

Juan Lu
AimQuest Corporation
1381 McCarthy Blvd.
Milpitas, California 95035

Phone: 408-273-2730 ext. 2762
EMail: juanlu@aimnet.net

John Alsop
i-Pass Alliance Inc.
650 Castro St., Suite 280
Mountain View, CA 94041

Phone: 415-968-2200
Fax: 415-968-2266
EMail: jalsop@ipass.com

James Ding
Asiainfo
One Galleria Tower
13355 Noel Road, #1340
Dallas, TX 75240

Phone: 214-788-4141
Fax: 214-788-0729
EMail: ding@bjai.asiainfo.com

Wei Wang
Merit Network, Inc.
4251 Plymouth Rd., Suite C
Ann Arbor, MI 48105-2785

Phone: 313-764-2874
EMail: weiwang@merit.edu